UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS

Tema:

AUDITORÍA DE LA SEGURIDAD INFORMÁTICA PARA EL HONORABLE GOBIERNO PROVINCIAL DE TUNGURAHUA MEDIANTE LA METODOLOGÍA OPEN SOURCE SECURITY TESTING METHODOLOGY MANUAL.

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

SUBLÍNEA DE INVESTIGACIÓN: Seguridad Informática

AUTOR: Nuela Guananga Byron Danilo
TUTOR: Ing. Mg. David Omar Guevara Aulestia

Ambato - Ecuador
Octubre 2015

APROBACIÓN DEL TUTOR

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

"AUDITORÍA DE LA SEGURIDAD INFORMÁTICA PARA EL HONORABLE GOBIERNO PROVINCIAL DE TUNGURAHUA MEDIANTE LA METODOLOGÍA OPEN SOURCE SECURITY TESTING METHODOLOGY MANUAL", del señor, Byron Danilo Nuela Guananga, estudiante de la Carrera de Ingeniería en Sistemas Computacionales e Informáticos, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, considero que el informe investigativo reúne los requisitos suficientes para que continúe con los trámites y consiguiente aprobación de conformidad con el numeral 7.2 de los Lineamientos Generales para la aplicación de Instructivos de las Modalidades de Titulación de las Facultades de la Universidad Técnica de Ambato.

Ambato, octubre de 2015

EL TUTOR

Ing. Mg. David Omar Guevara Aulestia

AUTORÍA

El presente trabajo de investigación titulado: **AUDITORÍA DE LA SEGURIDAD INFORMÁTICA PARA EL HONORABLE GOBIERNO PROVINCIAL DE TUNGURAHUA MEDIANTE LA METODOLOGÍA OPEN SOURCE SECURITY TESTING METHODOLOGY MANUAL**. 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, octubre de 2015

Byron Danilo Nuela Guananga

CC:

DERECHOS DE AUTOR

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

Cedo los derechos de mi Trabajo de Titulación, con fines de difusión pública, además autorizo su reproducción dentro de las regulaciones de la Universidad.

Ambato, octubre de 2015

Byron Danilo Nuela Guananga

CC:

APROBACIÓN COMISIÓN CALIFICADORES

La Comisión Calificadora del presente trabajo conformada por los señores docentesIng. Hernando Buenaño, Ing. Galo López, revisó y aprobó el Informe Final del Proyecto de Investigación titulado **"AUDITORÍA DE LA SEGURIDAD INFORMÁTICA PARA EL HONORABLE GOBIERNO PROVINCIAL DE TUNGURAHUA MEDIANTE LA METODOLOGÍA OPEN SOURCE SECURITY TESTING METHODOLOGY MANUAL"**, presentado por el señor Nuela Guananga Byron Danilo de acuerdo al numeral 9.1 de los Lineamientos Generales para la aplicación de Instructivos de las Modalidades de Titulación de las Facultades de la Universidad Técnica de Ambato.

Ing. Vicente Morales, Mg.
PRESIDENTE DEL TRIBUNAL

Ing. Hernando Buenaño, Mg.
DOCENTE CALIFICADOR

Ing. Galo López, Mg.
DOCENTE CALIFICADOR

DEDICATORIA

El proyecto está dedicado a mis padres Mariana y Oswaldo, a mis hermanos Edisson, Janeth y Patricia, a mi abuelita Teresa, que me han apoyado en todo momento cuanto han podido.

A mi hija Carol Denisse por quien cada día tiene sentido, luz de mi vida, origen de mis desvelos, mis preocupaciones y mis ganas de ser mejor persona, por prestarme el tiempo que le pertenece le dedico la culminación del presente proyecto, te amo.

A mis tíos y todos mis familiares quienes siempre han sabido apoyarme de una u otra manera.

A todas aquellas personas que colaboraron en mi vida estudiantil mediante enseñanzas, apoyo y palabras de aliento.

Danilo Nuela Guananga

AGRADECIMIENTO

Agradezco a mis padres por darme la vida, a toda mi familia porque gracias a ellos pude crecer como persona.

Agradezco a cada uno de los Docentes de la Facultad por compartir sus conocimientos, experiencias, tiempo y dedicación con todos los estudiantes.

Agradezco a la Universidad por abrirme sus puertas y aparte de capacitarme en una carrera profesional también me enseñó a ser una persona más humana.

Danilo Nuela Guananga

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN EJECUTIVO

El presente proyecto está dirigido a la Auditoría de Seguridad Informática en el Honorable Gobierno Provincial de Tungurahua mediante la metodología Open Source Security Testing Methodology Manual (OSSTMM) para el análisis, detección y explotación de vulnerabilidades mediante herramientas de seguridad informática.

OSSTMM presenta una planificación de ejecución y verificación de la seguridad en entornos informáticos, 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 la Información y los módulos: Revisión de la Inteligencia Competitiva, Revisión de la Privacidad y Recolección de Documentos, Sección Seguridad de las Tecnologías de Internet 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 Informática se refiere.

ABSTRACT

This project is aimed at Information Security Auditing on Tungurahua Provincial Government Honorable by Open Source Security Testing Methodology Manual (OSSTMM) for analysis, detection and exploitation of vulnerabilities by computer security tools.

OSSTMM presents a planning implementation and verification of security in computing environments, Each section includes modules that help in the development of safety analysis, taking the Section Information Security and modules: Competitive Intelligence Review, Privacy Review and Document Grinding, Sections Internet Technology Security and modules: Network Surveying, System Services Identification and Vulnerability Research and Verification.
The two sections are focused on the expected results allow to assess the level of safety in the institution and then propose changes or security measures including improving the current situation as far as IT security is concerned.

INTRODUCCIÓN

El presente proyecto de investigación tiene como finalidad el análisis, detección y explotación de vulnerabilidades mediante herramientas de Seguridad Informática guiados por la metodología OSSTMM y sus secciones Seguridad de la Información y Seguridad en las Tecnologías de Internet junto con varios de sus módulos, estas secciones son tomadas de acuerdo a los resultados esperados.

Capítulo 1, "El Problema", se describe el problema, la contextualización 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 alcanzarán con la presente investigación.

Capítulo 2, "Marco Teórico", se presenta los antecedentes investigativos sobre los cuales se desarrolla la propuesta, se presenta la fundamentación teórica que guía en la búsqueda de una solución al problema planteado.

Capítulo 3, "Metodología", se describe la modalidad de la investigación a utilizar, como se realizará la recolección y procesamiento de la información para su análisis y, las actividades a seguir para el desarrollo de los objetivos del proyecto.

Capítulo 4, "Desarrollo de la Propuesta", se describe el desarrollo del proyecto mediante las actividades realizadas para el cumplimiento de cada uno de los objetivos específicos.

Capítulo 5, "Conclusiones y Recomendaciones", se describe las conclusiones y recomendaciones finales en base a los resultados obtenidos de la aplicación del proyecto de investigación.

CAPÍTULO 1

El problema

1.1. Tema de Investigación

Auditoría de la Seguridad Informática para el Honorable Gobierno Provincial de Tungurahua mediante la Metodología Open Source Security Testing Methodology Manual.

1.2. Planteamiento del problema

La firma de seguridad cibernética Kaspersky, publicó en febrero 2015 un informe alarmante de una operación mundial que se infiltró en bancos de Rusia, instituciones financieras de Estados Unidos, Alemania, China y Ucrania, cientos de millones de dólares fueron robados de 100 bancos en 30 países. La firma se negó a nombrar bancos específicos por respeto a los contratos de confidencialidad con sus clientes. Los hackers utilizaron ejércitos de computadoras que diseminan spam, para enviar una oleada de correos electrónicos infectados con malware, los empleados bancarios que abrieron estos emails sin querer permitieron que los piratas informáticos se colaran en sus computadoras. Desde ahí tomaron el control completo de los sistemas con las credenciales de los empleados. Con el acceso los hackers abrieron cuentas en diferentes lugares y movieron dinero a su voluntad. Kaspersky señala que, en algunos casos, utilizaron la red interbancaria SWIFT (Society for Worldwide Interbank Financial Telecommunication) para transferir los fondos de un lugar a otro.
Christopher Doggett, director general de Kaspersky, comenta que un banco pudo haber evitado ser atacado de una manera particular si sus empleados hubieran aplicado la actualización habitual de Microsoft[1].

“En el año 2011 la red de piratas informáticos o hackers Anonymous amenazó con realizar ataques al gobierno del Ecuador por el supuesto acoso de este a los medios de comunicación y las limitaciones a la libertad de expresión, destacando la demanda al diario El Universo y a varios periodistas y directivos de medios de comunicación; también rechaza la incautación de varios medios de comunicación privados y el uso de estos con fines políticos” [2].
Según el Diario El Telégrafo en agosto 2011, “Los hackers que se identifican como Anonymous Iberoamérica han publicado información de la Corporación Nacional de Telecomunicaciones (CNT), de varios trabajadores del Aeropuerto de Quito, La página web de la empresa Hunter para Ecuador (http://www.hunter.com.ec) mostraba en su página principal una imagen de personas enmascaradas en un metro y con la leyenda "Somos Anonymous", se publicaron varios links que supuestamente llevarían al panel de control del sistema de videoconferencia del Ministerio de Medio Ambiente”[3].

El Honorable Gobierno Provincial de Tungurahua tiene como misión “impulsar las iniciativas de desarrollo económico, social, ambiental y territorial de Tungurahua, bajo los principios de participación, mancomunidad, equidad, ética, efectividad y transparencia”, ha sufrido ataques a varias páginas web de las que administra como son “El Parque de la Familia”, “Agenda de Productividad y Competitividad”, “Recursos Agropecuarios” las cuales están desarrolladas en Joomla CMS, junto con el acceso de personal no autorizado al servidor Proxy [4].

1.3. Delimitación

1.3.1. Delimitación de Contenidos:

- **Área Académica:** Hardware y Redes.
- **Línea de Investigación:** Sistemas Administradores de Recursos.
- **Sublínea de Investigación:** Seguridad Informática.

1.3.2. Delimitación espacial

El presente trabajo se va a realizar en el Honorable Gobierno Provincial de Tungurahua, ubicado en la Provincia de Tungurahua, Cantón Ambato.

1.3.3. Delimitación temporal

La presente investigación se desarrollará en 6 meses posteriores a la aprobación del proyecto por parte del H. Concejo Directivo de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

1.4. Justificación

El presente proyecto es importante debido a que la institución necesita una evaluación de la seguridad actual, de tal manera que se detecten vulnerabilidades que puedan ser explotadas por atacantes informáticos y corregirlas o reducirlas, para proteger la integridad tanto de la información como de los dispositivos conectados a la red.

La Auditoría de la Seguridad Informática sería de gran beneficio al Honorable Gobierno Provincial de Tungurahua, por que proporcionaría las recomendaciones para dar solución a las vulnerabilidades detectadas, junto con la elaboración de Políticas de Contingencia de Seguridad Informática que eviten contratiempos en el desempeño de los empleados, administrativos y contribuyentes, protegiendo los activos informáticos de debilidades, asegurando la integridad, confidencialidad y disponibilidad de la información.

El impacto sería positivo porque se podría determinar las amenazas y vulnerabilidades a los que está expuesto la institución, para que sean analizadas y tratar de explotarlas, confirmando su existencia y el impacto real que podría tener en la institución si éstas no son corregidas o reducidas.

La presente investigación es factible porque el Honorable Gobierno Provincial de Tungurahua aprobó el proyecto propuesto y se cuenta con la colaboración de la Dirección de Sistemas, de su Director y personal.

1.5. Objetivos

1.5.1. General

Implementar una Auditoría de la Seguridad Informática para el Honorable Gobierno Provincial de Tungurahua mediante la Metodología Open Source Security Testing Methodology Manual OSSTMM.

1.5.2. Específicos

- 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.
- Identificar las vulnerabilidades de los servidores de la red informática que puedan ser explotadas por intrusos malintencionados.
- Establecer un escenario para simular un ataque programado a los servidores de la red informática para explotar las vulnerabilidades que puedan ser utilizadas por intrusos malintencionados.
- Elaborar 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

En la Universidad Politécnica de Valencia, Alberto Hervalejo Sánchez en su proyecto "Auditorías de Seguridad Informática y la OSSTMM" en el año 2009. Menciona, "Nunca se puede saber y realizar todo lo que uno quiere, y la seguridad informáticas un claro ejemplo, donde además, siempre interviene otra parte (ya sea atacante o defensora).Siempre habrá alguien más listo y que sabrá más, y cada día, encontraremos nuevas herramientas que vulneran nuevos fallos. Aparecerán nuevas técnicas, que con el avance de la tecnología, harán a los sistemas más vulnerables". El proyecto realizado se centra en La Auditoría de Seguridad Informática (en especial, vulnerabilidades y test de intrusión), tomando como referencia, la metodología descrita por el Instituto para la Seguridad y Metodologías Abiertas (Institute for Security and Open Methodologies-ISECOM), la Open Source Security Testing Methodology Manual (OSSTMM). Teniendo en cuenta, que ésta es, quizás la metodología más extendida en el campo y ofrece métodos científicos a los tests de seguridad, pero además, ofrece una guía a los auditores para realizar una auditoría OSSTMM certificada" [5].

En la Escuela Politécnica del Litoral, Gabriela Hernández en su proyecto "Diseño de un Plan Estratégico de Seguridad de Información en una Empresa del Sector Comercial" en el año 2006. Plantea un diseño de un Plan de Seguridad Informática para ayudar a las organizaciones comerciales a tener una concienciación permanente de mantener seguros sus activos, teniendo en cuenta que la palabra activo son todos los recursos informáticos para que la organización funcione correctamente y alcance los objetivos propuestos[2].

Recomienda definir políticas de seguridad claras no solo por los riesgos derivados de los equipos de computación o de los servicios que brinda el área de sistemas, sino también por las pérdidas de productividad que puede generar un incidente de seguridad. Recomienda que toda empresa deba utilizar un esquema de seguridad basadas en estándares y/o normas referentes a la tecnología y proporcionando los recursos necesarios para mantener la seguridad informática[2].

En la Universidad Politécnica Salesiana, Fabricio Zavala en su proyecto "Diseño e Implementación de Seguridades en la Red de Datos de la Planta Central del Ministerio de Educación y Cultura del Ecuador, aplicando la tecnología OSSTMM" en el año 2010 recomienda que, para mantener un nivel alto de seguridad hay que estar constantemente investigando nuevas herramientas de seguridad y analizar los resultados, además un elemento fundamental son las políticas de seguridad planteadas, las mismas que se deben cumplir a cabalidad sin excepción alguna ya que solo basta uno que no cumpla para que la seguridad quede vulnerada. Las conexiones remotas no deben realizarse como administradores deben realizarse como usuarios de conexión y una vez ingresado darse privilegios [6].

En la Universidad Técnica de Ambato, Gloria Huilca en su proyecto "Hacking Ético para detectar vulnerabilidades en los servicios de la intranet del Gobierno Autónomo Descentralizado Municipal del Cantón Cevallos" en el año 2012. Menciona que, el objetivo principal de la aplicación de hacking ético es descubrir las deficiencias relativas a seguridad y las vulnerabilidades de los sistemas informáticos, analizarlas, calibrar su grado de riesgo y peligrosidad, y recomendar las posibles soluciones más apropiadas para cada una de ellas. Recomienda considerar la importancia y sensibilidad de la información y servicios críticos de la intranet por lo que es necesario establecer políticas de seguridad dentro de la institución [7].

2.2. Fundamentación teórica

Seguridad

Protección de los bienes personales y del negocio, a través del uso de controles de seguridad que restringen y gestionan el movimiento de personas y equipos[8].

Seguridad Informática
Es un conjunto de métodos, procedimientos, formas y estándares que permiten asegurar la información y las unidades tecnológicas e informáticas de la empresa u organización[9].

Escáner de Vulnerabilidades
Herramientas de análisis para los equipos de toda la red. Determinan servicios que se están ejecutando en un equipo remoto[9].

Pruebas de Penetración (PenTest)
Conjunto de técnicas y metodologías llevadas a cabo para determinar el nivel de seguridad de un sistema, tiene como objetivo detectar vulnerabilidades y obtener posibles soluciones mediante el uso de "hacking ético"[10].

Hacking
Persona llena de conocimiento capaz de comprometer a un sistema, robar información o borrar sus datos de un sitio web u organización[9].

Hacking Ético
Disciplina la cual está orientada a la búsqueda de vulnerabilidades ya sea en la red y las aplicaciones para usarlas a beneficio de la misma empresa[9].

Auditoría
Es la revisión independiente de alguna o algunas actividades, funciones específicas, resultados u operaciones de una entidad administrativa, realizada por un profesional de la auditoría, con el propósito de evaluar su correcta realización y, con base en ese análisis, poder emitir una opinión autorizada sobre la razonabilidad de sus resultados y el cumplimiento de sus operaciones[11].

Auditoría de Seguridad
Su función inicial es estrictamente económico-financiera y busca optimizar los recursos de todo el componente informático de la organización. La auditoría contiene elementos de análisis, de verificación y de exposición de debilidades y disfunciones. Aunque pueden aparecer sugerencias y planes de acción para eliminar las disfunciones y debilidades antedichas; estas sugerencias plasmadas en el Informe final reciben

el nombre de recomendaciones[12].

Auditoría Informática
Es la revisión técnica, especializada y exhaustiva que se realiza a los sistemas computacionales, software e información utilizados en una empresa, sean individuales, compartidos y/o de redes, así como a sus instalaciones, telecomunicaciones, mobiliario, equipos periféricos y demás componentes. Dicha revisión se realiza de igual manera a la gestión informática, el aprovechamiento de sus recursos, las medidas de seguridad y los bienes de consumo necesarios para el funcionamiento del centro de cómputo. El propósito fundamental es elevar el uso adecuado de los sistemas para el correcto ingreso de los datos, el procesamiento adecuado de la información y la emisión oportuna de sus resultados en la institución, incluyendo la evaluación en el cumplimiento de las funciones, actividades y operaciones de funcionarios, empleados y usuarios involucrados con los servicios que proporcionan los sistemas computacionales a la empresa[11].

Auditoría de Seguridad Informática
La auditoría de seguridad informática analiza los procesos relacionados únicamente con la seguridad, ésta puede ser física, lógica y locativa pero siempre orientada a la protección de la información. Es este el punto de mayor diferencia, la seguridad informática se preocupa por la integridad y disponibilidad de la información mientras la auditoría de sistemas incluye otras características más administrativas[12].

Una auditoría de seguridad informática es una evaluación de los sistemas informáticos cuyo fin es detectar errores y fallas y que mediante un informe detallado entregamos al responsable en el que se describe:

- Equipos instalados, servidores, programas, sistemas operativos...
- Procedimientos instalados
- Análisis de Seguridad en los equipos y en la red
- Análisis de la eficiencia de los Sistemas y Programas informáticos
- Vulnerabilidades que pudieran presentarse en una revisión de las estaciones de trabajo, redes de comunicaciones, servidores[13].

Contingencia
La contingencia es el modo de ser de lo que puede suceder o no, especialmente de un problema que se plantea de forma imprevista[14].

Plan de Contingencia
Un plan de contingencias es un instrumento de gestión inmediata de las Tecnologías de la Información y las Comunicaciones en relación al soporte y el desempeño[15].

Metodología
Es un conjunto de procedimientos racionales utilizados para alcanzar una gama de objetivos que rigen una investigación científica, una exposición doctrinal o tareas que requieran habilidades, conocimientos o cuidados específicos[16].

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 (ver figura 2.1), formada por 6 ítems los cuales comprenden todo el sistema actual, estos ítems son [17]:

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

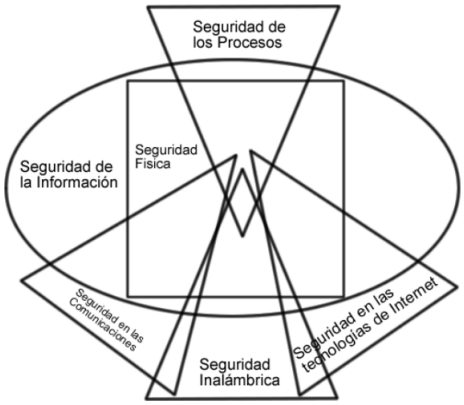

Figura 2.1: Mapa de seguridad OSSTMM

Fuente: Metodología OSSTMM

2.3. Propuesta de Solución

La Auditoría de la Seguridad Informática en el Honorable Gobierno Provincial de Tungurahua, mediante la metodología Open Source Security Testing Methodology Manual, 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

El tipo de investigación del presente proyecto es Investigación y Desarrollo (I + D), se investigará el estado de la Institución y desarrollará mejoras en los procesos actuales con respecto a los recursos tecnológicos.

Modalidad Bibliográfica
Se investigan libros, manuales, artículos, revistas, y todo documento digital y físico que proporcione información relevante relacionada al tema de investigación.

Modalidad Aplicada
Se aplican los conocimientos adquiridos a lo largo de la carrera universitaria en módulos relacionados a Seguridad Informática.

Modalidad Campo
Para el reconocimiento de la situación actual de la Institución y el desarrollo del proyecto en cuanto a detección de vulnerabilidades se refiere, se realizará la investigación de campo dentro del Departamento de Sistemas del H. Gobierno Provincial de Tungurahua.

3.2. 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 6 profesionales que pertenecen al Departamento de Sistemas.

Se aplica una encuesta con un cuestionario de preguntas del uso básico de equipos informáticos a 80 profesionales que pertenecen al Honorable Gobierno Provincial de Tungurahua.

3.3. 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.

Los resultados de la recolección de información se la organizan y se los presenta a través de gráficos estadísticos junto con su respectivo análisis en el Capítulo 4.

3.4. 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. Tema

Auditoría de la Seguridad Informática para el Honorable Gobierno Provincial de Tungurahua mediante la Metodología Open Source Security Testing Methodology Manual.

4.2. Datos informativos

Institución: Honorable Gobierno Provincial de Tungurahua.
Dirección: Calles Simón Bolívar y Mariano Castillo esquina, Cantón Ambato.
Beneficiario: Honorable Gobierno Provincial de Tungurahua
Tiempo: El presente proyecto se lo desarrollará de noviembre 2014 y mayo 2015.
Costo: El costo estimado para el desarrollo del proyecto es de $ 995,39
Tutor: Ing. Mg. David Omar Guevara Aulestia.

4.3. Antecedentes de la propuesta

En la actualidad, año 2015, empresas, instituciones públicas, privadas o gubernamentales han sufrido algún tipo de ataque informático, ya sean con el objetivo de obtener información o dejar inaccesible un servidor o servicio [18], por tal motivo se cree necesario tomar medidas de seguridad y tratar de evitar ataques los cuales puedan perjudicar a la institución.

Mediante las noticias tecnológicas sobre ataques informáticos, vulnerabilidades descubiertas, nuevo software de ataque, servidores comprometidos y lo referente a Seguridad Informática nace la necesidad de proponer la realización de una Auditoría de la Seguridad Informática la cual servirá para la detección de vulnerabilidades en los servidores del Honorable Gobierno Provincial de Tungurahua.

4.4. Justificación

El Honorable Gobierno Provincial de Tungurahua no cuenta con un análisis de vulnerabilidades en los servidores, esto justifica la realización del presente proyecto, lo cual evaluará el grado de vulnerabilidad en lo que a seguridad informática se refiere.

El presente proyecto se centra en la detección de vulnerabilidades más comunes y conocidas, de igual manera como son instalaciones, seguridad de servicios y configuraciones por defecto.

Como producto final se obtendrá el informe de Auditoría de Seguridad Informática en el cual se detallen las vulnerabilidades detectadas y las posibles soluciones que corrijan o disminuyan dichas vulnerabilidades junto con Políticas de Contingencia de Seguridad Informática, esto con el objetivo de que las debilidades no puedan ser explotadas por atacantes informáticos o usuarios mal intencionados.

4.5. Objetivos

4.5.1. Objetivo General

Implementar una Auditoría de la Seguridad Informática para el Honorable Gobierno Provincial de Tungurahua mediante la Metodología Open Source Security Testing Methodology Manual (OSSTMM).

4.5.2. Objetivo Específicos

- 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.

- Identificar las vulnerabilidades de los servidores de la red informática que puedan ser explotadas por intrusos malintencionados.
- Establecer un escenario para simular un ataque programado a los servidores de la red informática para explotar las vulnerabilidades que puedan ser utilizadas por intrusos malintencionados.
- Elaborar Políticas de Contingencia de Seguridad informática que mejoren la integridad, confidencialidad y disponibilidad de la información en base a las vulnerabilidades detectadas.

4.6. 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.

Factibilidad Operativa
En la Dirección de Sistemas del H. Gobierno Provincial de Tungurahua se encuentran en proceso de estructuración, el desarrollo de un análisis de vulnerabilidades es de gran importancia debido a que no se ha realizado dicho análisis anteriormente.
Por este motivo, el análisis de vulnerabilidades y la creación de políticas de contingencia serán de mucha ayuda para eliminar o reducir al máximo las debilidades descubiertas dentro de la Institución.

Factibilidad Técnica
Para la implementación de una Auditoría de la Seguridad Informática se cuenta con el apoyo del H. Gobierno Provincial de Tungurahua, la Dirección de Sistemas, 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, mencionado esto se indica que es factible desde el punto de vista técnico.

Factibilidad Económica
Al contar con el apoyo del H. Gobierno Provincial de Tungurahua y la Dirección de Sistemas, 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, consultas en internet, traslados a las oficinas y otros, serán sustentados por el investigador, indicando que la investigación tiene factibilidad económica.

4.7. Fundamentación

Kali linux.- Es un Sistema Operativo orientado a la auditoría y seguridad informática en general. Distribución avanzada para Pruebas de Penetración, Ethical Hacking y evaluaciones de la seguridad de la red[19].

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), la cual es mostrada en forma gráfica mediante una estructura de tipo árbol[20].

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[21].

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[22].

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[23].

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[24].

NMAP.- Es un explorador de redes y puertos orientado a las auditorías de seguridad[25].

Hping3.- Es un software orientado a la auditoría de la pila TCP / IP, para descubrir la política cortafuegos, para escanear los puertos TCP en de diferentes modos, para transferir archivos a través de un servidor de seguridad y muchas otras cosas[26].

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[27].

Nessus.- 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[28].

Metasploit Framework.- Es un framework 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 [29].

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[30].

