DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERIA DE SISTEMAS

TRABAJO DE TITULACIÓN, PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO DE SISTEMAS

TEMA: ANÁLISIS Y DIAGNÓSTICO DE VULNERABILIDADES INFORMÁTICAS EN LA RED DE DATOS DE LA EMPRESA YOUPHONE CIA. LTDA. UTILIZANDO HACKING ÉTICO

AUTOR: SANTOS CASTAÑEDA, DANIELA MERECEDES

DIRECTOR: RON EGAS, MARIO BERNABE

SANGOLQUI

2016

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

CERTIFICACIÓN

Certifico que el trabajo de titulación **"ANÁLISIS Y DIAGNÓSTICO DE VULNERABILIDADES INFORMÁTICAS EN LA RED DE DATOS DE LA EMPRESA YOUPHONE CIA. LTDA. UTILIZANDO HACKING ÉTICO"** realizado por la señorita DANIELA MERCEDES SANTOS, ha sido revisado en su totalidad y analizado por el software anti-plagio, cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de las Fuerzas Armadas ESPE, por lo tanto me permito acreditarlo y autorizar a la señorita DANIELA MERCEDES SANTOS para que lo sustente públicamente.

Sangolquí, 23 Agosto 2016

Ing. Mario B. Ron Egas MSc.

DIRECTOR

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

AUTORIA DE RESPONSABILIDAD

Yo, **DANIELA MERCEDES SANTOS CASTAÑEDA,** con cédula de identidad N. 1714110341, declaro que este trabajo de titulación **"ANÁLISIS Y DIAGNÓSTICO DE VULNERABILIDADES INFORMÁTICAS EN LA RED DE DATOS DE LA EMPRESA YOUPHONE CIA. LTDA. UTILIZANDO HACKING ÉTICO"** ha sido desarrollado considerando los métodos de investigación existentes, así como también se ha respetado los derechos intelectuales de terceros considerándose en las citas bibliográficas.

Consecuentemente declaro que este trabajo es de mi autoría, en virtud de ellos me declaro responsable del contenido, veracidad y alcance de la investigación mencionada.

Sangolquí 23 de agosto de 2016

Daniela Mercedes Santos Castañeda

C.C 1714110341

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

AUTORIZACIÓN

Yo, **DANIELA MERCEDES SANTOS CASTAÑEDA,** autorizo a la Universidad de las Fuerzas Armadas ESPE publicar en la biblioteca virtual de la institución el presente trabajo de titulación **"Análisis y diagnóstico de vulnerabilidades informáticas en la red de datos de la empresa YOUPHONE CIA. LTDA utilizando hacking ético"** cuyo contenido, ideas y criterios son de mi autoría y responsabilidad.

Sangolquí 23 de agosto de 2016

Daniela Mercedes Santos Castañeda

C.C 1714110341

DEDICATORIA

A Dios por brindarme salud y vida.

A mi padre por ser siempre mi gran apoyo y mi ejemplo a seguir.

A mi madre por su entrega y dedicación.

A mis hermanos por las risas y el compañerismo

A mi esposo, por su apoyo incondicional y por motivarme a culminar este proyecto.

Dany

AGRADECIMIENTOS

A la Universidad de las Fuerzas Armadas, por ser parte de esta gran institución.

A mi director de Tesis Ing. Mario Ron por brindarme sus conocimientos durante el desarrollo de este proyecto de Titulación

Dany

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

El presente trabajo tuvo como objetivo principal realizar el Análisis y Diagnóstico de vulnerabilidades informáticas en la red de datos de la empresa “Youphone CIA LTDA”, a través de técnicas, herramientas y procedimientos de “hacking ético”, para emitir recomendaciones que minimicen los riesgos asociados. Youphone es una empresa distribuidora de Telefónica que se dedica a la venta y comercialización de equipos celulares y planes telefónicos. Esta empresa se veía afectada por la lentitud de sus transacciones, suspensión de su servicio en horas pico y robo de información por lo cual se realizó este proyecto basado en el modelo de “Hacking Ético” bajo la metodología OSSTMM (Open Source Security Testing Methodology Manual) utilizando listas de Comprobación o “CheckList”. Las herramientas que se utilizaron fueron de software libre y bajo licencia, dentro de las herramientas gratuitas se utilizó Wireshark, Advanced Port Scanner, Angry IP Scanner entre otros y dentro de las herramientas pagadas se utilizaron aquellas que permitían su uso dentro de un tiempo limitado tales como Nessus y VisualRoute. Los resultados obtenidos permitieron encontrar fallas de seguridad, centradas básicamente en puertos abiertos, por lo que se realizó un plan de Optimización y priorización del tráfico de red y un Informe Ejecutivo en dónde se detallan recomendaciones y procedimientos a realizar para proteger a la organización de ataques informáticos futuros.

Palabras Clave:

- **CHECKLIST**
- **BRECHAS DE SEGURIDAD**
- **POLÍTICAS DE SEGURIDAD**
- **HACKING ÉTICO**

ABSTRACT

The present research has the main objective of the Analysis and Diagnostic of networking vulnerabilities of Youphone CIA. Among techniques, tools and procedures of ethical hacking in order to issue recommendations that will minimize the associated risk. Youphone is a retailer of Telefónica which is dedicated to sells cell phones and mobile plans. This enterprise is affected by the long waiting for transactions, suspension of service during peak hours and stolen information. Due to these facts this project was based on the Ethical Hacking Model under OSSTMM methodology (open source security Testing Methodology Manual) using CheckLists.The tools used during this project were free software and under license. Among the free tools can be mentioned Wireshark, Advanced Port Scanner, AngryIPScanner, etc On the other hand; the licensed tools used were those that allow in a limited time such as Nessus and VisualRoute. The final results allowed us to find security fails basically centered on open ports. Based on this, an optimization and prioritization of network traffic plan and Executive inform were issued in which procedures and recommendations were detailed in order to protect the company from future informatics attacks.

KeyWords:

- **ETHICAL HACKING**
- **OSSTMM**
- **CHECKLIST**
- **SECURITY'S HOLES**
- **OPTIMIZATION AND PRIORITIZATION PLAN**

CAPÍTULO 1. INTRODUCCIÓN

Actualmente no existe una sola empresa que no utilice tecnologías de información y comunicaciones (TIC), las mismas que permiten transmitir, procesar, gestionar y almacenar información. Lo más valioso que posee una compañía es su información, si ésta se ve vulnerada o susceptible de ataque afectaría el buen funcionamiento de la organización, de ahí la importancia de tener planes de seguridad informática que ayuden a proteger este bien tan preciado.

En las redes internas de las empresas se intercambia y se almacena información importante: situación financiera, datos de clientes, reportes de ventas, estrategias de negocios, etc. Información crítica, cuya seguridad debe ser objeto de análisis y estudio. Muchas veces no basta con tener el equipo suficiente para cubrir las necesidades de seguridad informática, es también necesario contar con personal capacitado que no sólo ayude a proteger la información, sino que actué de manera apropiada en el caso de un ataque a la información, puesto que, ningún método de seguridad es infalible.

Para mejorar la seguridad informática de una organización, muchos especialistas realizan “hacking ético” es decir, aplican las técnicas que utilizan los hackers o los crackers para encontrar vulnerabilidades de seguridad dentro de la red de una empresa, esto les permite evaluar las debilidades que se tiene y encontrar posibles soluciones que puedan corregir estos huecos informáticos ayudando a proteger la información de la empresa.

El presente capítulo muestra una breve introducción sobre el proyecto a realizarse, es decir los objetivos asociados al tema que se desean cumplir, así

como la justificación y el alcance. Se toma en cuenta que el lector ya tiene un conocimiento, al menos básico, sobre redes y seguridad informática.

1.1 Objetivo General

Realizar el Análisis y Diagnóstico de vulnerabilidades informáticas en la red de datos de la empresa "Youphone CIA LTDA", a través de técnicas, herramientas y procedimientos de "hacking ético", para emitir recomendaciones que minimicen los riesgos asociados.

1.2 Objetivos Específicos

- Realizar un análisis preliminar del sistema de información.
- Seleccionar las herramientas que serán utilizadas en el examen
- Identificar las falencias de seguridad de datos existentes en la intranet de la empresa.
- Analizar los resultados obtenidos de las pruebas de intrusión para diseñar las posibles soluciones.
- Presentar recomendaciones que permitan minimizar los riesgos asociados a las fallas detectadas.

1.3 Justificación

La empresa Youphone CIA CLTA. Como cualquier otra compañía cuenta con información valiosa, la misma que puede ser vulnerada. Se ha registrado ciertos ataques a los servidores de la empresa, cuyas consecuencias han sido suspender algunos servicios por algunas horas, afortunadamente no se ha comprometido la integridad de la información, es por ello que la empresa se ve en la necesidad de crear un plan de seguridad informática que le permita corregir brechas de seguridad, crear mecanismos de protección y tener procedimientos adecuados que le faciliten actuar de manera efectiva en el caso de un ataque malicioso.

Por ello el presente proyecto propone analizar las diferentes vulnerabilidades de seguridad de la empresa utilizando “hacking ético”, es decir aplicando técnicas de vulneración y ataque a redes de datos que utilizan los hackers, las mismas que ayudarán a diagnosticar puntos débiles y corregirlos en la manera que sea posible, lo que permita emitir recomendaciones que cubra las necesidades de seguridad de la organización.

1.4 Alcance

El proyecto actual tiene como finalidad utilizar el “hacking ético” en la red de datos de la empresa “Youphone CIA LTDA”, una compañía dedicada a la venta de equipos telefónicos portables y de servicios de telecomunicaciones, es distribuidor autorizado Movistar que cuenta con varios locales en la ciudad de Quito. Esta empresa cuenta con una red de datos, sistemas informáticos y equipos de computación susceptibles de ser atacados.

Se pretende realizar un estudio sobre el “Hacking ético” sus términos, uso, definiciones, técnicas, herramientas usadas y modos de ataques, así como el desarrollo de pruebas de intrusión en la red de datos de la empresa dentro de un marco legal aceptable con el fin de cubrir las necesidades puntuales de la organización que son:

Identificación de vulnerabilidades y brechas de seguridad en la red de datos.

Diseño de soluciones factibles, considerando herramientas de software existentes.

Recomendación de soluciones diseñadas, dentro de un ambiente real.

Análisis de los resultados obtenidos.

Presentación de un presupuesto referencial, para la implementación de las soluciones.

CAPITULO 2. MARCO TEÓRICO

2.1 Hacking Ético

El término “hacking ético” dentro del mundo informático hace referencia a todo un proceso, el mismo que consiste en que una persona con conocimientos de redes y seguridad informática haga pruebas o incluso ataques a una o varias redes de datos de una empresa u organización con el objetivo de encontrar vulnerabilidades y luego reportarlas con el fin de encontrar una solución que evite dichos fallos en la seguridad de la empresa, por lo tanto se puede considerar al “hacking ético” o “ethical hacking” como una disciplina de la seguridad informática que se basa en evaluar las amenazas de seguridad de una empresa a través de las técnicas que utilizan los hackers.

Muchas personas asocian el “hacking” a acciones ilícitas o malintencionadas que afectan el buen funcionamiento de una red de datos y si bien este término se refiere a buscar debilidades en la seguridad informática y aprovecharse de ellas, al unirlo con la palabra “ético” lo que se busca es encontrar esas debilidades pero con el fin de solucionarlas o corregirlas.

2.1.1 Definición y términos comunes

A continuación se verá el concepto de términos asociados al campo de hacking ético, que ayudarán a la comprensión y el buen entendimiento de este tema.

2.1.1.1 Hacker

Es una persona que tiene una fascinación y conocimiento sobre redes informáticas programación de sistemas o sistemas operativos (Experto

informático) cuyo objetivo es buscar debilidades en las seguridades de las mismas.

2.1.1.2 Cracker

Es un hacker, es decir un experto informático pero su objetivo es causar un perjuicio a los equipos informáticos o redes de datos.

2.1.1.3 Malware

Viene de la unión de dos palabras en inglés “malicious software” que traducido al español quiere decir programa malicioso o malintencionado cuyo objetivo es dañar el funcionamiento de los computadores.

2.1.1.4 Virus

Es un malware hecho para infectar archivos, de ahí su nombre de “virus” porque tiene la capacidad de propagarse como un virus biológico. Su objetivo es dañar o alterar archivos del computador o los datos almacenados en el mismo.

El modo en que operan es colocando código en los archivos ejecutables y no actúa hasta que se inicie el programa infectado, una vez iniciado el programa el virus (código) se queda en la memoria RAM del computador por lo que, aunque se haya dejado de usar el programa infectado, éste empezará a tomar control de los servicios básicos del sistema operativo infectando archivos ejecutables que sean llamados para su ejecución.

Las maneras más comunes en que un computador se infecta de un virus son las siguientes:

1. Insertando USBs, DVDs, CDs que contengan virus.
2. A través de archivos adjuntos de e-mails
3. Anuncios publicitarios engañosos o falsos.
4. Mensajes dejados en redes sociales (Facebook, twitter, etc.).

5. Descargando aplicaciones o programas del internet.
6. Abriendo sitios web sospechosos.

2.1.1.5 Troyanos

Es un tipo de virus, su nombre se debe al “caballo de troya” que fue un artefacto gigante en forma de caballo que utilizaron los griegos para introducirse en Troya, mencionado en la Odisea de Homero. Así como el caballo se introdujo en Troya, este tipo de virus se mete en un computador a través de instaladores de programas (manera más común) y en primera instancia parecen inofensivos pero una vez introducidos su función es capturar los datos confidenciales de un ordenador y reenviarlos hacía una dirección externa o abrir puertos de comunicación para que usuarios externos puedan controlar el ordenador de manera remota.

2.1.1.6 Gusanos

Se lo conoce también por sus siglas en inglés IWorm, I de Internet y Worm de gusano “gusano de Internet”. Es un malware que realiza copias de sí mismo, instalándose en diferentes ubicaciones del ordenador.

Los gusanos se propagan de ordenador sin la ayuda de una persona como lo hacen los virus. Un gusano toma como residencia la memoria del ordenador y no altera los archivos del mismo como un virus, sino que se duplica así mismo y se trasmite a otros ordenadores a través de medios como e-mails, mensajería instantánea, programas P2P, etc.

Por su capacidad de replicarse a sí mismo y de trasmitirse a través de redes de datos, el gusano provoca saturación de la memoria del sistema o consume demasiado ancho de banda por lo que provoca que los ordenadores o los servidores se vuelvan lentos o en su defecto dejen de responder.

2.1.1.7 Exploits

Proviene del inglés “to exploit” que significa explotar o aprovechar, es un pedazo de software: fragmento de datos o secuencia de comandos o acciones o una técnica cuyo objetivo es aprovechar una vulnerabilidad de seguridad. No es un malware como tal, sino que se lo utiliza para permitir el acceso a un sistema o como parte de un gusano o troyano (casos raros), en otras palabras se lo puede definir como la llave de ingreso hacia un sistema.

El objetivo de un exploit es violar una medida de seguridad para así tener acceso al sistema de información y utilizarlo en beneficio propio provocando comportamientos no deseados como: acceso de forma no autorizada, toma de control de un sistema de cómputo, consecución privilegios no concedidos lícitamente, consecución de ataques de denegación de servicio, etc.

Para poder atacar, los exploits depende mucho de los sistemas operativos, sus configuraciones y de las configuraciones de los programas que se están utilizando en el computador, así como de la red LAN donde se encuentran.

Los Hackers pueden atacar un sistema utilizando exploits simples o varios al mismo tiempo.

2.1.1.8 Threats

Es un término que se lo ha utilizado últimamente para hacer referencia a un evento que podría perjudicar y poner en riesgo la seguridad de un sistema, se lo puede denominar también como un “indicador” de un posible ataque. Los threats pueden ser provocados de manera accidental ya sea por un ordenador en mal funcionamiento o por eventos naturales como incendios, terremotos, etc. Sin embargo la mayoría de veces son provocadas de manera intencional con el fin de violar la seguridad de un sistema.

2.1.1.9 Escaneo de Puertos

Es la acción de analizar a través de un programa el estado de los puertos de una máquina o varias máquinas conectadas a una red de datos, nos muestra si los puertos están abiertos o cerrados o protegidos con por un firewall (cortafuegos). Muchos de los programas que se dedican a esto también identifican los equipos que se encuentran activos y los servicios que prestan dentro de la red, los sistemas que utilizan y cómo están organizados.

2.1.2 Seguridad Informática

La Seguridad Informática es un tema actual que se refiere a todas las características y condiciones de los sistemas de procesamiento de datos y su almacenamiento, para garantizar que éstos se mantengan íntegros y resguardados de cualquier vulnerabilidad o acción malintencionada.

Para lograr que los datos de una organización puedan mantenerse seguros a pesar de cualquier ataque o vulnerabilidad necesitamos básicamente:

1. Conocer el peligro
2. Clasificarlo.
3. Protegerse de los impactos o daños de la mejor manera posible

Una vez que se toma conciencia de las potenciales amenazas, agresores y sus intenciones dañinas (directas o indirectas), se puede tomar medidas de protección adecuadas, para que no se pierda o dañe los recursos valiosos de la organización.

Por lo tanto, la Seguridad Informática sirve para la protección de la información, en contra de amenazas o peligros, para evitar daños y para minimizar riesgos, relacionados con ella.

2.1.2.1 Definición

"Seguridad es la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles" (Información, 2004,)

El principal objetivo a proteger es información de la Organización, para ello se debe tener en cuenta las dimensiones de la seguridad:

Disponibilidad:

Es una propiedad que indica que los servicios o activos de una empresa u organización estén cuando sea necesario. La carencia de la misma provoca una interrupción del servicio afectando a la productividad de la empresa.

Integridad:

Es una propiedad que indica la completitud y buen estado de los datos. La carencia de la misma provoca que la información pueda aparecer manipulada, corrupta o incompleta, afectando al desempeño de las funciones de la empresa.

Confidencialidad:

Es una propiedad que indica que la información llega solamente a las personas autorizadas. La carencia de la misma provoca fugas y filtraciones de información a persona no deseadas, así como accesos no autorizados, afectando la privacidad de la empresa. La confidencialidad es muy difícil de recuperar, pudiendo minar la confianza de los demás en la organización.

Autenticidad:

Es una propiedad que indica que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. La carencia de la misma provoca suplantación de identidad, o que la fuente de los datos no sea fiable, afectando la confiabilidad de la empresa.

Trazabilidad:

Es una propiedad que indica que se puede determinar con total seguridad quién hizo qué y en qué momento. La carencia de la misma provoca incertidumbre y desconfianza, afectando la confianza de la empresa en sus colaboradores.

2.1.2.2 Gestión de Riesgos en la Seguridad Informática

De manera general la Gestión de Riesgo es un método de administración para determinar, analizar, valorar y clasificar el riesgo, para luego implementar mecanismos que permitan controlar el mismo.

Figura 1 Fases de la Gestión de Riesgos

Dentro de la informática la gestión de riesgos tiene varios métodos, de manera general todos estos métodos constan básicamente de 4 fases:

1. **Análisis**: en esta fase se establece los componentes de un sistema que requieren protección, sus vulnerabilidades que lo debilitan y las amenazas que lo ponen en peligro, con el resultado de revelar su grado de riesgo.
2. **Clasificación:** en esta fase se establece si los riesgos encontrados y los riesgos restantes son aceptables.
3. **Reducción:** en esta fase se define e implementa las medidas de protección, también se sensibiliza y capacita los usuarios conforme a las medidas.
4. **Control:** en esta etapa se analiza el funcionamiento, la efectividad y el cumplimiento de las medidas, para determinar y ajustar las medidas deficientes y sanciona el incumplimiento.

2.1.2.3 Amenazas y Vulnerabilidades (Red y Seguridad, 2015)

Dentro del campo de la seguridad informática se escucha mucho hablar de las amenazas y vulnerabilidades, para aplicar controles adecuados de seguridad, es preciso comprender estos conceptos, es decir conocer primero quién o qué es lo que amenaza un ambiente, así como de reconocer los riesgos que se encuentran en torno a esas situaciones.

Los problemas de seguridad se dividen principalmente en amenazas y vulnerabilidades.

2.1.2.3.1 Amenazas (Morales, 2015)

Las amenazas son eventos que pueden causar alteraciones a la información de la organización ocasionándole pérdidas materiales, económicas, de información, y de prestigio.

Es posible establecer medidas para protegerse de las amenazas o se puede atenuar su efecto, pero prácticamente imposible controlarlas y menos aún eliminarlas.

Fuentes de amenaza (Red y Seguridad, 2015)

Existen varias categorías de amenazas, se clasificaran por su origen, de esta forma se dividen en cinco tipos los cuales son:

- Amenazas Humanas
- De hardware
- De software
- De red
- Desastres naturales.

1) Factor humano

Las personas son la principal fuente de amenaza que existe en los sistemas de información y son el tipo de amenaza en el que se invierten más recursos para controlarlos y contrarrestar sus efectos.

Abarca actos malintencionados, incumplimiento de las medidas de seguridad como consecuencia de actos negligentes o falta de controles adecuados.

Tipos de amenazas humanas (Morales, 2015)

Los actos humanos que pueden afectar la seguridad de un sistema son variados, entre los más comunes e importantes están:

- **Curiosos:** se trata de personas que entran a sistemas (en algunos casos de manera accidental) a los que no están autorizados, motivados por la curiosidad, por el desafió personal, o por el deseo de aprender o

averiguar.

Generalmente este tipo de intrusos no tienen los conocimientos apropiados para lograr causar daños, pero no por eso se les debe ignorar sin tomar las precauciones necesarias.

Aunque se afirma que no tienen intenciones maliciosas, su sola intrusión al sistema representa una peligrosa amenaza ya que pueden causar daños no intencionales o dejar expuesta la estructura y seguridad del sistema.

- **Intrusos remunerados:** este tipo de atacante se encarga de penetrar a los sistemas a cambio de un pago. Aunque son menos comunes, en realidad son muy peligrosos ya que se trata de personas que poseen los conocimientos, experiencia y herramientas necesarias para penetrar en los sistemas, incluso en aquellos que tienen un nivel alto de seguridad.
- **Personal enterado:** se trata de personas que tienen acceso autorizado o conocen la estructura del sistema de cierta organización. Por lo general es el mismo personal interno de una empresa o un ex empleado, sus motivaciones van desde revanchas personales hasta ofertas y remuneraciones de organizaciones rivales.
- **Terroristas:** tienen como objetivo causar daños con diferentes fines por ejemplo proselitistas o religiosos.
- **Robo:** se refiere a la extracción física de la información por medio de unidades de almacenamiento secundario (diskettes, CD, cintas, etc.), robo físico de los componentes de hardware del sistema e incluso también se considera como robo el uso de los equipos para actividades diferentes a los que se les asigna en la organización,
- **Sabotaje:** consiste en reducir la funcionalidad del sistema por medio de acciones deliberadas dirigidas a dañar los equipos, logrando la interrupción de los servicios e incluso la destrucción completa del

sistema. Puede ser perpetuada por el personal interno o por opositores externos.

- **Fraude:** estas actividades no tienen como principal fin la destrucción del sistema, si no aprovechar los recursos que se manejan para obtener beneficios ajenos a los objetivos de la organización.

  Aun cuando los responsables del fraude sean identificados y detenidos, este tipo de actividad comúnmente se trata con suma discreción sin hacerle publicidad debido a que le da mala imagen a la organización implicada.

- **Ingeniería social:** en el campo de la seguridad informática ingeniería social es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos llevándolos a revelar información sensible, o bien a violar las políticas de seguridad típicas. Con este método, los ingenieros sociales aprovechan la tendencia natural de la gente a confiar en su palabra, antes que aprovechar agujeros de seguridad en los sistemas informáticos. Generalmente se está de acuerdo en que “los usuarios son el eslabón débil” en seguridad; éste es el principio por el que se rige la ingeniería social.

