



UNIVERSIDAD TÉCNICA DE AMBATO
FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E
INDUSTRIAL

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES
E INFORMÁTICOS

Tema:

ANÁLISIS DE VULNERABILIDADES MEDIANTE PRUEBAS DE PENETRACIÓN
EN LOS SERVIDORES DEL DEPARTAMENTO FINANCIERO DE LA EMPRESA
ELÉCTRICA AMBATO REGIONAL CENTRO NORTE S.A.

Trabajo de Titulación Modalidad: Proyecto de Investigación, presentado previo a la
obtención del título de Ingeniera en Sistemas Computacionales e Informáticos

ÁREA: Seguridad Informática

LÍNEA DE INVESTIGACIÓN: Sistemas administradores de recursos

AUTOR: Rosana Emperatriz Ruilova Romero

TUTOR: Ing. Edwin Hernando Buenaño Valencia, Mg.

Ambato – Ecuador

agosto - 2024

APROBACIÓN DEL TUTOR

En calidad de Tutor del Trabajo de Titulación con el tema: ANÁLISIS DE VULNERABILIDADES MEDIANTE PRUEBAS DE PENETRACIÓN EN LOS SERVIDORES DEL DEPARTAMENTO FINANCIERO DE LA EMPRESA ELÉCTRICA AMBATO REGIONAL CENTRO NORTE S.A., desarrollado bajo la modalidad Proyecto de Investigación por la señora Rosana Emperatriz Ruilova Romero, estudiante de la Carrera de Ingeniería en Sistemas Computacionales e Informáticos, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, me permito indicar que la estudiante ha sido tutorada durante todo el desarrollo del trabajo hasta la conclusión, de acuerdo a lo dispuesto en el Artículo 15 de Reglamento para obtener el Título de Tercer Nivel, de Grado de la Universidad Técnica de Ambato, y el numeral 7.4 del respectivo instructivo.

Ambato , agosto 2024



Firmado electrónicamente por:
EDWIN HERNANDO
BUENANO VALENCIA

Ing. Edwin Hernando Buenaño Valencia, Mg.

TUTOR

AUTORÍA

El presente Proyecto de Titulación: ANÁLISIS DE VULNERABILIDADES MEDIANTE PRUEBAS DE PENETRACIÓN EN LOS SERVIDORES DEL DEPARTAMENTO FINANCIERO DE LA EMPRESA ELÉCTRICA AMBATO REGIONAL CENTRO NORTE S.A., es absolutamente original, auténtico y personal. En tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, agosto 2024



Rosana Emperatriz Ruilova Romero

C.C 070575618-7

AUTOR

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que haga uso de este Trabajo de Titulación como un documento disponible para la lectura, consulta y procesos de investigación.

Cedo los derechos de mi Trabajo de Titulación en favor de la Universidad Técnica de Ambato, con fines de difusión pública. Además, autorizo su reproducción total o parcial dentro de las regulaciones de la institución.

Ambato, agosto 2024



Rosana Emperatriz Ruilova Romero

C.C 070575618-7

AUTOR

APROBACIÓN TRIBUNAL DE GRADO

En calidad de par calificador del Informe Final del Trabajo de Titulación presentado por la señora Rosana Emperatriz Ruilova Romero estudiante de la Carrera de Ingeniería en Sistemas Computacionales e Informáticos, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, bajo la Modalidad Proyecto de Investigación, titulado ANÁLISIS DE VULNERABILIDADES MEDIANTE PRUEBAS DE PENETRACIÓN EN LOS SERVIDORES DEL DEPARTAMENTO FINANCIERO DE LA EMPRESA ELÉCTRICA AMBATO REGIONAL CENTRO NORTE S.A., nos permitimos informar que el trabajo a sido revisado y calificado de acuerdo al Artículo 17 del Reglamento para obtener el Título de Tercer Nivel, de Grado de la Universidad Técnica de Ambato, y al numeral 7.6 del respectivo instructivo. Para cuya constancia suscribimos, conjuntamente con la señora Presidenta de Tribunal

Ambato, agosto 2024



Firmado electrónicamente por:
ELSA PILAR URRUTIA
URRUTIA

Ing. Pilar Urrutia, Mg.

PRESIDENTE DEL TRIBUNAL



Firmado electrónicamente por:
PABLO ISRAEL
MORALES PAREDES

Ing. Pablo Israel Morales Paredes, Mg.
PROFESOR CALIFICADOR



Firmado electrónicamente por:
LEONARDO DAVID
TORRES VALVERDE

Ing. Leonardo David Torres Valverde, Mg
PROFESOR CALIFICADOR

DEDICATORIA

El presente proyecto de investigación se lo dedico a mi amado esposo y a mis hijos que han sido un pilar fundamental en mi vida. Este logro es tanto mío como suyo.

A mis padres y a mi abuelita, que aunque ya no están conmigo, siguen siendo mi guía y mi inspiración. Todo lo que soy y lo que he logrado se lo debo a sus enseñanzas y amor incondicional. Gracias por todo lo que me dieron y por los valores que me inculcaron. Los llevo siempre en mi corazón.

Rosana Emperatriz Ruilova Romero

AGRADECIMIENTO

Agradezco a Dios por su infinita misericordia y por guiarme en cada paso de este camino. A mi esposo por siempre darme su apoyo incondicional.

A mi tutor, el Ingeniero Hernando Buenaño, por su apoyo brindado.

A los docentes de la carrera por compartir su conocimiento.

Rosana Emperatriz Ruilova Romero

ÍNDICE GENERAL DE CONTENIDOS

APROBACIÓN DEL TUTOR.....	ii
AUTORÍA.....	iii
DERECHOS DE AUTOR.....	iv
APROBACIÓN TRIBUNAL DE GRADO	v
DEDICATORIA	vi
AGRADECIMIENTO	vii
RESUMEN EJECUTIVO	xx
ABSTRACT	xxi
CAPÍTULO I.....	1
MARCO TEÓRICO	1
1.1 Tema de investigación.....	1
1.2 Antecedentes Investigativos.....	1
1.2.1 Contextualización del problema.....	2
1.2.2 Fundamentación teórica	3
1.2.2.1 Seguridad Informática	3
1.2.2.2 Riesgo Informático.....	4
1.2.2.3 Vulnerabilidades.....	6
1.2.2.3.1 Top Ten de Vulnerabilidades	7
1.2.2.4 Amenazas	8
1.2.2.4.1 Tipos de Amenazas.....	9
1.2.2.5 Hacking Ético.....	9
1.2.2.6 Los Hackers.....	10
1.2.2.7 La Ciberseguridad	10
1.2.2.7.1 Tipos de Ciberataques	11
1.2.2.8 Pruebas de Penetración	13
1.2.2.8.1 Actividades de un Pentester	13

4.1.2.8.2	Tipos de Pruebas de Penetración.....	14
1.2.2.9	Fases de Pentesting	15
1.2.2.10	Herramientas de Pentesting.....	16
1.2.2.11	Ciclo de Deming	18
1.3	Objetivos	19
1.3.1	Objetivo General	19
1.3.2	Objetivos Específicos.....	19
CAPÍTULO II		20
METODOLOGÍA		20
2.1	Materiales.....	20
2.2	Métodos.....	23
2.2.1	Modalidad de Investigación	23
	Investigación bibliográfica y documental	23
	Investigación de campo.....	23
2.2.2	Población y Muestra.....	23
2.2.3	Recolección de Información	23
2.3	Procesamiento y Análisis de Datos	24
2.4	Desarrollo del Proyecto.....	24
1.	Identificar los servidores.	24
2.	Seleccionar las herramientas de la investigación.	24
3.	Realizar pruebas de penetración.....	25
4.	Entregar el Informe detallado de las vulnerabilidades encontradas.....	25
CAPÍTULO III.....		26
RESULTADOS Y DISCUSIÓN		26
3.1	Análisis y discusión de resultados.....	26
3.1.1	Entrevista.....	26
3.1.2	Análisis e interpretación de resultados de la entrevista aplicada	29
3.2	Desarrollo de la Propuesta	30
3.2.1	Identificar los servidores.	30
3.2.1.1	Servidores del Departamento Financiero	30
3.2.1.2	Cuarto de Servidores	31
3.2.2	Seleccionar las herramientas de la investigación.	35

3.2.2.1 Herramientas de análisis de vulnerabilidades	35
3.2.2.2 Herramientas de explotación de vulnerabilidades.....	38
3.2.3 Realizar pruebas de penetración.....	39
3.2.3.1 Análisis de Vulnerabilidades con Nessus.....	39
3.2.3.2 Analisis de Vulnerabilidades con 11	115
3.2.3.3 Analisis de Vulnerabilidades con Nmap	122
3.2.4 Entregar el Informe detallado de las vulnerabilidades encontradas.....	130
CAPÍTULO IV	180
CONCLUSIONES Y RECOMENDACIONES	180
4.1 Conclusiones	180
4.2 Recomendaciones.....	181
BIBLIOGRAFÍA	183
ANEXOS	188
ANEXO A	189
ANEXO B.....	190
ANEXO C	191
ANEXO D.....	192
ANEXO E	197
ANEXO F	199
ANEXO G.....	202

ÍNDICE DE FIGURAS

Figura 1.1: Riesgo Informático	4
Figura 1.2: Fases de Pentesting	15
Figura 1.3: Ciclo de Deming	19
Figura 3.1: Ciclo de Deming Aplicado a la Investigación	30
Figura 3.2: Acceso al cuarto del centro de cómputo Matriz	32
Figura 3.3: Centro de cómputo Matriz.....	33
Figura 3.4: Circuito de Alarma cotra incendios y control de la puerta de acceso.....	33
Figura 3.5: Alarma de aire del Centro de cómputo Matriz	34
Figura 3.6: Rack de Servidores del Departamento Financiero en el Centro de cómputo Matriz	34
Figura 3.7: Interfaz de Nessus.....	40
Figura 3.8: Carpetas para realizar el analisis de vulnerabilidades	40
Figura 3.9: Interfaz Nessus, crear New Scan	40
Figura 3.10: Interfaz Nessus, Template de Scan para análisis de vulnerabilidades	41
Figura 3.11: Interfaz Nessus, Configuración del scaneo con la ip del servidor.....	41
Figura 3.12: Vulnerabilidades SSL Certificate Signed Using Weak Hashing Algorithm	42
Figura 3.13: Vulnerabilidades SSL Medium Strength Cipher Suites Supported (SWEET32).....	43
Figura 3.14: Vulnerabilidades SSL Certificate Cannot Be Trusted.....	44
Figura 3.15: Vulnerabilidades Terminal Services Doesn't use Network Level Authentication (NLA) Only	45
Figura 3.16: Vulnerabilidades TLS version 1.1 Deprecated Protocol.....	46
Figura 3.17: Vulnerabilidades SSL Medium Strenght Cipher Suites Supported	47
Figura 3.18: Vulnerabilidades SSL Certificate Cannot Be Trusted.....	48

Figura 3.19: Vulnerabilidades SSL Certificate with Wrong Hostname	49
Figura 3.20: Vulnerabilidades SMB Signing not required.....	50
Figura 3.21: Vulnerabilidades SSL Certificate Cannot Be Trusted.....	51
Figura 3.22: Vulnerabilidades SSL Certificate with Wrong Hostname	52
Figura 3.23: Vulnerabilidades mDNS Detection	53
Figura 3.24: Vulnerabilidades phpMyAdmin 4.x < 4.9.4 / 5.x < 5.0.1 SQLI.....	54
Figura 3.25: Vulnerabilidades Web Server Trasmits ClearText Credentials.....	55
Figura 3.26: Vulnerabilidades Treck TCP/IP stack multiple vulnerabilities.....	56
Figura 3.27: Vulnerabilidades Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)	57
Figura 3.28: Vulnerabilidades Oracle Database Unsupported Version Detection	58
Figura 3.29: Vulnerabilidades Unsupported Windows OS (remote)	59
Figura 3.30: Vulnerabilidades Oracle TNS Listener Remote	60
Figura 3.31: Vulnerabilidades SSL Certificate Signed Using Weak Hashing Algorithm	61
Figura 3.32: Vulnerabilidades SSL Medium Strength Cipher Suites Supported (SWEET32).....	62
Figura 3.33: Vulnerabilidades Remote Desktop Protocol Server Man-in-the-Middle Weakness.....	63
Figura 3.34: Vulnerabilidades SMB Signing not required.....	64
Figura 3.35: Vulnerabilidades SSL Certicate Cannot Be Trusted	65
Figura 3.36: Vulnerabilidades SSL Certicatewith Wrong Hostname.....	66
Figura 3.37: Vulnerabilidades SSL RC4 Cipher Suites Supported (Bar Mitzvah)	67
Figura 3.38: Vulnerabilidades Signed Certificate	68
Figura 3.39: Vulnerabilidades TLS Version 1.0 Protocol Detection.....	69
Figura 3.40: Vulnerabilidades TLS Version 1.1 Protocol Detection.....	70

Figura 3.41: Vulnerabilidades Terminal Services Doesn't Use Network Level Authentication (NLA) Only	71
Figura 3.42: Vulnerabilidades Terminal Services Encryption Level is Medium or Low.	72
Figura 3.43: Vulnerabilidades Terminal Services Encryption Level is not FIPS-140 Compliant.....	73
Figura 3.44: Vulnerabilidades SSL Certificate Signed Using Weak Hashing Algorithm	74
Figura 3.45: Vulnerabilidades SSL Medium Strength Cipher Suites Supported (SWEET32).....	75
Figura 3.46: Vulnerabilidades SSL Certificate Cannot Be Trusted.....	76
Figura 3.47: Vulnerabilidades SSL RC4 Cipher Suites Supported (Bar Mitzvah)	77
Figura 3.48: Vulnerabilidades SSL Self-Signed Certificate.....	78
Figura 3.49: Vulnerabilidades TLS Version 1.0 Protocol Detection	79
Figura 3.50: Vulnerabilidades TLS Version 1.1 Protocol Deprecated	80
Figura 3.51: Vulnerabilidades Terminal Services Doesn't Use Network Level Authentication (NLA) Only	81
Figura 3.52: Vulnerabilidades Unsupported Web Server Detection	82
Figura 3.53: Vulnerabilidades Unsupported Windows OS (remote)	83
Figura 3.54: Vulnerabilidades Oracle GlassFish Server Path Traversal	84
Figura 3.55: Vulnerabilidades Oracle GlassFish Server URL normalization Denial of Service.....	85
Figura 3.56: Vulnerabilidades Remote Desktop Protocol Server Man-in-the-Middle Weakness.....	86
Figura 3.57: Vulnerabilidades SMB Signing not required.....	87
Figura 3.58: Vulnerabilidades Terminal Services Doesn't use Network Level Authentication (NLA) Only	88
Figura 3.59: Vulnerabilidades Terminal Services Encryption Level is Medium or Low.	89

Figura 3.60: Vulnerabilidades Web Application Potentially Vulnerable to Clickjacking	90
Figura 3.61: Vulnerabilidades Web Server Allows Password Auto-Completion.....	91
Figura 3.62: Vulnerabilidades Web Server Transmits Cleartext Credentials.....	92
Figura 3.63: Vulnerabilidades Web Server Transmits Cleartext Credentials.....	93
Figura 3.64: Vulnerabilidades ESXi 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2021-0014)	94
Figura 3.65: Vulnerabilidades ESXi 7.0 / 8.0 Multiple Vulnerabilities (VMSA-2024-0006)	95
Figura 3.66: Vulnerabilidades ESXi 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2020-0026)	96
Figura 3.67: Vulnerabilidades ESXi 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2022-0004)	97
Figura 3.68: Vulnerabilidades ESXi 6.5 / 6.7 / 7.0 RCE (VMSA-2021-0002).....	98
Figura 3.69: Vulnerabilidades ESXi 7.0 DoS (VMSA-2020-0029)	99
Figura 3.70: Vulnerabilidades Vmware ESXi 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2022-0020).....	100
Figura 3.71: Vulnerabilidades Vmware ESXi 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2022-0016)	101
Figura 3.72: Vulnerabilidades SSL Certificate Cannot Be Trusted.....	102
Figura 3.73: Vulnerabilidades SSL Self-Signed Certificate.....	103
Figura 3.74: Vulnerabilidades Apache 2.4.x < 2.4.52 mod_lua Buffer Overflow	104
Figura 3.75: Vulnerabilidades Apache 2.4.x < 2.4.53 Multiple Vulnerabilities.....	105
Figura 3.76: Vulnerabilidades Apache 2.4.x < 2.4.54 Multiple Vulnerabilities.....	106
Figura 3.77: Vulnerabilidades Apache 2.4.x < 2.4.55 Multiple Vulnerabilities.....	107
Figura 3.78: Vulnerabilidades Apache 2.4.x < 2.4.56 Multiple Vulnerabilities.....	108

Figura 3.79: Vulnerabilidades Apache 2.4.x $\geq$ 2.4.7 / $<$ 2.4.52 Forward Proxy DoS / SSRF	109
Figura 3.80: Vulnerabilidades Apache 2.4.x $<$ 2.4.58 Multiple	110
Vulnerabilities	110
Figura 3.81: Vulnerabilidades Oracle WebLogic Server RCE (CVE-200-14882)	111
Figura 3.82: Vulnerabilidades HTTP TRACE / TRACK Methods Allowed	112
Figura 3.83: Vulnerabilidades SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795)	113
Figura 3.84: Vulnerabilidades Browsable Web Directories	114
Figura 3.85: Herramienta Dmitry SRV AD.....	115
Figura 3.86: Herramienta Dmitry SRV ILO.....	116
Figura 3.87: Herramienta Dmitry SRV NAS	117
Figura 3.88: Herramienta Dmitry SRV SIF PRINCIPAL	118
Figura 3.89: Herramienta Dmitry SRV PROCESO AUTOMÁTICO.....	119
Figura 3.90: Herramienta Dmitry SRV VMWARE.....	120
Figura 3.91: Herramienta Dmitry SRV VEAMBACKUP	121
Figura 3.92: Herramienta Dmitry SRV AIX	122
Figura 3.93: Nmap SRV AD	123
Figura 3.94: Nmap SRV ILO	124
Figura 3.95: Nmap SRV NAS	125
Figura 3.96: Nmap SRV SIF PRINCIPAL	126
Figura 3.97: Nmap SRV PROCESOS AUTOMATICOS	127
Figura 3.98: Nmap SRV VMWARE	128
Figura 3.99: Nmap SRV VEAMBACKUP	129
Figura 3.100: Nmap SRV AIX	130

Figura 3.101: Informe de Vulnerabilidades.....	131
Figura 3.102: Informe de Vulnerabilidades.....	132
Figura 3.103: Informe de Vulnerabilidades.....	133
Figura 3.104: Informe de Vulnerabilidades.....	134
Figura 3.105: Informe de Vulnerabilidades.....	135
Figura 3.106: Informe de Vulnerabilidades.....	136
Figura 3.107: Informe de Vulnerabilidades.....	137
Figura 3.108: Informe de Vulnerabilidades.....	138
Figura 3.109: Informe de Vulnerabilidades.....	139
Figura 3.110: Informe de Vulnerabilidades.....	140
Figura 3.111: Informe de Vulnerabilidades.....	141
Figura 3.112: Informe de Vulnerabilidades.....	142
Figura 3.113: Informe de Vulnerabilidades.....	143
Figura 3.114: Informe de Vulnerabilidades.....	144
Figura 3.115: Informe de Vulnerabilidades.....	145
Figura 3.116: Informe de Vulnerabilidades.....	146
Figura 3.117: Informe de Vulnerabilidades.....	147
Figura 3.118: Informe de Vulnerabilidades.....	148
Figura 3.119: Informe de Vulnerabilidades.....	149
Figura 3.120: Informe de Vulnerabilidades.....	150
Figura 3.121: Informe de Vulnerabilidades.....	151
Figura 3.122: Informe de Vulnerabilidades.....	152
Figura 3.123: Informe de Vulnerabilidades.....	153
Figura 3.124: Informe de Vulnerabilidades.....	154
Figura 3.125: Informe de Vulnerabilidades.....	155

Figura 3.126: Informe de Vulnerabilidades.....	156
Figura 3.127: Informe de Vulnerabilidades.....	157
Figura 3.128: Informe de Vulnerabilidades.....	158
Figura 3.129: Informe de Vulnerabilidades.....	159
Figura 3.130: Informe de Vulnerabilidades.....	160
Figura 3.131: Informe de Vulnerabilidades.....	161
Figura 3.132: Informe de Vulnerabilidades.....	162
Figura 3.133: Informe de Vulnerabilidades.....	163
Figura 3.134: Informe de Vulnerabilidades.....	164
Figura 3.135: Informe de Vulnerabilidades.....	165
Figura 3.136: Informe de Vulnerabilidades.....	166
Figura 3.137: Informe de Vulnerabilidades.....	167
Figura 3.138: Informe de Vulnerabilidades.....	168
Figura 3.139: Informe de Vulnerabilidades.....	169
Figura 3.140: Informe de Vulnerabilidades.....	170
Figura 3.141: Informe de Vulnerabilidades.....	171
Figura 3.142: Informe de Vulnerabilidades.....	172
Figura 3.143: Informe de Vulnerabilidades.....	173
Figura 3.145: Informe de Vulnerabilidades.....	175
Figura 3.146: Informe de Vulnerabilidades.....	176
Figura 3.147: Informe de Vulnerabilidades.....	177
Figura 3.148: Informe de Vulnerabilidades.....	178
Figura A.1: Carta compromiso de la Empresa Electrica Ambato Regional Centro Norte S.A. para realizar el proyecto de investigación.....	189

Figura B.1: Certificado de culminación de la Empresa Electrica Ambato Regional Centro Norte S.A.	190
Figura C.1: Normas y Políticas de Recursos Tecnológicos y de Seguridad.	191
Figura D.1: Plan de Contingencia Informática.	192
Figura D.2: Plan de Contingencia Informática.	193
Figura D.3: Plan de Contingencia Informática.	194
Figura D.4: Plan de Contingencia Informática.	195
Figura D.5: Plan de Contingencia Informática.	196
Figura E.1: Rack Servidores Departamento Financiero, parte delantera	197
Figura E.2: Parte superior servidor Synology NAS, parte inferior Servidor HP DL385	198
Figura E.3: Servidor HP ML350 generación 8	198
Figura F.1: Máquina Virtual de Kali Linux	199
Figura F.2: Instalación de Nessus.....	200
Figura F.3: Levantar el Servicio de Nessus.....	200
Figura F.4: Registro de Nessus Essential	201
Figura G.1: Explotación SSL	202
Figura G.2: Explotación SSL	203
Figura G.3: Consulta de Certificados.....	203
Figura G.4: Consulta de Certificados.....	204
Figura G.5: Vulnerabilidad BlueKeep.....	204
Figura G.6: Servidor Sif Principal	205
Figura G.7: Ejecución python al servidor, servidor en estado error	205
Figura G.8: Reinicio Servidor	206

ÍNDICE DE TABLAS

Tabla 1: Vulnerabilidades.....	7
Tabla 2: Entrevista para aplicar al Jefe de Área Informática del Departamento Financiero	21
Tabla 3: Formato de inventario de los servidores a identificar.	21
Tabla 4: Comparativo de Herramientas de Hacking Ético.....	22
Tabla 5: Recolección de Información	24
Tabla 6: Resultado de la entrevista	29
Tabla 7: Resumen de los Servidores	31
Tabla 8: Selección de las herramientas	38
Tabla 9: Herramientas de explotación de vulnerabilidades	39
Tabla 10: Comparativo.....	179

RESUMEN EJECUTIVO

El presente proyecto de investigación tiene como propósito realizar el análisis de vulnerabilidades en los servidores del Departamento Financiero de la Empresa Eléctrica Ambato Regional Centro Norte S.A., la cual permite mitigar riesgos asociados a la pérdida de información e indisponibilidad de servicios.

Para el desarrollo del proyecto, se usa el Ciclo de Deming, también conocido como PDCA (Planificar, Hacer, Verificar y Actuar). Ésta metodología asegura la gestión efectiva y la mejora continua de la investigación. Al complementar el Ciclo de Deming con las fases específicas del pentesting, se garantiza un control sistemático de cada una de las etapas, a saber: Reconocimiento, Análisis de Vulnerabilidades, Explotación, Escalamiento de Privilegios y la Elaboración de Informes. La integración de la metodología PDCA con las fases de un proyecto de pentesting garantiza una gestión eficiente, orientada hacia la mejora continua y la protección de los sistemas informáticos del Departamento Financiero.

Con el desarrollo de la investigación, se implementa mejoras de seguridad informática en los servidores del Departamento Financiero, mitigando los riesgos en los servicios y garantizando la disponibilidad de la información. Esta investigación permite identificar y corregir vulnerabilidades críticas, lo cual contribuye a mantener la infraestructura informática mas segura. Al hacerlo, se salvaguardan los activos digitales, y además se refuerza la confianza y satisfacción de todos los clientes.

Palabras clave: Vulnerabilidades, riesgos, metodología, PDCA, pentesting, integridad.

ABSTRACT

The purpose of this research project is to conduct a vulnerability analysis on the servers of the Financial Department of Empresa Eléctrica Ambato Regional Centro Norte S.A., which will allow for the mitigation of risks associated with the loss or leakage of information.

For the development of the project, the Deming Cycle, also known as PDCA (Plan, Do, Check, Act), is used. This methodology ensures effective management and continuous improvement of the research. By complementing the Deming Cycle with the specific phases of pentesting, systematic control of each stage is guaranteed, namely: Reconnaissance, Vulnerability Analysis, Exploitation, Privilege Escalation, and Reporting. The integration of the PDCA methodology with the phases of a pentesting project guarantees efficient management, oriented towards continuous improvement and the protection of the Financial Department's IT systems.

With the development of the research, IT security improvements will be implemented on the Financial Department's servers, mitigating risks to services and ensuring the availability of information. This research allows for the identification and correction of critical vulnerabilities, which contributes to maintaining a more secure IT infrastructure. In doing so, digital assets are safeguarded, and the trust and satisfaction of all clients are reinforced.

Keywords: Vulnerabilities, risks, methodology, PDCA, pentesting, integrity.

CAPÍTULO I

MARCO TEÓRICO

1.1 Tema de investigación

ANÁLISIS DE VULNERABILIDADES MEDIANTE PRUEBAS DE PENETRACIÓN EN LOS SERVIDORES DEL DEPARTAMENTO FINANCIERO DE LA EMPRESA ELÉCTRICA AMBATO REGIONAL CENTRO NORTE S.A.

1.2 Antecedentes Investigativos

Luego de examinar la biblioteca de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial y posterior a ello revisar las bases de datos de los diferentes centros de educación superior que respaldan la presente investigación, se puede mencionar lo siguiente:

En la Tesis de grado realizada por Karen Pintado y Cesar Hurtado, titulado “DIAGNÓSTICO DE LA VULNERABILIDADES INFORMÁTICAS EN LOS SISTEMAS DE INFORMACIÓN PARA PROPONER SOLUCIONES DE SEGURIDAD A LA RECTIFICADORA GABRIEL MOSQUERA S.A.”, en la Universidad Politécnica Salesiana del Ecuador, en el año 2015 identifican que: “Una evaluación efectiva de riesgos en la seguridad de la información considera tanto los temas organizacionales como los técnicos, examina cómo los usuarios emplean la infraestructura diariamente en su entorno. Además, es una práctica fundamental porque genera una visión para la empresa acerca de los riesgos, proporcionando una base para futuras mejoras” [1].

En la Tesis de grado desarrollada por Richard Catuto, titulado “ANÁLISIS DE AMENAZAS Y VULNERABILIDADES INFORMÁTICAS BASADO EN LA NORMA ISO 27002, EN EL PROCESO DE CITAS DEL SERVIDOR WEB DE UNA INSTITUCIÓN”, en la Universidad Estatal Península de Santa Elena, en el año 2021 identifica que: “Cuando los sistemas no cuentan con una gestión de seguridad adecuada,

la información sensible, como historias clínicas de pacientes, corre el riesgo de ser manipulada o incluso robada. Es esencial realizar un análisis del sistema para implementar controles que eviten la manipulación de datos, como la alteración de registros electrónicos o resultados de pruebas médicas” [2].

En la Tesis de grado desarrollada por Joseph Alvarado, titulado “ANÁLISIS DE LAS VULNERABILIDADES MEDIANTE EL USO DE PHISHING PARA MEJORAR LA SEGURIDAD INFORMÁTICA DE LOS EQUIPOS DE CÓMPUTO Y REDES DE LA MUNICIPALIDAD DISTRITAL DE INDEPENDENCIA”, en la Universidad Nacional “Santiago Antúnez de Mayolo”, en el año 2017 identifica que: “Los sitios de redes sociales han sido blancos frecuentes para los phishers, ya que la información compartida en estos sitios puede ser utilizada para robo de identidad. Experimentos han mostrado tasas de éxito del 90% en ataques de phishing en redes sociales. En 2006 y 2007, un gusano informático infectó algunas páginas de MySpace, redirigiendo enlaces a un sitio diseñado para robar información confidencial de los usuarios” [3].

1.2.1 Contextualización del problema

Las organizaciones enfrentan constantes desafíos en la seguridad de la información debido a la creciente digitalización y la interconexión de sistemas. Las amenazas cibernéticas se han vuelto más sofisticadas y persistentes, lo cual ha generado un mayor control en materia de seguridad informática.

A nivel mundial, la vulnerabilidad de los sistemas informáticos puede tener consecuencias significativas no solo para las empresas individuales, sino también para la estabilidad del sistema financiero global, comprometiendo información sensible. Un ejemplo significativo de estas consecuencias es el ataque que ocurrió con el Fondo Monetario Internacional en febrero del año que se elabora esta investigación [4].

En el Ecuador, en la mayoría de las empresas la falta de evaluación de las vulnerabilidades en los servidores afecta la relación con los stakeholders, clientes, proveedores y entidades reguladoras, quienes confían en la seguridad, disponibilidad y confidencialidad de la información financiera. Un caso particular se evidenció en el Consejo de la Judicatura del Ecuador en mayo del año 2024, la institución fue objeto de ataques cibernéticos que

pusieron en riesgo la integridad de los sistemas judiciales y la reputación institucional. Estos incidentes comprometieron la seguridad de datos sensibles y afectaron la disponibilidad de los servicios judiciales en línea [5].

La Empresa Eléctrica Ambato Regional Centro Norte S.A. es una entidad del sector estratégico ubicada en el centro del país, reconocida por ofrecer a la ciudadanía un servicio de calidad tanto en la parte eléctrica como en la atención al cliente. Actualmente la empresa cuenta con la certificación ISO 9001:2015 en gestión de calidad, lo que refleja su compromiso con la excelencia y la mejora continua. Por esta razón, se ve en la necesidad de mejorar la calidad en todos los ámbitos de su operación. Una parte crucial de este compromiso es proteger la información sensible almacenada en sus servidores y evitar la indisponibilidad de los servicios.

La falta de análisis de vulnerabilidades mediante pruebas de penetración en los servidores representa una amenaza directa para la integridad, confidencialidad y disponibilidad de la información financiera sensible. La incapacidad para identificar y mitigar adecuadamente las vulnerabilidades expone a la empresa a riesgos de pérdida de datos, fraudes financieros, interrupciones operativas y daños a la reputación. Además, puede generar tensiones internas y disfunciones en el equipo financiero, afectando la eficiencia y la moral de los funcionarios.

1.2.2 Fundamentación teórica

1.2.2.1 Seguridad Informática

La seguridad informática, es el campo que protege la integridad, disponibilidad y confidencialidad de la información en los sistemas informáticos. La información de una empresa debe ser utilizada únicamente por los empleados autorizados. Por lo tanto, se enfoca en proteger tanto los sistemas computacionales como los de teleinformática, con el objetivo principal de cuidar y prevenir cualquier riesgo a la información que se maneja y circula en estos entornos tecnológicos. [6]

1.2.2.2 Riesgo Informático

Riesgo se define como la eventualidad que imposibilita el cumplimiento de un objetivo. Cuantitativamente, el riesgo representa la posibilidad de no superar el objetivo planteado. Un riesgo puede tener dos tipos de consecuencias: ganancias o pérdidas. En el ámbito tecnológico, el riesgo se considera como una amenaza, evaluando el grado de exposición a una pérdida (por ejemplo, el riesgo de perder datos debido a rotura de disco o infecciones por virus informáticos, etc.). Según la Organización Internacional de Normalización (ISO) el riesgo tecnológico se define como: La probabilidad de que una amenaza se materialice, utilizando vulnerabilidades existentes de un activo o un grupo de activos, generándole pérdidas o daños. Esta definición resalta elementos claves como probabilidades, amenazas, vulnerabilidades, activos e impactos, que son esenciales para comprender el concepto de riesgo.

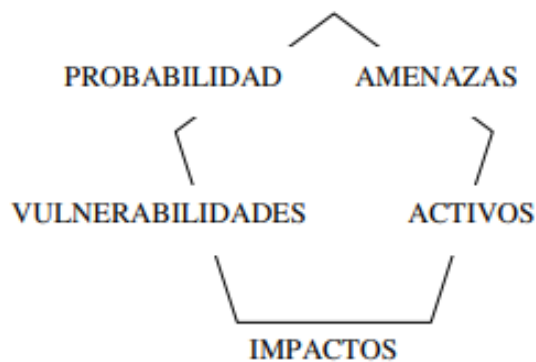


Figura 1.1: Riesgo Informático

Elaborado por: Leonardo Sena, Simón Mario Tenzer.

A continuación, se analiza cada uno de ellos:

- **Probabilidad:** la probabilidad de ocurrencia de un evento puede determinarse de manera cuantitativa o cualitativa, pero siempre considerando que la medida no debe contemplar la existencia de ninguna acción paliativa. Es decir, se debe evaluar las posibilidades de que una amenaza ocurra, independientemente de si se toman medidas para contrarrestarla o no.

Existen amenazas, como por ejemplo incendios, para las cuales hay información suficiente (series históricas, compañías de seguros, entre otros) que permite

establecer una probabilidad de ocurrencia. Sin embargo, hay otras amenazas cuya probabilidad presenta mayor dificultad de cuantificar, como el acceso no autorizado a datos, esto se estima en función de experiencias previas. Por ejemplo, para el personal interno del Centro de Cómputos (CPD), la probabilidad de acceso no autorizado puede ser del 70%; para el personal de la organización, pero externo al CPD, del 45%; y para personas externas, del 80% (a través de Internet).

- **Amenazas:** las amenazas son aquellas acciones que generan consecuencias negativas en la operatividad de las organizaciones. Las amenazas son fallas, accesos no autorizados, virus informáticos, uso incorrecto del software y desastres naturales como terremotos o inundaciones. Las amenazas también involucran la facilidad de acceso a las instalaciones.

Las amenazas pueden ser físicas o lógicas, por ejemplo, una inundación podría ser una amenaza física, mientras que el acceso no autorizado a una base de datos sería una amenaza lógica.

- **Vulnerabilidades:** son condiciones inherentes a los activos o a su entorno que facilitan la materialización de las amenazas, haciendo que activos sean susceptibles a riesgos.

Las amenazas existen en todos los ámbitos y logran materializarse, pero solo se concretan las amenazas siempre están presentes, pero sin la identificación de una vulnerabilidad no podrán ocasionar ningún impacto. Estas vulnerabilidades pueden ser de naturaleza variada, como la falta de conocimiento del usuario, tecnología insuficientemente probada, transmisión por redes públicas, entre otras. A modo de ejemplo es tener un antivirus desactualizado, lo que permite a un virus actuar y causar daños. Si el antivirus estuviera actualizado, la amenaza del virus, aunque potencialmente seguiría existiendo y no podría materializarse.

- **Activos:** Los activos a identificar incluyen aquellos vinculados a los sistemas de información. Ejemplos comunes son los datos, el hardware, el software, los servicios, los documentos, los edificios y el personal.

- **Impactos:** Las consecuencias de la materialización de diversas amenazas son siempre negativas. Las pérdidas resultantes pueden ser financieras o no, y pueden manifestarse tanto a corto plazo como a largo plazo. Las más habituales incluyen la pérdida directa de dinero, la disminución de confianza, la reducción de la eficiencia y la pérdida de oportunidades de negocio. Algunos menos frecuentes incluyen la pérdida de vidas humanas o el daño al medio ambiente, entre otros [7].

1.2.2.3 Vulnerabilidades

Las vulnerabilidades son fallos en el diseño de procedimientos o recursos. Estas vulnerabilidades no se crean; ya existen y representan deficiencias en el diseño de un sistema, un sistema desactualizado o una configuración incorrecta. Esto permite que un agente externo acceda sin los permisos adecuados al recurso o a la información gestionada por el sistema. Dependiendo del tipo de recurso, hay distintas fuentes de información donde se pueden identificar las vulnerabilidades aplicables a los sistemas existentes [8].

Podemos agrupar las vulnerabilidades en función de:

Etapas	Definición
Diseño	Un diseño inadecuado de protocolos en redes de datos y políticas de seguridad deficientes.
Implementación	La presencia de backdoors en dispositivos y sistemas informáticos. Buffers u overflows en las aplicaciones desarrolladas. Falta de implementación de parches y ausencia de soporte por parte de los fabricantes.
Uso	Configuraciones incorrectas en los sistemas.

	<p>Falta de concientización o capacitación a los usuarios y responsables de TI sobre el manejo y las fallas de los sistemas informáticos.</p> <p>Insuficiencia de recursos de seguridad en TI.</p>
Vulnerabilidad día cero	<p>Se refiere a los ataques contra las aplicaciones que se ejecutan de manera maliciosa en las vulnerabilidades detectadas en los sistemas, las cuales son desconocidas por los usuarios.</p>

Tabla 1: Vulnerabilidades

Elaborado por: El investigador.

1.2.2.3.1 Top Ten de Vulnerabilidades

OWASP actualiza regularmente una lista de las principales vulnerabilidades de seguridad. La versión más reciente, fue lanzada el 2021, se detalla a continuación:

- **Control de acceso roto:** Detalla las vulnerabilidades asociadas con el acceso no autorizado a recursos protegidos en aplicaciones web, proporcionando directrices y soluciones para abordar estos riesgos de seguridad de manera efectiva [9].
- **Fallos criptográficos:** Expone las vulnerabilidades relacionadas con el uso incorrecto de técnicas criptográficas en aplicaciones web, ofreciendo recomendaciones y soluciones para corregir estas deficiencias y fortalecer la seguridad de los sistemas [10].
- **Inyección:** Vulnerabilidades causadas por la inserción de código malicioso en aplicaciones web, destacando la importancia de validar y sanitizar los datos de entrada para prevenir ataques [11].
- **Diseño inseguro:** Vulnerabilidades originadas por diseños inseguros en aplicaciones web, subrayando la importancia de una arquitectura sólida y segura desde el inicio del desarrollo [12].

- **Configuración incorrecta de seguridad:** Examina las vulnerabilidades resultantes de configuraciones incorrectas o incompletas en aplicaciones web, enfatizando la importancia de una gestión adecuada de la configuración para mantener la seguridad [13].
- **Componentes vulnerabilidades y obsoletos:** Destaca las vulnerabilidades originadas por el uso de componentes desactualizados o vulnerables en aplicaciones web, señalando la importancia de mantener actualizados todos los componentes y bibliotecas de terceros [14].
- **Fallos de identificación y autenticación:** Aborda las vulnerabilidades relacionadas con fallos en la identificación y autenticación de usuarios en aplicaciones web, resaltando la importancia de implementar correctamente estos procesos para proteger los datos sensibles [15].
- **Fallos de integridad de datos y software:** Examina las vulnerabilidades relacionadas con fallos en la integridad de software y datos en aplicaciones web, enfocándose en la importancia de garantizar la confiabilidad y precisión de la información [16].
- **Errores de monitoreo y registro de seguridad:** Resalta las vulnerabilidades relacionadas con deficiencias en el registro y monitoreo de seguridad en aplicaciones web, enfocándose en la importancia de tener un sistema efectivo de registro y monitoreo para detectar y responder a posibles amenazas [17].
- **Falsificación de solicitudes del lado del servidor:** Vulnerabilidades relacionadas con la falsificación de solicitudes del lado del servidor en aplicaciones web, destacando la importancia de protegerse contra este tipo de ataques que pueden comprometer la seguridad y la integridad de los sistemas [18].

1.2.2.4 Amenazas

Una amenaza informática abarca eventos, ocurrencias o individuos, que tienen el potencial de causar daño a un sistema informático. Algunas de las tipificaciones más relevantes incluyen la destrucción, divulgación, robo, modificación de datos e interrupción del

servicio. Estas amenazas se manifiestan en ubicaciones específicas, con una duración e intensidad determinadas, lo que conlleva a la materialización del riesgo asociado. Es decir, una amenaza solo puede existir si hay una vulnerabilidad presente y explotable, sin importar si compromete o no la seguridad de un sistema de información [19].

1.2.2.4.1 Tipos de Amenazas

A continuación, se detalla algunas de las amenazas:

- Virus informáticos o códigos maliciosos.
- Uso no autorizado de Sistemas Informáticos
- Robo de información.
- Fraudes Basados en el uso de computadores.
- Suplantación de identidad.
- Denegación de Servicios (DOS).
- Ataque de Fuerza Bruta.
- Alteración de la Información.
- Divulgación de Información.
- Desastres Naturales.
- Sabotaje, vandalismo.
- Espionaje.

1.2.2.5 Hacking Ético

El hacking ético se define como el arte de identificar vulnerabilidades seguridad en una organización o mediante una auditoría realizada por profesionales en la seguridad de la información. El hacking ético es también conocido como prueba de intrusión o pentesting. Posteriormente, mediante un informe, se revela los fallos de seguridad encontrados con el

objetivo de mitigarlos, previniendo así las fugas de información y ataques informáticos [20].

1.2.2.6 Los Hackers

Persona con grandes habilidades en el manejo de computadoras que investiga un sistema informático para avisar de los fallos y desarrollar técnicas de mejora [21]. Su dedicación a proyectos no se limita a la búsqueda de recompensas económicas, sino que se basa en el disfrutar, crear y resolver desafíos. La libertad y autonomía son valores primordiales en su trabajo, ya que les permiten tomar decisiones sobre qué proyectos abordar y cómo hacerlo. La ética del hacker se distingue en compartir conocimientos, buscando oportunidades laborales que les permitan expresarse y desarrollar su potencial creativo de manera significativa. Además, los hackers se comprometen con la mejora continua de sus habilidades y tienen una responsabilidad hacia el bienestar general y el progreso de la comunidad global [22].

1.2.2.7 La Ciberseguridad

El concepto de "ciberseguridad" abarca las acciones y medidas dirigidas a proteger los sistemas de tecnologías de la información y comunicación (TIC), así como la información que estos contienen. Se trata de un campo interdisciplinario centrado en salvaguardar los sistemas informáticos, las redes y los datos contra amenazas cibernéticas. Este ámbito subraya la importancia de implementar estrategias y tecnologías para prevenir, detectar y responder ante riesgos y ataques que puedan comprometer la confidencialidad, integridad y disponibilidad de la información digital. Además, promueve la confianza en el uso de las tecnologías de la información y la comunicación mediante la protección de la infraestructura digital. [23].

La mayoría de los ciberataques no provocan daños significativos, pero la posibilidad de un ataque exitoso contra componentes críticos de la infraestructura plantea un riesgo considerable. Aunque estos ataques pueden generar costos considerables tanto para individuos como para organizaciones, evaluar su impacto económico resulta complejo y las estimaciones varían considerablemente [24].

