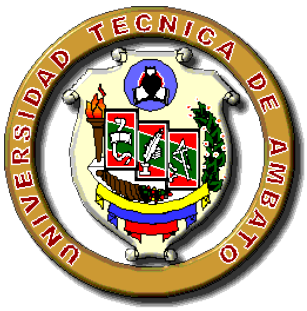


UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE TECNOLOGÍAS DE LA INFORMACIÓN, TELECOMUNICACIONES E INDUSTRIAL

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS

TEMA:

AUDITORÍA DE REDES, APLICANDO LA METODOLOGÍA OSSTMM V3, PARA EL MINISTERIO DE INCLUSIÓN ECONÓMICA Y SOCIAL.

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

LÍNEA DE INVESTIGACIÓN: Seguridad Informática

AUTOR: Miranda Silva Christian Paúl
TUTOR: Ing. Dennis Chicaiza Mg.

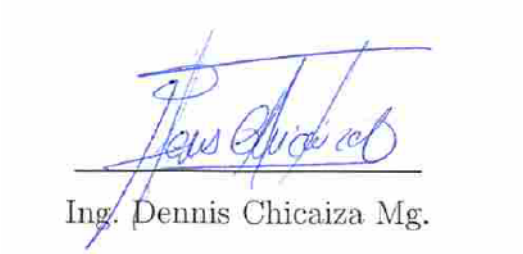
Ambato - Ecuador
Julio, 2019

CERTIFICACIÓN DEL TUTOR

En mi calidad de Tutor del Trabajo de Investigación sobre el Tema:

"AUDITORÍA DE REDES, APLICANDO LA METODOLOGÍA OSSTMM V3, PARA EL MINISTERIO DE INCLUSIÓN ECONÓMICA Y SOCIAL.", del señor Miranda Silva Christian Paúl, estudiante de la Carrera de Ingeniería en Sistemas Computacionales e Informáticos, de la Facultad de Tecnologías de la Información, Telecomunicaciones e Industrial, de la Universidad Técnica de Ambato, considero que el informe investigativo reúne los requisitos suficientes para que continúe con los trámites y consiguiente aprobación de conformidad con el Art. 16 del Capítulo II, del Reglamento de Graduación para Obtener el Título Terminal de Tercer Nivel de la Universidad técnica de Ambato

Ambato, Julio de 2019



Ing. Dennis Chicaiza Mg.

EL TUTOR

AUTORÍA DEL TRABAJO

El presente trabajo de investigación titulado: "AUDITORÍA DE REDES, APLICANDO LA METODOLOGÍA OSSTMM V3, PARA EL MINISTERIO DE INCLUSIÓN ECONÓMICA Y SOCIAL.". 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.

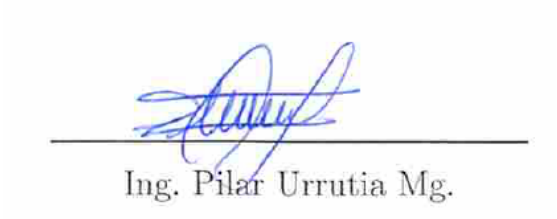
Ambato, Julio de 2019

Christian Paúl Miranda Silva

CC: 180434865-2

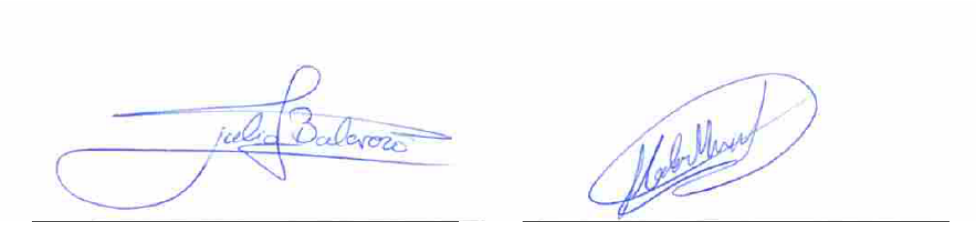
APROBACIÓN DEL TRIBUNAL DE GRADO

La Comisión Calificadora del presente trabajo conformada por los señores docentes Ing. Julio Balarezo PhD. e Ing. Carlos Núñez Mg., revisó y aprobó el Informe Final del trabajo de graduación titulado "AUDITORÍA DE REDES, APLICANDO LA METODOLOGÍA OSSTMM V3, PARA EL MINISTERIO DE INCLUSIÓN ECONÓMICA Y SOCIAL.", presentado por el señor Christian Paúl Miranda Silva, de acuerdo al Art. 17 del Reglamento de Graduación para obtener el título Terminal de tercer nivel de la Universidad Técnica de Ambato.



Ing. Pilar Urrutia Mg.

PRESIDENTE DEL TRIBUNAL



Ing. Julio Balarezo PhD.	Ing. Carlos Núñez Mg.
DOCENTE CALIFICADOR	DOCENTE CALIFICADOR

DEDICATORIA

A mis padres José Miranda y María Silva por haberme forjado como la persona que soy en la actualidad; muchos de mis logros se los debo a ustedes entre los cuales incluyo el presente proyecto.
Me formaron con reglas y con algunas libertades, pero al final de cuentas, me motivaron constantemente para alcanzar mis anhelos.
Mamá, Papá muchas gracias.

Christian Miranda Silva

AGRADECIMIENTO

Agradezco a Dios, a mis hermanos Maura, Liliana, Andrés , a mi novia Evelyn y por último pero muy importantes a mis padres José Miranda y María Silva quienes han creido en mí siempre dándome apoyo y ejemplo de superación, humildad y sacrificio; enseñandome a valorar todo lo que tengo.

A todos ellos les agradezco, porque han fomentado en mí, el deseo de superación y de triunfo en la vida, lo que contribuyó a la consecución de este logro. Espero contar siempre con su valioso e incondicional apoyo.

A todos muchas gracias.

Christian Miranda Silva

ÍNDICE

APROBACIÓN DEL TUTOR ii

AUTORÍA iii

APROBACIÓN COMISIÓN CALIFICADORA iv

Dedicatoria v

Agradecimiento vi

Introducción xiv

CAPÍTULO 1 El problema 1

1.1 Tema de Investigación 1
1.2 Planteamiento del problema 1
1.3 Delimitación 3
1.4 Justificación 3
1.5 Objetivos 3
1.5.1 General 3
1.5.2 Específicos 4

CAPÍTULO 2 Marco Teórico 5

2.1 Antecedentes Investigativos 5
2.2 Fundamentación Teórica. 6
2.2.1 Seguridad 6
2.2.2 Seguridad Informática 6
2.2.3 Escáner de Vulnerabilidades 6
2.2.4 Pruebas de Penetración (PenTest) 6
2.2.5 Hacking 7
2.2.6 Hacking Ético 7
2.2.7 Auditoría 7
2.2.8 Auditoría de Red 7

2.2.9 Metodología 7
2.2.10 OSSTM (Manual de la Metodología Abierta de Testeo de Seguridad) 7
2.3 Propuesta de Solución 8

CAPÍTULO 3 Metodología **10**
3.1 Modalidad de la investigación 10
3.2 Población y muestra 10
3.3 Recolección de información 10
3.4 Procesamiento y análisis de datos 10
3.5 Desarrollo del Proyecto 11

CAPÍTULO 4 Desarrollo de la propuesta **12**
4.1 Introducción 12
4.1.1 Instalación de Equipos de Cómputo 12
4.1.2 Mantenimiento de Equipos de Computo 12
4.1.3 Reubicación de Equipos 13
4.1.4 Control de Acceso al Equipo de Computo 13
4.1.5 Control de Acceso Local a la Red 13
4.1.6 Acceso a Internet 13
4.1.7 Adquisisción de Software 13
4.1.8 Instalación de Software 13
4.2 Análisis de Factibilidad 14
4.2.1 Factibilidad Operativa 14
4.2.2 Factibilidad Técnica 14
4.2.3 Factibilidad Económica 14
4.3 Fundamentación 14
4.4 Metodología 17
4.5 Determinaión del tipo de Políticas de Seguridad Informática aplicadas en el Ministerio de Inclusión Económica y Social 20
4.5.1 Análisis de la Situación Actual de la Institución en lo referente a los activos informáticos y sus Políticas de Seguridad 20
4.5.2 Realización de encuesta Dirigida al Personal que Labora en el MIES 26
4.6 Identificación de vulnerabilidades en los servidores de la red informática que puedan ser explotadas por intrusos malintencionados 34

4.6.1 Análisis de las estrategias y herramientas necesarias para la ejecución de las Pruebas de Penetración y Hacking Ético 34
4.6.2 Identificación de las vulnerabilidades en los servidores o fallos de sistemas que puedan ser explotadas por intrusos malintensionados 37
4.7 Determinación del escenario virtual para ejecutar un ataque programado a los servidores de la red informática para explotar las vulnerabilidades que puedan ser utilizadas por intrusos malintencionados. 66
4.7.1 Realización de Pruebas de Penetración en un entorno controlado de manera que no se ocasionen problemas a la red Institucional 66
4.7.1.1 Equipo virtual Windows 68
4.7.1.2 Equipo Virtual Ubuntu 77
4.7.1.3 Resumen de explotación de vulnerabilidades . . . 87
4.8 Políticas de contingencia de seguridad informática que mejoren la integridad, confidencialidad y disponibilidad de la información del Ministerio de Inclusión Económica y Social. 89
4.8.1 Políticas de Seguridad que mejoren la integridad, confidencialidad y disponibilidad de la información que se maneja a través de la red en base a las vulnerabilidades detectadas incluyendo soluciones orientadas a resolverlos. 89
4.8.2 Políticas de Contingencia de seguridad informática interna que resguarden los activos informáticos que maneja la institución. 102

CAPÍTULO 5 Conclusiones y Recomendaciones 107
5.1 Conclusiones 107
5.2 Recomendaciones 108

Bibliografia 109

ANEXOS 113

ÍNICE DE TABLAS

4.1 Sección y Módulos aplicables al proyecto 18
4.2 Tipos de Análisis y Detección de Vulnerabilidades 34
4.3 Herramientas de reconocimiento 35
4.4 Herramientas de sondeo de puertos 35
4.5 Herramientas de detección de vulnerabilidades 36
4.6 Herramientas de explotación de vulnerabilidades 37
4.7 Listado de servidores relacionados al dominio 45
4.8 Redes internas Ministerio de Inclusión Económica y Social 46
4.9 Servidores a auditar 47
4.10 Vulnerabilidades detectadas en emthsis.inclusion.gob.ec 53
4.11 Vulnerabilidades detectadas en info.inclusion.gob.ec 54
4.12 Vulnerabilidades detectadas en formacioncontinua.inclusion.gob.ec 55
4.13 Vulnerabilidades detectadas en siimiesalphapruebas.inclusion.gob.ec 55
4.14 Vulnerabilidades detectadas en siimies.inclusion.gob.ec 56
4.15 Vulnerabilidades detectadas en mail.inclusion.gob.ec 57
4.16 Vulnerabilidades detectadas en cz.inclusion.gob.ec 58
4.17 Vulnerabilidades detectadas en www.inclusion.gob.ec 59
4.18 Vulnerabilidades detectadas en info.inclusion.gob.ec 61
4.19 Vulnerabilidades detectadas en cz.inclusion.gob.ec 62
4.20 Vulnerabilidades detectadas en mail.inclusion.gob.ec 63
4.21 Vulnerabilidades detectadas en www.inclusion.gob.ec 63
4.22 Vulnerabilidades detectadas en siimies.inclusion.gob.ec 64
4.23 Vulnerabilidades detectadas en emthsis.inclusion.gob.ec 64
4.24 Vulnerabilidades detectadas en formacioncontinua.inclusion.gob.ec 65
4.25 Vulnerabilidades detectadas en siimiesalphapruebas.inclusion.gob.ec 65
4.26 Resumen de vulnerabilidades explotables 87
4.27 Resumen de servicios explotables 88

ÍNDICE DE FIGURAS

2.1 Mapa de Seguridad OSSTMM V3 8

4.1 Secciones OSSTMM V3 utilizadas en el proyecto 20
4.2 Esquema MIES 22
4.3 Esquema MIES 23
4.4 Pregunta: ¿Su usuario y contraseña, la tiene guardada en? 26
4.5 Pregunta: ¿Con qué frecuencia cambia su contraseña? 27
4.6 Pregunta: ¿Usualmente en su contraseña suele usar? 27
4.7 Pregunta: ¿Cada cuánto tiempo se brinda mantenimiento a los equipos? 28
4.8 Pregunta: ¿Cree que las medidas de seguridad que se manejan dentro del MIES sean seguras y adecuadas? 29
4.9 Pregunta: En el departamento de Tic's, ¿se realizan actividades para su monitoreo? 29
4.10 Pregunta: ¿Se revisa y actualiza el Software Instalado frecuentemente? 30
4.11 Pregunta: ¿Se ha dado a conocer sobre los "ataques informáticos", y las maneras de evitarlos? 31
4.12 Pregunta: 9. ¿Sabe del manejo de Políticas de Seguridad Informática? 31
4.13 Pregunta: ¿Su equipo de trabajo cuenta con internet? de ser el caso ¿cómo califica el servicio? 32
4.14 Pregunta: Cuando quiere consultar una página para obtener información ¿tiene acceso a ella? 33
4.15 Maltego, transformación del dominio inclusion.gob.ec 38
4.16 FOCA, nobres de usuarios detectados 39
4.17 Visual Route a www.inclusion.gob.ec 40
4.18 TheHarvester a dominio inclusion.gob.ec 41
4.19 The Harvester informe inclusion.gob.ec 42
4.20 Buscador de Google MIES 43
4.21 NIC consulta inclusion.gob.ec 44
4.22 Escenario para el análisis y detección de vulnerabilidades 47

4.23 Sondeo de Puertos con nmap 48
4.24 nmap a mail.inclusion.gob.ec 48
4.25 nmap a cz.inclusion.gob.ec 49
4.26 nmap a emthsis.inclusion.gob.ec 49
4.27 nmap a formacioncontinua.inclusion.gob.ec 50
4.28 nmap a info.inclusion.gob.ec 50
4.29 nmap a siimies.inclusion.gob.ec 51
4.30 Escaneo de Vulnerabilidades con OpenVAS 52
4.31 Escaneo de vulnerabilidades con Nessus 60
4.32 Inicio de msfconsole 66
4.33 Entorno virtualizado para la explotación de vulnerabilidades . . . 67
4.34 Ejecución de exploit de vulnerabilidad SMB 69
4.35 Ejecución del payload 70
4.36 Windows Server 2012 dado de baja 71
4.37 Ejecución y explotación de vulnerabilidad RDP 73
4.38 Fallo en explotación de vulnerabilidad RDP 73
4.39 Vista del servicio Apache Tomcat 75
4.40 Ejecución comando hping3 76
4.41 Éxito en el ataque por DoS al servicio web 76
4.42 Configuración y explotación de vulnerabilidad FTP 78
4.43 Conexión a FTP mediante anonymous 78
4.44 Diagrama de ataque de Man-in-the-Middle. 80
4.45 Configuración de ruteo de iptables. 80
4.46 Selección de ip a escuchar (sniffing) 81
4.47 Inicio de sesión en un ordenador envenenado. 82
4.48 Captura de tráfico y obtención de credenciales en ettercap 83
4.49 Servicio Apache en ejecutandose en servidor Ubuntu 84
4.50 Envió de paquetes mediante slowloris 85
4.51 Éxito en el ataque DoS al servicio Apache en el servidor Ubuntu . 86

Resumen Ejecutivo

El presente proyecto está dirigido a la Auditoría de Redes en el Ministerio de Inclusión Económica y Social, mediante la metodología OSSTMM V3 para el análisis, detección y explotación de vulnerabilidades mediante herramientas de seguridad informática.
OSSTMM V3 presenta una planificación de ejecución y verificación de la seguridad Informática, cada una de las secciones de la metodología proporciona módulos de ayuda para el desarrollo del análisis de seguridad, se toma la Sección Seguridad de Red y los módulos: Análisis de Seguridad, Pruebas de Seguridad Inalámbrica, Pruebas de Seguridad Telecomunicaciones, Datos de pruebas de Seguridad de redes y los módulos: Sondeo de la Red, Identificación de Servicios y Sistemas, Búsqueda y Verificación de Vulnerabilidades. Las dos secciones están enfocadas a los resultados esperados permitiendo valorar el nivel de seguridad existente en la Institución para luego proponer cambios o inclusión de medidas de seguridad mejorando así la situación actual en lo que a Seguridad de Red se refiere.

Abstract

This project is addressed to the Network Audit in the Ministry of Economic and Social Inclusion, through the OSSTMM V3 methodology for the analysis, detection and exploitation of vulnerabilities through computer security tools.
OSSTMM V3 presents a planning of execution and verification of computer security, each of the sections of the methodology provides help modules for the development of security analysis, the Network Security Section and modules are taken: Security Analysis, Testing of Wireless Security, Telecommunications Security Testing, Network Security Test Data and modules: Network Survey, Identification of Services and Systems, Vulnerability Search and Veri fi cation. The two sections are focused on the expected results, allowing to assess the level of security existing in the Institution and then propose changes or inclusion of security measures, thus improving the current situation regarding Network Security.

INTRODUCCIÓN

La falta de seguridad informática hoy en día es una latente preocupación en el campo de las redes especialmente donde se maneja información confidencial, el presente proyecto tiene como finalidad el análisis y detección de vulnerabilidades mediante herramientas de Seguridad Informática, las cuales guiadas por la metodología OSSTMM V3 y sus secciones de Seguridad de Redes y Seguridad Inalámbrica junto con varios módulos, estas secciones son tomadas de acuerdo a los resultados esperados:

Capítulo I, "El Problema": se plantea y describe el problema de investigación desde una óptica global hasta los problemas que poseen instituciones de la ciudad y la necesidad de ser corregidos, se plantea la justificación y los objetivos que se alcanzaran en el presente proyecto.

Capitulo II, "Marco Teórico": se manifiestan los antecedentes investigativos referentes a los cuales se desarrolla la propuesta, se presenta fundamentos teóricos que guía en la búsqueda de una solución al problema planteado.

Capitulo III, "Metodología": se describe la modalidad de investigación a utilizar, especificando el método de recolección y procesamiento de la información para su análisis y las actividades a seguir para el desarrollo del presente proyecto, por último, se presenta las diferentes actividades necesarias para cumplir con los objetivos planteados.

Capitulo IV,, "Desarrollo de la Propuesta": se presenta el desarrollo de la propuesta llevando a cabo las actividades detalladas para el cumplimiento de cada uno de los objetivos específicos.

Capítulo V, "Conclusiones y Recomendaciones": se establecen las conclusiones y recomendaciones finales en base a los resultados obtenidos en el transcurso del desarrollo del proyecto.

CAPÍTULO 1

El problema

1.1. Tema de Investigación

"Auditoría de Redes, Aplicando la Metodología OSSTMM V3, para El Ministerio de Inclusión Económica y Social"

1.2. Planteamiento del problema

El problema a tratar es la falta de seguridad en la red del Ministerio de Inclusión Económica y Social, en una breve charla con el director del departamento de Tics me supo manifestar que últimamente la empresa a sido víctima de fallos en sus sistemas web, también considera que se da un manejo incorrecto a los ordenadores y no ponen en práctica las políticas de contingencia ante problemas informáticos como virus. Hay que considerar también el cuidado de la información que imparten a la comunidad ambateña mediante la red y sus sistemas web, por este motivo se toma como medida evaluativa una Auditoría de redes aplicando la metodología OSSTMM V3.

"A nivel mundial las auditorías juegan un papel relevante ya que permiten mostrar el estado en el que se encuentra la protección de la información y de los activos dentro de las organizaciones. Además, involucra la identificación, análisis y evaluación de debilidades en las medidas de seguridad que han sido aplicadas, así como de los componentes tecnológicos de la empresa" [1].

Además, pueden tener distintas intenciones, por lo tanto, las revisiones de seguridad varían de acuerdo a condiciones como el alcance, los criterios que se utilizan como parámetros de comparación, las personas que las llevan a cabo, los propósitos que se desean alcanzar, entre otros elementos que determinan el tipo de revisión.

"En el caso específico de las redes, la auditoría está relacionada con un método o un conjunto de ellos para verificar el cumplimiento de los requisitos de seguridad" [1]. Es necesario verificar que se cumplan los requisitos de seguridad dentro de una colección de dispositivos interconectados como pueden ser routers, switches, hubs, computadoras y dispositivos móviles, entre otros.

"En cuanto a nivel nacional en Ecuador en la Universidad Central del Ecuador

el diseño y aplicación del procedimiento de auditoría permitió comprobar la vulnerabilidad desde el punto de vista práctico, en cuanto a la madurez de las capacidades de los procesos clasificados como primarios en la seguridad de las redes LAN arrojando resultados desfavorables. Se demostró que su aplicación contribuyó a la realización de recomendaciones necesarias para el mejoramiento de la seguridad de la red LAN de los laboratorios de computadoras de la Facultad de Ingeniería Ciencias Físicas y Matemática de la Universidad" [2].

Al realizar evaluaciones de auditoría en seguridad de las redes LAN tanto como en laboratorios de computadoras o empresas completas, se despierta el interés del personal administrativo, lo cual es favorable porque se genera un ambiente de conciencia para seguir con las normas establecidas.

"El MIES (Ministerio De Inclusión Económica Y Social), es una entidad pública que ejerce rectoría y ejecuta políticas para la inclusión social y atención durante el ciclo de vida, tiene una amplia gama de servicios para la población, especialmente, para los más vulnerables como niñas, niños, adolescentes, jóvenes, adultos mayores, personas con discapacidad y aquellas personas que se encuentran en situación de pobreza, a fin de fortalecer su movilidad social y salida de la pobreza" [3]. La Institución necesita una auditoria para detectar las posibles vulnerabilidades y posibles deficiencias que pueda tener la red y de esta manera determinar las medidas necesarias a tomar, para evitar cualquier tipo de ataque y mejorar la eficiencia de la red.

"El "Manual de la Metodología Abierta de Testeo de Seguridad Versión 3"(OSSTMM V3) es un documento que reúne, de forma estandarizada y ordenada, las diversas verificaciones y pruebas que debe realizar un profesional de la seguridad informática durante el desarrollo de las auditorías y verificaciones de la seguridad. Es un documento en constante evolución, fruto del trabajo conjunto de más de 150 colaboradores de todo el mundo. Con esta metodología es posible realizar el análisis de redes inalámbricas como acces point, Bluetooh y similares, estas verificaciones incluyen tanto la identificación de estas comunicaciones como la comprobación del nivel de seguridad de las redes ya identificadas"[4].

El personal del MIES se encuentra intrigado por posibles ataques hacia la empresa, por motivo de que la información que diariamente es manipulada es de suma iportancia y en el mayor de los casos confidencial, la cual no les gustaría perder o en el peor de los casos que se divulgue, así que si les gustaría saber qué medidas deberían tomar para evitar posibles ataques y aun peor perdidas de información o datos.

1.3. Delimitación

- Área Académica: Seguridad Informática.
- Línea de Investigación: Seguridad y Software.
- Sublínea de investigación: Redes.
- Delimitación espacial: Ministerio De Inclusión Económica Y Social.
- Delimitación temporal: La presente investigación se desarrolló a partir del 03 de septiembre de 2018 hasta el 03 de enero de 2019.

1.4. Justificación

La falta de seguridad informática hoy en día es una latente preocupación en el campo de las redes especialmente donde se maneja información confidencial, como bases de datos, correo electrónico, sistemas Informáticos, o páginas gubernamentales, debido al avance de la tecnología y la globalización de las redes de comunicación y todo esto gracias al Internet.
Realizar esta Auditoría aplicando la metodología OSSTMM V3, permitirá que el personal del MIES tenga un nivel de confianza o seguridad con sus informaciones, la cual corre el riesgo de ser obtenida mediante un mal manejo de la red, descuido o falta de seguridad de la misma.
La realización de dicha auditoría es de suma importancia para el MIES para lo cual se propone analizar los mecanismos de control implantados, determinando si los mismos son apropiados y cumplen con los objetivos planteados, esto abre puertas a mejoras o recomendaciones para reforzar la seguridad de la red implantada. De la misma manera abre paso a la innovación del establecimiento, de tal forma en que se están modernizando en el campo tecnológico lo cual podrá crecer aún más.

1.5. Objetivos

1.5.1. General

Implementar una Auditoría de redes aplicando la metodología OSSTMM V3 en el Ministerio de Inclusión Económica y Social.

1.5.2. Específicos

- Realizar un análisis, metódico y planificado de los mecanismos de defensa internos y externos. en la red del Ministerio de Inclusión Económica y Social.
- Aplicar la metodología OSSTMM V3 a fin de priorizar las necesidades de seguridad, simulando un ataque real.
- Proponer políticas de contingencia de seguridad informática que mejoren la integridad, confidencialidad y disponibilidad de la información en base a las vulnerabilidades detectadas.

CAPÍTULO 2

Marco Teórico

2.1. Antecedentes Investigativos

Los antecedentes que se ha encontrado son trabajos relacionados al presente tema de investigación. El cual uno de ellos los autores Edgar A. Maya y Daniel D. Jaramillo con el tema "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." [5]. En el cual concluye que aun cuando no existe un esquema de seguridad que cubra en su totalidad los posibles riesgos, sin embargo, se puede estar preparado y dispuesto a reaccionar con rapidez a las amenazas y las vulnerabilidades que pueden presentarse en el campo de la informática, lo cual se busca implementar en el presente proyecto.
También el autor Roberto López Santoyo con el tema PROPUESTA DE IMPLEMENTACIÓN DE UNA METODOLOGÍA DE AUDITORÍA DE SEGURIDAD INFORMÁTICA[6]. Concluye que con el desarrollo de la guía de implementación de la metodología OSSTMM facilita la tarea a un estudiante recién licenciado o a un profesional con poca experiencia en seguridad informática para que pueda empezar a realizar sus primeras auditorías de seguridad siguiendo una metodología de reconocido prestigio, por lo tanto con esto se observa que la metodología escogida es la apropiada para el presente proyecto.
Y por último el autor Daniel David Jaramillo Remache con el tema AUDITORÍA DE SEGURIDAD INFORMÁTICA PARA EL GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SANTA ANA DE COTACACHI, BASADA EN LAS NORMAS NTP ISO/IEC 17799:2007 Y LA METODOLOGÍA OSSTMM V2[7]. El cual concluye que se pudo constatar que los activos informáticos que posee el GAD municipal manejan información que es de mucha importancia para los ciudadanos del cantón, por lo tanto la auditoría de seguridad informática debe hacerse por gente altamente responsable, ya que una auditoría mal hecha puede acarrear consecuencias drásticas para la empresa auditada.

2.2. Fundamentación Teórica.

2.2.1. Seguridad

El término seguridad proviene del latín "securitas", éste significa el tener conocimiento y certeza sobre algo. La palabra seguridad refiere a la ausencia del peligro, miedo y riesgos[8].

2.2.2. Seguridad Informática

La seguridad informática es una disciplina que se encarga de proteger la integridad y la privacidad de la información almacenada en un sistema informático. De todas formas, no existe ninguna técnica que permita asegurar la inviolabilidad de un sistema. Un sistema informático puede ser protegido desde un punto de vista lógico (con el desarrollo de software) o físico (vinculado al mantenimiento eléctrico, por ejemplo). Por otra parte, las amenazas pueden proceder desde programas dañinos que se instalan en la computadora del usuario (como un virus) o llegar por vía remota (los delincuentes que se conectan a Internet e ingresan a distintos sistemas)[9].

2.2.3. Escáner de Vulnerabilidades

El Escaneo de Vulnerabilidades es la identificación, análisis y reporte sistemático de las vulnerabilidades de seguridad técnica que terceros e individuos no autorizados pueden usar para explotar y amenazar la confidencialidad, integridad y disponibilidad del negocio, los datos técnicos y la información. El escaneo de vulnerabilidades interno examina específicamente el perfil de seguridad de la organización desde la perspectiva de alguien interno o de alguien que tiene acceso a los sistemas y las redes detrás del perímetro de seguridad externo de la empresa[10].

2.2.4. Pruebas de Penetración (PenTest)

Una prueba de penetración es una operación cuyo propósito es evaluar la seguridad de alguna infraestructura de TI al explotar sus debilidades y vulnerabilidades del mismo modo que lo haría algún hacker mediante los sistemas operativos, servicios, aplicaciones, configuraciones inapropiadas o comportamiento del usuario final[11].

2.2.5. Hacking

Técnicas y procedimientos utilizados por un hacker para cumplir un determinado objetivo. Suele asociarse esta palabra a procedimientos ilegales o malignos[12].

2.2.6. Hacking Ético

Hacking ético es una forma de referirse al acto de una persona usar sus conocimientos de informática y seguridad para realizar pruebas en redes y encontrar vulnerabilidades, para luego reportarlas y que se tomen medidas, sin hacer daño[13].

2.2.7. Auditoría

Auditoría es un término que puede hacer referencia a tres cosas diferentes pero conectadas entre sí: puede referirse al trabajo que realiza un auditor, a la tarea de estudiar la economía de una empresa, o a la oficina donde se realizan estas tareas (donde trabaja el auditor). La actividad de auditar consiste en realizar un examen de los procesos y de la actividad económica de una organización para confirmar si se ajustan a lo fijado por las leyes o los buenos criterios[14].

2.2.8. Auditoría de Red

Su objetivo es evaluar la seguridad de la red interna de una empresa ante la posibilidad de recibir ataques por parte de un hacker que haya conseguido alcanzar la intranet o ataques provenientes del personal interno a la empresa[15].

2.2.9. Metodología

Se entiende por metodología el conjunto de pautas y acciones orientadas a describir un problema. Por la general, la metodología es un apartado de la investigación científica[16].

2.2.10. 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[4]:

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

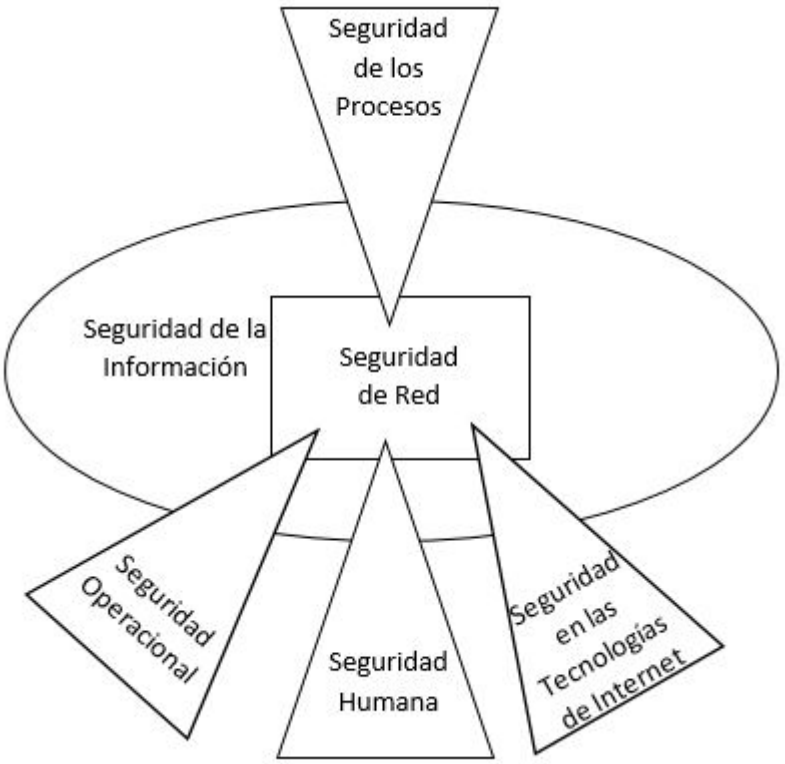


Figura 2.1: Mapa de Seguridad OSSTMM V3
Elaborado por: Christian Miranda

Cabe recalcar que de estos items se enfoca explícitamente a lo que se refiere en redes.

2.3. Propuesta de Solución

La Auditoría de Red en el Ministerio de Inclusión Económica y Social, mediante la metodología Open Source Security Testing Methodology Manual Version 3, permitiría detectar vulnerabilidades y riesgos informáticos desde el exterior al interior mediante Pruebas de Seguridad (PenTest) y Hacking Ético. Finalizando con la elaboración de Políticas de Contingencia de Seguridad Informática que

permitan resguardar y proteger la información buscando mantener la integridad, confidencialidad y disponibilidad de la misma.

CAPÍTULO 3

Metodología

3.1. Modalidad de la investigación

Este proyecto es de Investigación, Análisis y Resultados debido a que se recolectará información y posteriormente se analizará la misma y por último se recomendará que medidas hay que tomar para mejorar el rendimiento de la red, la investigación será bibliográfica porque utilizará fuentes como libros, documentos, artículos, revistas, etc. Para la construcción del marco teórico.
La investigación tendrá la modalidad de campo porque se buscará obtener la información en el lugar mismo en que se llevará a cabo el proyecto.

3.2. Población y muestra

La presente investigación por su característica si requiere población, el MIES esta conformada por 25 empleados a los cuales se puede referir como población, de estos empleados se recolecta información sobre el estado de la Red de la Empresa.

3.3. Recolección de información

Para la recolección de información interna se utilizará dos herramientas para la Auditoría Informática, la entrevista y la encuesta.
Se realiza una entrevista al director del Departamento de Sistemas.
Se aplica una encuesta con un cuestionario de preguntas del uso avanzado de equipos informáticos a profesionales que pertenecen al Departamento de Sistemas.
Se aplica una encuesta con un cuestionario de preguntas del uso básico de equipos informáticos a profesionales que pertenecen al Ministerio De Inclusión Económica Y Social.

3.4. Procesamiento y análisis de datos

Una vez terminada el proceso de recolección de información mediante la entrevista y las encuestas se procederá con el análisis de los resultados.

El procesamiento de datos se lo realizará utilizando una herramienta informática a fin de organizarlo a través de gráficos estadísticos de tal forma que permita observar el nivel de importancia que tiene la realización esta auditoría de red.

3.5. Desarrollo del Proyecto

A continuación, se definen actividades a seguir para el cumplimiento de los objetivos específicos planteados en el proyecto de Investigación y así obtener como resultado el objetivo general.