Ettercap.- Es un programa que permite interceptar conexiones, filtrar contenidos, generar ataques "ARP Spoofing" entre otras características[31].

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[32].

Sslstrip.- Es un programa para sistemas operativos linux capaz de descifrar tráfico https que viaja a través de una red [33].

4.8. Metodología

Para el presente proyecto se utiliza la metodología OSSTMM creada por el Instituto de Seguridad y Metodologías Abiertas (ISECOM) [17], la metodología 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 a ser auditada, está formada por 6 ítems los cuales comprenden todo el sistema actual, estos son:

- Seguridad de la Información.

En esta sección se revisa la privacidad de los empleados mediante la recolección de información en internet, esta información es analizada en busca de datos que puedan considerarse como privados y no deberían estar expuestos al exterior.

- Seguridad de los Procesos.

Esta sección realiza pruebas en las cuales se pueda tener algún acceso o privilegio mediante el uso de equipos de comunicación y la información de la sección anterior.

- 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.

- Seguridad en las Comunicaciones.

Esta sección realiza pruebas en los dispositivos de comunicación como son VoIP, FAX, Correo de voz, PBX.

- Seguridad Inalámbrica.

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

- Seguridad Física.

Esta sección evalúa la seguridad física de la institución como son los controles de acceso, monitoreo mediante cámaras de seguridad, respuesta de alarmas ante amenazas o catástrofes.

Estudio de la OSSTMM y el planteamiento de la propuesta
Para el cumplimiento de la Prueba de Seguridad (Pentest) se cumple con un orden lógico de etapas:

- Recolección de información
- Sondeo de la 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	Modulo
Recolección de información	Seguridad de la Información	Revisión de la Inteligencia Competitiva
		Revisión de la Privacidad
		Recolección de Documentos
Sondeo de la red	Seguridad de las Tecnologías de Internet	Sondeo de la Red
		Identificación de Servicios y Sistemas
Búsqueda de vulnerabilidades	Seguridad de las Tecnologías de Internet	Búsqueda y Verificación de Vulnerabilidades
Explotación de vulnerabilidades	Seguridad de las Tecnologías de Internet	Búsqueda y Verificación de Vulnerabilidades

Tabla 4.1: Sección y Módulos aplicables al proyecto

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 de la Información

- **Módulo Revisión de la Inteligencia Competitiva**: información recolectada a partir de la presencia en Internet.
- **Módulo Revisión de la Privacidad**: punto de vista legal y ético del almacenamiento, transmisión y control de los datos basados en la privacidad del empleado.
- **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 las Tecnologías de Internet

- **Módulo Sondeo de la Red**: introducción a los sistemas a estudiar, se encuentra el número de sistemas alcanzables que deben ser analizados sin exceder los límites legales.
- **Módulo Identificación de Servicios y Sistemas**: prueba invasiva de los servicios y puertos del sistema en los niveles de transporte y red.

- **Módulo Búsqueda y Verificación de Vulnerabilidades**: se identifica y verifica las debilidades, errores de configuración y vulnerabilidades en un servidor o en una red.

En la figura 4.1 del mapa de seguridad OSSTMM se puede observar las secciones identificadas mismas que posteriormente serán utilizadas con la certeza de que se cumplirán los objetivos prefijados.

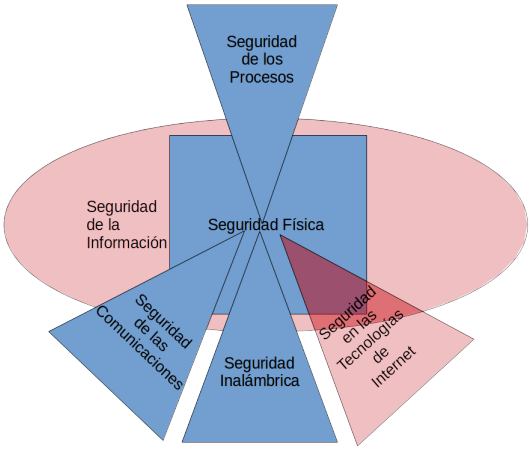

Figura 4.1: Secciones OSSTMM utilizadas en el proyecto

4.9. Determinación del tipo de Políticas de Seguridad Informática aplicadas en el Honorable Gobierno Provincial de Tungurahua

4.9.1. 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 Sistemas, a continuación se presenta cada una de las preguntas con su respectiva respuesta.

1. ¿La habitación de servidores cuenta con un sistema de refrigeración adecuado?

No se cuenta con un sistema de refrigeración adecuado pero la administración actual está gestionando la adquisición de un nuevo sistema que asegure el funcionamiento correcto del centro de datos.

2. ¿Las instalaciones (aulas, cubículos, cableado y oficinas) fueron diseñadas o adaptadas para su funcionamiento?
La infraestructura en la cual funciona el Departamento de Sistemas fue adaptada para su función, esto ha provocado optar por la adaptación de un cableado según las necesidades del Departamento.

3. ¿Se cuenta con un inventario de todos los equipos que integran la red informática?
El Departamento de Sistemas lleva un registro de los bienes informáticos de la Institución cada uno con su respectiva documentación, con respecto al software, se lleva un registro con sus respectivas licencias y manuales.

4. ¿Se tienen equipos dedicados a monitorear el tráfico y actividades de la red?
No, el Departamento de Sistemas fue creado en julio del 2014 por lo cual hay varias cosas que están en proceso de implementación.

5. ¿Qué sistemas tiene bajo su cargo o responsabilidad?
La Departamento de Sistemas tiene bajo su responsabilidad Servidores de Base de Datos, FTP, Firewall, Seguridad POA's, respaldos de información, tickes de mantenimiento de equipos, soporte a usuarios.

6. ¿Se posee bitácoras de fallos o ataques detectados en los servidores?
No, los equipos son revisados remotamente y los errores o fallos que se han presentado no son considerados como ataques.

7. ¿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.

8. ¿Se tienen sistemas de seguridad para evitar que se sustraiga equipo de la institución?
En el edificio en el cua funciona el Departamento de Sistemas se está implementando cámaras de seguridad en puntos estratégicos.

9. ¿Se cuenta con Políticas de Seguridad Informáticas?
No, las Políticas de Seguridad Informática están en proceso de implementación.

10. ¿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 Informática están en proceso de implementación.

11. ¿Se tienen instalados programas antivirus en cada equipo con sus respectivas actualizaciones?
Cada equipo cuenta con su respectivo antivirus Symantec actualizado, se cuenta con un firewall el cual filtra las peticiones de cada uno de los host.

12. ¿El sistema operativo que se maneja se revisa y actualiza el Software Instalado frecuentemente?
Si, en los sistemas propietario se cuenta con las actualizaciones recomendadas y sus respectivas licencias.

4.9.2. Realización de encuestas dirigidas al personal que labora en la Institución

Encuesta dirigida a 6 profesionales del Departamento de Sistemas.
Se aplican preguntas del uso avanzado de equipos informáticos a 6 profesionales que pertenecen al Departamento de Sistemas.

1. ¿La habitación de servidores cuenta con un sistema de refrigeración?
El 100 % de encuestados concluye que se cuenta con un sistema de refrigeración pequeño el cual no es adecuado, pero el Director de Sistemas se encuentra gestionando un sistema adecuado.

2. ¿El cableado estructurado de la red se encuentra correctamente instalado?
El 100 % de encuestados concluye que la infraestructura tecnológica del Departamento de Sistemas fue adaptada por el motivo de ser una edificación antigua no

diseñada para un Data Center.

3. ¿Con que frecuencia cambia sus contraseña?

2 meses_____ 3 meses_____ 6 meses_____ 1 año_____ nunca la cambia_____

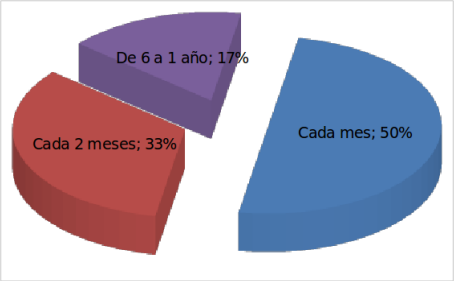

Figura 4.2: Pregunta: ¿Con que frecuencia cambia sus contraseña?

El 83 % menciona que cambia su contraseña en un periodo no más de 2 meses siendo esto recomendable y seguro ante el robo o descifrado de credenciales.

4. Determine una longitud aproximada para crear una contraseña.

Menor a 7_____ entre 7 y 9_____ entre 10 y 13_____ mayor a 13

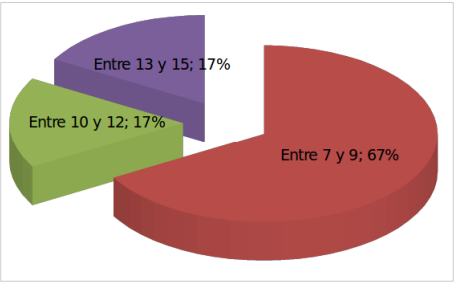

Figura 4.3: Pregunta: Determine una longitud aproximada para crear una contraseña

El 100 % de encuestados optan por claves consideradas con una longitud robusta y segura.

5. Usualmente en la creación de contraseñas suele usar:

Números___ letras mayúsculas___ letras minúsculas___ caracteres especiales___

Figura 4.4: Pregunta: Usualmente en la creación de contraseñas suele usar

Las contraseñas que utiliza el Departamento de Sistemas son consideradas como robustas ya que éstas tienen características como una combinación alfanumérica junto con caracteres especiales.

6. ¿Cree que las medidas de seguridad que se manejan dentro del centro de cómputo sean seguras y adecuadas?

Si _____No _____ ¿Por qué?_____

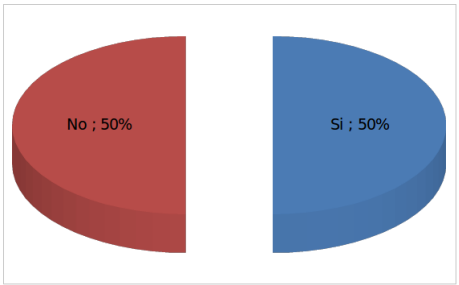

Figura 4.5: Pregunta: ¿Cree que las medidas de seguridad que se manejan dentro del centro de cómputo sean seguras y adecuadas?

El 50 % menciona que las medidas de seguridad no son las adecuadas, argumentan que por ser un edificio el cual no fue diseñado para el funcionamiento de un Data Center no cuenta con las garantías y que las conexiones debieron ser adaptadas.

7. ¿Se cuenta con un inventario de todos los equipos que integran el centro de informática?

Existe un responsable en el Departamento de Sistemas que lleva un registro de los bienes informáticos de la institución con su respectiva documentación, licencias y manuales.

8. ¿Se registran las acciones o modificaciones en los sistemas o servicios?
Si ____No____ (Observación_____)

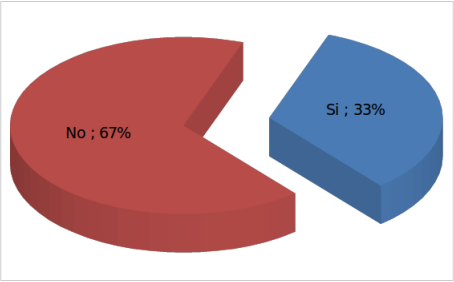

Figura 4.6: Pregunta: ¿Se registran las acciones o modificaciones en los sistemas o servicios?

El 67 % de los encuestados no llevan un registro de los cambios o modificaciones que realizan en los servicios o sistemas lo cual puede ser un problema al momento de presentar un fallo o un mal funcionamiento del servicio o sistema.

9. ¿Se cuenta con equipos dedicados a monitorear el tráfico y las actividades de la red?
Si____ No ____ ¿Con que frecuencia?_____
Se encuentra en estado de implementación el Firewall Gateprotect el cual funciona para filtrar las peticiones de cada uno de los host.

10. En los servidores, ¿se realizan actividades para su monitoreo?
Si_____ No ____ ¿Cuáles? _____

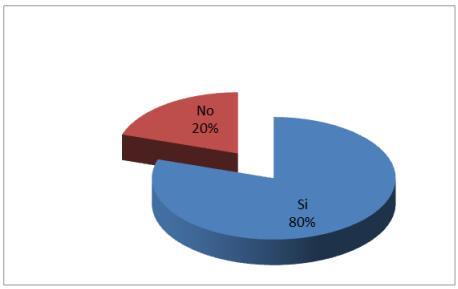

Figura 4.7: Pregunta: En los servidores, ¿se realizan actividades para su monitoreo?

El 80 % responde que los servidores son revisados de manera remota por parte del administrador y no cuentan con un software que detecte actividades sospechosas.

11. ¿Se revisa y actualiza el Software Instalado frecuentemente?

Si _____ No_____ Frecuencia_____

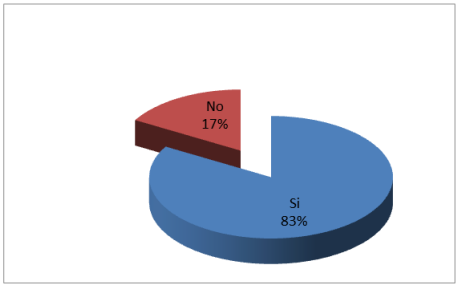

Figura 4.8: Pregunta: ¿Se revisa y actualiza el Software Instalado frecuentemente?

El 83 % responde que los sistemas propietario se cuenta con las actualizaciones recomendadas y sus respectivas licencias.

12. ¿Se cuenta con un plan de contingencia en caso de que surja algún desastre?

Si _____ No_____ (Observación_____)

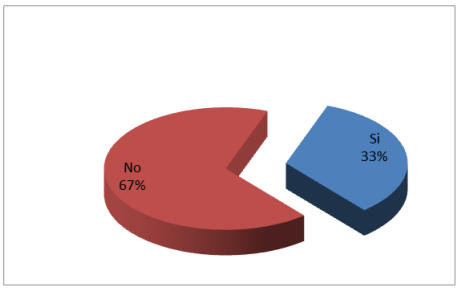

Figura 4.9: Pregunta: ¿Se cuenta con un plan de contingencia en caso de que surja algún desastre?

El 67 % responde que no se cuenta con un Plan de Contingencia ante desastres, esto dificultaría en el momento de reaccionar ante cualquier evento que atente la seguridad de la información.

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

Si _____ No_____ (Observación_____)

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

14. ¿Existe un programa de mantenimiento en las diferentes áreas que se lleve a cabo?
Se brinda mantenimiento a los equipos cada 6 meses si estos no presentan daño y, mediante un ticket creado por un usuario informando de fallos en el equipo éste es revisado y de ser el caso reparado.

Encuesta dirigida a 80 profesionales del H. Gobierno Provincial de Tungurahua.
Se aplican preguntas del uso básico de equipos informáticos a 80 profesionales que pertenecen al Honorable Gobierno Provincial de Tungurahua.

1. ¿Se cuentan con algún tipo de control de entradas y salidas de personal a la Institución?
Si____ No____ (¿Cuál ?_____)

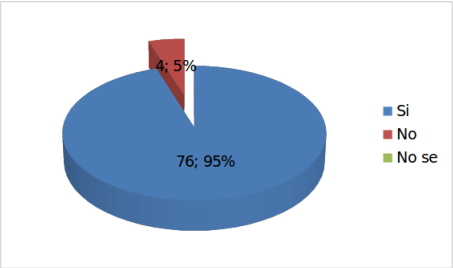

Figura 4.10: Pregunta: ¿Se cuentan con algún tipo de control de entradas y salidas de personal a la Institución?

El 76 % de encuestados menciona que cuentan con cámaras de seguridad, guardia en la puerta de ingreso y un reloj biométrico el cual controla las entradas y salidas del personal.
Estas seguridades es beneficioso para la Institución la cual puede prevenir la sustracción de equipos o algún bien de alguno de los departamentos.

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

No cuenta_____ Bueno_____ Regular_____ Malo_____ Pésimo_____

¿Por qué?_____

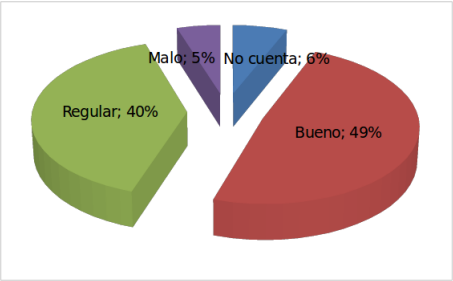

Figura 4.11: Pregunta: ¿Su equipo de trabajo cuenta con internet? de ser el caso ¿cómo califica el servicio?

El 94 % de los encuestados cuentan con acceso a internet, el 49 % califica el servicio como bueno, el 40 % lo califica como regular y un 5 % como malo mencionando que existen restricciones.

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

Si _____No _____ ¿Por qué?_____

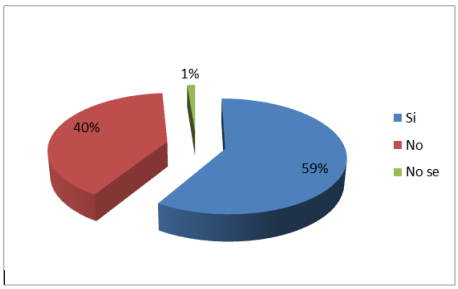

Figura 4.12: Pregunta: Cuando quiere consultar una página para obtener información ¿tiene acceso a ella?

Del 100 % de encuestados con acceso a internet, 40 % quienes califican el servicio como malo y regular argumentan que tienen varias páginas restringidas las cuales creen que son necesarias para consultas, creen conveniente tener un acceso sin restricciones.

4. Su usuario y contraseña, la tiene guardada en?

Celular_____ Computador_____ Papel_____ La memoriza_____

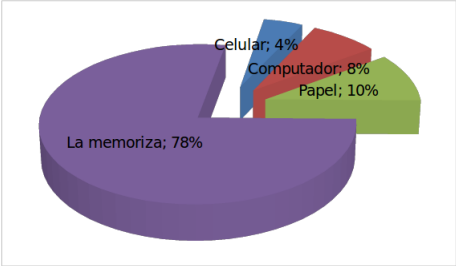

Figura 4.13: Pregunta: ¿Su usuario y contraseña, la tiene guardada en?

El 78 % de los encuestados memoriza la contraseña siendo esto la mejor opción ante la sustracción de algún documento físico como lo señala el 22 % restante.

5. Determine un periodo aproximado para el cambio o renovación de su contraseña.

2 meses_____ 3 meses_____ 6 meses_____ 1 año_____ nunca la cambia_____

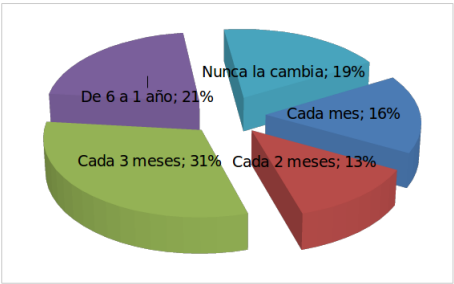

Figura 4.14: Pregunta: Determine un periodo aproximado para el cambio o renovación de su contraseña

El 60 % menciona que cambia su contraseña en un periodo no más de 3 meses siendo esto recomendable y seguro ante el robo de credenciales.

6. Determine una longitud aproximada para su contraseña

Menor a 7_____ entre 7 y 9_____ entre 10 y 13_____ mayor a 13

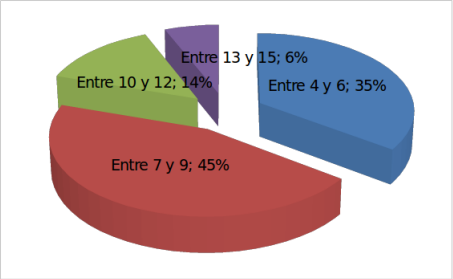

Figura 4.15: Pregunta: Determine una longitud aproximada para su contraseña

Un 35 % que utiliza una contraseña con longitud de entre 4 y 7 caracteres puede ser tomado como contraseñas débiles y fáciles de descifrar.

7. Usualmente en su contraseña suele usar:
Números_____ letras mayúsculas_____ letras minúsculas_____ caracteres especiales_____

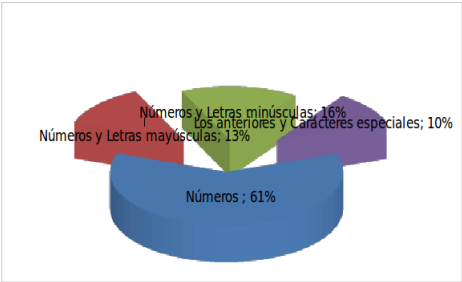

Figura 4.16: Pregunta: Usualmente en su contraseña suele usar

Un 61 % utiliza una contraseña la cual involucra solo números, esto puede ser tomado como contraseñas débiles fáciles de descifrar.

8. ¿Sabe del manejo de Políticas de Seguridad Informática?
Si____ No ____ (Observación_____)

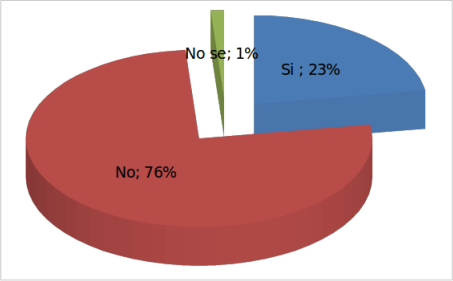

Figura 4.17: Pregunta: ¿Sabe del manejo de Políticas de Seguridad Informática?

El 76 % de encuestados no sabe del manejo de políticas de seguridad informática, el 23 % responde que si argumentando que mediante investigación personal sabe de seguridad informática y cómo manejar activos informáticos pero en lo institucional no ha existido conocimiento alguno.

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

Si____ No ____ (Observación_____)

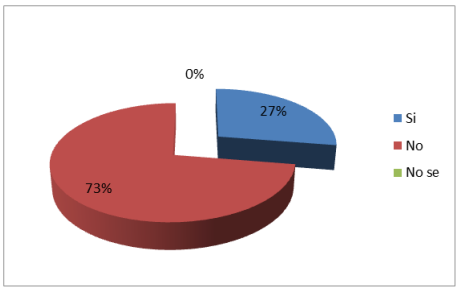

Figura 4.18: Pregunta: ¿Se ha dado a conocer sobre los "ataques informáticos", y las maneras de evitarlos?

El 73 % responde que no se ha dado a conocer sobre ataques informáticos y las maneras de evitarlos, el 27 % argumenta que lo poco que saben es debido a investigación personal.

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

Si ____ No____ ¿Cuál?_____

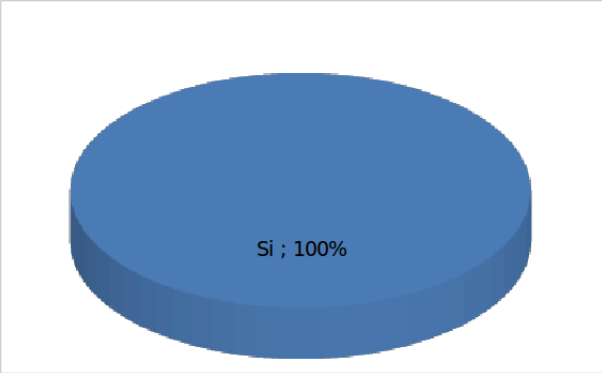

Figura 4.19: Pregunta: ¿Se tienen instalado programa antivirus en su equipo con sus respectivas actualizaciones?

El 100 % de encuestados responde que cada equipo cuenta con su respectivo antivirus actualizado.

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

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

Tipo	Característica	Aplicable al proyecto	Observación
Análisis de Vulnerabilidades	Tiene un objetivo definido	Si	Tiene como objetivo detectar vulnerabilidades en partes específicas
	Tiene en cuenta el entorno de seguridad actual	Si	Aplica vulnerabilidades y fallos conocidos
	Trata de comprometer los sistemas objetivos	No	Solo lista las vulnerabilidades detectadas
	Explota las vulnerabilidades	No	No explota las vulnerabilidades
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 y trata de comprometer los sistemas objetivos
	Explota las vulnerabilidades	Si	Explota las vulnerabilidades en un entorno real y virtual (simular 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 atacante 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

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

Característica	Maltego	The Harvester	Anubis	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, Server, Vista (32/64 bits),	Linux	Windows XP \ 2003 \ Vista \ 7, 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

De acuerdo a la tabla 4.3, Maltego, TheHarvester y Uniscan cuentan con sus versiones libres y constante actualización, también se suma que éstas herramientas ya vienen instaladas en el Sistema Operativo Kali Linux.
También se eligen VisualRoute y FOCA con sus versiones de prueba limitadas por un periodo no más de 30 días.

Herramientas de sondeo de puertos

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

Tabla 4.4: Herramientas de sondeo de puertos

Mediante el análisis de la tabla 4.4 la utilización de NMAP por el momento resulta ser la más eficaz porque cuenta con varias funciones y scripts para sondear redes de computadoras, incluyendo la detección de equipos y sistemas operativos.

Herramientas de detección de vulnerabilidades

Característica	OpenVAS	Nessus	Retina	Nexpose
Costo	Versión libre	Versión libre y de paga	Versión libre y de paga	Versión libre
Plataforma	Centos, Debian, Fedora, OpenSuse, RedHat, Ubuntu, Windows	Microsoft Windows, Mac OS X, Linux, FreeBSD	Windows Server 2008 o versiones posteriores y 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

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

Herramientas de explotación

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

Tabla 4.6: Herramientas de explotación de vulnerabilidades

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

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

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

Sección Seguridad de la Información

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

El objetivo de este 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 la institución a auditar.

Mediante la herramienta Maltego se investiga las relaciones existentes que tiene un determinado dominio en este caso **tungurahua.gob.ec**.

