UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS

SEMINARIO DE GRADUACIÓN
"SEGURIDAD INFORMÁTICA"

Tema:

"HACKING ÉTICO PARA DETECTAR VULNERABILIDADES EN LOS SERVICIOS DE LA INTRANET DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN CEVALLOS".

Trabajo de Graduación. Modalidad: **SEMINARIO DE GRADUACION**, previo a la obtención del Título de Ingeniera en Sistemas Computacionales e Informáticos.

AUTORA: Gloria Nataly Huilca Chicaiza.

TUTOR: Ing. M.Sc. Alberto Leopoldo Arellano Aucancela.

Ambato - Ecuador

Noviembre -2012

APROBACIÓN DEL TUTOR

En mi calidad de tutor del trabajo de investigación sobre el tema: "**HACKING ÉTICO PARA DETECTAR VULNERABILIDADES EN LOS SERVICIOS DE LA INTRANET DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN CEVALLOS"**, de la señorita Gloria Nataly Huilca Chicaiza, estudiante de la Carrera de Ingeniería en Sistemas, 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 Art. 16 del Capítulo II del Reglamento de Graduación para obtener el título terminal de tercer nivel de la Universidad Técnica de Ambato.

Ambato Noviembre 22, 2012

Ing. M.Sc. Alberto Arellano Aucancela.

AUTORÍA

El presente trabajo de investigación titulado: "**HACKING ÉTICO PARA DETECTAR VULNERABILIDADES EN LOS SERVICIOS DE LA INTRANET DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN CEVALLOS".** 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 Noviembre 22, 2012

Gloria Nataly Huilca Chicaiza

C.C.: 1803601408

APROBACIÓN DE LA COMISIÓN CALIFICADORA

La comisión calificadora del presente trabajo conformada por los señores docentes Ing. Mg. Klever Renato Urvina Barrionuevo e Ing. Mg. Galo Mauricio López Sevilla revisó y aprobó el Informe Final del trabajo de graduación titulado "**HACKING ÉTICO PARA DETECTAR VULNERABILIDADES EN LOS SERVICIOS DE LA INTRANET DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN CEVALLOS",** presentado por la señorita Gloria Nataly Huilca Chicaiza de acuerdo al Art. 18 del Reglamento de Graduación para Obtener el Título Terminal de Tercer Nivel de la Universidad Técnica de Ambato.

Ing. M.Sc. Oswaldo Paredes O.
PRESIDENTE DEL TRIBUNAL

Ing. Mg. Klever. Renato Urvina Barrionuevo
DOCENTE CALIFICADOR

Ing. Mg. Galo M. López Sevilla
DOCENTE CALIFICADOR

DEDICATORIA

El presente trabajo está dedicado a Dios, y mi familia especialmente a mis Padres, hermano e hijo que se han constituido en la luz que ilumina mi vida, estando a mi lado y apoyándome día a día en los momentos más difíciles.

.

Gloria Nataly Huilca Chicaiza.

AGRADECIMIENTO

Agradezco a Dios por haberme bendecido con mis padres que me apoyaron y me dieron la oportunidad de salir adelante.

A la facultad de Ingeniería en Sistemas Electrónica e industrial de la universidad Técnica de Ambato por darme la oportunidad de formarme como profesional, a todos y cada uno de los docentes que imparten cada día sus conocimientos en las aulas.

Al ingeniero Alberto Arellano que en calidad de tutor supo guiarme y brindarme su colaboración y conocimientos para la culminación de esta investigación.

Al gobierno Autónomo Descentralizado Municipal del Cantón Cevallos por haberme abierto las puertas y puesto su confianza en mí.

Gloria Nataly Huilca Chicaiza.

Índice de Contenidos

Pág.

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN EJECUTIVO

El tema del presente trabajo investigativo es hacking ético para detectar vulnerabilidades en los servicios de la intranet del gobierno autónomo descentralizado municipal del cantón Cevallos

La información representa un papel muy importante dentro de las instituciones pues es la parte más primordial y día a día se encuentra expuesta a sufrir modificaciones y en muchos casos a ser robada en su totalidad, es por esto importante asegurar la información.

El objetivo principal del GAD. Municipal del Cantón Cevallos es brindar atención a sus contribuyentes con servicios de calidad, para esto debe realizar todas sus actividades con mayor eficacia tratando de esta manera asegurar en lo posible la información procesada día a día.

A continuación se presenta el resumen por capítulos de toda la investigación realizada.

Capítulo I: denominado "EL PROBLEMA", se identifica el problema a investigar, se plantea la justificación y los objetivos.

Capítulo II: denominado "MARCO TEÓRICO", se presentan los antecedentes investigativos, la fundamentación legal, hipótesis y el señalamiento de las variables.

Capítulo III: denominado "METODOLOGÍA", se determina la metodología de investigación a utilizar, el enfoque, la modalidad básica de la investigación, el tipo de investigación, la población y muestra.

Capítulo IV: denominado "ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS", comprende el análisis e interpretación de resultados.

En el capítulo V: denominado "CONCLUSIONES Y RECOMENDACIONES", se presenta las conclusiones y recomendaciones en base los resultados obtenidos en la entrevista realizada al personal encargado del departamento de sistemas.

Capítulo VI: denominado "PROPUESTA", se presenta el desarrollo de la propuesta ante el problema planteado.

Anexos: contienen formato de cuestionarios, manuales de administración, usuario e instalación.

INTRODUCCIÓN

Un proyecto de Hacking Ético consiste en una penetración controlada en los sistemas informáticos de una empresa, de la misma forma que lo haría un hacker o pirata informático pero de forma ética, previa autorización.

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.

Por este motivo es de vital importancia usar el Hacking Ético para detectar vulnerabilidades en los servicios de la intranet del Gobierno Autónomo Descentralizado Municipal del Cantón Cevallos, por tal razón se expone a continuación una investigación que nos permitirá detectar a tiempo las vulnerabilidades existentes, brindar posibles soluciones para tratar de asegurar los servicios y por ende conseguir beneficiar al Gobierno Autónomo Descentralizado Municipal del Cantón Cevallos logrando brindar unos servicios seguros y de calidad especialmente a nivel de transmisión de información en la intranet.

CAPÍTULO I
EL PROBLEMA

1.1. Tema

"Hacking ético para detectar vulnerabilidades en los servicios de la intranet del Gobierno Autónomo Descentralizado Municipal del Cantón Cevallos."

1.2. Planteamiento del problema

1.2.1. Contextualización

A nivel mundial las instituciones tanto públicas como privadas poseen intranets para transmitir su información sea esta de menor o mayor volumen, el creciente desarrollo de las tecnologías de la información, hace que las empresas, gobierno e instituciones educativas estén ansiosas de ser parte de ésta evolución, pero en los últimos años se ha registrado un creciente número de ataques por parte de crackers hacia los usuarios de Internet, Extranet e Intranet.

Inicialmente este tipo de ataques o intrusiones eran medianamente benignas pues en el peor de los escenarios solo se lograba la ralentización del equipo; pronto pasaron a dañar sistemas completos, borrar archivos o extraer información confidencial sobre las empresas. En un intento de proteger los sistemas, los administradores restringían más el acceso a las computadoras pero en consecuencia los crackers comenzaron con ataques cada vez más destructivos y estructurados.

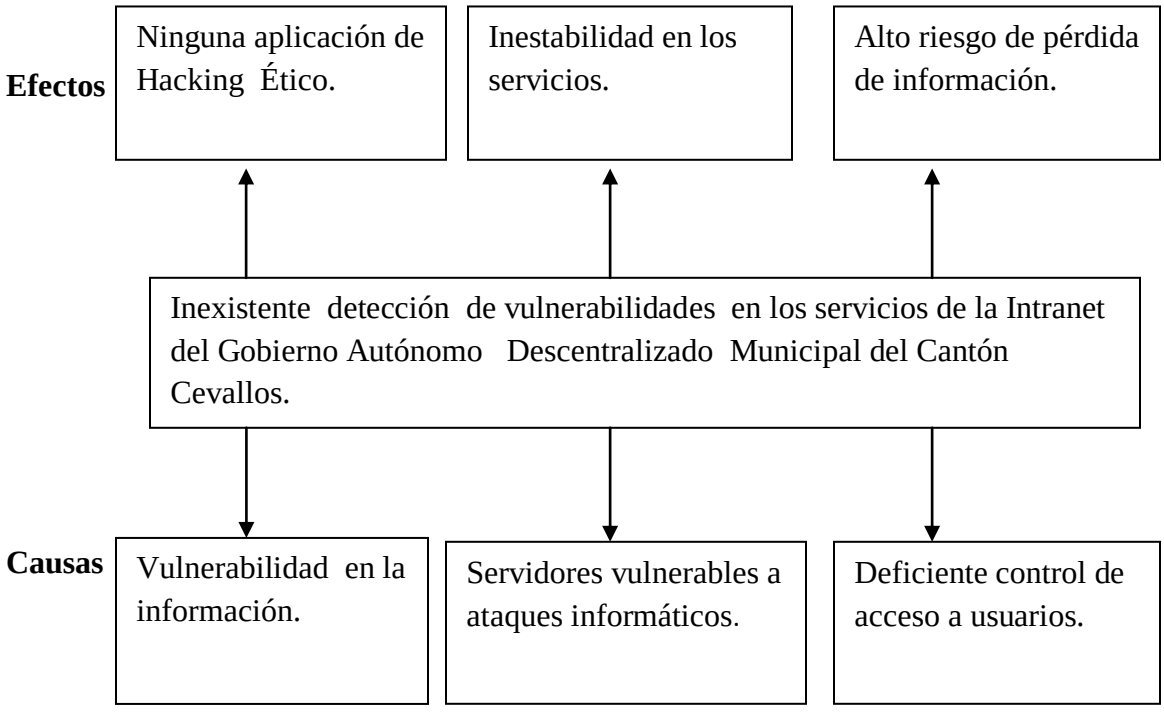
En el Ecuador y en la provincia las instituciones son cada vez más dependientes de sus redes informáticas y un problema que las afecte, por mínimo que sea, puede llegar a comprometer la continuidad de las operaciones.

La falta de medidas de seguridad en las redes especialmente en los servicios de red es un problema que está en crecimiento. Cada vez es mayor el número de atacantes considerando que estos están más organizados, y van adquiriendo día a día habilidades más especializadas que les permiten obtener mayores beneficios.

El Gobierno Autónomo Descentralizado Municipal del Cantón Cevallos posee una intranet con sus respectivos servicios la cual no ha sido sometida a ninguna técnica de "hacking ético" para detectar vulnerabilidades, pues estos presentan un nivel alto de vulnerabilidad ponen en riesgo la información la misma que puede ser alterada o en el peor de los casos robada en su totalidad, todo esto ocasionaría un impacto muy grande especialmente en el manejo de la información considerando que esta es el corazón de cualquier organización, en la mayoría de los casos estas vulnerabilidades son aprovechadas por personal interno mismo de la organización.

Por tal motivo el Gobierno Autónomo Descentralizado Municipal del Cantón Cevallos requiere llevar a cabo la aplicación de hacking ético para detectar vulnerabilidades en los servicios de la intranet, con el objetivo de tratar de mejorar los servicios en la red de datos y así disponer de una red de datos eficiente y segura ante los distintos ataques de intrusos.

1.2.2. Árbol del Problema



1.2.3. Análisis Crítico

La inexistente aplicación de hacking ético para detectar vulnerabilidades en los servicios de la intranet es uno de los principales problemas que tienen la mayoría de instituciones públicas y privadas como es el caso del Gobierno Autónomo Descentralizado Municipal del Cantón Cevallos pues esto conlleva a que no se puedan descubrir las deficiencias relativas en la seguridad de los servicios de la intranet provocando vulnerabilidad en la información, en la mayoría de casos se realiza la instalación de la red con sus respectivos servicios pero nunca se emplean herramientas para detectar vulnerabilidad existente en los mismos.

Los servidores vulnerables a ataques informáticos provocan Inestabilidad en los servicios ya que los servidores son los que contiene la información y si estos son vulnerables los servicios que estos prestan no serán seguros y así todos podrán acceder a la información ocasionando daños irreversibles. Es por esto que los servidores con sus respectivos servicios tienen que estar bien configurados con todas las medidas de seguridad, para cuando se necesite cualquier información esta sea transparente.

El deficiente control de acceso a usuarios ocasiona alto riesgo de pérdida de información confidencial, este robo de información acarrea muchas consecuencias negativas en el Gobierno Autónomo Descentralizado Municipal del Cantón Cevallos teniendo en cuenta que la información constituye el corazón de cualquier institución, sin su información o con la alteración de la misma significa que esté está totalmente perdido.

1.2.4. Prognosis

Si no se aplica el hacking ético para detectar vulnerabilidades en los servicios de la intranet del Gobierno Autónomo Descentralizado Municipal del Cantón Cevallos probablemente aumenten las inseguridades a nivel de los servicios de la intranet ocasionando alteraciones en la información, robo de información, filtración de información.

1.2.5. Planteamiento del problema

¿Cómo la inexistente aplicación de hacking ético influye en la detección de vulnerabilidades en los servicios de la intranet del Gobierno Autónomo Descentralizado Municipal del Cantón Cevallos?

1.2.6. Preguntas directrices.

¿Con la aplicación de hacking ético para detectar vulnerabilidades en los servicios de la intranet se descubrirán deficiencias relativas en los servicios de la intranet?

¿De qué forma se puede controlar el robo de información confidencial?

¿Cómo se puede determinar la inseguridad en la información?

¿El poco estudio de las vulnerabilidades existentes en los servicios de la intranet genera alteraciones en la determinación de un grado de riesgo y peligrosidad de la información?

1.2.7. Delimitación:

Campo: Seguridad Informática

Área: Redes

Aspecto: detección de vulnerabilidades

Delimitación Espacial: Esta investigación se la realizará en el Gobierno Autónomo Descentralizado Municipal del Cantón Cevallos.

Delimitación Temporal: Este problema será investigado, en el periodo comprendido entre Enero2012 – Julio 2012

1.3. Justificación:

Las entidades públicas necesitan brindar una transmisión de información ágil y segura tratando en lo posible de mantener los datos en forma confidencial aplicando nuevas tecnologías que no representen gastos económicos si no que ayuden a lograr una

máxima seguridad beneficiando así a los empleados, administrativos y contribuyentes que de alguna manera se encuentran vinculados con el GAD. Municipal de Cevallos.

Según un estudio realizado se pudo observar que la Municipalidad de Cevallos posee una intranet la cual presta algunos servicios los cuales pueden ser sometidos a un testeo de vulnerabilidades logrando así detectar las principales.

Por tal motivo existe la necesidad de detectar vulnerabilidades en los servicios de la intranet del Gobierno Autónomo Descentralizado Municipal del Cantón Cevallos, mediante la aplicación del Hacking Ético que es una nueva tecnología utilizada a nivel mundial para detectar las vulnerabilidades existentes en cualquier sistema, evaluarlas y determinar el grado de incidencia de las mismas en cuanto a la seguridad de la información se refiere, brindando de esta manera posibles soluciones para proteger la información, ayudando a alertar al administrador de red antes de un posible ataque.

1.4. Objetivos:

1.4.1. Objetivo general

Detectar vulnerabilidades en los servicios de la intranet del Gobierno Autónomo Descentralizado Municipal del Cantón Cevallos mediante el uso de Hacking ético.

1.4.2. Objetivos específicos

- Analizar la técnica de hacking ético y su aplicación en los servicios de la intranet.
- Realizar un diagnostico de los servicios existentes en la intranet del Gobierno Autónomo Descentralizado Municipal del Cantón Cevallos.
- Proponer la aplicación de “hacking ético” para detectar vulnerabilidades en los servicios de la intranet del Gobierno Autónomo Descentralizado Municipal del Cantón Cevallos

CAPITULO II
MARCO TEÓRICO

2.1. Antecedentes Investigativos

En la biblioteca de la facultad de Ciencias de la Computación y Electrónica de la Universidad Tecnológica Americana existe una tesis similar la cual titula: "HACKEO ÉTICO Y SUS PRINCIPALES METODOLOGÍAS", que fue desarrollada por: Liliana Rodríguez en el año 2010, como una memoria técnica previa a la obtención del título de ingeniera en informática.

2.2. Fundamentación legal

La presente investigación se basará en la ley publicada en el Registro Oficial N° 557 del 17 de Abril del 2002.

LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS

DE LAS INFRACCIONES INFORMÁTICAS

Art. 57.- Infracciones informáticas.- Se considerarán infracciones informáticas, las de carácter administrativo y las que se tipifican, mediante reformas al Código Penal, en la presente ley.

Reformas al Código Penal

Art. 58.- A continuación del Art. 202, inclúyanse los siguientes artículos enumerados:

"Art. ....- El que a empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica.

Si la información obtenida se refiere a seguridad nacional, o a secretos comerciales o industriales, la pena será de uno a tres años de prisión y multa de mil a mil quinientos dólares de los Estados Unidos de Norteamérica.

La divulgación o la utilización fraudulenta de la información protegida, así como de los secretos comerciales o industriales, serán sancionadas con pena de reclusión menor ordinaria de tres a seis años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

Si la divulgación o la utilización fraudulenta se realizan por parte de la persona o personas encargadas de la custodia o utilización legítima de la información, éstas serán sancionadas con pena de reclusión menor de seis a nueve años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

Art. ....- Obtención y utilización no autorizada de información.- La persona o personas que obtuvieren información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular o titulares, serán sancionadas con pena de prisión de dos meses a dos años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica.".

Art. 59.- Sustitúyase el Art. 262 por el siguiente:

"Art. 262.- Serán reprimidos con tres a seis años de reclusión menor, todo empleado público y toda persona encargada de un servicio público, que hubiere maliciosa y fraudulentamente, destruido o suprimido documentos, títulos, programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, de que fueren depositarios, en su calidad de tales, o que les hubieren sido encomendados en razón de su cargo.".

Art. 60.- A continuación del Art. 353, agréguese el siguiente artículo enumerado: "Art. ....- Falsificación electrónica.- Son reos de falsificación electrónica la persona o personas que con ánimo de lucro o bien para causar un perjuicio a un tercero, utilizando cualquier medio, alteren o modifiquen mensajes de datos, o la información incluida en éstos, que se encuentre contenida en cualquier soporte material, sistema de información o telemático, ya sea:

1. Alterando un mensaje de datos en alguno de sus elementos o requisitos de carácter formal o esencial;

2. Simulando un mensaje de datos en todo o en parte, de manera que induzca a error sobre su autenticidad;

3. Suponiendo en un acto la intervención de personas que no la han tenido o atribuyendo a las que han intervenido en el acto, declaraciones o manifestaciones diferentes de las que hubieren hecho.

El delito de falsificación electrónica será sancionado de acuerdo a lo dispuesto en este capítulo.".

Art. 61.- A continuación del Art. 415 del Código Penal, inclúyanse los siguientes artículos enumerados:

"Art. ....- Daños informáticos.- El que dolosamente, de cualquier modo o utilizando cualquier método, destruya, altere, inutilice, suprima o dañe, de forma temporal o definitiva, los programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, será reprimido con prisión de seis meses a tres años y multa de sesenta a ciento cincuenta dólares de los Estados Unidos de Norteamérica.

La pena de prisión será de tres a cinco años y multa de doscientos a seis cientos dólares de los Estados Unidos de Norteamérica, cuando se trate de programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, destinada a prestar un servicio público o vinculado con la defensa nacional.

Art. ....- Si no se tratare de un delito mayor, la destrucción, alteración o inutilización de la infraestructura o instalaciones físicas necesarias para la transmisión, recepción o

procesamiento de mensajes de datos, será reprimida con prisión de ocho meses a cuatro años y multa de doscientos a seis cientos dólares de los Estados Unidos de Norteamérica.".

Art. 62.- A continuación del Art. 553, añádanse los siguientes artículos enumerados:

"Art. ....- Apropiación ilícita.- Serán reprimidos con prisión de seis meses a cinco años y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, los que utilizaren fraudulentamente sistemas de información o redes electrónicas, para facilitar la apropiación de un bien ajeno, o los que procuren la transferencia no consentida de bienes, valores o derechos de una persona, en perjuicio de ésta o de un tercero, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas informáticos, sistemas informáticos, telemáticos o mensajes de datos.

Art. ....- La pena de prisión de uno a cinco años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica, si el delito se hubiere cometido empleando los siguientes medios:

1. Inutilización de sistemas de alarma o guarda;
2. Descubrimiento descifrado de claves secretas o encriptadas:
3. Utilización de tarjetas magnéticas o perforadas;
4. Utilización de controles o instrumentos de apertura a distancia; y,
5. Violación de seguridades electrónicas, informáticas u otras semejantes.".

Art. 63.- Añádase como segundo inciso del artículo 563 del Código Penal, el siguiente:

"Será sancionado con el máximo de la pena prevista en el inciso anterior y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, el que cometiere el delito utilizando medios electrónicos o telemáticos.".

DISPOSICIÓN FINAL

El Presidente de la República, en el plazo previsto en la Constitución Política de la República, dictará el reglamento a la presente Ley.

La presente Ley entrará en vigencia a partir de su publicación en el Registro Oficial.

Dada en la ciudad de San Francisco de Quito, Distrito Metropolitano, en la sala de sesiones del Pleno del Congreso Nacional del Ecuador, a los diez días del mes de abril del año dos mil dos.

2.3. Categorías Fundamentales.

Variable Independiente: Hacking ético

Variable Dependiente: Vulnerabilidad en los servicios de la intranet.

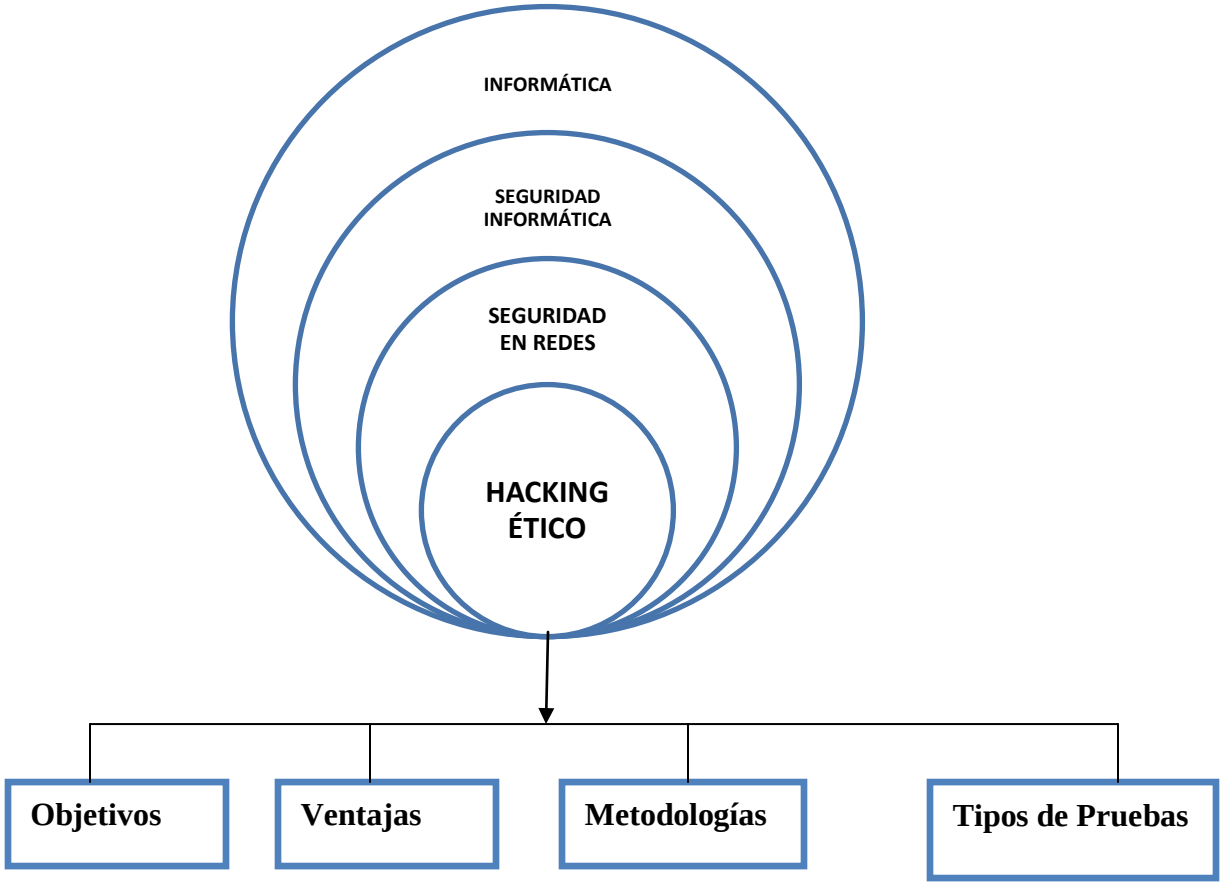


Figura 2. 1*variable Independiente*

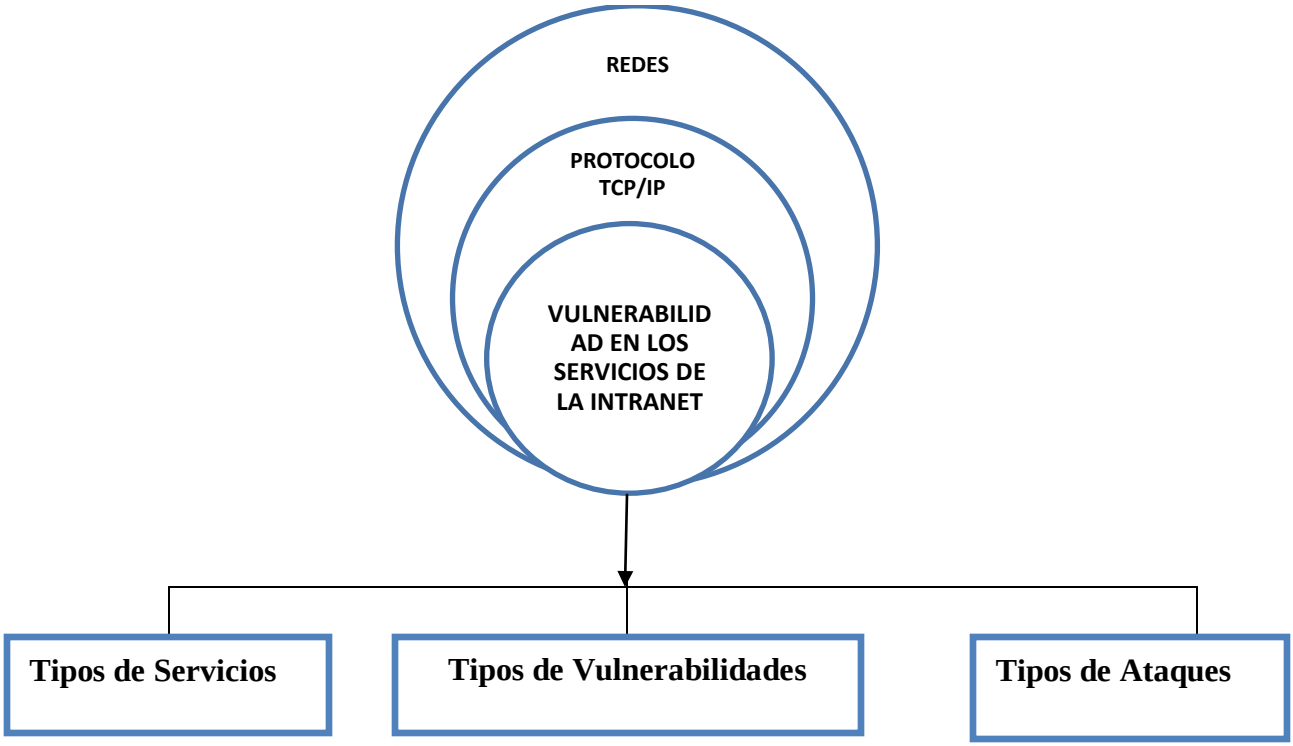


Figura 2. 2*variable Dependiente*

2.3.1. Fundamentación Teórica variable Independiente

2.3.1.1. Informática

Para Antonio Ortiz Medina (Internet: 5, Abril, 2004; 25, Octubre, 2011; 10:59:30), Extraído desde http://www.error500.net/garbagecollector/archives/categorias/apuntes/concepto_de_informatica.php argumenta que:"La informática es la ciencia que estudia el tratamiento automático de la información"

Según Anivar Torres(Internet:11,Octubre,2007;25,Octubre,2011;10:59:30).Extraído desde http://www.monografias.com/trabajos11/curinfa/curinfa.shtml argumenta que la informática es" El tratamiento racional, automático y adecuado de la información, por medio del computador, para lo cual se diseñan y desarrollan estructuras y aplicaciones especiales buscando seguridad e integridad. En el contexto de la informática la información constituye un recurso de gran valor y se busca mantenerla y utilizarla de la mejor manera."

Por otro lado Nervi L. Mejia González (Internet: 6, Noviembre, 2011; 18:34:16), Extraído desde http://www.monografias.com/trabajos15/introduccioninformatica

/introduccion informatica.shtml dice la informática es " la ciencia que se encarga de la automatización del manejo de la información."

Se puede decir entonces que la informática es una ciencia que estudia el comportamiento de la información para lo cual se diseñan y desarrollan estructuras y aplicaciones especiales abarcando el estudio y sistematización de la información.

2.3.1.2. Seguridad Informática.

La seguridad informática según AGUILERA, Purificación. ("s.f", pág. 9). "es una disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable "

Para el Diccionario de informática (internet:20, Noviembre,2011; 18:15:55), Extraído desde http://www.alegsa.com.ar/Dic/seguridad%20informatica.php "la seguridad informática es una disciplina que se relaciona a diversas técnicas, aplicaciones y dispositivos encargados de asegurar la integridad y privacidad de la información de un sistema informático y sus usuarios."

Libro Electrónico de Seguridad Informática y Criptografía. Jorge Aguirre (2006,pág.50) "la cualidad de un sistema informático exento de peligro."

Por lo tanto diremos que seguridad informática es un proceso que se enfoca a la protección de los recursos informáticos, hardware, software y datos, todos estos recursos deben ser utilizados por las personas a quienes se les ha autorizado y solamente para los fines predestinados, y además que estén libres de cualquier peligro, daño o riesgo.

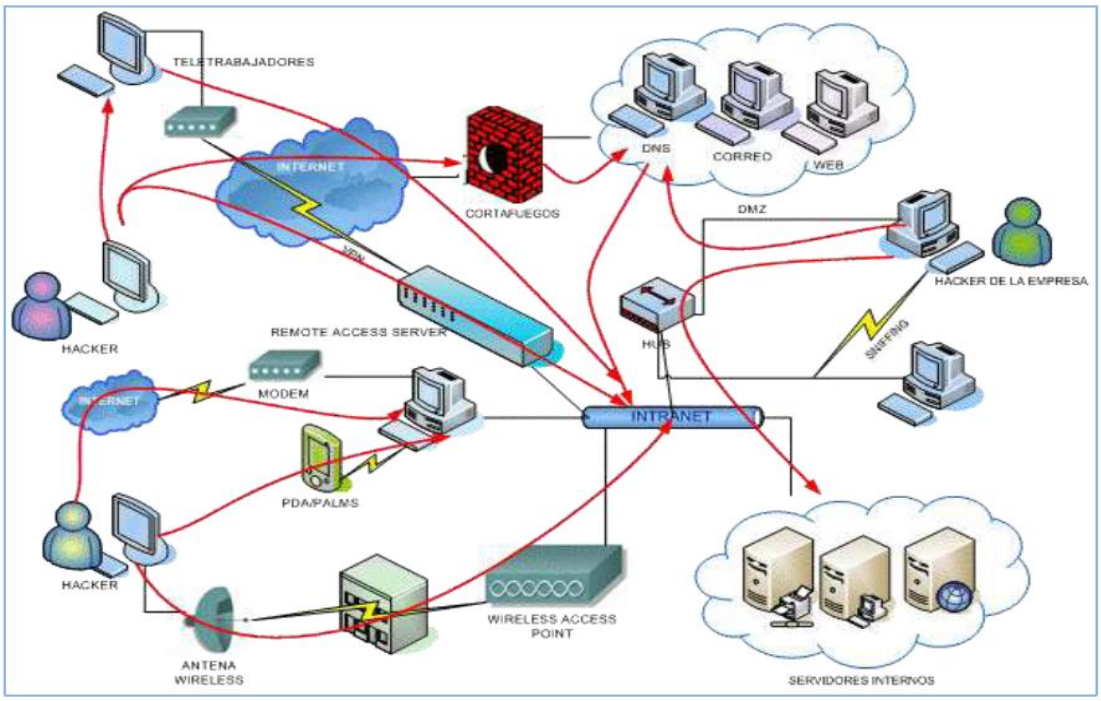


Figura 2. 3 *Topología de red con libre acceso para hackers*

Descripción figura 2.3

Las flechas en color rojo indican los accesos débiles en seguridad de esta red, por donde ingresan los hackers: a través de una VPN, consiguiendo acceso desde una conexión inalámbrica, o evadiendo un cortafuego a través de Internet. Por otro lado un hacker interno logra rápidamente su acceso escalando privilegios en la red o mediante el uso de un sniffing.

a.1. Objetivos de la seguridad informática

La seguridad informática está concebida para proteger los activos informáticos.

a.2. La información contenida

Según el libro Electrónico de Seguridad Informática y Criptografía.Dr. Jorge Ramiro Aguirre (2006, pág. 67) dice así: "La seguridad informática debe ser administrada según los criterios establecidos por los administradores y supervisores, evitando que usuarios externos y no autorizados puedan acceder a ella sin autorización. De lo contrario la organización corre el riesgo de que la información sea utilizada

maliciosamente para obtener ventajas de ella o que sea manipulada, ocasionando lecturas erradas o incompletas de la misma. Otra función de la seguridad informática en esta área es la de asegurar el acceso a la información en el momento oportuno, incluyendo respaldos de la misma en caso de que esta sufra daños o pérdida producto de accidentes, atentados o desastres."

Entonces la información contenida debe ser segura evitando que usuarios externos puedan acceder a ella sin autorización, porque si no se corre el riego de que la información sea utilizada para obtener ventajas de ella.

a.3. La infraestructura computacional

Libro Electrónico de Seguridad Informática y Criptografía. Dr. Jorge Ramiro Aguirre (2006, pág. 68) expresa que: "Una parte fundamental para el almacenamiento y gestión de la información, así como para el funcionamiento mismo de la organización. La función de la seguridad informática en esta área es velar que los equipos funcionen adecuadamente y prever en caso de falla planes de robos, incendios, boicot, desastres naturales, fallas en el suministro eléctrico y cualquier otro factor que atente contra la infraestructura informática."

Por lo tanto diremos que la infraestructura computacional es una parte muy importante dentro de la institución pues, aquí es donde se encarga del perfecto funcionamiento de los equipos de cómputo.

Libro Electrónico de Seguridad Informática y Criptografía. Dr. Jorge Ramió Aguirre (2006, pág. 69) "Son las personas que utilizan la estructura tecnológica, zona de comunicaciones y que gestionan la información. La seguridad informática debe establecer normas que minimicen los riesgos a la información o infraestructura informática. Estas normas incluyen horarios de funcionamiento, restricciones a ciertos lugares, autorizaciones, denegaciones, perfiles de usuario, planes de emergencia, protocolos y todo lo necesario que permita un buen nivel de seguridad informática minimizando el impacto en el desempeño de los funcionarios y de la

organización en general y como principal contribuyente al uso de programas realizados por programadores.”

Definiremos a los usuarios como personas que utilizan estructura tecnológica, zona de comunicaciones y que gestionan la información, los cuales deben estar sujetos a un horario, autorizaciones, denegaciones etc.

2.3.1.3. Seguridad en redes.

Redes de Computadoras. ANDREW S. TANENBAUM.4ta edición (2003, pág. 721) dice que " La seguridad es un tema amplio que cubre una multitud de pecados. En su forma más sencilla, la seguridad se ocupa de garantizar que los curiosos no puedan leer, o peor aún, modificar mensajes dirigidos a otros destinatarios. Tiene que ver con la gente que intenta acceder a servicios remotos no autorizados".

Según la Coordinación de Emergencia en Redes Teleinformáticas de la Administración Pública Argentina, (Internet:9, Noviembre, 2011; 16:17:13), Extraído desde http://www.arcert.gov.ar/webs/manual/manual_de_seguridad.pdf, dice así: “Seguridad en redes es mantener bajo protección los recursos y la información con que se cuenta en la red, a través de procedimientos basados en una política de seguridad tales que permitan el control de lo actuado.”

Es importante también considerar la opinión Julio César Chavez Urrea (Internet: 16 de octubre de 2008, 27, Octubre, 2011; 12:19:18), Extraído desde: http://www.monografias.com/trabajos/protocolotcpip/protocolotcpip.shtml define así: “La seguridad de redes es un nivel de seguridad que garantiza que el funcionamiento de todas las máquinas de una red sea óptimo y que todos los usuarios de estas máquinas posean los derechos que les han sido concedidos:”

Entonces diremos que la seguridad en redes es prevenir, corregir, impedir violaciones a la seguridad mediante niveles de seguridad que garanticen el nivel de seguridad durante la transmisión de los datos.

2.3.1.4. Hacking ético

El Ingeniero Juan David Berrio López (Internet: 2008; 20, Noviembre, 2011; 18:50:43), descargado desde http://www.dsteamseguridad.com/museo /HACKIN%20ETICO_VS_DEFENSA_PROFUNDIDAD_JUANBERRIO.pdf

Considera Desde el Punto de vista Comercial, el "Hacking Ético es un servicio de Auditoría de T.I, que ofrecen empresas especializadas, con el fin de evaluar la seguridad de un sistema informático de forma integral."

Carlos Tori, Hacking Ético (2008, Pág. 35) dice así: Ethical hacking es una metodología utilizada para simular un ataque malicioso sin causar daño.

Es importante también tomar en la definición de hacking ético publicada en Applicalia (Internet: 01, Diciembre, 20011; 10:42:43), extraído desde http://www.applicalia.com/hacking-etico.aspx "Se llama "Hacking Ético" debido a que las técnicas y metodologías usadas son similares a las empleadas por los hackers, pero el único objetivo es comprobar el estado real y actual de la seguridad."

Por lo tanto el hacking ético es una prueba de instrucción que combina pruebas técnicas y herramientas utilizados para una detección integral de vulnerabilidades de los sistemas informáticos.

b.1. VENTAJAS

- Conocer las vulnerabilidades de los diferentes sistemas informáticos para sugerir tomar los correctivos necesarios a tiempo, antes de ser víctimas de un ataque.
- Protección de la inversión, ahorro de costos y tiempo al prevenir pérdidas de información, en lugar de los costos asociados cuando se responde a un evento de forma reactiva.
- Mantenimiento de la imagen corporativa y de la confianza de los contribuyentes, contrario a lo que ocurriría cuando un incidente comprometa la seguridad.

b.2. Objetivos del Hackeo Ético.

- Evaluar la preparación de la empresa o institución para resistir y/o detectar un ataque dirigido, sea éste externo o interno y fortalecer la seguridad de los Sistemas de Información.
- Acceder a los ordenadores de la organización, con permisos de sus propietarios.
- Detectar debilidades y vulnerabilidades de la infraestructura de las tecnologías de información de las organizaciones, y elaborar informes.
- Proporcionar mayor protección y fiabilidad a los sistemas de información de las empresas.

b.3. Tipos de Pruebas de hackeo ético

b.3.1. Hacking de Caja Negra (Black Box Hacking)

Para el Ing. Javier Carracedo (Internet2010; 20, Noviembre,2011;18:38:23)Extraído dede:http://es.scribd.com/doc/68095909/Resumen-Conceptos-basicos-sobre seguridad-y-hacking-etico ,explica que el hacking ético de Caja Negra es el: "Desconocimiento total del cliente (ni direcciones IP, ni infraestructura de red, etc.).Información obtenida por otros medios (RIPE, ARIN, etc.)."

Carlos Tori, Hacking Ético (2008, Pág. 45) Describe al Hacking Ético de caja Negra como un: "chequeo que es llevado a cabo desde cero, sin información, tal como lo haría un intruso cual quiera y lleva mucho más tiempo."

Por lo tanto diremos que este tipo de hacking se efectúa usualmente sobre la red perimetral o pública del cliente, con absoluto desconocimiento de la infraestructura informática del cliente, es decir que no nos proporcionan ninguna información sobre sus sistemas informáticos. El objetivo es emular un ataque externo, realizado por un pirata informático que no tiene relación con la empresa cliente.

b.3.2. Hacking de Caja Gris (Gray Box Hacking)

Carlos Tori, Hacking Ético (2008, Pág. 42) Describe al Hacking Ético de caja Gris como aquel que: "cuenta con conocimientos parciales del objetivo, siempre brindados por la misma organización.

El Ing. Andrés Angulo Dávila (Internet: 27, Octubre, 2011:18:37:56), Extraído desde http://es.scribd.com/doc/91438262/Seminario-Ethical-Hacking argumenta que el hacking de caja gris es un "completo conocimiento de la infraestructura de red objetivo de prueba"

Por lo tanto el hacking de caja gris es aquel que se efectúa sobre la red privada del cliente, pero sin que se nos brinde mayor información sobre la misma; emulando un ataque perpetrado por un usuario interno no-autorizado, ya sea un empleado de la empresa o un asesor externo que tiene acceso físico a la red de la organización.

b.3.3. Hacking de Caja Blanca (White Box Hacking)

Para Javier de Pedro Carracedo(Internet:2010;20,Noviembre,2011;18:38:23)el hacking de caja blanca "Se dispone de toda la información de la organización. Análisis en profundidad de vulnerabilidades (scripts).Informe detallado de vulnerabilidades y recomendaciones."

Carlos Tori, Hacking Ético (2008, Pág. 45) Describe al Hacking Ético de caja Blanca como: "un chequeo lleva do a cabo por un pentester que tiene toda la información acerca del sistema

.Entonces esta clase de hacking también se efectúa sobre la red privada del cliente, pero en esta ocasión se nos debe proporcionar un punto de red con direccionamiento IP válido y un listado de las direcciones IP de los equipos a analizar. La idea es simular un ataque perpetrado por un usuario interno autorizado.

b.4. Metodologías del Hackeo Ético.

b.4.1. Metodología OSSTMM

Para Gonzalo Álvarez Marañon(Internet: 1997-2000; 25, Octubre, 2011; 11:59:48), Extraído desde: http://www.google.com.ec/hackingetico dice que la metodología OSSTMM "Es un estándar profesional para la evaluación de seguridad en cualquier entorno desde el exterior al interior, explica los pasos a seguir, cuando se debe analizar cada una de las áreas que propone."

Por otro lado Maikel Menéndez(Internet: Mayo;2009, 20;Noviembre, 2011; 18:29:30),Extraido desde: http://www.monografias.com/trabajos71/ethical-hacking-test-intrusion-metodologias/ethical-hacking-test-intrusion-metodologias.shtmldice que OSSTMM "Representa un estándar de referencia imprescindible, para todo aquel que quiera llevar a cabo un testeo de seguridad en forma ordenada y con calidad profesional."

Entonces se puede decir que la metodología OSSTMM es un estándar profesional para la evaluación de seguridad en cualquier entorno desde cada una de las áreas que propone.

Estas áreas involucran desde la seguridad de la empresa desde Internet hasta la seguridad física de los accesos a las instalaciones, pasando por técnicas de ingeniería social, incluye también plantillas de los resultados concretos de cada apartado para el cliente.

Esta metodología se limita a la evaluación de seguridad puramente externo, es decir, comprueba la seguridad desde un entorno no privilegiado hacia un entorno privilegiado, para ganar acceso privilegiado evadiendo los componentes de seguridad, procesos y alarmas.

Secciones y Módulos.

La metodología está dividida en secciones, módulos y tareas. Las secciones son puntos específicos en el mapa de seguridad que se superponen entre si y permiten descubrir un todo que es mucho mayor a la suma de sus partes.

Los módulos son el flujo de la metodología desde un punto de presencia de seguridad hacia otro.

Cada módulo tiene una salida y una entrada.

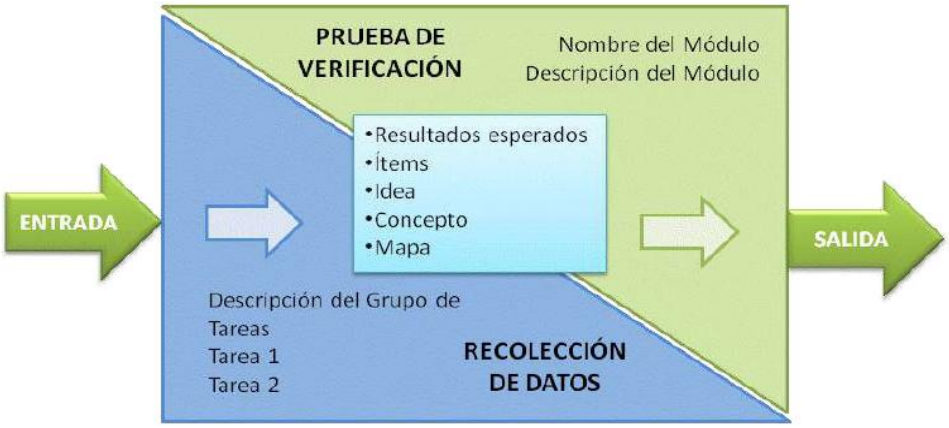


Figura 2. 4: *Módulo de Evaluación y Tareas de OSSTMM*

Metodología ISAAF

Según Maikel Menéndez Méndez(Internet: Mayo;2009, 20;Noviembre, 2011; 18:29:30) http://www.monografias.com/trabajos71/ethical-hacking-test-intrusion-metodologias/ethical-hacking-test-intrusion-metodologias.shtmlISAAF "Constituye un framework detallado respecto de las prácticas y conceptos relacionados con todas y cada una de las tareas a realizar al conducir un testeo de seguridad"

Por otro lado Javier de Pedro Carracedo(Internet:2010;20,Noviembre,2011;18:38:23)argumenta que ISAAF es un "Manual de buenas prácticas en las tareas involucradas en un test de intrusión."

Entonces ISAAF es una metodología estructurada de análisis de seguridad. PTF (Penetración Testing Framework) se trata de un entorno de trabajo detallado de las prácticas y conceptos de todas y cada una de las tareas a ejecutar en una evaluación de seguridad, se trata de un documento que se enfoca en los denominados "Criterios de Evaluación", cada uno de los cuales ha sido escrito y/o revisado por expertos en cada una de las áreas de aplicación.

ISSAF propone tres fases y nueve pasos de evaluación para la realización de una completa prueba de penetración:

Fase I – Planeación y Preparación

Fase II – Evaluación

Fase III – Presentación de Informes, Limpieza y Destrucción de Artefactos.

Fase I: Planeación y Preparación.

En esta fase se prepara todo el escenario para la realización del test de evaluación, considerando esencial un "Acuerdo de Evaluación", firmado por las dos partes, el evaluador y el cliente, que permitirá sentar las bases del proceso y poseer un amparo legal de protección mutua, donde entre otras cosas se especifican, compromiso del grupo de evaluación, tiempos de las pruebas, fechas, etc.

Esta fase se encarga de determinar el alcance, y acuerdos para los test

Fase II: Evaluación.

Es la fase donde se lleva a cabo la prueba de penetración. La figura 6.2 se indica los pasos que se deben seguir en esta fase, los mismos que se deben cumplir de manera cíclica hasta completarlos.

Figura 2. 5: *Fases de Evaluación de ISSAF*

Recolección de Información.

Permite obtener la mayor cantidad posible de información esta es una etapa muy importante para el test y debe realizarse con la mayor cautela para detectar los puntos de vulnerabilidad.

Sondeo de la Red.

Este proceso trata de tomar el "footprint" de la red y los recursos objetivo. Con el uso de varias herramientas y aplicaciones se crea una idea de la topología de red y los host mediante toda la información obtenida en el paso previo. Esto implica: buscar host, escaneo de puertos y servicios, sondeo del perímetro de la red (routers, firewall), identificación de servicios críticos, identificación de los Sistemas Operativos, identificación de routers usando Management Information Base (MIB).