2) Hardware (Red y Seguridad, 2015)

Se da la amenaza por fallas físicas que presente cualquiera de los elementos de hardware que conforman al sistema de cómputo. Estas fallas físicas pueden ser defectos de fabricación o mal diseño del hardware, pero también pueden ser el resultado de un mal uso y descuido en el mantenimiento.

Tipos de amenazas de hardware

- **Mal diseño:** es cuando los componentes de hardware del sistema no son apropiados y no cumplen los requerimientos necesarios, en otras

palabras, dicha pieza del módulo no fue diseñada correctamente para trabajar en el sistema.

- **Errores de fabricación:** es cuando las piezas de hardware son adquiridas con desperfectos de fabricación y posteriormente fallan al momento de intentar usarse. Aunque la calidad de los componentes de hardware es responsabilidad del fabricante, la organización que los adquiere es la más afectada por este tipo de amenaza.
- **Suministro de energía:** las variaciones de voltaje dañan los dispositivos, por ello es necesario verificar que las instalaciones de suministro de energía funcionen dentro de los parámetros requeridos. También debe procurarse que dichas instalaciones proporcionen los voltajes requeridos para hacer funcionar un dispositivo, pues existen componentes de hardware que necesitan ser energizados a ciertos niveles de voltaje especificados por los fabricantes, de lo contrario se acortara su vida útil.
- **Desgaste:** el uso constante del hardware produce un desgaste considerado como normal, con el tiempo este desgaste reduce el funcionamiento óptimo del dispositivo hasta dejarlo inutilizable.

Descuido y mal uso: todos los componentes deben ser usados dentro de los parámetros establecidos por los fabricantes, esto incluye tiempos de uso, periodos y procedimientos adecuados de mantenimiento, así como un apropiado almacenamiento. No seguir estas prácticas provoca un desgaste

3) Hardware (Red y Seguridad, 2015)

Se da la amenaza por fallas físicas que presente cualquiera de los elementos de hardware que conforman al sistema de cómputo. Estas fallas físicas pueden ser defectos de fabricación o mal diseño del hardware, pero también pueden ser el resultado de un mal uso y descuido en el mantenimiento.

Tipos de amenazas de hardware

- **Mal diseño:** es cuando los componentes de hardware del sistema no son apropiados y no cumplen los requerimientos necesarios, en otras palabras, dicha pieza del módulo no fue diseñada correctamente para trabajar en el sistema.
- **Errores de fabricación:** es cuando las piezas de hardware son adquiridas con desperfectos de fabricación y posteriormente fallan al momento de intentar usarse. Aunque la calidad de los componentes de hardware es responsabilidad del fabricante, la organización que los adquiere es la más afectada por este tipo de amenaza.

- **Suministro de energía:** las variaciones de voltaje dañan los dispositivos, por ello es necesario verificar que las instalaciones de suministro de energía funcionen dentro de los parámetros requeridos. También debe procurarse que dichas instalaciones proporcionen los voltajes requeridos para hacer funcionar un dispositivo, pues existen componentes de hardware que necesitan ser energizados a ciertos niveles de voltaje especificados por los fabricantes, de lo contrario se acortara su vida útil.

- **Desgaste:** el uso constante del hardware produce un desgaste considerado como normal, con el tiempo este desgaste reduce el funcionamiento óptimo del dispositivo hasta dejarlo inutilizable.

- **Descuido y mal uso:** todos los componentes deben ser usados dentro de los parámetros establecidos por los fabricantes, esto incluye tiempos de uso, periodos y procedimientos adecuados de mantenimiento, así como un apropiado almacenamiento. No seguir estas prácticas provoca un desgaste mayor que trae como consecuencia descomposturas prematuras y reducción del tiempo de vida útil de los recursos.

4) Software (Red y Seguridad, 2015)

Las amenazas de software incluyen posibles fallas dentro del software de un sistema operativo, software mal desarrollado, mal diseñado o mal implantado, además de que existe software de uso malicioso que representa una amenaza directa contra un sistema.

Tipos de amenaza de Software

- **Software de desarrollo:** es un tipo de software personalizado, puede ser creado con el fin de atacar un sistema completo o aprovechar alguna de sus características para violar su seguridad.

- **Software de aplicación:** este software no fue creado específicamente para realizar ataques, pero tiene características que pueden ser usadas de manera maliciosa para atacar un sistema.

- **Código malicioso** es cualquier software que entra en un sistema de cómputo sin ser invitado e intenta romper las reglas, esto incluye caballos de Troya, virus, gusanos informáticos, bombas lógicas y otras amenazas programadas.

- **Errores de programación y diseño:** el software creado para cumplir alguna función dentro de la organización (Por ejemplo un sistema de transacciones financieras, sistema de nómina, sistemas operativos, etc.), también pueden causar pérdida o modificación de la información. Esto ocurre cuando el software en cuestión no cumple con los estándares de seguridad requeridos pues nunca fue diseñado para dar soporte a una organización. Los errores de programación y fallas generales que puede tener un software de aplicación también representan una amenaza.

-

5) Red de datos (Red y Seguridad, 2015)

Esta amenaza se presenta cuando la red de comunicación no está disponible para su uso, esto puede ser provocado por un ataque deliberado por parte de un intruso o un error físico o lógico del sistema mismo. Las dos principales amenazas que se presentan en una red de datos son, la no disponibilidad de la red, y la extracción lógica de información a través de ésta.

Tipos de amenaza de Red de Datos (Red y Seguridad, 2015)

- **Topología seleccionada:** la topología es la disposición física en la que se conectan los nodos de una red de ordenadores o servidores, cada una presenta una serie de ventajas y desventajas. Dependiendo el alcance y recursos compartidos en una red, puede ser más conveniente seleccionar una topología sobre otra, pero debe tomarse en cuenta que las desventajas de cada arquitectura no solo limitan la comunicación, incluso pueden dejar la red fuera de servicio.

  Por ejemplo en una red de anillo la comunicación se da por el paso de un token o testigo, que se puede conceptualizar como un cartero que pasa recogiendo y entregando paquetes de información, de esta manera se evitan eventuales pérdidas de información debido a colisiones, pero si la comunicación en algún nodo se pierde, entonces la comunicación en todo el anillo se pierde.

- **Sistema operativo:** aunque el modelo OSI permite la comunicación entre equipos con diferentes sistemas operativos, se dan casos en los que ciertas opciones de operación difieren entre sistemas operativos, haciendo difícil el compartir ciertos recursos.

También cada sistema operativo tiene un nivel de protección diferente que los hace más susceptibles a ataques que otros, y a partir de ahí el atacante puede tomar acciones contra otros sistemas operativos con mayor nivel de seguridad. Este último punto es considerado más una vulnerabilidad que una amenaza.

- **Incumplimiento de las normas de instalación de la red:** la instalación del cableado físico de las redes de datos, deben seguir ciertas normas y estándares de diseño conocidos también como cableado estructurado.

  El cableado estructurado corresponde a un conjunto de normas internacionales que consiste en el tendido de cables en el interior de un edificio con el propósito de implantar una red de área local, es el sistema colectivo de cables, canalizaciones, conectores, etiquetas, espacios y demás dispositivos que deben ser instalados para establecer una infraestructura de telecomunicaciones genérica en un edificio, para ello hay que tener en cuenta las limitaciones de diseño que impone la tecnología de red de área local que se desea implantar:

  - La segmentación del tráfico de red.
  - La longitud máxima de cada segmento de red.
  - La presencia de interferencias electromagnéticas.
  - La necesidad de redes locales virtuales.

No tomar en cuenta estos puntos puede resultar en fallas de diseño que causen problemas de transmisión de datos, operabilidad o indisponibilidad de los recursos de red.

El cableado estructurado permite tener un mejor control en la administración de una red de datos

Desastres naturales (Red y Seguridad, 2015)

Son eventos que tienen su origen en las fuerzas de la naturaleza. Estos desastres no solo afectan a la información contenida en los sistemas, sino también representan una amenaza a la integridad del sistema completo (infraestructura, instalación, componentes, equipos, etc.) pudiendo dejar al sistema incluso en un estado de inoperatividad permanente. Este tipo de amenazas también incluye la falta de preparación.

Tipos de desastres naturales (Red y Seguridad, 2015)

Entre los tipos de desastres naturales que amenazan a un sistema de información, tenemos las inundaciones, los terremotos, incendios, huracanes, tormentas eléctricas, etc. Los cuales provocan cortos circuitos, destrucción total o parcial de los equipos de cómputo, o alteraciones físicas de las localidades, causando que ya no sean apropiadas para albergar un equipo de cómputo.

Por lo que es necesario considerar el punto geográfico en el que se llevara a cabo la instalación del equipo de cómputo, centro de servicios de información, centro de cómputo etc. y hacer un estudio que permita determinar las amenazas a las que serían susceptibles a fin de evitar ser víctimas de estos.

Adicionalmente considerar la importancia de un cableado no solo en la red de datos sino de las redes de energía eléctrica y suministro de aguas que de manera indirecta podrían causar algún desastre de este tipo y dañar la información de la organización.

El cableado eléctrico de un edificio no solo debe proporcionar continuidad del servicio sino también seguridad

2.1.2.3.2 Vulnerabilidades (Morales, 2015)

Dependiendo del enfoque que se le dé a la seguridad informática, un sistema informático está expuesto al peligro por medio de dos factores: Las amenazas y las vulnerabilidades.

Las vulnerabilidades constituyen el otro factor que pone en peligro la seguridad de un sistema, generalmente se cree que una vulnerabilidad es un punto débil de un sistema y aunque no es una definición incorrecta, tampoco expresa en su totalidad lo que es una vulnerabilidad.

Una vulnerabilidad informática es un elemento de un sistema informático que puede ser aprovechado por un atacante para violar la seguridad, así mismo pueden causar daños por sí mismos sin tratarse de un ataque intencionado.

A las vulnerabilidades se les consideran un elemento interno del sistema, por lo que es tarea de los administradores y usuarios el detectarlos, valorarlos y reducirlos.

Tipos de Vulnerabilidades (Morales, 2015)

Las vulnerabilidades son el resultado de errores de programación (bugs), fallos en el diseño del sistema, incluso las limitaciones tecnológicas pueden ser aprovechadas por los atacantes.

Se clasifican las vulnerabilidades en seis tipos:

1. Físicas.
2. Naturales.
3. De hardware.
4. De software.
5. De red.
6. De factor humano.

1) Física

Está relacionada con el acceso físico al sistema. Es todo lo referente al acceso y de las instalaciones donde se tienen los equipos de cómputo que contienen la información o forman partes de los procesos esenciales del sistema.

Las vulnerabilidades de este tipo se pueden presentar en forma de malas prácticas de las políticas de acceso de personal a los sistemas y uso de medios físicos de almacenamiento de información que permitan extraer datos del sistema de manera no autorizada.

2) Natural

Recordemos que las amenazas naturales son todo tipo de desastres causados por fuerzas naturales que causan daño a un sistema, por el lado de las amenazas naturales, estas se refieren al grado en que el sistema se puede ver afectado por este tipo de eventos.

Las vulnerabilidades de tipo natural se presentan principalmente en deficiencias de las medidas tomadas para afrontar los desastres, por ejemplo no disponer de reguladores, no-breaks, mal sistema de ventilación o calefacción, etc.

Aunque no se puede evitar que ocurra un fenómeno natural, si es necesario instalar medidas de seguridad para proteger al sistema de este tipo de eventos

3) Hardware (Morales, 2015)

Las vulnerabilidades de hardware representan la probabilidad de que las piezas físicas del sistema fallen (ya sea por mal uso, descuido, mal diseño etc.) dejando al sistema desprotegido o inoperable. También trata sobre las formas en que el hardware puede ser usado por personas para atacar la seguridad del

sistema, por ejemplo el sabotaje de un sistema al sobrecargarlo deliberadamente con componentes de hardware que no han sido diseñados correctamente para funcionar en el sistema.

4) Software

Cada programa (ya sea de paquetería o de sistema operativo) puede ser usado como medio para atacar a un sistema más grande, esto se da debido a errores de programación, o porque en el diseño no fueron considerados ciertos aspectos (por ejemplo controles de acceso, seguridad, implantación, etc.).

Ambos factores hacen susceptible al sistema a las amenazas de software.

5) Red

Las redes pueden llegar a ser sistemas muy vulnerables, al tratarse de una serie de equipos conectados entre sí compartiendo recursos, es posible atacar a toda la red penetrando primero en uno de los equipos y posteriormente expandirse al resto.

En una red la prioridad es la transmisión de la información, así que todas las vulnerabilidades están relacionadas directamente con la posible intercepción de la información por personas no autorizadas y con fallas en la disponibilidad del servicio.

Estos dos puntos hacen que las vulnerabilidades de las redes lleguen a ser una combinación de vulnerabilidades de hardware, software, físicas e incluso naturales.

6) Factor humano

Los elementos humanos de un sistema son los más difíciles de controlar lo que los convierte en constantes amenazas y al mismo tiempo una de las partes más vulnerables del sistema.

Las vulnerabilidades de origen humano más comunes son la falta de capacitación y concienciación, lo que puede dar lugar a la negligencia en el seguimiento de las políticas de seguridad, y mal uso del equipo de cómputo.

Los actos contra la seguridad realizados a conciencia por un elemento humano (Como el robo de información o la destrucción de los sistemas) pueden ser el resultado de una vulnerabilidad humana, ya sea por un usuario que accidentalmente revela las contraseñas de acceso o no revisa periódicamente las bitácoras de actividades de los equipo de cómputo a fin de buscar actividades sospechosas por citar algunos ejemplo.

Un usuario resentido o con poca lealtad a la organización es una amenaza y una vulnerabilidad humana al mismo tiempo, pues él puede convertirse en el autor directo de ataques al sistema o revelar intencionalmente información del sistema a personas no convenientes.

2.1.3 Clasificación de Hackers

A los hackers se los puede clasificar según el tipo de trabajo que realizan, es decir si realizan actividades ilícitas (crackers) o si su actividad es en defensa y protección de los sistemas informáticos.

2.1.3.1 White hacker

También llamado “hacker de sombrero blanco”. Son todos los administradores de Redes y consultores de seguridad informática que utilizan sus conocimientos sobre sistemas con propósitos defensivos, normalmente protegen las redes de información (Astudillo, 2013)

2.1.3.2 Black Hacker

También llamado “hacker de sombrero negro”, al contrario del “White Hacker” utilizan sus conocimientos con propósitos destructivos, dentro de esta categoría se encuentran los “crackers”.

Este término es también usado comúnmente para referirse a una persona a la que le gusta romper la seguridad de los sistemas informáticos. Los motivos pueden ser diversos, desde el mero deseo de satisfacer el ego y decir “pude romper X o Y sistema”, obtener dinero ilícito ejecutando fraudes electrónicos, o inclusive realizar protestas políticas. A este último tipo de cracker también se lo llama hacktivista.

Como ejemplo de hacktivistas podemos citar al grupo Anonymus, el cual realiza protestas de índole político infiltrándose en sistemas de gobierno o a través de ataques de denegación de servicio. (Astudillo, 2013)

2.1.3.3 Grey Hacker

También llamado “hacker de sombrero gris” son expertos informáticos que trabajan tanto en la defensa como en el ataque de sistemas informáticos, no se recomienda contratar a estos expertos porque no son de confianza puesto que se caracterizan por una “doble moral”.

2.1.3.4 Lammer

Hace referencia a una persona falta de habilidades técnicas, y poco conocimiento sobre tecnología pero qué desea convertirse en un hacker profesional, sin embargo, por su poco conocimiento, para sus ataques se limita a utilizar programas ya hechos por otros individuos.

Estas personas son las más numerosas y sus más frecuentes ataques son bombardear permanentemente el correo electrónico para colapsar los sistemas o emplean de forma habitual programas sniffers para controlar la red,

interceptar contraseñas y correos electrónicos, y después enviar mensajes con direcciones falsas, en muchas ocasiones, amenazando el sistema, lo que en realidad no es cierto, su alcance no va mucho más allá de poseer el control completo del disco duro, aun cuando el ordenador esté apagado.

2.1.4 Fases del Hacking Ético (Graves, 2010)

Un hacker ético sigue procesos similares a los de un atacante malicioso. Los pasos para obtener y mantener acceso al sistema informático son similares más allá de las intenciones del atacante. La figura de a continuación ilustra las cinco fases que los atacantes, en general, siguen para acceder a un sistema.

Figura 2 Fases del Hacking Ético

2.1.4.1 Reconocimiento pasivo y reconocimiento activo (Reconnaissance)

El reconocimiento pasivo involucra la recolección de información con respecto a un potencial blanco sin tener conocimientos particulares de ese blanco. El reconocimiento pasivo puede ser tan simple como espiar un edificio para ver en qué momento entran los empleados y cuándo salen.

Sin embargo, generalmente esto se realiza buscando en Internet o buscando a través de los buscadores (generalmente Google) información sobre una persona o sobre alguna compañía. Este proceso es denominado “Recolección de información” (Information Gathering).

La Ingeniería Social (Social Engineering) y el basureo (Dumpster Diving) también son considerados métodos de recolección de información pasiva. El Sniffing (olfatear) de red es otro de los métodos de reconocimiento pasivo y a través del cual es posible obtener información útil como direcciones IP, nombres convencionales, servidores o redes ocultas, y otros servicios disponibles en el sistema o en la red.

Realizar Sniffing en el tráfico de la red es similar a la construcción de la vigilancia: un atacante mira el flujo de datos para ver a qué hora se realizan las transacciones y hacia dónde va el tráfico de la red. El reconocimiento activo implica el sondeo de la red para descubrir hosts, direcciones IP y servicios que se ejecutan en la red. Generalmente esto significa un mayor riesgo de ser detectado que en el reconocimiento pasivo y a veces es llamado “ratting the doorknobs”.

El reconocimiento activo le puede brindar a un atacante información sobre las políticas de seguridad que se adoptan en el lugar, pero este proceso también aumenta la posibilidad de ser descubierto o al menos despertar sospechas.

Tanto el reconocimiento activo como el reconocimiento pasivo pueden conducir al descubrimiento de información útil que puede ser usada para realizar un ataque. Por lo general es fácil descubrir qué tipo de servidor web se está utilizando y la versión de los sistemas operativos que emplea la empresa.

Esta información puede permitir encontrar una vulnerabilidad relacionada con la versión de ese sistema operativo y explotar la vulnerabilidad para obtener

acceso PC, desde Internet o fuera de línea. Los ejemplos incluyen desbordamiento de búfer (Buffer Overflow), denegación de servicio (DoS – Denial of Service) y secuestro de sesión (Session hijacking). En el mundo de los atacantes, ganar acceso se conoce como “posesión del sistema”.

2.1.4.2 Exploración (Scanning)

La fase de exploración implica la toma de la información descubierta durante la fase de reconocimiento y utilizarla para examinar la red. Las herramientas que un atacante puede emplear durante la fase de exploración puede incluir port scanners, network mappers, sweepers y vulnerability scanners. Los atacantes buscan cualquier tipo de información que pueda ayudarles a perpetrar un ataque, como por ejemplo nombres de hosts, direcciones IP y cuentas de usuario.

2.1.4.3 Ganando acceso (Gaining access)

Esta es la fase en la que el verdadero hacking tiene lugar. Las vulnerabilidades descubiertas durante las fases de exploración y reconocimiento ahora son explotadas para obtener acceso al sistema.

El método de conexión que el atacante utiliza para vulnerar el sistema pueden ser a través de una red de área local (LAN, ya sea por cable o inalámbrica), acceso físico a la PC, desde Internet o fuera de línea. Los ejemplos incluyen desbordamiento de búfer denegación de servicio (DoS – Denial of Service) y secuestro de sesión (Session hijacking). En el mundo de los atacantes, ganar acceso se conoce como “posesión del sistema”.

2.1.4.4 Manteniendo el acceso (Maintaining access)

Una vez que el atacante ha conseguido acceder al sistema, busca mantener ese acceso para futuras intrusiones y ataques. A veces, endurecen el sistema de otros atacantes o personal de seguridad para asegurar su acceso exclusivo a través de backdoors, rootkits y troyanos.

Cuando posee el sistema puede utilizarlo como base para ejecutar ataques adicionales. En este caso, el sistema informático comprometido es denominado computadora Zombi.

2.1.4.5 Cubriendo las huellas (Covering tracks)

Una vez que el atacante ha sido capaz de ganar y mantener el acceso al sistema, cubre las huellas para evitar ser detectado por el personal de seguridad, para poder seguir usando el sistema comprometido, para eliminar evidencias de la violación al sistema y/o para evitar acciones legales. Es decir, trata de eliminar todos los rastros del ataque, como archivos de registro (log) o alarmas del Sistema de Detección de Intrusos (IDS). Ejemplos de actividades llevadas a cabo durante esta fase del ataque son la esteganografía (steganography), el empleo de protocolos de tunneling y la modificación de archivos de registro (log).

2.1.5 Tipos de hacking

Existen básicamente dos tipos de procedimiento de hacking ético, éstas reciben su nombre según desde dónde se ejecutan las pruebas de intrusión, por lo tanto un hacking ético puede ser externo o interno.

2.1.5.1 Hacking ético Externo

Este tipo de hacking ético es aquel que se realiza desde el internet, es decir que se realiza sobre los equipos de la organización que se encuentran expuestos al internet: servidores de correo, servidores web, enrutadores, cortafuegos, servidores de dominio, etc.

2.1.5.2 Hacking ético interno

Este tipo de hacking ético es aquel que se realiza dentro de la red interna de una organización, es decir se lo hace desde el punto de vista de un empleado de la empresa, un consultor o un asociado de negocios que tiene acceso a la red de datos de la organización.

En este tipo se suelen encontrar más vulnerabilidades de seguridad puesto que, los administradores de redes se preocupan por proteger el perímetro de su red y descuidan al atacante interno. Se ha demostrado según una encuesta en el Reino Unido que los atacantes de redes eran en un 75% internos y un 25% externos.

2.1.6 Modalidades del hacking ético

2.1.6.1 Caja blanca (White Box Hacking) (Ramagaes.com, 2015)

Se denomina también test de intrusión de caja blanca puesto que se dispone de toda la información necesaria (direcciones IP, puntos de acceso wifi, reglas de los cortafuegos, código fuente de aplicaciones, configuraciones y otra que pueda ser necesaria) para que el equipo de intrusión empiece a realizar el testeo de las posibles vulnerabilidades de los sistemas de información.

El valor añadido de este tipo de intrusión está en el análisis de la información proporcionada por la organización por parte del equipo auditor. Con todos estos datos se puede realizar un test de seguridad en profundidad que detecte no sólo vulnerabilidades inmediatas, si no código y configuraciones potencialmente peligrosas, puertas traseras y defectos de construcción. Es un tipo de test adecuado para entornos con necesidades de seguridad muy sensibles.

2.1.6.2 Caja negra (Black Box Hacking) (Ramagaes.com, 2015)

Un proyecto de hacking ético de caja negra es como uno de caja blanca pero empieza con un nivel de conocimiento cero por parte del equipo que realiza el test de intrusión. Por parte de la organización solamente el personal de nivel de gestión tiene conocimiento de las actividades que los hackers éticos llevan a cabo. A diferencia de los test de caja blanca, el valor añadido de un test de caja negra reside en detectar la facilidad que un atacante pueda tener para

encontrar información sobre la organización y cómo puede utilizarla en su favor. Se debe pensar que si el equipo ha sido capaz de encontrar vulnerabilidades, es muy probable que un atacante también. Este tipo de test de intrusión está recomendado para organizaciones que quieran saber cuál es su grado de seguridad a todos los niveles.

2.1.6.3 Hacking Ético de aplicaciones web (Ramagaes.com, 2015)

Se realiza un estudio preliminar y se ejecutan ataques reales controlados contra las aplicaciones web de la organización como pueden ser comercio electrónico, bases de datos, gestores de información, etc.