1. Determinar el tipo de Políticas de Seguridad Informática aplicadas en el Honorable Gobierno Provincial de Tungurahua para analizar y verificar los mecanismos de defensa internos y externos.
    - Análisis de la situación actual de la Institución en lo referente a los activos informáticos y sus políticas de seguridad.
    - Realización de encuestas dirigidas al personal que labore en la Institución.
2. Identificar las vulnerabilidades en los servidores de la red informática que puedan ser explotadas por intrusos malintencionados.
    - Análisis de las estrategias y herramientas necesarias para la ejecución de las Pruebas de Penetración (PenTest) y Hacking Ético.
    - Identificación de las vulnerabilidades en los servidores o fallos de sistemas que puedan ser explotadas por intrusos malintencionados.
3. Establecer un escenario virtual para ejecutar un ataque programado a los servidores de la red informática para explotar las vulnerabilidades que puedan ser utilizadas por intrusos malintencionados.
    - Realización de Pruebas de Penetración en un entorno controlado de manera que no se ocasionen problemas a la red institucional.
4. Elaborar Políticas de Contingencia de Seguridad informática que mejoren la integridad, confidencialidad y disponibilidad de la información en base a las vulnerabilidades detectadas.
    - Documentación de los estados de inseguridad detectados e incluyendo soluciones prácticas orientadas a resolverlos.
    - Elaboración de la propuesta de Políticas de Contingencia de Seguridad Informática que resguarde los activos informáticos asociados a los procesos del Honorable Gobierno Provincial de Tungurahua.

CAPÍTULO 4

Desarrollo de la propuesta

4.1. Introducción

Una vez revisado el diagnóstico del cual fue objeto el capítulo 3, se considera que el objetivo principal del departamento de Tics del MIES es tener continuidad en el servicio que día a día presta a la Ciudadanía del cantón, para esto es necesario de la auditoría a desarrollar.
Considerando que actualmente la red de Internet ha globalizado los procesos y ha facilitado el manejo de sistemas a través de la plataforma web, es de gran importancia contar con un método y procesos a seguir, mismo que impidan al máximo que información confidencial sea filtrada a terceras personas

4.1.1. Instalación de Equipos de Cómputo

- El departamento de Tics con la colaboración del departamento de inventarios y bodega tiene registrados cada uno de los equipos, propiedad del MIES.
- La protección física de los equipos será responsabilidad de quien sea asignado, y en caso de ser necesario el movimiento se deberá notificar al personal del departamento de Tics e inventarios y bodega

4.1.2. Mantenimiento de Equipos de Computo

- Es responsabilidad del departamento de Tics realizar el mantenimiento preventivo y correctivo de los equipos, así también la conservación de la instalación.
- Cuando el equipo necesite ser atendido por personas externas al MIES será necesario comunicar a inventario y bodega la salida del equipo fuera de las instalaciones para que se lleve un control proceso.
- El departamento de Tics es el encargado de informar a los usuarios, del personal que puede tener acceso a los equipos, así como brindar el servicio de mantenimiento y manipulación de los sistemas.

4.1.3. Reubicación de Equipos

- En caso de ser necesario el cambio un equipo tanto físico como de software este proceso se realizará únicamente por personal del departamento de Tics.
- El cambio de un equipo se notificará a inventarios y bodega, así como también el cambio de responsable de ser el caso

4.1.4. Control de Acceso al Equipo de Computo

- Cada uno de los equipos del MIES es asignado a un responsable, mismo que será el encargado del correcto funcionamiento del mismo.

4.1.5. Control de Acceso Local a la Red

- El departamento de Tics es el encargado de verificar constantemente el uso correcto del acceso a la red.
- El departamento de Informática es el encargado de la administración lógica y física de equipos especializados (switch, centrales telefónicas, enrutadores, entre otros) que se encuentren conectados a la red del MIES

4.1.6. Acceso a Internet

- El departamento de Tics es el responsable de controlar el acceso a los servidores de la red de internet, es decir solo se permitirá el acceso a páginas autorizadas por el MIES.

4.1.7. Adquisisción de Software

- El departamento de Tics es el encargado del análisis y selección de sistemas informáticos acorde a la necesidad institucional
- Es responsabilidad del departamento de Tics prever que los sistemas informáticos adquiridos provengas de sitios seguros y que se encuentren legalmente registrados por el autor.

4.1.8. Instalación de Software

- Es responsabilidad del departamento de Tics, la supervisión e instalación del software base para cualquier equipo.

- En los equipos de cómputo será instalado software con licenciamiento, o en su defecto software de código abierto acorde a la propiedad intelectual del autor.

4.2. Análisis de Factibilidad

El análisis de factibilidad se refiere a la disponibilidad de los recursos que son necesarios para desarrollar el proyecto, se debe tener ciertos aspectos de factibilidad

4.2.1. Factibilidad Operativa

En el Ministerio de Inclución Económica y Social (MIES), también se cuenta con los permisos necesarios para realizar la auditoría.

4.2.2. Factibilidad Técnica

Para la Implementación de la Auditoría de Red en el MIES se cuenta con el apoyo del Personal de la Institución pública, el departamento de Tics, el estudiante auditor con los conocimientos suficientes para el desarrollo del proyecto y los recursos necesarios como son un computador portátil con sistema operativo orientado a la seguridad informática Kali Linux, mencionando esto indica que es factible desde el punto de vista técnico.

4.2.3. Factibilidad Económica

Al contar con el apoyo del MIES y el departamento de Tics, se cuenta con los permisos para realizar un análisis de vulnerabilidades sobre la institución mediante el uso de software libre el cual no tiene costo de adquisición y los recursos necesarios como son computador portátil, investigación mediante el internet, traslados a las oficinas y otros, serán sustentados por el investigador, indicando que la investigación tiene factibilidad económica.

4.3. Fundamentación

Kali linux

Es un Sistema Operativo orientado a la auditoría y seguridad informática en general. Distribución avanzada para Pruebas de Penetración, Hacking Ético y evaluaciones de la seguridad de la red[17].

Maltego

Es una herramienta de código abierto creado por Paterva para el análisis y la visualización de las conexiones de datos, utiliza un sistema de entidades sobre las cuales se pueden realizar transformaciones y así obtener mayor información de la misma (dispositivos, DNS, servidores de correo, ips, tecnologías aplicadas, documentos, números telefónicos, correos, etc)[18].

Buscador web de Google

Buscador web de Google, es el primer producto de la empresa Google Inc. y producto estrella de ésta. En él se pueden realizar búsquedas de webs por la W.W.W. a base de un algoritmo exclusivo. Es el buscador más utilizado por la clasificación de páginas web que realiza y sus opciones de búsqueda avanzada[19].

FOCA

Es una herramienta para buscar metadatos e información oculta en documentos ofimáticos y pdf/ps/eps, extrae todos los datos para obtener información relevante de una empresa. Foca hace un Google y Bing Hacking para descubrir los archivos de extensión ya mencionados, los descarga, extrae los metadatos, organiza y muestra la información como usuarios del sistema, rutas de archivos, software utilizado, sistema operativo, fechas de creación y modificación de archivos, identificación de dispositivos, posicionamiento GPS, entre otras[20].

VisualRoute

Esta herramienta permite de una manera gráfica localizar los sitios por donde fluye una información hasta llegar a un destino. Es útil para localizar por donde pasa la información y desde donde se inicia a partir de una dirección web o una IP. Con esta herramienta podemos localizar el servidor de una web, lo que nos permite por tanto investigar si es fiable o no. Además permite realizar ping, tracer routers y realizar Whois[21].

TheHarvester

El objetivo de este programa es reunir a los correos electrónicos, subdominios, hosts, nombres de empleados de diferentes fuentes públicas, como los motores de búsqueda, los servidores de base de datos informáticas. Esta herramienta está diseñada para ayudar a los probadores de penetración en las primeras etapas de la prueba de penetración a fin de comprender la huella de cliente en el Internet.

También es útil para cualquier persona que quiere saber lo que un atacante puede ver sobre su organización[22].

NMAP

Es un explorador de redes y puertos orientado a las auditorías de seguridad[23].

Hping3

Es un software orientado a la auditoría de la pila TCP / IP, para descubrir la política cortafuegos, para escanear los puertos TCP de diferentes modos, para transferir archivos a través de un servidor de seguridad y muchas otras cosas[24].

OpenVAS

El Sistema de Evaluación de Vulnerabilidad abierto (OpenVAS) es un marco de diversos servicios y herramientas que ofrecen una solución completa y potente de análisis de vulnerabilidades y gestión de vulnerabilidades[25].

Nessus

Es un analizador de seguridad de redes potente y fácil de usar, con una amplia base de datos de plugins que se actualiza a diario. Nessus es creado por Tenable Network Security Inc., el cual mejora permanentemente el motor nessus, diseña plugins para el analizador y directivas de auditoría[26].

Metasploit Framework

Es un framework desarrollada en Perl y Ruby en su mayor parte, que provee información acerca de debilidades o vulnerabilidades de seguridad informática y ayuda a la ejecución de pruebas de penetración, está desarrollado en lenguaje de programación Ruby y es software libre, también cuenta con interfaces las cuales se pueden utilizar para la explotación de vulnerabilidades [27].

Hydra

Es un software que permite realizar rápidos ataques de diccionario contra varios protocolos en los que incluyen telnet, ftp, http, https, smb, ssh, varias bases de datos, y mucho más[28].

Ettercap

Es un programa que permite interceptar conexiones, filtrar contenidos, generar ataques "ARP Spoofing" entre otras características[29].

Iptables

Es la entrada de seguridad en una serie de servicios de firewall y administración de sistemas Linux, iptables es un producto de seguridad de uso generalizado mediante reglas[30].

Sslstrip

Es un programa para sistemas operativos linux capaz de descifrar tráfico https que viaja a través de una red [31].

4.4. Metodología

Para el presente proyecto se utiliza la metodología OSSSTMM V3 creada por el Instituto de Seguridad y Metodologías Abiertas (ISECOM). Se trata de una metodología para probar la seguridad operativa de ubicaciones físicas, las interacciones humanas, y todas las formas de comunicaciones tales como inalámbrica, cable, analógica y digital.
Una auditoría OSSTMM es una medición precisa de la seguridad a nivel operativo que está vacío de las hipótesis y evidencias anecdóticas [4]. La metodología tiene como propósito proporcionar una metodología científica para la exacta caracterización de la seguridad operacional a través del test y correlación de los resultados de pruebas de una manera consistente y fiable.

- Seguridad de Redes

Esta sección se refiere a la interacción entre el analista con la parte física de la red, esto se refiere a el cableado de la misma y realiza pruebas en los dispositivos de comunicación como VoIP, FAX, Correo de voz, PBX [4].

- Seguridad Informática

En esta sección se revisa la recolección de información en internet, para posteriormente comprobarlos en la empresa [4].

- Seguridad Inalámbrica

Se evalúan dispositivos que ofrecen comunicación sin cables, el objetivo es buscar configuraciones por defecto o comunicaciones inalámbricas inadecuadas [4].

- Seguridad en las Tecnologías de Internet

Esta sección identifica los servicios de los servidores en cuestión y aplicaciones de internet en busca de vulnerabilidades para luego de detectarlas proceder a explotarlas y generar su posible solución. También se realiza pruebas dirigidas en lo referente a peticiones de internet y sistemas de detección de intrusos [4].

Estudio de la OSSTMM y el planteamiento de la propuesta

Para que el analista pueda realizar una auditoría OSSTMM V3 correctamente se debe seguir las siguientes directrices:

- Recolección de información
- Sondeo de red
- Búsqueda de Vulnerabilidades
- Explotación de Vulnerabilidades

Mediante el estudio de la metodología OSSTMM y de acuerdo a los resultados esperados junto con las etapas descritas, se identifican las secciones y módulos específicos para la realización de las Pruebas de Seguridad de manera exitosa.

Etapa	Sección	Módulo
Recolección de información	Seguridad Informática	Revisión del esquema de la red
		Recolección de documentos
Sondeo de red	Seguridad de Red	Sondeo de la Red
		Identificación de Servicios y Sistemas
Búsqueda de Vulnerabilidades	Seguridad de Tecnologías de Internet	Búsqueda y verificación de vulnerabilidades
Explotación de Vulnerabilidades	Seguridad de Tecnologías de Internet	Búsqueda y verificación de vulnerabilidades

Tabla 4.1: Sección y Módulos aplicables al proyecto

Elaborado por: Christian Miranda

En la tabla 4.1 se puede observar la relación Etapa-Sección-Módulo que identifica la sección y módulos a seguir para el cumplimiento de cada una de las etapas de la Prueba de Seguridad y, a continuación, se los detalla.

Sección Seguridad Informática

Módulo Revisión del Esquema de la Red

En este módulo se determina como se encuentra estructurada la red y como se encuentra distribuida entre cada uno de los departamentos de la empresa.

Módulo Recolección de Documentos

En este módulo es importante la verificación de la información obtenida y perteneciente a varios niveles de lo que se considera seguridad de la información.

Sección Seguridad de Red

Módulo Sondeo de la Red

Introducción a los sistemas a estudiar, enviar consultas periódicamente a los dispositivos en la red las cuales determinaran el comportamiento de la misma. Se encuentra el número de sistemas alcanzables que deben ser analizados sin exceder los límites legales.

Módulo Identificación de Servicios y Sistemas

Prueba invasiva mediante las herramientas escogidas de los servicios y puertos del sistema en los niveles de transporte de red.

Sección Seguridad de Tecnologías de Internet

Módulo Búsqueda y Verificación de Vulnerabilidades

Se identifica y verifica las debilidades, falencias de configuración y vulnerabilidades que se encuentran en un activo o en un control y que puede ser explotada por una o más amenazas y de esta manera generar un impacto negativo en un servidor.
En la figura 4.1 del mapa de seguridad OSSTMM V3 se puede observar las secciones identificadas, estas secciones son seleccionadas tomando en cuenta que me limitaré a lo que me sea de utilidad para realizar correctamente la auditoría exclusivamente de red y cumplir los objetivos prefijados.

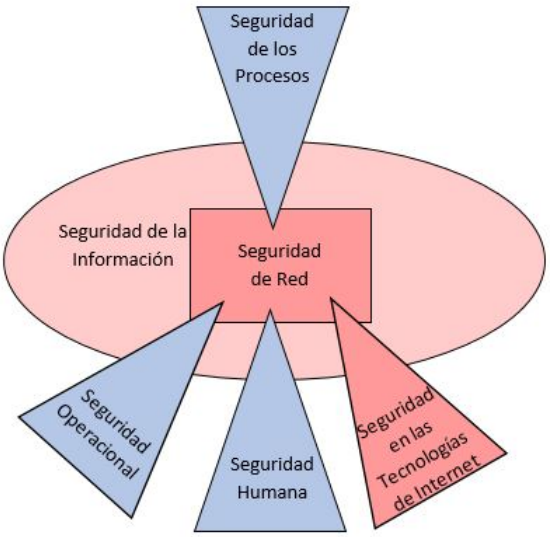


Figura 4.1: Secciones OSSTMM V3 utilizadas en el proyecto
Elaborado por: Christian Miranda

4.5. Determinaión del tipo de Políticas de Seguridad Informática aplicadas en el Ministerio de Inclusión Económica y Social

4.5.1. Análisis de la Situación Actual de la Institución en lo referente a los activos informáticos y sus Políticas de Seguridad

Mediante la entrevista aplicada al director del Departamento de Tics, a continuación, se presenta cada una de las preguntas con su respectiva respuesta, debido a que el director es nuevo en la institución sus respuestas fueron en base a documentación de anteriores directores.

1. **¿Cuántos y cuáles son sus departamentos?**

   El MIES cuenta con 41 departamentos distribuidos en 3 pisos los cuales se dividen de la siguiente manera:

   El departamento de Coordinador Zonal se subdivide en 7 departamentos los cuales son: Secretaría, Comunicación Social, Participación ciudadana, Coordinación de Servicios Sociales, Coordinación Administrativa Financiera, Coordinación de Planificación, Coordinación Judicial.

   El departamento de Coordinación de Servicios Sociales se subdivide en los siguientes departamentos: Coordinadora la cual cuenta con su Asistente, Desarrollo Infantil, Proyecto de Formación Continua, Gerontología, Protección Especial, Discapacidades, Bono Joaquín Gallegos Lara, Acom-

pañamiento Familiar, Inclusión Económica y Adopciones el mismo que se subdivide en Psicólogo y Trabajadora Social.

El departamento de Coordinación Administrativa Financiera se subdivide en los siguientes departamentos: Coordinadora la cual cuenta con su Asistente, departamento de presupuesto, departamento de contabilidad, Administrativo, Talento Humano, Tics, Infraestructura, Activos Fijos, Auxiliar de Servicios, Conductores, Recepción.

El departamento de Coordinación de Planificación se subdivide en los siguientes departamentos: Coordinador con su Asistente, Planificación, Planificación 2, Procesos Calidad.

Por último, el departamento de Coordinación Judicial se subdivide en los siguientes departamentos: Coordinador, Abogado 1 y Abogado 2.

A continuación, el esquema de la Institución quedaría de la siguiente manera:

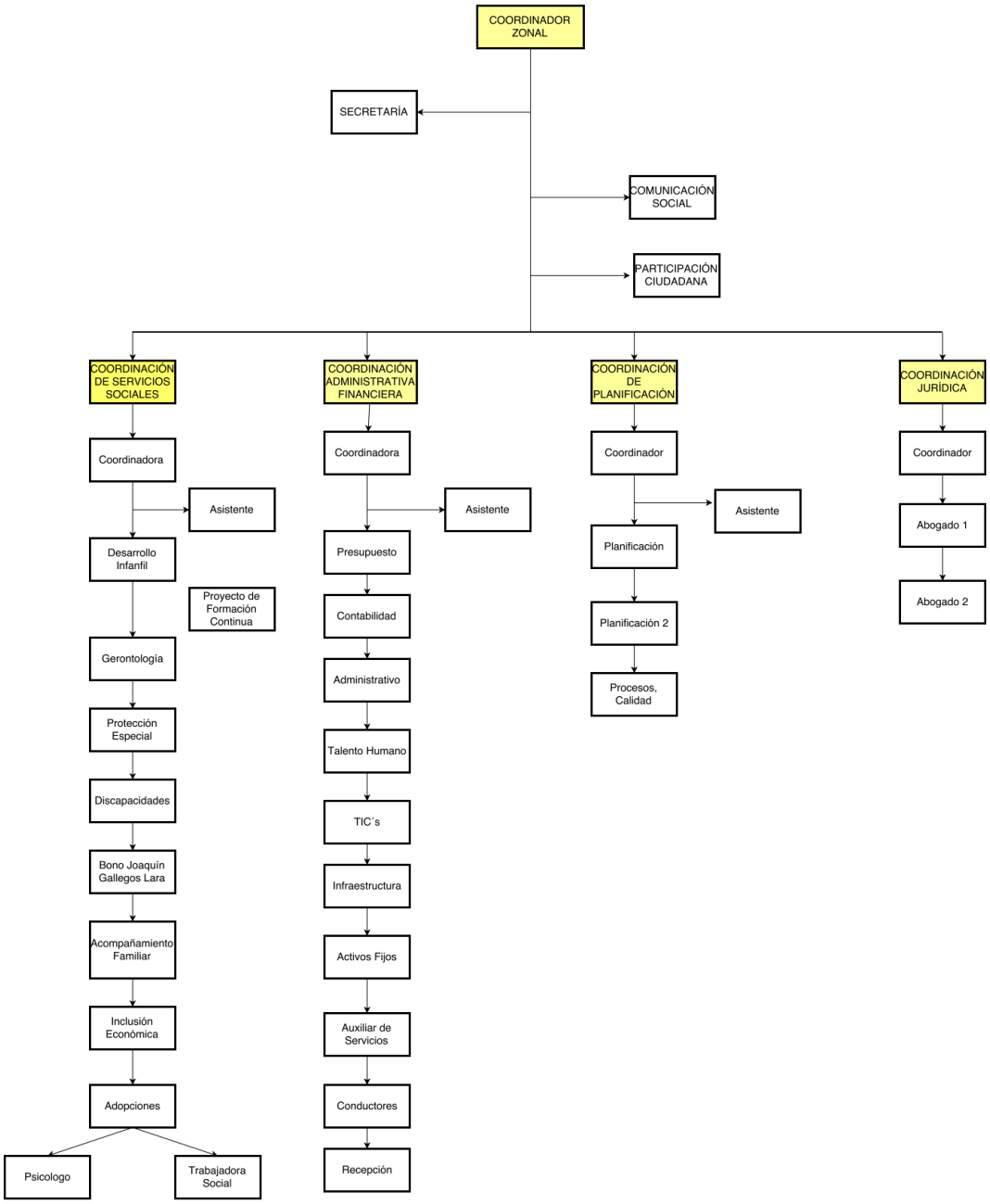


Figura 4.2: Esquema MIES
Elaborado por: Ministerio de Inclusión Económica y Social

2. **¿Qué topología física de la red utilizan?**

   La topología que esta implementada en esta Institución es denominada como topología de estrella y graficamente el esquema de red es de la siguiente manera:

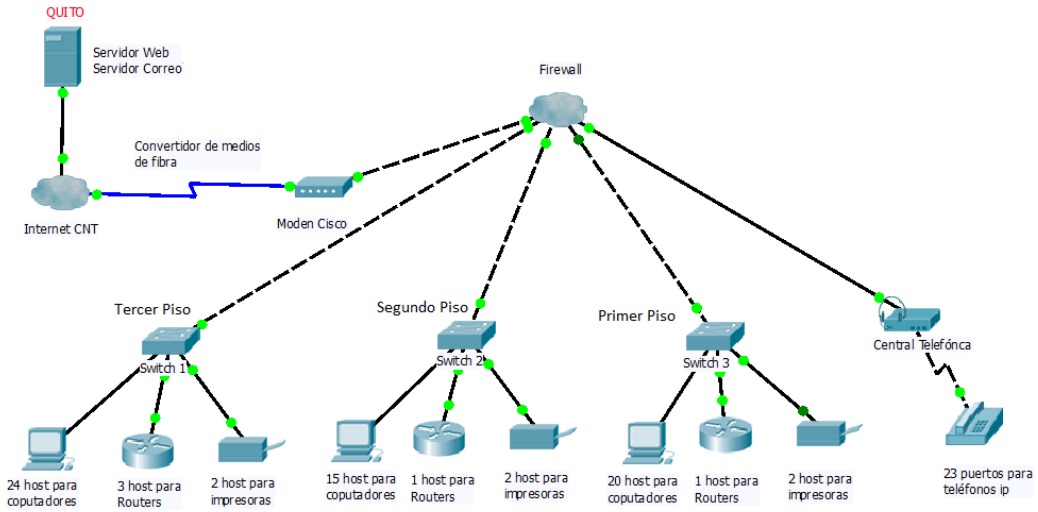


Figura 4.3: Esquema MIES
Elaborado por: Christian Miranda

En la figura 4.3 se puede observar que el Servidor tanto web, de correo y el Kaspersky con el cual se maneja el ministerio se encuentra alojado en Quito, se conectan al mismo vía Internet de la compañía CNT, el mismo que llega a un modem cisco y después de pasar x el firewall se conecta a 3 switchs uno para cada piso y una central telefónica.

En el switch designado para el tercer piso cuentan 20 host para computadores, 3 para routers y 2 para impresoras en red, en el switch asignado al segundo piso cuenta con 15 host para computadores, un host para router y 2 host para impresoras en red y por último en el switch asignado al primer piso se cuenta con 20 host para computadores, 1 host para routers y 2 host para impresoras en red.

La central telefónica cuenta con 23 host para teléfonos ip los cuales se distribuyen entre los 3 pisos y los diferentes departamentos de la institución.

3. **¿Tienen Servidor de correo?**

   Si cuenta con un servidor de correo llamado Zimbra en el cual trabajan con el dominio inclusion.gob.ec.

4. **¿Qué base de datos operan y cuáles son sus características?**

   En lo que se refiere a base de datos solo me supo manifestar que trabajan con PostgreSQL, en cuanto a características del mismo no me supo manifestar por el motivo de que el servidor se encuentra alojado en Quito y solo tenía acceso a algunas tablas.

5. **¿Cada cuánto tiempo se brinda mantenimiento a los equipos?**

   Me supo manifestar que se brinda mantenimiento con irregularidad a los equipos, pero por lo general brindan mantenimiento una vez cada 15 días como manera preventiva y para verificar malware.

6. **¿Las Instalaciones (aulas, cubículos, cableado y oficinas) fueron diseñadas o adaptadas para su funcionamiento?**

   Si se considera y cabe recalcar que la mayoría de cableado están ubicados correctamente en sus canaletas y sin obstaculizar nada, en lo referente a los cubículos están ergonómicamente bien ubicados.

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

   El Departamento de Contabilidad de la Institución es el encargado de llevar el inventario de todos los bienes tanto muebles como informáticos, cada uno con su respectiva documentación, en lo referente a software se lleva su registro con sus respectivas licencias y manuales pero esta no se encuentra en el departamento de contabilidad sino en el departamento de Tics, pero contabilidad lleva constancia.

8. **¿Se tienen equipos dedicados a monitorear el tráfico y actividades de la red?**

   No se cuenta, el director de Tics, es reciente en ese puesto por lo que aun se esta acoplando a sus actividades laborales, pero por el momento no monitorea el trafico de la red.

9. **¿Que sistemas tiene bajo su cargo o responsabilidad?**

   Los sistemas a cargo del Director de Tics son Zimbra administrador de correos, Quipux, SIMIES, ALFAMIES, INFOMIES, RIPS, BASE DE DATOS, MESA DE SERVICIOS, estos como principales.

10. **¿Con qué frecuencia cambia sus contraseñas, de que longitud es, utiliza caracteres especiales?**

    Por lo general se cambian las contraseñas cuando se realiza el mantenimiento, esto se maneja por active directory cada dos meses, la contraseñas mínimo cuentan con 8 caracteres entre mayúsculas, minúsculas y caracteres especiales.

11. **¿Se tienen instalado programa antivirus en su equipo con sus respectivas actualizaciones?**

    Cada equipo cuenta con su respectivo antivirus Kaspersky actualizado tanto la licencia como la versión, se cuenta también con firewall el cual filtra las peticiones de cada uno de los host.

12. **¿Se posee bitácoras de fallos o ataques detectados en el servidor?**

    No, los equipos son revisados remotamente desde Quito y los errores o fallos que se han presentado no son considerados como ataques, pero en caso de haberlos la central en Quito lo informaría inmediatamente.

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

    Si, los permisos son asignados de manera que un usuario no pueda contar con más privilegios de los necesarios.

14. **¿Se tienen sistemas de seguridad para evitar que se sustraiga equipo de la institución?**

    En el edificio se cuenta con un guardia de seguridad el cual es muy cuidadoso con quien deja entrar y salir, en cuanto a cámaras de seguridad no tienen.

15. **¿Se cuenta con Políticas de Seguridad Informáticas?**

    Si se cuenta con políticas de seguridad con sus manuales de seguridad.

16. **¿Se concientiza a los usuarios mediante charlas o reuniones a prevenir los "ataques informáticos"?**

    Reuniones y/o charlas para dar a conocer sobre amenazas de Seguridad en la Informática están en proceso de implementación.

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

    Si, cada equipo cuenta con su respectivo antivirus actualizado, se cuenta con un firewall el cual filtra las peticiones de cada uno de los host.

4.5.2. Realización de encuesta Dirigida al Personal que Labora en el MIES

Encuesta dirigida a 22 profesionales del Ministerio de Inclusión Economica y Social.

Se aplican preguntas del uso básico de las cuales el personal laboral del Instituto tenia conocimiento.

1. **¿Su usuario y contraseña, la tiene guardada en?**

   Celular____ Computador____ Papel____ La Memoriza____

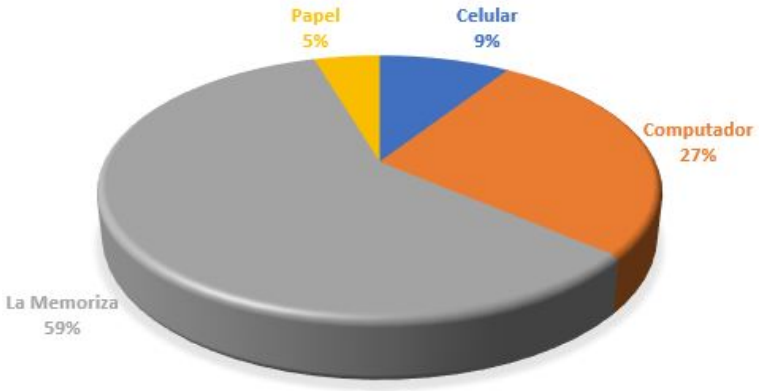


Figura 4.4: Pregunta: ¿Su usuario y contraseña, la tiene guardada en?
Elaborado por: Christian Miranda

El 59 % de la población encuestada menciona que su usuario y contraseña la tienen memorizada, siendo esto recomendable y seguro ante algún plagio de los mismo y de esta manera acceder a los datos tanto de la empresa o Institución como personales.

2. **¿Con qué frecuencia cambia su contraseña?**

   2 meses____ 3 meses____ 6 meses____ 1 año____ nunca ____

Figura 4.5: Pregunta: ¿Con qué frecuencia cambia su contraseña?
Elaborado por: Christian Miranda

El 54 % de la población encuestada menciona que cambia o es cambiada su contraseña por el departamento de Tics en un periodo de no más de 3 meses lo cual considero bastante bueno y seguro para evitar el robo o decifrado de credenciales.

3. **¿Usualmente en su contraseña suele usar?**

   Números____ letras mayúsculas____ letras minúsculas____ caracteres especiales____

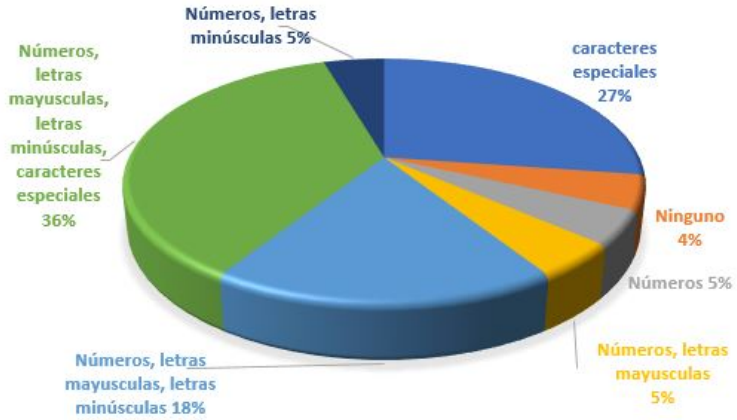


Figura 4.6: Pregunta: ¿Usualmente en su contraseña suele usar?
Elaborado por: Christian Miranda

El 36 % del personal utiliza contraseñas denominadas como robustas ya que

estas tienen características como una combinación alfanumérica y junto con caracteres especiales, que es una muy buena manera de proteger la información que llevan en sus ordenadores.

El 18 % del personal utiliza contraseñas denominadas como poco robusta ya que estas solo tienen características como una combinación alfanumérica, que es una manera aceptable de proteger la información, pero aun así es recomendable.

el otro 6 % del personal no se preocupan por la seguridad de sus datos y supieron dar escusas de que se olvidan las contraseñas, si en las mismas las digitan con combinaciones alfanuméricas y de caracteres, y como constantemente cambia de Director de Tics el MIES no mantienen una metica en ese aspecto.

4. **¿Cada cuánto tiempo se brinda mantenimiento a los equipos?**

   2 meses____ 3 meses____ 6 meses____ 1 año____ nunca ____

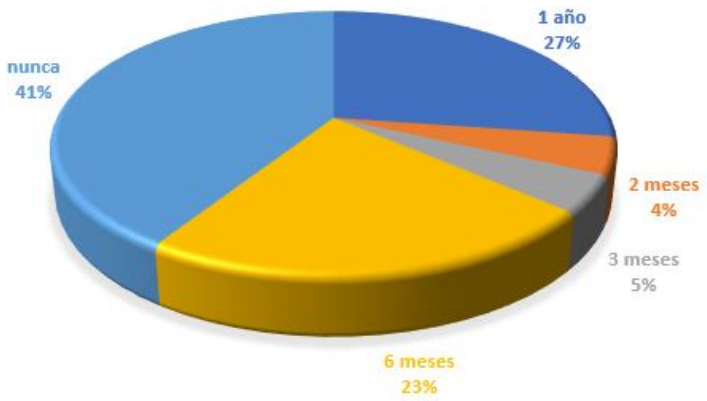


Figura 4.7: Pregunta: ¿Cada cuánto tiempo se brinda mantenimiento a los equipos?
Elaborado por: Christian Miranda

El 41 % del personal menciona que nunca se brinda mantenimiento a los equipos y el 27 % menciona que se brinda cada año, esto para nada es recomendable ni mucho menos seguro, ya que por esto los equipos podrían estar infestadas de virus, los cuales hacen que tanto los equipos como el acceso a internet sean lentos.

Aunque en el Departamento de Tics supieron decirme que si se da mantenimiento cada 2 o 3 meses cuando se cambian las contraseñas y que de los virus se encarga el Kaspersky.

5. **¿Cree que las medidas de seguridad que se manejan dentro del MIES sean seguras y adecuadas?**

   Si ____No ____ ¿Por qué? _____

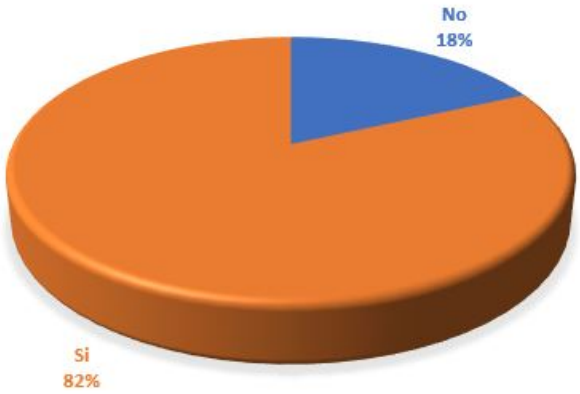


Figura 4.8: Pregunta: ¿Cree que las medidas de seguridad que se manejan dentro del MIES sean seguras y adecuadas?
Elaborado por: Christian Miranda

El 82 % menciona que las medidas de seguridad si son las adecuadas, argumentan que se brinda capacitaciones según los manuales que tienen en el departamento de Tics y la estructura del edificio está acorde a las conexiones.