Para la realización de este proceso es necesario establecer un plan previo, para lo cual se debe tomar en cuenta tres aspectos básicos: puntos de debilidad, los puntos más críticos para la organización y considerar todos los datos recolectados.

Identificación de Vulnerabilidades.

Para ello el evaluador debe ya haber identificado los puntos a testear. Durante este proceso se deben ejecutar varias tareas para explotar los puntos débiles detectados. Estas actividades incluyen: identificación de la vulnerabilidad de los servicios usando banners, explotación y verificación de falsos positivos y falsos negativos, enumerar las vulnerabilidades encontradas, estimar el impacto para el cliente, identificar las rutas de ataque y los escenarios para su explotación.

Penetración.

Aquí el evaluador trata de ganar acceso no autorizado para medir los niveles de seguridad, y prueba de las formas posibles el conseguir el acceso al sistema, utilizando tanto herramientas propias como externas.

Ganar Acceso y Escalar Privilegios.

Se intentan obtener cuentas de usuarios (login y contraseñas) del sistema analizado a través de herramientas automáticas utilizadas por los hackers. Se utilizan contraseñas por defecto del sistema, ataques por fuerza bruta, diccionarios de contraseñas, etc. El objetivo posterior al conseguir acceso mediante una cuenta no autorizada al sistema, es conseguir acceso de Administrador.

Manteniendo el Acceso.

Esta metodología toma muy en cuenta la verificación de canales cubiertos, puertas traseras (back doors) o despliegue de rootkits (programas de administración), pues si alguno de estos "huecos" de entrada permanece abierto representa un gran riesgo para

la infraestructura informática de la empresa si son detectadas por un verdadero atacante.

Cubrir las huellas.

Es una práctica común durante una prueba de penetración excepto cuando el cliente no desea. Se trata esencialmente de cubrir las huellas de la intrusión, de las evidencias y actividades que pueden haber realizado.

Ocultar archivos.

Una vez realizadas las pruebas anteriores el evaluador necesita eliminar las evidencias de las actividades realizadas para poder ganar y mantener el acceso en el sistema, con la finalidad de que quede en su estado normal con las seguridades aplicadas. Generalmente para ello simplemente se aplica el atributo "Oculto" que los archivos poseen.

Fase III: Presentación de Informes, Limpieza y Destrucción de Artefactos.

Un reporte mínimo debe constar de un informe verbal y un informe final por escrito.

Presentación de Informes.

Esta metodología se encarga de la presentación de tres tipos de informes, los informes verbales (que no son imprescindibles), el informe final y un informe de los elementos que deben ser eliminados de los sistemas (solo en caso necesario).

Informe Verbal.

En el transcursos de la prueba de penetración si algún aspecto identificado es crítico debe ser inmediatamente reportado para que la organización esté al tanto.

Informe Final.

Luego de completar todos los casos de test a realizar en el alcance previamente definido y estipulado en un documento en la Fase I, se escribe un reporte que describa en forma detallada los resultados de la prueba de penetración. El reporte debe presentar la siguiente estructura:

Resumen Ejecutivo

Alcance del proyecto, indicando los aspectos que no son considerados.

Herramientas que han sido utilizadas.

Registro de horas y fechas en las que se han realizado las pruebas

Los resultados de cada una de las pruebas realizadas.

Una lista de todas las vulnerabilidades detectadas, junto con las recomendaciones para resolverlas.

Limpieza y Destrucción de Artefactos.

Toda información creada y almacenada en los sistemas debe ser removida. Si esto no es posible desde el sistema remoto, todos estos archivos (con su localización) deben ser mencionados en un informe técnico al personal técnico del cliente par que puedan removerlos.

b.4.2. Metodología OWASP

Para Javier de Pedro Carracedo (Internet: 2010; 20, Noviembre, 2011; 18:38:23) "Evaluación de seguridad de aplicaciones web"

Es una metodología totalmente práctica que proporciona un catálogo compuesto por controles de seguridad a evaluar en toda aplicación web.

Esta metodología establece que las causas de un software inseguro se enfocan en vulnerabilidades, desarrolladores, estructura organizativa, procesos de desarrollo, tecnología, incremento de complejidad y de conectividad, y muchas veces también los requerimientos legales.

Se compone de dos partes; la primera parte abarca: principios de la evaluación, explicación de las técnicas, y acerca del entorno de trabajo de OWASP. Y en la segunda parte, se planifican todas las técnicas necesarias para evaluar cada paso del SDCL (Ciclo de Vida del Desarrollo de Software).

OWSAP en su apartado para las pruebas de intrusión de las aplicaciones web indica la manera de realizar la comprobación de vulnerabilidades bajo dos fases:

Modo Pasivo. Indica como la persona a cargo de la realización de las pruebas debería comprender la lógica de la aplicación y determinar los puntos de acceso.

Modo Activo. En esta fase la persona a cargo de la comprobación empieza a realizar las pruebas. Las cuales están divididas en las siguientes subcategorías.

Recopilación de información.

Pruebas de gestión de la configuración.

Pruebas de la lógica de negocio.

Pruebas de Autenticación.

Pruebas de Autorización.

Pruebas de gestión de sesiones.

Pruebas de Validación de datos.

Pruebas de denegación de servicio.

Pruebas de Servicios web.

Pruebas de AJAX.

2.3.2. Fundamentación Teórica variable Dependiente

2.3.2.1. Redes

Según Evelio Martínez (Internet: 20, julio, 2007; 25, Octubre, 2011; 11:18:23) http://www.eveliux.com/mx/concepto-de-red-y-tipos-de-redes.php dice que "una red (en general) es un conjunto de dispositivos (de red) interconectados físicamente (ya sea vía alámbrica o vía inalámbrica) que comparten recursos y que se comunican entre sí a través de reglas (protocolos) de comunicación.".

para Carmen D'Sousa (Internet: 25, Octubre, 2011; 11:40:27) http://www.monografias.com/trabajos11/reco/reco.shtml dice que redes "Es un conjunto de dispositivos físicos "hardware" y de programas "software", mediante el cual podemos comunicar computadoras para compartir recursos (discos, impresoras, programas, etc.) así como trabajo (tiempo de cálculo, procesamiento de datos, etc.)."

Por otro lado Julio César Chávez Urrea (Internet: 9, Noviembre, 2011; 16:57:20) http://www.monografias.com/trabajos/protocolotcpip/protocolotcpip.shtml
"Una red es una configuración de computadora que intercambia información"

Por lo tanto Redes es un conjunto de dispositivos físicos hardware y software que comparten recursos y permiten que circulen elementos o paquetes de información.

c.1. OBJETIVOS Y VENTAJAS

- Compartición de recursos: software y hardware disponibles al usuario independientes de su localización.
- Alta Confiabilidad: Fuentes de información redundantes.
- Ahorro económico: la relación precio rendimiento es mejor en computadores pequeños. Existe posibilidad de escalabilidad.
- Herramienta de comunicación para empleados y personas en particular: e-mail, videoconferencia, capacitación remota, etc.
- Acceso a facilidades e información de manera remota.
- Redes de computadoras han causado un gran impacto social.

c.2. COMPONENTES DE UNA RED

- Servidor: este ejecuta el sistema operativo de red y ofrece los servicios de red a las estaciones de trabajo.
- Estaciones de Trabajo: Cuando una computadora se conecta a una red, la primera se convierte en un nodo de la última y se puede tratar como una estación de trabajo o cliente.
- Tarjetas o Placas de Interfaz de Red: Toda computadora que se conecta a una red necesita de una tarjeta de interfaz de red que soporte un esquema de red específico, como Ethernet, ArcNet o Token Ring.
- Sistema de Cableado: El sistema de la red está constituido por el cable utilizado para conectar entre si el servidor y las estaciones de trabajo.
- Recursos y Periféricos Compartidos: Los dispositivos de almacenamiento ligados al servidor, las unidades de discos ópticos, las impresoras, los trazadores, etc.

c.3. Servicios que se pueden ofrecer dentro de una Intranet.

- Servicios de Usuario
- Servicios de red

c.3.1. Servicios de Usuario: suministran recursos y aplicaciones al usuario final.

- La Intranet facilita la ubicación y administración transparente y sin problemas de contenidos en toda la red, asegurando que solo las personas que tengan

permiso para acceder a la información, pueda obtenerla de manera actualizada y desde cualquier parte de la red.

- Navegación: La intranet facilita la búsqueda de cualquier información o recurso que se encuentre en la red, los usuarios obtienen la información de manera organizada y pueden estar atentos a los cambios que se realizan en los recursos existentes.
- Comunicación: El control de acceso y la seguridad permiten que el correo electrónico y los grupos de discusión sean privados, así como la autentificación en todas las partes en la red.
- El acceso a bases de datos y aplicaciones se lo realiza fácilmente desde una sola interfaz. Todos los servicios de la Intranet están a disposición de las aplicaciones, lo que incluye administración de contenidos, directorios y duplicación.

c.3.2. Servicios de red: permiten interconectar y ejecutar el entorno de red global.

- Directorio: Los servicios de directorio gestionan información referente a personas, control de acceso, configuración de servidores y recursos específicos de las aplicaciones. Los administradores pueden gestionar de manera centralizada el control de acceso y los parámetros de configuración de los servidores de toda la empresa.
- Seguridad: Los servicios de seguridad de la Intranet ofrecen métodos para proteger los recursos contra los usuarios no autorizados, para encriptar y autentificar las comunicaciones y para verificar la integridad de la información.
- Duplicación: La duplicación eleva al máximo la eficiencia de la red, al permitir que información tal como el contenido de las páginas web, los mensajes de los grupos de discusión, directorios y tablas de base de datos se distribuyan en la Intranet.
- Administración: La intranet proporciona una interfaz de administración común, integrada y sencilla de usar que permite gestionar con total seguridad los servidores y recursos desde cualquier lugar de la intranet.

c.4. FUNCIONES DE LOS EQUIPOS DE UNA RED

Los equipos de una red funcionan como clientes o como servidores.

c.4.1. Clientes:

Según Antonio Becerra Terán (Internet: 2001; 20, Enero, 2012; 10:34:23)" Los equipos cliente (por ejemplo, los equipos de los usuarios) solicitan servicios o datos en la red a equipos denominados servidores."

c.4.2. Servidores:

http://www.alegsa.com.ar/Dic/servidor%20de%20base%20de%20datos.php

Para Antonio Becerra Terán (Internet: 2001; 20, Enero, 2012; 10:34:23) Los servidores son equipos que proporcionan servicios y datos a los equipos cliente. Los servidores de una red realizan diversas tareas complejas.

c.4.. Servidores de archivos e impresión

Según Antonio Becerra Terrón (Internet: 2001; 20, Enero, 2012; 10:34:23), Los servidores de archivos e impresión proporcionan recursos de compartición de archivos e impresoras desde una ubicación centralizada.

c.4.1. Servidores de bases de datos

Según Antonio Becerra Terán (Internet: 2001; 20, Enero, 2012; 10:34:23), Los servidores de bases de datos pueden almacenar grandes cantidades de datos en una ubicación centralizada y ponerlos a disposición de los usuarios, quienes no tienen la necesidad de descargar toda la base de datos

c.4.2.Servidores de correo

Según Antonio Becerra Terán (Internet: 2001; 20, Enero, 2012; 10:34:23), Los servidores de correo funcionan igual que los servidores de bases de datos en cuanto a que existen partes de la aplicación en el servidor y partes en el cliente, con datos que se descargan de forma selectiva desde el servidor hasta el cliente.

c.4.3. Servidores de fax

Según Antonio Becerra Terán (Internet: 2001; 20, Enero, 2012; 10:34:23), Los servidores de fax gestionan el tráfico entrante y saliente de faxes en la red y comparten uno o más módems de fax. De este modo, el servicio de fax está disponible para cualquier usuario de la red sin necesidad de instalar una máquina de fax en cada equipo del usuario.

c.4.4. Servidores de servicios de directorio

Según Antonio Becerra Terán (Internet: 2001; 20, Enero, 2012; 10:34:23), Los servidores de servicios de directorio proporcionan una ubicación centralizada para almacenar información sobre la red, incluyendo la identidad de los usuarios que acceden a ella y los nombres de los recursos disponibles en la red. Esto permite administrar la seguridad de la red de modo centralizado.

2.3.2.2. Protocolo Tcp/Ip

El Ing. Francisco José Naranjo (Internet: 28, Septiembre; 9, Noviembre, 2011; 17:03:16) dice "TCP/IP es una familia de protocolos que permiten la comunicación entre máquinas en diferentes redes en una Internet TCP/IP".

Por otro lado Esteban Suarez Custodio da Silva (Internet: 26, Agosto, 2001; 9, Noviembre, 2011; 17:18:34) dice TCP/IP" es el lenguaje básico de comunicación o el protocolo de Internet. También puede ser utilizado como un protocolo de comunicaciones en una red privada (tanto una Intranet como una Extranet)"

Es importante también considerar la opinión de Julio César Chávez Urrea (Internet: 9, Noviembre, 2011; 16:57:20) "Es un protocolo DARPA que proporciona transmisión fiable de paquetes de datos sobre redes."

El protocolo Tcp/Ip es un medio de comunicación entre maquinas en diferentes redes, proporciona transmisión fiable de paquetes de datos sobre redes

2.3.2.3. Vulnerabilidad en los Servicios de la Intranet

Una Vulnerabilidad según AGUILERA, Purificación. ("s.f", pág. 14). "Posibilidades que existen de que una amenaza se materialice contra un activo. No todos los activos son Vulnerables a las mismas amenazas"

d.1. Tipos de Vulnerabilidades:

d.1.1. Físicas

Para los consultores en informática Cristian E. R. Bailey E. (Internet: 15, Diciembre; 2011:10:15:12) la vulnerabilidad física "Se encuentra en el nivel del edificio o entorno físico del sistema. Se relaciona con la posibilidad de entrar o acceder físicamente al sistema para robar, modificar o destruir el mismo"

Por lo tanto diremos que este tipo de vulnerabilidades se relacionan con el espacio donde se encuentran ubicados los dispositivos de la red.

d.1.2. En Hardware

Para los consultores en informática Cristian E. R. Bailey E. (Internet: 15, Diciembre; 2011:10:15:12) Consideran"Desde el punto de vista del hardware, ciertos tipos de dispositivos pueden ser más vulnerables que otros. Así, ciertos sistemas requieren la posesión de algún tipo de herramienta o tarjeta para poder acceder a los mismos.".

Entonces la vulnerabilidad en el hardware comprende aquellos componentes hardware de la red.

d.1.3. En Software

Para los consultores en informática Cristian E. R. Bailey E. (Internet: 15, Diciembre; 2011:10:15:12) la vulnerabilidad a nivel de software son **"**Ciertos fallos o debilidades del software del sistema hacen más fácil acceder al mismo y lo hacen menos fiable. En este apartado se incluyen todos los bugs en los sistemas operativos, u otros tipos de aplicaciones que permiten atacarlos.**".**

La vulnerabilidad a nivel de software Comprenden las aplicaciones de los sistemas Informáticos.

d.1.4. En la Transmisión de la Información

Los consultores en informática Cristian E. R. Bailey E. (Internet: 15, Diciembre; 2011:10:15:12) Argumentan que"Interceptar información que es transmitida desde o hacia el sistema.".

Diremos entonces que la vulnerabilidad en la transición de la información comprende el Inadecuado envió de información

d.2. Tipos de Ataques

d.2.1Interrupción o Denegación de Servicios

Según Oswaldo Puican(Internet:30,Enero,2008;15,Diciembre;2011:10:30:33) la denegación de servicios es" un tipo de ataque cuya meta fundamental es la de negar el acceso del atacado a un recurso determinado o a sus propios recursos.

Como consecuencia, los ataques de negación de servicio pueden esencialmente dejar inoperativa una computadora o una red. De esta forma, toda una organización puede quedar fuera de Internet durante un tiempo determinado."

Es cuando un intruso bloquea la transmisión de la información para que el receptor no la reciba por lo tanto afecta al principio de disponibilidad de la información.

d.2.2. Intercepción: La información es interceptada por una tercera persona cuando el emisor transmite al receptor.

d.2.3. Suplantación de Identidad: El atacante se hace pasar por el emisor generando información y transmitiéndola al receptor, es decir se permite el acceso a personas no autorizadas.

d.2.4. Modificación: La información enviada por el emisor es interceptada para ser alterada y posteriormente ser enviada al receptor.

d.3. Servicios de red

Según José María Barceló Ordinas (Internet: 27, Octubre, 2011; 18:52:34) se considera "Por servicio entendemos la comunicación que se produce dentro de una misma máquina y, por consiguiente, dentro de un único ámbito de responsabilidad"

Por otro lado Julio César Chávez Urrea (Internet: 19, Abril, 2010; 01, Noviembre, 2011:12:23:43) dice que los servicios de red son "un grupo de programas de aplicación que utilizan la red para llevar a cabo tareas útiles de comunicación "Para IPS Intranets(Internet:22,Marzo,1998;01,Noviembre,2011;12:31)"Los servicios de la intranet permiten a los usuarios realizar cualquier tipo de tarea: buscar información, enviar y recibir correo electrónico, buscar en directorios, integrar cualquier tipo de aplicación personalizada y de cualquier fabricante y finalmente centralizar la administración de la red incorporando funciones tales como seguridad y directorios. "

Por lo tanto un servicio de red es un grupo de programas de aplicación que utilizan la red para establecer tareas útiles de comunicación como: buscar información, enviar y recibir correo electrónico, buscar en directorios, integrar cualquier tipo de aplicación personalizada y centralizar la administración de la red incorporando funciones tales como seguridad y directorios.

d.3.1. Servicio web

Para Rafael Navarro Marset(Internet: Julio, 2006; 20,Noviembre, 2011; 19:15:23)" como sistemas software diseñados para soportar una interacción interoperable maquina a maquina sobre una red. Los Servicios Web suelen ser APIs Web que pueden ser accedidas dentro de una red (principalmente Internet) y son ejecutados en el sistema que los aloja."

El ing. Jimmy Wales (Internet: 20, Noviembre, 19:34:45) argumenta que el "Un servicio web (en inglés, Web service) es una pieza de software que utiliza un conjunto de protocolos y estándares que sirven para intercambiar datos entre aplicaciones. Distintas aplicaciones de software desarrolladas en lenguajes de

programación diferentes, y ejecutadas sobre cualquier plataforma, pueden utilizar los servicios web para intercambiar datos en redes de ordenadores como Internet.”

Entonces diremos que Estos servicios proporcionan mecanismos de comunicación estándares entre diferentes aplicaciones, que interactúan entre sí para presentar información dinámica al usuario. Para proporcionar interoperabilidad y extensibilidad entre estas aplicaciones, y que al mismo tiempo sea posible su combinación para realizar operaciones complejas, es necesaria una arquitectura de referencia estándar.

d.3.2. Servicio Ftp

Para Ciacci Miguel (Internet: 23, Noviembre, 2011; 18:42:14) “Es un servicio de Internet que permite transferencia de archivos. Se utiliza en modo cliente-servidor: conectados a un ordenador remoto (que actúa como servidor y que es un gran ordenador permanentemente conectado a Internet) nuestro programa (cliente) nos permite solicitar la transferencia de archivos en cualquiera de las dos direcciones.”

La Universidad de Jaen (Internet:13,Mayo, 2005; 29,Noviembre,2011;17:30:56) argumenta que el servicio Ftp es “El servicio FTP (File Transfer Protocol),es por tanto un servicio que se utiliza para transferir información, almacenada en ficheros, de una máquina remota a otra local, o viceversa. Para poder realizar esta operación es necesario conocer la dirección IP (o el "nombre") de la máquina a la que nos queremos conectar para realizar algún tipo de transferencia.”

Es importante también considerar la opinión de Brandon Harris (Internet 15, Noviembre, 2011; 01, Diciembre, 2011; 15:02:46)“FTP (siglas en inglés de File Transfer Protocol, 'Protocolo de Transferencia de Archivos') en informática, es un por lo tanto el servicio ftp es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor. Desde un equipo cliente se puede conectar a un servidor para descargar archivos desde él o para enviarle archivos, independientemente del sistema operativo utilizado en cada equipo.”

d.3.3. Servicio DHCP

Para Ciacci Miguel (Internet: 23, Noviembre, 2011; 18:42:14) “El servicio DHCP permite acelerar y facilitar la configuración de muchos hosts en una red evitando en gran medida los posibles errores humanos.”

Según Alejandro Disconsi (Internet: 1, Diciembre, 2011; 14:17:34) el servicio dhcp es “Protocolo de configuración dinámica de host Proporciona mecanismo rápido de configuración para el cliente, el administrador puede asignar a los clientes, direcciones IP dinámicas sin necesidad de asignar cliente a cliente los datos correspondientes a su IP”

Por otro lado Jimmy Wales (Internet: 1, Diciembre, 2011; 14:12:04)“DHCP (sigla en inglés de Dynamic Host ConfigurationProtocol - Protocolo de configuración dinámica de host) es un protocolo de red que permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.”

Entonces diremos que el servicio de correo electrónico es actualmente, en conjunto con el de acceso a Web sites, el servicio fundamental en Internet. Los objetivos en cuanto al uso de este servicio incluyen la posibilidad de enviar y recibir mail entre la red e Internet y también disponer de alguna forma de correo corporativo.”

d.3.4. Proxy

Para Dussaut Julieta (Internet: 29, Noviembre; 2011:17:33:34) “Permite el acceso a Internet a todos los equipos de una organización cuando sólo se puede disponer de un único equipo conectado, esto es, una única dirección IP.”

Según Miguel Ángel Álvarez (Internet: 1, Diciembre; 2011:14:33:24) "Un proxy es un programa o dispositivo que realiza una tarea acceso a Internet en lugar de otro ordenador. Un proxy es un punto intermedio entre un ordenador conectado a Internet y el servidor que está accediendo. Cuando navegamos a través de un proxy, nosotros en realidad no estamos accediendo directamente al servidor, sino que realizamos una solicitud sobre el proxy y es éste quien se conecta con el servidor que queremos acceder y nos devuelve el resultado de la solicitud."

Entonces diremos que el servicio proxy, en una red informática, es un programa o dispositivo que realiza una acción en representación de otro, esto es, si una hipotética máquina A solicita un recurso a una C, lo hará mediante una petición a B; C entonces no sabrá que la petición procedió originalmente de A. Su finalidad más habitual es la de servidor proxy, que sirve para interceptar las conexiones de red que un cliente hace a un servidor de destino, por varios motivos posibles como seguridad, rendimiento, anonimato.

2.4. Hipótesis

El uso de Hacking ético influirá en la detección de vulnerabilidades en los servicios de la intranet del Gobierno Autónomo Descentralizado Municipal del Cantón Cevallos.

2.5. Señalamientos de variables

Variable Independiente = Hacking ético

Variable Dependiente= Vulnerabilidad en los servicios de la intranet.

CAPITULO III
METODOLOGÍA

3.1. Enfoque

El proyecto será desarrollado bajo un enfoque Cualitativo porque el problema requiere investigación interna, pues es muy importante lo que se logre detectar con la aplicación del hacking ético para detectar vulnerabilidades en los servicios de la intranet del GAD. Municipal del cantón Cevallos, los objetivos son planteados para poder detectar las vulnerabilidades y el ataque de intrusos determinando una hipótesis con un fin especifico, se emplea un trabajo de campo junto con los miembros del departamento de sistemas, teniendo en cuenta que los resultados obtenidos no serán generalizados ya que nuestro trabajo investigativo va ha ser solamente para mejorar la seguridad en la los servicios de la intranet del GAD. Municipal del Cantón Cevallos.

3.2. Modalidades básicas de la investigación

En la presente investigación fueron tomadas en cuenta las siguientes modalidades:

Modalidad bibliográfica documentada: se ha considerado esta modalidad ya que se ha utilizado libros virtuales, tesis de grado, páginas de internet, monografías, bibliotecas, etc. Que aportaran durante el proceso de la investigación.

Modalidad experimental: se ha considerado la relación de la variable independiente Hacking ético y su influencia y relación en los servicios de la intranet para considerar sus causas y sus efectos.

Modalidad de campo: Se realizara una investigación de campo porque el estudio del problema es en el lugar donde se están generando los hechos; de esta manera podemos conocer mejor los inconvenientes que se producen en la Empresa al no

realizar una detección de vulnerabilidades. Ventaja que nos ayudara a proponer posibles soluciones y así cumplir con los objetivos del proyecto.

3.3. Tipos de investigación

Se ha realizado la investigación exploratoria, ya que permitió plantear el problema de la investigación ¿Cómo la aplicación de hacking ético influye en la detección de vulnerabilidades en los servicios de la intranet del Gobierno Autónomo Descentralizado Municipal del Cantón Cevallos? como de misma manera ayudó a plantear la hipótesis El uso de Hacking ético influirá en la detección de vulnerabilidades en los servicios de la intranet del Gobierno Autónomo Descentralizado Municipal del Cantón Cevallos.

Se consideró también la investigación descriptiva porque permitió analizar el problema en sus partes como delimitar en tiempo y en espacio construyendo el análisis crítico, la contextualización y los antecedentes investigativos.

Por otro lado se uso la investigación correlacional ya que ha permitido medir la compatibilidad de la variable independiente hacking ético con la variable dependiente Vulnerabilidad en los servicios de la intranet.

3.4. Población y muestra

3.4.1. Población

La población que se consideró en la presente investigación fue la totalidad del personal que actualmente labora en el departamento de sistemas del Gobierno Autónomo Descentralizado Municipal del Cantón Cevallos.

3.4.2. Muestra

Como la población a investigar es pequeña la muestra será el mismo valor de la población.

3.5. Operacionalización de variables.

Variable independiente: hacking ético

Concepto	**Categorías**	**Indicadores**	**Ítems**	**Técnicas e Instrumentos**
Es una prueba de intrusión que combina técnicas y herramientas utilizadas para una detección integral de vulnerabilidades en redes, sistemas, informáticos, etc.	Prueba de intrusión técnicas Herramientas Vulnerabilidades	• Grado de debilidad • Metodologías • Políticas de seguridad. • Puertos • Servicios	¿Se ha realizado alguna prueba de instrucción en la red interna de datos? ¿Cuentan la institución con alguna herramienta de software para detectar vulnerabilidades en la intranet? Existen políticas de seguridad dentro de la institución? Al momento del envió de información se utiliza	Entrevista aplicada al personal del departamento de sistemas.

	Sistemas informáticos	• Información • Software	encriptación?. Cree que los sistemas informáticos existentes en la organización son seguros? Alguna vez la información ha sido alterada dentro de la institución?	

Variable Dependiente = Vulnerabilidad en los servicios de la intranet

Concepto	**Categorías**	**Indicadores**	**Ítems**	**Técnicas y Instrumento**
Son puntos débiles dentro de los servicios de aplicación que utiliza la red para compartir recursos.	Puntos débiles. Programas Red	• Acceso • Filtración de información • contraseñas • usuarios • parches • Servidores • routers • Servicios	Se permite el acceso a los servidores a todo el personal? Existen puntos se acceso remoto dentro de la institución?. Conoce usted si existen host que ejecuten servicios innecesarios? Las contraseñas de los servidores son reutilizadas en todos? ¿Los archivos son compartidos	Entrevista aplicada al personal del departamento de sistemas.

	Recursos compartidos	• archivos	confidencialmente?	

3.6. Recolección y análisis de información

Se recolecto de estudios anteriores como son tesis de grado.

Las fuentes de información se encuentran en bibliotecas, internet

SECUNDARIA	PRIMARIA
Se recolecta de estudios realizados anteriormente como tesis de grado que se han realizado anteriormente. Se encuentra registrada en documentos y material impreso: libros, revistas especializadas, informes técnicos, memorias de eventos científicos, tesis de grado, etc. Las fuentes de información son: bibliotecas, hemerotecas, archivos,	Se recolecta directamente atraves del contacto directo con el personal del departamento de sistemas del Gobierno Autónomo Descentralizado Municipalidad del Cantón Cevallos.

Técnicas de investigación:

Bibliográficas	De campo
el análisis de documentos y el fichaje	Entrevista

Recolección de la información

preguntas	explicación

1. ¿Para qué?	Recolectar información primaria para comprobar y contrastar con la hipótesis.
2. ¿A qué personas o sujetos?	empleados
3. ¿Sobre qué aspectos?	VI: Hacking Ético VD: Vulnerabilidad en los servicios de la intranet.
4. ¿Quién?	Nataly Huilca
5. ¿Cuándo?	De acuerdo al cronograma establecido
6. ¿Lugar de recolección de la información?	Gobierno Autónomo Descentralizado Municipal del Cantón Cevallos.
7. ¿Cuántas veces?	1 sola vez
8. ¿Qué técnica de recolección?	Entrevista
9. ¿Con qué?	Cuestionario Cedula de la entrevista
10. ¿En qué situación?	Situación normal y cotidiano

3.7. Procesamiento y análisis de la información

Revisión y codificación de la información

Categorización y tabulación de la información

Tabulación manual

Tabulación computarizada

La presentación de los datos se lo ara atravez de los gráficos y cuadros para analizarlos e interpretarlos

Interpretación de los resultados

1. Describir los resultados analizar la hipótesis en relación con los resultados obtenidos para verificarla o rechazarla.

2. Estudiar cada uno de los resultados por separado

3. Redactar una síntesis general de los resultados

CAPITULO IV
ANALISIS E INTERPRETACION DE RESULTADOS

4.1. Análisis de la necesidad

El Gobierno Autónomo Descentralizado Municipal del Cantón Cevallos al ser una institución gubernamental tiene la obligación de mantener la información segura, es decir se deben cumplir los requerimientos de seguridad informática mencionados anteriormente en el capítulo II.

Entonces existe la necesidad de detectar vulnerabilidades dentro de los servicios de la intranet para dar posibles soluciones y así salvaguardar la información que día a día es transmitida por la red.

4.2. Análisis de los resultados

Para determinar la necesidad se realizó entrevistas aplicadas al personal del departamento de sistemas del Gobierno Autónomo Descentralizado Municipal del Cantón Cevallos el cual está conformado por tres personas un administrador de red el cual permanece en la institución, un revisor de servidores que realiza visitas para dar mantenimiento a los servidores, y por ultimo un funcionario encargado para cuando surja algunos inconvenientes y el administrador de sistemas no se encuentre.

Una vez aplicada la entrevista se obtuvieron como resultado los siguientes datos.

1. **¿Se ha realizado alguna prueba de intrucción(hacking ético) en la red interna de datos?**

Respuesta	Cantidad	Porcentaje
no	3	100%
si	0	0%

Tabla 4. 1: *Tabulación de la entrevista - pregunta 1*

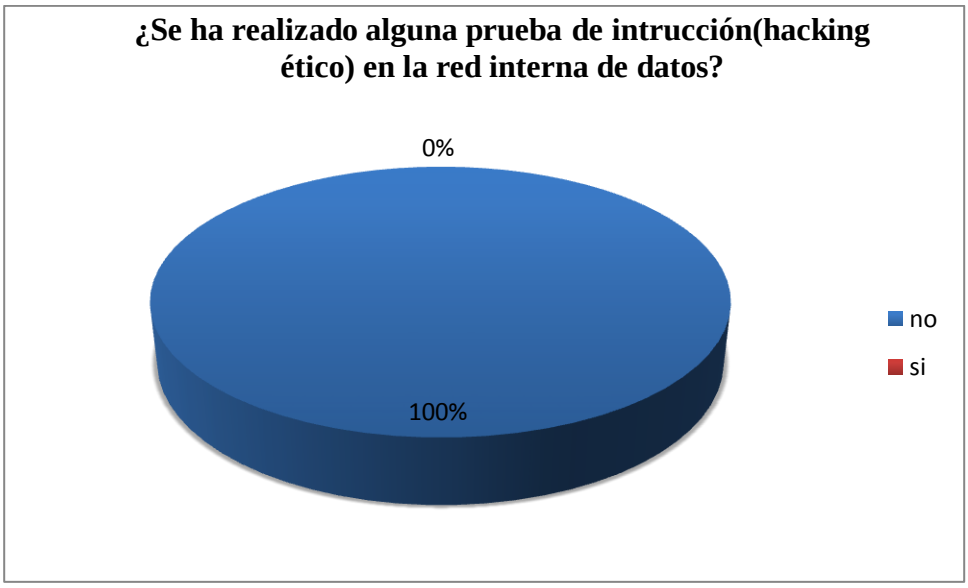


Figura 4. 1: ***Tabulación de la entrevista - pregunta 1***

Análisis Cuantitativo: De los entrevistados el 100% que representa 3 personas respondieron que no se ha realizado ninguna prueba de instrucción en la red interna de datos

Análisis Cualitativo: Por lo tanto se demuestra que en la institución no se ha realizado pruebas de instrucción en la intranet, por lo tanto va a ser la primera vez que se llevará a cabo una investigación de esta magnitud.

2. **¿Cuentan la institución con alguna herramienta de software para detectar vulnerabilidades en la intranet?**

Respuesta	Cantidad	Porcentaje
no	3	100%
si	0	0%

Tabla 4. 2: *Tabulación de la entrevista - pregunta 2*

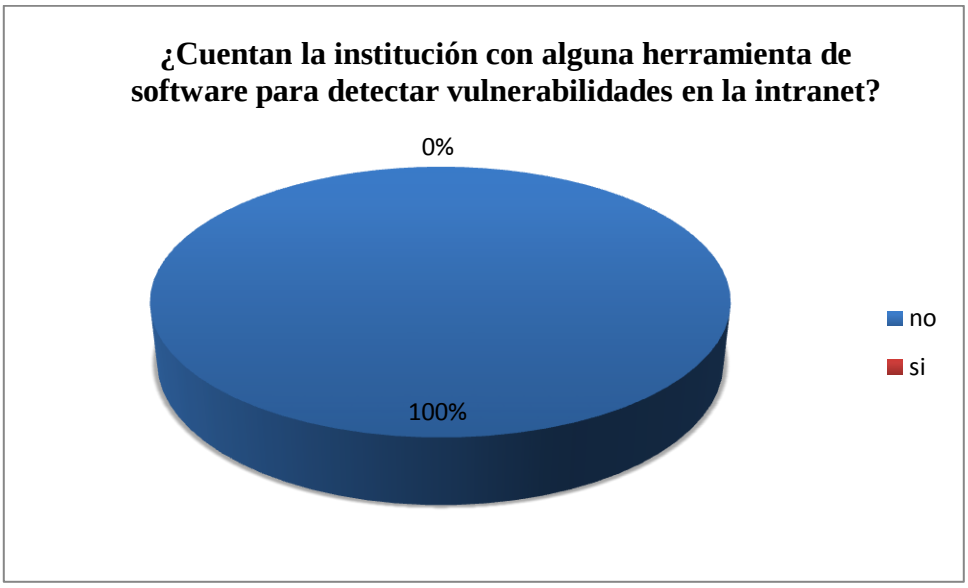


Figura 4. 2: *Tabulación de la entrevista - pregunta 2*

Análisis Cuantitativo: De los entrevistados el 100% que representa 3 personas manifestaron que la institución no cuenta con herramienta de software para detectar vulnerabilidades en la intranet.

Análisis Cualitativo: Se demuestra que en la institución no existen herramientas de software para detectar vulnerabilidades, por ende la intranet con sus respectivos servicios tiende a ser insegura.

3. ¿Existen políticas de seguridad dentro de la institución?

Respuesta	Cantidad	Porcentaje
NO	2	0%
Algunas	1	67%
si	0	33

Tabla 4. 3: *Tabulación de la entrevista - pregunta 3*

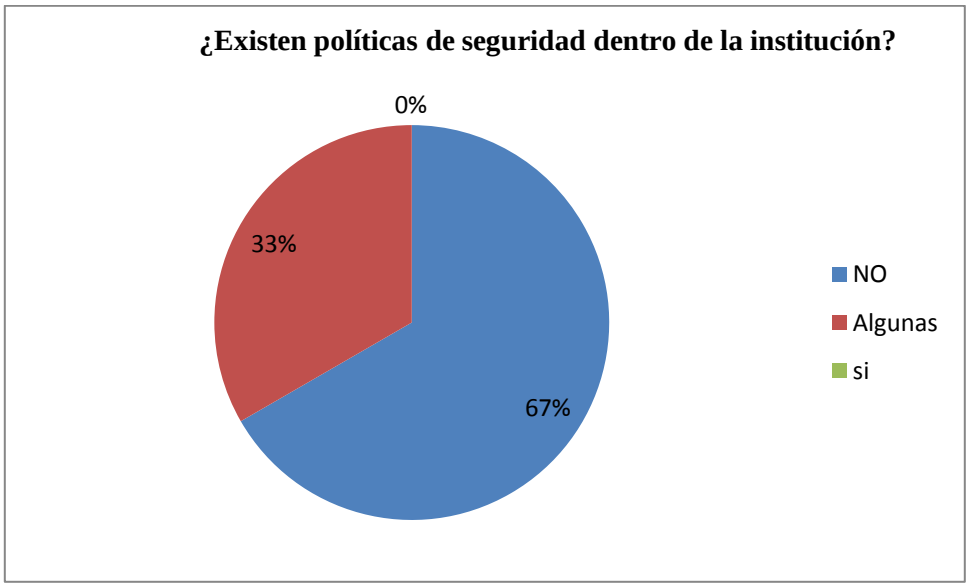


Figura 4. 3: *Tabulación de la entrevista - pregunta 3*

Análisis Cuantitativo: De los entrevistados el 67% que representa 2 personas dijeron que no existen políticas de seguridad dentro de la institución y un 33% equivalente a 1 persona dijo que la institución si cuenta con algunas políticas de seguridad como son Iptable y Routing.

Análisis Cualitativo: Se demuestra que en la institución si cuenta con algunas políticas de seguridad aunque estas no sean tan representativas, entonces se puede decir que la intranet si es un poco segura.

4. **¿Al momento del envió de información se utiliza encriptación?**

Respuesta	Cantidad	Porcentaje
NO	2	67%
NO SE	1	33%
SI	0	0%

Tabla 4. 4: *Tabulación de la entrevista - pregunta 4*

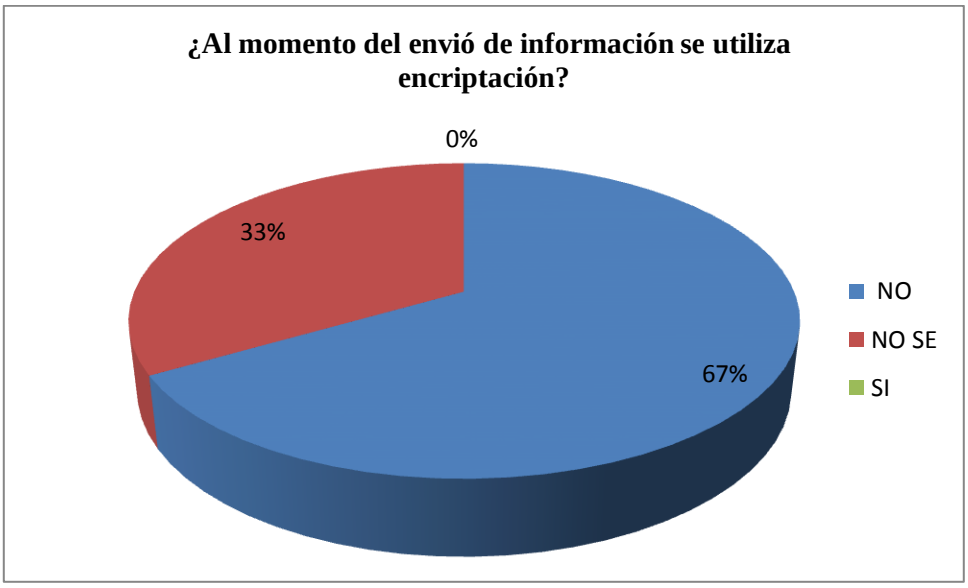


Figura 4. 4: *Tabulación de la entrevista - pregunta 4*

Análisis Cuantitativo: De los entrevistados el 67% que representa 2 personas indicaron que al momento del envió de información no se utiliza encriptación; mientras un 33% equivalente a 1 persona indico que no sabe nada al respecto.

Análisis Cualitativo: Se demuestra que en la institución al momento de envió de la información no se utiliza encriptación, entonces la información puede ser conocida o alterada por terceras personas.

5. **¿Cree que los sistemas informáticos existentes en la institución son seguros?**

Respuesta	Cantidad	Porcentaje
NO	2	67%
TALVEZ	1	33%
SI	0	0%

Tabla 4. 5: *Tabulación de la entrevista – pregunta 5*

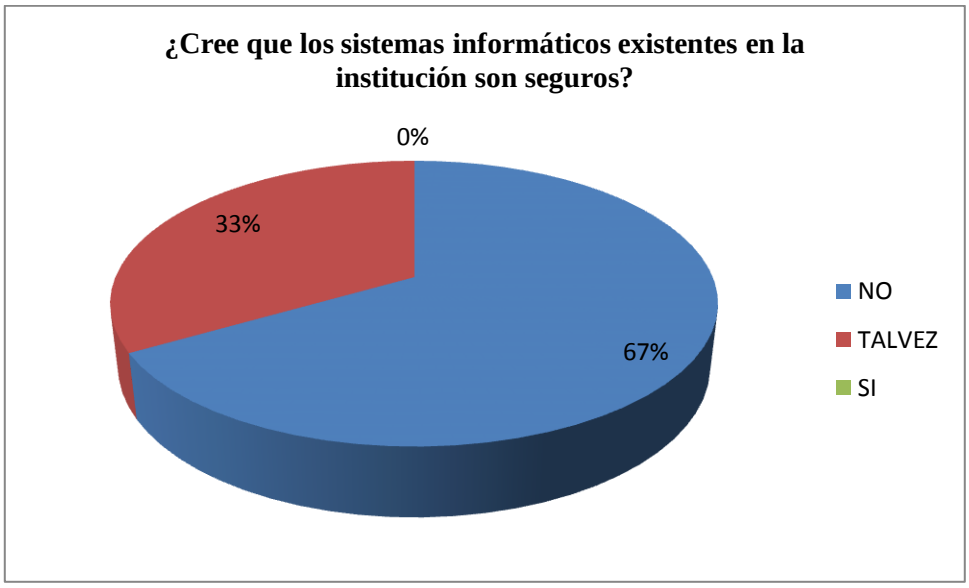


Figura 4. 5: *Tabulación de la entrevista - pregunta 5*

Análisis Cuantitativo: de los entrevistados un 67% equivalente a 2 persona respondió que no, mientras el 33% equivalente a una persona ha manifestado que tal vez los sistemas informáticos pueden ser seguros.

Análisis Cualitativo: no se puede decir que los sistemas informáticos son o no son seguros porque existen versiones diferentes por parte de los entrevistados.

6. ¿Alguna vez la información ha sido alterada dentro de la institución?

Respuesta	Cantidad	Porcentaje
NO	0	0%
SI	3	100%

Tabla 4. 6: *Tabulación de la entrevista – pregunta 6*

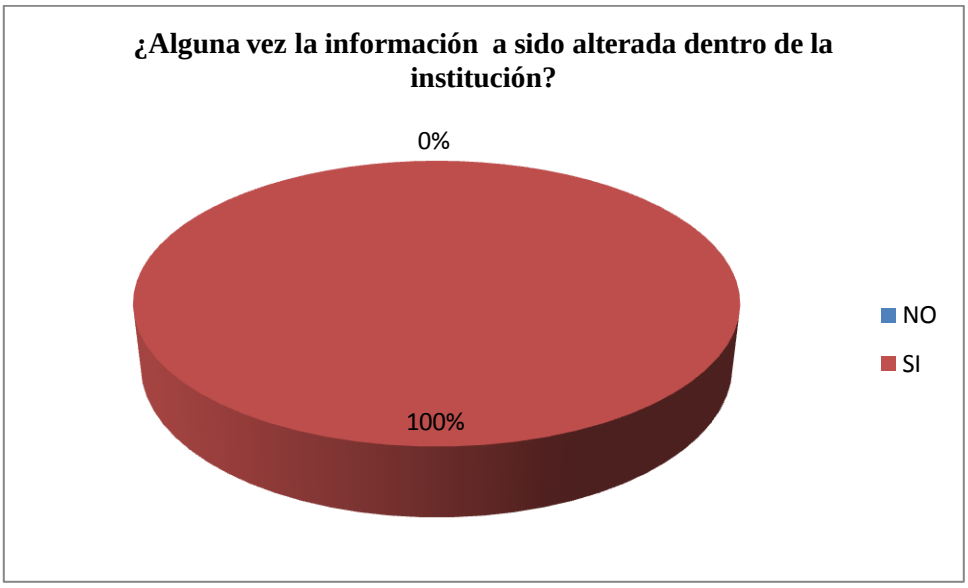


Figura 4. 6: *Tabulación de la entrevista – pregunta 6*

Análisis Cuantitativo: De los entrevistados el 100% equivalente a 3 persona respondieron que si alguna vez la información fue alterada debido a que fue hackeada la pagina web.

Análisis Cualitativo: por los antecedentes de hackeo de la página web es posible que existan vulnerabilidades en la intranet.

7. ¿Se permite el acceso a los servidores a todo el personal?

Respuesta	Cantidad	Porcentaje
NO	3	100%
SI	0	3%

Tabla 4. 7: *Tabulación de la entrevista – pregunta 7*

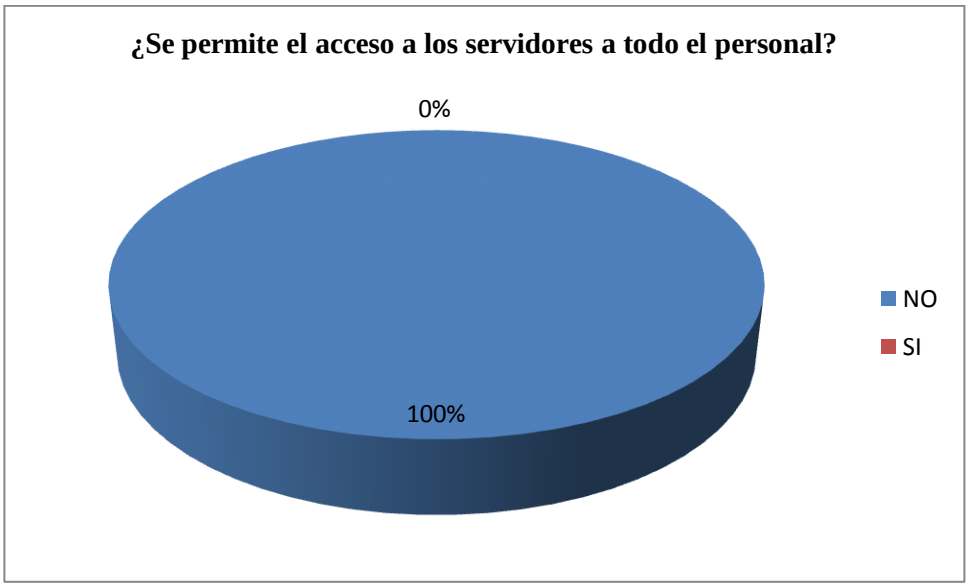


Figura 4. 7: *Tabulación de la entrevista - pregunta 7*

Análisis Cuantitativo: De los entrevistados el 100% equivalente a 3 persona respondió que no se permite el acceso a los servidores a todo el personal.

Análisis Cualitativo: se demuestra entonces que solamente el personal autorizado puede ingresar a los servidores.