El objetivo es la búsqueda de vulnerabilidades que puedan dar el control de la aplicación al atacante. Si la organización tiene aplicaciones web, ya sea en la intranet o de cara al público, le resultará crítico saber si cuentan con vulnerabilidades que puedan ser aprovechadas por usuarios malintencionados.

2.1.6.4 Caja Gris (Grey Box Hacking)

Este tipo de hacking se realiza sobre la red interna de la organización, aquí no se brinda mayor información de la misma, sólo se recibe los accesos que tendría un empleado de la organización y datos de la red local de la organización (direcciones IP, máscara de subred, Gateway y servidor DNS); pero no se entregar más información adicional como podría ser nombre de usuario y contraseña para unirse a un dominio, o la existencia de subredes anexas, etc.

2.2 Ética y Legalidad

La ética profesional es “un conjunto de normas morales que rigen la conducta humana” (Real Academia de la Lengua, 2016), por lo tanto, cuando un profesional actúa con ética se dice que está obrando de manera correcta y legal, puesto que se rige a las leyes establecidas. En la actualidad dentro del

campo informático, la “ética y legalidad” toma más fuerza, puesto que, la informática se ha convertido en buen blanco para cometer fraudes.

La seguridad informática no sólo se limita al Internet, sino a la preservación y buen manejo de la información, por lo que es necesario saber quién protege la información, de ahí la importancia de entender que estos dos aspectos la “ética y la legalidad” están relacionados entre sí, porque son estas características las que realmente brindan seguridad a nuestra información.

2.2.1 Aspectos éticos

La ética dentro del mundo informático se centra en regular la información que el usuario comparte de manera consciente, la ética tiene un tinte moral, por lo tanto depende de cada persona el uso que le dará a la información.

Existen dos valores a tomar en cuenta:

- **Respeto** a la información y a los usuarios.
- **Honestidad** (qué la información sea verídica).
- **Honradez** al obrar y cumplir las normas.
- **Responsabilidad** en lo que se dice, escribe o en la información que se manipula

2.2.2 Aspectos Legales

Los aspectos legales son normas ya establecidas por un ente superior, que al no ser normas morales como los aspectos éticos, si se incumplen dichas normas puede haber una sanción o un correctivo dependiendo del caso.

Algunos de los delitos informáticos más comunes son:

- **Fraudes**: son las alteraciones de la información o incluso la eliminación de la misma.
- **Espionaje Informático:** es la divulgación no autorizada de datos reservados.

- **Pornografía infantil:** es la utilización de menores de edad para el exhibicionismo con el fin de inducir, promocionar y favorecer la prostitución de niños y niñas.
- **Infracciones de Propiedad intelectual:** es la copia o reproducción de programas informáticos sin autorización legal.

2.3 Herramientas y Procedimientos

En el internet existen un sinnúmero de herramientas o programas que ayudan a monitorear las redes informáticas o en su defecto, dichas herramientas son utilizadas para realizar ataques u obtener información que en malas manos podría ser perjudicial.

Hay que tener en cuenta que incluso el mismo “Google” puede ser una gran herramienta a la hora de buscar información o en el mismo se puede encontrar procedimientos o “trucos” que facilitan la realización de cualquier tipo de auditoria.

A continuación se detalla las características de algunas herramientas que pueden ayudar a realizar una auditoría de vulnerabilidades de seguridad y por consiguientes son útiles para realizar un análisis de hacking ético.

2.3.1 Herramientas de Reconocimiento o footprinting

El reconocimiento como se vio previamente es la primera fase del hacking ético, el mismo que consiste en obtener la mayor cantidad de información útil o relevante de la empresa o de la víctima como puede ser:

- Nombres de dominio
- Direcciones Ips específicas
- Direcciones de red
- Servicios de red y aplicaciones
- Mecanismos de control de acceso
- Arquitectura del sistema

- Mecanismos de autenticación
- Números telefónicos
- Direcciones de contacto, etc.

Algunas de las herramientas o procedimientos que facilitan el footprinting son:

2.3.1.1 Footprinting con Google

Google es sin duda el buscador en internet por excelencia, ya que goza de gran popularidad por su tecnología “Page Rank” (clasificación de páginas web), la que permite realizar búsquedas acertadas y rápidas, por lo tanto se convierte en la principal fuente de obtención de información.

Muchas personas inexpertas obtienen información importante con solo teclear en google lo que desean obtener, de ahí la importancia de este buscador a la hora de recolectar información.

2.3.1.2 Whois

Es un servicio de consultas que muestra información completa de los nombres de dominio, es decir permite averiguar quién es el dueño de un dominio en particular proporcionando acceso directo a la información del dueño, o incluso permite saber si dicho dominio está disponible o no.

Las páginas de internet que prestan este servicio utilizan el protocolo TCP del mismo nombre “Whois” basado en petición/respuesta, es decir trabajan a través del puerto 23.

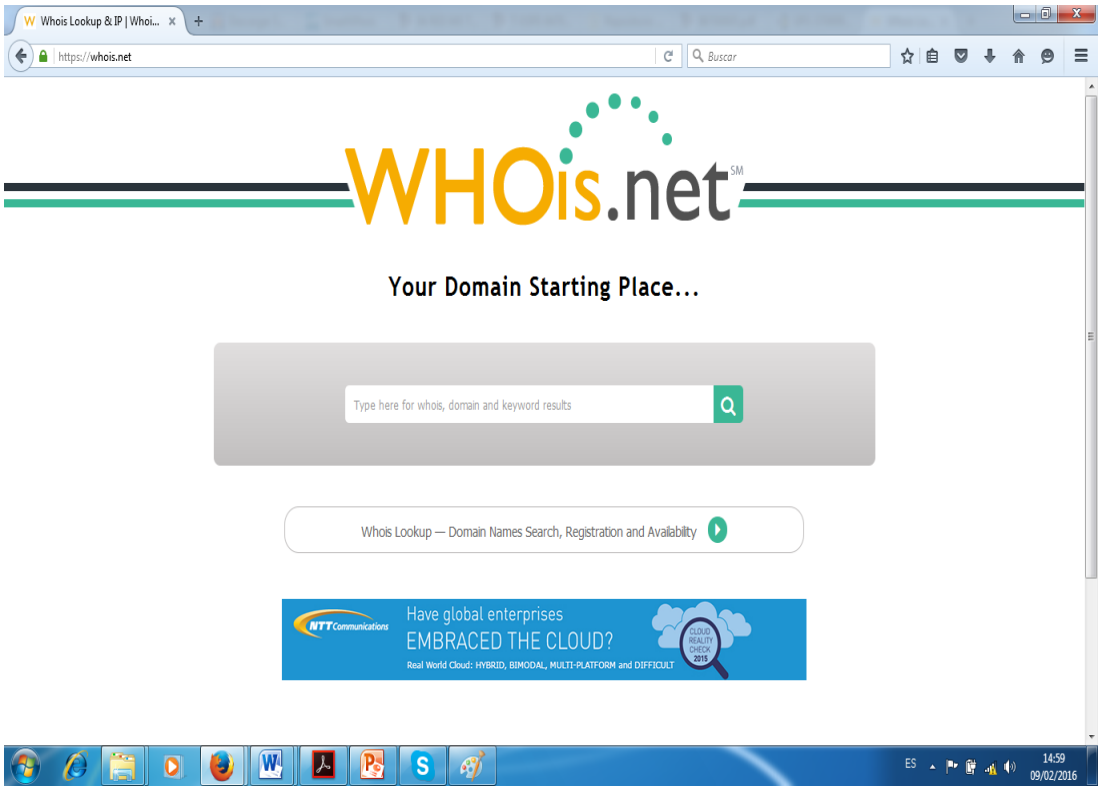

Figura 3 Captura de pantalla WHOis.net

2.3.1.3 SmartWhois

Es una aplicación que permite obtener información a partir de una dirección IP, un nombre de dominio o hostname. Los datos que proporciona son la información del servidor dónde está alojado el dominio, la empresa titular del servidor e incluso el país con el estado o provincia de procedencia.

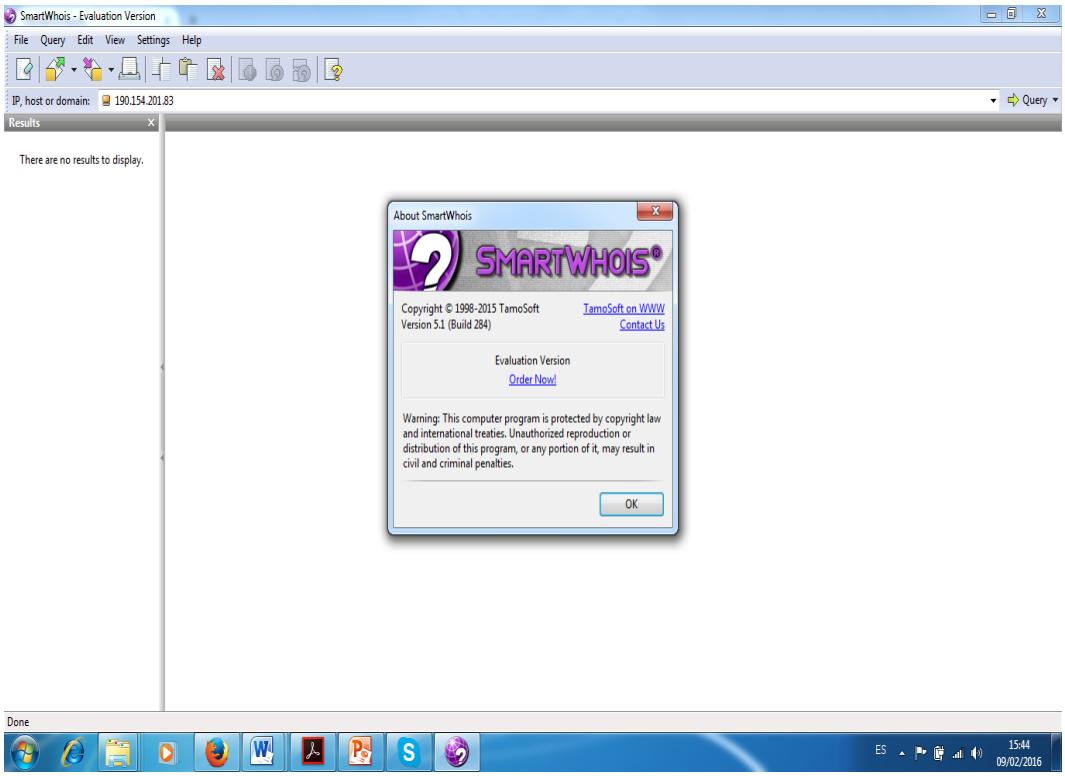

Figura 4 Captura de pantalla SMARTWHOIS

2.3.1.4 Nslookup

Sus siglas significan *"Name System Lookup"*. Es una herramienta de línea de comando que permite consultar un servidor de nombre y obtener información de dicho servidor de tal manera que se pueda diagnosticar algún tipo de problema que pudiera resultar en el DNS. Permite saber si el DNS está resolviendo correctamente las IPs y los nombres. Nslookup es un comando utilizado tanto en Windows como en Unix.

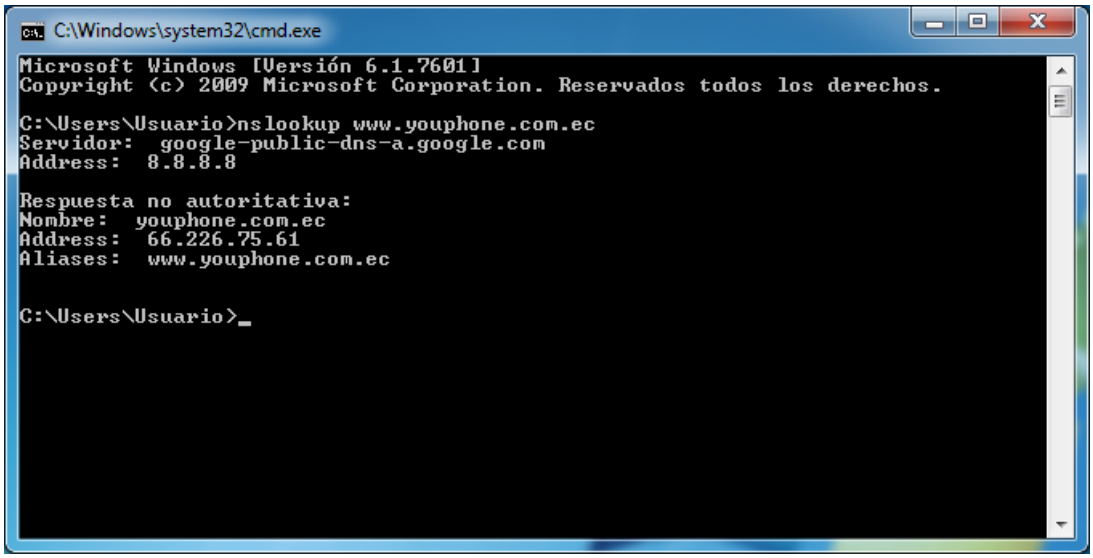

Figura 5 Comando nslookup en DOS

2.3.1.5 Traceroute (CCM, s.f.)

Es una herramienta de diagnóstico de redes, presente en la mayoría de los sistemas operativos. Esta herramienta permite determinar la ruta efectuada por un paquete. El comando Traceroute se puede usar para diagramar un mapa de los routers que se encontraron entre la máquina fuente y la máquina destino. El comando Traceroute difiere según cada sistema operativo.

El resultado de un Traceroute describe los nombres y las direcciones IP de la cadena de routers precedidos con un número secuencial y un tiempo de respuesta mínimo, promedio y máximo.

Por esta razón, Traceroute envía paquetes a un puerto UDP sin privilegios, el cual se cree que no está en uso (puerto 33434 como valor predeterminado), con un TTL configurado en 1. El primer router encontrado eliminará el paquete y enviará un paquete ICMP que incluye la dirección IP del router y la demora del bucle. Luego, el Traceroute aumenta el campo TTL de a 1 por vez para obtener una respuesta de cada router en la ruta, hasta que obtiene la respuesta "puerto ICMP inalcanzable" de la máquina destino.

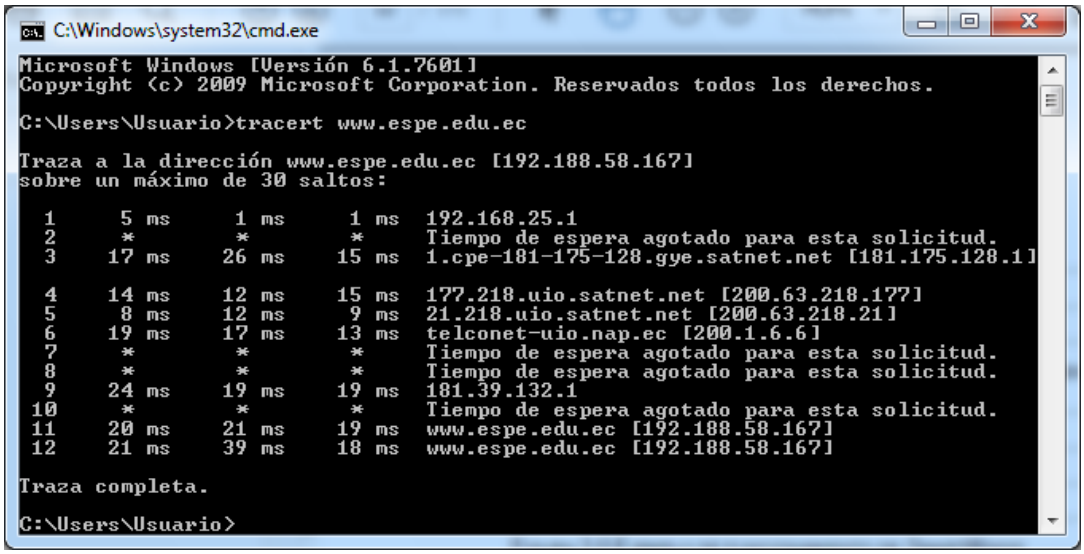

Figura 6 Comando tracert en DOS

En Unix y en Linux la herramienta se llama “traceroute”, mientras que en Windows se llama “tracert”.

Las aplicaciones comerciales de esta herramienta son:

- VisualRoute
- emailTrackerPro

2.3.1.6 VisualRoute

Es una herramienta de diagnóstico y resolución de problemas de redes de información, que ofrece la posibilidad de ver de manera gráfica a través de un mapamundi por donde va viajando la información cuando se recibe o se envía datos desde un ordenador conectado a internet.

Esta herramienta por ser comercial es mucho más completa y eficaz puesto que, procesa todas las direcciones IP’s de forma paralela y no consecutiva (como lo hacen los comandos).

Esta aplicación se considera eficiente porque realiza tareas de otras herramientas tales como:

- Whols
- Traceroute gráfico
- Pruebas de Ping

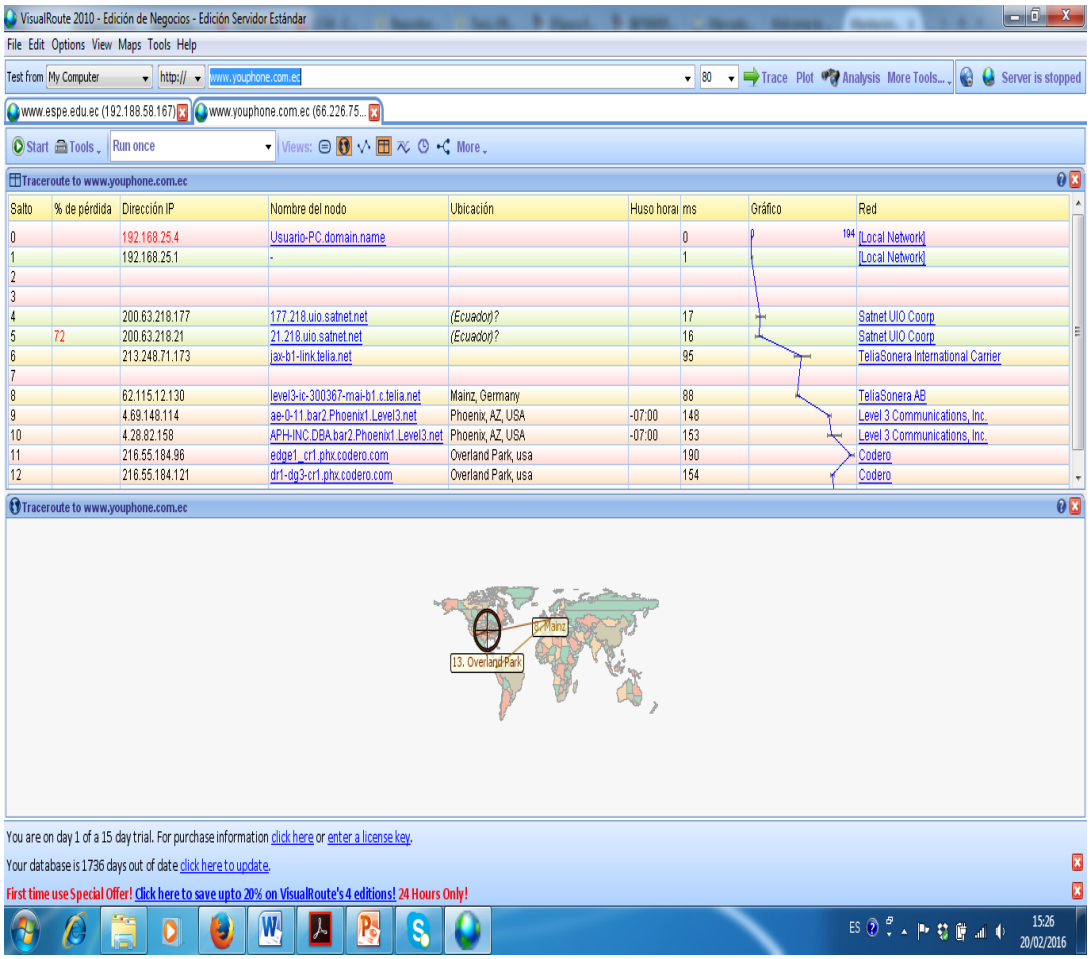

Figura7 Pantalla de VisualRoute

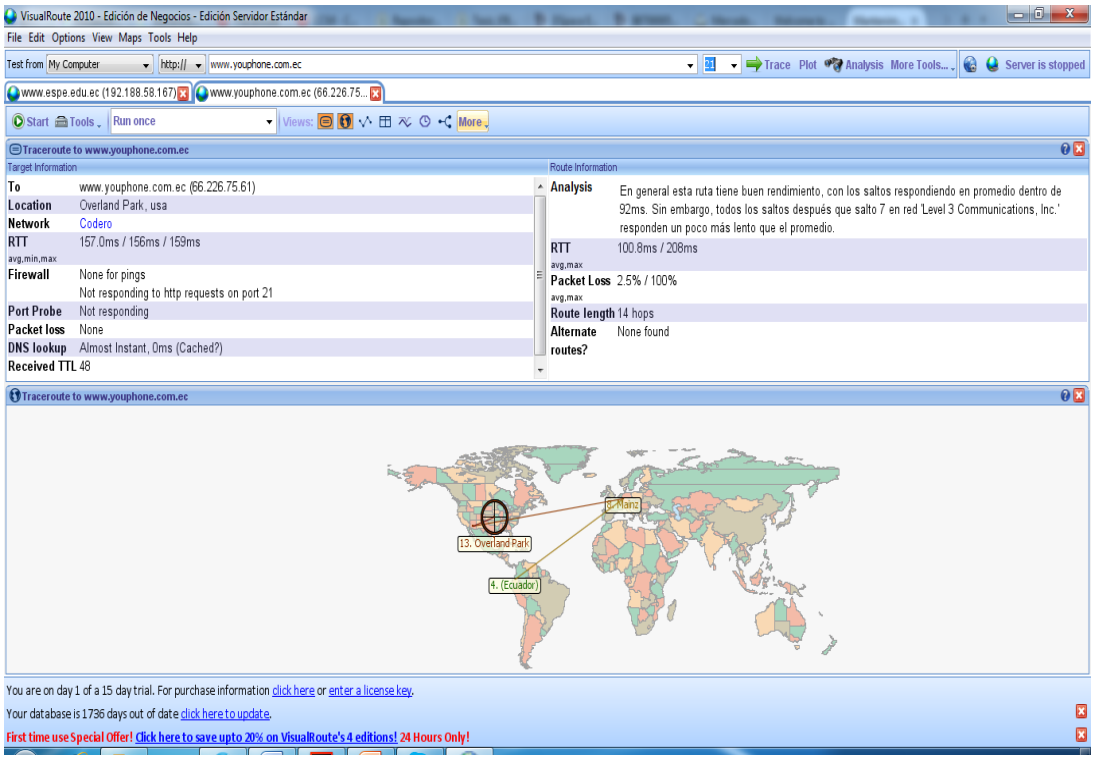

Figura 8 Pantalla de VisualRoute

2.3.1.7 eMailTrackerPro

Es una aplicación que ayuda a identificar la fuente de donde proviene un correo, así como de verificar al emisor del mensaje y rastrear el mismo para reportar los posibles correos sospechosos o spam. Analiza los encabezados de los mails que se reciben dando como resultado la dirección IP de dónde se envía el correo como su localización geográfica.

Otro adicional que tiene esta herramienta es que trabaja con Microsoft Outlook, además detecta tácticas de ocultamiento de direcciones de personas o equipos, una táctica muy utilizada por los famosos “spams”.