1.2.2.7.1 Tipos de Ciberataques

- **Ataque DoS:** Un ataque de denegación de servicio (DoS) saturar los recursos de un sistema, impidiendo que atienda solicitudes legítimas de servicio. A diferencia de otros ataques que buscan acceder al sistema, estos tienen como objetivo interrumpir el servicio. Aunque pueden beneficiar a competidores comerciales, los piratas informáticos no obtienen acceso directo al sistema objetivo. Además, un ataque DoS puede dejar el sistema vulnerable a otras intrusiones al forzar su desconexión. Los firewalls son una defensa común contra estos ataques, filtrando solicitudes ilegítimas y permitiendo que el tráfico legítimo continúe. Un ejemplo destacado ocurrió en febrero de 2020 contra Amazon Web Services (AWS) [25].
- **Malware:** Malware engloba diferentes tipos de software malicioso, como spyware, ransomware, virus y gusanos. Este software malintencionado se infiltra en las redes aprovechando vulnerabilidades, generalmente cuando un usuario interactúa con enlaces o archivos adjuntos peligrosos en correos electrónicos, lo que resulta en la instalación de programas riesgosos. Una vez dentro del sistema, el malware puede bloquear el acceso a partes clave de la red, instalar más malware o software dañino, recopilar información de forma clandestina al transmitir datos desde el disco duro (spyware) y modificar componentes específicos y dejar el equipo inutilizable [26].
- **Ataque MITM:** El ataque conocido como "hombre en el medio", tiene como objetivo interceptar la comunicación entre dos dispositivos conectados a una red sin autorización. Esto permite que un agente malintencionado manipule el tráfico interceptado de diversas maneras, como escuchando la comunicación para obtener información sensible o suplantando la identidad de alguna de las partes. Para que este ataque tenga éxito, el delincuente debe asegurarse de ser el único punto de comunicación entre los dispositivos, lo que implica estar presente en la misma red que los hosts atacados para manipular la tabla de enrutamiento de cada uno [27].
- **Ataque de Suplantación de Identidad y Spear Phishing:** Un Ataque de Suplantación de Identidad, o phishing, es una forma de engaño en línea donde los

ciberdelincuentes envían correos electrónicos falsos que parecen provenir de empresas legítimas, como bancos o tiendas en línea, con el fin de engañar a los destinatarios para que compartan información personal confidencial, como contraseñas o datos de tarjetas de crédito. Estos correos electrónicos suelen contener enlaces maliciosos o archivos adjuntos que, al ser interactuados, pueden instalar malware en los dispositivos de los usuarios. A diferencia del spear, phishing, que es altamente personalizado, el phishing no se adapta al destinatario y se basa en el envío masivo de correos electrónicos genéricos [28].

- **Ransomware:** El ransomware es un tipo de malware, bloquea el acceso a sistemas o archivos personales y solicita un rescate para recuperarlos. Aunque surgió en la década de 1980 con pagos por correo postal, hoy en día los ciberdelincuentes exigen pagos en criptomonedas o tarjetas de crédito.

Un método de infección común es el malspam, correos electrónicos no solicitados que contienen archivos adjuntos maliciosos o a su vez enlaces a sitios web dañinos. La ingeniería social se utiliza para engañar a los usuarios, haciéndoles creer que los mensajes son legítimos, incluso haciéndose pasar por instituciones de confianza o amigos [29].

- **Ataque de Fuerza Bruta:** Un ataque de fuerza bruta es una técnica de prueba y error utilizada para descifrar datos confidenciales, como contraseñas o claves de encriptación. A menudo, se emplea para descifrar contraseñas de inicio de sesión de sitios web mediante la generación de diferentes combinaciones de caracteres hasta encontrar la correcta. A diferencia de otros métodos de decodificación que pueden implicar estrategias más sofisticadas, los ataques de fuerza bruta no requieren un enfoque intelectual; simplemente prueban todas las posibles combinaciones de caracteres hasta lograr el acceso deseado. Este proceso se asemeja a un ladrón que intenta abrir una caja fuerte probando todas las combinaciones posibles de números hasta encontrar la correcta [30].
- **Ataque de Inyección SQL:** La inyección de SQL ocurre cuando un hacker introduce código SQL malicioso en un sitio web, aprovechando posibles fallos en

su desarrollo. Este código malicioso, también conocido como carga útil, se envía a la base de datos como una consulta legítima, lo que puede causar efectos no deseados o incluso comprometer la seguridad de la base de datos [31].

1.2.2.8 Pruebas de Penetración

Las pruebas de penetración, también conocidas como Pentesting, son herramientas utilizadas para evaluar o auditar sistemas informáticos, redes o aplicaciones web. Consisten en la realización de prácticas diseñadas para poner a prueba la seguridad de un sistema mediante la identificación de vulnerabilidades que podrían ser explotadas por posibles atacantes. Estas pruebas implican un ataque simulado y autorizado contra el sistema con el objetivo de evaluar su seguridad. Durante el Pentesting, se identifican las vulnerabilidades presentes en el sistema y se intentan explotar, de manera similar a como lo haría un atacante real con fines maliciosos. El objetivo final es proporcionar al cliente una evaluación de riesgos basada en los resultados de la prueba y recomendar un plan de medidas correctivas para mejorar la seguridad del sistema [32].

4.1.2.8.1 Actividades de un Pentester

Los pentesters realizan una variedad de actividades para evaluar y mejorar la seguridad de sistemas informáticos y redes. Estas actividades incluyen análisis de vulnerabilidades para identificar posibles debilidades, pruebas de penetración para simular ataques y evaluar la resistencia del sistema, evaluación de seguridad para analizar la efectividad de las medidas de seguridad existentes y proponer mejoras, elaboración de informes detallados sobre las vulnerabilidades descubiertas y recomendaciones para corregirlas, pruebas en redes y sistemas para detectar posibles fallos, evaluación de la seguridad de aplicaciones web para identificar vulnerabilidades como inyecciones SQL, y simulaciones de ataques para evaluar la respuesta y capacidad de detección de los sistemas de seguridad. Además, los pentesters también ofrecen formación y concienciación en seguridad a los equipos de desarrollo y otros profesionales de TI para prevenir futuras vulnerabilidades [33].

4.1.2.8.2 Tipos de Pruebas de Penetración

- **Pentesting de caja blanca:** también conocido como White Box, implica una evaluación exhaustiva de la estructura informática. Este tipo de prueba permite identificar fácilmente los puntos débiles del sistema y determinar qué aspectos pueden ser modificados. Es un proceso que requiere un tiempo considerable, ya que las empresas proporcionan a los hackers de sombrero blanco toda la información relacionada con sus redes y sistemas.
- **Pentesting de caja negra:** conocido como Black Box, implica una aproximación más auténtica, ya que el hacker de sombrero blanco tiene un conocimiento limitado sobre los datos de la empresa o usuario y desempeña el papel de un ciberdelincuente real. Estas pruebas se consideran como pruebas a ciegas, ya que el experto en ciberseguridad debe descubrir las vulnerabilidades y amenazas en la estructura informática sin información previa. Este tipo de prueba es útil para entender cómo un atacante sin conocimiento previo puede comprometer la seguridad de un sistema.
- **Pentesting de caja gris:** conocido como Grey Box, combina elementos de las pruebas de caja blanca y caja negra. En este tipo de evaluación, el experto en ciberseguridad dispone de información básica sobre la empresa o usuario, lo que le permite tener un punto de partida, pero sin conocer todos los detalles. Este tipo de prueba es considerada la más recomendable, ya que permite simular de manera más precisa las acciones de un atacante real que posee cierta información privilegiada, como credenciales de acceso. Las pruebas de caja gris son útiles para identificar amenazas internas y detectar vulnerabilidades dentro de un área específica de la red [34].

1.2.2.9 Fases de Pentesting



Figura 1.2: Fases de Pentesting

Elaborado por: Diego Echeverri Uribe

- **Fase de reconocimiento:** es crucial en el pentesting, ya que sienta las bases para las etapas posteriores y determina el éxito de la auditoría. Se divide en reconocimiento pasivo y activo. El pasivo se centra en recopilar información sin interactuar directamente, mientras que el activo implica interactuar con los sistemas para identificarlos.
- **Fase de escaneo de vulnerabilidades:** busca descubrir la configuración, versiones de sistemas operativos y servicios en uso. Se utilizan herramientas avanzadas como Nessus y Acunetix para identificar vulnerabilidades y contrastar la información con bases de datos de ataques. Sin embargo, estas herramientas pueden generar falsos positivos o negativos, por lo que se requiere la interpretación de los resultados.
- **Fase de explotación:** es la más emocionante, porque se prueban las vulnerabilidades encontradas para determinar si representan una amenaza real. Se emplean diversas metodologías, como la OWASP, para atacar servicios clave como Windows Active Directory y servidores web. Es crucial documentar todos los intentos de ataque y resultados para garantizar la transparencia y facilitar la reproducción de los ataques.
- **Fase de post-explotación:** una vez comprometido un sistema, se busca explorar a fondo el entorno, descubrir nuevos servicios y establecer persistencia en el sistema.

Se crean puertas traseras y canales encubiertos para acceder nuevamente al sistema comprometido. El movimiento lateral a otros servicios y activos de la red es crucial para obtener el control total de la infraestructura.

- **Fase de reporte:** consiste en documentar las vulnerabilidades encontradas, priorizar las amenazas y proponer soluciones para mejorar la seguridad del sistema. Se generan informes técnicos y ejecutivos que contienen recomendaciones claras, así como buenas prácticas para prevenir futuras vulnerabilidades [35].

1.2.2.10 Herramientas de Pentesting

- **Metasploit:** Es una herramienta de código abierto utilizada en pruebas de penetración y evaluaciones de seguridad. Ofrece una plataforma integral que permite a los expertos en seguridad evaluar la vulnerabilidad de sistemas informáticos y redes mediante la simulación de ataques. Metasploit proporciona una amplia gama de módulos y herramientas que permiten a los usuarios realizar diversas actividades, como escanear redes, identificar vulnerabilidades, explotar sistemas y realizar pruebas de intrusión de manera controlada y ética. Además, facilita la automatización de tareas y la generación de informes detallados sobre los hallazgos de seguridad, lo que ayuda a las organizaciones a mejorar su postura de seguridad y a mitigar posibles riesgos [36].
- **Nessus:** es un programa de ciberseguridad disponible en versiones de código abierto y de pago que se utiliza para escanear vulnerabilidades en diversos sistemas operativos. Estas vulnerabilidades son fallos informáticos que representan riesgos para la seguridad de un sistema. Nessus utiliza una extensa base de datos de vulnerabilidades para detectar estos fallos en dispositivos [37].

Nessus tiene varias características distintivas:

1. Realiza un análisis exhaustivo de la configuración del servidor, ampliando más allá de los análisis convencionales.

2. Cuenta con información actualizada sobre nuevas vulnerabilidades y ataques, garantizando la protección de los datos.
 3. Es un software de código abierto, lo que facilita su acceso y personalización.
 4. Se puede implementar en diversas plataformas, incluyendo Raspberry Pi, lo que lo hace versátil.
 5. Utiliza complementos compilados dinámicamente para mejorar la eficiencia de las tareas de escaneo.
 6. Integra más de 450 plantillas preconfiguradas para una gestión más efectiva de las vulnerabilidades.
 7. Permite la creación de informes personalizados para acceder a la información generada de manera específica [38].
- **Nmap:** Se trata de una aplicación de código abierto y gratuita, mediante línea de comandos de Linux . Entre sus características se incluyen:
 1. **Escaneo de Puertos:** Nmap puede escanear puertos específicos o rangos de puertos en un host para determinar cuáles están abiertos, cerrados o filtrados.
 2. **Detección de Servicios:** Identifica los servicios (como HTTP, FTP, SMTP) y versiones de software que se están ejecutando en puertos abiertos.
 3. **Identificación de Sistemas Operativos:** Utiliza técnicas de fingerprinting para determinar el sistema operativo que está corriendo en un host.
 4. **Detección de Vulnerabilidades:** Con scripts NSE (Nmap Scripting Engine), Nmap puede realizar pruebas de seguridad avanzadas y detectar vulnerabilidades conocidas en los servicios y aplicaciones de red.
 5. **Escaneo de Red Completa:** Permite escanear redes enteras para descubrir todos los dispositivos conectados y mapear la topología de la red.
 6. **Soporte para IPv6:** Puede escanear redes IPv6, además de IPv4.

7. **Salidas Flexibles:** Proporciona diversas opciones de salida, incluyendo formatos XML, HTML y texto, lo que facilita la integración con otras herramientas y sistemas de informes.
8. **Escaneo Silencioso:** Capaz de realizar escaneos en modo sigiloso para evitar la detección por sistemas de monitoreo y firewalls.
9. **Escaneo de Firewall y IDS/IPS:** Puede identificar reglas de firewall y sistemas de detección/preventivas de intrusiones (IDS/IPS) en la red.
10. **Escaneo Distribuido:** Soporta escaneos distribuidos mediante el uso de herramientas adicionales como Ncrack y Zenmap (la GUI de Nmap) [39].

1.2.2.11 Ciclo de Deming

El ciclo Deming, también conocido como ciclo PHVA, es un sistema que busca optimizar la calidad y competitividad, reducir costos y fallos, aumentar la productividad y eliminar riesgos. Se estructura en cuatro etapas: Planificar, Hacer, Verificar y Actuar, proporcionando un marco para la implementación de planes de mejora continua.

El ciclo Deming consta de cuatro etapas que se repiten en un ciclo continuo para mejorar procesos de manera sistemática.

La primera etapa, Planificar, implica identificar problemas, establecer objetivos y definir métodos.

La fase de Hacer involucra la implementación del plan, a menudo mediante una prueba piloto, seguida de la verificación y aplicación de correcciones.

La etapa de Controlar implica evaluar si se lograron los objetivos utilizando herramientas como Diagrama de Pareto.

En Actuar, se ajusta el plan de mejora y se implementa definitivamente si se alcanzan los objetivos; de lo contrario, se revisa el proceso y se inicia un nuevo ciclo [40].



Figura 1.3: Ciclo de Deming

Elaborado por: Christian Castillo, Carmen Ortega, Vanessa Benavides, Laura Velasco

1.3 Objetivos

1.3.1 Objetivo General

Realizar un análisis de vulnerabilidades mediante pruebas de penetración en los servidores del Departamento Financiero de la Empresa Eléctrica Ambato Regional Centro Norte S.A.

1.3.2 Objetivos Específicos

- Identificar los servidores en los cuales se realizarán las pruebas de penetración en el Departamento Financiero de la Empresa Eléctrica Ambato Regional Centro Norte S.A.
- Seleccionar las herramientas y técnicas de Hacking Ético correctas para la detección de vulnerabilidades en los servidores.
- Ejecutar pruebas de penetración sobre los servidores del Departamento Financiero.
- Desarrollar un informe detallado de las vulnerabilidades encontradas, sus posibles consecuencias y recomendaciones para mitigar los riesgos.

CAPÍTULO II

METODOLOGÍA

2.1 Materiales

- Instrumento que se va a utilizar: entrevista.

Preguntas	Respuestas
1. ¿El Departamento Financiero tiene servidores que son administrados por el responsable de TICS?	
2. ¿El Departamento Financiero dispone de un centro de cómputo en donde se almacenan los servidores de manera física?	
3. ¿Cómo se gestionan las credenciales y el control de acceso a los servidores?	
4. ¿Con qué frecuencia se realizan actualizaciones de software y parches de seguridad en los servidores?	
5. ¿Qué sistemas operativos y versiones están instalados en los servidores?	
6. ¿Se utilizan tecnologías de virtualización y contenedores en los servidores?	

7. ¿Existe un plan de respuesta ante incidentes de seguridad?	
8. ¿Existe algún mecanismo que utilice el Área Informática del Departamento Financiero para monitorear el tráfico de red para detectar actividades sospechosas?	
9. ¿Cómo administra la configuración de servidores?	
10. ¿Existe algún tipo de herramientas de análisis de vulnerabilidades que utilicen regularmente?	

Tabla 2: Entrevista para aplicar al Jefe de Área Informática del Departamento Financiero

Elaborado por: El investigador.

- Computador portátil toshiba.
- Servidores.

SERVIDORES						
UBICACIÓN	MARCA	MODELO	SISTEMA OPERATIVO	FUNCIONALIDAD / USO	ESTADO	OBSERVACIONES / COMENTARIOS
(Va la ubicación del servidor)	(Marca del servidor)	(Modelo del Servidor)	(SO del Servidor)	(Aporte de valor al departamento financiero)	(Elección entre Bueno – Malo - Descontinuado)	(Especificar si es un Servidor Físico o Virtualizado)

Tabla 3: Formato de inventario de los servidores a identificar.

Elaborado por: El investigador.

- Herramientas

HERRAMIENTAS	UTILIDAD	APORTE EN INVESTIGACIÓN
NESSUS 	Detección de Vulnerabilidades. Análisis de Configuración. Escaneo de Red. Detección de Malware. Generación de Informes.	Descubrimiento de puertos, host, dominio, dns, SO vulnerabilidades.
Dmitry 	Escaneo de Dominios. Subdominios. Escaneo de Puertos. Host.	Descubrimiento de puertos, dominios, host.
Nmap 	Escaneo de Puertos. Versiones. Escaneo de Red. Detección de SO. Detección de Vulnerabilidades. Firewall.	Descubrimiento de puertos, host, dominio, SO, vulnerabilidades, firewall.
Metasploit 	Explotación de vulnerabilidades. Exploits, payloads, auxiliary. BDD de vulnerabilidades.	Explotación de vulnerabilidades con la ayuda de exploits.

Tabla 4: Comparativo de Herramientas de Hacking Ético
 Elaborado por: El investigador.

2.2 Métodos

2.2.1 Modalidad de Investigación

Investigación bibliográfica y documental

La investigación se lleva a cabo utilizando un enfoque bibliográfico, dado que la consulta de libros, documentos técnicos, artículos y tesis en el campo de la informática es necesario para la elaboración del proyecto actual. Este método sirve para estructurar el análisis de las vulnerabilidades, y también para la entrega final del informe.

Investigación de campo

Esta modalidad fue adoptada debido a que se recurre a la Empresa Eléctrica Ambato Regional Centro Norte S.A. para identificar los servidores informáticos del Departamento Financiero. Las técnicas empleadas incluyeron entrevista y observación.

2.2.2 Población y Muestra

Para la realización del presente proyecto de investigación no es necesario definir una población ni una muestra específica, dado que el número de empleados del Área informática del Departamento Financiero no supera las 100 personas. Por lo tanto, se realizó una entrevista con el encargado de TI.

2.2.3 Recolección de Información

La información se recopila mediante una entrevista dirigida a la persona encargada del área de TI de la Empresa Eléctrica Ambato Regional Centro Norte S.A. Para ello, se utiliza un cuestionario con preguntas cerradas, obteniendo información clara, con el propósito de alcanzar los objetivos establecidos en el trabajo de investigación.

Preguntas Básicas	Explicación
1. ¿Para qué?	Para alcanzar los objetivos de la investigación.
2. ¿De qué personas u objetos?	Departamento Financiero

3. ¿Sobre qué aspectos?	Análisis de vulnerabilidades mediante pruebas de penetración en los servidores del departamento financiero de la Empresa Eléctrica Ambato Regional Centro Norte S.A.
4. ¿Quién, Quiénes?	Investigador: Rosana Emperatriz Ruilova Romero
5. ¿Cuándo?	En el periodo académico Marzo – Agosto 2024
6. ¿Dónde?	Empresa Eléctrica Ambato Regional Centro Norte S.A.
7. ¿Cuántas veces?	1 o 2 veces hasta tener la información requerida.
8. ¿Qué técnicas de recolección?	Entrevista
9. ¿Con qué?	Cuestionario

Tabla 5: Recolección de Información

Elaborado por: El investigador.

2.3 Procesamiento y Análisis de Datos

Una vez completado el proceso de recolección de información se procederá al análisis de los resultados obtenidos mediante la entrevistas y observación. El procesamiento de datos se realizará mediante una herramienta informática, con el fin de organizar los gráficos y que permitan observar el nivel de importancia de la realización del análisis de vulnerabilidades en los servidores.

2.4 Desarrollo del Proyecto

Para dar cumplimiento con los objetivos planteados en la presente investigación se gestiona las siguientes actividades:

1. Identificar los servidores,
2. Seleccionar las herramientas de la investigación,

3. Realizar pruebas de penetración,
4. Entregar el Informe detallado de las vulnerabilidades encontradas.

CAPÍTULO III

RESULTADOS Y DISCUSIÓN

3.1 Análisis y discusión de resultados

La entrevista se aplicó al Jefe del Área de TI del Departamento Financiero de la Empresa Eléctrica Ambato Regional Centro Norte S.A., la cual consta de un total de 10 preguntas.

3.1.1 Entrevista

Nombre del Entrevistado: Ing. Jorge Freire Mg.

Fecha: 12/06/2024

Cargo: Jefe del Área de TI del Departamento Financiero de la Empresa Eléctrica Ambato Regional Centro Norte S.A.

Lugar: Av. 12 de Noviembre 11-29 y Espejo, Edificio principal bloque A, Oficina del Jefe de Área Informática del Departamento Financiero de la Empresa Eléctrica Ambato Regional Centro Norte S.A.

Preguntas	Respuestas
1. ¿El Departamento Financiero tiene servidores que son administrados por el responsable de TICS?	Si dispone de 3 servidores físicos y 4 servidores virtuales.
2. ¿El Departamento Financiero dispone de un centro de cómputo en donde se almacenan los servidores de manera física?	Si, dispone del centro de cómputo Matriz en donde se alojan dentro de un rack con sistema de enfriamiento y energía redundante.

<p>3. ¿Cómo se gestionan las credenciales y el control de acceso a los servidores?</p>	<p>Actualmente se dispone de una llave física y de una clave de acceso automática para abrir la puerta del centro de cómputo. Por otra parte, los servidores se encuentran unidos al dominio que es administrado con un usuario y clave administrador del dominio df.eeasa.com.ec.</p> <p>Figura C.1: Normas y Políticas de Recursos Tecnológicos y de Seguridad Informática numeral ibídem 5 Políticas de recursos tecnológicos y de seguridad informática 5.1 Políticas de acceso a instalaciones físicas.</p>
<p>4. ¿Con qué frecuencia se realizan actualizaciones de software y parches de seguridad en los servidores?</p>	<p>Actualmente en EEASA no se dispone de una política para realizar actualizaciones, para aquello se procedió a la revisión de las Normas y políticas de Recursos tecnológicos y de Seguridad Informática; sin embargo esta actividad se la ejecuta al momento de realizar el mantenimiento preventivo de los servidores que aun disponen del carepack de hp, esto es al menos 1 vez al año.</p>
<p>5. ¿Qué sistemas operativos y versiones están instalados en los servidores?</p>	<p>Se detalla en la Tabla 7.</p>
<p>6. ¿Se utilizan tecnologías de virtualización y contenedores en los servidores?</p>	<p>Si, el servidor DL385 se encuentra virtualizado con VMware ESXi y no se</p>

	utiliza contenedores a la fecha de esta entrevista.
7. ¿Existe un plan de respuesta ante incidentes de seguridad?	<p>La EEASA dispone de un plan de contingencia informática para garantizar la continuidad de operaciones, este plan de respuesta tiene como responsable del Departamento Financiero a la Jefatura del Área Informática con un liderazgo otorgado para levantar los servicios en caso de alguna interrupción de operatividad informática. En la actualidad todos los servidores del Departamento Financiero se encuentran en el Centro de Cómputo Matriz, por lo que no se dispone de una infraestructura alterna en un sitio distinto.</p> <p>Anexo D: Documento de Plan de Contingencia Informática.</p>
8. ¿ Existe algún mecanismo que utilice el Área Informática del Departamento Financiero para monitorear el tráfico de red para detectar actividades sospechosas?	<p>En el manual de actividades de la Jefatura de Área Informática tiene como competencia 26 funciones lo que impide que se ejecuten tareas adicionales como el monitoreo de tráfico para la detección de actividades sospechosas, por este motivo no se lo realiza. Sin embargo, consiente de los riesgos operativos que pudiera ocasionar el no realizar estas actividades de rutina, ésta jefatura estaría dispuesto a invertir en una herramienta autónoma que</p>

	realice este tipo de monitorización, reforzando la ciberseguridad del Departamento Financiero.
9. ¿Cómo se gestiona la configuración de los servidores?	<p>Actualmente el mecanismo para la administración de servidores se los realiza mediante escritorio remoto a través del usuario administrador del dominio df.eeasa.com.ec.</p> <p>Para los servidores UNIX se lo administra desde una terminal POWERSHELL a través, de protocolo SSH.</p>
10. ¿Existe algún tipo de herramientas de análisis de vulnerabilidades que utilicen regularmente?	Actualmente no se ha llevado a cabo ningún análisis de vulnerabilidades en los servidores del Departamento Financiero.

Tabla 6: Resultado de la entrevista

Elaborado por: El investigador.

3.1.2 Análisis e interpretación de resultados de la entrevista aplicada

La entrevista realizada da la visión detallada de la infraestructura del Departamento Financiero en relación con sus servidores y servicios que se ejecutan.

Se determinó el número de servidores, los sistemas operativos y las funciones específicas. Ésta información sirve para comprender el entorno operativo y para llevar a cabo el análisis completo de vulnerabilidades. Con estos datos, podemos evaluar los riesgos potenciales, planificar estrategias de mitigación y mejorar la seguridad general de la infraestructura tecnológica del departamento.

Además, el conocimiento adquirido sobre la configuración y el uso de los servidores permitirá que las recomendaciones sean enfocadas para garantizar la protección de todas las áreas críticas del Departamento Financiero.

3.2 Desarrollo de la Propuesta

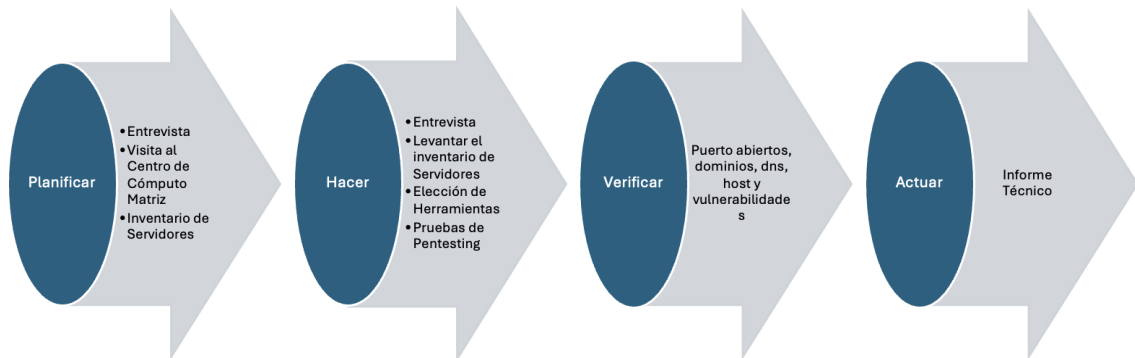


Figura 3.1: Ciclo de Deming Aplicado a la Investigación
Elaborado por: El investigador.

3.2.1 Identificar los servidores.

3.2.1.1 Servidores del Departamento Financiero

Para la identificación de los Servidores se visita al centro de cómputo matriz en el que se constata la existencia de 3 servidores físicos y 4 servidores virtuales.

SERVIDORES						
UBICACIÓN	MARCA	MODELO	SISTEMA OPERATIVO	FUNCIONALIDAD / USO	ESTADO	OBSERVACIONES / COMENTARIOS
Centro de Computo Matriz	HP	ProLiant DL385 Gen10	VMware ESXi 7.0.0	Servidor Global VMWARE ESXi 7.0	bueno	Servidor Físico
Centro de Computo Matriz	HP	ProLiant DL385 Gen10	Microsoft Windows Server 2008	Servidor Sistema Sip Principal	bueno	Maquina Virtualizada
Centro de Computo Matriz	HP	ProLiant DL385 Gen10	Microsoft Windows Server 2008	Servidor SISCAF Inventario 2015	bueno	Maquina Virtualizada
Centro de Computo Matriz	HP	ProLiant DL385 Gen10	Microsoft Windows Server 2008	Servidor Procesos Automaticos(robot)	bueno	Maquina Virtualizada

Centro de Computo Matriz	HP	ProLiant DL385 Gen10	AlmaLinux 8	Servidor Desarrollo Spring Boot	bueno	Maquina Virtualizada
Centro de Computo Matriz	HP	ProLiant ML350p Gen8	Microsoft Windows Server 2016	Servidor VEAMBAC KUP	descontinuado	Servidor Físico
Centro de Computo Matriz	Synology	RS818+	DSM 7.1.1	Servidor NAS	bueno	Servidor Físico

Tabla 7: Resumen de los Servidores

Elaborado por: El investigador.

Fuente: EEASA

3.2.1.2 Cuarto de Servidores

Los servidores se encuentran en el cuarto del centro de cómputo Matriz en donde se alojan dentro de un rack con sistema de enfriamiento y energía redundante.



Figura 3.2: Acceso al cuarto del centro de cómputo Matriz
Elaborado por: El investigador.



Figura 3.3: Centro de cómputo Matriz
Elaborado por: El investigador.



Figura 3.4: Circuito de Alarma contra incendios y control de la puerta de acceso
Elaborado por: El investigador.



Figura 3.5: Alarma de aire del Centro de cómputo Matriz
Elaborado por: El investigador.



Figura 3.6: Rack de Servidores del Departamento Financiero en el Centro de cómputo Matriz
Elaborado por: El investigador.

3.2.2 Seleccionar las herramientas de la investigación.

3.2.2.1 Herramientas de análisis de vulnerabilidades

Herramienta	Concepto	Características	Ventajas	Desventajas
Nessus	Es una herramienta de escaneo de vulnerabilidades que ayuda a identificar problemas de seguridad en sistemas, aplicaciones y redes. Nessus escanea dispositivos en busca de configuraciones incorrectas, software desactualizado y vulnerabilidades conocidas [42].	Cobertura de activos Diversos análisis Configuración y cumplimiento Detección de amenazas Informes	Actualización constante de Base de Datos de Plugins. Interfaz de usuario fácil de usar. Informes Detallados. Escaneo Eficientes.	Consumo de Rendimiento del Equipo. Desactualización de Base de Datos Plugin. Funciones Avanzadas de paga.
Nmap	Es una herramienta de código abierto	Escaneo de Puertos.	Código Abierto y Gratuito.	Alto rendimiento en la red.

	empleada para el escaneo de redes y la evaluación de seguridad. El objetivo es investigar redes, descubrir dispositivos y servicios activos, además de detectar vulnerabilidades en sistemas informáticos [45].	Detección de Versiones. Mapeo de Red. Escaneo de Vulnerabilidades. Auditoría de Seguridad.	Detección de Servicios y Sistemas Operativos. Comunidad de usuarios y desarrolladores. Se adapta a cualquier tamaño de una empresa.	No es apto para escaneo de vulnerabilidades en aplicaciones web. Falsos positivos y negativos.
Nikto	Es una herramienta de código abierto diseñada para realizar escaneos de seguridad en servidores web [43].	Escaneo de Vulnerabilidades. Base de Datos de Plugins. Escaneo de Puertos y Servicios. Actualizaciones Frecuentes.	Código Abierto y Gratuito. Detección de Vulnerabilidades Comunes en Servidores Web	Limitación de Escaneos. No tiene interfaz.

Dmitry	Es una herramienta diseñada para la recopilación de información en pruebas de penetración y auditorías de seguridad. Dmitry facilita la obtención de datos sobre un objetivo particular, como un nombre de dominio o una dirección IP, y ofrece una amplia gama de detalles que resultan útiles para los pentesters o auditores de seguridad [44].	Consultas Whois. Búsqueda de Subdominios. Búsqueda de Correos Electrónicos. Escaneo de Puertos. Recuperación de Tiempo de Actividad.	Simplicidad y Eficiencia. Gratuita y de Código Abierto. Versatilidad.	Carece de actualizaciones. No proporciona una evaluación completa.
Análisis	Luego de realizar el análisis correspondiente, se ha seleccionado 3 Herramientas: Nessus con su interfaz gráfica y un dominio en análisis de			

	servidores, Nmap que es Opensource y en línea de comandos nos permite realizar análisis completo para los servidores y Dmitry que permite conocer los host, dominios, puertos y correos. Se ha descartado la herramienta Nikto ya que es para análisis específicamente de servidores web.
--	---

Tabla 8: Selección de las herramientas

Elaborado por: El investigador.

3.2.2.2 Herramientas de explotación de vulnerabilidades

Herramienta	Concepto	Características	Ventajas	Desventajas
Metasploit  Metasploit	Es un framework de hacking de código abierto, que permite realizar la explotación de vulnerabilidades [45].	Escanear y recopilar información. Identificar y explotar vulnerabilidades mediante el uso de sus módulos: Exploits y Auxiliares.	Fácil uso. Bases de datos de vulnerabilidades en constante actualización.	Curva de aprendizaje para explotación, se necesitan conocimientos preliminares para descartar falsos positivos.
Canvas 	Es Una herramienta comercial de inyección de exploits, facilita la	Explotación de Vulnerabilidades	Calidad de Explotación	Herramienta de Paga.

	automatización de pruebas de penetración y la explotación de vulnerabilidades.			
Análisis	Luego de realizar el análisis correspondiente, se ha seleccionado el Framework Metasploit. Se ha descartado la herramienta Canvas ya que es para el análisis específicamente no necesitamos herramientas de paga.			

Tabla 9: Herramientas de explotación de vulnerabilidades
Elaborado por: El investigador.

3.2.3 Realizar pruebas de penetración

3.2.3.1 Análisis de Vulnerabilidades con Nessus

Para proceder con el Análisis de Vulnerabilidades ingresamos al aplicativo Nessus.

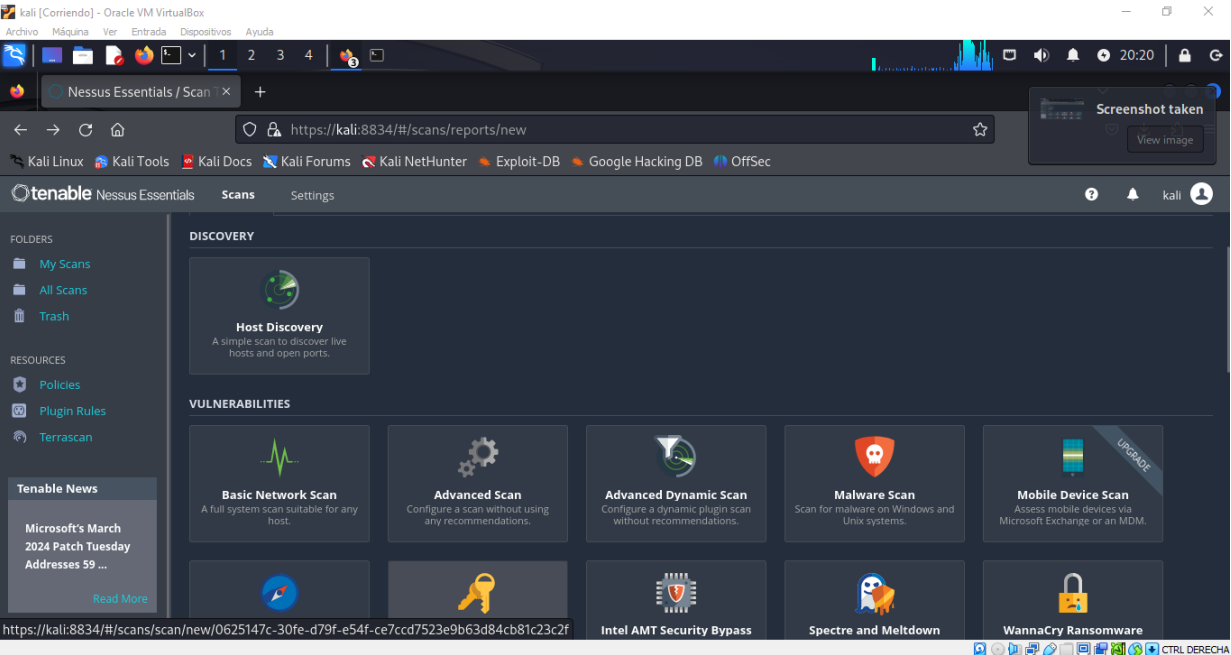


Figura 3.7: Interfaz de Nessus
Elaborado por: El investigador.

Para el análisis de vulnerabilidad de los 7 servidores se procede a crear 7 carpetas con las ips de cada servidor.

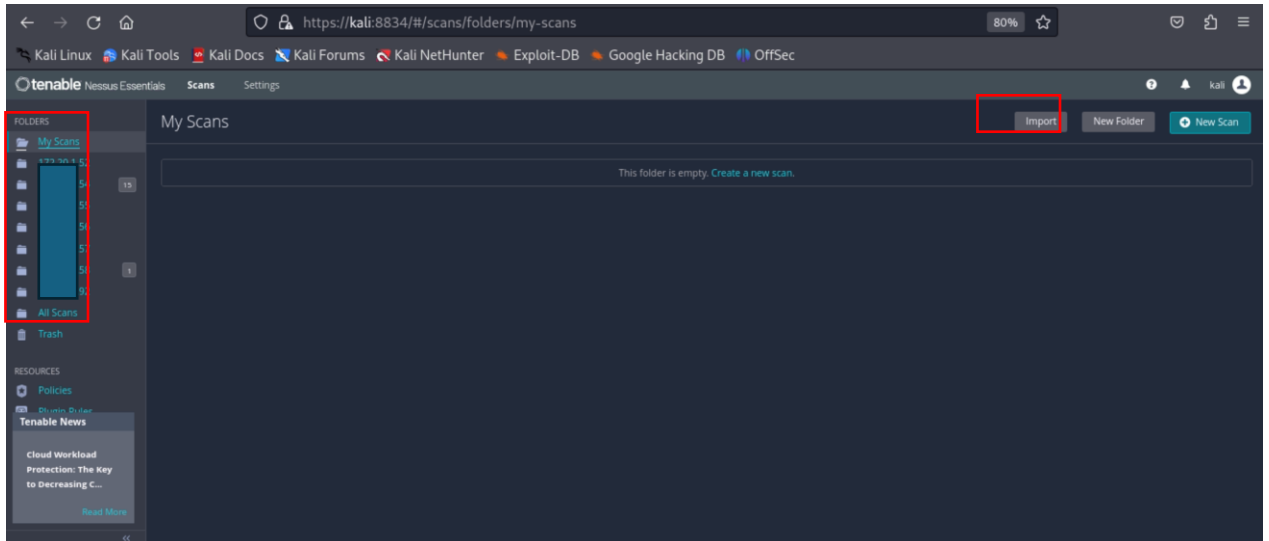


Figura 3.8: Carpetas para realizar el analisis de vulnerabilidades
Elaborado por: El investigador.

Ingresar a la carpeta para la configuracion de los hosts 172.20.1.* y empezar con el escaneo de vulnerabilidades en el ambiente controlado.

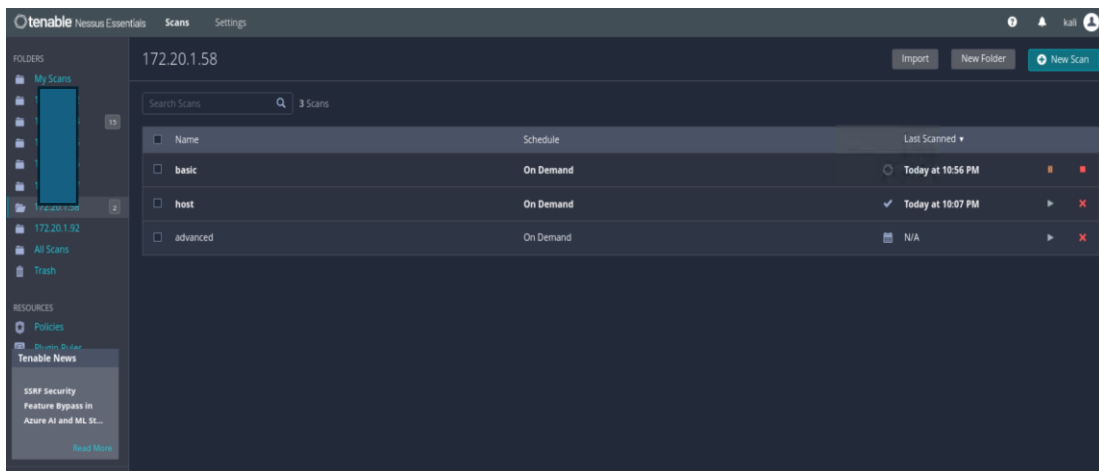


Figura 3.9: Interfaz Nessus, crear New Scan
Elaborado por: El investigador.

En la **Figura 3.10** se muestra los Templates que tiene Nessus para el analisis de vulnerabilidades de acuerdo a las necesidades.

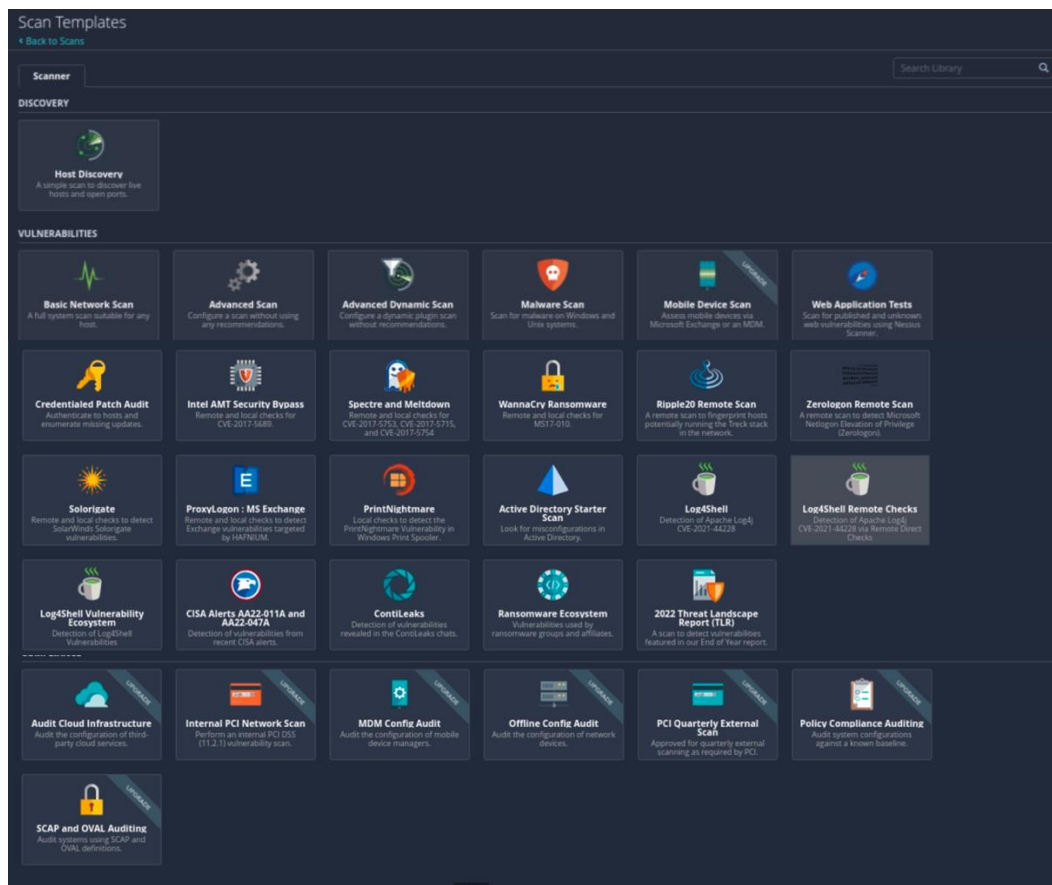


Figura 3.10: Interfaz Nessus, Template de Scan para análisis de vulnerabilidades
Elaborado por: El investigador.

En la **Figura 3.11**, se visualiza los datos ingresamos para el análisis.

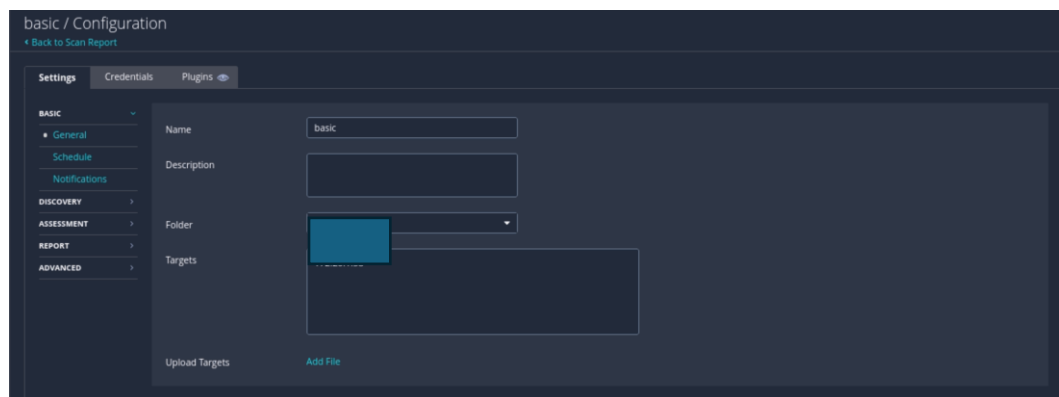


Figura 3.11: Interfaz Nessus, Configuración del scaneo con la ip del servidor
Elaborado por: El investigador.