8. Existen puntos se acceso remoto dentro de la institución?.

Respuesta	Cantidad	Porcentaje
NO	2	67%
NOSE	1	33%
SI	0	0%

Tabla 4. 8: *Tabulación de la entrevista – pregunta 9*

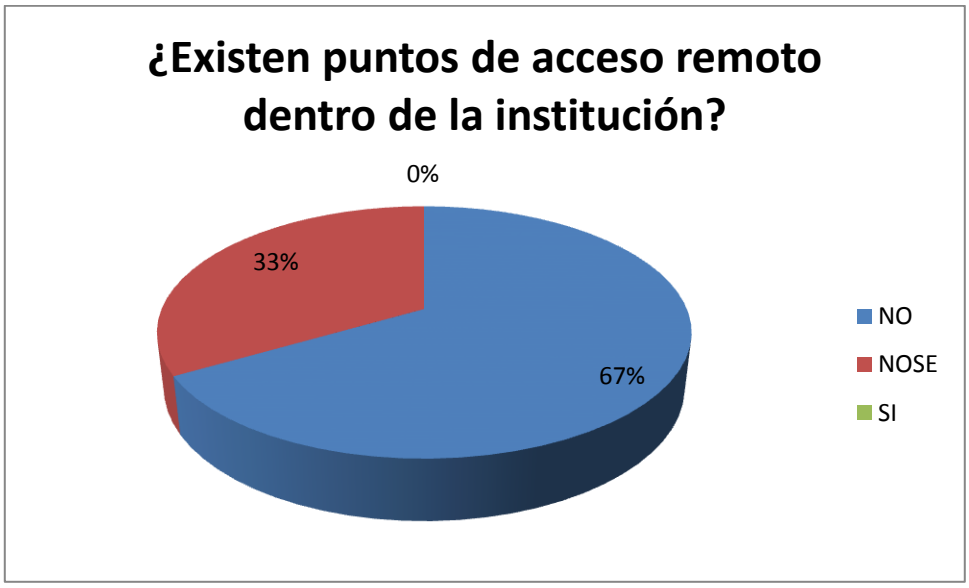


Figura 4. 8: *Tabulación de la entrevista – pregunta 8*

Análisis Cuantitativo: De los entrevistados el 67% equivalente a 2 personas manifestaron que no existen puntos de acceso remoto dentro de la institución; un 33% equivalente 1 persona respondió no sabe.

Análisis Cualitativo: entonces diremos que no existen puntos de acceso dentro de la institución.

9. ¿Conoce usted si existen host que ejecuten servicios innecesarios?

Respuesta	Cantidad	Porcentaje
NO	3	100%
SI	0	0%

Tabla 4. 9: *Tabulación de la entrevista – pregunta 9*

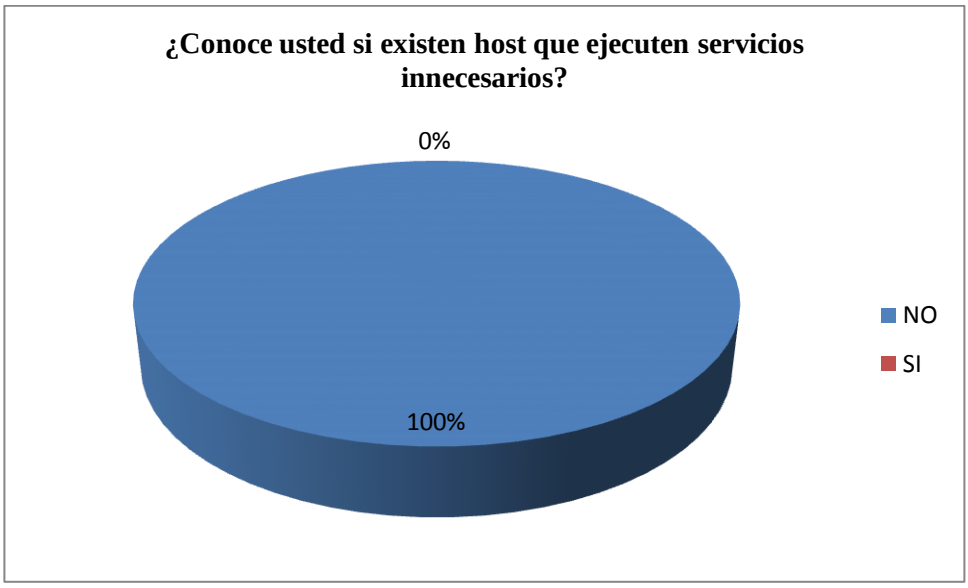


Figura 4. 9: *Tabulación de la entrevista – pregunta 9*

Análisis Cuantitativo: De los entrevistados el 100% equivalente a 3 persona respondió que no saben si existen host ejecutando servicios innecesarios.

Análisis Cualitativo: hace falta revisar utilizando herramientas de software para ver si existen o no host ejecutando servicios innecesarios.

10. ¿Las contraseñas de los servidores son reutilizadas en todos?

Respuesta	Cantidad	Porcentaje
NO	3	100%
SI	0	0%

Tabla 4. 10: *Tabulación de la entrevista – pregunta 10*

Figura 4. 9: *Tabulación de la entrevista – pregunta 10*

Análisis Cuantitativo: De los entrevistados el 100% equivalente a 3 persona respondió que las contraseñas no son reutilizadas en todos los servidores.

Análisis Cualitativo: es algo importante no reutilizar contraseñas ya que si alguien conoce la contraseña de uno ya conocería de todos.

11. ¿Los archivos son compartidos confidencialmente?

Respuesta	Cantidad	Porcentaje
NO	0	0%
AVECES	2	67%
SI	1	33%

Tabla 4. 8: *Tabulación de la entrevista – pregunta 11*

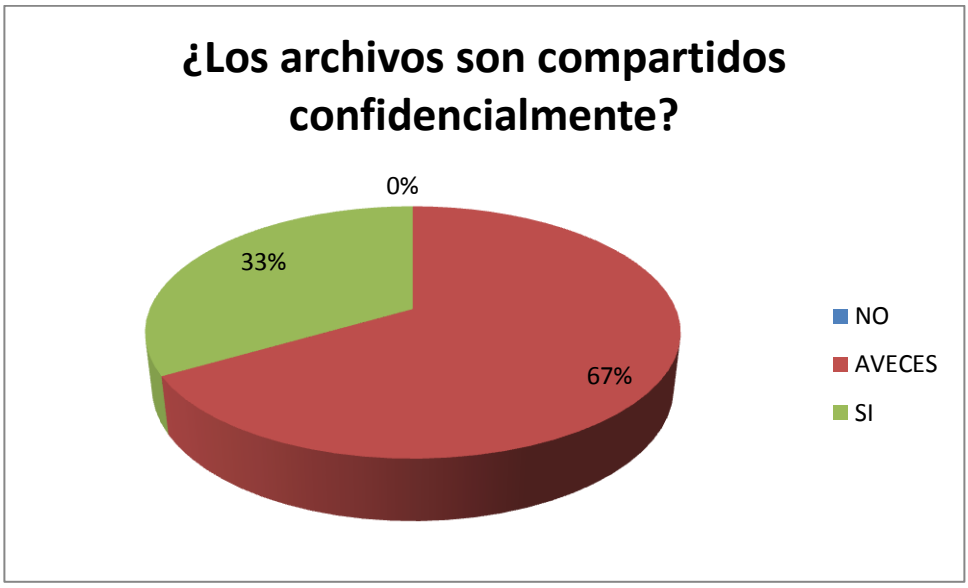


Figura 4. 8: *Tabulación de la entrevista – pregunta 11*

Análisis Cuantitativo: De los entrevistados el 67% equivalente a 2 persona manifestó que los archivos a veces son compartidos confidencialmente utilizando usuarios y contraseñas, el 37% equivalente a 1 persona dijo que si.

Análisis Cualitativo: diremos que a veces los archivos son compartidos confidencialmente.

Interpretación total entrevista

De acuerdo a las versiones que ha manifestado los señores encargados del departamento de sistemas del Gobierno Autónomo Descentralizado Municipal del Cantón Cevallos nunca se ha realizado una prueba de instrucción dentro de la institución, como tampoco la institución cuenta con herramientas de software para detectar vulnerabilidades a nivel de los servicios de la intranet, se menciona que se han tomado como medida de seguridad los iptables y el routing, el envió de información se lo realiza normalmente sin encriptación, con respecto a los sistemas informáticos estos no son seguros por lo cual pueden ocasionar la filtración de información cosa que ya sucedió el portal web de la institución fue atacado. En cuanto al acceso del personal se refiere solamente puede ingresar personal autorizado, no existen puntos de acceso dentro de la institución así como también existen host

que ejecuten servicios innecesarios, cada servidor tiene su propia contraseña y los archivos a veces son compartidos de forma confidencial utilizando cuentas de usuarios y contraseñas.

CAPITULO V
CONCLUSIONES Y RECOMENDACIONES

El presente capitulo comprende las conclusiones y recomendaciones fundamentadas en los resultados presentados y analizados, conforme a los objetivos de estudio.

5.1. CONCLUSIONES

- EL Gobierno Autónomo Descentralizado Municipal del Cantón Cevallos no cuenta con ningún software informático para detectar vulnerabilidades en los servicios de la intranet de acuerdo a la entrevista realizada al personal encargado del departamento de sistemas.
- Los sistemas informáticos que posee la institución no son totalmente seguros por lo que se está poniendo en riesgo la seguridad de la información mediante la utilización de sistemas informáticos inseguros.
- La institución no cuenta con suficientes políticas de seguridad para salvaguardar los datos existentes en la institución.
- Los archivos en ocasiones son compartidos confidencialmente utilizando usuarios y contraseñas.
- El portal web de la institución fue hackeado por lo que se puso en riesgo la seguridad de la información que posee la institución ya que esta pudo ser alterada modificada o en el peor de los casos pudo ser borrada en su totalidad.

5.2. RECOMENDACIONES

- Debido a la inexistencia de un software informático dentro del Gobierno Autónomo Descentralizado Municipal del Cantón Cevallos se recomienda contar con software informático para detectar vulnerabilidades en los servidores y servicios que posee la intranet este software debe ser libre para evitar costos de licencias.
- Por la inseguridad que poseen los sistemas informáticos existentes en la institución es necesario aumentar seguridades en los sistemas para asegurar la información.
- Se debe 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.
- Para conseguir una confidencialidad más segura en el momento del envió de archivos es importante además de crear claves y contraseñas tratar de obtener certificados de seguridad o encriptar los datos.
- Se recomienda usar el Hacking ético para detectar vulnerabilidades en los servicios de la intranet del Gobierno Autónomo Descentralizado Municipal del Cantón Cevallos porque con la detección de las mismas a tiempo se reportaran las fallas de seguridad en la red alertando al personal del área de sistemas y se podrá brindar posibles soluciones para que estos inmediatamente arreglen los problemas encontrados y así evitar un posible robo o alteración de la información.

Preguntas discriminantes

¿Se ha realizado alguna prueba de intrucción (hacking ético) en la red interna de datos?

Los señores encargados del departamento de sistemas del Gobierno Autónomo Descentralizado Municipal del Cantón Cevallos manifiesta que no se ha realizado ninguna prueba de instrucción en la red interna de datos.

2. ¿Cuentan la institución con alguna herramienta de software para detectar vulnerabilidades en la intranet?

Dando respuesta a la pregunta #2 los entrevistados argumentan que la institución no cuenta con ninguna herramienta de software para detectar vulnerabilidades en la intranet.

3. ¿Existen políticas de seguridad dentro de la institución?

Los entrevistados indican que en si existen algunas medidas de seguridad dentro de la institución que son las siguientes IPTables y Routing aunque una parte de los entrevistados indican que no son las suficientes.

Comentario

Se han tomado en cuenta estas preguntas porque mediante las mismas se puede saber si el proyecto de investigación que se llevará a cabo es útil para la institución y este a su vez ayudará a salvaguardar la información.

CAPITULO VI
PROPUESTA

6.1. DATOS INFORMATIVOS

- **Titulo**

"Hacking ético para detectar vulnerabilidades en los servicios de la intranet del Gobierno Autónomo Descentralizado Municipal del Cantón Cevallos".

- **Institución ejecutora**

  Gobierno Autónomo Descentralizado Municipal del Cantón Cevallos.

- **Director de tesis**

  Ing. Msc. Alberto Arellano A.

- **Beneficiario**

  Gobierno Autónomo Descentralizado Municipal del Cantón Cevallos.

- **Ubicación**

  Avenida 24 de Mayo y Felipa Real.

- **Tiempo estimado para la ejecución**

  Fecha de inicio: Enero del 2012

  Fecha de Finalización: Julio del 2012

- **Equipo técnico responsable**
  - Investigadora: Nataly Huilca

6.2. ANTECEDENTES DE LA PROPUESTA

Hoy en día la mayoría de empresas, instituciones públicas privadas y gubernamentales han sufrido un sinnúmero de ataques informáticos especialmente en lo que al robo, alteración y modificación de la información se refiere, por lo que se han visto en la necesidad de tomar medidas de seguridad para salvaguardar confidencialmente se información.

Luego de haber aplicado una entrevista al personal encargado del departamento de sistemas sea podido averiguar lo siguiente que el Gobierno Autónomo Descentralizado Municipal del Cantón Cevallos no cuenta con ningún software informático para detectar vulnerabilidades en los servicios de la intranet así como los sistemas informáticos que posee la institución no son confiables por lo que se está poniendo en riesgo la seguridad de la información. Además el portal web de la institución fue hackiado por lo que se puso en riesgo la seguridad de la información que posee la institución ya que esta pudo ser alterada modificada o en el peor de los casos pudo ser borrada en su totalidad.

Es por esto que el Gobierno Autónomo Descentralizado Municipal del Cantón Cevallos debe contar con software informático para detectar vulnerabilidades en los servidores y servicios que posee la intranet, así como también se debe aumentar la seguridades en los sistemas informáticos estableciendo algunas políticas de seguridad dentro de la institución, Para conseguir una confidencialidad más segura en el momento del envió de archivos por lo cual es conveniente usar el Hacking ético para detectar vulnerabilidades en los servicios de la intranet del Gobierno Autónomo Descentralizado Municipal del Cantón Cevallos

6.3. JUSTIFICACION

Es primordial que el presente trabajo investigativo se lo realice ya que la detección de vulnerabilidades en los servicios de la intranet del Gobierno Autónomo Descentralizado Municipal del Cantón Cevallos ayudará a evaluar, y determinar el

grado de incidencia de las mismas en cuanto a la seguridad de la información se refiere.

Proteger la información

Con la aplicación de Hacking ético se podrá detectar a tiempo las vulnerabilidades encontradas dentro de la intranet del Gobierno Autónomo Descentralizado Municipal del Cantón Cevallos, ayudando a alertar al administrador antes de un ataque a los servidores por ser estos vulnerables o en el caso de que la contraseña de la red inalámbrica sea descubierta.

Estabilidad en los servicios

Es importante que los servidores que son los que contiene la información sean seguros de esta manera los servicios que estos prestan serán seguros y así la transmisión de la información se realizara en forma segura. Es por esto que los servidores con sus respectivos servicios tienen que estar bien configurados con todas las medidas de seguridad, para cuando se necesite cualquier información esta sea transparente.

6.4. Objetivos

6.4.1. Objetivo General

Detectar vulnerabilidades en los servicios de la intranet del Gobierno Autónomo Descentralizado Municipal del Cantón Cevallos mediante el uso del Hacking ético.

6.4.2. Objetivo Específicos

- Seleccionar las herramientas de hacking ético bajo software libre que los hackers comúnmente utilizan.
- Realizar pruebas de intrucción en los servidores de la intranet del Gobierno Autónomo Descentralizado Municipal del Cantón Cevallos.

- Elaborar un informe técnico de las vulnerabilidades encontradas y del grado de incidencia de estas en la inseguridad de la información en los servicios de la intranet del Gobierno Autónomo Descentralizado Municipal del Cantón Cevallos.

6.5. Análisis de Factibilidad

Según el tipo de propuesta se debe tener en cuenta ciertos aspectos de viabilidad:

Política: El gobierno Autónomo Descentralizado Municipal del Cantón Cevallos tiene como política asegurar la información por lo cual es viable usar el hacking ético para detectar vulnerabilidades.

Socio Cultural: si hay un buen manejo de la información se minimizarán la s vulnerabilidades y se ayudará a tratar la información de los ciudadanos en forma ética y confidencial.

Tecnológica: El uso de hacking ético mejorara las condiciones de seguridad en los servicios de la intranet del gobierno Autónomo Descentralizado Municipal del Cantón Cevallos.

Ambiental: En la realización del presente proyecto no se afectará al medio ambiente.

Económico-financiera: el proyecto en el ámbito económico es factible de realizarlo ya que todas las herramientas de software que se utilizaran son libres por lo cual no se pagaran los costos de licencia.

Legal: El proyecto de investigación es viable porque está cumpliendo todas las leyes normas y metodologías de hackeo ético.

6.6. Fundamentación Científico Técnica

6.6.1. Herramientas del Hackeo Ético.

Footprinting

Para Víctor H. Montero (Internet: Noviembre, 2005; 23, Enero, 2011,17:33:4)" Es el análisis del perfil de la seguridad informática de la empresa mediante la obtención de información crítica, como nombre del dominio, direcciones de red y aplicaciones instaladas, arquitectura del sistema, IDS, mecanismos de control de acceso, datos personales de los empleados, etc."

En esta fase se define la estrategia o metodología que el atacante usará para efectuar el hackeo.

Las herramientas utilizadas son: base de datos WHOIS, DNS Stuff, nsloockup, traceroute, ping, email Hunter, newsGroupExplorer, email Logger, BackTrack, etc.

Scanning (Escaneo). Es la recopilación de información a manera de inventario de
Las vulnerabilidades, generalmente se realiza un escaneo de puertos asociados a
Los servicios que estén corriendo, que ayuda a planificar la estrategia para el
Ingreso al sistema.

Enumeration (Enumeración). Es la identificación de cuentas y grupos válidos de usuario, recursos compartidos de red, tablas de enrutamiento, información del
SNMP. Se enfoca a conexiones activas y dirigidas a un equipo específico, para lo cual se suelen respaldar en los logs, NAT (Network Address Traslation), BackTrack, Enum, UserInfo, SNMPutil, Advanced IPScan, etc.

Hackeo (Ataque). El hacker ingresa al sistema, para lo cual el hacker ético debe contar con el consentimiento del propietario de o representante de la empresa. El hacker trata de autenticarse remotamente con una cuenta de altos privilegios mediante la predicción de nombres de cuentas y contraseñas, u obtención de archivos hash de contraseñas, o utilizando un exploits y keyloggers (grabadores de impulsos del teclado). Se utilizan herramientas como: John the Ripper, keyloggers, Cain & Abel, Kismet, Aircrack (en redes inalámbricas).

Los hackers también utilizan rootkits, virus, troyanos, sniffers o scripts elaborados por ellos mismos.

6.6.2. BackTrack

Según el portal de software libre (Internet: 2010; 12, enero, 2012; 19:34:34) BackTrack "es una distribución GNU/Linux en formato LiveCD pensada y diseñada para la auditoría de seguridad y relacionada con la seguridad informática en general. Actualmente tiene una gran popularidad y aceptación en la comunidad que se mueve en torno a la seguridad informática."

Se deriva de la unión de dos grandes distribuciones orientadas a la seguridad, el Auditor + WHAX. WHAX es la evolución del Whoppix (WhiteHat Knoppix), el cual pasó a basarse en la distribución Linux SLAX en lugar de Knoppix. La última versión de esta distribución cambió el sistema base, antes basado en Slax y ahora en Ubuntu.

Incluye una larga lista de herramientas de seguridad listas para usar, entre las que destacan numerosos scanners de puertos y vulnerabilidades, archivos de exploits, sniffers, herramientas de análisis forense y herramientas para la auditoría Wireless.

Backtrack actualmente está constituida por más de 300 herramientas actualizadas, que están estructuradas de manera lógica de acuerdo al flujo de trabajo de los profesionales de seguridad. Esta estructura permite que incluso los recién llegados puedan ubicar las herramientas relacionadas para una determinada tarea que debe realizarse. Las nuevas tecnologías y técnicas de prueba son incluidas en BackTrack tan pronto como sea posible para mantenerla actualizada.

Ninguna otra plataforma de análisis Libre o Comercial ofrece un nivel equivalente de usabilidad con una configuración automatizada y enfocada a Pruebas Penetración.

Las nuevas características de BackTrack incluyen:

Kernel 2.6.18.1 con soporte mejorado de hardware.

El soporte nativo para tarjetas pico E12 y E16 es ahora completamente funcional, haciendo a BackTrack la primera distribución de Pruebas de Penetración que utiliza plenamente estas impresionantes máquinas diminutas.

Soporte para Arranque PXE – Arranque de BackTrack sobre la red con tarjetas PXE soportadas.

SAINT EXPLOIT – Proporcionado amablemente por SAINT Corporation para los usuarios de BackTrack con un número limitado de IPs gratis.

MALTEGO – Los chicos de Paterva hicieron un excelente trabajo con Maltego 2.0.2 el cual es utilizado en BackTrack en su community edition

Se han aplicado los últimos parches de inyección inalámbrica en mac80211, con varios parches personalizados para mejorar la velocidad de inyección en rtl8187. El soporte para inyección inalámbrica nunca ha sido tan amplio y funcional.

Unicornscan – Completamente funcional con soporte de registro postgresql e interfaz web.

6.6.3. FASES DE PENETRACIÓN DE UN SISTEMA

6.6.3.1. Footprinting

Es el análisis del perfil de seguridad de una empresa u organización, emprendido de una manera metodológica; se la considera metodológica debido a que se busca información crítica basada en un descubrimiento anterior.

Existen varios caminos para llegar a la informaciones es decir no existe una sola metodología, esta actividad es muy importante debido a que toda la información crítica necesita ser recopilada antes de que el hacker pueda decidir sobre la mejor acción a realizar.

El footprinting necesita ser desarrollado correctamente y en una manera organizada, la información descubierta puede pertenecer a varias capas de red, por ejemplo se puede descubrir detalles del nombre del dominio, direcciones de red, servicios de red y aplicaciones, arquitectura del sistema, IDS's, direcciones IP específicas, mecanismos de control de acceso, números telefónicos, direcciones de contacto, mecanismos de autenticación, entre otros.

La información recolectada durante la fase de footprinting se puede utilizar como un puente para poder escoger la metodología del ataque.

6.6.3.2. Scanning

Se refiere a la fase antes del ataque en la cual el atacante busca en la red con información específica obtenida durante la fase de reconocimiento. La búsqueda puede ser considerada como la consecuencia lógica del reconocimiento efectuado en la fase anterior. A menudo los atacantes usan herramientas automatizadas como buscadores de subredes y equipos para ubicar los sistemas y tratar de descubrir vulnerabilidades.

Cualquier atacante puede obtener información de red crítica como mapeo de los sistemas, enrutadores y firewalls, usando herramientas simples como el comando traceroute.

6.6.3.3. Identificación de vulnerabilidades

Una vulnerabilidad es cualquier falla inherente en el diseño, configuración o implementación de un sistema o una red que pueda desembocar en un evento que pueda comprometer la seguridad.

Las vulnerabilidades pretenden describir las debilidades y los métodos más comunes que se utilizan para perpetrar ataques a la seguridad de un sistema. Hay que establecer las prioridades en los elementos a proteger, de acuerdo al valor que representan para la organización y de esta forma poder prevenir los diferentes tipos de ataques que pueden sufrir, detectando las vulnerabilidades que presentan estos elementos.

6.6.3.4. Penetración al sistema

Esta es una de las fases más importantes para un hacker porque es la fase de penetración al sistema informático, en esta fase un hacker explota las vulnerabilidades que encontró. La explotación puede ocurrir localmente, [offline] sin estar colocado, sobre la red de área local (Local Área Network), o sobre el Internet y puede incluir técnicas como buffer overflows (desbordamiento de buffer), Denial-of-Service (denegación de servicio), sesión hijacking (secuestro de sesión), y password cracking (romper o adivinar claves usando varios métodos como: diccionary atack y brute forcé atack). En esta fase los factores que ayudarán a un hacker a tener una penetración con éxito a un sistema informático dependerá de:

Cómo es la arquitectura del sistema informático y de cómo está configurado el sistema objetivo y/o víctima. Una instalación y configuración de seguridad informática simple significa un acceso más fácil a un sistema informático, nada que comentar si esta seguridad informática ni siquiera existe.

Cuál es el nivel de destrezas, conjunto de habilidades y conocimientos sobre seguridad informática de los ingenieros, profesionales y auxiliares que instalen y configuren un sistema informático.

Nivel de destrezas, conjunto de habilidades y conocimientos sobre seguridad informática y redes que tengan un hacker y el nivel de acceso que obtuvo al principio de la penetración

6.6.3.5. Mantenimiento del acceso

Una vez que un hacker gana el acceso a un sistema informático su prioridad es mantener ese acceso que ganó. En esta fase el hacker utiliza recursos propios y los recursos del sistema informático objetivo y/o víctima.

Además, usa el sistema informático atacado como plataforma de lanzamiento de nuevos ataques informáticos para escanear y explotar a otros sistemas informáticos que pretende atacar. También usa programas informáticos denominados sniffers para capturar todo el tráfico de la red, incluyendo sesiones de Telnet y FTP (File Transfer Protocol). Es en esta fase donde un hacker puede tener la habilidad de subir (upload), bajar (download) y alterar el funcionamiento de aplicaciones de software y los datos del sistema informático asaltado.

En esta fase el hacker quiere permanecer indetectable, invisible, y para ello elimina cualquier evidencia de su penetración a un sistema informático y hace uso de técnicas de Backdoor (puertas traseras) y Troyanos para ganar acceso en otra ocasión y tratar de tener acceso a cuentas de usuario con privilegios de Administrador. También emplean los caballos de Troya (Trojans) para transferir nombres de usuarios, passwords e incluso información de tarjetas de crédito o cuentas bancarias almacenados en el sistema informático.

6.6.3.6. Borrado de huellas

En esta fase es donde un hacker trata de destruir toda evidencia de cualquier posible rastreo de sus actividades ilícitas y lo hace por varias razones, entre ellas: seguir manteniendo el acceso al sistema informático comprometido, ya que si borra sus huellas los administradores de redes no tendrán pistas claras del atacante y el hacker podrá seguir penetrando el sistema cuando quiera. Además borrando sus huellas evita ser detectado y por tanto, anula la posibilidad de ser atrapado por la policía informática y quedar así al margen del imperio de la ley.

Una de las principales actividades que un atacante realiza cuando intenta penetrar a un sistema es reunir toda la información posible y realizar un inventario de puertos abiertos usando alguna técnica de escaneo de puertos. El escaneo de puertos es una de las técnicas más populares de reconocimiento usada por hackers a nivel mundial. Una vez completado este proceso, esta lista ayuda al atacante a identificar algunos servicios que están ejecutándose en el sistema objetivo, usando una lista de puertos conocidos esto permite posteriormente crear una estrategia que conduzca a comprometer el sistema.

Al escanear cuáles puertos están disponibles en el equipo de la víctima, el atacante encuentra potenciales vulnerabilidades que pueden ser explotadas.

6.6.4. Selección de metodología de hackeo ético

Como ya se menciono en la fundamentación teórica en el apartado 3.3.1 las metodologías de hackeo ético, se describió cada una de ellas, sus partes, sus fases, sus herramientas, etc. Esto nos ayudo a escoger la mejor para este tipo de trabajo investigativo, la metodología que se escogió es la metodología ISSAF para establecer los requerimientos y escenario del ataque y para el desarrollo del hacking ético se seguirán las fases de hacking ético mencionadas en el apartado 6.6.3

6.6.5. Requerimientos:

Se especifica el contenido del Acuerdo de Evaluación, parte fundamental de la metodología ISSAF.

El Gobierno autónomo descentralizado Municipal del Cantón Cevallos somete su Intranet a la evaluación mediante una prueba de intrusión bajo las siguientes consideraciones:

- Dotación de una ip estática.
- No indisponer los recursos de red o información durante el proceso de la prueba.
- No modificar o eliminar archivos o directorios.
- No cambiar la configuración en ninguno de los equipos.
- Mantenerse ajeno a los empleados y clientes.
- Sobretodo mantener una estricta confidencialidad de la información que se administre en la Intranet, sin embargo se autoriza para los fines de esta investigación técnica mostrar el proceso y los resultados de la detección de vulnerabilidades.

6.6.6. Escenario utilizado en la prueba de instrucción

En la figura 6.1 se muestra el escenario que se utilizará para desarrollar la prueba de instrucción como se puede observar en la figura antes mencionada la maquina atacante estará dentro de la intranet como un usuario común y corriente.

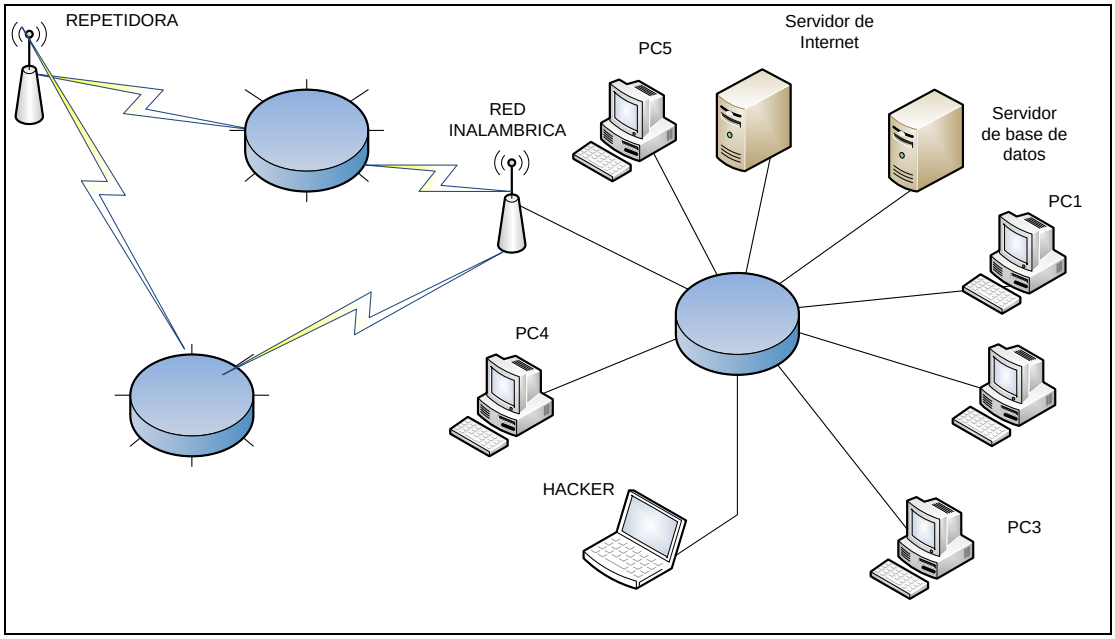


Figura 6. 1: escenario utilizado en la prueba de instrucción

6.7. ANÁLISIS DE VULNERABILIDADES A TRAVÉS DE HACKING ÉTICO

Para el análisis de vulnerabilidades a través de Hacking Ético, se utilizaron las fases de penetración a un sistema informático mencionadas.

6.7.1. FASE1: FOOTPRINTING

La regla numero uno antes de planificar o analizar un posible ataque a un sistema o red es conocer el objetivo es decir conocer su huella identificativa o footprinting – el arte de extraer toda la información posible de la red objetivo del ataque.

6.7.1.1. Objetivos del Footprinting:

- Extraer información de la topología de la red para tener una idea del esquema de cableado estructurado y encontrar las direcciones ip de los servidores existentes dentro de la institución.
- Encontrar la dirección ip del host en el cual se encuentra albergado el dominio
- Identificar a los servidores que son asignados dinámicamente mediante DHCP
- Utilizar el comando ping para probar conectividad con el servidor proxy y servidor de base de datos.

Ejecución comando ping al sitio cevallos.gob.ec

Se realizo un ping al nombre del dominio para tatar de conseguir información útil, lo primero que se hace al realizar un ping al nombre del dominio es analizar la dirección IP del host e imprimirla en pantalla, esta salida nos muestra una dirección IP y las peticiones DNS que en este caso están respondiendo con un nombre de dominio diferente al introducido inicialmente, entonces posiblemente nuestro objetivo se encuentre en un hosting.

Figura 6. 2: ping al nombre al dominio Cevallos.gob.ec

Con el programa de servicios de internet TracerRouter que permite saber todos los sistemas existentes en un camino entre dos equipos es decir nos permite conocer la ruta que toman los paquetes en la red se podrá obtener una lista de los elementos de red recorridos desde un computador origen a un computador destino a través de internet, el programa TracerRouter envía paquetes con un TTL de 1; luego de 2;luego de 3 y así sucesivamente hasta llegar a su destino y refuerza cada router a lo largo de la vía, para enviar de regreso mensajes de tiempo excedido, los cuales pueden ser usados para seguir la pista de cada punto de conexión desde la fuente hasta el destino.

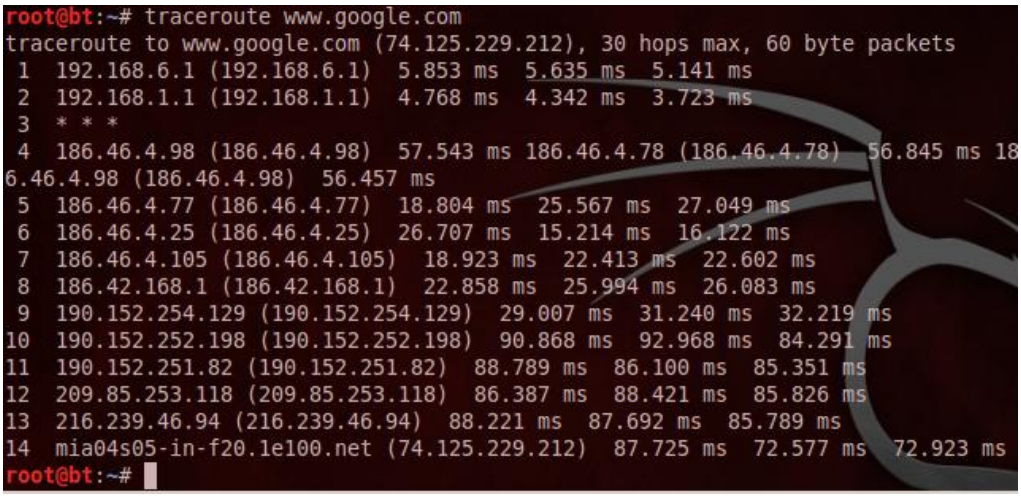


Figura 6. 3: Traceroute a www.google.com

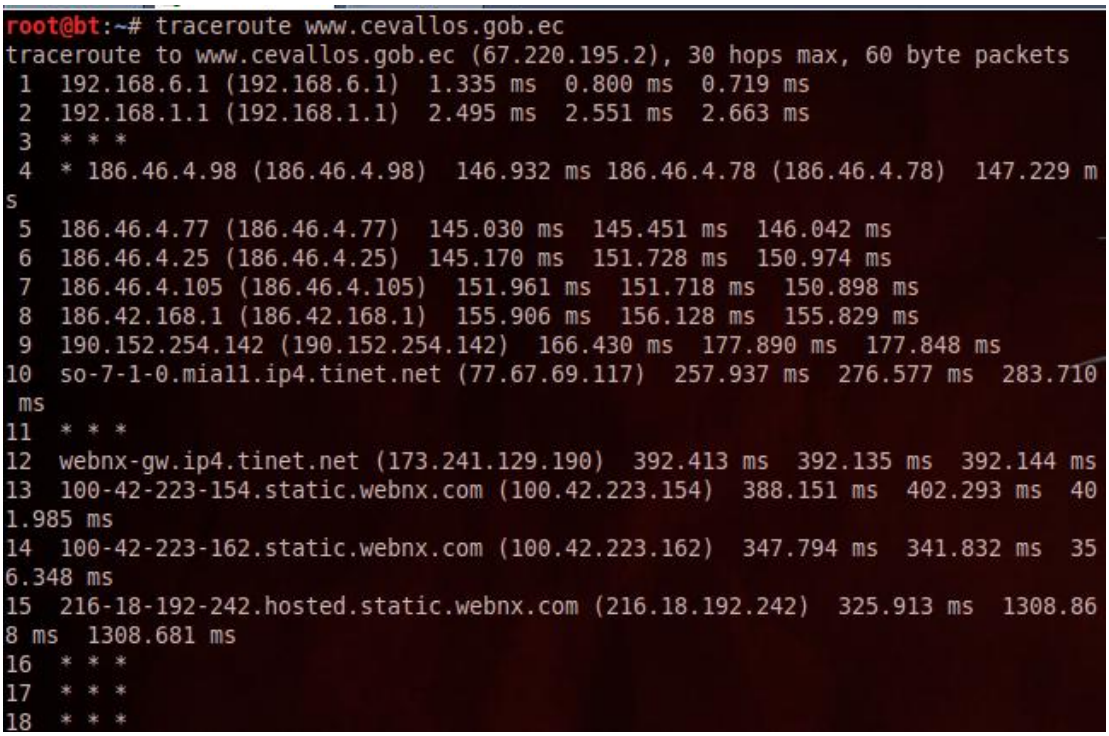


Figura 6. 4: Traceroute a www.cevallos.gob.ec

Se empleo Hping la cual es una excelente herramienta de tipo generador de paquetes TCP, UDP, ICMP, etc. Con esta herramienta y utilizando el comando adecuado podemos utilizar Hping como un trazador de rutas, solo basta con identificar un puerto que este abierto en el servidor objetivo para esto se tomo en cuenta el puerto

80 que casi todos los servidores lo tiene abierto debido a que este provee el servicio de HTTP.

Identificación de los servidores DNS que son asignados dinámicamente mediante DHCP.

Figura 6. 5: Identificación de los servidores DNS

Se usó la herramienta nslookup para consultar el servidor de nombres, buscar la dirección IP y obtener información relacionada.

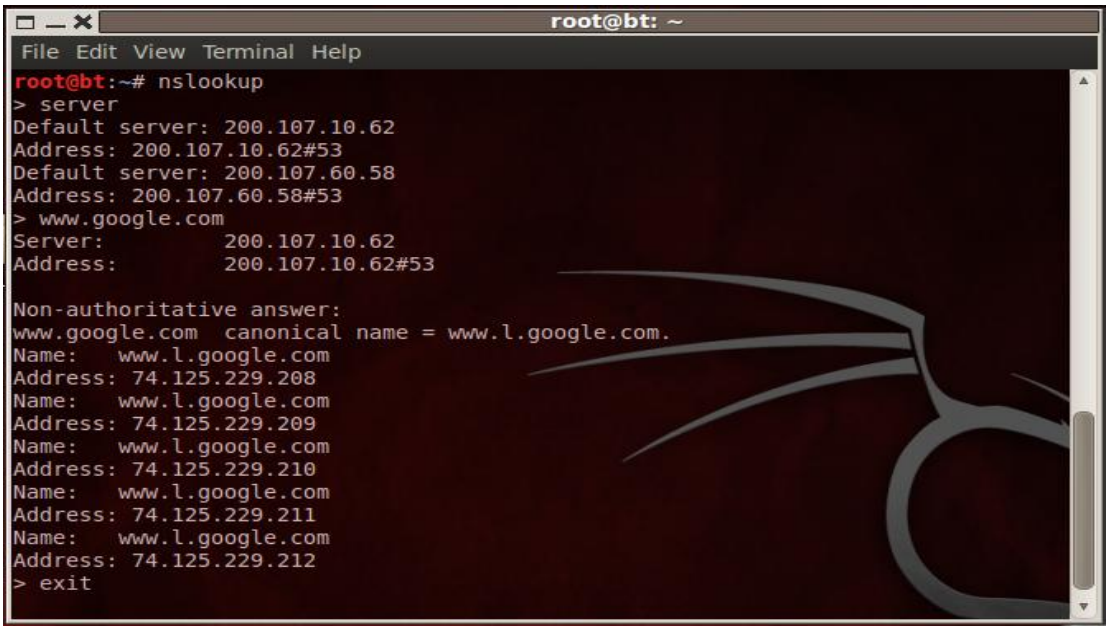


Figura 6. 6: Búsquedas en el servidor DNS

Se utilizo la transferencia de zonas para conocer si el dominio tiene servidores propios de DNS y así consultarlos para ver como tiene identificados los servidores con IP´s públicas que pasan por su dominio.

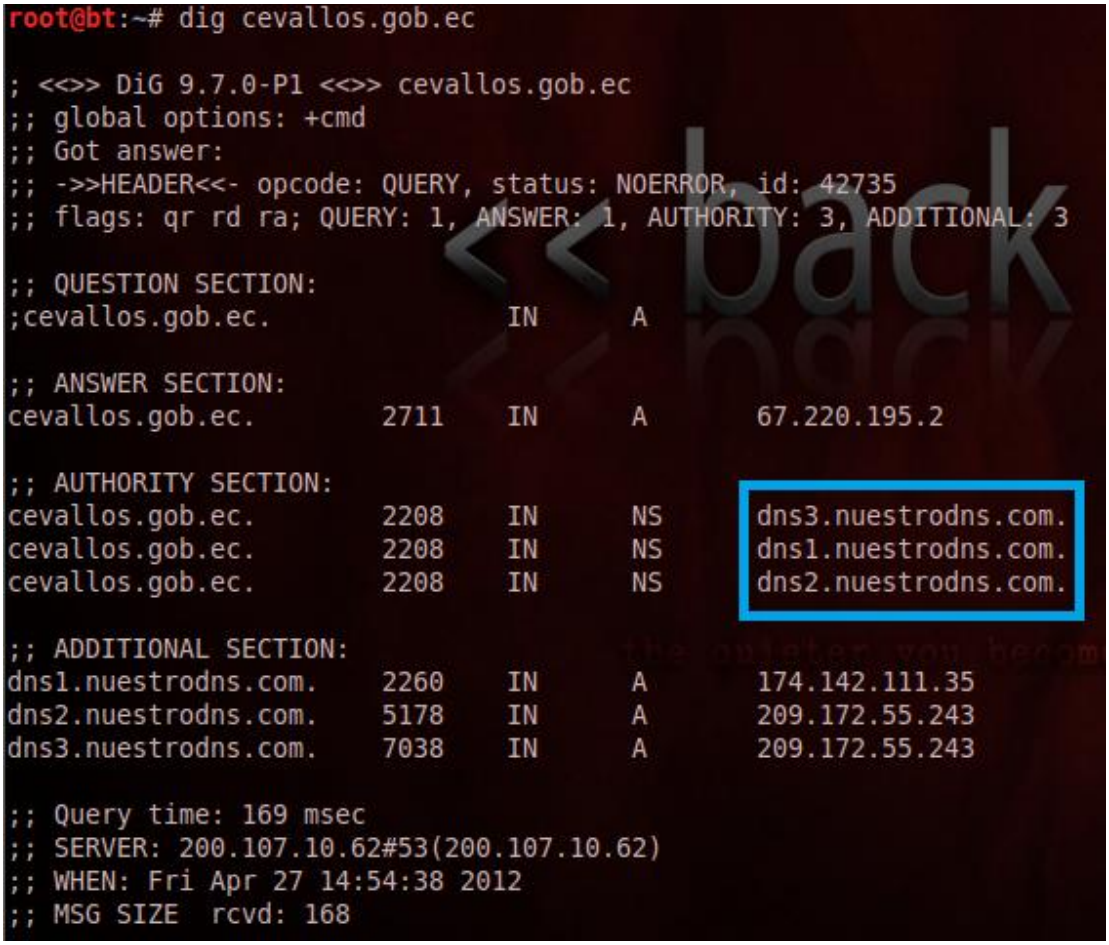


Figura 6. 7: Indagación de servidores propios de DNS

Tal como muestra la figura anterior nuestro objetivo es ubicar los servidores DNS, los cuales se muestran enmarcados en el rectángulo, también se puede observar sus respectivas direcciones IP´s, con esta información podemos completar el comando "dig" para que nos visualice la información de las diferentes IP y servidores que son resueltos por uno de estos DNS.

Con el fin de recolectar mayor información sobre el servidor DNS se utilizo el script dnsenum.pl existente en Backtrac 5 el cual es muy importante para la recolección de información sobre un dominio permitiendo hacer diferentes tipos de análisis,

variación y recolección de información, con esto simulamos ser los servidores DNS secundarios y solicitamos una recopilación de todas las zonas DNS primarias, para lo cual utilizamos el dominio cevallos.gob.ec.

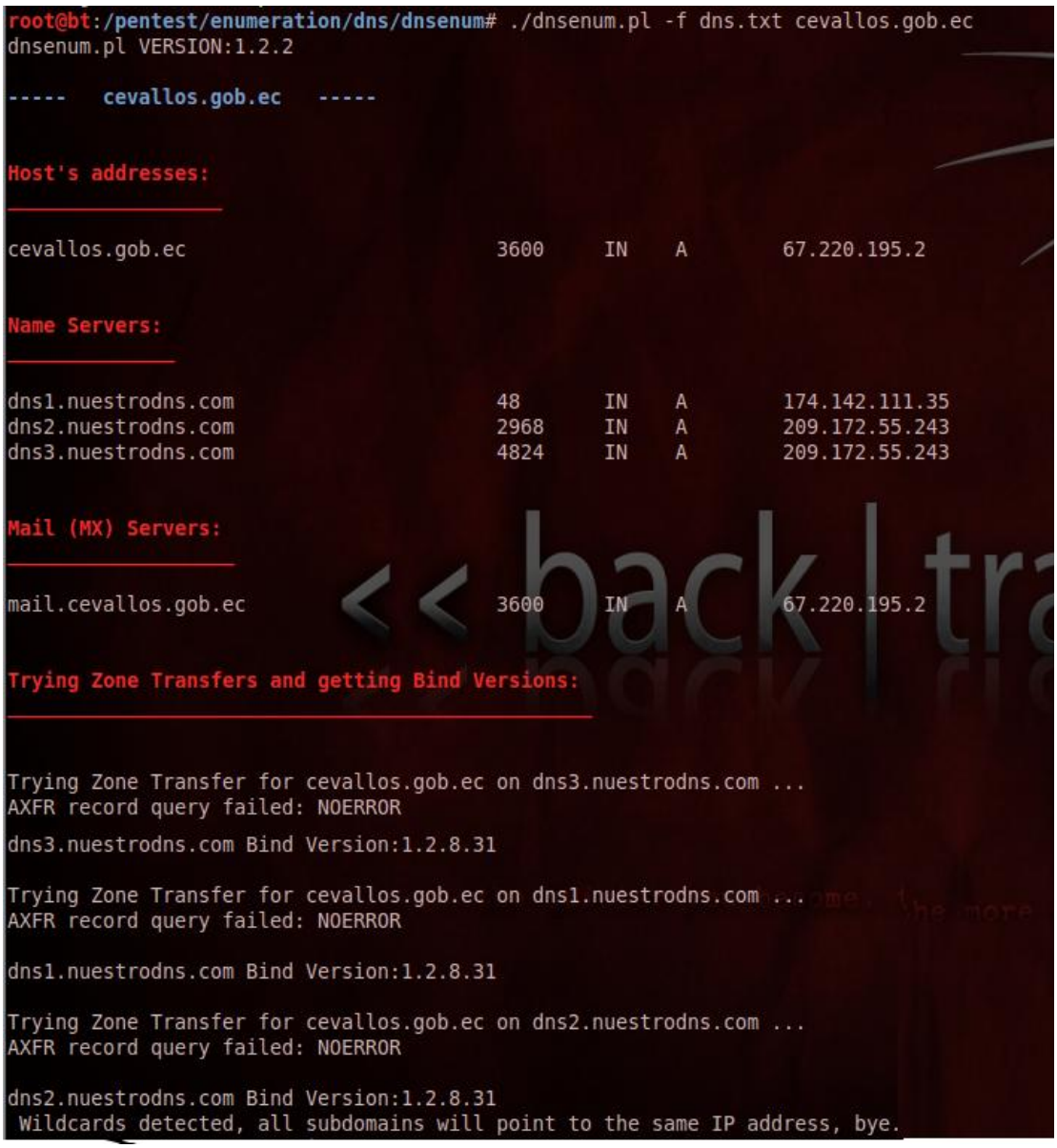


Figura 6. 8: Búsquedas en el DNS

Prueba de protocolo ICMP a las direcciones de los servidores de base de datos e internet.