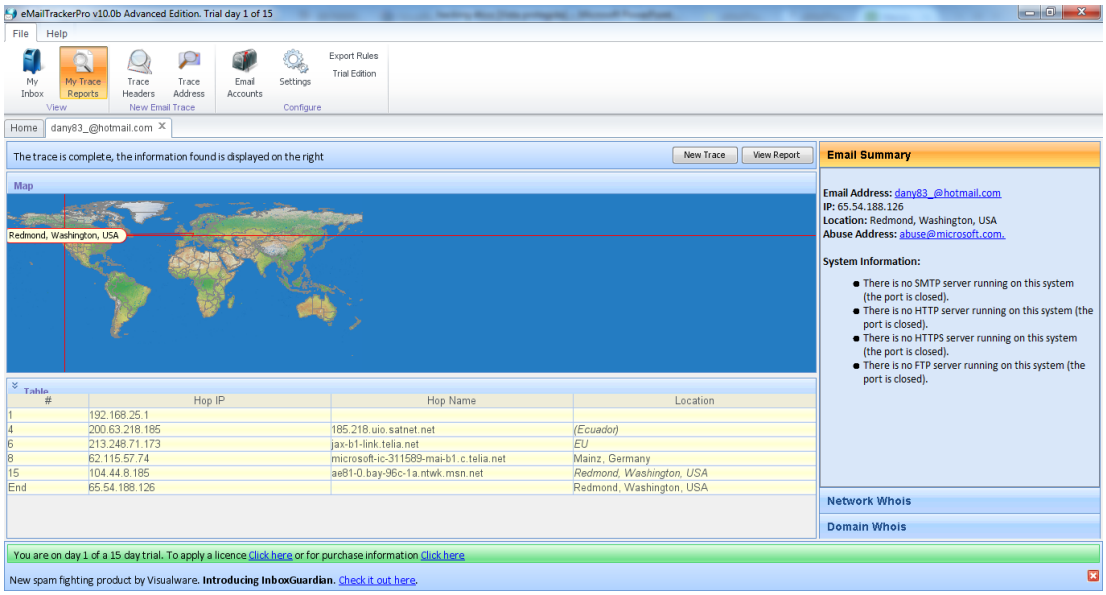

Figura 8 Pantalla EmailTrackerPro

2.3.1.8 Maltego

Es una herramienta que permite recabar datos sobre una organización de forma sencilla, a través del uso de objetos gráficos y menús contextuales que permiten aplicar “transformaciones” a dichos objetos, a través de las cuales se obtiene a su vez mayor información. (Astudillo, 2013)

La herramienta funciona de la siguiente manera:

- Maltego envía la petición a los servidores de semillas en formato XML a través de HTTPS.
- La petición del servidor de la semilla se da a los servidores TAS que se transmiten a los proveedores de servicios.
- Los resultados se envían al cliente Maltego. (We Live Security, 2016)

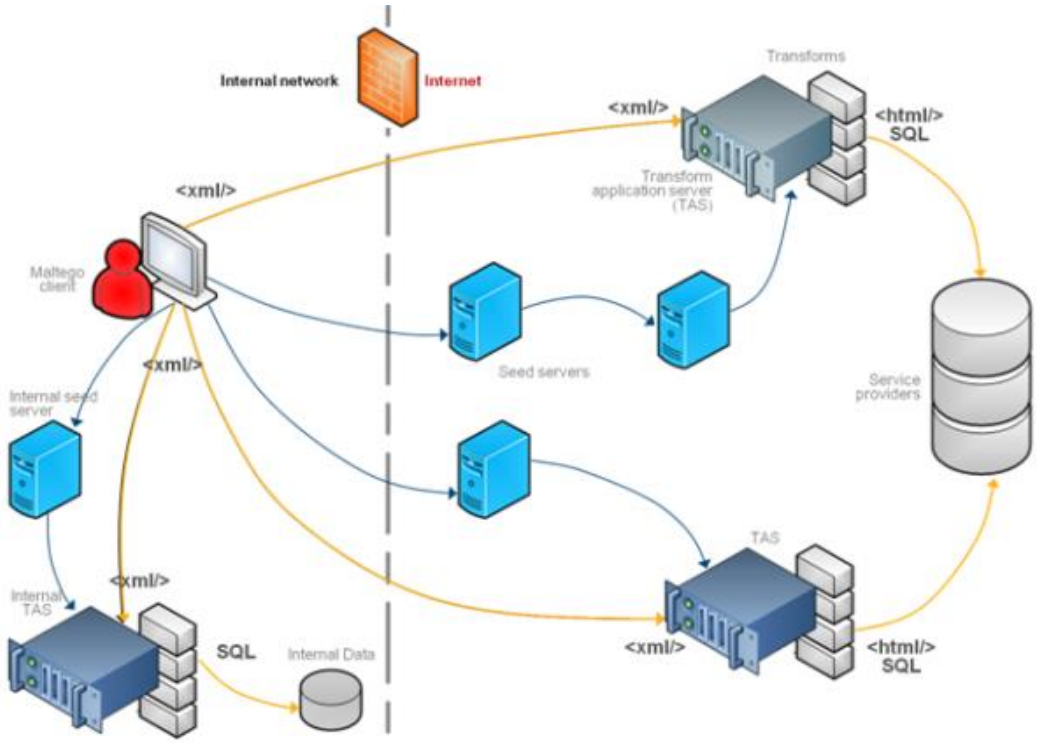

Figura 9 Esquema de funcionamiento de Maltego (We Live Security, 2016)

2.3.2 Herramientas de Exploración (Scanning)

En la fase anterior se recopila la mayor información posible sobre el objetivo deseado, el siguiente paso “Scanning” o exploración consiste en identificar los equipos o host que están activos a través de las IP’s que previamente se han encontrado en el paso anterior. Básicamente esta fase consiste en determinar puertos abiertos en los equipos que están activos y si se logra tener éxito se puede determinar el sistema operativo con el que trabaja dicho equipo y las aplicaciones o servicios que escuchan requerimientos en dichos puertos.

A continuación se detalla algunas herramientas que pueden ser útiles en esta fase.

2.3.2.1 Ping (CCM, s.f.)

Ping (forma abreviada de Packet Internet Groper) es la herramienta de administración de redes más conocida. Es una de las herramientas más simples ya que todo lo que hace es enviar paquetes para verificar si una máquina remota está respondiendo y, por ende, si es accesible a través de la red.

La herramienta ping permite de esta manera diagnosticar la conectividad a la red mediante comandos del tipo:

ping nombre.del.equipo

“nombre.del.equipo” representa la dirección IP de la máquina, o su nombre. Por lo general, se recomienda hacer una prueba usando la dirección IP de la máquina en primer lugar.

Ping depende del protocolo ICMP, el cual permite diagnosticar las condiciones de transmisión.

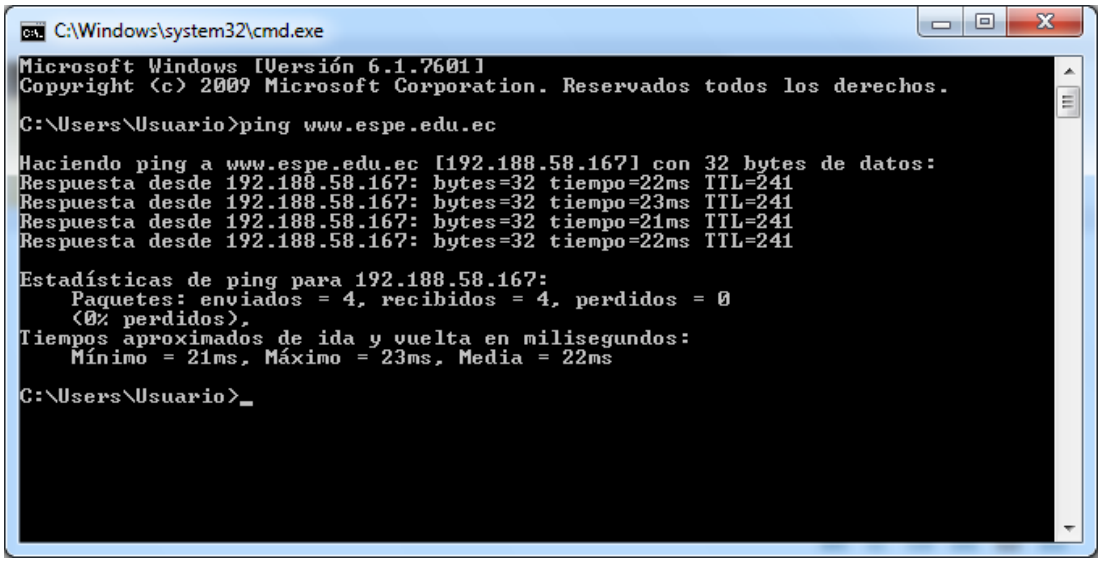

Figura10 Comando Ping www.espe.edu.ec

2.3.2.2 Pinger

Este programa en un archivo de texto llamado host.txt, en él se escriben las direcciones IP's, nombres de equipo o host a los cuales se quiere hacer la prueba y muestra los resultados como se muestra en las siguientes figuras.

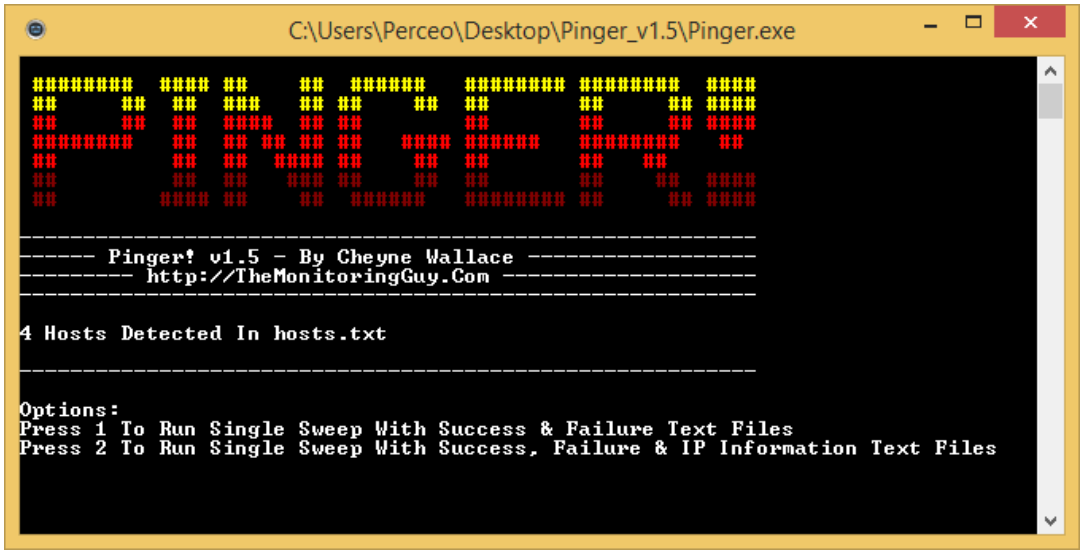

Figura 11 Pantalla Principal de aplicativo Pinger

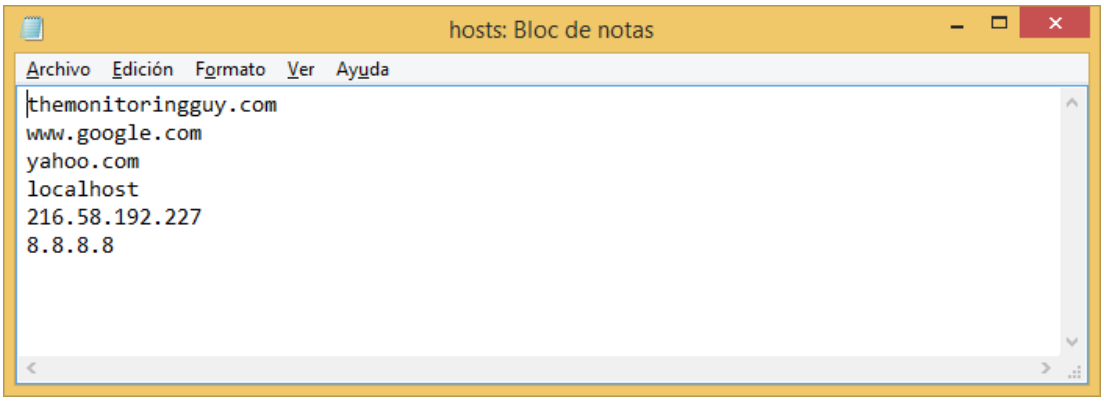

Figura 12 Contenido de archivo host.txt

Los resultados de este aplicativo son muy visuales, en verde se ven los equipos a los cuales el host dio positivo y en rojo cuando no se tuvo una respuesta, tal como se muestra en la figura de a continuación:

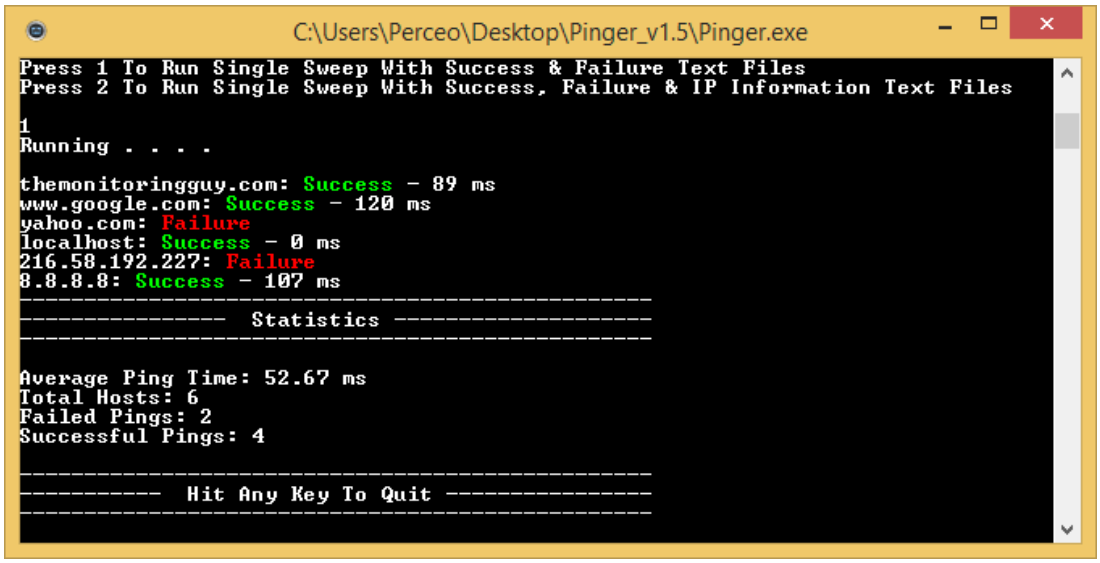

Figura13 Resultado de Pinger

2.3.2.3 Advanced IP Scanner

Este programa es el más común en internet, lo que hace es verificar las máquinas activas con su dirección IP y mostrar en una lista las que están

online, la pantalla es muy fácil de entender, reconoce la red en la que se encuentra, como por ejemplo 192.168.25.1

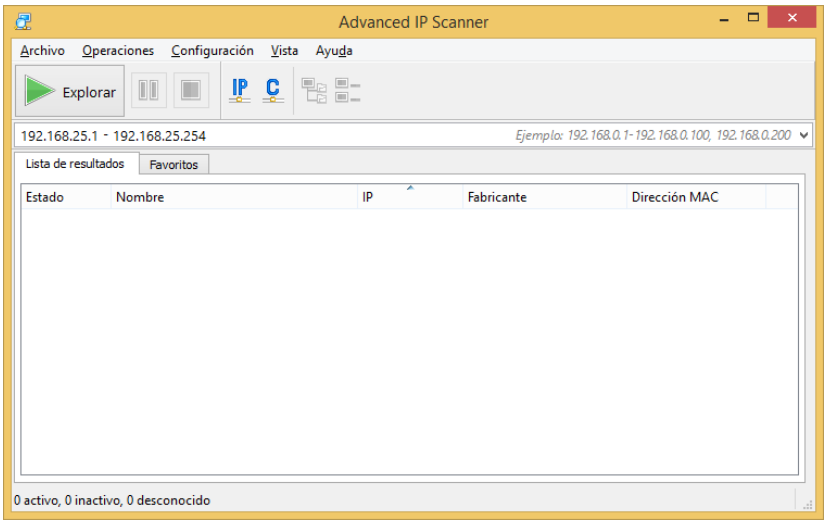

Figura 14 Pantalla Principal de Advanced IP Escanner

La siguiente figura muestra los resultados encontrados al realizar un escaneo en la red, dando como resultado 3 equipos detallados a continuación.

- 192.168.25.1 192.168.25.1
- JRONATE 192.168.25.5
- 192.168.25.7 192.168.25.7

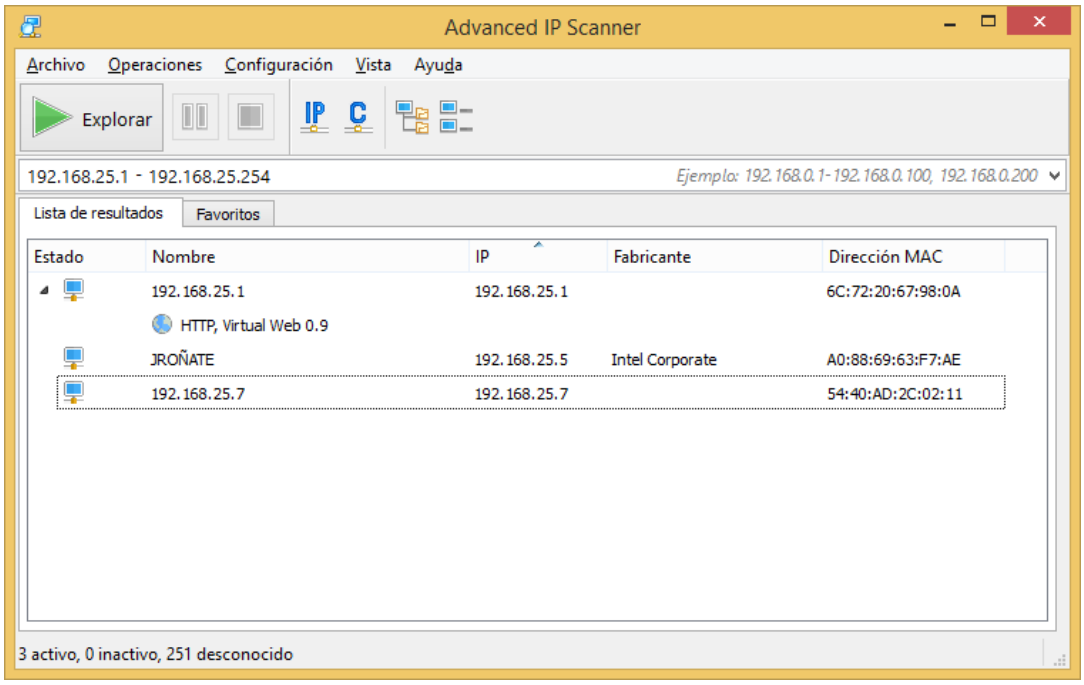

Figura 15 Resultados de Escaneo de Puertos

2.3.2.4 Super Scan

Esta es una herramienta importante para poder recabar información de las maquinas activas en la red, además tiene varias opciones para desde el mismo programa hacer ping, hacer traceroute, whois entre otras como lo muestra en la figura.

Una de las primeras opciones que se tiene en este aplicativo es hacer un escaneo de todas las máquinas de la red, tal como se muestra en la figura.

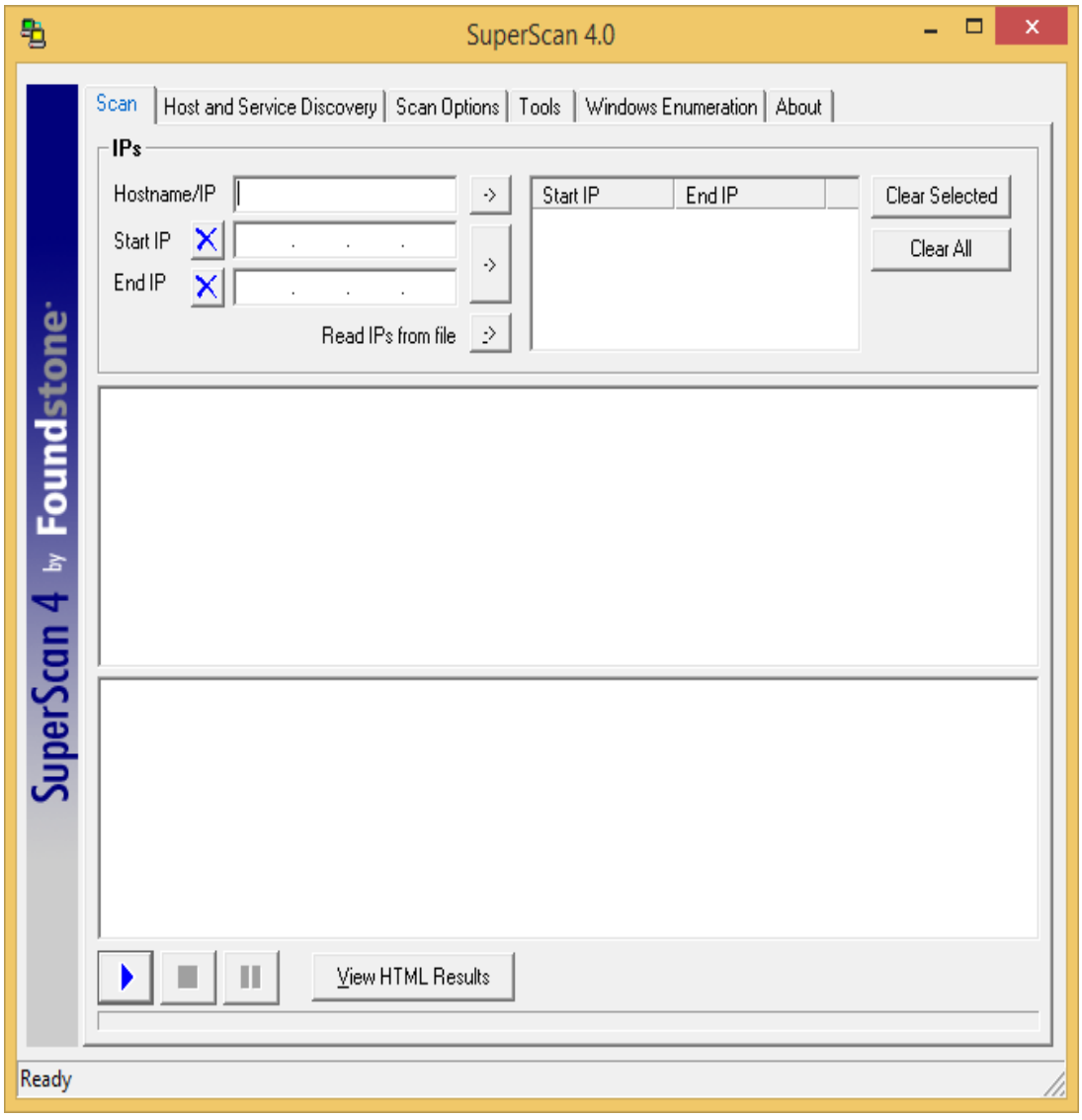

Figura 16 Interfaz de usuario de SuperScan

Los resultados se encuentran obtenidos en un formato visual y se pueden copiar a un texto para su análisis respectivo posterior. Esto puede verse en la figura 17.

