UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS

TEMA:

AUDITORÍA DE LA SEGURIDAD INFORMÁTICA SIGUIENDO LA METODOLOGÍA OPEN SOURCE SECURITY TESTING METHODOLOGY MANUAL (OSSTMM) PARA LA EMPRESA MEGAPROFER S.A.

Trabajo de Graduación. Modalidad: Proyecto de Investigación, presentado previo la obtención del título de Ingeniero en Sistemas Computacionales e Informáticos

LÍNEA DE INVESTIGACIÓN: Hardware y Redes

AUTOR: Allaica Caranqui Joel Franklin
TUTOR: Ing. David Omar Guevara Aulestia, Mg

Ambato - Ecuador
Agosto, 2020

APROBACIÓN DEL TUTOR

En mi calidad de Tutor del Trabajo de Investigación sobre el Tema: "AUDITORÍA DE LA SEGURIDAD INFORMÁTICA SIGUIENDO LA METODOLOGÍA OPEN SOURCE SECURITY TESTING METHODOLOGY MANUAL (OSSTMM) PARA LA EMPRESA MEGAPROFER S.A.", desarrollado bajo la modalidad Proyecto de Investigación por el señor Joel Franklin Allaica Caranqui, 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 el estudiante ha sido tutorado durante todo el desarrollo del trabajo hasta su conclusión, de acuerdo a lo dispuesto en el Artículo 15 del 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 2020.

Firmado electrónicamente por:
DAVID OMAR GUEVARA AULESTIA

Ing. David Omar Guevara Aulestia, Mg

EL TUTOR

AUTORÍA

El presente Proyecto de Investigación titulado: "AUDITORÍA DE LA SEGURIDAD INFORMÁTICA SIGUIENDO LA METODOLOGÍA OPEN SOURCE SECURITY TESTING METHODOLOGY MANUAL (OSSTMM) PARA LA EMPRESA MEGAPROFER 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 2020.

Joel Franklin Allaica Caranqui

CC: 1804450045

APROBACIÓN DEL TRIBUNAL DE GRADO

En calidad de par calificador del Informe Final del Trabajo de Titulación presentado por el señor Joel Franklin Allaica Caranqui, 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, "AUDITORÍA DE LA SEGURIDAD INFORMÁTICA SIGUIENDO LA METODOLOGÍA OPEN SOURCE SECURITY TESTING METHODOLOGY MANUAL (OSSTMM) PARA LA EMPRESA MEGAPROFER S.A.", nos permitimos informar que el trabajo ha 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 del Tribunal.

Ambato, agosto 2020.

Firmado electrónicamente por:
ELSA PILAR URRUTIA

Ing. Pilar Urrutia, Mg.

PRESIDENTE DEL TRIBUNAL

Firmado electrónicamente por:
FRANKLIN OSWALDO MAYORGA MAYORGA

Ing. Franklin Mayorga
DOCENTE CALIFICADOR

Firmado electrónicamente por:
JULIO ENRIQUE BALAREZO LOPEZ

Dr. Julio Balarezo
DOCENTE CALIFICADOR

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 2020.

Joel Franklin Allaica Caranqui

CC: 1804450045

DEDICATORIA

El presente proyecto va dedicado a mis padres quienes soñaron conmigo y confiaron en mi, brindándome su apoyo incondicional en cada unos de los pasos que daba en camino hacia la meta profesional.

Joel Franklin Allaica Caranqui

AGRADECIMIENTO

Gracias a Dios por su amor incondicional, por darme la fuerza para no rendirme a pesar de los tropiezos; hoy me permite cumplir una meta más aquella que alguna vez parecía ser solo un sueño lejano.

A mis padres Pedro y Rosa quienes con su amor, trabajo y apoyo son un pilar fundamental en mi vida, un ejemplo a seguir en la lucha constante, valentía y superación. Mis hermanos María y Jonathan por llenar mis días de alegría por sus palabras que me han dado la fortaleza para seguir adelante.

A mi tutor del proyecto Ing. David Guevara, Mg, ha dedicado su valioso tiempo compartiendo sus conocimientos para que el presente trabajo de investigación pueda ser culminado.

Joel Franklin Allaica Caranqui

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN EJECUTIVO

El proyecto de investigación desarrollado a continuación tiene como objetivo ejecutar una Auditoría de la Seguridad Informática siguiendo la metodología Open Source Security Testing Methodology Manual (OSSTMM) para la empresa Megaprofer S.A. con el fin de determinar las posibles falencias o vulnerabilidades que puede tener la infraestructura de red y posterior explotación de las debilidades mediante el uso de las herramientas informáticas adecuadas.

Con esta auditoria se puede determinar los riesgos que tiene la empresa en lo referente a la red y activos informáticos, el nivel de acceso que podría tener una persona o un agente externo dentro de la empresa al pretender producir algún tipo de perjuicio en los servicios o equipos tecnológicos y, a su vez al intentar substraer datos sensibles; tomando como fundamento los resultados conseguidos, para así plantear medidas y recomendaciones apropiadas que puedan garantizar la integridad, confidencialidad y disponibilidad de la información, así como posibles soluciones para mitigar a los inconvenientes encontrados.

Para llegar al propósito planteado en el tema, se utiliza el Manual de la Metodología Abierta de Testeo de Seguridad(OSSTMM por sus siglas en ingles), la metodológica nos permite efectuar una planificación y una posterior comprobación de manera precisa a cerca de la seguridad con la que se cuenta a nivel operativo en base a las pruebas ejecutadas en referente a los factores humanos, físicos, inalámbricos, telecomunicación, y redes de datos.

ABSTRACT

The research project developed below aims to carry out a Computer Security Audit following the methodology Open Source Security Testing Methodology Manual (OSSTMM) for the company Megaprofer S.A. in order to determine possible failures or vulnerabilities that they may have the infrastructure of network and the subsequent exploitation of weaknesses by using the appropriate computer tools.

With this audit it is possible to determine the risks that the company has in relation to the network and computer assets, the level of access that an external person or agent could have within the company when trying to produce some type of damage in the services or technological equipments and in turn when trying to subtract sensitive data; taked of the base on the results achieved, in order to propose appropriate measures and recommendations that can guarantee the integrity, confidentiality and availability of the information, as well as possible solutions to mitigate the inconvenient encountered.

To reach the purpose set out in the topic, the Open Source Security Testing Methodology Manual (OSSTMM), the methodology allows us to carry out a planning and subsequent verification in a precise way about security with the that is counted at the operational level based on the tests carried out in relation to human, physical, wireless, telecommunication, and data network factors.

CAPÍTULO I

MARCO TEÓRICO

1.1. Antecedentes Investigativos

Como antecedentes investigativos se puede mencionar. El trabajo presentado por Nuela Guananga Byron Danilo de título "Auditoría De La Seguridad Informática Para El Honorable Gobierno Provincial De Tungurahua Mediante La Metodología Open Source Security Testing Methodology Manual" (2015). Menciona que la explotación es conveniente realizar en un entorno virtual: "... La explotación de vulnerabilidades se la realiza en un entorno virtual similar al real, esto con el objetivo de no ocasionar daños ni perjuicios a los equipos reales, esto puede servir como caso práctico de tal forma que el lector sea capaz de aplicar y comprobar la utilidad de las herramientas descritas..."[1].

En el trabajo presentado por Ángel Rojas Carriel y Fernando Castro Pesantes de título "Análisis Y Detección De Vulnerabilidades En Los Servidores Públicos Del Centro De Cómputo De La Empresa Intermediara De Ventas Utilizando La Metodología Internacional OSSTMM". Concluye la importancia de realizar una fase intrusión. "... La fase de intrusión permitirá analizar la vulnerabilidad en los sistemas para tomar control y privilegios de las victimas suprimiendo los falso positivos"[2].

En el trabajo presentado por Cristian L. Bracho, Fabian G. Cuzme de título "Auditoría de seguridad informática siguiendo la metodología OSSTMMv3: caso de estudio". Concluye las ventajas de aplicar la metodología al momento de manejar vulnerabilidades de realizar una fase intrusión. "... El hecho de que la metodología separe en canales individuales las pruebas que se deben realizar es muy beneficioso, no solo para el auditor; sino también para la institución ya que esto permite conocer a ciencia cierta en que parte de la infraestructura del sistema de seguridad de la red se encuentra un mayor número de vulnerabilidades y así poder aplicar los métodos correctivos necesarios en el canal que lo necesite..."[3].

1.2. Objetivos

1.2.1. General

Realizar una Auditoría de Seguridad Informática utilizando la Metodología Open Source Security Testing Methodology Manual (OSSTMM) para la empresa Megaprofer S.A.

1.2.2. Específicos

- Analizar la metodología OSSTMM para determinar las mejores prácticas relacionadas a reducir vulnerabilidades y errores de usuario final.
- Realizar un análisis de los mecanismos de defensa internos y externos de Seguridad Informática utilizada en la empresa Megaprofer S.A.
- Elaborar Políticas de Contingencia de Seguridad Informática que ayuden a mejorar la integridad, confidencialidad y disponibilidad de la información en base a las vulnerabilidades detectadas.

1.3. Fundamentación teórica

Auditoría
Es la revisión independiente de alguna o algunas actividades, funciones específicas, resultados u operaciones de una entidad administrativa, realizada por un profesional de la auditoría, con el propósito de evaluar su correcta realización y, con base en ese análisis, poder emitir una opinión autorizada sobre la racionabilidad de sus resultados y el cumplimiento de sus operaciones[4].

Auditoría Informática
Es el conjunto de técnicas, actividades y procedimientos, destinados a analizar, evaluar, verifica y recomendar en asuntos relativos a la planificación, control, eficacia, seguridad y adecuación del servicio informático en la empresa, por lo que comprende un examen metódico, puntual y discontinuo del servicio informático, con vistas a mejorar en[5]:

- Rentabilidad.
- Seguridad.
- Eficacia.

Auditoría de la Seguridad
Es un servicio que ayuda a mejorar la seguridad de los sistemas informáticos, prevenir fugas de información y garantizar su disponibilidad[6].

Auditoría De Seguridad Informática
Una auditoría de seguridad informática o auditoría de seguridad de sistemas de información, es el estudio que comprende el análisis y gestión de los sistemas informáticos, realizado por una persona o grupo de personas, denominados auditores, que pueden ser del propio personal o ajeno a la organización; para identificar y posteriormente corregir las diversas vulnerabilidades que se pudieran presentar en una revisión exhaustiva de las estaciones de trabajo, redes de comunicaciones o servidores[5].

Seguridad
Resguardo de los haberes personales y establecimientos, a través de reglas de confianza que limitan y coordinan el flujo de personas y equipos.

Seguridad Informática
Por seguridad informática se entiende al conjunto de políticas, reglas, estándares, métodos y protocolos que se utilizan para la protección de la infraestructura de computadoras y toda la información contenida o administrada por ella[7].
Es el conjunto de procedimientos, estrategias y herramientas que permitan garantizar la integridad, la disponibilidad y la confidencialidad de la información.

Políticas

Las políticas son instrucciones gerenciales que trazan una dirección predeterminada o describen la manera de manejar un problema o situación.

Se puede definir también como planteamientos de alto nivel que transmiten a los trabajadores la orientación que necesitan para tomar decisiones presentes y futuras.

Otro concepto que se puede dar, son requisitos generalizados que deben ser escritos en papel y comunicados a ciertos grupos de personas dentro, y en algunos casos fuera, de la organización. Las políticas también pueden considerarse como reglas de negocio[8].

Contingencia

Es la característica respecto a la posibilidad de que algo puede o no suceder, generalmente viene de forma imprevista, con mayores o menores posibilidades de ocurrir.

Plan de contingencia

Es un tipo documento que las empresas establecen para saber cómo actuar ante un posible imprevisto. El plan de contingencia establece: los pasos que debemos seguir, las actividades a realizar y los recursos necesarios, con el objetivo principal de disminuir los daños que se puedan generar[9].

OSSTM (Manual de la Metodología Abierta de Testeo de Seguridad)

Es una metodología realizada por INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES (ISECOM), metodología que propone un proceso de evaluación de debilidades de una serie de áreas que refleja de manera fiel los niveles de seguridad presentes en la infraestructura que va a ser auditada, formada por 6 ítems los cuales comprenden todo el sistema actual, estos ítems son[10]:

- Seguridad de la Información.
- Seguridad de los Procesos.
- Seguridad en las tecnologías de Internet.
- Seguridad en las comunicaciones.
- Seguridad inalámbrica.
- Seguridad Física.

Vulnerabilidades
Consistirá en cualquier debilidad o fallo que puede explotarse para causar pérdida o daño al sistema[11]. De esta manera, el punto más débil de seguridad de un sistema se convierte en el punto mas vulnerable de la misma, estas pueden tener diferentes origines ya sean debilidades en el diseño, programación, configuración, políticas o procedimientos, formas de uso, entre otras.

Ataque
Es cualquier acción que explota una vulnerabilidad con el fin de causar algún tipo de daño a la seguridad de un sistema informático.

Pentest
Una prueba de penetración es un ataque a un sistema software o hardware con el objetivo de encontrar vulnerabilidades. El ataque implica un análisis activo de cualquier debilidad potencial, configuraciones deficientes o inadecuadas, tanto de hardware como de software, o deficiencias operativas en las medidas de seguridad. Este análisis se realiza desde la posición de un atacante potencial y puede implicar la explotación activa de fallos de seguridad. Tras la realización del ataque se presentará una evaluación de seguridad del sistema, indicando todos los problemas de seguridad detectados junto con una propuesta de mitigación o una solución técnica. La intención de una prueba de penetración es determinar la viabilidad de un ataque y el impacto en el negocio de un ataque exitoso[12].

Hacking Ético.- El propósito de esto es descubrir cuáles son los errores que se cometen en el trato con las personas en cuanto a divulgación de información supuestamente inofensiva y agentes externos a través de los medios de comunicación o en persona, es decir, desde el momento en que se la recibe en la empresa[7].

Política de seguridad.- Recoge las directrices y objetivos de una organización con respecto a la seguridad de la información. Forma parte de su política general y, por tanto, ha de ser aprobado por la dirección[13].

El objetivo principal de la redacción de una política de seguridad es la de concienciar a todo el personal de la organización, y en particular al involucrado directamente con el sistema de la información, en la necesidad de conocer qué principios rigen la seguridad de la entidad y cuáles son las normas para conseguir los objetivos de la seguridad planificados. Por tanto la política de seguridad deberá

redactarse de forma que pueda ser comprendida por todo el personal de una organización.
No todas las políticas de seguridad son iguales. El contenido depende de la realidad y de las necesidades de la organización para la que se elabora.

Una política de seguridad contendrá los objetivos de la empresa en materia de seguridad del sistema de información, generalmente englobados en cuatro grupos:

- Identificar las necesidades de seguridad y los riegos que amenazan al sistema de información, así como evaluar los impactos ante un eventual ataque.
- Relacionar todas las medidas de seguridad que deben implementarse para afrontar los riesgos de cada activo o grupo de activos.
- Proporcionar una perspectiva general de las reglas y los procedimientos que deben aplicarse para afrontar los riesgos identificados en los diferentes departamentos de la organización.
- Detectar toda as vulnerabilidades del sistema de información y controlar los fallos que se producen en los activos, incluidas las aplicaciones instaladas.
- Definir un plan de contingencias.

CAPÍTULO II

METODOLOGÍA

2.1. Materiales

- Entrevista semiestructurada
- Encuesta Web
- Observación
- Registros de información

2.2. Modalidad Básica de la investigación

Investigación de campo
La modalidad que se utiliza en esta investigación es de campo, debido a que es necesario trasladarse y realizar la investigación dentro del Departamento de Sistemas de la empresa Megaprofer S.A, de la ciudad de Ambato.

Modalidad Bibliográfica
Se basa en la información acumulada de documentos. Se investigan libros, manuales, artículos, revistas que proporcionen información relevante relacionada con el tema de investigación.

Enfoque
En la presente investigación se utilizara el enfoque mixto, ya que es se basa en datos cualitativos y cuantitativos

2.3. Población y muestra

La población considerada para la presente investigación son 40 personas que forman parte del personal administrativo de la empresa.

Tabla 2.1: Población

Departamento	**N° Empleados**	**%**
Sistemas	2	5
Contabilidad	6	15
Crédito y Cobranza	6	15
Call Center	10	20
Compras	5	13
Pos Ventas	4	10
Talento Humano	5	13
Logística	4	10
TOTAL	40	100

2.4. Recolección de información

Al realizar esta etapa del proyecto se necesitara información precisa y clara por ello para la recopilación de datos a nivel interno se emplea dos métodos, la entrevista y la encuesta.

Entrevista dirigida al Jefe del departamento de sistemas
A través de la entrevista aplicada al Jefe de TICs, seguidamente se presenta cada una de las preguntas con su respectiva respuesta.
Nombre de entrevistado: Ing. Jorge Luis Valencia Mogollon
Fecha: 20/11/2019
Cargo: Jefe de **TICs**
Lugar: Oficina de la empresa

1. ¿Se cuenta con un inventario de todos los equipos que integran la red informática?
Responde.- Sí, se cuenta con un inventario y se lo actualiza constantemente.

2. ¿Se tienen equipos dedicados al monitoreo del tráfico y actividades de la red?
Responde.- Sí, se hace un monitoreo de los servidores en producción tanto de los físicos como en los servidores que se tiene en la nube.

3. ¿Qué sistemas tiene bajo su cargo o responsabilidad?
Responde.- Actualmente los sistemas que tengo a mi cargo son: Erp-Atix, Easy Seguridad, Sistemas De Gestión De Almacenes (WMS), Digitalización, Genera-

Nomina, Qlik-Sense, Control de Asistencia.

4. ¿Se posee bitácoras de fallos o ataques detectados en los servidores?
Responde.- Sí, se posee la bitácora para evitar posibles fallos y una pronta solución los midmos; hacen hace cinco meses sufrimos el último ataque a uno de nuestros servidores, el ataque fue al servidor de correo electrónico Zimbra este servicio tenía varias vulnerabilidades en lo referente a las configuraciones realizadas ya no eras las adecuadas por lo cual decidimos migrar a Microsoft Cloud.

5. ¿Se identifican los tipos de usuarios, sus responsabilidades, permisos y restricciones?
Responde.- Sí, existe un control de perfil de acceso para cada uno de los colaboradores en base a los cargos que desempeñan.

6. ¿Se tienen un sistema de seguridad para evitar que se sustraiga equipos informáticos de la institución?
Responde.- Actualmente no se cuenta con dicho sistema.

7 ¿Se cuenta con Políticas de Seguridad Informática?
Responde.- Sí, se cuenta con políticas las mismas que son aprobadas por la normativa Business Alliance for Secure Commerce (BASC).

8. ¿Se concientiza a los usuarios mediante charlas o reuniones a prevenirlos "ataques informáticos"?
Responde.- Al momento de ingresar al colaborador en la inducción se explican las políticas, así como los posibles ataques informáticos y la manera de cómo evitarlos además en un periodo de cada 3 meses, a ciertos colaboradores se les realiza una auditoria con el fin de verificar el cumplimiento de las políticas y concientizar sobre el uso adecuado de las herramientas informáticas.

9. ¿Se tienen instalados programas antivirus en cada equipo con sus respectivas actualizaciones?
Responde.- Sí, tenemos un servidor de antivirus ESET y desplegamos clientes en cada uno de los equipos.

10. ¿El sistema operativo que se maneja se revisa y actualiza el software instalado frecuentemente?

Responde.- Sí, tenemos una política que se encarga de la validación y la ejecución de las actualizaciones, la misma se encuentra configurada en el Active Directory (AD).

11. ¿Con que frecuencia se pide a los usuarios que cambien de contraseña?
Responde.- Cada 90 días.

12. ¿Se realiza periódicamente una copia de seguridad de los datos de empresa?
Responde.- La información está en la nube y se cuenta con un contrato con el Partner de Microsoft y de los servidores sacamos backups diarios incremental semanal.

13 ¿Están los sitios web de la empresa protegidos?
Responde.- Cada uno de los sitios tiene Secure Sockets Layer (SSL).

14 ¿Se cuenta con un programa o dispositivo proxy?
Responde.- No

15 ¿Se cuenta con un programa o dispositivo firewall?
Responde.- Sí, se cuenta con FORTIGATE en el Data Center de Telefónica.
Recopilada la información y realizado el procesamiento correspondiente tomando en cuenta en primer lugar aquellos que representen un mayor riesgo dentro de la empresa se procede al análisis.

Encuesta a los colaboradores de la empresa

Se aplican preguntas de Seguridad Informática Colaboradores acerca del uso básico de las distintas herramientas y aplicativos tecnológicos a 40 profesionales que pertenecen la empresa Megaprofer S.A

Fecha: 20/11/2019

1 ¿Se cuentan con algún tipo de control de entradas y salidas del personal a la Empresa?

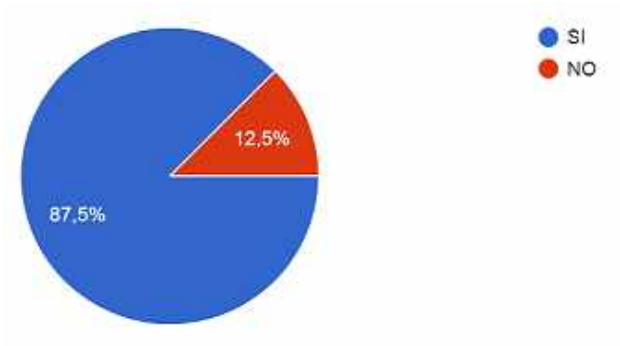


Figura 2.1: Pregunta: ¿Se cuentan con algún tipo de control de entradas y salidas del personal a la Empresa?
Desarrollado por: Joel F. Allaica C.

Análisis e Interpretación: El 87,5 % de los encuestados responde que que si cuenta con un control de entradas y salidas del personal mediante el personal de seguridad que se encuentra en la puerta de ingreso que se encarga de verifica la credencial de cada colaborador; un reloj biométrico, el cual controla las entradas y salidas del personal, cámaras de seguridad, ademas se maneja un control de salida de equipos/materiales. Este tipo de controles es provechoso para la empresa la cual puede prevenir la robo de equipos o algún bien de cualquiera de los departamentos.

2. Al recibir un correo desconocido. ¿Cuál es la medida que toma?

Figura 2.2: Pregunta: Al recibir un correo desconocido. ¿Cuál es la medida que toma?
Desarrollado por: Joel F. Allaica C.

Análisis e Interpretación: El 50 % de los encuestados mencionan que la medida que toman es marca como spam y borrar, el 25 % lo abre y lo lee para ver de que se trata, el 17,5 % notifica al personal de TICs el 7,5 % no hace nada.

Las medidas que toman los colaboradores es bastante buena ya con esto evitan posibles infiltraciones de archivos maliciosos o usuarios no deseados.

3. Cuándo quiere consultar una página en Internet para obtener información acerca de su trabajo. ¿Tiene acceso a ella?

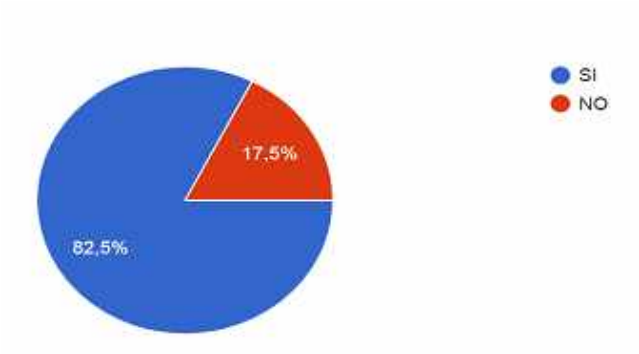


Figura 2.3: Pregunta: ¿Cuándo quiere consultar una página en Internet para obtener información acerca de su trabajo ¿tiene acceso a ella?
Desarrollado por: Joel F. Allaica C.

Análisis e Interpretación: El 82,5 % de los encuestados mencionan si tienen acceso a las paginas en Internet. El 17,5 indican que no tienen acceso, argumentando que tienen varias páginas bloqueadas a las cuales aluden que son indispensables para realizar consultas y creen que es conveniente tener un acceso sin restricciones.

4. ¿Sus usuarios y contraseñas de los distintos sistemas de Megaprofer principalmente la tiene guardada en?

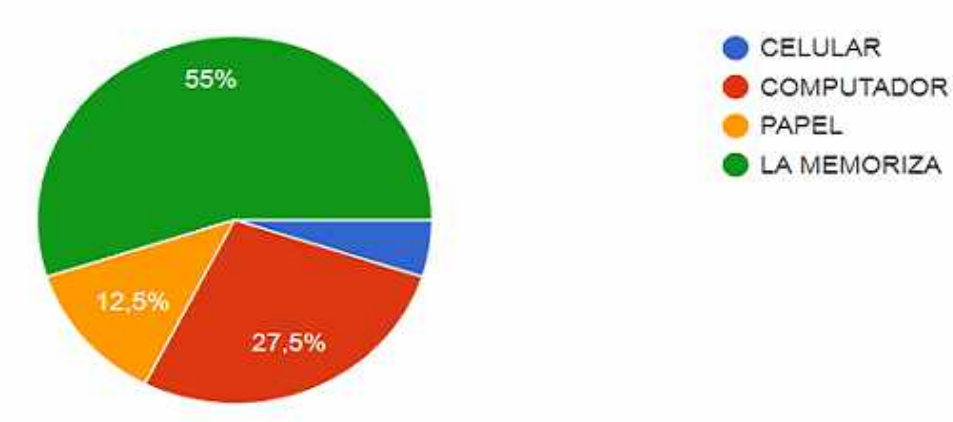


Figura 2.4: Pregunta: ¿Su usuarios y contraseñas de los distintos sistemas de Megaprofer principalmente la tiene guardada en?
Desarrollado por: Joel F. Allaica C.

Análisis e Interpretación: El 55 % de los encuestados mencionan que memorizan sus contraseñas, el 27,5 % la guardan en el computador, el 12,5 % la tienen guarda en papel, el 5 % en el celular. La mayor parte de los colaboradores la memoriza, siendo esta la mejor opción ante una ingeniera social.

5. ¿Cuál es el periodo promedio en el cual usted realiza cambio o renovación de su contraseña?

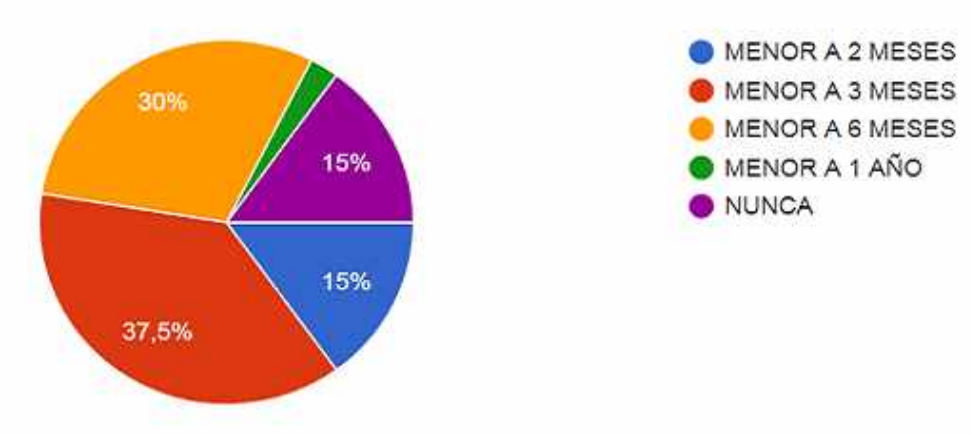


Figura 2.5: Pregunta 5:¿Cuál es el periodo promedio en el cual usted realiza cambio o renovación de su contraseña?
Desarrollado por: Joel F. Allaica C.

Análisis e Interpretación: El 37,5 % de los encuestados realiza el cambio de contraseña en un periodo menor a 3 meses, el 30 % lo cambia en el transcurso de 6 meses, el 15 % realiza el cambio en un rango de 2 meses, el otro 15 % nunca cambia sus contraseñas y el 2,5 % a lapso de un año. El 45,5 % menciona que cambia su contraseña en un periodo no mayor a 3 meses como el tiempo máximo, siendo esta una practica apropiado ante el robo de credenciales.

6. ¿Cual es la longitud aproximada de su contraseña?

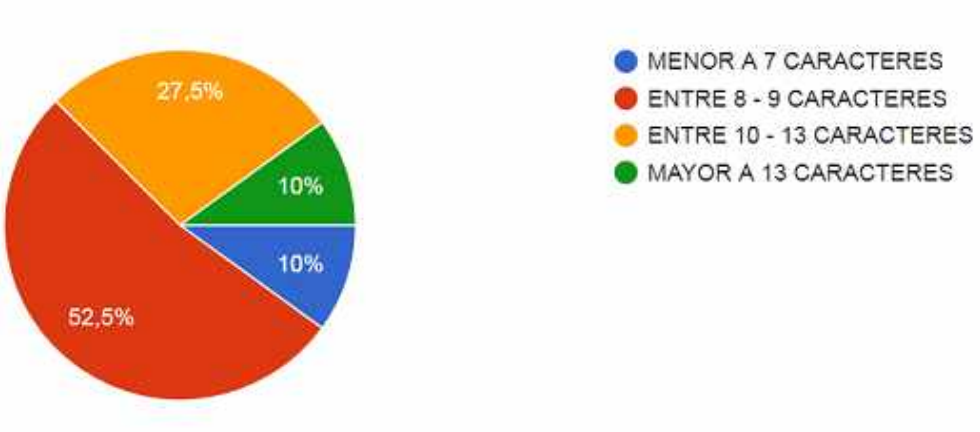


Figura 2.6: Pregunta: ¿Cual es la longitud aproximada de su contraseña?
Desarrollado por: Joel F. Allaica C.

Análisis e Interpretación: Del 52,5 % de los encuestados la contraseña está en el rango de 8 - 9 caracteres, 27,5 % entre 10 - 13 caracteres, 10 % mayor a 13 caracteres y 10 % menor a 7 caracteres. El 90 % de los colaboradores cuentan con contraseñas que cumplen uno de los parámetros para una contraseña segura así cumpliendo con las buenas practicas de seguridad.

7. ¿Sus contraseñas están compuestas de una combinación de: números, letras mayúsculas, minúsculas y caracteres especiales?

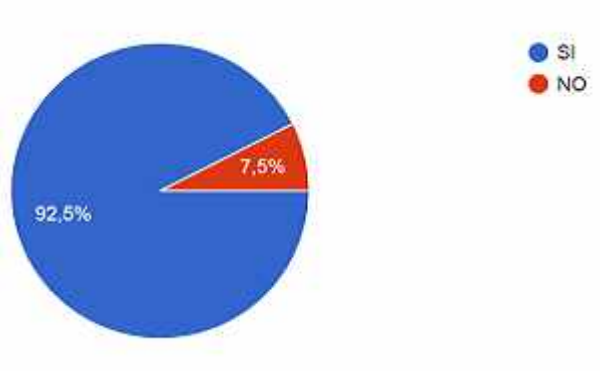


Figura 2.7: Pregunta: ¿Sus contraseñas están compuestas de una combinación de: números, letras mayúsculas, minúsculas y caracteres especiales?
Desarrollado por: Joel F. Allaica C.

Análisis e Interpretación: El 92,5 % de los colaboradores cumplen con todos los parámetros de una contraseña segura ayudando así a preservar la privacidad de los datos.

8. ¿Conoce usted el instructivo de uso de Herramientas Tecnológicas de Megaprofer?