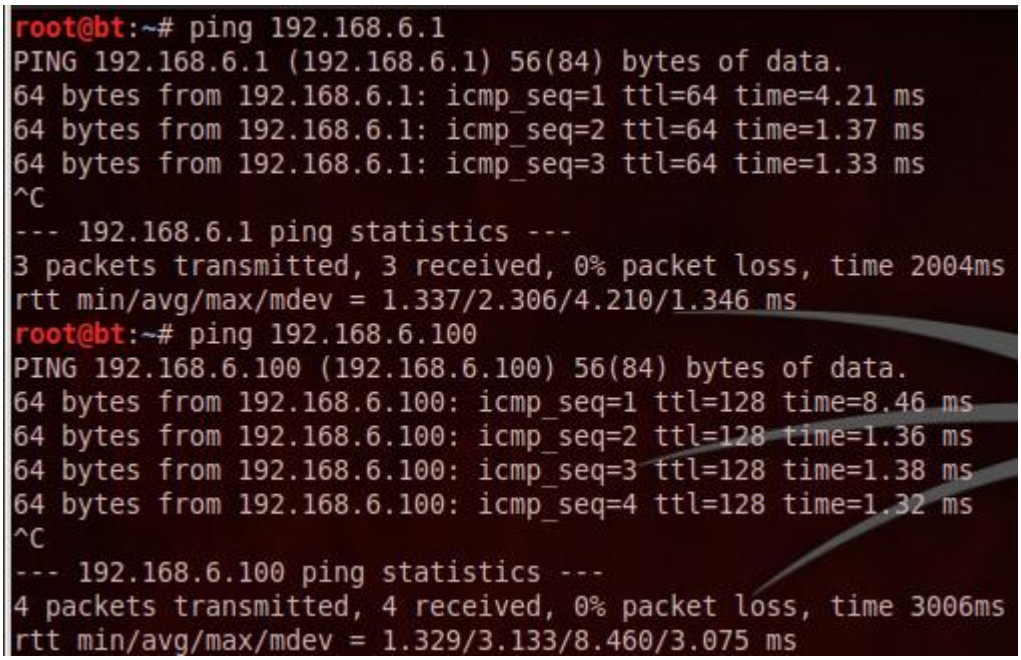


Figura 6. 9: Prueba de ICMP.

6.7.1.2. Resultados obtenidos luego de haber concluido la fase del Footprinting

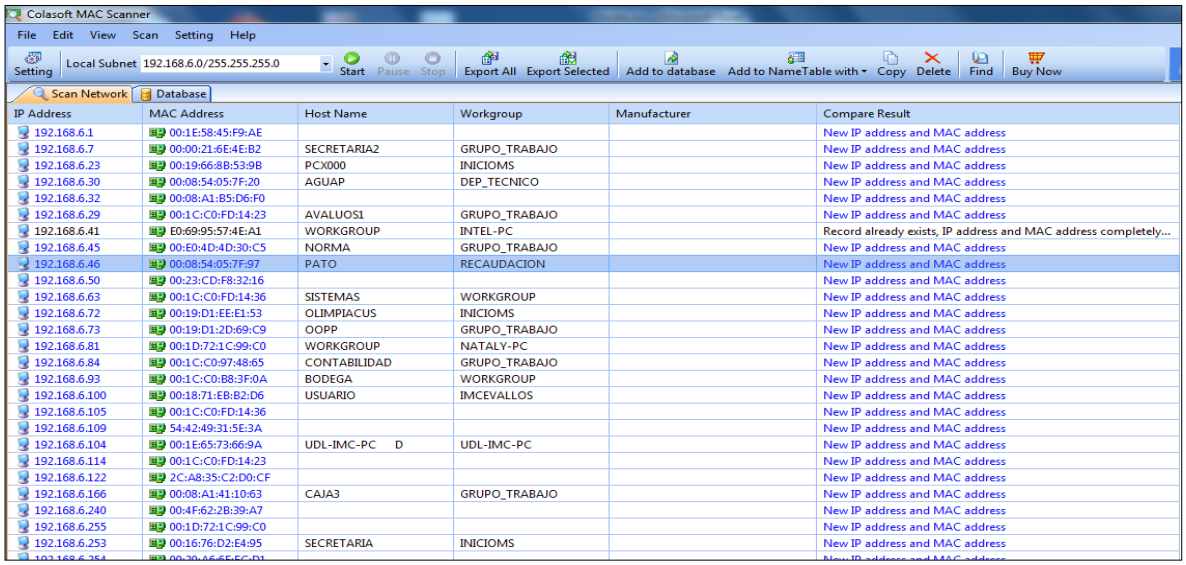
- El dominio se encuentra albergado en un hosting por lo tanto no existe servidor DNS dentro de las institución.
- Con la ejecución del comando traceroute y hping a las siguientes direcciones web www.google.com y a www.cevallos se obtuvo la ip del servidor proxy que es la 192.168.6.1, con esta ip podremos posteriormente en la fase del scanning ver puertos abiertos en este servidor proxy.
- Se encontraron los siguientes direcciones ip de servidores DNS 200.107.10.62, 200.107.60.58 pero no se encuentran dentro del GAD. Municipal por lo tanto dejan de ser objetivos de ataque.
- Prueba de conexión exitosa entre la máquina atacante y el servidor proxy utilizando la dirección ip obtenida anteriormente.
- Conexión exitosa con el servidor de base de datos.

6.7.2. FASE2: SCANNING

El escaneo de un sistema es el siguiente paso a llevar después de haber conocido nuestro objetivo tomando en cuenta que el escaneo es la denominación de las características de una red o sistemas remotos para identificar los equipos disponibles así como los servicios que ofrecen cada uno, procedemos al escaneo de red en forma activa para lo cual se empleó la herramienta Colasoft MAC Scanner la cual nos permite escanear host activos dentro de una red y los resultados los presenta en modo grafico, con esto se identificó todos los host activos dentro de la intranet, con su respectiva IP, MAC Address, Nombre de la PC y el grupo al que pertenece.

6.7.2.1. Objetivos del scanning:

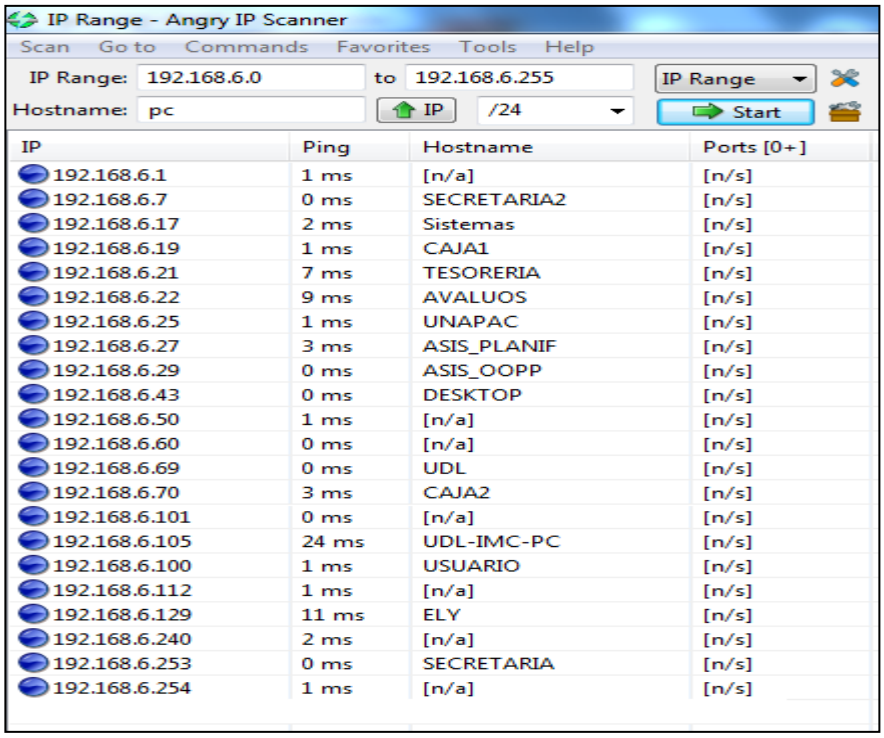
- Obtener los host activos dentro de la subred local 192.168.6.0 / 24 mediante la utilización de nmap, Colasoft MAC Scanner, y Angry IP Scanner
- Realizar un escaneo de puertos para detectar puertos abiertos en el servidor proxy, servidor de base de datos y routers y así ir pensando en los posibles ataques que se pueden realizar, tomando en cuenta los puertos abiertos y los servicios que prestan.
- Obtener las versiones del sistema operativo existente en los servidores
- Buscar carpetas compartidas y encontrar archivos confidenciales.
- Tratar de ingresar a los servidores mediante la utilización del comando netbios.



IP Address	MAC Address	Host Name	Workgroup	Manufacturer	Compare Result
192.168.6.1	00:1E:58:45:F9:AE				New IP address and MAC address
192.168.6.7	00:00:21:6E:4E:B2	SECRETARIA2	GRUPO_TRABAJO		New IP address and MAC address
192.168.6.23	00:19:66:8B:53:9B	PCX000	INICIOMS		New IP address and MAC address
192.168.6.30	00:08:54:05:7F:20	AGUAP	DEP_TECNICO		New IP address and MAC address
192.168.6.32	00:08:A1:B5:D6:F0				New IP address and MAC address
192.168.6.29	00:1C:C0:FD:14:23	AVALUOS1	GRUPO_TRABAJO		New IP address and MAC address
192.168.6.41	E0:69:95:57:4E:A1	WORKGROUP	INTEL-PC		Record already exists, IP address and MAC address completely...
192.168.6.45	00:E0:4D:4D:30:C5	NORMA	GRUPO_TRABAJO		New IP address and MAC address
192.168.6.46	00:08:54:05:7F:97	PATO	RECAUDACION		New IP address and MAC address
192.168.6.50	00:23:CD:F8:32:16				New IP address and MAC address
192.168.6.63	00:1C:C0:FD:14:36	SISTEMAS	WORKGROUP		New IP address and MAC address
192.168.6.72	00:19:D1:EE:E1:53	OLIMPIACUS	INICIOMS		New IP address and MAC address
192.168.6.73	00:19:D1:2D:69:C9	OOPP	GRUPO_TRABAJO		New IP address and MAC address
192.168.6.81	00:1D:72:1C:99:C0	WORKGROUP	NATALY-PC		New IP address and MAC address
192.168.6.84	00:1C:C0:97:48:65	CONTABILIDAD	GRUPO_TRABAJO		New IP address and MAC address
192.168.6.93	00:1C:C0:B8:3F:0A	BODEGA	WORKGROUP		New IP address and MAC address
192.168.6.100	00:18:71:EB:B2:D6	USUARIO	IMCEVALLOS		New IP address and MAC address
192.168.6.105	00:1C:C0:FD:14:36				New IP address and MAC address
192.168.6.109	54:42:49:31:5E:3A				New IP address and MAC address
192.168.6.104	00:1E:65:73:66:9A	UDL-IMC-PC D	UDL-IMC-PC		New IP address and MAC address
192.168.6.114	00:1C:C0:FD:14:23				New IP address and MAC address
192.168.6.122	2C:A8:35:C2:D0:CF				New IP address and MAC address
192.168.6.166	00:08:A1:41:10:63	CAJA3	GRUPO_TRABAJO		New IP address and MAC address
192.168.6.240	00:4F:62:2B:39:A7				New IP address and MAC address
192.168.6.255	00:1D:72:1C:99:C0				New IP address and MAC address
192.168.6.253	00:16:76:D2:E4:95	SECRETARIA	INICIOMS		New IP address and MAC address

Figura 6. 10: Escaneo de host activos con Colasoft MAC Scanner

También se tomó en cuenta para el escaneo de host activos la herramienta grafica Angry IP Scanner, con esto se podrá tener una idea más clara de la topología existente dentro de institución.



IP	Ping	Hostname	Ports [0+]
192.168.6.1	1 ms	[n/a]	[n/s]
192.168.6.7	0 ms	SECRETARIA2	[n/s]
192.168.6.17	2 ms	Sistemas	[n/s]
192.168.6.19	1 ms	CAJA1	[n/s]
192.168.6.21	7 ms	TESORERIA	[n/s]
192.168.6.22	9 ms	AVALUOS	[n/s]
192.168.6.25	1 ms	UNAPAC	[n/s]
192.168.6.27	3 ms	ASIS_PLANIF	[n/s]
192.168.6.29	0 ms	ASIS_OOPP	[n/s]
192.168.6.43	0 ms	DESKTOP	[n/s]
192.168.6.50	1 ms	[n/a]	[n/s]
192.168.6.60	0 ms	[n/a]	[n/s]
192.168.6.69	0 ms	UDL	[n/s]
192.168.6.70	3 ms	CAJA2	[n/s]
192.168.6.101	0 ms	[n/a]	[n/s]
192.168.6.105	24 ms	UDL-IMC-PC	[n/s]
192.168.6.100	1 ms	USUARIO	[n/s]
192.168.6.112	1 ms	[n/a]	[n/s]
192.168.6.129	11 ms	ELY	[n/s]
192.168.6.240	2 ms	[n/a]	[n/s]
192.168.6.253	0 ms	SECRETARIA	[n/s]
192.168.6.254	1 ms	[n/a]	[n/s]

Figura 6. 11: Escaneo de host activos con Angry IP Scanner

Escaneo de host activos con nmap

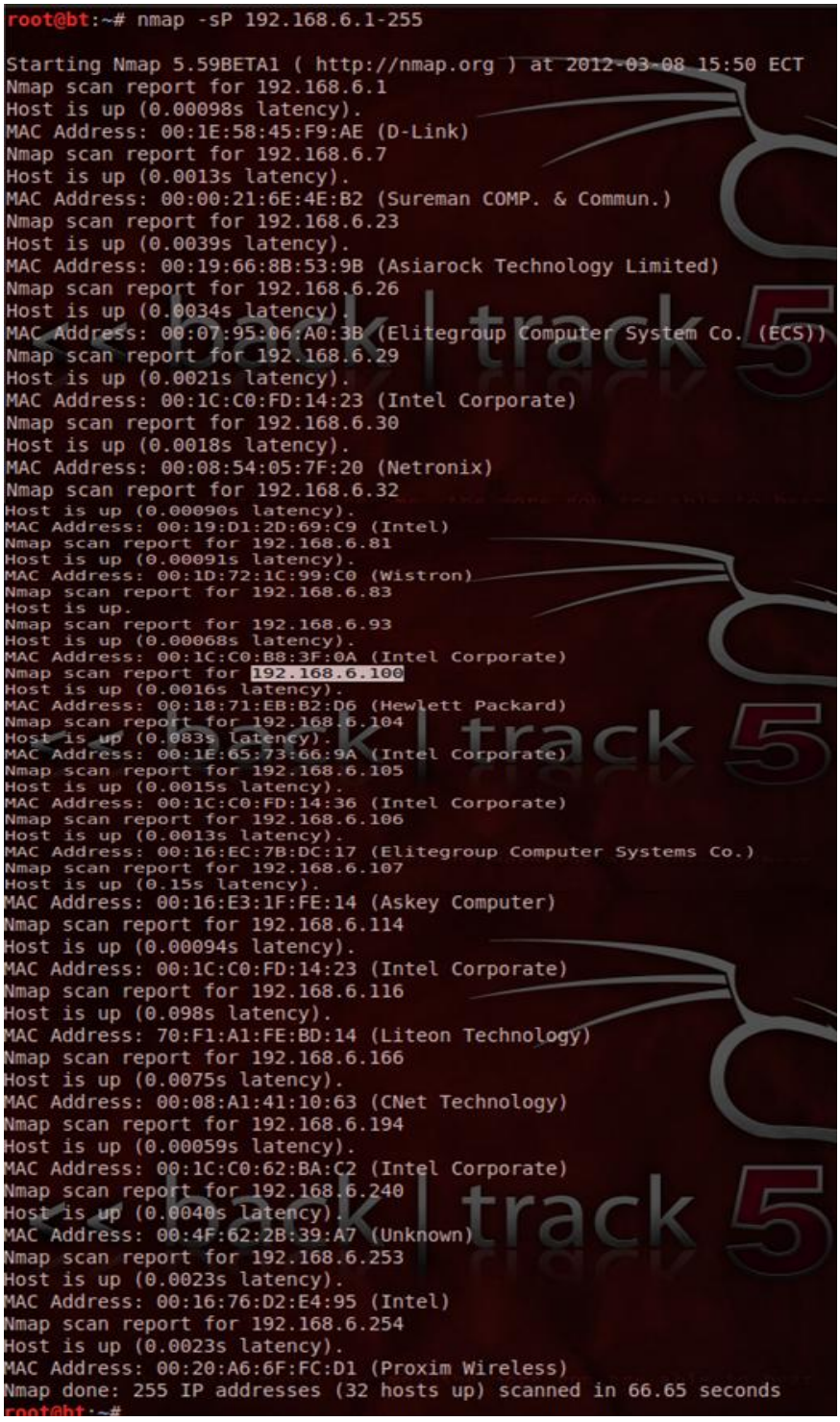


Figura 6. 12: Escaneo de host activos con nmap

Escaneo de puertos

Una vez que se dispone de los dispositivos a nivel IP activos en una red, fue tomada en cuenta la herramienta open source Nmap o zenmap el equivalente al modo grafico procedemos a verificar el estado de los puertos con sus respectivos servicios en los servidores de mayor importancia para detectar posibles vulnerabilidades según la información recabada en la los test anteriores.

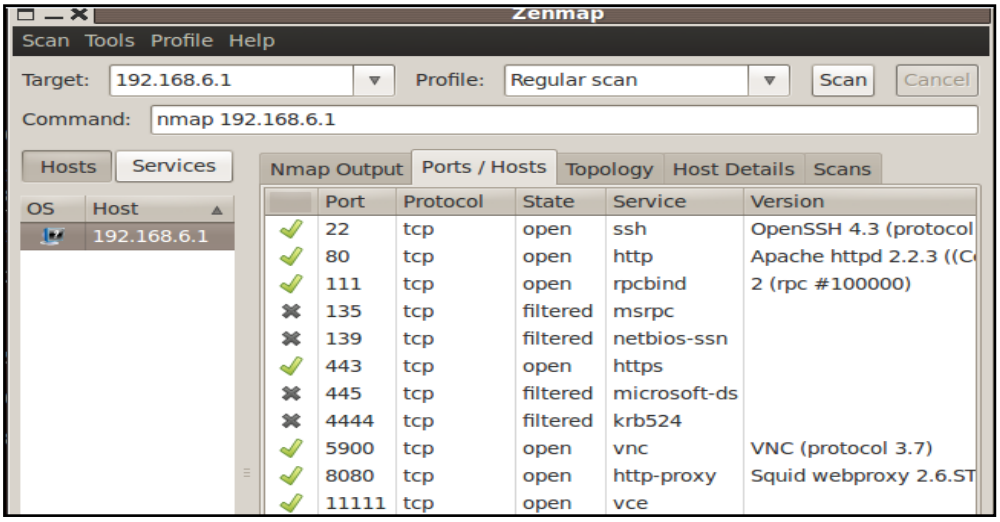


Figura 6. 13: Escaneo puertos abiertos y servicios en el servidor de Internet

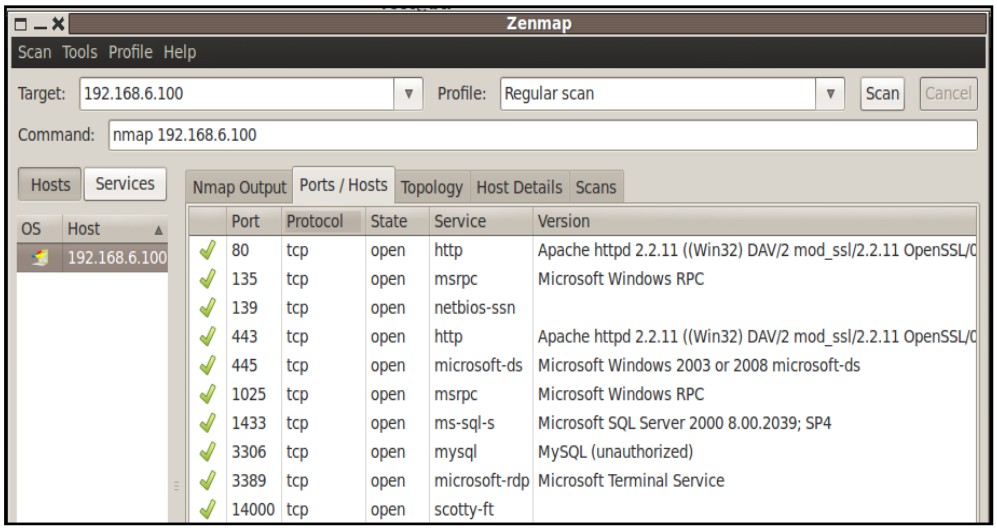


Figura 6. 14: Escaneo puertos abiertos y servicios en el servidor base de datos.

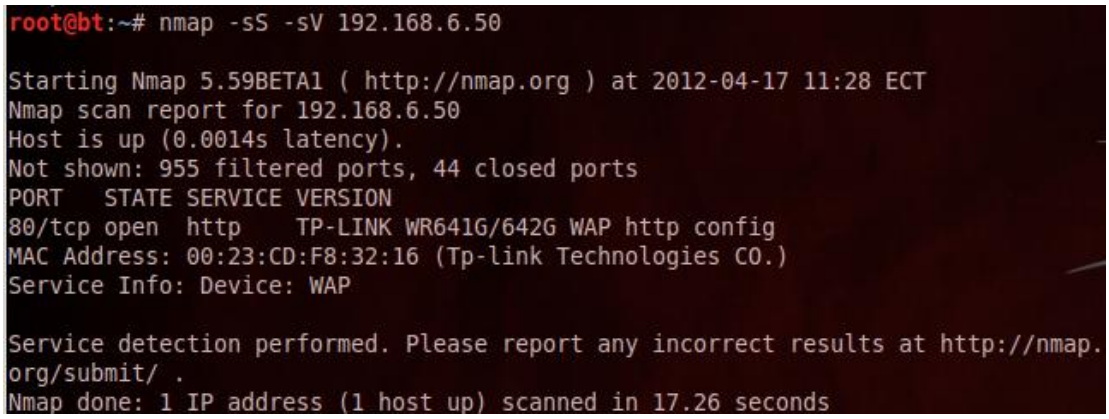


Figura 6. 15: Escaneo puertos abiertos router1.

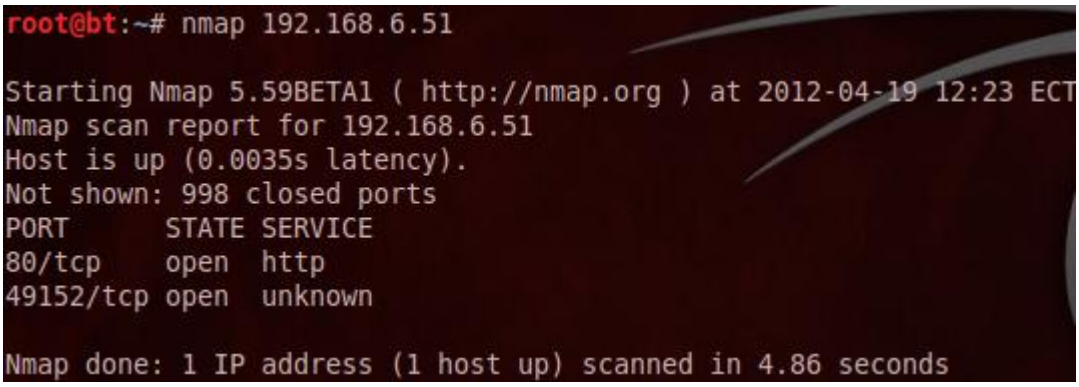


Figura 6. 16: Escaneo puertos abiertos router2.

Identificación del sistema

Con la herramienta Zenmap también podemos hacer una identificación del sistema operativo para los servidores ya identificados y testeados.

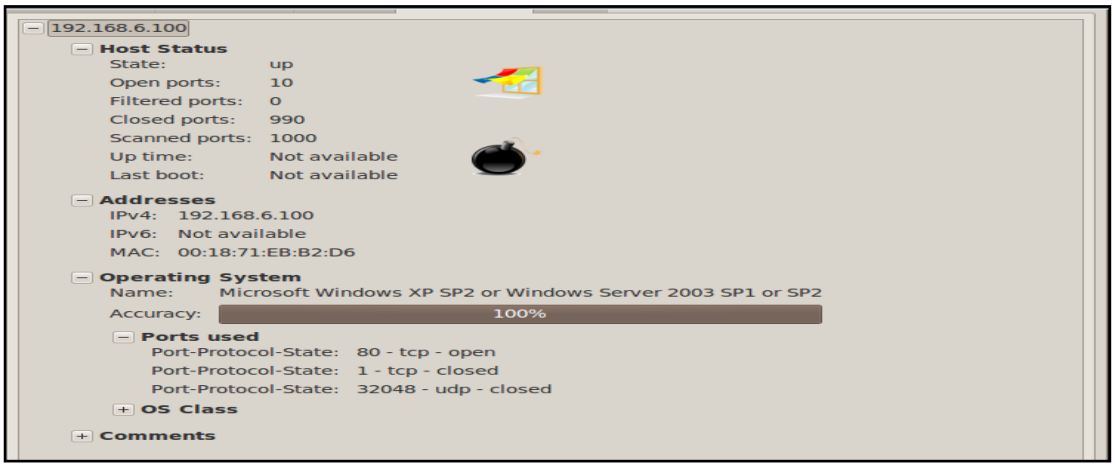


Figura 6. 17: Información del sistema 192.168.6.100.

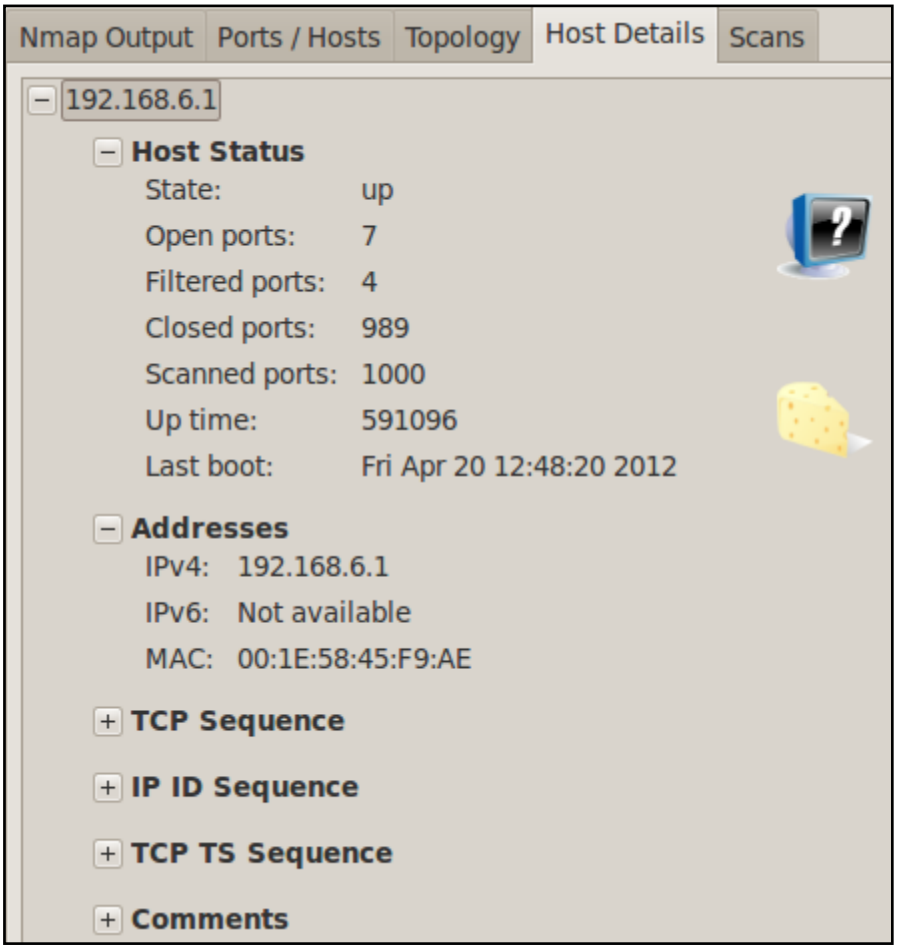


Figura 6. 18: Información del sistema 192.168.6.1.

Luego de obtener los puertos abiertos, se procede a buscar información de carpetas compartidas para esto utilizaremos nbtscan mediante el cual también podremos conocer la IP, el nombre de la PC y la Mac Address.

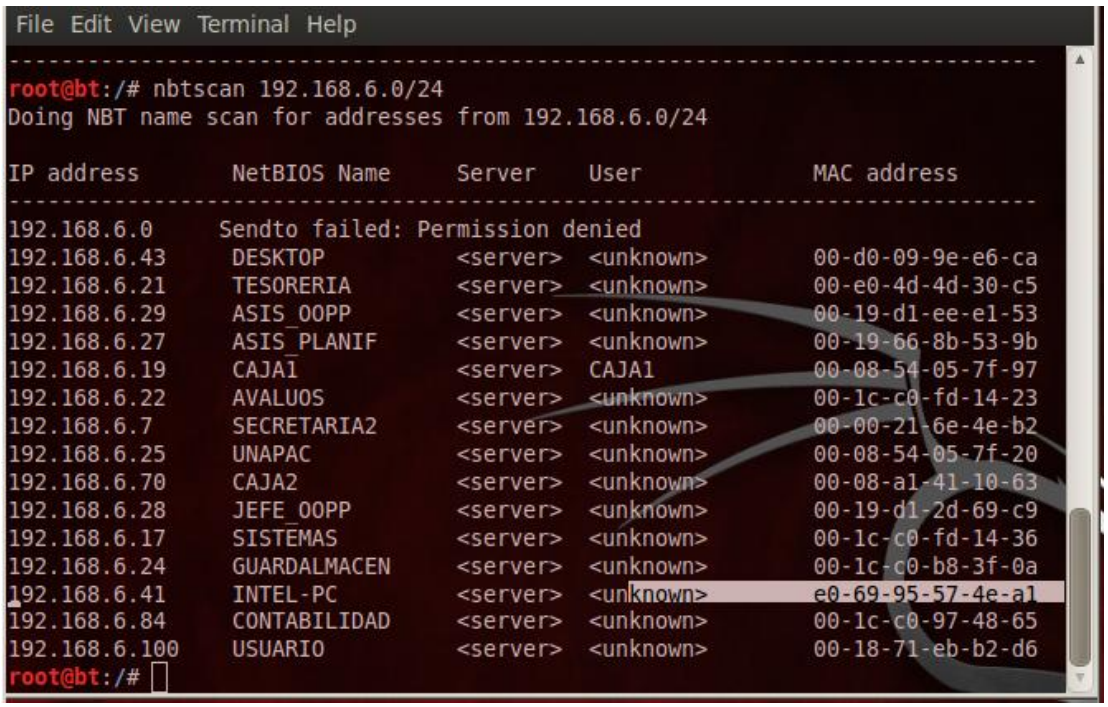


Figura 6. 19: Información del sistema 192.168.6.1.

Escaneo de carpetas compartidas con SoftPerfect Network Scanner, esta herramienta cumple las misma función que el nbtscan en el backtrac con la diferencia de que se muestran todos los host y únicamente los host que tiene carpetas compartidas se muestran con una + alado.

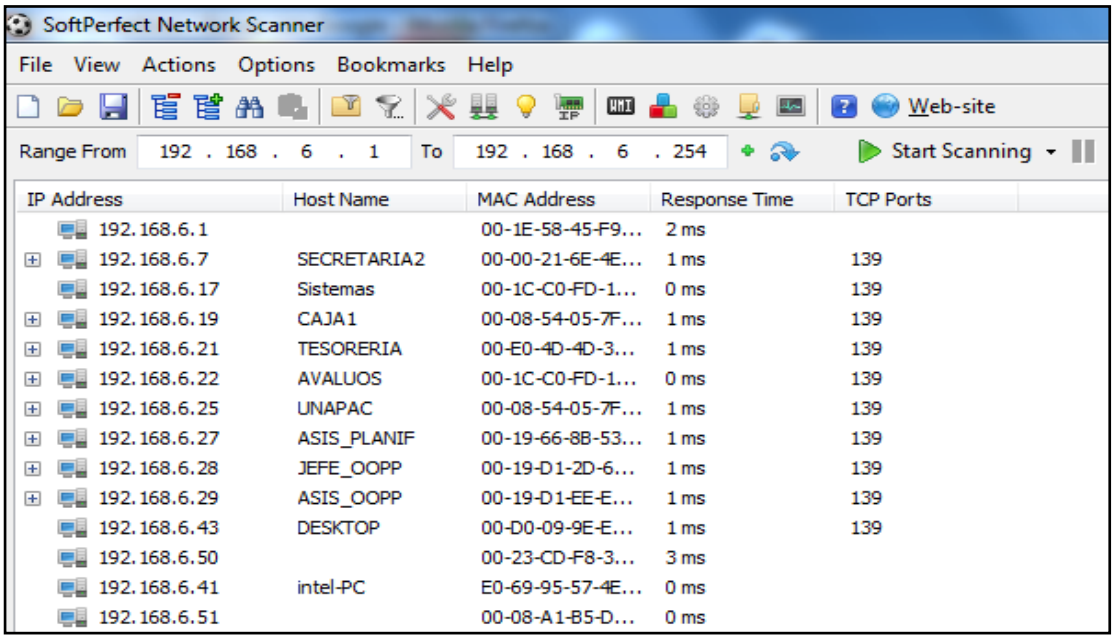


Figura 6. 20: carpetas compartidas

Para ver las carpetas compartidas simplemente tenemos que dar click en el + y posteriormente se mostraran todas las carpetas, con esto se pudo observar que en algunos Pcs no solamente existen carpetas compartidas si no también disco duros compartidos esta seria una vulnerabilidad a nivel de las estaciones de trabajo ya que todos los que están dentro de la red pueden observar los documentos compartidos y realizar cambios.

Documentos compartidos de una estación de trabajo.

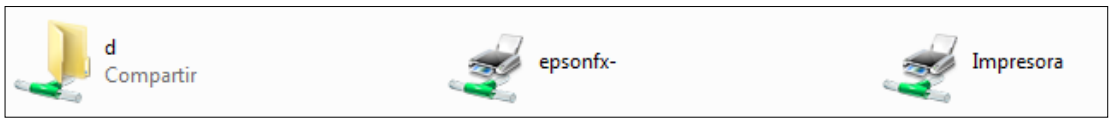


Figura 6. 21: archivos compartidos

Documento obtenido de entre las carpetas compartidas

PREDIAL RUSTICO	G. A. D. MUNICIPAL DEL CANTON CEVALLOS				RECIBO PROVISIONAL	
POR AÑO 2012	DEPARTAMENTO FINANCIERO				Nº Tit.:	
Ident. Predial:				Parroquia:		
Contribuyente:				Nombre del predio:		
Avalúo Terreno:	4.395,15		------- RUBROS -------		--- VALORES ---	
Avalúo Construcciones:	0,00					
Otras Inversiones:	0,00		Imp. Predial Rústico:.....		2,42	
Avalúo Propiedad:	4.395,15					
Exenciones y rebajas:	0,00		Bomberos.....		0,00	
Base Imponible:	4.395,15					
			Servicios administrativos.....		0,00	
0						
día/mes/año			VALOR EMITIDO.....	$.	2,42	
EMISION			DESCUENTO.....	$.	0,00	
			RECARGOS .....$.		0,00	
			INTERESES .....$.		0,00	
16/04/2012						
día/mes/año			TOTAL A PAGAR .....$.		2,42	
RECAUDACION						
	JEFE DE RENTAS	TESORERO				

Figura 6. 22: Documento encontrado en los archivos compartidos

ENTRANDO POR NETBIOS

Ocupando el prom del sistema de una maquina con Windows 7 trataremos de conectarnos por el puerto 139 del servidor Windows para verificar los servicios que corren en la maquina remota.

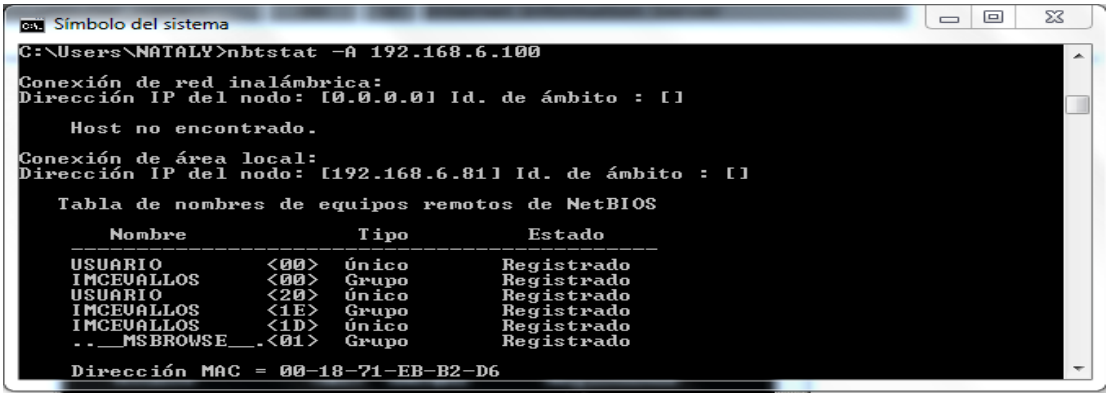


Figura 6. 23: verificación de servicios.

Es importante que el <20> que corresponde al "File Server Service" (Servicio servidor de archivos), aparezca ya que solo los PC que tienen el <20> tienen archivos compartidos y accesibles, para ver los archivos compartidos usamos el comando C:\>net view \\IP Como nos aparece lo siguiente System error 5 has occurred. Entonces primero tenemos que establecer "null session" con C:\>net use \\192.168.0.1\ipc$ "" /user:""

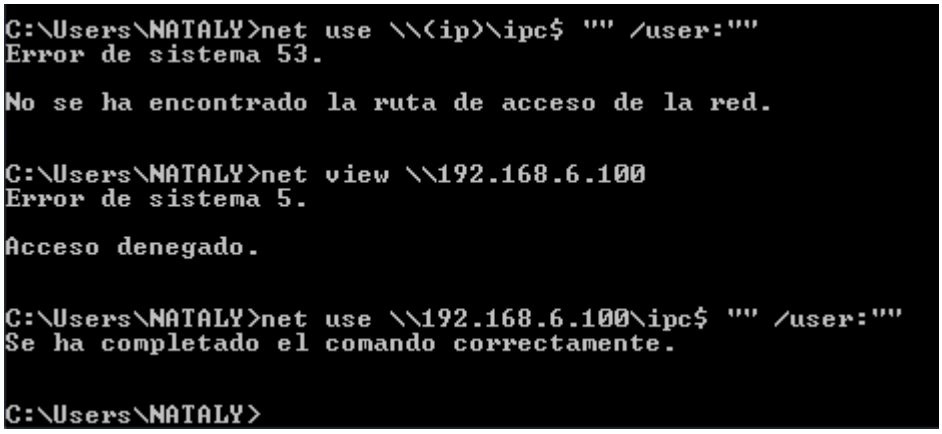


Figura 6. 24: configuraciones necesarias.

Seguidamente volvemos a usar el comando C:\>net view \\IP para tratar nuevamente de obtener los archivos compartidos.

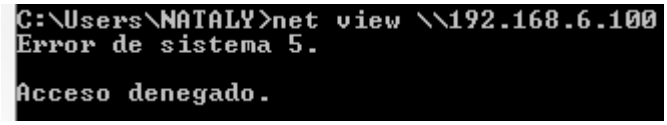


Figura 6. 25: visualizar archivos compartidos.

Como vemos nos vuelve a desplegar el mismo error de sistema 5 junto con Acceso denegado por lo tanto no se puede acceder al servidor Windows por el puerto 139.

Se trato de conectarnos remotamente con el servidor escribiendo en una ventana del símbolo de sistema \\192.168.6.100 pero no se iniciar sesión porque tiene contraseña.

Figura 6. 26: inicio de sesión en Windows.

6.7.2.2. Resultados obtenidos luego de concluir la fase de scanning

- Información confidencial compartida en la red como son los recibos del impuesto predial rustico.
- Se encontraron los siguientes host activos

IP	Ping	Hostname
192.168.6.1	1 ms	[n/a]
192.168.6.7	0 ms	SECRETARIA2
192.168.6.17	2 ms	Sistemas
192.168.6.19	1 ms	CAJA1
192.168.6.21	7 ms	TESORERIA
192.168.6.22	9 ms	AVALUOS
192.168.6.25	1 ms	UNAPAC
192.168.6.27	3 ms	ASIS_PLANIF
192.168.6.29	0 ms	ASIS_OOPP
192.168.6.43	0 ms	DESKTOP
192.168.6.50	1 ms	[n/a]
192.168.6.60	0 ms	[n/a]
192.168.6.69	0 ms	UDL
192.168.6.70	3 ms	CAJA2
192.168.6.101	0 ms	[n/a]
192.168.6.105	24 ms	UDL-IMC-PC
192.168.6.100	1 ms	USUARIO
192.168.6.112	1 ms	[n/a]
192.168.6.129	11 ms	ELY
192.168.6.240	2 ms	[n/a]
192.168.6.253	0 ms	SECRETARIA
192.168.6.254	1 ms	[n/a]

Tabla de resultados obtenidos por cada servidor:

Dirección IP	Sistema operativo	Puertos abiertos	Servicios por puerto	Sistemas
192.168.6.1	NO DETECTADO	22	ssh	OpenSSH 4.3
		80	http	Apache httpd 2.2.3
		111	rpcbind	
		443	https	
		5900	vnc	VNC(protocol 3.7)
		8080	http-proxy	Squid webproxy
		111111	vce	

Dirección IP	Sistema operativo	Puertos abiertos	Servicios por puerto	Sistemas
192.168.6.100	Microsoft windows server service pack 2	80	http	Apache httpd 2.2.11
		135	msrpc	Microsoft Windows RPC

	139	Netbios-ssn	
	443	https	Apache httpd 2.2.11
	445	Microsoft-ds	Microsoft Windows 2003 o 2008
	1025	msrpc	Microsoft Windows RPC
	1433	Ms-sql-s	Microsoft SQL server 2000
	3306	mysql	MySQL(Unauthorized)
	3389	Microsoft - rdp	Microsoft terminar Service
	14000	Scotty-ft	

- No se logro ingresar a los routers por lo tanto se pueden decir que son seguros.

6.7.3. FASE3: BUSQUEDA DE VULNERABILIDADES

Aquí se realizo un análisis de vulnerabilidades a nivel de puerto, tomando en cuenta del escaneo anterior de puertos abiertos en los servidores para esta fase utilizamos Nessus 5.0 en su versión Home el cual fue instalada en backtrack 5, se buscaron vulnerabilidades en los servidores de base de datos e internet.

6.7.3.1. Objetivos de la búsqueda de vulnerabilidades

- Escanear cada servidor para obtener vulnerabilidades dependiendo de los puertos abiertos y niveles de severidad de cada una.

Inicio nessus

Figura 6. 27: Login en Nessus

Una vez dentro procedemos a escanear los servidores para esto necesitamos añadir políticas de seguridad para añadir estas políticas nos vamos a la pestaña Policies y seguimos los pasos correspondientes creando de esta manera una política de seguridad personalizada, en nuestro caso utilizamos una política de seguridad ya existente en nessus , posteriormente procedimos a añadir un escaneo esto lo aremos en la pestaña Scans , inmediatamente se nos mostrará una figura similar a la siguiente en donde en Name pondremos el nombre del escaneo, en Police escogeremos la política que añadimos y en Scan Target digitaremos la ip de nuestro servidor de base de datos.

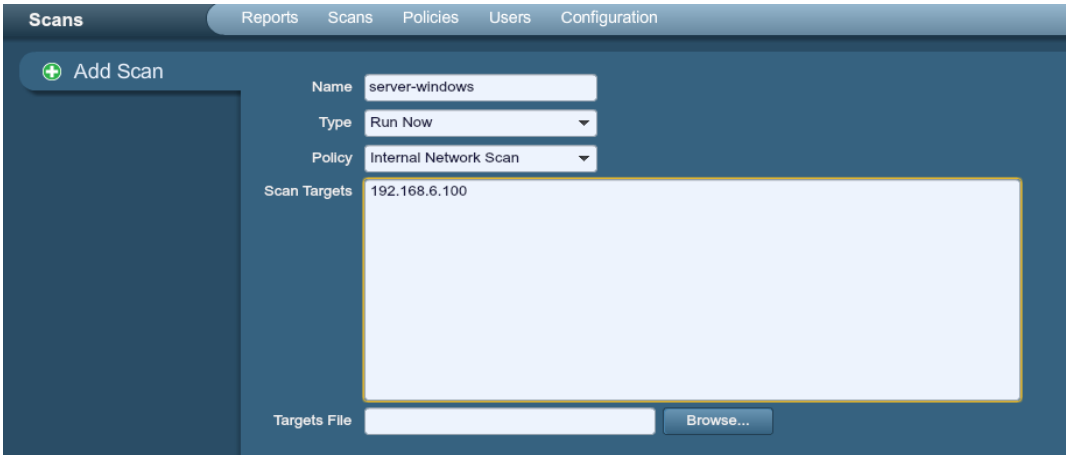


Figura 6. 28: Parámetros para realizar el escaneo de vulnerabilidades

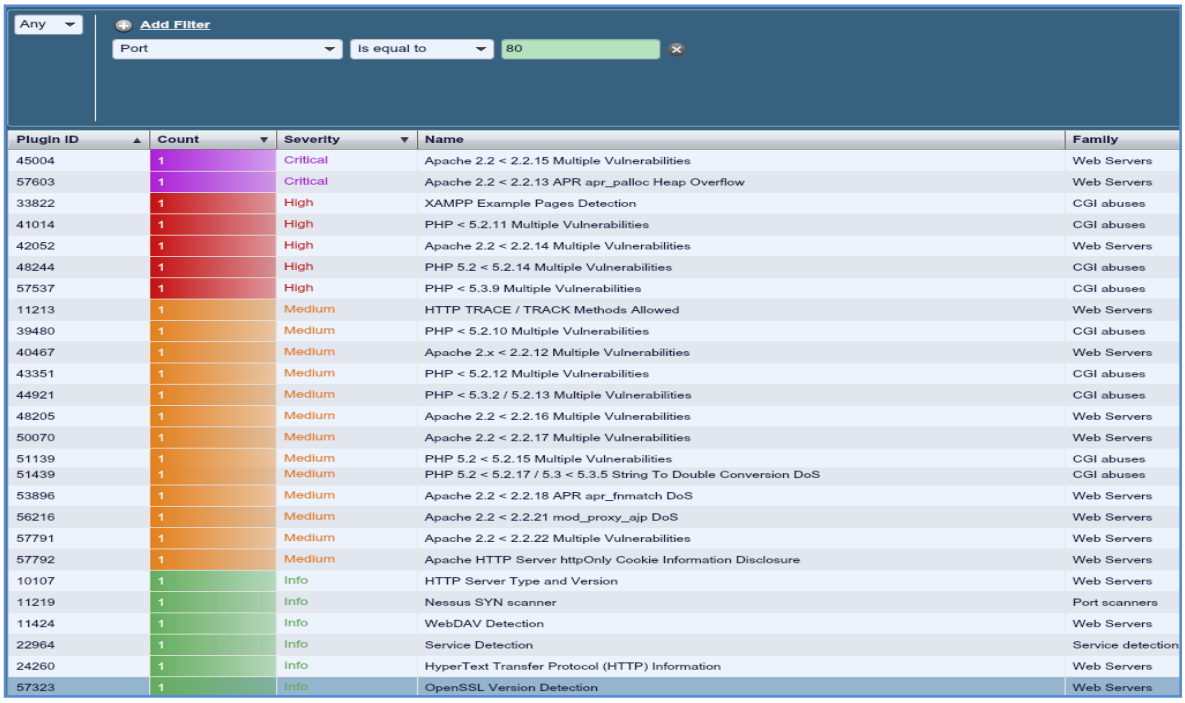
Luego de haber esperado a que se concluya el análisis de vulnerabilidad se visualizó todas las vulnerabilidades existentes en el servidor con su respectivo plugin ID, el grado de severidad, el nombre y las versiones de los sistemas instalados.