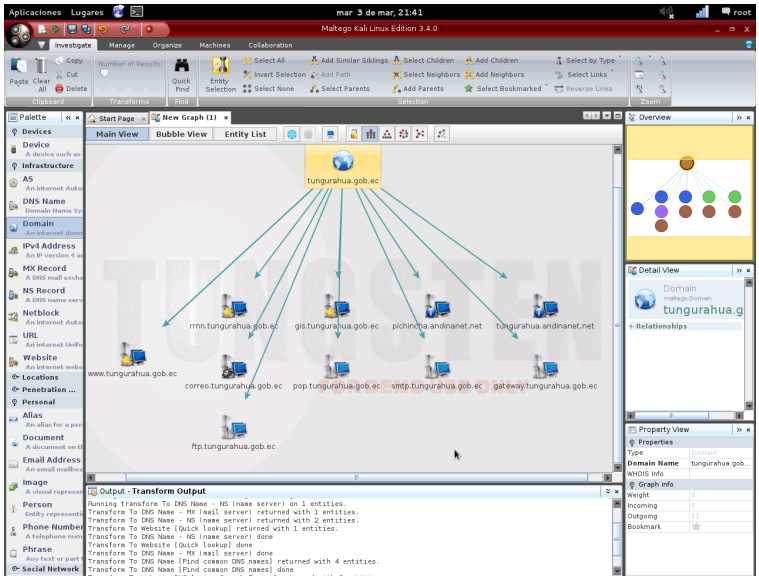

Figura 4.20: Maltego, transformación en relación al Dominio Tungurahua.gob.ec

En la figura 4.20 se puede observar las transformaciones DNS form Domain MX, NS y Dominios en común aplicado a un objeto de tipo Domain nombrado tungurahua.gob.ec, se muestra servidores DNS, servidores de correo y servidores relacionados. Las flechas indican que existe relación entre el objeto padre y los objetos hijos, las estrellas amarillas indican que el objeto provee servicios web.

Mediante la herramienta FOCA se busca toda información relacionada al dominio **tungurahua.gob.ec** la cual sirve para extraer los metadatos relevantes de la Institución.

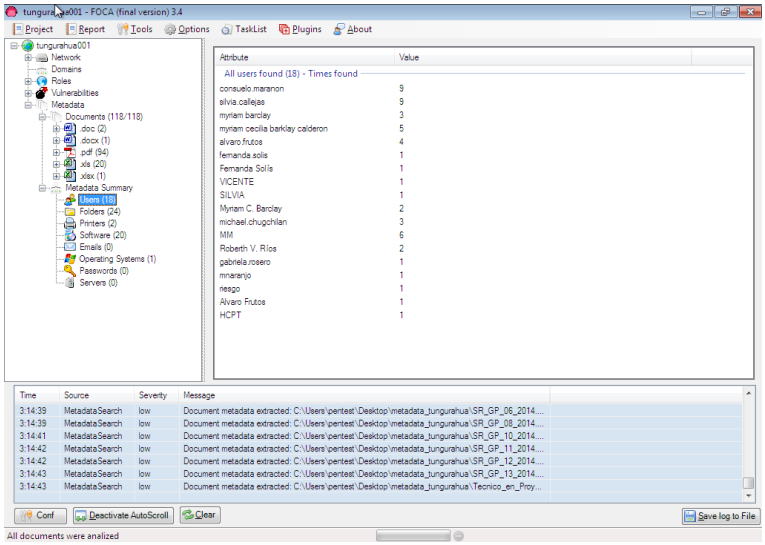

Figura 4.21: FOCA, nombres de usuarios detectados

En la figura 4.21 se observa el resultado de un proyecto ejecutado en foca con el dominio tungurauha.gob.ec, descargando 118 documentos de tipo .doc, .docx, .pfd, .xls, .xlsx de los cuales se extraen los metadatos y se obtiene:

- 18 nombres de usuarios.
- 24 direcciones de ubicación de archivos.
- 2 nombres de impresoras.
- Sistema operativo Windows en sus versiones XP y 7.

El peligro de la extracción de metadatatos radica en que a través de un metadato se averigüe la versión de un sistema operativo o software el cual cuente con algún fallo o una vulnerabilidad que pueda ser explotada.

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

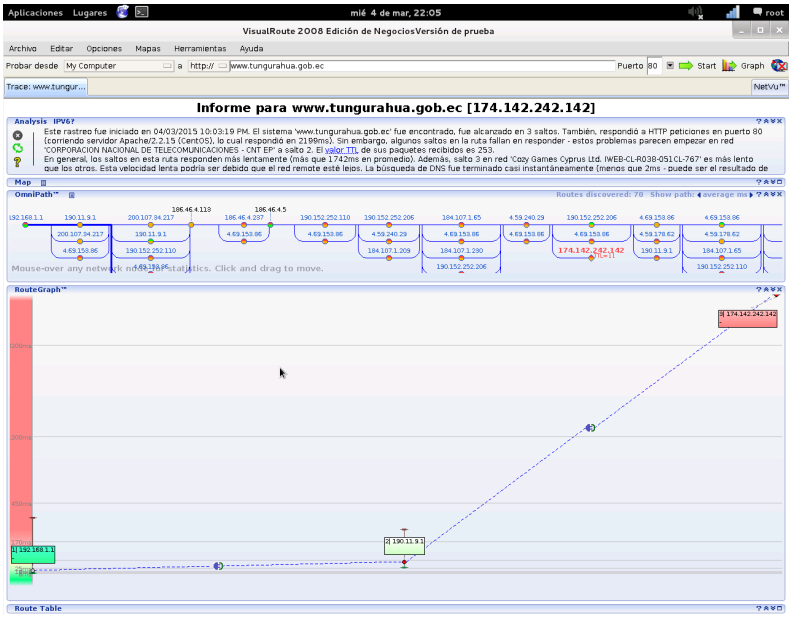

Figura 4.22: VisualRoute a www.tungurahua.gob.ec

En la figura 4.22 se observa el trazado de ruta que unen dos host siendo estos el host local y la web www.tungurahua.gob.ec, la importancia de investigar la ubicación es de saber si cuentan con un servidor local u oficinas con un host externo lo cual significaría la intrusión en empresas privadas.

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

Figura 4.23: TheHarvester a dominio tungurahua.gob.ec

En la figura 4.23 se puede observar resultados de la ejecución de TheHarvester dando como resultado varios correos electrónicos y servidores relacionados al dominio tungurahua.gob.ec.

El buscador de Google, el buscador 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".

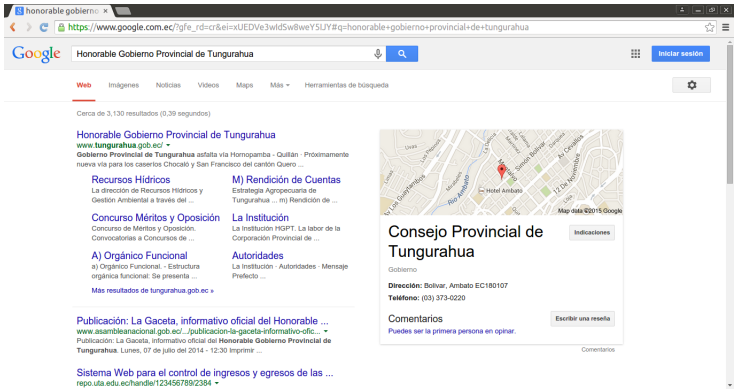

Figura 4.24: Búsqueda en GOOGLE

En la figura 4.24 se observa la búsqueda de "Honorable Gobierno Provincial de Tungurahua" en el buscador de google, el resultado es de más de tres mil resultados, el número de resultados se lo puede reducir mediante "Google Hacking".

Buscando información en la base de datos **NIC** (Network Information Center); "NIC es la autoridad que delega los nombres de dominio a 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 privadas"[34].

En el navegador de google se ingresa a la dirección https://nic.ec/home.htm y se digita el dominio en investigación.

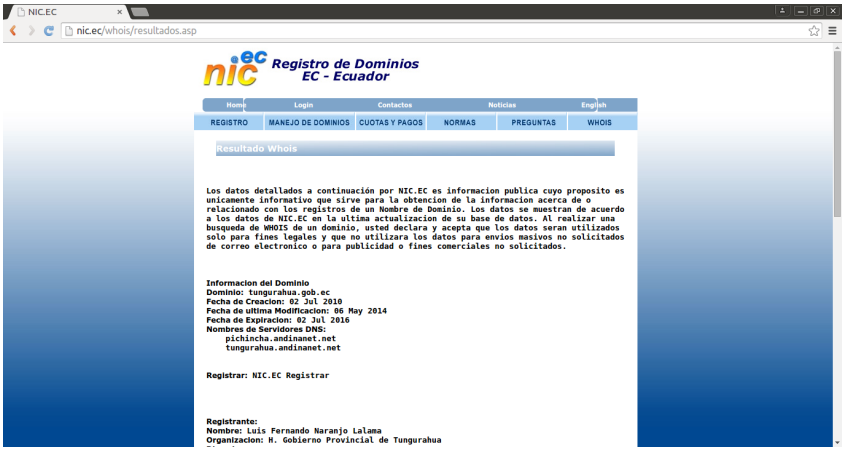

Figura 4.25: Consulta de tungurahua.gob.ec en NIC

En la figura 4.25 se observa el resultado de la consulta del dominio tungurahua.gob.ec en la base de datos NIC, se aprecian que existen datos reales de empleados de la Institución, el peligro de exponer la información mencionada es que ésta puede ser utilizada para un ataque de ingeniería social.
NIC puede mantener la información de manera privada mediante un pago extra anualmente.

Resultados obtenidos con Maltego:

Nombre	Dirección IP	Servicio	Observación
www.tungurahua.gob.ec	174.142.242.142	Website	Se encuentra en un hosting externo
correo.tungurahua.gob.ec	181.112.146.3	MX Record	
pop.tungurahua.gob.ec	181.112.146.3	DNS Name	
gateway.tungurahua.gob.ec	181.112.146.4	DNS Name	
gis.tungurahua.gob.ec	181.112.146.5	Website	
ftp.tungurahua.gob.ec	181.112.146.14	DNS Name	
rrnn.tungurahua.gob.ec	181.112.146.14	Website	
smtp.tungurahua.gob.ec	181.112.146.8	DNS Name	

Tabla 4.7: Listado de servidores relacionados al dominio

Resultados obtenidos de la Base de Datos NIC.

Nombre	Contacto	Dirección	Mail	Teléfono	Fax
Xavier Francisco López Andrade	Administrativo	Bolívar 491 y Castillo Ambato, Tungurahua 1801320 EC	tecnologiasinformaticas @tungurahua.gob.ec	593-3730220	593-32422297
Luis Alberto Bravo Moncayo	Técnico	Castillo y Sucre Ambato, Tungurahua	proyectosti@ tungurahua.gob.ec	593-33730220	
Yolanda Beatriz Pazmiño	Facturación	Bolívar 491 y Castillo Ambato, Tungurahua	yolanda.pazmino@ tungurahua.gob.ec	5933-2421993	593-2826419

Tabla 4.8: Datos obtenidos de NIC

La investigación de la Institución obtuvo como resultado varios documentos en los cuales involucraban Títulos de tercer nivel, apellidos, nombres y cargos de varios servidores del año 2013 y 2014.

- Se obtuvo las extensiones del directorio telefónico por áreas y nombre del contacto.
- Se obtuvo el distributivo de trabajo de los empleados junto con su respectiva remuneración.
- Se obtuvo el organigrama estructural de la Institución y una descripción de cada una de ellas.
- Se obtuvo el Reglamento Orgánico Funcional del H.G.P.T.
- Se descubrió que el Área de sistemas fue creado en julio del año 2014.

- **Módulo de Revisión de la Privacidad**

En este módulo se revisa que los datos de los empleados considerados como privados no sean expuestos ante todo el mundo, de igual manera la confidencialidad con la cual se maneja la distribución de información a los empleados.

Uno de los principios básicos de Seguridad Informática es la Confidencialidad la cual se define en, la no divulgación de información de manera no autorizada.

La información de instituciones públicas es transparente y están obligadas a difundirla mediante un portal o sitio web, esto permite acceder a nombres de autoridades, directores y demás empleados.

La web del Honorable Gobierno Provincial de Tungurahua proporciona la siguiente tabla de Autoridades.

No	Dirección	Director	Secretaría
1	Prefectura	Ing. Fernando Naranjo L.	Sara Salazar
2	Vice Prefectura	Lic. Cecilia Chacón	Amparito Núñez
3	Dirección Desarrollo Humano y Cultura	Lic. Nikolay Pangol	Carla Andrade
4	Dirección Financiera	Ec. Yolanda Pazmiño	Sandra Robayo
5	Dirección Recursos Hídricos	Ing. Carlos Sánchez	Elvia Lalama
6	Dirección Relaciones Externas	Dr. Juan Francisco Mora	Silvia Ortiz
7	Dirección Vías y Construcciones	Ing. Luwin Villacrés	María Eulalia Villacreses
8	Dirección Jurídica	Dra. Rosa María Ortega	Consuelo Marañón
9	Dirección de Producción	Lic. Manuel Ullauri	Rosario Maliza
10	Dirección Administrativa	Lic. Silvia Callejas	Miriam Barclay
11	Dirección de Planificación	Ing. Jorge Sánchez	María Isabel Pachano
12	Dirección de Sistemas	Ing. Francisco López	Diana Cifuentes

Tabla 4.9: Autoridades de las Direcciones existentes

- **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.

- Distributivo de trabajo de la institución que involucran el puesto y la remuneración.
- Informes de Auditorías internas de gastos.
- Resultados de Concurso de Méritos y Oposición para varios cargos.
- Solicitudes para el arrendamiento de bienes.

Mediante un análisis de los metadatos de los documentos obtenidos se puede definir nombres de usuarios relacionados con la institución y que se utiliza el sistema operativo de software propietario Microsoft Windows en sus versiones XP y 7. Los datos personales pueden ser usados para la aplicación de ingeniería social, robo de información mediante phishing, creación de diccionario de datos, entre otros.

Sección Seguridad en las Tecnologías de Internet

- **Módulo de Sondeo de la 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.

Lista de Redes internas de la institución

Red	Máscara	Observación
172.16.0.0	255.255.255.224	Administrativo
172.16.1.0	255.255.255.224	Hídricos
172.16.2.0	255.255.255.224	Planificación
172.16.3.0	255.255.255.224	Red de Servicios

Tabla 4.10: Redes internas del H. Gobierno Provincial de Tungurahua.

Lista de Servidores internos de la Institución

No	Dirección	Nombre	Sistema Operativo
1	172.16.1.132	oracle.tungurahua.gob.ec	Red Hat 64 bits
2	172.16.1.133	gis.tungurahua.gob.ec	Centos 2.16.0
3	172.16.1.134	correo.tungurahua.gob.ec	Ubuntu Server 14.04 LTS
4	172.16.1.135	dchgpt01.tungurahua.gob.ec	Windows Server 2012
5	172.16.1.136	tramites.tungurahua.gob.ec	Ubuntu Server 14.04 LTS
6	172.16.1.140	central4760	Windows XP Profesional
7	172.16.1.141	symantec.tungurahua.gob.ec	Windows Server 2003
8	172.16.1.142	local_domain	CentOS
9	172.16.1.143	mapas.tungurahua.gob.ec	CentOS
10	172.16.1.144	bddespacial	CentOS
11	172.16.1.145	srvap01	CentOS
12	172.16.1.146	rrnn.tungurahua.gob.ec	CentOS
13	172.16.1.147	bdd_nr	CentOS
14	172.16.1.148	bdd_r	CentOS
15	172.16.1.149	ftp.tungurahua.gob.ec	CentOS
16	172.16.1.159	citrix	Citrix version 6.1
17	172.16.1.161	serwebcentos	Centos
18	172.16.1.162	hgpt-serverprue	Windows XP Profesional
19	172.16.1.169	vm-servidor1	Vmware Vmvisor 5.5 Update 2

Tabla 4.11: Servidores a auditar

- **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 explorar la red, el auditor obtiene conexión al punto de acceso como un usuario más de la intranet, en la figura 4.26 se muestra un escenario creado según la información obtenida con anterioridad, una vez conectado a la red se ejecuta las herramientas seleccionadas según sea el caso.

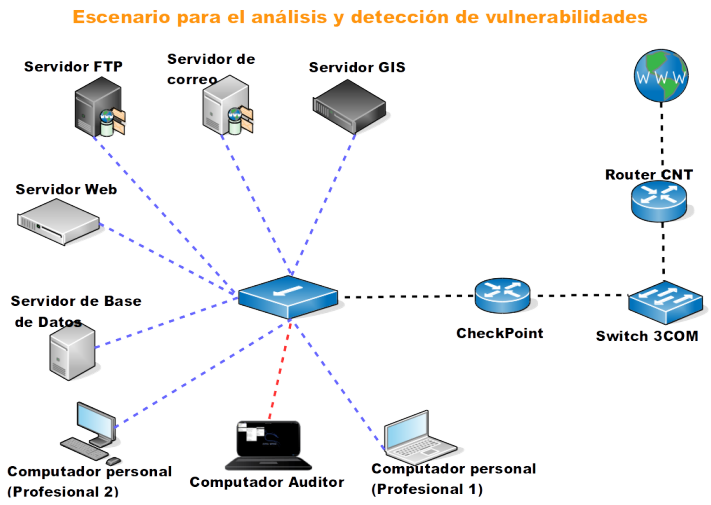

Figura 4.26: Escenario para el análisis y detección de vulnerabilidades.

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.

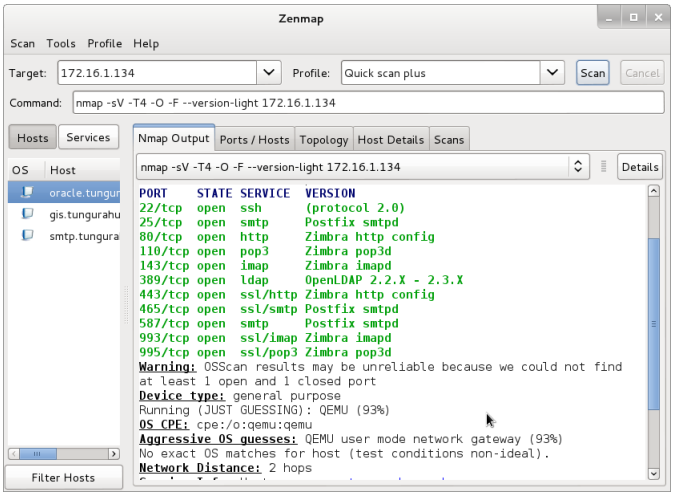

Figura 4.27: Sondeo de puertos con nmap

Servidor oracle.tungurahua.gob.ec

Puerto	Protocolo	Servicio	Detalle
22	tcp	ssh	OpenSSH 5.3
111	tcp	rpcbind	2-4 (RPC #100000)
1521	tcp	oracle	Oracle TNS Listener
5520	tcp	ormi	Oracle Remote Method Invocation
1158	tcp	http	Oracle Application Server 10g
3938	tcp	Oem-agent	Oracle Enterprise Manager Agent httpd 10.2.0
10948	tcp	Oracle-tns	Oracle TNS Listener
53	udp	Microsoft DNS	
88	tcp	Windows 2003 kerveros	
153	tcp	Microsoft Windows RPC	

Tabla 4.12: nmap a oracle.tungurahua.gob.ec

Servidor correo.tungurahua.gob.ec

Puerto	Protocolo	Servicio	Detalle
22	tcp	ssh	OpenSSH (protocol 2.0)
25	tcp	smtp	Postfix smtpd
80	tcp	http	Zimbra http
110	tcp	pop3	Zimbra pop3
143	tcp	imap	Zimbra imapd
389	tcp	ldap	OpenLDAP 2.3.X
443	tcp	ssl/http	Zimbra http
465	udp	ssl/smtp	Postfix smtpd
587	tcp	smtp	Postfix smtpd
993	tcp	ssl/imap	Zimbra imapd
995	tcp	ssl/pop3	Zimbra pop3

Tabla 4.13: nmap a correo.tungurahua.gob.ec

Servidor gis.tungurahua.gob.ec

Puerto	Protocolo	Servicio	Detalle
22	tcp	ssh	OpenSSH 4.3
80	tcp	http	Apache httpd
111	tcp	rpcbind	2 (RPC #100000)
443	tcp	http	Apache httpd
5432	tcp	postgresql	PostgreSQL DB (Spanish)
6000	tcp	x11	
6001	tcp	x11	
10000	tcp	http	MiniServ 1.690 (Webmin httpd)

Tabla 4.14: nmap a gis.tungurahua.gob.ec

Servidor dchgpt01.lan.tungurahua.gob.ec

Puerto	Protocolo	Servicio	Detalle
53	udp	Microsoft DNS	Microsoft DNS
88	tcp	Kerberos-sec	Windows 2003 kerberos
135	tcp	msrpc	Microsoft Windows RPC
139	tcp	Netbios-ssn	
389	tcp	ldap	
445	tcp	Netbios-ssn	
3389	tcp	Ms-wbt-server	
49157	tcp	ncacn_http	Microsoft Windows RPC over HTTP 1.0

Tabla 4.15: nmap a dchgpt01.lan.tungurahua.gob.ec

Servidor tramites.tungurahua.gob.ec

Puerto	Protocolo	Servicio	Detalle
22	tcp	ssh	OpenSSH (protocol 2.0)
80	tcp	http	Apache httpd
443	tcp	http	Apache httpd
10000	tcp	http	MiniServ 1.690 (Webmin httpd)

Tabla 4.16: nmap a tramites.tungurahua.gob.ec

Servidor CENTRAL4760

Puerto	Protocolo	Servicio	Detalle
80	tcp	http	Apache httpd
135	tcp	msrpc	Microsoft Windows RPC
139	tcp	Netbios-ssn	
389	tcp	ldap	(Anonymous bind)
445	tcp	Microsoft-ds	Microsoft Windows XP microsoft-ds
1025	tcp	giop	COBRA naming server
8009	tcp	ajp13	Apache Jserv (Protocol 1.3)

Tabla 4.17: nmap a CENTRAL4760

Servidor symantec.lan.tungurahua.gob.ec

Puerto	Protocolo	Servicio	Detalle
80	tcp	http	Apache httpd 2.2.21 (Win 32)
135	tcp	msrpc	Microsoft Windows RPC
139	tcp	Netbios-ssn	
443	tcp	http	Apache httpd 2.2.21 (Win 32)
445	tcp	Microsoft-ds	Microsoft Windows 2003
3306	tcp	mysql	MySQL 5.5.16
3389	tcp	Ms-wbt-server	Microsoft Terminal Service
8443	tcp	http	Symantec Messaging Gateway smtpd

Tabla 4.18: nmap a symantec.lan.tungurahua.gob.ec

Servidor local domain

Puerto	Protocolo	Servicio	Detalle
21	tcp	ftp	Vsftpd 2.0.5
22	tcp	ssh	OpenSSH 4.3 (Protocol 2.0)
111	tcp	rpcbind	2 (RPC #100000)
992	tcp	status	1 (RPC #100024)
5801	tcp	Vnc-http	RealVBC 4.0 (resolution: 400x250)
5901	tcp	vnc	VNC (protocol 3.8)
6001	tcp	X11	

Tabla 4.19: nmap a local domain

Servidor mapas.tungurahua.gob.ec

Puerto	Protocolo	Servicio	Detalle
22	tcp	ssh	OpenSSH 5.3 (protocol 2.0)
80	tcp	http	Apache httpd 2.2.15 (CentOS)
111	tcp	rpcbind	2-4 (RPC #100000)
443	tcp	http	Apache httpd 2.2.15 (CentOS)
59599	tcp	status	1 (RPC #100024)

Tabla 4.20: nmap a mapas.tungurahua.gob.ec

Servidor bddespacial

Puerto	Protocolo	Servicio	Detalle
22	tcp	ssh	OpenSSH 5.3 (protocol 2.0)
111	tcp	rpcbind	2-4 (RPC #100000)
5432	tcp	postgresql	PostgreSQL DB 9.2.0 – 9.2.2

Tabla 4.21: nmap a bddespacial

Servidor laptic.lan.tungurahua.gob.ec

Puerto	Protocolo	Servicio	Detalle
22	tcp	ssh	OpenSSH 4.3 (Protocol 2.0)
111	tcp	rpcbind	2-4 (RPC #100000)
8009	tcp	ajp13	Apache Jserv (Protocol 1.3)
8080	tcp	http	Apache Tomcat/Coyote JSP engine 1.1
8081	tcp	http	Apache Tomcat/Coyote JSP engine 1.1
8443	tcp	http	Apache Tomcat/Coyote JSP engine 1.1
9999	tcp	abyss	

Tabla 4.22: nmap a laptic.lan.tungurahua.gob.ec

Servidor Citrix

Puerto	Protocolo	Servicio	Detalle
22	tcp	ssh	OpenSSH 4.3 (Protocol 2.0)
80	tcp	http	Citrix Xen Simple HTTP Server (XenServer 6.1.0)
443	tcp	hhtp	Citrix Xen Simple HTTP Server (XenServer 6.1.0)

Tabla 4.23: nmap a Citrix

Servidor rrnn.tungurahua.gob.ec

Puerto	Protocolo	Servicio	Detalle
22	tcp	ssh	OpenSSH 5.3 (protocol 2.0)
25	tcp	smtp	Postfix smtpd
80	tcp	http	Apache httpd
81	tcp	http	Apache httpd
111	tcp	rpcbind	2-4 (RPC #100000)
443	tcp	https	Apache

Tabla 4.24: nmap a rrnn.tungurahua.gob.ec

Servidor bdd_nr

Puerto	Protocolo	Servicio	Detalle
22	tcp	ssh	OpenSSH 5.3 (protocol 2.0)
80	tcp	http	Apache httpd 2.2.15 (CentOS)
111	tcp	rpcbind	2-4 (RPC #100000)
443	tcp	http	Apache httpd 2.2.15 (CentOS)
5432	tcp	postgresql	PostgreSQL DB
27017	tcp	mongodb	MongoDB 2.6.1

Tabla 4.25: nmap a bdd_nr

Servidor ftp.tungurahua.gob.ec

Puerto	Protocolo	Servicio	Detalle
21	tcp	ftp	Vsftpd 2.2.2
22	tcp	ssh	OpenSSH 5.3 (protocol 2.0)
111	tcp	rpcbind	2-4 (RPC #100000)
3306	tcp	mysql	MySQL (unauthorized)

Tabla 4.26: nmap a ftp.tungurahua.gob.ec

Servidor SerWebCentos

Puerto	Protocolo	Servicio	Detalle
22	tcp	ssh	OpenSSH 4.3 (Protocol 2.0)
80	tcp	http	Apache httpd 2.2.3 (CentOS)

Tabla 4.27: nmap a SerWebCentos

Servidor HGPT-SERVERPRUE

Puerto	Protocolo	Servicio	Detalle
80	tcp	ssh	Apache httpd 2.2.11 ((Win 32) PHP/5.2.9-2)
135	tcp	msrpc	Microsoft Windows RPC
139	tcp	Netbios-ssn	
445	tcp	Microsoft-ds	Microsoft Windows XP microsoft-ds
3306	tcp	mysql	MySQL (unauthorized)
3389	tcp	Ms-wbt-server	Microsoft Terminal Service

Tabla 4.28: nmap a HGPT-SERVERPRUE

Servidor VM-Servidor1

Puerto	Protocolo	Servicio	Detalle
22	tcp	ssh	OpenSSH 5.6 (protocol 2.0)
80	tcp	http	Vmware Esxi Server httpd
443	tcp	http	Vmware Esxi Server httpd
8000	tcp	Http-alt	

Tabla 4.29: nmap a VM-Servidor1

- **Módulo Búsqueda y Verificación de Vulnerabilidades**

En esta sección se buscan posibles fallos, errores o vulnerabilidades de sistemas operativos, esto se lo realiza mediante el sondeo de vulnerabilidades, luego se explota (prueba 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 de 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 elige Full and very deep recomendado. Una vez creado lo necesario se procede a ejecutar las tareas (ver figura 4.28).