- **Servidor Virtualizado Active Directory**

Se procede a realizar el análisis de vulnerabilidades en el Servidor y se encontró las siguientes vulnerabilidades:

En la **Figura 3.12**, se visualiza la cantidad de vulnerabilidades encontradas en el AD, 5 grado high y 14 medium, también añade el nombre y el sistema operativo que maneja el AD. Detalle de las vulnerabilidades encontradas:

- 35291 – SSL Certificate Signed Using Weak Hashing Algorithm en grado high. En el reporte de nessus nos indica la solución y el riesgo en Medium

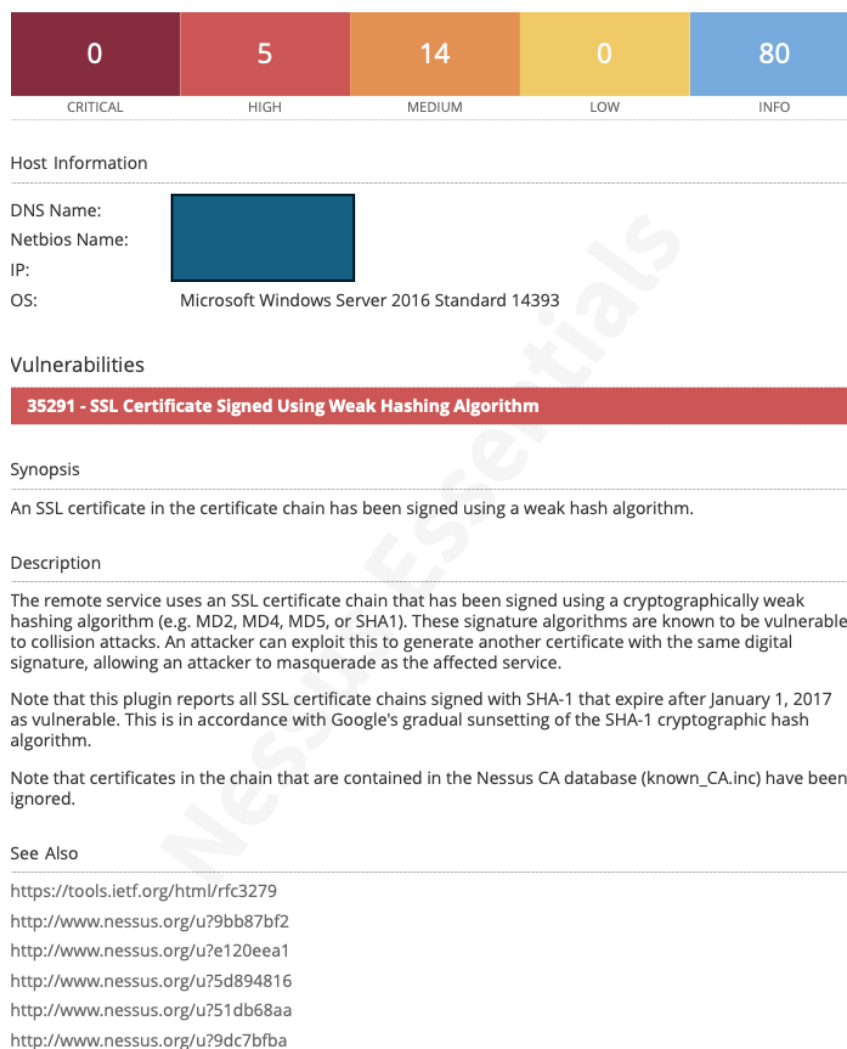


Figura 3.12: Vulnerabilidades SSL Certificate Signed Using Weak Hashing Algorithm
Elaborado por: El investigador.

- En la **Figura 3.13**, se puede visualizar la vulnerabilidad 42873 – SSL Medium Strength Cipher Suites Supported (SWEET32). En el reporte de nessus nos indica la solución y el riesgo en High.

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	
Synopsis	
The remote service supports the use of medium strength SSL ciphers.	
Description	
The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.	
Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.	
See Also	
https://www.openssl.org/blog/blog/2016/08/24/sweet32/ https://sweet32.info	
Solution	
Reconfigure the affected application if possible to avoid use of medium strength ciphers.	
Risk Factor	
Medium	
CVSS v3.0 Base Score	
7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)	
VPR Score	
5.1	
CVSS v2.0 Base Score	
5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)	
References	
CVE	CVE-2016-2183
Plugin Information	
Published: 2009/11/23, Modified: 2021/02/03	

Figura 3.13: Vulnerabilidades SSL Medium Strength Cipher Suites Supported (SWEET32)

Elaborado por: El investigador.

- En la **Figura 3.14**, se puede visualizar la vulnerabilidad 51192 – SSL Certificate Cannot Be Trusted. En el reporte de nessus nos indica la solución y el riesgo en Medium.

51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

See Also

<https://www.itu.int/rec/T-REC-X.509/en>

<https://en.wikipedia.org/wiki/X.509>

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Figura 3.14: Vulnerabilidades SSL Certificate Cannot Be Trusted

Elaborado por: El investigador.

- En la **Figura 3.15** se puede visualizar la vulnerabilidad 58453 – Terminal Services Doesn't use Network Level Authentication (NLA) Only. En el reporte de nessus nos indica la solución y el riesgo en Medium.

58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only
<p>Synopsis</p> <p>The remote Terminal Services doesn't use Network Level Authentication only.</p>
<p>Description</p> <p>The remote Terminal Services is not configured to use Network Level Authentication (NLA) only. NLA uses the Credential Security Support Provider (CredSSP) protocol to perform strong server authentication either through TLS/SSL or Kerberos mechanisms, which protect against man-in-the-middle attacks. In addition to improving authentication, NLA also helps protect the remote computer from malicious users and software by completing user authentication before a full RDP connection is established.</p>
<p>See Also</p> <p>https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732713(v=ws.11) http://www.nessus.org/u?e2628096</p>
<p>Solution</p> <p>Enable Network Level Authentication (NLA) on the remote RDP server. This is generally done on the 'Remote' tab of the 'System' settings on Windows.</p>
<p>Risk Factor</p> <p>Medium</p>
<p>CVSS v3.0 Base Score</p> <p>4.0 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:N/A:N)</p>
<p>CVSS v2.0 Base Score</p> <p>4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)</p>
<p>Plugin Information</p> <p>Published: 2012/03/23, Modified: 2024/05/20</p>
<p>Plugin Output</p> <p>tcp/3389/msrdp</p> <p>Nessus was able to negotiate non-NLA (Network Level Authentication) security.</p>

Figura 3.15: Vulnerabilidades Terminal Services Doesn't use Network Level Authentication (NLA) Only

Elaborado por: El investigador.

- En la **Figura 3.16**, se puede visualizar la vulnerabilidad 157288 – TLS version 1.1 Deprecated Protocol. En el reporte de nessus nos indica la solución y el riesgo en Medium.

157288 - TLS Version 1.1 Deprecated Protocol
Synopsis
The remote service encrypts traffic using an older version of TLS.
Description
The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1
As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.
See Also
https://datatracker.ietf.org/doc/html/rfc8996
http://www.nessus.org/u?c8ae820d
Solution
Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.
Risk Factor
Medium
CVSS v3.0 Base Score
6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)
CVSS v2.0 Base Score
6.1 (CVSS2#AV:N/AC:H/Au:N/C:I/P:A:N)
References
XREF CWE:327
Plugin Information
Published: 2022/04/04, Modified: 2024/05/14
Plugin Output
tcp/3389/msrdp

Figura 3.16: Vulnerabilidades TLS version 1.1 Deprecated Protocol
Elaborado por: El investigador.

Esas son las únicas vulnerabilidades detectadas en el Servidor NAS.

- **Servidor Físico ILO**

Se procede a realizar el análisis de vulnerabilidades en el Servidor y se encontró las siguientes vulnerabilidades:

En la **Figura 3.17**, se visualiza la cantidad de vulnerabilidades encontradas en la ILO, 1 con grado high y 2 con medium, también añade el nombre y el sistema operativo que maneja la ILO. Detalle de las vulnerabilidades encontradas:

- 42873 – SSL Medium Strength Cipher Suites Supported en grado high. En el reporte de nessus nos indica la solución y el riesgo en Medium.

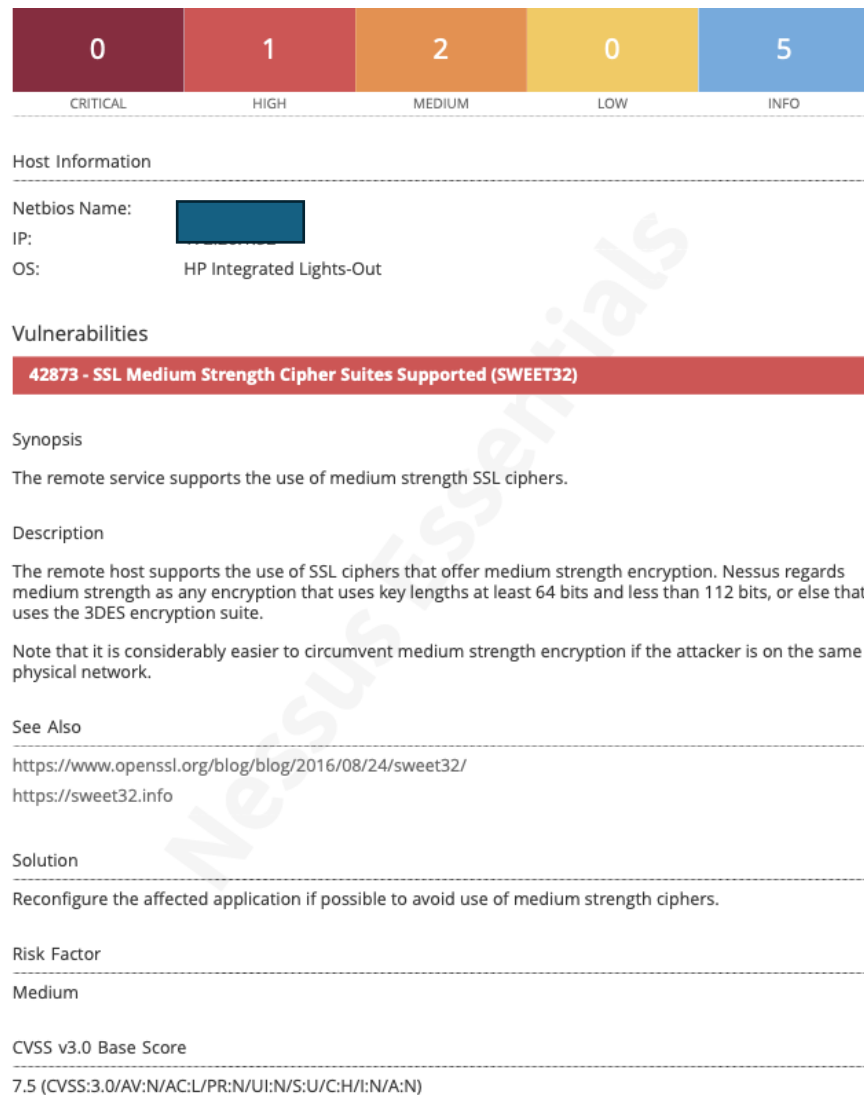


Figura 3.17: Vulnerabilidades SSL Medium Strength Cipher Suites Supported
Elaborado por: El investigador.

- En la **Figura 3.18**, se puede visualizar la vulnerabilidad 51192 – SSL Certificate Cannot Be Trusted. En el reporte de nessus nos indica la solución y el riesgo en Medium.

51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

See Also

<https://www.itu.int/rec/T-REC-X.509/en>

<https://en.wikipedia.org/wiki/X.509>

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Figura 3.18: Vulnerabilidades SSL Certificate Cannot Be Trusted
Elaborado por: El investigador.

- En la **Figura 3.19**, se puede visualizar la vulnerabilidad 45411 – SSL Certificate with Wrong Hostname. En el reporte de nessus nos indica la solución y el riesgo en Medium.

45411 - SSL Certificate with Wrong Hostname

Synopsis

The SSL certificate for this service is for a different host.

Description

The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine.

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

Plugin Information

Published: 2010/04/03, Modified: 2020/04/27

Plugin Output

tcp/443/www

The identities known by Nessus are :

The Common Name in the certificate is :

ILO2M201305JY

The Subject Alternate Name in the certificate is :

ILO2M201305JY

Figura 3.19: Vulnerabilidades SSL Certificate with Wrong Hostname
Elaborado por: El investigador.

Esas son las únicas vulnerabilidades detectadas en el Servidor ILO.

- **Servidor Físico NAS**

Se procede a realizar el análisis de vulnerabilidades en el Servidor y se encontró las siguientes vulnerabilidades.

En la **Figura 3.20**, se visualiza la cantidad de vulnerabilidades encontradas en el NAS, 6 Medium, también anade el nombre y el sistema operativo que maneja el NAS. Detalle de las vulnerabilidades encontradas:

- 57608 – SMB signing not required.

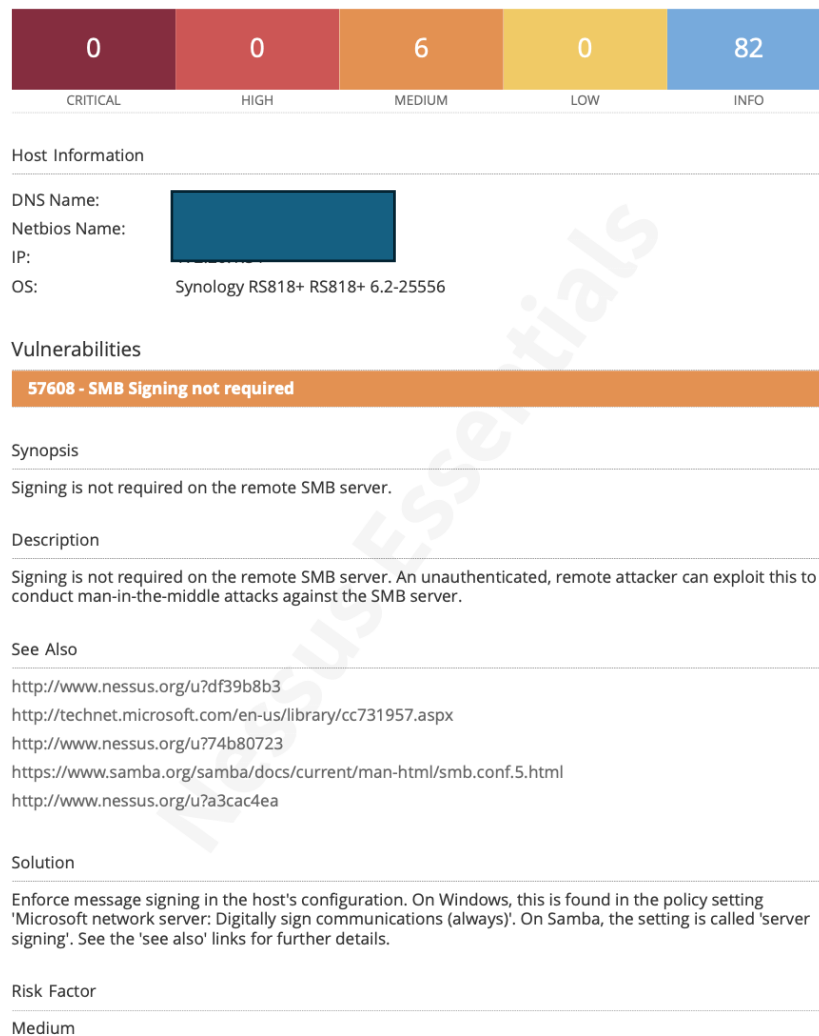


Figura 3.20: Vulnerabilidades SMB Signing not required
Elaborado por: El investigador.

- En la **Figura 3.21**, se puede visualizar la vulnerabilidad 51192 – SSL Certificate Cannot be Trusted. En el reporte de nessus nos indica la solución y el factor de riesgo en Medium.

51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

See Also

<https://www.itu.int/rec/T-REC-X.509/en>

<https://en.wikipedia.org/wiki/X.509>

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Figura 3.21: Vulnerabilidades SSL Certificate Cannot Be Trusted
Elaborado por: El investigador.

- En la **Figura 3.22**, se puede visualizar la vulnerabilidad 45411 – SSL Certificate with Wrong Hostname. En el reporte de nessus nos indica la solución y el factor de riesgo en Medium.

45411 - SSL Certificate with Wrong Hostname
<p>Synopsis</p> <p>The SSL certificate for this service is for a different host.</p>
<p>Description</p> <p>The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine.</p>
<p>Solution</p> <p>Purchase or generate a proper SSL certificate for this service.</p>
<p>Risk Factor</p> <p>Medium</p>
<p>CVSS v3.0 Base Score</p> <p>5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)</p>
<p>CVSS v2.0 Base Score</p> <p>5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)</p>
<p>Plugin Information</p> <p>Published: 2010/04/03, Modified: 2020/04/27</p>
<p>Plugin Output</p> <p>tcp/443/www</p> <div> <p>The identities known by Nessus are :</p> <p>[REDACTED].m</p> <p>The Common Name in the certificate is :</p> <p>synology.com</p> </div>

Figura 3.22: Vulnerabilidades SSL Certificate with Wrong Hostname
Elaborado por: El investigador.

- En la **Figura 3.23**, se puede visualizar la vulnerabilidad 12218 – mDNS Detection (Remote Network). En el reporte de nessus nos indica la solución configurando un filtro para controlar o bloquear este tráfico y el factor de riesgo en Medium.

12218 - mDNS Detection (Remote Network)

Synopsis

It is possible to obtain information about the remote host.

Description

The remote service understands the Bonjour (also known as ZeroConf or mDNS) protocol, which allows anyone to uncover information from the remote host such as its operating system type and exact version, its hostname, and the list of services it is running.

This plugin attempts to discover mDNS used by hosts that are not on the network segment on which Nessus resides.

Solution

Filter incoming traffic to UDP port 5353, if desired.

Risk Factor

Medium

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

Plugin Information

Published: 2004/04/28, Modified: 2021/06/28

Plugin Output

udp/5353/mdns

Nessus was able to extract the following information :

- mDNS hostname	:	
- Advertised services :	:	
o Service name	:	
Port number	:	
o Service name	:	
Port number	:	
o Service name	:	
Port number	:	
o Service name	:	
Port number	:	
o Service name	:	
Port number	:	

Figura 3.23: Vulnerabilidades mDNS Detection
Elaborado por: El investigador.

- En la **Figura 3.24**, se puede visualizar la vulnerabilidad 138595 – phpMyAdmin 4.x < 4.9.4 / 5.x < 5.0.1 SQLI. En el reporte de nessus nos indica la solución que se debe actualizar la versión del phpMyAdmin y como alternativa aplicar parches; y el factor de riesgo en Medium.



Figura 3.24: Vulnerabilidades phpMyAdmin 4.x < 4.9.4 / 5.x < 5.0.1 SQLi
Elaborado por: El investigador.

- En la **Figura 3.25**, se puede visualizar la vulnerabilidad 26194 – Web Server Transmits ClearText Credentials. En el reporte de nessus nos indica como solución que estemos seguros de que todas las comunicaciones se encuentren seguras y protegidas mediante el uso de HTTPS; y el factor de riesgo en Low.

26194 - Web Server Transmits Cleartext Credentials

Synopsis

The remote web server might transmit credentials in cleartext.

Description

The remote web server contains several HTML form fields containing an input of type 'password' which transmit their information to a remote web server in cleartext.

An attacker eavesdropping the traffic between web browser and server may obtain logins and passwords of valid users.

Solution

Make sure that every sensitive form transmits content over HTTPS.

Risk Factor

Low

CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

References

XREF	CWE:522
XREF	CWE:523
XREF	CWE:718
XREF	CWE:724
XREF	CWE:928
XREF	CWE:930

Plugin Information

Published: 2007/09/28, Modified: 2016/11/29

Plugin Output

tcp/80/www

```
Page : /phpMyAdmin/  
Destination Page: /phpMyAdmin/index.php  
  
Page : /phpMyAdmin/index.php  
Destination Page: /phpMyAdmin/index.php
```

Figura 3.25: Vulnerabilidades Web Server Transmits ClearText Credentials
Elaborado por: El investigador.

- En la **Figura 3.26**, se puede visualizar la vulnerabilidad 137702 – Treck TCP/IP stack multiple vulnerabilities. En el reporte de nessus nos indica que necesita que el tráfico ICMP se encuentre bloqueado entre el scanner y el host para que el plugin funcione correctamente; y el factor de riesgo en Critical.

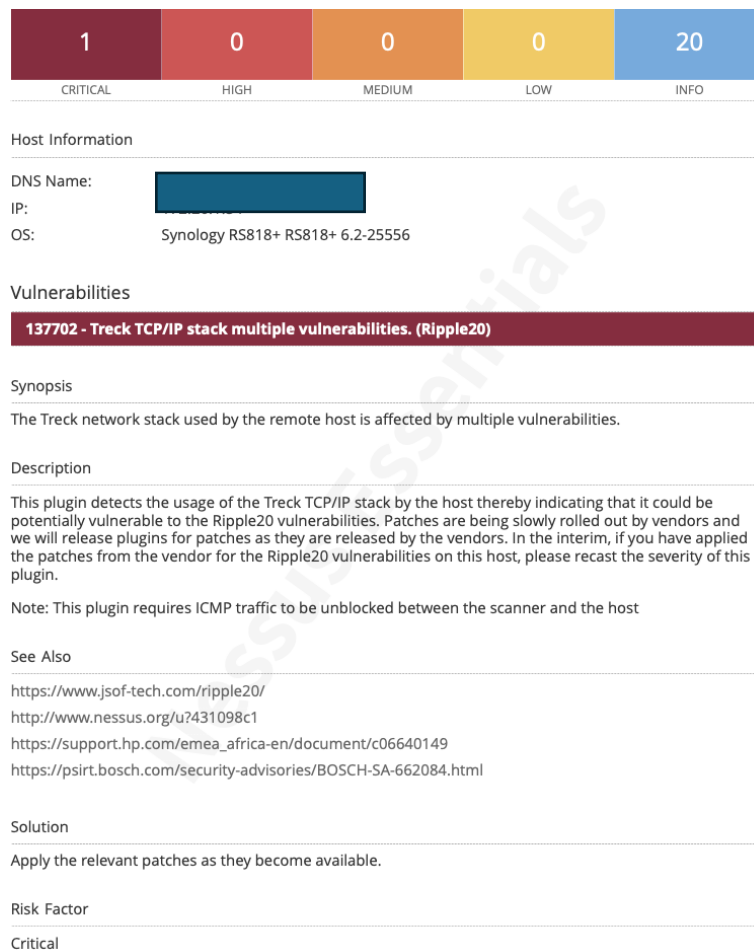


Figura 3.26: Vulnerabilidades Treck TCP/IP stack multiple vulnerabilities
Elaborado por: El investigador.

Esas son las únicas vulnerabilidades detectadas en el Servidor NAS.

- **Servidor Virtualizado del Sistema Informatico Financiero Principal**

Se procede a realizar el analisis de vulnerabilidades en el Servidor y se encontró las siguientes vulnerabilidades.

En la **Figura 3.27**, se visualiza la cantidad de vulnerabilidades encontradas en el El servidor Sif de la aplicación desarrollada en Power builder, son 3 critical, 3 high, 10 medium y 1 low. Detalle de las vulnerabilidades encontradas:

- Vulnerabilidad 125313 – Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (unauthenticated check), este servidor es de sistema operativo Microsoft Windows Server 2008 Standart Service Pack 2 por lo que nos muestra un factor

de riesgo Critico ya que estos sistemas operativo ya no cuentan con actualizaciones y estás a su vez evitan tener un servidor vulnerable.

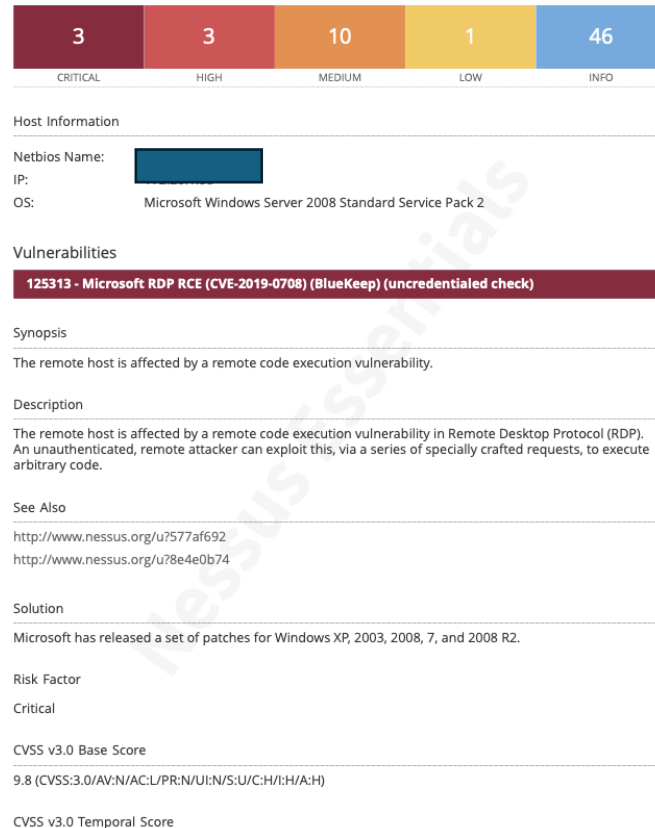


Figura 3.27: Vulnerabilidades Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)

Elaborado por: El investigador.

- En la **Figura 3.28**, se puede visualizar la vulnerabilidad 55786 – Oracle Database Unsupported Version Detection. En el reporte de nessus nos indica que es importante realizar la actualización de la versión de la Oracle para evitar vulnerabilidades de seguridad; y el factor de riesgo en Critical.

55786 - Oracle Database Unsupported Version Detection

Synopsis

The remote host is running an unsupported version of a database server.

Description

According to its version, the installation of Oracle Database running on the remote host is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

See Also

<http://www.nessus.org/u?ccd068d1>

Solution

Upgrade to a version of Oracle Database that is currently supported.

Risk Factor

Critical

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

XREF

IAVA:0001-A-0574

Plugin Information

Published: 2011/08/09, Modified: 2022/09/28

Plugin Output

tcp/1521/oracle_tnslnr

```

Version source      : TNSLSNR for 32-bit Windows: Version 11.1.0.6.0 - Production
TNS for 32-bit Windows: Version 11.1.0.6.0 - Production
Oracle Bequeath NT Protocol Adapter for 32-bit Windows: Version 11.1.0.6.0 - Production
Windows NT Named Pipes NT Protocol Adapter for 32-bit Windows: Version 11.1.0.6.0 - Production
Windows NT TCP/IP NT Protocol Adapter for 32-bit Windows: Version 11.1.0.6.0 - Production,,
Installed version   : 11.1.0.6.0
Supported versions  : 19c / 21c

```

Figura 3.28: Vulnerabilidades Oracle Database Unsupported Version Detection
 Elaborado por: El investigador.

- En la **Figura 3.29**, se puede visualizar la vulnerabilidad 108797 – Unsupported Windows OS (remote). En el reporte de nessus nos indica que es importante una actualización del services pack para mejorar la seguridad del SO; y el factor de riesgo en Critical.

108797 - Unsupported Windows OS (remote)	
Synopsis	The remote OS or service pack is no longer supported.
Description	The remote version of Microsoft Windows is either missing a service pack or is no longer supported. As a result, it is likely to contain security vulnerabilities.
See Also	https://support.microsoft.com/en-us/lifecycle
Solution	Upgrade to a supported service pack or operating system
Risk Factor	Critical
CVSS v3.0 Base Score	10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)
CVSS v2.0 Base Score	10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)
References	XREF IAVA:0001-A-0501
Plugin Information	Published: 2018/04/03, Modified: 2023/07/27
Plugin Output	tcp/0
The following Windows version is installed and not supported: Microsoft Windows Server 2008 Standard Service Pack 2	

Figura 3.29: Vulnerabilidades Unsupported Windows OS (remote)
Elaborado por: El investigador.

- En la **Figura 3.30**, se puede visualizar la vulnerabilidad 69552 – Oracle TNS Listener Remote. En el reporte de nessus nos indica que debemos seguir instrucciones de Oracle para implementar una alternativa y corregir de manera temporal hasta implementar una solución definitiva y el factor de riesgo en High.

69552 - Oracle TNS Listener Remote Poisoning
<p>Synopsis</p> <p>It was possible to register with a remote Oracle TNS listener.</p>
<p>Description</p> <p>The remote Oracle TNS listener allows service registration from a remote host. An attacker can exploit this issue to divert data from a legitimate database server or client to an attacker-specified system.</p> <p>Successful exploits will allow the attacker to manipulate database instances, potentially facilitating man-in-the-middle, session- hijacking, or denial of service attacks on a legitimate database server.</p>
<p>See Also</p> <p>http://www.nessus.org/u78c8334e6 http://www.nessus.org/u706d298e5 https://seclists.org/fulldisclosure/2012/Apr/204</p>
<p>Solution</p> <p>Apply the workaround in Oracle's advisory.</p>
<p>Risk Factor</p> <p>High</p>
<p>CVSS v3.0 Base Score</p> <p>7.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L)</p>
<p>CVSS v3.0 Temporal Score</p> <p>6.8 (CVSS:3.0/E:F/RL:O/RC:C)</p>
<p>VPR Score</p> <p>4.9</p>
<p>CVSS v2.0 Base Score</p> <p>7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)</p>
<p>CVSS v2.0 Temporal Score</p> <p>6.8 (CVSS2#E:F/RL:W/RC:C)</p>

Figura 3.30: Vulnerabilidades Oracle TNS Listener Remote
 Elaborado por: El investigador.

- En la **Figura 3.31**, se puede visualizar la vulnerabilidad 35291 – SSL Certificate Signed Using Weak Hashing Algorithm. En el reporte de nessus nos indica que debemos realizar un proceso de remisión de firma de certificado y esta a su vez ser enviado a la CA, y el factor de riesgo en Medium.

35291 - SSL Certificate Signed Using Weak Hashing Algorithm

Synopsis

An SSL certificate in the certificate chain has been signed using a weak hash algorithm.

Description

The remote service uses an SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g. MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks. An attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service.

Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.

Note that certificates in the chain that are contained in the Nessus CA database (known_CA.inc) have been ignored.

See Also

<https://tools.ietf.org/html/rfc3279>
<http://www.nessus.org/u?9bb87bf2>
<http://www.nessus.org/u?e120eea1>
<http://www.nessus.org/u?5d894816>
<http://www.nessus.org/u?51db68aa>
<http://www.nessus.org/u?9dc7bfba>

Solution

Contact the Certificate Authority to have the SSL certificate reissued.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N)

CVSS v3.0 Temporal Score

6.7 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

4.9

Figura 3.31: Vulnerabilidades SSL Certificate Signed Using Weak Hashing Algorithm
Elaborado por: El investigador.

- En la **Figura 3.32**, se puede visualizar la vulnerabilidad 42873 – SSL Medium Strength Cipher Suites Supported (SWEET32). En el reporte de nessus nos indica que debemos realizar un cambio de referencia en el algoritmo de compresión de fuerza media a compresión más fuerte, y el factor de riesgo en Medium.

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)

Synopsis

The remote service supports the use of medium strength SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

See Also

<https://www.openssl.org/blog/blog/2016/08/24/sweet32/>
<https://sweet32.info>

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

VPR Score

6.1

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

References

CVE CVE-2016-2183

Plugin Information

Published: 2009/11/23, Modified: 2021/02/03

Figura 3.32: Vulnerabilidades SSL Medium Strength Cipher Suites Supported (SWEET32)

Elaborado por: El investigador.

- En la **Figura 3.33**, se puede visualizar la vulnerabilidad 18405 – Remote Desktop Protocol Server Man-in-the-Middle Weakness. En el reporte de nessus nos indica que debemos realizar la configuración de un certificado SSL en el servidor y que sirva de comunicación y configurar el escritorio remoto más seguro, y el factor de riesgo en Medium.

18405 - Remote Desktop Protocol Server Man-in-the-Middle Weakness
<p>Synopsis</p> <p>It may be possible to get access to the remote host.</p>
<p>Description</p> <p>The remote version of the Remote Desktop Protocol Server (Terminal Service) is vulnerable to a man-in-the-middle (MITM) attack. The RDP client makes no effort to validate the identity of the server when setting up encryption. An attacker with the ability to intercept traffic from the RDP server can establish encryption with the client and server without being detected. A MITM attack of this nature would allow the attacker to obtain any sensitive information transmitted, including authentication credentials.</p> <p>This flaw exists because the RDP server stores a publicly known hard-coded RSA private key. Any attacker in a privileged network location can use the key for this attack.</p>
<p>See Also</p> <p>http://www.nessus.org/u78033da0d</p>
<p>Solution</p> <p>- Force the use of SSL as a transport layer for this service if supported, or/and</p> <p>- On Microsoft Windows operating systems, select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available.</p>
<p>Risk Factor</p> <p>Medium</p>
<p>CVSS v3.0 Base Score</p> <p>6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)</p>
<p>VPR Score</p> <p>2.5</p>
<p>CVSS v2.0 Base Score</p> <p>5.1 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)</p>
<p>CVSS v2.0 Temporal Score</p> <p>3.8 (CVSS2#E:U/RL:OF/RC:C)</p>
<p>References</p>

Figura 3.33: Vulnerabilidades Remote Desktop Protocol Server Man-in-the-Middle Weakness

Elaborado por: El investigador.

- En la **Figura 3.34**, se puede visualizar la vulnerabilidad 57608 – SMB Signing not required. En el reporte de nessus nos indica que debemos revisar la política de firma de mensajes digitales en nuestro servidor y verificar que se encuentre habilitada, y el factor de riesgo en Medium.

57608 - SMB Signing not required

Synopsis

Signing is not required on the remote SMB server.

Description

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

See Also

<http://www.nessus.org/u?df39b8b3>

<http://technet.microsoft.com/en-us/library/cc731957.aspx>

<http://www.nessus.org/u?74b80723>

<https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html>

<http://www.nessus.org/u?a3cac4ea>

Solution

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

CVSS v3.0 Temporal Score

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

Plugin Information

Figura 3.34: Vulnerabilidades SMB Signing not required
Elaborado por: El investigador.

- En la **Figura 3.35**, se puede visualizar la vulnerabilidad 51192 – SSL Certificate Cannot Be Trusted. En el reporte de nessus nos indica que debemos adquirir un certificado SSL y validarlo en CA, y el factor de riesgo en Medium.

51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

See Also

<https://www.itu.int/rec/T-REC-X.509/en>

<https://en.wikipedia.org/wiki/X.509>

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Figura 3.35: Vulnerabilidades SSL Certificate Cannot Be Trusted
Elaborado por: El investigador.

- En la **Figura 3.36**, se puede visualizar la vulnerabilidad 45411 – SSL Certificate with Wrong Hostname. En el reporte de nessus nos indica que debemos adquirir un certificado SSL y validarlo en CA, y el factor de riesgo en Medium.

45411 - SSL Certificate with Wrong Hostname

Synopsis

The SSL certificate for this service is for a different host.

Description

The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine.

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

Plugin Information

Published: 2010/04/03, Modified: 2020/04/27

Plugin Output

tcp/3389/msrdp

Figura 3.36: Vulnerabilidades SSL Certificate with Wrong Hostname

Elaborado por: El investigador.

- En la **Figura 3.37**, se puede visualizar la vulnerabilidad 65821 – SSL RC4 Cipher Suites Supported (Bar Mitzvah). En el reporte de nessus nos indica que debemos actualizar la configuración del servidor para el uso de TLS 1.2 o superior y el uso de suites de cifrado seguras como AES, y el factor de riesgo en Medium.

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Synopsis

The remote service supports the use of the RC4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites.

The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

See Also

<https://www.rc4nomore.com/>

<http://www.nessus.org/u?ac7327a0>

<http://cr.yp.to/talks/2013.03.12/slides.pdf>

<http://www.isg.rhul.ac.uk/tls/>

https://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

Risk Factor

Medium

CVSS v3.0 Base Score

5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

5.4 (CVSS:3.0/E:U/RL:X/RC:C)

VPR Score

3.6

CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

Figura 3.37: Vulnerabilidades SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Elaborado por: El investigador.

- En la **Figura 3.38**, se puede visualizar la vulnerabilidad 57582 – SSL Self-Signed Certificate. En el reporte de nessus nos indica que debemos adquirir un certificado SSL y validarlo en CA, y el factor de riesgo en Medium.

57582 - SSL Self-Signed Certificate

Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin Information

Published: 2012/01/17, Modified: 2022/06/14

Plugin Output

tcp/3389/msrdp

The following certificate was found at the top of the certificate chain sent by the remote host, but is self-signed and was not found in the list of known certificate authorities :

Figura 3.38: Vulnerabilidades Signed Certificate
Elaborado por: El investigador.

- En la **Figura 3.39**, se puede visualizar la vulnerabilidad 57582 – TLS Version 1.0 Protocol Detection. En el reporte de nessus nos indica que se debe actualizar la configuración del servidor para el uso de TLS 1.2 o superior, y el factor de riesgo en Medium.

104743 - TLS Version 1.0 Protocol Detection	
Synopsis	
The remote service encrypts traffic using an older version of TLS.	
Description	
<p>The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.</p> <p>As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.</p> <p>PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.</p>	
See Also	
https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00	
Solution	
Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.	
Risk Factor	
Medium	
CVSS v3.0 Base Score	
6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)	
CVSS v2.0 Base Score	
6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)	
References	
XREF	CWE:327
Plugin Information	
Published: 2017/11/22, Modified: 2023/04/19	
Plugin Output	

Figura 3.39: Vulnerabilidades TLS Version 1.0 Protocol Detection
Elaborado por: El investigador.

- En la **Figura 3.40**, se puede visualizar la vulnerabilidad 157288 – TLS Version 1.1 Protocol Detection. En el reporte de nessus nos indica que se debe actualizar la configuración del servidor para el uso de TLS 1.2 o superior, y el factor de riesgo en Medium.

157288 - TLS Version 1.1 Protocol Deprecated	
Synopsis	
The remote service encrypts traffic using an older version of TLS.	
Description	
The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1	
As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.	
See Also	
https://datatracker.ietf.org/doc/html/rfc8996 http://www.nessus.org/u?c8ae820d	
Solution	
Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.	
Risk Factor	
Medium	
CVSS v3.0 Base Score	
6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)	
CVSS v2.0 Base Score	
6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)	
References	
XREF	CWE:327
Plugin Information	
Published: 2022/04/04, Modified: 2023/04/19	
Plugin Output	
tcp/3389/msrdp	

Figura 3.40: Vulnerabilidades TLS Version 1.1 Protocol Detection
Elaborado por: El investigador.

- En la **Figura 3.41**, se puede visualizar la vulnerabilidad 58453 – Terminal Services Doesn’t Use Network Level Authentication (NLA) Only. En el reporte de nessus nos indica que se debe habilitar NLA que nos proporciona una capa adicional de seguridad para el entorno de Escritorio Remoto ya que asegura que los usuarios autorizados puedan establecer conexiones RDP, y el factor de riesgo en Medium.

58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only

Synopsis

The remote Terminal Services doesn't use Network Level Authentication only.

Description

The remote Terminal Services is not configured to use Network Level Authentication (NLA) only. NLA uses the Credential Security Support Provider (CredSSP) protocol to perform strong server authentication either through TLS/SSL or Kerberos mechanisms, which protect against man-in-the-middle attacks. In addition to improving authentication, NLA also helps protect the remote computer from malicious users and software by completing user authentication before a full RDP connection is established.

See Also

[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732713\(v=ws.11\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732713(v=ws.11))

<http://www.nessus.org/u?e2628096>

Solution

Enable Network Level Authentication (NLA) on the remote RDP server. This is generally done on the 'Remote' tab of the 'System' settings on Windows.

Risk Factor

Medium

CVSS v3.0 Base Score

4.0 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:N/A:N)

CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

Plugin Information

Published: 2012/03/23, Modified: 2024/02/21

Plugin Output

tcp/3389/msrdp

Nessus was able to negotiate non-NLA (Network Level Authentication) security.

Figura 3.41: Vulnerabilidades Terminal Services Doesn't Use Network Level Authentication (NLA) Only

Elaborado por: El investigador.

- En la **Figura 3.42**, se puede visualizar la vulnerabilidad 57690 – Terminal Services Encryption Level is Medium or Low. En el reporte de nessus nos indica que se debe cambiar la encriptación de nivel del RDP a High o FIPS Compilant, y el factor de riesgo en Medium.

57690 - Terminal Services Encryption Level is Medium or Low

Synopsis

The remote host is using weak cryptography.

Description

The remote Terminal Services service is not configured to use strong cryptography.

Using weak cryptography with this service may allow an attacker to eavesdrop on the communications more easily and obtain screenshots and/or keystrokes.

Solution

Change RDP encryption level to one of :

3. High

4. FIPS Compliant

Risk Factor

Medium

CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

Plugin Information

Published: 2012/01/25, Modified: 2024/02/22

Plugin Output

tcp/3389/msrdp

The terminal services encryption level is set to :

2. Medium

Figura 3.42: Vulnerabilidades Terminal Services Encryption Level is Medium or Low

Elaborado por: El investigador.

- En la **Figura 3.43**, se puede visualizar la vulnerabilidad 30218 – Terminal Services Encryption Level is not FIPS-140 Compliant. En el reporte de nessus nos indica que se debe cambiar la encriptación de nivel del RDP a FIPS Compliant, y el factor de riesgo en Low.

30218 - Terminal Services Encryption Level is not FIPS-140 Compliant
Synopsis
The remote host is not FIPS-140 compliant.
Description
The encryption setting used by the remote Terminal Services service is not FIPS-140 compliant.
Solution
Change RDP encryption level to :
4. FIPS Compliant
Risk Factor
Low
CVSS v2.0 Base Score
2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)
Plugin Information
Published: 2008/02/11, Modified: 2024/02/22
Plugin Output
tcp/3389/msrdp
<pre> The terminal services encryption level is set to : 2. Medium (Client Compatible) </pre>

Figura 3.43: Vulnerabilidades Terminal Services Encryption Level is not FIPS-140 Compliant

Elaborado por: El investigador.

Esas son las únicas vulnerabilidades detectadas en el Servidor de la aplicación SIF Principal.

- **Servidor Físico VEAMBACKUP de respaldos de la máquinas virtuales y bases de datos**

Se procede a realizar el analisis de vulnerabilidades en el Servidor y se encontró las siguientes vulnerabilidades.

En la **Figura 3.44** hasta la **Figura 3.51**, se visualiza la cantidad de vulnerabilidades encontradas en el servidor Veambackup, este servidor al ser un backup del servidor SIF principal muestra las mismas vulnerabilidades, son 5 high, 14 medium. Detalle de las vulnerabilidades encontradas a breves rasgos:

- Vulnerabilidad 35291 – SSL Certificate Signed Using Weak Hashing Algorithm, este servidor es de sistema operativo Microsoft Windows Server 2016 Standard 14393. En el reporte de nessus nos indica que debemos realizar un proceso de remisión de firma de certificado y esta a su vez ser enviado a la CA, y el factor de riesgo en high.

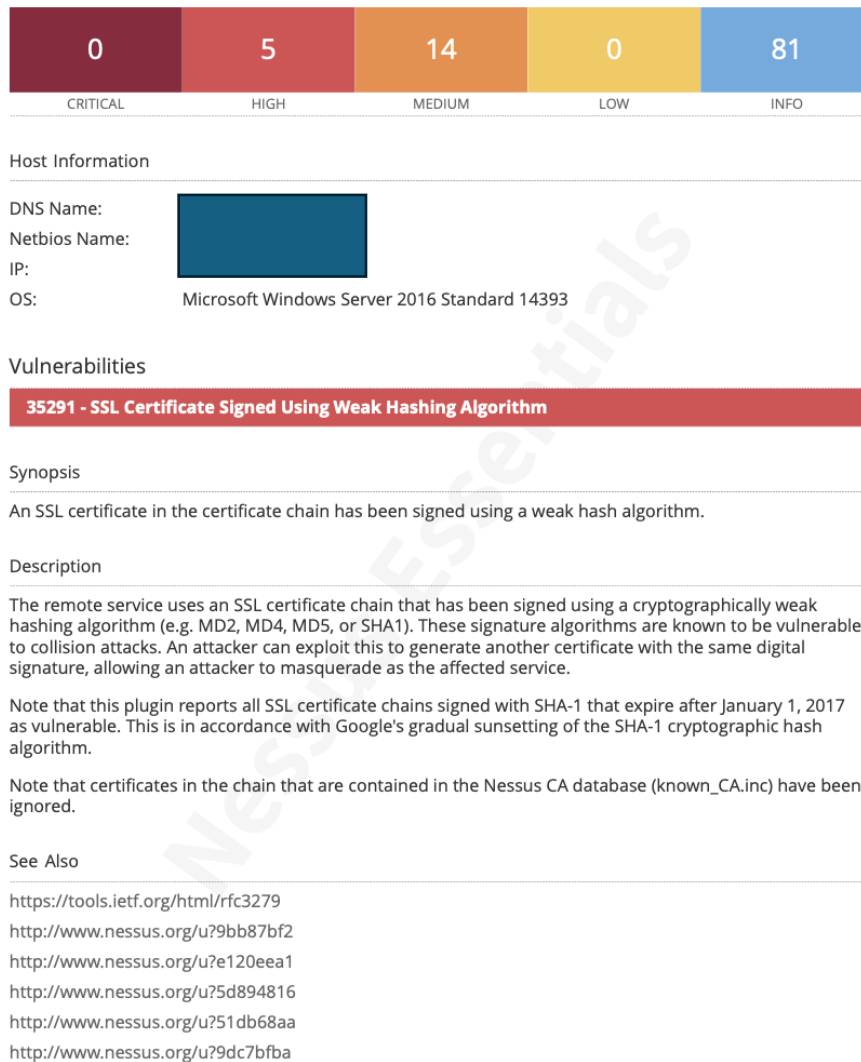


Figura 3.44: Vulnerabilidades SSL Certificate Signed Using Weak Hashing Algorithm
Elaborado por: El investigador.