6. **En el departamento de Tic's, ¿se realizan actividades para su monitoreo?**

   Si____ No ___ ¿Cuáles? _____

Figura 4.9: Pregunta: En el departamento de Tic's, ¿se realizan actividades para su monitoreo?
Elaborado por: Christian Miranda

En el departamento de Tics no se realizan las actividades de monitoreo, eso me supo manifestar su director, pero el monitoreo es realizado desde la central en Quito y si existe alguna anomalía informan al departamento de Tics el cual debe tomar control sobre la anomalía, por lo tanto, si se realiza actividades de monitoreo y el 45 % del personal es consciente del mismo.

7. **¿Se revisa y actualiza el Software Instalado frecuentemente?**

   Si ___ No___ Frecuencia_____

Figura 4.10: Pregunta: ¿Se revisa y actualiza el Software Instalado frecuentemente?

Elaborado por: Christian Miranda

El 73 % responde que los sistemas operativos no son revisados con frecuencia, pero si cuentan con las respectivas licencias

8. **¿Se ha dado a conocer sobre los "ataques informáticos", y las maneras de evitarlos?**

   Si___ No ___ (Observación_____)

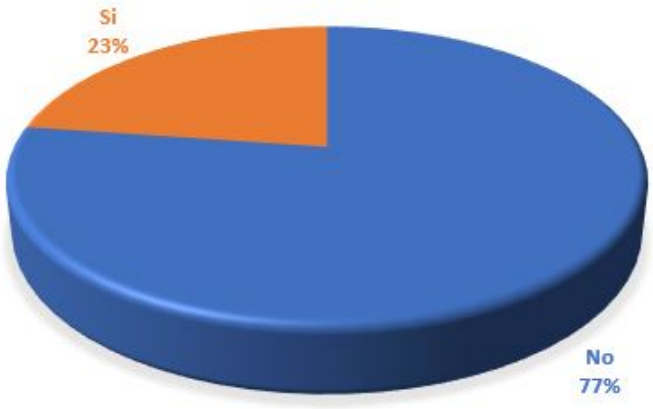


Figura 4.11: Pregunta: ¿Se ha dado a conocer sobre los "ataques informáticos", y las maneras de evitarlos?
Elaborado por: Christian Miranda

El 77 % del personal no tiene conocimientos sobre ataques informáticos ni mucho menos saben cómo reaccionar en caso de ser víctima de uno, en este aspecto esta encargada el director de Tics porque en caso de haber algún ataque se le reportara a él para que tome medidas sobre el asunto.

9. **¿Sabe del manejo de Políticas de Seguridad Informática?**

   Si___ No ___ (Observación_____)

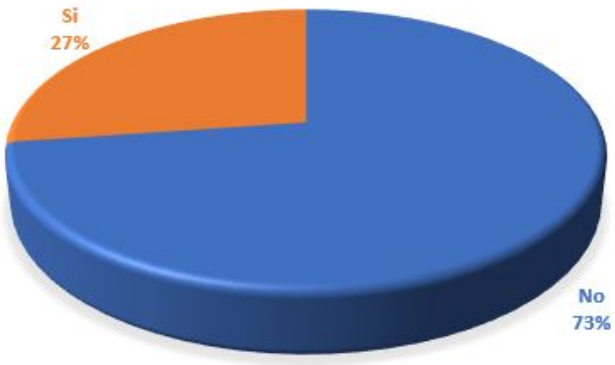


Figura 4.12: Pregunta: 9. ¿Sabe del manejo de Políticas de Seguridad Informática?
Elaborado por: Christian Miranda

El 73 % del personal encuestado no sabe del manejo de Políticas de seguridad, pero si tienen y recientemente se esta concientizando al personal del MIES de la existencia de las mismas.

10. **¿Su equipo de trabajo cuenta con internet? de ser el caso ¿cómo califica el servicio?**

    No cuenta___ Excelente____Bueno___ Regular___ Malo___ Pésimo___ ¿Por qué?_____

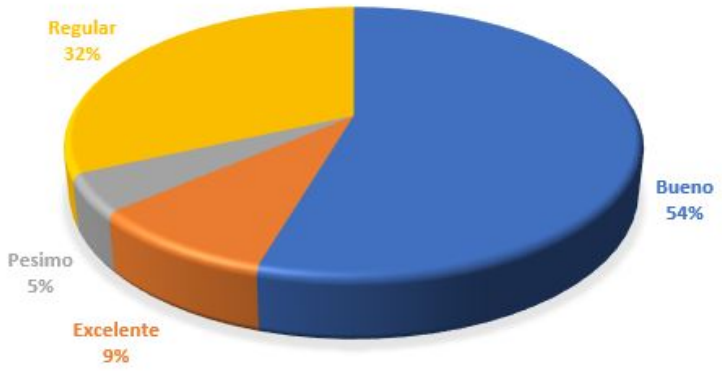


Figura 4.13: Pregunta: ¿Su equipo de trabajo cuenta con internet? de ser el caso ¿cómo califica el servicio?
Elaborado por: Christian Miranda

El 100 % de los encuestados cuentan con acceso a internet, el 9 % de los encuestados lo califica como excelente, el 54 % de los encuestados lo califican como bueno, el 32 % de los encuestados lo califican como regular y el 5 % de los encuestados lo califican como pésimo, el 37 % de encuestados que mencionan que el internet esta entre regular y pésimo, informan que la razón de su calificación es por el motivo que existen restricciones.

11. **Cuando quiere consultar una página para obtener información ¿tiene acceso a ella?**

    Si ___No ___ ¿Por qué?_____

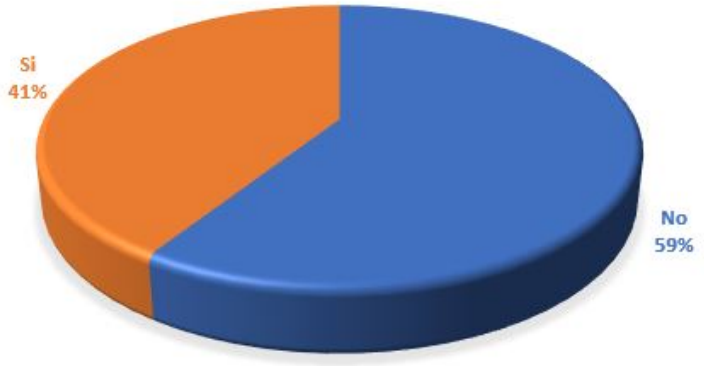


Figura 4.14: Pregunta: Cuando quiere consultar una página para obtener información ¿tiene acceso a ella?
Elaborado por: Christian Miranda

Del 100 % de encuestados con acceso a internet, el 59 % indican que no pueden obtener la información de manera completa que se solicita porque califican el servicio de internet entre regular y pésimo, también me saben manifestar que tienen varias páginas restringidas las cuales creen que son necesarias para consultas, creen conveniente tener un acceso sin restricciones.

4.6. Identificación de vulnerabilidades en los servidores de la red informática que puedan ser explotadas por intrusos malintencionados

4.6.1. Análisis de las estrategias y herramientas necesarias para la ejecución de las Pruebas de Penetración y Hacking Ético

Tipo	Características	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 las vulnerabilidades y fallos encontrados
Test de Penetración	Tiene un objetivo definido	Si	Tiene establecido un objetivo en partes específicas de la Infraestructura Tecnológica
	Tiene en cuenta el entorno de seguridad actual	Si	Aplica vulnerabilidades y fallos conocidos
	Trata de comprometer los sistemas objetivos	Si	Lista trata de comprometer los sistemas objetivos
	Explota las vulnerabilidades	Si	Explota las vulnerabilidades en un entorno real y virtual (similar un ataque real)
Hacking Ético	Tiene un objetivo definido	No	Toda la infraestructura Tecnológica es su objetivo
	Tiene en cuenta el entorno de seguridad actual	No	Actúa como un ataque real
	Trata de comprometer los sistemas objetivos	Si	Su análisis es más complejo y profundo al comprometer los sistemas objetivos
	Explota las vulnerabilidades	Si	Explota las vulnerabilidades de manera directa y pura

Tabla 4.2: Tipos de Análisis y Detección de Vulnerabilidades

Elaborado por: Christian Miranda

Mediante el análisis del tipo de detección y explotación de vulnerabilidades como se puede observar en la tabla 4.2 el Test de Penetración (Pentest) es elegido para la aplicación en el presente proyecto por orientarse a los servidores de la Institución.

Herramientas de reconocimiento

Características	Maltego	The Harvester	Anubls	Foca	Uniscan	VisualRoute
Costo	Versión libre y de paga	Versión libre	Versión libre y de paga	Versión libre y de paga	Versión libre	Versión de paga
Plataforma	Windows, Mac, Linux	Linux	Windows	Windows XP, 7, 8, 8.1, Server, Vista (32/ bits)	Linux	Windows XP/ 2003/ Vista/ 7/ 8.1, Mac OS X
Actualización / Soporte	Si	Si	No	Si	Si	Si
Facilidad de Manejo	Medio	Medio	Fácil	Fácil	Medio	Fácil

Tabla 4.3: Herramientas de reconocimiento

Elaborado por: Christian Miranda

De acuerdo a la tabla 4.3, Maltego, The Harverster y Uniscan cuentan con sus versiones libres y constante actualización, también se suma que éstas herramientas ya vienen instaladas en Sistema Operativo Kali Linux.
También se eligió Visual Route y FOCA con sus versiones de prueba limitadas por 30 días.

Herramientas de Sondeo de puertos

Características	SuperScan 4	NetScan 6	Nmap
Costo	Versión libre y de paga	Versión libre y de paga	Gratuito
Plataforma	Windows	Windows	Linux, Windows, Mac OS X y Unix
Actualización / Soporte	Si	Si	Si
Facilidad de Manejo	Fácil	Fácil	Fácil

Tabla 4.4: Herramientas de sondeo de puertos

Elaborado por: Christian Miranda

Mediante el análisis de la tabla 4.4 la utilización de NMAP por el momento resulta ser a mi criterio la más eficaz porque cuenta con varias funciones y scripts para

sondear la red de la Institución, incluyendo la detección de equipos y sistemas operativos.

Herramientas de detección de vulnerabilidade

Características	OpenVAS	Nessus	Retina	Nexpose
Costo	Versión libre	Versión libre y de paga	Versión libre y de paga	Versión libre
Plataforma	Centos, Debian, Fedora, OpenSuse Red Hat, Ubuntu, Windows	Microsoft Windows, Mac OS X, Linux, FreeBSD	Windows Server 2008 o versiones y posteriores requiere para su instalación de .Net Framework 3.5. servidor IIS habilitado y Microsoft SQL 2008 o posterior	MS Windows Server 2003 SP2 / Server 2003 R2, Red Hat Enterprise, Ubuntu LTS, SuSE Linux
Actualización / Soporte	Si	Si	Si	Si
Facilidad de Manejo	Fácil	Fácil	Fácil	Fácil

Tabla 4.5: Herramientas de detección de vulnerabilidades

Elaborado por: Christian Miranda

Por limitación de las herramientas de detección de vulnerabilidades en sus versiones libres (ver tabla 4.5), se elige Open Vas y Nessus que son las más opcionadas en cuanto al número de direcciones ip a analizar, actualización y generación de reportes.

Herramientas de explotación

Características	Metasplot	Hping3	Hydra	Ettercap
Costo	Versión libre y de paga	Versión libre	Versión libre	Versión libre
Plataforma	Windows 6-Bit, Linux: 6/32 Bits	GNU/Linux, FreeBSD, Solaris, NetBSD, Open BSD Y Mac OS X.	Linux	Linux / Windows
Actualización / Soporte	Si	Si	Si	Si
Facilidad de Manejo	Medio	Fácil	Fácil	Fácil

Tabla 4.6: Herramientas de explotación de vulnerabilidades

Elaborado por: Christian Miranda

El sistema Operativo Kali Linux diseñado principalmente para la Auditoría y Seguridad Informática en general, trae preinstalados más de 600 programas incluyendo Metasploid (software de pruebas de penetración), Ettercap (un sniffer), Hydra (crakeador de passwords) entre otras herramientas (ver tabla 4.6) las cuales son seleccionadas para utilizar en el presente proyecto.

4.6.2. Identificación de las vulnerabilidades en los servidores o fallos de sistemas que puedan ser explotadas por intrusos malintensionados

Para el cumplimiento de los módulos de las secciones en mención, se utiliza las herramientas informáticas ya etudiadas y seleccionadas

Sección Seguridad Informática

- **Módulo de Revisión de la Inteligencia Competitiva**

El objetivo de éste módulo es, recabar toda la información posible de la organización que se va a auditar, todo aquel documento el cual pueda revelar información. Esto se lo realiza de manera pasiva porque no se tiene un contacto directo con el personal que operan los servidores, por la razón de que estos se encuentran en Quito.
Mediante la herramienta Maltego se investiga las relaciones existentes que tiene un determinado dominio en este caso **inclusion.gob.ec.**

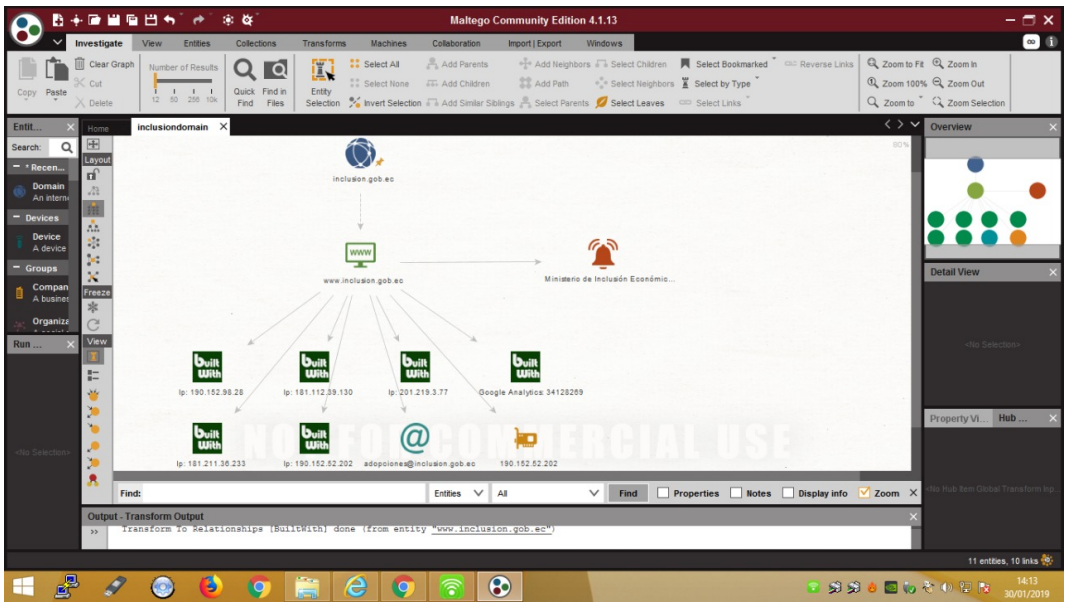


Figura 4.15: Maltego, transformación del dominio inclusion.gob.ec
Elaborado por: Christian Miranda

En la figura 4.15 se puede observar las transformaciones DNS aplicando a un tipo Domain nombrado inclusion.gob.ec, se muestra un servidor web relacionado y las tecnologías que utiliza el sitio mediante la API de BuilthWith.com, una dirección ip, también encontramos una dirección de correo electrónico el cual que utiliza la empresa para adopciones que es un servicio que brinda la misma y por último el título del sitio web.

Mediante la herramienta FOCA se busca toda la información relacionada a los dominios inclusion.gob.ec el cual sirve para extraer los metadatos relevantes de la Institución.

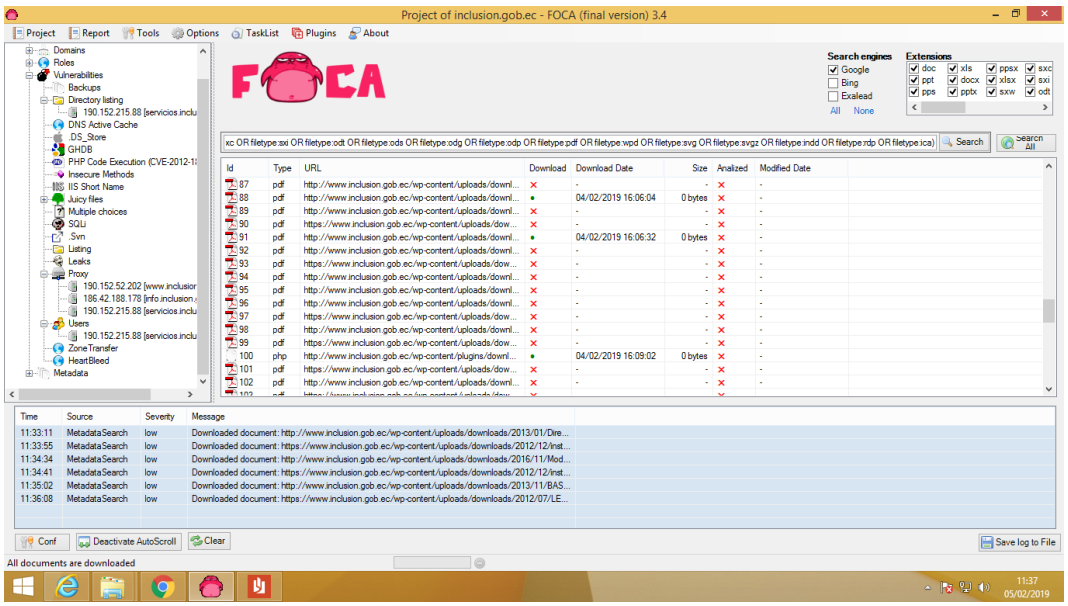


Figura 4.16: FOCA, nobres de usuarios detectados
Elaborado por: Christian Miranda

En la figura 4.16 se observa el resultado de un proyecto ejecutado en foca con el dominio inclusion.gob.ec, del cual se extrajeron 144 documentos entre los cuales podemos observar que hay currículos de empleados, proyectos realizados, matrices de costos y gastos en proyectos, solo se encontró un usuario el cual su dirección ip es 190.152.215.88 que pertenece a la página de servicios.inclusion.gob.ec.

El peligro de la extracción de los metadatos radica en que a través de un metadato se averigüe la versión de un sistema operativo o software el cual cuente con algún tipo de fallo o vulnerabilidad que pueda ser explotada, pero en este caso no encontramos nada de eso, apenas se puede apreciar el servidor web en la cual se crearon las páginas que es nginx.

Con la herramienta de VisualRoute se conoce la localización de un sitio web y los saltos que realizan los datos para llegar a su destino.

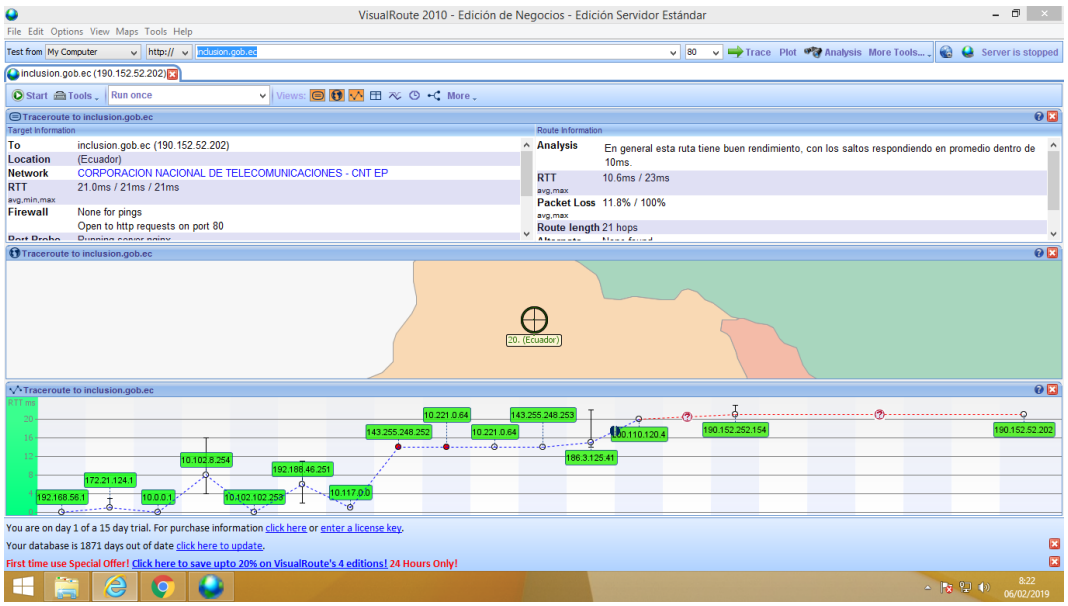


Figura 4.17: Visual Route a www.inclusion.gob.ec
Elaborado por: Christian Miranda

En la figura 4.17 se observa el trazado de una ruta que unen 14 host siendo estos desde el host local y la web www.inclusion.gob.ec, el motivo por el cual el trazado da tantos saltos es por la distancia que se encuentra el servidor (el servidor se encuentra en Quito) del lugar en el cual se hace la consulta, la importancia de investigar la ubicación es de saber si cuentan con un servidor local u oficinas con host externo lo cual significa la intrusión en empresas privadas, en este caso no se cuenta con servidor local, son extensiones en donde se dan los saltos cada milisegundo(ms).

Con la herramienta TheHarvester se obtiene información relacionada al dominio en investigación.

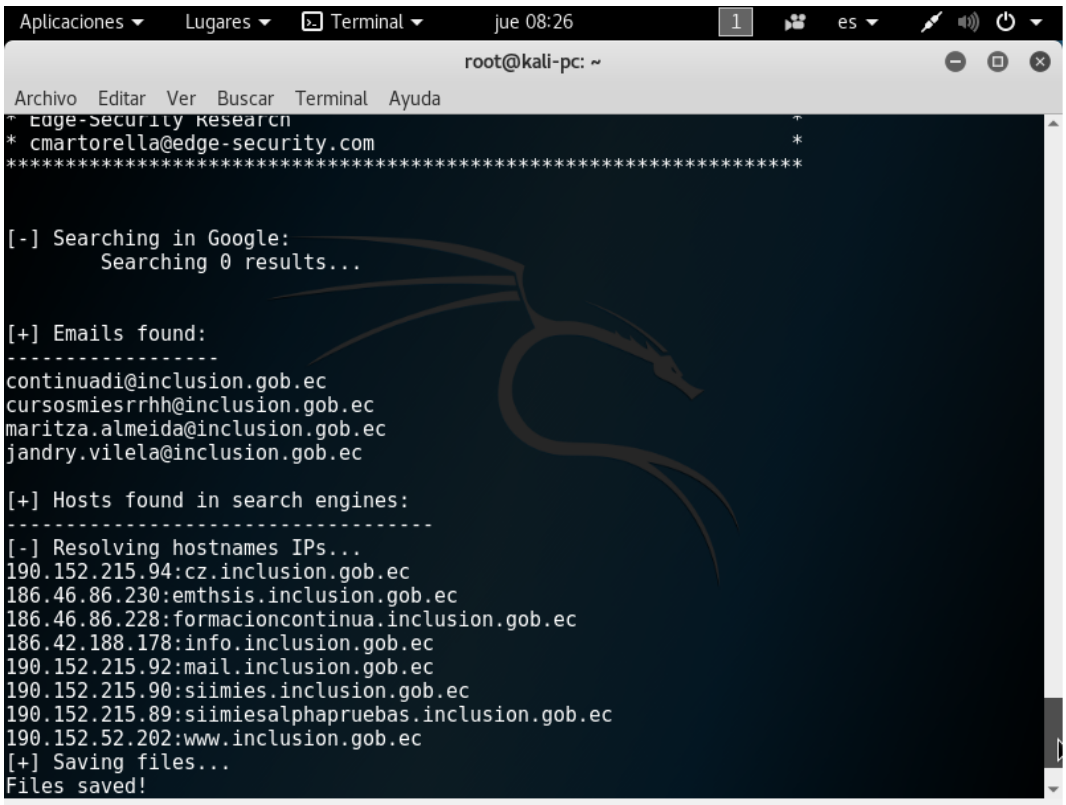


Figura 4.18: TheHarvester a dominio inclusion.gob.ec
Elaborado por: Christian Miranda

En la figura 4.18 se puede observar resultados de la ejecución de TheHarvester dando como resultado varios correos electrónicos y servidores relacionados al dominio inclusion.gob.ec.

Con esta herramienta también puedo obtener un reporte de la búsqueda, el mismo que se puede descargar en los formatos .html y .xml como se observa a continuación en la figura 4.19.

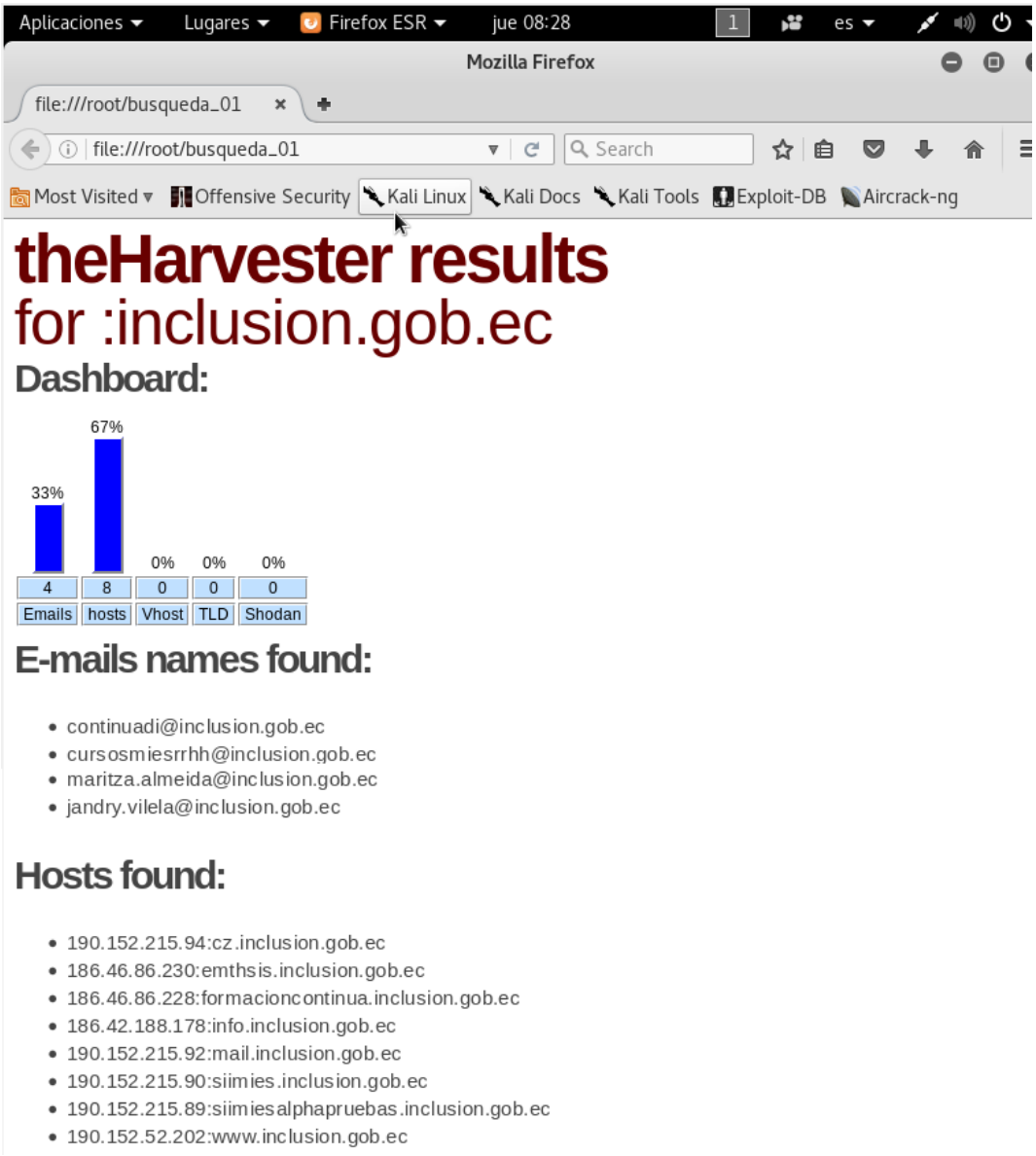


Figura 4.19: The Harvester informe inclusion.gob.ec
Elaborado por: Christian Miranda

El riesgo que se quiere evitar con esta herramienta es encontrar pública en internet una lista de direcciones de correos electrónicos de la empresa, a la cual luego se podría enviar correos masivos con algún malware mediante Ingeniería social.
El buscador de Google es más provechoso siempre y cuando se lo utilice de forma que se pueda filtrar información y reducir los resultados al máximo, esto se lo realiza mediante la utilización de sus operadores, esta técnica se la denomina "Google Hacking".

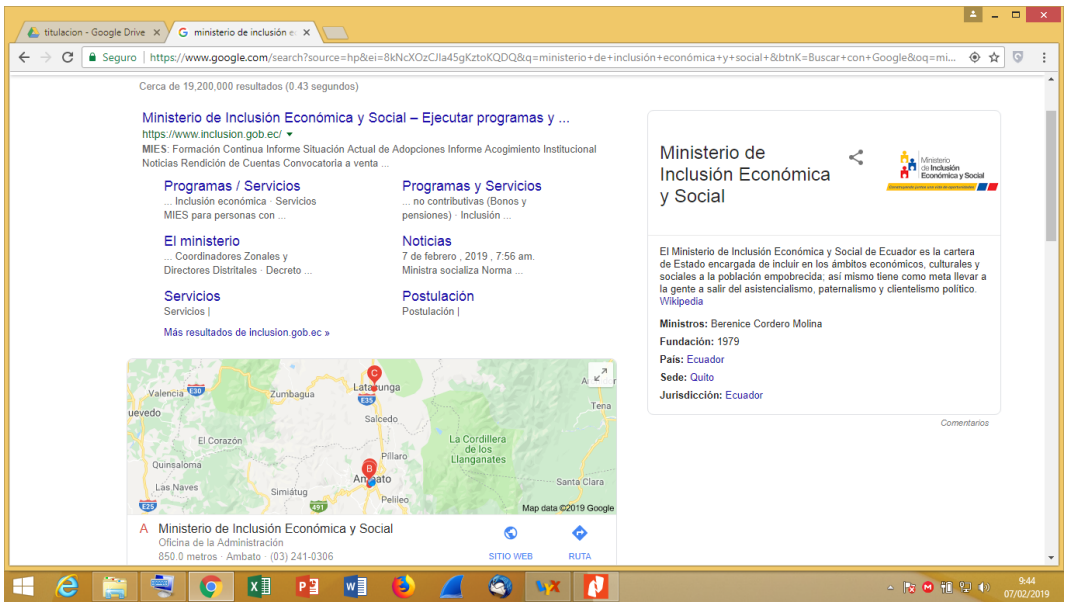


Figura 4.20: Buscador de Google MIES
Elaborado por: Christian Miranda

En la figura 4.20 se observa la búsqueda del "Ministerio de Inclusión Económica y Social" en el buscador de Google, el resultado es de cerca de 19 millones de páginas relacionadas con ese nombre.

Buscando información en la base de datos NIC(Network Information Center); "NIC es la autoridad que delega los nombres de dominio quienes los solicitan. Cada país en el mundo cuenta con una autoridad que registra los nombres bajo su jurisdicción. Por autoridad no nos referimos a una dependencia de un gobierno, muchos NIC's en el mundo son operados por universidades o compañías" [32].

En el navegador de preferencia se ingresa a la dirección https://nic.ec/ y se digita el dominio en investigación, en este caso **inclusion.gob.ec**.

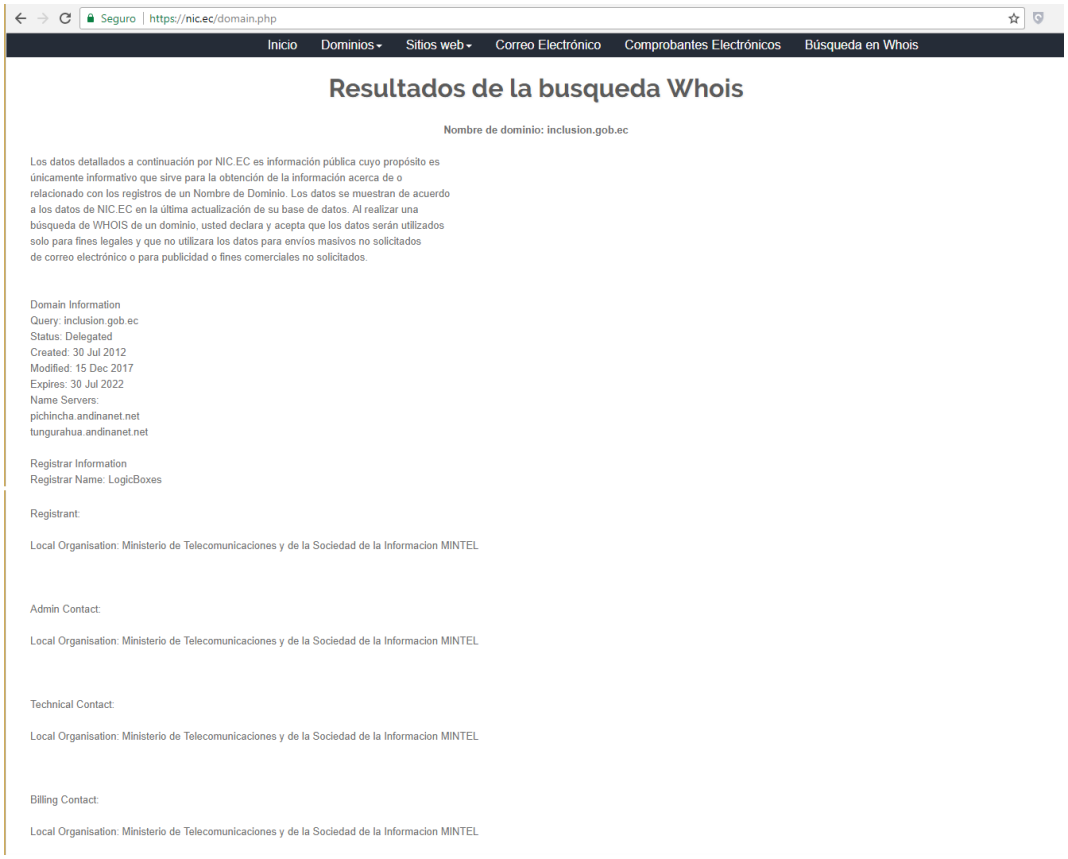


Figura 4.21: NIC consulta inclusion.gob.ec
Elaborado por: Christian Miranda

En la figura 4.21 se observa el resultado de la consulta del dominio inclusion.gob.ec en la base de datos NIC, se aprecian que los datos que obtengo como resultado es solamente con propósito informativo, no revela datos de personas naturales o empleados de la Institución ya que de esa manera se podría utilizar la información para un ataque de Ingeniería Social.
Esta información es privada por el motivo y se logra mediante un pago extra anualmente.
Resultados obtenidos de maltego.