Filters No Filters Add Filter

Plugin ID	Count	Severity	Name	Family
45004	2	Critical	Apache 2.2 < 2.2.15 Multiple Vulnerabilities	Web Servers
57603	2	Critical	Apache 2.2 < 2.2.13 APR apr_palloc Heap Overflow	Web Servers
33822	2	High	XAMPP Example Pages Detection	CGI abuses
41014	2	High	PHP < 5.2.11 Multiple Vulnerabilities	CGI abuses
42052	2	High	Apache 2.2 < 2.2.14 Multiple Vulnerabilities	Web Servers
48244	2	High	PHP 5.2 < 5.2.14 Multiple Vulnerabilities	CGI abuses
57537	2	High	PHP < 5.3.9 Multiple Vulnerabilities	CGI abuses
10862	1	High	Microsoft SQL Server Default Credentials	Databases
11213	2	Medium	HTTP TRACE / TRACK Methods Allowed	Web Servers
39480	2	Medium	PHP < 5.2.10 Multiple Vulnerabilities	CGI abuses
40467	2	Medium	Apache 2.x < 2.2.12 Multiple Vulnerabilities	Web Servers
43351	2	Medium	PHP < 5.2.12 Multiple Vulnerabilities	CGI abuses
44921	2	Medium	PHP < 5.3.2 / 5.2.13 Multiple Vulnerabilities	CGI abuses
48205	2	Medium	Apache 2.2 < 2.2.16 Multiple Vulnerabilities	Web Servers
50070	2	Medium	Apache 2.2 < 2.2.17 Multiple Vulnerabilities	Web Servers
51139	2	Medium	PHP 5.2 < 5.2.15 Multiple Vulnerabilities	CGI abuses
51439	2	Medium	PHP 5.2 < 5.2.17 / 5.3 < 5.3.5 String To Double Conversion DoS	CGI abuses
53896	2	Medium	Apache 2.2 < 2.2.18 APR apr_fnmatch DoS	Web Servers

Figura 6. 29: Análisis de vulnerabilidad completo en el servidor de Base de datos

Vulnerabilidades encontradas en el servidor de base de datos por puerto



Any Add Filter

Port Is equal to 80

Plugin ID	Count	Severity	Name	Family
45004	1	Critical	Apache 2.2 < 2.2.15 Multiple Vulnerabilities	Web Servers
57603	1	Critical	Apache 2.2 < 2.2.13 APR apr_palloc Heap Overflow	Web Servers
33822	1	High	XAMPP Example Pages Detection	CGI abuses
41014	1	High	PHP < 5.2.11 Multiple Vulnerabilities	CGI abuses
42052	1	High	Apache 2.2 < 2.2.14 Multiple Vulnerabilities	Web Servers
48244	1	High	PHP 5.2 < 5.2.14 Multiple Vulnerabilities	CGI abuses
57537	1	High	PHP < 5.3.9 Multiple Vulnerabilities	CGI abuses
11213	1	Medium	HTTP TRACE / TRACK Methods Allowed	Web Servers
39480	1	Medium	PHP < 5.2.10 Multiple Vulnerabilities	CGI abuses
40467	1	Medium	Apache 2.x < 2.2.12 Multiple Vulnerabilities	Web Servers
43351	1	Medium	PHP < 5.2.12 Multiple Vulnerabilities	CGI abuses
44921	1	Medium	PHP < 5.3.2 / 5.2.13 Multiple Vulnerabilities	CGI abuses
48205	1	Medium	Apache 2.2 < 2.2.16 Multiple Vulnerabilities	Web Servers
50070	1	Medium	Apache 2.2 < 2.2.17 Multiple Vulnerabilities	Web Servers
51139	1	Medium	PHP 5.2 < 5.2.15 Multiple Vulnerabilities	CGI abuses
51439	1	Medium	PHP 5.2 < 5.2.17 / 5.3 < 5.3.5 String To Double Conversion DoS	CGI abuses
53896	1	Medium	Apache 2.2 < 2.2.18 APR apr_fnmatch DoS	Web Servers
56216	1	Medium	Apache 2.2 < 2.2.21 mod_proxy_ajp DoS	Web Servers
57791	1	Medium	Apache 2.2 < 2.2.22 Multiple Vulnerabilities	Web Servers
57792	1	Medium	Apache HTTP Server httpOnly Cookie Information Disclosure	Web Servers
10107	1	Info	HTTP Server Type and Version	Web Servers
11219	1	Info	Nessus SYN scanner	Port scanners
11424	1	Info	WebDAV Detection	Web Servers
22964	1	Info	Service Detection	Service detection
24260	1	Info	HyperText Transfer Protocol (HTTP) Information	Web Servers
57323	1	Info	OpenSSL Version Detection	Web Servers

Figura 6. 30: Resumen de vulnerabilidades en el puerto 80.

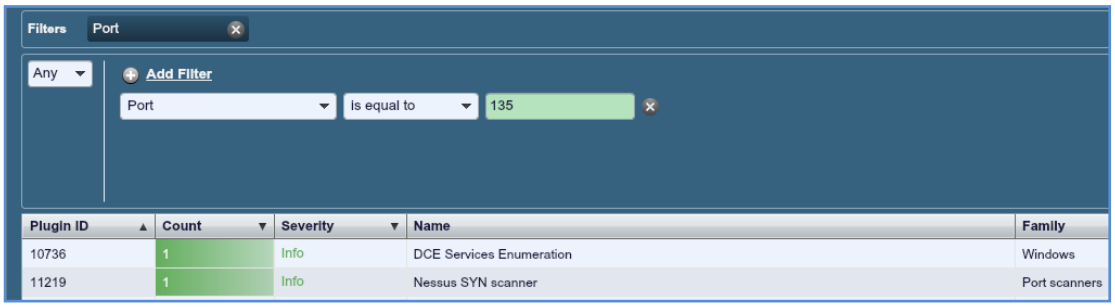


Figura 6. 31: Resumen de vulnerabilidades en el puerto 135.

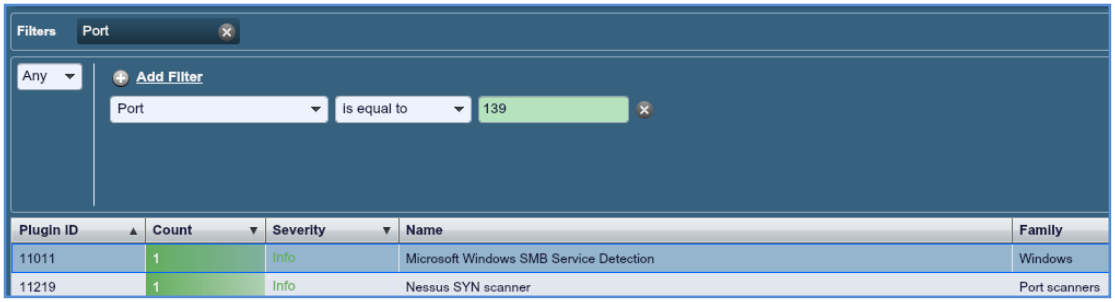


Figura 6. 32: Resumen de vulnerabilidades en el puerto 139.

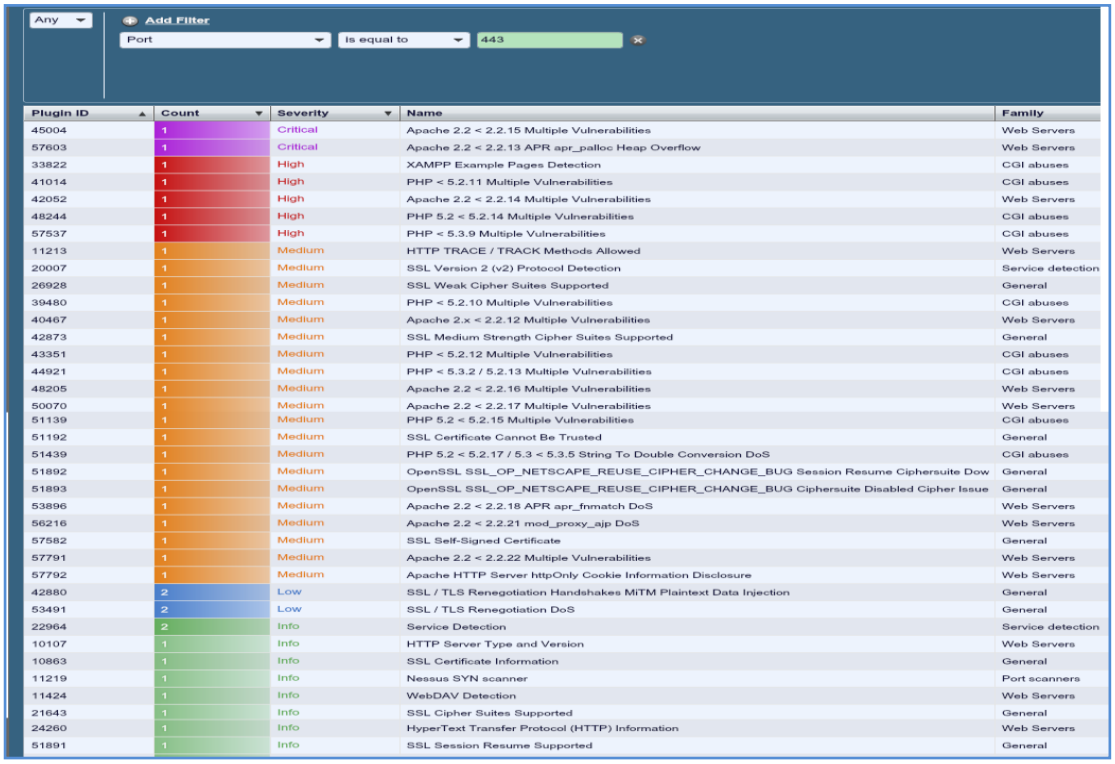
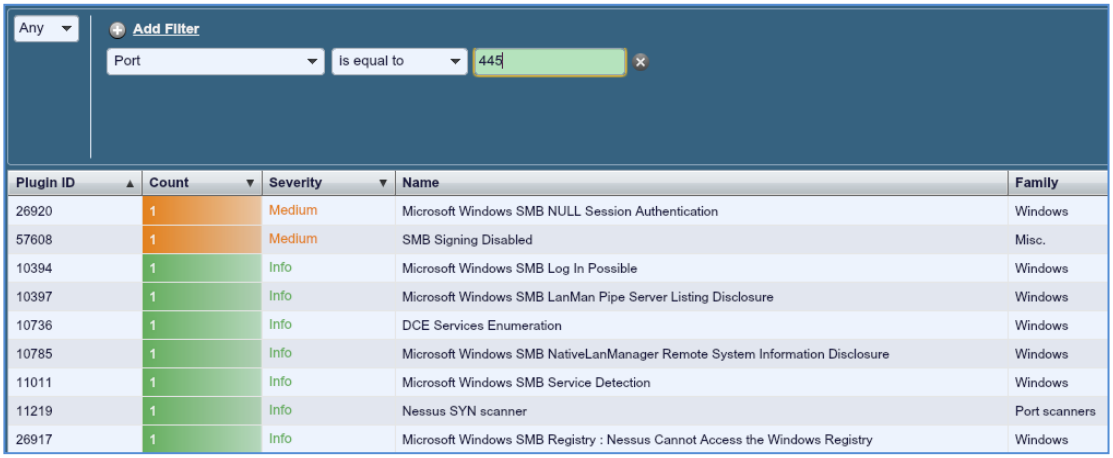
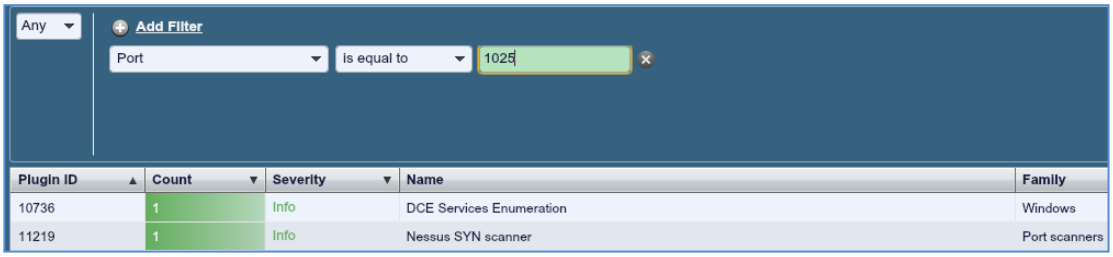


Figura 6. 33: Resumen de vulnerabilidades en el puerto 135.



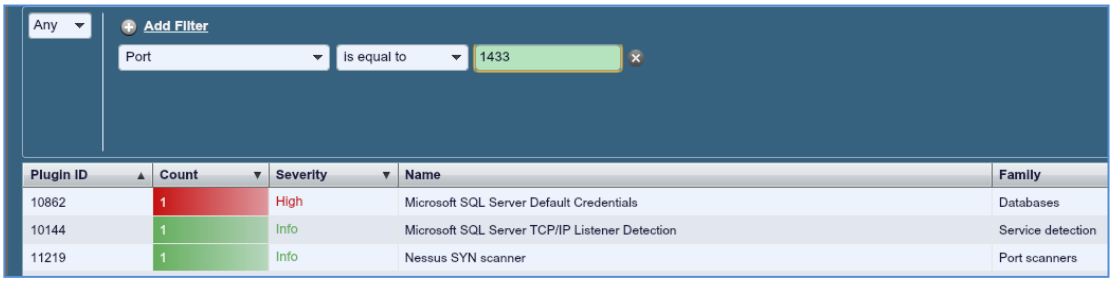
Plugin ID	Count	Severity	Name	Family
26920	1	Medium	Microsoft Windows SMB NULL Session Authentication	Windows
57608	1	Medium	SMB Signing Disabled	Misc.
10394	1	Info	Microsoft Windows SMB Log In Possible	Windows
10397	1	Info	Microsoft Windows SMB LanMan Pipe Server Listing Disclosure	Windows
10736	1	Info	DCE Services Enumeration	Windows
10785	1	Info	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure	Windows
11011	1	Info	Microsoft Windows SMB Service Detection	Windows
11219	1	Info	Nessus SYN scanner	Port scanners
26917	1	Info	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry	Windows

Figura 6. 34: Resumen de vulnerabilidades en el puerto 445.



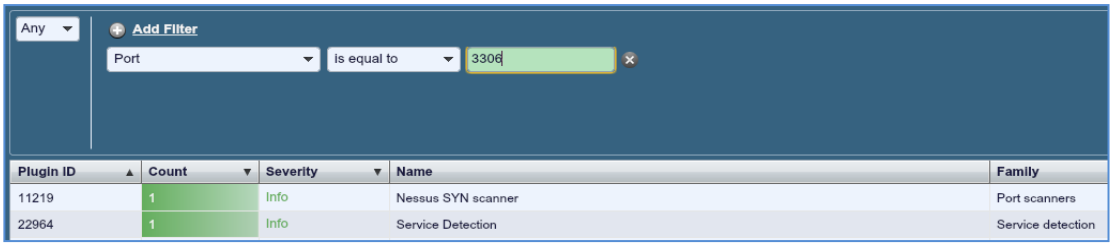
Plugin ID	Count	Severity	Name	Family
10736	1	Info	DCE Services Enumeration	Windows
11219	1	Info	Nessus SYN scanner	Port scanners

Figura 6. 35: Resumen de vulnerabilidades en el puerto 1025.



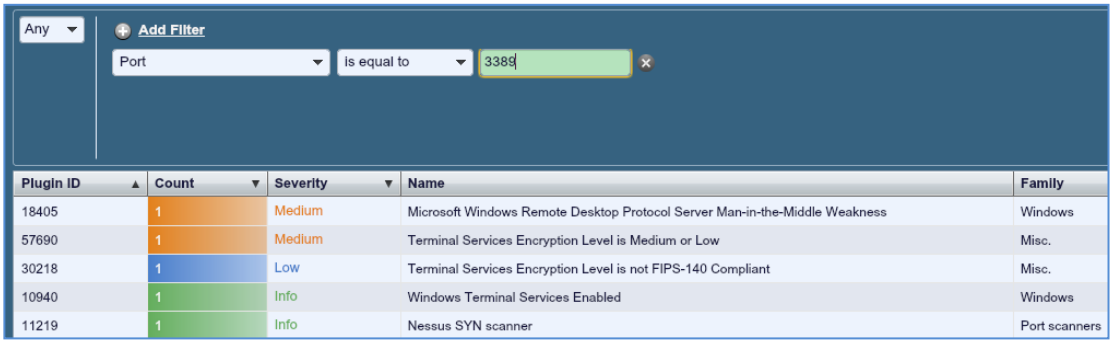
Plugin ID	Count	Severity	Name	Family
10862	1	High	Microsoft SQL Server Default Credentials	Databases
10144	1	Info	Microsoft SQL Server TCP/IP Listener Detection	Service detection
11219	1	Info	Nessus SYN scanner	Port scanners

Figura 6. 36: Resumen de vulnerabilidades en el puerto 1433.



Plugin ID	Count	Severity	Name	Family
11219	1	Info	Nessus SYN scanner	Port scanners
22964	1	Info	Service Detection	Service detection

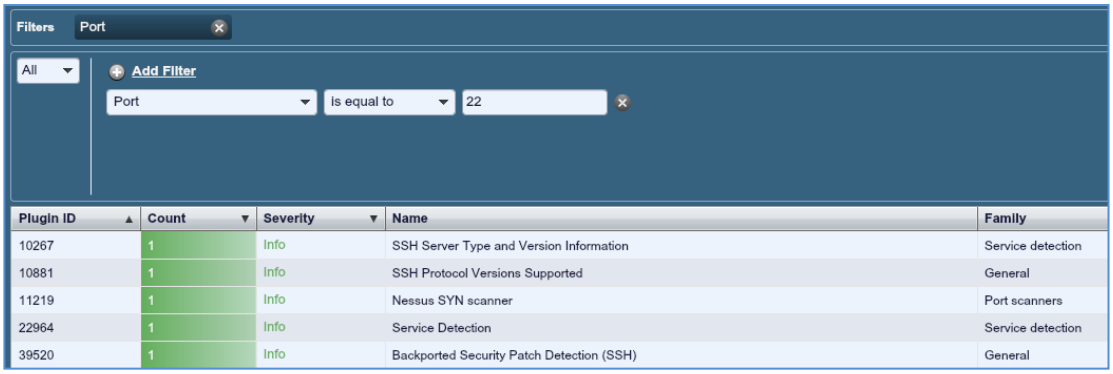
Figura 6. 37: Resumen de vulnerabilidades en el puerto 3306.



Plugin ID	Count	Severity	Name	Family
18405	1	Medium	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	Windows
57690	1	Medium	Terminal Services Encryption Level is Medium or Low	Misc.
30218	1	Low	Terminal Services Encryption Level is not FIPS-140 Compliant	Misc.
10940	1	Info	Windows Terminal Services Enabled	Windows
11219	1	Info	Nessus SYN scanner	Port scanners

Figura 6. 38: Resumen de vulnerabilidades en el puerto 3389.

Vulnerabilidades encontradas en el servidor de Internet por puerto

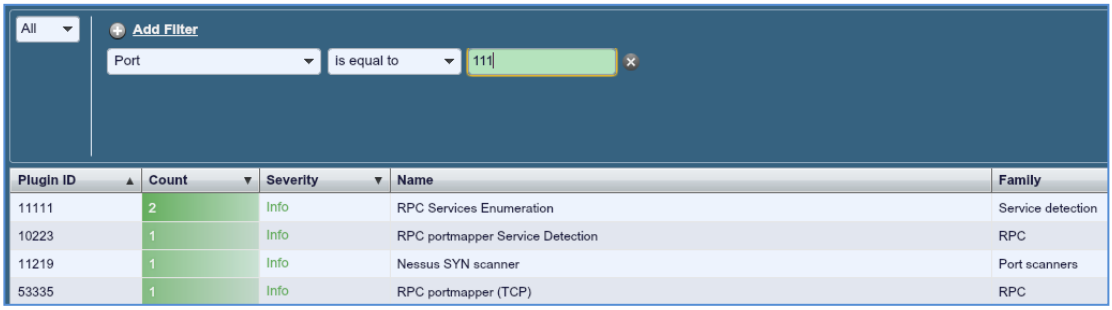


Plugin ID	Count	Severity	Name	Family
10267	1	Info	SSH Server Type and Version Information	Service detection
10881	1	Info	SSH Protocol Versions Supported	General
11219	1	Info	Nessus SYN scanner	Port scanners
22964	1	Info	Service Detection	Service detection
39520	1	Info	Backported Security Patch Detection (SSH)	General

Figura 6. 39: Resumen de vulnerabilidades en el puerto 22.

Plugin ID	Count	Severity	Name	Family
11213	1	Medium	HTTP TRACE / TRACK Methods Allowed	Web Servers
57792	1	Medium	Apache HTTP Server httpOnly Cookie Information Disclosure	Web Servers
10107	1	Info	HTTP Server Type and Version	Web Servers
11219	1	Info	Nessus SYN scanner	Port scanners
22964	1	Info	Service Detection	Service detection
24260	1	Info	HyperText Transfer Protocol (HTTP) Information	Web Servers
39521	1	Info	Backported Security Patch Detection (WWW)	General
43111	1	Info	HTTP Methods Allowed (per directory)	Web Servers

Figura 6. 40: Resumen de vulnerabilidades en el puerto 80.

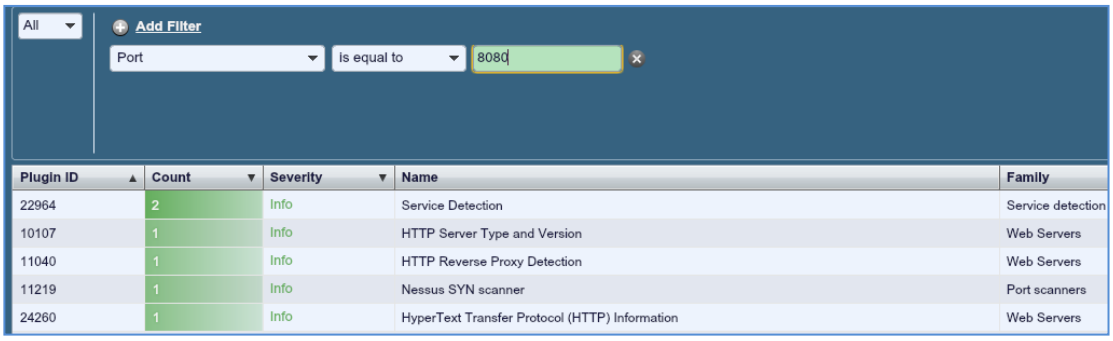


Plugin ID	Count	Severity	Name	Family
11111	2	Info	RPC Services Enumeration	Service detection
10223	1	Info	RPC portmapper Service Detection	RPC
11219	1	Info	Nessus SYN scanner	Port scanners
53335	1	Info	RPC portmapper (TCP)	RPC

Figura 6. 41: Resumen de vulnerabilidades en el puerto 111.

Plugin ID	Count	Severity	Name	Family
11213	1	Medium	HTTP TRACE / TRACK Methods Allowed	Web Servers
15901	1	Medium	SSL Certificate Expiry	General
42873	1	Medium	SSL Medium Strength Cipher Suites Supported	General
51192	1	Medium	SSL Certificate Cannot Be Trusted	General
57582	1	Medium	SSL Self-Signed Certificate	General
57792	1	Medium	Apache HTTP Server httpOnly Cookie Information Disclosure	Web Servers
22964	2	Info	Service Detection	Service detection
10107	1	Info	HTTP Server Type and Version	Web Servers
10863	1	Info	SSL Certificate Information	General
11219	1	Info	Nessus SYN scanner	Port scanners
21643	1	Info	SSL Cipher Suites Supported	General
24260	1	Info	HyperText Transfer Protocol (HTTP) Information	Web Servers
39521	1	Info	Backported Security Patch Detection (WWW)	General
43111	1	Info	HTTP Methods Allowed (per directory)	Web Servers
51891	1	Info	SSL Session Resume Supported	General
56984	1	Info	SSL / TLS Versions Supported	General

Figura 6. 42: Resumen de vulnerabilidades en el puerto 443.



Plugin ID	Count	Severity	Name	Family
22964	2	Info	Service Detection	Service detection
10107	1	Info	HTTP Server Type and Version	Web Servers
11040	1	Info	HTTP Reverse Proxy Detection	Web Servers
11219	1	Info	Nessus SYN scanner	Port scanners
24260	1	Info	HyperText Transfer Protocol (HTTP) Information	Web Servers

Figura 6. 43: Resumen de vulnerabilidades en el puerto 8080.

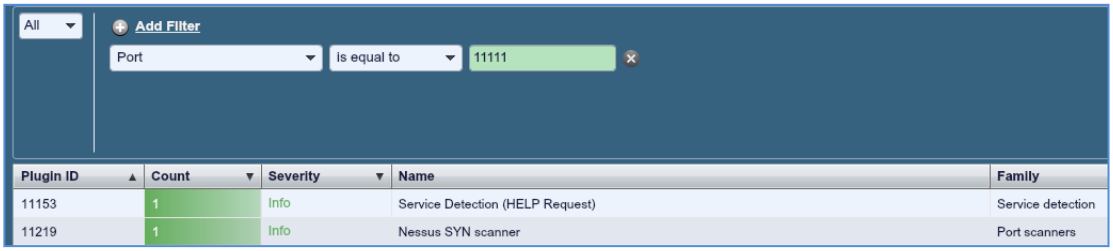


Figura 6. 44: Resumen de vulnerabilidades en el puerto 11111.

6.7.3.2. Resultados del escaneo de vulnerabilidades:

Vulnerabilidades encontradas en el servidor de base de de datos e internet:

- 1.-Microsoft SQL Server

  Nivel de severidad: Alta

  Vulnerabilidad: Las credenciales para el servidor de base de datos remota pueden ser descubiertas.

  Ingreso desde la maquina atacante al servidor de base de datos utilizando las credenciales de sql server por defecto, esta es una de las principales vulnerabilidades considerando que la base de datos es el corazón de cualquier sistema, toda la información albergada en esta base es de vital importancia para el GAD. Municipal y esta expuesta a robo o modificación de la misma.
- 2.-Microsoft Windows Server Man-in-the-Middle

  Nivel de severidad: Alta

  Vulnerabilidad Tal vez sea posible realizar ataques de hombre en el medio (MIT)
- Se obtuvieron contraseñas del servidor web
- 4.-PHP 5.2 < 5.2.17 / 5.3 < 5.3.5 DoS

  Nivel de severidad: media

  Vulnerabilidad: El servidor web remoto utiliza una versión de PHP que se ve afectado por una vulnerabilidad de denegación de servicio.
- 5.-Apache HTTP server DOS

  Nivel de severidad: critica

  Vulnerabilidad: La versión de Apache HTTP que se ve afectado por una vulnerabilidad de denegación de servicio

6.7.4. Fase4: Penetración al sistema

Una vez que ha realizado el escaneo de host activos, identificación de puertos abiertos y el escaneo de vulnerabilidades se procede a explotar las vulnerabilidades y tratar de ganar acceso desautorizado a los recursos informáticos vulnerables.

6.7.4.1. Objetivos de la penetración al sistema:

- atacar al servicio de Microsoft Windows SMB utilizando Metasploit para tratar de abrir sesión en el servidor de base de datos, ya que como se pudo averiguar en fases anteriores servidor posee un sistema operativo Windows 2003 server por lo tanto es viable realizar este tipo de ataque.
- Establecer conexión con el servidor de base de datos utilizando Microsoft sql server Enterprise 2008 desde la pc atacante.
- Realizar ataques de hombre en el medio para lograr conseguir contraseñas de ingresos a sistemas o correos electrónicos.
- Realizar ataques DOS en el servidor de internet y Windows tratando de saturar el ancho de banda así como también
- Tratar de eliminar temporalmente los servicios que presta apache en el caso de centos y XAMPP en el caso de Windows.

Ingresando al servidor de base de datos con sql server 2008.

Como primera instancia trataremos de ingresar al servidor de base de datos, pues con el monitoreo de vulnerabidades de nessus se pudo descubrir que en el Microsoft SQL Server existe una vulnerabilidad de credenciales predeterminadas, es decir el SQL Server posee un usuario y una contraseña por defecto y esta a su vez es común parra una o más cuentas, además mediante el escaneo de puertos se obtuvo la versión del SQL Server por lo tanto trataremos de establecer conexión utilizando el SQL Server 2008 todo esto con el objetivo de tener acceso a los registros de la base de datos.

Figura 6. 45: Conexión con la base de datos.

Una vez establecida la conexión se tuvo acceso a todas las bases que existentes, esta sería una de las principales vulnerabilidades pues mediante esta conexión se tiene el control total de la base de datos, se podría alterar, robar y borrar información.

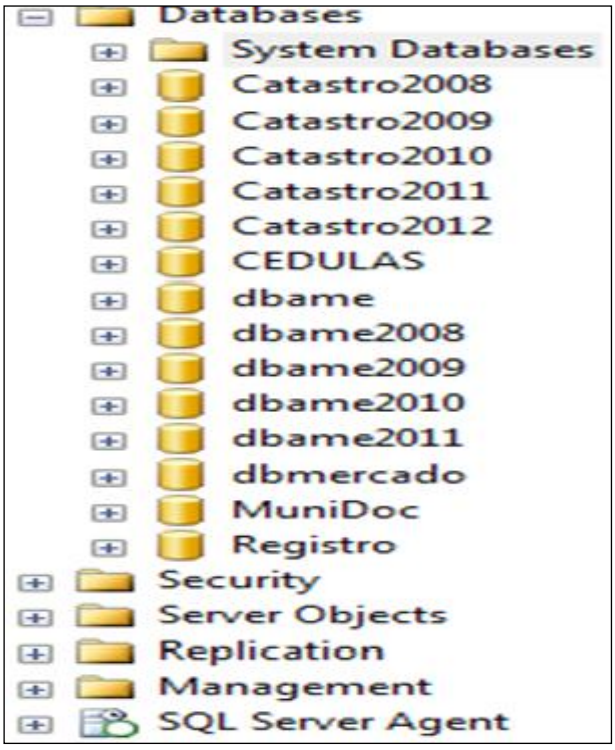


Figura 6. 46: Bases de datos existentes.

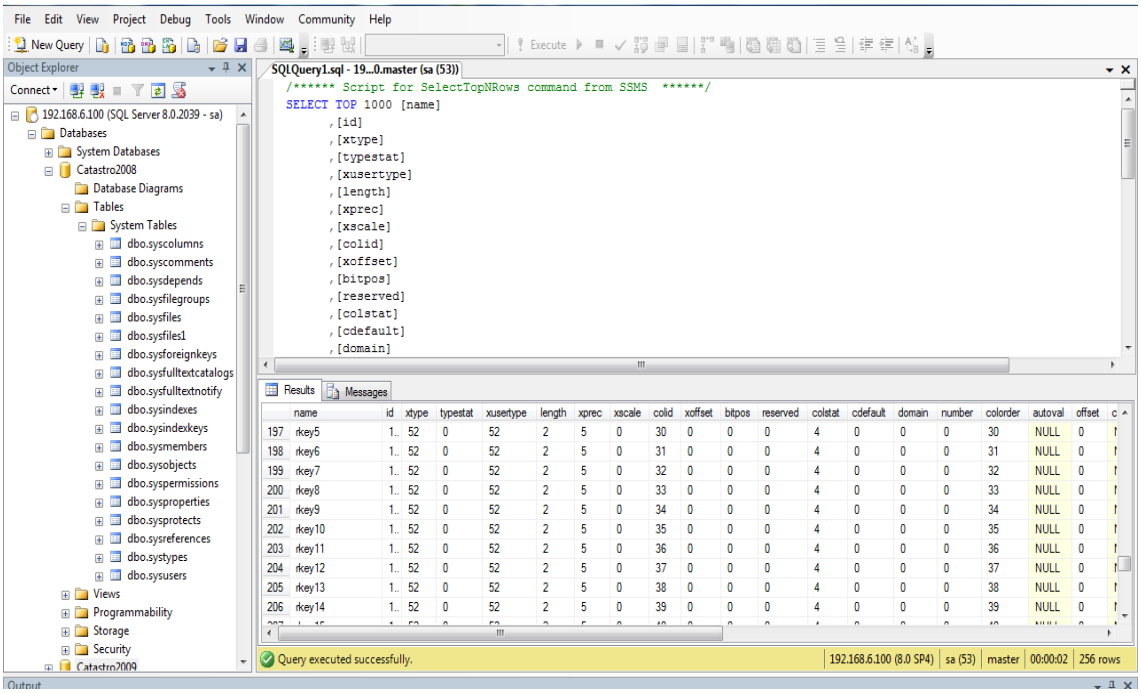


Figura 6. 47: Tablas catastro 2008.

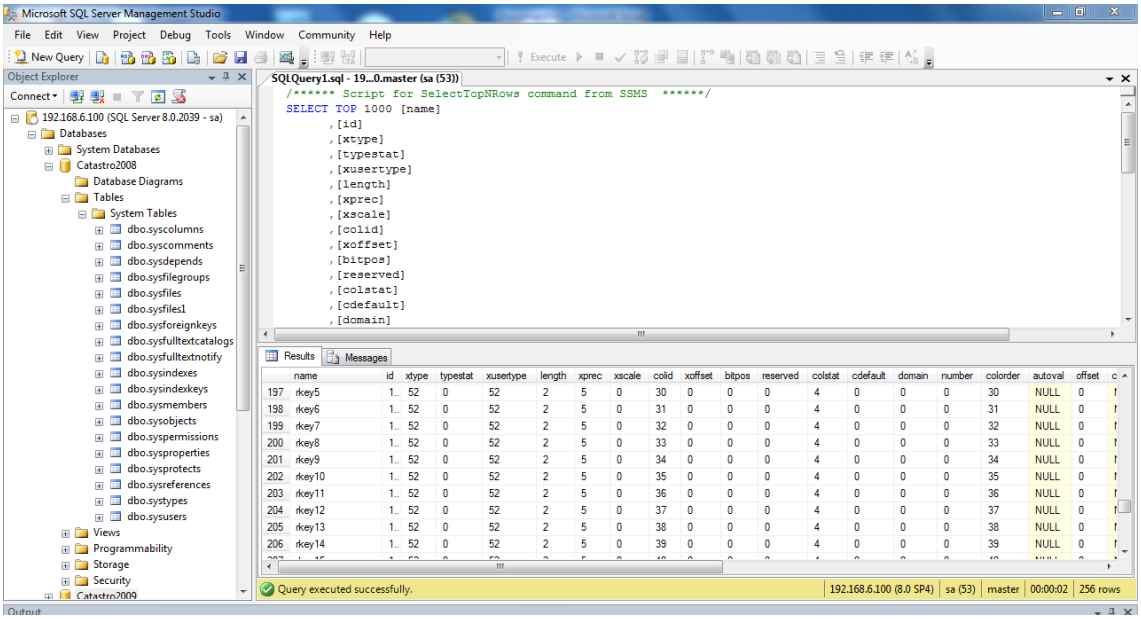


Figura 6. 48: Tablas catastro 2009.

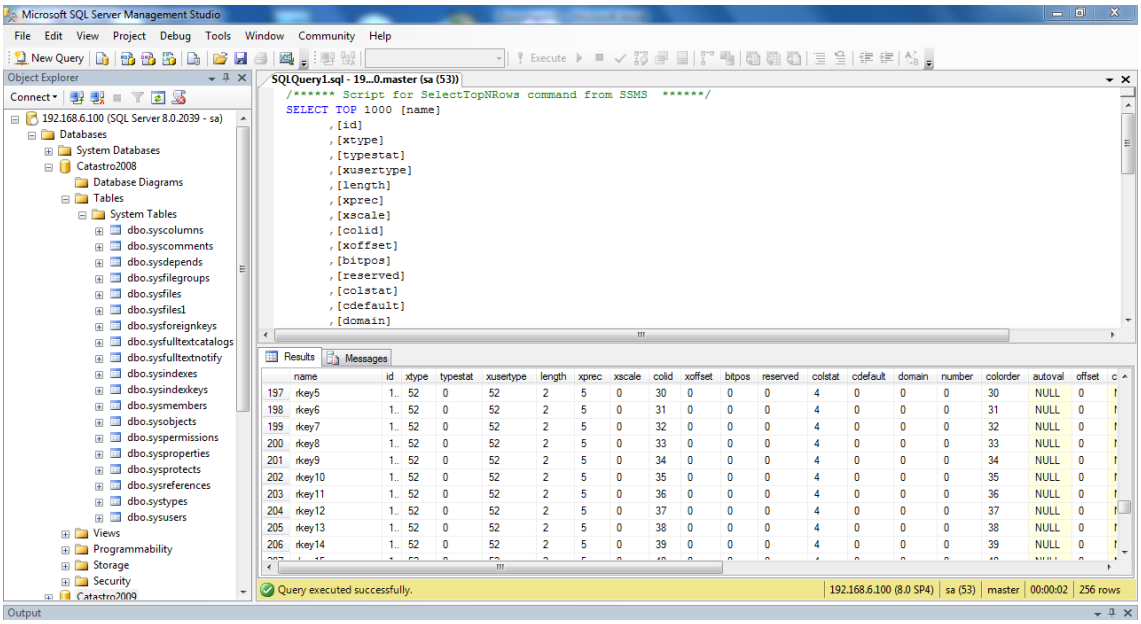


Figura 6. 49: Tablas catastro 2010.

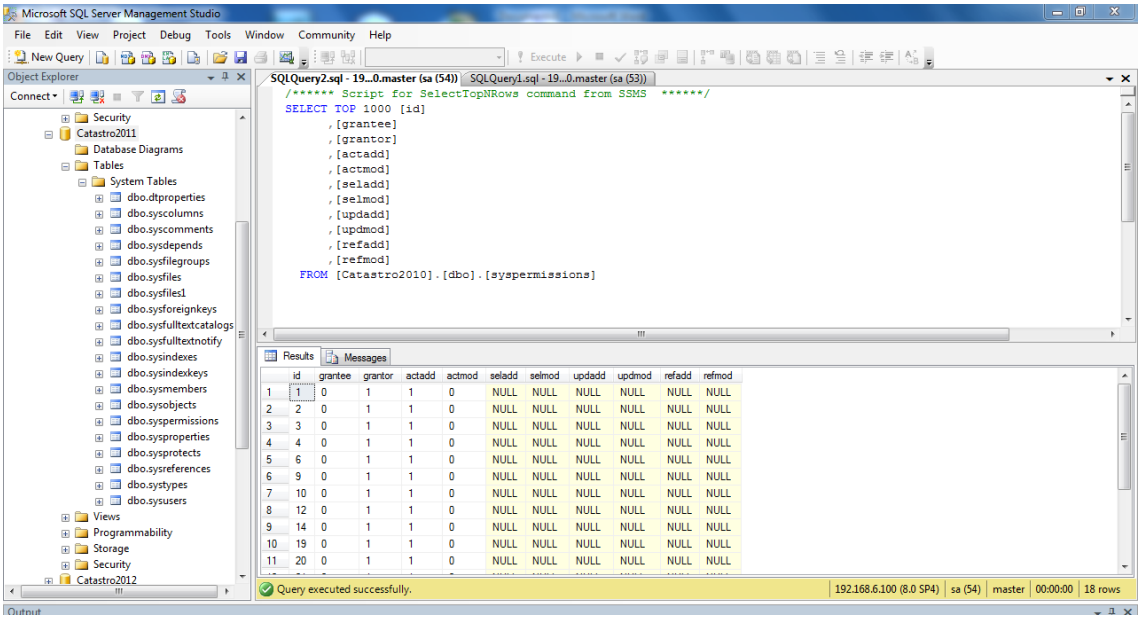


Figura 6. 50: Tablas catastro 2011.

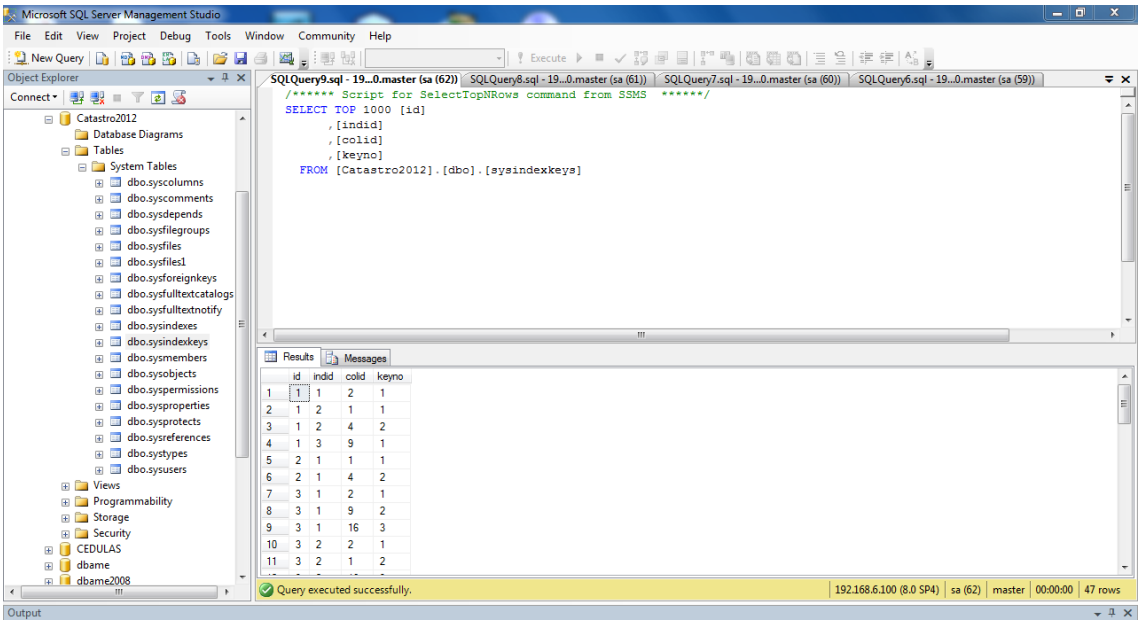


Figura 6. 51: Tablas catastro 2012.

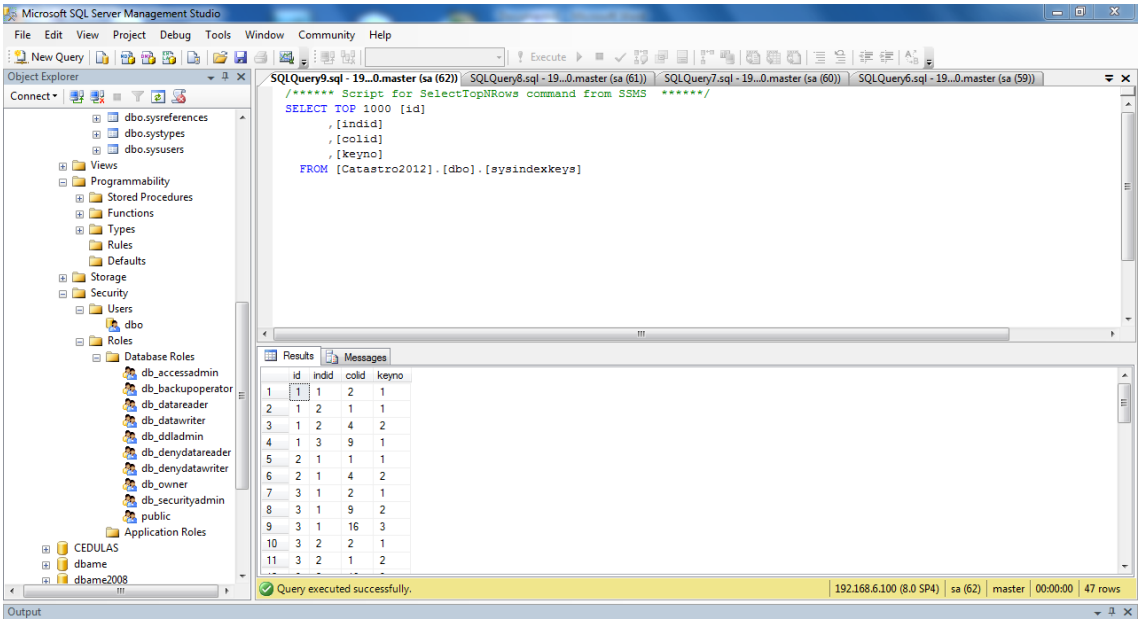


Figura 6. 52: roles catastro 2012.

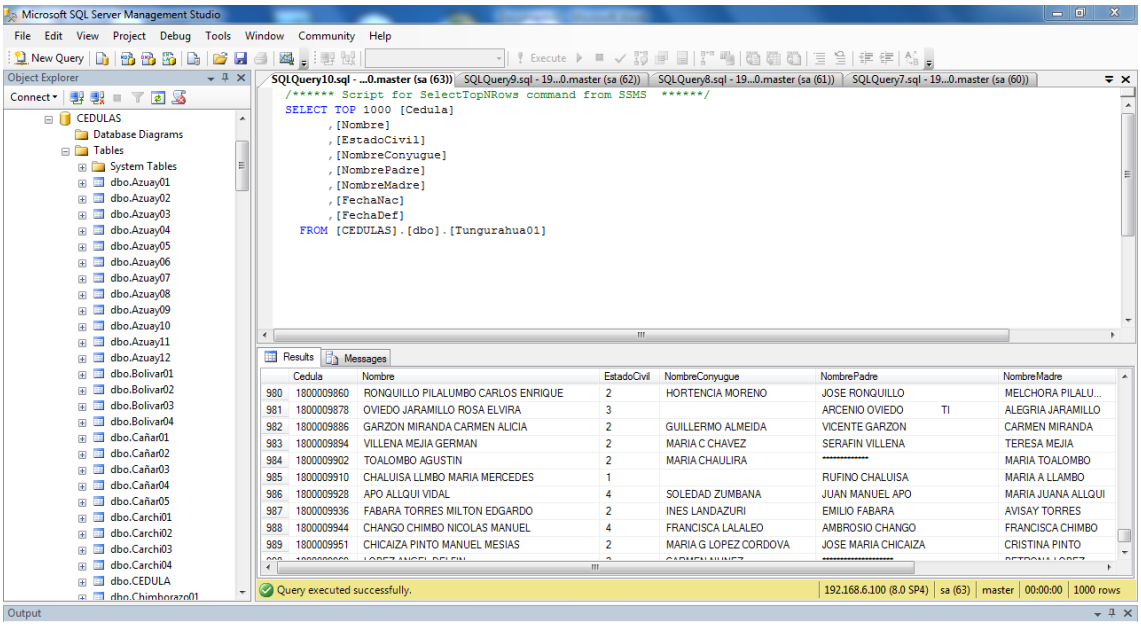


Figura 6. 53: Tablas de cédulas.

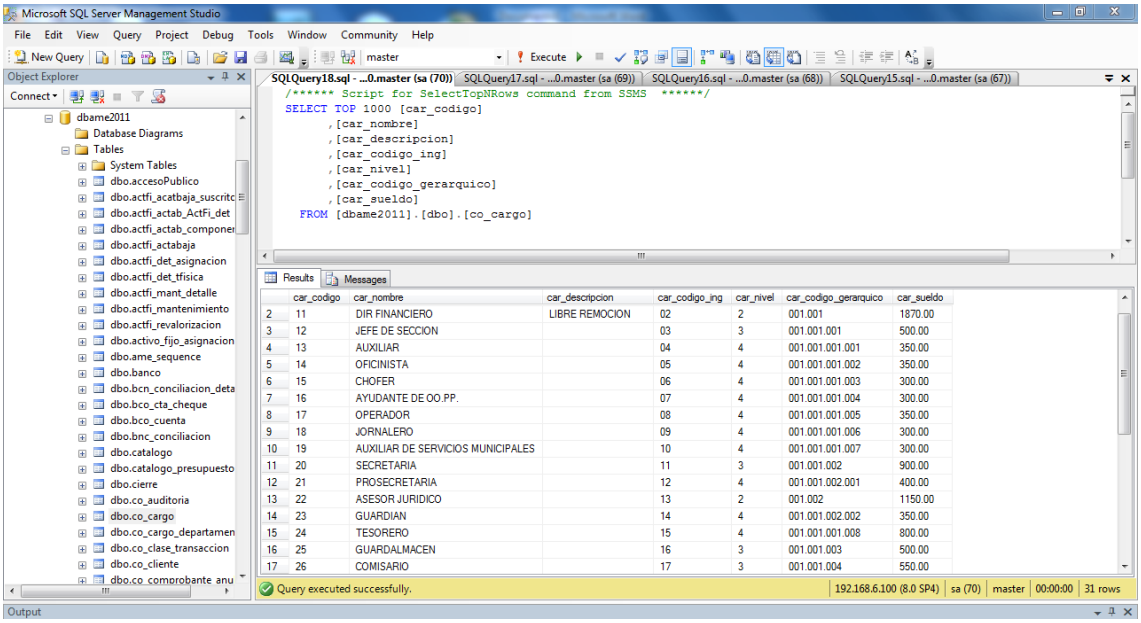


Figura 6. 54: Tabla de sueldos con rango de empleos.