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)

Synopsis

The remote service supports the use of medium strength SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

See Also

<https://www.openssl.org/blog/blog/2016/08/24/sweet32/>

<https://sweet32.info>

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

VPR Score

6.1

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

References

CVE CVE-2016-2183

Plugin Information

Published: 2009/11/23, Modified: 2021/02/03

Figura 3.45: Vulnerabilidades SSL Medium Strength Cipher Suites Supported (SWEET32)

Elaborado por: El investigador.

51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

See Also

<https://www.itu.int/rec/T-REC-X.509/en>

<https://en.wikipedia.org/wiki/X.509>

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Figura 3.46: Vulnerabilidades SSL Certificate Cannot Be Trusted
Elaborado por: El investigador.

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Synopsis

The remote service supports the use of the RC4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites.

The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

See Also

<https://www.rc4nomore.com/>

<http://www.nessus.org/u?ac7327a0>

<http://cr.yp.to/talks/2013.03.12/slides.pdf>

<http://www.isg.rhul.ac.uk/tls/>

https://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

Risk Factor

Medium

CVSS v3.0 Base Score

5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

5.4 (CVSS:3.0/E:U/RL:X/RC:C)

VPR Score

3.6

CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

Figura 3.47: Vulnerabilidades SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Elaborado por: El investigador.

57582 - SSL Self-Signed Certificate

Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin Information

Published: 2012/01/17, Modified: 2022/06/14

Plugin Output

tcp/3389/msrdp

The following certificate was found at the top of the certificate chain sent by the remote host, but is self-signed and was not found in the list of known certificate authorities :

Figura 3.48: Vulnerabilidades SSL Self-Signed Certificate
Elaborado por: El investigador.

104743 - TLS Version 1.0 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

See Also

<https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00>

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

CVSS v2.0 Base Score

6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)

References

XREF CWE:327

Plugin Information

Published: 2017/11/22, Modified: 2023/04/19

Plugin Output

Figura 3.49: Vulnerabilidades TLS Version 1.0 Protocol Detection
Elaborado por: El investigador.

157288 - TLS Version 1.1 Protocol Deprecated

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1.

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

See Also

<https://datatracker.ietf.org/doc/html/rfc8996>

<http://www.nessus.org/u?c8ae820d>

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

CVSS v2.0 Base Score

6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)

References

XREF CWE:327

Plugin Information

Published: 2022/04/04, Modified: 2023/04/19

Plugin Output

tcp/636/ldap

Figura 3.50: Vulnerabilidades TLS Version 1.1 Protocol Deprecated
Elaborado por: El investigador.

58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only
<p>Synopsis</p> <p>The remote Terminal Services doesn't use Network Level Authentication only.</p>
<p>Description</p> <p>The remote Terminal Services is not configured to use Network Level Authentication (NLA) only. NLA uses the Credential Security Support Provider (CredSSP) protocol to perform strong server authentication either through TLS/SSL or Kerberos mechanisms, which protect against man-in-the-middle attacks. In addition to improving authentication, NLA also helps protect the remote computer from malicious users and software by completing user authentication before a full RDP connection is established.</p>
<p>See Also</p> <p>https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732713(v=ws.11) http://www.nessus.org/u?e2628096</p>
<p>Solution</p> <p>Enable Network Level Authentication (NLA) on the remote RDP server. This is generally done on the 'Remote' tab of the 'System' settings on Windows.</p>
<p>Risk Factor</p> <p>Medium</p>
<p>CVSS v3.0 Base Score</p> <p>4.0 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:N/A:N)</p>
<p>CVSS v2.0 Base Score</p> <p>4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)</p>
<p>Plugin Information</p> <p>Published: 2012/03/23, Modified: 2024/02/21</p>
<p>Plugin Output</p> <p>tcp/3389/msrdp</p> <p>Nessus was able to negotiate non-NLA (Network Level Authentication) security.</p>

Figura 3.51: Vulnerabilidades Terminal Services Doesn't Use Network Level Authentication (NLA) Only
Elaborado por: El investigador.

Esas son las únicas vulnerabilidades detectadas en el Servidor de la aplicación Veambackup.

- Servidor Virtualizado Procesos Automáticos**

Se procede a realizar el analisis de vulnerabilidades en el Servidor y se encontró las siguientes vulnerabilidades.

En la **Figura 3.52**, se visualiza la cantidad de vulnerabilidades encontradas en el servidor de Procesos Automáticos, son 2 critical, 2 high, 5 medium, 3 low, dentro de este grupo se anadio vulnerabilidades encontradas al realizar escaneo de aplicaciones web. Detalle de las vulnerabilidades encontradas a breves rasgos:

- Vulnerabilidad 34460 – Unsupported Web Server Detection, este servidor es de sistema operativo Microsoft Windows Server 2008 R2 Standard Service Pack 1. En el reporte de nessus nos indica que debemos migrar o actualizar el servicio web a una versión actual esto permite mejorar la seguridad y evitar mantener servicios obsoletos, y el factor de riesgo se encuentra en critical.

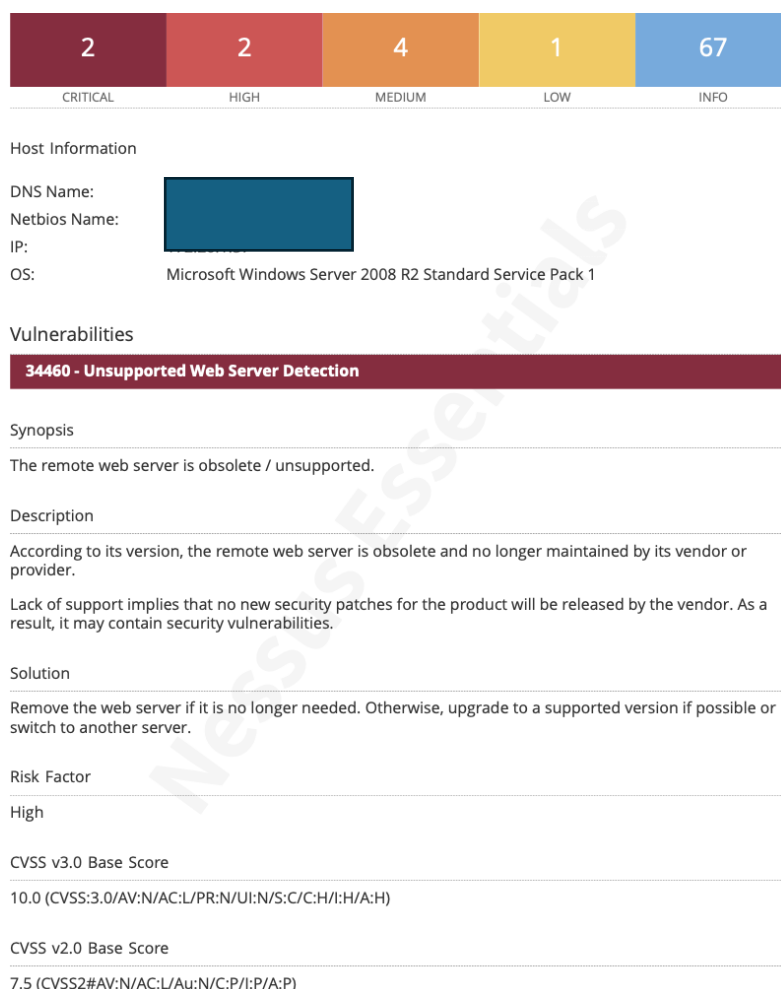


Figura 3.52: Vulnerabilidades Unsupported Web Server Detection
Elaborado por: El investigador.

- En la **Figura 3.53**, se puede visualizar la vulnerabilidad 108797 – Unsupported Windows OS (remote). En el reporte de nessus nos indica que se debe realizar un upgrade del sistema operativo, y el factor de riesgo se encuentra en critical.

108797 - Unsupported Windows OS (remote)	
Synopsis	
The remote OS or service pack is no longer supported.	
Description	
The remote version of Microsoft Windows is either missing a service pack or is no longer supported. As a result, it is likely to contain security vulnerabilities.	
See Also	
https://support.microsoft.com/en-us/lifecycle	
Solution	
Upgrade to a supported service pack or operating system	
Risk Factor	
Critical	
CVSS v3.0 Base Score	
10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)	
CVSS v2.0 Base Score	
10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)	
References	
XREF	IAVA:0001-A-0501
Plugin Information	
Published: 2018/04/03, Modified: 2023/07/27	
Plugin Output	
tcp/0	
<p>The following Windows version is installed and not supported:</p> <p>Microsoft Windows Server 2008 R2 Standard Service Pack 1</p>	

Figura 3.53: Vulnerabilidades Unsupported Windows OS (remote)

Elaborado por: El investigador.

- En la **Figura 3.54**, se puede visualizar la vulnerabilidad 110192 – Oracle GlassFish Server Path Traversal. En el reporte de nessus nos indica que se puede manipular las rutas de los archivos de la aplicación web y como solución solicita que se debe contactar con el proveedor de Oracle para realizar las

actualizaciones correspondientes y evitar vulnerabilidades, y el factor de riesgo se encuentra en high.

110192 - Oracle GlassFish Server Path Traversal	
Synopsis	
The remote web application server is affected by a path traversal vulnerability.	
Description	
The instance of Oracle GlassFish Server running on the remote host is affected by an authenticated and unauthenticated path traversal vulnerability. Remote attacker can exploit this issue, via a specially crafted HTTP request, to access arbitrary files on the remote host.	
See Also	
http://www.nessus.org/u?159578ad	
Solution	
Contact to vendor for patch options.	
Risk Factor	
Medium	
CVSS v3.0 Base Score	
7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)	
CVSS v3.0 Temporal Score	
7.3 (CVSS:3.0/E:F/RL:U/RC:X)	
VPR Score	
4.4	
CVSS v2.0 Base Score	
5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)	
CVSS v2.0 Temporal Score	
4.8 (CVSS2#E:F/RL:U/RC:ND)	
References	
CVE	CVE-2017-1000028
XREF	EDB-ID:39441

Figura 3.54: Vulnerabilidades Oracle GlassFish Server Path Traversal
Elaborado por: El investigador.

- En la **Figura 3.55**, se puede visualizar la vulnerabilidad 110612 – Oracle GlassFish Server URL normalization Denial of Service. En el reporte de nessus nos indica que se puede manipular las rutas, filtros de seguridad o XSS y como solución solicita que se debe contactar con el proveedor de Oracle o lanzar actualizaciones y evitar vulnerabilidades, y el factor de riesgo se encuentra en high.

110612 - Oracle GlassFish Server URL normalization Denial of Service

Synopsis

The remote application is vulnerable to a denial of service attack.

Description

The instance of Oracle GlassFish Server running on the remote host is affected by an authenticated and unauthenticated denial of service vulnerability.

The vulnerability is a result of an infinite loop in the normalize() method in com.sun.jsftemplating.util.filestreamer.ResourceContentSource.

A remote attacker can exploit this issue, via a specially crafted HTTP request to Admin Console component.

See Also

<http://www.nessus.org/u?81fcff67>

Solution

Contact to vendor for patch options.

Risk Factor

High

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVSS v2.0 Base Score

7.8 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:C)

References

XREF TRA:TRA-2018-06

Plugin Information

Published: 2018/06/19, Modified: 2018/09/17

Plugin Output

tcp/4848/www

Figura 3.55: Vulnerabilidades Oracle GlassFish Server URL normalization Denial of Service

Elaborado por: El investigador.

- **En la Figura 3.56**, se puede visualizar la vulnerabilidad 18405 – Remote Desktop Protocol Server Man-in-the-Middle Weakness. En el reporte de nessus nos indica que debemos realizar la configuración de un certificado SSL en el servidor y que sirva de comunicación y configurar el escritorio remoto más seguro, y el factor de riesgo en Medium.

18405 - Remote Desktop Protocol Server Man-in-the-Middle Weakness

Synopsis

It may be possible to get access to the remote host.

Description

The remote version of the Remote Desktop Protocol Server (Terminal Service) is vulnerable to a man-in-the-middle (MiTM) attack. The RDP client makes no effort to validate the identity of the server when setting up encryption. An attacker with the ability to intercept traffic from the RDP server can establish encryption with the client and server without being detected. A MiTM attack of this nature would allow the attacker to obtain any sensitive information transmitted, including authentication credentials.

This flaw exists because the RDP server stores a publicly known hard-coded RSA private key. Any attacker in a privileged network location can use the key for this attack.

See Also

<http://www.nessus.org/u?8033da0d>

Solution

- Force the use of SSL as a transport layer for this service if supported, or/and
- On Microsoft Windows operating systems, select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

VPR Score

2.5

CVSS v2.0 Base Score

5.1 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

3.8 (CVSS2#E:U/RL:OF/RC:C)

Figura 3.56: Vulnerabilidades Remote Desktop Protocol Server Man-in-the-Middle Weakness

Elaborado por: El investigador.

- **En la Figura 3.57,** se puede visualizar la vulnerabilidad 57608 – SMB Signing not required. En el reporte de nessus nos indica que debemos revisar la política de firma de mensajes digitales en nuestro servidor y verificar que se encuentre habilitada, y el factor de riesgo en Medium.

57608 - SMB Signing not required

Synopsis

Signing is not required on the remote SMB server.

Description

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

See Also

<http://www.nessus.org/u?df39b8b3>

<http://technet.microsoft.com/en-us/library/cc731957.aspx>

<http://www.nessus.org/u?74b80723>

<https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html>

<http://www.nessus.org/u?a3cac4ea>

Solution

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

CVSS v3.0 Temporal Score

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

Plugin Information

Figura 3.57: Vulnerabilidades SMB Signing not required

Elaborado por: El investigador.

- **En la Figura 3.58**, se puede visualizar la vulnerabilidad 58453 – Terminal Services Doesn't use Network Level Authentication (NLA) Only. En el reporte de nessus nos indica que debemos revisar la política de firma de mensajes digitales en nuestro servidor y verificar que se encuentre habilitada, y el factor de riesgo en Medium.

58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only

Synopsis

The remote Terminal Services doesn't use Network Level Authentication only.

Description

The remote Terminal Services is not configured to use Network Level Authentication (NLA) only. NLA uses the Credential Security Support Provider (CredSSP) protocol to perform strong server authentication either through TLS/SSL or Kerberos mechanisms, which protect against man-in-the-middle attacks. In addition to improving authentication, NLA also helps protect the remote computer from malicious users and software by completing user authentication before a full RDP connection is established.

See Also

[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732713\(v=ws.11\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732713(v=ws.11))

<http://www.nessus.org/u?e2628096>

Solution

Enable Network Level Authentication (NLA) on the remote RDP server. This is generally done on the 'Remote' tab of the 'System' settings on Windows.

Risk Factor

Medium

CVSS v3.0 Base Score

4.0 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:N/A:N)

CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

Plugin Information

Published: 2012/03/23, Modified: 2024/02/21

Plugin Output

tcp/3389/msrdp

Nessus was able to negotiate non-NLA (Network Level Authentication) security.

Figura 3.58: Vulnerabilidades Terminal Services Doesn't use Network Level Authentication (NLA) Only

Elaborado por: El investigador.

- **En la Figura 3.59**, se puede visualizar la vulnerabilidad 57690 – Terminal Services Encryption Level is Medium or Low. En el reporte de nessus nos indica que se debe cambiar la encriptación de nivel del RDP a High o FIPS Compilant, y el factor de riesgo en Medium.

57690 - Terminal Services Encryption Level is Medium or Low
<p>Synopsis</p> <p>The remote host is using weak cryptography.</p>
<p>Description</p> <p>The remote Terminal Services service is not configured to use strong cryptography.</p> <p>Using weak cryptography with this service may allow an attacker to eavesdrop on the communications more easily and obtain screenshots and/or keystrokes.</p>
<p>Solution</p> <p>Change RDP encryption level to one of :</p> <p>3. High</p> <p>4. FIPS Compliant</p>
<p>Risk Factor</p> <p>Medium</p>
<p>CVSS v2.0 Base Score</p> <p>4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)</p>
<p>Plugin Information</p> <p>Published: 2012/01/25, Modified: 2024/02/22</p>
<p>Plugin Output</p> <p>tcp/3389/msrdp</p> <pre>The terminal services encryption level is set to : 2. Medium</pre>

Figura 3.59: Vulnerabilidades Terminal Services Encryption Level is Medium or Low
Elaborado por: El investigador.

- En la Figura 3.60,** se puede visualizar la vulnerabilidad 85582 – Web Application Potentially Vulnerable to Clickjacking. En el reporte de nessus nos indica que se debe mejorar la configuración de políticas de seguridad para prevenir vulnerabilidades con el uso de frames e iframes en las páginas web, y el factor de riesgo en Medium.

85582 - Web Application Potentially Vulnerable to Clickjacking

Synopsis

The remote web server may fail to mitigate a class of web application vulnerabilities.

Description

The remote web server does not set an X-Frame-Options response header or a Content-Security-Policy 'frame-ancestors' response header in all content responses. This could potentially expose the site to a clickjacking or UI redress attack, in which an attacker can trick a user into clicking an area of the vulnerable page that is different than what the user perceives the page to be. This can result in a user performing fraudulent or malicious transactions.

X-Frame-Options has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors.

Content-Security-Policy (CSP) has been proposed by the W3C Web Application Security Working Group, with increasing support among all major browser vendors, as a way to mitigate clickjacking and other attacks. The 'frame-ancestors' policy directive restricts which sources can embed the protected resource.

Note that while the X-Frame-Options and Content-Security-Policy response headers are not the only mitigations for clickjacking, they are currently the most reliable methods that can be detected through automation. Therefore, this plugin may produce false positives if other mitigation strategies (e.g., frame-busting JavaScript) are deployed or if the page does not perform any security-sensitive transactions.

See Also

<http://www.nessus.org/u?399b1f56>

https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet

<https://en.wikipedia.org/wiki/Clickjacking>

Solution

Return the X-Frame-Options or Content-Security-Policy (with the 'frame-ancestors' directive) HTTP header with the page's response.

This prevents the page's content from being rendered by another site when using the frame or iframe HTML tags.

Risk Factor

Medium

CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N)

References

XREF

CWE:693

Figura 3.60: Vulnerabilidades Web Application Potentially Vulnerable to Clickjacking
Elaborado por: El investigador.

- **En la Figura 3.61**, se puede visualizar la vulnerabilidad 42057 – Web Server Allows Password Auto-Completion. En el reporte de nessus nos indica que se debe aumentar en los campos de formulario web con el atributo autocomplete=”off” ya que esto ayuda a que los datos sensibles como contraseñas sean almacenados por el navegador, y el factor de riesgo en Low.

42057 - Web Server Allows Password Auto-Completion

Synopsis

The 'autocomplete' attribute is not disabled on password fields.

Description

The remote web server contains at least one HTML form field that has an input of type 'password' where 'autocomplete' is not set to 'off'.

While this does not represent a risk to this web server per se, it does mean that users who use the affected forms may have their credentials saved in their browsers, which could in turn lead to a loss of confidentiality if any of them use a shared host or if their machine is compromised at some point.

Solution

Add the attribute 'autocomplete=off' to these fields to prevent browsers from caching credentials.

Risk Factor

Low

Plugin Information

Published: 2009/10/07, Modified: 2023/07/17

Plugin Output

tcp/4848/www

```
Page : /  
Destination Page: /j_security_check  
  
Page : /j_security_check  
Destination Page: /j_security_check
```

Figura 3.61: Vulnerabilidades Web Server Allows Password Auto-Completion
Elaborado por: El investigador.

- **En la Figura 3.62**, se puede visualizar la vulnerabilidad 26194 – Web Server Transmits Cleartext Credentials. En el reporte de nessus nos indica que es importante verificar que los formularios utilicen HTTPS para proteger los datos de los usuarios, y el factor de riesgo en Low.

26194 - Web Server Transmits Cleartext Credentials

Synopsis

The remote web server might transmit credentials in cleartext.

Description

The remote web server contains several HTML form fields containing an input of type 'password' which transmit their information to a remote web server in cleartext.

An attacker eavesdropping the traffic between web browser and server may obtain logins and passwords of valid users.

Solution

Make sure that every sensitive form transmits content over HTTPS.

Risk Factor

Low

CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

References

XREF	CWE:522
XREF	CWE:523
XREF	CWE:718
XREF	CWE:724
XREF	CWE:928
XREF	CWE:930

Plugin Information

Published: 2007/09/28, Modified: 2016/11/29

Plugin Output

tcp/4848/www

```
Page : /  
Destination Page: /j_security_check  
  
Page : /j_security_check  
Destination Page: /j_security_check
```

Figura 3.62: Vulnerabilidades Web Server Transmits Cleartext Credentials

Elaborado por: El investigador.

- **En la Figura 3.63,** se puede visualizar la vulnerabilidad 26194 – Teminal Services Encryption Level is not FIPS-140 Compliant. En el reporte de nessus nos indica que se debe cambiar el nivel de encriptación de RDP a FIPS Compliant, y el factor de riesgo en Low.

30218 - Terminal Services Encryption Level is not FIPS-140 Compliant	
Synopsis	The remote host is not FIPS-140 compliant.
Description	The encryption setting used by the remote Terminal Services service is not FIPS-140 compliant.
Solution	Change RDP encryption level to : 4. FIPS Compliant
Risk Factor	Low
CVSS v2.0 Base Score	2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)
Plugin Information	Published: 2008/02/11, Modified: 2024/02/22
Plugin Output	tcp/3389/msrdp The terminal services encryption level is set to : 2. Medium (Client Compatible)

Figura 3.63: Vulnerabilidades Web Server Transmits Cleartext Credentials
Elaborado por: El investigador.

Esas son las únicas vulnerabilidades detectadas en el Servidor de Procesos Automáticos .

- **Servidor Físico Global VMWARE ESXi 7.0**

Se procede a realizar el analisis de vulnerabilidades en el Servidor y se encontró las siguientes vulnerabilidades.

En la **Figura 3.64**, se visualiza la cantidad de vulnerabilidades encontradas en el servidor de Procesos Automáticos, son 2 crtical, 4 high y 6 medium. Detalle de las vulnerabilidades encontradas a breves rasgos:

- Vulnerabilidad 151665 – ESXi 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2021-0014), este servidor es de sistema operativo VMware ESXi 7.0.0 build-16324942. En el reporte de Nessus nos indica que existe dos vulnerabilidades a las cuales hace referencia SFCB y OpenSLP que es importante mitigar con parches o actualizaciones que previenen de comprometer información, y el factor de riesgo se encuentra en critical.

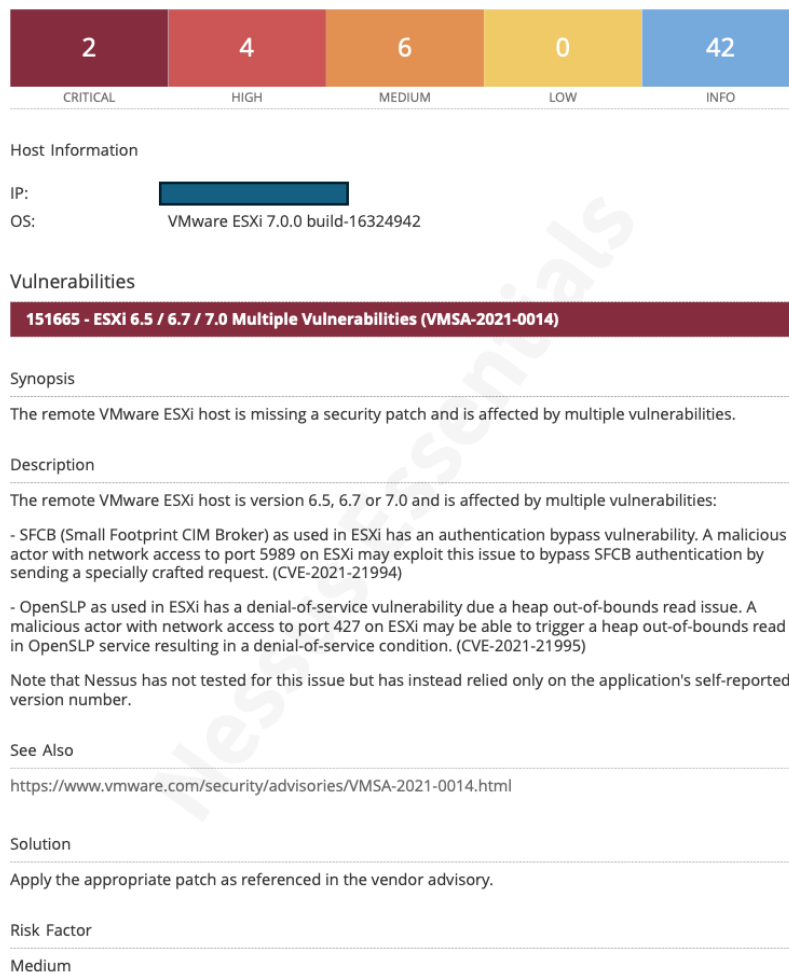


Figura 3.64: Vulnerabilidades ESXi 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2021-0014)

Elaborado por: El investigador.

- En la **Figura 3.65**, se puede visualizar la vulnerabilidad 191711 – ESXi 7.0 / 8.0 Multiple Vulnerabilities (VMSA-2024-0006). En el reporte de Nessus nos

indica que se debe actualizar a una versión actual ya que existe algunas vulnerabilidades del SO, y el factor de riesgo en Critical.

191711 - VMware ESXi 7.0 / 8.0 Multiple Vulnerabilities (VMSA-2024-0006)
Synopsis
The remote VMware ESXi host is affected by multiple vulnerabilities.
Description
The version of VMware ESXi installed on the remote host is prior to 7.0 Update 3p, 8.0 prior to 8.0 Update 1d, or 8.0 prior to 8.0 Update 2b. It is, therefore, affected by multiple vulnerabilities as referenced in the VMSA-2024-0006 advisory: - VMware ESXi, Workstation, and Fusion contain a use-after-free vulnerability in the XHCI USB controller. (CVE-2024-22252) - VMware ESXi, Workstation, and Fusion contain a use-after-free vulnerability in the UHCI USB controller. (CVE-2024-22253) - VMware ESXi contains an out-of-bounds write vulnerability. (CVE-2024-22254) - VMware ESXi, Workstation, and Fusion contain an information disclosure vulnerability in the UHCI USB controller. (CVE-2024-22255) Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.
See Also
https://www.vmware.com/security/advisories/VMSA-2024-0006.html
Solution
Upgrade to VMware ESXi 7.0 Update 3p, 8.0 Update 1d, or 8.0 Update 2b or later.
Risk Factor
High
CVSS v3.0 Base Score
9.3 (CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)
CVSS v3.0 Temporal Score
8.1 (CVSS:3.0/E:U/RL:O/RC:C)
VPR Score
9.2

Figura 3.65: Vulnerabilidades ESXi 7.0 / 8.0 Multiple Vulnerabilities (VMSA-2024-0006)

Elaborado por: El investigador.

- En la **Figura 3.66**, se puede visualizar la vulnerabilidad 143221 – ESXi 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2020-0026). En el reporte de nessus nos indica que se debe actualizar a una versión actual ya que existe algunas vulnerabilidades del SO debido a que se ha detectado escalamiento de privilegios y al uso después de liberar el controlador XHCI USB, y el factor de riesgo en High.

143221 - ESXi 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2020-0026)

Synopsis

The remote VMware ESXi host is missing a security patch and is affected by multiple vulnerabilities.

Description

According to its self-reported version number, the remote VMware ESXi host is version 6.5, 6.7 or 7.0 and is affected by multiple vulnerabilities.

- A use-after-free error exists in the XHCI USB controller. An unauthenticated, local attacker with local administrative privileges on a virtual machine can exploit this, to execute code as the virtual machine's VMX process running on the host. (CVE-2020-4004)

- A privilege escalation vulnerability exists in ESXi due to how certain system calls are managed. An authenticated, local attacker with privileges within the VPM process can exploit this, when chained with CVE-2020-4004, to obtain escalated privileges. (CVE-2020-4005)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<https://www.vmware.com/security/advisories/VMSA-2020-0026.html>

Solution

Apply the appropriate patch as referenced in the vendor advisory.

Risk Factor

High

CVSS v3.0 Base Score

8.2 (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.1 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

6.5

CVSS v2.0 Base Score

7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

Figura 3.66: Vulnerabilidades ESXi 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2020-0026)

Elaborado por: El investigador.

- En la **Figura 3.67** a la **Figura 3.71**, se puede visualizar la vulnerabilidad 158494 – ESXi 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2022-0004). En el reporte de nessus nos indica que se debe actualizar a una versión actual ya que existe algunas vulnerabilidades del SO debido a que se ha detectado

escalamiento de privilegios y al uso después de liberar el controlador XHCI USB, y el factor de riesgo en High y Medium.

158494 - ESXi 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2022-0004)
Synopsis
The remote VMware ESXi host is missing a security patch and is affected by multiple vulnerabilities.
Description
<p>The remote VMware ESXi host is version 6.5, 6.7 or 7.0 and is affected by multiple vulnerabilities, including the following:</p> <ul style="list-style-type: none">- VMware ESXi, Workstation, and Fusion contain a use-after-free vulnerability in the XHCI USB controller. A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual machine's VMX process running on the host. (CVE-2021-22040)- VMware ESXi, Workstation, and Fusion contain a double-fetch vulnerability in the UHCI USB controller. A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual machine's VMX process running on the host. (CVE-2021-22041)- VMware ESXi contains an unauthorized access vulnerability due to VMX having access to settingsd authorization tickets. A malicious actor with privileges within the VMX process only, may be able to access settingsd service running as a high privileged user. (CVE-2021-22042) <p>Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.</p>
See Also
https://www.vmware.com/security/advisories/VMSA-2022-0004.html
Solution
Apply the appropriate patch as referenced in the vendor advisory.
Risk Factor
Medium
CVSS v3.0 Base Score
7.8 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)
CVSS v3.0 Temporal Score
6.8 (CVSS:3.0/E:U/RL:O/RC:C)
VPR Score
5.9

Figura 3.67: Vulnerabilidades ESXi 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2022-0004)

Elaborado por: El investigador.

146827 - ESXi 6.5 / 6.7 / 7.0 RCE (VMSA-2021-0002)

Synopsis

The remote VMware ESXi host is missing a security patch and is affected by a remote code execution vulnerability.

Description

The remote VMware ESXi host is version 6.5, 6.7 or 7.0 and is affected by a remote code execution vulnerability. OpenSLP as used in ESXi (7.0 before ESXi70U1c-17325551, 6.7 before ESXi670-202102401-SG, 6.5 before ESXi650-202102101-SG) has a heap-overflow vulnerability. A malicious actor residing within the same network segment as ESXi who has access to port 427 may be able to trigger the heap-overflow issue in OpenSLP service resulting in remote code execution.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<https://www.vmware.com/security/advisories/VMSA-2021-0002.html>

<http://www.nessus.org/u?090c6180>

Solution

Apply the appropriate patch as referenced in the vendor advisory.

Risk Factor

Medium

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

8.4 (CVSS:3.0/E:H/RL:O/RC:C)

VPR Score

8.9

CVSS v2.0 Base Score

5.8 (CVSS2#AV:A/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

Figura 3.68: Vulnerabilidades ESXi 6.5 / 6.7 / 7.0 RCE (VMSA-2021-0002)

Elaborado por: El investigador.

145090 - ESXi 7.0 DoS (VMSA-2020-0029)

Synopsis

The remote VMware ESXi host is missing a security patch and is affected by a DoS vulnerability

Description

According to its self-reported version number, the remote VMware ESXi host is version 7.0. It is, therefore, affected by a DoS vulnerability due to improper input validation in GuestInfo. A malicious actor with normal user privilege access to a virtual machine can crash the virtual machine's vmx process leading to a denial of service condition.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<https://www.vmware.com/security/advisories/VMSA-2020-0029.html>

Solution

Apply the appropriate patch as referenced in the vendor advisory.

Risk Factor

Low

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

5.7 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

4.4

CVSS v2.0 Base Score

2.1 (CVSS2#AV:L/AC:L/Au:N/C:N/I:N/A:P)

CVSS v2.0 Temporal Score

1.6 (CVSS2#E:U/RL:OF/RC:C)

Figura 3.69: Vulnerabilidades ESXi 7.0 DoS (VMSA-2020-0029)

Elaborado por: El investigador.

192466 - VMware ESXi 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2022-0020)

Synopsis

The remote VMware ESXi host is affected by multiple vulnerabilities.

Description

The remote VMware ESXi host is version 6.5, 6.7 or 7.0 and is affected by multiple vulnerabilities, as follows:

- Intel microprocessor generations 6 to 8 are affected by a new Spectre variant that is able to bypass their retpoline mitigation in the kernel to leak arbitrary data. An attacker with unprivileged user access can hijack return instructions to achieve arbitrary speculative code execution under certain microarchitecture-dependent conditions. (CVE-2022-29901)

- Non-transparent sharing of return predictor targets between contexts in some Intel(R) Processors may allow an authorized user to potentially enable information disclosure via local access. (CVE-2022-26373)

- Aliases in the branch predictor may cause some AMD processors to predict the wrong branch type potentially leading to information disclosure. (CVE-2022-23825)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<https://www.vmware.com/security/advisories/VMSA-2022-0020.html>

Solution

Apply the appropriate patch or workaround as referenced in the vendor advisory.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

5.7 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

6.0

CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:L/Au:S/C:C/I:N/A:N)

Figura 3.70: Vulnerabilidades VMware ESXi 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2022-0020)

Elaborado por: El investigador.

192568 - VMware ESXi 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2022-0016)

Synopsis

The remote VMware ESXi host is affected by multiple vulnerabilities.

Description

The version of VMware ESXi installed on the remote host is prior to 6.7 P07, or 7.x prior to 7.0 Update 3e. It is, therefore, affected by multiple vulnerabilities as referenced in the VMSA-2022-0016 advisory:

- Incomplete cleanup of multi-core shared buffers for some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. (CVE-2022-21123)

- Incomplete cleanup of microarchitectural fill buffers on some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. (CVE-2022-21125)

- Incomplete cleanup in specific special register write operations for some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. (CVE-2022-21166)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://www.vmware.com/security/advisories/VMSA-2022-0016.html>

Solution

Upgrade to VMware ESXi 6.7 P07, or 7.0 U3e or later.

Risk Factor

Low

CVSS v3.0 Base Score

5.5 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

4.8 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

4.4

CVSS v2.0 Base Score

2.1 (CVSS2#AV:L/AC:L/Au:N/C:P/I:N/A:N)

Figura 3.71: Vulnerabilidades VMware ESXi 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2022-0016)

Elaborado por: El investigador.

- En la **Figura 3.72**, se puede visualizar la vulnerabilidad 51192 – SSL Certificate Cannot Be Trusted. En el reporte de Nessus nos indica la solución y el riesgo en Medium.

51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

See Also

<https://www.itu.int/rec/T-REC-X.509/en>

<https://en.wikipedia.org/wiki/X.509>

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Figura 3.72: Vulnerabilidades SSL Certificate Cannot Be Trusted
Elaborado por: El investigador.

- En la **Figura 3.73**, se puede visualizar la vulnerabilidad 57582 – SSL Self-Signed Certificate. En el reporte de nessus nos indica que debemos adquirir un certificado SSL y validarlo en CA, y el factor de riesgo en Medium.

57582 - SSL Self-Signed Certificate

Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

5.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS v2.0 Base Score

5.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin Information

Published: 2012/01/17, Modified: 2022/06/14

Plugin Output

tcp/9080/www

The following certificate was found at the top of the certificate chain sent by the remote host, but is self-signed and was not found in the list of known certificate authorities :

| -Subject : O=VMware Installer

Figura 3.73: Vulnerabilidades SSL Self-Signed Certificate
Elaborado por: El investigador.

Esas son las únicas vulnerabilidades detectadas en el Servidor VMware ESXi 7.0.

- **Servidor AIX 5.3**

Se procede a realizar el análisis de vulnerabilidades en el Servidor y se encontró las siguientes vulnerabilidades.

En la **Figura 3.74** a la **Figura 3.80**, se visualiza la cantidad de vulnerabilidades encontradas en el servidor AIX, son 5 critical, 1 high. En el reporte de nessus nos indica que es importante la actualización de Apache debido a múltiples vulnerabilidades encontradas como HTTP Request Smuggling Mod-Lua que cualquier atacante podría manipular las solicitudes del HTTP permitiendo el acceso no autorizado, desbordamiento de buffer provocando que se pueda ejecutar código malicioso, se podría llevar a cabo una denegación de servicios o DoS, entre otras. A continuación se detalla las vulnerabilidades encontradas a breves rasgos:

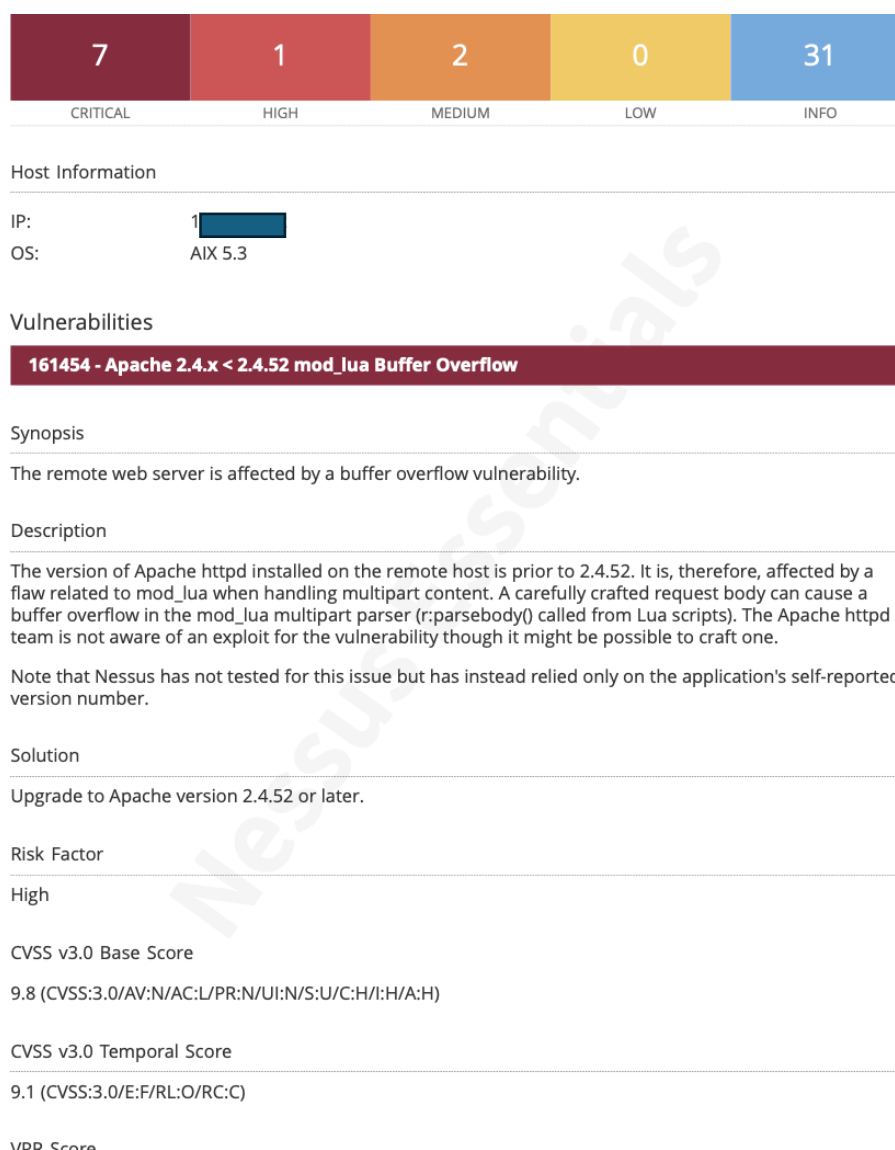


Figura 3.74: Vulnerabilidades Apache 2.4.x < 2.4.52 mod_lua Buffer Overflow
Elaborado por: El investigador.

158900 - Apache 2.4.x < 2.4.53 Multiple Vulnerabilities

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.53. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.53 advisory.

- mod_lua Use of uninitialized value of in r:parsebody: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier. Acknowledgements: Chamal De Silva (CVE-2022-22719)

- HTTP request smuggling: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling Acknowledgements: James Kettle <james.kettle@portswigger.net> (CVE-2022-22720)

- Possible buffer overflow with very large or unlimited LimitXMLRequestBody in core: If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier. Acknowledgements: Anonymous working with Trend Micro Zero Day Initiative (CVE-2022-22721)

- Read/write beyond bounds in mod_sed: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions. Acknowledgements: Ronald Crane (Zippenhop LLC) (CVE-2022-23943)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<http://www.apache.org/dist/httpd/Announcement2.4.html>

https://httpd.apache.org/security/vulnerabilities_24.html

Solution

Upgrade to Apache version 2.4.53 or later.

Risk Factor

High

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

Figura 3.75: Vulnerabilidades Apache 2.4.x < 2.4.53 Multiple Vulnerabilities
Elaborado por: El investigador.

161948 - Apache 2.4.x < 2.4.54 Multiple Vulnerabilities

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.54. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.54 advisory.

- Possible request smuggling in mod_proxy_ajp: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions. Acknowledgements: Richter Z @ 360 Noah Lab (CVE-2022-26377)
- Read beyond bounds in mod_isapi: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module. Acknowledgements: The Apache HTTP Server project would like to thank Ronald Crane (Zippenhop LLC) for reporting this issue (CVE-2022-28330)
- Read beyond bounds via ap_rwrite(): The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_lua's r:puts() function. Acknowledgements: The Apache HTTP Server project would like to thank Ronald Crane (Zippenhop LLC) for reporting this issue (CVE-2022-28614)
- Read beyond bounds in ap_strcmp_match(): Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected. Acknowledgements: The Apache HTTP Server project would like to thank Ronald Crane (Zippenhop LLC) for reporting this issue (CVE-2022-28615)
- Denial of service in mod_lua r:parsebody: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size. Acknowledgements: The Apache HTTP Server project would like to thank Ronald Crane (Zippenhop LLC) for reporting this issue (CVE-2022-29404)
- Denial of Service mod_sed: If Apache HTTP Server 2.4.53 is configured to do transformations with mod_sed in contexts where the input to mod_sed may be very large, mod_sed may make excessively large memory allocations and trigger an abort. Acknowledgements: This issue was found by Brian Moussalli from the JFrog Security Research team (CVE-2022-30522)
- Information Disclosure in mod_lua with websockets: Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer. Acknowledgements: The Apache HTTP Server project would like to thank Ronald Crane (Zippenhop LLC) for reporting this issue (CVE-2022-30556)
- X-Forwarded-For dropped by hop-by-hop mechanism in mod_proxy: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application. Acknowledgements: The Apache HTTP Server project would like to thank Gaetan Ferry (Synacktiv) for reporting this issue (CVE-2022-31813)

Figura 3.76: Vulnerabilidades Apache 2.4.x < 2.4.54 Multiple Vulnerabilities

Elaborado por: El investigador.

170113 - Apache 2.4.x < 2.4.55 Multiple Vulnerabilities

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.55. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.55 advisory.

- A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash. This issue affects Apache HTTP Server 2.4.54 and earlier. (CVE-2006-20001)

- Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions. (CVE-2022-36760)

- Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client. (CVE-2022-37436)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Apache version 2.4.55 or later.

Risk Factor

High

CVSS v3.0 Base Score

9.0 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.8 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

6.5

CVSS v2.0 Base Score

7.6 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

Figura 3.77: Vulnerabilidades Apache 2.4.x < 2.4.55 Multiple Vulnerabilities
Elaborado por: El investigador.

172186 - Apache 2.4.x < 2.4.56 Multiple Vulnerabilities

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.56. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.56 advisory.