Nombre	Dirección IP	Servicio	Observación
www.inclusion.gob.ec www.educacionsuerior.gob.ec www.mmineria.gob.ec	190.150.52.202	Website	Se encuentran en un hosting externo
www.w3-edge.com	52.90.1.218	Website	
sin.gob.ec	186.47.101.207	Website	
www.trabajo.gob.ec	190.152. 44.130	Website	
formacioncontinua.inclusion.gob.ec	186. 46.86.228	Website	
www.senecyt.gob.ec	186. 46.74.240	Website	
bit.ly	67.199.248.11 67.199.248.10	Website	
viajes.administracionpublica.gob.ec	190.152.52.204	Website	
gpr.administracionpublica.gob.ec	190.152.52.223	Website	
educación.gob.ec	186. 47.213.28	Website	

Tabla 4.7: Listado de servidores relacionados al dominio

Elaborado por: Christian Miranda

- **Módulo de Recolección de Documentos**

En este punto se procesa toda la información recogida anteriormente para extraer datos importantes de cada uno de los documentos tales como nombres de usuarios, empleados claves de la institución, correos electrónicos, entre otros.
Se obtuvo documentos publicados en internet como:

- Nombres completos de varios empleados y autoridades pertenecientes a la Institución.
- Datos personales como cédula, dirección de domicilio, fechas de nacimiento, entre otros.
- Informes de Auditorías internas de gastos.

Mediante un análisis de los metadatos de los documentos obtenidos se puede definir nombres de usuarios relacionados con la institución. Los datos personales pueden ser usados para la aplicación de Ingeniería Social, robo de información mediante phishing, creación de diccionario de datos, entre otros.
Como auditor me dieron acceso solo a algunos equipos de la Institución de los cuales pude extraer la siguiente información que se replican en todas las máquinas:

- Sistema operativo Windows 7 profesional Service Pack1 de 64bits.
- Procesador Intel Core i3, x64.
- Memoria de 4GB de ram.
- Utilizan servidor proxy con iptables configurados para que solo accedan a paginas Institucionales.
- Tipo de conexión Ethernet con velocidad de 100.0 Mbps..
- Puerta de enlace 10.2.78.1.
- Mascara 255.255.255.0.
- Tienen licencia del Kaspersky actualizada.

Sección Seguridad en las Tecnologías de Internet

- **Módulo de Sondeo de Red**

En este punto se obtiene las direcciones ip a auditar por parte de la institución y se hace un reconocimiento de la red institucional de manera detallada, cabe mencionar que existe información confidencial a la cual el auditor no tiene acceso.

Red	Mascara	Observación
10.1.78.0	255.255.255.0	Piso 1
10.2.78.0	255.255.255.0	Piso 2
10.3.78.0	255.255.255.0	Piso 3
192.168.21.0	255.255.255.0	Acces point

Tabla 4.8: Redes internas Ministerio de Inclusión Económica y Social

Elaborado por: Christian Miranda

Lista de Servidores internos de la Institución.

Numero	Dirección	Nombre
1	190.152.52.202	www.inclusion.gob.ec
2	190.152.215.92	mail.inclusion.gob.ec
3	186. 42.188.178	info.inclusion.gob.ec
4	186. 46.86.228	formacioncontinua.inclusion.gob.ec
5	190.152.215.90	simies.inclusion.gob.ec
6	190.152.215.94	cz.inclusion.gob.ec
7	186. 46.86.230	emthsis.inclusion.gob.ec

Tabla 4.9: Servidores a auditar

Elaborado por: Christian Miranda

- **Módulo Identificación de Servicios y Sistemas**

Esta sección realiza un sondeo de puertos en cada servidor para descubrir qué servicios se están ejecutando actualmente.
Para explotar la red, debido a que el servidor se encuentra en Quito se lo realiza remotamente, como un usuario cualquiera, en la figura 4.22 se muestra un escenario creado según la información obtenida con anterioridad.

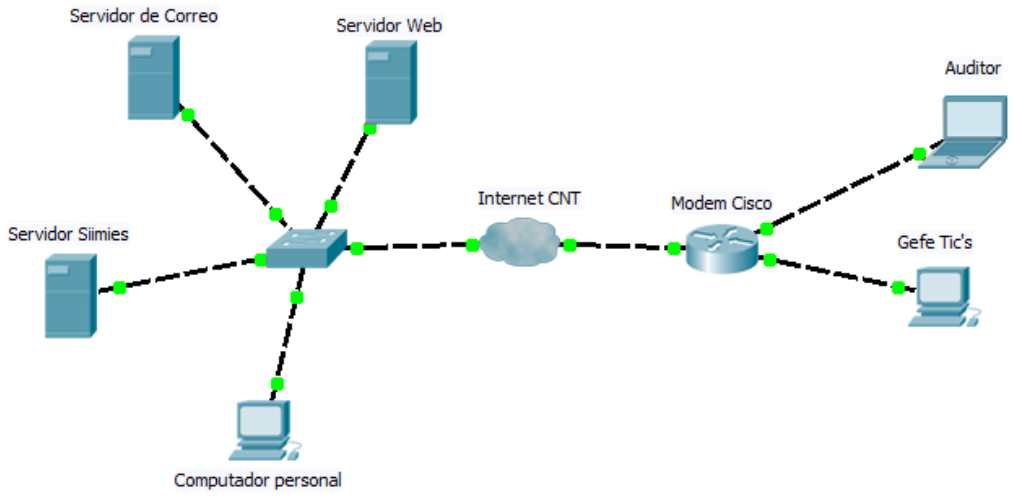


Figura 4.22: Escenario para el análisis y detección de vulnerabilidades
Elaborado por: Christian Miranda

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.

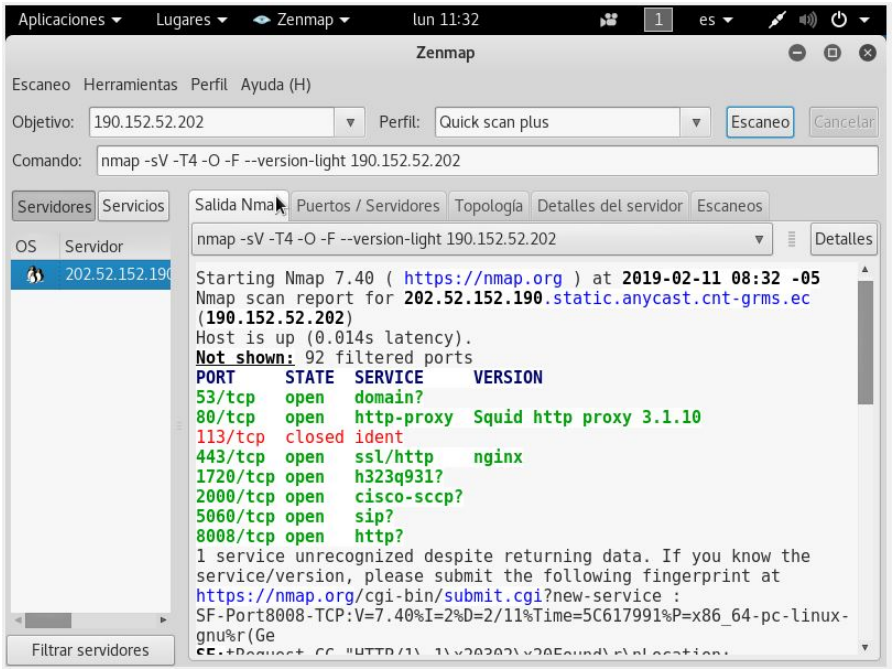


Figura 4.23: Sondeo de Puertos con nmap
Elaborado por: Christian Miranda

Servidor mail.inclusion.gob.ec

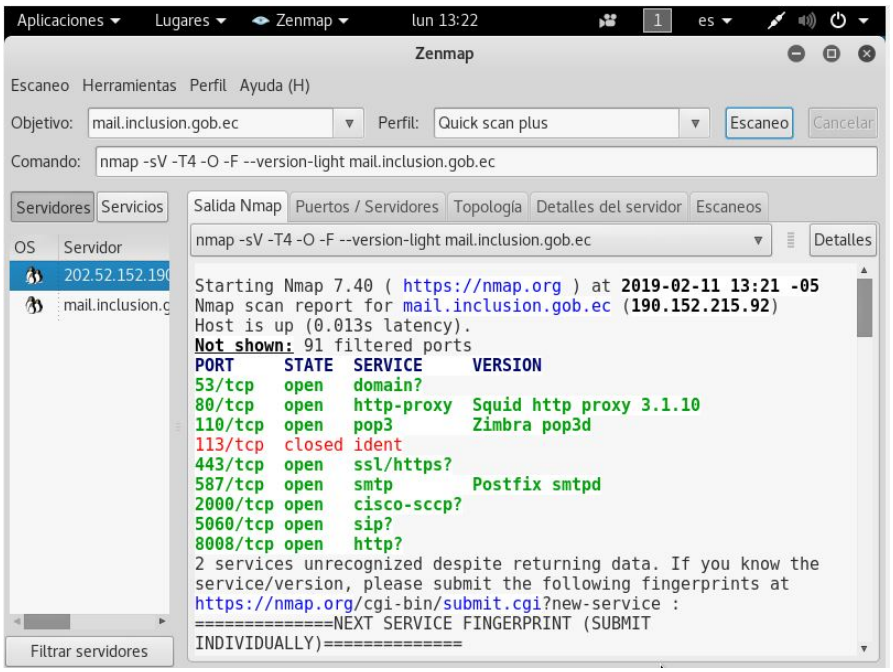


Figura 4.24: nmap a mail.inclusion.gob.ec
Elaborado por: Christian Miranda

Servidor cz.inclusion.gob.ec

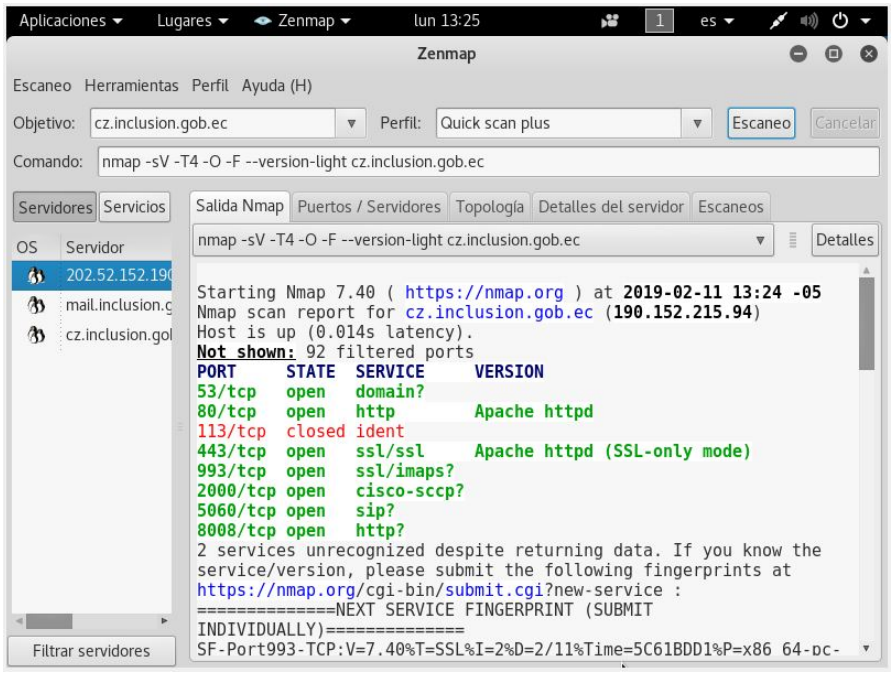


Figura 4.25: nmap a cz.inclusion.gob.ec
Elaborado por: Christian Miranda

Servidor emthsis.inclusion.gob.ec

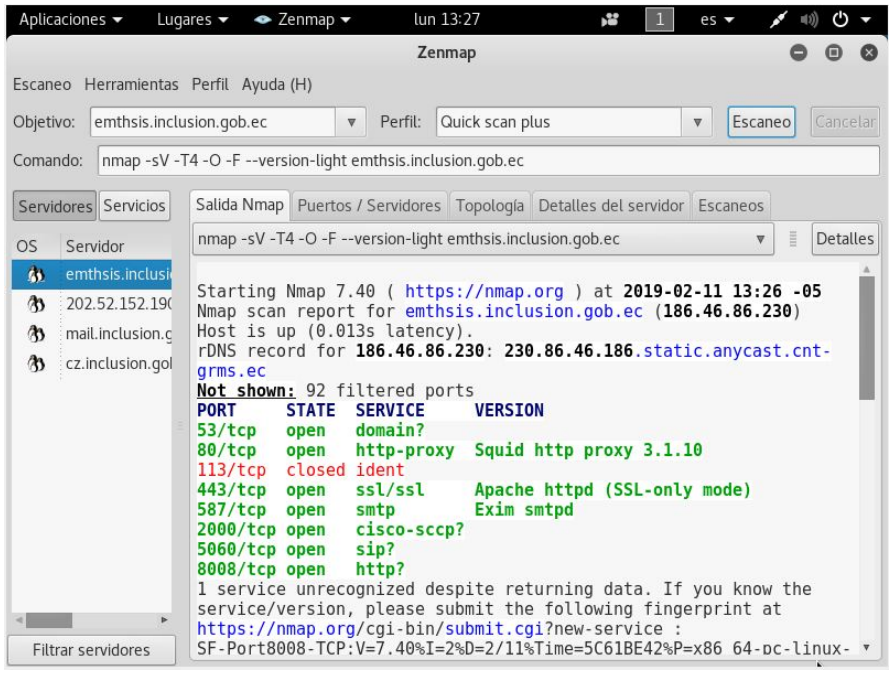


Figura 4.26: nmap a emthsis.inclusion.gob.ec
Elaborado por: Christian Miranda

Servidor formacioncontinua.inclusion.gob.ec

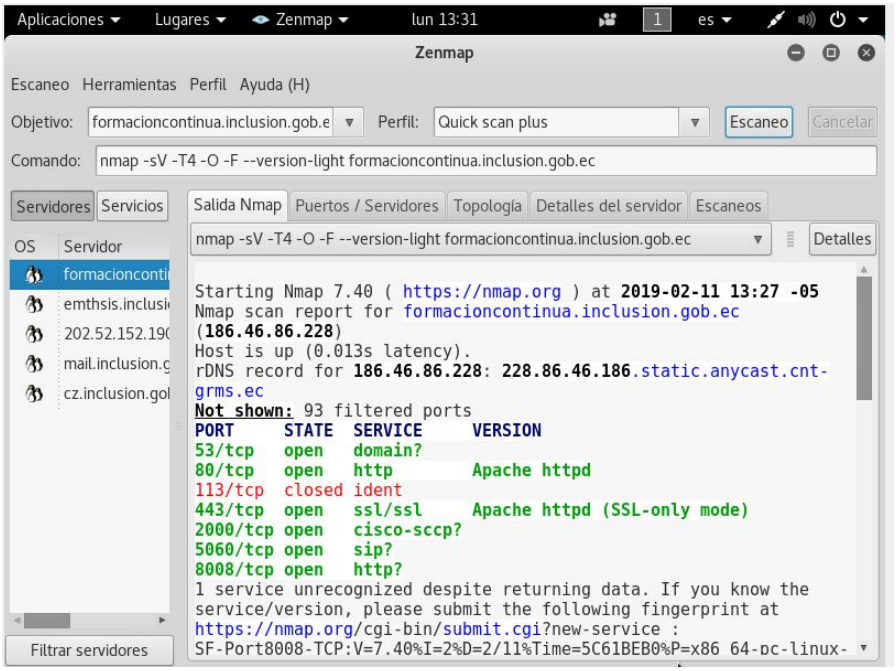


Figura 4.27: nmap a formacioncontinua.inclusion.gob.ec
Elaborado por: Christian Miranda

Servidor info.inclusion.gob.ec

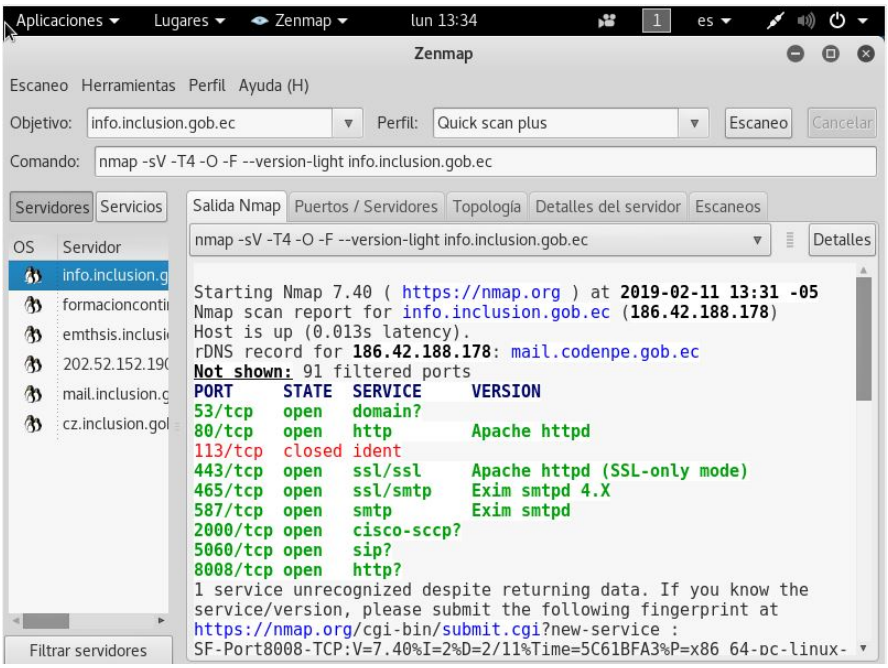


Figura 4.28: nmap a info.inclusion.gob.ec
Elaborado por: Christian Miranda

Servidor siimies.inclusion.gob.ec

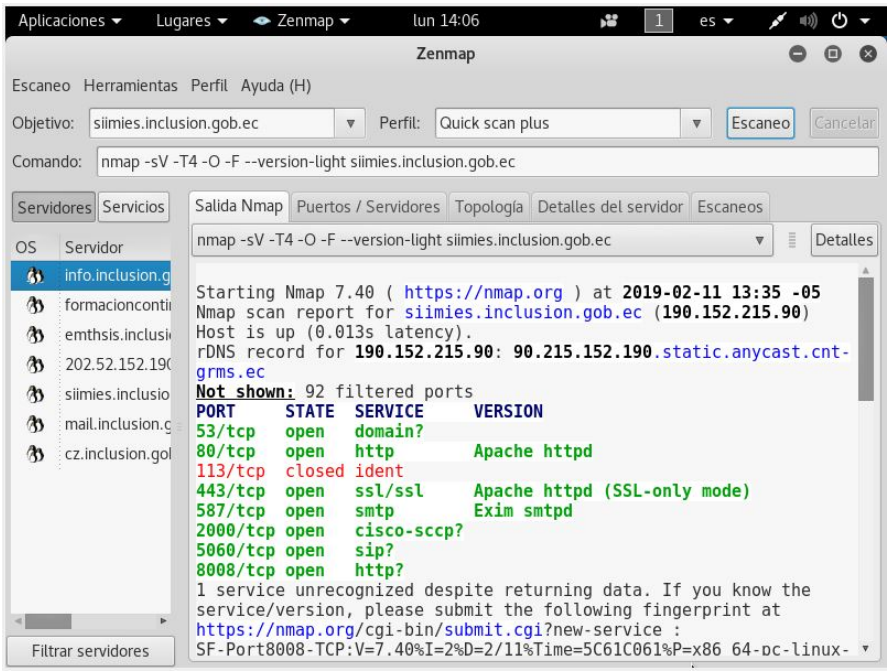


Figura 4.29: nmap a siimies.inclusion.gob.ec
Elaborado por: Christian Miranda

En todos los escaneos de puertos con la herramienta nmap y su interfaz zenmap podemos observar lo siguiente:

- El puerto 113 se encuentra cerrado, este puerto brinda el servicio de autenticación o identificación.
- El servidor squid tienen la versión Squid http proxy 3.1.10
- El servidor de correo se llama Postfix que también utiliza zimbra como aplicación para su funcionamiento.
- Utiliza también el servidor Apache httpd el cual es de código abierto para plataformas Unix como BSD, GNU/Linux, etc.
- El servidor de emthsis.inclusion.gob.ec y siimies.inclusion.gob.ec utilizan el agente "Exim smtp" que es un agente para el transporte de correos electrónicos.

Módulo de Búsqueda y Verificación de Vulnerabilidades

En esta sección se buscan los posibles fallos, errores o vulnerabilidades de sistemas operativos, esto se lo realiza mediante el sondeo de vulnerabilidades, luego se explota (pruebas de penetración) los fallos que se hayan detectado en el objetivo. Para realizar lo mencionado se utilizan los programas de escaneo de vulnerabilidades Nessus y OpenVAS, para la verificación, un framework de explotación el cual incluye herramientas de reconocimiento, escaneo, análisis y explotación de vulnerabilidades.

Análisis de vulnerabilidades con OpenVAS

Para el uso de OpenVAS se lo puede hacer por medio de la interfaz del escritorio o web, en este caso se utiliza la segunda, la interfaz web Asistente de Seguridad Greenbone.

Se crea un Target(objetivo) que viene a ser la ip a escanear y una Task(tarea) para cada una de las Targets, para el tipo de escaneo se inflige Full and very deep recomendado. Una vez creado lo necesario se procede a ejecutar las tareas(ver figura 4.30).

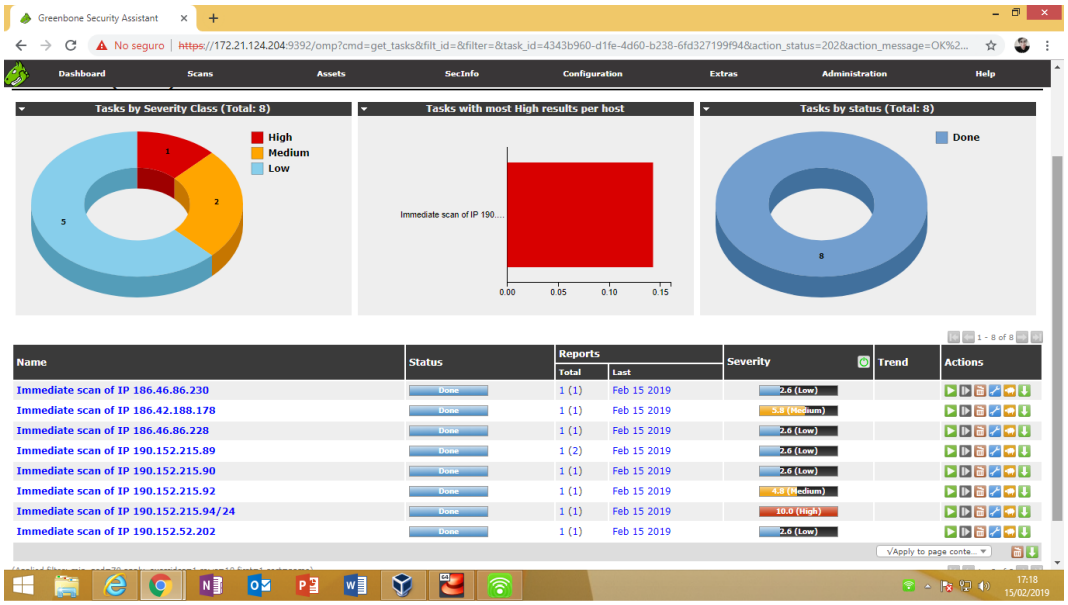


Figura 4.30: Escaneo de Vulnerabilidades con OpenVAS
Elaborado por: Christian Miranda

A continuación se detallan las vulnerabilidades detectadas con OpenVAS:
Servidor emthsis.inclusion.gob.ec (186.46.86.230)

Servicio	Vulnerabilidad	Riesgo	Observación
HTTP	El servidor web remoto es de tipo squid/3.1.10	Bajo	El servidor http de Apache pueden ser explotado para divulgar información potencialmente sensible y comprometer un sistema vulnerable.
DIRB (NASL wrapper)	Estos son los directorios / archivos encontrados con fuerza bruta: http://230.86.46.186.static.anycast.cnt http://186.46.86.230:80/	Bajo	Esta secuencia de comandos utiliza DIRB para buscar directorios y archivos en aplicaciones web a través de forzados brutos. Vea la sección de preferencias para las opciones de configuración.
Servicio puerto 80, 8008/tcp	Un servidor web está corriendo en este puerto	Bajo	Esta rutina intenta adivinar qué servicio se está ejecutando en los puertos remotos y hace que esta información esté disponible para otras rutinas de verificación.
Servicio puerto 53/tcp	El servicio cerró la conexión después de 18 segundos sin enviar ningún dato. Podría estar protegido por algún contenedor TCP	Bajo	Esta rutina intenta adivinar qué servicio se está ejecutando en los puertos remotos y hace que esta información esté disponible para otras rutinas de verificación.
La exploración CGI se deshabilitará para este host.	Este servidor web está [mal] configurado porque no devuelve los códigos de error '404 No encontrado' cuando se solicita un archivo inexistente, tal vez devolviendo un mapa del sitio, una página de búsqueda o una página de autenticación.	Bajo	El escáner habilitó algunas contramedidas para eso, sin embargo, podrían ser insuficientes. Si se produce una gran cantidad de agujeros de seguridad para este puerto, es posible que no todos sean precisos

Tabla 4.10: Vulnerabilidades detectadas en emthsis.inclusion.gob.ec

Elaborado por: Christian Miranda

Servidor info.inclusion.gob.ec (186.42.188.178)

Servicio	Vulnerabilidad	Riesgo	Observación
HTTP	Las funciones de depuración están habilitadas en el servidor web remoto. Un atacante puede usar esta falla para engañar a sus usuarios legítimos de la web para que le den sus credenciales.	Medio	Se ha demostrado que los servidores web que admiten estos métodos están sujetos a ataques de scripts entre sitios, llamados XST para el rastreo de sitios cruzados, cuando se usan junto con varias debilidades en los navegadores.
TCP	El host remoto implementa marcas de tiempo TCP y, por lo tanto, permite calcular el tiempo de actividad.	Bajo	Los paquetes de IP especiales se falsifican y se envían con un pequeño retraso entre la IP de destino. Las respuestas se buscan por una marca de tiempo. Si se encuentran, se informan las marcas de tiempo.
Apache	El tipo de servidor web remoto es apache y la directiva "Server Tokens" es solo producto Apache no permite ocultar el tipo de servidor.	Bajo	Apache emana la información del servidor en sus encabezados de respuesta.
DIRB	Estos son los directorios / archivos encontrados con fuerza bruta: http://mail.codenpe.gob.ec:8008/	Bajo	Esta secuencia de comandos utiliza DIRB para buscar directorios y archivos en aplicaciones web a través de forzados brutos.
CPE	186.42.188.178|cpe:/a:apache:http_server 186.42.188.178|cpe:/a:exim:exim 186.42.188.178|cpe:/a:squid-cache:squid:3.1.10	Bajo	Mediante este servicio CPE (http://cpe.mitre.org/) se detectan sistemas operativos, servicios y aplicaciones detectados durante la exploración.

Tabla 4.11: Vulnerabilidades detectadas en info.inclusion.gob.ec

Elaborado por: Christian Miranda

Servidor formacioncontinua.inclusion.gob.ec (186.46.86.228)

Servicio	Vulnerabilidad	Riesgo	Observación
Apache	El tipo de servidor web remoto es apache y la directiva "Server_Tokens" es solo producto Apache no permite ocultar el tipo de servidor.	Bajo	Apache emana la información del servidor en sus encabezados de respuesta.
DIRB	Estos son los directorios / archivos encontrados con fuerza bruta: http://228.86.46.186.static.anycast.cnt https://228.86.46.186.static.anycast.cnt http://186.46.86.228:80/	Bajo	Esta secuencia de comandos utiliza DIRB para buscar directorios y archivos en aplicaciones web a través de forzados brutos.
TCP	El host remoto implementa marcas de tiempo TCP y, por lo tanto, permite calcular el tiempo de actividad.	Bajo	Un efecto secundario de esta característica es que a veces se puede calcular el tiempo de actividad del host remoto.
CGI 443/TCP	El nombre de host / IP "228.86.46.186.static.anycast.cnt-grms.ec" se utilizó para acceder al host remoto.		Si bien esto no es, en sí mismo, un error, debe inspeccionar manualmente estos directorios para asegurarse de que cumplen con los estándares de seguridad de la compañía.
CPE	186.46.86.228|cpe:/a:apache:http_server 186.46.86.228|cpe:/a:squid-cache:squid:3.1.10	Bajo	Mediante este servicio CPE (http://cpe.mitre.org/) se detectan sistemas operativos, servicios y aplicaciones detectados durante la exploración.

Tabla 4.12: Vulnerabilidades detectadas en formacioncontinua.inclusion.gob.ec

Elaborado por: Christian Miranda

Servidor siimiesalphapruebas.inclusion.gob.ec (190.152.52.89)

Servicio	Vulnerabilidad	Riesgo	Observación
HTTP	Esto detecta el tipo y la versión del servidor HTTP: squid/3.1.10	Bajo	Apache emana la información del servidor en sus encabezados de respuesta.
DIRB	Estos son los directorios / archivos encontrados con fuerza bruta: http://mail.ppa.gov.ec:8008/ http://190.152.215.89:80/	Bajo	Esta secuencia de comandos utiliza DIRB para buscar directorios y archivos en aplicaciones web a través de forzados brutos.
CGI 443/TCP	El nombre de host / IP "mail.ppa.gov.ec" se utilizó para acceder al host remoto.	Bajo	Si bien esto no es, en sí mismo, un error, debe inspeccionar manualmente estos directorios para asegurarse de que cumplen con los estándares de seguridad de la compañía.
CPE	190.152.215.89|cpe:/a:squid-cache:squid:3.1.10	Bajo	Mediante este servicio CPE (http://cpe.mitre.org/) se detectan sistemas operativos, servicios y aplicaciones detectados durante la exploración.

Tabla 4.13: Vulnerabilidades detectadas en siimiesalphapruebas.inclusion.gob.ec

Elaborado por: Christian Miranda

Servidor siimies.inclusion.gob.ec (190.152.215.90)

Servicio	Vulnerabilidad	Riesgo	Observación
SMTP	El servidor SMTP remoto está anunciando los siguientes comandos ESMTP disponibles a través de una conexión no cifrada: 250-sophos.inclusion.gob.ec Hello example.com [192.188.46.103] 250-SIZE 10485760 250-8BITMIME 250-PIPELINING 250-STARTTLS 250 HELP	Bajo	Se detecta el tipo de servidor SMTP y la versión conectándose al servidor y procesando el búfer recibido.
DIRB	Estos son los directorios / archivos encontrados con fuerza bruta: http://90.215.152.190.static.anycast.cnt http://190.152.215.90:80/	Bajo	Esta secuencia de comandos utiliza DIRB para buscar directorios y archivos en aplicaciones web a través de forzados brutos.
CGI 443/TCP	El nombre de host / IP " 90.215.152.190.static.anycast.cnt-grms.ec " se utilizó para acceder al host remoto.	Bajo	Si bien esto no es, en sí mismo, un error, debe inspeccionar manualmente estos directorios para asegurarse de que cumplen con los estándares de seguridad de la compañía.
TCP	El host remoto implementa marcas de tiempo TCP y, por lo tanto, permite calcular el tiempo de actividad.	Bajo	Un efecto secundario de esta característica es que a veces se puede calcular el tiempo de actividad del host remoto.
CPE	190.152.215.90|cpe:/a:exim:exim 190.152.215.90|cpe:/a:squid-cache:squid:3.1.10	Bajo	Mediante este servicio CPE (http://cpe.mitre.org/) se detectan sistemas operativos, servicios y aplicaciones detectados durante la exploración.

Tabla 4.14: Vulnerabilidades detectadas en siimies.inclusion.gob.ec

Elaborado por: Christian Miranda

Servidor mail.inclusion.gob.ec (190.152.215.92)

Servicio	Vulnerabilidad	Riesgo	Observación
POP3	El servidor POP3 remoto acepta los inicios de sesión a través de los siguientes mecanismos de autenticación de texto simple en conexiones no cifradas: USER	Medio	Un atacante puede descubrir nombres de usuario y contraseñas rastreando el tráfico al demonio POP3 si se usa un mecanismo de autenticación menos seguro (por ejemplo, comando del USUARIO, PLAIN AUTOMÁTICO, INICIACIÓN AUTOMÁTICA).
TCP	El host remoto implementa marcas de tiempo TCP y, por lo tanto, permite calcular el tiempo de actividad.	Bajo	Un efecto secundario de esta característica es que a veces se puede calcular el tiempo de actividad del host remoto.
CPE	Sistema operativo: Linux CPE: cpe: / o: linux: kernel Encontrado por NVT: 1.3.6.1.4.1.25623.1.0.111068 (Identificación del SO del servidor SMTP / POP3 / IMAP) Concluido del banner POP3 en el puerto 110 / tcp: mail.inclusion.gob.ec Servidor POP3 de Zimbra listo IMPLEMENTACIÓN ZIMBRAIN Configuración de la clave "Host / runs_unixoide"	Bajo	Esta secuencia de comandos consolida la información del sistema operativo detectada por varios NVT Mediante este servicio CPE (http://cpe.mitre.org/) se detectan sistemas operativos, servicios y aplicaciones detectados durante la exploración.
SIP	Se identificó un servicio compatible con el protocolo SIP.	Bajo	Este complemento es un complemento de find_service.nasl. Envía una solicitud de OPCIONES 'SIP' a los servicios desconocidos restantes e intenta identificarlos.
CGI 443/TCP	El nombre de host / IP " mail.inclusion.gob.ec" se utilizó para acceder al host remoto.	Bajo	Si bien esto no es, en sí mismo, un error, debe inspeccionar manualmente estos directorios para asegurarse de que cumplen con los estándares de seguridad de la compañía.
TCP	El host remoto implementa marcas de tiempo TCP y, por lo tanto, permite calcular el tiempo de actividad.	Bajo	Un efecto secundario de esta característica es que a veces se puede calcular el tiempo de actividad del host remoto.