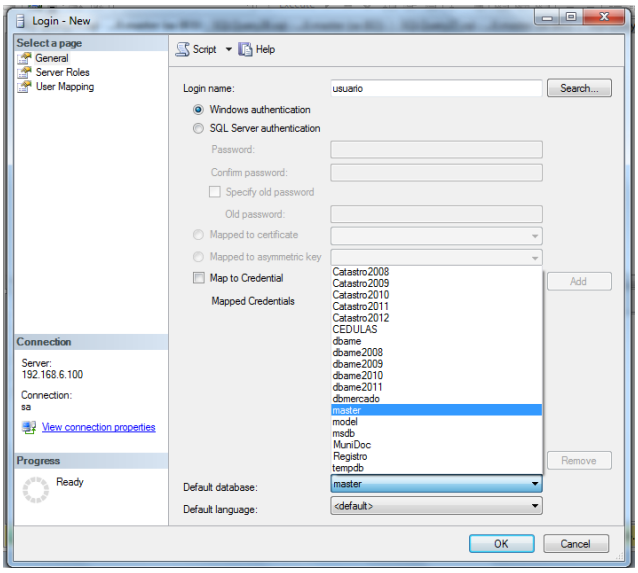


Figura 6. 55: Agregando nuevo usuario.

Ataque al servicio de Microsoft Windows SMB

Este ataque se lo aplico al puerto 445 correspondiente al servicio de Microsoft Windows SMB, para esto se empleo el framework metasploit existente en backtrack, el cual es una herramienta GNU escrita en Perl y con utilización de diversos lenguajes de programación como C, Pyton, ASM, etc. Metasploit se ejecuta bajo una consola CYGWIN y trabaja con una base de datos en la cual se encuentran toda la lista de exploits y vulnerabilidades, lo único que tenemos que indicarle a metasploit es que vulnerabilidad utilizaremos, que sistema atacaremos, que tipo de ataque utilizaremos y datos diversos que utilizara para atacar al host.

Para ejecutarlo en modo consola, tenemos que escribir msfconsole en la terminal.

Figura 6. 56: Ingreso a metasploit.

Figura 6. 57: pantalla inicial metasploit.

Ya dentro del metasploit tipiamos el comando show exploits el mismo que nos mostrara una gran lista de exploits disponibles, de los cuales tendremos que Seleccionar alguno y dependiendo del sistema que deseemos atacar en nuestro caso escogeremos el exploit ms08_067_netapi para tratar de provocar un buffer overflow en el sistema y conseguir inyectar código malicioso a través de un payload.

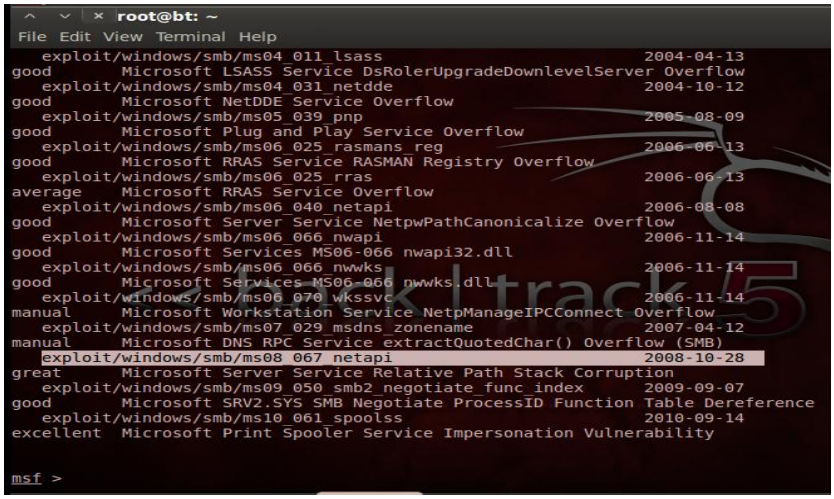


Figura 6. 58: lista de exploits.

Una vez que encontramos un exploit adecuado, le diremos a metasploit que utilizaremos el exploit Microsoft ms08_067_netapi

Figura 6. 59: uso de exploits.

Seguidamente escogemos el payload Windows/meterpreter/reverse_tcp para tratar de establecer una conexión remota.

Figura 6. 60: uso del payload.

Para poder establecer conexión emplearemos los siguientes comandos:

Set LHOST IP de la maquina atacante

Set RHOST IP de la maquina VICTIMA

Luego de esta configuración ejecutaremos el exploit

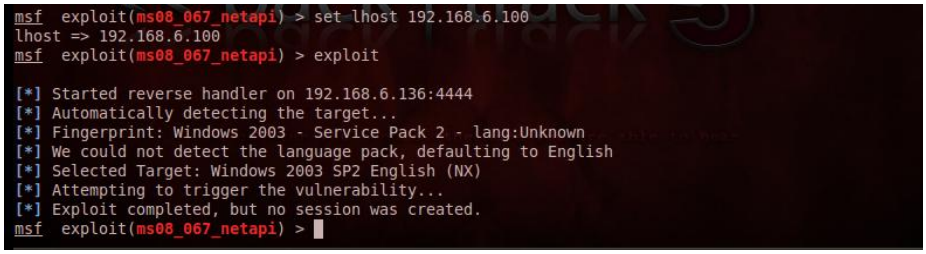


Figura 6. 61: Ejecución exploit.

En los resultados obtenidos se puede observar que es exploit ha sido enviado pero sin embargo no fue abierta la sesión en el servidor.

Con el fin de averiguar a qué se debe que la sesión del servidor no fue abierta con el ataque anterior se procedió a realizar el mismo ataque a un servidor de otra institución con las mismas características de sistema operativo pero con la única diferencia que este servidor no posee licencias de actualizaciones.

Se empleó el mismo exploit anterior y esta vez si se pudo abrir sesión es decir ya estamos dentro de la maquina victima.

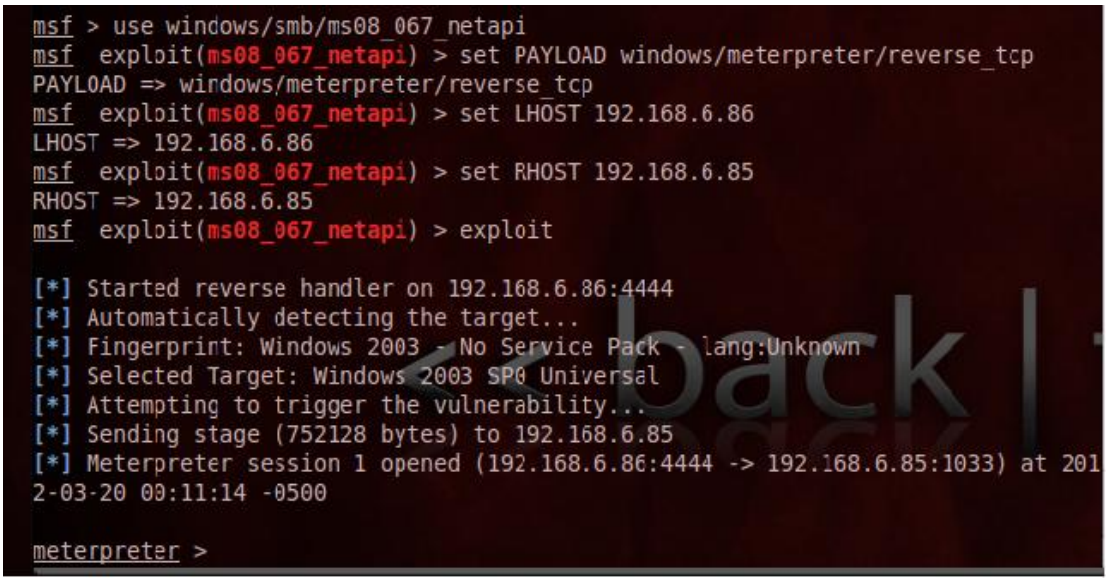


Figura 6. 62: abriendo sesión.

Seguidamente procedemos a entrar en el prom del sistema de la maquina víctima, ya aquí se puede usar diferentes script para conseguir información.

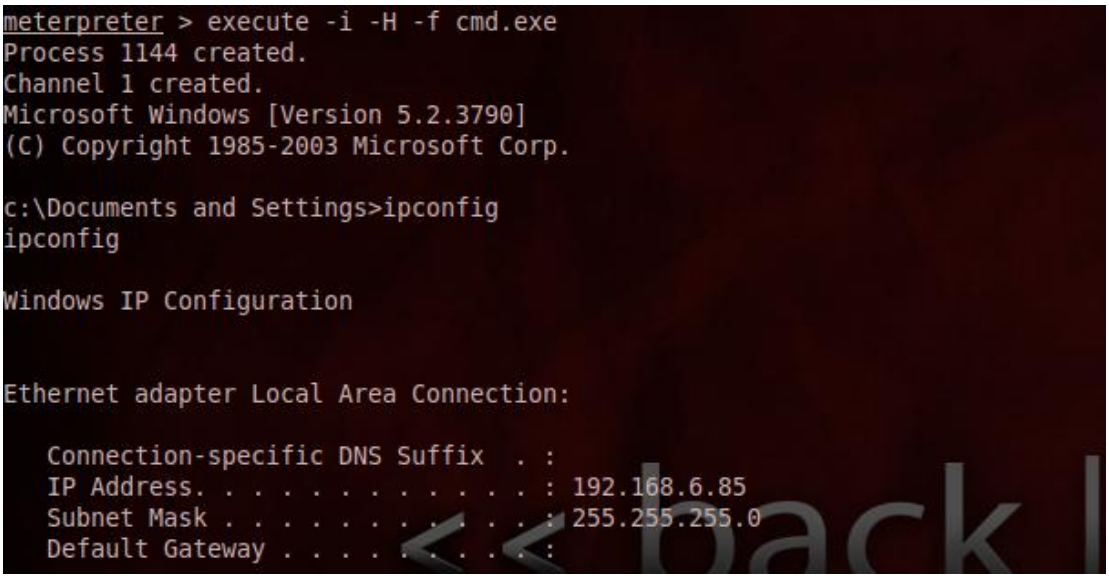


Figura 6. 63: prom del sistema.

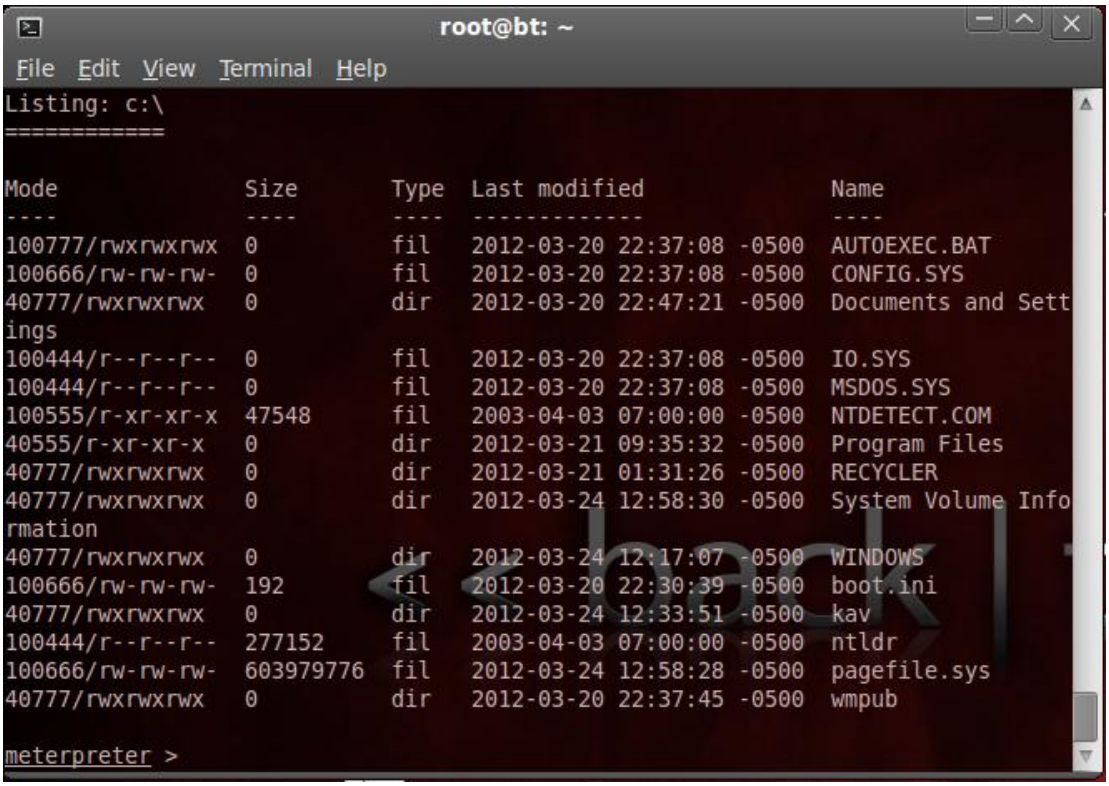


Figura 6. 64: archivos existentes en el disco c.

ATAQUES MIT

Con este tipo de ataque se puede hacer creer a las máquinas de un dominio de broadcast que el equipo atacante es su Gateway, de esta manera las victimas enviaran todo su tráfico al impostor, pudiendo este reenviar el tráfico una vez que ha leído su contenido, para realizar esto se ha escogido Ettercap que viene en backtrack 5

Figura 6. 65: Ingreso a Ettercap.

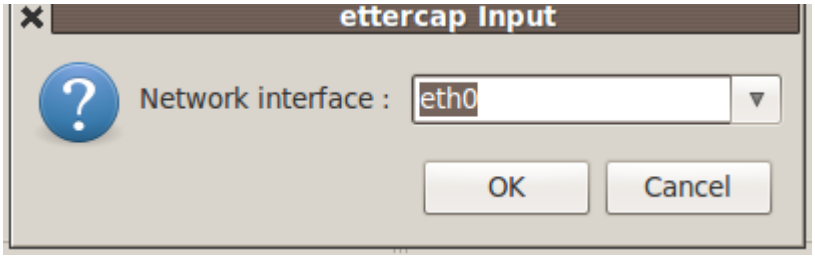


Figura 6. 66: Elección interfaz.

Figura 6. 67: información de arranque de Ettercap.

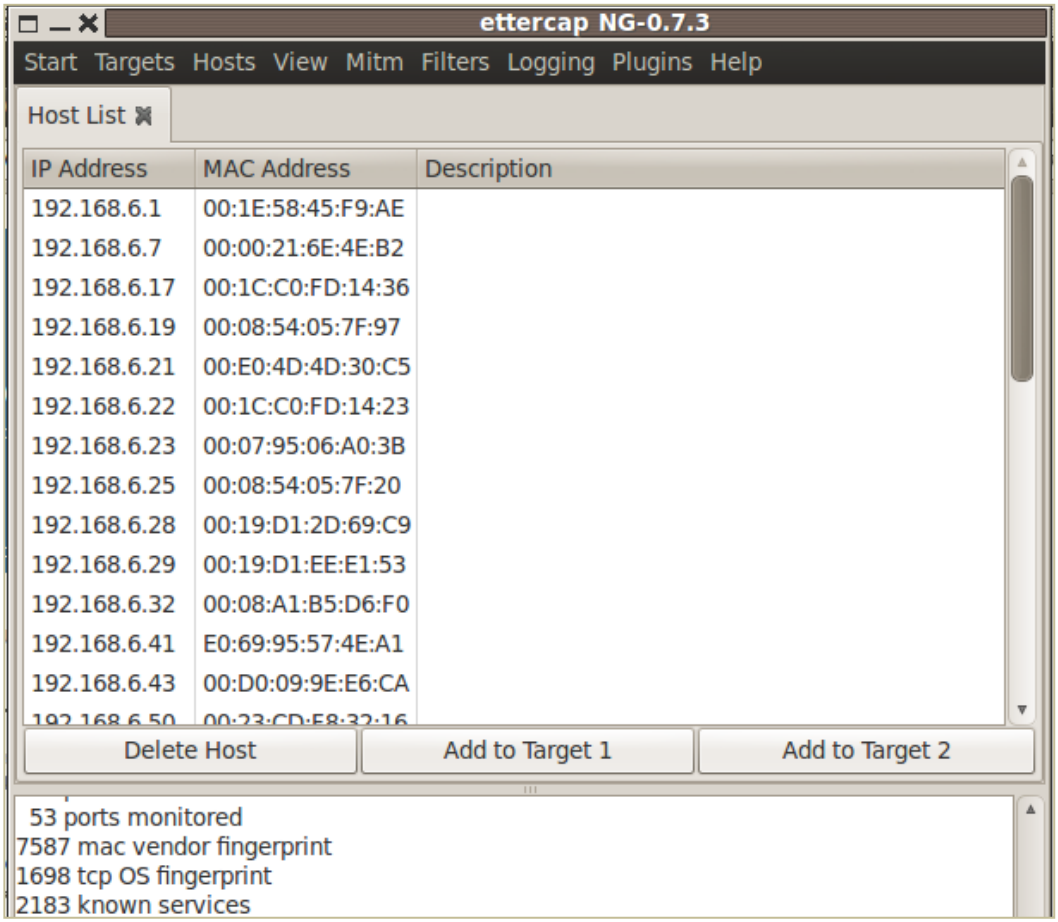


Figura 6. 68: Lista de Host escaneados.

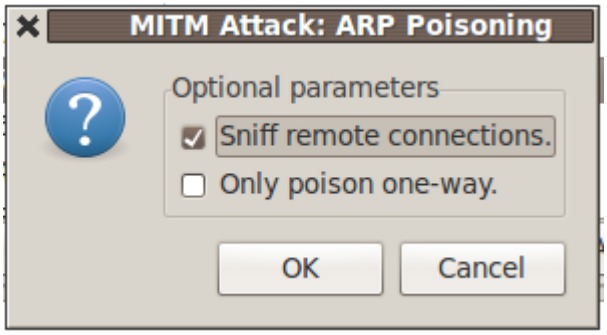


Figura 6. 69: Conexión del ataque.

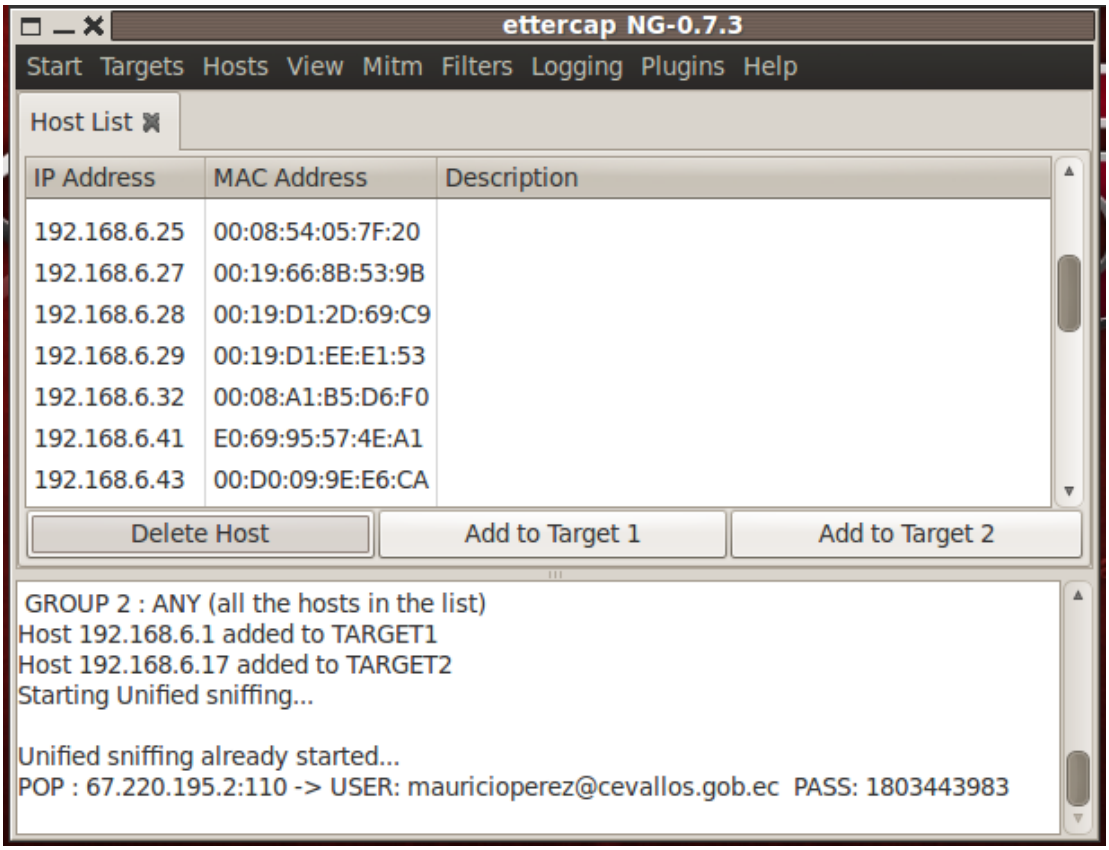


Figura 6. 70: capturando pasword.

Este ataque fue exitoso ya que se pudo obtener un pasword del correo electrónico del administrador de red.

Ataque Dos en el servidor Proxy

Un ataque de denegación de servicios se centra en sobrepasar los límites de recursos establecidos para un servicio determinado, obteniendo como resultado la eliminación temporal del servicio, estos ataques generalmente son realizados en servidores Web, o DNS así como también en elementos básicos de la red, routers o enlaces de red, es por esto que se realizó un ataque de denegación de servicios al servidor de internet utilizando Etercap, para esto nos ubicamos en la pestaña plugins y escogemos dos_attack y ponemos la ip de la victima en nuestro caso pondremos la ip del servidor de Internet.

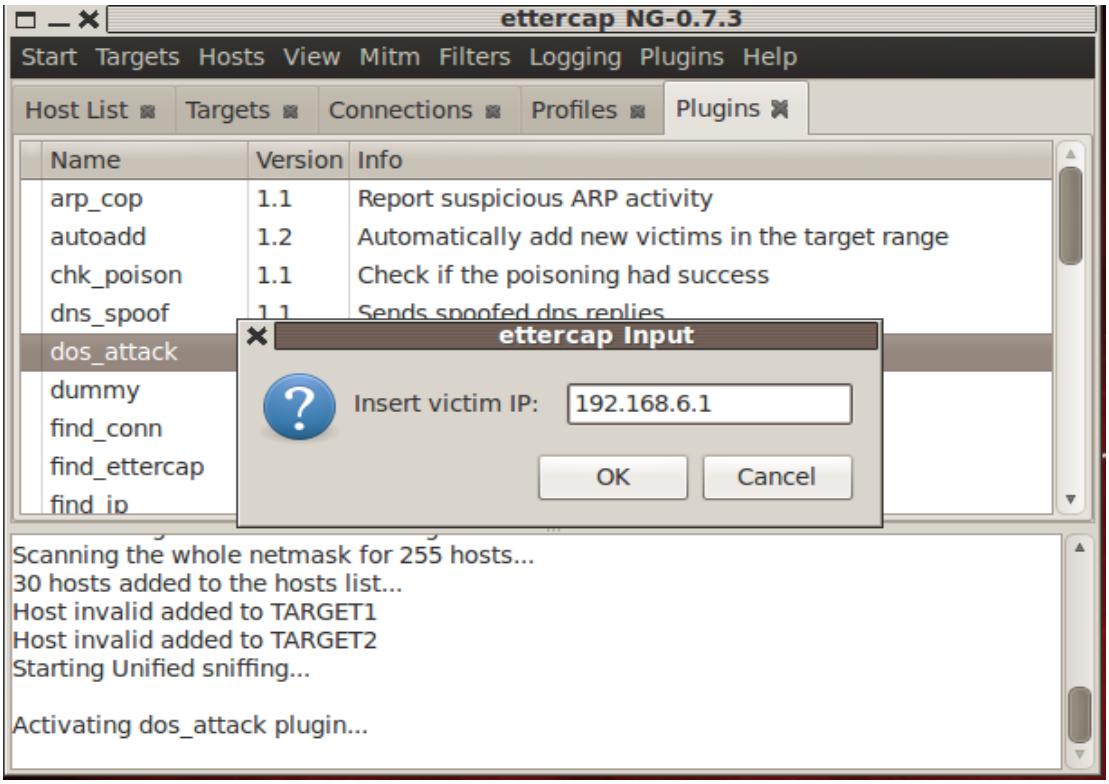


Figura 6. 71: Insertando Ip de Victima.

Seguidamente insertamos cualquier ip para sustituir la ip anterior y así conseguir una denegación.

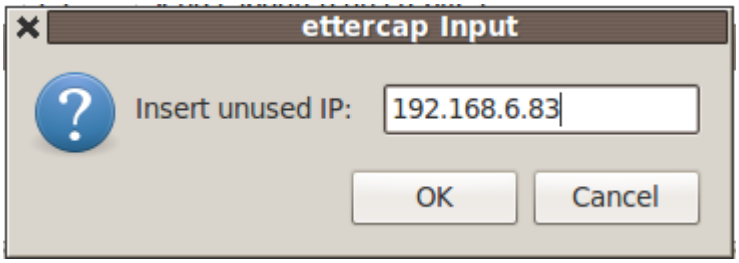


Figura 6. 72: Insertando ip de reemplazo

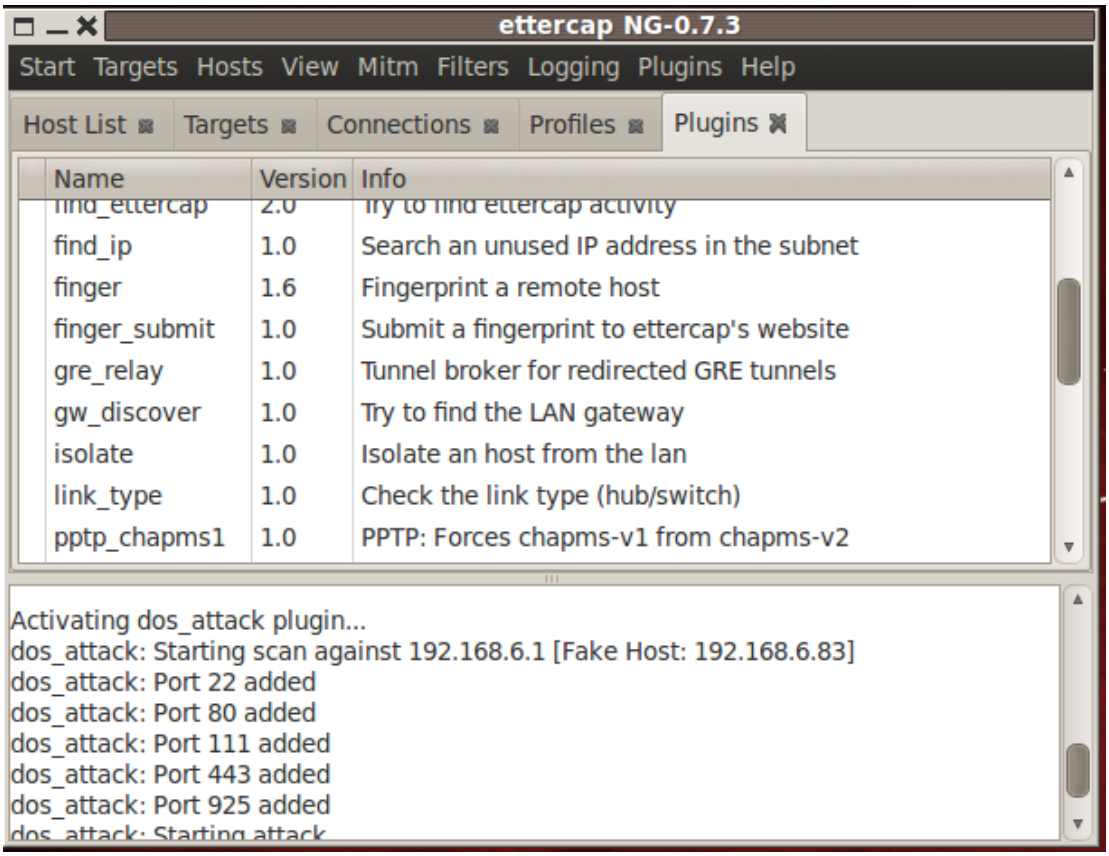


Figura 6. 73: Resultado de ataque.

Entonces nuestro ataque tubo éxito se ataco por el puerto 22, 80, 111, 443, 925.

También se realizo un ataque de denegación de servicios por el puerto 80 que provee el servicio http para esto utilizaremos un archivo ejecutable D2.bat el cual esta programado en Java.

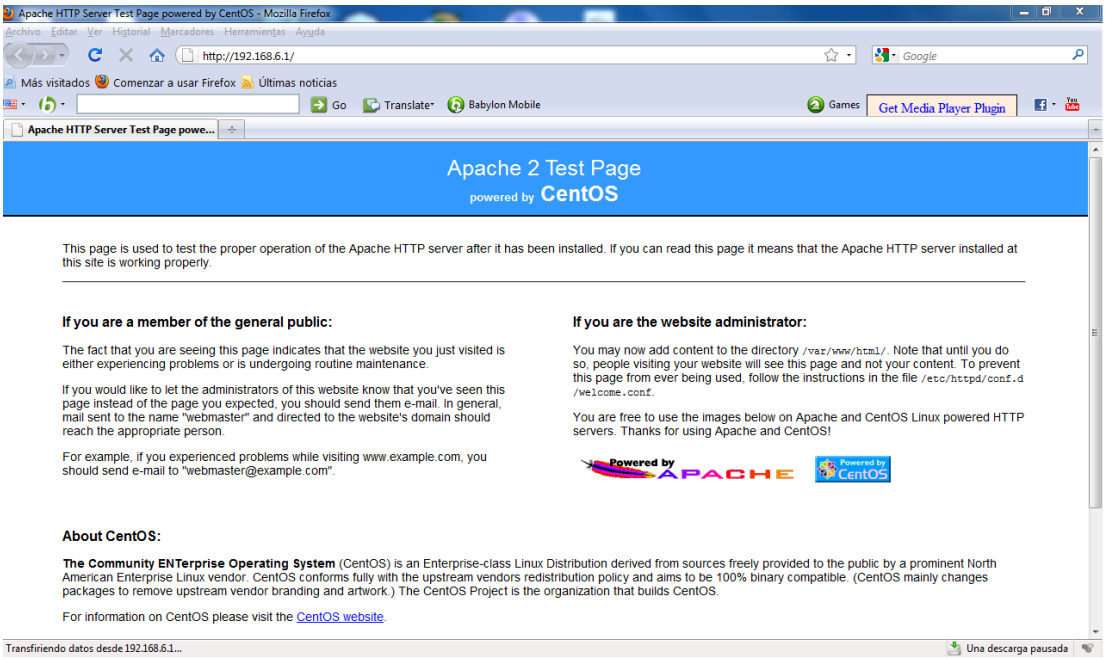


Figura 6. 74: conexión con apache.

Una vez ejecutado el archivo ejecutable D2.bat aparece la siguiente pantalla en la cual ingresaremos la dirección IP del servidor de esta manera así como también podemos ingresar un sitio web ya que mediante esta herramienta se realizan varias peticiones hasta saturar el ancho de banda.

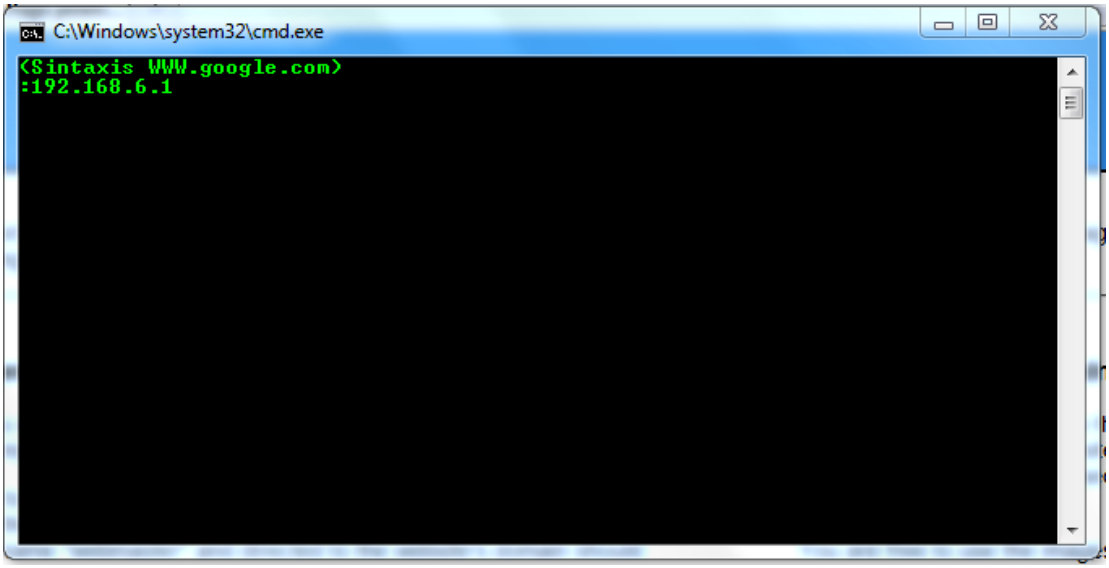


Figura 6. 75: ejecución archivo D2b.bat.

Luego de dar enter nos aparecen los parámetros para proceder a la realización del ataque.

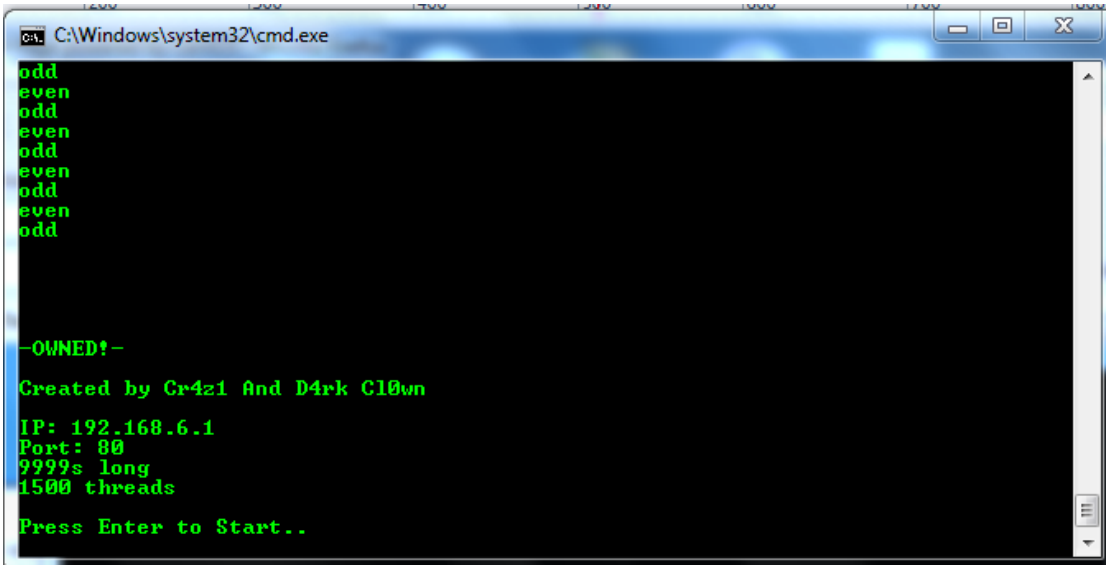


Figura 6. 76: estableciendo parámetros

Luego presionamos enter para que se ejecute el ataque, si el ataque tiene éxito nos aparecerán puntos caso contrario xx en nuestro caso el ataque es exitoso es decir se realizo varias peticiones al servidor apache hasta que se saturo el ancho de banda y dejo de responder la página de inicio de Apache.

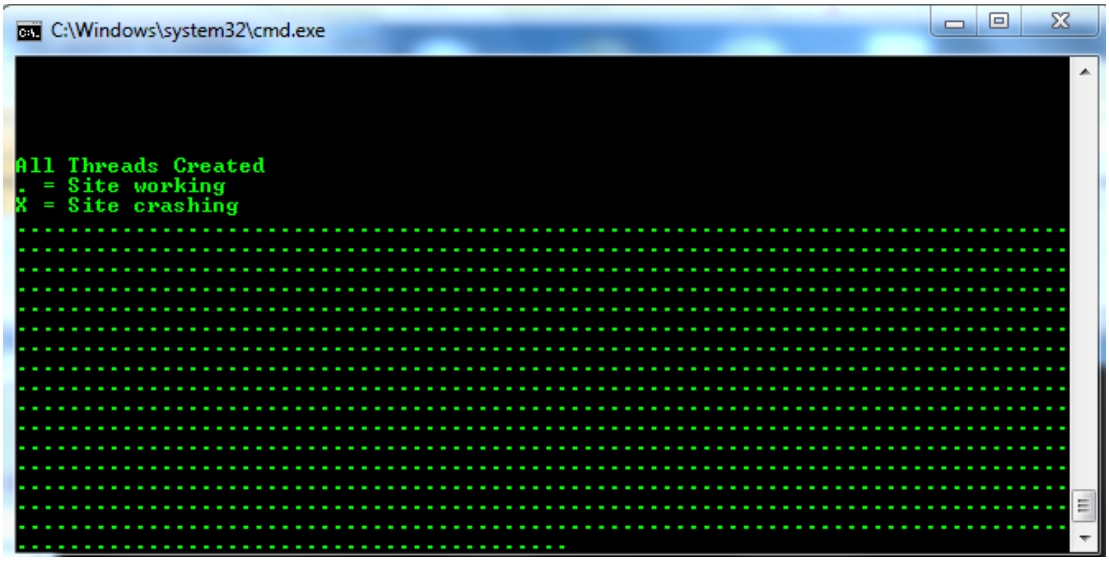


Figura 6. 77: atacando a apache 2.11.

Para la comprobación del éxito del ataque se tratara de conectar nuevamente con apache y se observa que no se puede establecer conexión.

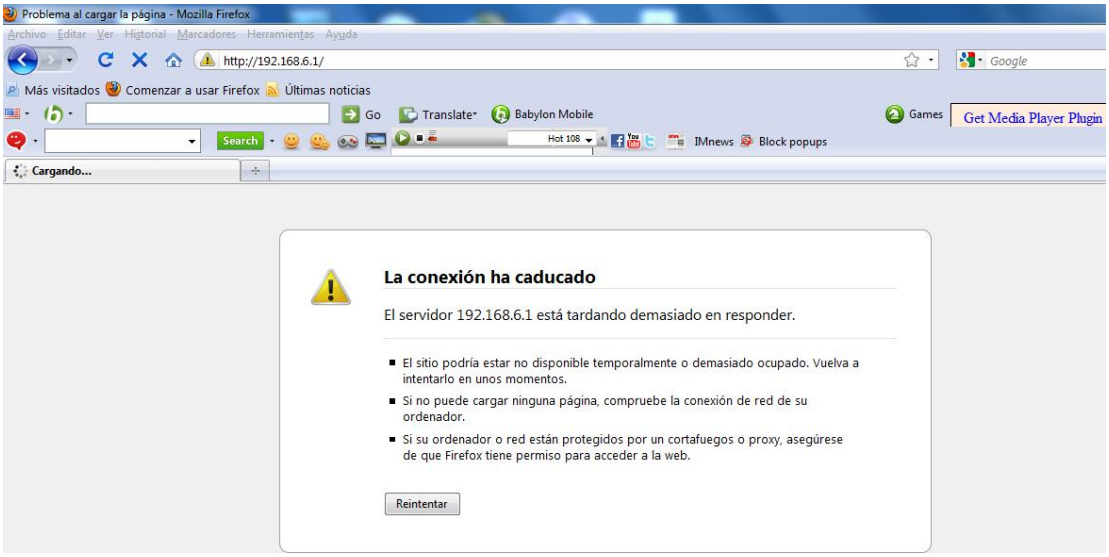


Figura 6. 78: tratando de establecer conexión con apache

Se efectuó el mismo ataque en el servidor de base de datos mediante la conexión a XAMPP para Windows.

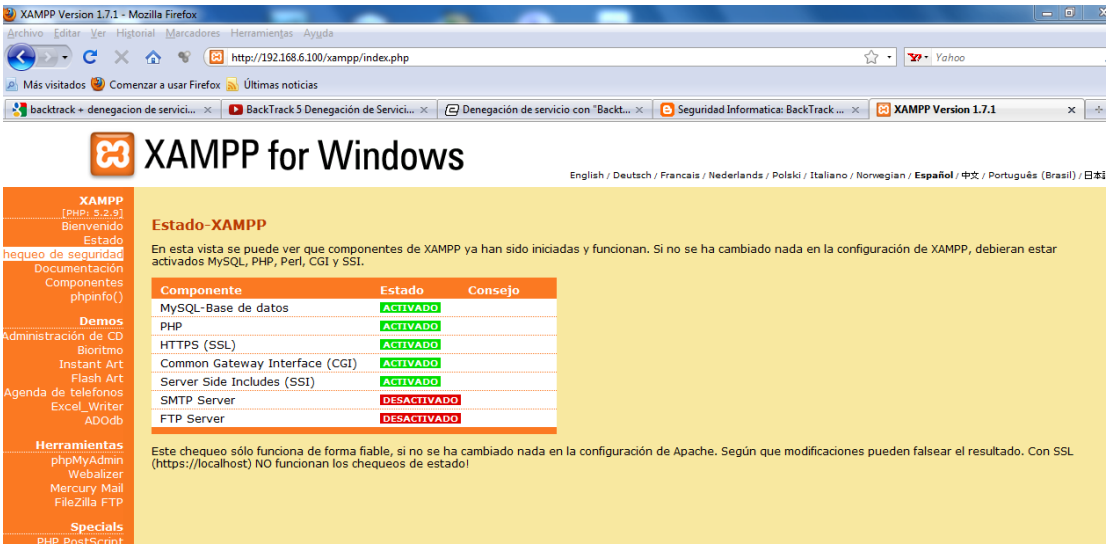


Figura 6. 79: Presentación De XAMPP

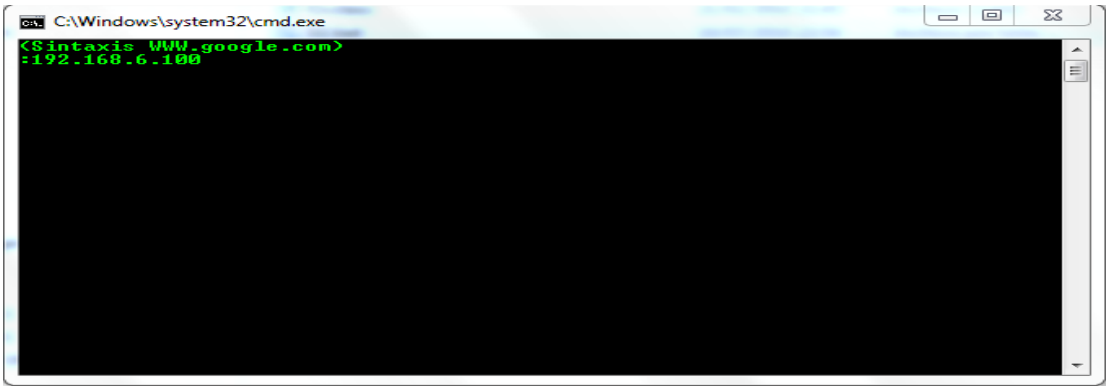


Figura 6. 80: Puesta de IP

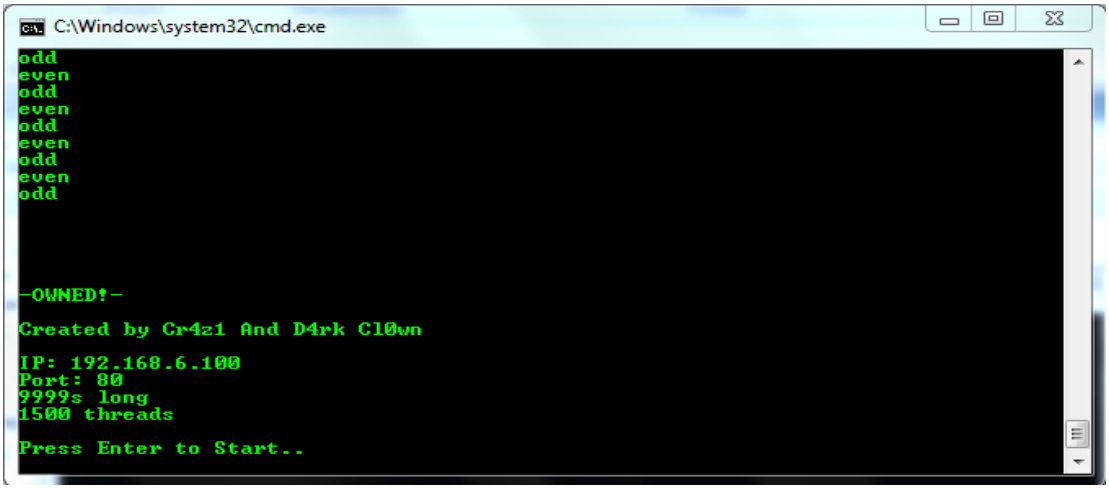


Figura 6. 81: Ejecución

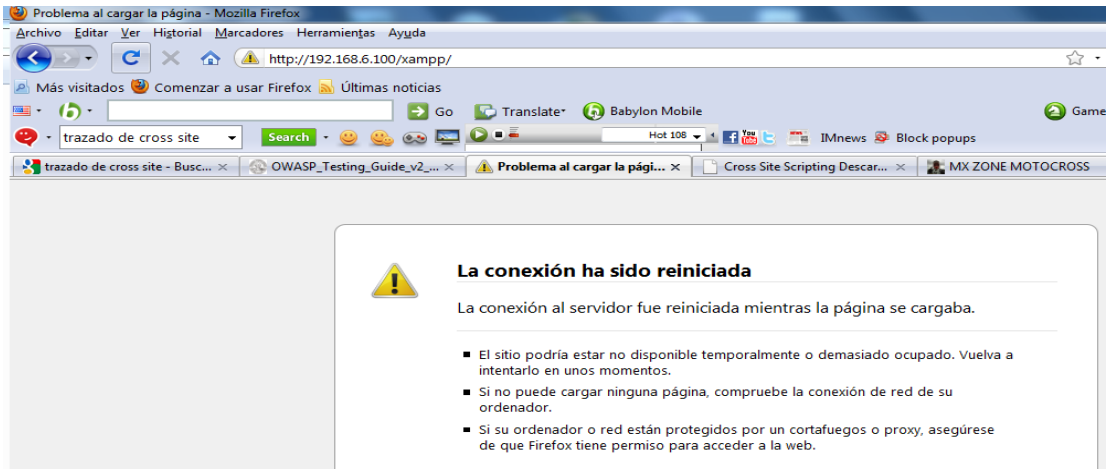


Figura 6. 82: conexión rechazada

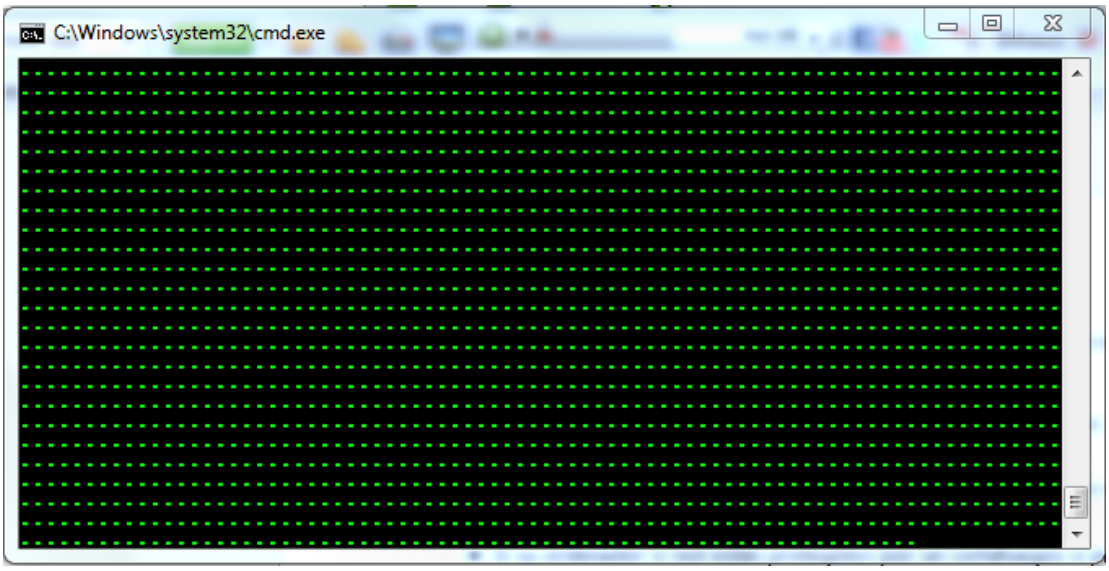


Figura 6. 83: Ataque Exitoso

6.7.4.2. Resultados de ingresos a los servidores de Internet y Base de Datos.

- El ataque a Windows SMB del servidor de Base de Datos utilizando Metasploit no fue exitoso ya que se pudo enviar el exploit pero no se logro abrir la sesión debido a que la versión de Windows server tenia licencias por lo tanto se iban haciendo parques para evitar este tipo de ataques se llego a esta conclusión porque se monto otro servidor con las mismas características pero sin licencia y si se pudo abrir sesión.
- Se logro ingresar a la base de datos del GAD. Municipal y manipular información.
- Los ataques de denegación de servicios en el servidor proxy fueron exitosos ya que se logro eliminar temporalmente los servicios que prestaba por los puertos 22, 80, 111, 443 y 925.
- En el servidor de base de datos también era posible ejecutar el ataque DOS pero no se llevo a cabo para evitar tener problemas con los usuarios y además producir alteraciones en la base de datos.
- Los ataques de saturación de ancho de banda también logrando eliminar temporalmente el servicio de apache en el caso de Linux y XAMPP en el caso de Windows.