- HTTP request splitting with mod_rewrite and mod_proxy: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack. Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like: RewriteEngine on RewriteRule ^/here/(.*) http://example.com:8080/elsewhere?\$1 http://example.com:8080/elsewhere ; [P] ProxyPassReverse /here/ http://example.com:8080/ http://example.com:8080/ Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Acknowledgements: finder: Lars Krapf of Adobe (CVE-2023-25690)

- Apache HTTP Server: mod_proxy_uwsgi HTTP response splitting: HTTP Response Smuggling vulnerability in Apache HTTP Server via mod_proxy_uwsgi. This issue affects Apache HTTP Server: from 2.4.30 through 2.4.55.

Special characters in the origin response header can truncate/split the response forwarded to the client.

Acknowledgements: finder: Dimas Fariski Setyawan Putra (nyxsorcerer) (CVE-2023-27522)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Apache version 2.4.56 or later.

Risk Factor

Critical

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

8.8 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

6.7

Figura 3.78: Vulnerabilidades Apache 2.4.x < 2.4.56 Multiple Vulnerabilities
Elaborado por: El investigador.

156255 - Apache 2.4.x >= 2.4.7 / < 2.4.52 Forward Proxy DoS / SSRF

Synopsis

The remote web server is affected by a denial of service or server-side request forgery vulnerability.

Description

The version of Apache httpd installed on the remote host is equal to or greater than 2.4.7 and prior to 2.4.52.

It is, therefore, affected by a flaw related to acting as a forward proxy.

A crafted URI sent to httpd configured as a forward proxy (ProxyRequests on) can cause a crash (NULL pointer dereference) or, for configurations mixing forward and reverse proxy declarations, can allow for requests to be directed to a declared Unix Domain Socket endpoint (Server Side Request Forgery).

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Apache version 2.4.52 or later.

Risk Factor

High

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

9.1 (CVSS:3.0/E:F/RL:O/RC:C)

VPR Score

7.4

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

6.2 (CVSS2#E:F/RL:OF/RC:C)

STIG Severity

Figura 3.79: Vulnerabilidades Apache 2.4.x >= 2.4.7 / < 2.4.52 Forward Proxy DoS / SSRF

Elaborado por: El investigador.

183391 - Apache 2.4.x < 2.4.58 Multiple Vulnerabilities

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.58. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.58 advisory.

- mod_macro buffer over-read: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server. This issue affects Apache HTTP Server: through 2.4.57. Acknowledgements: finder: David Shoon (github/davidshoon) (CVE-2023-31122)

- Apache HTTP Server: DoS in HTTP/2 with initial windows size 0: An attacker, opening a HTTP/2 connection with an initial window size of 0, was able to block handling of that connection indefinitely in Apache HTTP Server. This could be used to exhaust worker resources in the server, similar to the well known slow loris attack pattern. This has been fixed in version 2.4.58, so that such connection are terminated properly after the configured connection timeout. This issue affects Apache HTTP Server: from 2.4.55 through 2.4.57. Users are recommended to upgrade to version 2.4.58, which fixes the issue.

Acknowledgements: (CVE-2023-43622)

- Apache HTTP Server: HTTP/2 stream memory not reclaimed right away on RST: When a HTTP/2 stream was reset (RST frame) by a client, there was a time window where the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that. This was found by the reporter during testing of CVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test client. During normal HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out. Users are recommended to upgrade to version 2.4.58, which fixes the issue. Acknowledgements: (CVE-2023-45802)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Apache version 2.4.58 or later.

Risk Factor

High

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

6.5 (CVSS:3.0/E:U/RL:O/RC:C)

Figura 3.80: Vulnerabilidades Apache 2.4.x < 2.4.58 Multiple Vulnerabilities

Elaborado por: El investigador.

- En la **Figura 3.81** a la **Figura 3.89**, se visualiza la cantidad de vulnerabilidades encontradas en el servidor AIX, son 1 critical, 3 medium. En el reporte de nessus nos indica que es importante revisar la Vulnerabilidad de Oracle WebLogic RCE y como solución sugiere aplicar el parche, la vulnerabilidad de HTTP Trace / Track solicita deshabilitar estos métodos en el servidor web ya que se pueden

dar ataques de cross-site XST, Browsable web directories indica que los directores web son navegables y se pueden atacar con facilidad, entre otras. A continuación se detalla las vulnerabilidades encontradas a breves rasgos:

142594 - Oracle WebLogic Server RCE (CVE-2020-14882)

Synopsis

An application server installed on the remote host is affected by a remote code execution vulnerability.

Description

The version of Oracle WebLogic Server installed on the remote host is affected by a remote code execution vulnerability in the Oracle Fusion Middleware Console subcomponent. An unauthenticated, remote attacker can exploit this, via a specially crafted HTTP request, to execute arbitrary commands.

No reliable remote exploit has been published for Oracle WebLogic Server 10.3.6.X or 12.1.3.X, so Nessus will not be able to determine if the remote server is affected or not for these versions.

See Also

<https://www.oracle.com/a/tech/docs/cpuoct2020cvrf.xml>

<https://www.oracle.com/security-alerts/cpuoct2020.html>

<https://www.oracle.com/security-alerts/alert-cve-2020-14750.html>

Solution

Apply the appropriate patch according to the October 2020 Oracle Critical Patch Update advisory and the Oracle Security Alert advisory for CVE-2020-14750.

Risk Factor

Critical

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

9.4 (CVSS:3.0/E:H/RL:O/RC:C)

VPR Score

9.4

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:I/C/A:C)

CVSS v2.0 Temporal Score

8.7 (CVSS2#E:H/RL:OF/RC:C)

Figura 3.81: Vulnerabilidades Oracle WebLogic Server RCE (CVE-200-14882)

Elaborado por: El investigador.

11213 - HTTP TRACE / TRACK Methods Allowed

Synopsis

Debugging functions are enabled on the remote web server.

Description

The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.

See Also

<http://www.nessus.org/u?e979b5cb>

<http://www.apacheweek.com/issues/03-01-24>

<https://download.oracle.com/sunalerts/1000718.1.html>

Solution

Disable these HTTP methods. Refer to the plugin output for more information.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

CVSS v3.0 Temporal Score

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

4.0

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

References

BID 9506

Figura 3.82: Vulnerabilidades HTTP TRACE / TRACK Methods Allowed
Elaborado por: El investigador.

187315 - SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795)

Synopsis

The remote SSH server is vulnerable to a mitm prefix truncation attack.

Description

The remote SSH server is vulnerable to a man-in-the-middle prefix truncation weakness known as Terrapin. This can allow a remote, man-in-the-middle attacker to bypass integrity checks and downgrade the connection's security.

Note that this plugin only checks for remote SSH servers that support either ChaCha20-Poly1305 or CBC with Encrypt-then-MAC and do not support the strict key exchange countermeasures. It does not check for vulnerable software versions.

See Also

<https://terrapin-attack.com/>

Solution

Contact the vendor for an update with the strict key exchange countermeasures or disable the affected algorithms.

Risk Factor

Medium

CVSS v3.0 Base Score

5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N)

CVSS v3.0 Temporal Score

5.3 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

6.7

CVSS v2.0 Base Score

5.4 (CVSS2#AV:N/AC:H/Au:N/C:N/I:C/A:N)

CVSS v2.0 Temporal Score

4.2 (CVSS2#E:POC/RL:OF/RC:C)

Figura 3.83: Vulnerabilidades SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795)

Elaborado por: El investigador.

40984 - Browsable Web Directories

Synopsis

Some directories on the remote web server are browsable.

Description

Multiple Nessus plugins identified directories on the web server that are browsable.

See Also

<http://www.nessus.org/u?0a35179e>

Solution

Make sure that browsable directories do not leak confidential information or give access to sensitive resources. Additionally, use access restrictions or disable directory indexing for any that do.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

Plugin Information

Published: 2009/09/15, Modified: 2021/01/19

Plugin Output

tcp/80/www

```
The following directories are browsable :  
http://172.20.1.9/  
http://172.20.1.9/  
http://172.20.1.9/  
http://172.20.1.9/  
http://172.20.1.9/  
http://172.20.1.9/contents/  
http://172.20.1.9/  
http://172.20.1.9/...star/  
http://172.20.1.9/...ocks/  
http://172.20.1.9/assets/demo/images/blocks/logos/
```

Figura 3.84: Vulnerabilidades Browsable Web Directories

Elaborado por: El investigador.

A estas vulnerabilidades obtenidas en la herramienta de Nessus se les aplicaron pruebas de penetración con el framework metasploit en el **ANEXO** se detalla de los casos exitosos que se tuvo.

3.2.3.2 Análisis de Vulnerabilidades con 11

Se procede a realizar el analisis respectivo desde la herramienta Dmitry que es incluida en Kali linux. Desde la **Figura 3.85 a la Figura 3.92**, se logra evidenciar el analisis desarrollado en los servidores:

```
HostIP:172.20.1.51
HostName:svdf01.df.eeasa.com

Gathered Inet-whois information for 172.20.1.51
-----
inetnum: 171.76.0.0 - 172.80.127.255
netname: NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr: IPv4 address block not managed by the RIPE NCC
remarks:
remarks:
remarks: For registration information,
remarks: you can consult the following sources:
remarks:
remarks: IANA
remarks: http://www.iana.org/assignments/ipv4-address-space
remarks: http://www.iana.org/assignments/iana-ipv4-special-registry
remarks: http://www.iana.org/assignments/ipv4-recovered-address-space
remarks:
remarks: AFRINIC (Africa)
remarks: http://www.afrinic.net/ whois.afrinic.net
remarks:
remarks: APNIC (Asia Pacific)
remarks: http://www.apnic.net/ whois.apnic.net
remarks:
remarks: ARIN (Northern America)
remarks: http://www.arin.net/ whois.arin.net
remarks:
remarks: LACNIC (Latin America and the Caribbean)
remarks: http://www.lacnic.net/ whois.lacnic.net
remarks:
country: EU # Country is really world wide
admin-c: IANA1-RIPE
tech-c: IANA1-RIPE
status: ALLOCATED UNSPECIFIED
mnt-by: RIPE-NCC-HM-MNT
created: 2024-01-29T14:42:11Z
last-modified: 2024-01-29T14:42:11Z
source: RIPE

role: Internet Assigned Numbers Authority
address: see http://www.iana.org.
admin-c: IANA1-RIPE
tech-c: IANA1-RIPE
nic-hdl: IANA1-RIPE
remarks: For more information on IANA services
remarks: go to IANA web site at http://www.iana.org.
mnt-by: RIPE-NCC-MNT
created: 1970-01-01T00:00:00Z
last-modified: 2001-09-22T09:31:27Z
source: RIPE # Filtered

% This query was served by the RIPE Database Query Service version 1.112 (ABERDEEN)

Gathered Inic-whois information for svdf01.df.eeasa.com
-----
ERROR: Unable to locate Name Whois data on svdf01.df.eeasa.com

Gathered Netcraft information for svdf01.df.eeasa.com
-----
Retrieving Netcraft.com information for svdf01.df.eeasa.com
Netcraft.com Information gathered

Gathered Subdomain information for svdf01.df.eeasa.com
-----
Searching Google.com:80...
Searching Altavista.com:80...
Found 0 possible subdomain(s) for host svdf01.df.eeasa.com, Searched 0 pages containing 0 results

Gathered E-Mail information for svdf01.df.eeasa.com
-----
Searching Google.com:80...
Searching Altavista.com:80...
Found 0 E-Mail(s) for host svdf01.df.eeasa.com, Searched 0 pages containing 0 results
```

Figura 3.85: Herramienta Dmitry SRV AD
Elaborado por: El investigador.

```

ERROR: Unable to locate Host Name for 172.20.1.52
Continuing with limited modules
HostIP:172.20.1.52
HostName:

Gathered Inet-whois information for 172.20.1.52
-----

inetnum:      171.76.0.0 - 172.80.127.255
netname:      NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr:        IPv4 address block not managed by the RIPE NCC
remarks:      -----
remarks:
remarks:      For registration information,
remarks:      you can consult the following sources:
remarks:
remarks:      IANA
remarks:      http://www.iana.org/assignments/ipv4-address-space
remarks:      http://www.iana.org/assignments/iana-ipv4-special-registry
remarks:      http://www.iana.org/assignments/ipv4-recovered-address-space
remarks:
remarks:      AFRINIC (Africa)
remarks:      http://www.afrinic.net/ whois.afrinic.net
remarks:
remarks:      APNIC (Asia Pacific)
remarks:      http://www.apnic.net/ whois.apnic.net
remarks:
remarks:      ARIN (Northern America)
remarks:      http://www.arin.net/ whois.arin.net
remarks:
remarks:      LACNIC (Latin America and the Carribean)
remarks:      http://www.lacnic.net/ whois.lacnic.net
remarks:
remarks:      -----
country:      EU # Country is really world wide
admin-c:      IANA1-RIPE
tech-c:       IANA1-RIPE
status:       ALLOCATED UNSPECIFIED
mnt-by:       RIPE-NCC-HM-MNT
created:      2024-01-29T14:42:11Z
last-modified: 2024-01-29T14:42:11Z
source:       RIPE

role:         Internet Assigned Numbers Authority
address:      see http://www.iana.org.
admin-c:      IANA1-RIPE
tech-c:       IANA1-RIPE
nic-hdl:      IANA1-RIPE
remarks:      For more information on IANA services
remarks:      go to IANA web site at http://www.iana.org.
mnt-by:       RIPE-NCC-MNT
created:      1970-01-01T00:00:00Z
last-modified: 2001-09-22T09:31:27Z
source:       RIPE # Filtered

% This query was served by the RIPE Database Query Service version 1.112 (SHETLAND)

```

Figura 3.86: Herramienta Dmitry SRV ILO
Elaborado por: El investigador.

```

HostIP:172.20.1.54
HostName:nas_financiero.df.eeasa.com

Gathered Inet-whois information for 172.20.1.54
-----

inetnum:        171.76.0.0 - 172.80.127.255
netname:        NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr:          IPv4 address block not managed by the RIPE NCC
remarks:        -----
remarks:        For registration information,
remarks:        you can consult the following sources:
remarks:
remarks:        IANA
remarks:        http://www.iana.org/assignments/ipv4-address-space
remarks:        http://www.iana.org/assignments/iana-ipv4-special-registry
remarks:        http://www.iana.org/assignments/ipv4-recovered-address-space
remarks:
remarks:        AFRINIC (Africa)
remarks:        http://www.afrinic.net/ whois.afrinic.net
remarks:
remarks:        APNIC (Asia Pacific)
remarks:        http://www.apnic.net/ whois.apnic.net
remarks:
remarks:        ARIN (Northern America)
remarks:        http://www.arin.net/ whois.arin.net
remarks:
remarks:        LACNIC (Latin America and the Caribbean)
remarks:        http://www.lacnic.net/ whois.lacnic.net
remarks:        -----
country:        EU # Country is really world wide
admin-c:        IANA1-RIPE
tech-c:         IANA1-RIPE
status:         ALLOCATED UNSPECIFIED
mnt-by:         RIPE-NCC-HM-MNT
created:        2024-01-29T14:42:11Z
last-modified:  2024-01-29T14:42:11Z
source:         RIPE

role:           Internet Assigned Numbers Authority
address:        see http://www.iana.org.
admin-c:        IANA1-RIPE
tech-c:         IANA1-RIPE
nic-hdl:        IANA1-RIPE
remarks:        For more information on IANA services
remarks:        go to IANA web site at http://www.iana.org.
mnt-by:         RIPE-NCC-MNT
created:        1970-01-01T00:00:00Z
last-modified:  2001-09-22T09:31:27Z
source:         RIPE # Filtered

% This query was served by the RIPE Database Query Service version 1.112 (SHETLAND)

Gathered Inic-whois information for nas_financiero.df.eeasa.com
-----
ERROR: Unable to locate Name Whois data on nas_financiero.df.eeasa.com

Gathered Netcraft information for nas_financiero.df.eeasa.com
-----

Retrieving Netcraft.com information for nas_financiero.df.eeasa.com
Netcraft.com Information gathered

Gathered Subdomain information for nas_financiero.df.eeasa.com
-----
Searching Google.com:80...
Searching Altavista.com:80...
Found 0 possible subdomain(s) for host nas_financiero.df.eeasa.com, Searched 0 pages containing 0
results

Gathered E-Mail information for nas_financiero.df.eeasa.com
-----
Searching Google.com:80...
Searching Altavista.com:80...
Found 0 E-Mail(s) for host nas_financiero.df.eeasa.com, Searched 0 pages containing 0 results

```

Figura 3.87: Herramienta Dmitry SRV NAS
Elaborado por: El investigador.

```

ERROR: Unable to locate Host Name for 172.20.1.55
Continuing with limited modules
HostIP:172.20.1.55
HostName:

Gathered Inet-whois information for 172.20.1.55
-----
inetnum:      171.76.0.0 - 172.80.127.255
netname:      NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr:        IPv4 address block not managed by the RIPE NCC
remarks:      -----
remarks:
remarks:      For registration information,
remarks:      you can consult the following sources:
remarks:
remarks:      IANA
remarks:      http://www.iana.org/assignments/ipv4-address-space
remarks:      http://www.iana.org/assignments/iana-ipv4-special-registry
remarks:      http://www.iana.org/assignments/ipv4-recovered-address-space
remarks:
remarks:      AFRINIC (Africa)
remarks:      http://www.afrinic.net/ whois.afrinic.net
remarks:
remarks:      APNIC (Asia Pacific)
remarks:      http://www.apnic.net/ whois.apnic.net
remarks:
remarks:      ARIN (Northern America)
remarks:      http://www.arin.net/ whois.arin.net
remarks:
remarks:      LACNIC (Latin America and the Caribbean)
remarks:      http://www.lacnic.net/ whois.lacnic.net
remarks:
remarks:      -----
country:      EU # Country is really world wide
admin-c:      IANA1-RIPE
tech-c:       IANA1-RIPE
status:       ALLOCATED UNSPECIFIED
mnt-by:       RIPE-NCC-HM-MNT
created:      2024-01-29T14:42:11Z
last-modified: 2024-01-29T14:42:11Z
source:       RIPE

role:         Internet Assigned Numbers Authority
address:      see http://www.iana.org.
admin-c:      IANA1-RIPE
tech-c:       IANA1-RIPE
nic-hdl:      IANA1-RIPE
remarks:      For more information on IANA services
remarks:      go to IANA web site at http://www.iana.org.
mnt-by:       RIPE-NCC-MNT
created:      1970-01-01T00:00:00Z
last-modified: 2001-09-22T09:31:27Z
source:       RIPE # Filtered

% This query was served by the RIPE Database Query Service version 1.112 (DEXTER)

```

Figura 3.88: Herramienta Dmitry SRV SIF PRINCIPAL
Elaborado por: El investigador.


```

HostIP:172.20.1.57
HostName:serverdf06.df.eeasa.com

Gathered Inet-whois information for 172.20.1.57
-----

inetnum:      171.76.0.0 - 172.80.127.255
netname:      NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr:        IPv4 address block not managed by the RIPE NCC
remarks:      -----
remarks:
remarks:      For registration information,
remarks:      you can consult the following sources:
remarks:
remarks:      IANA
remarks:      http://www.iana.org/assignments/ipv4-address-space
remarks:      http://www.iana.org/assignments/iana-ipv4-special-registry
remarks:      http://www.iana.org/assignments/ipv4-recovered-address-space
remarks:
remarks:      AFRINIC (Africa)
remarks:      http://www.afrinic.net/ whois.afrinic.net
remarks:
remarks:      APNIC (Asia Pacific)
remarks:      http://www.apnic.net/ whois.apnic.net
remarks:
remarks:      ARIN (Northern America)
remarks:      http://www.arin.net/ whois.arin.net
remarks:
remarks:      LACNIC (Latin America and the Caribbean)
remarks:      http://www.lacnic.net/ whois.lacnic.net
remarks:      -----
country:      EU # Country is really world wide
admin-c:      IANA1-RIPE
tech-c:       IANA1-RIPE
status:       ALLOCATED UNSPECIFIED
mnt-by:       RIPE-NCC-HM-MNT
created:      2024-01-29T14:42:11Z
last-modified: 2024-01-29T14:42:11Z
source:       RIPE

role:         Internet Assigned Numbers Authority
address:      see http://www.iana.org.
admin-c:      IANA1-RIPE
tech-c:       IANA1-RIPE
nic-hdl:      IANA1-RIPE
remarks:      For more information on IANA services
remarks:      go to IANA web site at http://www.iana.org.
mnt-by:       RIPE-NCC-MNT
created:      1970-01-01T00:00:00Z
last-modified: 2001-09-22T09:31:27Z
source:       RIPE # Filtered

% This query was served by the RIPE Database Query Service version 1.112 (SHETLAND)

Gathered Inic-whois information for serverdf06.df.eeasa.com
-----
ERROR: Unable to locate Name Whois data on serverdf06.df.eeasa.com

Gathered Netcraft information for serverdf06.df.eeasa.com
-----

Retrieving Netcraft.com information for serverdf06.df.eeasa.com
Netcraft.com Information gathered

Gathered Subdomain information for serverdf06.df.eeasa.com
-----
Searching Google.com:80...
Searching Altavista.com:80...
Found 0 possible subdomain(s) for host serverdf06.df.eeasa.com, Searched 0 pages containing 0
results

Gathered E-Mail information for serverdf06.df.eeasa.com
-----
Searching Google.com:80...
Searching Altavista.com:80...
Found 0 E-Mail(s) for host serverdf06.df.eeasa.com, Searched 0 pages containing 0 results

```

Figura 3.89: Herramienta Dmitry SRV PROCESO AUTOMÁTICO
Elaborado por: El investigador.


```

ERROR: Unable to locate Host Name for 172.20.1.58
Continuing with limited modules
HostIP:172.20.1.58
HostName:

Gathered Inet-whois information for 172.20.1.58
-----

inetnum:        171.76.0.0 - 172.80.127.255
netname:        NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr:          IPv4 address block not managed by the RIPE NCC
remarks:        -----
remarks:        For registration information,
remarks:        you can consult the following sources:
remarks:        IANA
remarks:        http://www.iana.org/assignments/ipv4-address-space
remarks:        http://www.iana.org/assignments/iana-ipv4-special-registry
remarks:        http://www.iana.org/assignments/ipv4-recovered-address-space
remarks:        AFRINIC (Africa)
remarks:        http://www.afrinic.net/ whois.afrinic.net
remarks:        APNIC (Asia Pacific)
remarks:        http://www.apnic.net/ whois.apnic.net
remarks:        ARIN (Northern America)
remarks:        http://www.arin.net/ whois.arin.net
remarks:        LACNIC (Latin America and the Carribean)
remarks:        http://www.lacnic.net/ whois.lacnic.net
remarks:        -----
country:        EU # Country is really world wide
admin-c:        IANA1-RIPE
tech-c:         IANA1-RIPE
status:         ALLOCATED UNSPECIFIED
mnt-by:         RIPE-NCC-HM-MNT
created:        2024-01-29T14:42:11Z
last-modified:  2024-01-29T14:42:11Z
source:         RIPE

role:           Internet Assigned Numbers Authority
address:        see http://www.iana.org.
admin-c:        IANA1-RIPE
tech-c:         IANA1-RIPE
nic-hdl:        IANA1-RIPE
remarks:        For more information on IANA services
remarks:        go to IANA web site at http://www.iana.org.
mnt-by:         RIPE-NCC-MNT
created:        1970-01-01T00:00:00Z
last-modified:  2001-09-22T09:31:27Z
source:         RIPE # Filtered

% This query was served by the RIPE Database Query Service version 1.112 (DEXTER)

```

Figura 3.90: Herramienta Dmitry SRV VMWARE
Elaborado por: El investigador.

```

HostIP:172.20.1.59
HostName:SRVVEAMBACKUP.df.eeasa.com

Gathered Inet-whois information for 172.20.1.59
-----
inetnum:      171.76.0.0 - 172.80.127.255
netname:      NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr:        IPv4 address block not managed by the RIPE NCC
remarks:      -----
remarks:      For registration information,
remarks:      you can consult the following sources:
remarks:      IANA
remarks:      http://www.iana.org/assignments/ipv4-address-space
remarks:      http://www.iana.org/assignments/iana-ipv4-special-registry
remarks:      http://www.iana.org/assignments/ipv4-recovered-address-space
remarks:      AFRINIC (Africa)
remarks:      http://www.afrinic.net/ whois.afrinic.net
remarks:      APNIC (Asia Pacific)
remarks:      http://www.apnic.net/ whois.apnic.net
remarks:      ARIN (Northern America)
remarks:      http://www.arin.net/ whois.arin.net
remarks:      LACNIC (Latin America and the Caribbean)
remarks:      http://www.lacnic.net/ whois.lacnic.net
remarks:      -----
country:      EU # Country is really world wide
admin-c:      IANA1-RIPE
tech-c:       IANA1-RIPE
status:       ALLOCATED UNSPECIFIED
mnt-by:       RIPE-NCC-HM-MNT
created:      2024-01-29T14:42:11Z
last-modified: 2024-01-29T14:42:11Z
source:       RIPE

role:          Internet Assigned Numbers Authority
address:       see http://www.iana.org.
admin-c:      IANA1-RIPE
tech-c:       IANA1-RIPE
nic-hdl:      IANA1-RIPE
remarks:      For more information on IANA services
remarks:      go to IANA web site at http://www.iana.org.
mnt-by:       RIPE-NCC-MNT
created:      1970-01-01T00:00:00Z
last-modified: 2001-09-22T09:31:27Z
source:       RIPE # Filtered

% This query was served by the RIPE Database Query Service version 1.112 (BUSA)

Gathered Inic-whois information for SRVVEAMBACKUP.df.eeasa.com
-----
ERROR: Unable to locate Name Whois data on SRVVEAMBACKUP.df.eeasa.com

Gathered Netcraft information for SRVVEAMBACKUP.df.eeasa.com
-----
Retrieving Netcraft.com information for SRVVEAMBACKUP.df.eeasa.com
Netcraft.com Information gathered

Gathered Subdomain information for SRVVEAMBACKUP.df.eeasa.com
-----
Searching Google.com:80...
Searching Altavista.com:80...
Found 0 possible subdomain(s) for host SRVVEAMBACKUP.df.eeasa.com, Searched 0 pages containing 0
results

Gathered E-Mail information for SRVVEAMBACKUP.df.eeasa.com
-----
Searching Google.com:80...
Searching Altavista.com:80...
Found 0 E-Mail(s) for host SRVVEAMBACKUP.df.eeasa.com, Searched 0 pages containing 0 results

```

Figura 3.91: Herramienta Dmitry SRV VEAMBACKUP
Elaborado por: El investigador.

```

ERROR: Unable to locate Host Name for 172.20.1.92
Continuing with limited modules
HostIP:172.20.1.92
HostName:

Gathered Inet-whois information for 172.20.1.92
-----

inetnum:      171.76.0.0 - 172.80.127.255
netname:      NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr:        IPv4 address block not managed by the RIPE NCC
remarks:      -----
remarks:
remarks:      For registration information,
remarks:      you can consult the following sources:
remarks:
remarks:      IANA
remarks:      http://www.iana.org/assignments/ipv4-address-space
remarks:      http://www.iana.org/assignments/iana-ipv4-special-registry
remarks:      http://www.iana.org/assignments/ipv4-recovered-address-space
remarks:
remarks:      AFRINIC (Africa)
remarks:      http://www.afrinic.net/ whois.afrinic.net
remarks:
remarks:      APNIC (Asia Pacific)
remarks:      http://www.apnic.net/ whois.apnic.net
remarks:
remarks:      ARIN (Northern America)
remarks:      http://www.arin.net/ whois.arin.net
remarks:
remarks:      LACNIC (Latin America and the Carribean)
remarks:      http://www.lacnic.net/ whois.lacnic.net
remarks:      -----
country:      EU # Country is really world wide
admin-c:      IANA1-RIPE
tech-c:       IANA1-RIPE
status:       ALLOCATED UNSPECIFIED
mnt-by:       RIPE-NCC-HM-MNT
created:      2024-01-29T14:42:11Z
last-modified: 2024-01-29T14:42:11Z
source:       RIPE

role:         Internet Assigned Numbers Authority
address:      see http://www.iana.org.
admin-c:      IANA1-RIPE
tech-c:       IANA1-RIPE
nic-hdl:      IANA1-RIPE
remarks:      For more information on IANA services
remarks:      go to IANA web site at http://www.iana.org.
mnt-by:       RIPE-NCC-MNT
created:      1970-01-01T00:00:00Z
last-modified: 2001-09-22T09:31:27Z
source:       RIPE # Filtered

% This query was served by the RIPE Database Query Service version 1.112 (SHETLAND)

```

Figura 3.92: Herramienta Dmitry SRV AIX

Elaborado por: El investigador.

3.2.3.3 Analisis de Vulnerabilidades con Nmap

Se procede a realizar el analisis respectivo desde la herramienta Nmap. Desde la **Figura 3.93 a la Figura 3.100**, se logra evidenciar el analisis desarrollado en los servidores:


```

Starting Nmap 7.94SVN (https://nmap.org) at 2024-06-20 08:54 EDT
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 08:54
Completed NSE at 08:54, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 08:54
Completed NSE at 08:54, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 08:54
Completed NSE at 08:54, 0.00s elapsed
Initiating Ping Scan at 08:54
Scanning 172.20.1.55 [4 ports]
Completed Ping Scan at 08:54, 0.03s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 08:54
Scanning 172.20.1.55 [65535 ports]
Discovered open port 3389/tcp on 172.20.1.55
Discovered open port 445/tcp on 172.20.1.55
Discovered open port 139/tcp on 172.20.1.55
Discovered open port 1025/tcp on 172.20.1.55
Discovered open port 139/tcp on 172.20.1.55
Completed SYN Stealth Scan at 08:55, 26.40s elapsed (65535 total ports)
Initiating Service scan at 08:55
Scanning 5 services on 172.20.1.55
Completed Service scan at 08:56, 81.53s elapsed (5 services on 1 host)
NSE: Script scanning 172.20.1.55.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 08:56
Completed NSE at 08:56, 14.42s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 08:56
Completed NSE at 08:56, 0.07s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 08:56
Completed NSE at 08:56, 0.00s elapsed
Nmap scan report for 172.20.1.55
Host is up, received reset ttl 255 (0.00071s latency).
Scanned at 2024-06-20 08:54:36 EDT for 122s
Not shown: 65535 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE      REASON      VERSION
135/tcp    open  msrpc        syn-ack ttl 255 Microsoft Windows RPC
139/tcp    open  netbios-ssn syn-ack ttl 255 Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds syn-ack ttl 255 Windows Server (R) 2008 Standard 6002 Service Pack 2 microsoft-ds
1025/tcp   open  ssl          syn-ack ttl 255 Microsoft Windows RPC
3389/tcp   open  ms-wbt-server syn-ack ttl 255
_ ss-:date: 2024-06-20T12:56:48+08:00 --+ from scanner time.
_ ss-cert: Subject: commonName=SERVERDF03.df.eeasa.com
Issuer: commonName=SERVERDF03.df.eeasa.com
Public Key type: rsa
Public Key bits: 2048
Signature Algorithm: sha1WithRSAEncryption
Not valid before: 2024-02-17T14:57:19
Not valid after: 2024-08-18T14:57:19
MD5: c1bd:57da:48fc:02c7:093d:4387:d2a2:dc71
SHA-1: 441a:2876:687f:5204:c787:8a96:b900:1055:57c2:9028
-----BEGIN CERTIFICATE-----
MIIC8jCAdqggAwIBAQIDQQUHVDgtcSRHEz5AJAIDAFDANBgkqhkiG9w0BAQFADAIB
MCAhBgkqhkiG9w0BAQwRMBYwIHZYIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEi
NDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAw
IHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5
cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9
ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpd
jEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiN
DAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAw
IHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5
cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9
ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpd
jEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiN
DAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAw
IHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5
cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9
ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpd
jEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiN
DAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAw
IHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5
cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9
ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpd
jEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiN
DAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAw
IHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5
cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9
ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpd
jEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiN
DAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAw
IHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5
cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9
ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpd
jEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiN
DAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAw
IHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5
cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9
ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpd
jEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiN
DAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAw
IHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5
cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9
ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpd
jEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiN
DAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAw
IHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5
cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9
ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpd
jEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiN
DAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAw
IHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5
cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9
ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpd
jEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiN
DAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAw
IHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5
cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9
ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpd
jEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiN
DAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAw
IHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5
cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9ImNpdjEiNDAwIHR5cGU9
ImNpdjEiNDAwIHR5c
```

Elaborado por: El investigador.

```

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-20 08:58 EDT
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 08:58
Completed NSE at 08:58, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 08:58
Completed NSE at 08:58, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 08:58
Completed NSE at 08:58, 0.00s elapsed
Initiating Ping Scan at 08:58
Scanning 172.20.1.57 [4 ports]
Completed Ping Scan at 08:58, 0.01s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 08:58
Scanning 172.20.1.57 [65535 ports]
Discovered open port 80/tcp on 172.20.1.57
Discovered open port 139/tcp on 172.20.1.57
Discovered open port 135/tcp on 172.20.1.57
Discovered open port 8080/tcp on 172.20.1.57
Discovered open port 445/tcp on 172.20.1.57
Discovered open port 3389/tcp on 172.20.1.57
Completed SYN Stealth Scan at 08:58, 26.34s elapsed (65535 total ports)
Initiating Service scan at 08:58
Scanning 6 services on 172.20.1.57
Completed Service scan at 08:58, 16.29s elapsed (6 services on 1 host)
NSE: Script scanning 172.20.1.57.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 08:58
Completed NSE at 08:59, 15.15s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 08:59
Completed NSE at 08:59, 0.04s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 08:59
Completed NSE at 08:59, 0.00s elapsed
Nmap scan report for 172.20.1.57
Host is up, received reset ttl 255 (0.00063s latency).
Scanned at 2024-06-20 08:58:16 EDT for 57s
Not shown: 65529 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE      REASON      VERSION
80/tcp    open  http         syn-ack ttl 255 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-methods:
|_ Supported Methods: OPTIONS
|_ http-title: Site doesn't have a title.
|_ http-server-header: Microsoft-IIS/7.5
135/tcp    open  msrpc        syn-ack ttl 255 Microsoft Windows RPC
139/tcp    open  netbios-ssn  syn-ack ttl 255 Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds syn-ack ttl 255 Windows Server 2008 R2 Standard 7601 Service Pack 1 microsoft-ds
3389/tcp   open  ms-wbt-server syn-ack ttl 255 Microsoft Terminal Service
8080/tcp   open  http         syn-ack ttl 255 Oracle GlassFish 4.1.1 (Servlet 3.1; JSP 2.3; Java 1.8)
|_ http-methods:
|_ Supported Methods: GET HEAD POST PUT DELETE TRACE OPTIONS
|_ Potentially risky methods: PUT DELETE TRACE
|_ http-server-header: GlassFish Server Open Source Edition 4.1.1
|_ http-title: GlassFish Server - Server Running
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
|_ clock-skew: mean: 1h34m33s, deviation: 2h53m15s, median: -5m28s
|_ smb-os-discovery:
|_ OS: Windows Server 2008 R2 Standard 7601 Service Pack 1 (Windows Server 2008 R2 Standard 6.1)
|_ OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
|_ Computer name: SERVERDF06
|_ NetBIOS computer name: SERVERDF06\x00
|_ Domain name: df.eeasa.com
|_ Forest name: eeasa.com
|_ FQDN: SERVERDF06.df.eeasa.com
|_ System time: 2024-06-20T07:53:36-05:00
|_ smb2-time:
|_ date: 2024-06-20T12:53:35
|_ start_date: 2024-06-19T21:26:36
|_ p2p-conficker:
|_ Checking for Conficker.C or higher...
|_ Check 1 (port 30820/tcp): CLEAN (Couldn't connect)
|_ Check 2 (port 35375/tcp): CLEAN (Couldn't connect)
|_ Check 3 (port 26018/udp): CLEAN (Timeout)
|_ Check 4 (port 59364/udp): CLEAN (Timeout)
|_ 0/4 checks are positive: Host is CLEAN or ports are blocked
|_ smb2-security-mode:
|_ 2.1.0:
|_ Message signing enabled but not required
|_ smb-security-mode:
|_ account_used: guest
|_ authentication_level: user
|_ challenge_response: supported
|_ message_signing: disabled (dangerous, but default)

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 08:59
Completed NSE at 08:59, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 08:59
Completed NSE at 08:59, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 08:59
Completed NSE at 08:59, 0.00s elapsed
Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 58.13 seconds
Raw packets sent: 131088 (5.768MB) | Rcvd: 1520 (60.824KB)

```

Figura 3.97: Nmap SRV PROCESOS AUTOMATICOS
Elaborado por: El investigador.


```
NSE: Script Post-scanning.
NSE: Starting rulelevel: 1 (of 3) scan.
Initiating NSE at 00:52
Completed NSE at 00:52, 0.00s elapsed
NSE: Starting rulelevel: 2 (of 3) scan.
Initiating NSE at 00:52
Completed NSE at 00:52, 0.00s elapsed
NSE: Starting rulelevel: 3 (of 3) scan.
Initiating NSE at 00:52
Completed NSE at 00:53, 0.00s elapsed
Read data files from: /usr/bin/.share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 54.43 seconds
Raw packets sent: 131095 (5.760MiB) Rcvd: 25 (1.008KiB)
```

Elaborado por: El investigador.


```

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-20 09:08 EDT
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 09:08
Completed NSE at 09:08, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 09:08
Completed NSE at 09:08, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 09:08
Completed NSE at 09:08, 0.00s elapsed
Initiating Ping Scan at 09:08
Scanning 172.20.1.92 [4 ports]
Completed Ping Scan at 09:08, 0.04s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 09:08
Scanning 172.20.1.92 [65535 ports]
Discovered open port 22/tcp on 172.20.1.92
Discovered open port 80/tcp on 172.20.1.92
Completed SYN Stealth Scan at 09:08, 26.41s elapsed (65535 total ports)
Initiating Service scan at 09:08
Scanning 2 services on 172.20.1.92
Completed Service scan at 09:08, 5.00s elapsed (2 services on 1 host)
NSE: Script scanning 172.20.1.92.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 09:08
Completed NSE at 09:09, 20.31s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 09:09
Completed NSE at 09:09, 0.01s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 09:09
Completed NSE at 09:09, 0.00s elapsed
Nmap scan report for 172.20.1.92
Host is up, received reset ttl 255 (0.00064s latency).
Scanned at 2024-06-20 09:08:12 EDT for 51s
Not shown: 65533 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE      REASON      VERSION
22/tcp    open  tcpwrapped  syn-ack ttl 255
|_ ssh-hostkey: ERROR: Script execution failed (use -d to debug)
80/tcp    open  tcpwrapped  syn-ack ttl 255
|_ http-methods:
|_   Supported Methods: OPTIONS
|_ http-server-header: Apache/2.4.51 (AlmaLinux)

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 09:09
Completed NSE at 09:09, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 09:09
Completed NSE at 09:09, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 09:09
Completed NSE at 09:09, 0.00s elapsed
Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 52.07 seconds
Raw packets sent: 131092 (5.768MB) | Rcvd: 26 (1.048KB)

```

Figura 3.100: Nmap SRV AIX
Elaborado por: El investigador.

3.2.4 Entregar el Informe detallado de las vulnerabilidades encontradas.

A continuación, presento el informe entregado al Jefe del Área Informática del Departamento Financiero de la Empresa Eléctrica Regional Centro Norte S.A. desde la **Figura 3.101** hasta la **Figura 3.148**.

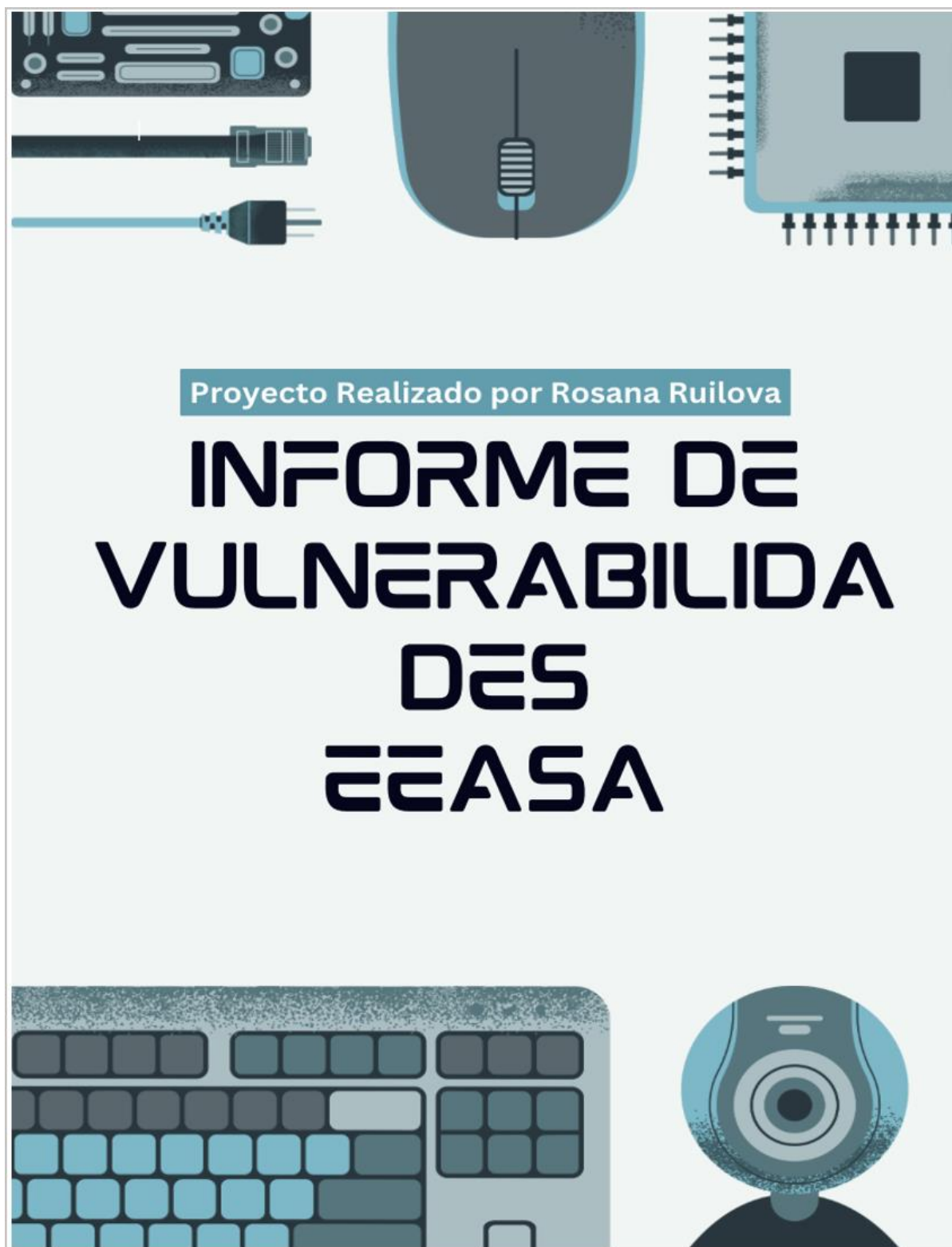


Figura 3.101: Informe de Vulnerabilidades
Elaborado por: El investigador.

INDEX

1.	INTRODUCCIÓN	3
2.	RESULTADOS	4
A.	SERVIDOR VIRTUALIZADO AD	4
B.	SERVIDOR FÍSICO ILO.....	9
C.	SERVIDOR FÍSICO NAS	11
D.	SERVIDOR VIRTUALIZADO DEL SISTEMA INFORMATICO FINANCIERO PRINCIPAL	15
E.	SERVIDOR FÍSICO VEAMBACKUP DE RESPALDOS DE LA MÁQUINAS VIRTUALES Y BASES DE DATOS	25
F.	SERVIDOR VIRTUALIZADO PROCESOS AUTOMÁTICOS	29
G.	SERVIDOR FÍSICO GLOBAL VMWARE ESXI 7.0.....	33
H.	SERVIDOR AIX 5.3	41
3.	TABLAS DE CRITICIDAD	46
4.	RECOMENDACIONES GENERALES	48

Figura 3.102: Informe de Vulnerabilidades
Elaborado por: El investigador.

1. Introducción

En el entorno digital actual, la seguridad de la información se ha convertido en una prioridad esencial para las organizaciones. La proliferación de ataques cibernéticos y la sofisticación de las técnicas utilizadas por los atacantes hacen que las empresas del sector estratégico implementen medidas de seguridad proactivas y efectivas. Este informe se centra en el análisis de vulnerabilidades mediante el uso de herramientas de pruebas de penetración (pentesting) para evaluar y fortalecer la seguridad de los sistemas y aplicaciones en la Empresa Eléctrica Ambato.