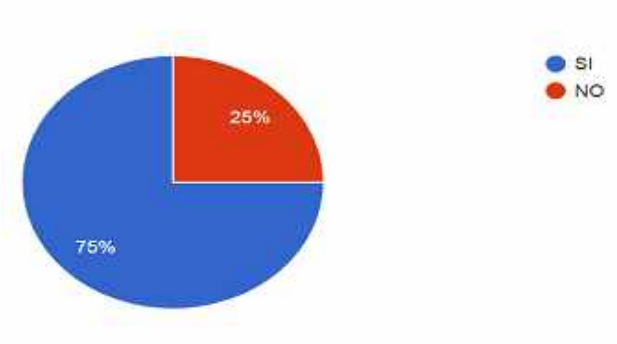


Figura 2.8: Pregunta: ¿Conoce usted el instructivo de uso de Herramientas Tecnológicas de Megaprofer?
Desarrollado por: Joel F. Allaica C.

Análisis e Interpretación: El 75 % de los encuestados mencionan que si conocen el instructivo de uso de herramientas tecnológicas de Megaprofer, el 25 % no las conoce. La mayor parte del personal tiene conocimiento de las políticas permitiendo así mantener un control de sus accesos en entornos laborales hiper-digitalizados y garantizar la seguridad de los datos de la empresa.

9. ¿Se ha dado a conocer a usted en la empresa sobre los "ataques informáticos", y las maneras de evitarlos?

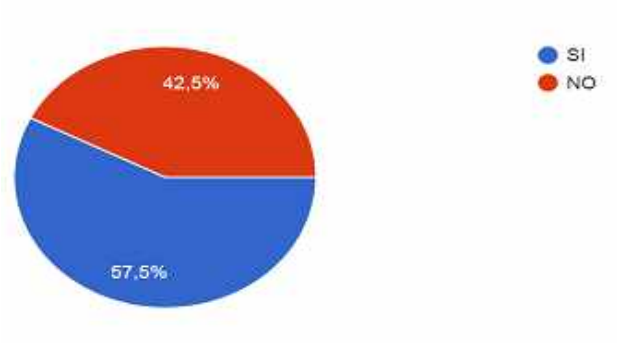


Figura 2.9: Pregunta: ¿Se ha dado a conocer a usted en la empresa sobre los "ataques informáticos", y las maneras de evitarlos?
Desarrollado por: Joel F. Allaica C.

Análisis e Interpretación: El 57,5 % de los encuestados mencionan que si se han dado a conocer sobre ataques informáticos y como evitarlos fomentando así las buenas prácticas y así protegiendo los activos empresariales.

10. ¿Con que frecuencia usted ha recibido notificaciones de las actualizaciones del antivirus?

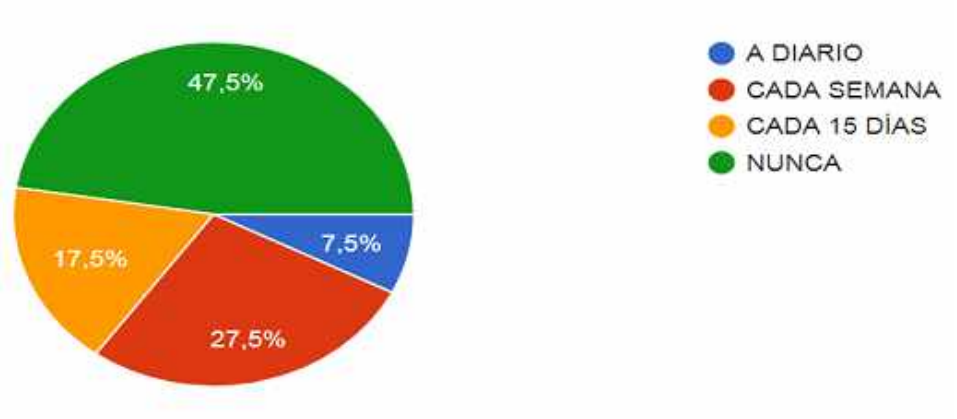


Figura 2.10: Pregunta: ¿Con que frecuencia usted ha recibido notificaciones de las actualizaciones del antivirus?
Desarrollado por: Joel F. Allaica C.

Análisis e Interpretación: El 47,5 % de los encuestados nunca reciben actualizaciones del antivirus, el 27,5 % lo recibe cada semana, el 17,5 % cada 15 días y el 7,5 % lo recibe a diario. Se puede identificar que existe algún tipo de inconveniente la configuración del antivirus instalado, medida que se debe corregir para cerrar la puerta a una posible infiltración.

11. ¿Normalmente en donde guarda usted la información?

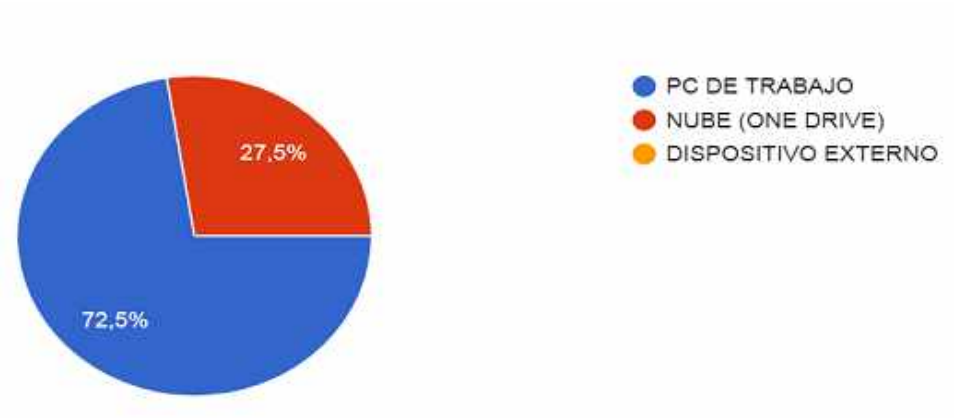


Figura 2.11: Pregunta: ¿Normalmente en donde guarda usted la información?
Desarrollado por: Joel F. Allaica C.

Análisis e Interpretación: El 72,5 % guarda la información en su pc, el 27,5 % en el One Drive y nadie lo almacena en un dispositivo externo. La mayor parte del personal mantiene su información únicamente en su pc generando así un riesgo

de pérdida de información relevante de la empresa.

12. ¿Se ha conectado remotamente a su equipo de la empresa mediante alguna de las siguientes herramientas?

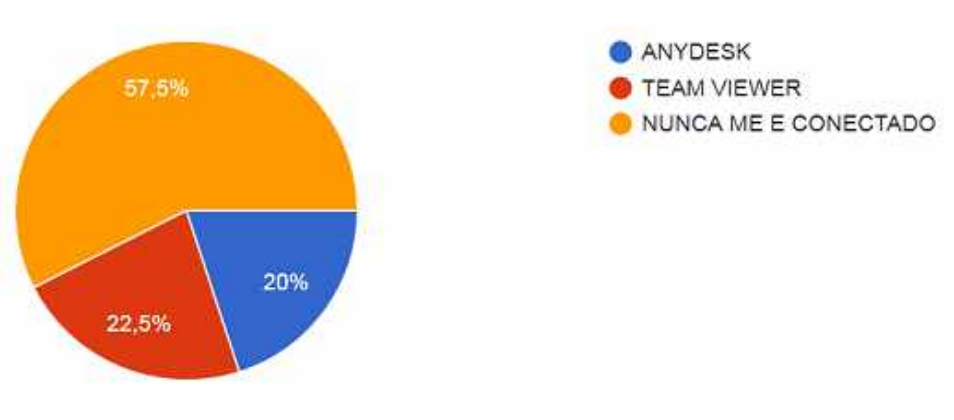


Figura 2.12: Pregunta: ¿Se ha conectado remotamente a su equipo de la empresa mediante alguna de las siguientes herramientas?
Desarrollado por: Joel F. Allaica C.

Análisis e Interpretación: El 57,5 de los encuestados nunca se ha conectado remotamente, el 22,5 % se ha conectado por Team Viewer, el 20 % a utilizado Any Desk. Las conexiones se lo están realizando por aplicaciones que utilizan los sistemas de criptografía reduciendo así el riesgo de la comunicación sea interceptada y terceros puedan ver lo que se esta trasmitiendo.

2.5. Procesamiento y análisis de datos

Debido a un ataque sufrido al servidor Zimbra ahora cuentan con bitácoras de fallos para así evitar daños o perdidas de datos; cuentan ademas con el personal que está en constante monitoreo del tráfico de la red, así como de los servidores.

Para garantizar la seguridad informática de la empresa tienen un servidor de antivirus, un servidor de Active Directory y un Firewall; los usuarios son notificados cada 3 meses de realizar el cambio de contraseñas y cada uno de ellos acceden a los distintos sistemas bajo roles asignados.

En cuanto los activos informáticos se lleva un registro claro de estos, pero no se cuanta con software especializado para el registro o el control de salida y en-

trada a la empresa. Los respaldos de seguridad son realizados de tipo incremental.

La mayor parte de los colaboradores están conscientes de los peligros de un ataque informático, así como de las medidas que se deben tomar, no obstante la información que manejan la mayor parte de colaboradores solo se la guardan en su computador y menciona que nunca reciben actualizaciones del antivirus instalado en su equipo de trabajo.

Un porcentaje pequeño indica que las contraseña nunca son cambiados, las contraseñas son guardados en papel, los correos desconocidos se abren sin ninguna medida de prevención; este tipo de brechas por mas pequeñas que parezcan pueden convertirse rápidamente en medio para que un malware pueda realizar algún tipo de infección.

Es necesario depurar las falencias encontradas mediante controles mas severos y capacitaciones frecuentes en temas relacionado a los colaboradores en relación a la seguridad informática y afines.

CAPÍTULO III

RESULTADOS Y DISCUSIÓN

Para el presente proyecto se utilizo la metodología Open Source Security Testing Methodology Manual(OSSTMM).

¿Que es el Manual de metodología de pruebas de seguridad de código abierto ?
OSSTMM El "Manual de metodología de pruebas de seguridad de código abierto" es un esfuerzo revisado por pares destinado a proporcionar una metodología integral específica para las pruebas de penetración. El OSSTMM agrupa las inquietudes de la administración (como las "Reglas de participación") junto con los pasos de las pruebas de penetración reales, y cubre cómo armar el "informe de hallazgos". Con respecto a las pruebas de penetración reales, el OSSTMM se centra en la seguridad de la tecnología de Internet, la seguridad de las comunicaciones, la seguridad inalámbrica y la seguridad física[14].

El OSSTMM es una metodología estandarizada para una verificación y medición exhaustivas del estado operativo y de seguridad actual. En realidad, es una gran cantidad de charlas académicas para decir que el OSSTMM lo ayudará a realizar una prueba de seguridad de acuerdo con una receta que le permite no solo ejecutar la mejor prueba posible que puede generar de la manera más eficiente (ahorrando tiempo ahorra dinero), pero eso también le da números que representan de manera realista su nivel actual de seguridad[15].

Dimensiones de Seguridad
El proceso de un análisis de seguridad, se concentra en evaluar las siguientes áreas, que reflejan los niveles de seguridad presentes, siendo estos el ambiente definido para el análisis de seguridad[10].

Visibilidad
La visibilidad es lo que puede encontrarse, registrarse, o monitorearse en el nivel de seguridad de manera independiente de algún dispositivo electrónico. Estas pueden ser: ondas de frecuencia, equipos de comunicación como por ejemplo te-

léfonos, sistema global para las comunicaciones móviles(GSM con sus siglas en ingles), correo electronico y paquetes de red como TCP/IP.

Acceso

El acceso es el punto de ingreso en lo referente a seguridad pero no necesariamente deber ser una muro físico. Estas pueden ser: una conexión de red, una página web, ondas de frecuencia, o cualquier objeto cuya espacio se comprendido con la definición de casi-público o en donde un equipo de computo interactúa con otro por mediante una red.

Limitar el acceso significa evitar el paso de cualquier tipo de dato a excepción de aquello que esta permitido financiera mente y por buenas prácticas.

Confianza

La confianza es una trayecto especializado en correspondencia con el nivel de seguridad. La confianza incluye el nivel y el tipo de autenticación, no-repudio, revisión de acceso, contabilización, confidencialidad e integridad entre varios factores internamente a nivel de seguridad.

Autenticación

¿Cuáles son los requisitos (o barreras, para aquellos sin autenticación) para ingresar a través de la puerta de enlace? Si le pido su pasaporte antes de permitirle entrar a su puerta, lo autenticaré[15].

La autenticación es proceso de seguridad que permite validad si un algo es verdaderamente quien dice ser.

No-repudio

¿Qué existe para evitar que la fuente asumida niegue su papel en cualquier interactividad, independientemente de si se obtuvo la entrada? Si puedo hacer una copia de seguridad de un correo electrónico enviado desde su computadora con una cinta de video con tiempo limitado de usted sentado en esa computadora componiendo el correo, entonces estoy produciendo el no repudio de usted y sus acciones[15].

El no-repudio proporciona la garantía de que ninguna persona o sistema pueda negar la participación en alguno de los procesos en cuestión.

Confidencialidad

La confidencialidad es la seguridad que solamente aquellos que estén involucrados

ya sean dispositivos físicos, digitales o personas que formen parte de la comunicación en el proceso que se este realizando tengan acceso a los datos privilegiados del mismo.

Privacidad
La privacidad indica que el proceso en desarrollo es únicamente conocido por los sistemas o partes involucradas.

Autorización
La autorización es la certeza que el proceso tiene una razón o justificación de negocio y es administrado responsablemente, dando acceso permitido a los sistemas.

Integridad
La integridad es la convicción de que el proceso tiene algún tipo de propósito, y esta no puede ser modificado, extendido, redirigido o reversado fuera del conocimiento de los sistemas o partes involucradas.

Seguridad
La seguridad son los mecanismos que brindan la garantía necesaria a un proceso para que no pueda averiar otros sistemas o procesos, inclusive en cuestión de una falla completa del mismo.

Alarma
La alarma es el aviso adecuado y preciso de las actividades que infringen o intentan quebrantar cualquiera de los aspectos de la seguridad. En la mayoría de infracciones la alarma es el único método que permite reaccionar de manera oportuna.

Mapa de Seguridad

El mapa de seguridad es un imagen de la presencia de seguridad. Esta corresponde al ambiente de un análisis de seguridad y está compuesta por seis secciones equivalentes a las de este manual. Las secciones se superponen entre si y contienen elementos de todas las otras secciones. Un análisis apropiado de cualquier sección debe incluir los elementos de todas las otras secciones, directa o indirectamente[10].

Las secciones en este manual son:

1 Seguridad de la Información
2 Seguridad de los Procesos
3 Seguridad en las tecnologías de Internet
4 Seguridad en las Comunicaciones
5 Seguridad Inalámbrica
6 Seguridad Física

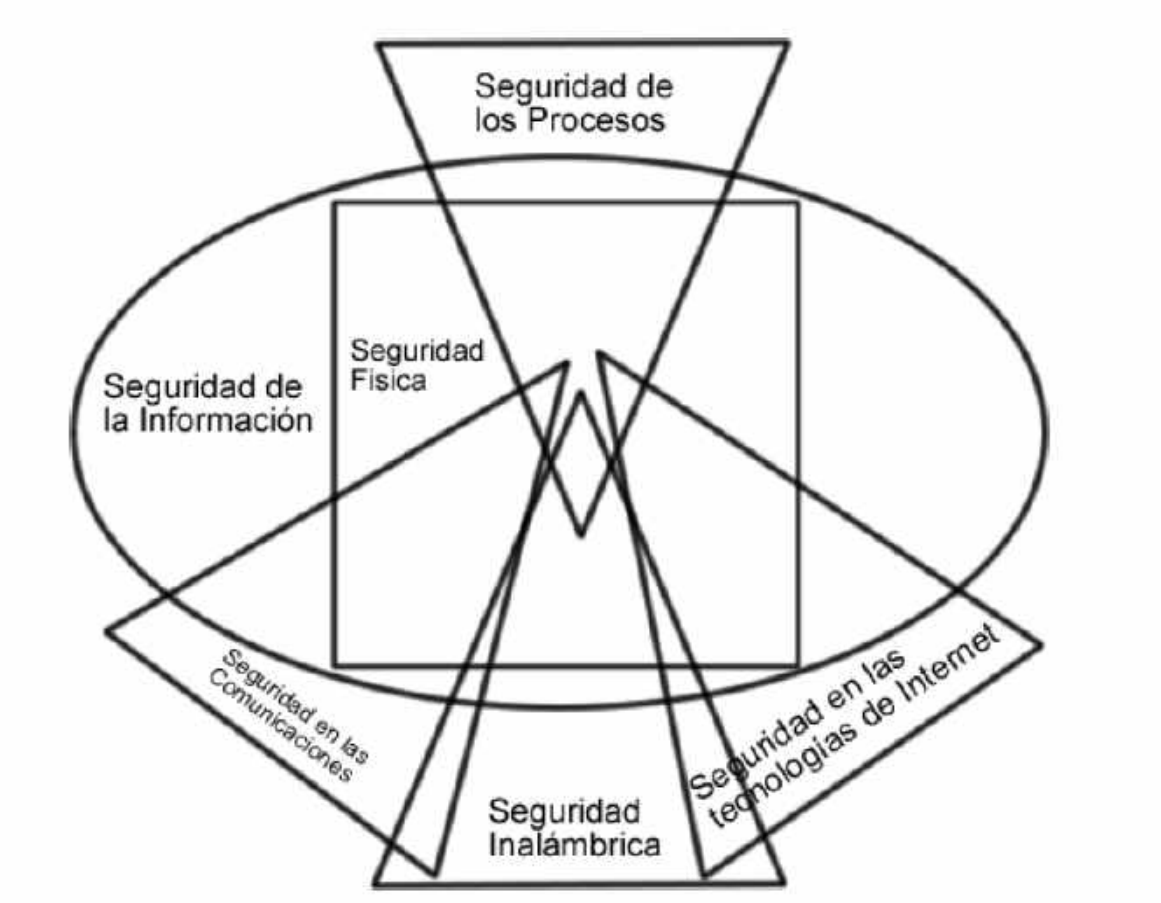


Figura 3.1: Mapa de la presencia de seguridad con todos los canales para el acceso a la información y la propiedad física
Fuente: P. V. Herzog, "OSSTMM", 2003.

3.1. Análisis de la metodología Open Source Security Testing Methodology Manual (OSSTMM)

La metodología propone un proceso de evaluación de debilidades mediante una serie de procesos que refleja de manera fiel los niveles de seguridad presentes en

la infraestructura a ser auditada.

Operación
En OSSTMM, el énfasis está en las pruebas de penetración, que está probando la seguridad de un sistema informático para encontrar vulnerabilidades. La piratería ética es otro término alternativo utilizado para describir las pruebas de penetración.
Efectivamente, es un conjunto de reglas para las pruebas de penetración e incorpora una metodología estándar para encontrar lagunas en la seguridad de las redes.
Las pruebas suelen dar como resultado soluciones recomendadas, pero no son obligatorias. Como resultado, después de las pruebas de seguridad, comparten un informe llamado Informe de auditoría de pruebas de seguridad (STAR), que forma parte del manual. STAR cubre todos los detalles de la prueba, incluyendo más información de los elementos perdidos durante el proceso más las anomalías descubiertas.

Auditoría
ISECOM define una auditoría OSSTMM como "una medición precisa de la seguridad a nivel operativo que está sin suposiciones y pruebas anecdóticas"[10].

Secciones
Está formada por 6 ítems los cuales comprenden todo el sistema actual, estas son:

- **Seguridad de la Información.**
  Se revisa tres aspectos: revisión inteligencia competitiva, revisión de privacidad y recolección de documentos.

  La revisión inteligencia competitiva.- es la información recolectada a partir de la presencia en Internet de la empresa la misma que puede ser analizada con inteligencia de negocio, con el objetivo de saber el tamaño, alcance y justificaciones de la red de la organización de una manera discreta; para poder tener una idea clara de cómo están las instalaciones informáticas se buscan todos los datos sensibles o no, sobre la misma. Los datos que se pueden recabar son diversos, tales como: los servicios que nos ofrece la empresa, números de teléfono, correos electrónicos, empresas con las que trabaja o está relacionada, socios, alianzas estrategias de la organización,

páginas web, IPs, versiones de servidores, servicios y sistemas operativos con que trabajan, entre otros. Uno o varios de estos datos puede servir para realizar un ataque por parte de usuarios mal intencionados.

La revisión de la privacidad.- es el enfoque legal e integro de almacenamiento, transmisión y control de los información basados en la privacidad del cliente y el empleado[10].
Se revisa que se respeten los derechos de las personas internamente en la empresa, para que sus datos personales no queden desprotegidos en el Internet. También realiza una revisión de cómo se distribuyen las contraseñas ya que no es igual entregar los datos mediante vocablo que, por escrito, por correo electrónico, etc. Esto puede llegar a ser estrechamente peligroso ya sea para la empresa como para los colaboradores. Es muy habitual, hallar contraseñas escritas en lugares visibles para cualquier persona, por ejemplo, post-its pegados en el borde del la pantalla del equipo trabajo.

La recolección de documentos.- tiene cierta relación con la revisión de inteligencia competitiva, pero con un enfoque más centrado en aspectos pequeños y concretos como correos electrónicos, ofertas de trabajo, medios de contacto entres otros. Esta información comúnmente se los puede extraer de los metadatos ocultos en los archivos subidos al Internet.

- **Seguridad de los Procesos.**
  Se revisa tres aspectos: testeo de solicitud, testeo de seguridad dirigida, testeo de personas confiables.

El testeo de solicitud.- busca obtener privilegios de acceso a una empresa y sus activos mediante preguntas al personal de acceso, a través de diversos métodos teniendo como principal la ingeniería social.

La Ingeniería Social tiene un papel fundamental en una gran cantidad de ciberataques, más allá de lo grande, pequeño o sofisticado que sea el crimen. Tal es el punto que siempre se ha mantenido como “una constante a lo largo de toda la historia de la seguridad de Internet”.
Uno de los fundamentos principales de la ingeniería social manifiesta, que “los usuarios son el eslabón débil”, por lo cual el usuario es la primera opción para obtener información, un ejemplo practico y sencillo seria, fingir ser el administrador de departamento de sistemas, para de esta manera solicitar a

los colaboradores sus contraseñas mediante un correo electrónico alegando que es para un proceso legítimo correspondiente a la empresa. Este tipo de casos son muy comunes en cualquier tipo de empresas; por mencionar alguno, cuando se recibe la llamada "phishing" de alguna institución, que piden los números de nuestra tarjeta de crédito para ejecutar alguna comprobación.

El testeo de seguridad dirigida.- es la detección de puntos de accesos privilegiados de una organización a través del teléfono, e-mail. Chat, etc. Convirtiéndose en otra rama de la ingeniería social por ende tienen gran relación con los módulos anteriores, la principal diferencia es que para este caso en cuestión el atacante se hace pasar por otro individuo.

El testeo de las personas confiables.- es un método el cual busca obtener acceso a la empresa a través de personas de confianza tales como un empleado o socio o alguna persona interna, con el fin de recabar información. Este aparato evidencia si existe algún camino o privilegio libre mediante la utilización de equipos de comunicación sumadas los datos recolectados del aparato anterior.

- **Seguridad en las Tecnologías de Internet.**
  Se realiza un sondeo general de la red para identificar los servicios de los distintos sistemas, realizando testeos de aplicaciones en Internet, detección de intrusos, medias de contingencia y denegación de servicios en busca de vulnerabilidades para luego de detectarlas, explotar y generar su posible solución. Además, se analizan las políticas de seguridad enfocadas a la reducción de riesgos.

  Sondeo de la red.- es la primera acción en lo referente al reconocimiento de la red. Se intenta obtener la mayor cantidad de información pero de una manera no invasiva. Se lo realiza fuera, intentando averiguar todo lo que podamos de ella, como rangos de IP, registros de dominios, subdominios etc.
  Este apartado es bastante parecido a la sección A, la principal diferencia es que que se busca información más precisa, sobre mapeos de red, bloques de IP y se enfoca en documentar todas IP que encontremos para posteriormente filtrarla y analizar.

Identificación de los Servicios de Sistemas. - se realiza el escaneo de puertos buscando obtener como resultado, puertos abiertos, cerrados o filtrados, direcciones IP de los sistemas activos, tipos de servicios, mapa de red, entre otros.
Se enumera los servicios de Internet activos o accesibles con el objetivo de encontrar maquinas activas.

Búsqueda y Verificación de Vulnerabilidades.- realiza una identificación, análisis y verificación de las debilidades en los servidores o de red en conjunto, es donde se va a realizar el ataque en cuestión: a las bases de datos, servidores de correos, servicios web. Buscando como resultado el tipo de aplicación o servicio por vulnerabilidad, un listado de las posibles vulnerabilidades o servicios denegados.
Habitualmente este tipo de escaneo se los realiza con programas automatizados, las cuales buscan errores de seguridad ya documentadas acerca de programas y sistemas operativos que usan las máquinas. Es necesario acentuar, OSSTMM demanda que se emplee por lo menos 2 programas distintos, para evidenciar las congruencia entre estos, y de esta manera tener obtener información con un nivel de porcentaje mas cercano a la realizad.

Testeo de Aplicaciones de Internet.- en este tipo de testeo, se analizan las aplicaciones clientes-servidor de la empresa que se está auditando. Se comprueba la robustez de estos, y se tratará de buscar vulnerabilidades o amenazas y explotarlos. La diferencia de modulo anterior (Búsqueda y Verificación de Vulnerabilidades) es que aquí desarrollamos nuestros propios fragmentos de software(exploits) de una manera evidente y personalizada.

Descifrado de Contraseña. – busca validar la robustez de las contraseñas mediante el uso de aplicativos o scripts automatizados con el fin de descifrar algoritmos o contraseñas débiles tendiendo como objetivo generar una lista de cuentas con usuario o contraseña del sistema.
Este módulo puede incluir técnicas para averiguar manualmente las contraseñas, que explote los usuarios y contraseñas por defecto en aplicaciones o sistemas operativos (p.ej. Usuario: System Contraseña: Test) o fácilmente predecible por parte del error de un usuario (p.ej. Usuario: joe Contraseña: joe)[10].

Testeo de Denegación de Servicios. - se enfoca en revisar el correcto funcionamiento de un sistema de detección de intrusos (IDS). El término IDS (Sistema de detección de intrusiones) hace mención a un procedimiento donde de manera discreta se pude escuchar el tráfico en la red para encontrar actividades extrañas o sospechosas, y de esta manera, mitigar el peligro de intromisión.
La inundación y ataques de denegación de servicio no están específicamente comprobadas y ademas están prohibidos por el manual, sin embargo, nos dan las pautas para analizar la continuidad de los sistemas.
Los ataques de inundación y los ataques DDoS siempre causarán algún tipo de problema y a veces no solamente al objetivo sino también a los enrutadores y sistemas entre el auditor y el objetivo.

Evaluación de Políticas de Seguridad. – el objetivo es comparar los resultados con los lineamientos a lograr, especificados por las políticas de seguridad. Esta activad se lo debe ejecutar una vez culminada las secciones técnicas y obtenido la vulnerabilidades, ya que de lo contrario, los resultados obtenidos aquí, no podrán ser comparadas con las políticas de seguridad que deben de cumplir.
Es fundamental evidenciar que las políticas de seguridad documentadas estén justificadas de manera legal y ética. Hay que prestar una especial atención a que se cumplan las normativas en referencia a los derechos y responsabilidades de empleador como del empleado, y además que, todo lo revisado esté acorde a las leyes internacionales y locales.
Una de las funciones esenciales en este módulo y posiblemente la mas importante es el cotejo de las medidas documentadas de manera física, y aquellas que estén implementadas se encuentran en funcionamiento de manera correcta. Por lo cual, es necesario realizar la comprobación de que las políticas de seguridad planteadas estén correctamente implementadas y configuradas[16].

- **Seguridad en las Comunicaciones.**
  Se realiza pruebas en los dispositivos de comunicación tales como: Central telefónica, PBX, Correo de voz, VoIP, FAX, esto con la finalidad de conseguir algún tipo de acceso y hallar posibles vulnerabilidades e información de la empresa o de los colaboradores.

- **Seguridad Inalámbrica.**

Se encarga de analizar el campo inalámbrica para ello realiza la verificación de radiación electromagnética, verificación de redes inalámbricas, verificación de redes bluetooth, verificación de dispositivos de entrada inalámbricos, verificación de dispositivos de manos inalámbricos, verificación de comunicaciones sin cable, verificación de dispositivos de vigilancia inalámbricos, verificación de dispositivos de transacción inalámbricos, verificación de RFDI, verificación de sistemas infrarrojos y revisión de privacidad, con el fin de incentivar a que la organización de una adecuada política de seguridad en la utilización de tecnologías inalámbricas[10].
Se examinar los dispositivos que brindan comunicación sin la necesidad esta interconectadas por cables, el objetivo es averiguar configuraciones por defecto o comunicaciones inalámbricas que estén mal implementadas.

- **Seguridad Física.**
  Se enfoca que realiza la inspección de perímetro, reconocimiento de controles de acceso, análisis de ubicación, inspección de entorno, chequeo de monitoreo, revisión de respuesta de alarmas. Evaluar la seguridad física de una organización brinda conocer la ubicación de la organización, sus bienes, un listado de las áreas protegidas y áreas no monitoreadas, los tipos de medidas existentes en las rutas de acceso, como alarmas o dispositivos de control de acceso, etc[10].
  Se evalúa de manera especifica la seguridad física de la empresa como son los controles de acceso, el tipo de monitoreo que se tienen con las cámaras de seguridad, la reacciona de alarmas ante catástrofes o amenazas.

Estudiado la metodología OSSTMM para la práctica se toman distintas módulos de la Seguridad de la Información(sección A), Seguridad de los Procesos(sección B), Seguridad en las tecnologías de Internet(sección C), Seguridad en las Comunicaciones(sección D), Seguridad Inalámbrica(sección E) y Seguridad Física(sección F) puesto que hace referencia al tema en estudio y los errores que comenten los usuarios finales mismas que son necesarios mitigarlos.

Al realizar la auditoria mediante esta metodología se puede realizar una serie de tareas o pruebas basados en cada unos de los módulos. En la sección A y B se realiza un estudio enfocado principalmente a los procesos que realizan de forma manual los colaboradores así como el punto de vista legal y ético de la empresa. Se puede identificar también de manera general la estructura de esta.

La sección C, D y E se estudia los equipos informáticos y el software que se tiene implementado con el fin de obtener un listado de los sistemas realizar el análisis correspondiente con respecto a la seguridad que posiblemente no hayan sido identificados en el caso de estudio evitar futuros ataques y perdidas económicas a la empresa.

Finalmente la ultima sección F permite conocer la ubicación de Megaprofer a nivel físico, de sus bienes, áreas protegidas, áreas no monitoreadas y áreas restringidas para los colaboradores y personas externas de la empresa, con el fin de mitigar daños al personal o a los equipos informáticos.

3.2. Fundamentación

Kali Linux.- es una distribución de Linux basada en Debian destinada a pruebas avanzadas de penetración y auditoría de seguridad. Kali contiene varios cientos de herramientas que están orientadas a diversas tareas de seguridad de la información, como pruebas de penetración, investigación de seguridad, informática forense e ingeniería inversa[17].

Maltego.- Maltego, es una herramienta que se basa en la información y aplicación forense y muestra cómo la información está conectado el uno al otro. Con Maltego, podemos encontrar las relaciones que las personas mayormente usan en la actualidad, incluyendo su perfil social (Facebook – Twitter), amigos mutuos, las empresas que se relacionan con la información recopilada, y sitios web. Si queremos recoger información relacionada con cualquier infraestructura, se puede reunir relación entre los dominios y nombres de DNS[18].
Servicio que tiene el potencial de encontrar información sobre personas y empresas en Internet, permitiendo cruzar datos para obtener perfiles en redes sociales, servidores de correo, etc[19].