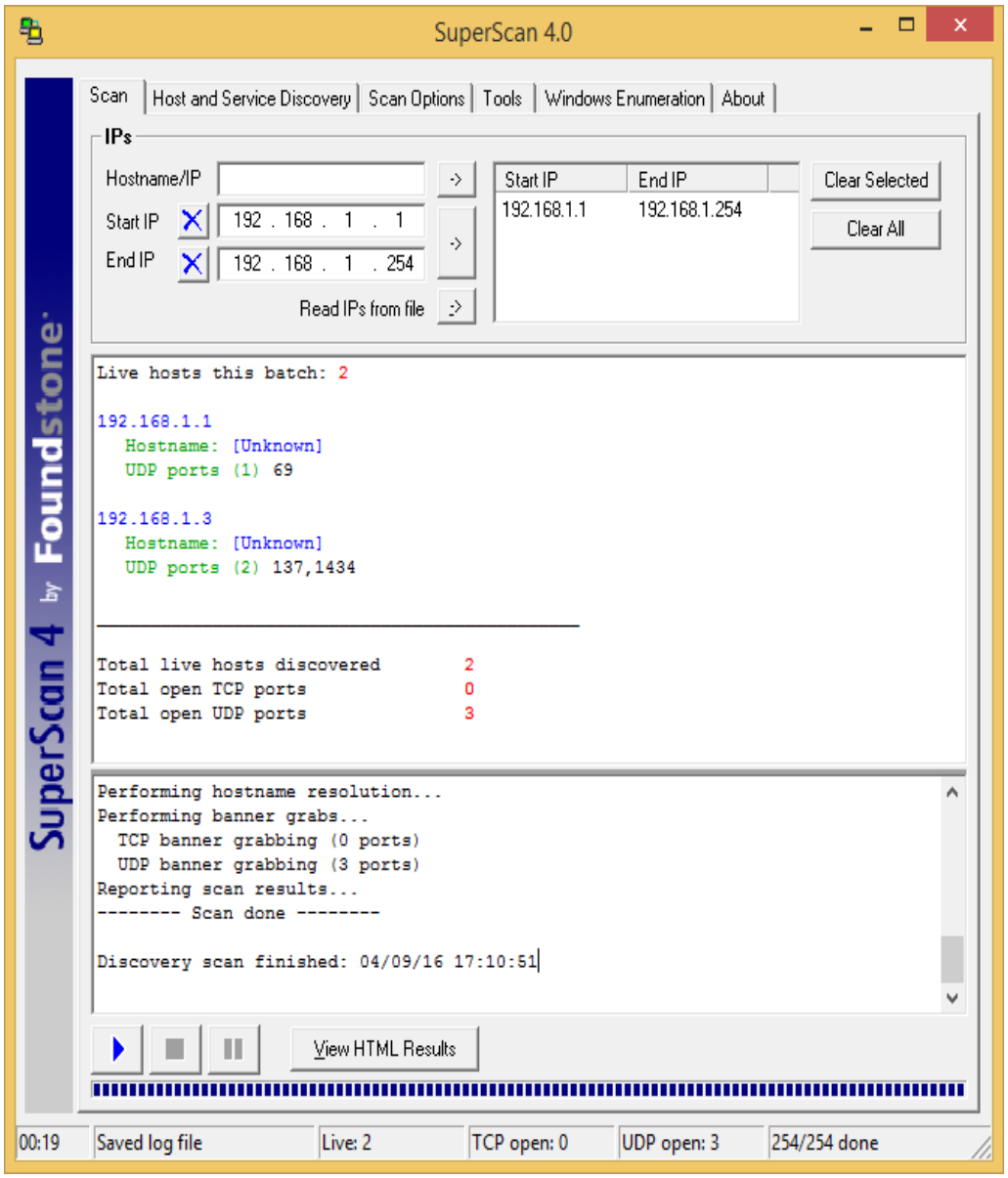

Figura 17 Resultados Obtenidos haciendo Pruebas de Escaneo

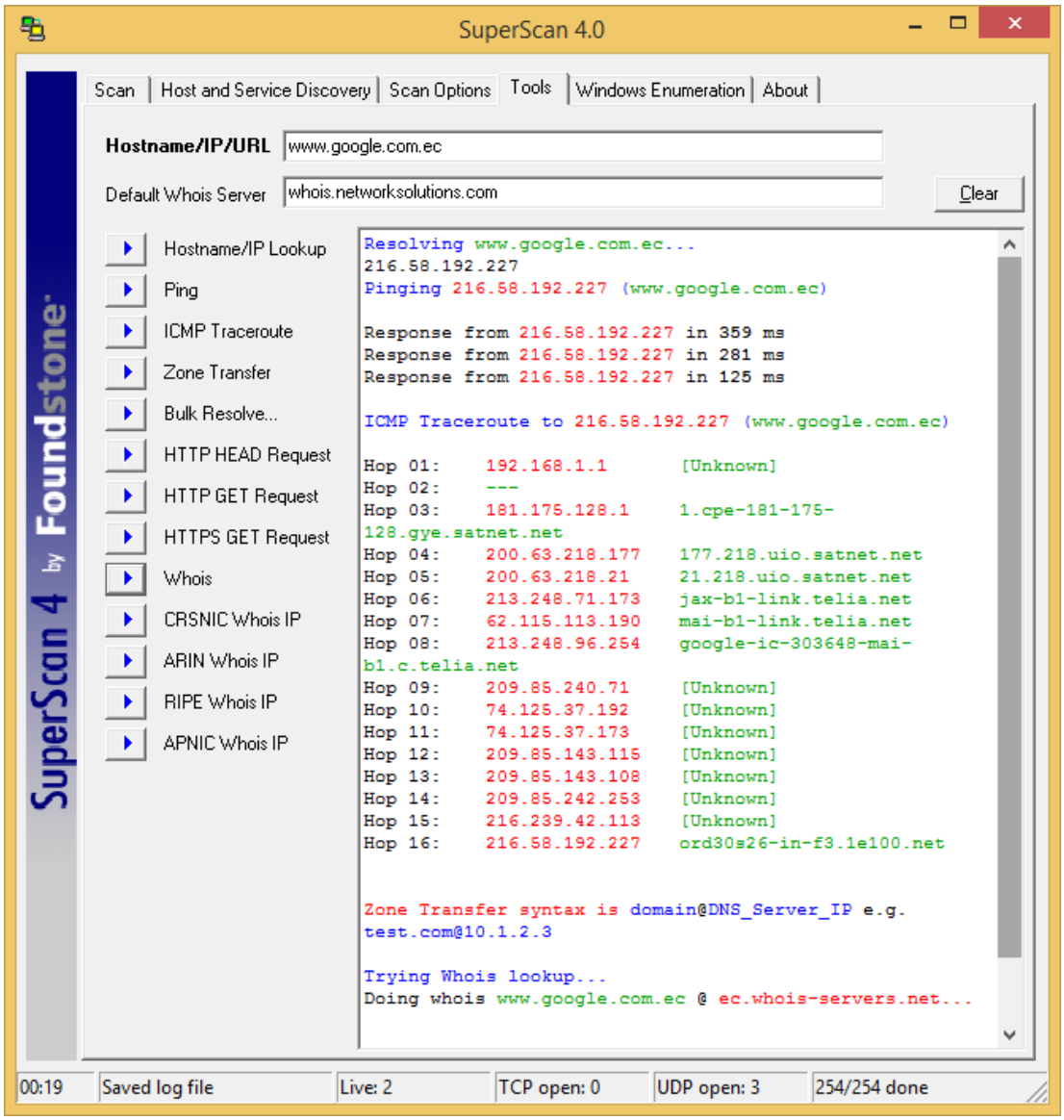

Figura18 Herramientas adicionales de Super Scan

2.3.2.5 Zenmap – nmap

"Es la interfaz gráfica oficial de Nmap, el conocido programa de código abierto para hacer escaneo de puertos a fondo de cualquier equipo conectado. Zenmap proporciona una interfaz gráfica para ejecutar los diferentes tipos de análisis de puertos que tiene Nmap y también para mostrarlos de forma intuitiva a los usuarios menos experimentados" (Redes @ Zone, 2016)

Nmap es un programa de código abierto que sirve para efectuar rastreo de puertos que se encuentra actualmente a cargo de una comunidad. Fue creado para Linux en un principio pero en la actualidad es multiplataforma. Se usa para evaluar la seguridad de sistemas informáticos, descubrir servicios o servidores en una red informática

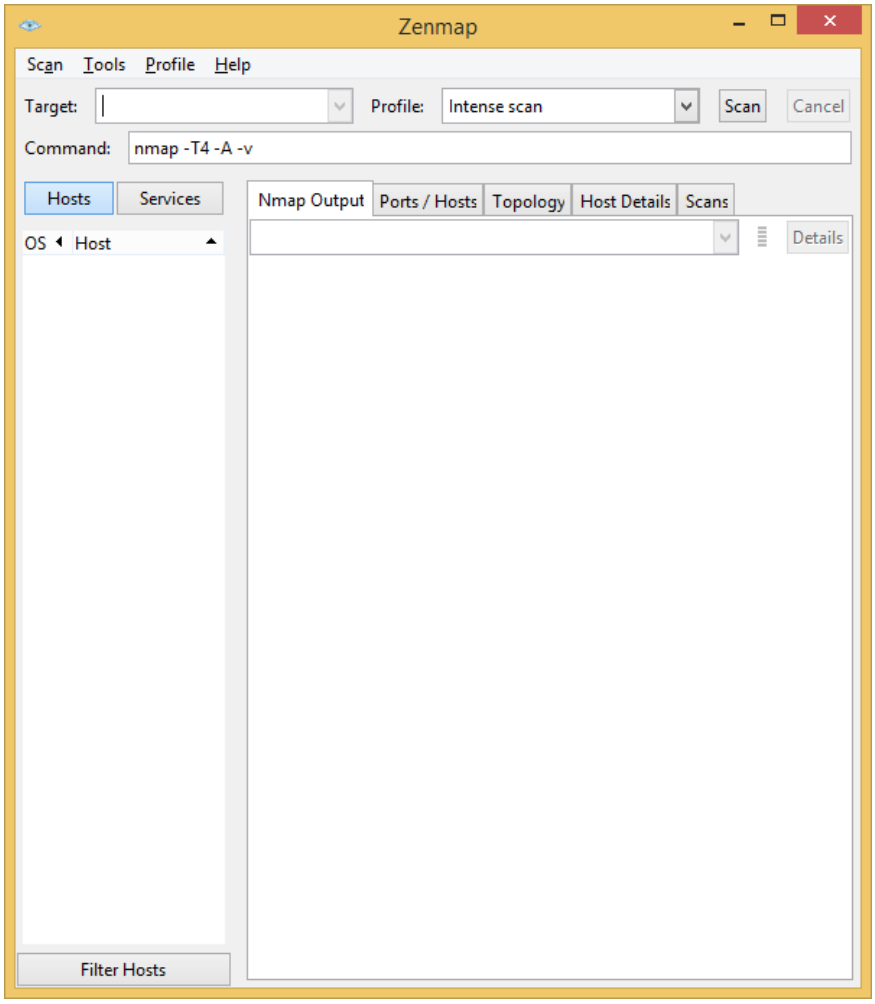

Figura 19 Pantalla principal Zenmap

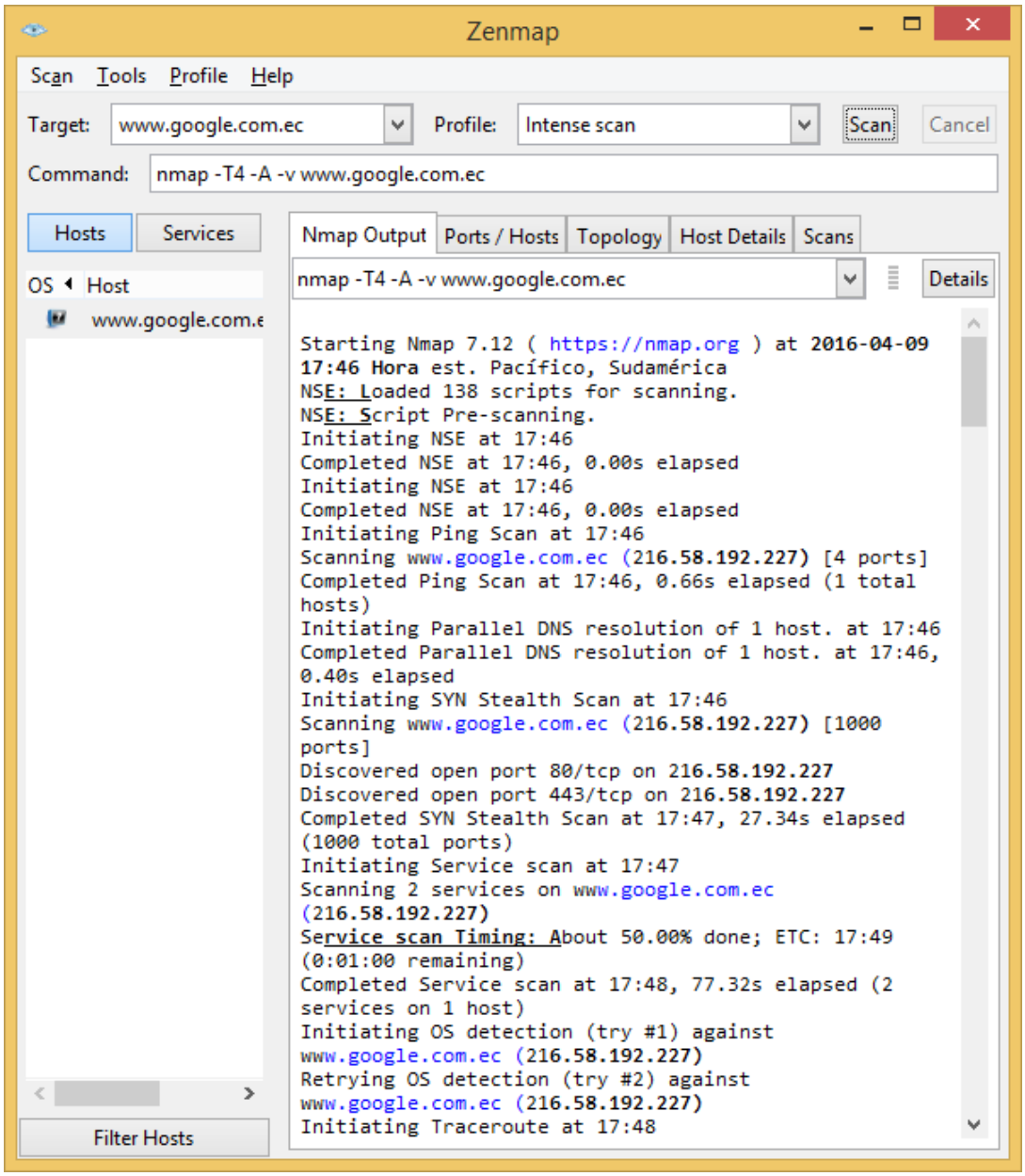

Figura 20 Ejemplo de Zenmap a www.google.com.ec

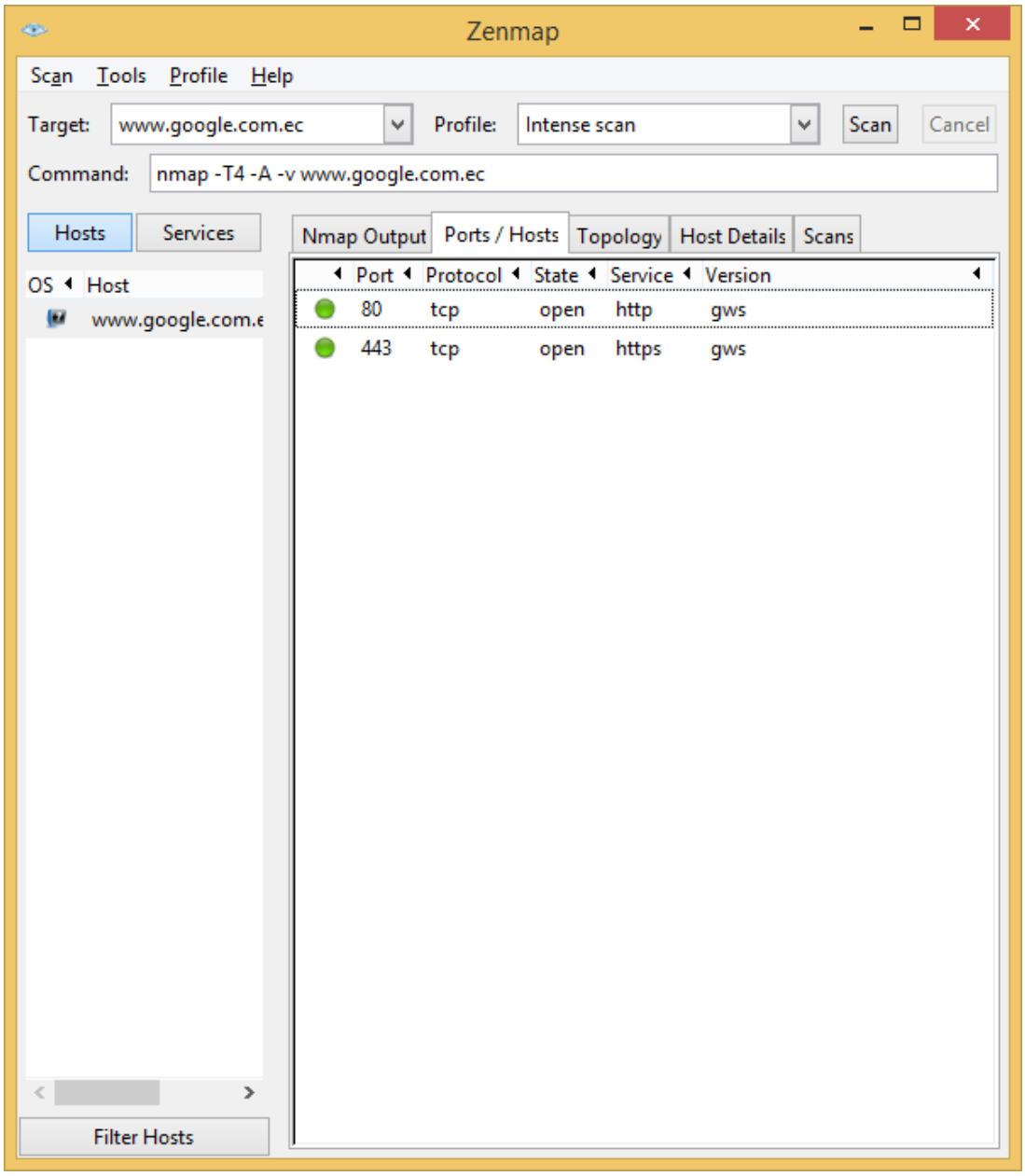

Figura 21 Escaneo de puertos a www.google.com.ec

2.3.2.6 Angry IP Scanner

Es una herramienta de escaneo de red de código abierto que permite de manera fácil escanear direcciones IP's, puertos, etc.

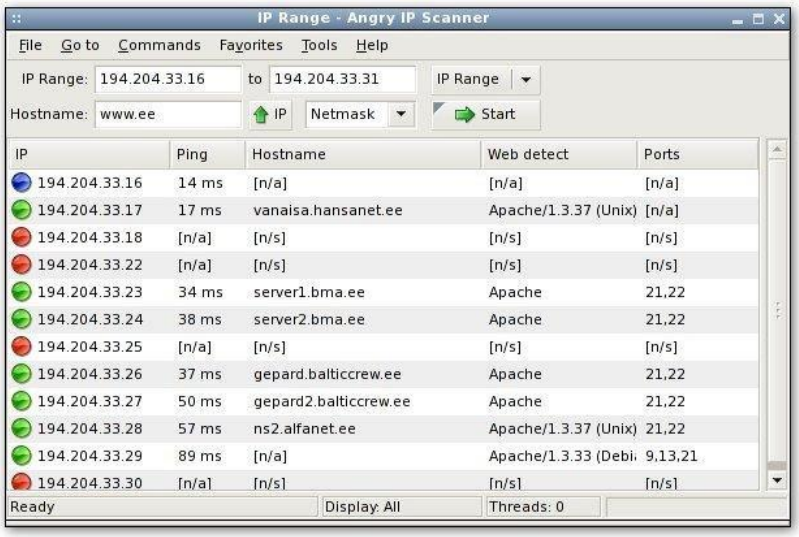

Figura 22 Escaneo de IP's Angry IP Scanner

2.3.2.7 Network Security Auditor

Es un software de auditoría de redes, que permite hacer escaneo de puertos, posee herramientas más especializadas y ofrece resultados gráficos. Es un programa pagado, sin embargo se puede usar por un mes de forma gratuita.

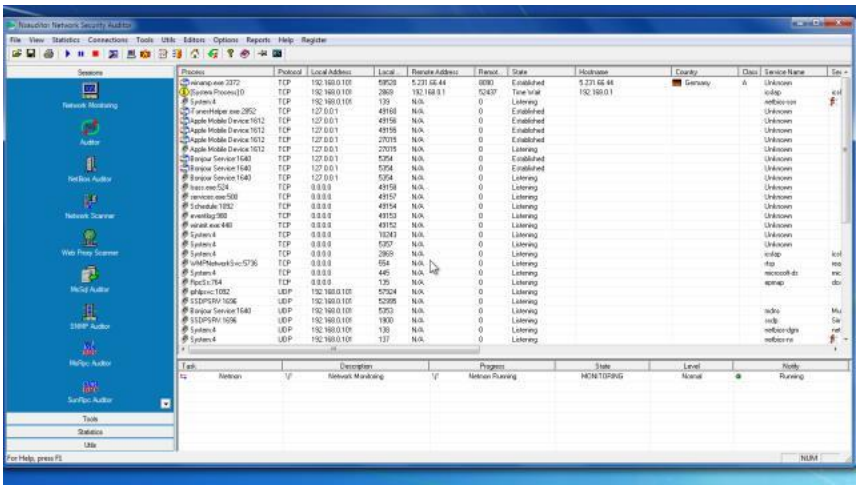

Figura 23 Pantalla del Network Security Auditor

2.3.2.8 Metaesploit

Es una herramienta de red portátil que permite encontrar vulnerabilidades a través de escaneo de puertos y comando específicos para explotar la vulnerabilidad encontrada. Esta herramienta nació de un proyecto del mismo nombre y es abierta

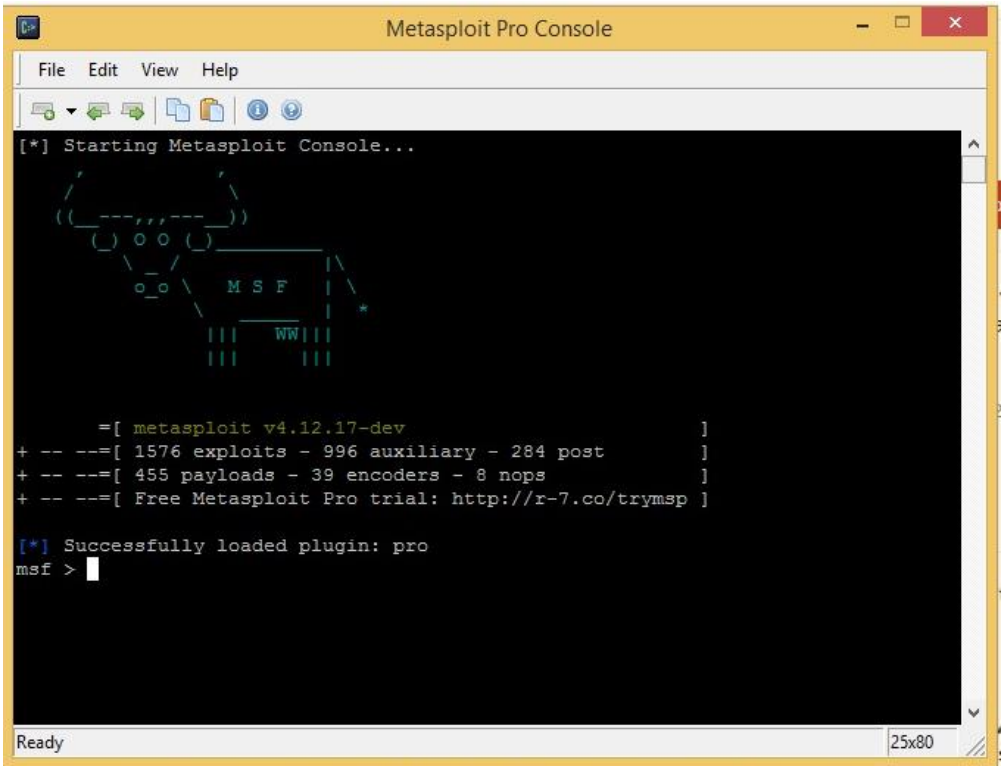

Figura 24 Instalación de metaesploit

2.3.3 Herramientas de Enumeración o gaining Access

La enumeración o Gaining Access se considera una subfase del Scanning, ya que en esta instancia se reúne la mayor información posible de la víctima, aprovechando una debilidad ya sea en los protocolos o en los servicios activos que se han detectado previamente.