Las herramientas de pentesting, como Nmap, Dmitry, Nessus y Metasploit, son necesarias para identificar y mitigar los riesgos de seguridad existentes. Estas herramientas permiten detectar vulnerabilidades antes de que puedan ser explotadas por actores malintencionados. El presente informe documenta el uso de estas herramientas para realizar el análisis de los servidores y aplicaciones, identificando debilidades y proponiendo recomendaciones para mejorar la postura de seguridad de la organización.

El presente informe no solo proporciona una visión detallada de las vulnerabilidades actuales, sino que también ofrece un conjunto de medidas preventivas para evitar posibles incidentes de seguridad en el futuro. A través de una metodología sistemática, se busca garantizar la integridad, disponibilidad y confidencialidad de los datos, protegiendo así los activos más valiosos de la empresa.

En los siguientes apartados, se describen las herramientas utilizadas, las vulnerabilidades detectadas y las recomendaciones específicas para cada una de ellas. Asimismo, se incluyen conclusiones sobre la efectividad de las herramientas de pentesting empleadas en el ambiente controlado de la EEASA y la importancia de mantener un enfoque constante y actualizado en la gestión de la seguridad informática.

Figura 3.103: Informe de Vulnerabilidades
Elaborado por: El investigador.

2. Resultados

a. Servidor Virtualizado AD

Nombre: 35291 - SSL Certificate Signed Using Weak Hashing Algorithm

Criticidad: Media

Descripción:

El servicio remoto utiliza una cadena de certificados SSL que ha sido firmada utilizando un algoritmo de hash criptográficamente débil (por ejemplo, MD2, MD4, MD5 o SHA1). Se sabe que estos algoritmos de firma son vulnerables a ataques de colisión. Un atacante puede explotar esta vulnerabilidad para generar otro certificado con la misma firma digital, lo que permitiría al atacante hacerse pasar por el servicio afectado.

Cabe destacar que este complemento informa todas las cadenas de certificados SSL firmadas con SHA-1 que expiran después del 1 de enero de 2017 como vulnerables. Esto está en conformidad con la eliminación gradual del algoritmo de hash criptográfico SHA-1 por parte de Google.

Además, se han ignorado los certificados en la cadena que están contenidos en la base de datos CA de Nessus (known_CA.inc).

Recomendación:

Para mitigar la vulnerabilidad asociada con el uso de algoritmos de hash criptográficamente débiles en certificados SSL, se recomienda lo siguiente:

Actualizar Certificados SSL, Verificar la Cadena de Certificados, Configurar Correctamente los Servicios SSL/TLS.

Nombre: 51192 - SSL Certificate Cannot Be Trusted

Criticidad: Media

Descripción:

Figura 3.104: Informe de Vulnerabilidades
Elaborado por: El investigador.

El certificado X.509 del servidor no puede ser confiado. Esta situación puede ocurrir de tres maneras diferentes, en las cuales la cadena de confianza puede romperse, como se indica a continuación:

- Primero, la parte superior de la cadena de certificados enviada por el servidor puede no descender de una autoridad de certificación pública conocida. Esto puede ocurrir cuando la parte superior de la cadena es un certificado autofirmado no reconocido, o cuando faltan certificados intermedios que conectarían la parte superior de la cadena de certificados con una autoridad de certificación pública conocida.
- Segundo, la cadena de certificados puede contener un certificado que no es válido en el momento del escaneo. Esto puede ocurrir cuando el escaneo se realiza antes de una de las fechas 'notBefore' del certificado, o después de una de las fechas 'notAfter' del certificado.
- Tercero, la cadena de certificados puede contener una firma que no coincide con la información del certificado o que no pudo ser verificada. Las firmas defectuosas pueden ser corregidas haciendo que el certificado con la firma defectuosa sea firmado nuevamente por su emisor. Las firmas que no pudieron ser verificadas son el resultado de que el emisor del certificado utiliza un algoritmo de firma que Nessus no soporta o no reconoce.

Si el host remoto es un host público en producción, cualquier ruptura en la cadena hace más difícil para los usuarios verificar la autenticidad e identidad del servidor web. Esto podría facilitar la realización de ataques de tipo hombre-en-el-medio contra el host remoto.

Recomendación:

Adquiera o genera un certificado SSL adecuado para este servicio.

Nombre: 65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Criticidad: Media

Descripción:

Figura 3.105: Informe de Vulnerabilidades
Elaborado por: El investigador.

El host remoto admite el uso de RC4 en una o más suites de cifrado. El cifrado RC4 tiene fallos en la generación de un flujo de bytesseudorandomizado, lo que introduce una gran variedad de pequeños sesgos en el flujo, disminuyendo su aleatoriedad. Si el texto plano se cifra repetidamente (por ejemplo, cookies HTTP) y un atacante es capaz de obtener muchos (es decir, decenas de millones) textos cifrados, el atacante podría ser capaz de derivar el texto plano.

Recomendación:

Reconfigure la aplicación afectada, si es posible, para evitar el uso de cifrados RC4. Considere utilizar TLS 1.2 con suites AES-GCM, dependiendo del soporte del navegador y del servidor web.

Nombre: 57582 - SSL Self-Signed Certificate

Criticidad: Media

Descripción:

La cadena de certificados X.509 para este servicio no está firmada por una autoridad de certificación reconocida. Si el host remoto es un host público en producción, esto invalida el uso de SSL ya que cualquier persona podría llevar a cabo un ataque de hombre en el medio contra el host remoto. Ten en cuenta que este complemento no verifica las cadenas de certificados que terminan en un certificado que no está autofirmado, pero que está firmado por una autoridad de certificación no reconocida.

Recomendación:

Adquiera o genera un certificado SSL adecuado para este servicio.

Nombre: 104743 - TLS Version 1.0 Protocol Detection

Criticidad: Media

Descripción:

Figura 3.106: Informe de Vulnerabilidades
Elaborado por: El investigador.

El servicio remoto acepta conexiones cifradas utilizando TLS 1.0. TLS 1.0 presenta una serie de fallos de diseño criptográfico. Las implementaciones modernas de TLS 1.0 mitigan estos problemas, pero versiones más nuevas como TLS 1.2 y 1.3 están diseñadas para evitar estos fallos y deben ser utilizadas siempre que sea posible.

A partir del 31 de marzo de 2020, los puntos finales que no estén habilitados para TLS 1.2 y versiones superiores dejarán de funcionar correctamente con los principales navegadores web y proveedores importantes.

El estándar PCI DSS v3.2 requiere que TLS 1.0 sea deshabilitado completamente para el 30 de junio de 2018, excepto para terminales POS POI (y los puntos de terminación SSL/TLS a los que se conectan) que puedan ser verificados como no susceptibles a ninguna explotación conocida.

Recomendación:

Habilita el soporte para TLS 1.2 y 1.3, y deshabilita el soporte para TLS 1.0.

Nombre: 157288 - TLS Version 1.1 Deprecated Protocol

Criticidad: Media

Descripción:

El servicio remoto acepta conexiones cifradas utilizando TLS 1.0. TLS 1.0 presenta una serie de fallos de diseño criptográfico. Las implementaciones modernas de TLS 1.0 mitigan estos problemas, pero versiones más nuevas como TLS 1.2 y 1.3 están diseñadas para evitar estos fallos y deben ser utilizadas siempre que sea posible.

A partir del 31 de marzo de 2020, los puntos finales que no estén habilitados para TLS 1.2 y versiones superiores dejarán de funcionar correctamente con los principales navegadores web y proveedores importantes.

El estándar PCI DSS v3.2 requiere que TLS 1.0 sea deshabilitado completamente para el 30 de junio de 2018, excepto para terminales POS POI (y los puntos de terminación SSL/TLS a

Figura 3.107: Informe de Vulnerabilidades
Elaborado por: El investigador.

los que se conectan) que puedan ser verificados como no susceptibles a ninguna explotación conocida.

Recomendación:

Habilita el soporte para TLS 1.2 y/o 1.3, y deshabilita el soporte para TLS 1.1.

Nombre: 58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only

Criticidad: Media

Descripción:

Los Servicios de Terminal remoto no están configurados para utilizar exclusivamente la Autenticación de Nivel de Red (NLA, por sus siglas en inglés). NLA utiliza el protocolo de Soporte de Seguridad de Credenciales (CredSSP) para realizar una autenticación robusta del servidor mediante mecanismos TLS/SSL o Kerberos, lo cual protege contra ataques de hombre en el medio. Además de mejorar la autenticación, NLA ayuda a proteger la computadora remota de usuarios y software maliciosos al completar la autenticación del usuario antes de establecer una conexión completa de RDP.

Recomendación:

Para habilitar la Autenticación de Nivel de Red (NLA) en el servidor remoto de RDP, generalmente se realiza en la pestaña 'Remote' (Remoto) de la configuración del sistema en Windows.

b. Servidor Físico ILO

Nombre: 42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)

Figura 3.108: Informe de Vulnerabilidades
Elaborado por: El investigador.

Criticidad: Crítica

Descripción:

El host remoto admite el uso de cifrados SSL que ofrecen cifrado de fuerza media. Nessus considera cifrado de fuerza media a aquel que utiliza longitudes de clave de al menos 64 bits y menos de 112 bits, o que utiliza la suite de cifrado 3DES.

Es importante tener en cuenta que es considerablemente más fácil evitar la seguridad proporcionada por el cifrado de fuerza media si el atacante está en la misma red física.

Recomendación:

Reconfigure la aplicación afectada, si es posible, para evitar el uso de cifrados de fuerza media.

Nombre: 51192 - SSL Certificate Cannot Be Trusted

Criticidad: Media

Descripción:

El certificado X.509 del servidor no puede ser confiado. Esta situación puede ocurrir de tres maneras diferentes, en las cuales la cadena de confianza puede romperse, como se indica a continuación:

- Primero, la parte superior de la cadena de certificados enviada por el servidor puede no descender de una autoridad de certificación pública conocida. Esto puede ocurrir cuando la parte superior de la cadena es un certificado autofirmado no reconocido, o cuando faltan certificados intermedios que conectarían la parte superior de la cadena de certificados con una autoridad de certificación pública conocida.
- Segundo, la cadena de certificados puede contener un certificado que no es válido en el momento del escaneo. Esto puede ocurrir cuando el escaneo se realiza antes de una de las fechas 'notBefore' del certificado, o después de una de las fechas 'notAfter' del certificado.

Figura 3.109: Informe de Vulnerabilidades
Elaborado por: El investigador.

- Tercero, la cadena de certificados puede contener una firma que no coincide con la información del certificado o que no pudo ser verificada. Las firmas defectuosas pueden ser corregidas haciendo que el certificado con la firma defectuosa sea firmado nuevamente por su emisor. Las firmas que no pudieron ser verificadas son el resultado de que el emisor del certificado utiliza un algoritmo de firma que Nessus no soporta o no reconoce.

Si el host remoto es un host público en producción, cualquier ruptura en la cadena hace más difícil para los usuarios verificar la autenticidad e identidad del servidor web. Esto podría facilitar la realización de ataques de tipo hombre-en-el-medio contra el host remoto.

Recomendación:

Adquiera o genera un certificado SSL adecuado para este servicio.

Nombre: 45411 - SSL Certificate with Wrong Hostname

Criticidad: Media

Descripción:

El atributo 'commonName' (CN) del certificado SSL presentado para este servicio corresponde a una máquina diferente.

Recomendación:

Adquiere o genera un certificado SSL adecuado para este servicio.

G. Servidor Físico NAS

Nombre: 57608 - SMB Signing not required

Criticidad: Media

Descripción:

En el servidor remoto SMB no se requiere la firma. Un atacante remoto no autenticado puede aprovechar esto para realizar ataques de hombre en el medio contra el servidor SMB.

Figura 3.110: Informe de Vulnerabilidades
Elaborado por: El investigador.

Recomendación:

Para asegurar la firma de mensajes en la configuración del host, en Windows se encuentra en la configuración de directivas bajo 'Microsoft network server: Digitally sign communications (always)'. En Samba, esta configuración se llama 'server signing'. Consulta los enlaces relacionados para más detalles.

Nombre: 51192 - SSL Certificate Cannot Be Trusted

Criticidad: Media

Descripción:

El certificado X.509 del servidor no puede ser confiado. Esta situación puede ocurrir de tres maneras diferentes, en las cuales la cadena de confianza puede romperse, como se indica a continuación:

- Primero, la parte superior de la cadena de certificados enviada por el servidor puede no descender de una autoridad de certificación pública conocida. Esto puede ocurrir cuando la parte superior de la cadena es un certificado autofirmado no reconocido, o cuando faltan certificados intermedios que conectarían la parte superior de la cadena de certificados con una autoridad de certificación pública conocida.
- Segundo, la cadena de certificados puede contener un certificado que no es válido en el momento del escaneo. Esto puede ocurrir cuando el escaneo se realiza antes de una de las fechas 'notBefore' del certificado, o después de una de las fechas 'notAfter' del certificado.
- Tercero, la cadena de certificados puede contener una firma que no coincide con la información del certificado o que no pudo ser verificada. Las firmas defectuosas pueden ser corregidas haciendo que el certificado con la firma defectuosa sea firmado nuevamente por su emisor. Las firmas que no pudieron ser verificadas son el resultado de que el emisor del certificado utiliza un algoritmo de firma que Nessus no soporta o no reconoce.

Figura 3.111: Informe de Vulnerabilidades
Elaborado por: El investigador.

Si el host remoto es un host público en producción, cualquier ruptura en la cadena hace más difícil para los usuarios verificar la autenticidad e identidad del servidor web. Esto podría facilitar la realización de ataques de tipo hombre-en-el-medio contra el host remoto.

Recomendación:

Adquiera o genera un certificado SSL adecuado para este servicio.

Nombre: 45411 - SSL Certificate with Wrong Hostname

Criticidad: Media

Descripción:

El atributo 'commonName' (CN) del certificado SSL presentado para este servicio corresponde a una máquina diferente.

Recomendación:

Adquiere o genera un certificado SSL adecuado para este servicio.

Nombre: 12218 - mDNS Detection (Remote Network)

Criticidad: Media

Descripción:

El servicio remoto comprende el protocolo Bonjour (también conocido como ZeroConf o mDNS), que permite a cualquiera descubrir información del host remoto como el tipo exacto y versión del sistema operativo, su nombre de host y la lista de servicios que está ejecutando. Este plugin intenta descubrir el uso de mDNS por parte de hosts que no están en el segmento de red en el que reside Nessus.

Recomendación:

Filtra el tráfico entrante al puerto UDP 5353, si así se desea.

Figura 3.112: Informe de Vulnerabilidades
Elaborado por: El investigador.

Nombre: 138595 - phpMyAdmin 4.x < 4.9.4 / 5.x < 5.0.1 SQLi (PMASA-2020-1)

Criticidad: Critica

Descripción:

Según el número de versión autoinformado, la aplicación phpMyAdmin alojada en el servidor web remoto es 4.x anterior a 4.9.4 o 5.x anterior a 5.0.1. Por lo tanto, es vulnerable a una vulnerabilidad de inyección SQL (SQLi) en la página de cuentas de usuario. Un atacante remoto autenticado puede explotar esto al inyectar SQL personalizado en lugar de su propio nombre de usuario, para manipular o inyectar consultas SQL en la base de datos backend, lo que podría resultar en la divulgación o manipulación de datos arbitrarios.

Nessus no ha intentado explotar estos problemas, sino que se ha basado únicamente en el número de versión autoinformado por la aplicación.

Recomendación:

Actualiza phpMyAdmin a la versión 4.9.4, 5.0.1 o posterior. Alternativamente, aplica los parches mencionados en los avisos del proveedor.

Nombre: 26194 - Web Server Transmits Cleartext Credentials

Criticidad: Media

Descripción:

El servidor web remoto contiene varios campos de formulario HTML que contienen una entrada de tipo 'password' y transmiten su información a un servidor web remoto en texto plano. Un atacante que intercepte el tráfico entre el navegador web y el servidor puede obtener los nombres de usuario y contraseñas de los usuarios válidos.

Recomendación:

Asegúrate de que cada formulario sensible transmita su contenido a través de HTTPS.

Figura 3.113: Informe de Vulnerabilidades
Elaborado por: El investigador.

d. Servidor Virtualizado del Sistema Informatico Financiero Principal

Nombre: 125313 - Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)

Críticidad: Crítica

Descripción:

El host remoto está afectado por una vulnerabilidad de ejecución remota de código en el Protocolo de Escritorio Remoto (RDP). Un atacante remoto no autenticado puede explotar esto mediante una serie de solicitudes especialmente diseñadas para ejecutar código arbitrario.

Recomendación:

Microsoft ha lanzado un conjunto de parches para Windows XP, 2003, 2008, 7 y 2008 R2. Estos parches abordan diversas vulnerabilidades y problemas de seguridad en esos sistemas operativos. Es recomendable aplicar estos parches para proteger los sistemas contra posibles ataques y problemas de seguridad.

Nombre: 55786 - Oracle Database Unsupported Version Detection

Críticidad: Crítica

Descripción:

Según su versión, la instalación de Oracle Database que se ejecuta en el host remoto ya no tiene soporte. La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, es probable que contenga vulnerabilidades de seguridad.

Recomendación:

Figura 3.114: Informe de Vulnerabilidades
Elaborado por: El investigador.

Actualiza a una versión de Oracle Database que esté actualmente soportada. Esto garantizará que recibas parches de seguridad y soporte continuo del proveedor, reduciendo así el riesgo de vulnerabilidades de seguridad.

Nombre: 108797 - Unsupported Windows OS (remote)

Criticidad: Crítica

Descripción:

La versión remota de Microsoft Windows carece de un service pack o ya no tiene soporte. Como resultado, es probable que contenga vulnerabilidades de seguridad. Es importante considerar actualizar a una versión compatible y soportada por Microsoft para mitigar estos riesgos.

Recomendación:

Actualiza a un service pack o sistema operativo compatible y soportado. Esto ayudará a asegurar que recibas parches de seguridad y soporte continuo del proveedor, reduciendo así la exposición a vulnerabilidades de seguridad.

Nombre: 69552 - Oracle TNS Listener Remote Poisoning

Criticidad: Alta

Descripción:

El TNS listener remoto de Oracle permite el registro de servicios desde un host remoto. Un atacante puede explotar este problema para desviar datos de un servidor o cliente de base de datos legítimo hacia un sistema especificado por el atacante.

Los exploits exitosos permitirán al atacante manipular instancias de bases de datos, potencialmente facilitando ataques de hombre en el medio, secuestro de sesiones o ataques de denegación de servicio en un servidor de base de datos legítimo.

Recomendación:

Figura 3.115: Informe de Vulnerabilidades
Elaborado por: El investigador.

Aplica la solución temporal o el workaround recomendado en el aviso de Oracle. Esto ayudará a mitigar el problema del TNS listener que permite el registro de servicios desde hosts remotos y reducirá el riesgo de explotación por parte de un atacante.

Nombre: 35291 - SSL Certificate Signed Using Weak Hashing Algorithm

Criticidad: Media

Descripción:

El servicio remoto utiliza una cadena de certificados SSL que ha sido firmada utilizando un algoritmo de hash criptográficamente débil (por ejemplo, MD2, MD4, MD5 o SHA1). Se sabe que estos algoritmos de firma son vulnerables a ataques de colisión. Un atacante puede explotar esta vulnerabilidad para generar otro certificado con la misma firma digital, lo que permitiría al atacante hacerse pasar por el servicio afectado.

Cabe destacar que este complemento informa todas las cadenas de certificados SSL firmadas con SHA-1 que expiran después del 1 de enero de 2017 como vulnerables. Esto está en conformidad con la eliminación gradual del algoritmo de hash criptográfico SHA-1 por parte de Google.

Además, se han ignorado los certificados en la cadena que están contenidos en la base de datos CA de Nessus (known_CA.inc).

Recomendación:

Para mitigar la vulnerabilidad asociada con el uso de algoritmos de hash criptográficamente débiles en certificados SSL, se recomienda lo siguiente:

Actualizar Certificados SSL, Verificar la Cadena de Certificados, Configurar Correctamente los Servicios SSL/TLS.

Nombre: 42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)

Criticidad: Critica

Figura 3.116: Informe de Vulnerabilidades
Elaborado por: El investigador.

Descripción:

El host remoto admite el uso de cifrados SSL que ofrecen cifrado de fuerza media. Nessus considera cifrado de fuerza media a aquel que utiliza longitudes de clave de al menos 64 bits y menos de 112 bits, o que utiliza la suite de cifrado 3DES.

Es importante tener en cuenta que es considerablemente más fácil evitar la seguridad proporcionada por el cifrado de fuerza media si el atacante está en la misma red física.

Recomendación:

Reconfigure la aplicación afectada, si es posible, para evitar el uso de cifrados de fuerza media.

Nombre: 18405 - Remote Desktop Protocol Server Man-in-the-Middle Weakness

Criticidad: Media

Descripción:

El servidor remoto del Protocolo de Escritorio Remoto (Terminal Service) es vulnerable a un ataque de hombre en el medio (MiTM). El cliente RDP no realiza ningún esfuerzo para validar la identidad del servidor al establecer la encriptación. Un atacante con la capacidad de interceptar el tráfico del servidor RDP puede establecer encriptación con el cliente y el servidor sin ser detectado. Un ataque MiTM de esta naturaleza permitiría al atacante obtener cualquier información sensible transmitida, incluidas las credenciales de autenticación.

Esta vulnerabilidad existe porque el servidor RDP almacena una clave privada RSA codificada en duro y conocida públicamente. Cualquier atacante en una ubicación de red privilegiada puede usar esta clave para llevar a cabo este tipo de ataque.

Recomendación

Para mitigar los riesgos asociados con el Protocolo de Escritorio Remoto (RDP), puedes implementar las siguientes medidas:

1. Forzar el uso de SSL como capa de transporte

Figura 3.117: Informe de Vulnerabilidades
Elaborado por: El investigador.

2. Configurar Network Level Authentication (NLA)

Implementar estas medidas ayudará a fortalecer la seguridad de las conexiones RDP y a mitigar los riesgos asociados con posibles ataques de interceptación de datos.

Nombre: 57608 - SMB Signing not required

Criticidad: Media

Descripción:

En el servidor remoto SMB no se requiere la firma. Un atacante remoto no autenticado puede aprovechar esto para realizar ataques de hombre en el medio contra el servidor SMB.

Recomendación:

Para asegurar la firma de mensajes en la configuración del host, en Windows se encuentra en la configuración de directivas bajo 'Microsoft network server: Digitally sign communications (always)'. En Samba, esta configuración se llama 'server signing'. Consulta los enlaces relacionados para más detalles.

Nombre: 51192 - SSL Certificate Cannot Be Trusted

Criticidad: Media

Descripción:

El certificado X.509 del servidor no puede ser confiado. Esta situación puede ocurrir de tres maneras diferentes, en las cuales la cadena de confianza puede romperse, como se indica a continuación:

- Primero, la parte superior de la cadena de certificados enviada por el servidor puede no descender de una autoridad de certificación pública conocida. Esto puede ocurrir cuando la parte superior de la cadena es un certificado autofirmado no reconocido, o cuando faltan

Figura 3.118: Informe de Vulnerabilidades
Elaborado por: El investigador.

certificados intermedios que conectarían la parte superior de la cadena de certificados con una autoridad de certificación pública conocida.

- Segundo, la cadena de certificados puede contener un certificado que no es válido en el momento del escaneo. Esto puede ocurrir cuando el escaneo se realiza antes de una de las fechas 'notBefore' del certificado, o después de una de las fechas 'notAfter' del certificado.

- Tercero, la cadena de certificados puede contener una firma que no coincide con la información del certificado o que no pudo ser verificada. Las firmas defectuosas pueden ser corregidas haciendo que el certificado con la firma defectuosa sea firmado nuevamente por su emisor. Las firmas que no pudieron ser verificadas son el resultado de que el emisor del certificado utiliza un algoritmo de firma que Nessus no soporta o no reconoce.

Si el host remoto es un host público en producción, cualquier ruptura en la cadena hace más difícil para los usuarios verificar la autenticidad e identidad del servidor web. Esto podría facilitar la realización de ataques de tipo hombre-en-el-medio contra el host remoto.

Recomendación:

Adquiera o genera un certificado SSL adecuado para este servicio.

Nombre: 45411 - SSL Certificate with Wrong Hostname

Criticidad: Media

Descripción:

El atributo 'commonName' (CN) del certificado SSL presentado para este servicio corresponde a una máquina diferente.

Recomendación:

Adquiere o genera un certificado SSL adecuado para este servicio.

Nombre: 65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Figura 3.119: Informe de Vulnerabilidades
Elaborado por: El investigador.

Criticidad: Media

Descripción:

El host remoto admite el uso de RC4 en una o más suites de cifrado. El cifrado RC4 tiene fallos en la generación de un flujo de bytes seudorandomizado, lo que introduce una gran variedad de pequeños sesgos en el flujo, disminuyendo su aleatoriedad. Si el texto plano se cifra repetidamente (por ejemplo, cookies HTTP) y un atacante es capaz de obtener muchos (es decir, decenas de millones) textos cifrados, el atacante podría ser capaz de derivar el texto plano.

Recomendación:

Reconfigure la aplicación afectada, si es posible, para evitar el uso de cifrados RC4. Considere utilizar TLS 1.2 con suites AES-GCM, dependiendo del soporte del navegador y del servidor web.

Nombre: 57582 - SSL Self-Signed Certificate

Criticidad: Media

Descripción:

La cadena de certificados X.509 para este servicio no está firmada por una autoridad de certificación reconocida. Si el host remoto es un host público en producción, esto invalida el uso de SSL ya que cualquier persona podría llevar a cabo un ataque de hombre en el medio contra el host remoto. Ten en cuenta que este complemento no verifica las cadenas de certificados que terminan en un certificado que no está autofirmado, pero que está firmado por una autoridad de certificación no reconocida.

Recomendación:

Adquiera o genera un certificado SSL adecuado para este servicio.

Nombre: 104743 - TLS Version 1.0 Protocol Detection

Figura 3.120: Informe de Vulnerabilidades
Elaborado por: El investigador.

Criticidad: Media

Descripción:

El servicio remoto acepta conexiones cifradas utilizando TLS 1.0. TLS 1.0 presenta una serie de fallos de diseño criptográfico. Las implementaciones modernas de TLS 1.0 mitigan estos problemas, pero versiones más nuevas como TLS 1.2 y 1.3 están diseñadas para evitar estos fallos y deben ser utilizadas siempre que sea posible.

A partir del 31 de marzo de 2020, los puntos finales que no estén habilitados para TLS 1.2 y versiones superiores dejarán de funcionar correctamente con los principales navegadores web y proveedores importantes.

El estándar PCI DSS v3.2 requiere que TLS 1.0 sea deshabilitado completamente para el 30 de junio de 2018, excepto para terminales POS POI (y los puntos de terminación SSL/TLS a los que se conectan) que puedan ser verificados como no susceptibles a ninguna explotación conocida.

Recomendación:

Habilita el soporte para TLS 1.2 y 1.3, y deshabilita el soporte para TLS 1.0.

Nombre: 157288 - TLS Version 1.1 Deprecated Protocol

Criticidad: Media

Descripción:

El servicio remoto acepta conexiones cifradas utilizando TLS 1.0. TLS 1.0 presenta una serie de fallos de diseño criptográfico. Las implementaciones modernas de TLS 1.0 mitigan estos problemas, pero versiones más nuevas como TLS 1.2 y 1.3 están diseñadas para evitar estos fallos y deben ser utilizadas siempre que sea posible.

Figura 3.121: Informe de Vulnerabilidades
Elaborado por: El investigador.

A partir del 31 de marzo de 2020, los puntos finales que no estén habilitados para TLS 1.2 y versiones superiores dejarán de funcionar correctamente con los principales navegadores web y proveedores importantes.

El estándar PCI DSS v3.2 requiere que TLS 1.0 sea deshabilitado completamente para el 30 de junio de 2018, excepto para terminales POS POI (y los puntos de terminación SSL/TLS a los que se conectan) que puedan ser verificados como no susceptibles a ninguna explotación conocida.

Recomendación:

Habilita el soporte para TLS 1.2 y/o 1.3, y deshabilita el soporte para TLS 1.1.

Nombre: 58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only

Criticidad: Media

Descripción:

Los Servicios de Terminal remoto no están configurados para utilizar exclusivamente la Autenticación de Nivel de Red (NLA, por sus siglas en inglés). NLA utiliza el protocolo de Soporte de Seguridad de Credenciales (CredSSP) para realizar una autenticación robusta del servidor mediante mecanismos TLS/SSL o Kerberos, lo cual protege contra ataques de hombre en el medio. Además de mejorar la autenticación, NLA ayuda a proteger la computadora remota de usuarios y software maliciosos al completar la autenticación del usuario antes de establecer una conexión completa de RDP.

Recomendación:

Para habilitar la Autenticación de Nivel de Red (NLA) en el servidor remoto de RDP, generalmente se realiza en la pestaña 'Remote' (Remoto) de la configuración del sistema en Windows.

Figura 3.122: Informe de Vulnerabilidades
Elaborado por: El investigador.

Nombre: 57690 - Terminal Services Encryption Level is Medium or Low

Criticidad: Media

Descripción:

El servicio remoto de Terminal Services no está configurado para utilizar criptografía fuerte. Utilizar criptografía débil con este servicio puede permitir que un atacante intercepte más fácilmente las comunicaciones y obtenga capturas de pantalla y/o pulsaciones de teclas.

Para mejorar la seguridad, es recomendable configurar el servicio de Terminal Services para utilizar criptografía fuerte, como TLS con cifrados robustos y adecuados para proteger las comunicaciones contra posibles ataques de interceptación.

Recomendación:

Para cambiar el nivel de cifrado RDP en un entorno Windows a uno de los niveles especificados (High o FIPS Compliant), sigue estos pasos:

1. Abrir la Configuración de Escritorio Remoto:
2. Configurar el Nivel de Cifrado:

Seleccionar el Nivel de Cifrado:

3. Aplicar y Guardar Cambios

Nombre: 30218 - Terminal Services Encryption Level is not FIPS-140 Compliant

Criticidad: Baja

Descripción:

La configuración de cifrado utilizada por el servicio remoto de Terminal Services no cumple con FIPS-140.

Recomendación:

Figura 3.123: Informe de Vulnerabilidades
Elaborado por: El investigador.

Cambiar el nivel de cifrado RDP a: 4. Compatible con FIPS.

e. Servidor Físico VEAMBACKUP de respaldos de la máquinas virtuales y bases de datos

Nombre: 35291 - SSL Certificate Signed Using Weak Hashing Algorithm

Criticidad: Media

Descripción:

El servicio remoto utiliza una cadena de certificados SSL que ha sido firmada utilizando un algoritmo de hash criptográficamente débil (por ejemplo, MD2, MD4, MD5 o SHA1). Se sabe que estos algoritmos de firma son vulnerables a ataques de colisión. Un atacante puede explotar esta vulnerabilidad para generar otro certificado con la misma firma digital, lo que permitiría al atacante hacerse pasar por el servicio afectado.

Cabe destacar que este complemento informa todas las cadenas de certificados SSL firmadas con SHA-1 que expiran después del 1 de enero de 2017 como vulnerables. Esto está en conformidad con la eliminación gradual del algoritmo de hash criptográfico SHA-1 por parte de Google.

Además, se han ignorado los certificados en la cadena que están contenidos en la base de datos CA de Nessus (known_CA.inc).

Recomendación:

Para mitigar la vulnerabilidad asociada con el uso de algoritmos de hash criptográficamente débiles en certificados SSL, se recomienda lo siguiente:

Actualizar Certificados SSL, Verificar la Cadena de Certificados, Configurar Correctamente los Servicios SSL/TLS.

Figura 3.124: Informe de Vulnerabilidades
Elaborado por: El investigador.

Nombre: 42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)

Criticidad: Critica

Descripción:

El host remoto admite el uso de cifrados SSL que ofrecen cifrado de fuerza media. Nessus considera cifrado de fuerza media a aquel que utiliza longitudes de clave de al menos 64 bits y menos de 112 bits, o que utiliza la suite de cifrado 3DES.

Es importante tener en cuenta que es considerablemente más fácil evitar la seguridad proporcionada por el cifrado de fuerza media si el atacante está en la misma red física.

Recomendación:

Reconfigure la aplicación afectada, si es posible, para evitar el uso de cifrados de fuerza media.

Nombre: 51192 - SSL Certificate Cannot Be Trusted

Criticidad: Media

Descripción:

El certificado X.509 del servidor no puede ser confiado. Esta situación puede ocurrir de tres maneras diferentes, en las cuales la cadena de confianza puede romperse, como se indica a continuación:

- Primero, la parte superior de la cadena de certificados enviada por el servidor puede no descender de una autoridad de certificación pública conocida. Esto puede ocurrir cuando la parte superior de la cadena es un certificado autofirmado no reconocido, o cuando faltan certificados intermedios que conectarían la parte superior de la cadena de certificados con una autoridad de certificación pública conocida.

Figura 3.125: Informe de Vulnerabilidades
Elaborado por: El investigador.

- Segundo, la cadena de certificados puede contener un certificado que no es válido en el momento del escaneo. Esto puede ocurrir cuando el escaneo se realiza antes de una de las fechas 'notBefore' del certificado, o después de una de las fechas 'notAfter' del certificado.

- Tercero, la cadena de certificados puede contener una firma que no coincide con la información del certificado o que no pudo ser verificada. Las firmas defectuosas pueden ser corregidas haciendo que el certificado con la firma defectuosa sea firmado nuevamente por su emisor. Las firmas que no pudieron ser verificadas son el resultado de que el emisor del certificado utiliza un algoritmo de firma que Nessus no soporta o no reconoce.

Si el host remoto es un host público en producción, cualquier ruptura en la cadena hace más difícil para los usuarios verificar la autenticidad e identidad del servidor web. Esto podría facilitar la realización de ataques de tipo hombre-en-el-medio contra el host remoto.

Recomendación:

Adquiera o genera un certificado SSL adecuado para este servicio.

Nombre: 65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Criticidad: Media

Descripción:

El host remoto admite el uso de RC4 en una o más suites de cifrado. El cifrado RC4 tiene fallos en la generación de un flujo de bytes pseudorandomizado, lo que introduce una gran variedad de pequeños sesgos en el flujo, disminuyendo su aleatoriedad. Si el texto plano se cifra repetidamente (por ejemplo, cookies HTTP) y un atacante es capaz de obtener muchos (es decir, decenas de millones) textos cifrados, el atacante podría ser capaz de derivar el texto plano.

Recomendación:

Figura 3.126: Informe de Vulnerabilidades
Elaborado por: El investigador.

Reconfigure la aplicación afectada, si es posible, para evitar el uso de cifrados RC4. Considere utilizar TLS 1.2 con suites AES-GCM, dependiendo del soporte del navegador y del servidor web.

Nombre: 57582 - SSL Self-Signed Certificate

Criticidad: Media

Descripción:

La cadena de certificados X.509 para este servicio no está firmada por una autoridad de certificación reconocida. Si el host remoto es un host público en producción, esto invalida el uso de SSL ya que cualquier persona podría llevar a cabo un ataque de hombre en el medio contra el host remoto. Ten en cuenta que este complemento no verifica las cadenas de certificados que terminan en un certificado que no está autofirmado, pero que está firmado por una autoridad de certificación no reconocida.

Recomendación:

Adquiera o genera un certificado SSL adecuado para este servicio.

Nombre: 104743 - TLS Version 1.0 Protocol Detection

Criticidad: Media

Descripción:

El servicio remoto acepta conexiones cifradas utilizando TLS 1.0. TLS 1.0 presenta una serie de fallos de diseño criptográfico. Las implementaciones modernas de TLS 1.0 mitigan estos problemas, pero versiones más nuevas como TLS 1.2 y 1.3 están diseñadas para evitar estos fallos y deben ser utilizadas siempre que sea posible.

A partir del 31 de marzo de 2020, los puntos finales que no estén habilitados para TLS 1.2 y versiones superiores dejarán de funcionar correctamente con los principales navegadores web y proveedores importantes.

Figura 3.127: Informe de Vulnerabilidades
Elaborado por: El investigador.

El estándar PCI DSS v3.2 requiere que TLS 1.0 sea deshabilitado completamente para el 30 de junio de 2018, excepto para terminales POS POI (y los puntos de terminación SSL/TLS a los que se conectan) que puedan ser verificados como no susceptibles a ninguna explotación conocida.

Recomendación:

Habilita el soporte para TLS 1.2 y 1.3, y deshabilita el soporte para TLS 1.0.

f. Servidor Virtualizado Procesos Automáticos

Nombre: 34460 - Unsupported Web Server Detection

Criticidad: Critica

Descripción:

El servidor web remoto está obsoleto y ya no es mantenido por su proveedor o fabricante. La falta de soporte implica que no se lanzarán nuevos parches de seguridad para el producto por parte del proveedor. Como resultado, puede contener vulnerabilidades de seguridad.

Recomendación:

Elimine el servidor web si ya no es necesario. De lo contrario, actualice a una versión compatible si es posible o cambie a otro servidor.

Nombre: 108797 - Unsupported Windows OS (remote)

Criticidad: Critica

Descripción:

La versión remota de Microsoft Windows no tiene un service pack o ya no es compatible. Como resultado, es probable que contenga vulnerabilidades de seguridad.

Recomendación:

Actualice a un service pack o sistema operativo compatible.

Figura 3.128: Informe de Vulnerabilidades
Elaborado por: El investigador.

Nombre: 110192 - Oracle GlassFish Server Path Traversal

Criticidad: Alta

Descripción:

La instancia de Oracle GlassFish Server que se ejecuta en el host remoto está afectada por una vulnerabilidad de recorrido de directorios autenticada y no autenticada. Un atacante remoto puede explotar esta vulnerabilidad, mediante una solicitud HTTP especialmente diseñada, para acceder a archivos arbitrarios en el host remoto.

Recomendación:

Póngase en contacto con el proveedor

Nombre: 110612 - Oracle GlassFish Server URL normalization Denial of Service

Criticidad: Alta

Descripción:

La instancia de Oracle GlassFish Server que se ejecuta en el host remoto está afectada por una vulnerabilidad de denegación de servicio autenticada y no autenticada. La vulnerabilidad es el resultado de un bucle infinito en el método `normalize()` en `com.sun.jsftemplating.util.fileStreamer.ResourceContentSource`. Un atacante remoto puede explotar esta vulnerabilidad mediante una solicitud HTTP especialmente diseñada al componente Admin Console.

Recomendación:

Póngase en contacto con el proveedor

Nombre: 18405 - Remote Desktop Protocol Server Man-in-the-Middle Weakness

Figura 3.129: Informe de Vulnerabilidades
Elaborado por: El investigador.

Criticidad: Media

Descripción:

La versión del servidor del Protocolo de Escritorio Remoto (Remote Desktop Protocol Server - Terminal Service) es vulnerable a un ataque de hombre en el medio (MiTM). El cliente RDP no hace ningún esfuerzo por validar la identidad del servidor al establecer la encriptación. Un atacante con la capacidad de interceptar el tráfico desde el servidor RDP puede establecer la encriptación con el cliente y el servidor sin ser detectado. Un ataque MiTM de esta naturaleza permitiría al atacante obtener cualquier información sensible transmitida, incluidas las credenciales de autenticación.

Recomendación:

En los sistemas operativos Microsoft Windows, seleccionar la opción 'Permitir conexiones solo desde equipos que ejecuten Escritorio Remoto con Autenticación a Nivel de Red (Network Level Authentication)' si está disponible.

Nombre: 57608 - SMB Signing not required

Criticidad: Media

Descripción:

En el servidor remoto SMB no se requiere la firma. Un atacante remoto no autenticado puede aprovechar esto para realizar ataques de hombre en el medio contra el servidor SMB.

Recomendación:

Para asegurar la firma de mensajes en la configuración del host, en Windows se encuentra en la configuración de directivas bajo 'Microsoft network server: Digitally sign communications (always)'. En Samba, esta configuración se llama 'server signing'. Consulta los enlaces relacionados para más detalles.

Figura 3.130: Informe de Vulnerabilidades

Elaborado por: El investigador.

Nombre: 58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only

Criticidad: Media

Descripción:

Los Servicios de Terminal remoto no están configurados para utilizar exclusivamente la Autenticación de Nivel de Red (NLA, por sus siglas en inglés). NLA utiliza el protocolo de Soporte de Seguridad de Credenciales (CredSSP) para realizar una autenticación robusta del servidor mediante mecanismos TLS/SSL o Kerberos, lo cual protege contra ataques de hombre en el medio. Además de mejorar la autenticación, NLA ayuda a proteger la computadora remota de usuarios y software maliciosos al completar la autenticación del usuario antes de establecer una conexión completa de RDP.

Recomendación:

Para habilitar la Autenticación de Nivel de Red (NLA) en el servidor remoto de RDP, generalmente se realiza en la pestaña 'Remote' (Remoto) de la configuración del sistema en Windows.

Nombre: 57690 - Terminal Services Encryption Level is Medium or Low

Criticidad: Media

Descripción:

El servicio remoto de Terminal Services no está configurado para utilizar criptografía fuerte. Utilizar criptografía débil con este servicio puede permitir que un atacante intercepte más fácilmente las comunicaciones y obtenga capturas de pantalla y/o pulsaciones de teclas.

Para mejorar la seguridad, es recomendable configurar el servicio de Terminal Services para utilizar criptografía fuerte, como TLS con cifrados robustos y adecuados para proteger las comunicaciones contra posibles ataques de interceptación.

Recomendación:

Figura 3.131: Informe de Vulnerabilidades
Elaborado por: El investigador.

Para cambiar el nivel de cifrado RDP en un entorno Windows a uno de los niveles especificados (High o FIPS Compliant), sigue estos pasos:

1. Abrir la Configuración de Escritorio Remoto:
2. Configurar el Nivel de Cifrado:

Seleccionar el Nivel de Cifrado:

3. Aplicar y Guardar Cambios

Nombre: 30218 - Terminal Services Encryption Level is not FIPS-140 Compliant

Criticidad: Baja

Descripción:

La configuración de cifrado utilizada por el servicio remoto de Terminal Services no cumple con FIPS-140.

Recomendación:

Cambiar el nivel de cifrado RDP a: 4. Compatible con FIPS.

g. Servidor Físico Global VMWARE ESXi 7.0

Nombre: 151665 - ESXi 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2021-0014)

Criticidad: Crítica

Descripción:

El host remoto VMware ESXi está en la versión 6.5, 6.7 o 7.0 y es vulnerable a múltiples vulnerabilidades:

Figura 3.132: Informe de Vulnerabilidades
Elaborado por: El investigador.

- SFCB (Small Footprint CIM Broker), utilizado en ESXi, tiene una vulnerabilidad de bypass de autenticación. Un actor malintencionado con acceso a la red al puerto 5989 en ESXi puede explotar este problema para evadir la autenticación de SFCB enviando una solicitud especialmente diseñada. (CVE-2021-21994)
- OpenSLP, utilizado en ESXi, tiene una vulnerabilidad de denegación de servicio debido a un problema de lectura fuera de límites en el heap. Un actor malintencionado con acceso a la red al puerto 427 en ESXi puede provocar una lectura fuera de límites en el servicio OpenSLP, lo que resulta en una condición de denegación de servicio. (CVE-2021-21995)

Es importante aplicar los parches correspondientes proporcionados por VMware para mitigar estos riesgos de seguridad.

Recomendación:

Aplica el parche adecuado según se indica en el aviso del proveedor (VMware). Esto ayudará a mitigar las vulnerabilidades mencionadas en el host VMware ESXi afectado. Asegúrate de seguir las recomendaciones específicas de VMware para la instalación y la gestión de parches, lo que ayudará a mantener la seguridad y la integridad de tu entorno virtualizado.

Nombre: 191711 - VMware ESXi 7.0 / 8.0 Multiple Vulnerabilities (VMSA-2024-0006)

Criticidad: Alta

Descripción:

The version of VMware ESXi installed on the remote host is vulnerable to multiple issues as outlined in the VMSA-2024-0006 advisory:

- VMware ESXi, Workstation, and Fusion contain a use-after-free vulnerability in the XHCI USB controller (CVE-2024-22252).
- VMware ESXi, Workstation, and Fusion contain a use-after-free vulnerability in the UHCI USB controller (CVE-2024-22253).

Figura 3.133: Informe de Vulnerabilidades
Elaborado por: El investigador.

- VMware ESXi contains an out-of-bounds write vulnerability (CVE-2024-22254).
- VMware ESXi, Workstation, and Fusion contain an information disclosure vulnerability in the UHCI USB controller (CVE-2024-22255).