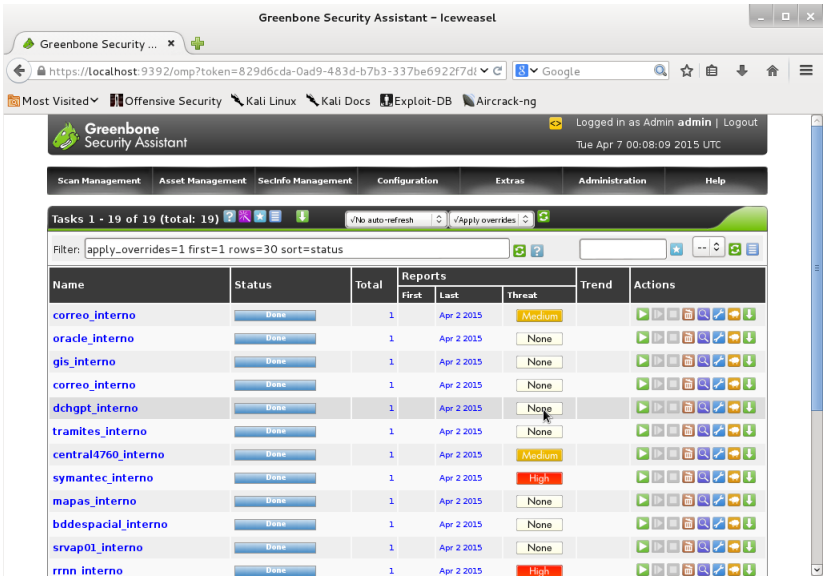

Figura 4.28: Escaneo de vulnerabilidades con OpenVAS

A continuación se detallan las vulnerabilidades detectadas con OpenVAS:

Servidor symantec.lan.tungurahua.gob.ec

Servicio	Vulnerabilidad	Riesgo	Observación
Apache httpd 2.2.21 (Win 32)	Denegación de servicio	Alto	El servicio es propenso a desbordamiento de buffer y causar una denegación de servicio.
Ms-wbt-server Microsoft Terminal Service	Debilidad de man-in-the-middle en el Protocolo Remoto de Escritorio	Alto	Escritorio remoto podría permitir la ejecución remota de código y un atacante podría enviar una secuencia de paquetes RDP y explotar la vulnerabilidad.
Apache httpd 2.2.21 (Win 32)	Divulgación de información	Medio	El servidor http de Apache pueden ser explotadas para divulgar información potencialmente sensible y comprometer un sistema vulnerable.
Apache httpd	Certificado SSL no es confiable	Medio	Certificado SSL no tiene una firma de una autoridad de certificación pública conocida. Esto podría hacer que sea más fácil de llevar a cabo ataques man-in-the-middle contra el host remoto.

Tabla 4.30: Vulnerabilidades detectadas en symantec.lan.tungurahua.gob.ec

Servidor Central4760

Servicio	Vulnerabilidad	Riesgo	Observación
Apache Jserv (Protocol v1.3)	Apache Tomcat/JSP instalado con los archivos por defecto	Medio	Estos archivos pueden ayudar a obtener una información del Tomcat remoto.

Tabla 4.31: Vulnerabilidades detectadas en Central4760

Servidor rrnn.tungurahua.gob.ec

Servicio	Vulnerabilidad	Riesgo	Observación
Nfs-utils rpc.statd	Vulnerabilidades de cadena de formato a distancia	Alto	Una explotación exitosa podría permitir a atacantes ejecutar código arbitrario con los privilegios del proceso rpc.statd.
Apache httpd	Métodos HTTP TRACE / TRACK permitidos	Medio	Los métodos HTTP TRACE / TRACK pueden ser susceptibles a el robo de credenciales.
Apache httpd	Certificado SSL no es confiable	Medio	Certificado SSL no tiene una firma de una autoridad de certificación pública conocida. Esto podría hacer que sea más fácil de llevar a cabo ataques man-in-the-middle contra el host remoto.

Tabla 4.32: Vulnerabilidades detectadas en rrnn.tungurahua.gob.ec

Servidor correo.tungurahua.gob.ec

Servicio	Vulnerabilidad	Riesgo	Observación
Apache httpd	Certificado SSL no es confiable	Medio	Certificado SLL del servidor no tiene una firma de una autoridad de certificación pública conocida. Es posible un ataque man-in-the-middle contra el host remoto.
Vulnerabilidad cifrado degradado	El host remoto se ve afectado por una vulnerabilidad MitM conocido como POODLE	Medio	La vulnerabilidad se debe a la forma en que SSL 3.0 se encarga de bytes de relleno cuando descifra mensajes cifrados usando el modo de encadenamiento de bloques de cifrado (CBC).

Tabla 4.33: Vulnerabilidades detectadas en correo.tungurahua.gob.ec

Análisis de vulnerabilidades con NESSUS

En Nessus se crea un nuevo escaneo con una política ya existente Advanced Scan (recomendado), se ingresa las direcciones de los host a escanear, se guarda e inmediatamente empieza el análisis de vulnerabilidades.

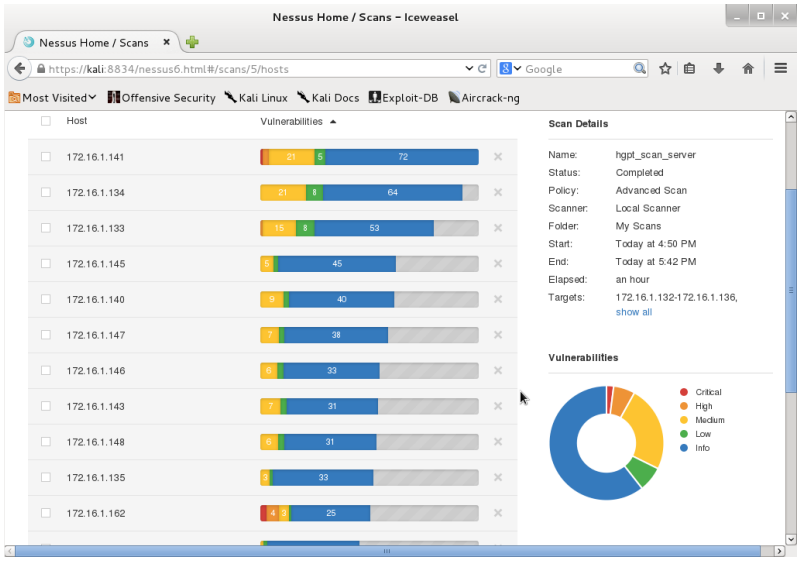

Figura 4.29: Escaneo de vulnerabilidades con Nessus

En las figuras 4.28 y 4.29 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.

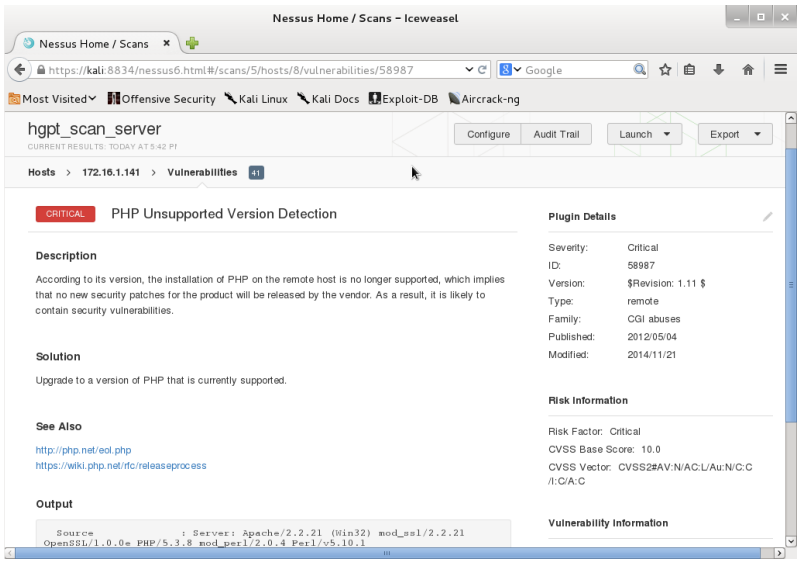

Figura 4.30: Detalle de vulnerabilidad detectada con Nessus

A continuación se detallan las vulnerabilidades detectadas con Nessus:

Servidor correo.tungurahua.gob.ec

Servicio	Vulnerabilidad	Riesgo	Observación
OpenLDAP 2.3.X	No se puede confiar en el certificado SSL	Medio	Es vulnerable a ataques man-in-the-middle contra el host remoto.
Zimbra	Versión SSL sufre de fallas criptográficas	Medio	La versión en mención sufren fallas criptográficas en conexiones remotas las cuales podrían ser descifradas por un atacante.
OpenLDAP 2.3.X	SSLv3 cifrado débil	Medio	Cifrado SSLv3 es propenso y vulnerable a divulgación de información ante el ataque de un ma-in-the-middle.
Postfix	Servidor SSL permite la autenticación anónima	Medio	El host remoto es vulnerable a divulgación de información ante el ataque de un ma-in-the-middle.

Tabla 4.34: Vulnerabilidades detectadas en gis.tungurahua.gob.ec

Servidor gis.tungurahua.gob.ec

Servicio	Vulnerabilidad	Riesgo	Observación
PostgreSQL DB (Spanish)	Cuenta PostgreSQL configuración por defecto	Alto	Es posible conectar con el servidor remoto PostgreSQL usando una cuenta por defecto.
Apache httpd	Certificado SSL no es confiable	Medio	Certificado SLL del servidor no tiene una firma de una autoridad de certificación pública conocida. Es posible un ataque man-in-the-middle contra el host remoto.
MiniServ 1.690 (Webmin httpd)	SSLv3 se ve afectado por una vulnerabilidad MitM	Medio	Se trata de una vulnerabilidad MitM en SSLv3. Desactivación de SSLv3 es la única manera de mitigar completamente la vulnerabilidad.
mDNS	Es posible obtener información sobre el host remoto.	Medio	El servicio remoto permite que cualquiera pueda descubrir la información del host remoto como su tipo de sistema operativo, versión exacta, nombre de host y la lista de servicios ejecutándose.

Tabla 4.35: Vulnerabilidades detectadas en correo.tungurahua.gob.ec

Servidor dchgpt01.lan.tungurahua.gob.ec

Servicio	Vulnerabilidad	Riesgo	Observación
Microsoft DNS	Divulgación de información del Servidor DNS	Medio	El servidor DNS remoto responde a las preguntas de los dominios de terceros. Esto podría permitir a un atacante remoto determinar qué dominios recientemente se han resuelto a través de este servidor de nombres.
Ms-wbt-server	Certificado SSL no es confiable	Medio	El certificado SSL no tiene una firma de una autoridad de certificación pública conocida. Esto podría hacer que sea más fácil de llevar a cabo ataques man-in-the-middle contra el host remoto.

Tabla 4.36: Vulnerabilidades detectadas en dchgpt01.lan.tungurahua.gob.ec

Servidor Central4760

Servicio	Vulnerabilidad	Riesgo	Observación
Apache Jserv (Protocol v1.3)	Apache Tomcat/JSP instalado con los archivos por defecto	Medio	Estos archivos pueden ayudar a obtener una información del Tomcat remoto.
ldap (Protocolo Ligero de Acceso a Directorios)	Protocolo SSL versión 2 y 3 detectado	Medio	SSL 2.0 y / o SSL 3.0 sufren de varias fallas criptográficas. Un atacante podría realizar ataques man-in-the-middle o descifrar las comunicaciones entre el servicio afectado y clientes.

Tabla 4.37: Vulnerabilidades detectadas en Central4760

Servidor mapas.tungurahua.gob.ec

Servicio	Vulnerabilidad	Riesgo	Observación
Apache httpd 2.2.15 (CentoOS)	Métodos HTTP TRACE / TRACK permitidos	Medio	Los métodos HTTP TRACE / TRACK pueden ser susceptibles a el robo de credenciales.
Apache httpd 2.2.15 (CentoOS)	Certificado SSL no es confiable	Medio	Certificado SSL no tiene una firma de una autoridad de certificación pública conocida. Esto podría hacer que sea más fácil de llevar a cabo ataques man-in-the-middle contra el host remoto.

Tabla 4.38: Vulnerabilidades detectadas en mapas.tungurahua.gob.ec

Servidor symantec.lan.tungurahua.gob.ec

Servicio	Vulnerabilidad	Riesgo	Observación
Apache httpd 2.2.21 (Win 32)	Denegación de servicio	Alto	El servicio es propenso a desbordamiento de buffer y causar una denegación de servicio.
Ms-wbt-server Microsoft Terminal Service	Debilidad de man-in-the-middle en el Protocolo Remoto de Escritorio	Alto	Escritorio remoto podría permitir la ejecución remota de código y un atacante podría enviar una secuencia de paquetes RDP y explotar la vulnerabilidad.
MySQL 5.5.16	MySQL es vulnerable a múltiples vulnerabilidades no especificadas	Medio	Vulnerabilidades no detectadas que que deben ser corregidas mediante los parches adecuados.
Symantec Messaging Gateway smtpd	Cifrado SSL contiene claves RSA menos de 2048 bits	Bajo	De acuerdo a los estándares de la industria establecidos por la Autoridad de Certificación / Navegador, los certificados emitidos después de 01 de enero 2014 deben ser de al menos 2048 bits.

Tabla 4.39: Vulnerabilidades detectadas en symantec.lan.tungurahua.gob.ec

Servidor srvap01

Servicio	Vulnerabilidad	Riesgo	Observación
Apache Tomcat/Coyote JSP engine 1.1	Certificado SSL no es confiable	Medio	El certificado SSL del servidor no tiene una firma de una autoridad de certificación pública conocida. Esto podría hacer que sea más fácil de llevar a cabo ataques man-in-the-middle contra el host remoto.
Apache Tomcat/Coyote JSP engine 1.1	SSLv3 se ve afectado por una vulnerabilidad MitM	Medio	Se trata de una vulnerabilidad SSLv3 que puede permitir ataques man-in-the-middle

Tabla 4.40: Vulnerabilidades detectadas en srvap01

Servidor SerWebCentos

Servicio	Vulnerabilidad	Riesgo	Observación
Apache httpd 2.2.3 (CentOS)	Métodos HTTP TRACE / TRACK permitidos	Medio	Los métodos HTTP TRACE / TRACK pueden ser susceptibles a el robo de credenciales.

Tabla 4.41: Vulnerabilidades detectadas en SerWebCentos

Servidor bdd_nr

Servicio	Vulnerabilidad	Riesgo	Observación
Apache httpd 2.2.15 (CentoOS)	Métodos HTTP TRACE / TRACK permitidos	Medio	Los métodos HTTP TRACE / TRACK pueden ser susceptibles a el robo de credenciales.
Apache httpd 2.2.15 (CentoOS)	Certificado SSL no es confiable	Medio	Certificado SSL no tiene una firma de una autoridad de certificación pública conocida. Esto podría hacer que sea más fácil de llevar a cabo ataques man-in-the-middle contra el host remoto.

Tabla 4.42: Vulnerabilidades detectadas en bdd_nr

Servidor HGPT-SERVERPRUE

Servicio	Vulnerabilidad	Riesgo	Observación
Oracle-tns (Oracle TNS Listener 10.2.0.3 (32 bits Windows)	Oracle Database desactualizada	Alto	De acuerdo con su versión es probable que contenga vulnerabilidades de seguridad.
Apache httpd 2.2.11 ((Win32) PHP/5.2.9-2)	Múltiples vulnerabilidades en Apache 2.2 o inferior	Alto	La versión de Apache 2.2 se ve afectada por las vulnerabilidades: 'mod_headers', 'mod_deflate' y 'mod_status'. Un atacante remoto podría provocar que el servidor consuma recursos de memoria y / o CPU significativos
Ms-wbt-server Microsoft Terminal Service	Vulnerabilidad en Escritorio remoto	Alto	Existe una vulnerabilidad en la aplicación del Protocolo de escritorio remoto (RDP). La vulnerabilidad se debe a la forma en que RDP accesa a un objeto en la memoria que se ha inicializado incorrectamente o se ha eliminado.
Apache httpd 2.2.11 ((Win32) PHP/5.2.9-2)	Métodos HTTP TRACE / TRACK permitidos	Medio	Los métodos HTTP TRACE / TRACK pueden ser susceptibles a el robo de credenciales.
Ms-wbt-server Microsoft Terminal Service	Debilidad de man-in-the-middle en el Protocolo Remoto de Escritorio	Medio	El cliente RDP no hace ningún esfuerzo para validar la identidad del servidor. Un atacante puede interceptar el tráfico desde el servidor RDP puede establecer el cifrado con el cliente y el servidor sin ser detectado.

Tabla 4.43: Vulnerabilidades detectadas en HGPT-SERVERPRUE

Servidor rrnn.tungurahua.gob.ec

Servicio	Vulnerabilidad	Riesgo	Observación
Apache httpd	Métodos HTTP TRACE / TRACK permitidos	Medio	Los métodos HTTP TRACE / TRACK pueden ser susceptibles a el robo de credenciales.
Apache httpd	Certificado SSL no es confiable	Medio	Certificado SSL no tiene una firma de una autoridad de certificación pública conocida. Esto podría hacer que sea más fácil de llevar a cabo ataques man-in-the-middle contra el host remoto.

Tabla 4.44: Vulnerabilidades detectadas en rrnn.tungurahua.gob.ec

4.11. 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

4.11.1. 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 se procede con la explotación, se realizan 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 mfsconsole 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 4.31 se puede observar lo mencionado.

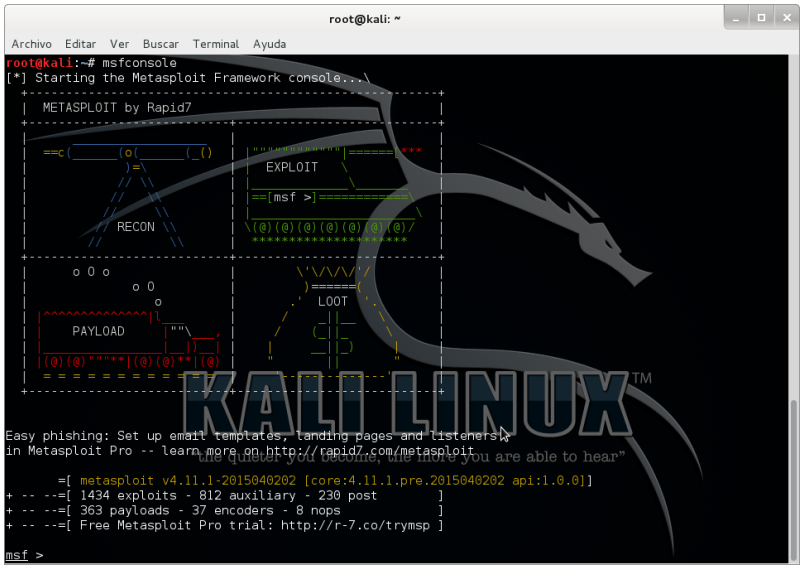

Figura 4.31: Inicio de msfconsole

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, también se realizará ataques a vulnerabilidades o fallos ya investigados en los sistemas operativos Windows junto con sus servicios.

Con el objetivo de no atentar la integridad de la red y los dispositivos del Honorable Gobierno Provincial de Tungurahua se crean equipos virtuales con similares características a los reales (ver figura 4.32), esto se lo realiza como medida de seguridad ante la probabilidad de dejar inutilizable un servidor o inaccesible un servicio.

Figura 4.32: Entorno virtualizado para explotación de vulnerabilidades.

4.11.1.1. Equipo virtual CentOS

Se crea un equipo virtual con características similares a los servidores CentOS que brindan servicios de base de datos PostgreSQL, servicio Web, FTP y con el servicio ssh ejecutándose.

- **Datos:**
  - Máquina virtual con sistema operativo kali linux con ip 172.16.1.251 (la cual llamaremos *auditor*).
  - Máquina virtual con sistema operativo CentOS 2.6.32 con ip 172.16.1.133 con instalaciones por defecto (la cual llamaremos *objetivo*).

Vulnerabilidad de configuración de PostrgreSQL por defecto.
En el proceso de instalación del motor de Base de Datos PostgreSQL 8.4.18 se crea por defecto un usuario administrador llamado **postgres**, esta cuenta no tiene defi-

nida una clave de acceso en el equipo instalado [35].

El objetivo del presente ataque es explotar la configuración por defecto del usuario **postgres**, esto se lo realiza mediante la ejecución de un auxiliar y un diccionario de datos para iniciar una sesión en el equipo remoto.

- Auxiliar auxiliary/scanner/postgres/postgres_login.
- Archivo (diccionario de datos) de usuarios y contraseñas por defecto o las más comunes.

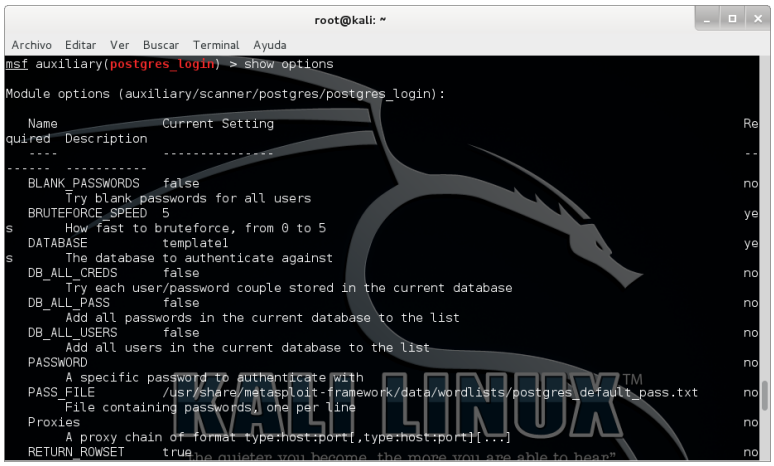

Figura 4.33: Opciones de auxiliar postgres_login

En msfconsole se selecciona el auxiliar necesario mediante,

use auxiliary/scanner/postgres/postgres_login,

el auxiliar tiene definido los archivos de usuarios y contraseñas por defecto como se observa en la figura 4.33, se ingresa como dato necesario **RHOSTS** (objetivo), una vez hecho esto se ejecuta mediante el comando **run**.

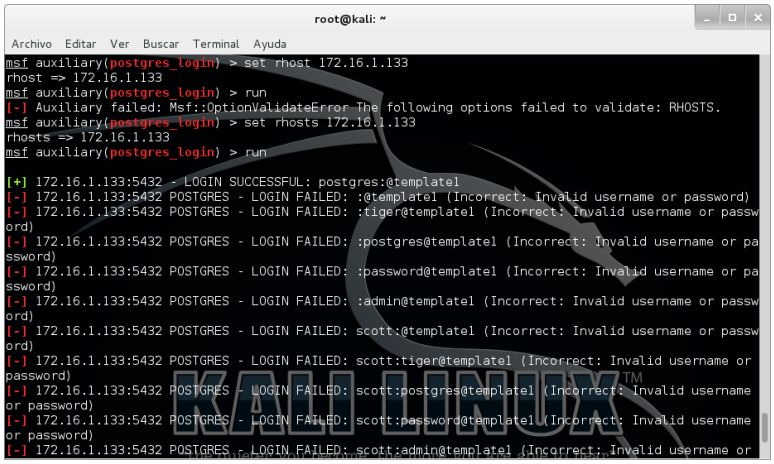

Figura 4.34: Ejecución del auxiliar postgres_login.

En la figura 4.34 se observa que se ha conseguido una conexión con la base de datos remota, una vez descubierto esto se procede a conectarse con el servidor mediante la sentencia **psql -h 172.16.1.133 -U postgres** en donde:

- **psql:** terminal interactivo de postgreSQL.
- **-h:** es la ip del servidor postgreSQL.
- **-U:** define el usuario, en este caso **postgres**.

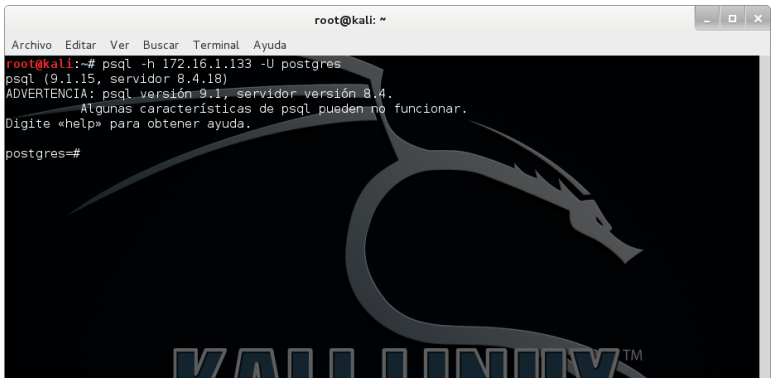

Figura 4.35: Inicio de sesión en el servidor postgreSQL

En la figura 4.35 se puede observar el éxito obtenido al iniciar sesión con el usuario administrador **postgres**, ya conectado al servidor se puede ejecutar cualquier comando **psql**.

Ataque de Denegación de Servicio (DoS).

El objetivo del ataque es provocar que el servicio que ofrece un servidor sea inaccesible mediante DoS (Denial of Service). Un ataque de este tipo provoca que servicios como SMTP, HTTP, POP3, etc. queden inoperables.