A continuación se detalla algunas aplicaciones que pueden ser útiles en esta fase.

2.3.3.1 GetAcct

Esta aplicación le pertenece a la empresa *"Security Friday",* tiene una interfaz gráfica sencilla y los informes son presentados en formatos delimitados por comas (.cvs).

Esta aplicación permite obtener información privilegiada acerca de todas las cuentas de usuario en los equipos que utilizan el sistema operativo Windows. Para obtener esta información, solamente es necesario ingresar la dirección IP del equipo remoto, el RID2 final, y presionar el botón "Get Account".

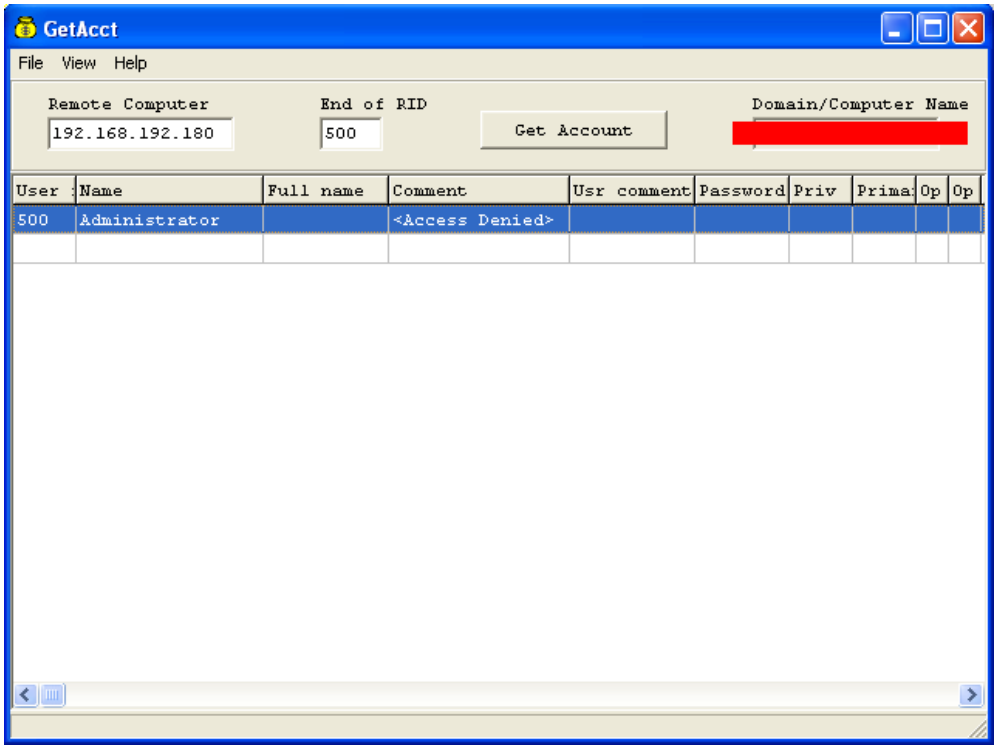

Figura 25 Pantalla GetAcct

2.3.3.2 DumpSec y Hyena

Estos aplicativos ofrecen opciones como:

- Listar usuarios
- Grupos
- Servicios
- Sesiones

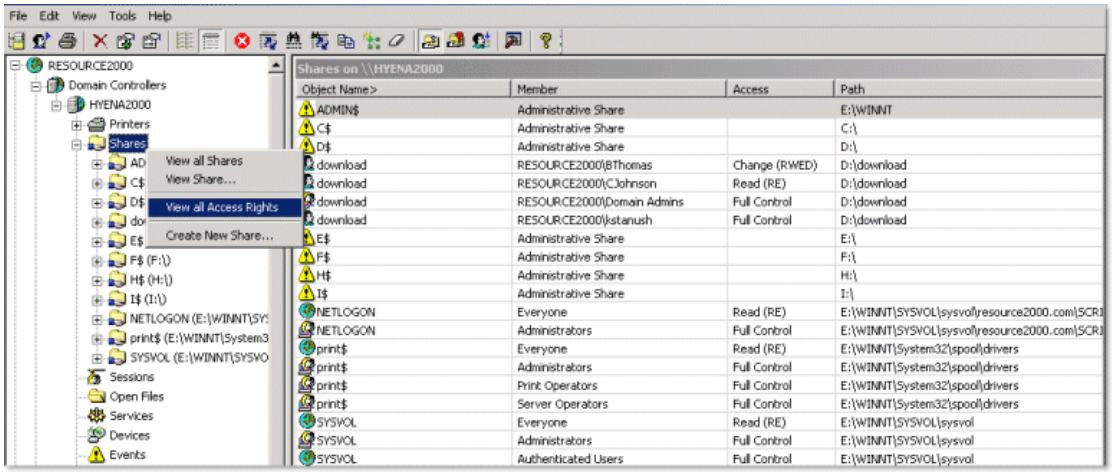

Figura 26 Pantalla de Hyena

2.3.3.3 LANguard Network Scanner

Es un programa que permite analizar una red LAN e identificar posibles agujeros de seguridad y caballos de Troya. Su analizador de puertos puede comprobar si existe alguna aplicación no autorizada ejecutándose en un sistema, examinar puertos de firewall, telnet y proxy, comprobar los accesos al router, ejecutar controles básicos de seguridad, etc.

LanGuard Network Scanner proporciona información NETBIOS sobre cada ordenador: nombre de host, sesión de usuario, datos compartidos, entre otras.

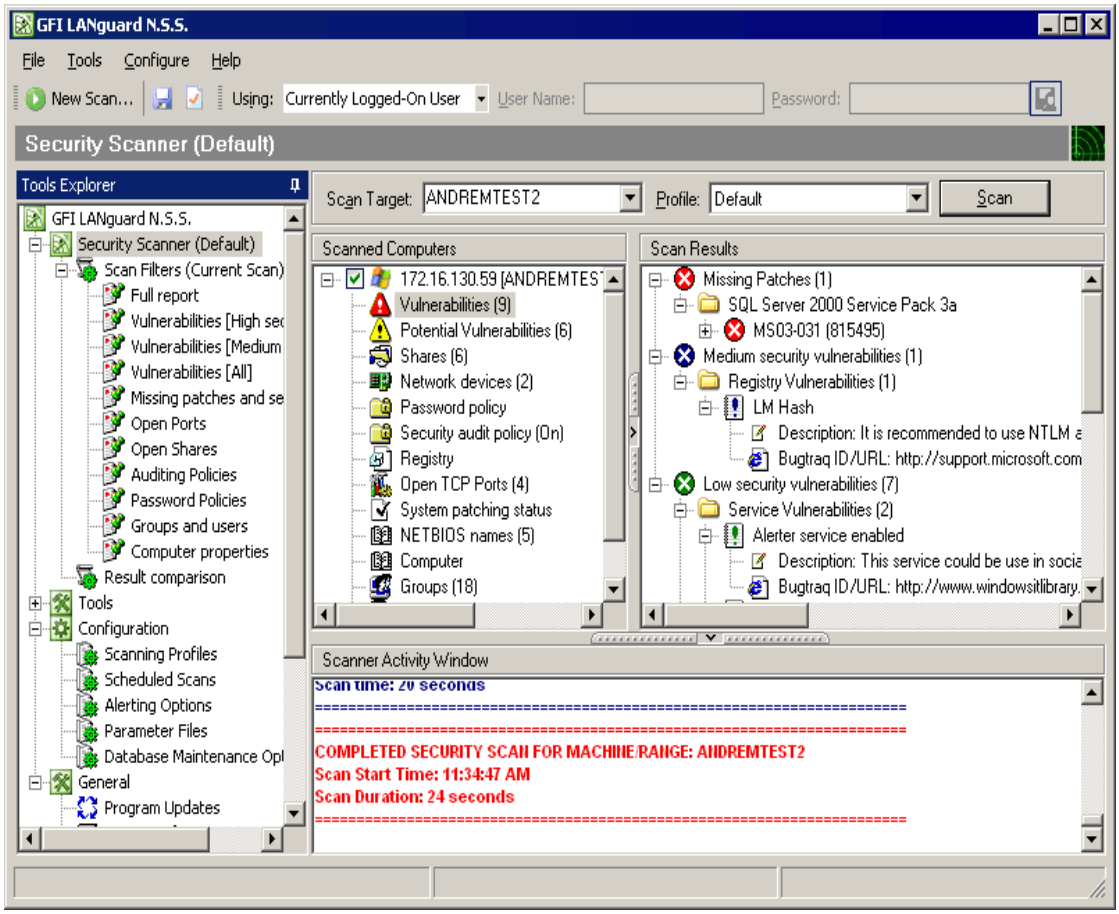

Figura 27 Pantalla LANGuard Network Scanner

2.3.3.4 WireShark

Es una herramienta para realizar sniffing (captura y análisis de tráfico) en una red de datos, es utilizado principalmente para localizar averías, análisis, etc.

Funciona en las plataformas actuales, incluyendo Unix, Linux, y Windows.

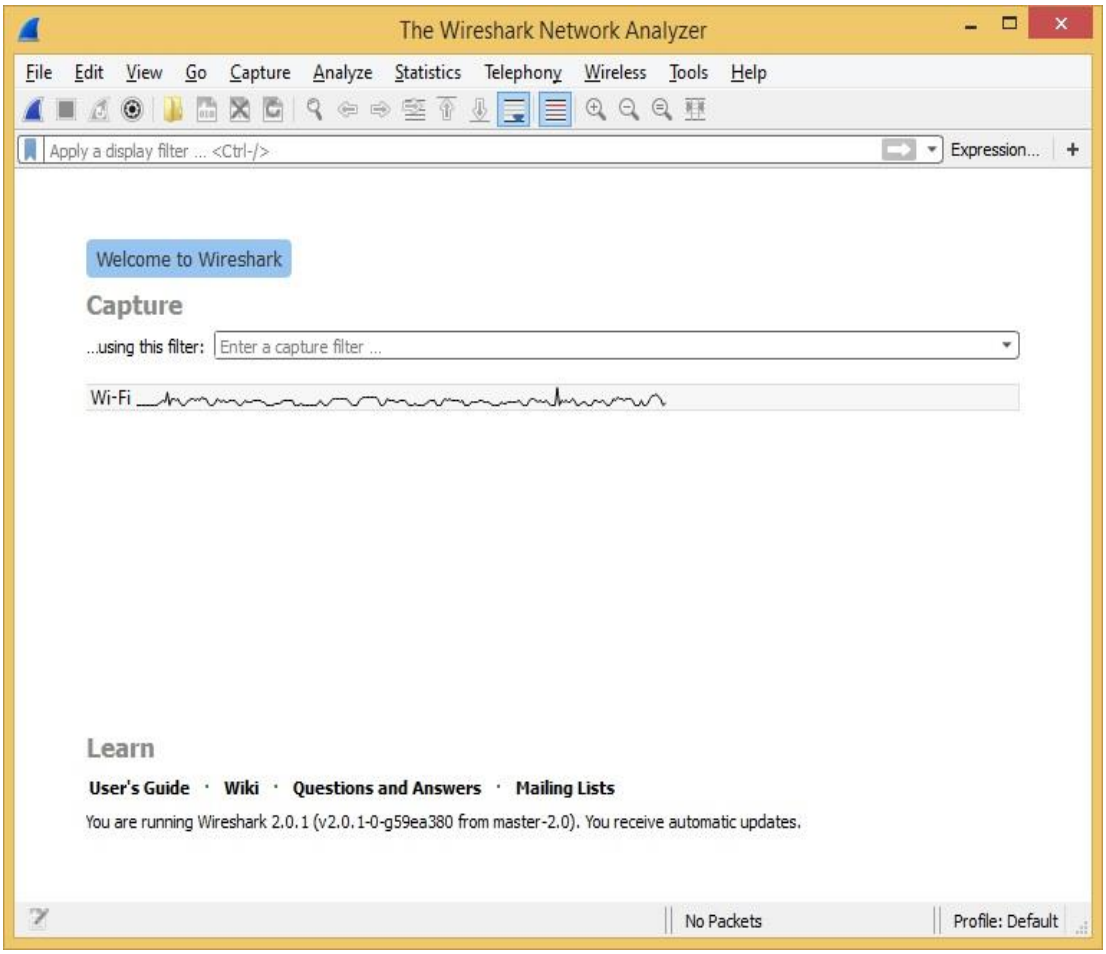

Figura 28 Programa Wireshark

2.3.3.5 Nessus

Es un programa completo de escaneo de vulnerabilidades. Consiste en un en un programa residente (demonio o daemon), que realiza el escaneo en el sistema. Se muestra el avance e informa sobre el estado de los escaneos de manera gráfica.

Utiliza nmap para buscar puertos abiertos y después intentar varios exploits para atacarlo.

Nessus realiza algunas de las pruebas de vulnerabilidades, las mismas que pueden causar que los servicios o sistemas operativos se corrompan y caigan, sin embargo el usuario puede evitar esto desactivando esta opción.

Esta herramienta es pagada, a pesar de ello se puede utilizar el programa de manera gratuita por un tiempo.

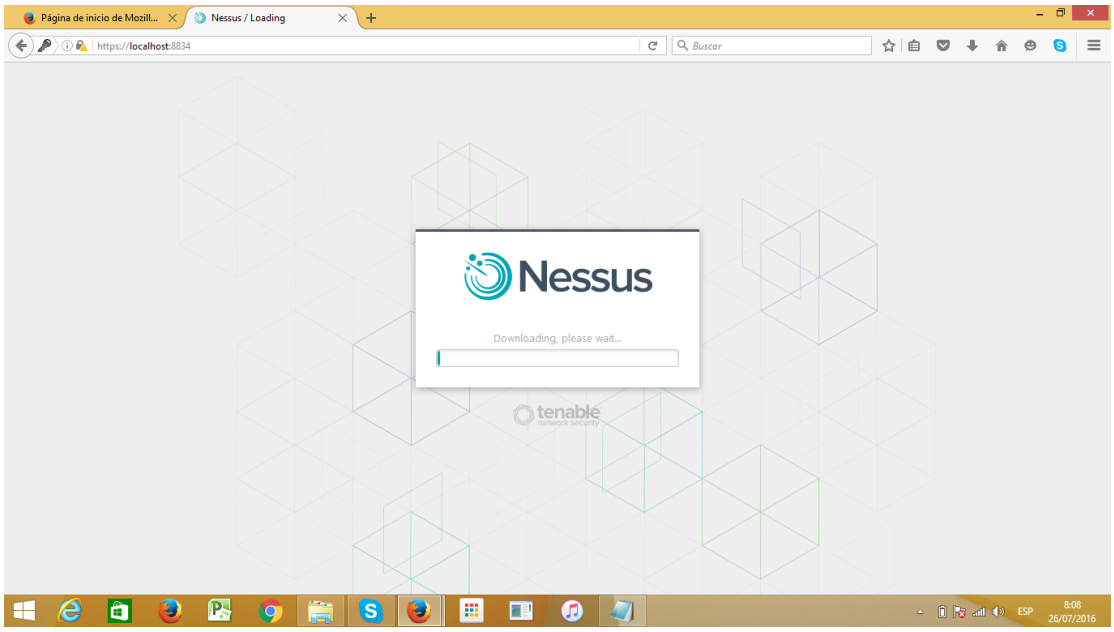

Figura 29 Ventana de instalación del programa Nessus

CAPÍTULO 3. DIAGNÓSTICO DE VULNERABILIDADES

Youphone CIA LTA es un distribuidor autorizado de Telefónica Movistar que se dedica a la venta de equipos celulares y tablets, así como a la venta de planes telefónicos prepagos y postpagos cuya misión es ser una empresa líder en este tipo de ventas y su visión está encaminada en consolidar su liderazgo expandiendo sus locales de ventas y brindado siempre un servicio de calidad.

Cuenta actualmente con tres locales de venta: un local en el centro comercial “El Condado” y dos locales en el centro comercial “Iñaquito CCI”, siendo el más grande, aquel que se encuentra ubicado en el Condado.

3.1 Análisis de la Situación Actual

Se realiza una inspección física a las instalaciones de la empresa, se comprueban los equipos informáticos que la organización posee para determinar cuáles de ellos son susceptibles de auditar.

3.1.1 Diagrama de red

Un diagrama de re muestra la manera en que los equipos se encuentran conectados y comunicados en la empresa. Como se mencionó anteriormente existen 3 locales, por lo cual se realiza 3 diagramas de red (Una por cada local) y finalmente un diagrama de cómo se encuentran conectados todos los locales

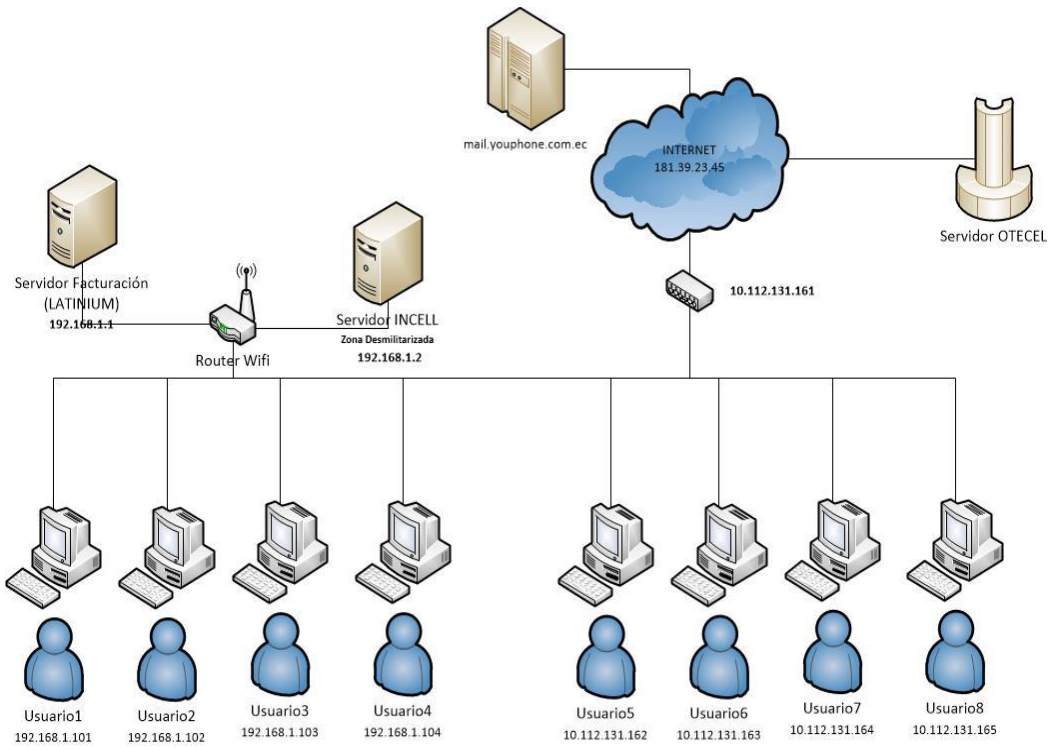

Figura 30 Diagrama de Red Youphone CAVS "Condado Shopping"

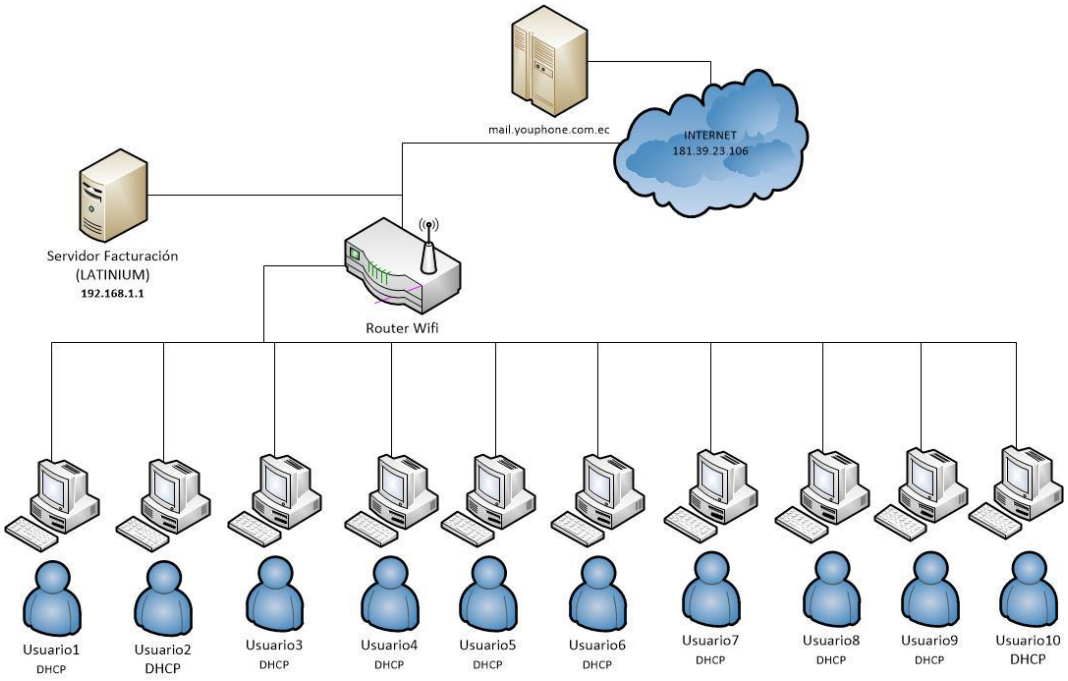

Figura 31 Diagrama de Red Youphone CAVS CCI

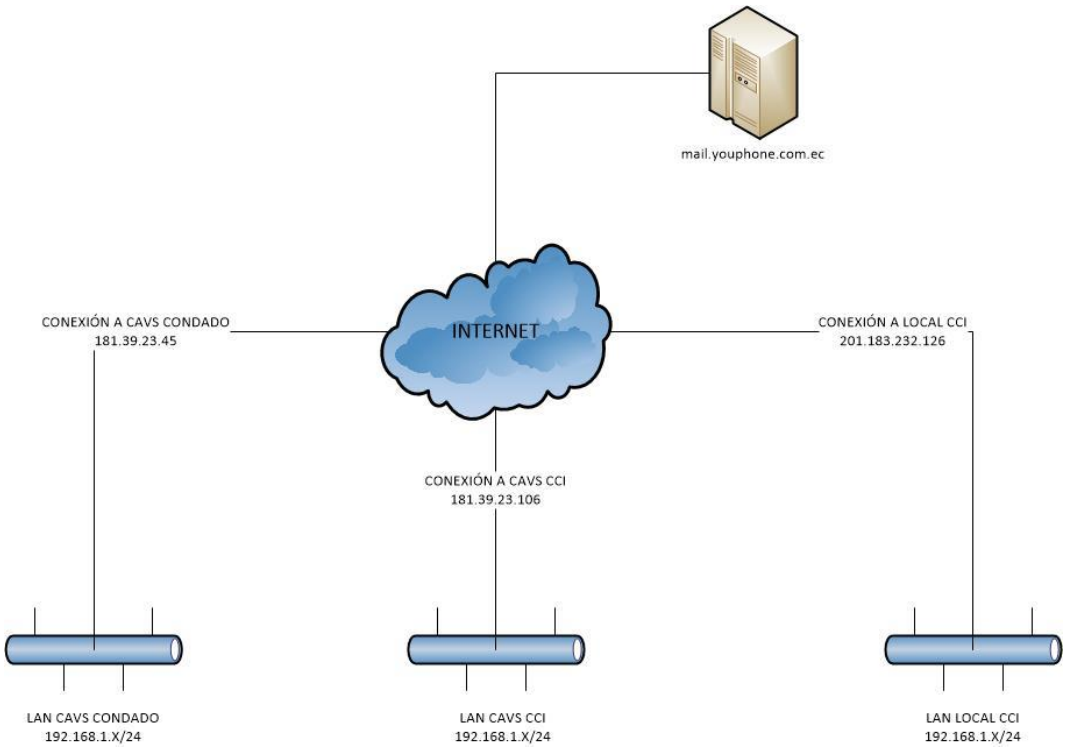

Figura32 Diagrama General de Red Youphone Cia. Ltda.