Tabla 4.15: Vulnerabilidades detectadas en mail.inclusion.gob.ec

Elaborado por: Christian Miranda

Servidor cz.inclusion.gob.ec (190.152.215.94)

Servicio	Vulnerabilidad	Riesgo	Observación
Mikrotik RouterOS	Este host ejecuta Mikrotik RouterOS y es propenso a la vulnerabilidad de divulgación de información.	Medio	La explotación exitosa permitirá que un atacante remoto se conecte al puerto WinBox y descargue un archivo de base de datos de usuario. El usuario remoto puede iniciar sesión y tomar el control del enrutador.
Squid	La falla existe debido a una validación de entrada incorrecta en el procesamiento de la solicitud HTTP.	Medio	La explotación exitosa permitirá a los atacantes remotos causar envenenamiento de caché y evitar la política de seguridad del mismo origen.
MatrixSSL	MatrixSSL es propenso a múltiples vulnerabilidades	Alto	Un atacante remoto no autenticado puede crear una condición de denegación de servicio o ejecutar código arbitrario en el contexto de la pila SSL.
Apache	Los siguientes archivos están llamando a la función phpinfo () que revela información potencialmente confidencial: http://mail.hdgg.gob.ec/info.php	Alto	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
Denegación de Servicios de Squid	Existen múltiples fallas debido a: - Una saturación del búfer en la función 'Icmp6:: Recv' en el script 'icmp / Icmp6.cc' en el proceso 'pinger'. - Una comprobación de límites incorrecta al procesar las respuestas HTTP.	Alto	La explotación exitosa permitirá a los servidores HTTP remotos provocar una denegación de servicio o escribir información confidencial en los archivos de registro.
Telnet	El host remoto está ejecutando un servicio Telnet que permite inicios de sesión de texto simple en conexiones no cifradas.	Medio	Un atacante puede descubrir nombres de inicio de sesión y contraseñas al rastrear el tráfico al servicio Telnet.
GlassFish Server	El host está ejecutando GlassFish Server y es propenso a la vulnerabilidad de denegación de servicio.	Medio	Una explotación exitosa podría permitir que los atacantes remotos causen una denegación de servicio a través de un formulario especialmente diseñado enviado en una solicitud HTTP POST.
Geoserver XML	Una vulnerabilidad XXE en Geoserver permite ver contenidos de archivos y listar directorios en el servidor	Medio	Un atacante puede explotar este problema para obtener acceso a información confidencial, lo que puede llevar a más ataques.
FTP	El servicio FTP remoto acepta inicios de sesión sin un comando 'AUTH TLS' enviado previamente. Respuesta (s): Sesiones anónimas: 331 Contraseña requerida para anónimo Sesiones no anónimas: 331 Se requiere contraseña para openvas-vt	Medio	Un atacante puede descubrir nombres y contraseñas de inicio de sesión mediante la detección del tráfico al servicio FTP.
SSL/TLS	Tamaño de clave temporal del servidor: 1024 bits. Un atacante podría descifrar la comunicación SSL / TLS sin conexión.	Medio	La seguridad del secreto final depende del tamaño de estos parámetros. Se encontró que 512 y 768 bits eran débiles, 1024 bits para ser rompibles por atacantes realmente poderosos como los gobiernos.
TCP	El host remoto implementa marcas de tiempo TCP y, por lo tanto, permite calcular el tiempo de actividad.	Bajo	Un efecto secundario de esta característica es que a veces se puede calcular el tiempo de actividad del host remoto.

Tabla 4.16: Vulnerabilidades detectadas en cz.inclusion.gob.ec

Elaborado por: Christian Miranda

Servidor www.inclusion.gob.ec (190.152.52.202)

Servicio	Vulnerabilidad	Riesgo	Observación
HTTP	Esto detecta el tipo y la versión del servidor HTTP: squid/3.1.10	Bajo	Apache emana la información del servidor en sus encabezados de respuesta.
DIRB	Estos son los directorios / archivos encontrados con fuerza bruta: http://202.52.152.190.static.anycast.cnt	Bajo	Esta secuencia de comandos utiliza DIRB para buscar directorios y archivos en aplicaciones web a través de forzados brutos.
CPE	SO: Linux Kernel CPE: cpe: / o: linux: kernel Encontrado por NVT: 1.3.6.1.4.1.25623.1.0.102002 (huella dactilar basada en ICMP) Concluido a partir de la huella digital del sistema operativo ICMP Configuración de la clave "Host / runs_unixoide" basada en esta información.	Bajo	Esta secuencia de comandos consolida la información del sistema operativo detectada por varios NVT Mediante este servicio CPE (http://cpe.mitre.org/) se detectan sistemas operativos, servicios y aplicaciones detectados durante la exploración.
CGI 443/TCP	El nombre de host / IP " 202.52.152.190.static.anycast.cnt-grms.ec" se utilizó para acceder al host remoto.	Bajo	Si bien esto no es, en sí mismo, un error, debe inspeccionar manualmente estos directorios para asegurarse de que cumplen con los estándares de seguridad de la compañía.

Tabla 4.17: Vulnerabilidades detectadas en www.inclusion.gob.ec

Elaborado por: Christian Miranda

Análisis de vulnerabilidades con NESSUS

En Nessus se crea un nuevo escaneo con una política ya existente Advanced Scan la cual es recomendad, consiste en ingresar las direcciones ip de los host a escanear, continuamente se las guarda e inmediatamente empieza el análisis de vulnerabilidades.

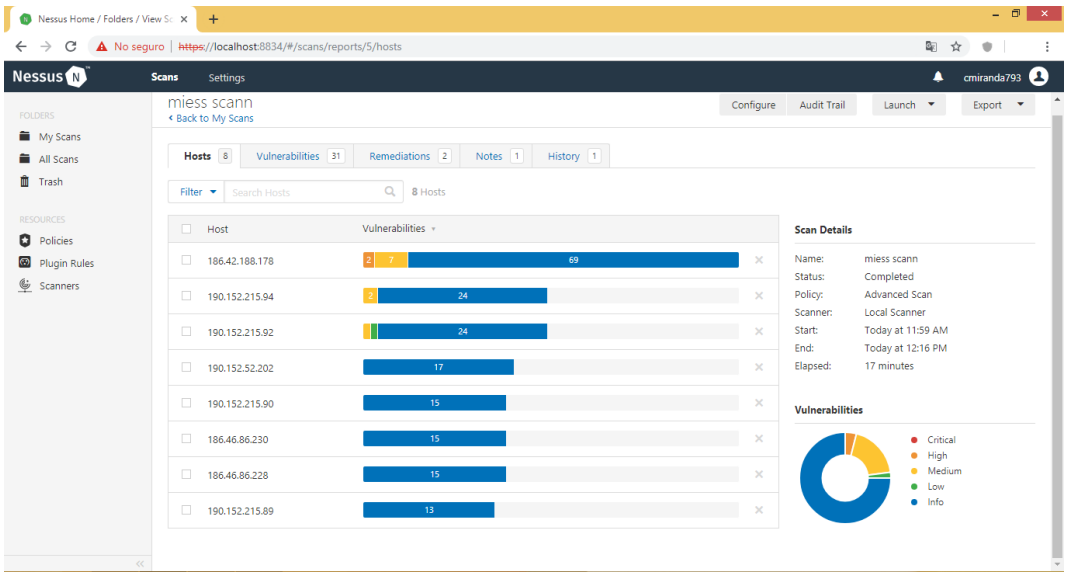


Figura 4.31: Escaneo de vulnerabilidades con Nessus
Elaborado por: Christian Miranda

En las figuras 4.30 y 4.31 se puede observar que las dos herramientas utilizadas detallan la vulnerabilidad detectada junto con su nivel de riesgo y su posible solución. También brindan la opción de exportar un reporte en formatos como html, pdf, xml entre otros.

A continuación se detallarán las vulnerabilidades detectadas con Nessus:

Servidor info.inclusion.gob.ec (186.42.188.178)

Servicio	Vulnerabilidad	Riesgo	Observación
PHP Versión	Según su banner, la versión de PHP que se ejecuta en el servidor web remoto es 7.2.8 antes de 7.2.14. Es, por lo tanto, afectado por múltiples vulnerabilidades.	Alto	Un atacante remoto autenticado puede explotar esto enviando un nombre de servidor IMAP especialmente diseñado para provocar la ejecución de comandos arbitrarios en el sistema de destino
TCP	El servidor web remoto es compatible con los métodos TRACE y / o TRACK.	Medio	TRACE y TRACK son métodos HTTP que se utilizan para depurar las conexiones del servidor web.
APACHE Versión	La versión de Apache que se ejecuta en el host remoto es 2.4.33 antes de 2.4.39. Es, por lo tanto, afectado por múltiples vulnerabilidades como: Existe una vulnerabilidad de escalada de privilegios en las secuencias de comandos de los módulos debido a la capacidad de ejecutar código arbitrario	Medio	Apache httpd también se ve afectado por varias vulnerabilidades adicionales, entre las que se incluyen la denegación de servicio, la lectura después de la desconexión y la incoherencia de la normalización de la ruta URL.
SYN	Con el escáner de puertos SYN razonablemente rápido incluso contra un objetivo con cortafuegos el cual encontró varios puertos abiertos	Bajo	Hay que tener en cuenta que esto puede causar problemas para firewalls menos robustos y también dejar conexiones no cerradas en el destino remoto, si la red está cargada.
SSL	El servicio remoto utiliza una cadena de certificados SSL que contiene un certificado de Autoridad de Certificación raíz auto firmado en la parte superior de la cadena.	Bajo	Hay que tomar en cuenta que, si este certificado no cumple con las políticas de uso y seguridad aceptables, seria riesgoso para la organización
TLS 1.1	Este servicio carece de soporte para los conjuntos de cifrado actuales y recomendados.	Bajo	PCI DSS v3.2 aún permite TLS 1.1 a partir del 30 de junio de 2018, pero recomienda encarecidamente el uso de TLS 1.2 o 1.3.

Tabla 4.18: Vulnerabilidades detectadas en info.inclusion.gob.ec

Elaborado por: Christian Miranda

Servidor cz.inclusion.gob.ec (190.152.215.94)

Servicio	Vulnerabilidad	Riesgo	Observación
SSL	El certificado X.509 del servidor no se puede confiar.	Medio	Si el host remoto es un host público en producción, cualquier ruptura en la cadena hace que sea más difícil para los usuarios verificar la autenticidad y la identidad del servidor web. Esto podría hacer que sea más fácil llevar a cabo ataques de hombre en el medio contra el host remoto.
Apache	Los siguientes archivos están llamando a la función phpinfo () que revela información potencialmente confidencial: http://mail.hdgg.gob.ec/info.php	Medio	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
Squid	La falla existe debido a una validación de entrada incorrecta en el procesamiento de la solicitud HTTP.	Medio	La explotación exitosa permitirá a los atacantes remotos causar envenenamiento de caché y evitar la política de seguridad del mismo origen.
SYN	Con el escáner de puertos SYN razonablemente rápido incluso contra un objetivo con cortafuegos el cual encontró varios puertos abiertos	Bajo	Hay que tener en cuenta que esto puede causar problemas para firewalls menos robustos y también dejar conexiones no cerradas en el destino remoto, si la red está cargada.
TLS 1.1	Este servicio carece de soporte para los conjuntos de cifrado actuales y recomendados.	Bajo	PCI DSS v3.2 aún permite TLS 1.1 a partir del 30 de junio de 2018, pero recomienda encarecidamente el uso de TLS 1.2 o 1.3.
TCP	El host remoto implementa marcas de tiempo TCP y, por lo tanto, permite calcular el tiempo de actividad.	Bajo	Un efecto secundario de esta característica es que a veces se puede calcular el tiempo de actividad del host remoto.

Tabla 4.19: Vulnerabilidades detectadas en cz.inclusion.gob.ec

Elaborado por: Christian Miranda

Servidor mail.inclusion.gob.ec (190.152.215.92)

Servicio	Vulnerabilidad	Riesgo	Observación
SSL	El host remoto admite el uso de cifrados SSL que ofrecen cifrado de intensidad media	Medio	Hay que tener en cuenta que es mucho más fácil evitar el cifrado de intensidad media si el atacante está en la misma red física
SSL / TLS	El host remoto permite conexiones SSL / TLS con uno o más módulos Diffie-Hellman menores o iguales a 1024 bits	Bajo	A través del análisis criptográfico, un atacante recuperar el texto sin formato o potencialmente violar la integridad de las conexiones.
SYN	Con el escáner de puertos SYN razonablemente rápido incluso contra un objetivo con cortafuegos el cual encontró varios puertos abiertos	Bajo	Hay que tener en cuenta que esto puede causar problemas para firewalls menos robustos y también dejar conexiones no cerradas en el destino remoto, si la red está cargada.
TLS 1.1	Este servicio carece de soporte para los conjuntos de cifrado actuales y recomendados.	Bajo	PCI DSS v3.2 aún permite TLS 1.1 a partir del 30 de junio de 2018, pero recomienda encarecidamente el uso de TLS 1.2 o 1.3.

Tabla 4.20: Vulnerabilidades detectadas en mail.inclusion.gob.ec

Elaborado por: Christian Miranda

Servidor www.inclusion.gob.ec (190.152.52.202)

Servicio	Vulnerabilidad	Riesgo	Observación
SYN	Con el escáner de puertos SYN razonablemente rápido incluso contra un objetivo con cortafuegos el cual encontró varios puertos abiertos	Bajo	Hay que tener en cuenta que esto puede causar problemas para firewalls menos robustos y también dejar conexiones no cerradas en el destino remoto, si la red está cargada.
CPE	Esta secuencia de comandos consolida la información del sistema operativo detectado. cpe:/o:linux:linux_kernel:2.2 cpe:/o:linux:linux_kernel:2.4 cpe:/o:linux:linux_kernel:2.6	Bajo	Mediante este servicio CPE (http://cpe.mitre.org/) se detectan sistemas operativos, servicios y aplicaciones detectados durante la exploración.
TCP	El host remoto implementa marcas de tiempo TCP y, por lo tanto, permite calcular el tiempo de actividad.	Bajo	Un efecto secundario de esta característica es que a veces se puede calcular el tiempo de actividad del host remoto.
ICMP	El host remoto responde a una solicitud de marca de hora ICMP.	Bajo	Esto puede ayudar a un atacante remoto no autenticado a vencer los protocolos de autenticación basados en el tiempo.
DNS	El nombre de esta máquina no se resuelve o se resuelve en una dirección IP diferente.	Bajo	Como resultado, las URL en la salida del complemento pueden no ser directamente utilizables en un navegador web y algunas pruebas web pueden estar incompletas.

Tabla 4.21: Vulnerabilidades detectadas en www.inclusion.gob.ec

Elaborado por: Christian Miranda

Servidor siimies.inclusion.gob.ec (190.152.215.90)

Servicio	Vulnerabilidad	Riesgo	Observación
SYN	Con el escáner de puertos SYN razonablemente rápido incluso contra un objetivo con cortafuegos el cual encontró varios puertos abiertos	Bajo	Hay que tener en cuenta que esto puede causar problemas para firewalls menos robustos y también dejar conexiones no cerradas en el destino remoto, si la red está cargada.
CPE	Esta secuencia de comandos consolida la información del sistema operativo detectado. cpe:/o:linux:linux_kernel:2.2 cpe:/o:linux:linux_kernel:2.4 cpe:/o:linux:linux_kernel:2.6	Bajo	Mediante este servicio CPE (http://cpe.mitre.org/) se detectan sistemas operativos, servicios y aplicaciones detectados durante la exploración.
DNS	El nombre de esta máquina no se resuelve o se resuelve en una dirección IP diferente.	Bajo	Como resultado, las URL en la salida del complemento pueden no ser directamente utilizables en un navegador web y algunas pruebas web pueden estar incompletas.
TCP	El host remoto implementa marcas de tiempo TCP y, por lo tanto, permite calcular el tiempo de actividad.	Bajo	Un efecto secundario de esta característica es que a veces se puede calcular el tiempo de actividad del host remoto.

Tabla 4.22: Vulnerabilidades detectadas en siimies.inclusion.gob.ec

Elaborado por: Christian Miranda

Servidor emthsis.inclusion.gob.ec (186.46.86.230)

Servicio	Vulnerabilidad	Riesgo	Observación
SYN	Con el escáner de puertos SYN razonablemente rápido incluso contra un objetivo con cortafuegos el cual encontró varios puertos abiertos	Bajo	Hay que tener en cuenta que esto puede causar problemas para firewalls menos robustos y también dejar conexiones no cerradas en el destino remoto, si la red está cargada.
CPE	Esta secuencia de comandos consolida la información del sistema operativo detectado. cpe:/o:linux:linux_kernel:2.2 cpe:/o:linux:linux_kernel:2.4 cpe:/o:linux:linux_kernel:2.6	Bajo	Mediante este servicio CPE (http://cpe.mitre.org/) se detectan sistemas operativos, servicios y aplicaciones detectados durante la exploración.
TCP	El host remoto implementa marcas de tiempo TCP y, por lo tanto, permite calcular el tiempo de actividad.	Bajo	Un efecto secundario de esta característica es que a veces se puede calcular el tiempo de actividad del host remoto.

Tabla 4.23: Vulnerabilidades detectadas en emthsis.inclusion.gob.ec

Elaborado por: Christian Miranda

Servidor formacioncontinua.inclusion.gob.ec (186.46.86.228)

Servicio	Vulnerabilidad	Riesgo	Observación
SYN	Con el escáner de puertos SYN razonablemente rápido incluso contra un objetivo con cortafuegos el cual encontró varios puertos abiertos	Bajo	Hay que tener en cuenta que esto puede causar problemas para firewalls menos robustos y también dejar conexiones no cerradas en el destino remoto, si la red está cargada.
CPE	Esta secuencia de comandos consolida la información del sistema operativo detectado. cpe:/o:linux:linux_kernel:2.2 cpe:/o:linux:linux_kernel:2.4 cpe:/o:linux:linux_kernel:2.6	Bajo	Mediante este servicio CPE (http://cpe.mitre.org/) se detectan sistemas operativos, servicios y aplicaciones detectados durante la exploración.
TCP	El host remoto implementa marcas de tiempo TCP y, por lo tanto, permite calcular el tiempo de actividad.	Bajo	Un efecto secundario de esta característica es que a veces se puede calcular el tiempo de actividad del host remoto.

Tabla 4.24: Vulnerabilidades detectadas en formacioncontinua.inclusion.gob.ec

Elaborado por: Christian Miranda

Servidor siimiesalphapruebas.inclusion.gob.ec (190.152.52.202)

Servicio	Vulnerabilidad	Riesgo	Observación
SYN	Con el escáner de puertos SYN razonablemente rápido incluso contra un objetivo con cortafuegos el cual encontró varios puertos abiertos	Bajo	Hay que tener en cuenta que esto puede causar problemas para firewalls menos robustos y también dejar conexiones no cerradas en el destino remoto, si la red está cargada.
CPE	Esta secuencia de comandos consolida la información del sistema operativo detectado. cpe:/o:linux:linux_kernel:2.2 cpe:/o:linux:linux_kernel:2.4 cpe:/o:linux:linux_kernel:2.6	Bajo	Mediante este servicio CPE (http://cpe.mitre.org/) se detectan sistemas operativos, servicios y aplicaciones detectados durante la exploración.
TCP	El host remoto implementa marcas de tiempo TCP y, por lo tanto, permite calcular el tiempo de actividad.	Bajo	Un efecto secundario de esta característica es que a veces se puede calcular el tiempo de actividad del host remoto.
ICMP	El host remoto responde a una solicitud de marca de hora ICMP.	Bajo	Esto puede ayudar a un atacante remoto no autenticado a vencer los protocolos de autenticación basados en el tiempo.
DNS	El nombre de esta máquina no se resuelve o se resuelve en una dirección IP diferente.	Bajo	Como resultado, las URL en la salida del complemento pueden no ser directamente utilizables en un navegador web y algunas pruebas web pueden estar incompletas.

Tabla 4.25: Vulnerabilidades detectadas en siimiesalphapruebas.inclusion.gob.ec

Elaborado por: Christian Miranda

4.7. Determinación del escenario virtual para ejecutar un ataque programado a los servidores de la red informática para explotar las vulnerabilidades que puedan ser utilizadas por intrusos malintencionados.

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

Una vez terminada la etapa de identificación de vulnerabilidades procedo con la explotación de las mismas, para lo cual realizo pruebas de acuerdo a los servicios y vulnerabilidades presentes con el objetivo de explotar de manera exitosa y obtener acceso no autorizado a recursos o servicios del sistema vulnerable.
Kali Linux trae en sus herramientas Metasploit Framework, MSF cuenta con varias interfaces cada una con sus ventajas y desventajas, en este caso se utiliza msfconsole la cual es capaz de acceder a la mayoría de características de MSF.
En un terminal de kali linux se escribe **msfconsole** para iniciar, una vez iniciado se carga la consola con detalles como la versión de metasploit, cantidad de exploits, módulos auxiliares y payload existentes, en la figura 4.32 se puede observar lo mencionado.

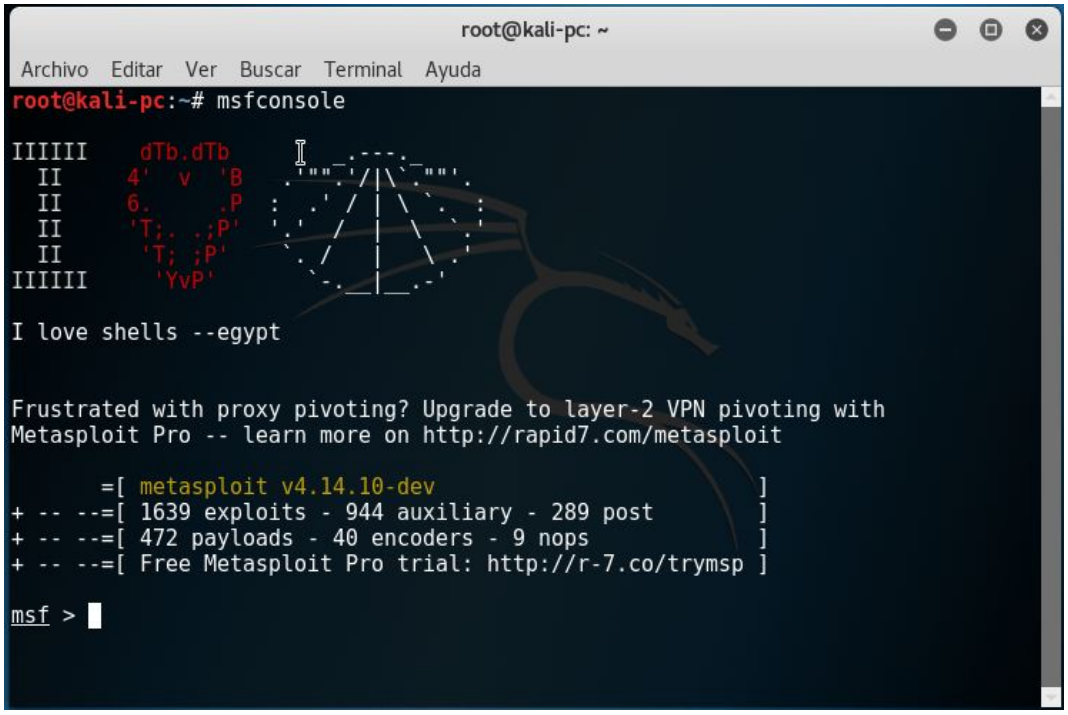


Figura 4.32: Inicio de msfconsole
Elaborado por: Christian Miranda

Para obtener información sobre los comandos se lo hace escribiendo el comando **help** o el símbolo **?**.
Los comandos básicos necesarios que se utilizan para realizar un ataque de forma manual son:

- **search:** busca módulos que contienen la característica especificada.
- **info:** muestra detalles del módulo especificado.
- **use:** selecciona el módulo que se especifica.
- **set/unset:** configura los parámetros del módulo que se está usando.
- **exploit:** explota o ejecuta el módulo.
- **run:** ejecuta un módulo auxiliar que se está usando.

Las vulnerabilidades las cuales se tratan de explotar son las consideradas como altas ya enumeradas con anterioridad.
Con el objetivo de no atentar la integridad de la red y los dispositivos del Ministerio de Inclusión Económica y Social de Ambato se crean equipos virtuales con similares características a los reales (ver figura 4.33), esto se lo realiza como medida de seguridad ante la probabilidad de dejar inutilizable un servidor o inaccesible un servicio.

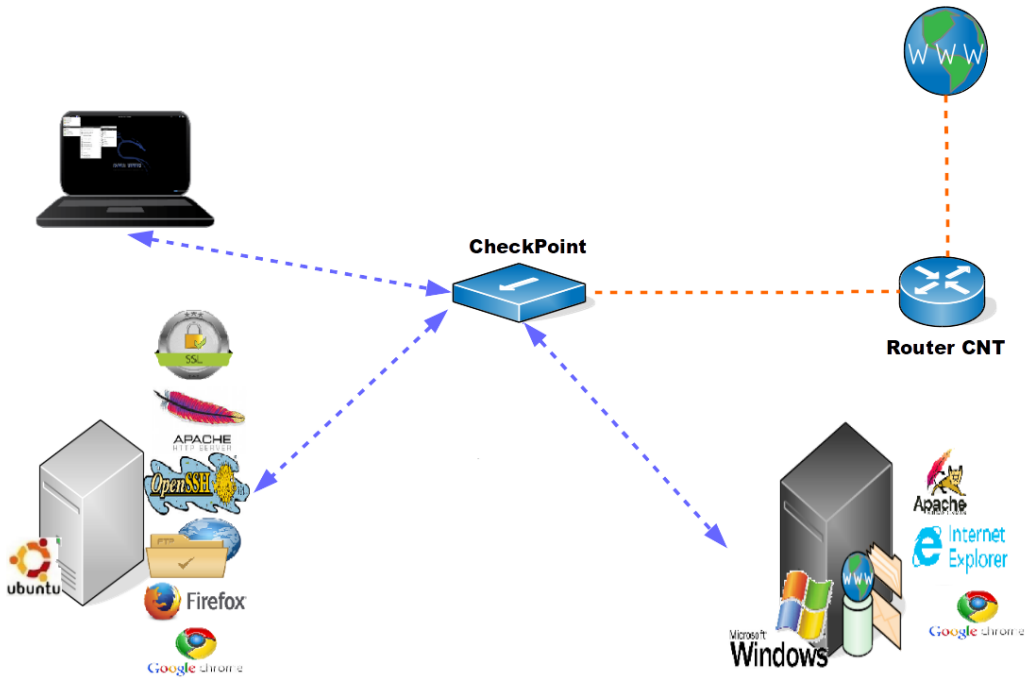


Figura 4.33: Entorno virtualizado para la explotación de vulnerabilidades
Elaborado por: Christian Miranda

4.7.1.1. Equipo virtual Windows

Se crea un equipo virtual Windows Server 2012 con similares características a los servidores reales, cabe mencionar que varias versiones de Windows son afectadas por la misma vulnerabilidad y de igual manera sus servicios.

- **Datos:**
  - Máquina virtual con sistema operativo kali linux con ip 172.21.124.124 (la cual llamaremos auditor).
  - Máquina virtual con sistema operativo Windows Server 2012 R2 con ip 172.21.124.119 (la cual llamaremos objetivo).

Explotación de vulnerabilidad en el servicio SMB.

Una vulnerabilidad en el servicio SMB (Server Message Block) que podría permitir la ejecución remota de código recomendando a sus clientes que apliquen las actualizaciones de manera inmediata. SMB es un protocolo para compartir archivos en la red Microsoft [33].
El objetivo de este ataque es tratar de iniciar una sesión mediante la explotación de la vulnerabilidad del servicio SMB de Windows, este ataque es viable debido a que el sistema operativo Windows en sus versiones Server 2008 y Server 2012 R2 tienen una vulnerabilidad que afecta al servicio en mención y se cuentan con exploit públicos para su explotación[33].

- Exploit windows/smb/eternalblue.
- Payload windows/meterpreter/reverse_tcp.
- Puerto de ataque 445 de servicio SMB.

En msfconsole se selecciona el exploit, **use exploit/multi/handler**, el payload **windows/x64/shell/reverse_tcp**.
Se ingresan los datos necesarios como son LHOST y LPORT que vienen a ser la ip del auditor y el puerto por el cual se realizará la explotación de la vulnerabilidad, cabe mencionar que el puerto por el cual escucha el auditor ya está definido y el puerto definido es el que utiliza el SMB, una vez hecho esto se ejecuta mediante el comando EXPLOIT, ver figura 4.34.

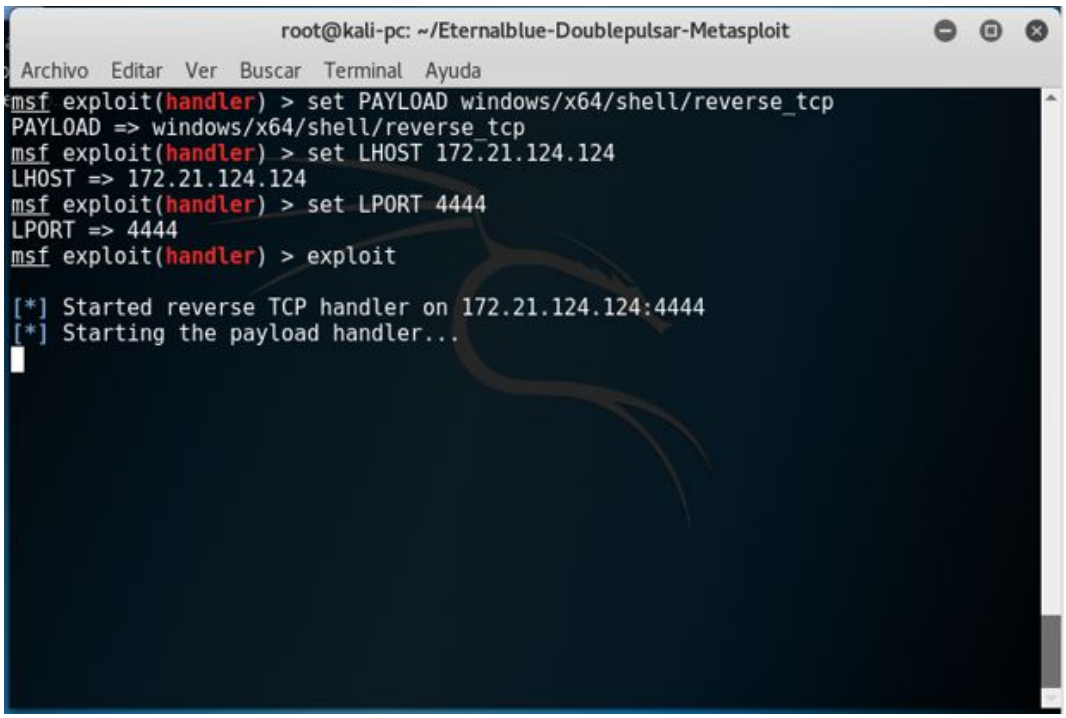


Figura 4.34: Ejecución de exploit de vulnerabilidad SMB
Elaborado por: Christian Miranda

Ahora ejecutamos el PAYLOAD reverse_tcp en la cual mandamos la ip del servidor de destino o al cual estamos efectuando la explotación del servicio y verificamos que se realice la explotación, como se puede observar en la figura 4.35.

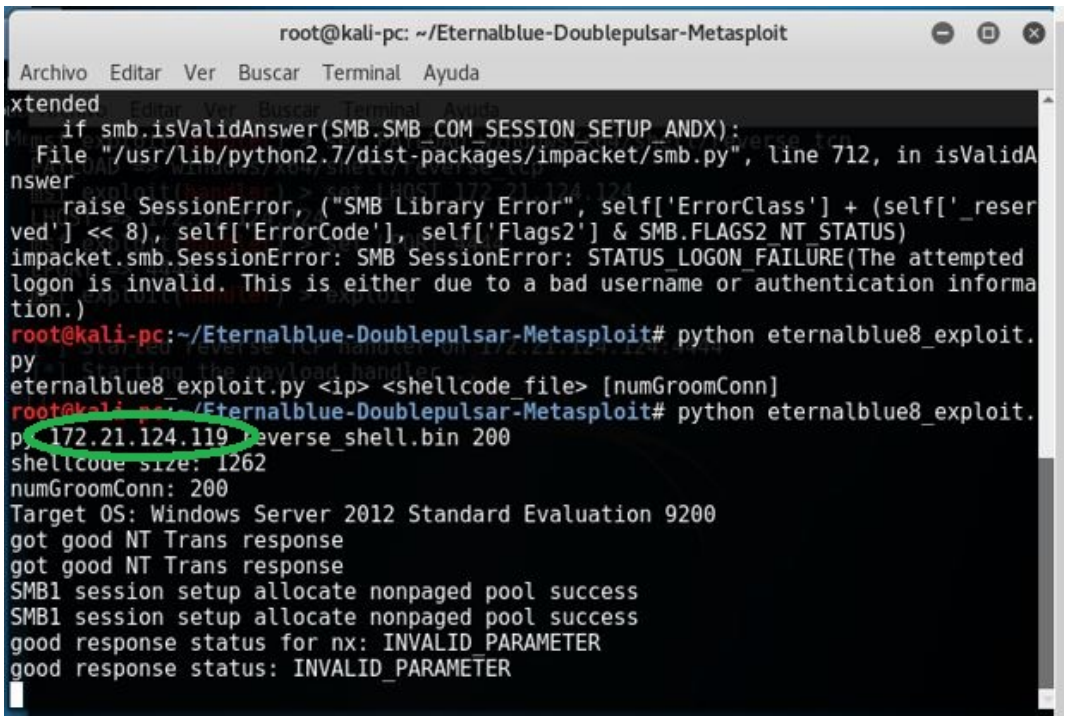


Figura 4.35: Ejecución del payload
Elaborado por: Christian Miranda

Como podemos observar el ataque se realiza con cierto grado de éxito, ya que debido a la configuración que tiene el servidor no me permite iniciar sesión a la consola de Windows, pero aun así se detuvo el servidor como se puede observar en la figura 4.36.