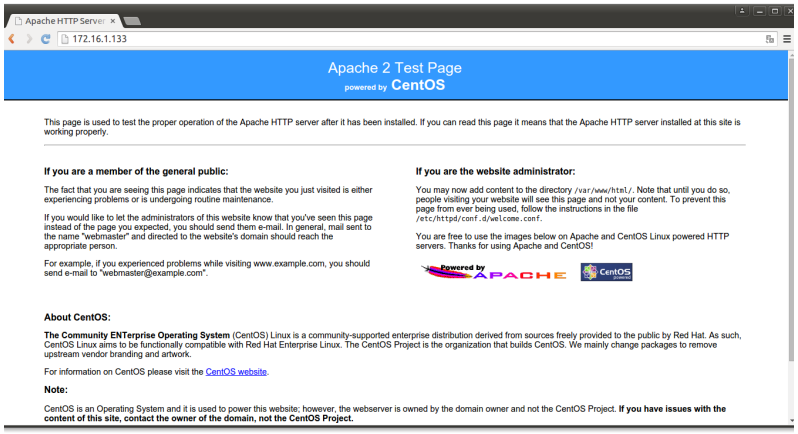

Figura 4.36: Servicio Apache en ejecutándose en el servidor CentOS.

El ataque se lo realiza al Servicio Web Apache 2.2.15 por el puerto 80 que brinda el servidor CentOS (ver figura 4.36), se utiliza **Hping3** para provocar un "request time out" mediante el envío de solicitudes a un servidor el cual se congestiona y no es capaz de responder, en el terminal de kali se ejecuta lo siguiente,

hping3 -S 172.16.1.133 –flood –rand-source -d 5000 -p 80

en donde:

- **-p:** el puerto a atacar.
- **-S:** activa el flag Syn.
- **–flood:** le indica a hping3 que envié los paquetes a la máxima velocidad posible.
- **-a:** para que la ip no sea visible.
- **–rand-source:** genera direcciones al azar

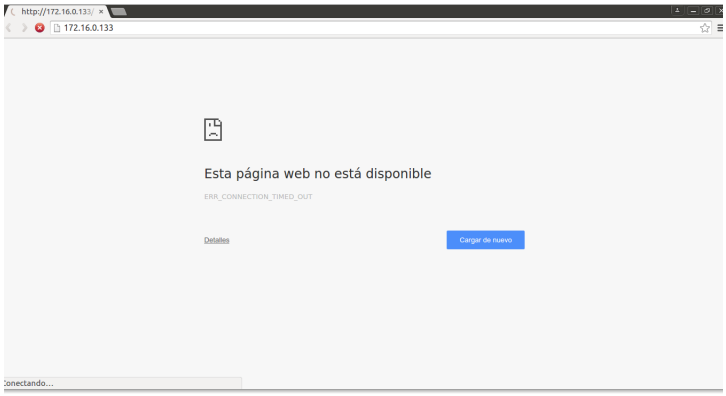

Figura 4.37: Éxito en el ataque DoS al servicio Apache en el servidor CentOS

En la figura 4.37 se aprecia el éxito del ataque DoS al servicio en mención mediante la ejecución del programa hping3 provocando que el servicio web esté inaccesible.

Ataque de fuerza bruta al Servicio OpenSSH 5.3

Uno de los ataques más comunes que se realizan son los conocidos como fuerza bruta, se intenta autentificarse en un área protegida por un nombre de usuario y contraseña mediante el método de prueba y error. Existen tres tipos de ataques siendo el más común el de uso de diccionario el cual tiene un listado de usuarios y contraseñas. Los diccionarios son creados de manera personalizada con toda la información recopilada en la sección anterior como son números de cédulas y celulares, correos, nombres, apellidos, etc.

En el terminal de kali se digita lo siguiente,

hydra -L /root/Desktop/diccionario_usuarios.txt -P /root/Desktop/diccionario_password_user.txt 172.16.0.133 ssh

en donde:

- **-L:** diccionario de nombres de usuario.
- **-P:** diccionario de contraseñas.
- **ssh:** el protocolo a atacar.

En este caso para el usuario **root** se crea una contraseña débil "**centos**".

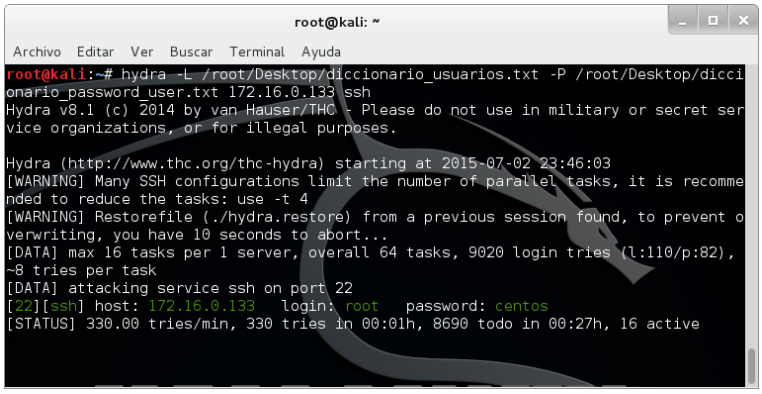

Figura 4.38: Éxito en el ataque de fuerza bruta al servicio ssh del servidor CentOS.

En la figura 4.38 se puede observar el éxito del ataque de fuerza bruta en el cual se utilizó diccionario de usuario y contraseña, esto puede llegar a ser tan sencillo como imposible según factores como el sistema al cual va dirigido el ataque, la existencia de un sistemas de detección de intrusos y por supuesto la robustez de la contraseña.

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

El Protocolo de Transferencia de Archivos tiene como objetivos, promover el intercambio de archivos, fomentar indirecta o implícita uso de equipos remotos para brindar almacenamiento de archivos entre hosts y transferir datos de forma fiable y eficiente [36].

Es muy fácil de configurar y utilizar, sin embargo debe tomarse en cuenta que su seguridad se basa sobre listas de de control de acceso compuestas por direcciones IP o nombres de anfitrión [37].

En este caso, para el ataque de fuerza bruta al servicio FTP se utiliza msfconsole junto con uno de sus auxiliares.

- Auxiliar auxiliary/scanner/ftp/ftp_login.
- Puerto de ataque 21 del servicio ftp.

En msfconsole se selecciona el auxiliar,

auxiliary/scanner/ftp/ftp_login,

el auxiliar tiene definido los archivos de usuarios y contraseñas por defecto pero se direcciona a los diccionarios de usuarios y contraseñas ya creados, cabe mencionar

que para el éxito del ataque, se configura un usuario y contraseña débiles los cuales se encuentran en los diccionarios de ataque, se ingresa como dato necesario **RHOSTS**, **USER_FILE** y **PASS_FILE,** una vez hecho esto se ejecuta mediante el comando **run**.

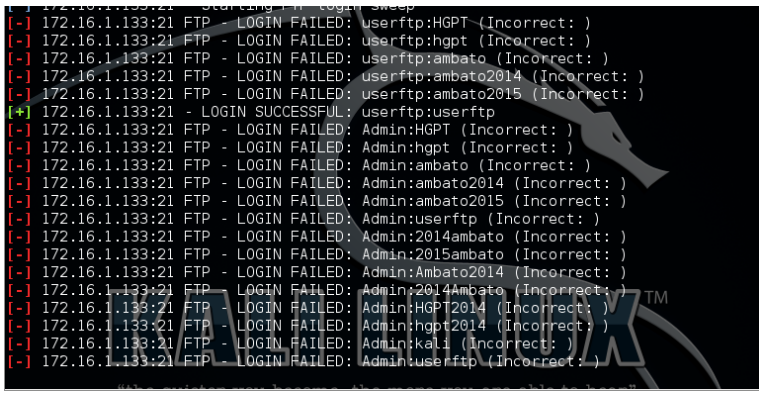

Figura 4.39: Detección de inicio de sesión en el servicio ftp.

En la figura 4.39 se observa que se ha conseguido una conexión con el servicio **ftp**, una vez descubierto esto se puede conectar al servidor y obtener acceso a los archivos protegidos por usuario y contraseña.

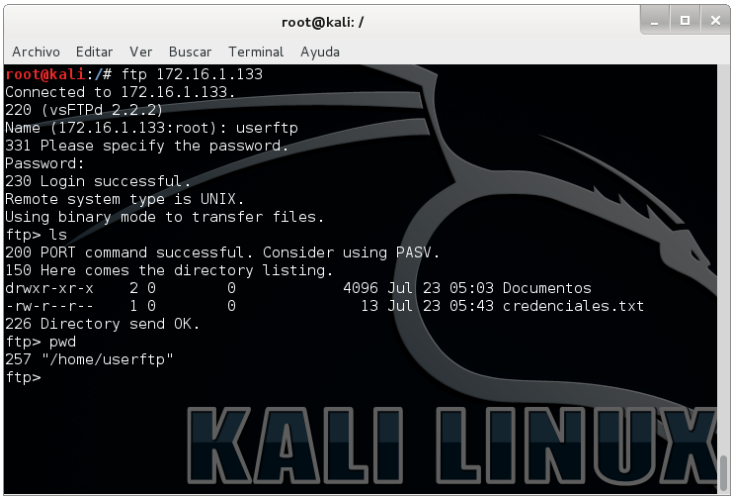

Figura 4.40: Inicio de sesión en el servidor ftp.

En la figura 4.40 se puede observar el inicio de sesión del servicio ftp obteniendo acceso a archivos del servidor CentOS.

Explotación de vulnerabilidad de desbordamiento de memoria a FTP. FTP en versiones anteriores 1.2-1.3 tienen una vulnerabilidad de desbordamiento de búffer mediante el envío de datos que contienen un gran número de comandos Telnet IAC en plataformas Linux [38].

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 sistema objetivo en caso de tener éxito en la explotación.

- Exploit exploit/linux/ftp/proftp_telnet_iac.
- Payload generic/shell_reverse_tcp.
- Puerto de ataque 21 del servicio ftp.

En msfconsole se selecciona el exploit,

exploit/linux/ftp/proftp_telnet_iac,

y el payload,

generic/shell_reverse_tcp,

se ingresa **RHOST** que viene a ser la ip objetivo, cabe mencionar que el puerto ya están definido por defecto como se observa en la siguiente imagen, una vez hecho esto se ejecuta el exploit.

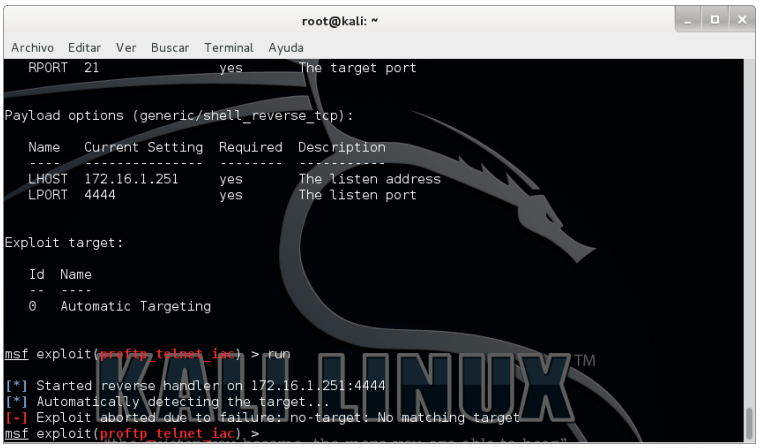

Figura 4.41: Ejecución y explotación de vulnerabilidad FTP

En la figura 4.41 se observa la ejecución del exploit junto con su payload para explotar la vulnerabilidad FTP sin tener éxito alguno, en este caso, la versión FTP instalada ya no es vulnerable a lo detallado con anterioridad.

4.11.1.2. Equipo virtual Windows

Se crea un equipo virtual Windows XP con las 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 172.16.1.251 (la cual llamaremos *auditor*).
  - Máquina virtual con sistema operativo Windows XP SP3 con ip 172.16.1.247 (la cual llamaremos *objetivo*).

Explotación de vulnerabilidad en el servicio SMB.
Microsoft publicó 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 de Microsoft [39].

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 XP, 7 y Server 2003 tienen una vulnerabilidad que afecta al servicio en mención y se cuentan con exploit públicos para su explotación[39].

- Exploit windows/smb/ms08_067_netapi.
- Payload windows/meterpreter/reverse_tcp.
- Puerto de ataque 445 de servicio SMB.

En msfconsole se selecciona el exploit,

windows/smb/ms08_067_netapi,

y el payload,

windows/meterpreter/reverse_tcp,

se ingresa los datos necesarios como son **RHOST** y **LHOST** que vienen a ser la ip objetivo e ip del auditor respectivamente, cabe mencionar que los puertos tanto como el del servicio **SMB** y el puerto de escucha del auditor ya están definidos por defecto como se puede observar en la figura 4.42, una vez hecho esto se ejecuta mediante el comando **exploit**.

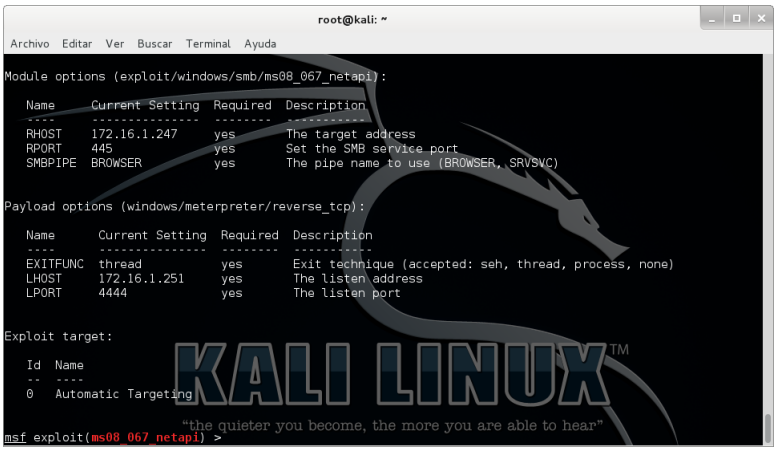

Figura 4.42: Ejecución de exploit de vulnerabilidad SMB.

En este caso, la explotación de la vulnerabilidad ha sido un éxito logrando establecer una sesión meterpreter con el sistema objetivo.

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 se elige uno que pueda seguir ejecutándose con normalidad, uno del sistema por ejemplo (PID 592 proceso winlogon).

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

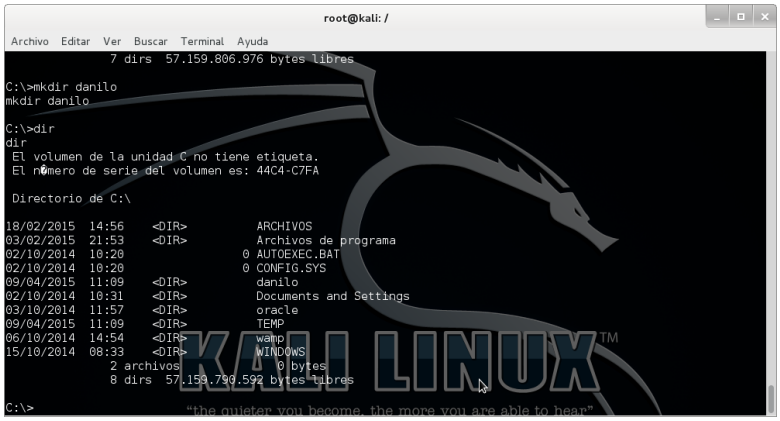

Figura 4.43: Ejecución de shell en el sistema comprometido

En la figura 4.43 se observa la ejecución de comandos CMD del equipo comprometido, en este caso se crea una carpeta con el nombre **danilo** y se lista el contenido del directorio actual.

Explotación de vulnerabilidad en Remote Desktop Protocol.
Microsoft publicó un aviso de seguridad en donde advierte sobre una vulnerabilidad que afecta a Remote Desktop Protocol, la vulnerabilidad reside en la forma de que RDP manipula los paquetes que recibe mediante una conexión. RDP es un protocolo desarrollado por Microsoft que permite la comunicación en la ejecución de una aplicación entre un terminal y un servidor Windows [39].

El objetivo de este ataque es aprovechar la vulnerabilidad de Microsoft RDP y producir un error del sistema el cual provoque la conocida "pantalla azul de la muerte".

- Auxiliar /dos/windows/rdp/ms12_020_maxchannelods.
- Puertos de ataque 3389 de servicio RDP.

En msfconsole se selecciona el auxiliar,

/dos/windows/rdp/ms12_020_maxchannelods,

se ingresa **RHOST** que viene a ser la ip objetivo, cabe mencionar que el puerto del protocolo RDP ya están definido por defecto como se observa en la figura 4.44 , una vez hecho esto se ejecuta mediante el comando **run**.

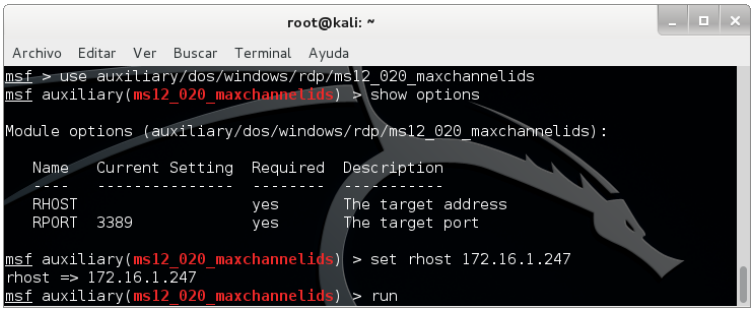

Figura 4.44: Ejecución y explotación de vulnerabilidad RDP

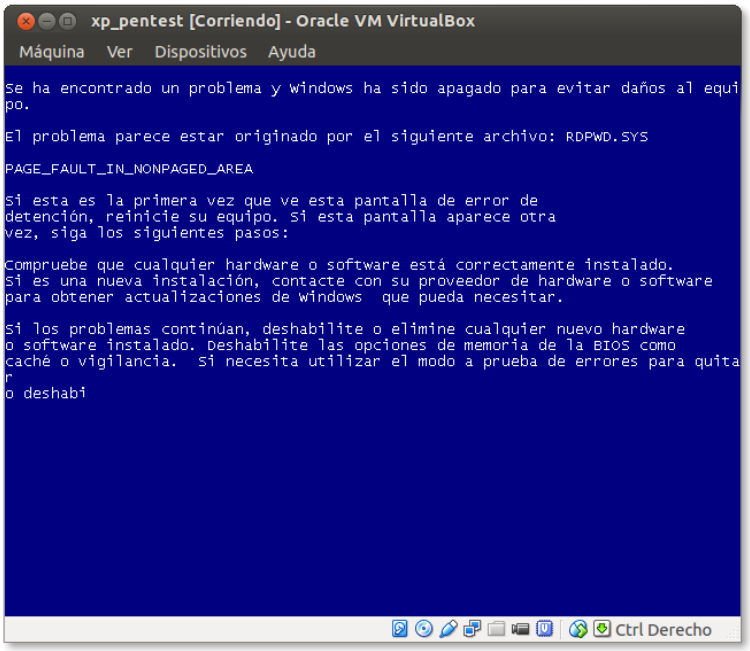

Figura 4.45: Éxito en explotación de vulnerabilidad RDP

En la figura 4.45 se observa el éxito de la explotación de la vulnerabilidad RDP el cual provoca una pantalla azul notificando que se ha encontrado un problema originado por el archivo RDPWD.SYS seguidamente de un reinicio del sistema operativo.

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.

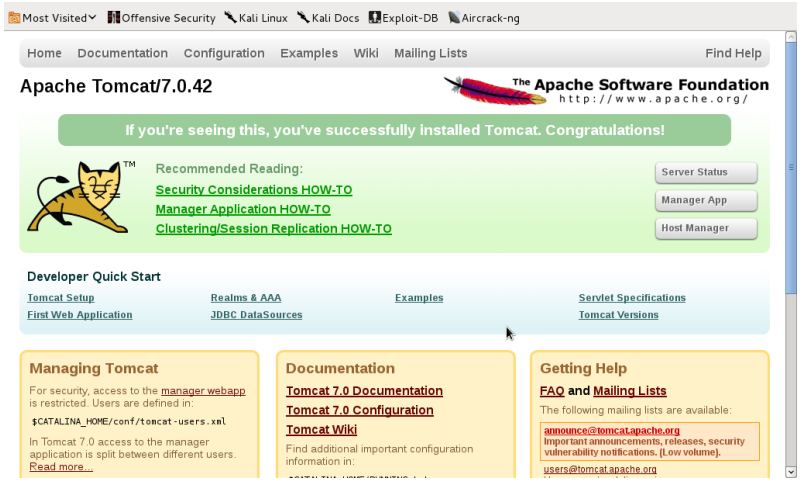

Figura 4.46: Vista del servicio Apache Tomcat

En la figura 4.46 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 Servicio (DoS).
El objetivo del ataque es provocar que el servicio que ofrece un servidor sea inaccesible mediante DoS (Denial of Service). Un ataque de este tipo provoca que servicios como SMTP, HTTP, POP3, etc. queden inoperables.

Se utiliza para provocar un "request time out" mediante el envío de solicitudes a un servidor el cual se congestiona y no es capaz de responder.

hping3 -S 172.16.1.247 –flood –rand-source -d 5000 -p 80

- **-p:** el puerto a atacar.
- **-S:** activa el flag Syn.
- **–flood** le 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

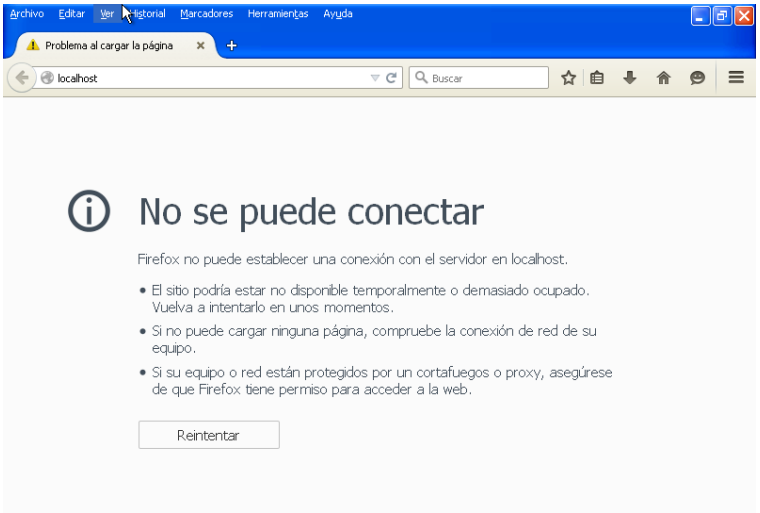

Figura 4.47: Éxito en el ataque DoS al servicio web.

En la figura 4.47 se aprecia el éxito de la ejecución de hping3 provocando que el servicio web esté inaccesible.

Explotación de vulnerabilidad del servicio msrpc RPC.
La vulnerabilidad del servicio RPC (Remote Procedure Call) podría representar una amenaza seria de la seguridad, la explotación exitosa de la vulnerabilidad en el servicio de un sistema Windows podrían permitir la ejecución de código remoto. La vulnerabilidad afecta a las versiones Windows 2000, XP y Windows Server 2003[28]. RPC es un protocolo de red que permite a un programa de computadora ejecutar código en otra máquina remota sin tener que preocuparse por las comunicaciones entre ambas[39].

El objetivo de este ataque es tratar de iniciar una sesión mediante la explotación de la vulnerabilidad que presenta el servicio **RPC** de Windows, este ataque es viable debido a que el sistema operativo Windows cuenta con una vulnerabilidad que afecta al servicio en mención y se cuentan con exploit públicos para su explotación[28].

- Exploit exploit/windows/dcerpc/ms03_026_dcom, exploit/windows/dcerpc/ms05_017_msmq.
- Payload generic/shell_bind_tcp, win32_reverse_meterpreter.
- Puerto de ataque 135 de servicio msrpc RPC.

En msfconsole se selecciona el exploit,

windows/dcerpc/ms03_026_dcom

y el payload

windows/meterpreter/reverse_tcp,

se ingresa los datos de **RHOST**, cabe mencionar que el puerto del servicio **msrpc RPC** está definido por defecto, una vez hecho esto se ejecuta mediante el comando **exploit**.

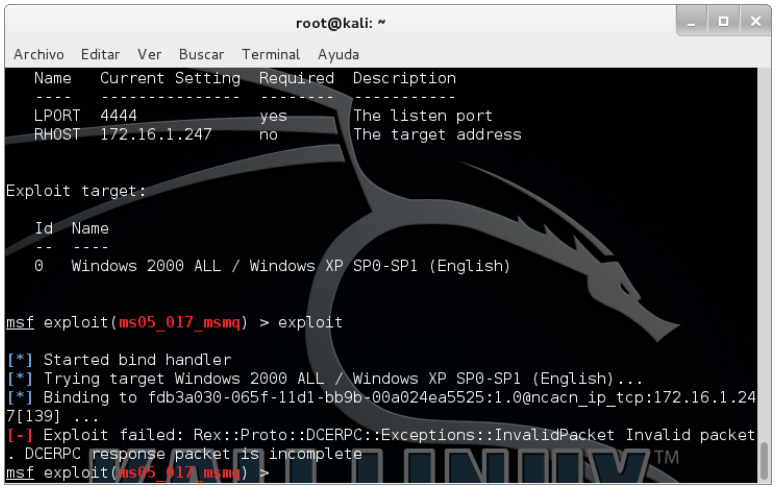

Figura 4.48: Ejecución del exploit dirigido al servicio rpc.

En la figura 4.48 se puede observar que el exploit se ejecuta sin ningún éxito ante el sistema operativo objetivo, en este caso las versiones superiores a Windows 2000 y XP SP1 ya no son vulnerables.

4.11.1.3. Equipo virtual Ubuntu

Se crea un equipo virtual Ubuntu 14.04. LTS para verificar la vulnerabilidad MITM, 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.

Ante la vulnerabilidad de "Certificado SSL no es confiable" considerada con 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.

Certificados SSL

Un certificado SSL es un archivo que contiene un código de seguridad que permite encriptar el tráfico de un sitio web entre un servidor y un usuario final, el tráfico web es transmitido usando el protocolo HTTPS que es el protocolo HTTP estándar encapsulado con encriptación de capas de socket seguro, asegura que la información no se transmita en texto plano. En febrero 2009, conferencia Sombrero Negro realizada en Washintong DC, se presenta la herramienta de software sslstrip diseñado para eliminar la protección SSL de los sitios web, dicho programa intercepta conexiones entre un navegador web y un sitio de confianza y presentar la información sin cifrado SSL (la página web se carga sin SSL "HTTP"). Sslstrip no demuestra una debilidad en el cifrado SSL sino que se aprovecha de los usuarios que no toman en cuenta el cifrado de confianza SSL[40].