3.1.2 Levantamiento de Información

Se procede a hacer un inventario de los equipos informáticos de la empresa, detallando las características de software y hardware.

3.1.2.1 Equipos de Conexión

Los equipos activos que permiten conectar de la red de datos de Youphone Cia. Ltda. son los siguientes:

Tabla 1
Descripción de los equipos de conectividad y su respectiva dirección IP

	EQUIPOS	MARCA	MODELO	DIRECCION IP	USO
CAVS CONDADO	ROUTER	TPLINK	EL6120	192.168.1.210	CONEXIÓN A INTERNET
	SWITCH	DLINK	DES2014	-	CONEXIÓN DE EQUIPOS
	SWITCH	CISCO	XXXXX	192.168.25.1	ENLACE INTERNET-TELEFONIA
	ROUTER	TPLINK	XXXXX	192.168.25.1	ENLACE A TELEFONICA
CAVS CCI	ROUTER	NEXXT	XXXXXX	192.168.1.200	CONEXIÓN A INTERNET
	SWITCH	3COM	BASELINE 1016	-	CONEXIÓN DE EQUIPOS
	ROUTER	TPLINK	XXXXX	-	ENLACE A TELEFONICA
LOCAL CCI	ROUTER	TPLINK	WR741N v1/v2	192.168.1.1	CONEXIÓN A INTERNET

Equipos Computacionales (Computadoras)

A continuación se presenta una breve descripción de las computadoras de la empresa incluida la dirección IP que se ha asignado a cada equipo así como a la red y el grupo al que pertenecen.

Local o CAVS Condado

En este local, se encuentra en el centro comercial “Condado Shopping” y cuenta con 23 computadoras de usuario, detalladas a continuación:

Tabla 2
Características Computadora I-FLOW (Condado)

ETIQUETA	I-FLOW
SISTEMA OPERATIVO	Windows 7 Ultimate x32
PROCESADOR	Intel Pentium D 2,8 GHz
RAM	1 GB
DISCO	150 GB C: 97,5 GB D: 55 GB
NOMBRE	DISTRIUIDUIOYPN54
NOMBRE COMPLETO	DISTRIUIDUIOYPN54.otecel.com.ec
RED	IP: 10.112.131.165 MASK: 255.255.255.240 GATEWAY: 10.112.131.161

Tabla 3
Características Computadora Modulo 2 (Condado)

ETIQUETA	Modulo 2
SISTEMA OPERATIVO	Windows 7 Ultimate x32
PROCESADOR	Intel Core i5 3 GHz
RAM	4 GB
DISCO	500 GB C: 300 GB D: 200 GB
NOMBRE	DISTRIUIDUIOYOU73
NOMBRE COMPLETO	DISTRIUIDUIOYOU73.otecel.com.ec
RED	IP: 10.112.133.226 MASK: 255.255.255.224 GATEWAY: 10.112.133.238 IP: 192.168.1.96 MASK: 255.255.255.0 DNS PREFERIDO: 10.112.157.49 DNS ALTERNO: 10.112.157.48

Tabla 4
Características Computadora DIGITACION (Condado)

ETIQUETA	DIGITACION
SISTEMA OPERATIVO	Windows 7 Ultimate
PROCESADOR	Intel Dual Core 2,5 GHz
RAM	3 GB
DISCO	320 GB C: 100 GB D: 200 GB
NOMBRE	Digitacion Ant
NOMBRE COMPLETO	
RED	IP: 192.168.1.167 MASK: 255.255.255.0 GATEWAY: 192.168.1.210

Tabla 5
Descripción Computadora módulo 3 (Condado)

ETIQUETA	modulo 3 (Desktop)
SISTEMA OPERATIVO	Windows 7 x32
PROCESADOR	Intel Core i3
RAM	2 GB
DISCO	250 GB C: 97,65 GB D: 200,43 GB
NOMBRE	DISTRIUIOYOU06
NOMBRE COMPLETO	
\RED	IP: 10.112.133.227 MASK: 255.255.255.224 GATEWAY: 10.112.133.238 IP: 192.168.1.234 MASK: 255.255.255.O DNS PREFERIDO: 10.112.157.49 DNS ALTERNO: 10.112.157.48

Tabla 6
Descripción Computadora servicio cliente 6 (Condado)

ETIQUETA	servicio cliente 6 (Desktop)
SISTEMA OPERATIVO	Windows 7 x32
PROCESADOR	Intel Core i3 3,30GHz
RAM	4 GB
DISCO	250 GB C: 97,65 GB D: 200,43 GB
NOMBRE	DISTRIDUIOYOU75
NOMBRE COMPLETO	DISTRIDUIOYOU75.otecel.com.ec
RED	IP: 10.112.131.169 MASK: 255.255.255.240 GATEWAY: 10.112.131.161 IP: 192.168.1.133 MASK: 255.255.255.O DNS PREFERIDO: 10.112.157.49 DNS ALTERNO: 10.112.157.48

Tabla 7
Descripción Computadora SC 6 (Condado)

ETIQUETA	SC 6 (Desktop)
SISTEMA OPERATIVO	Windows 8 x32
PROCESADOR	Intel Core i5 2,90 GHz
RAM	4 GB
DISCO	500 GB C: 100 GB D: 365,42 GB
NOMBRE	DISTRIUIDUIOPRED04
NOMBRE COMPLETO	DISTRIUIDUIOPRED04.otecel.com.ec
RED	IP: 10.112.131.162 MASK: 255.255.255.240 GATEWAY: 10.112.131.161 IP: 192.168.1.162 MASK: 255.255.255.O DNS PREFERIDO: 10.112.157.49 DNS ALTERNO: 10.112.157.48

Tabla 8
Descripción Computadora SC 4 (Condado)

ETIQUETA	SC 4 (Desktop)
SISTEMA OPERATIVO	Windows 7 Professional x32
PROCESADOR	Pentium Dual core 2,50 GHz
RAM	2 GB
DISCO	150 GB C: 97,56 GB D: 51,39 GB
NOMBRE	DISTRIUIDUIOYOU87
NOMBRE COMPLETO	DISTRIUIDUIOYOU87.otecel.com.ec
RED	IP: 10.112.131.168 MASK: 255.255.255.240 GATEWAY: 10.112.131.161 IP: 192.168.1.29 MASK: 255.255.255.0 DNS PREFERIDO: 10.112.157.49 DNS ALTERNO: 10.112.157.48

Tabla 9
Descripción Computadora Supervisión 1 (Condado)

ETIQUETA	Supervisión 1(Desktop) Servicio al Cliente
SISTEMA OPERATIVO	Windows 7 Ultimate x32
PROCESADOR	Intel Core i5 2,90 GHz
RAM	4 GB
DISCO	500 GB C: 195,44 GB D: 270,32 GB
NOMBRE	DIGITADOR
NOMBRE COMPLETO	DIGITADOR
RED	DHCP HABILITADO

Tabla 10
Descripción Computadora Supervisor (Condado)

ETIQUETA	Supervisor (Desktop) Servicio al Cliente 9
SISTEMA OPERATIVO	Windows 7 Ultimate
PROCESADOR	Intel Core i5 2,90 GHz
RAM	4 GB
DISCO	500 GB C: 195,44 GB F: 270,31 GB
NOMBRE	DISTRIUIDUIOYP01
NOMBRE COMPLETO	DISTRIUIDUIOYP01.otecel.com.ec
RED	IP: 10.112.133.231 MASK: 255.255.255.224 GATEWAY: 10.112.133.238 IP: 192.168.1.231 MASK: 255.255.255.0 DNS PREFERIDO: 10.112.157.48 DNS ALTERNO: 10.112.157.49

Tabla 11
Descripción Computadora servicio cliente 8 (Condado)

ETIQUETA	servicio cliente 8 (Desktop)
SISTEMA OPERATIVO	Windows 7 Ultimate x32
PROCESADOR	Intel Core i5 2,90GHz
RAM	4 GB
DISCO	500 GB C: 195,45 GB D: 270,31 GB
NOMBRE	DISTRIDUIOYOU50
NOMBRE COMPLETO	DISTRIDUIOYOU50.otecel.com.ec
RED	IP: 10.112.131.174 MASK: 255.255.255.240 GATEWAY: 10.112.131.161 IP: 192.168.1.145 MASK: 255.255.255.o DNS PREFERIDO: 10.112.157.49 DNS ALTERNO: 10.112.157.48

Tabla 12
Descripción Computadora SC 5 (Condado)

ETIQUETA	SC 5 (Desktop)
SISTEMA OPERATIVO	Windows 7 Ultimate x32
PROCESADOR	Intel Pentium CPU G630 2,70 GHz
RAM	4 GB
DISCO	500 GB C: 195,44 GB D: 270,32 GB
NOMBRE	DISTRIDUIOYOU50
NOMBRE COMPLETO	DISTRIDUIOYOU50.otecel.com.ec
RED	IP: 10.112.131.173 MASK: 255.255.255.240 GATEWAY: 10.112.131.161 IP: 192.168.1.192 MASK: 255.255.255.0 DNS PREFERIDO: 10.112.157.48 DNS ALTERNO: 10.112.157.49

Tabla 13.
Descripción Computadora turnos (Condado)

ETIQUETA	Turnos
SISTEMA OPERATIVO	Windows 7 Ultimate x32
PROCESADOR	Intel Pentium CPU G630 2,70 GHz
RAM	4 GB
DISCO	500 GB C: 195,44 GB D: 270,32 GB
NOMBRE	DISTRIUIDUIOYOU80
NOMBRE COMPLETO	DISTRIUIDUIOYOU80.otecel.com.ec
RED	IP: 10.112.133.225 MASK: 255.255.255.224 GATEWAY: 10.112.133.238 IP: 192.168.1.73 MASK: 255.255.255.0 DNS PREFERIDO: 10.112.157.49 DNS ALTERNO: 10.112.157.48

Tabla 14
Descripción Computadora 6 (Condado)

ETIQUETA	6
SISTEMA OPERATIVO	Windows 7 Ultimate x32
PROCESADOR	Intel Core i5 2,90 GHz
RAM	4 GB
DISCO	500 GB C: 195,44 GB D: 270,32 GB
NOMBRE	DISTRIUIDUIOYOUP9
NOMBRE COMPLETO	DISTRIUIDUIOYOUP9.otecel.com.ec
RED	IP: 10.112.133.167 MASK: 255.255.255.240 GATEWAY: 10.112.131.161 IP: 192.168.1.177 MASK: 255.255.255.0 DNS PREFERIDO: 10.112.157.49 DNS ALTERNO: 10.112.157.48

Tabla 15
Descripción Computadora SC9 (Condado)

ETIQUETA	SC9
SISTEMA OPERATIVO	Windows 7 Ultimate x64
PROCESADOR	Intel Core i3 3,50 GHz
RAM	4 GB
DISCO	1TR C: 390,63 GB D: 540,79 GB
NOMBRE	DISTRIUIDUIOYOU88
NOMBRE COMPLETO	DISTRIUIDUIOYOU88.otecel.com.ec
RED	IP: 10.112.133.234 MASK: 255.255.255.224 GATEWAY: 10.112.133.238 IP: 192.168.1.249 MASK: 255.255.255.0 DNS PREFERIDO: 10.112.157.48 DNS ALTERNO: 10.112.157.49

Tabla 16
Descripción Computadora AutoGestión (Condado)

ETIQUETA	AutoGestión
SISTEMA OPERATIVO	Windows 7 Ultimate x32
PROCESADOR	Intel Core 2 Duo 2,8 GHz
RAM	3 GB
DISCO	1TR C: 390,63 GB D: 540,79 GB
NOMBRE	DISTRIUIDUIOYOU95
NOMBRE COMPLETO	DISTRIUIDUIOYOU95.otecel.com.ec
RED	IP: 10.112.133.233 MASK: 255.255.255.224 GATEWAY: 10.112.133.238 DNS PREFERIDO: 10.112.157.48 DNS ALTERNO: 10.112.157.49

Tabla 17
Descripción Computadora DIGITACION (Condado)

ETIQUETA	DIGITACION
SISTEMA OPERATIVO	Windows 7 Ultimate
PROCESADOR	Intel Dual Core 2,5 GHz
RAM	3 GB
DISCO	320 GB C: 100 GB D: 200 GB
NOMBRE	Digitacion Ant
NOMBRE COMPLETO	
RED	IP: 192.168.1.4 MASK: 255.255.255.0 GATEWAY: 192.168.10.1

Tabla 18
Descripción Computadora BOD (Condado)

ETIQUETA	BOD
SISTEMA OPERATIVO	Windows 7 Ultimate x32
PROCESADOR	Pentium Dual Core 3 GHz
RAM	4 GB
DISCO	500 GB C: 150 GB D: 300 GB
NOMBRE	DISTRIUIDUIOYOU54
NOMBRE COMPLETO	DISTRIUIDUIOYOU54.otecel.com.ec
RED	IP: 10.112.133.229 MASK: 255.255.255.224 GATEWAY: 10.112.133.238 IP: 192.168.1.182 MASK: 255.255.255.0 DNS PREFERIDO: 10.112.157.48 DNS ALTERNO: 10.112.157.49

Tabla 19
Descripción Computadora Servicio Técnico 1 (Condado)

ETIQUETA	Servicio Técnico 1 ST 1
SISTEMA OPERATIVO	Windows 7 Ultimate x64
PROCESADOR	Intel Core i5 3 GHz
RAM	4 GB
DISCO	1) 500 GB C: 200 GB 2) 300 GB: 100 GB D: 270 GB 200 GB
NOMBRE	
NOMBRE COMPLETO	
RED	IP: 10.112.131.165 MASK: 255.255.255.240 GATEWAY: 10.112.131.161 IP: 192.168.1.163 MASK: 255.255.255.0 DNS PREFERIDO: 10.112.157.49 DNS ALTERNO: 10.112.157.48

Tabla 20
Descripción Computadora CAJA OTECEL (Condado)

ETIQUETA	CAJA OTECEL
SISTEMA OPERATIVO	Windows 7 Ultimate x32
PROCESADOR	Intel Core i5 2,9 GHz
RAM	4 GB
DISCO	500 GB C: 200 GB D: 270 GB
NOMBRE	DISTRIUIDUIOYOU65
NOMBRE COMPLETO	DISTRIUIDUIOYOU65.otecel.com.ec
RED	IP: 10.112.131.171 MASK: 255.255.255.240 GATEWAY: 10.112.131.161 IP: 192.168.1.227 MASK: 255.255.255.0 DNS PREFERIDO: 10.112.157.49 DNS ALTERNO: 10.112.157.48

Tabla 21
Descripción Computadora CAJA YOUPHONE (Condado)

ETIQUETA	CAJA YOUPHONE
SISTEMA OPERATIVO	Windows 7 Ultimate x64
PROCESADOR	Intel Core i5 2,9 GHz
RAM	4 GB
DISCO	500 GB C: 200 GB D: 270 GB
NOMBRE	DISTRIUIDUIOYOU72
NOMBRE COMPLETO	DISTRIUIDUIOYOU72.otecel.com.ec
RED	IP: 10.112.133.230 MASK: 255.255.255.224 GATEWAY: 10.112.133.238 IP: 192.168.1.199 MASK: 255.255.255.0 DNS PREFERIDO: 10.112.157.49 DNS ALTERNO: 10.112.157.48

Tabla 22
Descripción Computadora Contabilidad 4 (Condado)

ETIQUETA	Contabilidad 4
SISTEMA OPERATIVO	Windows 7 Professional x64
PROCESADOR	Intel Core i5 2,9 GHz
RAM	4 GB
DISCO	500 GB C: 200 GB D: 250 GB
NOMBRE	Usuario I5-PC
NOMBRE COMPLETO	
RED	IP: 192.168.1.37 MASK: 255.255.255.0 GATEWAY: 192.168.1.210

Tabla 23
Descripción Computadora Contabilidad 2 (Condado)

ETIQUETA	Contabilidad 2
SISTEMA OPERATIVO	Windows 7 Professional x64
PROCESADOR	Intel Core i5 3 GHz
RAM	4 GB
DISCO	500 GB C: 243,04 GB D: 222,62 GB
NOMBRE	CajaYouphone
NOMBRE COMPLETO	
RED	DHCP HABILITADO
ETIQUETA	Contabilidad 3
SISTEMA OPERATIVO	Windows 7 Ultimate x32
PROCESADOR	Intel Core 2 Duo 2,80 GHz
RAM	4 GB
DISCO	300 GB C: 298,09 GB
NOMBRE	CONTABILIDAD 2
NOMBRE COMPLETO	
RED	DHCP HABILITADO

Tabla 24
Descripción Computadora Asistencia Gerencia (Condado)

ETIQUETA	Asistencia Gerencia
SISTEMA OPERATIVO	Windows 7 Ultimate x64
PROCESADOR	Intel Core i5 3 GHz
RAM	8 GB
DISCO	500 GB C: 195,21 GB D: 270,45 GB
NOMBRE	PC-DIGITACIONI5
NOMBRE COMPLETO	
RED	DHCP HABILITADO

Local CAVS CCI

Este es uno de los locales que se encuentran en el centro comercial “CCI”, es el más grande los dos y cuenta con 10 computadoras con dirección IP dinámico (DHCP) detalladas a continuación:

Tabla 25
Descripción Computadora 1 (CCI)

ETIQUETA	1 (Desktop)
SISTEMA OPERATIVO	Windows 7 Ultimate x64
PROCESADOR	Intel Pentium 3GHz
RAM	4GB
DISCO	500 GB C:244,04 GB F: 221,62GB

Tabla 26
Descripción Computadora 2 (CCI)

ETIQUETA	2 (Desktop)
SISTEMA OPERATIVO	Windows 7 x32
PROCESADOR	Intel Core i3 3,60GHz
RAM	4GB
DISCO	500 GB C:195,31 GB D: 270,35GB

Tabla 27
Descripción Computadora 3 (CCI)

ETIQUETA	3 (Desktop)
SISTEMA OPERATIVO	Windows 7 Ultimate
PROCESADOR	Intel Core i5
RAM	4GB
DISCO	500 GB C:195 GB D: 270 GB

Tabla 28
Descripción Computadora 4 (CCI)

ETIQUETA	4 (Desktop)
SISTEMA OPERATIVO	Windows 7 Ultimate
PROCESADOR	Intel Core i3 3,60 GHz
RAM	4GB
DISCO	500 GB C:195 GB D: 270 GB

Tabla 29
Descripción Computadora 5 (CCI)

ETIQUETA	5 (Desktop)
SISTEMA OPERATIVO	Windows XP x32
PROCESADOR	Pentium 4 2,40 GHz
RAM	896 MB
DISCO	500 GB C:74,52GB

Tabla 30
Descripción Computadora 6 (CCI)

ETIQUETA	6 (Desktop)
SISTEMA OPERATIVO	Windows 7 Ultimate
PROCESADOR	Intel Pentium Dual 2,00 GHz
RAM	1GB
DISCO	150 GB C:58,59 GB D: 90,45 GB

Tabla 31
Descripción Computadora 7 (CCI)

ETIQUETA	7 (Desktop)
SISTEMA OPERATIVO	Windows 7 Professional
PROCESADOR	Intel Xeon 2GHz
RAM	16GB
DISCO	500 GB C:465 GB

Tabla 32
Descripción Computadora 8 (CCI)

ETIQUETA	8 (Desktop)
SISTEMA OPERATIVO	Windows 7 Ultimate
PROCESADOR	Intel Core i3 3,60 GHz
RAM	4GB
DISCO	500 GB C:195 GB D: 270 GB

Tabla 33
Descripción Computadora 9 (CCI)

ETIQUETA	9 (Laptop)
SISTEMA OPERATIVO	Windows 8 Pro
PROCESADOR	Intel Core i3
RAM	4GB
DISCO	500 GB C:243,80 GB D: 221,62 GB

Tabla 34
Descripción Computadora 10 (CCI)

ETIQUETA	10 (Desktop)
SISTEMA OPERATIVO	Windows 7 Ultimate x32
PROCESADOR	Intel Core 2 Quad 2,40 GHz
RAM	3GB
DISCO	500 GB C:243,80 GB D: 221,62 GB

Local CCI

Este es uno de los dos locales que se encuentran dentro del centro comercial “CCI”, es el más pequeño y cuenta con dos máquinas de usuario.

Tabla 35
Descripción Computadora CCI1 (CCI)

ETIQUETA	CCI1 (Desktop)
SISTEMA OPERATIVO	Windows 7 Ultimate x32
PROCESADOR	Intel Core I5
RAM	4GB
DISCO	500 GB C:195 GB D: 270 GB

Tabla 36
Descripción Computadora CCI2 (CCI)

ETIQUETA	CCI2 (Desktop)
SISTEMA OPERATIVO	Windows 7 Professional
PROCESADOR	Intel Pentium Dual 200 Ghz
RAM	2GB
DISCO	150 GB C:73.1 GB D: 75.7 GB

Servidores

Youphone Cia. Ltda. Cuenta con tres servidores principales, descritos a continuación:

Tabla 37
Descripción servidores Youphone Cia. Ltda

Nombre	Función	Descripción
Servidor1	Servidor de Facturación, contiene el programa Latinium, la misma que sirve para registrar todo el proceso de facturación así como la impresión de la factura. Este servidor se encuentra ubicado CAVS Condado Shopping	• HP 166066 • 12 GB de RAM • 1,5TB Disco Duro • Sistema Operativo Windows Server 2012 • SQL Express • Dirección IP 192.168.1.1
Servidor2	Servidor del aplicativo de contratos INCELL, el mismo que sirve para llenar los contratos de nuevas líneas telefónicas hechas con el cliente externo. Este servidor se encuentra ubicado CAVS Condado Shopping	• Intel Server • 8GB de RAM • 1TB Disco Duro • Sistema Operativo Windows 7 64bits • Dirección IP 192.168.1.2
Servidor3	Servidor de Facturación, contiene el programa Latinium, la misma que sirve para registrar todo el proceso de facturación así como la impresión de la factura. Este servidor se encuentra ubicado CAVS CCI	• Intel Core I7 • Sistema Operativo Windows 7 64bits • 8GB de RAM • Disco Duro 1 TB • 192.168.1.1

3.2 Procedimiento

Existen algunos modelos para la realización de hacking ético, en este trabajo se va a utilizar la metodología OSSTMM (Open Source Security Testing

Methodology) que es un Manual de la Metodología Abierta de Pruebas de Seguridad, que abarca lo siguiente:

- Seguridad de la Información
- Seguridad de los Procesos
- Seguridad en las Tecnologías de Internet
- Seguridad en las Comunicaciones
- Seguridad Inalámbrica
- Seguridad Física

Entonces en combinación con el modelo de listas de comprobación se realizan Tablas de todas las revisiones necesarias de las fases que plantea el modelo antes mencionado.