Figura 4.36: Windows Server 2012 dado de baja
Elaborado por :Christian Miranda

Una de las primeras cosas que un atacante real hace al tener éxito en iniciar una sesión con un sistema objetivo es, migrar el proceso para que éste pueda seguir ejecutándose sin ser descubierto o finalizado, esto se lo realiza con el comando migrate seguido del PID (Identificador de proceso). Con el comando ps se lista los procesos y así se lo puede seguir ejecutando con normalidad.

Para dejar el meterpreter y utilizar directamente la consola del sistema comprometido se utiliza el comando **shell**, después de esto se puede ejecutar cualquier comando del cmd de Windows.

Explotación de vulnerabilidades en Remote Desktop Protocol.

Microsoft publicó un nuevo aviso de seguridad (Microsoft Security Advisories 904797), donde advierte sobre una vulnerabilidad en el componente "Escritorio remoto" (Remote Desktop), la cual permite crear sesiones virtuales en un equipo con alguna de las versiones mencionadas de Windows, para ejecutar aplicaciones y acceder a datos desde computadoras remotas.
RDP funciona a través de cualquier conexión TCP/IP, incluidas una conexión de acceso telefónico, una red de área local (LAN), una red de área extensa (WAN), una Red digital de servicios integrados (ISDN), DSL o una Red privada virtual (VPN), la vulnerabilidad detectada, podría ser utilizada para realizar ataques de denegación de servicio (DoS), mediante peticiones creadas maliciosamente, y enviadas al protocolo RDP[34].
Para esto ingreso metasploit y utilizo el módulo ms12_020_maxchannelids, el cual usa como puerto de ataque al puerto 3389 del servicio RPD.
Para configurar el Metasploit se selecciona el modulo y seguidamente se ingresa **RHOST** que viene a ser la ip objetivo de la siguiente manera:

- **use auxiliary/dos/windows/rpd/ms12_020_maxchannelids.**
- **set RHOST 172.21.124.119.**

Por último se ejecuta mediante el comando **run**, (ver figura 4.37).

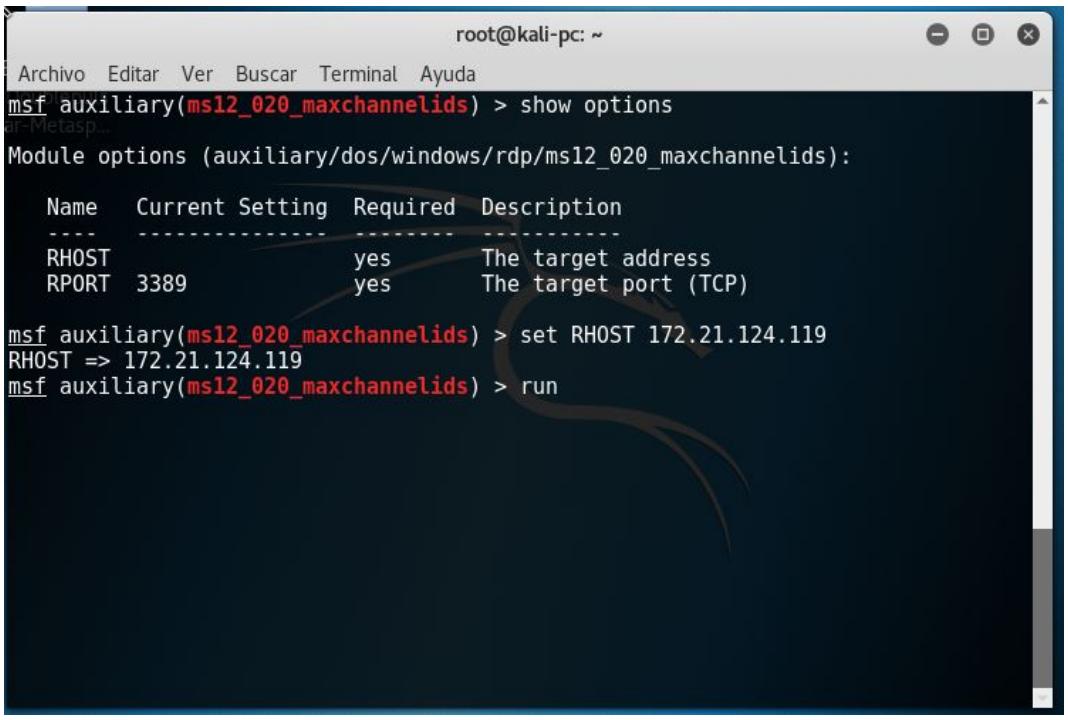


Figura 4.37: Ejecución y explotación de vulnerabilidad RDP
Elaborado por: Christian Miranda

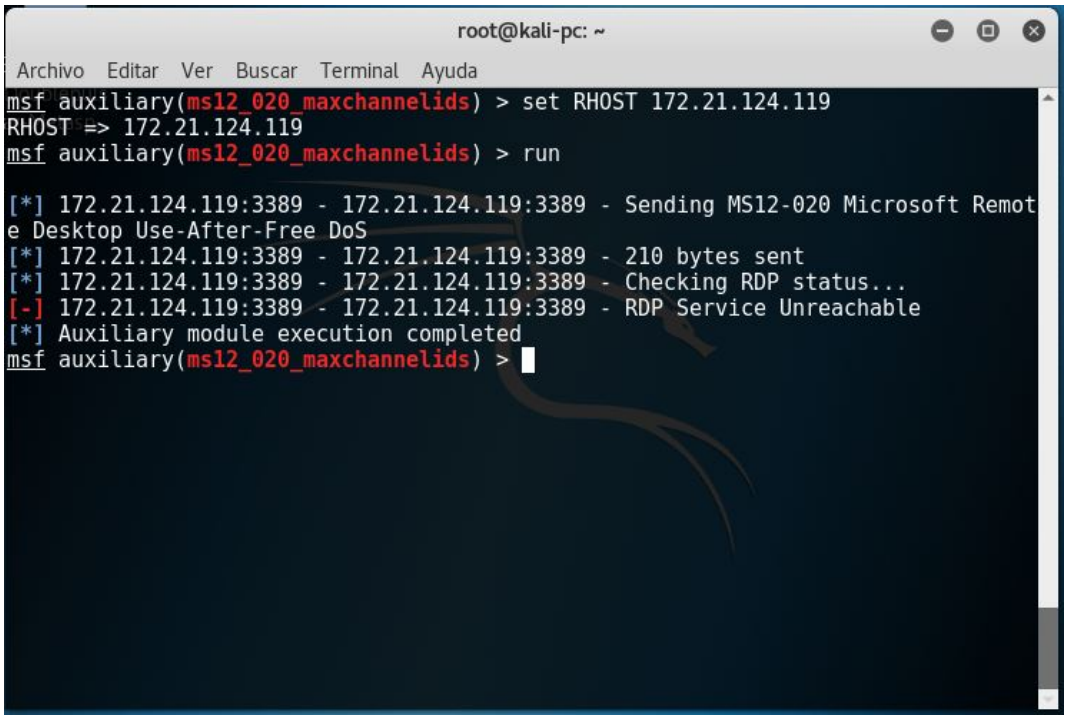


Figura 4.38: Fallo en explotación de vulnerabilidad RDP
Elaborado por: Christian Miranda

En la figura 4.38 se observa el fallo de la explotación de la vulnerabilidad RDP el cual es causado porque en el sistema operativo Windows server 2012 r2 el personal de Microsoft le dieron solución esa vulnerabilidad, los sistemas afectados (si se activa el servicio), son los siguientes

- Microsoft Windows 2000 Service Pack 4
- Microsoft Windows XP Service Pack 1
- Microsoft Windows XP Service Pack 2
- Microsoft Windows XP Professional x64 Edition
- Microsoft Windows Server 2003
- Microsoft Windows Server 2003 (Itanium-based Systems)
- Microsoft Windows Server 2003 Service Pack 1
- Microsoft Windows Server 2003 SP1 (Itanium-based Systems)
- Microsoft Windows Server 2003 x64 Edition [34].

Explotación de vulnerabilidad de divulgación de información del servicio Apache.

Esta vulnerabilidad permite a un atacante obtener una visión general de la configuración del servidor web remoto Apache mediante la solicitud de la "URL :puerto". Este resumen incluye información como módulos instalados, su configuración y la configuración de tiempo de ejecución surtidos.

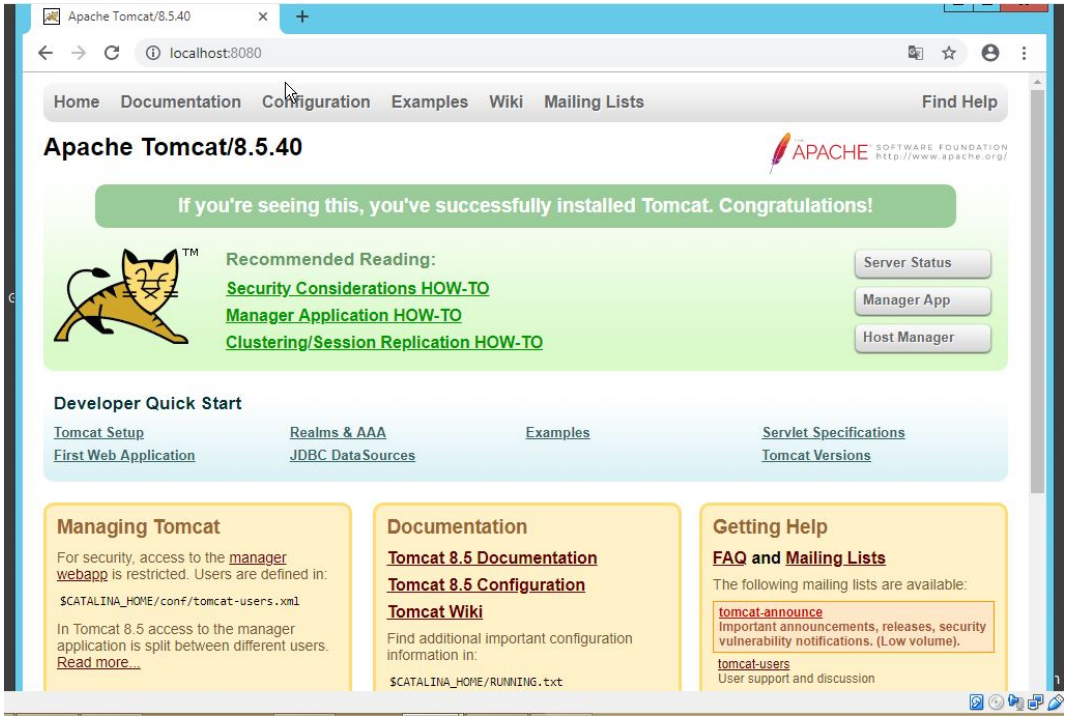


Figura 4.39: Vista del servicio Apache Tomcat
Elaborado por: Christian Miranda

En la figura 4.39 se observa las configuraciones de Apache en el servidor remoto. Un Administrador debe realizar varias configuraciones luego de instalar Apache, una de ellas es eliminar los mensajes de bienvenida y archivos por defecto los cuales facilitan información, esto hace más fácil la etapa de reconocimiento para un atacante.

Ataque de Denegación de Servicios (DoS).

El objetivo del ataque es provocar que el servicio que ofrece un servidor sea inaccesible mediante DoS (Denegación de Servicio). Un ataque de este tipo provoca que servicios como SMTP, HTTP, POP3, etc. queden sin servicio o inoperables.
Se utiliza para provoca un "request time out" mediante el envío de solicitudes a un servidor el cual se congestiona y no es capaz de responder (ver figura 4.40).
hping3 -S 172.214.119 –flood –rand-source -a 5000 -p 8080

- **-p:** el puerto a atacar.
- **-S:** activa el flag Syn.
- **–flood:** indica a hping3 que envíe los paquetes a la máxima velocidad posible.

- **-a:** para que la ip no sea visible.
- **–rand-source:** genera direcciones al azar.

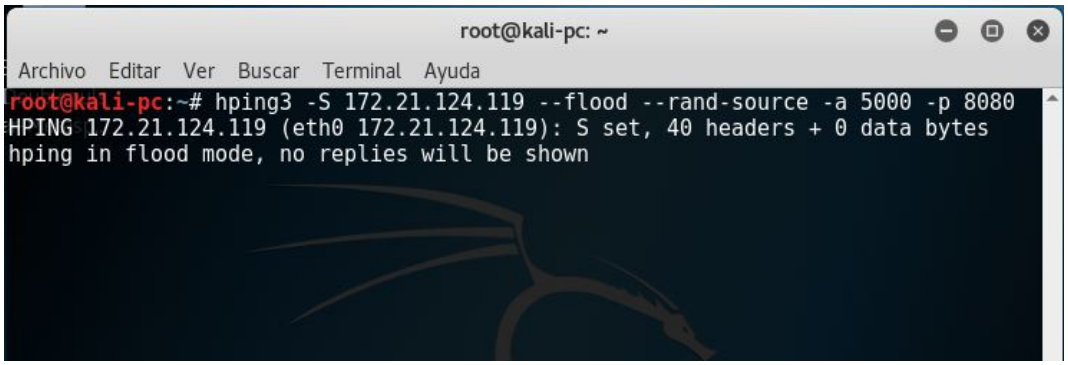


Figura 4.40: Ejecución comando hping3
Elaborado por: Christian Miranda

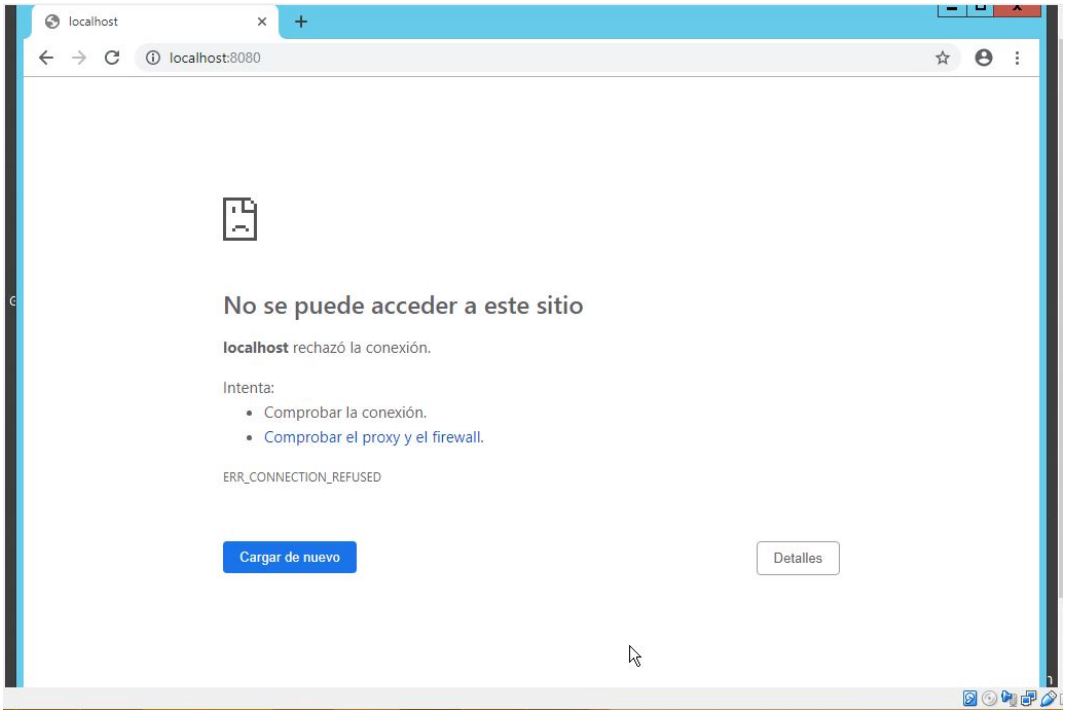


Figura 4.41: Éxito en el ataque por DoS al servicio web
Elaborado por: Christian Miranda

En la figura 4.41 se aprecia el éxito de la ejecución de hping3 provocando que el servicio web esté inaccesible.

4.7.1.2. Equipo Virtual Ubuntu

Se crea un equipo virtual Ubuntu 14.04.2 LTS para verificar la vulnerabilidad MITM (man-in-the-middle), esto se lo realiza por motivo de que dicho ataque puede provocar denegación de servicio de red, pérdidas de conexión o que los dispositivos de la red tengan que ser reiniciados.

- **Datos:**
  - Maquina virtual con sistema operativo kali linux con ip 172.21.124.124 (la cual llamareos auditor).
  - Máquina virtual con sistema operativo Ubuntu 14.04.2 con ip 172.21.124.120 (la cual llamaremos objetivo).

Explotación de vulnerabilidad de desbordamiento de búfer en FTP.

Una vulnerabilidad fue encontrada en FTP Server 3.1.0 (File Transfer Software) y clasificada como crítica. Una función desconocida es afectada por esta vulnerabilidad. A través de la manipulación de un input desconocido se causa una vulnerabilidad de clase desbordamiento de búfer. Esto tiene repercusión sobre la confidencialidad, integridad y disponibilidad[35].
El ataque se puede efectuar a través de la red. La explotación no necesita ninguna autentificación específica[35].
El objetivo de este ataque es aprovechar la vulnerabilidad del servicio **ftp** de desbordamiento de búfer y ejecutar código arbitrario mediante msfconsole e iniciar sesión en el sistemas objetivo en caso de tener éxito en la explotación.

- Exploit auxiliary/scanner/ftp/anonymous
- Puerto de ataque 21 del servicio ftp.

En msfconsole se selecciona el exploit y se ingresa RHOST que viene a ser la ip objetivo, cabe mencionar que el puerto ya se encuentra definido como se observa en la siguiente imagen, una vez hecho esto se ejecuta el exploit.

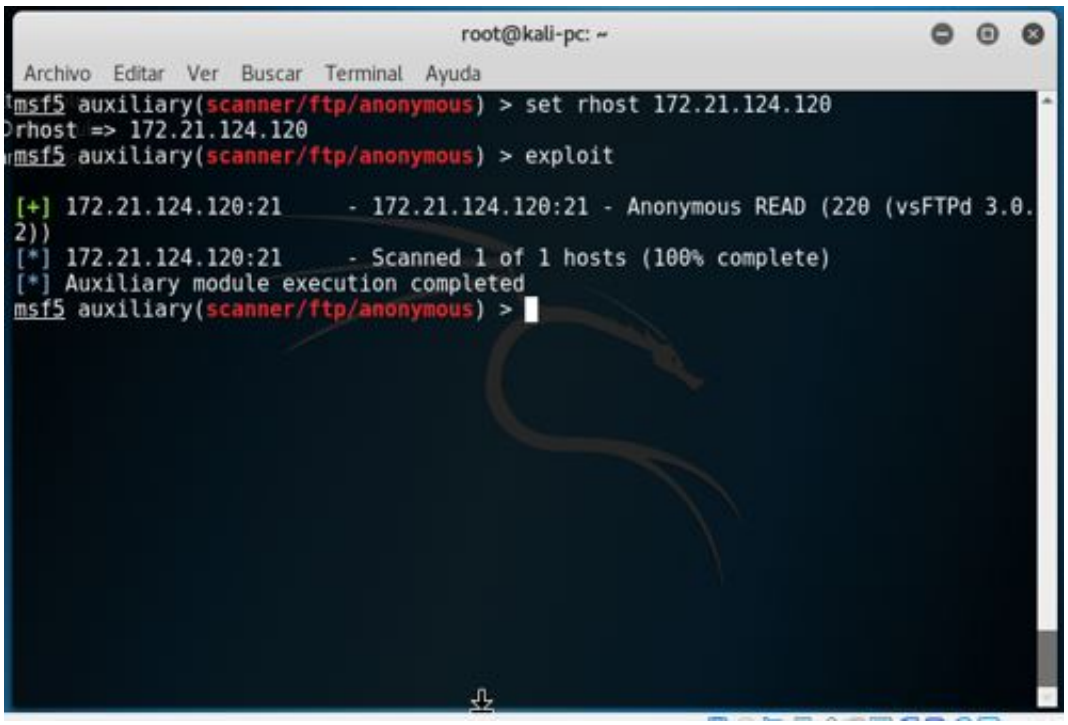


Figura 4.42: Configuración y explotación de vulnerabilidad FTP
Elaborado por: Christian Miranda

En la figura 4.42 se observa la ejecución del exploit teniendo éxito, por el motivo de que en la configuración del servicio FTP se encuentra activada la opción de anonymous, lo que significa que los usuarios pueden conectarse mediante esa autenticación.

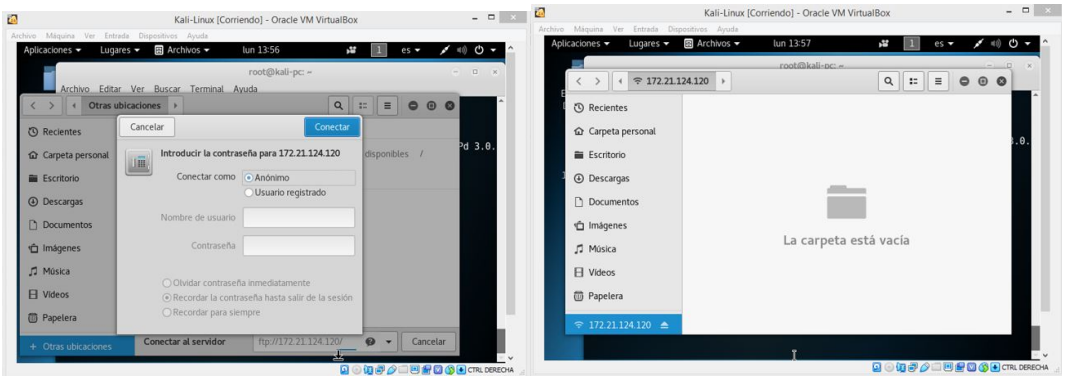


Figura 4.43: Conexión a FTP mediante anonymous
Elaborado por: Christian Miranda

Certificado SSL

Ante la vulnerabilidad de "Certificado SSL no confiable" considerada como un nivel de riesgo medio el cual podría facilitar ataques man-in-the-middle contra el

host remoto a continuación una breve introducción sobre certificados SSL.
La seguridad en la capa de aplicación (SSL), proporciona la confidencialidad, integridad y autenticidad de los datos, entre dos aplicaciones que se comunican entre sí. El presente artículo es el resultado de haber implementado certificados SSL / TLS gratuitos en servidores de aplicación, determinando las características relevantes que debe tener un certificado SSL/TLS, la Autoridad certificadora que lo emita. Se realiza un análisis de las vulnerabilidades en los servidores web y se establece un canal cifrado de comunicaciones con el fin de proteger de ataques como hombre en el medio, phising y mantener la integridad de la información que es trasmitida entre el cliente y servidor[36].

Ataque Man-in-the-middle

Según el autor M. Markovi en su artículo de investigación define "Main the middle como su nombre indica, un ataque de hombre en el medio ocurre cuando alguien entre dos usuarios intercepta la comunicación supervisando, capturando y controlando la comunicación sin el conocimiento de los usuarios. Por ejemplo, un agresor puede negociar claves de cifrado con ambos usuarios y cada usuario envía datos cifrados al atacante, que puede descifrar los datos con las claves públicas y privadas" (Markovi, 2007). La mayoría de los protocolos criptográficos incluyen alguna forma de autentificación de extremos específicamente para prevenir los ataques Hombre en el medio (siglas en ingles MITM), un ejemplo sería SSL que autentica al servidor web mediante una autoridad de certificación de confianza [36].
Para la ejecución del ataque y comprobar la existencia de la amenaza en la capa de transporte, se la realiza mediante las herramientas como SslStrip, que permite filtrar todo acceso por HTTPS a HTTP y Ettercap en la que se intercepta los paquetes seleccionando la tarjeta de red, ambas vienen integradas en Kali Linux [36].

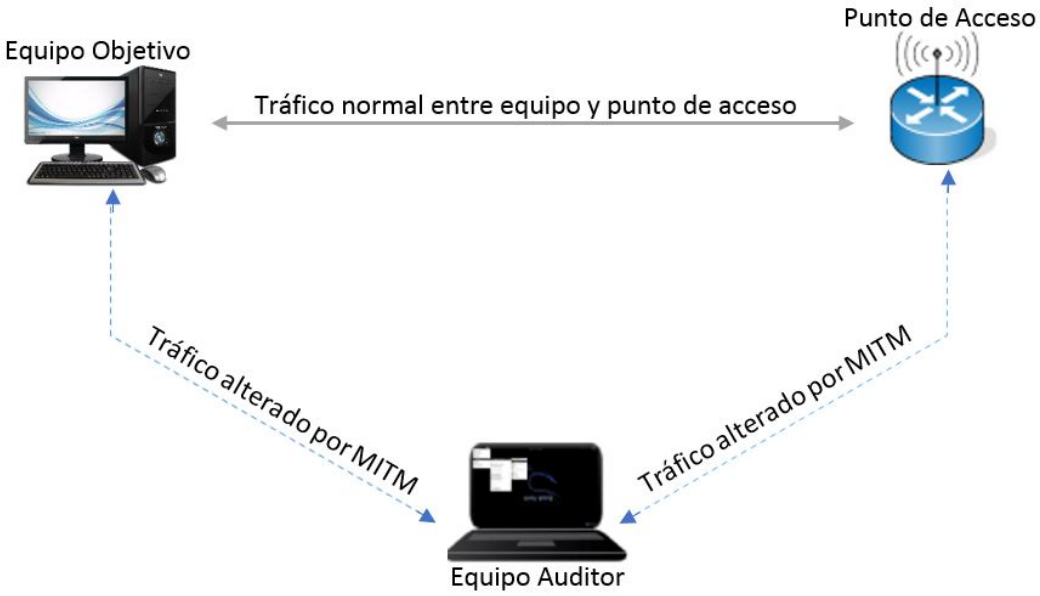


Figura 4.44: Diagrama de ataque de Man-in-the-Middle.
Elaborado por: Christian Miranda

Lo primero que se realiza en el equipo auditor es habilitar el reenvío de tráfico, esto se lo hace modificando **ip_forwarding** (modo ruteador) mediante **echo 1 > /proc/sys/net/ipv4/ip_forward**, luego se crea una regla de redireccionamiento en iptables de la siguiente manera **iptables -t nat -A PREROUTING -tcp --destination-port 80 -j REDIRECT -to-port 16000**, la regla permite que las solicitudes direccionadas al puerto 80 sean redireccionadas al puerto 16000, para empezar a descifrar el tráfico del puerto 16000 se digita **sslstrip -l 16000** (ver figura 4.45).

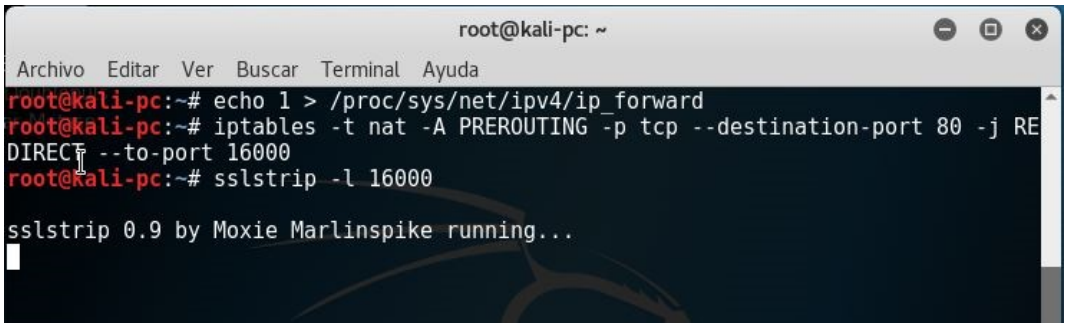


Figura 4.45: Configuración de ruteo de iptables.
Elaborado por: Christian Miranda

Iniciando **ettercap**, se elige el envenamiento ARP, **Sniff > Unified Sniff** en la barra de menú con la taerjeta de red respectiva.
Mediante el escaneo de host se elige la ip objetivo como TARGET1 y la puerta de

enlace como TARGET2, seguidamente se procede con el envenenamiento ARP e iniciar escuchar (sniffing) la red.

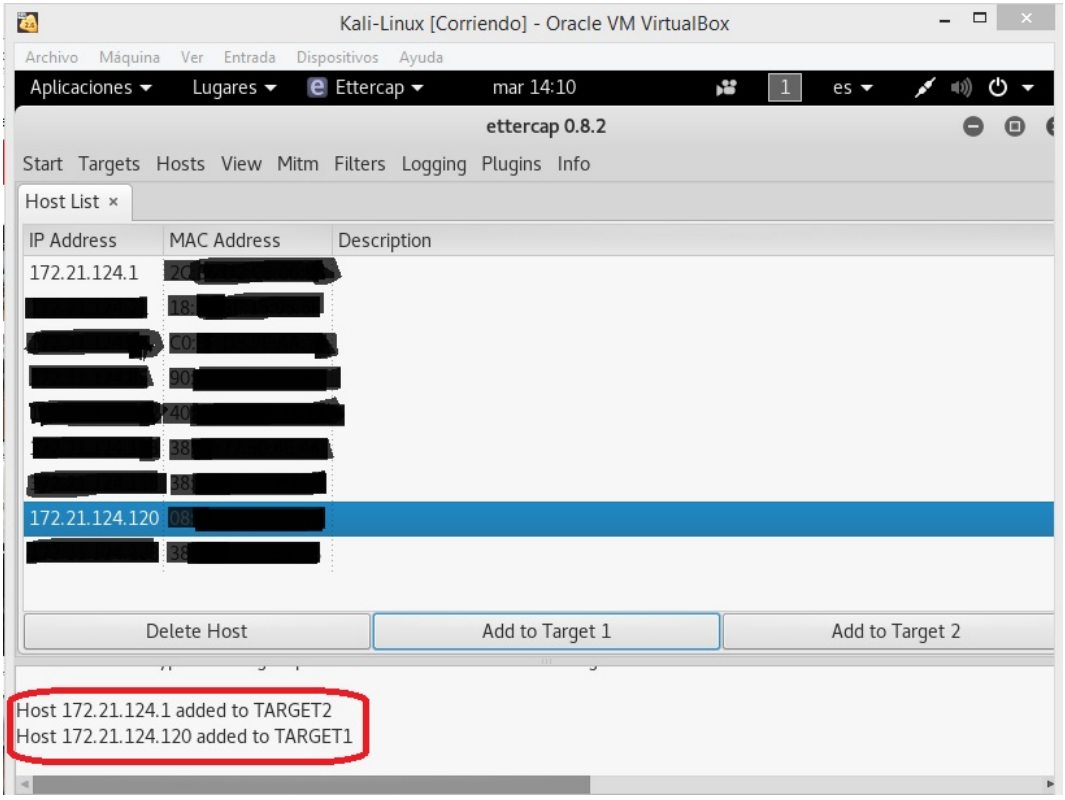


Figura 4.46: Selección de ip a escuchar (sniffing)
Elaborado por: Christian Miranda

En la figura 4.46 se observa la herramienta Ettercap seleccionando el equipo objetivo y añadiéndolo como TARGET1.
En el equipo objetivo o víctima se ingresa a sitios web seguros como son hotmail, gmail, etc., es decir sitios con certificados SSL y tambien se ingresa a sitios sin certificados SSL.

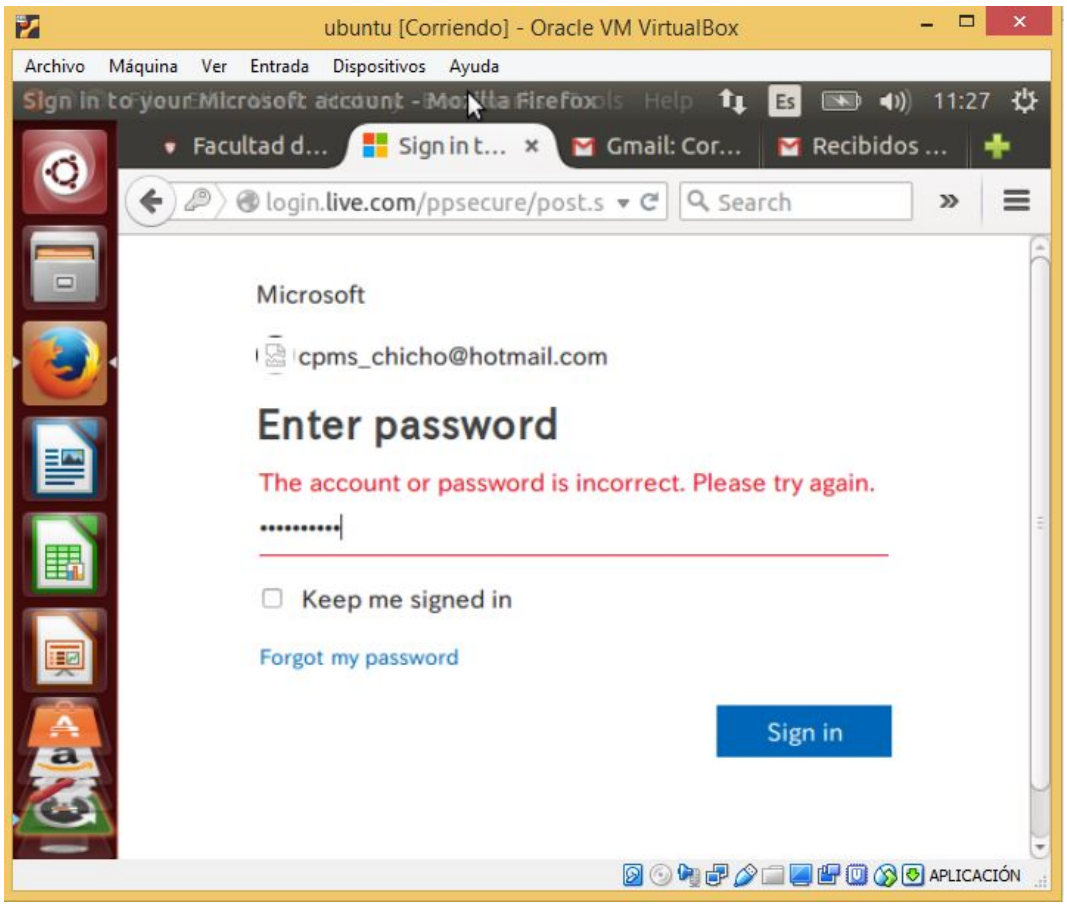


Figura 4.47: Inicio de sesión en un ordenador envenenado.
Elaborado por: Christian Miranda

En la figura 4.47 se observa el ingreso de credenciales en un sitio de confianza desde el navegador web en el Sistema operativo Ubuntu.
En el equipo auditor se puede observar la información capturada del equipo objetivo mediante **Etterap**, ver figura 49.