- **Datos:**
  - Máquina virtual con sistema operativo kali linux con ip 172.16.1.251 (la cual llamaremos *auditor*).
  - Máquina virtual con sistema operativo Ubuntu 14.04 con ip 172.16.1.136 con instalaciones por defecto (la cual llamaremos *objetivo*).

Ataque Man-in-the-middle

MITM (Man-InThe-Middle), este ataque permite interceptar la señal del emisor (ver figura 4.49), controlar, insertar e incluso modificar las señales y enviarlas al receptor, el ataque es dirigido al protocolo ARP con el objetivo de observar los mensajes entre dos víctima [41].

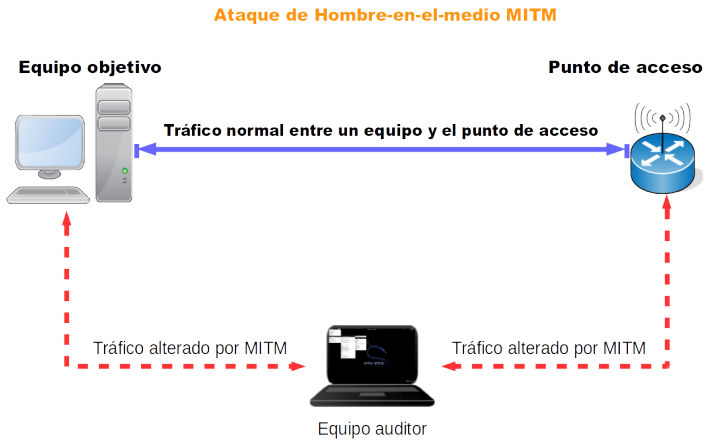

Figura 4.49: Diagrama de ataque de Man-in-the-Middle.

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:

iptables -t nat -A PREROUTING -tcp –destination-port 80 -j REDIRECT –to-por 16000,

la regla anterior permite que las solicitudes al puerto 80 sean redireccionadas al puerto 16000, para empezar a descifrar el tráfico del puerto 16000 se digita **sslstrip -l 16000** (ver figura 4.32).

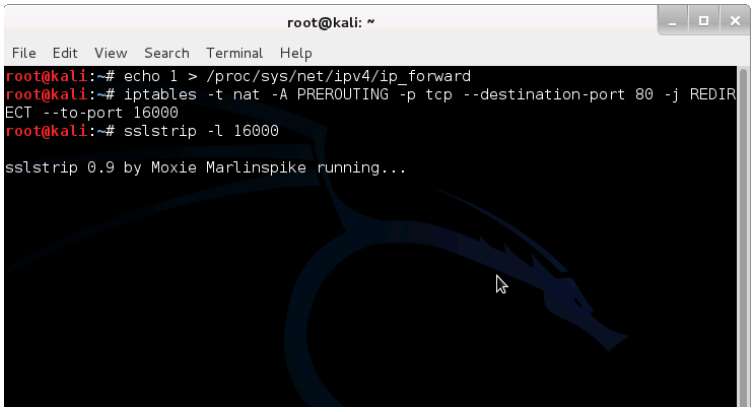

Figura 4.50: Configuración de ruteo e iptables.

Iniciado **ettercap**, se elige el envenenamiento ARP, **Sniff** > **Unified Sniff** en la barra de menú con la tarjeta de red respectiva.
Mediante el escaneo de hosts se elige la ip objetivo (TARGET1) y la puerta de enlace (TARGET2), luego se procede al envenenamiento ARP e iniciar escuchar (sniffing) la red.

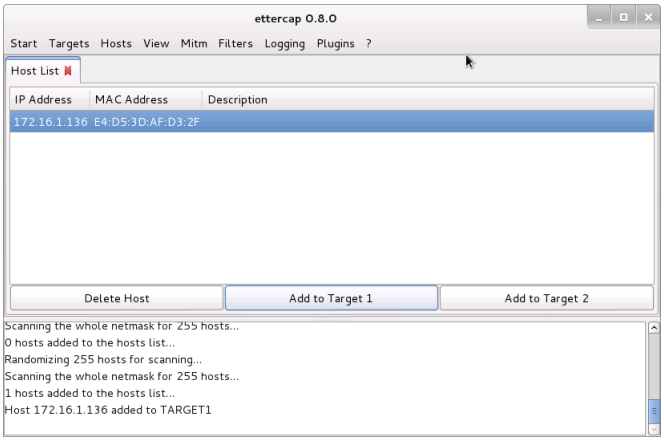

Figura 4.51: Selección de ip a escuchar (sniffing)

En la figura 4.51 se observa la herramienta Ettercap seleccionado el equipo objetivo y añadiéndolo como TARGET1.
En el equipo objetivo se ingresa a sitios web seguros como son gmail, yahoo y msn, también a sitios sin certificados SSL.

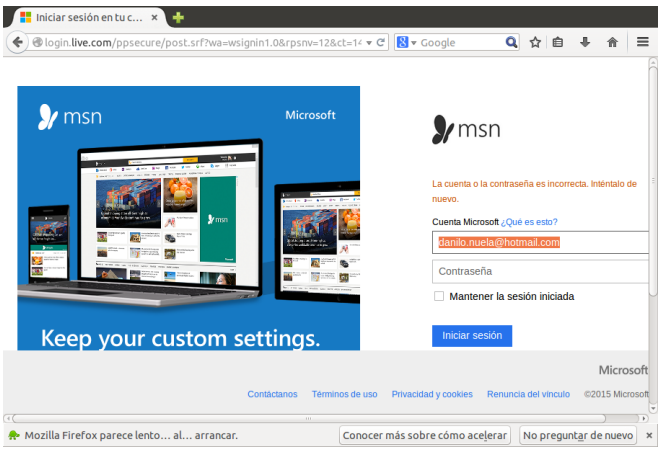

Figura 4.52: Inicio de sesión en un ordenador envenenado

En la figura 4.52 se observa el ingreso de credenciales en un sitio de confianza desde el navegador web Firefox.

En el equipo auditor se puede observar la información capturada del equipo objetivo mediante **Ettercap**, ver figura 4.53.

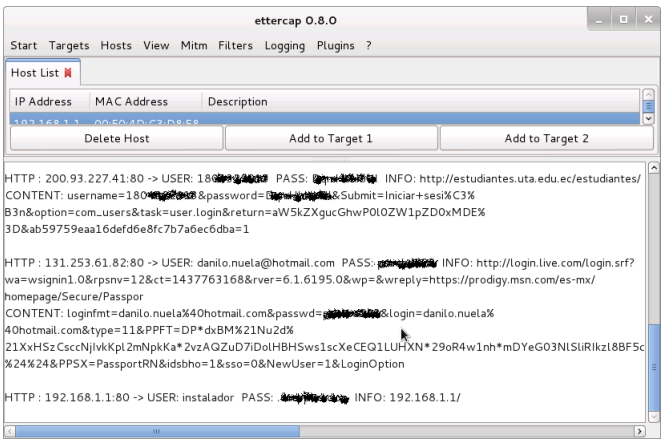

Figura 4.53: Captura del tráfico y obtención de credenciales en ettercap

Como se puede observar en la figura 4.53, se han realizado capturas de paquetes de un sitio seguro y de dos inseguros dando como resultados credenciales las cuales fueron ingresados por el usuario en el navegador Firefox del equipo objetivo.
Cabe aclarar que cada navegador web tiene sus propias características de seguridad internas y gestiona los aspectos de protección avanzados, se realiza la misma prueba con los navegadores Chrome e Internet Explorer.

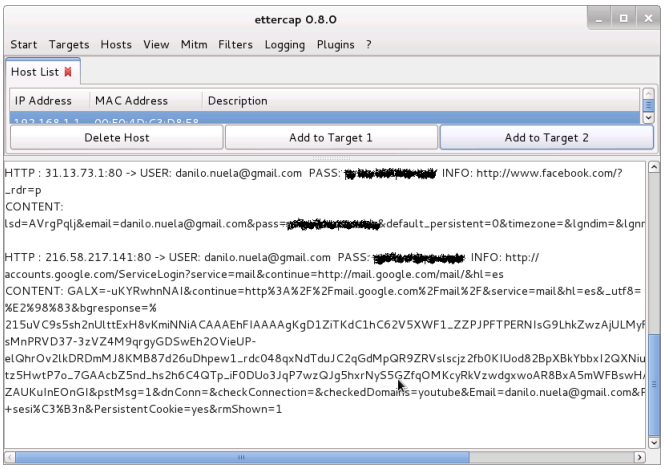

Figura 4.54: Captura del tráfico y obtención de credenciales en ettercap IE

En la figura 4.54 se observa la captura de paquetes de sitios de confianza como son gmail y facebook obteniendo así las credenciales ingresadas por el usuario en un

navegador Internet Explorer, se puede concluir que los navegadores Firefox y Chrome son más seguros al momento de navegar ya que los mismos exigen un certificado de seguridad e incluso no se conectan si no se cuenta con un certificado de seguridad.

4.11.2. Resumen de explotación de vulnerabilidades

Sistema Operativo	Versión	Vulnerabilidad	Explotable	Observación
Windows XP	Service Pack 1	MS06-030, Servicio SMB	Si	Existe actualización de seguridad que cubre varias vulnerabilidades como la del servicio SMB y la de provocar denegación de servicio (DoS).
		MS06-031, Servicio msrpc RPC	Si	
		MS12-020, Microsoft RDP	Si	
		MS08-067, Servicio en solicitud RPC	Si	
	Service Pack 2	MS06-030, Servicio SMB	Si	
		MS12-020, Microsoft RDP	Si	
		MS06-031, Servicio msrpc RPC	No	
		MS08-067, Servicio en solicitud RPC	No	
	Service Pack 3	MS06-030, Servicio SMB	No	
		MS12-020, Microsoft RDP	Si	
		MS06-031, Servicio msrpc RPC	No	
		MS08-067, Servicio en solicitud RPC	No	
Windows Server	2003	MS06-030, Servicio SMB	No	Existe actualización de seguridad que cubre varias vulnerabilidades como la del servicio SMB, desbordamiento de memoria y la de provocar denegación de servicio (DoS).
		MS12-020, Microsoft RDP	Si	
		MS06-031, Servicio msrpc RPC	No	
		MS08-067, Servicio en solicitud RPC	No	
	2008	MS06-030, Servicio SMB	No	
		MS12-020, Microsoft RDP	Si	
		MS06-031, Servicio msrpc RPC	No	
	2012	MS06-030, Servicio SMB	No	
		MS12-020, Microsoft RDP	No	
		MS06-031, Servicio msrpc RPC	No	
Windows 7	Profesional	MS06-030, Servicio SMB	No	Existe actualización de seguridad que cubre varias vulnerabilidades como la del servicio SMB.
		MS12-020, Microsoft RDP	Si	
		MS06-031, Servicio msrpc RPC	No	
Linux	Centos 2.6.32	Divulgación de información	Si	Las instalaciones por defecto puede divulgar información delicada del sistema o servidor.
	Ubuntu 14.04	Divulgación de información	Si	

Tabla 4.45: Resumen de vulnerabilidades explotables

Servicio	Sistema Operativo	Ataque	Explotable
PostgreSQL 8.4.18	CentOS 2.6.32	Cuenta PostgreSQL por defecto	Si
OpenSSH 5.3	CentOS 2.6.32	Fuerza Bruta	Si
Apache Web Server	CentOS 2.6.32	Divulgación de información	Si
Apache Web Server	Windows XP SP3	Divulgación de información	Si
Protocolo de Transferencia de Archivo FTP	CentOS 2.6.32	Fuerza Bruta	Si
Protocolo de Transferencia de Archivo FTP	Ubuntu 14.04	Fuerza Bruta	Si
Apache Web Server	CentOS 2.6.32	Denegación de Servicio DoS	Si
Apache Web Server	Windows XP SP3	Denegación de Servicio DoS	Si
Protocolo de Transferencia de Archivo FTP	CentOS 2.6.32	Desbordamiento de Memoria	No
Protocolo de Transferencia de Archivo FTP	Ubuntu 14.04	Desbordamiento de Memoria	No
Navegador Internet Explorer	Windows XP SP3	Man-In-The-Middle	Si
Navegador Firefox	CentOS 2.6.32	Man-In-The-Middle	No
Navegador Firefox	Ubuntu 14.04	Man-In-The-Middle	No
Navegador Internet Explorer	Windows 7 Profesional	Man-In-The-Middle	Si
Apache Web Server	Windows Server 2003	Denegación de Servicio DoS	Si
Apache Web Server	Windows Server 2008	Denegación de Servicio DoS	Si
Apache Web Server	Windows Server 2012	Denegación de Servicio DoS	Si

Tabla 4.46: Resumen de servicios explotados

4.12. Elaboración de Políticas de Contingencia de Seguridad Informática que mejoren la integridad, confidencialidad y disponibilidad de la información en base a las vulnerabilidades detectadas

4.12.1. Documentación de los estados de inseguridad detectados e incluyendo soluciones prácticas orientadas a resolverlos

A continuación se documentan de manera más detallada las vulnerabilidades detectadas en los servidores institucionales incluyendo la posible solución para proteger los activos de la Red Informática del Honorable Gobierno Provincial de Tungurahua ante los daños y perjuicios que puedan ser causados por la explotación exitosa de dichas vulnerabilidades.

- **Servidor symantec.lan.tungurahua.gob.ec**

Vulnerabilidad: Denegación de servicio a Apache httpd
Riesgo: Alto
Descripción: Una explotación exitosa podría permitir a atacantes ejecutar código arbitrario y los intentos fallidos probablemente resultará en condiciones de denegación de servicio.
Código CVE: CVE-2012-2688
Fecha de publicación: 04/05/2012
Explotado: Si
Solución: Actualizar a PHP 5.4.5 o posterior
Referencias:
URL:http://www.php.net/ChangeLog-5.php
URL:http://en.securitylab.ru/nvd/427456.php

Vulnerabilidad: Escritorio remoto podría permitir la ejecución remota de código
Riesgo: Alto
Descripción: Existe una vulnerabilidad remota de código arbitrario en la aplicación del Protocolo de Escritorio Remoto (RDP). La vulnerabilidad se debe a la forma en que RDP accede a un objeto en la memoria que se ha inicializado incorrectamente o se ha eliminado. Un atacante remoto no autenticado podría aprovechar esta vulnerabilidad para provocar que el sistema para ejecutar código arbitrario mediante el envío de una secuencia de paquetes RDP especialmente diseñados para ello.

Código CVE: CVE-2012-0002, CVE-2012-0152
Fecha de publicación: 03/13/2012
Explotado: Si
Solución: Microsoft ha publicado un conjunto de parches para Windows XP, 2003, Vista, 2008, 7 y 2008 R2.
Referencias:
http://technet.microsoft.com/en-us/security/bulletin/ms12-020

Vulnerabilidad: Apache mod_info / server-info Divulgación de Información
Riesgo: Medio
Descripción: Es posible obtener una visión general de la configuración del servidor web remoto Apache mediante la solicitud de la URL "/ server-info '. Este resumen incluye información como módulos instalados, su configuración y los ajustes de tiempo de ejecución surtidos.
Código CVE:
Fecha de publicación: 28/05/2001
Explotado: Si
Solución: Actualizar el archivo de configuración de Apache y desactivar mod_info o asegurarse de que el acceso está limitado a usuarios válidos.
Referencias:
http://httpd.apache.org/docs/mod/mod_info.html

Vulnerabilidad: Múltiples vulnerabilidades (Man in the Middle)
Riesgo: Medio
Descripción: El servidor web remoto utiliza una versión de OpenSSL 1.0.0 o inferior. La biblioteca OpenSSL está afectada por varias vulnerabilidades.
Código CVE: CVE-2014-3569, CVE-2014-3570, CVE-2014-3571, CVE-2014-3572, CVE-2014-8275, CVE-2015-0204, CVE-2015-0205, CVE-2015-0206.
Fecha de publicación: 21/10/2014
Explotado: Si
Solución: Actualizar OpenSSL posterior a 1.0.0p.
Referencias:
https://www.openssl.org/news/openssl-1.0.0-notes.html
https://www.openssl.org/news/secadv_20150108.txt

https://www.openssl.org/news/vulnerabilities.html

Vulnerabilidad: Detección de versión PHP no compatible
Riesgo: Alto
Descripción: De acuerdo con su versión, la instalación de PHP en el host remoto ya no es compatible, lo que implica que no hay nuevos parches de seguridad para el producto por el proveedor. Como resultado, es probable que contenga vulnerabilidades de seguridad.
Código CVE:
Fecha de publicación: 04/05/2012
Explotado: Si
Solución: Actualizar a una versión de PHP que se soporta actualmente
Referencias:
http://php.net/eol.php
https://wiki.php.net/rfc/releaseprocess

Vulnerabilidad: Apache 2.2 <2.2.28 Múltiples vulnerabilidades
Riesgo: Alto
Desrcipción: De acuerdo con la versión de Apache 2.2 instalado en el host remoto, es anterior a la 2.2.28. Está, por lo tanto, afectada por las vulnerabilidades: CVE-2014-0.118, CVE-2014-0226 y CVE-2.014-0231. Tenga en cuenta que Nessus no ha probado para estas cuestiones, sino que se ha basado únicamente en el número de versión de auto-reporte de la aplicación.
Código CVE: CVE-2013-5704, CVE-2014-0118, CVE-2014-0226, CVE-2014-0231
Fecha de publicación: 04/09/2014
Explotado: No
Solución: Actualizar a Apache versión 2.2.29 o posterior.
Referencias:
http://www.apache.org/dist/httpd/CHANGES_2.2.29
http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerabilidad: MySQL Múltiples vulnerabilidades no especificadas (Windows)
Riesgo: Alto
Desrcipción: Es posible obtener una visión general de la configuración del servidor web remoto. Este resumen incluye información como módulos instalados,

su configuración y los ajustes de tiempo de ejecución surtidos..
Código CVE: CVE-2014-6559, CVE-2014-6555, CVE-2014-6507, CVE-2014-6500
Fecha de publicación: 02/10/2014
Explotado: Si
Solución: Revise los archivos y eliminar los que no son necesarios.
Referencias:
http://www.osvdb.com/113259
http://secunia.com/advisories/60599

- **Servidor Central4760**

Vulnerabilidad: Apache Tomcat servlet / archivos predeterminados
Riesgo: Medio
Descripción: Ejemplo JSP y servlets se instalan en el servlet contenedor remoto Apache Tomcat / JSP. Estos archivos deben ser removidos ya que pueden ayudar a divulgar información a un atacante acerca de Tomcat.
Código CVE:
Fecha de publicación: 02/03/2004
Explotado: Si
Solución: Revisar los archivos y eliminar los que no son necesarios.
Referencias:
http://cwe.mitre.org/data/definitions/442
http://cwe.mitre.org/data/definitions/864

Vulnerabilidad: SSL Versión Detección 2 y 3 del Protocolo
Riesgo: Medio
Descripción: El servicio remoto acepta conexiones cifradas mediante SSL 2.0 y / o SSL 3.0, que al parecer sufren de varios defectos criptográficas. Un atacante podría ser capaz de aprovechar estas cuestiones para realizar ataques man-in-the-middle o descifrar las comunicaciones entre el servicio afectado y los clientes.
Código CVE:
Fecha de publicación:
Explotado: No
Solución: Consulte la documentación de la aplicación para deshabilitar SSL 2.0 y 3.0. Usar TLS 1.0 o superior en su lugar.

Referencias:
http://support.microsoft.com/kb/187498
http://www.linux4beginners.info/node/disable-sslv2

- **Servidor rrnn.tungurahua.gob.ec**

Vulnerabilidad: Vulnerabilidades de cadena de formato remoto múltiple
Riesgo: Alto
Descripción: El anfitrión se está ejecutando el servicio statd y es propenso a múltiples vulnerabilidades de cadena de formato a distancia. Una explotación exitosa podría permitir a atacantes ejecutar código arbitrario con los privilegios del proceso rpc.statd, normalmente root.
Código CVE: CVE-2000-0666, CVE-2000-0800
Fecha de publicación:
Explotado: No
Solución: Actualizar a la última versión de nfs-utils 0.1.9.1 o posterior
Referencias:
http://www.cert.org/advisories/CA-2000-17.html
http://www.iss.net/security_center/reference/vuln/RPC_Statd_Format_Attack →.htm

Vulnerabilidad: Apache httpd Métodos HTTP TRACE / TRACK permitidos
Riesgo: Medio
Descripción: El servidor web remoto es compatible con los métodos TRACE / TRACK. Son métodos HTTP que se utilizan para las conexiones del servidor de depuración web.
Código CVE: CVE-2003-1567, CVE-2004-2320, CVE-2010-0386
Fecha de publicación: 23/01/2003
Explotado: No
Solución: Deshabilitar estos métodos. Consulte la salida de plug-in para más información.
Referencias:
http://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf
http://www.apacheweek.com/issues/03-01-24
http://download.oracle.com/sunalerts/1000718.1.html

Vulnerabilidad: Certificado SSL no es confiable
Riesgo: Medio
Descripción: Certificado X.509 del servidor no tiene una firma de una autoridad de certificación pública conocida. Si la máquina remota es un anfitrión pública en la 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 de llevar a cabo ataques man-in-the-middle contra el host remoto.
Código CVE:
Fecha de publicación: 15/12/2010
Explotado: No
Solución: Comprar o generar un certificado adecuado para este servicio.
Referencias:

Vulnerabilidad: Detección de versión del Protocolo SSL 2 y 3
Riesgo: Medio
Descripción: El servicio remoto acepta conexiones cifradas mediante SSL 2.0 y / o SSL 3.0, que al parecer sufren de varios defectos criptográficas. Un atacante podría ser capaz de aprovechar estas cuestiones para realizar ataques man-in-the-middle o descifrar las comunicaciones entre el servicio afectado y los clientes.
Código CVE:
Fecha de publicación:
Explotado: No
Solución: Consultar la documentación de la aplicación para deshabilitar SSL 2.0 y 3.0. Usar TLS 1.0 o superior en su lugar.
Referencias:
http://support.microsoft.com/kb/187498
http://www.linux4beginners.info/node/disable-sslv2

- **Servidor correo.tungurahua.gob.ec**

Vulnerabilidad: Certificado SSL no es confiable
Riesgo: Medio
Descripción: Certificado X.509 del servidor no tiene una firma de una autoridad de certificación pública conocida. Si la máquina remota es un anfitrión pública en la 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 de llevar a cabo ataques man-in-the-middle contra el host remoto.
Código CVE:
Fecha de publicación: 15/12/2010
Explotado: No
Solución: Comprar o generar un certificado adecuado para este servicio.
Referencias:

Vulnerabilidad: Vulnerabilidad de cifrado degradado (POODLE)
Riesgo: Medio
Descripción: El host remoto se ve afectado por una vulnerabilidad MitM conocido como POODLE. La vulnerabilidad se debe a la forma en que SSL 3.0 se encarga de bytes de relleno cuando descifra mensajes cifrados usando el modo de encadenamiento de bloques de cifrado (CBC).
Código CVE: CVE-2014-3566
Fecha de publicación: 14/10/2014
Explotado: No
Solución: Servicios que deben soportar SSLv3 debería permitir que el mecanismo de TLS o desactivar completamente SSL 3.0 en el lado del cliente y el servidor.
Referencias:
https://www.imperialviolet.org/2014/10/14/poodle.html
https://www.openssl.org/~bodo/ssl-poodle.pdf
https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00

Vulnerabilidad: Detección de versión del Protocolo SSL 2 y 3
Riesgo: Medio
Descripción: El servicio remoto acepta conexiones cifradas mediante SSL 2.0 y / o SSL 3.0, que al parecer sufren de varios defectos criptográficas. Un atacante podría ser capaz de aprovechar estas cuestiones para realizar ataques man-in-the-middle o descifrar las comunicaciones entre el servicio afectado y los clientes.
Código CVE:
Fecha de publicación:
Explotado: No
Solución: Consultar la documentación de la aplicación para deshabilitar SSL 2.0 y 3.0. Usar TLS 1.0 o superior en su lugar.