To mitigate these vulnerabilities, VMware has released updates. It is recommended to apply the appropriate updates as per the VMSA-2024-0006 advisory to secure your VMware ESXi environment. Regularly updating your VMware ESXi hosts helps ensure protection against known vulnerabilities and strengthens overall security posture.

Recomendación:

Actualiza a VMware ESXi 7.0 Update 3p, 8.0 Update 1d o 8.0 Update 2b o una versión posterior. Estas versiones contienen correcciones para múltiples vulnerabilidades mencionadas en el aviso VMSA-2024-0006. La actualización garantizará que tu entorno VMware ESXi esté protegido contra las vulnerabilidades conocidas y mejorará la seguridad general del sistema.

Nombre: 143221 - ESXi 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2020-0026)

Criticidad: Alta

Descripción:

Según el número de versión autoreportado, el host remoto VMware ESXi en las versiones 6.5, 6.7 o 7.0 está afectado por múltiples vulnerabilidades:

- Existe un error de uso después de liberar en el controlador USB XHCI. Un atacante local no autenticado con privilegios administrativos locales en una máquina virtual puede aprovechar esto para ejecutar código como el proceso VMX de la máquina virtual en el host. (CVE-2020-4004)
- Existe una vulnerabilidad de escalada de privilegios en ESXi debido a cómo se gestionan ciertas llamadas al sistema. Un atacante local autenticado con privilegios

Figura 3.134: Informe de Vulnerabilidades
Elaborado por: El investigador.

dentro del proceso VPM puede explotar esto, en combinación con CVE-2020-4004, para obtener privilegios escalados. (CVE-2020-4005)

Recomendación:

Aplica el parche adecuado según se indica en el aviso del proveedor (VMware). Esto ayudará a mitigar las vulnerabilidades mencionadas en el host VMware ESXi afectado. Asegúrate de seguir las instrucciones específicas proporcionadas por VMware para la instalación y gestión de parches, lo que garantizará la corrección de las vulnerabilidades y mejorará la seguridad de tu entorno de virtualización.

Nombre: 158494 - ESXi 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2022-0004)

Criticidad: Media

Descripción:

El host remoto VMware ESXi en las versiones 6.5, 6.7 o 7.0 está afectado por múltiples vulnerabilidades, que incluyen las siguientes:

- VMware ESXi, Workstation y Fusion contienen una vulnerabilidad de uso después de liberar en el controlador USB XHCI. Un actor malintencionado con privilegios administrativos locales en una máquina virtual puede explotar este problema para ejecutar código como el proceso VMX de la máquina virtual en el host. (CVE-2021-22040)
- VMware ESXi, Workstation y Fusion contienen una vulnerabilidad de doble fetch en el controlador USB UHCI. Un actor malintencionado con privilegios administrativos locales en una máquina virtual puede explotar este problema para ejecutar código como el proceso VMX de la máquina virtual en el host. (CVE-2021-22041)
- VMware ESXi contiene una vulnerabilidad de acceso no autorizado debido a que VMX tiene acceso a tickets de autorización de settingsd. Un actor malintencionado con privilegios dentro del proceso VMX puede acceder al servicio settingsd que se ejecuta como usuario de alto privilegio. (CVE-2021-22042)

Figura 3.135: Informe de Vulnerabilidades
Elaborado por: El investigador.

Recomendación:

Para mitigar estas vulnerabilidades, es recomendable aplicar los parches específicos proporcionados por VMware según se detalla en sus avisos de seguridad. Asegúrate de seguir las recomendaciones de VMware para la instalación y gestión de parches, lo cual es crucial para mantener la seguridad de tus sistemas ESXi frente a posibles ataques.

Nombre: 168828 - ESXi 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2022-0030)

Criticidad: Media

Descripción:

El host remoto VMware ESXi en las versiones 6.5, 6.7 o 7.0 está afectado por múltiples vulnerabilidades, que incluyen las siguientes:

- Un problema de corrupción de memoria que puede conducir a un escape del sandbox de ESXi. (CVE-2022-31696)
- Una vulnerabilidad de desbordamiento de montón (heap overflow) que puede ser explotada para divulgar información. (CVE-2022-31699)

Recomendación:

Para mitigar estas vulnerabilidades, se recomienda aplicar los parches específicos proporcionados por VMware según se detalla en sus avisos de seguridad. Es crucial seguir las recomendaciones de VMware para la instalación y gestión de parches, lo cual ayudará a proteger tu entorno VMware ESXi contra posibles amenazas y vulnerabilidades conocidas.

Nombre: 146827 - ESXi 6.5 / 6.7 / 7.0 RCE (VMSA-2021-0002)

Criticidad: Media

Descripción:

Figura 3.136: Informe de Vulnerabilidades

Elaborado por: El investigador.

El host remoto VMware ESXi en las versiones 6.5, 6.7 o 7.0 está afectado por una vulnerabilidad de ejecución remota de código. OpenSLP utilizado en ESXi tiene una vulnerabilidad de desbordamiento de montón (heap overflow). Un actor malicioso que reside en el mismo segmento de red que ESXi y que tiene acceso al puerto 427 podría aprovechar esta vulnerabilidad para desencadenar el problema de desbordamiento de montón en el servicio OpenSLP, lo que podría resultar en la ejecución remota de código.

Recomendación:

Para mitigar esta vulnerabilidad, es recomendable aplicar los parches específicos proporcionados por VMware:

- Para ESXi 7.0: Actualizar a ESXi70U1c-17325551 o una versión posterior.
- Para ESXi 6.7: Actualizar a ESXi670-202102401-SG o una versión posterior.
- Para ESXi 6.5: Actualizar a ESXi650-202102101-SG o una versión posterior.

Sigue las instrucciones proporcionadas por VMware para descargar e instalar estos parches de seguridad. Esto ayudará a proteger tu entorno VMware ESXi contra posibles ataques de ejecución remota de código aprovechando esta vulnerabilidad en OpenSLP.

Nombre: 145090 - ESXi 7.0 DoS (VMSA-2020-0029)

Criticidad: Baja

Descripción:

El host remoto VMware ESXi en la versión 7.0 está afectado por una vulnerabilidad de denegación de servicio (DoS) debido a una validación incorrecta de entrada en GuestInfo. Un actor malicioso con acceso de usuario normal a una máquina virtual puede hacer que se bloquee el proceso vmx de la máquina virtual, lo que lleva a una condición de denegación de servicio.

Recomendación:

Figura 3.137: Informe de Vulnerabilidades
Elaborado por: El investigador.

Para mitigar esta vulnerabilidad, es recomendable aplicar los parches específicos proporcionados por VMware para abordar este problema de seguridad en ESXi 7.0.

Nombre: 51192 - SSL Certificate Cannot Be Trusted

Criticidad: Media

Descripción:

El certificado X.509 del servidor no puede ser confiado. Esta situación puede ocurrir de tres maneras diferentes, en las cuales la cadena de confianza puede romperse, como se indica a continuación:

- Primero, la parte superior de la cadena de certificados enviada por el servidor puede no descender de una autoridad de certificación pública conocida. Esto puede ocurrir cuando la parte superior de la cadena es un certificado autofirmado no reconocido, o cuando faltan certificados intermedios que conectarían la parte superior de la cadena de certificados con una autoridad de certificación pública conocida.

- Segundo, la cadena de certificados puede contener un certificado que no es válido en el momento del escaneo. Esto puede ocurrir cuando el escaneo se realiza antes de una de las fechas 'notBefore' del certificado, o después de una de las fechas 'notAfter' del certificado.

- Tercero, la cadena de certificados puede contener una firma que no coincide con la información del certificado o que no pudo ser verificada. Las firmas defectuosas pueden ser corregidas haciendo que el certificado con la firma defectuosa sea firmado nuevamente por su emisor. Las firmas que no pudieron ser verificadas son el resultado de que el emisor del certificado utiliza un algoritmo de firma que Nessus no soporta o no reconoce.

Si el host remoto es un host público en producción, cualquier ruptura en la cadena hace más difícil para los usuarios verificar la autenticidad e identidad del servidor web. Esto podría facilitar la realización de ataques de tipo hombre-en-el-medio contra el host remoto.

Figura 3.138: Informe de Vulnerabilidades
Elaborado por: El investigador.

Recomendación:

Adquiera o genera un certificado SSL adecuado para este servicio.

Nombre: 57582 - SSL Self-Signed Certificate

Criticidad: Media

Descripción:

La cadena de certificados X.509 para este servicio no está firmada por una autoridad de certificación reconocida. Si el host remoto es un host público en producción, esto invalida el uso de SSL ya que cualquier persona podría llevar a cabo un ataque de hombre en el medio contra el host remoto. Ten en cuenta que este complemento no verifica las cadenas de certificados que terminan en un certificado que no está autofirmado, pero que está firmado por una autoridad de certificación no reconocida.

Recomendación:

Adquiera o genera un certificado SSL adecuado para este servicio.

Nombre: 192466 - VMware ESXi 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2022-0020)

Criticidad: Media

Descripción:

El host remoto VMware ESXi en las versiones 6.5, 6.7 o 7.0 está afectado por múltiples vulnerabilidades, detalladas a continuación:

- Las generaciones de microprocesadores Intel de la 6ª a la 8ª están afectadas por una nueva variante de Spectre que puede eludir su mitigación retpoline en el kernel para filtrar datos arbitrarios. Un atacante con acceso de usuario no privilegiado puede manipular instrucciones de retorno para lograr ejecución de código especulativo

Figura 3.139: Informe de Vulnerabilidades
Elaborado por: El investigador.

arbitrario bajo ciertas condiciones dependientes de la microarquitectura. (CVE-2022-29901)

- El compartir no transparente de objetivos del predictor de retorno entre contextos en algunos procesadores Intel(R) podría permitir a un usuario autorizado potencialmente habilitar la divulgación de información mediante acceso local. (CVE-2022-26373)
- Los alias en el predictor de ramificación pueden hacer que algunos procesadores AMD predigan incorrectamente el tipo de rama, lo que potencialmente lleva a la divulgación de información. (CVE-2022-23825)

Recomendación:

Para mitigar se debe actualizar los parches necesarios

h. Servidor AIX 5.3

Nombre: 161454 - Apache 2.4.x < 2.4.52 mod_lua Buffer Overflow

Criticidad: Crítica

Descripción:

La versión de Apache httpd instalada en el host remoto es anterior a 2.4.52. Por lo tanto, está afectada por una vulnerabilidad relacionada con mod_lua al manejar contenido multipartes. Un cuerpo de solicitud cuidadosamente diseñado puede provocar un desbordamiento de búfer en el analizador multipartes de mod_lua (específicamente en la función r:parsebody() cuando se llama desde scripts Lua). El equipo de Apache httpd no tiene conocimiento de la existencia de un exploit para esta vulnerabilidad, aunque es posible que se pueda crear uno.

Recomendación:

Actualiza a Apache versión 2.4.52 o posterior.

Nombre: 158900 - Apache 2.4.x < 2.4.53 Multiple Vulnerabilities

Criticidad: Alta

Figura 3.140: Informe de Vulnerabilidades
Elaborado por: El investigador

Descripción:

La versión de Apache httpd instalada en el host remoto es anterior a 2.4.53. Por lo tanto, está afectada por múltiples vulnerabilidades según se detalla en el aviso de la versión 2.4.53:

- **mod_lua Uso de un valor no inicializado en r:parsebody:** Un cuerpo de solicitud cuidadosamente diseñado puede causar una lectura en un área de memoria aleatoria, lo que podría llevar a que el proceso se bloquee. Este problema afecta a Apache HTTP Server 2.4.52 y versiones anteriores. Agradecimientos: Chamal De Silva (CVE-2022-22719).
- **HTTP request smuggling:** Apache HTTP Server 2.4.52 y versiones anteriores no cierran la conexión de entrada cuando se encuentran errores al desechar el cuerpo de la solicitud, exponiendo al servidor al ataque de HTTP Request Smuggling. Agradecimientos: James Kettle <james.kettle portswigger.net> (CVE-2022-22720).
- **Posible desbordamiento de búfer con LimitXMLRequestBody muy grande o ilimitado en el núcleo:** Si LimitXMLRequestBody está configurado para permitir cuerpos de solicitud mayores de 350 MB (por defecto es 1 MB) en sistemas de 32 bits, puede ocurrir un desbordamiento de entero que luego causa escrituras fuera de límites. Este problema afecta a Apache HTTP Server 2.4.52 y versiones anteriores. Agradecimientos: Anonymous working with Trend Micro Zero Day Initiative (CVE-2022-22721).
- **Lectura/escritura más allá de los límites en mod_sed:** Una vulnerabilidad de escritura fuera de límites en mod_sed de Apache HTTP Server permite a un atacante sobrescribir memoria de montón con datos proporcionados por el atacante. Este problema afecta a Apache HTTP Server 2.4 versión 2.4.52 y versiones anteriores. Agradecimientos: Ronald Crane (Zippenhop LLC) (CVE-2022-23943).

Recomendación:

Se recomienda actualizar a Apache versión 2.4.53 o posterior para mitigar estas vulnerabilidades.

Figura 3.141: Informe de Vulnerabilidades
Elaborado por: El investigador

Nombre: 161948 - Apache 2.4.x < 2.4.54 Multiple Vulnerabilities

Criticidad: Alta

Descripción:

La versión de Apache httpd instalada en el host remoto es anterior a 2.4.54. Por lo tanto, está afectada por múltiples vulnerabilidades según se detalla en el aviso de la versión 2.4.54:

- **Posible smuggling de solicitud en mod_proxy_ajp:** Vulnerabilidad de 'Interpretación inconsistente de solicitudes HTTP' en mod_proxy_ajp de Apache HTTP Server que permite a un atacante introducir solicitudes a través del servidor AJP al que reenvía solicitudes. Este problema afecta a Apache HTTP Server versión 2.4.53 y versiones anteriores. Agradecimientos: Richter Z @ 360 Noah Lab (CVE-2022-26377).
- **Lectura fuera de límites en mod_isapi:** Apache HTTP Server 2.4.53 y versiones anteriores en Windows pueden leer fuera de los límites cuando están configurados para procesar solicitudes con el módulo mod_isapi. Agradecimientos: El proyecto Apache HTTP Server agradece a Ronald Crane (Zippenhop LLC) por informar este problema (CVE-2022-28330).
- **Lectura fuera de límites a través de ap_rwrite():** La función ap_rwrite() en Apache HTTP Server 2.4.53 y versiones anteriores puede leer memoria no deseada si un atacante puede hacer que el servidor refleje una entrada muy grande utilizando ap_rwrite() o ap_rputs(), como con la función r

() de mod_lua. Agradecimientos: El proyecto Apache HTTP Server agradece a Ronald Crane (Zippenhop LLC) por informar este problema (CVE-2022-28614).
- **Lectura fuera de límites en ap_strcmp_match():** Apache HTTP Server 2.4.53 y versiones anteriores pueden fallar o revelar información debido a una lectura fuera de límites en ap_strcmp_match() cuando se proporciona un búfer de entrada extremadamente grande. Aunque ningún código distribuido con el servidor puede ser forzado a realizar dicha llamada, módulos de terceros o scripts de lua que usen

Figura 3.142: Informe de Vulnerabilidades

Elaborado por: El investigador

ap_strcmp_match() podrían verse afectados hipotéticamente. Agradecimientos: El proyecto Apache HTTP Server agradece a Ronald Crane (Zippenhop LLC) por informar este problema (CVE-2022-28615).

- **Denegación de servicio en mod_lua r**

() En Apache HTTP Server 2.4.53 y versiones anteriores, una solicitud maliciosa a un script lua que llama a r

() puede causar una denegación de servicio debido a que no hay un límite predeterminado en el tamaño posible de entrada. Agradecimientos: El proyecto Apache HTTP Server agradece a Ronald Crane (Zippenhop LLC) por informar este problema (CVE-2022-29404).

- **Denegación de servicio en mod_sed:** Si Apache HTTP Server 2.4.53 está configurado para hacer transformaciones con mod_sed en contextos donde la entrada a mod_sed puede ser muy grande, mod_sed puede hacer asignaciones de memoria excesivamente grandes y provocar una terminación abrupta. Agradecimientos: Este problema fue encontrado por Brian Moussalli del equipo de investigación de seguridad de JFrog (CVE-2022-30522).

- **Divulgación de información en mod_lua con websockets:** Apache HTTP Server 2.4.53 y versiones anteriores pueden devolver longitudes a las aplicaciones que llaman que apuntan más allá del final del almacenamiento asignado para el búfer. Agradecimientos: El proyecto Apache HTTP Server agradece a Ronald Crane (Zippenhop LLC) por informar este problema (CVE-2022-30556).

- **X-Forwarded-For omitido por mecanismo hop-by-hop en mod_proxy:** Apache HTTP Server 2.4.53 y versiones anteriores pueden no enviar los encabezados X-Forwarded- al servidor de origen basado en el mecanismo hop-by-hop del encabezado Connection del cliente. Esto puede utilizarse para evitar la autenticación basada en IP en el servidor de origen/aplicación. Agradecimientos: El proyecto Apache HTTP Server agradece a Gaetan Ferry (Synacktiv) por informar este problema (CVE-2022-31813).

Figura 3.143: Informe de Vulnerabilidades

Elaborado por: El investigador

Recomendación:

Se recomienda actualizar a Apache versión 2.4.54 o posterior para mitigar esta vulnerabilidad.

Nombre: 170113 - Apache 2.4.x < 2.4.55 Multiple Vulnerabilities

Criticidad: Alta

Descripción:

La versión de Apache httpd instalada en el host remoto es anterior a 2.4.55. Por lo tanto, está afectada por múltiples vulnerabilidades según se detalla en el aviso de la versión 2.4.55:

- **Cabecera de solicitud If: cuidadosamente elaborada:** Puede causar una lectura de memoria, o la escritura de un solo byte cero, en una ubicación de memoria de montón (heap) más allá del valor de la cabecera enviada. Esto podría provocar que el proceso se bloquee. Este problema afecta a Apache HTTP Server 2.4.54 y versiones anteriores. (CVE-2006-20001)
- **Vulnerabilidad de 'Interpretación inconsistente de solicitudes HTTP' en mod_proxy_ajp:** Permite a un atacante introducir solicitudes al servidor AJP al que | reenvía las solicitudes. Este problema afecta a Apache HTTP Server versión 2.4.54 y versiones anteriores. (CVE-2022-36760)
- **Truncamiento prematuro de encabezados de respuesta:** Antes de Apache HTTP Server 2.4.55, un backend malicioso puede causar que los encabezados de respuesta se truncen prematuramente, lo que resulta en que algunos encabezados se incorporen al cuerpo de respuesta. Si los encabezados posteriores tienen algún propósito de seguridad, no serán interpretados por el cliente. (CVE-2022-37436)

Recomendación:

Se recomienda actualizar a Apache versión 2.4.55 o posterior para mitigar estas vulnerabilidades.

Figura 3.144: Informe de Vulnerabilidades
Elaborado por: El investigador

3. Tablas de Criticidad

Servidores	Vulnerabilidad	Criticidad
Servidor Virtualizado AD	35291 - SSL Certificate Signed Using Weak Hashing Algorithm	Alta
	42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	Alta
	51192 - SSL Certificate Cannot Be Trusted	Media
	65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Media
	57582 - SSL Self-Signed Certificate	Media
	157288 - TLS Version 1.1 Deprecated Protocol	Media
	58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only	Media
Servidor Físico ILO	42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	Alta
	51192 - SSL Certificate Cannot Be Trusted	Media
	45411 - SSL Certificate with Wrong Hostname	Media
Servidor Físico NAS	57608 - SMB Signing not required	Media
	51192 - SSL Certificate Cannot Be Trusted	Media
	45411 - SSL Certificate with Wrong Hostname	Media
	12218 - mDNS Detection (Remote Network)	Media
Servidor Virtualizado del Sistema Informático Financiero Principal	125313 - Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)	Critica
	55786 - Oracle Database Unsupported Version Detection	Critica
	108797 - Unsupported Windows OS (remote)	Critica
	69552 - Oracle TNS Listener Remote Poisoning	Alta
	35291 - SSL Certificate Signed Using Weak Hashing Algorithm	Alta
	42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	Alta
	18405 - Remote Desktop Protocol Server Man-in-the-Middle Weakness	Media
	57608 - SMB Signing not required	Media
	51192 - SSL Certificate Cannot Be Trusted	Media
	45411 - SSL Certificate with Wrong Hostname	Media
	65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Media
	57582 - SSL Self-Signed Certificate	Media
	157288 - TLS Version 1.1 Protocol Deprecated	Media

Figura 3.145: Informe de Vulnerabilidades
Elaborado por: El investigador

	58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only	Media
	57690 - Terminal Services Encryption Level is Medium or Low	Media
	30218 - Terminal Services Encryption Level is not FIPS-140 Compliant	Baja
Servidor Físico VEAMBACKUP de respaldos de la máquinas virtuales y bases de datos	35291 - SSL Certificate Signed Using Weak Hashing Algorithm	Alta
	42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	Alta
	51192 - SSL Certificate Cannot Be Trusted	Media
	65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Media
	57582 - SSL Self-Signed Certificate	Media
	104743 - TLS Version 1.0 Protocol Detection	Media
	157288 - TLS Version 1.1 Protocol Deprecated	Media
	58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only	Media
Servidor Virtaulizado Procesos Automáticos	34460 - Unsupported Web Server Detection	Crítica
	108797 - Unsupported Windows OS (remote)	Crítica
	110192 - Oracle GlassFish Server Path Traversal	Alta
	110612 - Oracle GlassFish Server URL normalization Denial of Service	Alta
	18405 - Remote Desktop Protocol Server Man-in-the-Middle Weakness	Media
	57608 - SMB Signing not required	Media
	58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only	Media
	57690 - Terminal Services Encryption Level is Medium or Low	Media
	30218 - Terminal Services Encryption Level is not FIPS-140 Compliant	Baja
Servidor Físico Global VMWARE ESXi 7.0	151665 - ESXi 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2021-0014)	Crítica
	191711 - VMware ESXi 7.0 / 8.0 Multiple Vulnerabilities (VMSA-2024-0006)	Crítica
	143221 - ESXi 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2020-0026)	Alta
	158494 - ESXi 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2022-0004)	Alta
	168828 - ESXi 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2022-0030)	Alta
	146827 - ESXi 6.5 / 6.7 / 7.0 RCE (VMSA-2021-0002)	Alta

Figura 3.146: Informe de Vulnerabilidades
Elaborado por: El investigador

	145090 - ESXi 7.0 DoS (VMSA-2020-0029)	Media
	51192 - SSL Certificate Cannot Be Trusted	Media
	51192 - SSL Certificate Cannot Be Trusted	Media
	57582 - SSL Self-Signed Certificate	Media
	192466 - VMware ESXi 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2022-0020)	Media
	192568 - VMware ESXi 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2022-0016)	Media
Servidor AIX 5.3	161454 - Apache 2.4.x < 2.4.52 mod_lua Buffer Overflow	Crítica
	158900 - Apache 2.4.x < 2.4.53 Multiple Vulnerabilities	Crítica
	161948 - Apache 2.4.x < 2.4.54 Multiple Vulnerabilities	Crítica
	170113 - Apache 2.4.x < 2.4.55 Multiple Vulnerabilities	Crítica
	172186 - Apache 2.4.x < 2.4.56 Multiple Vulnerabilities	Crítica
	156255 - Apache 2.4.x >= 2.4.7 / < 2.4.52 Forward Proxy DoS / SSRF	Crítica
	142594 - Oracle WebLogic Server RCE (CVE-2020-14882)	Crítica
	183391 - Apache 2.4.x < 2.4.58 Multiple Vulnerabilities	Alta
	11213 - HTTP TRACE / TRACK Methods Allowed	Media
	187315 - SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795)	Media

Figura 3.147: Informe de Vulnerabilidades
Elaborado por: El investigador

4. Recomendaciones Generales

- Para reducir el riesgo de la vulnerabilidad SQLi (PMASA-2020-1) en PHPMyAdmin, es recomendable actualizar el software a las versiones 4.9.4 o posteriores para la rama 4.x y 5.0.1 o posteriores para la rama 5.x. Así como también permitir la conexión a la consola únicamente a hosts limitados, y no a todas las direcciones ip como actualmente se encuentra configurado.
- Para mitigar la vulnerabilidad Oracle TNS Listener Remote Poisoning, actualice el TNS Listener a la última versión disponible y configure estrictamente el acceso y la seguridad según las recomendaciones de Oracle.
- Para mitigar la vulnerabilidad de detección de servidores web no compatibles, migre a una versión soportada que reciba actualizaciones de seguridad, mantenga el servidor actualizado con parches y realice monitoreos regulares. Además, limite el acceso utilizando configuraciones de firewall.
- Se recomienda que para mitigar la vulnerabilidad SSL Medium Strength Cipher Suites Supported (SWEET32), se deben desactivar los conjuntos de cifrado de fuerza media en la configuración SSL/TLS y configurar solo cifrados fuertes y seguros, esto realizarlo desde la consola de configuración del servidor.
- Se recomienda actualizar las aplicaciones en los servidores para garantizar la seguridad, dado que las actualizaciones típicamente solucionan vulnerabilidades críticas. Además, estas actualizaciones mejoran el rendimiento y la estabilidad al optimizar el código y resolver errores. Mantenerse al día garantiza la compatibilidad con otros elementos del sistema y facilita la adopción de nuevas funciones y mejoras, esenciales para mantener operaciones empresariales eficaces y sin contratiempos. Esta última recomendación se encuentra ligada a la actualización del servidor WEBLOGIC 12 en donde se encuentra centralizadas todas las aplicaciones web de EEASA.

Figura 3.148: Informe de Vulnerabilidades
Elaborado por: El investigador

Presentacion de resultados del escaneo de vulnerabilidades

	Nessus	Nmap	Dmitry
Hostname	Si	Si	Si
Sistema operativo	Si	Si	No
Dominio	Si	Si	No
Puertos abiertos	Si	Si	Si
Servidores de aplicaciones	Si	Si	No
Certificados SSL	Si	Si	No
Vulnerabilidades	Si	No	No
Interfaz gráfica	Si	No	No

Tabla 10: Comparativo

Elaborado por: El investigador.

CAPÍTULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

- En el Departamento Financiero de la Empresa Eléctrica de Ambato Regional Centro Norte S.A., hasta la fecha no se ha realizado ningún análisis destinado a verificar las posibles vulnerabilidades en los servidores. Por lo tanto, la investigación realizada ha sido importante para proporcionar una visión clara de los riesgos existentes y de la necesidad urgente de implementar medidas de seguridad adecuadas para proteger los activos informáticos y garantizar la integridad de la operación financiera de la empresa.
- En la elección de las herramientas y técnicas apropiadas de hacking ético para detectar vulnerabilidades en servidores, se combinaron herramientas tales como Nmap, Dmitry, Nessus y Metasploit dentro de la red institucional de la EEASA. Estas herramientas ofrecen un método completo y eficiente al área de Informática para identificar vulnerabilidades y riesgos en los servidores del Departamento Financiero.
- Los objetivos establecidos para este proyecto de investigación se han cumplido con éxito. La habilidad para distinguir entre falsos positivos y vulnerabilidades reales ha fortalecido la seguridad y ha mejorado la preparación de la EEASA para prevenir posibles ataques. Por esta razón, se han formulado recomendaciones específicas para mitigar amenazas de seguridad.
- Nessus, en la presente investigación, actuó como una herramienta esencial para la detección y gestión de vulnerabilidades de los servidores del Departamento Financiero de la EEASA. Su capacidad para realizar escaneos detallados por cada servidor genera informes para identificar y mitigar riesgos de seguridad. Al mantenerse actualizado con las últimas amenazas, permite a la Jefatura de Área Informática del Departamento Financiero fortalecer sus defensas y asegurar la integridad de la infraestructura informática.

- En el informe de vulnerabilidades, se destaca un hallazgo significativo en el servidor que aloja el sistema informático financiero. Se identificó una vulnerabilidad crítica, conocida como Microsoft RDP RCE (CVE-2019-0708), la cual, mediante un exploit configurado, logró denegar el servicio de manera inmediata.

4.2 Recomendaciones

- Se recomienda mantener actualizado el inventario de hardware y software de servidores, llevando una bitácora de actualizaciones de sistema operativo, firmware, antivirus y antimalware, y evitando la instalación de aplicaciones de usuario final.
- Elaboración de procedimientos y capacitación constante en materia de seguridad informática para la utilización de las herramientas ejecutadas en la presente investigación.
- Se recomienda establecer un plan periódico de análisis de vulnerabilidades para mantener un constante monitoreo sobre los servidores y así detectar posibles puntos débiles que podrían ser aprovechados por atacantes. Implementar este tipo de análisis de manera regular proporciona tranquilidad al asegurar que los sistemas están siendo protegidos contra amenazas cibernéticas.
- Se recomienda actualizar los sistemas operativos que cuentan con versiones desatendidas, ya que un sistema operativo con actualizaciones al día proporciona la seguridad de estar protegido contra las nuevas vulnerabilidades.
- Se sugiere actualizar el protocolo TLS en los servidores para mejorar la seguridad de las comunicaciones encriptadas y asegurar configuraciones seguras de TLS. Esto ayuda a reducir riesgos y protege de manera efectiva la integridad de los datos sensibles y los sistemas.
- Es recomendable tener un servidor redundante para asegurar que las operaciones críticas puedan continuar sin interrupciones en caso de fallos o problemas con el servidor principal. Esto asegura que los servicios que se encuentran en los

servidores del Departamento Financiero de la Empresa Eléctrica de Ambato Regional Centro Norte S.A. estén disponibles y sean confiables en todo momento.

- Se recomienda actualizar las aplicaciones en los servidores para garantizar la seguridad, dado que las actualizaciones típicamente solucionan vulnerabilidades críticas. Además, estas actualizaciones mejoran el rendimiento y la estabilidad al optimizar el código y resolver errores. Mantenerse al día garantiza la compatibilidad con otros elementos del sistema y facilita la adopción de nuevas funciones y mejoras, esenciales para mantener operaciones empresariales eficaces y sin contratiempos.
- Se recomienda actualizar el nivel de cifrado RDP a High o FIPS Compliant.
- Se recomienda que, para mitigar la vulnerabilidad SSL Medium Strength Cipher Suites Supported (SWEET32), se deben desactivar los conjuntos de cifrado de fuerza media en la configuración SSL/TLS y configurar solo cifrados fuertes y seguros.
- Para reducir el riesgo de la vulnerabilidad SQLi (PMASA-2020-1) en PHPMyAdmin, es recomendable actualizar el software a las versiones 4.9.4 o posteriores para la rama 4.x y 5.0.1 o posteriores para la rama 5.x. Además, permitir la conexión a la consola únicamente a hosts limitados, y no a todas las direcciones IP como actualmente se encuentra configurado.
- Para mitigar la vulnerabilidad Oracle TNS Listener Remote Poisoning, actualice el TNS Listener a la última versión disponible y configure estrictamente el acceso y la seguridad según las recomendaciones de Oracle.
- Para mitigar la vulnerabilidad de detección de servidores web no compatibles, migre a una versión soportada que reciba actualizaciones de seguridad, mantenga el servidor actualizado con parches y realice monitoreos regulares. Además, limite el acceso utilizando configuraciones de firewall.

BIBLIOGRAFÍA

- [1] K. A. Pintado Cuji y C. L. Hurtado Valero, «Diagnóstico de las vulnerabilidades informáticas en los sistemas de información para proponer soluciones de seguridad a la rectificadora Gabriel Mosquera S.A.,» Guayaquil, 2015.
- [2] R. M. C. Pilay, «Análisis de amenazas y vulnerabilidades informáticas basado en la Norma ISO 27002,,» La libertad, 2021.
- [3] J. D. A. Tolentino, «ANÁLISIS DE LAS VULNERABILIDADES EN SEGURIDAD INFORMÁTICA DE LOS EQUIPOS DE CÓMPUTO Y REDES DE LA MUNICIPALIDAD DISTRITAL DE INDEPENDENCIA, MEDIANTE EL USO DE PHISHING,» Pimentel - Perú, 2017.
- [4] El país, «El Fondo Monetario Internacional sufre un ciberataque,» 18 03 2024. [En línea]. Available: <https://elpais.com/economia/2024-03-18/el-fondo-monetario-internacional-sufre-un-ciberataque.html>.
- [5] Primicias, «Consejo de la Judicatura denuncia ataque a su sistema informático,» 28 05 2024. [En línea]. Available: <https://www.primicias.ec/noticias/sucesos/consejo-judicatura-ataque-informatico-denuncia-efectos/>.
- [6] G. B. Urbina, Introducción a la Seguridad Informática, México: Patria, 2016.
- [7] S. Leonardo y T. Simón Mario, Introducción a Riesgo Informático, 2004.
- [8] M. I. Romero Castro, G. L. Figueroa Morán, D. S. Vera Navarrete, J. E. Álava Cruzatty, G. R. Parrales Anzúles, C. J. Álava Mero, Á. L. Murillo Quimiz y M. A. Castillo Merino, Introducción a la Seguridad Informática y el análisis de Vulnerabilidades, Alicante: Área de Innovación y Desarrollo, S.L, 2018.
- [9] OWASP, «A01:2021 – Broken Access Control,» 2021. [En línea]. Available: https://owasp.org/Top10/A01_2021-Broken_Access_Control/.

- [10] OWASP, «A02:2021 – Cryptographic Failures,» 2021. [En línea]. Available: https://owasp.org/Top10/A02_2021-Cryptographic_Failures/.
- [11] OWASP, «A03:2021 – Injection,» 2021. [En línea]. Available: https://owasp.org/Top10/A03_2021-Injection/.
- [12] OWASP, «A04:2021 – Insecure Design,» 2021. [En línea]. Available: https://owasp.org/Top10/A04_2021-Insecure_Design/.
- [13] OWASP, «A05:2021 – Security Misconfiguration,» 2021. [En línea]. Available: https://owasp.org/Top10/A05_2021-Security_Misconfiguration/.
- [14] OWASP, «A06:2021 – Vulnerable and Outdated Components,» 2021. [En línea]. Available: https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/.
- [15] OWASP, «A07:2021 – Identification and Authentication Failures,» 2021. [En línea]. Available: https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/.
- [16] OWASP, «A08:2021 – Software and Data Integrity Failures,» 2021. [En línea]. Available: https://owasp.org/Top10/A08_2021-Software_and_Data_Integrity_Failures/.
- [17] OWASP, «A09:2021 – Security Logging and Monitoring Failures,» 2021. [En línea]. Available: https://owasp.org/Top10/A09_2021-Security_Logging_and_Monitoring_Failures/.
- [18] OWASP, «A10:2021 – Falsificación de solicitudes del lado del servidor (SSRF),» 2021. [En línea]. Available: https://owasp.org/Top10/A10_2021-Server-Side_Request_Forgery_%28SSRF%29/.
- [19] C. H. T. T., Amenazas informáticas y seguridad de la información, HeinOnline, 2007.

- [20] A. G. Soriano, «HACKING ÉTICO: MITOS Y REALIDADES,» Seguridad Cultura de Prevención para ti, vol. 2, nº 1, pp. 44-46, 2012.
- [21] Real Academia Española, «Real Academia Española - jáquer,» [En línea]. Available: <https://dle.rae.es/jáquer#>.
- [22] P. Himanen, The Hacker Ethic: A Radical Approach to the Philosophy of Business, Random House Publishing Group, 2009.
- [23] D. Craigen, N. Diakun-Thibault y R. Purse, «Defining Cybersecurity,» Management Review, 10 2014. [En línea]. Available: <http://doi.org/10.22215/timreview/835>.
- [24] E. A. Fischer, «Cybersecurity Issues and Challenges: In Brief,» 12 08 2016. [En línea]. Available: <https://a51.nl/sites/default/files/pdf/R43831.pdf>.
- [25] FORTINET, «Tipos de ciberataques: ataque DDoS, ransomware y más,» [En línea]. Available: <https://www.fortinet.com/lat/resources/cyberglossary/types-of-cyber-attacks>.
- [26] CISCO, «¿Cuáles son los ciberataques más comunes?,» [En línea]. Available: https://www.cisco.com/c/es_mx/products/security/common-cyberattacks.html.
- [27] D. Cunha Barbosa, «Qué es un ataque de Man-in-the-Middle y cómo funciona,» ESET, 28 12 2021. [En línea]. Available: <https://www.welivesecurity.com/la-es/2021/12/28/que-es-ataque-man-in-the-middle-como-funciona/>.
- [28] Kaspersky, «¿Qué es el spear phishing? Definición y riesgos,» [En línea]. Available: <https://latam.kaspersky.com/resource-center/definitions/spear-phishing#>.
- [29] Malwarebytes, «Ransomware,» [En línea]. Available: <https://es.malwarebytes.com/ransomware/>.
- [30] Cloudflare, «¿Qué es un ataque de fuerza bruta?,» [En línea]. Available: <https://www.cloudflare.com/es-es/learning/bots/brute-force-attack/>.

- [31] I. Belcic, «¿Qué es la inyección de SQL y cómo funciona?,» 22 09 2020. [En línea]. Available: <https://www.avast.com/es-es/c-sql-injection>.
- [32] C. Castro, «Pruebas de Penetración e Intrusión,» 2019. [En línea]. Available: <https://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6273/00005218.pdf?sequence=1&isAllowed=y>.
- [33] Keep coding, «¿Qué hace un pentester?,» 2023. [En línea]. Available: <https://keepcoding.io/blog/que-hace-un-pentester/>.
- [34] K. Ortega, «¿Qué tipos de pentesting existen?,» 29 05 2024. [En línea]. Available: <https://worldcampus.saintleo.edu/noticias/que-tipos-de-pruebas-de-penetracion-existen-en-seguridad-informatica>.
- [35] P. Alcarria Lozano, «Fases del pentesting: Pasos para asegurar tus sistemas,» 29 09 2023. [En línea]. Available: <https://openwebinars.net/blog/fases-del-pentesting-pasos-para-asegurar-tus-sistemas/>.
- [36] F. Catoira, «PRUEBAS DE PENETRACIÓN PARA PRINCIPIANTES: EXPLOTANDO UNA VULNERABILIDAD CON METASPLOIT FRAMEWORK,» 18 09 2013. [En línea]. Available: <https://revista.seguridad.unam.mx/numero-19/pruebas-de-penetración-para-principiantes-explotando-una-vulnerabilidad-con-metasploit-fra>.
- [37] Keep Coding, «¿Qué es Nessus?,» [En línea]. Available: <https://keepcoding.io/blog/que-es-nessus/>.
- [38] C. Laprovittera, «Curso Gratis de Redes #24 Nessus,» 12 01 2024. [En línea]. Available: <https://achirou.com/curso-gratis-de-redes-24-nessus/>.
- [39] BlackeyeB, «Qué es Nmap y cómo usarlo: Un tutorial para la mejor herramienta de escaneo de todos los tiempos,» 23 04 2023. [En línea]. Available: <https://www.freecodecamp.org/espanol/news/que-es-nmap-y-como-usarlo-un-tutorial-para-la-mejor-herramienta-de-escaneo-de-todos-los-tiempos/>.

- [40] Eurofins, «El ciclo Deming: en qué consiste y cómo ayuda en la gestión y mejora de procesos,» 10 08 2023. [En línea]. Available: <https://www.eurofins-environment.es/es/el-ciclo-deming-que-consiste-y-como-ayuda-gestion-procesos/>.
- [41] fferia, «Nessus Vulnerability Scanner,» [En línea]. Available: <https://fferia.wordpress.com/nessus/>.
- [42] Tarlogic, «Nessus Vulnerability Scanner Nessus Profesional es la solución de evaluación de las vulnerabilidades más implementada,» [En línea]. Available: <https://www.tarlogic.com/es/productos/nessus-vulnerability-scanner/>.
- [43] S. Daza, «Nessus ¿Cómo hallar vulnerabilidades?,» 04 06 2021. [En línea]. Available: <https://behacker.pro/nessus-como-hallar-vulnerabilidades/>.
- [44] hackingloops, «Dmitry Deepmagic Information Gathering Penetration Testing Tutorial,» [En línea]. Available: <https://www.hackingloops.com/dmitry-deepmagic-information-gathering-penetration-testing-tutorial/>.
- [45] C. Laprovittera, «Guía de Hacking y Pentesting – Capítulo 3: Nmap Reconocimiento y enumeración,» 28 12 2023. [En línea]. Available: <https://achirou.com/guia-de-hacking-y-pentesting-capitulo-3-nmap-reconocimiento-y-enumeracion/>.

ANEXOS

ANEXO A



**Empresa Eléctrica Ambato
Regional Centro Norte S.A.**

Pasión por el servicio..!

CARTA DE COMPROMISO EMPRESARIAL

Ambato, 11 de Abril de 2024

Ingeniero
Carlos Sánchez
Presidente
Unidad de titulación
Carrera de Ingeniería en Sistemas Computacionales e Informáticos
Facultad de Ingeniería en Sistemas, Electrónica e Industrial
Presente.-

Yo FREIRE SILVA JORGE ENRIQUE en mi calidad de Jefe de Área Informática del DEPARTAMENTO FINANCIERO de la EMPRESA ELÉCTRICA AMBATO REGIONAL CENTRO NORTE S.A., me permito poner en su conocimiento la aceptación y respaldo para el desarrollo del Trabajo de Titulación bajo el Tema: "ANÁLISIS DE VULNERABILIDADES MEDIANTE PRUEBAS DE PENETRACIÓN EN LOS SERVIDORES DEL DEPARTAMENTO FINANCIERO DE LA EMPRESA ELÉCTRICA AMBATO REGIONAL CENTRO NORTE S.A." propuesto por la señorita RUILOVA ROMERO ROSANA EMPERATRIZ, portadora de la cédula de ciudadanía **0705756187**, estudiante de la Carrera de Ingeniería en sistemas computacionales e informáticos de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato.

A nombre de la Institución a la cual represento, me comprometo a apoyar en el desarrollo del proyecto.

Particular que comunico a usted para los fines pertinentes.

Atentamente.



Ing. Jorge Enrique Freire Silva, Mgr.
JEFE DE ÁREA INFORMÁTICA DEL DEPARTAMENTO FINANCIERO
EMPRESA ELÉCTRICA AMBATO REGIONAL CENTRO NORTE S.A. (EEASA)
1804738662
03 299 8600 Ext. 1248
0983925985
jfreire@eeasa.com.ec

Av. 12 de Noviembre 11-29 y Espejo Casilla 18-01-446
Telf: (03) 2998600 Reparaciones: 136 Fax: (03) 2421265
www.eeasa.com.ec e-mail: presidencia@eeasa.com.ec
Ambato - Ecuador



Figura A.1: Carta compromiso de la Empresa Eléctrica Ambato Regional Centro Norte S.A. para realizar el proyecto de investigación.

Elaborado por: El investigador.

ANEXO B



**Empresa Eléctrica Ambato
Regional Centro Norte S.A.**

Pasión por el servicio..!

INFORME DEL CUMPLIMIENTO DEL 100% EMITIDO POR EL COORDINADOR
EMPRESARIAL

Ambato, 24/06/2024

Ingeniero,
Carlos Sánchez
PRESIDENTE DE LA UNIDAD DE TITULACIÓN
Facultad de Ingeniería en Sistemas, Electrónica e Industrial
Presente.-

De mi consideración:

JORGE ENRIQUE FREIRE SILVA en mi calidad de Jefe de Área Informática del DEPARTAMENTO FINANCIERO de la Empresa ELECTRICA AMBATO REGIONAL CENTRO NORTE S.A. , me permito poner en su conocimiento que el Trabajo de Titulación con el tema: "ANÁLISIS DE VULNERABILIDADES MEDIANTE PRUEBAS DE PENETRACIÓN EN LOS SERVIDORES DEL DEPARTAMENTO FINANCIERO DE LA EMPRESA ELÉCTRICA AMBATO REGIONAL CENTRO NORTE S.A." desarrollado en esta empresa por la señorita RUILOVA ROMERO ROSANA EMPERATRIZ, portadora de la cédula de ciudadanía 0705756187, estudiante de la Carrera de Ingeniería en Sistemas, Computacionales e Informáticos de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato ha culminado exitosamente **cumpléndose con el 100% de los objetivos y las actividades programadas.**

Particular que comunico a usted para los fines pertinentes.

Atentamente.



Ing. Jorge Enrique Freire Silva, Mgtr.
JEFE DE ÁREA INFORMÁTICA DEL DEPARTAMENTO FINANCIERO
EMPRESA ELÉCTRICA AMBATO REGIONAL CENTRO NORTE S.A.(EEASA)
1804738662
(03) 299-8600 ext 1248
0983925985
jfreire@easa.com.ec

Av. 12 de Noviembre 11-29 y Espejo Casilla 18-01-446
Telf: (03) 2998600 Reparaciones: 136 Fax: (03) 2421265
www.easa.com.ec e-mail: presidencia@easa.com.ec
Ambato - Ecuador



Figura B.1: Certificado de culminación de la Empresa Electrica Ambato Regional Centro Norte S.A.