Vega.- Vega es un escáner de vulnerabilidades de código abierto y gratuito. Según sus propias palabras, Vega puede usarse "para pruebas rápidas y un proxy interceptor para inspección táctica. El escáner Vega encuentra XSS (cross.site scripting), inyección de SQL y otras vulnerabilidades. Vega se puede extender usando un poderoso API en el lenguaje de la web: JavaScrip "[20].
VEGA incluye un escáner automatizado para ejecutar verificaciones rápidas a demás de un un proxy de interpretación para la inspección táctica. El escáner de VEGA encuentra XSS (cross-site scripting), inyección de SQL y otras

vulnerabilidades[21].

TheHarvester.- El propósito del software es reunir correos electrónicos, subdominios, hosts, nombres del pesonal, puertos abiertos y pancartas de diferentes fuentes públicas como motores de búsqueda, servidores de claves PGP y bases de datos informáticas SHODAN.
Esta herramienta está diseñada para ayudar a los evaluadores de penetración en las primeras etapas de la prueba de penetración para comprender la huella del cliente en Internet. También es útil para cualquier persona que quiera saber qué puede ver un atacante sobre su organización[22].

Google Hacking.- El pirateo de Google, a veces, conocido como Google dorking, es una técnica de recopilación de información utilizada por un atacante que aprovecha las técnicas avanzadas de búsqueda de Google. Las consultas de búsqueda de pirateo de Google se pueden utilizar para identificar vulnerabilidades de seguridad en aplicaciones web, recopilar información para objetivos arbitrarios o individuales, descubrir mensajes de error que revelan información confidencial, descubrir archivos que contienen credenciales y otros datos confidenciales[23].

Foca.- (Fingerprinting Organizations with Collected Archives) es una programa utilizad con el objetivo de extraer metadatos e información oculta en los documentos. Estos documentos se pueden encontrar en la pagina web de la empresa, y con FOCA se pueden descargar y analizar.
Los documentos que puede analizar son muy variados, siendo los más comunes los archivos de Microsoft Office, Open Office, o ficheros PDF, no obstante también analiza ficheros de Adobe InDesign, o svg por ejemplo[24].

Nmap.- es una herramienta usada para ejecutar la auditoria de la seguridades de la redes, con la cual se realiza análisis de cada paquete IP, por lo general los administradores de las redes llevan adelante inventarios de las mismas ya que NMAP trabaja con información DNS, en la cual se considera el tipo de puerto, protocolos, estados de los puertos y direcciones Mac que están vinculados a dichos puertos[25].

OpenVAS.- es un escáner de vulnerabilidades con todas las funciones. Sus capacidades incluyen pruebas no autenticadas, pruebas autenticadas, varios protocolos industriales y de Internet de alto y bajo nivel, ajuste de rendimiento para escaneo

a gran escala y un potente lenguaje de programación interno para implementar cualquier tipo de prueba de vulnerabilidad[26].

Nessus.- es un evaluador de seguridad de redes eficiente y fácil de usar, con una amplia base de datos de plugins que se actualiza a diario. Nessus es desarrollada por Tenable Network Security Inc., esta mejora permanentemente el motor nessus, diseña plugins para el evaluador y directivos de auditorías[27].

Metasploit Framework.- es una plataforma de prueba de penetración modular basada en Ruby que le permite escribir, probar y ejecutar código de explotación. Metasploit Framework contiene un conjunto de herramientas que puede usar para probar vulnerabilidades de seguridad, enumerar redes, ejecutar ataques y evadir la detección. En esencia, Metasploit Framework es una colección de herramientas de uso común que proporcionan un entorno completo para pruebas de penetración y desarrollo de exploits[28].

Slowloris.- es un programa de ataque de denegación de servicio que permite a un atacante abrumar a un servidor objetivo abriendo y manteniendo muchas conexiones HTTP simultáneas entre el atacante y el objetivo[29].

Hydra.- es un cracker de inicio de sesión paralelo que admite numerosos protocolos para atacar. Es muy rápido y flexible, y los nuevos módulos son fáciles de agregar. Esta herramienta hace posible que los investigadores y consultores de seguridad muestren lo fácil que sería obtener acceso no autorizado a un sistema de forma remota[30].

Medusa.- es otro cracker de contraseñas en línea para servicios de red. Tiene Las características de ser veloz, masivamente paralelo y modular. Actualmente, cuenta con módulos para los siguientes servicios: CVS, FTP, HTTP, IMAP, MS-SQL, NCP (NetWare), PcAnywhere, POP3, PostgresSQL, rexec, Rlogin, rsh, SMB, SMTP (VRFY), SNMP, SSHv2, SVN, Telnet, VmAuthd, VNC y un módulo envoltorio genérico[31].

Medusa está destinada a ser una fuerza bruta de inicio de sesión rápida, masivamente paralela, modular. El objetivo es admitir tantos servicios que permitan la autenticación remota como sea posible[7].

Sslstrip.- es una herramienta que secuestra de manera transparente el tráfico HTTP en una red, observa los enlaces HTTPS y los redireccionamientos, y luego asigna esos enlaces en enlaces HTTP parecidos o enlaces HTTPS homográficos similares. También admite modos para suministrar un favicon que se parece a un icono de candado, registro selectivo y denegación de sesión[32].

CVE(Common Vulnerabilities and Exposures).-Vulnerabilidades y exposiciones comunes (CVE®) es una lista de identificadores comunes para vulnerabilidades de seguridad cibernética conocidas públicamente[33].
CVE es:

- Un identificador para una vulnerabilidad o exposición.
- Una descripción estandarizada para cada vulnerabilidad o exposición.
- Un diccionario en lugar de una base de datos.
- Cómo las bases de datos y herramientas dispares pueden "hablar" el mismo idioma.
- El camino hacia la interoperabilidad y una mejor cobertura de seguridad.
- Una base para la evaluación entre servicios, herramientas y bases de datos.
- Gratis para descarga y uso público.

Avalado por la industria a través de las Autoridades de Numeración de CVE, la Junta de CVE y numerosos productos y servicios que incluyen CVE[33].

Certificado SSL/HTTPS.- El protocolo HTTPS funciona trasfiriendo de manera segura y cifrados datos entre el servidor y el usuario, siendo utilizado en la actualidad por sitios de comercio electrónico, banco on-line, instituciones gubernamentales y toda web que requiera manejo de datos personales. Este cifrado está basado en la tecnología SSL(Secure Socker Layer) o TSL(Transport Layer Security), una capa de conexión segur que hace uso de certificados digitales e impiden que la transferencia de datos sea interpretada en caso de intercepción malintencionada. Un certificado SSL no es otra cosa que un documento digital único que garantiza la vinculación entres una persona o entidad con su clave pública[34].

Man-In-The-Middle.- El término Man-In-The-Middle (persona en el medio en inglés) denota un ataque de encriptación en una red de equipos informáticos.

Es un tercer host que reenvía la información digital de forma nítido como una pasarela entre dos o más socios de comunicación y espías simultáneamente. El remitente y el receptor no saben que hay un tercer host entre los dos y que en realidad no se están comunicando directamente. Este tipo de asalto se denomina ataque de Man-In-The-Middle (abreviado ataque MITM). Los objetivos más comunes son las conexiones SSL seguras, como en la banca en línea[35].

3.3. Análisis de los métodos y herramientas necesarias para la ejecución de las Pruebas de Penetración (PenTest) y Hacking Ético.

Tabla 3.1: Tipos de Análisis y Detección de Vulnerabilidades

Tipo	Característica	Aplicable al proyecto	Observación
Análisis de Vulnerabilidades	Tiene un objetivo definido	Si	Tiene como objetivo detectar vulnerabilidades en partes específicas
	Tiene en cuenta el entorno de seguridad actual	Si	Aplica vulnerabilidades y fallos conocidos
	Trata de comprometer los sistemas objetivos	No	Solo lista las vulnerabilidades detectadas
	Explota las vulnerabilidades	No	No explota vulnerabilidades
Test de Penetración	Tiene un objetivo definido	Si	Tiene establecido un objetivo en partes específicas de la Infraestructura Tecnológica específicas
	Tiene en cuenta el entorno de seguridad actual	Si	Aplica vulnerabilidades y fallos conocidos
	Trata de comprometer los sistemas objetivos	Si	Además de listar las vulnerabilidad las intenta comprometer
	Explota las vulnerabilidades	Si	Explota vulnerabilidades mediante la simulación de un ataque
Hacking Ético	Tiene un objetivo definido	Si	Toda la Infraestructura Tecnológica es su objetivo específicas
	Tiene en cuenta el entorno de seguridad actual	Si	Actúa como un atacante real
	Trata de comprometer los sistemas objetivos	No	Su análisis es más complejo y profundo al comprometer los sistemas objetivos
	Explota las vulnerabilidades	No	Explota las vulnerabilidades de manera directa

Realizado el estudio de los tipos de detección y explotación de vulnerabilidades, las mismas que se encuentran resumidas en la tabla 3.1, se selecciona el Test de Penetración (Pentest) para la aplicación en este trabajo ya que el proyecto tiene cierto enfoque al análisis a los servidores de la empresa

Herramientas de reconocimiento

Tabla 3.2: Herramientas de reconocimiento

Caracteristica	Maltego	The Harvester	Anubis	Foca	Unicas	Angry IP Scanner
Licencia	Versión libre y pagada	Versión libre	Versión libre y pagada	Gratuito	Versión libre	Versión libre
Plataforma	Windows, Mac, Linux.	Linux	Windows	Windows	Linux	Windows, Mac, Linux.
Actualización / Soporte	Si	Si	No	Si	Si	Si
Facilidad de Manejo	Medio	Medio	Fácil	Fácil	Medio	Fácil

Mediante el análisis de la tabla 3.2, Maltego, TheHarvester y Uniscan tienen sus versiones libres y frecuentes actualizaciones logrando así que la herramienta trabaje de mejor manera, las herramientas no son difíciles de usar y vienen instalados el Sistema Operativo Kali Linux. También se elige Foca y Angry IP Scanner en su versión para Windows.

Herramientas de sondeo de puertos

Tabla 3.3: Herramientas de sondeo de puertos

Caracteristica	SuperScan 4	NetScan 6	Nmap	Advanced IP Scanner
Licencia	Versión libre y pagada	Versión libre y pagada	Gratuito	Gratuito
Plataforma	Windows	Windows	Linux, Mac OS X, Windows y UNIX	Windows
Actualización / Soporte	Si	Si	Si	Si
Facilidad de Manejo	Fácil	Fácil	Medio	Fácil

Mediante el estudio de las herramientas de sondeo de puertos resumida en tabla 3.3 se selecciona la herramienta NMAP como la mas optima ya que permite identificar las computadoras en una red, ver los puertos abiertos, los servicios que se

están ejecutando y el sistema operativo que tiene instalada.

Herramientas de detección de vulnerabilidades

Tabla 3.4: Herramientas de detección de vulnerabilidades

Caracteristica	OpenVAS	Nessus	Vega	Nexpose
Licencia	Versión libre	Versión libre y pagada	Versión libre	Versión libre y pagada
Plataforma	Centos, Debian, Fedora, OpenSuse, RedHat, Ubuntu, Windows	Microsoft Windows, Mac OS X, Linux, FreeBSD	Linux, OS X y Windows.	Windows
Actualización / Soporte	Si	Si	Si	Si
Facilidad de Manejo	Fácil	Fácil	Fácil	Fácil

Realizado el análisis de las herramientas de detección de vulnerabilidades(ver tabla 3.4) y debido a las limitaciones en sus versiones libres, se selecciona OpenVAS y Vega que son las más aconsejadas tomando en cuenta en el número de direcciones IP que permite analizar, actualización, facilidad de uso y la generación de reportes. Adicional se elige Nessus en su versión libre (Nessus Esentials).

Herramientas de explotación

Tabla 3.5: Herramientas de explotación

Caracteristica	Metasploit	Hping3	Hydra	Ettercap	Medusa	Medusa
Licencia	Versión libre y pagada	Versión libre	Versión libre	Versión libre	Versión libre	Versión libre
Plataforma	Windows 64-Bit, Linux: 64/32 Bits	GNU/linux, FreeBSD, NetBSD, OpenBSD, Solaris y Mac OS X.	Linux	Linux, Windows	Linux	Linux
Actualización / Soporte	Si	Si	Si	Si	Si	Si
Facilidad de Manejo	Medio	Fácil	Fácil	Medio	Fácil	Fácil

El Sistema Operativo Kali Linux, una distro con las mejores herramientas en lo referente a auditoría de redes en general y la seguridad informática, viene ya instalados más de 600 programas incluida Metasploit (software de pruebas de penetración), Ettercap (un sniffer), Hydra y Medussa (crackeador de passwords) entre otras herramientas (ver tabla 3.5)

3.4. Identificación de las vulnerabilidades en los servidores o fallos de sistemas que puedan ser utilizadas por intrusos malintencionados

Para el cumplir con los objetivos planteados en el proyecto así como con cada una de las actividades establecidas, se uso las herramientas previamente estudiadas y seleccionadas.

3.4.1. Seguridad de la Información

- **Revisión de la Inteligencia Competitiva**

Con la ayuda de la herramienta Maltego se indaga las interconexiónes existentes entre y un determinado dominio en este caso www.megaprofer.com

Figura 3.2: Maltego, transformación en relación al Dominio www.megaprofer.com
Desarrollado por: Joel F. Allaica C.

En la figura 3.2 se puede registrar las transformaciones DNS form Domain MX, NS y Dominios en común aplicado a un objeto de tipo Domain denominado como megaprofer.com, se observa el sistema de nombres de dominio(DNS por sus sigla en ingles), servidores de correo y servidores relacionados a megapofer.com. Las flechas muestran que hay conexión entre el objeto principal(padres) y los objetos secundarios(hijos), las estrellas amarillas reflejan que el objeto provee servicios web.

Resultados obtenidos con Maltego:

Tabla 3.6: Listado de servidores relacionados al dominio megaprofer.com

No	Dirección	IP Pública	Servicio
1	fe.megaprofer.com	186.46.29.222	Website
2	www.megaprofer.com	186.46.29.220	DNS Name
3	amb.megaprofer.com	186.46.29.218	DNS Name
4	ventas.megprofer.com	186.196.50.170	DNS Name
5	mail.megaprofer.com	190.95.136.138	MX Record
6	amb.megaprofer.com/prolan/mp	186.46.29.218	DNS Name

Con la herramienta TheHarvester se consigue información relacionada al dominio en exploración.

Figura 3.3: TheHarvester a dominio megaprofer.com
Desarrollado por: Joel F. Allaica C.

En la Figura 3.3 se puede ver los resultados de la ejecución de TheHarvester dando como resultado cuatro correos electrónicos así como los servidores relacionados al dominio megaprofer.com. Las direcciónes de correo no deben ser publicadas abiertamente ya que esto permitiría a los ciberdelincuentes realizar ataques personalizados por por este medio de manera fácil y efectiva.

El buscador de Google se puede utilizar para encontrar información indexada en el sistema, siempre que se de el uso correcto, para este caso, que se pueda filtrar información y disminuir la cantidad de datos obtenidos al máximo y de esta manera hallar resultados mas precisos, esto se lo realiza mediante la utilización de sus operadores, esta técnica se la conoce como “Google Hacking”.

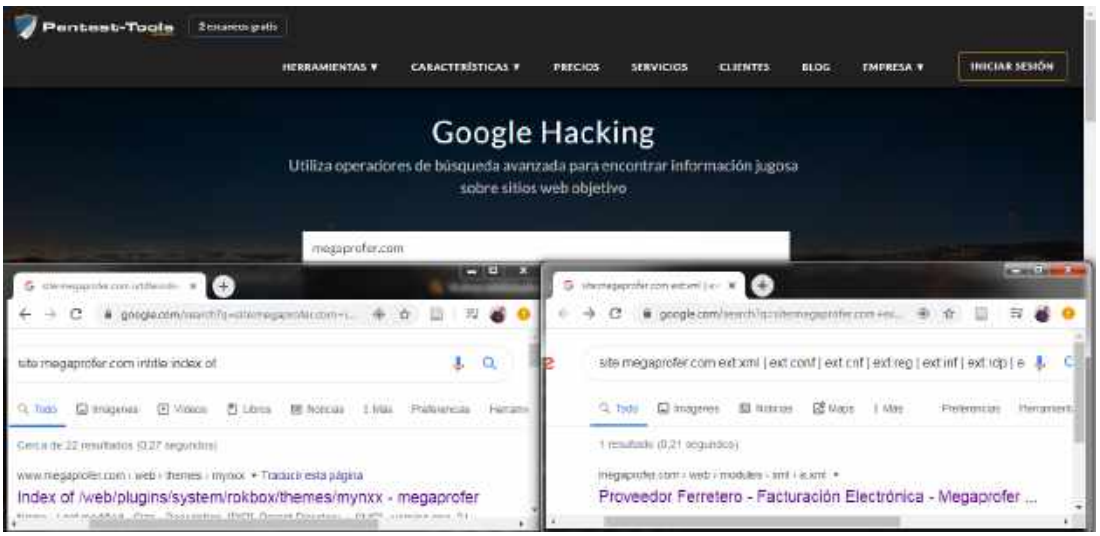


Figura 3.4: Resultados de Google Hacking en relación al Dominio www.megaprofer.com
Desarrollado por: Joel F. Allaica C.

En la figura 3.4 se observa la búsqueda de "Megaprofer S.A." en el buscador de Google, se encuentran más de treinta y nueve mil resultados, estos valores se puede reducir aplicando la técnica antes mencionada.

- **Revisión de Privacidad**

En este punto se hace una revisión de la privacidad, revisando las partes éticas y legales referentes al almacenaje, transmisión y control de datos de colaboradores y clientes. Se hace referencia al buen uso y distribución de las contraseñas, estableciendo políticas para su buen empleo.

Uno de los principios básicos de Seguridad Informática es la Confidencialidad de la información la cual menciona que no se debe divulgar la información de modo inadecuado y sin autorización.
El Art. 66 de la Constitución de la República, en su parte pertinente dispone "...Se reconoce y garantizará a las personas: 19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos de información requerirán la autorización del titular y el mandato de la ley"[36].

El la página web de empresa se pueden observar unicamente los datos necesario y relevantes, como el nombre y apellido del Gerente General, Estados Financieros

de la empresa, resolución de papel comercial, números de contacto, catálogos de productos, información que debe ser público y no representa un riesgo considerable (ver figura 3.5).

Figura 3.5: Datos públicos en pagina web de Megaprofer S.A.
Desarrollado por: Joel F. Allaica C.

Como segunda instancia se revisa los respaldos de las bases de datos, donde solamente el 75 % de los datos de la empresa se encuentran protegidas. Ademas no se encuentra la documentación que acredite la correcta ejecución y estado de los respaldos existentes.

- **Recolección de Documentos**

Mediante la herramienta FOCA para extraer los metadatos e información relevante oculta en los documentos y luego muestra un resumen de los resultados en un informe simple y fácil de entender. Es capaz de analizar archivos de Microsoft Office, Open Office, ficheros PDF, Adobe InDesign, o Gráficos vectoriales escalables (SVG).

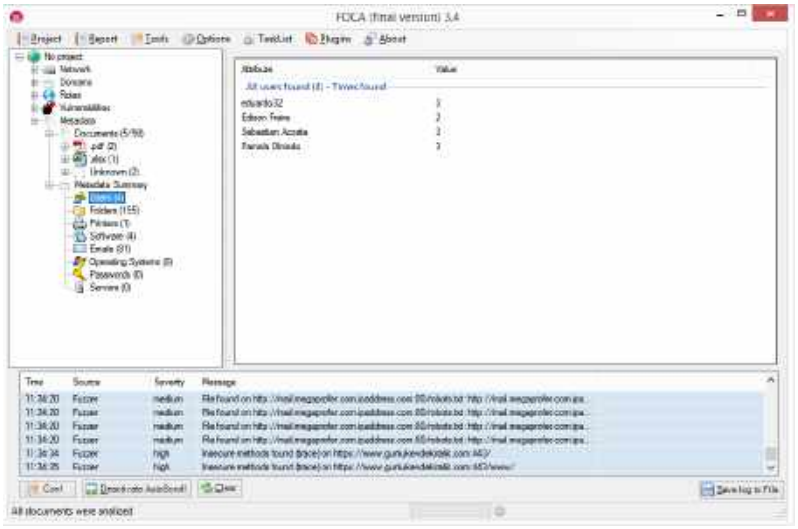


Figura 3.6: Resultados de Foca en relación al Dominio www.megaprofer.com
Desarrollado por: Joel F. Allaica C.

Mediante el análisis al dominio megaprofer.com se pudieron encontrar 89 registros de extensión: xlsx, txt, pl, php, pdf, jsf, html, ec, com, ca, de estos se extraen los metadatos y se obtienen:

- 4 nombres de usuarios
- 155 direcciones de ubicación de archivos
- 1 dirección de y nombre de impresora
- 4 software
- 81 correos electrónicos

La extracción de metadatatos deja un canal abierto para los hackers a que través de un metadato se pueda averiguar la versión de un sistema operativo que se maneje en la empresa, el software que utilizar los colaboradores o alguna información de carácter privado que debería estar oculta ya que pueden ser utilizadas para aplicar ingeniería social, robo de información mediante phishing, creación de diccionario de datos, entre otros, se pude también hallar algún fallo o una vulnerabilidad en la configuración de los servicios las mismas que pueden ser explotadas.
El resultado depende de numerosos factores, incluida la aplicación que se utilizó en la creación de cada uno de los archivos publicados.

Con estas revisión se demostró la facilidad de las herramientas para poder obtener datos de los distintos servidores y servicios con los que cuenta la empresa

esto con el fin de indicar al personal de TICs los riegos a los que están expuestos para que de esta manera puedan mejorar los controles de seguridad.

3.4.2. Seguridad de los Procesos

- **Testeo de Solicitud**

Se trató de obtener información, mediante una llamada telefónica, obteniendo un resultado positivo puesto que la persona que contesto la llamada, facilito los datos de contacto (cargo, nombre, correo, extensión, domicilio) sobre el responsable del departamento de sistemas, adicional se obtuvo el nombre del ERP que manejan actualmente.

Se ha realizado una prueba una segunda prueba ya conociendo datos del personal responsable del departamento de sistemas.
En la entrada de la empresa se encuentra el personal de seguridad custodiando la puerta principal y verificando la entrada de cualquier persona a las instalaciones. Se solicitó que se permita el acceso al cuarto de equipos con el fin de: "realizar una evaluación", respondiendo a la petición el personal de seguridad solicito la autorización de la dirección del departamento de sistemas.

Realizado el testeo de solicitud se puede concluir que el colaborador que toma las llamas no tiene cuidado suficiente en revelar información.

- **Testeo de Sugerencia Dirigida**

Se realizó, la prueba mediante la suplantación de identidad física, conociendo que el ingeniero jefe del departamento estaría ausente de las instalaciones de la empresa; se ha enviado una persona a la cual le doy nombre de "lucas" para el caso de estudio hasta las instalaciones de Megapofer. Lucas que se ha identificado como pariente del colaborador a cargo del departamento y ha comentado al personal de seguridad que se encuentra en la entrada de la empresa que ha sido enviado para que le faciliten cierta información.
El personal de seguridad desconociendo el tema realizo una llamada al número de extensión del departamento de sistemas, para notificar a los compañeros si tenían conocimiento del caso, el personal del departamento menciona que no tienen conocimiento y se comunican inmediatamente con el Jefe del departamento para para validar dicha la información, teniendo como resultado una negativa para el

acceso a las oficinas a lucas.

Realizado el testeo de sugerencia dirigida se concluye que el personal de seguridad física, así como los del departamento de sistemas si tiene el conocimiento adecuado para evitar que personas mal intencionadas puedan acceder a las instalaciones, así como a la información que se maneja en dicho departamento.

- **Testeo de las Personas Confiables**

  Para realizar el testeo, se solicitó a un familiar de uno de los colaboradores de Megaprofer, el mismo que tenia como objetivo recabar información sobre los aplicativos que se manejan y los servidores donde se ejecutan, indicando que es para un trabajo universitario.

  El cual obtuvo una respuesta negativa, ya que para dicha actividad previamente se debía entregar una solicitud autorizada por la institución donde se detalle la información que se necesita y mediante un análisis se verifica si es factible o no brindar la información solicitada.

Realizado el testeo de personas confiables se concluye que el personal encargado del departamento de sistemas tiene el conocimiento adecuado para evitar que personas mal intencionadas puedan acceder a la información que se maneja.

3.4.3. Seguridad en las tecnologías de Internet

- **Sondeo de Red**

Se refiere a la recolección y evaluación de los datos y las políticas de control, sirve como una breve introducción a los sistemas a se analizados.

Escaneo de vulnerabilidades de los sitios web
Se trató de ingresar a página web de la empresa Megaprofer S.A. www.megaprofer.com, como administrador de la página, sin ningún éxito ya que es necesario el usuario y la contraseña de administrador. Se realizaron pruebas con claves por defecto y aplicando Inyección SQL; obteniendo un resultado negativo.

Figura 3.7: Panel de administración de la página web www.megaprofer.com
Desarrollado por: Joel F. Allaica C.

Escaneo de vulnerabilidades con VEGA

Para realizar el escaneo de los otros aplicativos web se utiliza la herramienta VEGA; para iniciar y usar el escáner VEGA se lanza un escaneo por defecto pinchando en el icono de "New Scan".

La herramienta VEGA contiene 3 ventanas con opciones diferentes la una es Website View, que es en donde muestra la URL que se está analizando. La opción Scan Alerts que muestra las vulnerabilidades encontradas según el riesgo de cada una, y Scan Alert Summary que muestra el resumen de el proceso final cuando ha terminado de ejecutar la herramienta el debido análisis lo muestra según su categoría y riesgo.

Escaneo a amb.megaprofer.com
Local Filesystem Paths Found

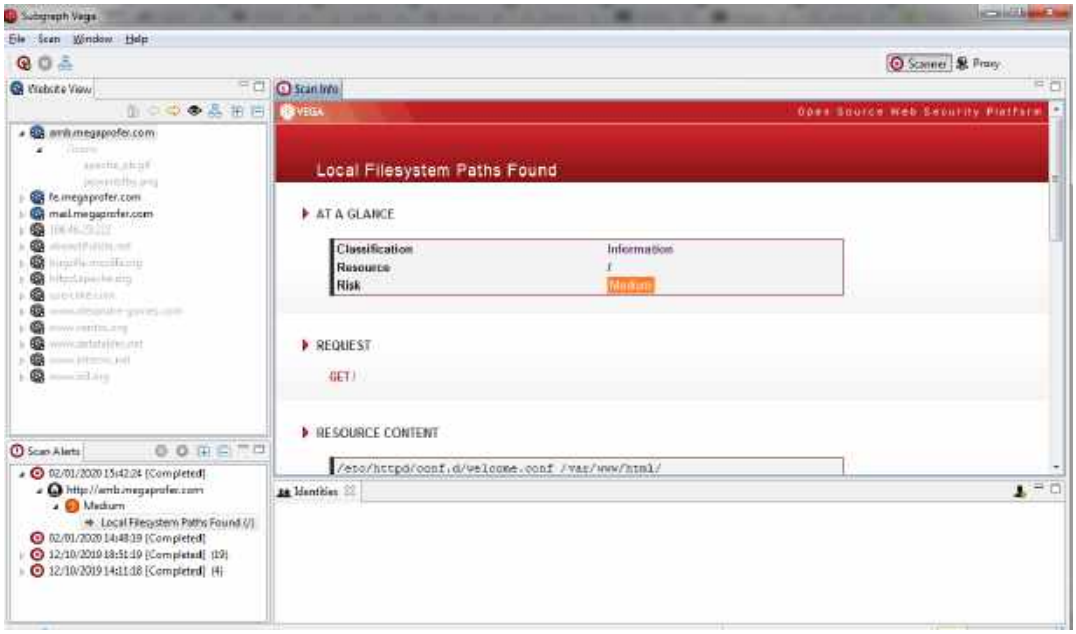


Figura 3.8: Figura que muestra Local Filesystem Paths Found
Desarrollado por: Joel F. Allaica C.

Contenido del recurso

/etc/httpd/conf.d/welcome.conf /var/www/html/

Discusión

Vega ha detectado una posible ruta absoluta del sistema de archivos (es decir, una que no es relativa a la raíz web). Esta información es confidencial, ya que puede revelar cosas sobre el entorno del servidor a un atacante. Conocer el diseño del sistema de archivos puede aumentar las posibilidades de éxito de los ataques a ciegas. Las rutas completas del sistema se encuentran muy a menudo en la salida de error. Esta salida nunca debe enviarse a clientes en sistemas de producción. Se debe redirigir a otro canal de salida (como un registro de errores) para que los desarrolladores y administradores del sistema lo analicen.

Impacto

Vega ha detectado lo que pueden ser rutas absolutas del sistema de archivos en el contenido escaneado. La divulgación de estas rutas revela información sobre el diseño del sistema de archivos. Esta información puede ser sensible, su divulgación puede aumentar las posibilidades de éxito de otros ataques.

Recomendación

Las rutas absolutas a menudo se encuentran en la salida de error. Tanto los administradores del sistema como los desarrolladores deben ser conscientes, ya que el problema puede deberse a un error de la aplicación o una configuración incorrecta del servidor. La salida de error que contiene información confidencial, como rutas de sistema absolutas, no debe enviarse a clientes remotos en servidores de producción. Esta salida debe enviarse a otra secuencia de salida, como un registro de errores.

Escaneo a fe.megaprofer.com

Cleartext Password over HTTP

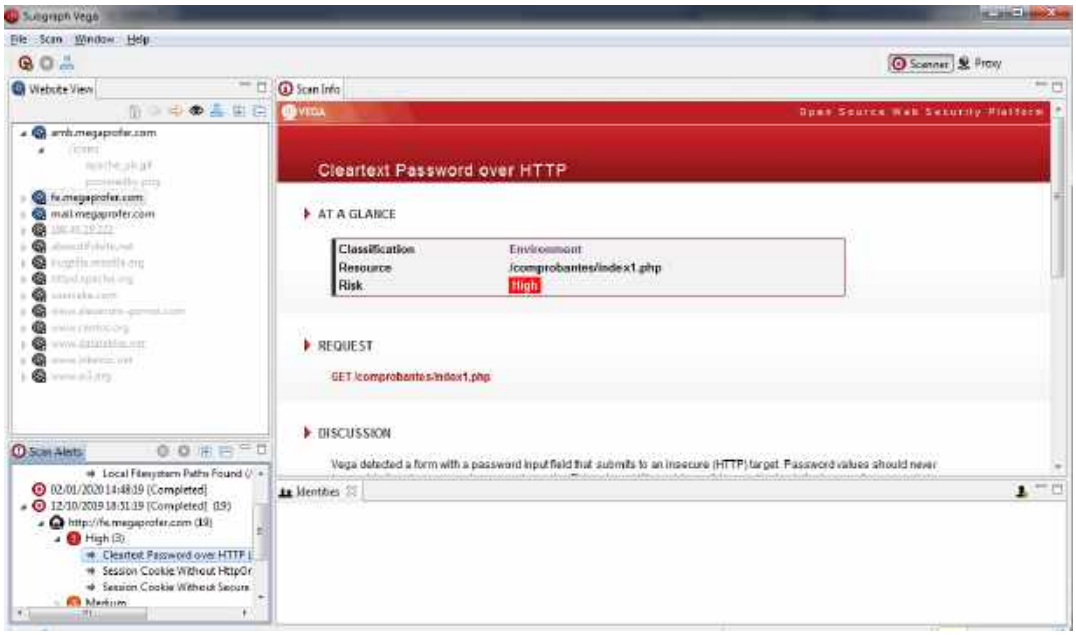


Figura 3.9: Figura que muestra Cleartext Password over HTTP
Desarrollado por: Joel F. Allaica C.