Referencias:
http://support.microsoft.com/kb/187498
http://www.linux4beginners.info/node/disable-sslv2

Vulnerabilidad: Certificado SSL autofirmado
Riesgo: Medio
Descripción: La cadena de certificados X.509 para este servicio no está firmado por una autoridad de certificación reconocida. Si la máquina remota es un anfitrión pública en la producción, esto anula el uso de SSL como cualquiera podría establecer un ataque man-in-the-middle contra el host remoto.
Código CVE:
Fecha de publicación: 17/01/2012
Explotado: No
Solución: Comprar o generar un certificado adecuado para este servicio
Referencias:

- **Servidor gis.tungurahua.gob.ec**

Vulnerabilidad: Cuenta PostgreSQL por defecto
Riesgo: Alto
Descripción: Es posible conectarse al servidor de base de datos PostgreSQL remota usando una cuenta por defecto. Esto podría permitir a un atacante lanzar nuevos ataques contra la base de datos.
Código CVE: CVE-1999-0508
Fecha de publicación: 17/07/1999
Explotado: Si
Solución: Acceder a este host y establecer una contraseña para todas las cuentas afectadas utilizando el comando 'ALTER USUARIO.
Además, configure el servicio mediante la edición del archivo 'pg_hba.conf' para requerir una contraseña de autenticación para todos los hosts remotos que tengan acceso legítimo a este servicio y para requerir una contraseña localmente usando la línea "local all password'.
Referencias:
http://www.tenable.com/plugins/index.php?view=single&id=51192

Vulnerabilidad: Certificado SSL no es confiable
Riesgo: Medio
Descripción: Certificado X.509 del servidor no tiene una firma de una autoridad de certificación pública conocida. Si la máquina remota es un anfitrión pública en la 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 de llevar a cabo ataques man-in-the-middle contra el host remoto.
Código CVE:
Fecha de publicación: 15/12/2010
Explotado: Si
Solución: Comprar o generar un certificado adecuado para este servicio.
Referencias:

Vulnerabilidad: Detección de versión del Protocolo SSL 2 y 3
Riesgo: Medio
Descripción: El servicio remoto acepta conexiones cifradas mediante SSL 2.0 y / o SSL 3.0, que al parecer sufren de varios defectos criptográficas. Un atacante podría ser capaz de aprovechar estas cuestiones para realizar ataques man-in-the-middle o descifrar las comunicaciones entre el servicio afectado y los clientes.
Código CVE:
Fecha de publicación:
Explotado: Si
Solución: Consultar la documentación de la aplicación para deshabilitar SSL 2.0 y 3.0. Usar TLS 1.0 o superior en su lugar.
Referencias:
http://support.microsoft.com/kb/187498
http://www.linux4beginners.info/node/disable-sslv2

Vulnerabilidad: Obtención de información mDNS (Red remota)
Riesgo: Medio
Descripción: El servicio remoto entiende la Bonjour (también conocido como ZeroConf o mDNS) protocolo, permite que cualquiera pueda descubrir la información del host remoto como su tipo de sistema operativo y versión exacta, su nombre de host, y la lista de servicios que se está ejecutando.
Código CVE:

Fecha de publicación: 28/04/2004
Explotado: Si
Solución: Filtrar el tráfico de entrada al puerto UDP 5353, si lo desea.
Referencias:

- **Servidor dchgpt01.lan.tungurahua.gob.ec**

Vulnerabilidad: Servidor DNS divulgación de información a distancia
Riesgo: Medio
Descripción: El servidor DNS remoto responde a las preguntas de los dominios de terceros que no tienen el conjunto de bits recursividad. Esto puede permitir a un atacante remoto determinar qué dominios recientemente se han resuelto a través de este servidor de nombres, y por lo tanto, que los ejércitos se han visitado recientemente.
Código CVE:
Fecha de publicación:
Explotado: Si
Solución: Póngase en contacto con el proveedor del software de DNS para un arreglo.
Referencias:
http://www.rootsecure.net/content/downloads/pdf/dns_cache_snooping.pdf

Vulnerabilidad: Certificado SSL autofirmado
Riesgo: Medio
Descripción: La cadena de certificados X.509 para este servicio no está firmado por una autoridad de certificación reconocida. Si la máquina remota es un anfitrión pública en la producción, esto anula el uso de SSL como cualquiera podría establecer un ataque man-in-the-middle contra el host remoto.
Código CVE:
Fecha de publicación: 17/01/2012
Explotado: No
Solución: Comprar o generar un certificado adecuado para este servicio
Referencias:

- **Servidor mapas.tungurahua.gob.ec**

Vulnerabilidad: Apache httpd Métodos HTTP TRACE / TRACK permitidos
Riesgo: Medio
Descripción: El servidor web remoto es compatible con los métodos TRACE / TRACK. Son métodos HTTP que se utilizan para las conexiones del servidor de depuración web.
Código CVE: CVE-2003-1567, CVE-2004-2320, CVE-2010-0386
Fecha de publicación: 23/01/2003
Explotado: No
Solución: Deshabilitar estos métodos. Consulte la salida de plug-in para más información.
Referencias:
http://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf
http://www.apacheweek.com/issues/03-01-24
http://download.oracle.com/sunalerts/1000718.1.html

Vulnerabilidad: Certificado SSL autofirmado
Riesgo: Medio
Descripción: La cadena de certificados X.509 para este servicio no está firmado por una autoridad de certificación reconocida. Si la máquina remota es un anfitrión pública en la producción, esto anula el uso de SSL como cualquiera podría establecer un ataque man-in-the-middle contra el host remoto.
Código CVE:
Fecha de publicación: 17/01/2012
Explotado: No
Solución: Comprar o generar un certificado adecuado para este servicio
Referencias:

- **Servidor srvap01 145**

Vulnerabilidad: SSL Versión Detección 2 y 3 del Protocolo
Riesgo: Medio
Descripción: El servicio remoto acepta conexiones cifradas mediante SSL 2.0 y / o SSL 3.0, que al parecer sufren de varios defectos criptográficas. Un atacante podría

ser capaz de aprovechar estas cuestiones para realizar ataques man-in-the-middle o descifrar las comunicaciones entre el servicio afectado y los clientes.
Código CVE:
Fecha de publicación:
Explotado: No
Solución: Consultar la documentación de la aplicación para deshabilitar SSL 2.0 y 3.0. Usar TLS 1.0 o superior en su lugar.
Referencias:
http://support.microsoft.com/kb/187498
http://www.linux4beginners.info/node/disable-sslv2

Vulnerabilidad: Vulnerabilidad de cifrado degradado (POODLE)
Riesgo: Medio
Descripción: El host remoto se ve afectado por una vulnerabilidad MitM conocido como POODLE. La vulnerabilidad se debe a la forma en que SSL 3.0 se encarga de bytes de relleno cuando descifra mensajes cifrados usando el modo de encadenamiento de bloques de cifrado (CBC).
Código CVE: CVE-2014-3566
Fecha de publicación: 14/10/2014
Explotado: No
Solución: Servicios que deben soportar SSLv3 debería permitir que el mecanismo de TLS o desactivar completamente SSL 3.0 en el lado del cliente y el servidor.
Referencias:
https://www.imperialviolet.org/2014/10/14/poodle.html
https://www.openssl.org/~bodo/ssl-poodle.pdf
https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00

Vulnerabilidad: Apache httpd Métodos HTTP TRACE / TRACK permitidos
Riesgo: Medio
Descripción: El servidor web remoto es compatible con los métodos TRACE / TRACK. Son métodos HTTP que se utilizan para las conexiones del servidor de depuración web.
Código CVE: CVE-2003-1567, CVE-2004-2320, CVE-2010-0386
Fecha de publicación: 23/01/2003
Explotado: No

Solución: Deshabilitar estos métodos. Consulte la salida de plug-in para más información.
Referencias:
http://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf
http://www.apacheweek.com/issues/03-01-24
http://download.oracle.com/sunalerts/1000718.1.html

- **Servidor bdd_nr**

Vulnerabilidad: Apache httpd Métodos HTTP TRACE / TRACK permitidos
Riesgo: Medio
Descripción: El servidor web remoto es compatible con los métodos TRACE / TRACK. Son métodos HTTP que se utilizan para las conexiones del servidor de depuración web.
Código CVE: CVE-2003-1567, CVE-2004-2320, CVE-2010-0386
Fecha de publicación: 23/01/2003
Explotado: No
Solución: Deshabilitar estos métodos. Consulte la salida de plug-in para más información.
Referencias:
http://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf
http://www.apacheweek.com/issues/03-01-24
http://download.oracle.com/sunalerts/1000718.1.html

Vulnerabilidad: Certificado SSL no es confiable
Riesgo: Medio
Descripción: Certificado X.509 del servidor no tiene una firma de una autoridad de certificación pública conocida. Si la máquina remota es un anfitrión pública en la 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 de llevar a cabo ataques man-in-the-middle contra el host remoto.
Código CVE:
Fecha de publicación: 15/12/2010
Explotado: Si
Solución: Comprar o generar un certificado adecuado para este servicio.

Referencias:

- **Servidor HGPT-SERVERPRUE**

Vulnerabilidad: Base de datos Oracle no compatible
Riesgo: Alto
Descripción: De acuerdo con su versión, la instalación de la base de datos de Oracle en el host remoto ya no es compatible.
La falta de apoyo implica que no hay nuevos parches de seguridad para el producto por el proveedor. Como resultado, es probable que contenga vulnerabilidades de seguridad.
Código CVE:
Fecha de publicación: 09/08/2011
Explotado: No
Solución: Actualizar la versión más reciente de base de datos de Oracle compatible.
Referencias:
http://www.nessus.org/u?ccd068d1

Vulnerabilidad: Detección de versión PHP no compatible
Riesgo: Alto
Descripción: De acuerdo con su versión, la instalación de PHP en el host remoto ya no es compatible, lo que implica que no hay nuevos parches de seguridad para el producto por el proveedor. Como resultado, es probable que contenga vulnerabilidades de seguridad.
Código CVE:
Fecha de publicación: 04/05/2012
Explotado: Si
Solución: Actualizar a una versión de PHP más reciente.
Referencias:
http://php.net/eol.php https://wiki.php.net/rfc/releaseprocess

Vulnerabilidad: Apache 2.2 <2.2.28 Múltiples vulnerabilidades
Riesgo: Alto
Descripción: De acuerdo con la versión de Apache 2.2 instalado en el host remoto, es anterior a la 2.2.28. Está, por lo tanto, afectada por las vulnerabilidades: CVE-

2014-0.118, CVE-2014-0226 y CVE-2.014-0231. Tenga en cuenta que Nessus no ha probado para estas cuestiones, sino que se ha basado únicamente en el número de versión de auto-reporte de la aplicación.
Código CVE: CVE-2013-5704, CVE-2014-0118, CVE-2014-0226, CVE-2014-0231
Fecha de publicación: 04/09/2014
Explotado: No
Solución: Actualizar Apache a la versión 2.2.29 o posterior.
Referencias:

Vulnerabilidad: Escritorio remoto podrían permitir la ejecución remota de código
Riesgo: Alto
Descripción: Existe una vulnerabilidad remota de código arbitrario en la aplicación del Protocolo de Escritorio Remoto (RDP). La vulnerabilidad se debe a la forma en que RDP acceso a un objeto en la memoria que se ha inicializado incorrectamente o se ha eliminado. Un atacante remoto no autenticado podría aprovechar esta vulnerabilidad para provocar que el sistema para ejecutar código arbitrario mediante el envío de una secuencia de paquetes RDP especialmente diseñados para ello.
Código CVE: CVE-2012-0002, CVE-2012-0152
Fecha de publicación: 03/13/2012
Explotado: Si
Solución: Microsoft ha publicado un conjunto de parches para Windows XP, 2003, Vista, 2008, 7 y 2008 R2.
Referencias:
http://technet.microsoft.com/en-us/security/bulletin/ms12-020

Vulnerabilidad: Oracle TNS Listener Envenenamiento remoto
Riesgo: Alto
Descripción: La escucha de Oracle TNS remoto permite el registro de servicios de un host remoto. Un atacante puede aprovechar este problema para desviar los datos de un servidor de base legítima o cliente a un sistema atacante-especificado.
Hazañas exitosas permitirán que el atacante manipular las instancias de base de datos, lo que podría facilitar man-in-the-middle, secuestro sessión, o ataques de denegación de servicio en el servidor de base de datos legítimo.
Código CVE: CVE-2012-1675
Fecha de publicación: 30/04/2012

Explotado: No
Solución: Aplicar la solución alternativa en la asesoría de Oracle.
Referencias:
http://www.nessus.org/u?1feaed5b
http://www.nessus.org/u?29d9db9b

Vulnerabilidad: Apache httpd Métodos HTTP TRACE / TRACK permitidos
Riesgo: Medio
Descripción: El servidor web remoto es compatible con los métodos TRACE / TRACK. Son métodos HTTP que se utilizan para las conexiones del servidor de depuración web.
Código CVE: CVE-2003-1567, CVE-2004-2320, CVE-2010-0386 Fecha de publicación: 23/01/2003
Explotado: No
Solución: Deshabilitar estos métodos. Consulte la salida de plug-in para más información.
Referencias:
http://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf
http://www.apacheweek.com/issues/03-01-24
http://download.oracle.com/sunalerts/1000718.1.html

Vulnerabilidad: Servidor Microsoft Windows Remote Desktop Protocol con debilidad Man-in-the-Middle
Riesgo: Medio
Descripción: La versión remota del Escritorio remoto (Terminal Service) es vulnerable a un ataque man-in-the-middle. El cliente RDP no hace ningún esfuerzo para validar la identidad del servidor al configurar el cifrado. Un atacante con la capacidad para interceptar el tráfico desde el servidor RDP puede establecer el cifrado con el cliente y el servidor sin ser detectado. Un ataque MiTM de esta naturaleza permitiría al atacante obtener información sensible transmitida, incluyendo las credenciales de autenticación.
Código CVE: CVE-2005-1794
Fecha de publicación: 28/05/2005
Explotado: No

Solución: Forzar el uso de SSL y / o ajustar 'permitir sólo las conexiones desde equipos que ejecuten Escritorio remoto con Autenticación a nivel de red' si está disponible.
Referencias:
http://www.oxid.it/downloads/rdp-gbu.pdf
http://www.nessus.org/u?e2628096

4.12.2. Elaboración de Políticas de Contingencia de Seguridad Informática que resguarde los activos informáticos del Honorable Gobierno Provincial de Tungurahua.

Las Políticas de Contingencia de Seguridad Informática que a continuación se describen tienen como objetivo ayudar a eliminar o reducir vulnerabilidades detectadas para salvaguardar la Información junto con todos los activos de la Red Informática de la Institución.

- **Seguridad del Personal**

Mediante los resultados del análisis de las encuestas aplicadas a los 80 empleados de la Institución se crean Políticas de Contingencia de Seguridad Informática que eliminen o reduzcan vulnerabilidades descubiertas en los mismos.

Política ante el mal uso de activos informáticos
Capacitación de usuarios para el uso adecuado de los activos informáticos y de la información de la Institución.

- Dar a conocer a los usuarios de la responsabilidad que tienen sobre los activos informáticos que usan junto con el cumplimiento de las Políticas de la Institución.
- Los usuarios deben comprometerse con la Institución y de ser el caso firmar un acuerdo de confidencialidad y el uso adecuado de los activos informáticos.
- El Departamento de Sistemas debe realizar reuniones, conferencias y/o charlas en las cuales den a conocer de las nuevas amenazas en lo que a Seguridad Informática se refiere.

Política ante el uso de dispositivos externos
Está prohibido el uso de dispositivos tecnológicos externos a la Institución.

- La utilización de dispositivos especiales debe realizarse previa justificación y autorización del Departamento correspondiente.
- Los usuarios que dispongan bajo su resguardo este tipo de dispositivos serán responsables del correcto uso que se le dé.
- Dar a conocer que dispositivos ajenos a la institución como son los discos externos pueden ser transmisores de código malicioso como virus, gusanos o caballos de troya.

Política de tratamiento de dispositivos
Establecer y/o obligar un tratamiento adecuado de los dispositivos informáticos por parte de los usuarios.

- Los usuarios deben notificar de manera urgente al Departamento de Sistemas sobre anomalías físicas o a nivel de software.
- Los usuarios no deben reubicar, modificar o alterar equipos informáticos bajo ningún concepto.
- Para problemas considerados de manera no urgente, debe realizarse mediante la creación de un ticket para el mantenimiento preventivo o correctivo de ser el caso.
- Los equipos informáticos deben ser asignados a los usuarios para uso exclusivo de las funciones de la Institución.

Mediante los datos obtenidos en la etapa de reconocimiento como son nombres de usuarios e información personal de empleados, se crea la siguiente Política.

Política de administración de usuarios y contraseñas
Administración de usuarios y contraseñas del personal de la Institución.

- La asignación de usuarios y contraseñas debe realizarse de manera individual y confidencial.

- Los usuarios deben crear o cambiar su contraseña con una longitud de entre mayor o igual a 8 caracteres.
- Usar letras mayúsculas y minúsculas junto con números y al menos un carácter especial.
- No usar la misma contraseña para varios servicios y cambiarla en un periodo de dos o tres meses máximo.
- Prohibir a los empleados que utilicen su nombre de usuario como contraseña.
- Prohibir que las contraseñas o datos confidenciales se encuentren de forma legible en lugares donde personas ajenas a la Institución puedan verlos.

- **Seguridad Física**

Mediante los resultados del análisis de las encuestas aplicadas a los 6 profesionales del Departamento de Sistemas, a continuación se crean las siguientes Políticas.

Política ante la inadecuada infraestructura del Centro de Datos

Establecer una infraestructura adecuada para el funcionamiento de un Centro de Datos de la Institución.

- Destinar una área restringida y adecuada para que sirva como Centro de Datos donde sean ubicados los servidores y sistemas de comunicación.
- Adoptar por un sistema de refrigeración según los estándares vigentes que minimicen el riesgo de daños de los dispositivos del Centro de Datos.
- Adoptar por un sistema de cableado estructurado que ofrezca un adecuado desempeño de cada uno de los dispositivos del Centro de Datos actual y futuro.

Política de seguridad de acceso físico a la Institución

Contar con mecanismos de control de acceso tanto como para la Institución como para las instalaciones.

- Instalar dispositivos de seguridad que resguarde los activos físicos de la Institución no solo a nivel de entradas y salidas también deben resguardarse las instalaciones de acceso restringido para terceras personal.

- Monitorear los accesos e instalaciones de la Institución y reportar cualquier anomalía o mal actuar del personal o terceras personas.
- Determinar áreas restringidas en la Institución y darles su nivel de acceso adecuado al personal autorizado.

Política de seguridad de acceso físico a instalaciones

Llevar un registro de personal que tenga acceso a instalaciones consideradas como restringidas.

- Las áreas consideradas como restringidas deben contar con un registro el cual debe llenarse ante el ingreso del personal autorizado, el registro debe contar con detalles importantes como: fecha y hora, datos personales del empleado, motivo de ingreso, detalle del ingreso entre otros.
- En caso de daños de equipos los cuales deban ser trasladados para su arreglo o mantenimiento, debe ser tratado únicamente con el departamento correspondiente el cual lleve el caso según Políticas de la Institución.
- El ingreso de terceras personas a áreas restringidas en todo momento debe ser vigilado.

Política de área restringida

Establecer como área restringida al Departamento de Sistemas junto con sus activos.

- El Departamento de Sistemas debe tener un resguardo especial en cuanto a vigilancia se refiere.
- Establecer el personal autorizado para el ingreso y labor en el Departamento de Sistemas.
- Usar identificación Institucional con fotografía y los datos personales del empleado.

- **Administración de Operaciones de Cómputo**

Mediante los resultados obtenidos de la aplicación del presente proyecto se crean las siguientes Políticas para mejorar el funcionamiento y un adecuado uso de equipos.

Política de seguridad de equipos

Protección de equipos mediante el uso y actualización de un software Antivirus.

- El Departamento de Sistemas debe proporcionar una solución de seguridad que integre herramientas como antivirus, antispyware, firewall y prevención de intrusiones.
- Todos los equipos de cómputo deben tener instalado una solución Antivirus proporcionada por el Departamento de Sistema y con su respectiva licencia de ser el caso.
- Realizar periódicamente un análisis del equipo y actualizar la base de datos y firmas de antivirus proporcionadas por el fabricante.

Política de uso de software

Establecer el uso y manejo adecuado de software por parte del usuario.

- Los usuarios no pueden instalar software que no esté autorizado por la Institución y de ser el caso en que lo requieran deberán justificar y pedir autorización al Departamento correspondiente.
- Prohibir la instalación de software de dudosa procedencia y los riesgos que traen consigo en el caso que lo hicieran.

Política ante la exploración de la red

Seguridad en la red informática ante ejecución de software no autorizado.

- Queda prohibido la ejecución de software el cual realice cualquier tipo de exploración y/o analizador de la red informática.
- Considerar como ataque la ejecución de herramientas de auditoría informática que tengan fines de detectar y explotar una posible vulnerabilidad.
- Prohibir el uso de herramientas de software o hardware que viole la integridad o los controles de Seguridad Informática.

Política ante la navegación de sitios prohibidos

Control y monitoreo de la navegación en internet por parte de los usuarios.

- El Departamento de Sistemas debe monitorear las actividades que los usuarios realizan en internet.
- Crear reglas de acceso a páginas no autorizadas y descargas de archivos no confiables, bloquear sitios denominados “proxy webs”.
- Dar a conocer al usuario que la utilización del internet es para el desempeño del puesto en función no para propósitos personales.

- **Seguridad Lógica de Servidores**

Mediante el sondeo y la detección de sistemas operativos que en la actualidad no cuentan con soporte por parte del fabricante se crea la siguiente Política.

Política ante Sistemas desactualizados
Administración de Software de Sistema.

- Instalar un Sistema que garantice la protección y estabilidad del equipo, gestione los recursos y servicios necesarios.
- Actualizar periódicamente el Sistema del Servidor según sean notificadas nuevas actualizaciones o parches de seguridad.
- Configurar los sistemas de manera que se brinde solo los servicios y recursos necesarios para utilización de los usuarios.
- Deben ser monitoreados constantemente junto con el mantenimiento en donde se incluya una depuración de Log.

Mediante la exploración de los servidores y la detección de software desactualizado y en algunos de los casos sin soporte, se crea la siguiente Política.

Política ante Software desactualizado
Administración de Software de Servicios sobre el Servidor.

- La instalación de programas para brindar servicio debe realizarse de manera que se proporcione seguridad y una buena gestión de recursos.

- El software debe ser actualizado constantemente según sean notificados las actualizaciones de versiones o parches de seguridad.
- Declarar responsables que mantengan vigilante el software de uso diario no solo con el distribuidor oficial sino también a nivel de foros en los cuales mencionen fallos o vulnerabilidades.

Ante la detección de software con configuraciones por defecto y la exposición del éxito de la explotación del mismo, se crea la siguiente Política.

Política ante configuraciones por defecto
Configuración de servicios de un Servidor.

- Eliminar las configuraciones por defectos de los servicios confidenciales a los cuales tengan acceso varios usuarios.
- Proteger los privilegios de la cuenta de administrador mediante la creación y asignación de usuarios y roles.
- Realizar cambios en los archivos de configuración por defectos los cuales puedan proporcionar divulgación de información mediante mensajes de bienvenida.
- Restringir a un mínimo el número de usuarios con acceso a las cuentas Administrador de un servicio instalado, limitar los intentos de conexión fallidos.

Mediante las respuestas obtenidas de la entrevista con el Director de Sistemas en lo referente a llevar respaldos de información se define lo siguiente.

Política ante pérdida de información
Respaldo de Información.

- Generar de manera periódica un respaldo de las bases de datos de la Institución de forma automática o manual.
- Los respaldos deben ser comprimidos (recomendado) y resguardados en dispositivos externos.

- Resguardar los respaldos en un sitio externo a la Institución, fuera del lugar en el que se encuentren los equipos aplicando los estándares de calidad para el almacenamiento de medios magnéticos.

Al no contar con un Sistema de Detección de Intrusos (IDS) y exponer los daños que esto puede causar se sugiere la siguiente Política.

Política ante ataques a servidores
Implementación de Sistemas de Detección de Intrusos (IDS).

- Implementar una herramienta de seguridad Sistema de Detección de Intrusos encargada de monitorizar los eventos que ocurren en un sistema informático en busca de intentos de intrusión.
- Configurar un IDS de tal manera que alerte cualquier intento de comprometer la confidencialidad, integridad, disponibilidad o evitar los mecanismos de seguridad de una red o computadora.
- Crear un procedimiento de contingencia ante el registro de una actividad sospechosa o en el peor de los casos un ataque.

CAPÍTULO 5

Conclusiones y Recomendaciones

Se definen conclusiones y recomendaciones con base en los resultados analizados en conformidad a los objetivos de estudio.

5.1. Conclusiones

- El Honorable Gobierno Provincial de Tungurahua no ha realizado auditorías de seguridad informática en lo que a detección de vulnerabilidades se refiere, tampoco cuenta con herramientas que faciliten un análisis, detección y explotación de vulnerabilidades por lo cual el proyecto es beneficioso mediante la investigación de lo mencionado.

- La herramientas utilizadas para llevar a cabo el presente proyecto de investigación funcionaron según lo esperado y son software libre lo cual es muy importante debido a que no presentaron gastos extras, además dichas herramientas pueden ser recomendadas para dar un seguimiento al análisis y detección de vulnerabilidades dentro de la Institución.

- La explotación de vulnerabilidades se la realiza en un entorno virtual similar al real, esto con el el objetivo de no ocasionar daños ni perjuicios a los equipos reales, esto puede servir como caso práctico de tal forma que el lector sea capaz de aplicar y comprobar la utilidad de las herramientas descritas.

- Los objetivos del presente proyecto de investigación se ha cumplido mediante el desarrollo del mismo, por cuanto al estudio y aplicación de herramientas de seguridad informática para la detección y explotación de vulnerabilidades

dando como resultado Políticas de Contingencia de Seguridad Informática que deben ser aplicadas para eliminar o reducir vulnerabilidades existentes.

- Las secciones y módulos de la metodología OSSTMM fueron seleccionados de acuerdo a los resultados esperados teniendo éxito y llegando a detectar vulnerabilidades existentes en los servidores de la Institución y recomendar las medidas de seguridad que se deben tomar.

5.2. Recomendaciones

- Se recomienda al Director del Departamento de Sistemas del Honorable Gobierno Provincial de Tungurahua, aplicar y dar un seguimiento correcto las Políticas de Contingencia de Seguridad Informática recomendadas con el objetivo de eliminar o reducir las vulnerabilidades detectadas, garantizado la integridad de la información junto con los activos de red informática.

- Se sugiere al Director del Departamento de Sistemas, implementar funciones a nivel de administrador y de carácter obligatorio, el estudio de herramientas de seguridad informática que ayuden a la detección de vulnerabilidades y sean ejecutados periódicamente en la red Informática de la Institución.

- Se sugiere a cada uno de los profesionales pertenecientes al Departamento de Sistemas, continuar con la investigación acerca de métodos y tecnologías que se involucran en la seguridad informática con respecto a la prevención de intrusos como es el caso de IDS's, IPS's, Honeypots y Honeynets, puesto que brindan mecanismos ante posibles ataques informáticos.

- Se recomienda al Director del Departamento de Sistemas, tomar la metodología OSSTMM como referencia para el análisis de la seguridad, la metodología propone un proceso de evaluación de debilidades de una serie de áreas que refleja los niveles de seguridad presentes en la infraestructura a ser auditada, permite valorar los riesgos, vulnerabilidades que se puedan explotar y el impacto de una explotación real finalizando con un reporte incluyendo soluciones a los problemas de seguridad descubiertos.

BIBLIOGRAFÍA

[1] K. Lab, "Lo que sabemos del mayor 'hackeo' bancario de la historia." [en línea]. Disponible en: http://latam.kaspersky.com/sobre-kaspersky/centro-de-prensa/ultimas-noticias/cnn-expansión-pan-regional-lo-que-sabemos-del-mayo.

[2] M. G. Hernández Pinto, "Diseño de un plan estratégico de seguridad de información en una empresa del sector comercial." [en línea]. Disponible en: http://www.dspace.espol.edu.ec/handle/123456789/10730, 2006.

[3] P. F. M. Guangashi, "Medidas de protección informática para evitar el robo de identidad provocado por el ataque phishing "the tabnabbing attack"para la facultad de ingeniería en sistemas electrónica e industrial." [en línea]. Disponible en: http://repo.uta.edu.ec/handle/123456789/2378, Juio 2012.