6.7.4.3. Hackeo de la contraseña de la red inalámbrica.

Objetivos del hackeo a la red inalámbrica

- Descifrar las contraseñas para establecer la conexión.
- Conectarse a la red por la wireless y de esta manara robar o manipular información.
- Se pudo descifrar la contraseña de la red por lo tanto se logro ingresar como usuario a la red viendo de esta manera los mismos resultados como si estuviéramos conectados con un cable de red, esta es una de las mas graves vulnerabilidades tomando en cuenta que una persona mal intencionada no tiene necesidad de estar dentro del municipio si no que se puede conectar desde las afueras del mismo y de esta manera radien se diera cuenta.

Requisitos para el proceso de hackeo de la red inalambrica:

Se utilizó un DVD booteable de Backtrack5 con el objetivo de poder capturar todas las conexiones inalámbricas existentes dentro de la institución.

Como primera instancia se procedió a ejecutar bactrack5.

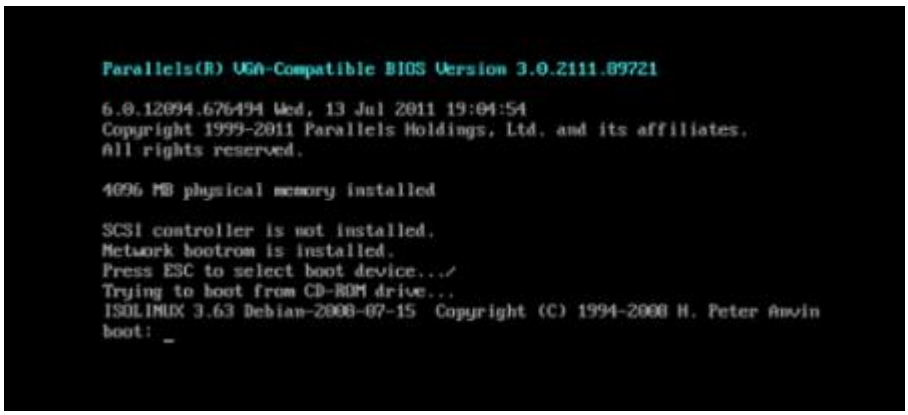


Figura 6. 84: Arranque del equipo desde bactrack5.

Una vez aquí abrimos la terminal porque necesitamos utilizar la línea de comandos, en la misma escribimos el comando iwconfig, esto para que nos muestre una lista con todas las interfaces de red que tenemos instaladas en nuestra computadora, es decir estamos buscando una wlan0, ath0 o wifi0.

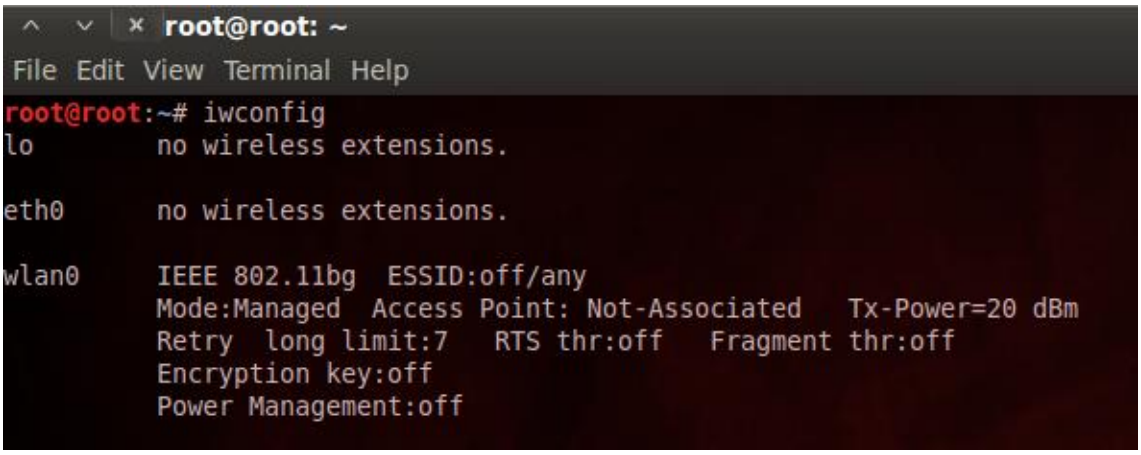


Figura 6. 85: Interfaces de red instaladas.

Simulando ser un hacker cambiamos nuestra Mac Address por seguridad para no ser descubiertos, detenemos la interfaz con el comando airmon-ng y procedemos al cambio de Macc Address

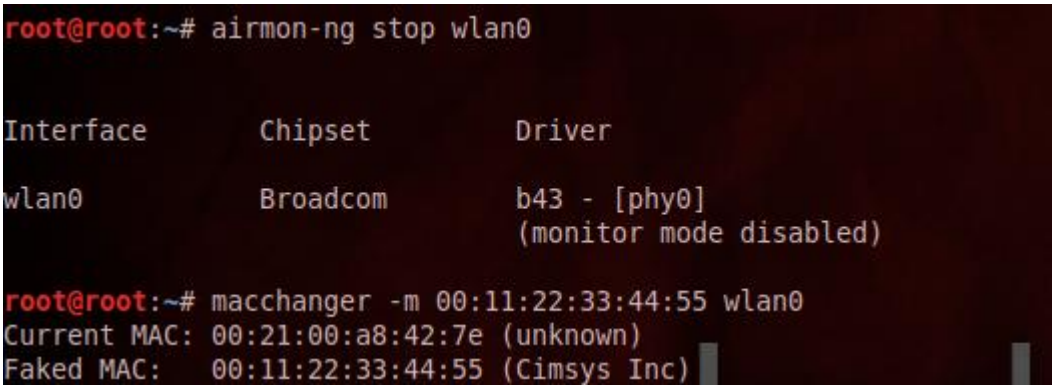


Figura 6. 86: Cambio de Macc Adrees.

Como siguiente paso se colocó la tarjeta en modo monitor es decir que en lugar de tratar de unirse a una red única e ignorar todas las demás redes, va grabar todo lo que le indiquemos y lo que le sea posible.

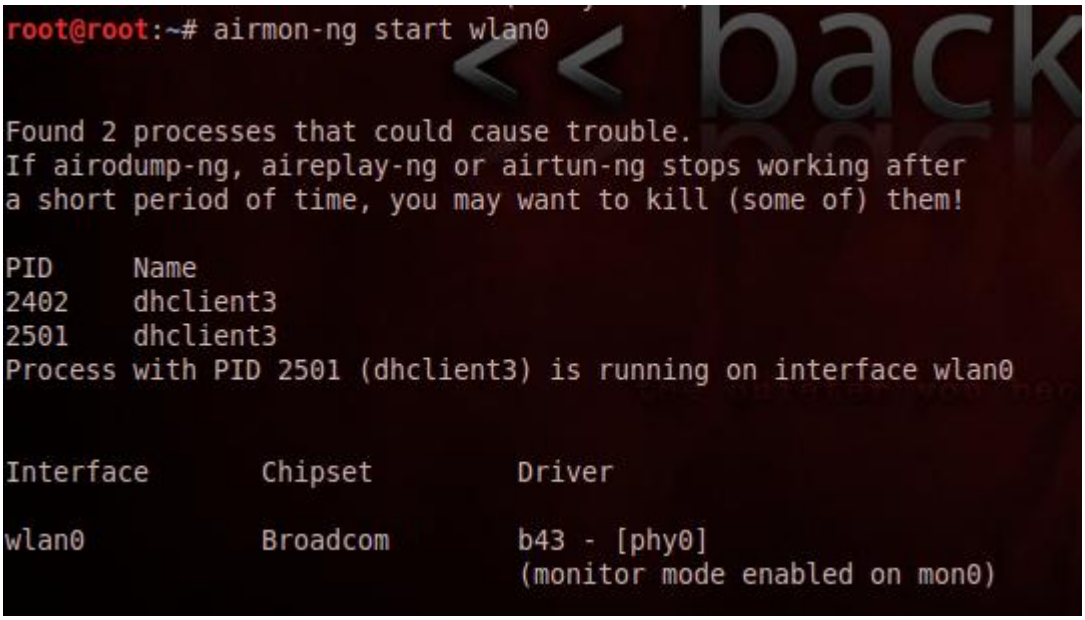


Figura 6. 87: Puesta de la tarjeta en modo monitor.

Como tuvimos éxito para pasar el dispositivo a "modo monitor "pues nos apareció (monitor mode enabled on mon0), procedimos a escanear las ondas de radio para averiguar algo más de información para esto utilizamos el comando airodump-ng mon0 este comando nos va mostrar una pantalla llena de información sobre todas las redes inalámbricas individuales y todos los clientes conectados a ellas.

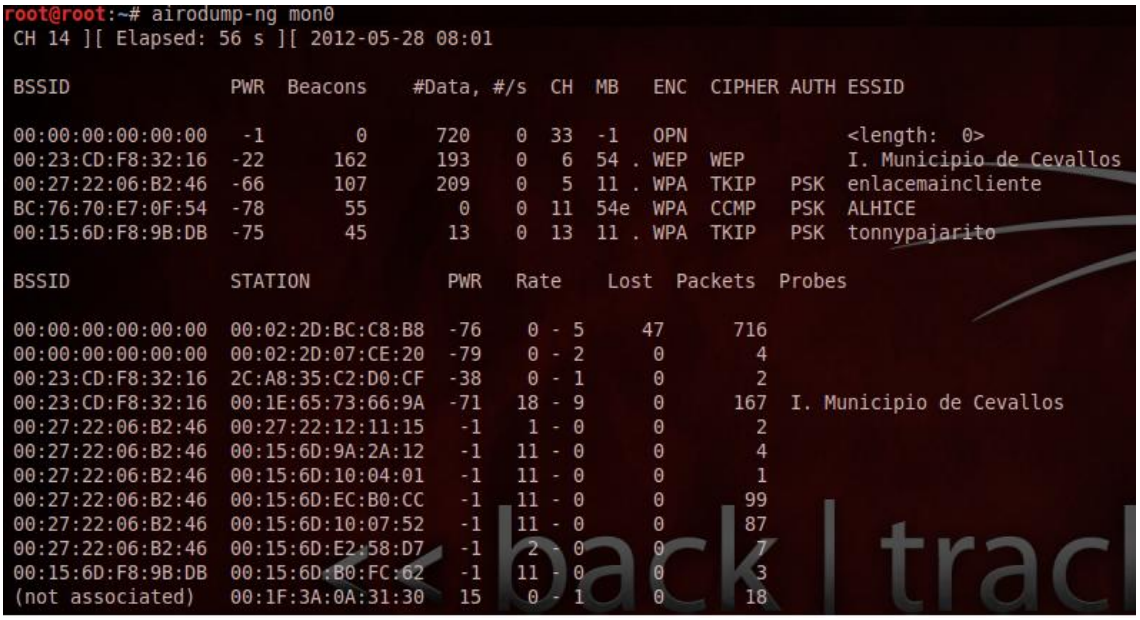


Figura 6. 88: Monitoreo de redes inalámbricas.

Ahora ubicamos la red wifi que queremos hackear de entre la lista obtenida anteriormente y copiamos el numero hexadecimal de la columna denominada BSSID (dirección MAC del router), en la columna ENC podemos observar la seguridad que en este caso está protegida con WEP, con toda esta información el siguiente paso fue concentrarnos en la red inalámbrica que era nuestro objetivo para poder bloquearla en el canal correcto.

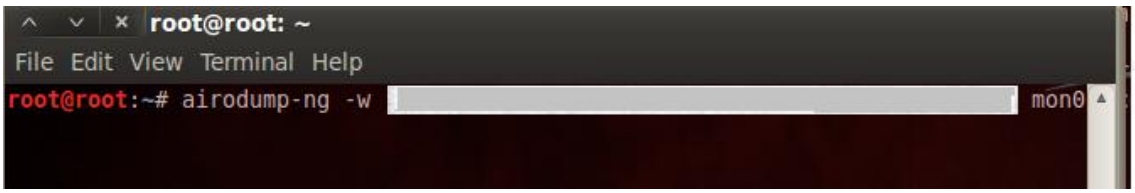


Figura 6. 89: Comando para grabar paquetes de datos de la red seleccionada.

Aquí se están grabando los paquetes de datos del archivo de la red seleccionada, cabe mencionar que debemos tener al menos una persona conectada para que esto funcione, en la columna con la etiqueta #Data es la cantidad de paquetes con datos útiles que se van capturando.

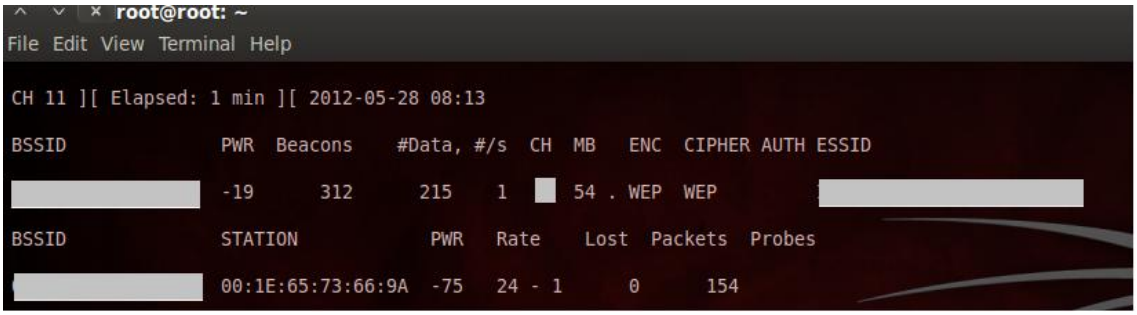


Figura 6. 90: Grabando los paquetes de datos en un archivo de la red seleccionada.

Una vez que el numero de paquetes coleccionados alcanzo los 5000, empezamos a crackear estos paquetes, utilizando otra consola en la cual usamos el comando aircrack-ng <bssid> <output filename="" from="" earlier="">*.cap</output></bssid>

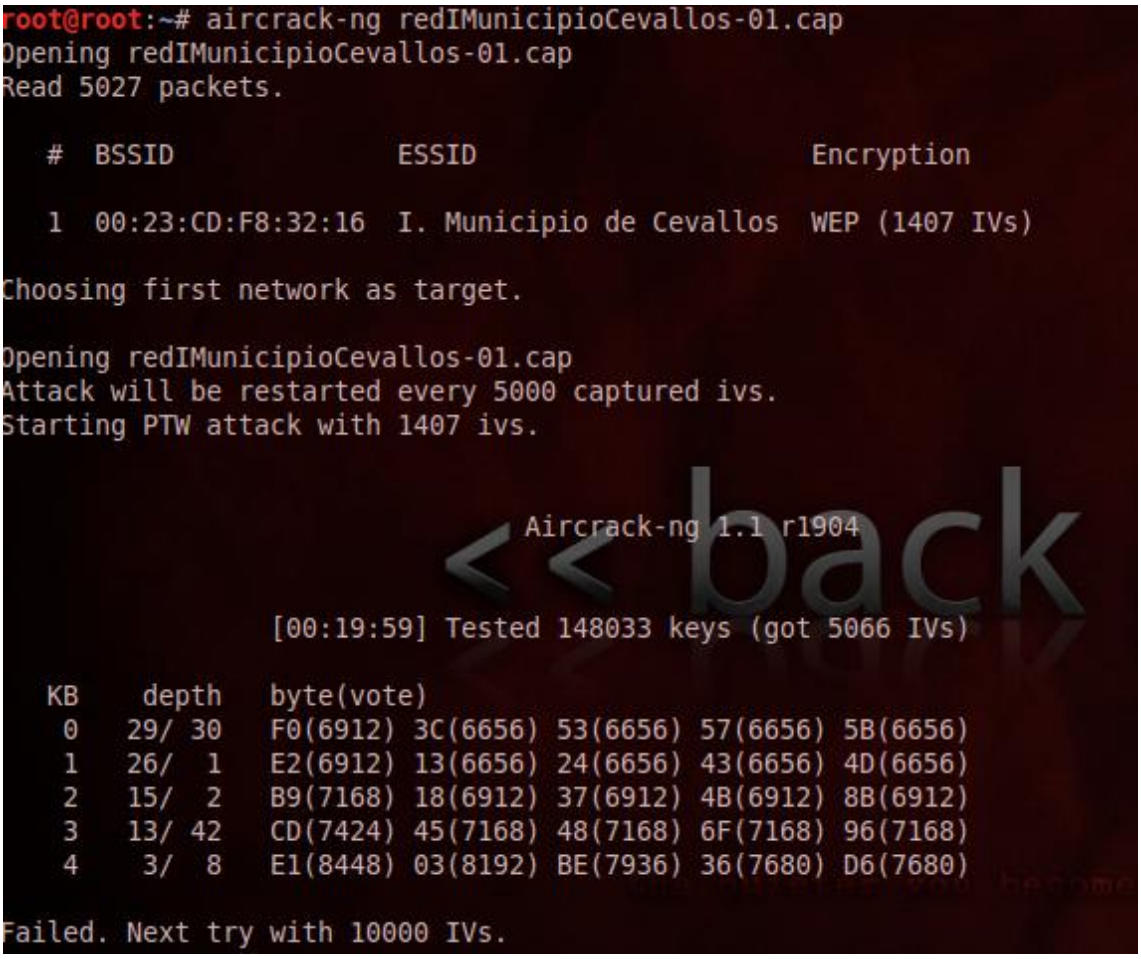


Figura 6. 91: Descifrando contraseña

Como todavía aun no son suficientes los paquetes coleccionados para descifrar la contraseña esperamos a que se completen y ponemos el comando anterior para ver si esta vez ya logramos descifrar la contraseña.

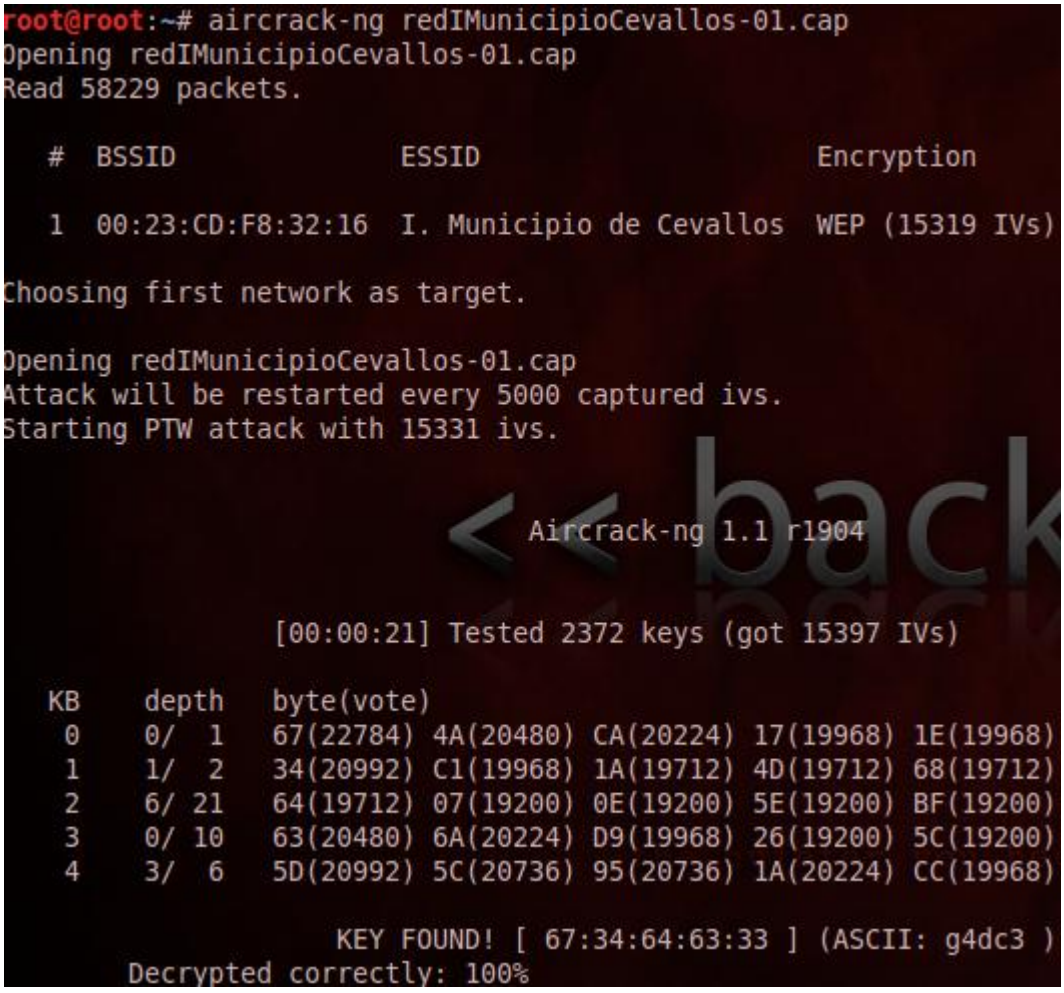


Figura 6. 92: Obtención de la contraseña

Capturados 15397 paquetes ya logramos descifrar la contraseña la cual nos devolvió en formato hexadecimal y también en formato ASCII.

6.7.5. Fase 5: BORRADO DE HUELLAS

Cabe recalcar que en el presente análisis de vulnerabilidades y hacking ético no es necesaria la realización de la fase de borrador de huellas, puesto que todas las

pruebas, accesos y ataques, fueron realizados en un ambiente seguro, bajo la autorización y vigilancia del Ing. Administrador de la Red
De Datos Del Gobierno Autónomo Descentralizado Municipal del Cantón Cevallos.

6.8. Conclusiones y Recomendaciones

6.8.1. Conclusiones

- Mediante la aplicación del hacking ético se pudo determinar las siguientes vulnerabilidades:
- Servidor de base de datos tenemos las siguientes credenciales: Microsoft SQL Server credenciales predeterminadas, Microsoft Windows server vulnerable a ataques MIT, vulnerabilidad en el servidor web PHP ante ataques de denegación de servicios.
- Servidor de Internet: tenemos la versión de Apache HTTP Server no se encuentra actualizada, puede ser Afectada por un ataque de denegación de servicios así como también es vulnerable a ataques MIT.
- Wireless LAN: el tipo de encriptación de la wireless es Web por lo tanto se puede descifrar la contraseña, considerando que esta sería la mayor vulnerabilidad y la más perjudicial debido a que el hacker no necesita estar conectado adentro de la institución si no que puede simplemente conectarse desde los alrededores del municipio y robar alterar o borrar en su totalidad toda la información.
- Para la realización de los principales ataque de seguridad informática se utilizo la distribución GNU BackTrack en su versión 5 R1, la cual cuenta con herramientas importantes útiles en el desarrollo de todas las fases del hackeo ético.

6.8.2. Recomendaciones.

- Rediseñar la estructura en cuanto al diseño de la LAN empleando router y switch para la creación de VLANs de esta manera se puede conseguir mayor confidencialidad, agilidad en cuanto a la transmisión de datos y evitar colisiones de ancho de banda.
- Implementar mecanismos de autenticación más robustos aplicando todas las normas de elección de claves, no dejar los valores por defecto en el ingreso a la base de datos.
- Implementar cortafuegos en el servidor de Base DE Base de Datos para restringir el acceso a la red para evitar denegación de servicios a ataques MIT
- Crear IPTABLES en el servidor de internet para tener con control de las maquinas mediante su IP y MAC y así evitar ataques de denegación de servicios, ataques Mit.
- Usar autentificación 802.1x para las redes inalámbricas con el objetivo de proporcionar acceso controlado entre dispositivos inalámbricos clientes, así como también es importante la implementación de un portal cautivo para vigilar el trafico http.
- También se podría recomendar realizar periódicamente testeos de red con la distribución libre BackTrack que posee todas las herramientas útiles en cuanto al testeo de vulnerabilidades y así ir detectando las diferentes anomalías que se vayan presentando.

6.9. Bibliografía.

- **Libros:**
  - Carlos Tori, Hacking Ético, primera impresión mayo del 2008 en Mastroianni impresiones Buenos aires argentina
  - JORGE Ramiro Aguirre, Libro Electrónico de Seguridad Informática y Criptografía, año de publicación 2006. Versión 4.1
  - ANDREW s. Tanenbaum, Redes de Computadoras 4ta edición, pearson educación, México, 2003
  - AGUILERA, Purificación. Seguridad Informática. Editorial Editex, Madrid- España.
- **Tesis**
  - Liliana Rodríguez, "HACKEO ÉTICO Y SUS PRINCIPALES METODOLOGÍAS", Facultad de Ciencias de la Computación y Electrónica de la Universidad Tecnológica, memoria técnica previa a la obtención del título de ingeniera en informática.
- **Leyes**
  - Ley de comercio electrónico, firmas electrónicas y mensajes de datos, ley publicada en el Registro Oficial N° 557 del 17 de Abril del 2002.
- **Internet**
  - Garbage collector, Informática, extraído el 25 de octubre del 2011 desde:http://www.error500.net/garbagecollector/archives/categorias/apuntes/concepto_de_informatica.php
  - Introducción a la Informática recuperado el 6 de Noviembre del 2001 desde:http://www.monografias.com/trabajos15/introduccion-informatica/introduccion-informatica.shtml
  - curso de informática básica, extraído el 25 de octubre del 2011 desde: http://www.monografias.com/trabajos11/curinfa/curinfa.shtml
  - Introducción a la Informática

http://www.monografias.com/trabajos15/introduccion-informatica/introduccion-informatica.shtml

- Diccionario de informática consultado el 20 de Noviembre del 2011 desde http://www.alegsa.com.ar/Dic/seguridad%20informatica.php
- Hacking ético versus defensa en profundidad descargado el 20 de Noviembre del 2011 desde: http://www.dsteamseguridad.com/museo/HACKIN%20ETICO_VS_DEFENSA_PROFUNDIDAD_JUANBERRIO.pdf
- Instituto para la Seguridad en Internet extraído el 25 de Octubre de 2011 desde http://www.instisec.com/publico/verarticulo.asp?id=58
- Coordinación de emergencia en redes informáticas de la república de argentina descargado el 9 de Noviembre del 2011 desde http://www.arcert.gov.ar/webs/manual/manual_de_seguridad.pdf

- Ethical hacking: Test de intrusión. Principales metodologías consultado el 20 de Octubre del 2011 desde: http://www.monografias.com/trabajos71/ethical-hacking-test-intrusion-metodologias/ethical-hacking-test-intrusion-metodologias.shtml
- Seguridad en redes consultado el 27 de Octubre del 2011 desde: http://www.monografias.com/trabajos/protocolotcpip/protocolotcpip.shtml
- Protocolo Tcp/iP descargado el 20 de Noviembre del 2011 desde: https://www.tlm.unavarra.es/~daniel/docencia/lir/lir05_06/slides/1-Conceptosbasicos.pdf
- Pruebas de instrucción descargado el 10 de Enero del 2012 desde: http://www.espe.edu.ec/portal/files/sitiocongreso/congreso/c_computacion/Seminario_Ethical_Hacking.pdf
- conceptos de red y tipos de redes extraído el 19 de Noviembre del 2011 desde: http://www.eveliux.com/mx/concepto-de-red-y-tipos-de-redes.php
- Redes de Computadoras consultado El 20 de Noviembre del 2011 desde: http://www.monografias.com/trabajos11/reco/reco.shtml

- Servicio web. Descargado el 20 de Noviembre del 2011 desde: http://www.it.aut.uah.es/~jdp/at/SEGURIDAD06.pdf
- Servicio mail, extraído el 17 de Noviembre del 2011 desde: http://www.ilustrados.com/tema/1551/Configuracion-Intranet.html
- Servicio ftp, extraído el 17 de Noviembre del 2011 desde: http://www.monografias.com/trabajos15/servicios-tcp-ip/servicios-tcp-ip.shtml
- Servidor FTP consultado el 17 de Noviembre del 2011 desde: http://mmc.geofisica.unam.mx/LuCAS/Manuales-LuCAS/doc-unixsec/unixsec-html/node218.html
- Intranet, descargado el 17 de Noviembre del 2011 desde: http://cs.uns.edu.ar/~mc/Auditoria/downloads/Exposiciones/INTRANETS.pdf
- Auditoria y seguridad Informática, consultado el 27 de enero del 2012 desde: http://www.monografias.com/trabajos32/auditoria-seguridad-informatica/auditoria-seguridad-informatica2.shtml
- Herramientas de hackeo ético consultado el 27 de enero del 2012 desde: http://www.cybsec.com/upload/VictorMonteroSeminarioTecnicasdelPenetrationTestingArgentina.pdf
- Seguridad informática extraído el 23 de marzo del 2012 desde: http://www.monografias.com/trabajos82/la-seguridad-informatica/la-seguridad-informatica2.shtml
- Equipamiento tecnológico de redes consultado el 27 de marzo del 2012 desde: http://recursostic.educacion.es/observatorio/web/es/equipamiento-tecnologico/redes/1005-como-crear-tu-portal-cautivo-con-easy-hotspot
- Implementación de un portal cautivo extraído el 14 de marzo del 2012 desde: http://www.eset-la.com/threat-center/1732-informe-malware-america-latina

6.10. GLOSARIO DE TÉRMINOS.

- **Crack**.- Inclusión de líneas de código en los archivos de registro del software que impide que dicho programa caduque, o localización del número de serie del programa, mediante un generador de números de serie.
- **Denegación de servicios (DoS)**.- Es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.
- **DMZ**.- Zona Desmilitarizada, red interna separada de la red pública.
- **Escáner de puerto**.- Programa que "llama" a cada puerto (un total de 65.535) para comprobar cuáles están abiertos para acceder a una red
- **IDS**.- Sistema de Detección de Intrusión, software o dispositivo que analiza todo el tráfico de una red.
- **Log**.- Registro de datos o información sobre quién, que, cuando, donde y porque un evento ocurre para un dispositivo en particular o aplicación
- **Parche**.- Programa para resolver la vulnerabilidad de una aplicación o sistema
- **Sniffer**.- Programa que permite monitorear una red, y capturar paquetes de la misma, permite también la detección de fallos de seguridad
- **Intrusión.-** Para definir lo de un modo simple, significa lograr el acceso a re cursos de un sistema sin tener la autorización de su dueño o de quien lo controla. Quien lleve a cabo es te tipo de accesos no permitidos es lisa y llanamente un intruso, sea como fue re que lo cataloguen los me dios, las autoridades o el resto de la gente.
- **Exploit.-** es un programa de prueba de concepto que puede estar en código fuente para compilar (fuente.c) o formato binario tipo .exe. Sir ve para aprovechar o demostrar una vulnerabilidad en una aplicación y puede estar escrita en varios lenguajes de programación.
- **Metodología.-** Esto es el resulta do de un grupo de piezas previamente ensambladas: habilidades personales de lógica y creatividad.

- **Footprinting**.- (siguiendo la huella de pisadas) a esta recolección de in formación previa.
- **Penetración testing o chequeo de seguridad**.- consiste en descubrir las vulnerabilidades del sistema antes de que éstas sean encontradas y explotadas por un tercero no autorizado u otra amenaza.
- **TraceRoute**.-devuelve la máquina y la IP de cada salto que da un paquete desde la máquina original hasta la de destino por Inter net. Además, también informa el tiempo en milisegundos que tarda éste.
- **Ping.-**envía un echo request a una máquina especifica en la red. Esto puede ser utilizado para chequear la comunicación entre dos máquinas o para ver si el host específico está corriendo o existe.
- **NsLookup.-** resuelve un hostname a dirección IP o viceversa.
- **Escaneo de vulnerabilidades.-** podrá conocer descuidos de administración o vulnerabilidades previamente conocidas.
- **Nessus.-** busca vulnerabilidades, pero no trata de explotarlas

Anexos

ANEXO 1. MODELO DE ENTREVISTA PERSONAL

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS

Entrevista aplicada al personal del departamento de sistemas.

OBJETIVO DE LA ENTREVISTA: Recolectar información sobre la seguridad de la información transmitida en la intranet del Gobierno Autónomo Descentralizado Municipal del Cantón Cevallos.

CUESTIONARIO

¿Se ha realizado alguna prueba de instrucción en la red interna de datos?

Cuentan la institución con alguna herramienta de software para detectar vulnerabilidades en la intranet?

Existen políticas de seguridad dentro de la institución?.

Al momento del envió de información se utiliza encriptación?.

Cree que los sistemas informáticos existentes en la organización son seguros?

Alguna vez la información ha sido alterada dentro de la institución?

Se permite el acceso a los servidores a todo el personal?

Existen puntos se acceso remoto dentro de la institución?.

Conoce usted si existen host que ejecuten servicios innecesarios?

Las contraseñas de los servidores son reutilizadas en todos?

¿Los archivos son compartidos confidencialmente?

ANEXO 2. MANUAL DE INSTALACIÓN DE BACKTRACK

Instalación de backtrack5

1. Cuando la imagen haya sido cargada y se proceda al encendido de la nueva máquina virtual la pantalla de inicio será la imagen que se muestra a continuación, para lo cual se debe escoger la primera opción, un arranque de BackTrack en modo texto.

Pantalla arranque de BackTrack

2. Una vez que el sistema arranque, en el escritorio podremos ver un script llamado install, lo ejecutamos y obtendremos la pantalla para iniciar la instalación, primeramente escogiendo el idioma de la distribución

Selección de idioma de BackTrack

3. Procedemos a seleccionar la zona horario y región de ubicación

Selección de zona horaria

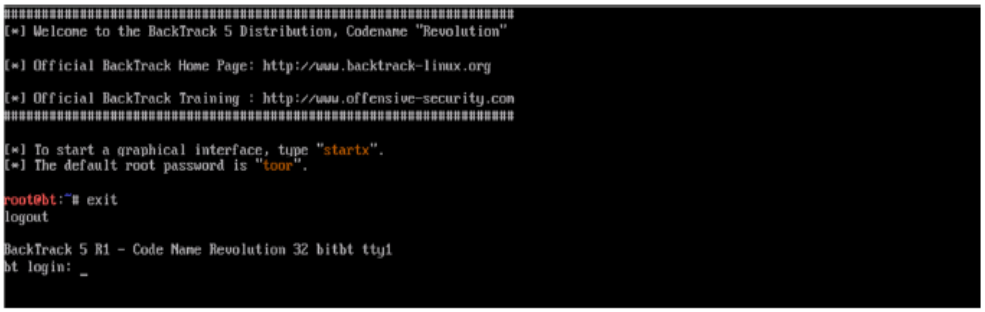
4. Escogemos la distribución de teclado correspondiente

Selección del teclado

5. Después de estos sencillos pasos, comenzara la instalación de BackTrack

Instalando BackTrack

6. Una vez que hemos instalado el S.O. el user por defecto es root y el password es toor



Ingreso a BackTrack

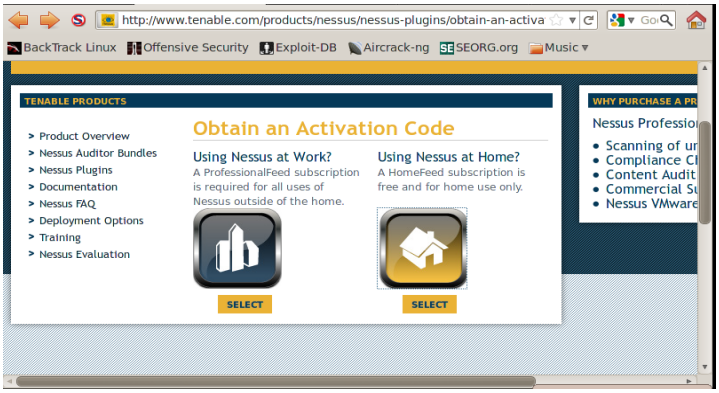
7. Para iniciar el modo grafico ingresamos el comando startx

Interfaz grafica de BackTrack

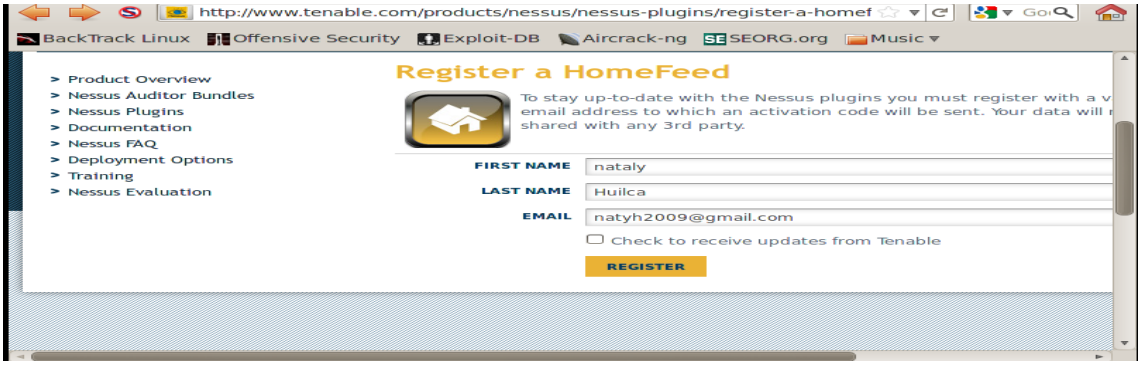
ANEXO 3. MANUAL DE INSTALACIÓN DE NESSUS EN BACKTRACK

Instalación de nessus5 en backtrac5

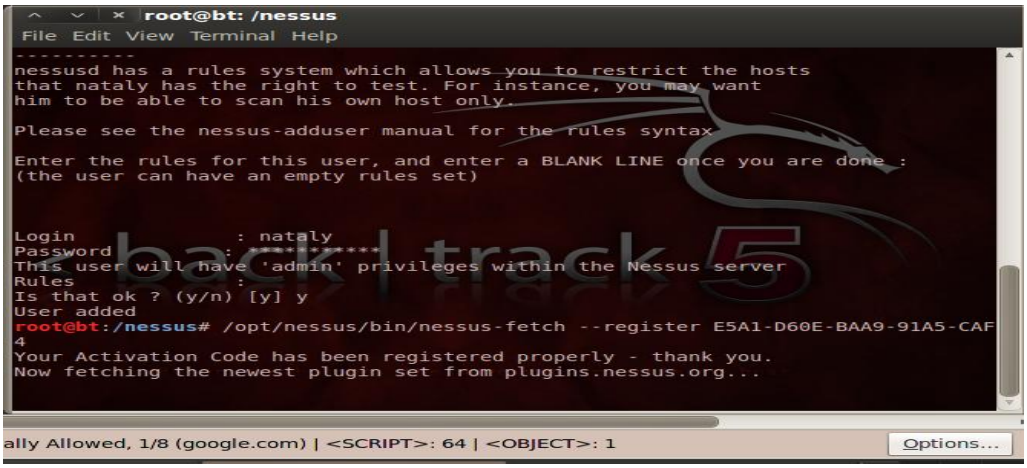
Obteniendo código de activación



Registrando para obtener clave.

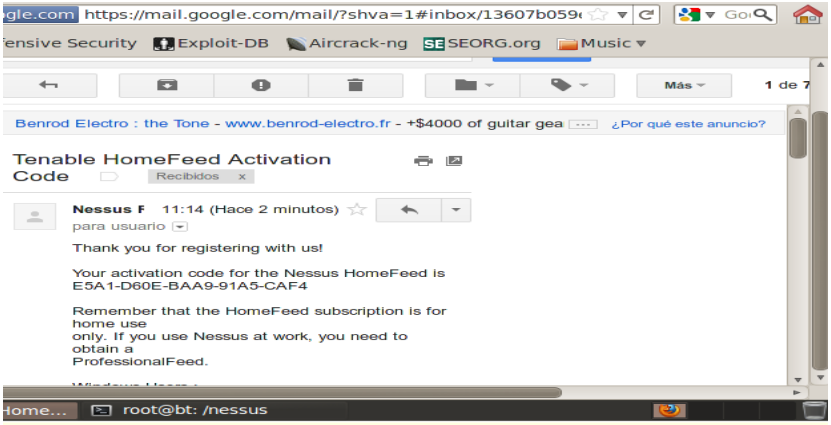


Activando plugins´

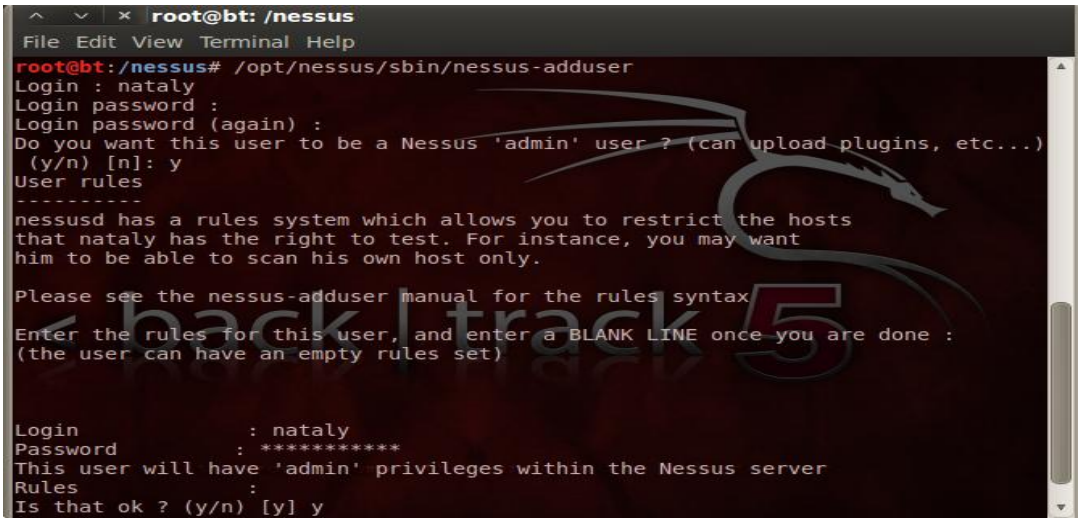


Primeramente creamos una carpeta llamada nessus en la cual vamos a instalar el paquete de nessus.

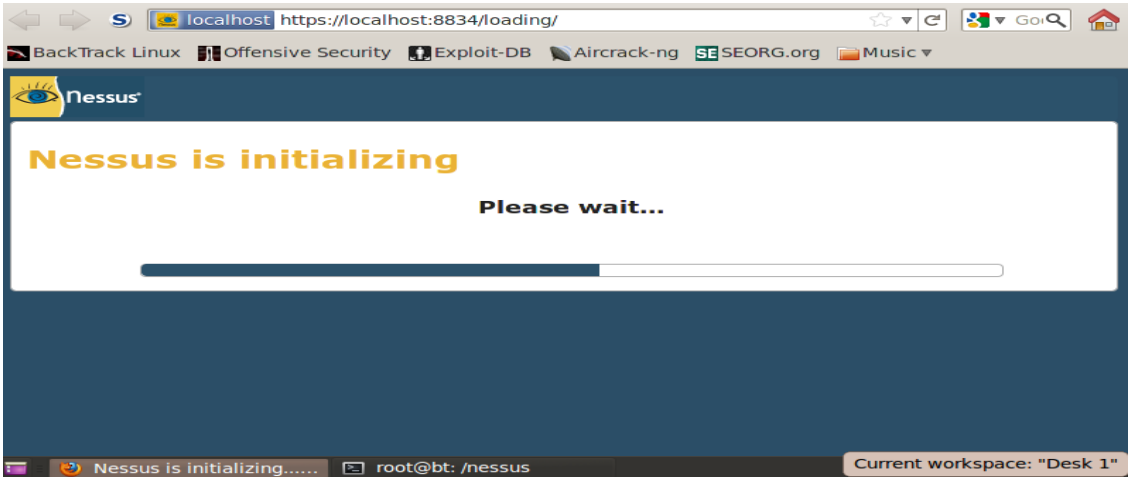
Activamos nesus con la clave previamente obtenida una vez que nos hayamos suscrito en nessus.



: Luego creamos el usuario y la contraseña



Iniciando nessus



ANEXO 4. INFORME TÉCNICO

Resumen Ejecutivo

Este documento detalla las pruebas de intrusión realizadas a la Intranet del Gobierno Autónomo Descentralizado Municipal del Cantón Cevallos.

Se realizó la ejecución de un proceso de hackeo ético, que reúne un conjunto de pruebas de intrusión simulando a un hacker interno y utilizando para ello todos los recursos y habilidades técnicos necesarios.

Durante el proceso se realizaron varias pruebas, que van desde la recolección de información crítica, escaneo de puertos, pruebas de intrusión para lograr accesos no autorizados, entre otras. Una vez concluidas las fases del hacking ético se logro evaluar y auditar la seguridad en la intranet utilizando herramientas y aplicaciones que ofrece el software libre, permitiendo de esta manera describir como resultado una lista de vulnerabilidades con sus respectivas amenazas y proponiendo para cada una de éstas algunas recomendaciones para reducir los riesgos potenciales causados por las vulnerabilidades encontradas y por tanto mejorar el nivel de seguridad de la intranet del Gobierno Autónomo Descentralizado Municipal del Cantón Cevallos.

Detalle de las pruebas realizadas.

Las pruebas fueron realizas en función a lo que especifica la metodología ISSAF y las fases de hackeo ético las cuales se presentan a continuación:

FOOTPRINTING

Se utilizó software para identificar las direcciones IP, los nombres de los servidores DNS dominios y equipos. Con esta información fue posible hacerse una idea del esquema existente en la red. En esta fase se utilizó ping, nsloockup, hping, dig y traceroute.

SCANNING

En esta fase se identificaron los equipos disponibles, sistemas operativos, y los puertos abiertos con su respectivo servicio en cada uno de los equipos, se escanearon

para este efecto las IP desde la 192.168.6.1 hasta la 192.168.6.254 con las herramientas Colasoft MAC Scanner, Angry IP Scanner, Nmap y Zenmap.

Se utilizo el comando nbtscan y la herramienta SoftPerfect Network Scanner para verificar si existen carpetas compartidas.

También se trato de ingresar por NetBIOS mediante el comando nbtstat.

BUSQUEDA DE VULNERABILIDADES

Para la detección automática de vulnerabilidades se contó con Nessus 5.0.