Contenido del recurso

/GET /comprobantes/index1.php

Discusión

Vega detectó un formulario con un campo de entrada de contraseña que se envía a un objetivo inseguro (HTTP). Los valores de las contraseñas nunca deben enviarse en claro a través de canales inseguros. Esta vulnerabilidad podría resultar en la divulgación no autorizada de contraseñas a atacantes de red pasivos.

Impacto

Vega ha detectado un formulario que puede provocar el envío de una contraseña a través de un canal inseguro.
Esto podría dar lugar a la divulgación de contraseñas a los espías de la red.

Recomendación

Las contraseñas nunca deben enviarse por texto sin cifrar. El formulario debe enviarse a un objetivo HTTPS.

Session Cookie Without HttpOnly Flag

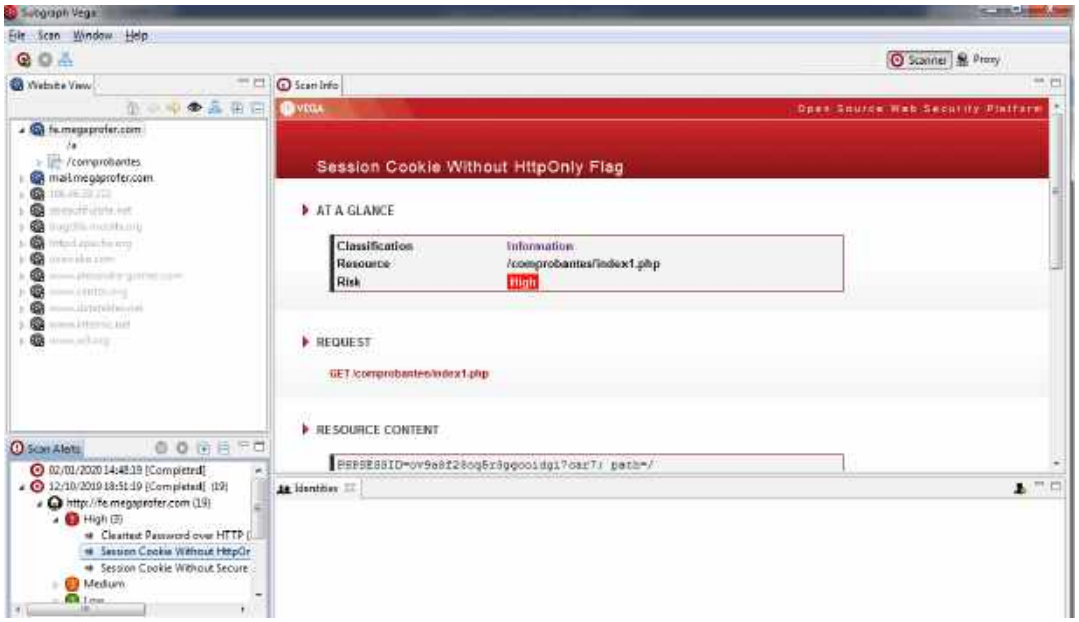


Figura 3.10: Figura que muestra Session Cookie Without HttpOnly Flag
Desarrollado por: Joel F. Allaica C.

Contenido del recurso

PHPSESSID=ov9a8f28cq5r3ggcoidgi7car7; path=/

Discusión

Vega ha detectado que una cookie de sesión puede haberse configurado sin el

indicador HttpOnly. Cuando este indicador no está presente, es posible acceder a la cookie a través del código de script del lado del cliente. El indicador HttpOnly es una medida de seguridad que puede ayudar a mitigar el riesgo de ataques de secuencias de comandos entre sitios que se dirigen a las cookies de sesión de la víctima. Si se establece el indicador HttpOnly y el navegador admite esta función, el código de script proporcionado por el atacante no podrá acceder a la cookie.

Recomendación

Al crear la cookie en el código, establezca el indicador HttpOnly en verdadero.

Session Cookie Without Secure Flag

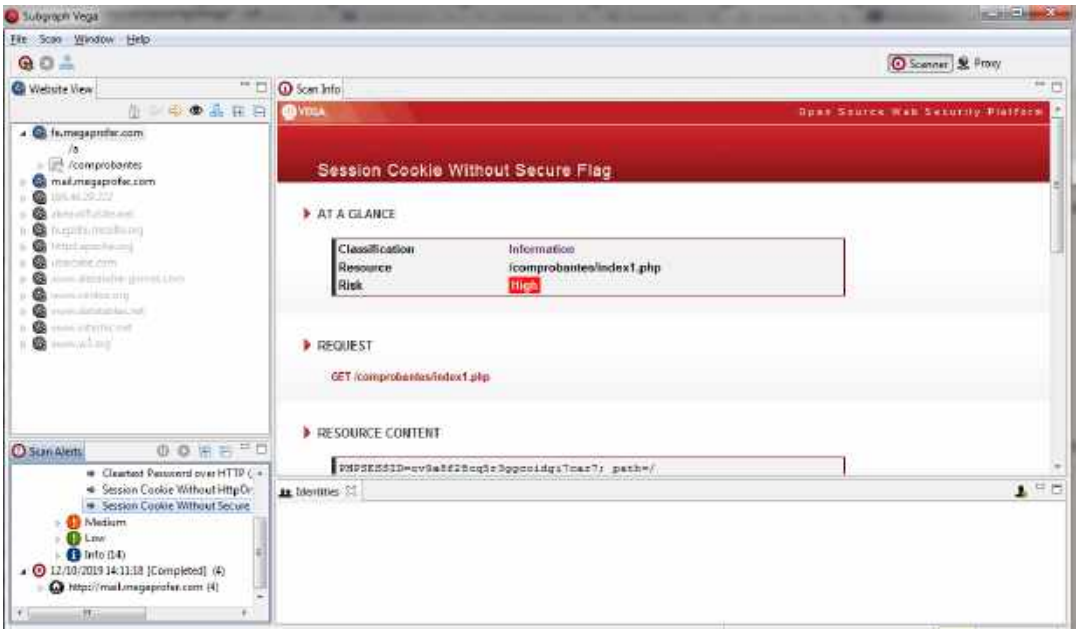


Figura 3.11: Figura que muestra Session Cookie Without Secure Flag
Desarrollado por: Joel F. Allaica C.

Contenido del recurso

/PHPSESSID=ov9a8f28cq5r3ggcoidgi7car7; path=/

Discusión

Vega ha detectado que una cookie de sesión conocida puede haberse configurado sin el indicador de seguridad.

Impacto

Las cookies pueden estar expuestas a los espías de la red.

Las cookies de sesión son credenciales de autenticación; Los atacantes que los

obtienen pueden obtener acceso no autorizado a las aplicaciones web afectadas.

Recomendación

Al crear la cookie en el código, establezca el indicador seguro en verdadero.

Escaneo a amb.megaprofer.com/prolan/mp

Servidor de pedidos en linea

HTTP Trace Support Detected

Figura 3.12: Figura que muestra HTTP Trace Support Detected
Desarrollado por: Joel F. Allaica C.

Discusión

HTTP TRACE es un método HTTP que solicita que el servidor repita la solicitud TRACE al cliente. Esto incluye encabezados que se enviaron junto con la solicitud. Se puede abusar de la compatibilidad con HTTP TRACE en escenarios en los que se ha encontrado una vulnerabilidad de secuencias de comandos entre sitios, pero no se puede explotar para recuperar los valores de las cookies porque las cookies de destino se establecen con el indicador HttpOnly. La bandera HttpOnly indica a los navegadores que no permitan el acceso a la cookie por Javascript. Si se encuentra una vulnerabilidad de secuencias de comandos entre sitios, pero la cookie de sesión está configurada HttpOnly, el soporte para HTTP TRACE abrirá una oportunidad para el robo de cookies. Un atacante puede utilizar la vulnerabilidad de secuencias de comandos entre sitios para que el navegador del usuario objetivo emita una solicitud de RASTREO al servidor a través de XMLHttpRequest (o una función similar) y luego recupere la cookie de la respuesta, que contendrá la solicitud enviada por el navegador, incluidas las

cookies.

Impacto

Permitir HTTP TRACE puede permitir el rastreo entre sitios. Los atacantes pueden usar el rastreo entre sitios con secuencias de comandos entre sitios para recuperar el valor de las cookies HttpOnly.

Recomendación

Para los servidores basados en Apache, la directiva TraceEnable se puede usar para deshabilitar la compatibilidad con HTTP TRACE. Para los servidores basados en IIS, la configuración del registro EnableTraceMethod controla la compatibilidad con HTTP TRACE.

- **Identificación de los Servicios de Sistemas**

La identificación de los servicios de sistemas abarca el escaneo de puertos TCP, UDP de los servidores para descubrir qué servicios se están ejecutando actualmente.

A continuación se realiza el escaneo de los servidores de la red para ellos se utiliza la herramienta NMAP con su interfaz Zenmap para realizar los respectivos sondeos de puertos y servicios a cada uno de los equipos en cuestión.

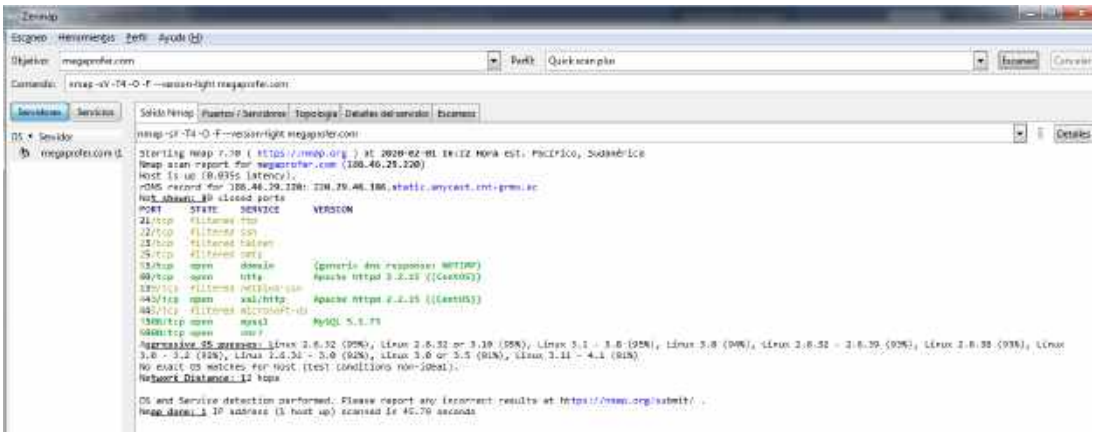


Figura 3.13: Sondeo de puertos con Nmap
Desarrollado por: Joel F. Allaica C.

Servidor megaprofer.com

Tabla 3.7: Sondeo de puertos a megaprofer.com con nmap

Puerto	Protocolo	Servicio	Detalle
22	tcp	ssh	OpenSSH 5.3 (protocol 2.0)
53	tcp	domain	Generic DNS response: NOTIMP
80	tcp	http	Apache httpd 2.2.15 (Centos)
443	tcp	ssl/http	Apache httpd 2.2.15 (Centos)
3306	tcp	mysql	Mysql 5.1.73
5900	tcp	vnc	

Central Telefónica

Tabla 3.8: Sondeo de puertos a central telefónica

Puerto	Protocolo	Servicio	Detalle
22	tcp	ssh	OpenSSH 4.3 (protocol 2.0)
25	tcp	smtp	Postfix smtpd
80	tcp	http	Apache httpd 2.2.3
110	tcp	pop3	Cyrus pop3d 2.3.7-Invoca-RPM-2.3.7-16.el5_11
111	tcp	rpcbind	
143	tcp	imap	Cyrus imapd 2.3.7-Invoca-RPM-2.3.7-16.el5_11
443	tcp	ssl/http	Apache httpd 2.2.3 ((CentOS))
993	tcp	ssl/imap	Cyrus imapd 2.3.7-Invoca-RPM-2.3.7-16.el5_11
995	tcp	ssl/pop3	Cyrus pop3d 2.3.7-Invoca-RPM-2.3.7-16.el5_11
2000	tcp	cisco-sccp	
3306	tcp	mysql	MySQL 5.0.95
5060	tcp	sip	

Servidor mail.megaprofer.com

Tabla 3.9: Sondeo de puertos a mail.megaprofer.com con nmap

Puerto	Protocolo	Servicio	Detalle
22	tcp	ssh	OpenSSH 5.3 (protocol 2.0)
25	tcp	smtp	Postfix smtpd
53	tcp	domain	Generic DNS response: NOTIMP
80	tcp	http	Apache httpd 2.2.15 (Centos)
110	tcp	pop3	Zimbra Collabration Suite pop3d
143	tcp	imap-proxy	Zimbra imapd
389	tcp	ldap	OpenLDAP 2.2.X - 2.3.X
443	tcp	ssl/http	nginx
445	tcp	ssl/smtp	microsoft-ds
465	tcp	ssl/smtp	Postfix smtpd
993	tcp	ssl/imap-proxy	Zimbra imapd
995	tcp	ssl/pop3	Zimbra Collabration Suite pop3d
8443	tcp	ssl/http	Zimbra http config

Servidor amb.megaprofer.com

Tabla 3.10: Sondeo de puertos a amb.megaprofer.com con nmap

Puerto	Protocolo	Servicio	Detalle
21	tcp	ftp	
22	tcp	ssh	OpenSSH 7.4 (protocol 2.0)
23	tcp	telnet	
25	tcp	smtp	
53	tcp	domain	Generic DNS response: NOTIMP
80	tcp	http	Apache httpd 2.2.15 (Centos)
110	tcp	pop3	
111	tcp	rpcbind	
139	tcp	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: SAMBA)
143	tcp	imap	
443	tcp	https	
445	tcp	microsoft-ds	
993	tcp	imaps	
995	tcp	pop3	
3306	tcp	mysql	MySQL 5.1.73

Servidor ventas.megaprofer.com

Tabla 3.11: Sondeo de puertos a amb.megaprofer.com con nmap

Puerto	Protocolo	Servicio	Detalle
21	tcp	ftp	
22	tcp	ssh	OpenSSH 7.4 (protocol 2.0)
23	tcp	telnet	
25	tcp	smtp	
53	tcp	domain	Generic DNS response: NOTIMP
80	tcp	http	Apache httpd 2.2.15 (Centos)
110	tcp	pop3	
111	tcp	rpcbind	
139	tcp	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: SAMBA)
143	tcp	imap	
443	tcp	https	
445	tcp	microsoft-ds	
993	tcp	imaps	
995	tcp	pop3	
3306	tcp	mysql	MySQL 5.1.73

Servidor fe.megaprofer.com

Tabla 3.12: Sondeo de puertos a fe.megaprofer.com con nmap

Puerto	Protocolo	Servicio	Detalle
22	tcp	ssh	OpenSSH 5.3 (protocol 2.0)
53	tcp	domain	Generic DNS response: NOTIMP
80	tcp	http	Apache httpd 2.2.15 (Centos)
110	tcp	pop3	Dovecot pop3d
111	tcp	rpcbind	
143	tcp	imap	Dovecot imap
443	tcp	ssl/http	Apache httpd 2.2.15 (Centos)
993	tcp	ssl/imap	Dovecot imap
995	tcp	ssl/pop3	Dovecot pop3d
3306	tcp	mysql	MySQL 5.1.73
3389	tcp	ms-wbt-server	xrdp
6001	tcp	X11	

Servidor pedidos en linea

Tabla 3.13: Sondeo de puertos a amb.megaprofer.com/prolan/mp con nmap

Puerto	Protocolo	Servicio	Detalle
22	tcp	ssh	OpenSSH 5.3 (protocol 2.0)
80	tcp	http-proxy	Squid Apache httpd proxy 3.1.23
111	tcp	rpcbind	Filtred
443	tcp	ssl/http	Apache httpd 2.2.15 (Centos)
3306	tcp	mysql	Mysql 5.1.73

Se pudo determinar que los servidores tienen los puertos 22 / SSH, 25 / SMTP, 80 / HTTP y 443 / HTTPS abiertos, estos son identificados con facilidad por parte de intrusos; las configuraciones de este tipo podría provocar la pérdida de datos, la denegación de servicios y hacen que la identificación de amenazas sea cada vez más difícil permitiendo que los atacantes tengan la facilidad en ejecutar ataques contra estos u otros dispositivos.

- **Búsqueda y Verificación de Vulnerabilidades**

Se exploro posibles errores en los sistemas operativos, esto se lleva acabo mediante la búsqueda de vulnerabilidades en lo equipos mencionados, inmediatamente se explotan los errores que hayan encontrado en las pruebas de penetración previamente ejecutadas, esto se lo desarrolla con OpenVAS y Nessus, que son programas de escaneo de vulnerabilidades, el framework incorpora herramientas de reconocimiento, escaneo, análisis y explotación de debilidades

Análisis de vulnerabilidades con OpenVAS.- El análisis con OpenVAS se realiza mediante su interfaz gráfica, disponible para web. Mencionado eso se utiliza el Asistente de Seguridad propia del aplicativo para crear un objetivo(target) que es la IP a escanear y una tarea(task) para cada una de los objetivos a escanear, realizada la configuración necesaria se procede a ejecutar las tareas(ver figura 3.14).

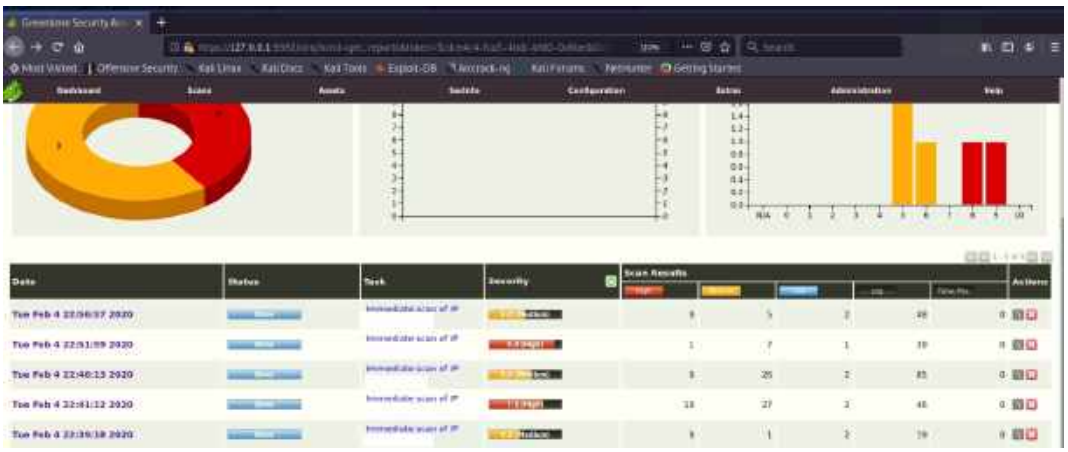


Figura 3.14: Escaneo de vulnerabilidades con OpenVAS
Desarrollado por: Joel F. Allaica C.

Como resultado se obtiene la vulneravilidad con un detalle fácil de interpretar.

Análisis de vulnerabilidades con NESSUS.- El análisis con Nessus se realiza mediante su interfaz gráfica en la web. Se procede a configurar un nuevo escaneo para lo cual se puede configurar todo desde cero o seleccionar una de las plantillas con políticas propias del aplicativo, se elige "Advanced Scan" y se llenan los campos solicitados, un nombre cualquiera: "megaprofer" para este caso, las direcciones IP a examinar, las carpeta donde se desea guardar el análisis esto se pude deja por defecto(recomendado), guarda y de inmediato se pude iniciar el análisis de vulnerabilidades.

Figura 3.15: Escaneo de vulnerabilidades con Nessus
Desarrollado por: Joel F. Allaica C.

Cada uno de los programas utilizados detallan de manera clara el error encontrado junto con su nivel de riesgo y su viable solución. OpenVas indica también si la vulnerabilidad a sido explotada. De igual forma las herramientas permiten

exportar el reporte en formato PDF.

A continuación se detallan las vulnerabilidades detectadas con su nivel de riesgo:

Servidor ventas.megaprofer.com

Tabla 3.14: Vulnerabilidades detectadas en ventas.megaprofer.com

Servicio	Vulnerabilidad	Riesgo	Observación
MySQL	Fue posible iniciar sesión con credenciales sencillas	Alto	Una explotación exitosa podría permitir a los atacantes ejecutar código arbitrario con privilegios de administrador, pudiendo comprometer totalmente el servidor que está ejecutando la versión afectada de MySQL
Apache HTTP	Métodos HTTP: TRACE habilitado	Medio	Un atacante puede usar esta falla para engañar a sus usuarios web legítimos para que le roben sus credenciales
Apache SSL/TLS	Conjuntos de cifrado 'nulos' aceptados por este servicio a través del protocolo TLSv1.0	Medio	Esto podría permitir a los atacantes remotos obtener información confidencial o tener otro impacto no especificado
Apache SSL/TLS: SSLv3 Protocolo CBC	SSL / TLS: Protocolo SSLv3 Vulnerabilidad de divulgación de información en conjuntos de cifrado CBC (POODLE)	Medio	La explotación exitosa permitirá a los atacantes de hombre en el medio obtener acceso al flujo de datos de texto sin formato
Apache SSL/TLS	El certificado SSL / TLS del servidor remoto expirado	Medio	Un atacante podría usar esto para ataques MitM, acceder a datos sensibles y otros ataques.
Apache SSH	Algoritmos de cifrado débiles SSH admitidos	Medio	Contienen método que no proporciona protección de confidencialidad, y NO SE RECOMIENDA usarlo.
TCP	Marcas de tiempo TCP habilitado	Bajo	El host remoto implementa marcas de tiempo TCP y, por lo tanto, permite calcular el tiempo de actividad.

Servidor fe.megaprofer.com

Tabla 3.15: Vulnerabilidades detectadas en fe.megaprofer.com

Servicio	Vulnerabilidad	Riesgo	Observación
Apache HTTP	Métodos HTTP: TRACE habilitado	Medio	Un atacante puede usar esta falla para engañar a sus usuarios web legítimos para que le roben sus credenciales
Apache SSL/TLS	El certificado SSL / TLS del servidor remoto expirado	Medio	Un atacante podría usar esto para ataques MitM, acceder a datos sensibles y otros ataques.
Apache SSH	Algoritmos de cifrado débiles SSH admitidos	Medio	Contienen método que no proporciona protección de confidencialidad, y NO SE RECOMIENDA usarlo.
Apache SSH	SSH Algoritmos de MAC débiles admitidos	Bajo	Algoritmos MAC de servidor a cliente débiles son compatibles con el servicio remoto
TCP	Marcas de tiempo TCP habilitado	Bajo	El host remoto implementa marcas de tiempo TCP y, por lo tanto, permite calcular el tiempo de actividad.

Servidor www.megaprofer.com

Tabla 3.16: Vulnerabilidades detectadas en www.megaprofer.com

Servicio	Vulnerabilidad	Riesgo	Observación
Joomla	Es propenso a múltiples vulnerabilidades de seguridad	Alto	La explotación exitosa permitiría a un atacante acceder a información confidencial o ejecutar comandos arbitrarios.
PHP	Archivos llaman a la función phpinfo () que revela información potencialmente confidencial	Alto	Se puede obtener información como: nombre de usuario del usuario que ejecuta el proceso PHP, si es un usuario sudo, la dirección IP del host, la versión del servidor web, la versión del sistema y el directorio raíz del Servidor web.
Apache SSL/TLS	Certificado del servicio remoto expirado	Medio	Un atacante podría usar esto para ataques MitM, acceder a datos sensibles y otros ataques.
HTTP	Métodos HTTP: TRACE habilitado	Medio	Un atacante puede usar esta falla para engañar a sus usuarios web legítimos para que le den sus credenciales
Apache SSH	Algoritmos de cifrado débiles SSH admitidos	Medio	Contienen método que no proporciona protección de confidencialidad, y NO SE RECOMIENDA usarlo.
Apache SSH	SSH Algoritmos de MAC débiles admitidos	Bajo	Algoritmos MAC de servidor a cliente débiles son compatibles con el servicio remoto
TCP	Marcas de tiempo TCP habilitado	Bajo	El host remoto implementa marcas de tiempo TCP y, por lo tanto, permite calcular el tiempo de actividad.

Servidor mail.megaprofer.com

Tabla 3.17: Vulnerabilidades detectadas en mail.megaprofer.com

Servicio	Vulnerabilidad	Riesgo	Observación
Apache SSL/TLS	SSL / TLS: Informe de conjuntos de cifrado 'anónimos'	Medio	Esto podría permitir a los atacantes remotos obtener información confidencial o tener otros impactos no especificados.
Apache SSL/TLS	El certificado SSL / TLS del servidor remoto expirado	Medio	Un atacante podría usar esto para ataques MitM, acceder a datos sensibles y otros ataques.
Http	Falta el atributo de cookie `httpOnly`	Medio	Un atacante podría usar esto para ataques MitM, acceder a datos sensibles y otros ataques.
Post Office Protocolo (POP3)	El servidor remoto POP3 acepta inicios de sesión a través de conexiones sin cifrar	Medio	Un atacante puede descubrir nombres de usuario y contraseñas olfateando el tráfico al servicio POP3 si se utiliza un mecanismo de autenticación menos seguro (por ejemplo, comando USER, AUTH PLAIN, AUTH LOGIN).
Zimbra Collaboration Suite Persistent XSS	Vulnerabilidad de XSS persistente en Zimbra Collaboration Suite-02 de febrero	Medio	La explotación exitosa permitirá a los atacantes remotos inyectar HTML arbitrario y código de script en el sitio web.
Apache SSH	SSH Algoritmos de MAC débiles admitidos	Bajo	Algoritmos MAC de servidor a cliente débiles son compatibles con el servicio remoto
TCP	Marcas de tiempo TCP habilitado	Bajo	El host remoto implementa marcas de tiempo TCP y, por lo tanto, permite calcular el tiempo de actividad.

Servidor amb.megaprofer.com

Tabla 3.18: Vulnerabilidades detectadas en amb.megaprofer.com

Servicio	Vulnerabilidad	Riesgo	Observación
Portainer	Portainer es propenso a múltiples vulnerabilidades.	Alto	La explotación exitosa de esta vulnerabilidad permitiría a un usuario autenticado obtener permiso completo en el sistema de archivos del host
Apache HTTP	El host / aplicación transmite información confidencial (nombre de usuario, contraseñas) en texto claro a través de HTTP	Medio	Un atacante podría usar esta situación para comprometer o espiar la comunicación HTTP entre el cliente y el servidor utilizando un ataque de intermediario para obtener acceso a datos confidenciales como nombres de usuario o contraseñas.
Apache SSL/TLS	El certificado SSL / TLS del servidor remoto expirado	Medio	Un atacante podría usar esto para ataques MitM, acceder a datos sensibles y otros ataques.
Apache SSH	Algoritmos de cifrado débiles SSH admitidos	Medio	Contienen método que no proporciona protección de confidencialidad, y NO SE RECOMIENDA usarlo.
TCP	Marcas de tiempo TCP habilitado	Bajo	El host remoto implementa marcas de tiempo TCP y, por lo tanto, permite calcular el tiempo de actividad.

Servidor Pedidos en linea

Tabla 3.19: Vulnerabilidades detectadas servidor de pedidos en línea

Servicio	Vulnerabilidad	Riesgo	Observación
Apache SSL/TLS	SSL / TLS: informe de conjuntos de cifrado vulnerables para HTTPS.	Medio	No hay impacto en la integridad del sistema. Afecta parcialmente a la confidencialidad del sistema. No hay impacto en la disponibilidad del sistema
Apache SSL/TLS: SSLv3 Protocolo CBC	SSL / TLS: Protocolo SSLv3 Vulnerabilidad de divulgación de información en conjuntos de cifrado CBC (POODLE)	Medio	La explotación exitosa permitirá a los atacantes de hombre en el medio obtener acceso al flujo de datos de texto sin formato
Apache SSL/TLS	El certificado SSL / TLS del servidor remoto expirado	Medio	Un atacante podría usar esto para ataques MitM, acceder a datos sensibles y otros ataques.
Apache SSH	Algoritmos de cifrado débiles SSH admitidos	Medio	Contienen método que no proporciona protección de confidencialidad, y NO SE RECOMIENDA usarlo.
Apache SSH	SSH Algoritmos de MAC débiles admitidos	Bajo	Algoritmos MAC de servidor a cliente débiles son compatibles con el servicio remoto
TCP	Marcas de tiempo TCP habilitado	Bajo	El host remoto implementa marcas de tiempo TCP y, por lo tanto, permite calcular el tiempo de actividad.

- **Testeo de Aplicaciones de Internet**

Con la finalidad de no violar la integridad de los equipos interconectados de la empresa, Megaprofer S.A. o dejar uno de los servicios con algún tipo de daño y muy probablemente dejarlo sin funcionamiento se crean y configurar equipos virtuales incluido los servicios con características iguales en las mayoría y similares a las reales en otras; las actividades de explotación se desarrollan en el ítem 4.5.4. Mencionadas tareas, se lo realiza como medida de prevención y seguridad.

- **Descifrado de Contraseña**

Se trata de validar el nivel de seguridad de acceso a los servidores y el nivel de robustez que tienen las contraseñas mediante el uso de herramientas de recuperación para su obtención. Con el fin de encontrar los usuarios o cuentas de los sistemas que usan.
Como una parte del desarrollo se ha revisado algunas de las contraseñas del acceso en los servidores, para comprobar el nivel de seguridad, tiempo que se cambia cada una de ellas y existencia de contraseñas de defecto.

Realizado el proceso se concluye que el nivel de seguridad del 80 % de claves es muy bueno, puesto que varias incluyen números letras, caracteres especiales y una longitud superior a las 15 caracteres pero la ultima vez que se cambio las contraseñas fue a finales del año 2018 del 70 % de estas ademas existen 2 contraseñas por defecto,

Las contraseñas se deben cambiar en un periodo máximo de 90 días, con una clave sumamente difícil, a fin de evitar que sean descifradas con facilidad y pudad ingresen a los ordenadores y servidores; de esta manera se pueden evitar ataque por parte de los cibernéticos entre los cuales el "ransomware" es el más común en América Latina.

- **Evaluación de Políticas de Seguridad**

Las políticas de seguridad es un documento escrito con claridad y legible donde se delinean las políticas para la reducción de riesgos en el ámbito de TICs. En la empresa Megaprofer S.A. cuenta con un instructivo de uso de Herramientas Tecnológicas donde se definen las políticas de uso y seguridad aplicables a las herramientas e infraestructura de la organización las mismas están enfocadas en los equipos tecnológicos asignados, cuentas y accesos empresariales, confidencialidad

de la información, contraseñas y redes la cual es firmada por los colaboradores al ingresar a la empresa, donde se comprometen al uso adecuado que se le deben dar a las herramientas tecnológicas asignadas a su cargo y son propiedad de la empresa.

La seguridad existente en los servidores, se basa principalmente en la confianza en el personal que labora en el área de informática de no divulgar las claves, no se permitirá el acceso desde el Internet a personas ajenas a la institución con el objetivo de producir un daño a la misma. También se verificó que algunas de sus herramientas donde un porcentaje representativo de lo sistemas operativos no están complemente actualizadas lo que deja puertas abiertas a nivel informático las mismas que pueden ser utilizados por agentes externos.