[4] G. P. de Tungurahua, "Misión." [en línea]. Disponible en: http://www.tungurahua.gob.ec/, 2014.

[5] A. H. Sánchez, "Auditorías de seguridad informática y la OSSTMM." [en línea]. Disponible en: http://es.scribd.com/doc/17740680/Auditorias-de-Seguridad-Informatica-y-la-OSSTMM, 2009.

[6] E. F. Zavala Vela *et al.*, "Diseño e implementación de seguridades en la red de datos de la planta central del ministerio de educación y cultura del ecuador, aplicando la tecnología osstmm (open source security testing methodology manual); y, creación de políticas de seguridad mínimas para las subsecretarías, direcciones provinciales y cantonales de educación," 2010.

[7] G. N. Huilca Chicaiza, "Hacking ético para detectar vulnerabilidades en los servicios de la intranet del gobierno autónomo descen-

tralizado municipal del cantón cevallos." [en línea]. Disponible en: http://repo.uta.edu.ec/handle/123456789/2900.

[8] M. T. ASSOCIATE, "Student study guide." [en línea]. Disponible en: ftp://ftp.certiport.com/Marketing/Mta/docs/.

[9] C. Tori, *Hacking Ético.* Mastroianni Impresiones, 2008.

[10] V. D. Casares, "Metodologías avanzadas de pen-test." [en línea]. Disponible en: http://archivos.usuaria.org.ar/segurinfo2014/uruguay/agenda.html.

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

[12] J. E. Martínez, "Auditoria de seguridad informatica," *Password s.a.*, 2004.

[13] A. Bahamontes, "Auditoría de seguridad informática," *antpji.com*, 2013.

[14] R. Audi, *The Cambridge Dictionary of Philosophy (2nd Edition).* Cambridge University Press, 1999.

[15] C. O. S.A., "Itil Â® - gestión de servicios ti." [en línea]. Disponible en: http://itil.osiatis.es/, 2011.

[16] M. EYSSAUTIER De la Mora, "Metodología de la investigación: desarrollo de la inteligencia," *México, Ecafsa*, 2002.

[17] P. V. Herzog, *Manual de la Metodología Abierta de Testeo de Seguridad.*

[18] pcworld.com, "Hackers increasingly target small businesses, symantec warns." [en línea]. Disponible en: http://www.pcworld.com/article/260431/, 2012.

[19] https://www.kali.org/, "Kali linux." [en línea]. Disponible en: https://www.kali.org/, 2015.

[20] D. Bradbury, "Computer fraud and security." [en línea]. Disponible en: http://www.sciencedirect.com/science/article/pii/S1361372311701014, 2011.

[21] G. Inc, "Ayuda google." [en línea]. Disponible en: https://support.google.com/vault/answer/2474474?hl=es, 2015.

[22] dragonjar, "Foca, herramienta para análisis de meta datos." [en línea]. Disponible en: http://www.dragonjar.org/foca-herramienta-para-analisis-meta-datos.xhtml, 2012.

[23] seguridadpublica.es, "Visualroute herramienta de ping, whois y traceroute." [en línea]. Disponible en: http://www.seguridadpublica.es/2012/12/visualroute-herramienta-de-ping-whois-y-traceroute/, 2012.

[24] theharvester, "theharvester information gathering." [en línea]. Disponible en: https://code.google.com/p/theharvester/.

[25] nmap.org, "Guía de referencia de nmap." [en línea]. Disponible en: https://nmap.org/man/es/.

[26] E. J. Kamerling, "The hping idle host scan." [en línea]. Disponible en: http://www.ouah.org/hping2idle.html, 2001.

[27] openvas.org, "El escáner de vulnerabilidades más avanzado del mundo open source." [en línea]. Disponible en: http://www.openvas.org/about.html, 2014.

[28] tenable network security, "Guía de instalación y configuración de nessus 5.0." [en línea]. Disponible en: http://static.tenable.com/documentation, 2012.

[29] inforensicsuex, "Tests de penetración. explotación de vulnerabilidades con metasploit framework." [en línea]. Disponible en: https://inforensicsuex.wordpress.com/2014/05/15/, 2014.

[30] sectools.org, "Thc hydra." [en línea]. Disponible en: http://sectools.org/tool/hydra, 2015.

[31] F. Gutiérrez Benito *et al.*, "Laboratorio virtualizado de seguridad informática con kali linux," 2014.

[32] D. Hoffman, D. Prabhakar, and P. Strooper, "Testing iptables," in *Proceedings of the 2003 conference of the Centre for Advanced Studies on Collaborative research*, pp. 80–91, IBM Press, 2003.

[33] J. Elks, "Man in the middle attack: Focus on sslstrip," 2011.

[34] uServers Comunicaciones, "Â¿ qué es el nic ?." [en línea]. Disponible en: http://web.uservers.net/ayuda/soluciones/dominios, 2015.

[35] rafaelma, "Asegurando la cuenta de administrador postgres." [en línea]. Disponible en: http://www.postgresql.org.es/node/224, 2009.

[36] J. Postel and J. Reynolds, “File transfer protocol,” 1985.

[37] J. B. Duenas, “Configuración de servidor nf.” [en línea]. Disponible en: http://www.alcancelibre.org/staticpages/index.php/12-como-nfs, 2014.

[38] W. Katz, J. van der Lelie, and B. Roos, “Research project 2: Metasploit-able honeypots,” 2013.

[39] T. de seguridad, “Boletín de seguridad de microsoft.” [en línea]. Disponible en: https://technet.microsoft.com/es-es/security/bulletin, 2015.

[40] D. Inc, “Digicert certificados ev ssl.” [en línea]. Disponible en: https://www.digicert.com/es/noticias/2009-02-19-sslstrip-ev.htm, 2009.

[41] J. A. Bertolín, “Análisis de los riesgos y contramedidas en seguridad-privacidad de la tecnología nfc en móviles,” *Revista española de electrónica*, no. 684, pp. 42–51, 2011.

Anexos y Apéndices

Anexo A

Aprobación para realizar el Proyecto de Investigación

H. GOBIERNO PROVINCIAL DE TUNGURAHUA

PBX: 03-3730220 FAX: 2422-297
e-mail: gobierno.provincial@tungurahua.gob.ec

Ambato - Ecuador

Casilla: 18-01-320
Bolívar y Castillo

Ambato septiembre 23, 2014
OP-1054-2014

Ingeniero
Vicente Morales
Decano de la Facultad de Sistemas, Electrónica e Industrial
Universidad Técnica de Ambato
Ciudad

De mi consideración:

Es grato comunicarle que el señor Byron Danilo Nuela Guananga, Egresado de la Facultad de Sistemas de la Universidad Técnica de Ambato, fue aprobado para realizar el Trabajo de Investigación en la Dirección de Sistemas del H. Gobierno Provincial de Tungurahua, previo la obtención del título de Ingeniero en Sistemas.

Gracias por su atención.

Atentamente,

Ing. José Sanguil Portero
Jefe de la Unidad de Talento Humano

GOBIERNO PROVINCIAL DE TUNGURAHUA
DPTO. RECURSOS HUMANOS

Anexo B

Certificado de culminación del Proyecto de Investigación

H. GOBIERNO PROVINCIAL DE TUNGURAHUA

PBX: 03-3730220 FAX: 2422-297
e-mail: gobierno.provincial@tungurahua.gob.ec

Ambato - Ecuador

Casilla: 18-01-320
Bolívar y Castillo

Ambato, 5 de agosto de 2015

0344

Ingeniero M.Sc.
Vicente Morales Lozada
DECANO FACULTAD DE INGENIERIA EN
SISTEMAS, ELECTRONICA E INDUSTRIAL
UNIVERSIDAD TECNICA DE AMBATO
Presente

Señor Decano:

Por medio del presente, en calidad de representante legal de esta empresa certifico que el trabajo de investigación: Auditoría de la Seguridad Informática para el H. Gobierno Provincial de Tungurahua, mediante la metodología Open Source Security Testing Methodology Manual, desarrollado por el señor Byron Danilo Nuela Guananga, ha sido concluido de conformidad a los intereses de la Empresa.

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

Atentamente,

Ing. Fernando Naranjo Lalama
Prefecto Provincial

GOBIERNO PROVINCIAL
DE TUNGURAHUA
PREFECTURA

Anexo C

Informe de escaneo Nessus

Nessus Report

Nessus Scan Report

06/Apr/2015:17:42:51

Nessus Home: Commercial use of the report is prohibited

Table Of Contents

Hosts Summary (Executive)

172.16.1.132

Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	8	8

Details

Severity	Plugin Id	Name
Info	10223	RPC portmapper Service Detection
Info	10287	Traceroute Information
Info	11111	RPC Services Enumeration
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	19506	Nessus Scan Information
Info	45590	Common Platform Enumeration (CPE)
Info	54615	Device Type

172.16.1.133

Summary

Critical	High	Medium	Low	Info	Total
0	1	10	4	26	41

Details

Severity	Plugin Id	Name
High (7.5)	10483	PostgreSQL Default Unpassworded Account
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.0)	12218	mDNS Detection (Remote Network)
Medium (5.0)	15901	SSL Certificate Expiry
Medium (5.0)	20007	SSL Version 2 and 3 Protocol Detection
Medium (5.0)	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
Medium (4.3)	26928	SSL Weak Cipher Suites Supported
Medium (4.3)	42873	SSL Medium Strength Cipher Suites Supported
Medium (4.3)	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
Medium (4.0)	60108	SSL Certificate Chain Contains Weak RSA Keys
Low (2.6)	10407	X Server Detection
Low (2.6)	10891	X Display Manager Control Protocol (XDMCP) Detection
Low (2.6)	65821	SSL RC4 Cipher Suites Supported
Low	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
Info	10107	HTTP Server Type and Version
Info	10223	RPC portmapper Service Detection
Info	10287	Traceroute Information
Info	10342	VNC Software Detection
Info	10757	Webmin Detection
Info	10758	VNC HTTP Server Detection
Info	10863	SSL Certificate Information
Info	11111	RPC Services Enumeration
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	17975	Service Detection (GET request)

Info	19506	Nessus Scan Information
Info	21643	SSL Cipher Suites Supported
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	26024	PostgreSQL Server Detection
Info	43111	HTTP Methods Allowed (per directory)
Info	45590	Common Platform Enumeration (CPE)
Info	51891	SSL Session Resume Supported
Info	53335	RPC portmapper (TCP)
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	62563	SSL Compression Methods Supported
Info	66334	Patch Report
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported

172.16.1.134

Summary

Critical	High	Medium	Low	Info	Total
0	0	9	4	21	34

Details

Severity	Plugin Id	Name
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.0)	20007	SSL Version 2 and 3 Protocol Detection
Medium (5.0)	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
Medium (4.3)	26928	SSL Weak Cipher Suites Supported
Medium (4.3)	42873	SSL Medium Strength Cipher Suites Supported
Medium (4.3)	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
Medium (4.0)	52609	IMAP Service STARTTLS Plaintext Command Injection
Medium (4.0)	52610	POP3 Service STLS Plaintext Command Injection
Low (2.6)	15855	POP3 Cleartext Logins Permitted
Low (2.6)	31705	SSL Anonymous Cipher Suites Supported
Low (2.6)	65821	SSL RC4 Cipher Suites Supported
Low	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
Info	10185	POP Server Detection
Info	10263	SMTP Server Detection
Info	10287	Traceroute Information
Info	10863	SSL Certificate Information
Info	11219	Nessus SYN scanner
Info	11414	IMAP Service Banner Retrieval
Info	19506	Nessus Scan Information
Info	20870	LDAP Server Detection
Info	21643	SSL Cipher Suites Supported
Info	22964	Service Detection
Info	25701	LDAP Crafted Search Request Server Information Disclosure
Info	42085	IMAP Service STARTTLS Command Support
Info	42329	LDAP Service STARTTLS Command Support

Info	50350	OS Identification Failed
Info	50845	OpenSSL Detection
Info	51891	SSL Session Resume Supported
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	62563	SSL Compression Methods Supported
Info	66334	Patch Report
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported

172.16.1.135

Summary

Critical	High	Medium	Low	Info	Total
0	0	3	1	21	25

Details

Severity	Plugin Id	Name
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.0)	12217	DNS Server Cache Snooping Remote Information Disclosure
Low (2.6)	65821	SSL RC4 Cipher Suites Supported
Info	10287	Traceroute Information
Info	10863	SSL Certificate Information
Info	10884	Network Time Protocol (NTP) Server Detection
Info	10940	Windows Terminal Services Enabled
Info	11002	DNS Server Detection
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	19506	Nessus Scan Information
Info	20870	LDAP Server Detection
Info	21643	SSL Cipher Suites Supported
Info	22964	Service Detection
Info	25701	LDAP Crafted Search Request Server Information Disclosure
Info	43829	Kerberos Information Disclosure
Info	45590	Common Platform Enumeration (CPE)
Info	51891	SSL Session Resume Supported
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	62563	SSL Compression Methods Supported
Info	64814	Terminal Services Use SSL/TLS
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported

172.16.1.136

Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	6	6

Details

Severity	Plugin Id	Name
Info	10287	Traceroute Information
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	19506	Nessus Scan Information
Info	45590	Common Platform Enumeration (CPE)
Info	54615	Device Type

172.16.1.140

Summary

Critical	High	Medium	Low	Info	Total
0	0	9	2	26	37

Details

Severity	Plugin Id	Name
Medium (6.8)	12085	Apache Tomcat servlet/JSP container default files
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (5.8)	42880	SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection
Medium (5.0)	10722	LDAP NULL BASE Search Access
Medium (5.0)	20007	SSL Version 2 and 3 Protocol Detection
Medium (5.0)	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
Medium (4.3)	26928	SSL Weak Cipher Suites Supported
Medium (4.3)	42873	SSL Medium Strength Cipher Suites Supported
Medium (4.3)	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
Low (2.6)	65821	SSL RC4 Cipher Suites Supported
Low	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
Info	10107	HTTP Server Type and Version
Info	10287	Traceroute Information
Info	10863	SSL Certificate Information
Info	10884	Network Time Protocol (NTP) Server Detection
Info	11154	Unknown Service Detection: Banner Retrieval
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	17975	Service Detection (GET request)
Info	19506	Nessus Scan Information
Info	20108	Web Server / Application favicon.ico Vendor Fingerprinting
Info	20870	LDAP Server Detection
Info	21186	AJP Connector Detection
Info	21643	SSL Cipher Suites Supported
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information

Info	25701	LDAP Crafted Search Request Server Information Disclosure
Info	39446	Apache Tomcat Default Error Page Version Detection
Info	43111	HTTP Methods Allowed (per directory)
Info	45590	Common Platform Enumeration (CPE)
Info	51891	SSL Session Resume Supported
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	62563	SSL Compression Methods Supported
Info	66334	Patch Report
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported

172.16.1.141

Summary

Critical	High	Medium	Low	Info	Total
1	3	12	3	22	41

Details

Severity	Plugin Id	Name
Critical (10.0)	58987	PHP Unsupported Version Detection
High (9.3)	58435	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)
High (7.5)	77285	PHP 5.3.x < 5.3.29 Multiple Vulnerabilities
High (7.5)	77531	Apache 2.2 < 2.2.28 Multiple Vulnerabilities
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.1)	18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness
Medium (5.0)	10677	Apache mod_status /server-status Information Disclosure
Medium (5.0)	10678	Apache mod_info /server-info Information Disclosure
Medium (5.0)	20007	SSL Version 2 and 3 Protocol Detection
Medium (5.0)	80567	OpenSSL 1.0.0 < 1.0.0p Multiple Vulnerabilities
Medium (5.0)	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
Medium (4.3)	11213	HTTP TRACE / TRACK Methods Allowed
Medium (4.3)	26928	SSL Weak Cipher Suites Supported
Medium (4.3)	42873	SSL Medium Strength Cipher Suites Supported
Medium (4.3)	57690	Terminal Services Encryption Level is Medium or Low
Low (2.6)	30218	Terminal Services Encryption Level is not FIPS-140 Compliant
Low (2.6)	65821	SSL RC4 Cipher Suites Supported
Low	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
Info	10107	HTTP Server Type and Version
Info	10287	Traceroute Information
Info	10863	SSL Certificate Information
Info	10940	Windows Terminal Services Enabled
Info	11219	Nessus SYN scanner
Info	11936	OS Identification

Info	19506	Nessus Scan Information
Info	21643	SSL Cipher Suites Supported
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	45590	Common Platform Enumeration (CPE)
Info	48243	PHP Version
Info	50845	OpenSSL Detection
Info	51891	SSL Session Resume Supported
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	57323	OpenSSL Version Detection
Info	62563	SSL Compression Methods Supported
Info	66173	RDP Screenshot
Info	66334	Patch Report
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported

172.16.1.142

Summary

Critical	High	Medium	Low	Info	Total
0	0	1	1	15	17

Details

Severity	Plugin Id	Name
Medium (5.0)	12218	mDNS Detection (Remote Network)
Low (2.6)	10407	X Server Detection
Info	10092	FTP Server Detection
Info	10107	HTTP Server Type and Version
Info	10223	RPC portmapper Service Detection
Info	10287	Traceroute Information
Info	10342	VNC Software Detection
Info	10758	VNC HTTP Server Detection
Info	11111	RPC Services Enumeration
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	19506	Nessus Scan Information
Info	22964	Service Detection
Info	45590	Common Platform Enumeration (CPE)
Info	52703	vsftpd Detection
Info	53335	RPC portmapper (TCP)
Info	54615	Device Type

172.16.1.143

Summary

Critical	High	Medium	Low	Info	Total
0	0	7	2	24	33

Details

Severity	Plugin Id	Name
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.0)	15901	SSL Certificate Expiry
Medium (5.0)	20007	SSL Version 2 and 3 Protocol Detection
Medium (4.3)	11213	HTTP TRACE / TRACK Methods Allowed
Medium (4.3)	42873	SSL Medium Strength Cipher Suites Supported
Medium (4.3)	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
Low (2.6)	65821	SSL RC4 Cipher Suites Supported
Low	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
Info	10107	HTTP Server Type and Version
Info	10223	RPC portmapper Service Detection
Info	10287	Traceroute Information
Info	10863	SSL Certificate Information
Info	11111	RPC Services Enumeration
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	18261	Apache Banner Linux Distribution Disclosure
Info	19506	Nessus Scan Information
Info	21643	SSL Cipher Suites Supported
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	39521	Backported Security Patch Detection (WWW)
Info	45590	Common Platform Enumeration (CPE)
Info	48243	PHP Version
Info	50845	OpenSSL Detection
Info	51891	SSL Session Resume Supported

Info	53335	RPC portmapper (TCP)
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	62563	SSL Compression Methods Supported
Info	66334	Patch Report
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported

172.16.1.144

Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	3	3

Details

Severity	Plugin Id	Name
Info	10287	Traceroute Information
Info	11219	Nessus SYN scanner
Info	19506	Nessus Scan Information

172.16.1.145

Summary

Critical	High	Medium	Low	Info	Total
0	0	5	2	24	31

Details

Severity	Plugin Id	Name
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.0)	15901	SSL Certificate Expiry
Medium (5.0)	20007	SSL Version 2 and 3 Protocol Detection
Medium (4.3)	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
Low (2.6)	10407	X Server Detection
Low (2.6)	65821	SSL RC4 Cipher Suites Supported
Info	10107	HTTP Server Type and Version
Info	10223	RPC portmapper Service Detection
Info	10287	Traceroute Information
Info	10342	VNC Software Detection
Info	10863	SSL Certificate Information
Info	11111	RPC Services Enumeration
Info	11154	Unknown Service Detection: Banner Retrieval
Info	11219	Nessus SYN scanner
Info	19506	Nessus Scan Information
Info	20108	Web Server / Application favicon.ico Vendor Fingerprinting
Info	21186	AJP Connector Detection
Info	21643	SSL Cipher Suites Supported
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	39446	Apache Tomcat Default Error Page Version Detection
Info	39521	Backported Security Patch Detection (WWW)
Info	43111	HTTP Methods Allowed (per directory)
Info	51891	SSL Session Resume Supported
Info	53335	RPC portmapper (TCP)

Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	62563	SSL Compression Methods Supported
Info	66334	Patch Report
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported

172.16.1.146

Summary

Critical	High	Medium	Low	Info	Total
0	0	6	2	23	31

Details

Severity	Plugin Id	Name
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.0)	15901	SSL Certificate Expiry
Medium (5.0)	20007	SSL Version 2 and 3 Protocol Detection
Medium (4.3)	11213	HTTP TRACE / TRACK Methods Allowed
Medium (4.3)	42873	SSL Medium Strength Cipher Suites Supported
Low (2.6)	65821	SSL RC4 Cipher Suites Supported
Low	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
Info	10107	HTTP Server Type and Version
Info	10223	RPC portmapper Service Detection
Info	10263	SMTP Server Detection
Info	10287	Traceroute Information
Info	10863	SSL Certificate Information
Info	11111	RPC Services Enumeration
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	19506	Nessus Scan Information
Info	21643	SSL Cipher Suites Supported
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	45590	Common Platform Enumeration (CPE)
Info	46180	Additional DNS Hostnames
Info	48243	PHP Version
Info	50845	OpenSSL Detection
Info	51891	SSL Session Resume Supported
Info	53335	RPC portmapper (TCP)

Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	62563	SSL Compression Methods Supported
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported

172.16.1.147

Summary

Critical	High	Medium	Low	Info	Total
0	0	7	2	26	35

Details

Severity	Plugin Id	Name
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.0)	15901	SSL Certificate Expiry
Medium (5.0)	20007	SSL Version 2 and 3 Protocol Detection
Medium (4.3)	11213	HTTP TRACE / TRACK Methods Allowed
Medium (4.3)	42873	SSL Medium Strength Cipher Suites Supported
Medium (4.3)	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
Low (2.6)	65821	SSL RC4 Cipher Suites Supported
Low	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
Info	10107	HTTP Server Type and Version
Info	10223	RPC portmapper Service Detection
Info	10287	Traceroute Information
Info	10863	SSL Certificate Information
Info	11111	RPC Services Enumeration
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	18261	Apache Banner Linux Distribution Disclosure
Info	19506	Nessus Scan Information
Info	21643	SSL Cipher Suites Supported
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	26024	PostgreSQL Server Detection
Info	39521	Backported Security Patch Detection (WWW)
Info	45590	Common Platform Enumeration (CPE)
Info	48243	PHP Version
Info	50845	OpenSSL Detection

Info	51891	SSL Session Resume Supported
Info	53335	RPC portmapper (TCP)
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	62563	SSL Compression Methods Supported
Info	65914	MongoDB Detection
Info	66334	Patch Report
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported

172.16.1.148

Summary

Critical	High	Medium	Low	Info	Total
0	0	6	2	22	30

Details

Severity	Plugin Id	Name
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.0)	15901	SSL Certificate Expiry
Medium (4.3)	11213	HTTP TRACE / TRACK Methods Allowed
Medium (4.3)	42873	SSL Medium Strength Cipher Suites Supported
Medium (4.3)	62565	Transport Layer Security (TLS) Protocol CRIME Vulnerability
Low (2.6)	65821	SSL RC4 Cipher Suites Supported
Low	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
Info	10107	HTTP Server Type and Version
Info	10223	RPC portmapper Service Detection
Info	10287	Traceroute Information
Info	10863	SSL Certificate Information
Info	11111	RPC Services Enumeration
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	18261	Apache Banner Linux Distribution Disclosure
Info	19506	Nessus Scan Information
Info	21643	SSL Cipher Suites Supported
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	39521	Backported Security Patch Detection (WWW)
Info	45590	Common Platform Enumeration (CPE)
Info	48243	PHP Version
Info	50845	OpenSSL Detection
Info	53335	RPC portmapper (TCP)
Info	54615	Device Type

Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	62563	SSL Compression Methods Supported
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported

172.16.1.149

Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	7	7

Details

Severity	Plugin Id	Name
Info	10223	RPC portmapper Service Detection
Info	10287	Traceroute Information
Info	10919	Open Port Re-check
Info	11111	RPC Services Enumeration
Info	11219	Nessus SYN scanner
Info	19506	Nessus Scan Information
Info	53335	RPC portmapper (TCP)

172.16.1.159

Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	4	4

Details

Severity	Plugin Id	Name
Info	10287	Traceroute Information
Info	10919	Open Port Re-check
Info	11219	Nessus SYN scanner
Info	19506	Nessus Scan Information

172.16.1.161

Summary

Critical	High	Medium	Low	Info	Total
0	0	1	0	13	14

Details

Severity	Plugin Id	Name
Medium (4.3)	11213	HTTP TRACE / TRACK Methods Allowed
Info	10107	HTTP Server Type and Version
Info	10287	Traceroute Information
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	18261	Apache Banner Linux Distribution Disclosure
Info	19506	Nessus Scan Information
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	39521	Backported Security Patch Detection (WWW)
Info	43111	HTTP Methods Allowed (per directory)
Info	45590	Common Platform Enumeration (CPE)
Info	54615	Device Type

172.16.1.162

Summary

Critical	High	Medium	Low	Info	Total
2	4	3	1	16	26

Details

Severity	Plugin Id	Name
Critical (10.0)	55786	Oracle Database Unsupported
Critical (10.0)	58987	PHP Unsupported Version Detection
High (9.3)	58435	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)
High (8.3)	58988	PHP < 5.3.12 / 5.4.2 CGI Query String Code Execution
High (7.5)	69552	Oracle TNS Listener Remote Poisoning
High (7.5)	77531	Apache 2.2 < 2.2.28 Multiple Vulnerabilities
Medium (5.1)	18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness
Medium (4.3)	11213	HTTP TRACE / TRACK Methods Allowed
Medium (4.3)	57690	Terminal Services Encryption Level is Medium or Low
Low (2.6)	30218	Terminal Services Encryption Level is not FIPS-140 Compliant
Info	10107	HTTP Server Type and Version
Info	10287	Traceroute Information
Info	10658	Oracle Database tnslsnr Service Remote Version Disclosure
Info	10940	Windows Terminal Services Enabled
Info	11153	Service Detection (HELP Request)
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	19506	Nessus Scan Information
Info	22074	Oracle Default SID
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	45590	Common Platform Enumeration (CPE)
Info	48243	PHP Version
Info	54615	Device Type
Info	66173	RDP Screenshot

Info	66334	Patch Report