Elaborado por: El investigador.

ANEXO C

Empresa Eléctrica Ambato Regional Centro Norte S.A. Normas y Políticas de Recursos Tecnológicos y de Seguridad Informática	Código:	POL-001
	Versión:	1.0
	Fecha:	19/09/18
	Página:	15 de 48

5. POLÍTICAS DE RECURSOS TECNOLÓGICOS Y DE SEGURIDAD INFORMÁTICA

5.1 POLÍTICA DE ACCESO A INSTALACIONES FÍSICAS

OBJETIVO: Precautelar la infraestructura de misión crítica instalada en los Centros de Cómputo y/o sitios restringidos.

PROCEDIMIENTO:

El personal de Informática de los diferentes departamentos, verificarán el requerimiento de accesos a los Centros de Cómputo y/o sitios restringidos, el mismo que coordinará el acceso.

El personal de Informática acompañará durante todo el tiempo que la contratista o personal de EEASA requiera visitar dichos centros. Los visitantes deberán permanecer escoltados y portar un distintivo o escarapela claramente visible que identifique sus nombres y a la firma que representa o labora. El personal que labora en la EEASA y que requieran ingresar a áreas críticas también deben permanecer escoltados. Además, tanto los visitantes como los empleados mencionados únicamente deben tener la información y recursos necesarios para el desarrollo de sus actividades.

Se debe mantener el registro de acceso del personal autorizado, como también de ser el caso los comprobantes de servicio técnico realizado.

En el evento que los funcionarios dejen de tener vínculos laborales con la entidad todos sus códigos de acceso deben ser cambiados o desactivados. Además, en caso de pérdida de la tarjeta de acceso también deben desactivarse dichos códigos.

Como mecanismo de prevención todos los empleados y visitantes no deben comer, fumar o beber en los Centros de Cómputo y/o sitios restringidos, al hacerlo estarían exponiendo los equipos a daños eléctricos, riesgos de contaminación sobre los dispositivos de almacenamiento y activación del sistema de detección y extinción de incendios.

Todos los sistemas de control de acceso deben ser monitoreados permanentemente.

Los equipos computacionales existente en los Centros de Cómputo y/o sitios restringidos no deben moverse o reubicarse, no se deberá realizar ninguna interconexión de red ni desconexión sin la aprobación previa del Coordinador Informático.

R

B X

Figura C.1: Normas y Políticas de Recursos Tecnológicos y de Seguridad.
Elaborado por: EEASA.

ANEXO D

Empresa Eléctrica Ambato Regional Centro Norte S.A. Plan de Contingencia Informática	Código:	PCI-001
	Versión:	2.0
	Fecha:	18/11/2020
	Página:	22 de 53

Oracle 12c ubicado en centro de cómputo CECON.

Se encuentra en ejecución la implementación de la Etapa II del Sistema de contingencia, que consiste en la implementación de un Sistema similar al ubicado en el CECON en el centro de cómputo del nuevo edificio de la Sucursal Mayor Puyo.

Fallos en equipos de cómputo

- **Mantenimiento Preventivo por Equipo Informático**

El mantenimiento de los equipos personales, impresoras y escáner será realizado de forma anual y coordinado por el Jefe de Área Informática del Departamento Financiero, quien realizará los lineamientos para la contratación externa para las tareas de mantenimiento, donde por lo menos se realizarán tareas como: levantamiento de información del equipamiento, limpieza interna y externa de todos los componentes y en el caso de los equipos de computación revisión de instalación de software antivirus y que se encuentre actualizado y sincronizado con las consolas del antivirus empresarial.

- **Inventario de hardware y software**

Se gestiona los activos hardware y software de la EEASA, los mismos que serán administrados por medio del procedimiento de infraestructura del Sistema de Gestión de Calidad - SGC y alimentado periódicamente por las actualizaciones remitidas por el personal de informática de los diferentes departamentos, que facilite una rápida identificación y restauración de las aplicaciones instaladas.

9.2.1 PLAN DE ACCIÓN

9.2.1.1 SISTEMA DE ALTA DISPONIBILIDAD

OBJETIVO: Establecer responsables y tareas necesarias para garantizar el funcionamiento del sistema de alta disponibilidad de la EEASA.

PROCEDIMIENTO:

- El personal de informática de los Departamentos de Subtransmisión, Planificación, Financiero y DZOP deberán realizar los trámites para los respectivos mantenimientos preventivos y/o correctivos de la infraestructura de los Centros de Cómputo de la EEASA. Estos contratos de mantenimientos deberán ser anuales con una revisión de la infraestructura de forma

Figura D.1: Plan de Contingencia Informática.
Elaborado por: EEASA.

Empresa Eléctrica Ambato Regional Centro Norte S.A.**Plan de Contingencia Informática**

Código:	PCI-001
Versión:	2.0
Fecha:	18/11/2020
Página:	23 de 53

cuatrimestral por parte del contratista.

- El personal de informática de los diferentes departamentos deberá reportar de alguna novedad y/o inconveniente en los servicios prestados por los sistemas de alta disponibilidad y/o infraestructura de los Centros de Cómputo al los Líderes de Tecnología.
- El personal de informática Departamento de Subtransmisión y personal del área CECON, en todos los eventos de pérdida de suministro eléctrico que involucre más de 10 minutos deberá notificar de manera oportuna por todos los medios al personal de Informática, Telecomunicaciones y Coordinador Informático sobre el fallo de suministro eléctrico en el área de concesión de la empresa y que afecten los Centros de cómputo y áreas críticas donde se disponga equipos, para coordinación, toma de decisiones y maniobras en los diferente sitios o departamentos de la empresa.
- El tiempo de respaldo de energía en los Centro de Cómputo es de aproximadamente entre los 30 a 90 minutos, dependiendo de la carga instalada y del estado de las baterías.
- El tiempo máximo de funcionamiento de los servidores en los Centros de Cómputo de la EEASA sin aire acondicionado por falta de suministro eléctrico es de 10 minutos. Pasado este tiempo los servidores empiezan alarmarse y proceden al apagado abrupto por protección.
- En los Centros de Cómputo, se dispone de redundancia activa - activa a nivel de UPS, aires acondicionados, telecomunicaciones y servidores.
- Los Centros de Cómputo CECON y DZOP disponen de un grupo electrógeno.
- En los casos donde la situación del fallo del suministro eléctrico supere el tiempo de respaldo de energía y/o carga térmica se deberá realizar el apagado total del equipamiento, considerando que toma aproximadamente unos 30 minutos el apagado total de cada uno de los centros de cómputo.
- En el caso de apagado del equipamiento de los centros de cómputo, se deberá coordinar el encendido, el mismo que toma aproximadamente de tres horas, este incremento se debido a que es necesario el monitoreo del correcto funcionamiento de cada componente o sistema. La puesta en funcionamiento y revisión de los sistemas informáticos y telecomunicaciones de la matriz y DZOP deberán ser realizados de la siguiente manera:

RESPONSABLE	SISTEMAS REVISADOS Y PUESTOS A PUNTO
Líderes de infraestructura de redes y comunicaciones	Red de datos anillo Subestaciones y routers de core Sistema de Cámaras IP Red de datos LAN e inalámbrica.
Jefe de Área Informática Planificación	Servidor ARCGIS base de datos Servidores SISDE base de datos Servidor Oracle LITE sistemas móviles

Figura D.2: Plan de Contingencia Informática.
Elaborado por: EEASA.

Empresa Eléctrica Ambato Regional Centro Norte S.A.	Código: PCI-001
Plan de Contingencia Informática	Versión: 2.0
	Fecha: 18/11/2020
	Página: 24 de 53

	Servidores Aplicaciones Oracle WebLogic Balanceadores LTM de Aplicaciones Servidores de Licencias CYME, ESRI, ARCFM
Jefe de Área Informática Financiero	Servidores Sistema Financiero Servidor de almacenamiento NAS
Coordinador Informático	Servidor de Almacenamiento, matriz y DZOP Servidores de Base de Datos y Administración Storage, matriz y DZOP Servidores de Telemedición Base de datos y Aplicaciones Servidores de Virtualización (3 físicos, 21 virtuales) Balanceadores LC Enlace a Internet Servidores de Internet (8 servidores) Monitoreo de funcionamiento y estado red LAN y WAN Servidores de Seguridad y Antivirus Revisión funcionamiento equipos Firewall e IPS Revisión funcionamiento Wireless Controller y servidor proxy Servidores Centro de Cómputo DZOP Sincronización solución de respaldo base de datos en Standby
Jefe Call Center	Sistema de Telefonía IP Call Center
Jefe de Área Informática DZOP	Soporte DZOP para encendido y administración de sistema alta disponibilidad.

- El Jefe de Servicios Generales con personal de los Departamentos de Relaciones Industriales, Subtransmisión y Distribución deberán realizar el análisis para la implementación de grupo electrógeno en los sitios donde no se dispone de un grupo electrógeno como es el caso de edificio matriz y edificio DZON, que permita el suministro para la capacidad instalada en dichos centros.

9.2.1.2 SISTEMAS INFORMÁTICOS

OBJETIVO: Proporcionar las directrices para enfrentar la interrupción o falta de continuidad en el procesamiento de información y servicios informáticos, debido a fallas generadas por causas naturales, error humano, sabotaje, siniestro, etc.

PROCEDIMIENTO:

- Los departamentos disponen de un servidor de almacenamiento de disco NAS (Network Attached Storage), que deben ser utilizados para el almacenamiento de respaldos de información.
- Adicionalmente, el departamento de Planificación de La EEASA dispone de un servidor de almacenamiento de disco NAS (Network Attached Storage) en el centro de cómputo matriz donde el personal de Informática de los diferentes departamentos y/o encargados del desarrollo de software de EEASA deberán almacenar los códigos fuentes de los sistemas informáticos con sus respectivas versiones y documentación. A la vez este repositorio se replica automáticamente a otra solución de almacenamiento NAS ubicado en el Centro

Figura D.3: Plan de Contingencia Informática.

Elaborado por: EEASA.

Empresa Eléctrica Ambato Regional Centro Norte S.A.**Plan de Contingencia Informática**

Código:	PCI-001
Versión:	2.0
Fecha:	18/11/2020
Página:	25 de 53

de Cómputo del Departamento Zona Oriental Pastaza (sitio de contingencia).

- Se realizará un respaldo automático diario de la base de datos del sistema de alta disponibilidad, el mismo que reposa en un servidor de almacenamiento SAN (Storage Area Network) del Centro de Cómputo CECON, asimismo, diariamente se realiza un respaldo incremental a una servidor de respaldo ubicado en el mismo Centro, todos los días viernes de la semana se realizará un respaldo completo de la base de datos a la librería.
- Se dispone de una base de datos de contingente con información del sistema de alta disponibilidad de la matriz.
- La infraestructura de la matriz y sitio de contingencia disponen de una arquitectura redundante (Activa / Activa y Activa / Pasiva) en la infraestructura de centros de cómputo, servidores de procesamiento (base de datos y aplicaciones), almacenamiento, red de datos e Internet.
- La EEASA dispone de sistemas denominados de alta disponibilidad, compuesto de infraestructura redundante en servidores de procesamiento, red de Storage Area Network (SAN), almacenamiento, entre otros, donde se dispone de Oracle Database con Real Application Cluster - RAC con una configuración cluster Activa / Activa.
- El personal de Informática de los diferentes departamentos y telecomunicaciones, deberá contar con contratos de garantía de la infraestructura de misión crítica y redes, en su defecto dispondrán de un stock de repuestos mínimo que permita superar una contingencia por fallas en los equipos o dispositivos de comunicación.
- El personal de Informática de los diferentes departamentos deberán gestionar anualmente el mantenimiento preventivo y/o correctivo de los equipos de cómputo e impresoras de la EEASA.
- Todo Sistema Informático de la EEASA en producción deberá tener los manuales de usuario, técnico y diccionario de datos, entre otros, como documentada las acciones de recuperación de servicio, ante cualquier tipo de emergencia, los mismos que estarán a cargo del personal de informático responsable de cada departamento. Asimismo, mencionados manuales deben ser constantemente actualizados.
- El personal de Telecomunicaciones del departamento de Subtransmisión deberá garantizar la redundancia de los canales de comunicación a los Centros de Cómputo donde se dispone de los sistemas de alta disponibilidad.
- El acceso a los Centros de Cómputo y sitios donde se disponga de equipos de misión crítica, deben ser restringidos. En el caso de ser requerido los invitados y/o contratistas siempre serán escoltados por personal de Informática de la EEASA encargados de los trabajos.
- Los Administradores de Red e Internet deberán monitorear permanentemente los sistemas de comunicación e Internet con el propósito de verificar su

Figura D.4: Plan de Contingencia Informática.

Elaborado por: EEASA.

Empresa Eléctrica Ambato Regional Centro Norte S.A.	Código: PCI-001
Plan de Contingencia Informática	Versión: 2.0
	Fecha: 18/11/2020
	Página: 26 de 53

adecuado funcionamiento y detectar posibles intromisiones a los sistemas y debilidades del sistema.

- Los Administrador de Red e Internet deberán disponer de un respaldo de las configuraciones de los dispositivos de red y seguridad de la EEASA.

Figura D.5: Plan de Contingencia Informática.

Elaborado por: EEASA.

ANEXO E

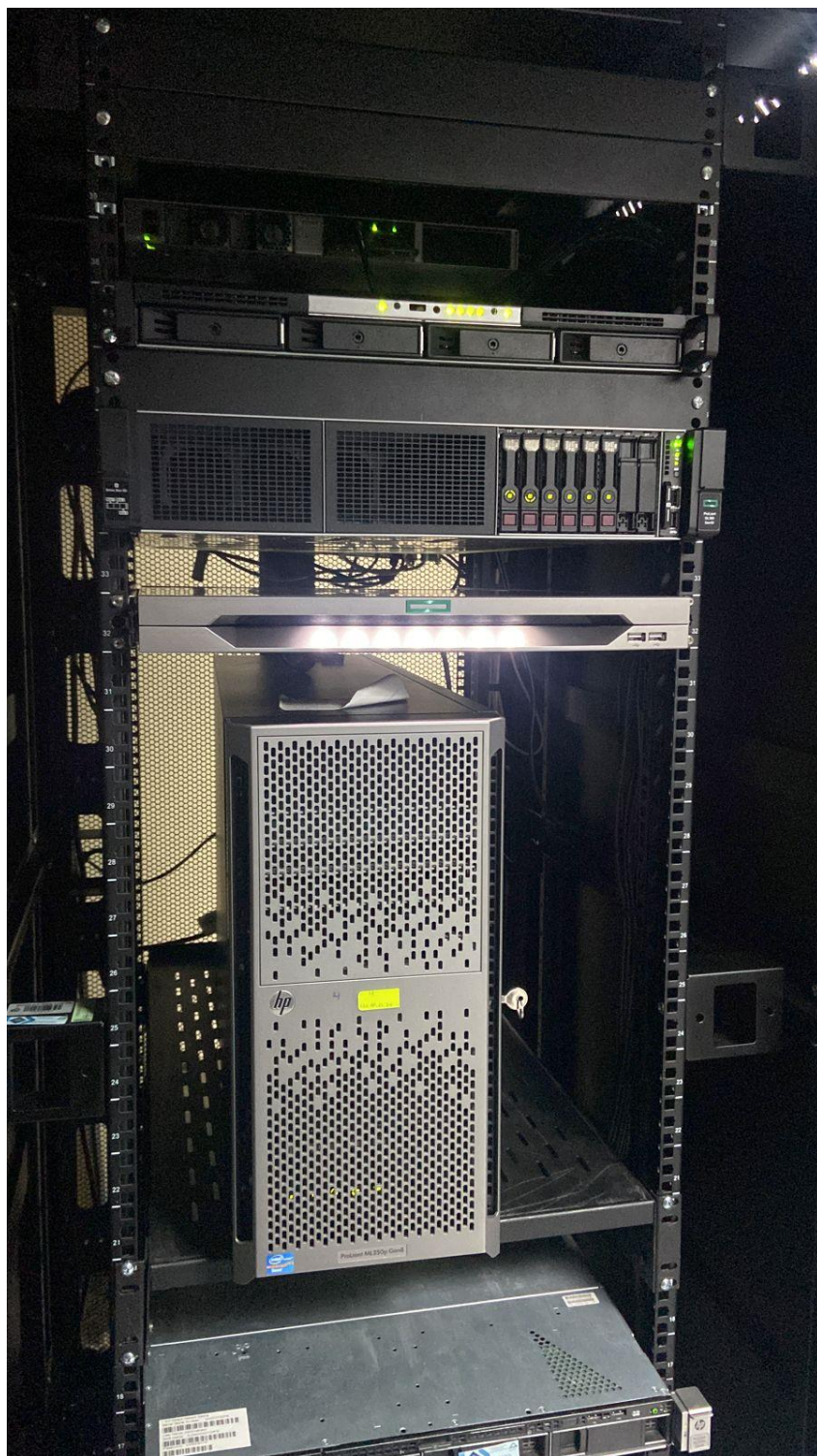


Figura E.1: Rack Servidores Departamento Financiero, parte delantera
Elaborado por: el investigador.



Figura E.2:Parte superior servidor Synology NAS, parte inferior Servidor HP DL385
Elaborado por: el investigador.



Figura E.3:Servidor HP ML350 generación 8
Elaborado por: el investigador.

ANEXO F

Instalación de Nessus para el análisis de vulnerabilidades en los servidores.

Para realizar la instalación, hemos preparado una máquina con Kali Linux como se muestra en la **Figura F.1**.

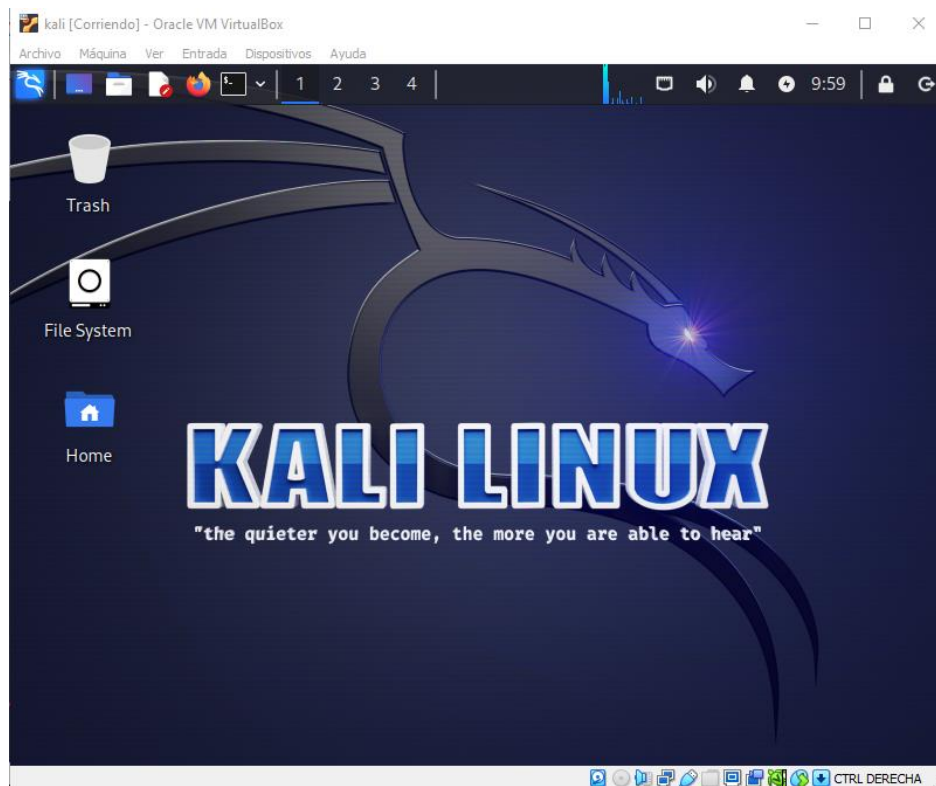
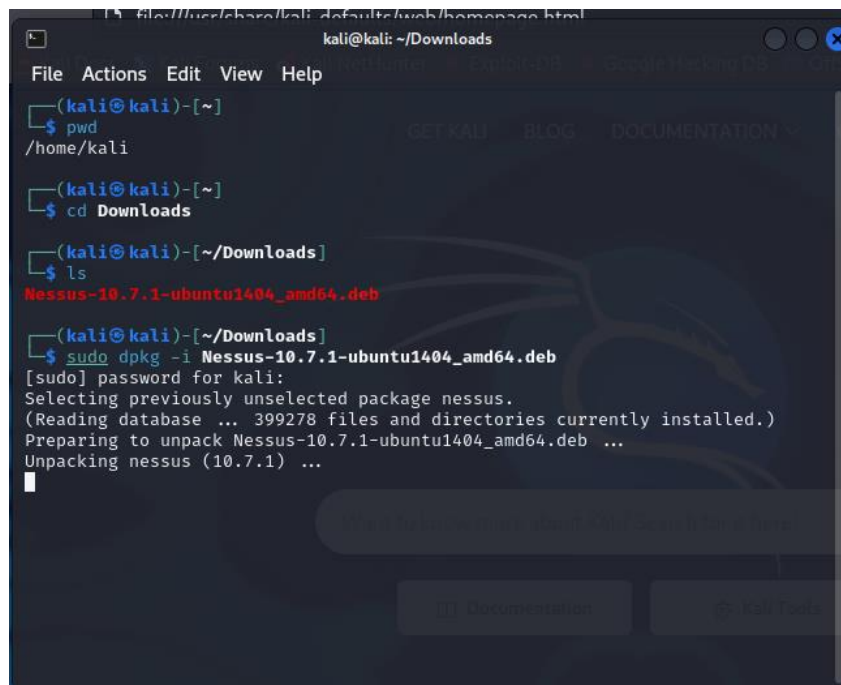


Figura F.1: Máquina Virtual de Kali Linux

Elaborado por: El investigador.

En la **Figura F.2** podemos observar la instalación de Nessus mediante la terminal de Kali con el comando preparación de la máquina con Kali Linux que nos sirve para el desarrollo de la investigación.



```
kali@kali: ~/Downloads
File Actions Edit View Help

(kali@kali)-[~]
$ pwd
/home/kali

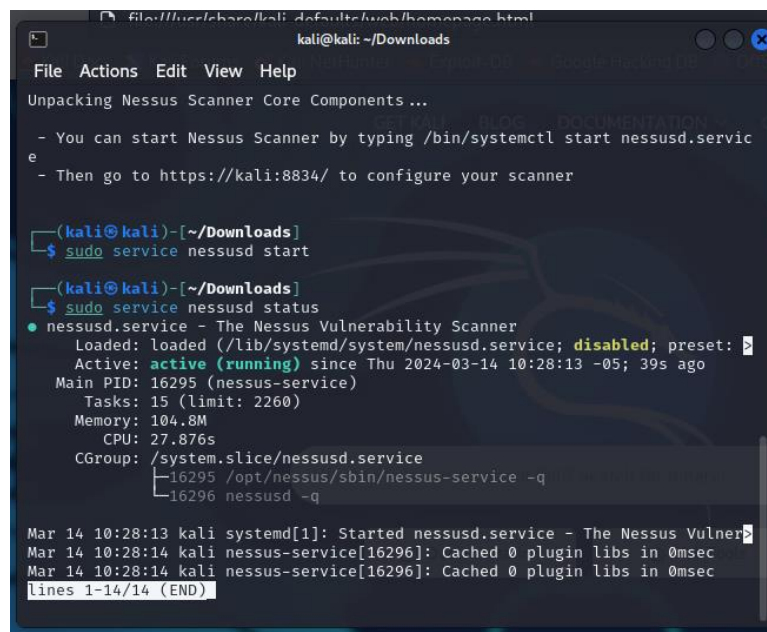
(kali@kali)-[~]
$ cd Downloads

(kali@kali)-[~/Downloads]
$ ls
Nessus-10.7.1-ubuntu1404_amd64.deb

(kali@kali)-[~/Downloads]
$ sudo dpkg -i Nessus-10.7.1-ubuntu1404_amd64.deb
[sudo] password for kali:
Selecting previously unselected package nessus.
(Reading database ... 399278 files and directories currently installed.)
Preparing to unpack Nessus-10.7.1-ubuntu1404_amd64.deb ...
Unpacking nessus (10.7.1) ...
```

Figura F.2: Instalación de Nessus
Elaborado por: El investigador.

En la **Figura F.3** podemos observar la habilitación del Servicio de Nessus en Kali.



```
kali@kali: ~/Downloads
File Actions Edit View Help

Unpacking Nessus Scanner Core Components ...

- You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
- Then go to https://kali:8834/ to configure your scanner

(kali@kali)-[~/Downloads]
$ sudo service nessusd start

(kali@kali)-[~/Downloads]
$ sudo service nessusd status
● nessusd.service - The Nessus Vulnerability Scanner
   Loaded: loaded (/lib/systemd/system/nessusd.service; disabled; preset:
   Active: active (running) since Thu 2024-03-14 10:28:13 -05; 39s ago
   Main PID: 16295 (nessus-service)
     Tasks: 15 (limit: 2260)
    Memory: 104.8M
       CPU: 27.876s
    CGroup: /system.slice/nessusd.service
           └─16295 /opt/nessus/sbin/nessus-service -q
             └─16296 nessusd -q

Mar 14 10:28:13 kali systemd[1]: Started nessusd.service - The Nessus Vulner
Mar 14 10:28:14 kali nessus-service[16296]: Cached 0 plugin libs in 0msec
Mar 14 10:28:14 kali nessus-service[16296]: Cached 0 plugin libs in 0msec
lines 1-14/14 (END)
```

Figura F.3: Levantar el Servicio de Nessus
Elaborado por: El investigador.

En la **Figura F.4** podemos observar como ingresamos a nuestra página de Nessus Essential y procedemos a registrarlos

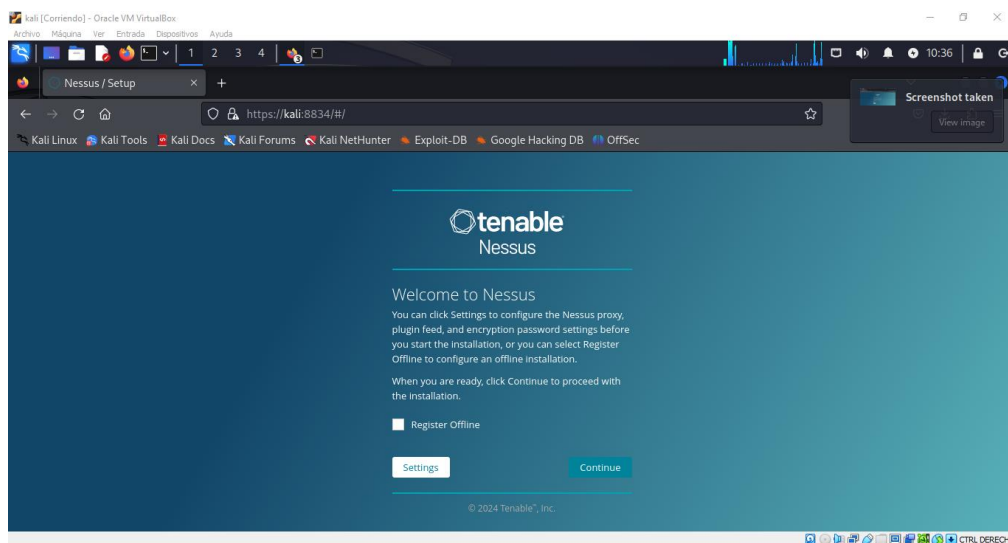


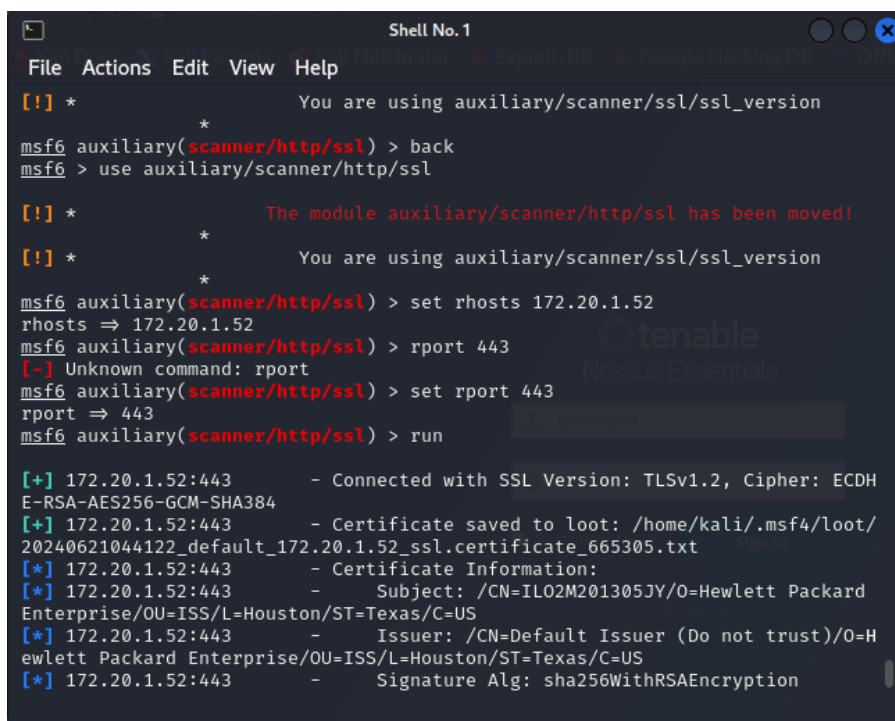
Figura F.4: Registro de Nessus Essential
Elaborado por: El investigador.

ANEXO G

Prueba de explotación de vulnerabilidades encontradas en los Servidores con el framework metasploit.

Para esta práctica se ejecuta en kali la herramienta metasploit y se importa la base que nos emite el nessus.

En la **Figura G.1** y **Figura G.2** escogemos el auxiliar que ayudó en la prueba de penetración, ponemos los valor de la ip del servidor, el puerto y ejecutamos.



```
Shell No. 1
File Actions Edit View Help
[!] * You are using auxiliary/scanner/ssl/ssl_version
*
msf6 auxiliary(scanner/http/ssl) > back
msf6 > use auxiliary/scanner/http/ssl
[!] * The module auxiliary/scanner/http/ssl has been moved!
*
[!] * You are using auxiliary/scanner/ssl/ssl_version
*
msf6 auxiliary(scanner/http/ssl) > set rhosts 172.20.1.52
rhosts => 172.20.1.52
msf6 auxiliary(scanner/http/ssl) > rport 443
[-] Unknown command: rport
msf6 auxiliary(scanner/http/ssl) > set rport 443
rport => 443
msf6 auxiliary(scanner/http/ssl) > run

[+] 172.20.1.52:443 - Connected with SSL Version: TLSv1.2, Cipher: ECDH
E-RSA-AES256-GCM-SHA384
[+] 172.20.1.52:443 - Certificate saved to loot: /home/kali/.msf4/loot/
20240621044122_default_172.20.1.52_ssl.certificate_665305.txt
[*] 172.20.1.52:443 - Certificate Information:
[*] 172.20.1.52:443 - Subject: /CN=ILO2M201305JY/O=Hewlett Packard
Enterprise/OU=ISS/L=Houston/ST=Texas/C=US
[*] 172.20.1.52:443 - Issuer: /CN=Default Issuer (Do not trust)/O=H
ewlett Packard Enterprise/OU=ISS/L=Houston/ST=Texas/C=US
[*] 172.20.1.52:443 - Signature Alg: sha256WithRSAEncryption
```

Figura G.1: Explotación SSL

Elaborado por: El investigador.

```

Shell No.1
File Actions Edit View Help
.. possible self signed certificate
[*] 172.20.1.52:443 - Has common name IL02M201305JY
[+] 172.20.1.52:443 - Connected with SSL Version: TLSv1.2, Cipher: DHE-
RSA-AES256-GCM-SHA384
[+] 172.20.1.52:443 - Connected with SSL Version: TLSv1.2, Cipher: ECDH
E-RSA-AES128-GCM-SHA256
[+] 172.20.1.52:443 - Connected with SSL Version: TLSv1.2, Cipher: DHE-
RSA-AES128-GCM-SHA256
[+] 172.20.1.52:443 - Connected with SSL Version: TLSv1.2, Cipher: ECDH
E-RSA-AES256-SHA384
[+] 172.20.1.52:443 - Connected with SSL Version: TLSv1.2, Cipher: DHE-
RSA-AES256-SHA256
[+] 172.20.1.52:443 - Connected with SSL Version: TLSv1.2, Cipher: ECDH
E-RSA-AES128-SHA256
[+] 172.20.1.52:443 - Connected with SSL Version: TLSv1.2, Cipher: DHE-
RSA-AES128-SHA256
[+] 172.20.1.52:443 - Connected with SSL Version: TLSv1.2, Cipher: AES2
56-GCM-SHA384
[+] 172.20.1.52:443 - Connected with SSL Version: TLSv1.2, Cipher: AES1
28-GCM-SHA256
[+] 172.20.1.52:443 - Connected with SSL Version: TLSv1.2, Cipher: AES2
56-SHA256
[+] 172.20.1.52:443 - Connected with SSL Version: TLSv1.2, Cipher: AES1
28-SHA256
[+] 172.20.1.52:443 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/ssl) >

```

Figura G.2: Explotación SSL
Elaborado por: El investigador.

En la **Figura G.3** y **Figura G.4** ejecutamos en Kali el siguiente comando `openssl s_client -connect ip -showcerts`, que permite visualizar los certificados del servidor.

```

kali@kali: ~
File Actions Edit View Help
.. possible self signed certificate
(kali@kali)-[~]
$ openssl s_client -connect 172.20.1.52:443 -showcerts
CONNECTED(00000003)
Can't use SSL_get_servername
depth=0 CN = IL02M201305JY, O = Hewlett Packard Enterprise, OU = ISS, L = Hou
ston, ST = Texas, C = US
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 CN = IL02M201305JY, O = Hewlett Packard Enterprise, OU = ISS, L = Hou
ston, ST = Texas, C = US
verify error:num=21:unable to verify the first certificate
verify return:1
depth=0 CN = IL02M201305JY, O = Hewlett Packard Enterprise, OU = ISS, L = Hou
ston, ST = Texas, C = US
verify return:1
---
Certificate chain
 0 s:CN = IL02M201305JY, O = Hewlett Packard Enterprise, OU = ISS, L = Housto
n, ST = Texas, C = US
  i:CN = Default Issuer (Do not trust), O = Hewlett Packard Enterprise, OU =
ISS, L = Houston, ST = Texas, C = US
  a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA256
  v:NotBefore: Mar 26 10:36:03 2020 GMT; NotAfter: Mar 26 10:36:03 2035 GMT
---BEGIN CERTIFICATE---
MIIDuzCCAqOgAwIBAgIIPk0CR2YsVYYwDQYJKoZIhvcNAQELBQAwYoxJjAkBgNV
BAMMHURLZmF1bHQgSXNzdWVYIChEbyBub3R1b3QgHJ1c3QpMSMwIQYDVQQKDBpIZXds

```

Figura G.3: Consulta de Certificados
Elaborado por: El investigador.

```
kali@kali: ~
File Actions Edit View Help
-----END CERTIFICATE-----
Server certificate
subject=CN = IL02M201305JY, O = Hewlett Packard Enterprise, OU = ISS, L = Houston, ST = Texas, C = US
issuer=CN = Default Issuer (Do not trust), O = Hewlett Packard Enterprise, OU = ISS, L = Houston, ST = Texas, C = US
No client certificate CA names sent
Peer signing digest: SHA512
Peer signature type: RSA
Server Temp Key: ECDH, secp384r1, 384 bits
SSL handshake has read 1498 bytes and written 581 bytes
Verification error: unable to verify the first certificate
New, TLSv1.2, Cipher is ECDHE-RSA-AES256-GCM-SHA384
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol : TLSv1.2
    Cipher   : ECDHE-RSA-AES256-GCM-SHA384
    Session-ID: 031A4E1DC14E0B3900EE9E088ED76D43B0D5505AD63BCF00E478F13DF59BB
58A
```

Figura G.4: Consulta de Certificados
Elaborado por: El investigador.

En la **Figura G.5** escogemos el auxiliar para explotar la vulnerabilidad bluekeep que se encontró en el servidor Sif Principa.

```
Shell No. 1
File Actions Edit View Help
0 auxiliary/scanner/rdp/cve_2019_0708_bluekeep 2019-05-14 normal
Yes CVE-2019-0708 BlueKeep Microsoft Remote Desktop RCE Check
1 exploit/windows/rdp/cve_2019_0708_bluekeep_rce 2019-05-14 manual
Yes CVE-2019-0708 BlueKeep RDP Remote Windows Kernel Use After Free

Interact with a module by name or index. For example info 1, use 1 or use exploit/windows/rdp/cve_2019_0708_bluekeep_rce

msf6 > use auxiliary/scanner/rdp/cve_2019_0708_bluekeep
msf6 auxiliary(scanner/rdp/cve_2019_0708_bluekeep) > set rhosts 172.20.1.55
rhosts => 172.20.1.55
msf6 auxiliary(scanner/rdp/cve_2019_0708_bluekeep) > set rport 3389
rport => 3389
msf6 auxiliary(scanner/rdp/cve_2019_0708_bluekeep) > run

[+] 172.20.1.55:3389 - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
[*] 172.20.1.55:3389 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/rdp/cve_2019_0708_bluekeep) > run

[+] 172.20.1.55:3389 - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
[*] 172.20.1.55:3389 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/rdp/cve_2019_0708_bluekeep) >
```

Figura G.5: Vulnerabilidad BlueKeep
Elaborado por: El investigador.

En la **Figura G.6** a la **Figura G.8** se visualiza el servidor y el kali en el que se debe ejecutar el archivo python que tenemos listo para la explotación o ataque de DoS al servidor.

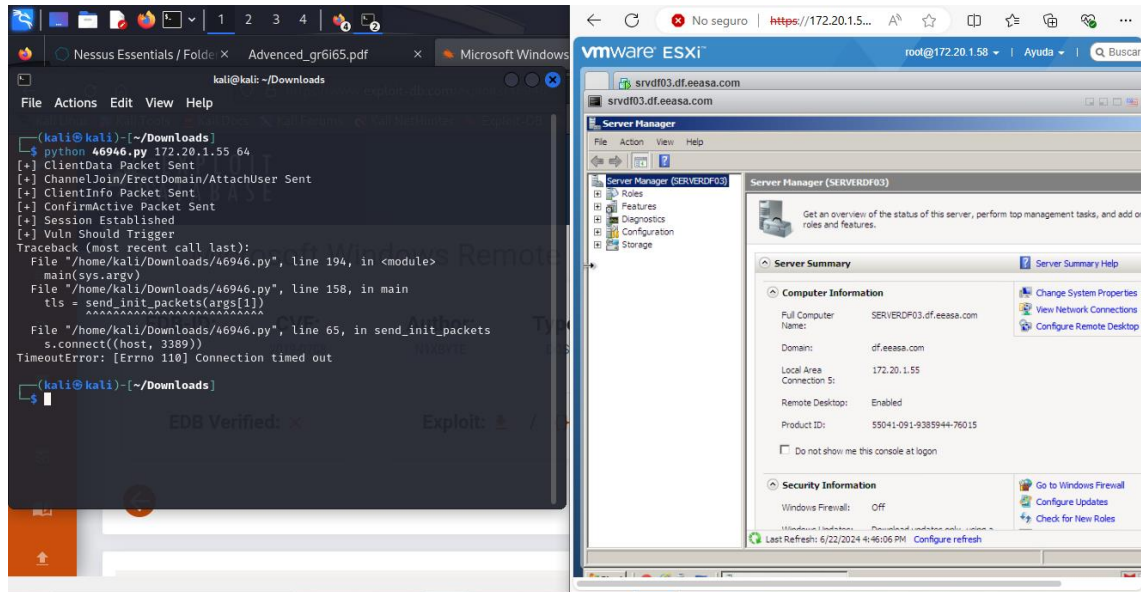


Figura G.6: Servidor Sif Principal
Elaborado por: El investigador.

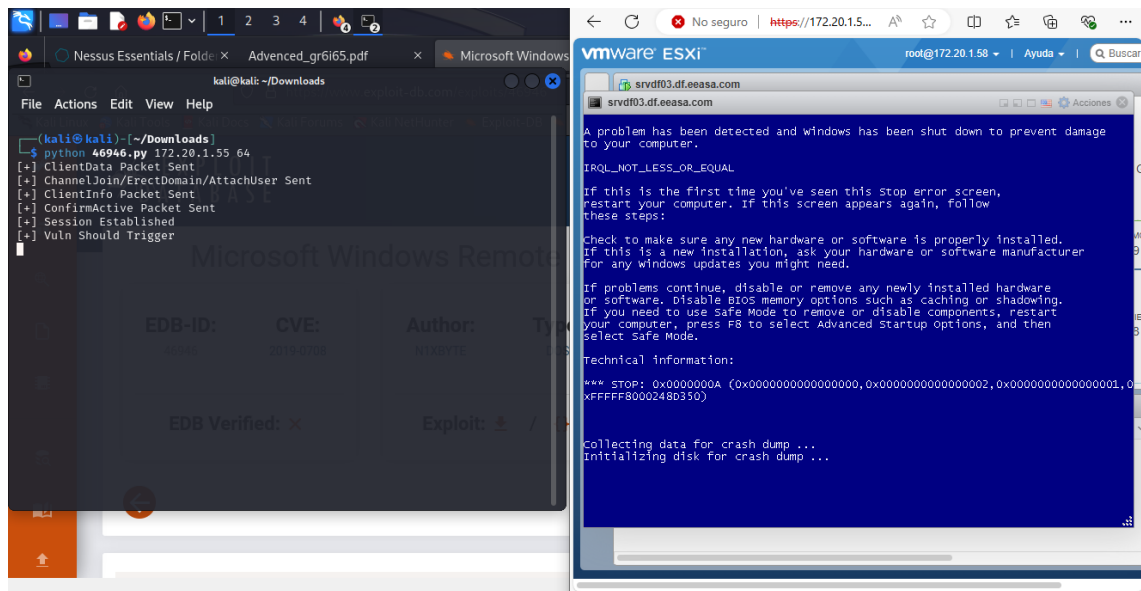


Figura G.7: Ejecución python al servidor, servidor en estado error
Elaborado por: El investigador.

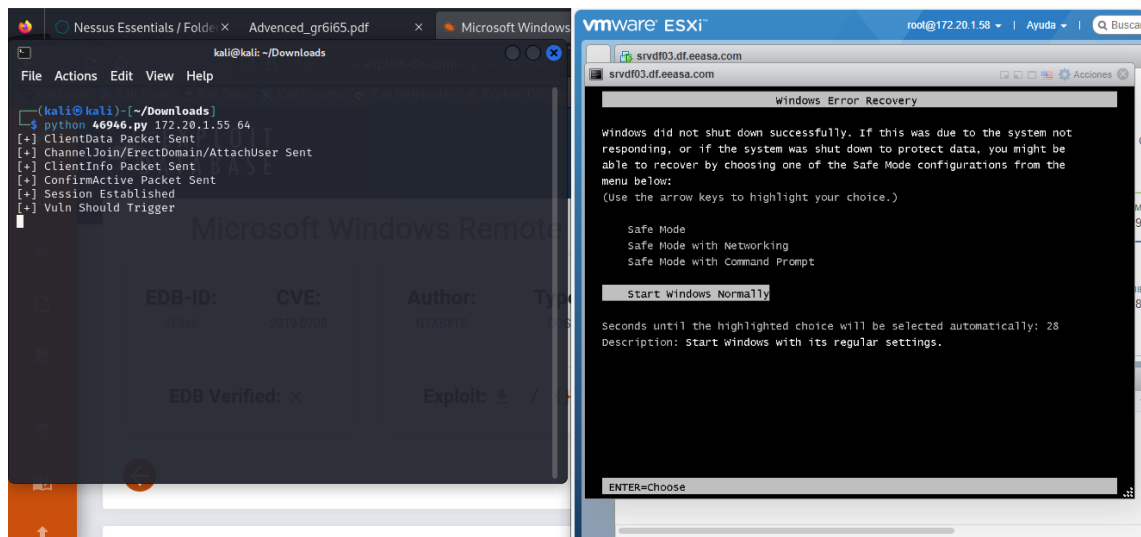


Figura G.8: Reinicio Servidor
Elaborado por: El investigador.