PENETRACIÓN, OBTENCIÓN DE ACCESO Y ESCALADO DE PRIVILEGIOS.

En esta fase se uso SQL Server 2008 Enterprise para lograr la conexión con la base de datos existente en el Municipio.

Para el Ataque al servicio de Microsoft Windows SMB del servidor de base de datos se utilizo el exploit ms08_067_netapi existente en el Metasploit de BackTrack.

Mediante Ettercap se logro realizar ataques Mit para escuchar todo lo que pasa por la puerta ethernet, con los cuales se pudo obtener passwords de cuentas de usuarios.

Además con Ettercap se efectuaron ataques de denegación de servicios.

En este paso se uso el archivo ejecutable D2.bat el cual está programado en Java, cuya función es realizar varias peticiones al servidor hasta provocar la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima.

Resultados de cada una de las pruebas realizadas.

Escaneo de toda la red con nmap.


root@bt:~# nmap -sP 192.168.6.1-255
Starting Nmap 5.59BETA1 (http://nmap.org) at 2012-03-08 15:50 ECT
Nmap scan report for 192.168.6.1
Host is up (0.00098s latency).
MAC Address: 00:1E:58:45:F9:AE (D-Link)
Nmap scan report for 192.168.6.7
Host is up (0.0013s latency).
MAC Address: 00:00:21:6E:4E:B2 (Sureman COMP. & Commun.)
Nmap scan report for 192.168.6.23
Host is up (0.0039s latency).
MAC Address: 00:19:66:8B:53:9B (Asiarock Technology Limited)
Nmap scan report for 192.168.6.26
Host is up (0.0034s latency).
MAC Address: 00:07:95:06:A0:3B (Elitegroup Computer System Co. (ECS))
Nmap scan report for 192.168.6.29
Host is up (0.0021s latency).
MAC Address: 00:1C:C0:FD:14:23 (Intel Corporate)
Nmap scan report for 192.168.6.30
Host is up (0.0018s latency).
MAC Address: 00:08:54:05:7F:20 (Netronix)
Nmap scan report for 192.168.6.32
Host is up (0.00090s latency).
MAC Address: 00:19:D1:2D:69:C9 (Intel)
Nmap scan report for 192.168.6.81
Host is up (0.00091s latency).
MAC Address: 00:1D:72:1C:99:C0 (Wistron)
Nmap scan report for 192.168.6.83
Host is up.
Nmap scan report for 192.168.6.93
Host is up (0.00068s latency).
MAC Address: 00:1C:C0:B8:3F:0A (Intel Corporate)
Nmap scan report for 192.168.6.100
Host is up (0.0016s latency).
MAC Address: 00:18:71:EB:B2:D6 (Hewlett Packard)
Nmap scan report for 192.168.6.104
Host is up (0.083s latency).
MAC Address: 00:1E:65:73:66:9A (Intel Corporate)
Nmap scan report for 192.168.6.105
Host is up (0.0015s latency).
MAC Address: 00:1C:C0:FD:14:36 (Intel Corporate)
Nmap scan report for 192.168.6.106
Host is up (0.0013s latency).
MAC Address: 00:16:EC:7B:DC:17 (Elitegroup Computer Systems Co.)
Nmap scan report for 192.168.6.107
Host is up (0.15s latency).
MAC Address: 00:16:E3:1F:FE:14 (Askey Computer)
Nmap scan report for 192.168.6.114
Host is up (0.00094s latency).
MAC Address: 00:1C:C0:FD:14:23 (Intel Corporate)
Nmap scan report for 192.168.6.116
Host is up (0.098s latency).
MAC Address: 70:F1:A1:FE:BD:14 (Liteon Technology)
Nmap scan report for 192.168.6.166
Host is up (0.0075s latency).
MAC Address: 00:08:A1:41:10:63 (CNet Technology)
Nmap scan report for 192.168.6.194
Host is up (0.00059s latency).
MAC Address: 00:1C:C0:62:BA:C2 (Intel Corporate)
Nmap scan report for 192.168.6.240
Host is up (0.0040s latency).
MAC Address: 00:4F:62:2B:39:A7 (Unknown)
Nmap scan report for 192.168.6.253
Host is up (0.0023s latency).
MAC Address: 00:16:76:D2:E4:95 (Intel)
Nmap scan report for 192.168.6.254
Host is up (0.0023s latency).
MAC Address: 00:20:A6:6F:FC:D1 (Proxim Wireless)
Nmap done: 255 IP addresses (32 hosts up) scanned in 66.65 seconds
root@bt:~#

Resumen del escaneo de puertos y servicios servidor de Internet.

Dirección IP	**Sistema operativo**	**Puertos abiertos**	**Servicios por puerto**	**Sistemas**
192.168.6.1	NO DETECTADO	22	ssh	OpenSSH 4.3
		80	http	Apache httpd 2.2.3
		111	rpcbind	
		443	https	
		5900	vnc	VNC(protocol 3.7)
		8080	http-proxy	Squid webproxy
		111111	vce	

Resumen del escaneo de puertos y servicios servidor de Base de Datos.

Dirección IP	**Sistema operativo**	**Puertos abiertos**	**Servicios por puerto**	**Sistemas**
192.168.6.100	Microsoft windows server service pack 2	80	http	Apache httpd 2.2.11
		135	msrpc	Microsoft Windows RPC

	139	Netbios-ssn	
	443	https	Apache httpd 2.2.11
	445	Microsoft-ds	Microsoft Windows 2003 o 2008
	1025	msrpc	Microsoft Windows RPC
	1433	Ms-sql-s	Microsoft SQL server 2000
	3306	mysql	MySQL(Unauthorized)
	3389	Microsoft - rdp	Microsoft terminar Service
	14000	Scotty-ft	

Carpetas compartidas de toda la red.

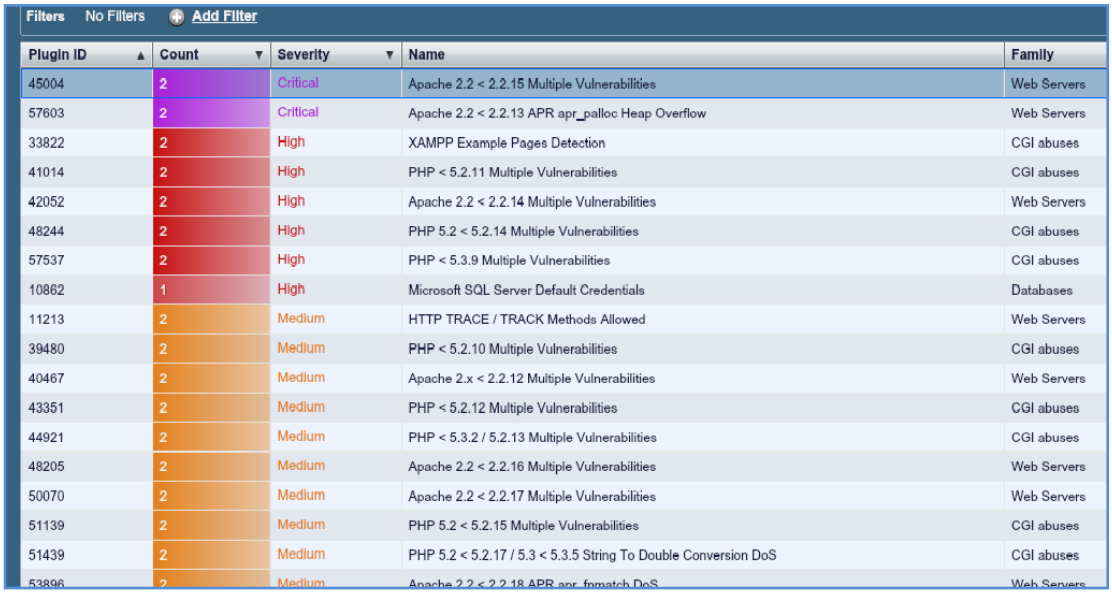
```
File  Edit  View  Terminal  Help
------------------------------------------------------------------------------
root@bt:/# nbtscan 192.168.6.0/24
Doing NBT name scan for addresses from 192.168.6.0/24

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
192.168.6.0     Sendto failed: Permission denied
192.168.6.43     DESKTOP          <server>  <unknown>        00-d0-09-9e-e6-ca
192.168.6.21     TESORERIA        <server>  <unknown>        00-e0-4d-4d-30-c5
192.168.6.29     ASIS_OOPP        <server>  <unknown>        00-19-d1-ee-e1-53
192.168.6.27     ASIS_PLANIF      <server>  <unknown>        00-19-66-8b-53-9b
192.168.6.19     CAJA1            <server>  CAJA1            00-08-54-05-7f-97
192.168.6.22     AVALUOS          <server>  <unknown>        00-1c-c0-fd-14-23
192.168.6.7      SECRETARIA2      <server>  <unknown>        00-00-21-6e-4e-b2
192.168.6.25     UNAPAC           <server>  <unknown>        00-08-54-05-7f-20
192.168.6.70     CAJA2            <server>  <unknown>        00-08-a1-41-10-63
192.168.6.28     JEFE_OOPP        <server>  <unknown>        00-19-d1-2d-69-c9
192.168.6.17     SISTEMAS         <server>  <unknown>        00-1c-c0-fd-14-36
192.168.6.24     GUARDALMACEN     <server>  <unknown>        00-1c-c0-b8-3f-0a
192.168.6.41     INTEL-PC         <server>  <unknown>        e0-69-95-57-4e-a1
192.168.6.84     CONTABILIDAD     <server>  <unknown>        00-1c-c0-97-48-65
192.168.6.100    USUARIO          <server>  <unknown>        00-18-71-eb-b2-d6
root@bt:/#
```

Documentos compartidos de una estación de trabajo.

Documento obtenido de entre las carpetas compartidas

PREDIAL RUSTICO	G. A. D. MUNICIPAL DEL CANTON CEVALLOS				RECIBO PROVISIONAL	
POR AÑO 2012	DEPARTAMENTO FINANCIERO				Nº Tit.:	
Ident. Predial:				Parroquia:		
Contribuyente:				Nombre del predio:		
Avalúo Terreno:	4.395,15		------- RUBROS -------		--- VALORES ---	
Avalúo Construcciones:	0,00					
Otras Inversiones:	0,00		Imp. Predial Rústico:.....		2,42	
Avalúo Propiedad:	4.395,15					
Exenciones y rebajas:	0,00		Bomberos.....		0,00	
Base Imponible:	4.395,15					
			Servicios administrativos.....		0,00	
0						
día/mes/año			VALOR EMITIDO.....	$.	2,42	
EMISION			DESCUENTO.....	$.	0,00	
			RECARGOS .....$.		0,00	
			INTERESES .....$.		0,00	
16/04/2012						
día/mes/año			TOTAL A PAGAR .....$.		2,42	
RECAUDACION						
	JEFE DE RENTAS	TESORERO				

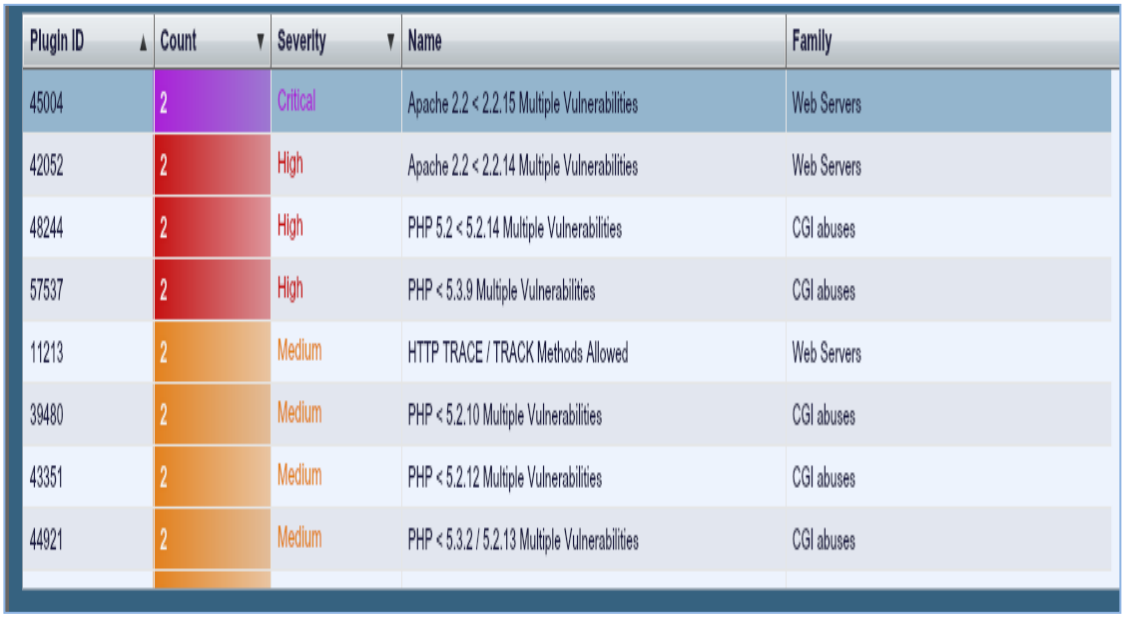
Vulnerabilidades encontradas con nessus en el servidor de Base de Datos



Filters No Filters Add Filter

Plugin ID	Count	Severity	Name	Family
45004	2	Critical	Apache 2.2 < 2.2.15 Multiple Vulnerabilities	Web Servers
57603	2	Critical	Apache 2.2 < 2.2.13 APR apr_palloc Heap Overflow	Web Servers
33822	2	High	XAMPP Example Pages Detection	CGI abuses
41014	2	High	PHP < 5.2.11 Multiple Vulnerabilities	CGI abuses
42052	2	High	Apache 2.2 < 2.2.14 Multiple Vulnerabilities	Web Servers
48244	2	High	PHP 5.2 < 5.2.14 Multiple Vulnerabilities	CGI abuses
57537	2	High	PHP < 5.3.9 Multiple Vulnerabilities	CGI abuses
10862	1	High	Microsoft SQL Server Default Credentials	Databases
11213	2	Medium	HTTP TRACE / TRACK Methods Allowed	Web Servers
39480	2	Medium	PHP < 5.2.10 Multiple Vulnerabilities	CGI abuses
40467	2	Medium	Apache 2.x < 2.2.12 Multiple Vulnerabilities	Web Servers
43351	2	Medium	PHP < 5.2.12 Multiple Vulnerabilities	CGI abuses
44921	2	Medium	PHP < 5.3.2 / 5.2.13 Multiple Vulnerabilities	CGI abuses
48205	2	Medium	Apache 2.2 < 2.2.16 Multiple Vulnerabilities	Web Servers
50070	2	Medium	Apache 2.2 < 2.2.17 Multiple Vulnerabilities	Web Servers
51139	2	Medium	PHP 5.2 < 5.2.15 Multiple Vulnerabilities	CGI abuses
51439	2	Medium	PHP 5.2 < 5.2.17 / 5.3 < 5.3.5 String To Double Conversion DoS	CGI abuses
53896	2	Medium	Apache 2.2 < 2.2.18 APR apr_fnmatch DoS	Web Servers

Vulnerabilidades encontradas con nessus en el servidor de Internet.



Plugin ID	Count	Severity	Name	Family
45004	2	Critical	Apache 2.2 < 2.2.15 Multiple Vulnerabilities	Web Servers
42052	2	High	Apache 2.2 < 2.2.14 Multiple Vulnerabilities	Web Servers
48244	2	High	PHP 5.2 < 5.2.14 Multiple Vulnerabilities	CGI abuses
57537	2	High	PHP < 5.3.9 Multiple Vulnerabilities	CGI abuses
11213	2	Medium	HTTP TRACE / TRACK Methods Allowed	Web Servers
39480	2	Medium	PHP < 5.2.10 Multiple Vulnerabilities	CGI abuses
43351	2	Medium	PHP < 5.2.12 Multiple Vulnerabilities	CGI abuses
44921	2	Medium	PHP < 5.3.2 / 5.2.13 Multiple Vulnerabilities	CGI abuses

Resumen de vulnerabilidades encontradas en el servidor de Base de Datos

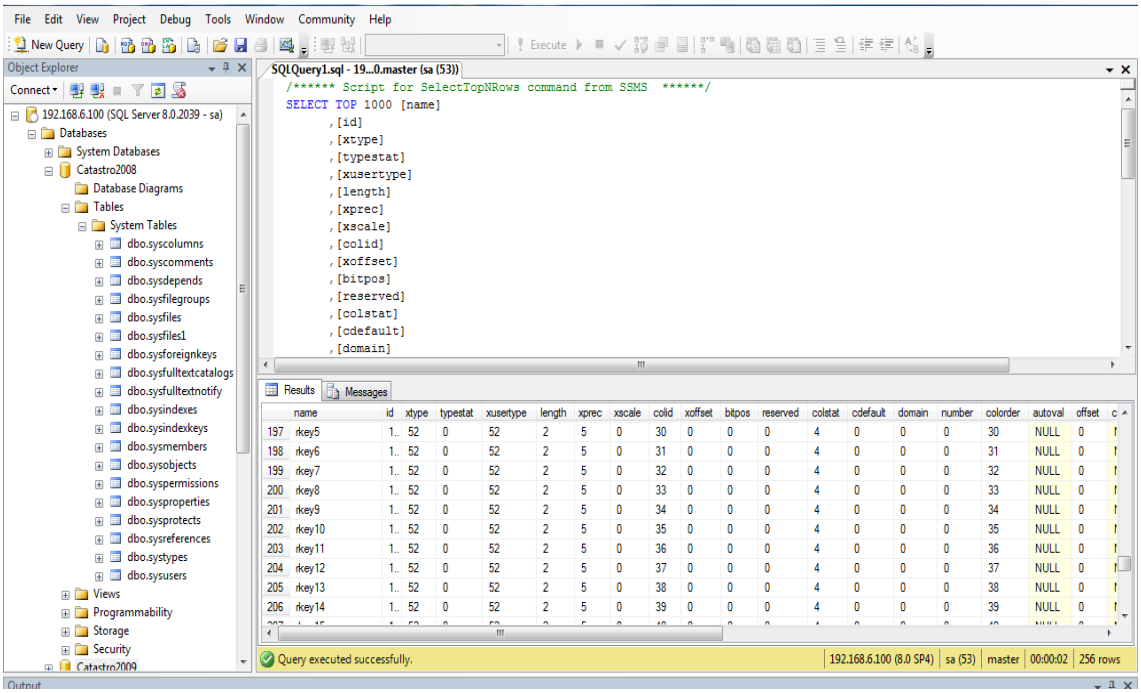
Nivel de Vulnerabilidad	**contenido**	**Problema**
Alta	Microsoft SQL Server credenciales predeterminadas	Las credenciales para el servidor de base de datos remota pueden ser descubiertas**.**
medio	Microsoft Windows Server Man-in-the-Middle	Tal vez sea posible realizar ataques de hombre en el medio (MIT).
medio	SSL Versión 2 (v2) Protocolo	El servicio remoto acepte conexiones cifradas con SSL 2.0, que al parecer sufre de mostrar distintas defectos y ha quedado en desuso desde hace varios años. Un atacante puede ser capaz de explotar estas cuestiones para llevar a cabo man-in- the-middle el medio de ataque o descifrar las comunicaciones

		entre el servicio y los clientes afectados
Critica	PHP 5.2 < 5.2.17 / 5.3 < 5.3.5 DoS	El servidor web remoto utiliza una versión de PHP que se ve afectado por una vulnerabilidad de denegación de servicio.

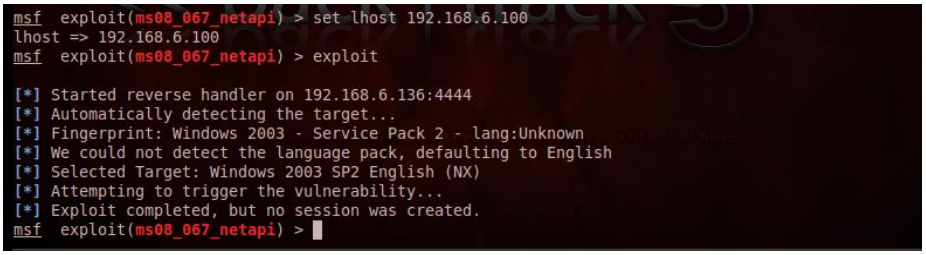
Resumen de vulnerabilidades encontradas en el servidor de Internet

Nivel de Vulnerabilidad	**contenido**	**Problema**
Alta	Apache HTTP Server	La versión de Apache HTTP Server no se encuentra actualizada.
Alta	Apache HTTP Server DOS	La versión de Apache HTTP que se ve afectado por una vulnerabilidad de denegación de servicio.
Alta	Apache HTTP Server man-in-the-middle	La versión de Apache HTTP que se ve afectado por una vulnerabilidad de posibles ataque man-in- the-middle.

Ingreso a las bases de datos con SQL Server 2008

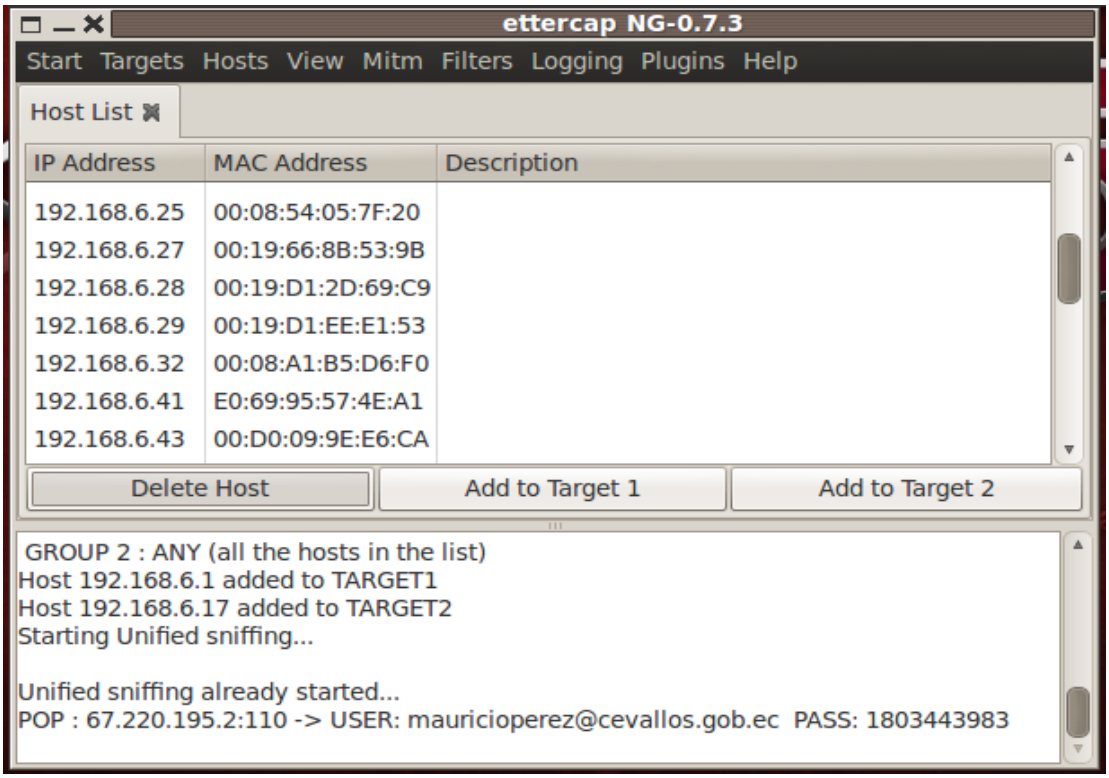


Resultado del Ataque al servicio de Microsoft Windows SMB
Envió exploit Microsoft ms08_067_netapi



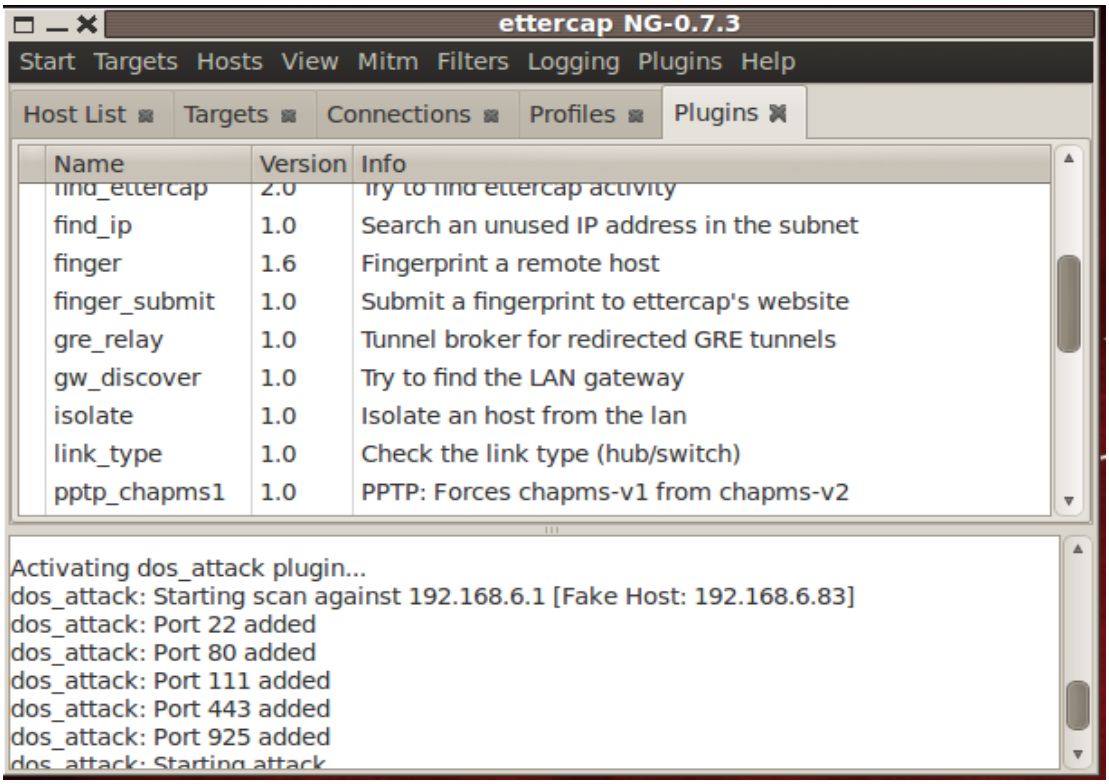
Ataque MIT

Ejecución del Ataque MIT mediante la obtención del password de un correo electrónico con ettercap



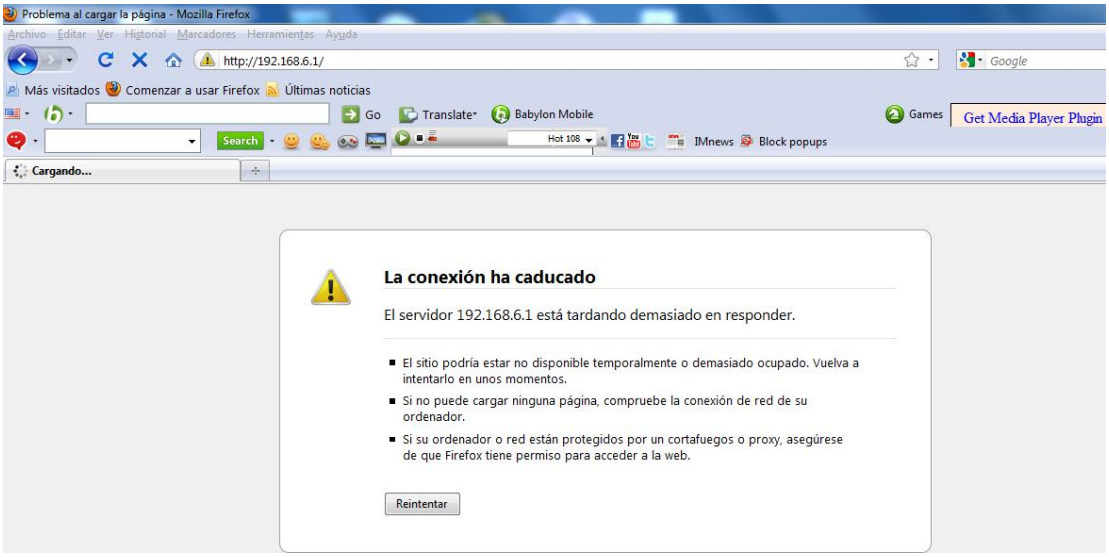
Ataque DOS

Ejecución ataque de Denegación de servicios al servicio de internet se ataco por el puerto 22, 80, 111, 443, 925.

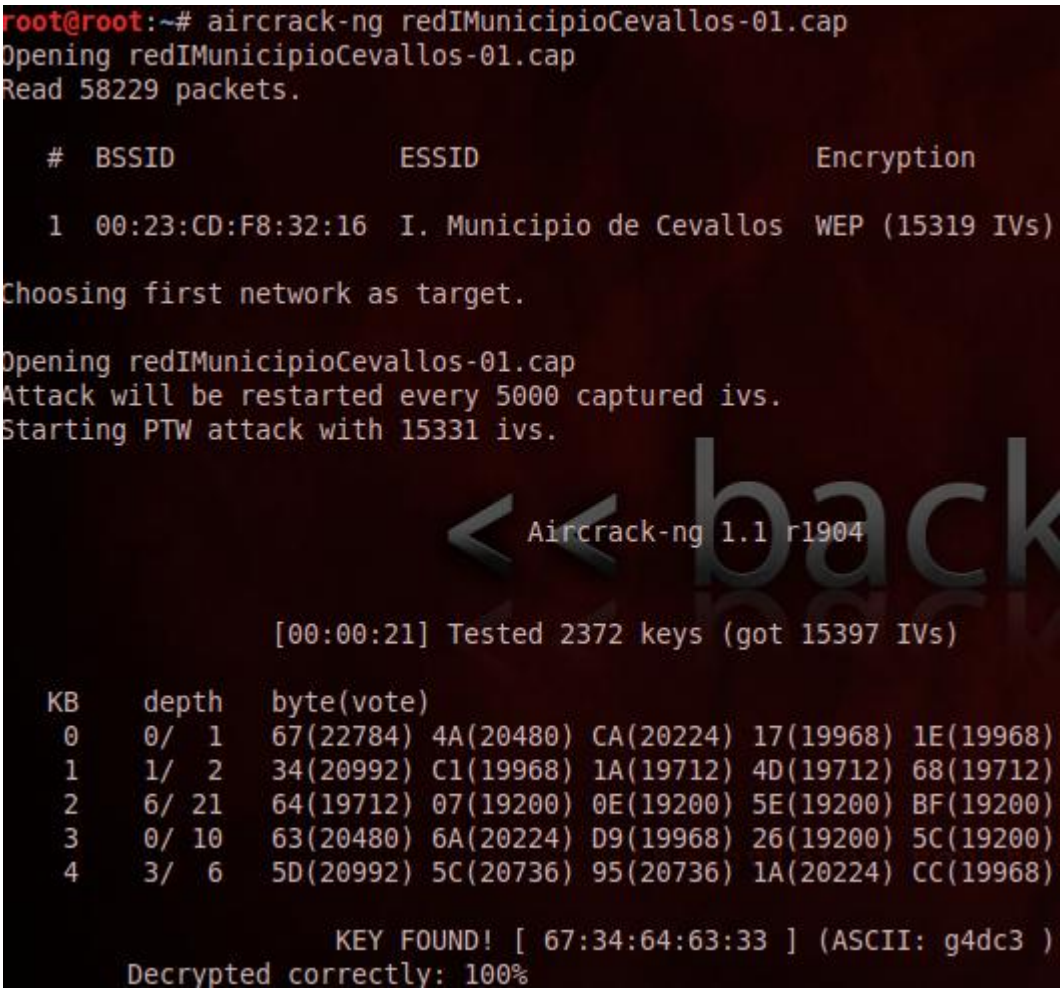


Ataque Apache

Una vez ejecutado el archivo ejecutable D2.bat aparece la siguiente pantalla en la cual ya no es posible ingresar a Apache.



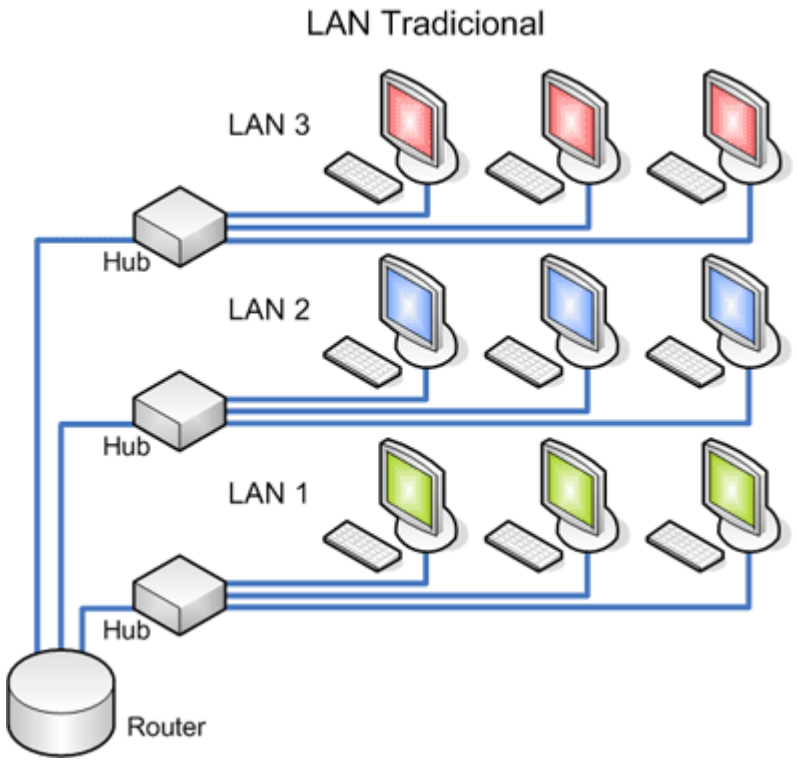
Hackeo de la contraseña de la red inalámbrica obtención de la contraseña.

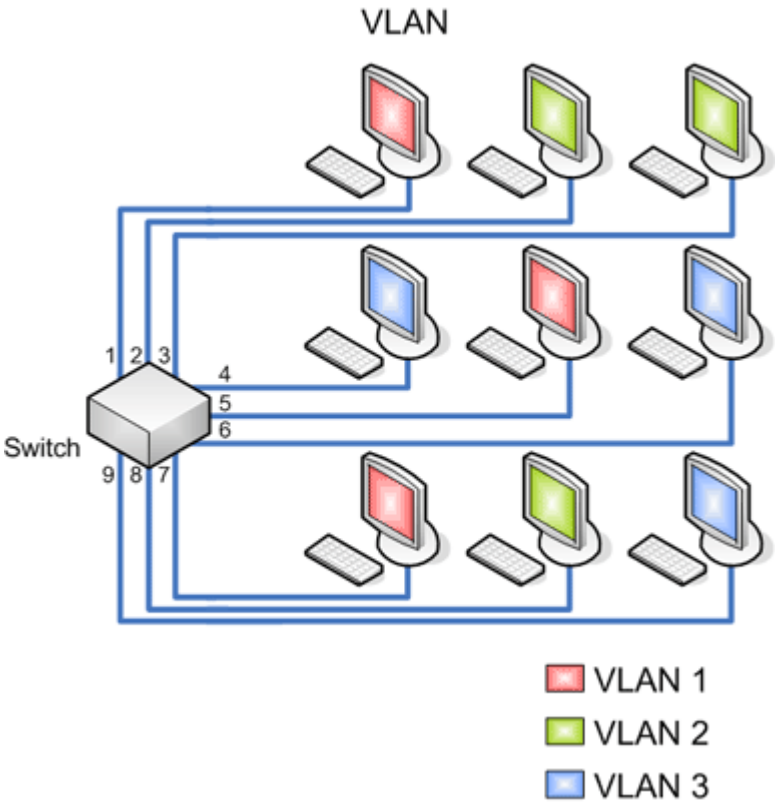


Luego de haber presentado los resultados es importante mencionar que la estructura en cuanto al diseño de la Red LAN necesita ser reestructurada para evitar uno de los problemas que actualmente sufre el Gobierno autónomo Descentralizado Municipal del cantón Cevallos como es el de una confidencialidad entre usuarios de la LAN como pueden ser los directivos de la misma, también estando todas las estaciones de trabajo en un mismo dominio de colisión el ancho de banda de la misma no era aprovechado correctamente.

Es por esto que se recomienda la creación de VLANs utilizando Switches, de esta manera que esto permita un control más inteligente del tráfico de la red, ya que este dispositivo trabaja a nivel de la capa 2 del modelo OSI y es capaz de aislar el tráfico,

logrando así que la eficiencia en la red entera se incremente. Por otro lado, al distribuir a los usuarios de un mismo grupo lógico a través de diferentes segmentos, se logra el incremento del ancho de banda en dicho grupo de usuarios. Así:





Lista de todas las vulnerabilidades detectadas, junto con las recomendaciones para resolverlas.

Niveles de severidad de las vulnerabilidades

Alta: son las vulnerabilidades que representan un peligro y que deben ser corregidas lo más pronto posible.

Baja: es considerada una vulnerabilidad baja cuando no permite obtener información valiosa de por si.

Media: es aquella que no es baja ni alta pero que también requiere corregir las fallas detectadas.

1.-Microsoft SQL Server

Nivel de severidad: Alta

Vulnerabilidad: Las credenciales para el servidor de base de datos remota pueden ser descubiertas.

Configuraciones predeterminadas: Las configuraciones por defecto, tanto en los sistemas operativos, las aplicaciones y los dispositivos implementados en el ambiente informático, conforman una de las debilidades que comúnmente son poco atendidas por pensar erróneamente que se tratan de factores triviales que no se encuentran presentes en la lista de los atacantes.

Sin embargo, las configuraciones predeterminadas hacen del ataque una tarea sencilla para quien lo ejecuta ya que es muy común que las vulnerabilidades de un equipo sean explotadas a través de la utilización de usuarios y contraseñas por defecto las cuales se basan en que el objetivo se encuentra configurado con los parámetros por defecto.

Recomendaciones:

Sobre la base de lo anteriormente explicado, se pueden sugerir algunas recomendaciones para fortalecer este aspecto de la seguridad, es posible:

Cambiar los valores por defecto: para esto se deben verificar aspectos como las opciones que se configuran de manera predeterminada al instalar sistemas operativos, gestores de bases de datos y demás recursos, como los nombres de rutas, nombres de carpetas, componentes, servicios, configuraciones y otros ajustes necesarios, o innecesarios, que brinden un adecuado nivel de protección.

"Nada hace que atacar un objetivo dentro de una red sea tan fácil como cuando los objetivos se encuentran con los valores por defecto establecidos por el fabricante del dispositivo."

Implementar mecanismos de autenticación más robustos: Se podría implementar como "autenticación fuerte de doble factor", donde no sólo se necesita contar con la contraseña sino que también es necesario contar con algo que se tiene, como por ejemplo una llave electrónica USB o una tarjeta que almacene certificados digitales para que a través de ellos se pueda validar o no el acceso de los usuarios a los recursos de la organización.

“De nada sirve utilizar contraseñas fuertes si luego son olvidadas o compartidas, ya que con ello se compromete la seguridad de todo el mecanismo de autenticación.”

Muchas aplicaciones automatizadas están diseñadas para aprovechar estas vulnerabilidades teniendo en cuenta las configuraciones predeterminadas, incluso, existen sitios web que almacenan bases de datos con información relacionada a los nombres de usuario y sus contraseñas asociadas, códigos de acceso, configuraciones, entre otras, de los valores por defecto de sistemas operativos, aplicaciones y dispositivos físicos. Sólo basta con escribir en un buscador las palabras claves “default passwords” (contraseña por defecto) para ver la infinidad de recursos disponibles que ofrecen este tipo de información.

Normas de Elección de Claves

No utilizar contraseñas que sean palabras.

No usar contraseñas completamente numéricas con algún significado (teléfono, D.N.I., fecha de nacimiento, patente del automóvil, etc.).

No utilizar terminología técnica conocida.

Elegir una contraseña que mezcle caracteres alfabéticos (mayúsculas y minúsculas) y numéricos.

Deben ser largas, de 8 caracteres o más.

Tener contraseñas diferentes en máquinas diferentes y sistemas diferentes.

Deben ser fáciles de recordar para no verse obligado a escribirlas

Combinar palabras cortas con algún número o carácter de puntuación.

No permitir ninguna cuenta sin contraseña. Si se es administrador del sistema, repasar este hecho periódicamente (auditoría).

Nunca compartir con nadie la contraseña.

No teclear la contraseña si hay alguien.

2.-Inseguridad Inalámbrica

Nivel de severidad: Alta

Vulnerabilidad: la contraseña de ingreso inalámbrico puede ser descifrada.

Seguridad Inalámbrica

La seguridad en las redes inalámbricas es sumamente importante, por la facilidad con que cualquiera puede encontrarlas y acceder a ellas, cualquier persona con una computadora portátil puede encontrar fácilmente el punto de acceso inalámbrico de una red inalámbrica y así ingresar en archivos, utilizar las conexión a internet, obtener datos importantes que se transfieran en la red inalámbrica, introducir virus o software maligno etc.

Es por este motivo q hay que configurar bien un punto de acceso ya que un punto de acceso inalámbrico mal configurado se convierte en una puerta trasera que vulnera por completo la seguridad informática de la institución.

Recomendaciones:

Usar autentificación 802.1x basada en EAP para redes inalámbricas: Se trata de un mecanismo de seguridad diseñado para proporcionar acceso controlado entre dispositivos inalámbricos clientes, puntos de acceso y servidores.

Con esto se lograra minimizar los riesgos asociados al acceso indebido en redes inalámbricas. Entre las principales recomendaciones de este tipo se encuentran:

Evitar la difusión del identificador de red o SSID

Establecer listas de control de acceso por direcciones físicas o de MAC

(Media Access Control) de los dispositivos que acceden a la red.

Utilizar cifrado en las conexiones inalámbricas.

Segmentar los puntos de acceso inalámbricos en zonas de seguridad administradas por un firewall.

Establecer redes privadas virtuales o VPNs en las conexiones inalámbricas.

Combinar mecanismo de autenticación a la red y cifrado de datos

Ventajas

Costos asociados: con la utilización de servidores de autenticación (RADIUS, IAS) que ya existen en las organizaciones y no se requiere actualizaciones firmware o compatibilidad con WPA en los dispositivos inalámbricos utilizados.

Adaptabilidad: a los cambios o crecimientos de las infraestructuras tecnológicas y también se pueden utilizar modelos de autenticación distribuidos para organizaciones con varias sedes o varias redes LAN.

Nivel de Seguridad alto: Se trata de un esquema de autenticación de seguridad elevado porque puede emplear certificados de cliente o nombres de usuarios y contraseñas

Autenticación de usuarios y de equipos: Permite la autenticación por separado de usuario y de equipo. La autenticación por separado de un equipo permite administrarlo incluso cuando ningún usuario ha iniciado la sesión.

Transparencia: proporciona una autenticación y una conexión a la WLAN transparentes.

Interoperabilidad: Aunque 802.1x disfruta de una aceptación casi universal, el uso de distintos métodos de EAP implica que la interoperabilidad no siempre está garantizada.

Cifrado más seguro: permite un cifrado muy seguro de los datos de la red.

Bajo coste: bajo coste del hardware de red.

Alto rendimiento: dado que el cifrado se lleva a cabo en el hardware de

WLAN y no en la CPU del equipo cliente, el cifrado de WLAN no influirá en el nivel de rendimiento del equipo cliente.

Disponibilidad: Por ser compleja la configuración en lo que respecta a la seguridad de WLAN, muchas de las empresas no disponen del estándar 802.1x.

Portal cautivo para redes inalámbricas públicas

Implementar un portal cautivo: esto para vigilar el tráfico http y hacer que los usuarios primero pasen por una página inicial la cual requiere una autenticación especial si requieren salida a internet. Aunque realmente depende de los criterios de

la seguridad que se necesiten implementar, en ocasiones se puede dejar sin autenticación únicamente mostrando las normal de uso y la duración de la navegación.

Software

Chillispot

MikroTik Hotspot

Requisitos previos

Para el montaje del Captive Portal (Portal Cautivo) necesitaremos:

- Un ordenador donde instalar el portal cautivo con 2 tarjetas de red
- Un Wireless Access Point (Punto de acceso WiFi)
- Cables de red
- Acceso a Internet
- Nociones medias de Linux
- CD de instalación de EasyHotSpot

3.-Microsoft Windows Server Man-in-the-Middle

Nivel de severidad: Alta

Vulnerabilidad Tal vez sea posible realizar ataques de hombre en el medio (MIT).

Este tipo de ataques son perjudiciales en cuanto a la confidencialidad de claves se refiere ya que se pueden lograr capturar password de correos electrónicos, ingresos a sistemas, claves gubernamentales, etc.

Recomendaciones:

Implementación de Vlans en un Switch capa 3 de Cisco gama media-alta, los cuales presentan un auto configuración de snooping, técnica que permite evitar los ataques MITM.

Una de las maneras para prevenir el ARP Spoofing de manera manual, es el uso de: Tablas de caché ARP de forma estáticas, este protocolo utiliza para supervisar y modificar la tabla de asignaciones de direcciones IP y direcciones MAC las cuales son manipuladas manualmente de forma que no existe caché dinámica, cada entrada de la tabla mapea una dirección MAC con su correspondiente dirección IP.

Obtención de certificados EV SSL: estos certificados ayudaran a establecer un canal seguro entre dos partes proporcionando autenticación, integridad y confidencialidad. Los Certificados EV SSL confirman en forma definitiva la identidad de la organización que posee el sitio web prestando atención cuando falta el brillo o color verde Los criminales informáticos no tienen acceso a los Certificados EV SSL de los sitios que falsifican y, por lo tanto, no pueden imitar el color verde que muestra que un sitio web autenticado es seguro.

Los objetivos del protocolo SSL son, en orden de prioridad:

Seguridad Criptográfica. Debe ser usado para establecer una conexión segura entre dos partes.

Interoperabilidad. Programadores independientes deben poder desarrollar aplicaciones que, utilizando SSL, permitan intercambiar en forma exitosa parámetros de cifrado sin tener conocimiento del código utilizado por el otro.

Flexibilidad. Debe ser una base sobre la cual puedan incorporarse nuevos métodos de cifrado. Esto trae aparejado dos objetivos más: evitar la creación de un protocolo nuevo y la implementación de una nueva biblioteca de seguridad

Eficiencia. Dado que las operaciones de cifrado consumen gran cantidad de recursos, en especial CPU, incorpora ciertas facilidades que permiten mejorar este aspecto, además de mejorar el uso de la red.

4.-PHP 5.2 < 5.2.17 / 5.3 < 5.3.5 DoS

Nivel de severidad: media

Vulnerabilidad: El servidor web remoto utiliza una versión de PHP que se ve afectado por una vulnerabilidad de denegación de servicio.

Recomendaciones:

Implementación de un cortafuego: con esto se lograra realizar restricciones de accesos a la red s podrá permitir o denegar el tráfico a usuarios durante el acceso al servidor SSH.

Características habituales

Manejar y controlar el tráfico en la red.

Autenticar accesos.

Oculta la estructura interna.

Actuar como intermediario.

Proteger los recursos.

Registrar y almacenar información sobre eventos.

5.-Apache HTTP server DOS

Nivel de severidad: critica

Vulnerabilidad: La versión de Apache HTTP que se ve afectado por una vulnerabilidad de denegación de servicio

Creación de Iptables: en todas las distribuciones de Linux actuales existen una herramienta de cortafuegos que permite no solamente filtrar paquetes, sino también realizar traducción de direcciones de red (NAT) para IPv4 o mantener registros de log.

Con esto se lograra tener un control total de todas las maquinas existentes en la red de las cuales se registra su dirección IP Y MAC para de esta manera permitir o denegar acciones coma la conexión a internet y accesos a diferentes estaciones de trabajo.

6.-Nivel de severidad: Alta

Vulnerabilidad: Archivos compartidos en la red

Los archivos compartidos en la red constituyen una peligrosidad ya que se pueden modificar o eliminar la información.

Recomendaciones

No compartí archivos sin la utilización de contraseñas.