3.4.4. Seguridad en las Comunicaciones

- **Testeo de PBX**

Se realizo el testeo del funcionamiento de la central telefónica, con el objetivo de encontrar alguna anomalía.
Se genero un reporte de llamadas en la central telefónica IP ELASTIX , para determinar si se ha realizado el uso indebido de la central telefónica, obteniendo un resultado negativo, todas las llamadas salientes corresponden a las extensiones permitidas. Ver Figura 3.16.

Extension	Nombre Usuario	# Llamadas Entrantes	# Llamadas Salientes	Tiempo total (Llamadas Entrantes)	Tiempo total (Llamadas Salientes)	Detalles
300	RECEPCION UIO	5317	514	64h. 07m. 17s	06h. 24m. 36s	Ver
413	ECO IBARRA MARIANO ACOSTA	262	321	07h. 59m. 09s	11h. 55m. 15s	Ver
466	CENTRO DE ACOPIO IBARRA	318	256	15h. 41m. 17s	17h. 09m. 08s	Ver
345	TESORERIA	1075	222	31h. 42m. 48s	02h. 50m. 39s	Ver
416	ECO IBARRA HELECODORO AYALA	108	214	03h. 52m. 15s	04h. 38m. 53s	Ver
331	PAUL MANOSALVAS	266	208	04h. 27m. 29s	05h. 53m. 56s	Ver
417	ECO IBARRA ATAHUALPA	222	204	07h. 18m. 44s	05h. 19m. 10s	Ver
311	ANA ANDRADE	103	172	02h. 02m. 42s	03h. 51m. 40s	Ver
323	JACQUELINE MARTINEZ	151	154	03h. 04m. 08s	01h. 02m. 05s	Ver
322	DENNIS VELASCO	94	123	03h. 02m. 15s	01h. 46m. 48s	Ver
319	PAULINA GUERRA	45	121	09h. 03m. 57s	04h. 22m. 58s	Ver
303	RECEPCION PRESIDENCIA	57	120	00h. 16m. 34s	02h. 20m. 29s	Ver

Figura 3.16: Resumen de llamas de la Central IP
Fuente: Megaprofer S.A.

Reporte total de llamadas desde el primero de octubre del 2019

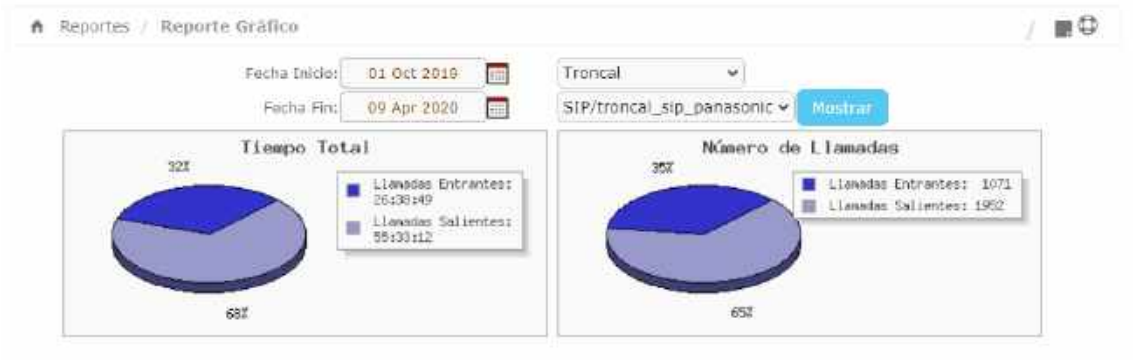


Figura 3.17: Reporte de llamadas de Central IP
Fuente: Megaprofer S.A.

En figura 3.17 se puede evidenciar que se ha realizando más llamadas salientes. Se obtiene el detalle de un 65 % de salientes y un 35 % de entrantes.
En el reporte de tiempo total, se observa que las llamadas entrantes y salientes tienen cierta equidad. En llamadas salientes se tiene un resultado de 55 horas 33 minutos y 12 segundos. Para un total de llamadas de 1952.

Se realizo ademas un testeo de vulnerabilidades las mismas que se detalladas a continuación:

Bash "ShellShock" Injection

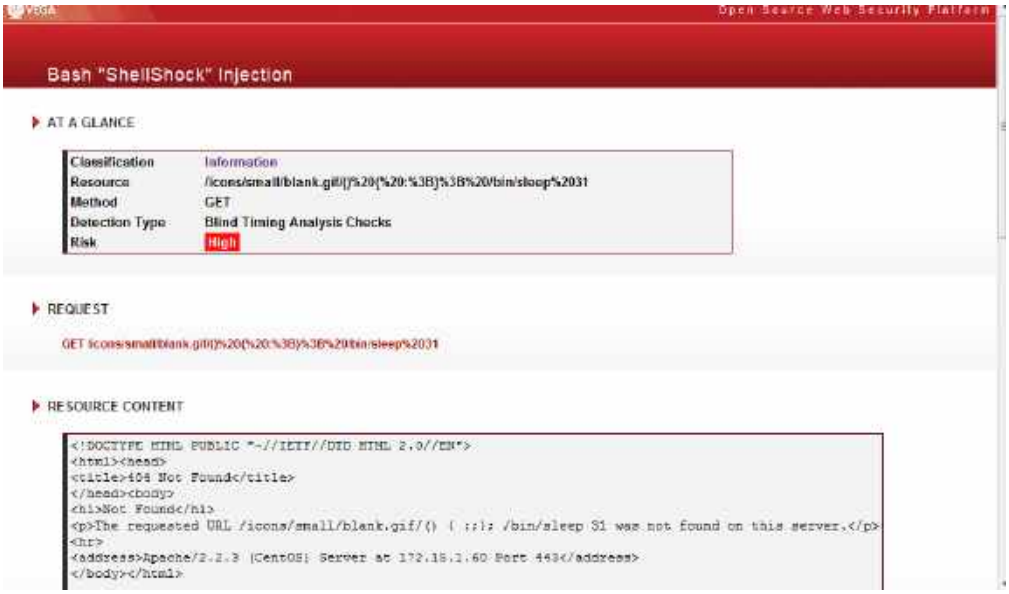


Figura 3.18: Figura que muestra Bash "ShellShock" Injection
Desarrollado por: Joel F. Allaica C.

Contenido del recurso

GET /icons/small/blank.gif/() %20{ %20: %3B} %3B %20/bin/sleep %2031

Discusión

El problema que Vega identificó se debe a una vulnerabilidad en el shell Bash. Esta vulnerabilidad puede manifestarse de forma remota en aplicaciones web si la entrada suministrada por el usuario se pasa al entorno de shell Bash, lo que puede ocurrir si los valores de encabezado o parámetro se convierten en variables de entorno locales. Si se explota con éxito, esta vulnerabilidad puede conducir a la ejecución de comandos en el host subyacente.

Impacto

Vega ha detectado una posible vulnerabilidad de inyección de comandos.
Los atacantes pueden ejecutar comandos en el servidor.
La explotación puede conducir a un acceso remoto no autorizado.

Recomendación

El shell bash debe actualizarse en el host afectado. Esto a menudo se puede hacer a través del sistema de gestión de paquetes, como apt o yum.
Los desarrolladores deben examinar el código correspondiente a la página en detalle para determinar si existe la vulnerabilidad.
Se debe evitar la ejecución de comandos del sistema a través de un intérprete de comandos, como con system ().
Si es absolutamente necesario, el desarrollador debe tener especial cuidado al validar la entrada antes de pasarla al intérprete.

HTTP Trace Support Detected

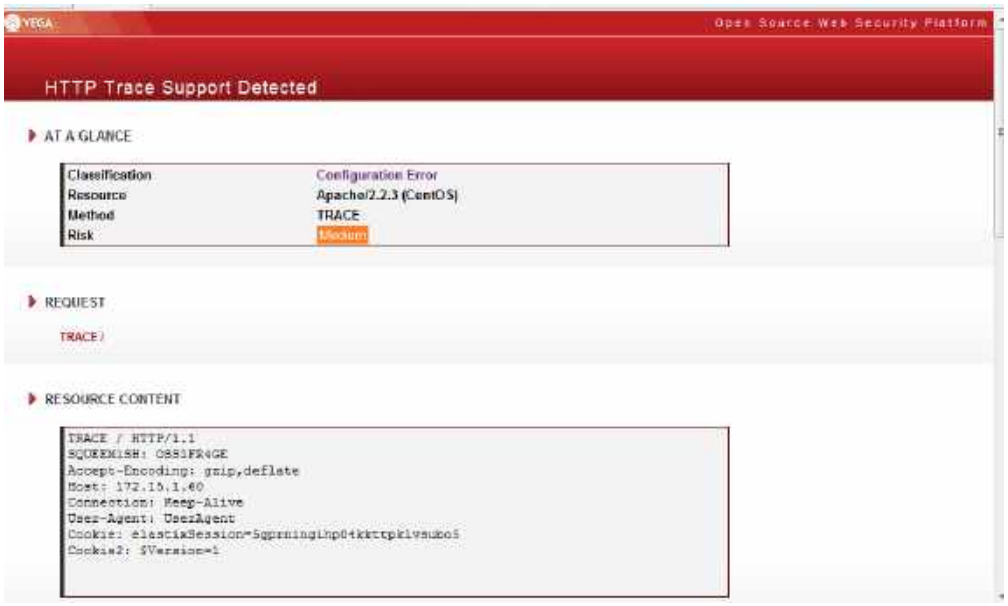


Figura 3.19: Figura que muestra HTTP Trace Support Detected
Desarrollado por: Joel F. Allaica C.

Contenido del recurso

C:\\fakepath\\

Discusión

HTTP TRACE es un método HTTP que solicita que el servidor repita la solicitud TRACE al cliente. Esto incluye encabezados que se enviaron junto con la solicitud. Se puede abusar de la compatibilidad con HTTP TRACE en escenarios en los que se ha encontrado una vulnerabilidad de secuencias de comandos entre sitios, pero no se puede explotar para recuperar los valores de las cookies porque las cookies de destino se establecen con el indicador HttpOnly. La bandera HttpOnly indica a los navegadores que no permitan el acceso a la cookie por Javascript. Si se encuentra una vulnerabilidad de secuencias de comandos entre sitios, pero la cookie de sesión está configurada HttpOnly, el soporte para HTTP TRACE abrirá una oportunidad para el robo de cookies.

Un atacante puede utilizar la vulnerabilidad de secuencias de comandos entre sitios para que el navegador del usuario objetivo emita una solicitud de RASTREO al servidor a través de XMLHttpRequest (o una función similar) y luego recupere la cookie de la respuesta, que contendrá la solicitud enviada por el navegador, incluidas las cookies.

Impacto

Permitir HTTP TRACE puede permitir el rastreo entre sitios.

Los atacantes pueden usar el rastreo entre sitios con secuencias de comandos entre sitios para recuperar el valor de las cookies HttpOnly.

Recomendación

Para los servidores basados en Apache, la directiva TraceEnable se puede usar para deshabilitar la compatibilidad con HTTP TRACE.

Para los servidores basados en IIS, la configuración del registro EnableTraceMethod controla la compatibilidad con HTTP TRACE

Form Password Field with Autocomplete Enabled

Figura 3.20: Figura que muestra HTTP Trace Support Detected
Desarrollado por: Joel F. Allaica C.

Contenido del recurso

GET /themes/blackmin/_common/login.tpl

Discusión

Vega detectó un formulario que incluía un campo de entrada de contraseña. El atributo de auto completar no estaba desactivado. Esto puede provocar que algunos navegadores almacenen valores ingresados por los usuarios localmente, donde pueden ser recuperados por terceros. Impacto Se puede almacenar un valor de contraseña en el sistema de archivos local del cliente.

Las contraseñas almacenadas localmente podrían ser recuperadas por otros usua-

rios o código malicioso.

Recomendación
La declaración del formulario debe tener un atributo de auto completar con su valor establecido en "off".

Adicional se verifica el estado de las cuentas de usuarios que tienen acceso a la central telefónica; se han cambiado la contraseña por defecto, y que las claves cuentas con los parámetros de una contraseña segura.

Después de la evaluación del PBX encontramos que se deben realizar ciertas correcciones en las configuraciones.

3.4.5. Seguridad Inalámbrica

- **Verificación de Redes Inalámbricas [802.11]**

Se ha verificado que en las instalaciones de la empresa existen únicamente las redes inalámbricas instaladas por el personal del área de sistemas, es importante considerar que dichas redes han sido instaladas para permitir el acceso, a usuarios que se dificulta el acceso mediante cable de red.

En la empresa se encuentran instalado un dispositivo Unifi que permiten el acceso inalámbrico a la red de datos. Al acceso a físico al dispositivo es compleja y difícil de ubicar para una persona no autorizada ya que se encuentra debajo del cielo razo del tercer piso.

Se verifica que se cambio de cambio de SSID por defecto del punto de acceso, ademas se encuentra deshabilitada el WPS, evitando así conectarse a las redes WiFi mediante un pin de 8 dígitos; métodos que son desarrollados bajo el concepto de evaluar el nivel de seguridad de los dispositivos pero también pueden ser usados por usuarios mal intencionados. La contraseña para conectarse al ap es segura(ver figura 3.21) garantizando así que se conecten unicamente usuarios autorizados.

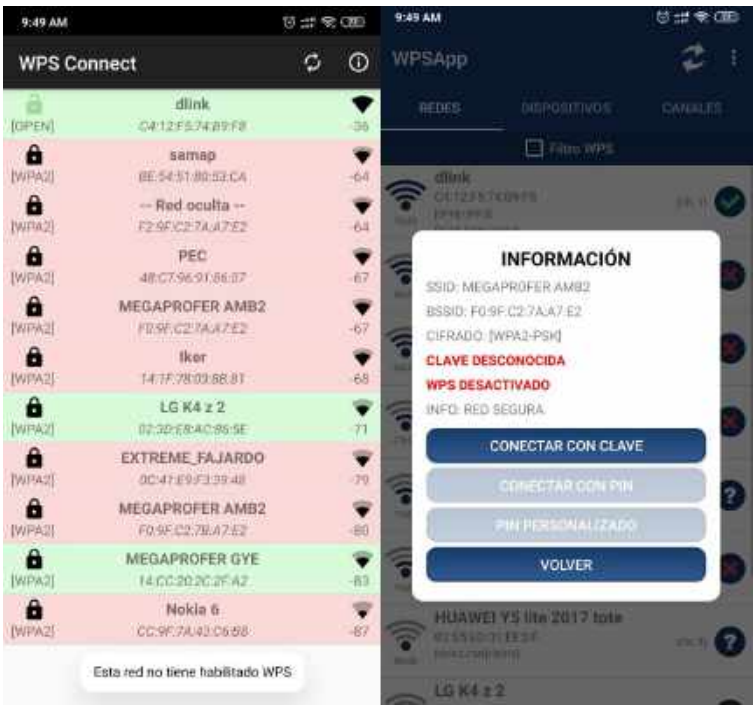


Figura 3.21: Verificación del nivel de seguridad de la red WiFi
Desarrollado por: Joel F. Allaica C.

- **Verificación de Dispositivos de Vigilancia Inalámbricos**

Se refiere a los dispositivos de seguridad que han remplazado a los alámbricos como cámaras y micrófonos. Son equipos que están completamente ocultos.
Una vez realizado la inspección necesaria, se ha determinado que no existe dispositivos de vigilancia inalámbricos, la vigilancia se lo se realiza mediante un conjunto de cámaras de seguridad alámbricos que están instaladas a nivel de toda la empresa.

3.4.6. Seguridad Física

- **Revisión de Perímetro**

Este es un método para evaluar la seguridad física de una organización y sus bienes informáticos, verificando las medidas de seguridad de su perímetro físico.

Mapa de la primera y segunda planta:

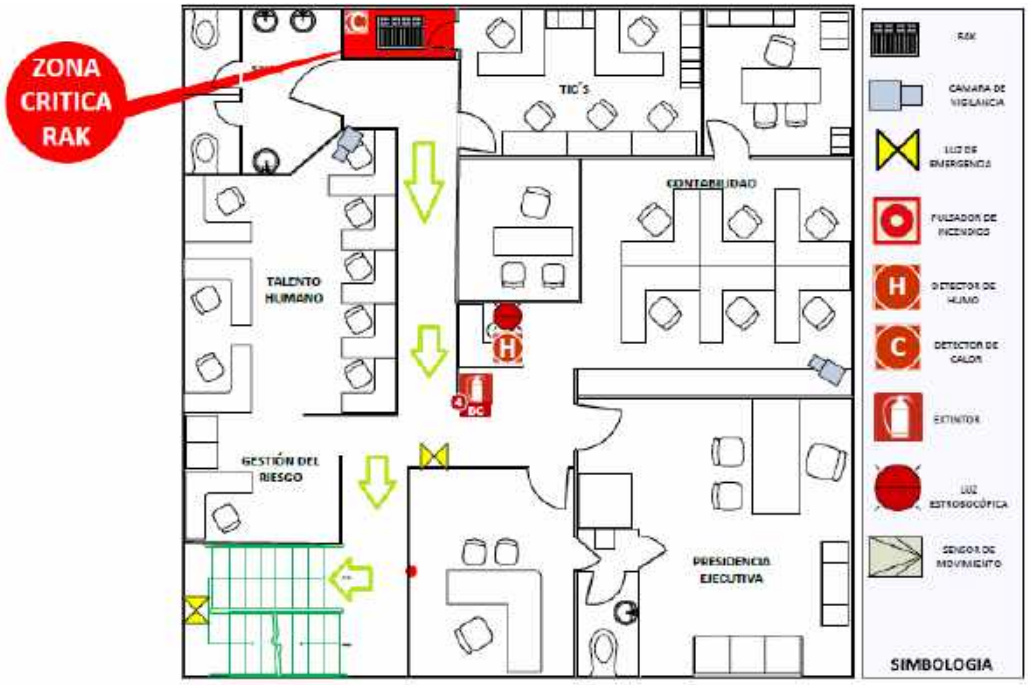


Figura 3.22: Mapa: 1ra Planta Alta
Fuente: Megaprofer S.A.

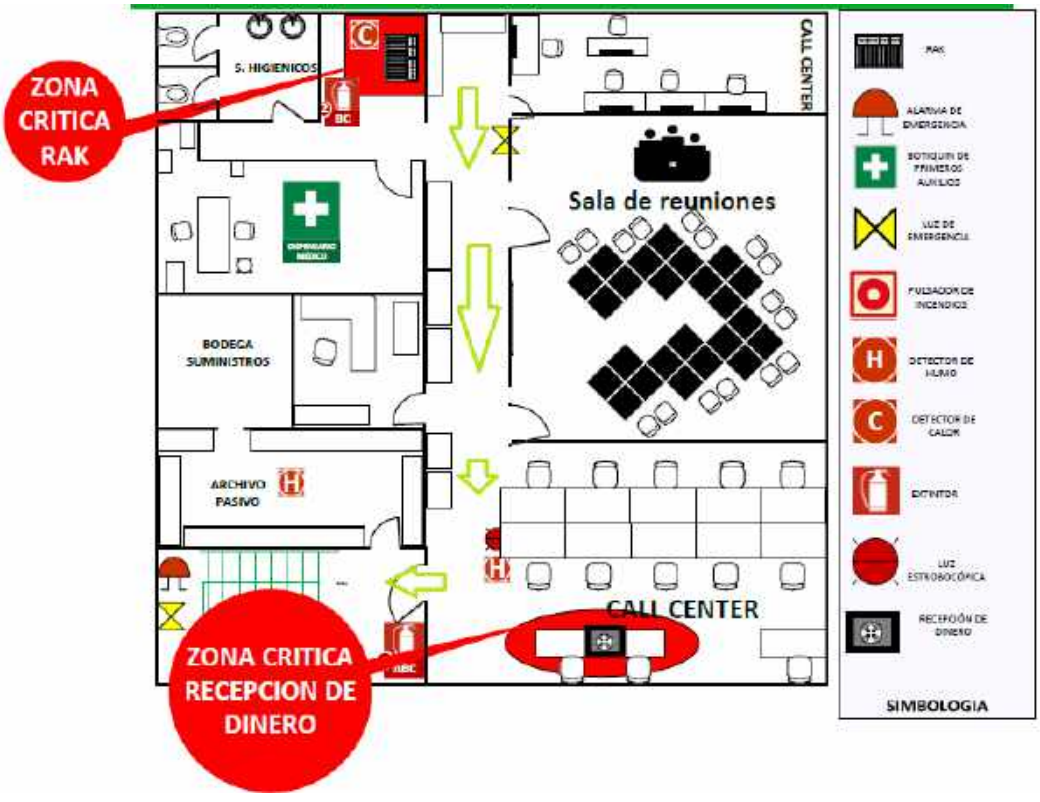


Figura 3.23: Mapa: 2da Planta Alta
Fuente: Megaprofer S.A.

Se obtuvo el mapa de evacuación en caso de emergencia en cual se detallan cada uno de los departamentos; el piso donde esta el departamento(primera planta alta), aquí se muestra las medidas de protección físicas y las rutas de acceso hacia cada uno de departamentos incluido el de sistemas.

Después de haber realizado la evaluación física del perímetro se concluye, que el perímetro físico no presenta ninguna anomalía y que la seguridad prestada es buena.

- **Revisión de monitoreo**

Este es un método para descubrir puntos de acceso monitoreos, a una organización y sus bienes, por medio del descubrimiento de custodia y monitoreo electrónico.

En la empresa cuentan con 26 cámaras de seguridad las mismas que están siendo monitoreadas constantemente por el personal de seguridad, garantizado así la seguridad del personal y de los bienes de la empresa.

- **Evaluación de Controles de Acceso**

Este es un método para evaluar los privilegios de acceso a una organización y a sus bienes a través de puntos de acceso físicos.

Una vez realizado la inspección a las instalaciones de Megaprofer S.A se ha determinado que no existe control de acceso al departamento de sistemas, no se tiene alarmas, de seguridad o algún tipo de control de acceso sofisticado. La única seguridad que se cuenta es en el Data Center, la misma esta cerrado con llave y solo el personal autorizado puede acceder.

Resumen de servicios y protocolos vulnerables

Tabla 3.20: Tabla resumen de vulnerabilidades explotables

Nro	Servicio/Protocolo	Vulnerabilidad	Explotable
1	Web	Local Filesystem Paths Found	Si
2	HTTP	Cleartext Password over HTTP	Si
3	TLS	Session Cookie Without HttpOnly Flag	Si
4	SSL/TLS	Session Cookie Without Secure Flag	Si
5	Open SSH 5.3	Métodos HTTP: TRACE habilitado	Si
6	Apache HTTP	El certificado SSL / TLS del servidor remoto expirado	Si
7	Apache SSL/TLS	Algoritmos de cifrado débiles SSH admitidos	Si
8	Apache SSH	SSH Algoritmos de MAC débiles admitidos	Si
9	TCP	Marcas de tiempo TCP habilitado	Si
10	Joomla	Es propenso a múltiples vulnerabilidades de seguridad	Si
11	PHP	Archivos llaman a la función phpinfo () que revela información potencialmente confidencial	Si
12	MySQL	Fue posible iniciar sesión con credenciales sencillas	Si
13	Post Office Protocolo (POP3)	Post Office Protocolo (POP3)	Si
14	Zimbra Collaboration Suite Persistent XSS	Vulnerabilidad de XSS persistente en Zimbra Collaboration Suite-02 de febrero	Si
15	HTML	Bash "ShellShock" Injection	Si
16	HTTP	HTTP Trace Support Detected	Si
17	HTML	Form Password Field with Autocomplete Enabled	Si
18	Portainer	Portainer es propenso a múltiples vulnerabilidades	Si

3.5. Realización de Pruebas de Penetración en un entorno controlado de manera que no se ocasionen problemas a la red

Culminada la etapa de identificación de vulnerabilidades en cada uno de los servidores de la empresa se procede con la explotación, mediante pruebas a los servicios con mayor número de vulnerabilidades encontradas en la fase anterior esto con el fin de conseguir un acceso no autorizado a los recursos o servicios sensibles de los sistemas. La pruebas de penetración se realizan un entorno virtualizado.

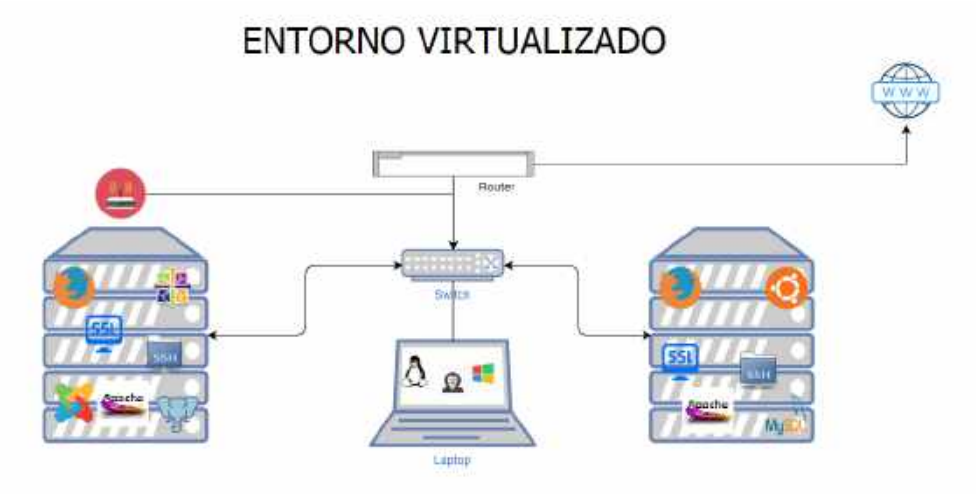


Figura 3.24: Entorno virtualizado para explotación de vulnerabilidades
Desarrollado por: Joel F. Allaica C.

Explotación de vulnerabilidades al equipo virtual CentOS

Se crea y configura una maquina virtual con similares características a los servidores CentOS de la empresa incluyendo las versiones que se manejan, donde se ejecutan los servicios de: base de datos PostgreSQL, servicio Web, FTP y SSH. Datos:

- Máquina virtual con sistema operativo kali linux con ip 192.168.0.90 (maquina auditor).
- Máquina virtual con sistema operativo CentOS 6.1 con ip 192.168.0.91 con instalaciones por defecto (maquina objetivo).

Kali linux trae entre sus herramientas Metasploit Framework, esta cuenta con varias interfaces que además de verificar vulnerabilidades, administrar evaluaciones de seguridad, permite siempre estar un paso delante de los riegos que se pueden generar. MSF tiene incluido MsfGUI, Msfconsole, Msfcli, Msfweb,

Metasploit Proy Armitage para esta fin se usa mfsconsole la cual es capaz de acceder a la mayoría de las características de la herramienta.
En la consola de kali linux se escribe msfconsole para ejecutar la herramienta, una vez iniciado se despliega en la consola los detalles de la misma como por ejemplo la versión de metasploit, cantidad de exploits, módulos auxiliares y payload existentes; ver figura 3.25.

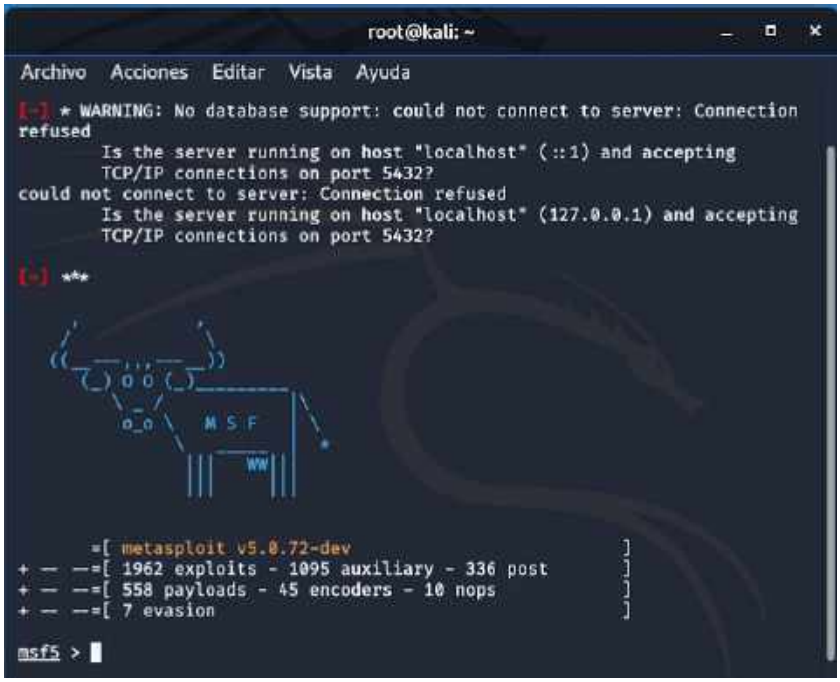


Figura 3.25: Inicio de msfconsole
Desarrollado por: Joel F. Allaica C.

Para conseguir ayuda se escribe: **help** o el símbolo interrogación hacia abajo(?). Los comandos principales para realizar un ataque de forma manual son los siguientes:

- **search:** busca módulos que contienen la característica especificada.
- **info:** indica los características del módulo especificado.
- **use:** escoge el módulo que se especifica.
- **set/unset:** configura los parámetros del módulo que se está usando.
- **exploit:** explota o inicia el módulo.
- **run:** iniciar el módulo auxiliar que se está usando.

Vulnerabilidad de configuración de PostrgreSQL por defecto

Se realizo la instalación del motor de Base de Datos PostgreSQL 9.2.24. En el cual se dejo el usuario administrador llamado **postgres**, con la clave **postgres** sin ninguna modificación adicional esto con el objetivo de explotar la configuración predeterminada del usuario postgres; para esto se utilizo un auxiliar de la herramienta.

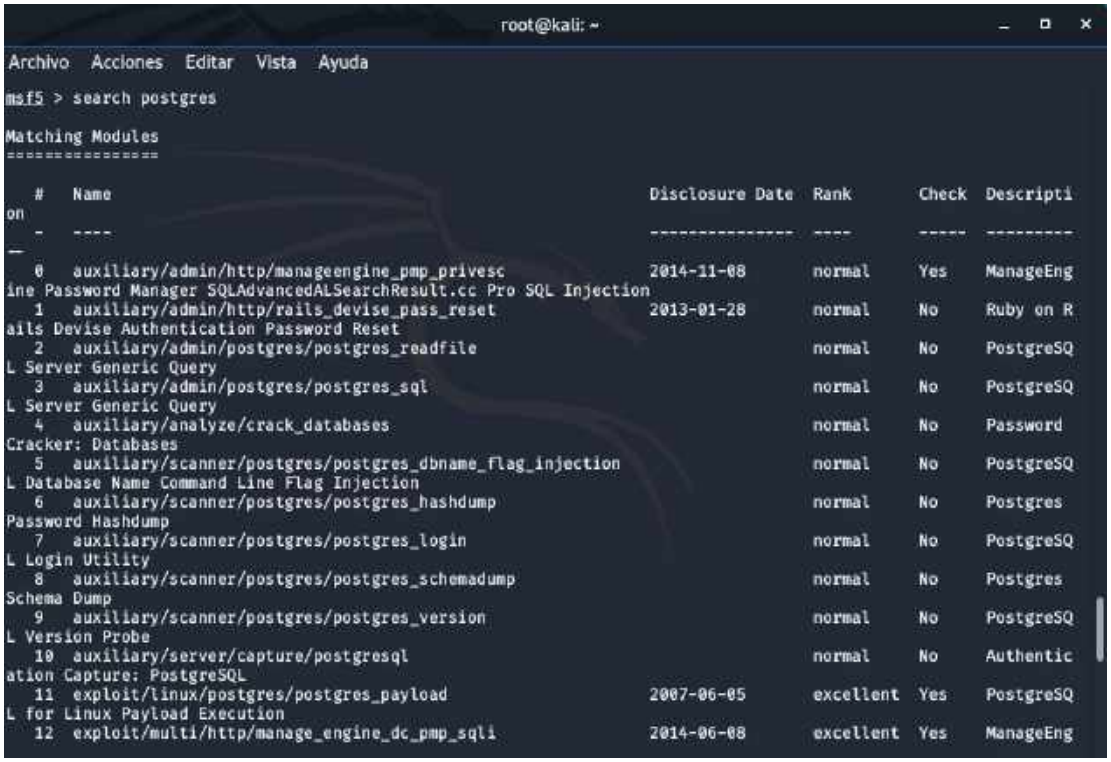


Figura 3.26: Opciones de msfconsole para postgres
Desarrollado por: Joel F. Allaica C.