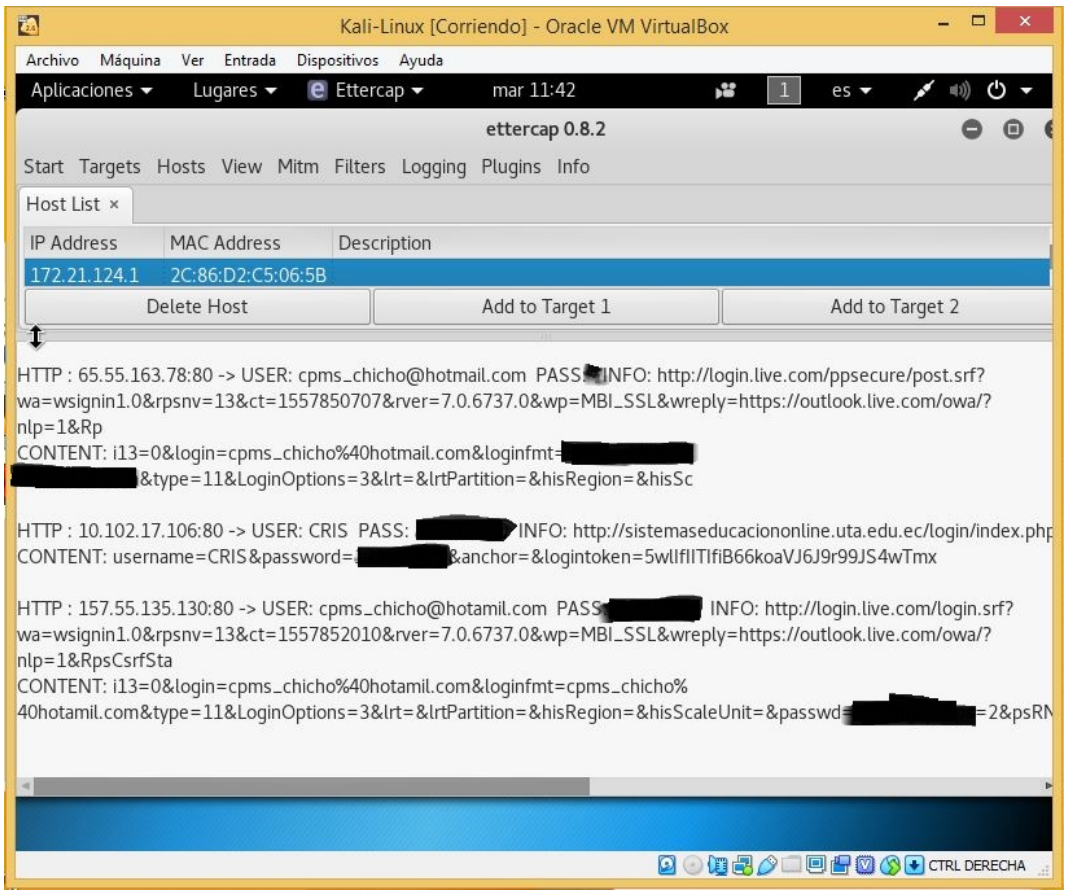


Figura 4.48: Captura de tráfico y obtención de credenciales en ettercap
Elaborado por: Christian Miranda

Como se puede observar en la figura 4.48, se ha realizado capturas de paquetes de un sitio seguro y de un sitio inseguro dando como resultados credenciales las cuales fueron ingresados por el usuario en el navegador del equipo objetivo.

Ataque de Denegación de Servicios (DoS).

Una vulnerabilidad fue encontrada en Squid Proxy (Firewall Software) y clasificada como problemática. Una función desconocida del componente Cache es afectada por esta vulnerabilidad. Por la manipulación de un input desconocido se causa una vulnerabilidad de clase denegación de servicio. Esto tiene repercusión sobre la integridad y disponibilidad[37].

La explotación se considera fácil. El ataque se puede efectuar a través de la red. La explotación no necesita ninguna autentificación específica. No se conoce los detalles técnicos ni hay ningún exploit disponible[37].

El objetivo del ataque es provocar que el servicio que ofrece el servidor sea inaccesible mediante DOS(Denial of Service), y sin que el software de Firewall se

interponga (squid). Un ataque de este tipo provoca que servicios como SMTP, HTTP, POP3, etc. queden inoperables.
Se envía una serie de paquetes para provocar un congestionamiento de tráfico y así lograr un "request time out", es decir no es capaz de responder.

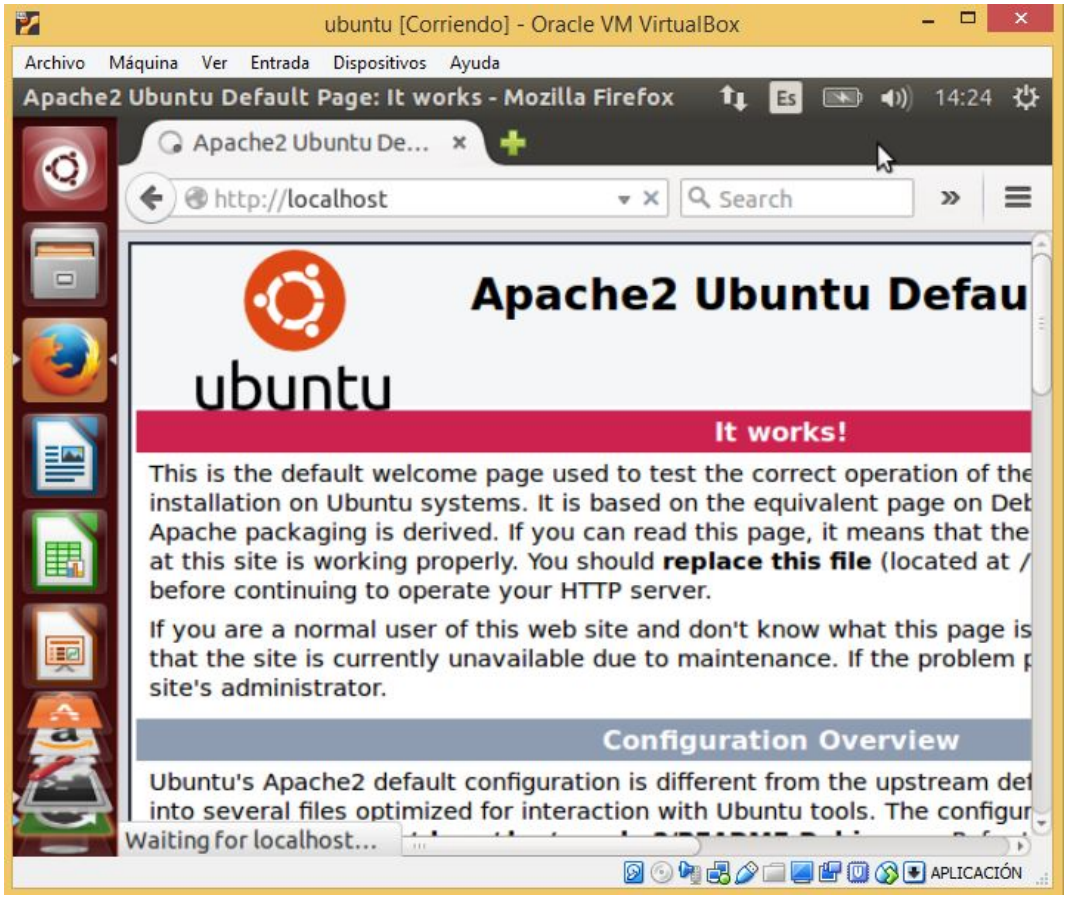


Figura 4.49: Servicio Apache en ejecutandose en servidor Ubuntu
Elaborado por: Christian Miranda

En la figura 4.49 se observa el servicio apache ejecutándose correctamente en el puerto 80. Se utiliza la herramienta **slowloris.pl** para provocar el congestionamiento del servidor, para lo cual se debe realizar lo siguiente.

perl slowloris.pl -dns 172.21.124.120 -port 80 -timeout 20 -num 6000 -cache

en donde:

- **-dns:** es la ip del servidor a atacar.
- **-port**: el protocolo a atacar.
- **-timeout:** el tiempo de espera en segundos para enviar los paquetes.

- **-num:** el numero de paquetes a enviar.
- **-cache:** en este caso se envia el ataque hacia la cache.

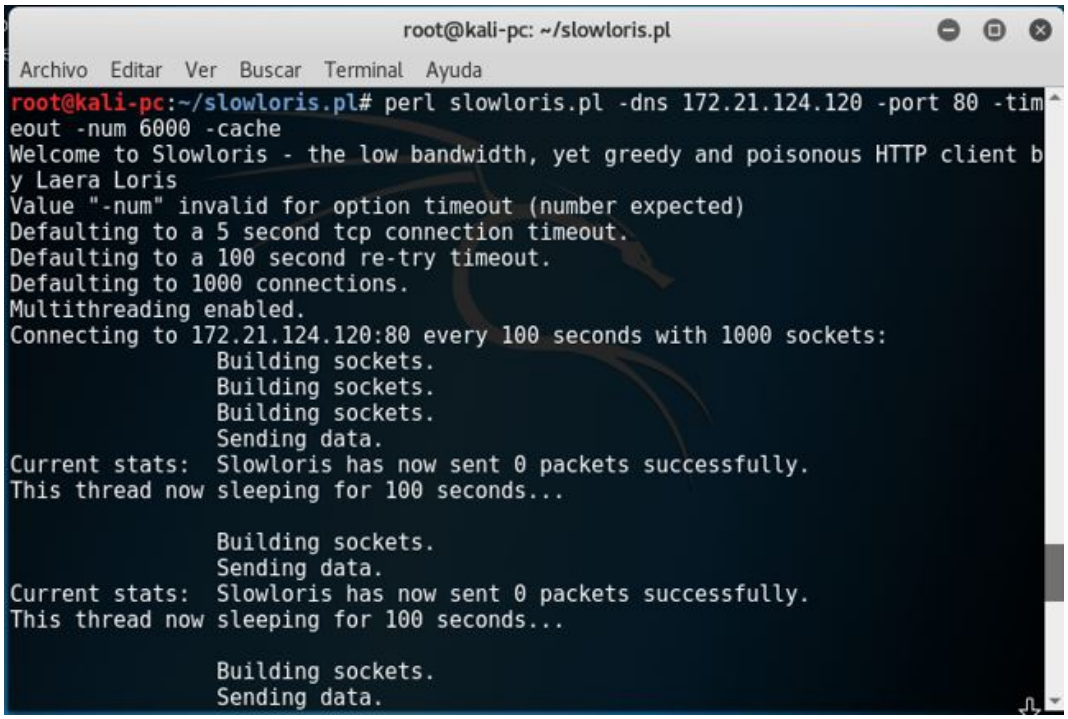


Figura 4.50: Envió de paquetes mediante slowloris
Elaborado por: Christian Miranda

En la figura 4.50 se observa el envió de paquetes mediante la herramienta slowloris.pl hacia nuestro servidor en el cual está en ejecución el servicio apache.

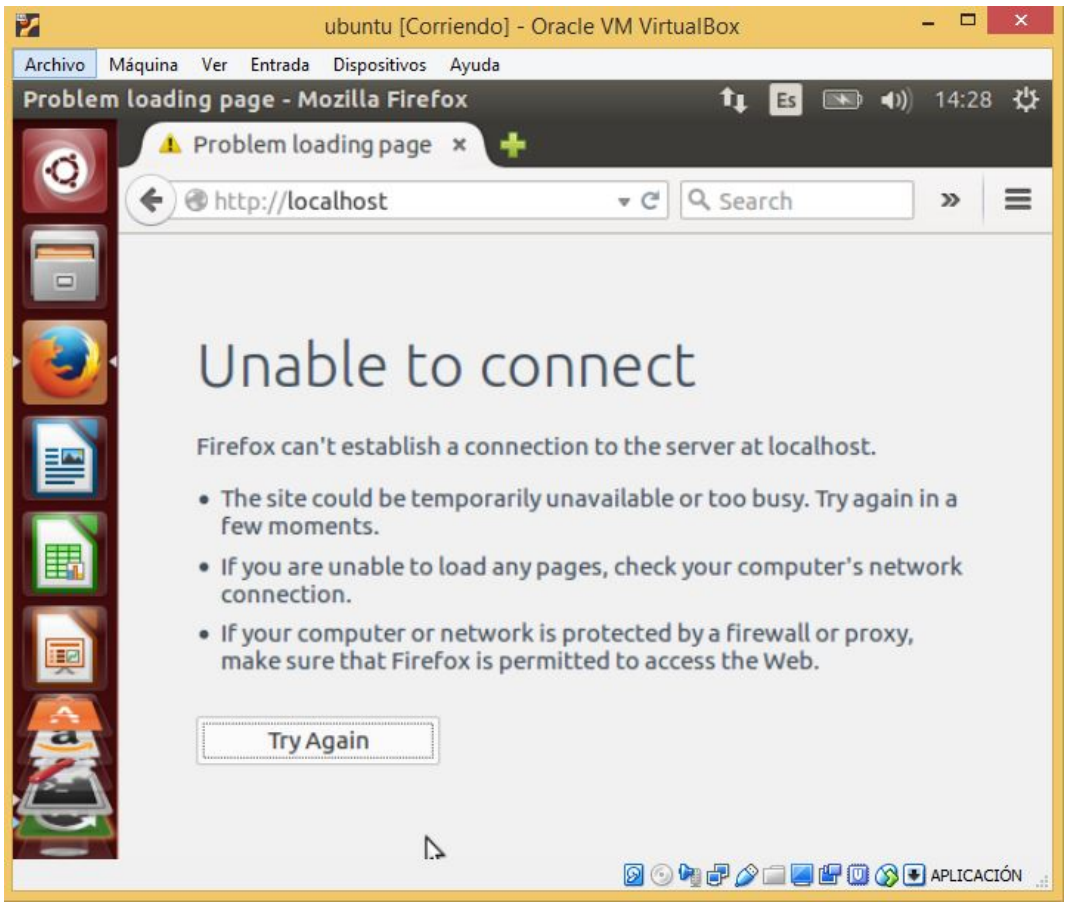


Figura 4.51: Éxito en el ataque DoS al servicio Apache en el servidor Ubuntu
Elaborado por: Christian Miranda

En la figura 4.51 se aprecia el éxito del ataque DoS al servicio en mención mediante la ejecución del comando con la herramienta slowloris.pl, de esta manera provocando que el servicio web sea inaccesible.

4.7.1.3. Resumen de explotación de vulnerabilidades

Sistema Operativo	Versión	Vulnerabilidad	Explotable	Observación
Windows Server	2003	Eternalblue, Servicio SMB.	No	Existe actualización de seguridad la cual cubre varias vulnerabilidades como la del servicio SMB y la de denegación de servicios (DoS).
		/ms12_020_maxchannelids, Microsoft RDP.	Si	
		Eternalblue, Servicio RPC.	No	
	2012 r2	Eternalblue, Servicio SMB.	Si	
		/ms12_020_maxchannelids, Microsoft RDP.	No	
		Eternalblue, Servicio RPC.	No	
Linux	Ubuntu 14.04	Divulgación de Información	Si	Las instalaciones por defecto pueden divulgar información delicada del sistema o servicio

Tabla 4.26: Resumen de vulnerabilidades explotables

Elaborado por: Christian Miranda

Servicio	Sistema Operativo	Ataque	Explotable
Apache Web service	Windows Server 2012 r2	Denegación de Servicios (DoS)	No
Apache Web service	Windows Server 2012 r2	Divulgación de Información	Si
Apache Web service	Windows Server 2012 r2	Desbordamiento de Memoria	Si
Protocolo de transferencia de archivos FTP	Windows Server 2012 r2	Desbordamiento de Memoria	Si
Protocolo de transferencia de archivos FTP	Ubuntu 14.04	Desbordamiento de Memoria	Si
Navegador Internet Explorer	Windows Server 2012 r2	Men – In – The – Middle	Si
Navegador Firefox	Ubuntu 14.04	Men – In – The – Middle	Si
Navegador Google Chrome	Windows Server 2012 r2	Men – In – The – Middle	Si
Apache Web service	Ubuntu 14.04	Denegación de Servicios	Si
Apache Web service	Ubuntu 14.04	Desbordamiento de Memoria	Si
OpenSSH	Ubuntu 14.04	Men – In – The – Middle	Si
Apache Web service	Windows Server 2003	Divulgación de Información	Si

Tabla 4.27: Resumen de servicios explotables

Elaborado por: Christian Miranda

4.8. Políticas de contingencia de seguridad informática que mejoren la integridad, confidencialidad y disponibilidad de la información del Ministerio de Inclusión Económica y Social.

4.8.1. Políticas de Seguridad que mejoren la integridad, confidencialidad y disponibilidad de la información que se maneja a través de la red en base a las vulnerabilidades detectadas incluyendo soluciones orientadas a resolverlos.

A continuación se documenta de manera más detallada las vulnerabilidades detectadas en los servidores institucionales incluyendo la posible solución para proteger los activos de la red del Ministerio de Inclusión Económica y Social ante daños y perjuicios que puedan ser causados por la explotación exitosa de dichas vulnerabilidades.

- **Servidor info.inclusion.gob.ec**

Vulnerabilidad: La versión de php que se ejecuta es la numero 7.2.x antes de 7.2.14, por lo tanto es afectado por denegación de Servicios
Riesgo: Alto
Descripción: Existe una vulnerabilidad de denegación de servicios (DoS) en ext/imap/php_imap.c. Un atacante remoto no autenticado puede tener un impacto no especificado a través de una solicitud especialmente diseñada, para provocar una lectura fuera de límites o una condición de lectura después de libre, lo que podría resultar en un compromiso completo del sistema.
Código CVE: CVE-2016-10166, CVE-2018-19935, CVE-2019-6977, CVE-2019-9020, CVE-2019-9021, CVE-2019-9022, CVE-2019-9023, CVE-2019-9024
Explotado: Si.
Solución: Actualizar a la versión de PHP 7.2.14 o superior.
Referencias:
URL: http://php.net/ChangeLog-7.php#7.2.14

Vulnerabilidad: El servidor web tiene habilitados los siguientes métodos HTTP: TRACE
Riesgo: medio
Descripción: Un atacante puede usar esta falla para engañar a sus usuarios legìtimos de la red para que le den sus credenciales.
Código CVE: CVE-2003-1567, CVE-2004-2320, CVE-2004-2763, CVE2005-3398, CVE-2006-4683, CVE-2007-3008, CVE-2008-7253, CVE-2009-2823, CVE-2010-0386, CVE-2012-2223, CVE-2014-7883

Explotado: Si.
Solución: Desactive los métodos TRACE y TRACK en la configuración de su servidor web.
Referencias:
URL: http://httpd.apache.org/docs/current/de/mod/core.html#traceenable
URL: http://www.owap.org/index.php/Cross_Site_Tracing

Vulnerabilidad: La versión de Apache que se ejecuta es 2.4.x, por lo tanto es afectado por múltiples vulnerabilidades.
Riesgo: medio
Descripción: Existe una vulnerabilidad de escalada de privilegios en las secuencias de comandos de los módulos debido a la capacidad de ejecutar código arbitrario como proceso principal mediante la manipulación de del cuadro de indicadores.
Código CVE: CVE-2019-0196, CVE-2019-0197, CVE-2019-0211, CVE-2019-0215, CVE-2019-0217, CVE-2019-0220.
Explotado: Si.
Solución: Actualice a la versión 2.4.39 de Apache o posterior.
Referencias:
URL: http://www.nessus.org/u?a84bee48
URL: http://www.nessus.org/u?586e6a34

Vulnerabilidad: Se detectò que el host implementa RFC1323
Riesgo: bajo
Descripción: Un atacante puede calcular el tiempo de actividad del host remoto, mediante el envio de paquetes especiales falsificados. Si se encuentran, se informan las marcas de tiempo.
Código CVE:
Explotado: Si.
Solución: Para deshabilitar las marcas de tiempo TCP en linux, agregue la lìnea 'net.ipv.tcp_timestamps = 0' a /etc/sysctl.conf. Ejecutar 'sysctl -p' para aplicar la configuraciòn en tiempo de ejecuciòn.
Para deshabilitar las marcas de tiempo TCP en Windows ejecute 'netsh int tcp set global timestamps = disabled'.
Referencias:
URL: http://www.ietf.org/rfc/rfc1323.txt

Vulnerabilidad: HTTP tipo y versión de servidor.
Riesgo: bajo
Descripción: El tipo de servidor web remoto es apache y la directiva "Server Tokens" es ProductOnly Apache, no permite ocultar el tipo de servidor.
Código CVE:
Explotado: Si.
Solución: Configurar el servidor para usar un nombre alternativo como 'WintendohttpD w/Domatrix display'.
Asegurese de eliminar los logotipos comunes como apache_pb.gif.
Con Apahe, puede configurar la directiva 'Server Tokens Prod' para limitar la informaciòn que emana del servidor en sus encabezados de respuesta.
Para deshabilitar las marcas de tiempo TCP en Windows ejecute 'netsh int tcp set global timestamps = disabled'.
Referencias:

- **Servidor cz.inclusión.gob.ec**

Vulnerabilidad: Este host ejecuta Mikrotik RouterOS y es propenso a la vulnerabilidad de divulgación de información.
Riesgo: Medio
Descripción: La explotación exitosa permitirá que un atacante remoto se conecte al puerto WinBox y descargue un archivo de base de datos de usuario. El usuario puede iniciar sesión y tomar el control del enrutador.
Código CVE: CVE-2018-14847
Explotado: No.
Solución: Actualizar a MikroTik RouterOS version 6.42.1 o 6.3rc4 o superior.
Referencias:
URL: http://forum.mikritik.com/viewtopic.php?t=133533

Vulnerabilidad: El host está ejecutando Squid y es propenso a la vulnerabilidad de envenenamiento de caché
Riesgo: Medio
Descripción: La explotación exitosa permitirá a los atacantes remotos causar envenenamiento de caché y evitar la política de seguridad del mismo origen.
Código CVE: CVE-2016-4554
Explotado: Si.
Solución: Actualizar Squid a la versión 3.5.18 o superior.

Referencias:
URL: http://www.squid-cache.org/Advistories/SQUID-2016_8.txt

Vulnerabilidad: Denegación de Servicios de Squid
Riesgo: Alto
Descripción: La explotación exitosa permitirá a los servidores HTTP provocar una denegación de servicio o escribir información confidencial en los archivos de registro.
Código CVE: CVE-2016-3947, CVE-2016-3948
Explotado: Si.
Solución: Actualizar Squid a la versión 4.0.8 o superior.
Referencias:
URL: http://access.redhat.com/security/cve/cve-2016-3947
URL: http://access.redhat.com/security/cve/cve-2016-3948
URL: http://www.squid-cache.org/Advisories/SQUID-2016_4.txt
URL: http://www.squid-cache.org/Advisories/SQUID-2016_3.txt
URL: http://www.squid-cache.org

Vulnerabilidad: Este host ejecuta GlassFish Server y es propenso a una vulnerabilidad de omisión de seguridad.
Riesgo: Medio
Descripción: La explotación exitosa permitirá a los atacantes remotos ejecutar códigos de script arbitrarios en el navegador de un usuario desprevenido en el contexto de una aplicación afectada.
Código CVE: CVE-2011-4358
Explotado: Si.
Solución: Aplicar el parche de aviso referido.
Referencias:
URL: http://secunia.com/advisories/49956/
URL: http://secunia.com/advisories/46959/
URL: http://java.net/jira/browse/JAVASERVERFACES-2247
URL: http://www.oracle.com/technetwork/topics/security/cpujul2012-392727.html
URL: http://www.oracle.com/technetwork/topics/security/cpujul2012verbose-392736.html#O

Vulnerabilidad: El certificado SSL no puede ser de confianza.
Riesgo: Medio

Descripción: El certificado X.509 del servidor no se puede confiar. Esta situación puede ocurrir de tres formas diferentes, en las que se puede romper la cadena de confianza, como se indica a continuación:
- Primero, la parte superior de la cadena de certificados enviada por el servidor podría no descender de una autoridad certificadora pública conocida. Esto puede ocurrir cuando la parte superior de la cadena es un certificado autenticado no reconocido o cuando faltan certificados intermedios que conectan la parte superior de la cadena de certificados con una autoridad de certificación pública conocida.
- Segundo, la cadena de certificados puede contener un certificado que no es válido en el momento de la exploración. Esto puede ocurrir cuando la exploración se produce antes de una de las fechas de "no antes" del certificado, o después de una de las "no después" del certificado
- En tercer lugar, la cadena de certificados puede contener una firma que no coincide con la información del certificado o no se pudo verificar. Las firmas incorrectas se pueden arreglar al obtener el certificado con la firma incorrecta para que el emisor vuelva a firmarlo. Las firmas que no se pudieron verificar son el resultado de que el emisor del certificado haya usado un algoritmo de firma que Nessus no admite o no reconoce.
Si el host remoto es un host público en producción, cualquier interrupción en la cadena hace que sea más difícil para los usuarios verificar la autenticidad y la identidad del servidor web. Esto podría hacer que sea más fácil llevar a cabo ataques de hombre en el medio contra el host remoto.
Código CVE:
Explotado: Si.
Solución: Compre o genere un certificado adecuado para este servicio.
Referencias:
URL: https://www.itu.int/rec/T-REC-X.509/en
URL: https://en.wikipedia.org/wiki/X.509

Vulnerabilidad: Detección de protocolo TLS versión 1.0
Riesgo: Bajo
Descripción: El servicio remoto acepta conexiones cifradas usando TLS 1.0. TLS 1.0 tiene una serie de fallas de diseño criptográfico. Las implementaciones modernas de TLS 1.0 mitigan estos problemas, pero las versiones más nuevas de TLS como 1.1 y 1.2 están diseñadas contra estas fallas y deben usarse siempre que sea posible.
PCI DSS v3.2 requiere que TLS 1.0 se deshabilite por completo antes del 30

de junio de 2018, excepto los terminales POS POI (y los puntos de terminación SSL / TLS a los que se conectan) que pueden verificarse como no susceptibles a cualquier explotación conocida.
Código CVE:
Explotado: No
Solución: Habilite la compatibilidad con TLS 1.1 y 1.2, y deshabilite la compatibilidad con TLS 1.0.
Referencias:
URL: https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00
URL: http://www.nessus.org/u?c8ae820d

- **Servidor mail.inclusion.gob.ec**

Vulnerabilidad: Inicio de sesión de texto sin cifrar POP3
Riesgo: Medio
Descripción: El servidor POP3 remoto acepta los inicios de sesión a través de los siguientes mecanismos de autenticación de texto simple en conexiones no cifradas: USER.
El servidor POP3 remoto es compatible con el comando 'STLS' pero no impone su uso para los mecanismos de autenticación de texto sin cifrar.
Un atacante puede descubrir nombres de usuario y contraseñas rastreando el tráfico al demonio POP3 si se usa un mecanismo de autenticación menos seguro (por ejemplo, eg, USER command, AUTH PLAIN, AUTH LOGIN).
Código CVE:
Explotado: Si
Solución: Configure el servidor remoto para forzar siempre las conexiones cifradas a través de SSL / TLS con el comando 'STLS'.
Referencias:
URL: http://www.ietf.org/rfc/rfc2222.txt
URL: http://www.ietf.org/rfc/rfc2595.txt

Vulnerabilidad: Suites de cifrado SSL de potencia media compatibles (SWEET32)
Riesgo: Medio
Descripción: El host remoto admite el uso de cifrados SSL que ofrecen cifrado de intensidad media. Nessus considera la fuerza media como cualquier cifrado que use longitudes de clave de al menos 64 bits y menos de 112 bits, o bien que use el conjunto de cifrado 3DES.

Hay que tener en cuenta que es considerablemente más fácil evitar el cifrado de intensidad media si el atacante está en la misma red física.
Código CVE: CVE-2016-2183
Explotado: Si
Solución: Reconfigure la aplicación afectada si es posible para evitar el uso de cifrados de fuerza media.
Referencias:
URL: https://www.openssl.org/blog/blog/2016/08/24/sweet32/
URL: https://sweet32.info

Vulnerabilidad: Marcas de tiempo TCP, se detectó que el host implementa RFC1323.
Riesgo: Bajo
Descripción: Un efecto secundario de esta característica es que a veces se puede calcular el tiempo de actividad del host remoto.
Código CVE:
Explotado: Si
Solución: Para deshabilitar las marcas de tiempo TCP en linux, agregue la lìnea 'net.ipv.tcp_timestamps = 0' a /etc/sysctl.conf. Ejecutar 'sysctl -p' para aplicar la configuraciòn en tiempo de ejecuciòn.
Para deshabilitar las marcas de tiempo TCP en Windows ejecute 'netsh int tcp set global timestamps = disabled'.
Referencias:
URL: http://www.ietf.org/rfc/rfc1323.txt

Vulnerabilidad: Módulo Diffie-Hellman SSL / TLS <= 1024 Bits
Descripción: El host remoto permite conexiones SSL / TLS con uno o más módulos Diffie-Hellman menores o iguales a 1024 bits. A través del análisis criptográfico, un tercero puede encontrar el secreto compartido en un corto período de tiempo (dependiendo del tamaño del módulo y los recursos del atacante). Esto puede permitir a un atacante recuperar el texto sin formato o potencialmente violar la integridad de las conexiones.
Código CVE: CVE-2015-4000
Explotado: No
Solución: Reconfigure el servicio para usar un único módulo Diffie-Hellman de 2048 bits o más.
Referencias:

URL: https://weakdh.org/

Vulnerabilidad: Detección de protocolo TLS versión 1.1
Riesgo: Bajo
Descripción: El servicio remoto acepta conexiones cifradas usando TLS 1.1. TLS 1.1 tiene una serie de fallas de diseño criptográfico. Las implementaciones modernas de TLS 1.1 mitigan estos problemas, pero las versiones más nuevas de TLS como 1.2 y 1.3 están diseñadas contra estas fallas y deben usarse siempre que sea posible.
PCI DSS v3.2 requiere que TLS 1.1 se deshabilite por completo antes del 30 de junio de 2018, excepto los terminales POS POI (y los puntos de terminación SSL / TLS a los que se conectan) que pueden verificarse como no susceptibles a cualquier explotación conocida.
Código CVE:
Explotado: No
Solución: Habilite la compatibilidad con TLS 1.2 y 1.3, y deshabilite la compatibilidad con TLS 1.1.
Referencias:
URL: https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00
URL: http://www.nessus.org/u?c8ae820d

- **Servidor www.inclusion.gob.ec**

Vulnerabilidad: Escáner Nessus SYN
Riesgo: Bajo
Descripción: Tenga en cuenta que los escaneos SYN son menos intrusivos que los escaneos TCP (conexión completa) contra servicios rotos, pero pueden causar problemas para firewalls menos robustos y también dejar conexiones no cerradas en el destino remoto, si la red está cargada.
Código CVE:
Explotado: No
Solución: Protege tu objetivo con un filtro de IP.
Referencias:

Vulnerabilidad: Marcas de tiempo TCP, se detectó que el host implementa RFC1323.
Riesgo: Bajo

Descripción: Un efecto secundario de esta característica es que a veces se puede calcular el tiempo de actividad del host remoto.
Código CVE:
Explotado: Si
Solución: Para deshabilitar las marcas de tiempo TCP en linux, agregue la lìnea 'net.ipv.tcp_timestamps = 0' a /etc/sysctl.conf. Ejecutar 'sysctl -p' para aplicar la configuraciòn en tiempo de ejecuciòn.
Para deshabilitar las marcas de tiempo TCP en Windows ejecute 'netsh int tcp set global timestamps = disabled'.
Referencias:
URL: http://www.ietf.org/rfc/rfc1323.txt

Vulnerabilidad: Traceroute
Riesgo: Bajo
Descripción: Se realizó un traceroute desde el servidor de escaneo al sistema de destino. Este traceroute se proporciona principalmente para el valor informativo solamente. En la gran mayoría de los casos, no representa una vulnerabilidad. Sin embargo, si el traceroute mostrado contiene alguna dirección privada que no debería haber sido visible públicamente, entonces tiene un problema que debe corregir.
Código CVE:
Explotado: No
Solución: Bloquea los paquetes no deseados para que no puedan escapar de tu red.
Referencias:

- **Servidor siimies.inclusion.gob.ec**

Vulnerabilidad: Marcas de tiempo TCP, se detectó que el host implementa RFC1323.
Riesgo: Bajo
Descripción: Un efecto secundario de esta característica es que a veces se puede calcular el tiempo de actividad del host remoto.
Código CVE:
Explotado: Si
Solución: Para deshabilitar las marcas de tiempo TCP en linux, agregue la lìnea 'net.ipv.tcp_timestamps = 0' a /etc/sysctl.conf. Ejecutar 'sysctl -p' para aplicar la configuraciòn en tiempo de ejecuciòn.