En **msfconsole** se escoge el auxiliar esencial:

use auxiliary/scanner/postgres/postgres_login,

el auxiliar ya tiene pre definido los archivos de usuarios y contraseñas por defecto, se ingresa como dato necesario **RHOSTS** (objetivo)) para posteriormente ejecutar el comando **run**.

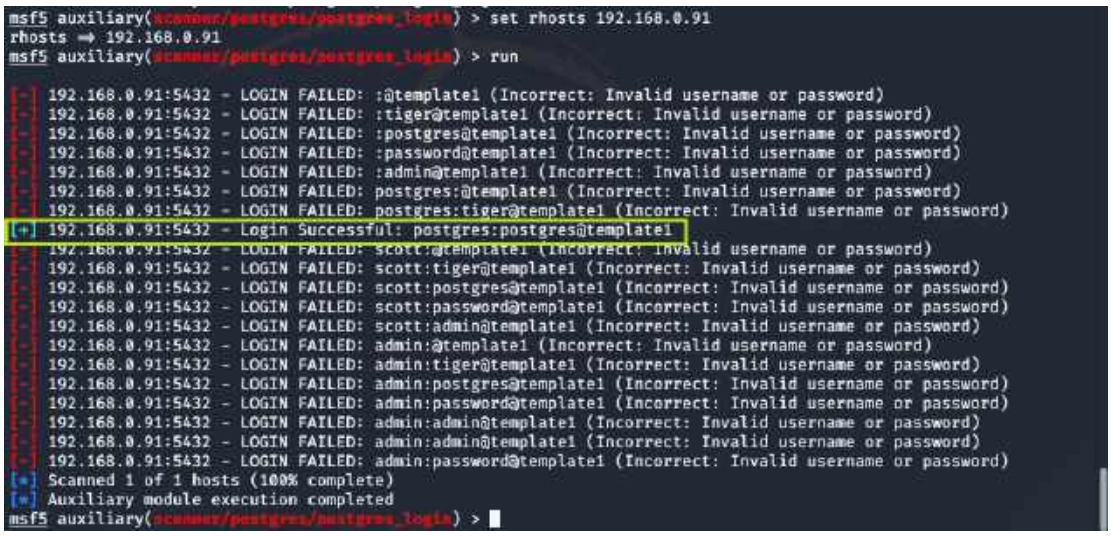


Figura 3.27: Éxito de ataque con el auxiliar postgres_login.
Desarrollado por: Joel F. Allaica C.

En la figura 3.27 se observa que se ha conseguido las credenciales para acceder a la base de datos, con los datos hallados se intente acceder al servidor mediante la siguiente sentencia **psql -h 192.168.0.91 -U postgres** donde:
psql: terminal interactivo de postgreSQL.
-h: indica la IP servidor donde esta la base de datos postgreSQL.
-U: idica el usuario: “postgres”, para este caso.

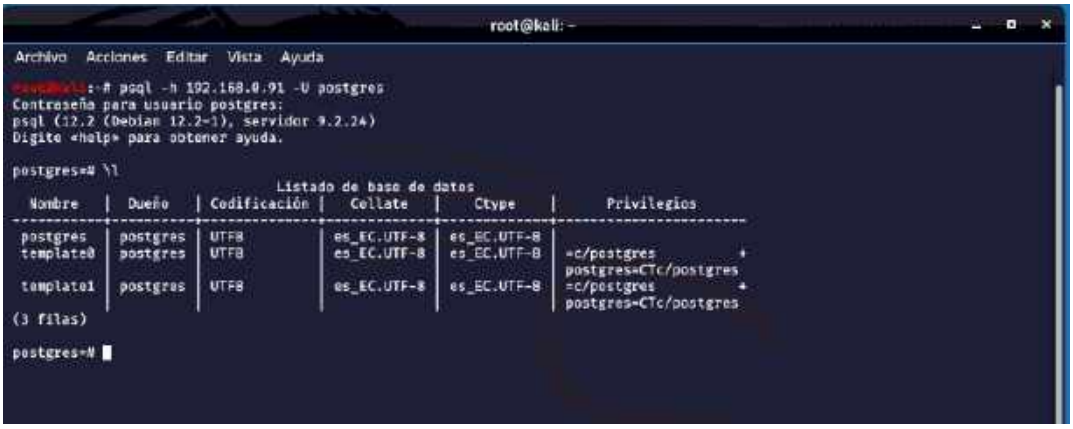


Figura 3.28: Acceso al servidor postgreSQL
Desarrollado por: Joel F. Allaica C.

En la figura 3.28 se puede observar el éxito que se tiene al iniciar sesión con el usuario administrador **postgres** y su contraseña por defecto **postgres**, una vez conectado al servidor se puede ejecutar cualquier comando **psql**. Dejando en evidencia lo fácil que puede llegar a ser tomar el control de un servidor de base de

datos que no se encuentra correctamente configurada.

Ataque de Denegación de Servicio (DoS)

En seguridad informática, también conocida como DOS(siglas en Inglés De Denial Of Service) O DDOS (de Distributed Denial Of Service), es un taque a red o un sistema de computadoras que provoca que un servicio o un recurso quede inaccesible a los usuarios legítimos, dicho objetivo se provoca mediante la saturación de los puertos con el flujo de información, logrando que servidor se sobrecargue. Esto se lo podría lograr con un número suficiente de personas recargando la web continuamente o con el uso de alguna herramienta, en este caso es Slowloris.

Slowloris es un script de Perl para realizar un tipo de ataque DDoS que trata de mantener muchas conexiones con el servidor Web de destino abierto enviando solicitudes HTTP parciales. Continúa enviando encabezados posteriores a intervalos regulares para evitar que se cierren los sockets. Es un ataque SYN-flood(una inundación), pero dirigido directamente a Apache. como resultado agotar las conexiones disponibles en un servidor.

Se realiza el ataque al Servicio Web Apache 2.2.15 por el puerto por defecto: 80 que proporciona el servidor CentOS (ver figura 3.29).

Figura 3.29: Servicio Apache en ejecutándose
Desarrollado por: Joel F. Allaica C.

Para realizar el ataque es necesario descargar el código slowloris y guardarlo como ".pl", otorgar todos los permisos (chmod 777) y ejecutar el siguiente comando

desde la consola:

perl slowloris.pl -dns 192.168.0.91 -p 80

Figura 3.30: Slowloris ejecutándose
Desarrollado por: Joel F. Allaica C.

donde:

- **-dns**: dominio, en este caso directo a la ip de la máquina
- **-p:** el puerto que se va a escanear

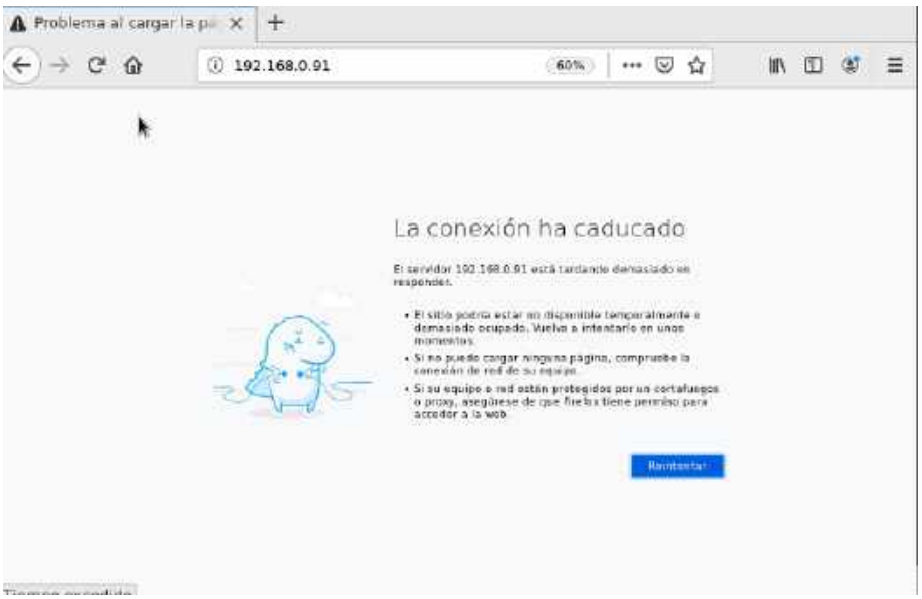


Figura 3.31: Éxito en el ataque DoS al servicio Apache
Desarrollado por: Joel F. Allaica C.

En la figura 3.31 se evidencia el éxito que tiene el ataque DoS al servicio de Web Apache gracias a la ejecución del script slowloris ocasionado que el servicio web se encuentre inaccesible.

Ataque de fuerza bruta al Servicio OpenSSH 5.3

Uno de los ataques más comunes que se realizan son los conocidos como fuerza bruta, se caracteriza por una tentativa de obtener acceso a un servicio del sistema (ssh, smtp, http, etc.), ingresando diversas combinaciones de usuarios y contraseñas basado en el método de prueba y error. Existen varios tipos de ataques el el más común el de ellos es mediante el uso de diccionario el cual tiene una base datos de usuarios y contraseñas. La efectividad de un taque de diccionario dependerá del bueno que sea al utilizarlo. Los diccionarios se las pueden encontrar en Internet los datos mas comunes utilizados por los usuarios o aquellos que viene por defecto en los servicios estas se puede personalizar con la información recopilada en relación a lo que hace la empresa y los empleados estos datos pueden ser como son números de cédulas y nombres, correos, apellidos, cargos, etc. Para este caso se crear dos diccionarios una de usuarios y otra de contraseñas donde se almacena las contraseñas por defecto y mas comunes de que se suelen configurar.

Hydra permite configuraciones más sutiles al permitir disminuir o aumentar el número de conexiones a la vez que permitirá realizar al servicio atacado. En el caso de los servicios SSH, es recomendable tener este número muy bajo. Por de-

fecto Hydra permite 36 conexiones en paralelo, sin embargo, esto también puede denegar el servicio en el ordenador. Para SSH es mejor bajar estas conexiones a una a la vez. Para permanecer en el anonimato[**?**].
En la consola de comando de kali se ejecuta lo siguiente,

hydra -L /root/usuarios.txt -P /root/passlist.txt 192.168.0.91 ssh

en donde:
-L: definir el diccionario de usarios
-P: definir el diccionario de contraseñas
ssh: el protocolo a atacar.

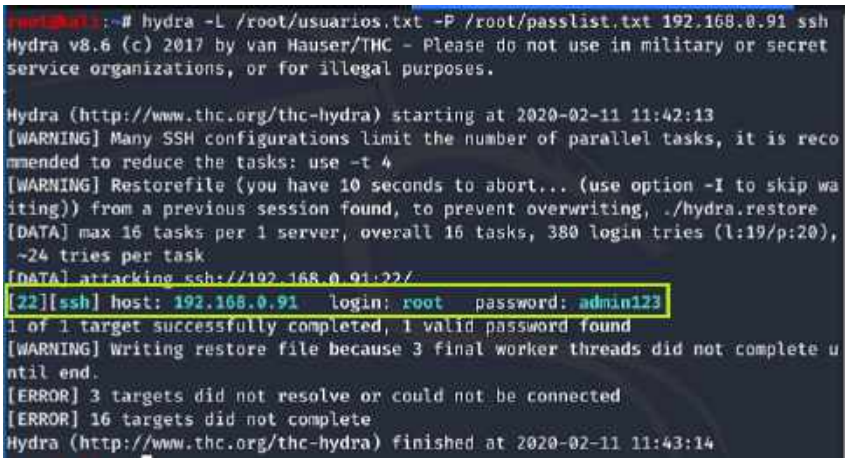


Figura 3.32: Éxito en el ataque DoS al servicio OpenSSH con Hydra
Desarrollado por: Joel F. Allaica C.

En la figura 4.43 se puede observar que el ataque tuvo éxito gracias al diccionario personalizado que de usuarios y contraseñas que se creo, esto puede llegar a tener una efectividad al 100 % como pude ser un fracaso total basado en diversos factores como: la existencia de un sistema de detección de intrusos, limite de conexiones permitidas, puerto de los servicios y por supuesto la robustez de la contraseña.

Otra de las grandes herramientas para la fuerza bruta es Medusa un software para atacar a nivel de fuerza bruta basándonos en diccionarios de palabras, es muy estable, sencillo, rápido y nos permitirá realizar el ataque a muchos servicios y también se tiene disponible en Kali. Para realizar el ataque se ejecuta lo siguiente:

medusa -h 192.168.0.193 -u root -P /root/passlist.txt -M ssh

en donde:

-h: para especificar una lista de hosts

-u: para especificar una lista de usuarios

-P: para especificar diccionario de contraseñas.

-M: el módulo que deseamos emplear

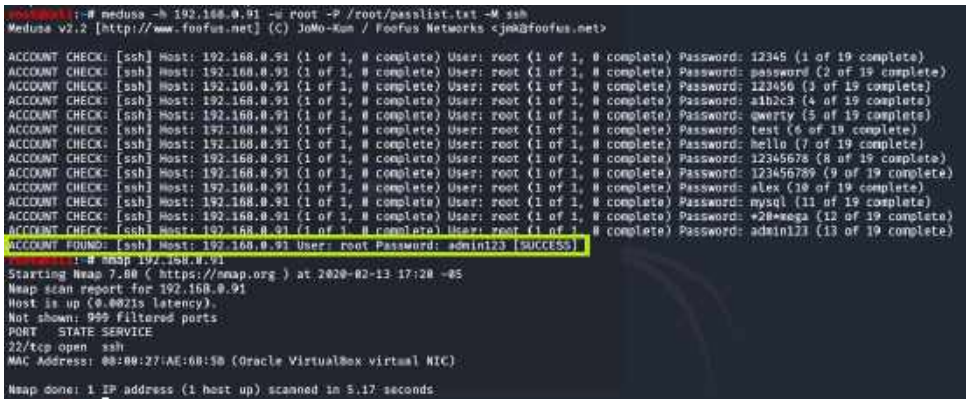


Figura 3.33: Éxito en el ataque DoS al servicio OpenSSH con Medusa
Desarrollado por: Joel F. Allaica C.

El la figura 4.44 se pude evidenciar el éxito al acceso del servicio ssh.

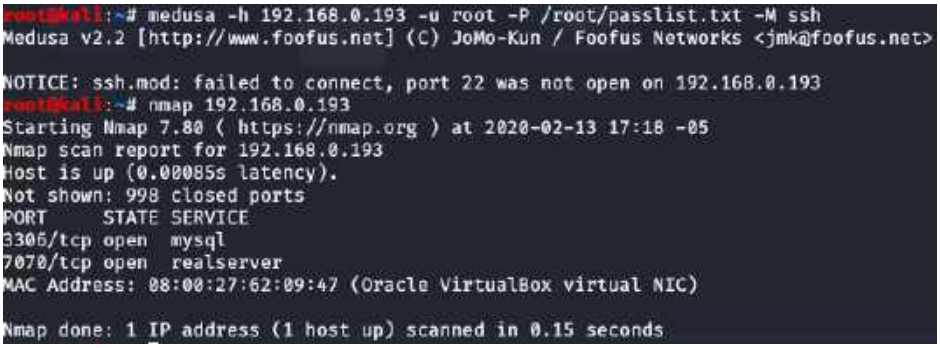


Figura 3.34: Ataque DoS al servicio OpenSSH con Medusa
Desarrollado por: Joel F. Allaica C.

Lo que no paso con el otro servidor(ver figura 3.34) que tenia el puerto por defecto del servicio ssh(22) inhabilitado

Ataque de fuerza bruta al Servicio FTP (File Transfer Protocol)

El objetivo principal de este ataque es explotar las configuraciones por defecto para lo cual se usa msfconsole junto son sus auxiliares:

auxiliary/scanner/ftp/anonymous

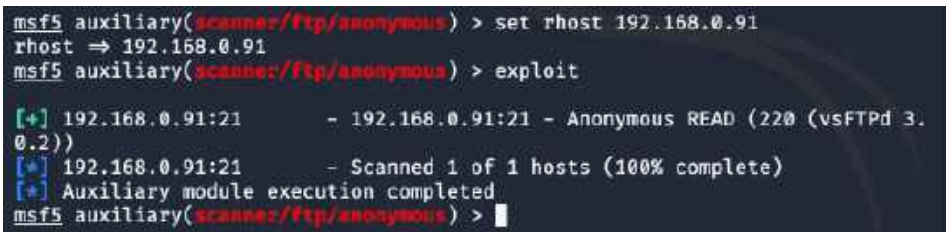


Figura 3.35: Ataque a servico FTP con msfconsole
Desarrollado por: Joel F. Allaica C.

En la Figura 4.46 se puede observar el éxito de ataque obteniendo el acceso mediante el usuario anonymous el cual no fue bloqueada en las configuraciones iniciales. Granparte del éxito del ataque fue que el ataque se lo realizo por el puerto por defecto del servicio(puerto 21).
Ademas se ejecutan pruebas con usuarios por defecto como se observa en la Figura 4.41

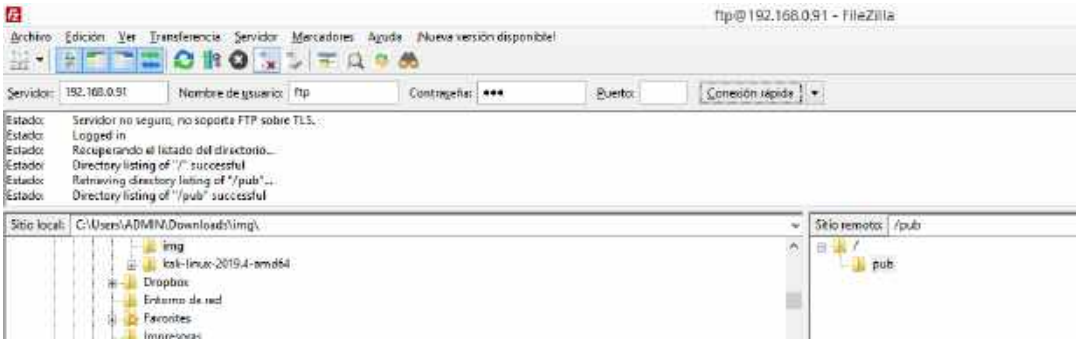


Figura 3.36: Ataque a servico FTP con msfconsole
Desarrollado por: Joel F. Allaica C.

Ataque Man-in-the-middle

Entre las técnicas de ataque que aprovechan las vulnerabilidades de los protocolos de red se encuentra la familia de ataque Man-in-the-Middle (hombre en medio). En este tipo de explotación el atacante trata de situarse entre dos terminales legítimos, haciendo que la comunicación entres ambos pasen a través de él[37].

Para llevar a cabo este ataque es necesario desviar el tráfico de la víctima al equipo del auditor y esta a su vez da paso al destino original, para el caso en estudio se utiliza dos máquinas virtuales; la víctima con sistema operativo Windows 10 y el atacante con Kali Linux. Ver Figura 3.37

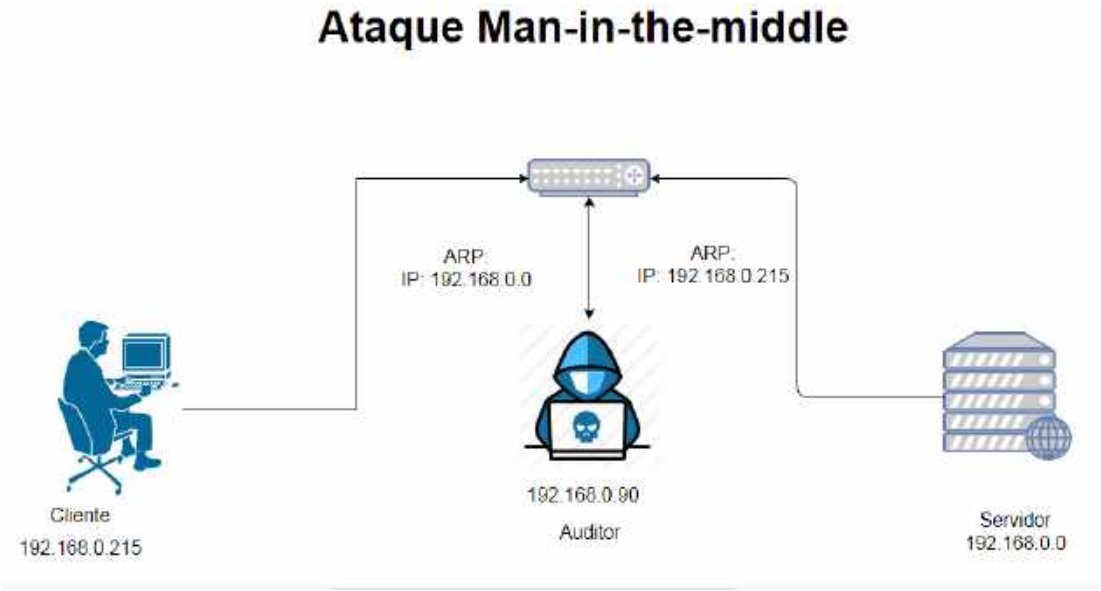


Figura 3.37: Funcionamiento de ARP Spoofing
Desarrollado por: Joel F. Allaica C.

Para ejecutar el ataque se debe habilitar el reenvío de tráfico en el equipo del auditor, esto se logra modificando ip_forwarding (modo ruteador) y ejecutando el comando:

echo 1 > /proc/sys/net/ipv4/ip_forward

Después se crea la regla para el re direccionamiento en iptables con el el siguiente comando:

iptables -t nat -A PREROUTING -p tcp –destination-port 80 -j REDIRECT –to-port 10000

La regla establecita permite que las solicitudes al puerto 80 sean redireccionadas al puerto 10000, para iniciar a descifrar todo tráfico del puerto 10000 se ejecuta el comandado:

sslstrip -l 10000 (ver figura 3.38).

Figura 3.38: Configuración de ruteo e iptables
Desarrollado por: Joel F. Allaica C.

Ahora se inicia ettercap, se elige el envenenamiento ARP, **Sniff > Sniff remote connections** que se encuentra en el menú, con su respectiva tarjeta de red. A través el escaneo de hosts se elige la IP objetivo y se lo añade a la TARGET1 y puerta de enlace se añade en la TARGET2 ; la configuración se lo realiza con el objetivo de que todo pase por la maquina del auditor después se procede al envenenamiento ARP donde se iniciar a escuchar (sniffing) la red.

En la maquina del objetivo se ingresa a sitios web seguros como son outlook, gmail, kali.org, entre otros y de las misma manera se accede a sitios sin certificados SSL.

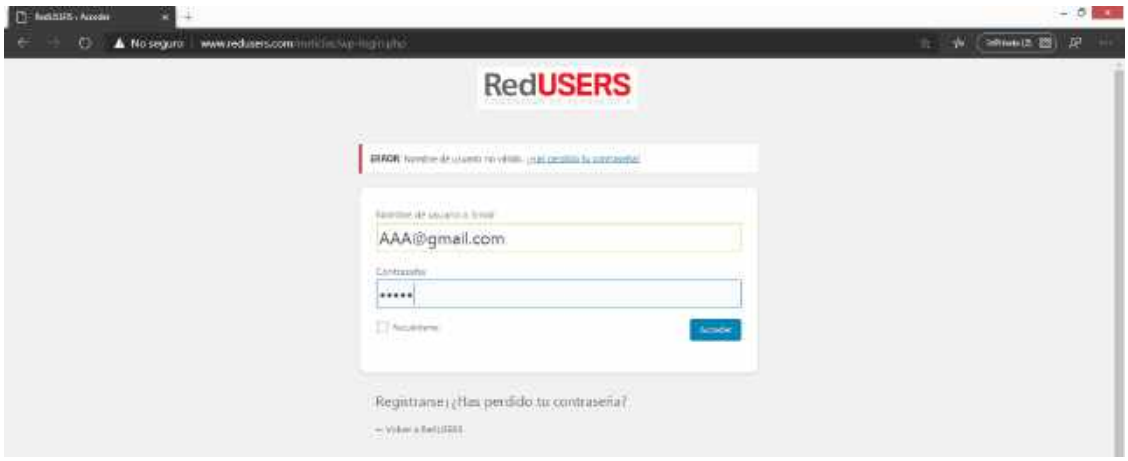


Figura 3.39: Inicio de sesión en el ordenador objetivo
Desarrollado por: Joel F. Allaica C.

En la figura 3.39 se pude evidenciar el ingreso del usuario y contraseña en un sitio sin certificado SSL desde el navegador web Chrome.

Mediante el equipo auditor se puede ver las credenciales capturada de la maquina objetivo con la herramienta Ettercap.

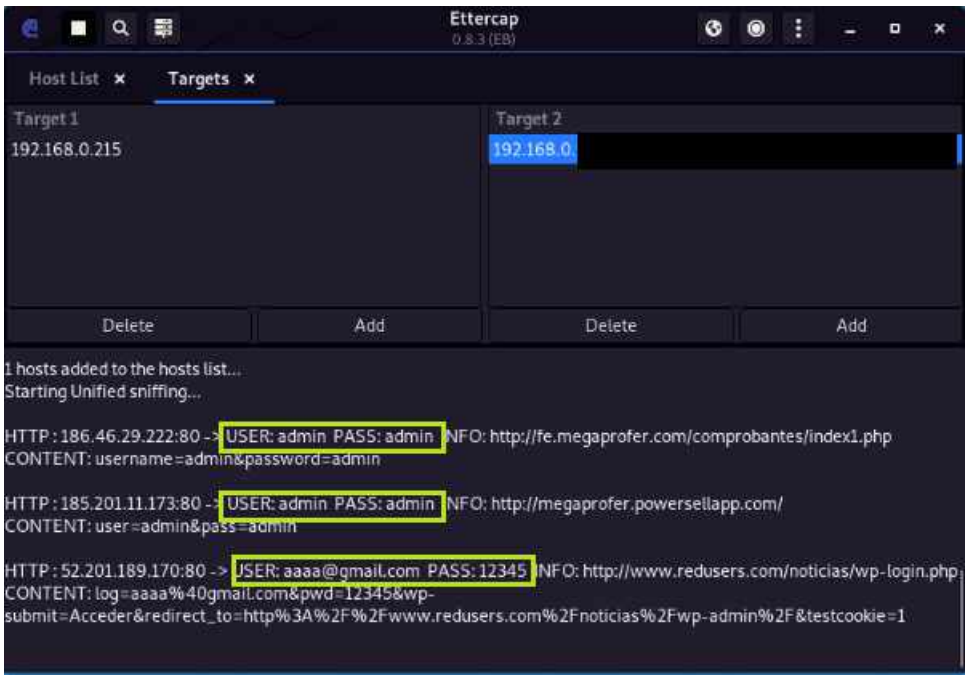


Figura 3.40: Captura de datos mediante el ataque Man-in-the-middle
Desarrollado por: Joel F. Allaica C.

En la figura 3.40 se pude ver la captura de paquetes de un sitio inseguro dando como resultados credenciales(ingresadas incorrectas a propósito) las cuales fueron ingresados por el usuario en los navegadores Chrome, Mozilla y Microsoft Edge. Dejando en evidencia el riesgo de mantener un pagina web sin un certificado de seguridad web.

Resumen de vulnerabilidades explotados

Tabla 3.21: Tabla resumen de servidos explorados

Nro	Servicio	Sistema Operativo	Ataque	Explotable
1	PostgreSQL 9.2.24	Centos 6.10	Explotación la configuración por defecto del usuario postgres	Si
2	FTP(File Transfer Protocol)	Centos 7	Explotación la configuración por defecto	Si
3	Apache Web Server	Centos 6.10	Denegación de servicio	Si
4	Open SSH 5.3	Centos 6.10	Fuerza bruta	Si
5	Open SSH 5.3	Ubuntu 16	Fuerza bruta	No
6	Navegador Chrome	Windows 10 Pro	Ataque Man-in-the-middle	Si
7	Navegador Firefox	Windows 10 Pro	Ataque Man-in-the-middle	Si
8	Navegador Microsft Edge	Windows 8.1 SL	Ataque Man-in-the-middle	Si

3.6. Elaborar Políticas de Contingencia de Seguridad Informática que ayuden a mejorar la integridad, confidencialidad y disponibilidad de la información en base a las vulnerabilidades detectadas.

3.6.1. Elaborar un informe con los estados de inseguridad detectados incluyendo soluciones prácticas encaminadas a resolverlos.

Documentación de manera detallada los resultados de las vulnerabilidades encontradas en cada uno de los servidores de la empresa incluyendo las recomendaciones y posibles soluciones para proteger los activos de la Red Informática de la empresa Megaprofer S.A. ante los daños y perjuicios que puedan ser ocasionados a partir de la explotación exitosa de las vulnerabilidades listadas.

- **Servidor fe.megaprofer.com**

Vulnerabilidad: Métodos de depuración HTTP (TRACE / TRACK) habilitados.
Riesgo: Medio
Descripción: El servidor web remoto admite los métodos TRACE y / o TRACK. TRACE y TRACK son métodos HTTP que se utilizan para depurar conexiones de servidor web.
Código CVE: CVE-2003-1567, CVE-2009-2823, CVE-2014-7883
Fecha de publicación: 15/01/2009
Explotado: No
Solución: Deshabilite los métodos TRACE y TRACK en la configuración de su servidor web.
Referencias:
http://www.kb.cert.org/vuls/id/288308
http://www.kb.cert.org/vuls/id/867593
http://httpd.apache.org/docs/current/de/mod/core.html#traceenable
https://www.owasp.org/index.php/Cross_Site_Tracing

Vulnerabilidad: El certificado SSL / TLS del servidor remoto expirado.
Riesgo: Medio
Descripción: Un atacante podría usar esto para ataques MitM(man-in-the-middle), acceder a datos sensibles y otros ataques.
Código CVE: Fecha de publicación: 15/12/2010
Explotado: No

Solución: Reemplazar el certificado SSL / TLS por uno nuevo.
Referencias:
https://docs.digicert.com/manage-certificates/renew-ssltls-certificate/

Vulnerabilidad: Algoritmos de cifrado débiles SSH admitidos.
Riesgo: Medio
Descripción: El servidor SSH remoto está configurado para permitir algoritmos de cifrado débiles o ningún algoritmo.
Código CVE: Fecha de publicación:
Explotado: No
Solución: Deshabilitar los algoritmos de cifrado débiles.
Referencias:
https://tools.ietf.org/html/rfc4253#section-6.3
https://www.kb.cert.org/vuls/id/958563

Vulnerabilidad: SSH Algoritmos de MAC débiles admitidos
Riesgo: Bajo Descripción: El servidor SSH remoto está configurado para permitir algoritmos débiles de MD5 y / o MAC de 96 bits.
Código CVE:
Fecha de publicación: 19/04/2016
Explotado: No
Solución: Deshabilitar los débiles algoritmos MAC.
Referencias: https://bettercrypto.org/
https://mozilla.github.io/server-side-tls/ssl-config-generator/
https://sweet32.info/

Vulnerabilidad: Marcas de tiempo TCP habilitado.
Riesgo: Bajo
Descripción: La desventaja de las marcas de tiempo de TCP es que los adversarios pueden calcular de forma remota el tiempo de actividad del sistema y el tiempo de arranque de la máquina y el reloj del host con una precisión de milisegundos. Estos tiempos de actividad y tiempos de arranque calculados también pueden ayudar a detectar sistemas operativos ocultos habilitados para la red, así como para vincular direcciones IP y MAC falsificadas y más.
Código CVE:
Fecha de publicación: 24/10/2008
Explotado: No

Solución: Deshabilitar las marcas de tiempo TCP.
Referencias:
http://www.ietf.org/rfc/rfc1323.txt
http://www.microsoft.com/en-us/download/details.aspx?id=9152

- **Servidor megaprofer.com**

Vulnerabilidad: El host ejecuta Joomla y es propenso a múltiples vulnerabilidades.
Riesgo: Alto
Descripción: Un atacante puede explotar estas vulnerabilidades para ejecutar código de script arbitrario, robar credenciales de autenticación basadas en cookies, revelar o modificar información confidencial, explotar vulnerabilidades latentes en la base de datos subyacente, negar el servicio a usuarios legítimos, redirigen a una víctima a un sitio potencialmente malicioso.
Código CVE: CVE-2018-15880, CVE-2018-15882
Fecha de publicación: 29/08/2018
Explotado: Si
Solución: Actualizar a Joomla a la última versión con los respectivos parches de seguridad.
Referencias:
https://developer.joomla.org/security-centre/777-20190401-core-directory-traversal-in-com-media
https://developer.joomla.org/security-centre/778-20190402-core-helpsites-refresh-endpoint-callable-for-unauthenticated-users
https://developer.joomla.org/security-centre.html
http://www.securityfocus.com/bid/105164

Vulnerabilidad: Archivo phpinfo() es visible y puede revelar información potencialmente confidencial.
Riesgo: Alto
Descripción: Parte de la información que se puede recopilar de este archivo incluye: El nombre de usuario del usuario que ejecuta el proceso PHP, si es un usuario sudo, la dirección IP del host, la versión del servidor web, la versión del sistema (Unix, Linux, Windows, ...) y el directorio raíz del Servidor web.
Código CVE:
Fecha de publicación: 13/10/2019

Explotado: Si
Solución: Eliminar los archivos enumerados o restringir el acceso a ellos.
Referencias:

Vulnerabilidad: Métodos de depuración HTTP (TRACE / TRACK) habilitados.
Riesgo: Medio
Descripción: El servidor web remoto admite los métodos TRACE y / o TRACK. TRACE y TRACK son métodos HTTP que se utilizan para depurar conexiones de servidor web.
Código CVE: CVE-2003-1567, CVE-2009-2823, CVE-2014-7883
Fecha de publicación: 15/01/2009
Explotado: No
Solución: Deshabilite los métodos TRACE y TRACK en la configuración de su servidor web.
Referencias:
http://www.kb.cert.org/vuls/id/288308
http://www.kb.cert.org/vuls/id/867593
http://httpd.apache.org/docs/current/de/mod/core.html#traceenable
https://www.owasp.org/index.php/Cross_Site_Tracing

Vulnerabilidad: El certificado SSL / TLS del servidor remoto expirado.
Riesgo: Medio Descripción: Un atacante podría usar esto para ataques MitM(man-in-the-middle), acceder a datos sensibles y otros ataques.
Código CVE:
Fecha de publicación: 15/12/2010
Explotado: No
Solución: Reemplazar el certificado SSL / TLS por uno nuevo.
Referencias:
https://docs.digicert.com/manage-certificates/renew-ssltls-certificate/

Vulnerabilidad: Algoritmos de cifrado débiles SSH admitidos.
Riesgo: Medio
Descripción: El servidor SSH remoto está configurado para permitir algoritmos de cifrado débiles o ningún algoritmo.
Código CVE: Fecha de publicación:
Explotado: No

Solución: Deshabilitar los algoritmos de cifrado débiles.
Referencias:
https://tools.ietf.org/html/rfc4253#section-6.3
https://www.kb.cert.org/vuls/id/958563

Vulnerabilidad: SSH Algoritmos de MAC débiles admitidos.
Riesgo: Bajo
Descripción: El servidor SSH remoto está configurado para permitir algoritmos débiles de MD5 y / o MAC de 96 bits.
Código CVE:
Fecha de publicación: 19/04/2016
Explotado: No
Solución: Deshabilitar los débiles algoritmos MAC.
Referencias: https://bettercrypto.org/
https://mozilla.github.io/server-side-tls/ssl-config-generator/
https://sweet32.info/

Vulnerabilidad: Marcas de tiempo TCP habilitado.
Riesgo: Bajo Descripción: La desventaja de las marcas de tiempo de TCP es que los adversarios pueden calcular de forma remota el tiempo de actividad del sistema y el tiempo de arranque de la máquina y el reloj del host con una precisión de milisegundos. Estos tiempos de actividad y tiempos de arranque calculados también pueden ayudar a detectar sistemas operativos ocultos habilitados para la red, así como para vincular direcciones IP y MAC falsificadas y más.
Código CVE:
Fecha de publicación: 24/10/2008
Explotado: No
Solución: Deshabilitar las marcas de tiempo TCP.
Referencias:
http://www.ietf.org/rfc/rfc1323.txt
http://www.microsoft.com/en-us/download/details.aspx?id=9152

- **Servidor ventas.megaprofer.com**

Vulnerabilidad: Fue posible iniciar sesión con credenciales sencillas.
Riesgo: Alto

Descripción: Una explotación exitosa podría permitir a los atacantes ejecutar código arbitrario con privilegios de administrador, pudiendo comprometer totalmente el servidor que está ejecutando la versión afectada de MySQL.
Código CVE:
Fecha de publicación: 06/09/2019
Explotado: Si
Solución: Cambiar la contraseña.
Referencias:

Vulnerabilidad: SSL / TLS: Protocolo SSLv3 Vulnerabilidad de divulgación de información en conjuntos de cifrado CBC (POODLE).
Riesgo: Medio
Descripción: El protocolo SSL 3.0, como se utiliza en OpenSSL a través de 1.0.1i y otros productos, utiliza relleno CBC no determinista, lo que facilita a los atacantes intermedios obtener datos de texto sin formato a través de un ataque de oráculo de relleno, también conocido como "POODLE " problema.
Código CVE: CVE-2014-3566
Fecha de publicación: 14/05/2014
Explotado: No
Solución: Deshabilitar SSLv3 Desactivar las suites de cifrado que admiten modos de cifrado CBC Habilitar TLS_FALLBACK_SCSV si el servicio proporciona TLSv1.0 +.
Referencias:
https://www.openssl.org/~bodo/ssl-poodle.pdf
https://www.imperialviolet.org/2014/10/14/poodle.html
https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html

Vulnerabilidad: SSL / TLS: Protocolo SSLv3 Vulnerabilidad de divulgación de información en conjuntos de cifrado CBC (POODLE).
Riesgo: Medio
Descripción: El protocolo SSL 3.0, como se utiliza en OpenSSL a través de 1.0.1i y otros productos, utiliza relleno CBC no determinista, lo que facilita a los atacantes intermedios obtener datos de texto sin formato a través de un ataque de oráculo de relleno, también conocido como "POODLE " problema
Código CVE: CVE-2014-3566
Fecha de publicación: 14/05/2014
Explotado: No

Solución: Deshabilitar SSLv3 Desactivar las suites de cifrado que admiten modos de cifrado CBC Habilitar TLS_FALLBACK_SCSV si el servicio proporciona TLSv1.0 +.
Referencias:
https://www.openssl.org/~bodo/ssl-poodle.pdf
https://www.imperialviolet.org/2014/10/14/poodle.html
https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html

Vulnerabilidad: El certificado SSL / TLS del servidor remoto expirado.
Riesgo: Medio
Descripción: Un atacante podría usar esto para ataques MitM(man-in-the-middle), acceder a datos sensibles y otros ataques.
Código CVE:
Fecha de publicación: 15/12/2010
Explotado: No
Solución: Reemplazar el certificado SSL / TLS por uno nuevo.
Referencias:
https://docs.digicert.com/manage-certificates/renew-ssltls-certificate/

Vulnerabilidad: Algoritmos de cifrado débiles SSH admitidos.
Riesgo: Medio
Descripción: El servidor SSH remoto está configurado para permitir algoritmos de cifrado débiles o ningún algoritmo.
Código CVE:
Fecha de publicación:
Explotado: No
Solución: Deshabilitar los algoritmos de cifrado débiles.
Referencias:
https://tools.ietf.org/html/rfc4253#section-6.3
https://www.kb.cert.org/vuls/id/958563

Vulnerabilidad: Marcas de tiempo TCP habilitado.
Riesgo: Bajo
Descripción: La desventaja de las marcas de tiempo de TCP es que los adversarios pueden calcular de forma remota el tiempo de actividad del sistema y el tiempo de arranque de la máquina y el reloj del host con una precisión de milisegundos. Estos tiempos de actividad y tiempos de arranque calculados

también pueden ayudar a detectar sistemas operativos ocultos habilitados para la red, así como para vincular direcciones IP y MAC falsificadas y más.
Código CVE:
Fecha de publicación: 24/10/2008
Explotado: No
Solución: Deshabilitar las marcas de tiempo TCP.
Referencias:
http://www.ietf.org/rfc/rfc1323.txt
http://www.microsoft.com/en-us/download/details.aspx?id=9152

- **Servidor amb.megaprofer.com**

Vulnerabilidad: Portainer es propenso a múltiples vulnerabilidades.
Riesgo: Alto
Descripción: La explotación exitosa de esta vulnerabilidad permitiría a un usuario autenticado obtener permiso completo en el sistema de archivos del host.
Código CVE: CVE-2019-16872, CVE-2019-16873, CVE-2019-16874, CVE-2019-16876, CVE-2019-16877, CVE-2019-16878 Fecha de publicación: 25/09/2019
Explotado: Si
Solución: Actualizar Portainer 1.22.1 o una versión superior.
Referencias:
https: //fortiguard.com/zeroday/FG-VD-19-120

Vulnerabilidad: Transmisión de texto en claro de información confidencial a través de HTTP.
Riesgo: Medio
Descripción: El software transmite datos confidenciales o críticos para la seguridad en texto sin formato en un canal de comunicación que puede ser rastreado por actores no autorizados.
Código CWE: CWE-319
Fecha de publicación:
Explotado: No
Solución: Hacer cumplir la transmisión de datos confidenciales a través de una conexión SSL / TLS encriptada. Además, asegúrese de que el host / aplicación esté redirigiendo a todos los usuarios a la conexión SSL / TLS segura antes de permitir ingresar datos confidenciales en las funciones mencionadas.
Referencias:
https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_

and_Session_Management
https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure
https://cwe.mitre.org/data/definitions/319.html

Vulnerabilidad: El certificado SSL / TLS del servidor remoto expirado.
Riesgo: Medio
Descripción: Un atacante podría usar esto para ataques MitM(man-in-the-middle), acceder a datos sensibles y otros ataques.
Código CVE:
Fecha de publicación: 15/12/2010
Explotado: No
Solución: Reemplazar el certificado SSL / TLS por uno nuevo.
Referencias:
https://docs.digicert.com/manage-certificates/renew-ssltls-certificate/

Vulnerabilidad: Algoritmos de cifrado débiles SSH admitidos.
Riesgo: Medio
Descripción: El servidor SSH remoto está configurado para permitir algoritmos de cifrado débiles o ningún algoritmo.
Código CVE:
Fecha de publicación:
Explotado: No
Solución: Deshabilitar los algoritmos de cifrado débiles.
Referencias:
https://tools.ietf.org/html/rfc4253#section-6.3
https://www.kb.cert.org/vuls/id/958563

Vulnerabilidad: Marcas de tiempo TCP habilitado.
Riesgo: Bajo
Descripción: La desventaja de las marcas de tiempo de TCP es que los adversarios pueden calcular de forma remota el tiempo de actividad del sistema y el tiempo de arranque de la máquina y el reloj del host con una precisión de milisegundos. Estos tiempos de actividad y tiempos de arranque calculados también pueden ayudar a detectar sistemas operativos ocultos habilitados para la red, así como para vincular direcciones IP y MAC falsificadas y más.
Código CVE:
Fecha de publicación: 24/10/2008

Explotado: No
Solución: Deshabilitar las marcas de tiempo TCP.
Referencias:
http://www.ietf.org/rfc/rfc1323.txt
http://www.microsoft.com/en-us/download/details.aspx?id=9152

- **Servidor mail.megaprofer.com**

Vulnerabilidad: SSL / TLS: Informe de conjuntos de cifrado 'anónimos'
Riesgo: Medio
Descripción: La configuración predeterminada de cifrado SSL en Apache Tomcat 4.1.28 a 4.1.31, 5.0.0 a 5.0.30 y 5.5.0 a 5.5.17 utiliza ciertos cifrados inseguros, incluido el cifrado anónimo, que permite a los atacantes remotos obtener información confidencial o tener otros impactos no especificados.
Código CVE: CVE-2007-1858, CVE-2014-0351
Fecha de publicación: 24/10/2007
Explotado: No
Solución: La configuración de estos servicios debe cambiarse para que ya no acepte los conjuntos de cifrado 'Anónimo'.
Referencias:
https://bettercrypto.org/
https://mozilla.github.io/server-side-tls/ssl-config-generator/

Vulnerabilidad: El certificado SSL / TLS del servidor remoto expirado.
Riesgo: Medio
Descripción: Un atacante podría usar esto para ataques MitM(man-in-the-middle), acceder a datos sensibles y otros ataques.
Código CVE: Fecha de publicación: 15/12/2010
Explotado: No
Solución: Reemplazar el certificado SSL / TLS por uno nuevo.
Referencias:
https://docs.digicert.com/manage-certificates/renew-ssltls-certificate/

Vulnerabilidad: El servidor remoto POP3 acepta inicios de sesión a través de conexiones sin cifrar.
Riesgo: Medio
Descripción: El host remoto está ejecutando un demonio POP3 que permite inicios de sesión de texto sin cifrar a través de conexiones sin cifrar.

Código CVE: Fecha de publicación: 2004
Explotado: No
Solución: Configure el servidor remoto para hacer cumplir siempre las conexiones cifradas a través de SSL / TLS con el comando 'STLS'
Referencias:
http://www.ietf.org/rfc/rfc2222.txt
http://www.ietf.org/rfc/rfc2595.txt

Vulnerabilidad: Vulnerabilidad de XSS persistente en Zimbra Collaboration Suite-02 de febrero
Riesgo: Medio
Descripción: Este host ejecuta Zimbra Collaboration Suite y es propenso a la vulnerabilidad XSS persistente.
Código CVE: CVE-2017-17703
Fecha de publicación: 17/07/2017
Explotado: No
Solución: Actualice a la versión 8.8.3 o posterior.
Referencias:
https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories

Vulnerabilidad: SSH Algoritmos de MAC débiles admitidos
Vulnerabilidad: Bajo
Descripción: El servidor SSH remoto está configurado para permitir algoritmos débiles de MD5 y / o MAC de 96 bits.
Código CVE:
Fecha de publicación: 19/04/2016
Explotado: No
Solución: Deshabilitar los débiles algoritmos MAC.
Referencias:
https://bettercrypto.org/
https://mozilla.github.io/server-side-tls/ssl-config-generator/
https://sweet32.info/

Vulnerabilidad: Marcas de tiempo TCP habilitado.
Riesgo: Bajo
Descripción: La desventaja de las marcas de tiempo de TCP es que los adversarios pueden calcular de forma remota el tiempo de actividad del sistema

y el tiempo de arranque de la máquina y el reloj del host con una precisión de milisegundos. Estos tiempos de actividad y tiempos de arranque calculados también pueden ayudar a detectar sistemas operativos ocultos habilitados para la red, así como para vincular direcciones IP y MAC falsificadas y más.
Código CVE:
Fecha de publicación: 24/10/2008
Explotado: No
Solución: Deshabilitar las marcas de tiempo TCP.
Referencias:
http://www.ietf.org/rfc/rfc1323.txt http://www.microsoft.com/en-us/download /details.aspx?id=9152

- **Servidor pedidos en línea**

Vulnerabilidad: SSL / TLS: informe de conjuntos de cifrado vulnerables para HTTPS.
Riesgo: Medio
Descripción: Los cifrados DES y Triple DES, como se usan en los protocolos TLS, SSH e IPSec y otros protocolos y productos, tienen un límite de cumpleaños de aproximadamente cuatro mil millones de bloques, lo que facilita a los atacantes remotos obtener datos de texto sin cifrar a través de un ataque de cumpleaños contra una sesión encriptada de larga duración, como lo demuestra una sesión HTTPS usando Triple DES en modo CBC, también conocido como un ataque "Sweet32".
Código CVE: CVE-2016-2183, CVE-2016-6329
Fecha de publicación: 01/09/2016
Explotado: No Solución: La configuración de estos servicios debe cambiarse para que ya no acepte los conjuntos de cifrado enumerados.
Referencias:
https://bettercrypto.org/
https://mozilla.github.io/server-side-tls/ssl-config-generator/
https://sweet32.info/

Vulnerabilidad: SSL / TLS: Protocolo SSLv3 Vulnerabilidad de divulgación de información en conjuntos de cifrado CBC (POODLE).
Riesgo: Medio
Descripción: El protocolo SSL 3.0, como se utiliza en OpenSSL a través de 1.0.1 y otros productos, utiliza relleno CBC no determinista, lo que facilita a los

atacantes intermedios obtener datos de texto sin formato a través de un ataque de oráculo de relleno, también conocido como "POODLE " problema.
Código CVE: CVE-2014-3566
Fecha de publicación: 14/05/2014
Explotado: No
Solución: Deshabilitar SSLv3 Desactivar las suites de cifrado que admiten modos de cifrado CBC Habilitar TLS_FALLBACK_SCSV si el servicio proporciona TLSv1.0 +.
Referencias:
https://www.openssl.org/~bodo/ssl-poodle.pdf
https://www.imperialviolet.org/2014/10/14/poodle.html
https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html

Vulnerabilidad: El certificado SSL / TLS del servidor remoto expirado.
Riesgo: Medio
Descripción: Un atacante podría usar esto para ataques MitM(man-in-the-middle), acceder a datos sensibles y otros ataques.
Código CVE:
Fecha de publicación: 15/12/2010
Explotado: No
Solución: Reemplazar el certificado SSL / TLS por uno nuevo.
Referencias:
https://docs.digicert.com/manage-certificates/renew-ssltls-certificate/

Vulnerabilidad: Algoritmos de cifrado débiles SSH admitidos.
Riesgo: Medio
Descripción: El servidor SSH remoto está configurado para permitir algoritmos de cifrado débiles o ningún algoritmo.
Código CVE:
Fecha de publicación:
Explotado: No
Solución: Deshabilitar los algoritmos de cifrado débiles.
Referencias:
https://tools.ietf.org/html/rfc4253#section-6.3
https://www.kb.cert.org/vuls/id/958563

Vulnerabilidad: SSH Algoritmos de MAC débiles admitidos.

Riesgo: Bajo
Descripción: El servidor SSH remoto está configurado para permitir algoritmos débiles de MD5 y / o MAC de 96 bits.
Código CVE:
Fecha de publicación: 19/04/2016
Explotado: No
Solución: Deshabilitar los débiles algoritmos MAC.
Referencias:
https://bettercrypto.org/
https://mozilla.github.io/server-side-tls/ssl-config-generator/
https://sweet32.info/

Vulnerabilidad: Marcas de tiempo TCP habilitado.
Riesgo: Bajo
Descripción: La desventaja de las marcas de tiempo de TCP es que los adversarios pueden calcular de forma remota el tiempo de actividad del sistema y el tiempo de arranque de la máquina y el reloj del host con una precisión de milisegundos. Estos tiempos de actividad y tiempos de arranque calculados también pueden ayudar a detectar sistemas operativos ocultos habilitados para la red, así como para vincular direcciones IP y MAC falsificadas y más.
Código CVE:
Fecha de publicación: 24/10/2008
Explotado: No
Solución: Deshabilitar las marcas de tiempo TCP.
Referencias:
http://www.ietf.org/rfc/rfc1323.txt
http://www.microsoft.com/en-us/download/details.aspx?id=9152

- **Servidor central telefónica**

Vulnerabilidad: Bash "ShellShock" Injection.
Riesgo: Alto
Descripción: Esta vulnerabilidad puede manifestarse de forma remota en aplicaciones web si la entrada suministrada por el usuario se pasa al entorno de shell Bash, lo que puede ocurrir si los valores de encabezado o parámetro se convierten en variables de entorno locales.
Los atacantes pueden ejecutar comandos en el servidor.

La explotación puede conducir a un acceso remoto no autorizado.
Código CVE: CVE-2014-6271
Fecha de publicación: 24/09/2014
Explotado: No
Solución: El shell bash debe actualizarse en el host afectado.
Se debe evitar la ejecución de comandos del sistema a través de un intérprete de comandos, como con system ().
Referencias:
https://blog.qualys.com/securitylabs/2014/09/24/bash-remote-code-execution-vulnerability-cve-2014-6271

Vulnerabilidad: Vulnerabilidad del método HTTP TRACE XSS.
Riesgo: Bajo
Descripción: El servidor web admite los métodos TRACE y/o TRACK. Los servidores que admiten este método están sujetos a ataques de scripting entre sitios cuando se utilizan junto con varias debilidades en los navegadores.
Código CVE: CVE-2003-1567, CVE-2004-2320, CVE-2007-3008, CVE-2010-0386
Fecha de publicación:
Explotado: No
Solución: Deshabilite los métodos TRACE y TRACK.
Soluciones específicas del producto: IIS: Use el análisis de URL de Microsoft para evitar estos dos métodos
Apache 2.0: Modifique el archivo security.conf ubicado en /etc/apache2/conf.d/security y establezca la opción Track en Off
Referencias:
http://www.cert.org/advisories/CA-2000-02.html
https://cve.mitre.org/data/downloads/allcves.html
http://www.securityfocus.com/bid/5986/solution

3.6.2. Elaboración de la propuesta de Políticas de Contingencia de Seguridad Informática que resguarde los activos informáticos asociados a los procesos de la empresa Megaprofer S.A.

Por el análisis de la situación actual, prueba de vulnerabilidades y ataques realizados, se procede a crear las siguientes Políticas de Contingencia de Seguridad Informática, que permitieran corregir las deficiencias en el departamento de sistemas, proteger la información con todos los activos informáticos y establecer

directrices para afrontar los posibles riesgos de la empresa.

La Dirección de TICs a través de su personal serán los encargados del cumplimientos de estas.

Seguridad personal y equipos tecnológicos
Política Dirigida a: Todos
Ambientes de Seguridad: Todos
Política para concientización, formación y capacitación en seguridad de la información.

- Todos los colaboradores de la empresa y donde sea relevante, contratistas y usuarios de terceros deberían recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos corporativos que sean notables para la función de su trabajo.
- El Departamento de Sistemas debe realizar reuniones, conferencias y/o charlas en las cuales den a conocer de las nuevas amenazas en lo que a Seguridad Informática se refiere.
- Todos los colaboradores deben recibir capacitaciones acerca del uso correcto de las nuevas herramientas informáticas, plataformas y aplicativos implementados a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.

Política ante el mal uso de activos informáticos

- Los usuarios deben comprometerse con la corporación y de ser el caso firmar un acuerdo de confidencialidad y el uso adecuado de los activos informáticos.
- El mal uso de los recursos informáticos que sea detectado será reportado a los departamentos correspondientes para tomar las medidas correctivas de manera inmediata.
- Los usuarios finales deben estar debidamente informados sobre las acciones que constituyen infracciones de seguridad informática y que tales infracciones serán registradas.

Políticas para el manejo de equipos tecnológicos asignados

- Los equipos entregados son herramientas para facilitar el trabajo por lo que el uso del software instalado debe estar relacionado a los fines corporativos, cualquier otro programa o aplicativo de multimedia, entretenimiento o streaming quedan prohibidos.
- Evitar por completo almacenar contactos, fotos, videos u otro contenido de índole personal.
- Al detectarse cualquier mal funcionamiento debe remitirse al proceso de TIC para derivarse al servicio técnico autorizado y de ser necesario aplicarse la garantía.
- En el caso de personal administrativo si es necesario el uso de equipos Megaprofer fuera de las instalaciones de la empresa, esta situación debe ser notificada al proceso de TIC por parte del jefe directo del empleado para autorizar la salida del equipo, cabe recalcar que en todo momento el equipo es responsabilidad del usuario.
- Los equipos tienen cuentas establecidas por el proceso de TIC, el usuario no debe cambiar las configuraciones o eliminarlas.
- El usuario tiene la obligación de proteger todos los equipos informáticos que se encuentren bajo su administración, aún cuando no se utilicen y contengan información reservada o confidencial.
- Las computadores, laptops o dispositivos móviles deberán estar protegidos mediante una clave.
- Los equipos deben permanecer bloqueados, si el colaborador no se encuentra en su puesto de trabajo.
- Los funcionarios que se desvinculen y los contratistas que culminen su vínculo con Megaprofer S.A, deberán hacer la entrega formal de los equipos asignados, así como de la totalidad de la información electrónica que se produjo y se recibió con motivo de sus funciones y actividades, como requisito para la liquidación de su contrato.

Política de administración de contraseñas

- Es responsabilidad del usuario garantizar la fortaleza de sus contraseñas.
- Las contraseñas de los aplicativos de la corporación deberán ser cambiadas cada 60 días.

- Queda expresamente prohibido que las contraseñas o datos confidenciales se encuentren de forma legible en lugares donde personas ajenas a la corporación puedan verlas.
- Las contraseñas deben contener un mínimo de ocho (8) caracteres y debe contener al menos una letra mayúscula, una letra minúscula, un número y un carácter especial (+-*/@#$%&). No debe contener vocales tildadas, ni eñes, ni espacios. Nunca usar secuencias de sólo números, minúsculas o mayúsculas.
- Evitar que la contraseña contenga: nombres de familiares, fechas especiales, lugares visitados, secuencias como 123456 o qwerty, etc.
- Las contraseñas iniciales de acceso a los aplicativos u equipos que le sea asignada deben ser cambiadas la primera vez que acceda a estos.

Política de administración cuentas y accesos empresariales

- Queda expresamente prohibido compartir los usuarios y contraseñas de cualquier cuenta asignada por Megaprofer a terceros.
- Las cuentas de mensajería deben estar limitadas a contactos laborales y colaboradores de la empresa, de la misma manera se debe evitar a toda costa transmitir contenidos que puedan afectar a la imagen de la empresa.
- Las cuentas de mensajería no deben usarse para envío masivo de mensajes, material de uso no institucional o innecesario (entiéndase contenido como cadenas, publicidad y propaganda comercial, política o social, etc.).
- En caso de ser necesario el acceso a un nuevo rol en alguno de los aplicativos administrados por el proceso de TIC, el jefe directo del empleado debe solicitarlo por correo electrónico al proceso.
- El Departamento de Sistemas debe manejar un estándar para la creación de las cuentas de los usuarios administrados por el proceso.
- El Departamento de Sistemas debe desactivar y bloquear todas las cuentas de los aplicativo administrados por el proceso de TIC en caso de que un colaborador se desvincule.

Política para la confidencialidad de la información

- Queda prohibido difundir información sensible o esencial para el funcionamiento de la empresa por cualquier medio.
- La información de la empresa bajo ningún concepto podrá copiarse o distribuirse en cuentas de correo o almacenamiento remoto de índole personal.
- Está prohibido eliminar de manera deliberada la información de las unidades compartidas, o de los recursos informáticos asignados.
- Los computadores portátiles(laptops) con información sensibles deben emplear el cifrado de los discos duros para proteger todos los archivos.

Política ante el uso de dispositivos externos.

- La utilización de dispositivos externos debe realizarse previa justificación y autorización del departamento correspondiente.
- Los usuarios que dispongan bajo su custodio dispositivos externos serán responsables del correcto uso que se le dé dentro y fuera de la empresa.
- Queda expresamente prohibido conectar dispositivos que contengan algún tipo de código malicioso como virus, gusanos o caballos de troya que puedan dañar el correcto funcionamiento de los equipos.

Seguridad Física Política
Dirigida a: Todos
Ambientes de Seguridad: Todos
Políticas de seguridad física y ambiental

- El o los Data Center deberán contar con sistema de protección contra incendios, control de temperatura (aire acondicionado) permanente a una temperatura no superior a 22 grados centígrados y un sistema eléctrico de respaldo (UPS).
- Se debe seguir los estándares de protección eléctrica vigentes para minimizar el riesgo de daños físicos de los equipos de telecomunicaciones y servidores.

- Los equipos que hacen parte de la infraestructura tecnológica, tales como servidores, estaciones de trabajo, centro de cableado, UPS, dispositivos de almacenamiento, entre otros, deben estar protegidos y ubicados en sitios libres de amenazas como robo, incendio, inundaciones, humedad, agentes biológicos, explosiones, vandalismo y terrorismo.
- Los usuarios no deben mover o reubicar los equipos de cómputo o de telecomunicaciones, ni retirar sellos de estos sin la autorización del personal de TIC, debiéndose solicitar a la misma en caso de requerir este servicio.

Política de seguridad de área restringida

- El ingreso de terceras personas a áreas restringidas en todo momento debe ser vigilado.
- El acceso donde se almacenan equipos informáticos y se procesan datos del proceso de TIC no es accesible al público todo el tiempo, el ingreso a las mismas debe ser con la autorización o vigilancia del personal del departamento de sistemas.
- El área donde se almacena la información sensible deberá estar ubicado en un lugar que no esté expuesto riesgos físicos y acceso al público.

Administración de Operaciones de Cómputo
Política Dirigida a: Todos
Ambientes de Seguridad: Todos
Política de uso de software

- Los usuarios no pueden instalar software que no esté autorizado por el proceso de TIC y de ser el caso en que lo requieran deberán justificar y pedir autorización para su instalación.
- Se restringe la instalación de software de dudosa procedencia por los riesgos que traen consigo en el caso que lo hicieran.

Política para el uso de redes

- Las redes fijas o móviles facilitadas por Megaprofer deben usarse dentro del ámbito laboral, lo que involucra que, bajo ningún concepto acceder a páginas de contenido de redes sociales personales, páginas de entretenimiento, pornográfico, juegos de azar, armas, denudes, alcohol, contenido ilegal,
- En el caso de detectarse un mal uso de la red para fines recreacionales o ilícitos, el proceso de TIC debe notificar a la gestión de Talento Humano para proceder a las sanciones respectivas.
- Queda prohibido la ejecución de software el cual realice cualquier tipo de exploración y/o analizador de la red informática de Megaprofer sin la autorización del proceso correspondiente. Considerar como ataque la ejecución de herramientas de auditoría informática detectar y explotar una posible vulnerabilidad.
- Se prohíbe el uso de herramientas de software o hardware que infrinja la integridad o los controles de Seguridad Informática.
- El Departamento de Sistemas juntamente con los directivos del corporativo determinará los estándares para los contenidos considerados como oficiales para uso laboral y administrativo. Cualquier otra página o sitio web puede ser bloqueado sin necesidad de comunicación al usuario.