Para deshabilitar las marcas de tiempo TCP en Windows ejecute 'netsh int tcp set global timestamps = disabled'.
Referencias:
URL: http://www.ietf.org/rfc/rfc1323.txt

Vulnerabilidad: Nombre de host y Dirección IP inconsistentes
Riesgo: Bajo
Descripción: El nombre de esta máquina no se resuelve o se resuelve en una dirección IP diferente.
Esto puede provenir de un DNS inverso mal configurado, como resultado, las URL en la salida del complemento pueden no ser directamente utilizables en un navegador web y algunas pruebas web pueden estar incompletas.
Código CVE:
Explotado: No
Solución: Arregle el DNS inverso o el archivo host.
Referencias:

Vulnerabilidad: HTTP tipo y versión de servidor.
Riesgo: bajo
Descripción: El tipo de servidor web remoto es apache y la directiva "Server Tokens" es ProductOnly Apache, no permite ocultar el tipo de servidor.
Código CVE:
Explotado: Si.
Solución: Configurar el servidor para usar un nombre alternativo como 'WintendohttpD w/Domatrix display'.
Asegúrese de eliminar los logotipos comunes como apache_pb.gif.
Con Apahe, puede configurar la directiva 'Server Tokens Prod' para limitar la informaciòn que emana del servidor en sus encabezados de respuesta.
Para deshabilitar las marcas de tiempo TCP en Windows ejecute 'netsh int tcp set global timestamps = disabled'.
Referencias:

Vulnerabilidad: Traceroute
Riesgo: Bajo
Descripción: Se realizó un traceroute desde el servidor de escaneo al sistema de destino. Este traceroute se proporciona principalmente para el valor informativo solamente. En la gran mayoría de los casos, no representa una vulnerabilidad.

Sin embargo, si el traceroute mostrado contiene alguna dirección privada que no debería haber sido visible públicamente, entonces tiene un problema que debe corregir.
Código CVE:
Explotado: No
Solución: Bloquea los paquetes no deseados para que no puedan escapar de tu red.
Referencias:

- **Servidor emthsis.inclusion.gob.ec**

Vulnerabilidad: Marcas de tiempo TCP, se detectó que el host implementa RFC1323.
Riesgo: Bajo
Descripción: Un efecto secundario de esta característica es que a veces se puede calcular el tiempo de actividad del host remoto.
Código CVE:
Explotado: Si
Solución: Para deshabilitar las marcas de tiempo TCP en linux, agregue la lìnea 'net.ipv.tcp_timestamps = 0' a /etc/sysctl.conf. Ejecutar 'sysctl -p' para aplicar la configuraciòn en tiempo de ejecuciòn.
Para deshabilitar las marcas de tiempo TCP en Windows ejecute 'netsh int tcp set global timestamps = disabled'.
Referencias:
URL: http://www.ietf.org/rfc/rfc1323.txt

Vulnerabilidad: HTTP tipo y versión de servidor.
Riesgo: bajo
Descripción: El tipo de servidor web es squid/3.1.10.
Código CVE:
Explotado: Si.
Solución: Configurar el servidor para usar un nombre alternativo como 'WintendohttpD w/Domatrix display'.
Asegúrese de eliminar los logotipos comunes como apache_pb.gif.
Con Apahe, puede configurar la directiva 'Server Tokens Prod' para limitar la informaciòn que emana del servidor en sus encabezados de respuesta.
Referencias:

Vulnerabilidad: Traceroute
Riesgo: Bajo
Descripción: Se realizó un traceroute desde el servidor de escaneo al sistema de destino. Este traceroute se proporciona principalmente para el valor informativo solamente. En la gran mayoría de los casos, no representa una vulnerabilidad. Sin embargo, si el traceroute mostrado contiene alguna dirección privada que no debería haber sido visible públicamente, entonces tiene un problema que debe corregir.
Código CVE:
Explotado: No
Solución: Bloquea los paquetes no deseados para que no puedan escapar de tu red.
Referencias:

- **Servidor formacioncontinua.inclusion.gob.ec**

Vulnerabilidad: HTTP tipo y versión de servidor.
Riesgo: bajo
Descripción: El tipo de servidor web es squid/3.1.10.
Código CVE:
Explotado: Si.
Solución: Configurar el servidor para usar un nombre alternativo como 'WintendohttpD w/Domatrix display'.
Asegúrese de eliminar los logotipos comunes como apache_pb.gif.
Con Apahe, puede configurar la directiva 'Server Tokens Prod' para limitar la informaciòn que emana del servidor en sus encabezados de respuesta.
Referencias:

Vulnerabilidad: Marcas de tiempo TCP, se detectó que el host implementa RFC1323.
Riesgo: Bajo
Descripción: Un efecto secundario de esta característica es que a veces se puede calcular el tiempo de actividad del host remoto.
Código CVE:
Explotado: Si

Solución: Para deshabilitar las marcas de tiempo TCP en linux, agregue la lìnea 'net.ipv.tcp_timestamps = 0' a /etc/sysctl.conf. Ejecutar 'sysctl -p' para aplicar la configuraciòn en tiempo de ejecuciòn.
Para deshabilitar las marcas de tiempo TCP en Windows ejecute 'netsh int tcp set global timestamps = disabled'.
Referencias:
URL: http://www.ietf.org/rfc/rfc1323.txt

- **Servidor siimiesalphapruebas.inclusion.gob.ec**

Vulnerabilidad: HTTP tipo y versión de servidor.
Riesgo: bajo
Descripción: El tipo de servidor web es squid/3.1.10.
Código CVE:
Explotado: Si.
Solución: Configurar el servidor para usar un nombre alternativo como 'WintendohttpD w/Domatrix display'.
Asegúrese de eliminar los logotipos comunes como apache_pb.gif.
Con Apahe, puede configurar la directiva 'Server Tokens Prod' para limitar la informaciòn que emana del servidor en sus encabezados de respuesta.
Referencias:

Vulnerabilidad: Marcas de tiempo TCP, se detectó que el host implementa RFC1323.
Riesgo: Bajo
Descripción: Un efecto secundario de esta característica es que a veces se puede calcular el tiempo de actividad del host remoto.
Código CVE:
Explotado: Si
Solución: Para deshabilitar las marcas de tiempo TCP en linux, agregue la lìnea 'net.ipv.tcp_timestamps = 0' a /etc/sysctl.conf. Ejecutar 'sysctl -p' para aplicar la configuraciòn en tiempo de ejecuciòn.
Para deshabilitar las marcas de tiempo TCP en Windows ejecute 'netsh int tcp set global timestamps = disabled'.
Referencias:
URL: http://www.ietf.org/rfc/rfc1323.txt

Vulnerabilidad: Traceroute
Riesgo: Bajo
Descripción: Se realizó un traceroute desde el servidor de escaneo al sistema de destino. Este traceroute se proporciona principalmente para el valor informativo solamente. En la gran mayoría de los casos, no representa una vulnerabilidad. Sin embargo, si el traceroute mostrado contiene alguna dirección privada que no debería haber sido visible públicamente, entonces tiene un problema que debe corregir.
Código CVE:
Explotado: No
Solución: Bloquea los paquetes no deseados para que no puedan escapar de tu red.
Referencias:

4.8.2. Políticas de Contingencia de seguridad informática interna que resguarden los activos informáticos que maneja la institución.

Se tiene como objetivo salvaguardar la Información junto con todos los activos de la Red Informática de la Institución.
Mediante los resultados de las encuestas aplicadas a 22 empleados de la Institución se crean Políticas de Contingencia de Seguridad que ayuden a eliminar o reducir las vulnerabilidades descubiertas en los mismos, siempre y cuando se las ponga en práctica.

Política ante el uso indebido o erróneo de los activos informáticos

Se sugiere que en este punto se debe brindar capacitación a los usuarios sobre el uso adecuado tanto de los activos y de la información de la Institución.

- El departamento de tics debe dar a conocer a los usuarios y empleados la responsabilidad que tienen al manejar activos informáticos.
- Los usuarios deben comprometerse con la Institución, o a su vez firmar un acuerdo de confidencialidad por el uso adecuado de los activos informáticos.
- El departamento de tics tiene la obligación de realizar reuniones, conferencias y/o charlas para dar a conocer cuáles son las nuevas amenazas en lo que se refiere a seguridad de red e informática.

Política ante el uso indebido o erróneo de dispositivos externos

Se sugiere que el Ministerio de Inclusión Económica y Social prohíba, ya sea mediante un dominio o control manual el uso de dispositivo tecnológicos externos ya sean estos como discos duros externos, memort flash, cd, etc.

- Para la utilización de estos dispositivos debe realizarse con previa justificación y autorización de Departamento correspondiente.
- Los usuarios que dispongan bajo su resguardo alguno de estos dispositivos deberá darle un correcto uso.
- El departamento correspondiente debe dar a conocer que estos dispositivos externos que no pertenecen a la institución pueden ser tramitadores de código malicioso como virus, gusanos o caballos de troya.

Política para el tratamiento adecuado de dispositivos

Para esto es necesario establecer y/u obligar el adecuado tratamiento de los dispositivos informáticos por parte de los usuarios.

- En caso de anomalías físicas y a nivel de software, los usuarios deberán notificar de manera urgente al Departamento de Tics.
- Al usuario se le prohíbe reubicar, modificar o alterar los equipos/activos informáticos bajo ningún concepto.
- Dar a conocer a los usuarios que los equipos/activos informáticos son asignados para uso exclusivo de las funciones de la Institución.
- Dar a conocer a los usuarios que los equipos/activos informáticos son asignados para uso exclusivo dentro de la Institución.

Política de asignación y administración de usuarios y contraseñas

- La asignación de usuario y contraseña debe ser realizado de manera individual y confidencial.
- Los empleados deben cambiar su contraseña de manera individual con una longitud de al menos 7 caracteres, donde al menos 3 caracteres deben ser alfanuméricos y al menos 3 deben ser numéricos, de la misma manera combinar letras mayúsculas y minúsculas, por la razón de que entre mas larga y compleja sea la contraseña, mas dificil sera de romperla.

- Se debe prohibir a los empleados que las contraseñas o archivos confidenciales de la Institución se encuentren de forma legible o en lugares donde personas ajenas a la empresa puedan encontrarlos.

Política de seguridad de equipos en la Institución.

Para la protección necesaria de equipos se lo realiza mediante el uso y actualizaciones de un software de Antivirus y antimalware, tambien se sugiere la adquisición de un firewall o cortafuegos, ya sean estos personales o de paga.

- El departamento de tics tiene la obligación de proporcionar una solución de seguridad que integren herramientas como antimalware, antispyware, firewall y prevención de intrusiones.
- Todos los equipos de cómputo deben tener instalado una solución antimalware proporcionada por el Departamento de Tics y con su respectiva licencia.
- Se debe realizar periódicamente un escaneo del equipo y actualizar la base de datos de virus proporcionadas por el fabricante.

Política de uso de software

Indicar al usuario el uso y manejo adecuado de software.

- Se prohíbe la instalación de software de dudosa procedencia, debido a que con la misma abarca riesgos para la Empresa
- A los usuarios no se les permite instalar software que no esté autorizado por la Institución, de ser el caso en que el mismo lo requiera deberá pedir autorización y brindar justificación al Departamento correspondiente.

Política de prevención ante la exploración de la red

Esta se rige a la seguridad en la red informática que es ejecutada por software no autorizado.

- Está prohibido la ejecución de software el cual tenga como propósito analizar o explorar la red informática.
- Se considerará como ataque a la ejecución de cualquier herramienta que ejecute comandos para el análisis de la red informática y explotación de una posible vulnerabilidad.

- También se prohíbe el uso de herramientas de software o hardware que viole la integridad de la seguridad informática.

Política hacia el uso incorrecto del Internet

Se debe controlar y monitorear la navegación en internet por parte de los usuarios.

- El departamento de tics se encargará de monitorear las actividades que los usuarios realizan en internet.
- Crear e implementar reglas de acceso a paginas no autorizadas y que prohíban la descarga de archivos no confiables, los cuales se denominan "proxy webs".
- Se debe dejar en claro al usuario que el uso del internet es para el desempeño del puesto en función más no para propósitos personales.

Política ante software desactualizado en servidores de la Institución.

- El software previamente instalado en el servidor debe ser actualizado constantemente según sean notificadas las actualizaciones de versión o parches de seguridad.
- El departamento de Tics debe mantenerse vigilante en el software de uso diario no solo con el distribuidor oficial sinó también a nivel de foros en los cuales se mencionen fallos o vulnerabilidades.
- Se debe configurar los sistemas de manera que se brinde los servicios y recursos que sean explícitamente necesarios para la utilización de los usuarios.

Política ante configuraciones por defecto en el servidor, de los servicios que utiliza la Institución.

- Se debe eliminar las configuraciones por defecto de los servicios que sean utilizados por varios usuarios.
- La cuenta de administrador se debe proteger mediante la creación y asignación de usuarios y roles.
- Cambiar o eliminar los archivos de configuración por defecto de los servicios que puedan divulgar información mediante mensajes de bienvenida.

- La cuenta de Administrador debe ser usado por el mínimo de personal posible y limitar los intentos de conexión fallidos.

Política frente a pérdida de información

Se sugiere realizar un respaldo o backup de información siguiendo un plan de contingencia.

- Configurar automáticamente una manera periódica y contante de respaldo de la base de datos, en caso de ser posible usar bases de datos distribuidas para evitar la pérdida de información.
- Los archivos de backup se recomienda comprimirlos y resguardarlos en dispositivos externos.

Política frene a ataques a servidores

Implementar un sistema de detección de intrusos (IDS).

- Instalar y configurar una herramienta de seguridad para detección de intrusos, la cual se encargará de monitorizar los eventos que ocurren en un sistema informático en busca de intentos de penetración.
- Crear un o más procedimientos de contingencia ante el riesgo de una actividad sospechosa o peor aún un ataque, que comprometa la confidencialidad, integridad y disponibilidad de la Institución.

CAPÍTULO 5

Conclusiones y Recomendaciones

Las conclusiones y recomendaciones se las realiza en base a los resultados analizados en conformidad a los objetivos de estudio.

5.1. Conclusiones

- El Ministerio de Inclusión Económica y Social de Ambato no ha realizado auditorías de seguridad de red, por lo cual, si nos referimos a detección de vulnerabilidades, no cuentan con herramientas que faciliten el análisis, detección y explotación de vulnerabilidades, con esto puedo concluir que el proyecto es beneficioso mediante la investigación de lo mencionado.

- Las secciones y módulos de la metodología OSSTMM V3 fueron seleccionados de manera acertada, ya que los resultados obtenidos del presente proyecto fueron los esperados, teniendo éxito y llegando a detectar vulnerabilidades existentes en los servidores de la Institución y mediante dichas vulnerabilidades poder recomendar las medidas de seguridad que se deben tomar.

- La explotación de vulnerabilidades detectadas se las realizó en un entorno virtualizado configurado de igual manera que los originales, 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 anteriormente dichas.

- Una vez realizad el análisis metódico de la red, mediante la Metodología OSSTMM V3 y con ayuda de la herramientas Nmap, se observó que hay varios puertos abiertos, los mismos que pueden ser vulnerables a diversos tipos de ataques, y considero que las polìticas de Contingencia de Seguridad de Red deben ser aplicadas para eliminar o en gran parte reducir vulnerabilidades existentes.

- Con la Herramienta Open Vas y Nessus se ha realizado el diagnóstico al sistema de red, se observó que la seguridad es vulnerable a fallos, y considero

que es de mucha importancia que el departamento de Tics del MIES, tenga continuidad en el servicio que día a día prestan a la ciudadanía del cantón.

- El buen ejercicio de una empresa obedece a la eficiencia de su red y sus sistemas informáticos; una empresa puede tener gente de primera, pero si posee una red propensa a fallos, vulnerable e inestable y si no hay un equilibrio entre estas dos cosas, la empresa nunca podrá brindar un servicio de calidad.

5.2. Recomendaciones

- Recomiendo al director del departamento de Tics del Ministerio de Inclusión Económica y Social de Ambato, aplicar y dar un seguimiento correcto a las Políticas de Contingencia de Seguridad de Red previamente realizadas con el objetivo de eliminar o reducir las vulnerabilidades detectadas, garantizando la integridad de la información que se maneja junto con los activos informáticos.

- Se recomienda al director del Departamento de Tics, tomar la metodología OSSTMM V3 como referencia para el análisis de la seguridad, dicha metodología propone un proceso de evaluación de debilidades en varias áreas no solo en la de sistemas, los cuales reflejan niveles de seguridad presentes en la infraestructura a ser auditada, de la misma forma permite valorar riesgos y el impacto que pueden provocar en caso de sufrir un ataque real.

- Se recomienda que el departamento de Tics conjuntamente con la sucursal del MIES en Quito adopten como una buena práctica la planificación e implementación de las Políticas de Contingenica de Seguridad de Red, de esta manera se podrá asegurar que los objetivos relacionados a la seguridad de red se estén cumpliendo.

- Las pruebas de vulnerabilidades se las realizó en un entorno virtualizado; recomiendo realizar las mismas pruebas en los servidores reales ya que las pruebas en los servidores reales tendrián mejor impacto.

Bibliografia

[1] M. Pilamunga, "Procedimiento de Auditoría para la Seguridad de las Redes LAN en los Laboratorios de Computadoras de la Escuela de Ciencias de la Facultad de Ingeniería Ciencias Físicas Y Matemática de la Universidad Central Del Ecuador," Master's thesis, UNIVERSIDAD CENTRAL DEL ECUADOR, 2016.

[2] M. n. Mendoza, "Conoce los tipos de auditorías de redes y qué puede revisar cada una." url: https://www.welivesecurity.com/la-es/2015/04/20/auditorias-de-redes/, Apr. 2015.

[3] MIES, "Ministerio de Inclusion Económica y Social." url: http://www.inclusion.gob.ec, 2019.

[4] P. Herzog, "The Open Source Security Testing Methology Manual." url: http://www.isecom.org/mirror/OSSTMM.3.pdf, 2015.

[5] D. D. J. E. A. Maya, "Auditoría de seguridad informática para el Gobierno Autónomo Descentralizado de Santa Ana de Cotacachi, basada en las normas NTP ISO/IEC 17799:2007 y la metodología OSSTMM v2.," *Repositorio Digital Universidad Técnica del Norte*, 2015.

[6] R. L. Santoyo, "Propuesta de implementación de una metodología de auditoría de seguridad informática." url: https://repositorio.uam.es/handle/10486/668900, June 2015.

[7] D. D. Jaramillo, ""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.," Master's thesis, UNIVERSIDAD TÉCNICA DEL NORTE, 2015.

[8] M. E. Raffino, "Concepto de Seguridad." url: https://concepto.de/seguridad/, Feb. 2019.

[9] M. M. J. Pérez, "Definición de seguridad Informática." url: https://definicion.de/seguridad-informatica/, 2018.

[10] C. Case, "Una Auditoría." url: https://www.controlcase.com/solutions/one-audit/, 2017.

[11] wizlynx, "Evaluaciones y Auditorías de Seguridad." url: https://www.wizlynxgroup.com/mx/ciberseguridad-mexico/pentest-y-hacking-etico, 2017.

[12] ALEGSA, "Definición de Hacking." url: http://www.alegsa.com.ar/Dic/hacking.php, 2016.

[13] SOLUTECSA, "Hacking ético." url: http://www.internetglosario.com/1131/hackingetico.h June 2017.

[14] A. G. J. Pérez, "Definición de Auditoría." url: https://definicion.de/auditoria/, 2015.

[15] ISecAuditors, "Auditoría de Red Interna." url: https://www.isecauditors.com/auditoria-de-red-interna, 2019.

[16] J. Navarro, "Definición de Metodología." url: https://www.definicionabc.com/ciencia/metodologia.php, 2017.

[17] "Kali linux." url: https://www.kali.org/, 2015.

[18] A. Azamar, "Maltego." url: https://securityassessmentsblog.wordpress.com/2017/11/14/m Nov. 2017.

[19] G. Inc, "Ayuda google." url: https://support.google.com/vault/answer/2474474?hl=es, 2015.

[20] A. Chema, "FOCA Open Source." url: http://www.elladodelmal.com/2017/10/foca-open-source.html, Oct. 2017.

[21] S. J. Bosco, "RED Y TRANSMISIÓN DE DATOS VisualRoute," *Universidad Nacional de la Patagonia*, 2016.

[22] L. Zuno, "theharvester information gathering." url: https://code.google.com/p/theharvester/.

[23] G. Lyon, "Guía de referencia de nmap." url: https://nmap.org/man/es/.

[24] R. Velasco, "HPING3: MANUAL DE UTILIZACIÓN DE ESTA HERRAMIENTA PARA MANIPULAR PAQUETES TCP/IP." url: https://www.redeszone.net/gnu-linux/hping3-manual-de-utilizacion-de-esta-herramienta-para-manipular-paquetes-tcp-ip/, Feb. 2015.

[25] Greenbone, “El escáner de vulnerabilidades más avanzado del mundo open source.” url: http://www.openvas.org/about.html, 2019.

[26] Tenable, “Guía de instalación y configuracion de nessus 6.8.” url: https://docs.tenable.com/nessus/6_8/*Content/GettingStarted.htm*, *Oct.*2018.

[27] H. Rizaldos, “Qué es Metasploit framework.” url: https://openwebinars.net/blog/que-es-metasploit/, Oct. 2018.

[28] G. Lyon, “The hydra.” url: http://sectools.org/tool/hydra, 2015.

[29] M. V. A. Ornaghi, “Ettercap,” 2017.

[30] G. N. ”Purdy, *Linux iptables Pocket Reference: Firewalls, NAT & Accounting*. O’Reilly Media, Inc., 2017.

[31] J. .[El]ks, *Man in the middle attack: Focus on sslstrip*. GRIN Verlag, 2017.

[32] “¿Qué es el nic?.” url: http://web.uservers.net/ayuda/soluciones/dominios, 2017.

[33] Microsoft, “Una vulnerabilidad en SMB podría permitir la ejecución remota de código.” url: https://support.microsoft.com/es-us/help/957097/ms08-068-vulnerability-in-smb-could-allow-remote-code-execution, Apr. 2018.

[34] A. Ruiz, “Vulnerabilidad en Remote Desktop Protocol (RDP).” url: http://www.vsantivirus.com/vul-windows-rdp-160705.htm, July 2015.

[35] A. Biznya, “GENE6 G6 FTP SERVER 3.1.0 DESBORDAMIENTO DE BÚFER,” *vuldb.com*, 2016.

[36] D. J. A. ”M. E. Cueva, “Análisis de Certificados SSL/TLS gratuitos y su implementación como Mecanismo de seguridad en Servidores de Aplicación.,” *Universidad Nacional de Loja*, Feb. 2017.

[37] “SQUID PROXY HASTA 2.5.STABLE7 CACHE VULNERABILIDAD DESCONOCIDA.” url: https://vuldb.com/es/?id.23915, Sept. 2018.

Anexos y Apéndices

Anexo A

Aprobación para realizar el proyecto de Investigación

MINISTERIO DE INCLUSIÓN ECONÓMICA Y SOCIAL

MINISTERIO DE INCLUSIÓN ECONÓMICA Y SOCIAL

Oficio Nro. MIES-CZ-3-2018-0073-OF

Ambato, 11 de mayo de 2018

Asunto: Autorización para que el Sr. Paúl Miranda realice Trabajo de Investigación.

Magister
Julio Enrique Cuji Rodriguez
PRESIDENTE, UNIDAD DE TITULACIÓN CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS, UNIVERSIDAD TÉCNICA DE AMBATO.
En su Despacho

De mi consideración:

Reciba un cordial saludo de la Coordinación Zonal 3 del Ministerio de Inclusión Económica y Social, a la vez deseándole éxitos en sus funciones diarias.

En mi calidad de Coordinador Zonal 3 del Ministerio de Inclusión Económica y Social y en respuesta a Oficio FISEI-UT-PROY-INV-COORD-SIS-004 me permito manifestar a Usted, que el Sr. Christian Paúl Miranda Silva, portador (a) de la cédula de ciudanía N° 1804348652, estudiante de Décimo nivel en el período académico Marzo – Agosto 2018 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 tiene la autorización y respaldo para desarrollar en la institución a la que represento su Trabajo de Investigación, para lo cual designo como Tutor Institucional al Ing. Héctor Vladimir Robayo Villarroel , Analista TIC´s Zonal.

Con estos antecedentes informo que la realización de este Trabajo de Investigación es de gran importancia para esta dependencia ministerial, el estudiante tiene total apoyo para su desarrollo y ejecución.

Con sentimientos de distinguida consideración.

Atentamente,

Documento firmado electrónicamente

Mgs. Francisco German Escobar Montenegro
COORDINADOR ZONAL 3

Referencias:
- MIES-CZ-3-2018-0153-EXT

Anexo B

Certificado de culminación del Proyecto de Investigación

MINISTERIO DE INCLUSIÓN ECONÓMICA Y SOCIAL

Oficio Nro. MIES-CZ-3-2019-0160-OF

Ambato, 20 de junio de 2019

Asunto: Culminación Proyecto De Investigación: "Auditoría de Redes, Aplicando la Metodología Osstmm V3, para el Ministerio de Inclusión Económica Y Social"

Señora Magíster
Elsa Pilar Urrutia Urrutia , DECANA DE LA FACULTAD DE TECNOLOGIAS DE LA INFORMACIÓN, TELECOMUNICACIONES E INDUSTRIAL
UNIVERSIDAD TÉCNICA DE AMBATO
En su Despacho

De mi consideración:

Reciba un cordial saludo desde la Coordinación Zonal 3 y deseándole éxitos en sus funciones diarias.

Por medio de la presente me permito informar que el Sr. Miranda Silva Christian Paul Con C.I 1804348652 estudiante de la carrera de Ingeniería en Sistemas Computacionales e Informáticos de la Facultad De Tecnologías de la Información, Telecomunicaciones e Industrial, que una vez que la responsable de la Unidad de Tecnologías de esta Coordinación Zonal ha revisado el Proyecto De Investigación denominado: "Auditoría de Redes, Aplicando la Metodología Osstmm V3, para el Ministerio de Inclusión Económica Y Social" donde se encontró que el estudiante culminó su trabajo; mismo que se basa en el funcionamiento y parámetros establecidos en la red interna del mies coordinación zonal 3.

Con sentimientos de distinguida consideración.

Atentamente,

Ministerio de Inclusión Económica y Social Coordinación Zonal 3
MIES
COORDINADOR ZONAL

Documento firmado electrónicamente

Mgs. Francisco German Escobar Montenegro
COORDINADOR ZONAL 3

Referencias:
- MIES-CZ-3-DDA-2019-2320-M

*Documento firmado electrónicamente por Quipux

Anexo C

Reporte de escaneo con Nessus

miess scann

Report generated by Nessus™ Mon, 08 Apr 2019 11:59:05 GMT-0500

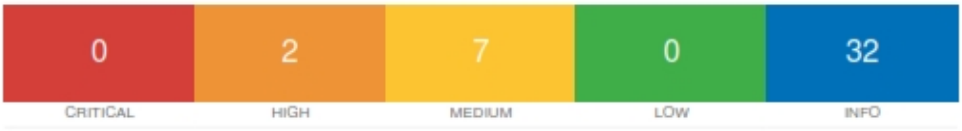
TABLE OF CONTENTS

Hosts Executive Summary

- 186.42.188.178 4
- 186.46.86.228 6
- 186.46.86.230 7
- 190.152.52.202 8
- 190.152.215.89 9
- 190.152.215.90 10
- 190.152.215.92 11
- 190.152.215.94 13

Hosts Executive Summary

186.42.188.178

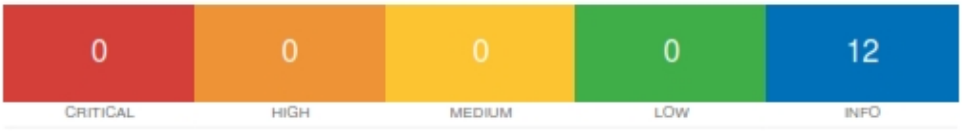


Vulnerabilities Total: 41

SEVERITY	CVSS	PLUGIN	NAME
HIGH	9.3	119766	PHP 7.2.x < 7.2.13 Multiple vulnerabilities
HIGH	7.5	121353	PHP 7.2.x < 7.2.14 Multiple vulnerabilities.
MEDIUM	6.9	123642	Apache 2.4.x < 2.4.39 Multiple Vulnerabilities
MEDIUM	6.8	123754	PHP 7.2.x < 7.2.17 Multiple vulnerabilities.
MEDIUM	5.0	111788	Apache 2.4.x < 2.4.34 Multiple Vulnerabilities
MEDIUM	5.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	4.3	117807	Apache 2.4.x < 2.4.35 DoS
MEDIUM	4.3	121355	Apache 2.4.x < 2.4.38 Multiple Vulnerabilities
MEDIUM	4.3	117500	PHP 7.2.x < 7.2.10 Transfer-Encoding Parameter XSS Vulnerability
INFO	N/A	48204	Apache HTTP Server Version
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	42823	Non-compliant Strict Transport Security (STS)
INFO	N/A	50350	OS Identification Failed
INFO	N/A	50845	OpenSSL Detection

INFO	N/A	48243	PHP Version Detection
INFO	N/A	66334	Patch Report
INFO	N/A	10263	SMTP Server Detection
INFO	N/A	42088	SMTP Service STARTTLS Command Support
INFO	N/A	56984	SSL / TLS Versions Supported
INFO	N/A	56472	SSL Certificate Chain Contains Unnecessary Certificates
INFO	N/A	56471	SSL Certificate Chain Not Sorted
INFO	N/A	10863	SSL Certificate Information
INFO	N/A	95631	SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)
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	42822	Strict Transport Security (STS) Detection
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	104743	TLS Version 1.0 Protocol Detection
INFO	N/A	121010	TLS Version 1.1 Protocol Detection
INFO	N/A	10287	Traceroute Information
INFO	N/A	10386	Web Server No 404 Error Code Check
INFO	N/A	15588	Web Server SSL Port HTTP Traffic Detection

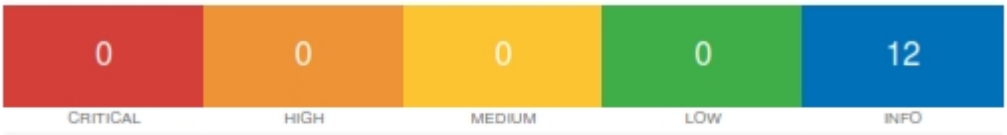
186.46.86.228



Vulnerabilities Total: 12

SEVERITY	CVSS	PLUGIN	NAME
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	54615	Device Type
INFO	N/A	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	46215	Inconsistent Hostname and IP Address
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	11936	OS Identification
INFO	N/A	22964	Service Detection
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	10287	Traceroute Information
INFO	N/A	10386	Web Server No 404 Error Code Check

186.46.86.230



Vulnerabilities Total: 12

SEVERITY	CVSS	PLUGIN	NAME
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	54615	Device Type
INFO	N/A	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	46215	Inconsistent Hostname and IP Address
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	11936	OS Identification
INFO	N/A	22964	Service Detection
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	10287	Traceroute Information
INFO	N/A	10386	Web Server No 404 Error Code Check

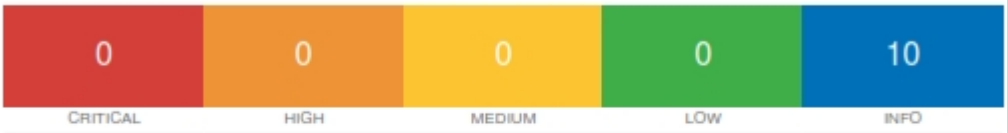
190.152.52.202

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	0	0	13

Vulnerabilities Total: 13

SEVERITY	CVSS	PLUGIN	NAME
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	54615	Device Type
INFO	N/A	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	46215	Inconsistent Hostname and IP Address
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	11936	OS Identification
INFO	N/A	22964	Service Detection
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	10287	Traceroute Information
INFO	N/A	10386	Web Server No 404 Error Code Check

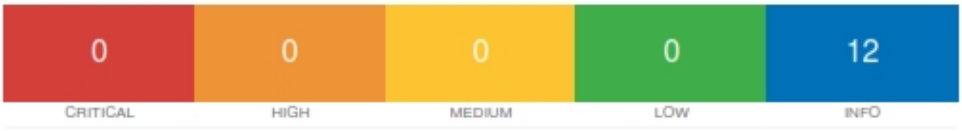
190.152.215.89



Vulnerabilities Total: 10

SEVERITY	CVSS	PLUGIN	NAME
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	54615	Device Type
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	11936	OS Identification
INFO	N/A	22964	Service Detection
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	10287	Traceroute Information
INFO	N/A	10386	Web Server No 404 Error Code Check

190.152.215.90



Vulnerabilities Total: 12

SEVERITY	CVSS	PLUGIN	NAME
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	54615	Device Type
INFO	N/A	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	46215	Inconsistent Hostname and IP Address
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	11936	OS Identification
INFO	N/A	22964	Service Detection
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	10287	Traceroute Information
INFO	N/A	10386	Web Server No 404 Error Code Check

190.152.215.92

Vulnerabilities Total: 21

SEVERITY	CVSS	PLUGIN	NAME
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
LOW	2.6	83875	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
INFO	N/A	46180	Additional DNS Hostnames
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	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	56984	SSL / TLS Versions Supported
INFO	N/A	10863	SSL Certificate Information
INFO	N/A	95631	SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)
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	104743	TLS Version 1.0 Protocol Detection
INFO	N/A	121010	TLS Version 1.1 Protocol Detection

INFO	N/A	10287	Traceroute Information
INFO	N/A	10386	Web Server No 404 Error Code Check

190.152.215.94

Vulnerabilities Total: 21

SEVERITY	CVSS	PLUGIN	NAME
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	5.0	15901	SSL Certificate Expiry
INFO	N/A	12053	Host Fully Qualified Domain Name (FQDN) Resolution
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	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	50845	OpenSSL Detection
INFO	N/A	56984	SSL / TLS Versions Supported
INFO	N/A	45410	SSL Certificate 'commonName' Mismatch
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	22964	Service Detection
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	104743	TLS Version 1.0 Protocol Detection
INFO	N/A	121010	TLS Version 1.1 Protocol Detection

INFO	N/A	10287	Traceroute Information
INFO	N/A	10386	Web Server No 404 Error Code Check