Seguridad para servidores y aplicativos
Política Dirigida a: Personal Técnico y Dirección de TIC
Ambientes de Seguridad: Todos
Política ante Sistemas desactualizados

- Instalar un sistema que garantice la protección y estabilidad del servicio.
- Aplicar constantemente los parches de seguridad que se publica por parte de los fabricantes y desarrolladores después del lanzamiento del producto.

Política ante Software desactualizado

- Decretar uno o varios responsables que verifique las nuevas actualizaciones o vulnerabilidades que se presenten en el software de uso cotidiano.

- Las aplicaciones utilizadas en la empresa se deben actualizar a sus versiones estables con sus respectivos parches de seguridad instalados, estén conectados a la red o no.
- Verificar las actualizaciones del sistema operativo y los navegadores instalados.

Política ante certificados de seguridad caudados.

- Todos los aplicativos Web deben contar con un certificado de seguridad (SSL) activo y actualizado.
- El acceso paginas sin un certificado SSL debe ser a través de una Red Privada Virtual(VPN).

Política de seguridad de equipos

- En Departamento de Sistemas deberá llevar un control total y sistematizado de los recursos tecnológicos tanto de hardware como de software.
- Las contraseñas de los usuarios administradores de las plataformas tecnológicas y sistemas de información de la corporación deben ser salvaguardadas por el proceso de TIC en un archivo o aplicativo con técnicas de cifrado de datos u otro mecanismo seguro.
- El jefe encargado de TIC debe verificar el cambio de contraseñas y el cumplimiento de la política de administración contraseñas en los servidores y aplicativos de la empresa, el cumplimento de la política debe ser registrado.
- El mantenimiento lógico preventivo a los equipos de cómputo se debe realizar cada 6 meses y mantenimiento físico preventivo mínimo una vez por año, esta debe incluir el cableado estructurado.
- El proceso de TIC debe elaborar el plan y cronograma de mantenimientos, el cual será notificado a los usuarios.
- Todos los equipos de cómputo deben tener instalado un Antivirus proporcionada por el Departamento de Sistema y con su respectiva licencia de ser el caso.

Política ante pérdida de información

- El respaldo de los bases esenciales utilizados por los sistemas informáticos de la empresa se deben realizar de manera diaria.
- Manejar mínimo dos (2) copias de seguridad y tres versiones anteriores de los respaldos de seguridad.
- Uno de los respaldos se debe almacenar en un sitio externo a la empresa de manera comprimida(recomendación).
- Todos los sistemas de aplicaciones que manejen información sensible de la empresa deben generar registros de bitácoras que capten toda adición, cambio y eliminación de dicha información.
- El jefe encargado de TIC debe realizar de manera semanal las pruebas de legibilidad de los documentos con información sensibles. La comprobación se de manera aleatoria en cualquiera de los medios de respaldos realizados, los resultados deberán ser registrados.
- Los colaborados del proceso de TIC no deben eliminar los registros o la información que sea potencialmente importante, sin la previa autorización específica de la dirección del proceso.
- La Dirección de Tecnologías de la Información y la Comunicación debe prepara y mantener de planes de contingencia política.

Política ante configuraciones por defecto

- Para toda transferencia de archivos a un servidor se deben usar protocolos de seguridad (SFTP, FTPS, SFTP). Además, es recomendable revisar las políticas de seguridad de los productos, logs de incidencias y realizar un monitoreo frecuentemente de las alertas.
- Realizar la configuración de un nuevo dispositivo móvil o un sistema operativo de forma manual dejando activos solamente los servicios que vaya a utilizarse, eliminar las configuraciones por defecto.
- Configurar las aplicaciones y los servicios de red mediante un hardening del sistema operativo o servicio.

- Cifrar información sensible o generar nombres de usuario y perfiles propios. Proteger la cuenta de administrador mediante la creación y asignación de usuarios y roles.

CAPÍTULO IV

Conclusiones y Recomendaciones

CONCLUSIONES

- El correcto funcionamiento de una empresa depende de la eficiencia de los sistemas que tiene implementado, para ellos es necesario mantener sistemas informáticos estables y libres de vulnerabilidades o fallas.

- En el estudio de estado actual de la empresa se pudo constatar que la información que maneja Megaprofer S.A. es bastante delicada y está en constante crecimiento pero no tienen implementado herramientas o procesos actualizados para garantizar el correcto funcionamiento de los sistemas, así como para la detección de vulnerabilidades y la explotación de estas, dejando abierta la brecha para los atacantes informáticos.

- Una vez realizado el diagnóstico de la red, se pudo evidenciar los inconvenientes que se tienen a nivel de seguridad, y basados en el objetivo del proceso de TICs es que mantener la continuidad del servicio, del cual depende el desarrollo normal de las actividades empresa, se elaboró una propuesta de políticas de contingencia que ayuden a mejorar los servicios implementados y aquellos que se vaya a adquirir.

- La explotación de vulnerabilidades se lo realizo en ambientes virtualizados con el fin de evitar daños irreparables o posibles perdidas de datos en el servidor de la empresa. Además, se utiliza herramientas libres evitando de esta forma gastos extras en la investigación así también recomendar la implementación definitiva de estas para la detección de fallos en la empresa.

- Los módulos de la metodología OSSTMM fueron seleccionados de manera acertada, ya que se pudo cumplir con los objetivos del proyecto, teniendo éxito y llegando a detectar vulnerabilidades existentes en los servidores de la empresa; mediante estos resultados se pudo plantear medias y políticas de seguridad acordes a las necesidad de la empresa en lo referente a seguridad informática.

- Al realizar el análisis de la metodología se pudo determinar que no todos los módulos y todas las actividad descritas en el manual se pueden desarrollar debido a que la empresa no tiene implementado todos los recursos y sistemas que se indica estudiar o a su vez estas no son necesarias para flujo normal de Megaprofer.

RECOMENDACIONES

- Se recomienda mejorar las políticas de contingencia de seguridad informática planteadas con fin de mantener el óptimo funcionamiento de sus servicios y ayuden al cumplimiento de las metas empresariales. Estas deben ser actualizadas constantemente basado en la evolución de la tecnología.

- Mantener constantes capacitaciones en cuanto a la seguridad informática y realizar evaluaciones del correcto funcionamiento de los recursos informáticos para determinar las mejores prácticas relacionadas a reducir vulnerabilidades y errores de usuario final.

- Se sugiere al jefe del departamento de sistemas asignar personal responsable para estudio de herramientas de seguridad informática y posterior implementación de la administración de seguridad en los distintos servicios que ayuden a la detección de vulnerabilidades y corrección de errores, las mismas que deben ser ejecutados periódicamente en la red informática de la empresa.

- Se recomienda actualizar de manera urgente la capa de conexión segura (SSL), parches de seguridad y realizar el cambio de contraseñas de los distintos servidores.

Bibliografia

[1] B. D. Nuela Guananga, "Auditoria de la Seguridad Informática para el Honorable Gobierno Provincial de Tungurahua Mediante la Metodología Open Source Security Testing Methodolog y Manual," p. 171. Trabajo de Graduación, Fac. de Ing. en Sis. Elec. e Ind., Univ. Tec. de Ambato, 2015.

[2] Á. R. Carriel and F. C. Pesantes, "Análisis Y Detección De Vulnerabilidades en los Servidores Públicos del Centro de Cómputo de la Empresa Intermediaria de Ventas Utilizando la Metodología Internacional Osstmm," p. 207. Proyecto De Titulación, Fac. de Cien. Mat. y Fis., Univ. de Guayaquil, 2015.

[3] C. Bracho-Ortega, F. Cuzme-Rodríguez, C. Pupiales-yepez, L. Suárez-Zambrano, D. Peluffo-Ordoñez, and C. Moreira-Zambrano, "Auditoría de seguridad informática siguiendo la metodología OSSTMMv3 : caso de estudio," *Maskana*, vol. 8, pp. 307–319, 2017.

[4] C. Razo, *Auditoría en sistemas computacionales*. Pearson Educación, 2002.

[5] G. Rivas, *Auditoría informática*. Díaz de Santos, 1989.

[6] C. y. R. T. Tarlogic Security | Ciberseguridad, "Auditoría de seguridad servicios de seguridad informática ciberseguridad." [En línea]. Disponible en: https://www.tarlogic.com/servicios/auditoria-de-seguridad-servicios-de-seguridad/ , 2019. [Accedido: 17-May-2019].

[7] C. Tori, "Hacking Ético," vol. I, p. 334, 2008.

[8] C. Charles Cresson Wood, CISA, *Políticas de Seguridad Informática - Mejores Prácticas Internacionales*. Profesional, NetIQ, Inc., 1233 West Loop South 1800, Houston, TX 77027, 2002.

[9] E. E. de Excelencia, "Gestión de riesgos iso 9001 plan de contingencias." [En línea]. Disponible en: https://www.escuelaeuropeaexcelencia.com/2016/09/gestion-de-riesgos-plan-contingencia/ , Sep 2016. [Accedido: 15-Ago-2019].

[10] P. V. Herzog, "Manual de la metodología abierta de testeo de seguridad OSSTMM," p. 133, 2003.

[11] E. Bernardis, H. Bernardis, M. Berón, and G. A. Montejano, "Seguridad en servicios web," pp. 1094–1098, 2017.

[12] G. V. Villacís and R. A. R. Morocho, "Vulnerabilidades y amenazas a los servicios web de la intranet de la universidad técnica de babahoyo," vol. I. Fac. de Adm, Fin. e Inf., Univ. Tec. de Babahoyo, 2017.

[13] P. López, *Seguridad informática*. Ciclos Formativos, Editorial Editex, 2010.

[14] J. Faircloth and C. Hurley, *Penetration Tester's Open Source Toolkit*. Penetration Tester's Open Source Toolkit Series, Elsevier Science, 2007.

[15] J. Long, *Google Hacking for Penetration Testers*. Elsevier Science, 2004.

[16] D. D. J. R., "Auditoría de Seguridad Informática para el Gobierno Autónomo Descentralizado de Santa Ana de Cotacachi, basada en la norma NTP-ISO/IEC 17799:2007 y la metodología OSSTMM V2.," p. 184. Trabajo de Grado, Fac. de Ing. en Cien. Apli, Univ. Tec. del Norte, 2014.

[17] KALI, "What is kali linux? | kali linux documentation." https://www.kali.org/docs/introduction/what-is-kali-linux/, Ene 2019. [Accedido: 12-Ago-2019].

[18] C. Bucker, "Penetration testing | análisis and vulnerabilidades, evaluación de and análisis, métodos d e and web, d e aplicaciones," p. 22, 2012.

[19] WeLiveSecurity, "Maltego, la herramienta que te muestra qué tan expuesto estás en internet."

[20] R. Svensson, *From Hacking to Report Writing: An Introduction to Security and Penetration Testing*. Apress.

[21] R. Ghaznavi-Zadeh, *Kali Linux: Hacking Tools Introduction*. Primedia E-launch LLC.

[22] KALITOOLS, "the Harvester | herramientas de prueba de penetración." [En línea]. Disponible en: https://tools.kali.org/information-gathering/theharvester/ , Ene 2019. [Accedido: 21-Nov-2019].

[23] KALITOOLS, “Google hacking: Â¿qué es un google hack?.” [En línea]. Disponible en: https://www.acunetix.com/websitesecurity/google-hacking/ , May 2017. [Accedido: 03-Dic-2019].

[24] ElevenPaths, “Foca.” [En línea]. Disponible en: https://www.elevenpaths.com/es/labstools/foca-2/index.html , Oct 2017. [Accedido: 03-Dic-2019].

[25] P. O. R. Karla, T. Jimenez, Y. M. Angel, and R. Salgado, “Prevención, detección y reducción de riesgos,” p. 79. Trabajo de Graduación, Carr. de Ing. e Inf., Univ. Tec. de Ambato, Sangolqui Ecuador, 2013.

[26] OpenVAS, “Openvas - escáner de evaluación de vulnerabilidad abierta.” [En línea]. Disponible en: https://www.openvas.org/ , Ene 2009. [Accedido: 03-Dic-2019].

[27] Tenable, “Nessus.” [En línea]. Disponible en: https://docs.tenable.com/ , Ene 2009. [Accedido: 03-Dic-2019].

[28] Metasploit, “Metasploit Framework.” [En línea]. Disponible en: https://metasploit.help.rapid7.com/docs/msf-overview . [Accedido: 12-Dic-2019].

[29] Cloudflare, “Slowloris DDoS attack | flama de nube.” [En línea]. Disponible en: https://www.cloudflare.com/learning/ddos/ddos-attack-tools/slowloris/ , Nov 2018. [Accedido: 27-Dic-2019].

[30] KALITOOLS, “THC-hydra | herramientas de prueba de penetración.” [En línea]. Disponible en: https://tools.kali.org/password-attacks/hydra , Ene 2019. [Accedido: 12-Dic-2019].

[31] L. Allen, T. Heriyanto, and S. Ali, *Kali Linux â Assuring Security by Penetration Testing*. Community experience distilled, Packt Publishing.

[32] KALITOOLS, “sslstrip | herramientas de prueba de penetración.” [En línea]. Disponible en: https://tools.kali.org/information-gathering/sslstrip , Ene 2019. [Accedido: 10-Ene-2019].

[33] C. Vulnerabilities and E. (CVEÂ®). [En línea]. Disponible en: https://cve.mitre.org/about/index.html , Nov 2019. [Accedido: 12-Dic-2019].

[34] J. Ramos, *SEO: Guía práctica de posicionamiento en buscadores*. XinXii-GD Publishing, 2012.

[35] RYTEWIKI, "Man In The Middle, Â¿qué es el ataque man in the middle? - ryte wiki." [En línea]. Disponible en: https://es.ryte.com/wiki/Man-In-The-Middle , 2019. [Accedido: 05-Oct-2019].

[36] A. N. C. de Ecuador de 2007-2008, "Constitución de la republica del ecuador 2008."

[37] C. Alonso, D. Gabriel, A. Ignacio, and S. Elio, *PROCESOS Y HERRAMIENTAS PARA LA SEGURIDAD DE REDES*. Grado, UNED, 2014.

[38] MEGAPROFER S.A., "[En línea]. Disponible en: www.megaprofer.com/web/ ," Ene 2020. [Accedido: 20-Ene-2020].

[39] F. Medina, "El ciberataque global impactó en ecuador." El Comercio. [En línea]. Disponible en: www.elcomercio.com/actualidad/ciberataque-wannacry-impacto-ecuador-hackeo.html, May 2017. [Accedido: 17-May-2019].

[40] CNNExpansión, "Cada 33 segundos hay un ataque cibernético en américa latina." CNN. [En línea]. Disponible en:, https://cnnespanol.cnn.com/2017/09/19/cada-33-segundos-hay-un-ataque-cibernetico-en-america-latina/ .

[41] C. Sanz, "Las PYMES son las principales receptoras de ataques informáticos." Mercado2. [En línea]. Disponible en: https://www.merca2.es/pymes-principales-receptoras-ataques-informaticos/ , Feb 2020. [Accedido: 27-Feb-2020].

[42] C. Rueda, "Ecuador está en el grupo de los rezagados en ciberseguridad." Expreso. [En línea]. Disponible en: https://www.expreso.ec/actualidad/ecuador-grupo-rezagados-temas-ciberseguridad-6240.html , Mar 2020. [Accedido: 15-Mar-2020].

Anexos y Apéndices

Anexo A

Anexo A

Aprobación para realizar el proyecto de investigación

CARTA DE COMPROMISO

Ambato, 22/05/2019

Ingeniero Mg.
Julio Cuji Rodríguez
PRESIDENTE
UNIDAD DE TITULACIÓN
CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFOMÁTICOS
FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

Gutierrez Tobar Edisson Javier en mi calidad de Gerente General de la Empresa Megaprofer S.A., me permito poner en su conocimiento la aceptación y respaldo para el desarrollo del Trabajo de Titulación bajo el Tema: "Auditoría de la Seguridad Informática siguiendo la Metodología Open Source Security Testing Methodology Manual para la empresa Megaprofer S.A." propuesto por el estudiante Allaica Caranqui Joel Franklin portador de la Cédula de ciudadanía No 180445004-5 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.

.....
Gutierrez Tobar Edisson Javier
1802917011
03-244-0844 ext. 117
0995815314
edissong@megaprofer.com

Anexo B

Anexo B

Certificado de haber culminado el proyecto de investigación

Ambato, 12 de mayo de 2020

Ingeniera Mg.
Pilar Urrutia U.
DECANA
Facultad de Ingeniería en Sistemas Electrónica e Industrial
Presente

Señora Decana:

Por medio del presente, en calidad de asistente de infraestructura del departamento de sistemas de esta empresa certifico que el trabajo de investigación: ***"AUDITORÍA DE LA SEGURIDAD INFORMÁTICA SIGUIENDO LA METODOLOGÍA OPEN SOURCE SECURITY TESTING METHODOLOGY MANUAL (OSSTMM) PARA LA EMPRESA MEGAPROFER S.A."*** desarrollado por el señor: **Allaica Caranqui Joel Franklin**, con C.I. **1804450045**, ha sido concluido de conformidad a los intereses de la empresa.

Por la atención que se sirva dar al presente, me suscribo de usted.

Atentamente,

Fernando Paúl Manosalvas Llerena
1716120769
Asistente de Infraestructura
(02) 3827470 ext. 331
098 336 3013
paul.manosalvas@megaprofer.com

Anexo C

Anexo C

Entrevista de seguridad para jefe de TICS

Entrevista de seguridad para Jefe TIC´s

Entrevista aplicada al Jefe de Sistemas con el objetivo de realizar un análisis de la situación actual de la Institución en lo referente a los activos informáticos y sus Políticas de Seguridad

1. ¿Se cuenta con un inventario de todos los equipos que integran la red informática?

2. ¿Se tienen equipos dedicados al monitorear del tráfico y actividades de la red?

3. ¿Qué sistemas tiene bajo su cargo o responsabilidad?

4. ¿Se posee bitácoras de fallos o ataques detectados en los servidores?

5. ¿Se identifican los tipos de usuarios, sus responsabilidades, permisos y restricciones?

6. ¿Se tienen un sistema de seguridad para evitar que se sustraiga equipos informáticos de la institución?

7. ¿Se cuenta con Políticas de Seguridad Informática?

8. ¿Se concientiza a los usuarios mediante charlas o reuniones a prevenirlos “ataques informáticos”?

9. ¿Se tienen instalados programas antivirus en cada equipo con sus respectivas actualizaciones?

10. ¿El sistema operativo que se maneja se revisa y actualiza el Software Instalado frecuentemente?

11. ¿Con que frecuencia se pide a los usuarios que cambien de contraseña ?

12. ¿Se realiza periódicamente una copia de seguridad de los datos de empresa?

13. ¿Están los sitios web de la empresa protegidos?

14. ¿Se cuenta con un programa o dispositivo proxy?

15. ¿Se cuenta con un programa o dispositivo firewall?

Anexo D

Anexo D

Encuesta de Seguridad Informática para colaboradores de Megaprofer S.A.

Encuesta de Seguridad Informática

Con el objetivo ayudar a eliminar o reducir vulnerabilidades y salvaguardar la Información de la empresa se realiza una encuesta dirigida a los distintos colaboradores de la empresa.

1. ¿Se cuentan con algún tipo de control de entradas y salidas del personal a la Empresa?

   Marca solo un óvalo.

   - SI
   - NO

   ¿Cual?

2. Al recibir un correo desconocido. ¿Cuál es la medida que toma?

   Marca solo un óvalo.

   - ABRIR Y LEER PARA VER DE QUE SE
   - TRATA MARCAR COMO SPAM Y BORRAR
   - NOTIFICAR A TIC'S
   - NO HACE NADA

3. ¿Cuándo quiere consultar una página de internet para obtener información acerca de su trabajo ¿Tiene acceso a ella?

Marca solo un óvalo.

- SI
- NO

En caso de que su respuesta sea NO indique el ¿Por qué?

4. ¿Su usuarios y contraseñas de los distintitos sistemas de Megaprofer principalmente la tiene guardada en?

Marca solo un óvalo.

- CELULAR
- COMPUTADOR
- PAPEL
- LA MEMORIZA

5. ¿Cuál es el periodo promedio en el cual usted realiza cambio o renovación de su contraseña?

Marca solo un óvalo.

- MENOR A 2 MESES
- MENOR A 3 MESES
- MENOR A 6 MESES
- MENOR A 1 AÑO
- NUNCA

6. ¿Cuál es la longitud aproximada de su contraseña?

Marca solo un óvalo.

- MENOR A 7 CARACTERES
- ENTRE 8 - 9 CARACTERES
- ENTRE 10 - 13 CARACTERES
- MAYOR A 13 CARACTERES

7. ¿Sus contraseñas están compuestas de una combinación de: números, letras mayúsculas, minúsculas y caracteres especiales?

Marca solo un óvalo.

- SI
- NO

8. ¿Conoce usted el instructivo de uso de Herramientas Tecnológicas de Megaprofer?

Marca solo un óvalo.

- SI
- NO

9. ¿Se ha dado a conocer a usted en la empresa sobre los “ataques informáticos”, y las maneras de evitarlos?

Marca solo un óvalo.

- SI
- NO

10. ¿Con que frecuencia usted ha recibido notificaciones de las actualizaciones del antivirus?

Marca solo un óvalo.

- A DIARIO
- CADA SEMANA
- CADA 15 DÍAS
- NUNCA

11. ¿Normalmente en donde guarda usted la información?

Marca solo un óvalo.

- PC DE TRABAJO
- NUBE (ONE RIVE)
- DISPOSITIVO EXTERNO

12. ¿Se ha conectado remotamente a su equipo de la empresa mediante alguna de las siguientes herramientas?

Marca solo un óvalo.

- ANYDESK
- TEAM VIEWER
- OTRAS APLICACIONES
- NUNCA ME E CONECTADO

Anexo E

Anexo E

Informe de escaneo Nessus

Comprobantes

1	1	9	5	42
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities

Total: 58

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	58987	PHP Unsupported Version Detection
HIGH	7.1	20007	SSL Version 2 and 3 Protocol Detection
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	6.1	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.1	121010	TLS Version 1.1 Protocol Detection
MEDIUM	5.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.0	15901	SSL Certificate Expiry
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	4.3	90317	SSH Weak Algorithms Supported
MEDIUM	4.3	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
LOW	2.6	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6	71049	SSH Weak MAC Algorithms Enabled
LOW	2.6	83875	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
LOW	2.6	10407	X Server Detection
LOW	N/A	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	10223	RPC portmapper Service Detection
INFO	N/A	18261	Apache Banner Linux Distribution Disclosure
INFO	N/A	48204	Apache HTTP Server Version
INFO	N/A	39520	Backported Security Patch Detection (SSH)
INFO	N/A	39521	Backported Security Patch Detection (WWW)

INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	84502	HSTS Missing From HTTPS Server
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	11414	IMAP Service Banner Retrieval
INFO	N/A	42085	IMAP Service STARTTLS Command Support
INFO	N/A	117886	Local Checks Not Enabled (info)
INFO	N/A	10719	MySQL Server Detection
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	110723	No Credentials Provided
INFO	N/A	11936	OS Identification
INFO	N/A	50845	OpenSSL Detection
INFO	N/A	48243	PHP Version Detection
INFO	N/A	10185	POP Server Detection
INFO	N/A	42087	POP3 Service STLS Command Support
INFO	N/A	11111	RPC Services Enumeration
INFO	N/A	53335	RPC portmapper (TCP)
INFO	N/A	70657	SSH Algorithms and Languages Supported

INFO	N/A	10881	SSH Protocol Versions Supported
INFO	N/A	10267	SSH Server Type and Version Information
INFO	N/A	56984	SSL / TLS Versions Supported
INFO	N/A	10863	SSL Certificate Information
INFO	N/A	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	21643	SSL Cipher Suites Supported
INFO	N/A	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	94761	SSL Root Certification Authority Certificate Information
INFO	N/A	51891	SSL Session Resume Supported
INFO	N/A	22964	Service Detection
INFO	N/A	11153	Service Detection (HELP Request)
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	10287	Traceroute Information
INFO	N/A	10342	VNC Software Detection

ATIX

Vulnerabilities Total: 34

SEVERITY	CVSS	PLUGIN	NAME
MEDIUM	5.0	57608	SMB Signing not required
LOW	2.6	70658	SSH Server CBC Mode Ciphers Enabled
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	39520	Backported Security Patch Detection (SSH)
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	42410	Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure
INFO	N/A	17651	Microsoft Windows SMB : Obtains the Password Policy
INFO	N/A	10394	Microsoft Windows SMB Log In Possible
INFO	N/A	10859	Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration
INFO	N/A	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	11011	Microsoft Windows SMB Service Detection
INFO	N/A	60119	Microsoft Windows SMB Share Permissions Enumeration
INFO	N/A	10395	Microsoft Windows SMB Shares Enumeration
INFO	N/A	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)

INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	50350	OS Identification Failed
INFO	N/A	10860	SMB Use Host SID to Enumerate Local Users
INFO	N/A	70657	SSH Algorithms and Languages Supported
INFO	N/A	10881	SSH Protocol Versions Supported
INFO	N/A	10267	SSH Server Type and Version Information
INFO	N/A	25240	Samba Server Detection
INFO	N/A	104887	Samba Version
INFO	N/A	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	22964	Service Detection
INFO	N/A	11153	Service Detection (HELP Request)
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	10287	Traceroute Information
INFO	N/A	135860	WMI Not Available
INFO	N/A	10150	Windows NetBIOS / SMB Remote Host Information Disclosure

Correo

0	0	9	5	48
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 62

SEVERITY	CVSS	PLUGIN	NAME
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	6.1	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.1	121010	TLS Version 1.1 Protocol Detection
MEDIUM	5.0	12217	DNS Server Cache Snooping Remote Information Disclosure
MEDIUM	5.0	10595	*DNS Server Zone Transfer Information Disclosure (AXFR)*
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	4.3	90317	SSH Weak Algorithms Supported
MEDIUM	4.3	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
LOW	2.6	15855	POP3 Cleartext Logins Permitted
LOW	2.6	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6	71049	SSH Weak MAC Algorithms Enabled
LOW	2.6	31705	SSL Anonymous Cipher Suites Supported
LOW	2.6	83875	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	39520	Backported Security Patch Detection (SSH)
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	10028	DNS Server BIND version Directive Remote Version Detection
INFO	N/A	35373	DNS Server DNSSEC Aware Resolver

INFO	N/A	11002	DNS Server Detection
INFO	N/A	72779	DNS Server Version Detection
INFO	N/A	35371	DNS Server hostname.bind Map Hostname Disclosure
INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	84502	HSTS Missing From HTTPS Server
INFO	N/A	43111	HTTP Methods Allowed (per directory)
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	11414	IMAP Service Banner Retrieval
INFO	N/A	42085	IMAP Service STARTTLS Command Support
INFO	N/A	25701	LDAP Crafted Search Request Server Information Disclosure
INFO	N/A	20870	LDAP Server Detection
INFO	N/A	42329	LDAP Service STARTTLS Command Support
INFO	N/A	117886	Local Checks Not Enabled (info)
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	110723	No Credentials Provided
INFO	N/A	11936	OS Identification
INFO	N/A	50845	OpenSSL Detection
INFO	N/A	10185	POP Server Detection
INFO	N/A	54580	SMTP Authentication Methods
INFO	N/A	10263	SMTP Server Detection
INFO	N/A	42088	SMTP Service STARTTLS Command Support

INFO	N/A	70657	SSH Algorithms and Languages Supported
INFO	N/A	10881	SSH Protocol Versions Supported
INFO	N/A	10267	SSH Server Type and Version Information
INFO	N/A	56984	SSL / TLS Versions Supported
INFO	N/A	10863	SSL Certificate Information
INFO	N/A	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	21643	SSL Cipher Suites Supported
INFO	N/A	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	94761	SSL Root Certification Authority Certificate Information
INFO	N/A	22964	Service Detection
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	84821	TLS ALPN Supported Protocol Enumeration
INFO	N/A	87242	TLS NPN Supported Protocol Enumeration
INFO	N/A	62564	TLS Next Protocols Supported
INFO	N/A	10287	Traceroute Information
INFO	N/A	10302	Web Server robots.txt Information Disclosure
INFO	N/A	72584	Zimbra Collaboration Server Web Detection
INFO	N/A	106375	nginx HTTP Server Detection

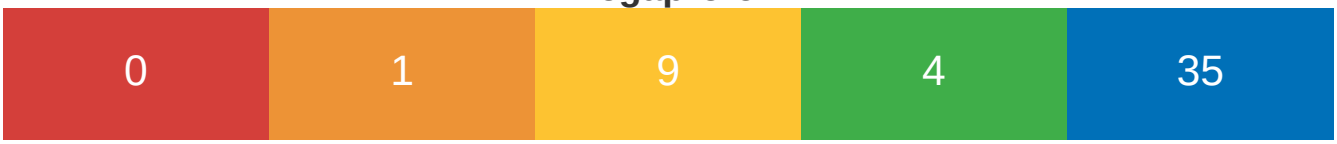
Pedidos en línea

Vulnerabilities Total: 23

SEVERITY	CVSS	PLUGIN	NAME
MEDIUM	5.0	57608	SMB Signing not required
MEDIUM	4.3	90317	SSH Weak Algorithms Supported
LOW	2.6	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6	71049	SSH Weak MAC Algorithms Enabled
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	39520	Backported Security Patch Detection (SSH)
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	117886	Local Checks Not Enabled (info)
INFO	N/A	11011	Microsoft Windows SMB Service Detection
INFO	N/A	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	110723	No Credentials Provided
INFO	N/A	11936	OS Identification
INFO	N/A	70657	SSH Algorithms and Languages Supported
INFO	N/A	10881	SSH Protocol Versions Supported
INFO	N/A	10267	SSH Server Type and Version Information

INFO	N/A	22964	Service Detection
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	10287	Traceroute Information
INFO	N/A	135860	WMI Not Available

Página Megaprofer



Vulnerabilities Total: 49

SEVERITY	CVSS	PLUGIN	NAME
HIGH	7.1	20007	SSL Version 2 and 3 Protocol Detection
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	6.1	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.1	121010	TLS Version 1.1 Protocol Detection
MEDIUM	5.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.0	15901	SSL Certificate Expiry
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	4.3	90317	SSH Weak Algorithms Supported
MEDIUM	4.3	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
LOW	2.6	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6	71049	SSH Weak MAC Algorithms Enabled
LOW	2.6	83875	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
LOW	N/A	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	18261	Apache Banner Linux Distribution Disclosure
INFO	N/A	48204	Apache HTTP Server Version
INFO	N/A	84574	Backported Security Patch Detection (PHP)
INFO	N/A	39520	Backported Security Patch Detection (SSH)

INFO	N/A	39521	Backported Security Patch Detection (WWW)
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	84502	HSTS Missing From HTTPS Server
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	117886	Local Checks Not Enabled (info)
INFO	N/A	10719	MySQL Server Detection
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	110723	No Credentials Provided
INFO	N/A	11936	OS Identification
INFO	N/A	50845	OpenSSL Detection
INFO	N/A	48243	PHP Version Detection
INFO	N/A	70657	SSH Algorithms and Languages Supported
INFO	N/A	10881	SSH Protocol Versions Supported
INFO	N/A	10267	SSH Server Type and Version Information
INFO	N/A	56984	SSL / TLS Versions Supported
INFO	N/A	10863	SSL Certificate Information
INFO	N/A	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	21643	SSL Cipher Suites Supported
INFO	N/A	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	94761	SSL Root Certification Authority Certificate Information

INFO	N/A	51891	SSL Session Resume Supported
INFO	N/A	22964	Service Detection
INFO	N/A	11153	Service Detection (HELP Request)
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	10287	Traceroute Information