3.2.1 Listas de Comprobación o "Checklist" y OSSTMM (pdcahome, 2016)

Una lista de comprobación generalmente tiene un párrafo de texto para cada tarea, con un cuadrado vacío en la parte izquierda o derecha. Una vez que la tarea ha sido terminada, el cuadrado se rellena con una pequeña marca de verificación.

Las "listas de control", "listas de chequeo", "check-lists" u "hojas de verificación", son formatos creados para realizar actividades repetitivas, controlar el cumplimiento de una lista de requisitos o recolectar datos ordenadamente y de forma sistemática. Se usan para hacer comprobaciones sistemáticas de actividades o productos asegurándose de que el trabajador o inspector no se olvida de nada importante.

Los usos principales de los checklist son los siguientes:

- Realización de actividades en las que es importante que no se olvide ningún paso y/o deben hacerse las tareas con un orden establecido.

- Realización de inspecciones donde se debe dejar constancia de cuáles han sido los puntos inspeccionados.
- Verificar o examinar artículos.
- Examinar o analizar la localización de defectos. Verificar las causas de los defectos.
- Verificación y análisis de operaciones.
- Recopilar datos para su futuro análisis.

En definitiva, estas listas suelen ser utilizadas para la realización de comprobaciones rutinarias y para asegurar que al operario o el encargado de dichas comprobaciones no se le pasa nada por alto, además de para la simple obtención de datos.

La ventaja de los checklist es que, además de sistematizar las actividades a realizar, una vez rellenados sirven como registro, que podrá ser revisado posteriormente para tener constancia de las actividades que se realizaron en un momento dado.

Es importante que las listas de control queden claramente establecidas e incluyan todos los aspectos que puedan aportar datos de interés para la organización. Es por ello preciso que quede correctamente recogido en la lista de control:

- Qué tiene que controlarse o chequearse.
- Cuál es el criterio de conformidad o no conformidad (qué es lo correcto y qué lo incorrecto).
- Cada cuánto se inspecciona: frecuencia de control o chequeo.
- Quién realiza el chequeo y cuáles son los procedimientos aplicables.

Conviene, que se disponga de un apartado de observaciones con el fin de poder obtener información previa sobre posibles motivos que han causado la disconformidad.

Por otro lado, si vamos a usar los checklists para la obtención de datos, también se pueden utilizar para construir gráficas o diagramas para controlar la evolución de una característica o actividad. También se utilizan para reportar diariamente el estado de las operaciones y poder evaluar la tendencia y/o dispersión de la producción, sin que sea necesaria la realización de estadísticas o gráficas de mayor complejidad.

A medida que ha avanzado el presente trabajo se puede observar los siguientes cuadros o Tablas ubicadas en el punto de “Análisis de la situación Actual”:

- Información de la empresa (Descripción)
- Características de los equipos computacionales de la empresa.
- Características de los servidores.

Más adelante se desarrollarán las Tablas de a continuación:

- Detalle de software a utilizarse
- Detalle de protocolos
- Detalle de puertos abiertos.

Tabla 38
Lista o CheckList de procesos a realizar en Youphone

Lugar:			
Máquina o recurso:			
Dirección IP:			
	Si	No	Observación
Análisis de situación Actual			
Diagramas de red			
Inventario de Equipos			
Revisión de Software			
Antivirus			
Firewall			
Parches de Seguridad			
Hacking ético			
Reconocimiento con:			
WHOIS			

Comando nslookup			
Comando tracert			
Visual Route			
Escaneo con:			
AngryIP Scanner			
Advanced Port Scanner			
Network Auditor Security			
Ping de la muerte			
Enumeración con:			
Nessus			
Wireshark			
Manteniendo Acceso			
Borrar Huellas			

3.2.2 Reglas del procedimiento

Las reglas que se establecieron de mutuo acuerdo fueron las siguientes:

- No se puede realizar pruebas o procedimientos que alteren permanentemente el funcionamiento de los sistemas informáticos.
- No se podrá cubrir las huellas.
- No se almacenará ninguna copia del informe o documento donde se describa las pruebas ejecutadas en ningún equipo dentro de la empresa
- No se podrá instalar “backdoors” en ningún equipo.

3.2.3 Configuración de herramientas para hacking ético

De las aplicaciones que se decribieron en el capítulo anterior se usaron aquellas descritas en la Tablade a continuación, todas fueron instaladas en Sistema Operativo Windows 7. Los programas VisualRoute y Nessus son herramientas pagadas, sin embargo son gratuitas por un tiempo determinado, lo cual sirvió para realizar el análisis.

Tabla 39
Lista de Programas usados en el proyecto

Reconocimiento	Escaneo	Enumeración
WHOIS	Angry IP Scanner	Nessus
Comando nslookup	Advanced Port Scanner	WireShark
Comando tracert	Network Auditor Security	
VisualRoute		

3.3 Aplicación de Herramientas

En este paso del procedimiento, lo que se hace es aplicar las herramientas descritas en el ítem anterior, según los pasos del Hacking ético.

3.3.1 Reconocimiento

Se obtiene información importante de la empresa a través de la aplicación de herramientas descritas en el capítulo 2 obteniendo los siguientes resultados:

WHOIS

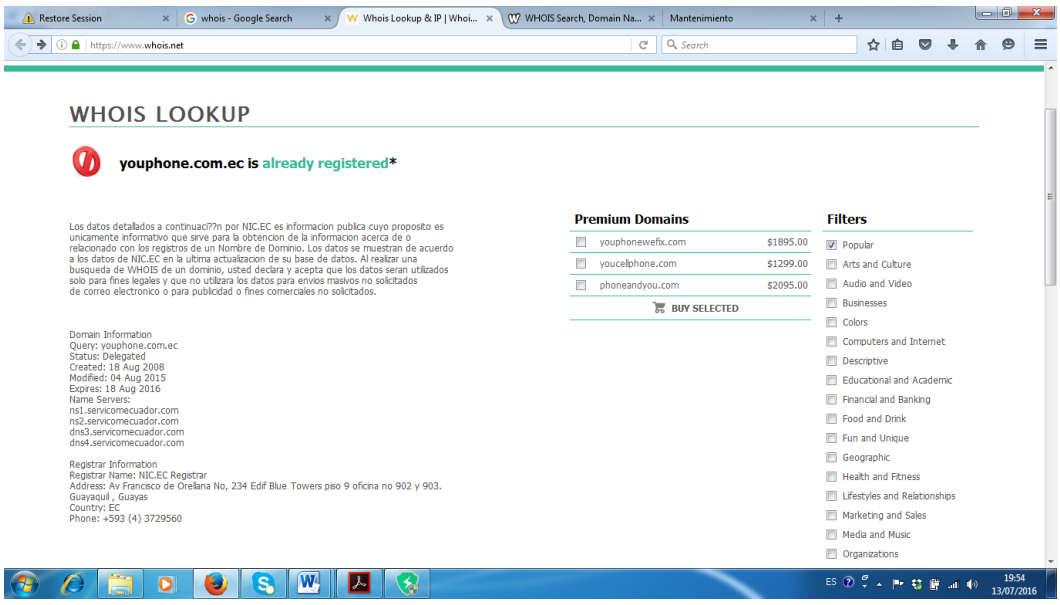

Figura 33 WHOIS aplicado a www.youphone.com.ec

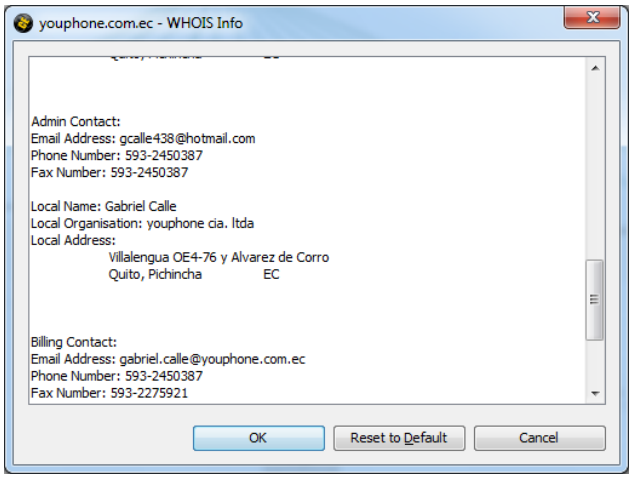

Figura 34 Datos del contacto administrativo del dominio WHOIS

Nslookup

Al aplicar el comando *nslookup* se observa que la IP donde se encuentra alojado el dominio 66.226.75.61

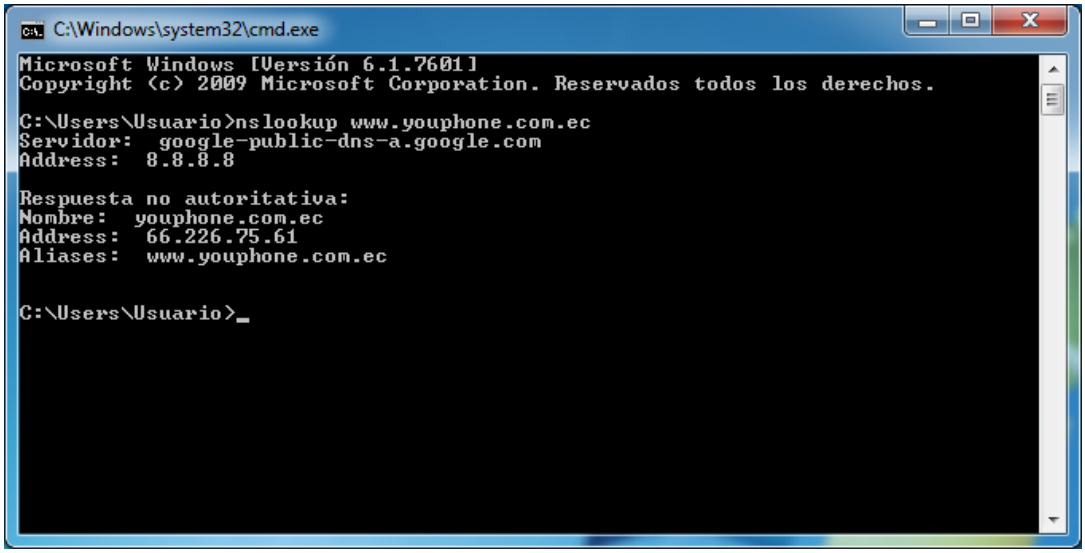

Figura35 Comando nslookup aplicado a www.youphone.com.ec

Traceroute

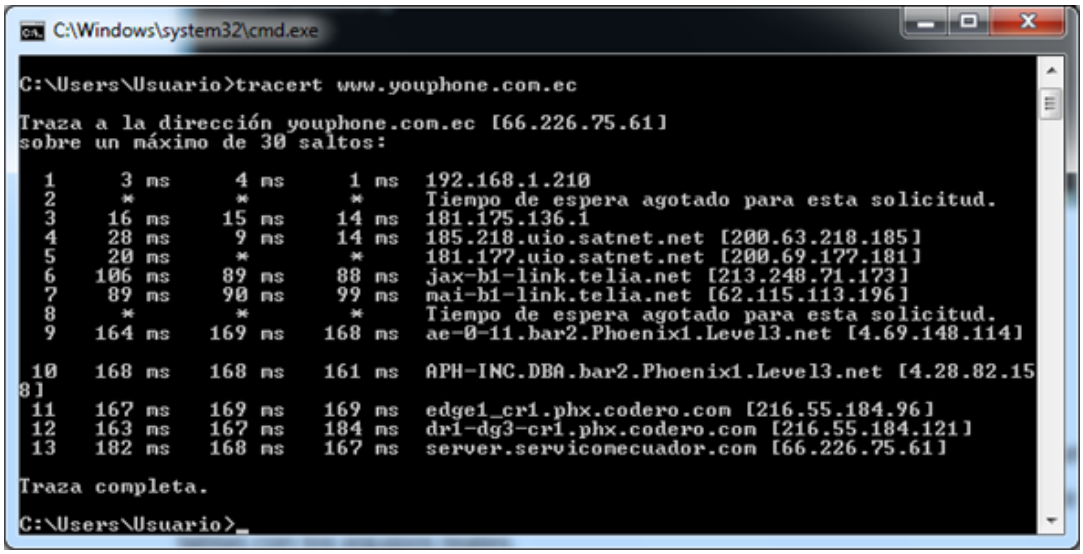

Figura36 Comando tracert aplicado a www.youphone.com.ec

VisualRoute

Esta herramienta muestra de manera más amigable lo que realizó el comando *tracerout.*

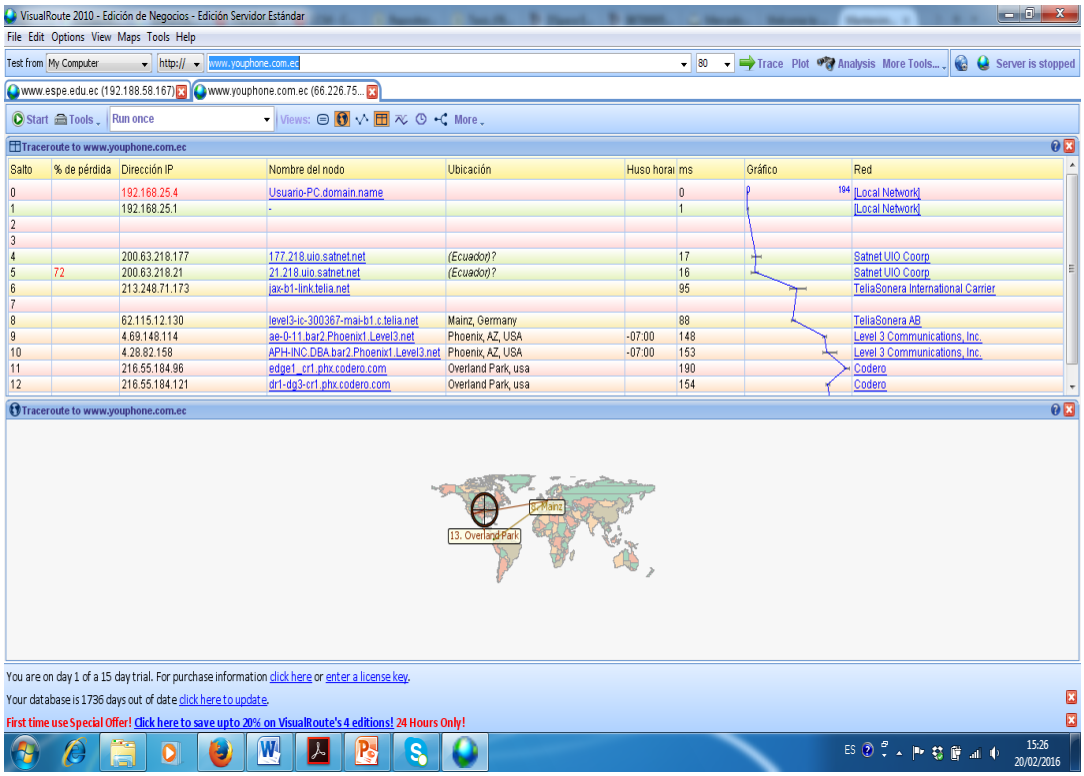

Figura 37 Visualización gráfica de los saltos a través de VisualRoute

3.3.2 Escaneo (Exploración)

En esta fase se encuentran las vulnerabilidades a través de los puertos abiertos. Los puertos que se encuentran en mayor uso son:

Tabla 40
Puertos, número de puerto, descripción y protocolo

SIGLAS	NÚMERO DE PUERTO	DESCRIPCIÓN	PROTOCOLO
FTP	20/21	File Transfer Protocol	Tcp
TELNET	23	Manejo remoto de equipos, inseguro	Tcp
SMTP	25	Simple Mail Transfer Protocol	Tcp
NAME	43		Tcp
NICNAME	43		Tcp
DNS	53	Domain Name System	Udp
FACETIME	53		tcp/udp
BOOTPS	67	BootStrap Protocol (Server)	Udp
BOOTPC	68	BootStrap Protocol	Udp

		(Client)	
TFTP	69	Trivial File Transfer Protocol	Udp
FINGER	79		Tcp
HTTP	80	Hyper Text Transfer Protocol	Tcp
KERBEROS	88	Agente de autenticación	Tcp
POP3	110	Post Office Protocol	Tcp
SUNRPC	111		Tcp
IDENT	113	Sistema de Identificación	Tcp
NTP	123	Protocolo de sincronización de Tiempo	Udp
RCP	1352	IMB Lotus Notes /Domino	Tcp
NETBIOS-DGM	138	Servicio de envío de datagramas	Tcp
NETBIOS	137	Servicio de nombres	Tcp
IMAP	143	Internet Message Access Protocol	Tcp
SNMP TOADNODE	161		Udp
SNMP	162	Simple Network Managment Protocol	Tcp
LDAP	389	Protocolo de acceso ligero a Base de Datos	Tcp
SSL	443	Security Socket Layer	Tcp
MSFT DS	445	Active Directory	Tcp
SYSLOG	514	Logs del Sistema	Udp
ROUTER	520		Tcp
SQL SERVER S	433	Microsoft SQL - Server	Tcp
SQL SERVER M	434	Microsoft SQL - Monitor	Tcp
Proxy Web	1080	Servidor Proxy	Tcp

Las herramientas que se utilizaron en este paso son:

Angry IP Scanner

Esta herramienta sirve para encontrar las IP’s que se encuentran asignadas a los equipos, con esto se puede comparar los resultados de las Tablas con los equipos reales

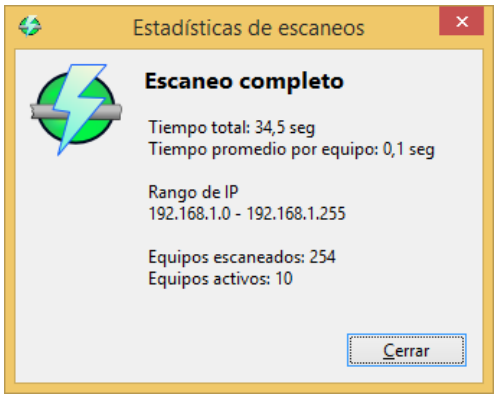

Figura 38 Resumen estadístico Angry IP Scan

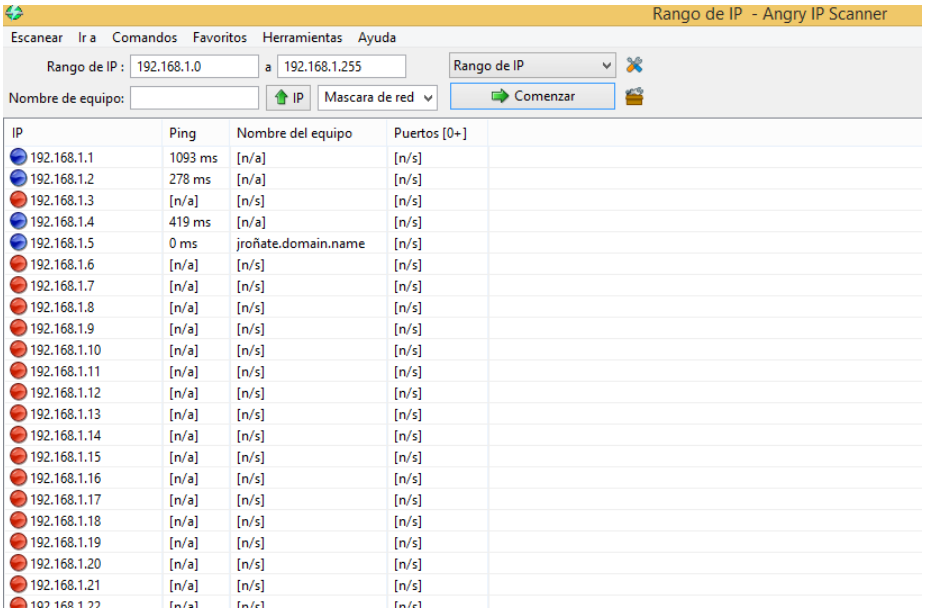

Figura39 Ejecución de Angry IP Scanner. Ejemplo de Búsqueda de Equipos activos en CAVS Condado Shopping

Advanced Port Scanner

Con esta herramienta se puede determinar los puertos que se encuentran abiertos. En este ejemplo se lo hace a la ip Wan de Cavs Condado 181.39.23.42

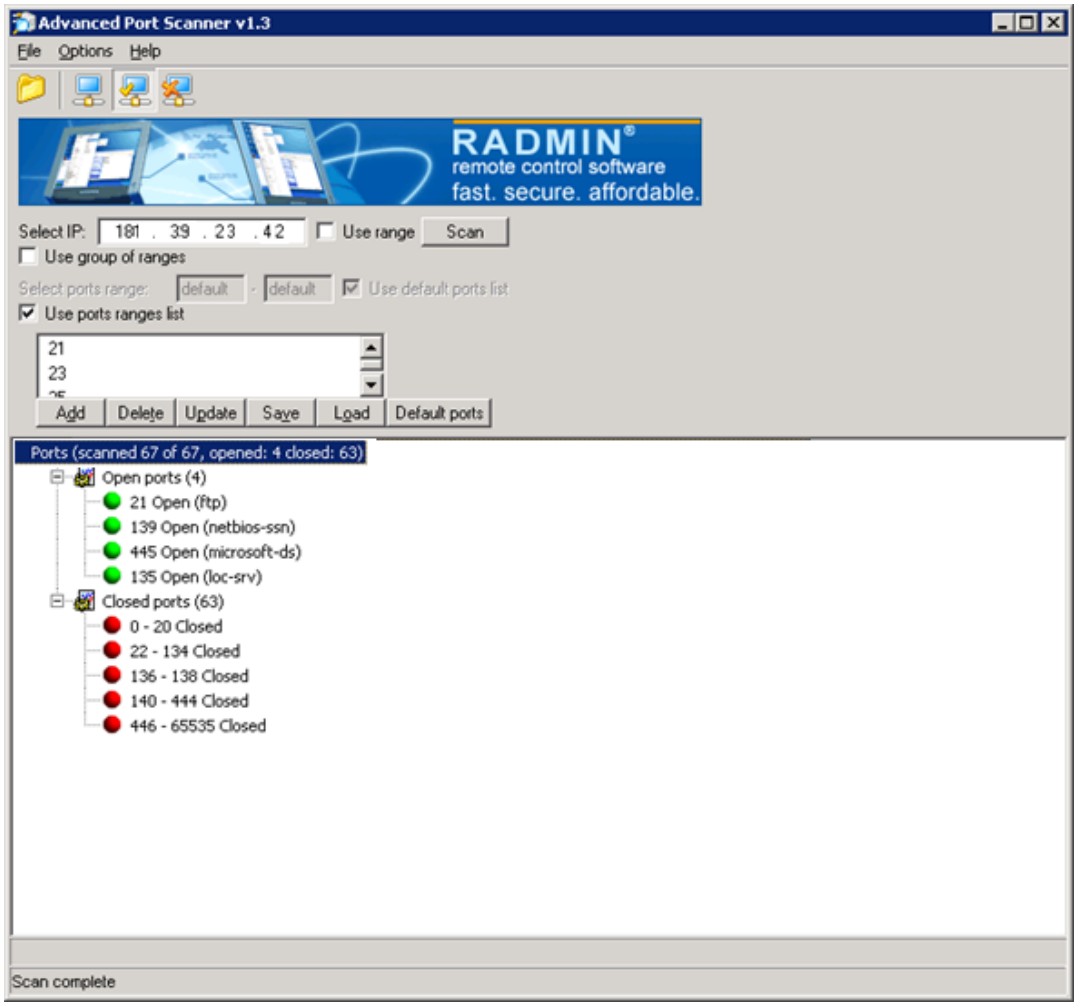

Figura 40 Ejemplo de ejecución de Advanced Port Scanner CAVS Condado

Network Security Auditor

A continuación se muestra las Pruebas de Puertos a los servidores de los diferentes locales.

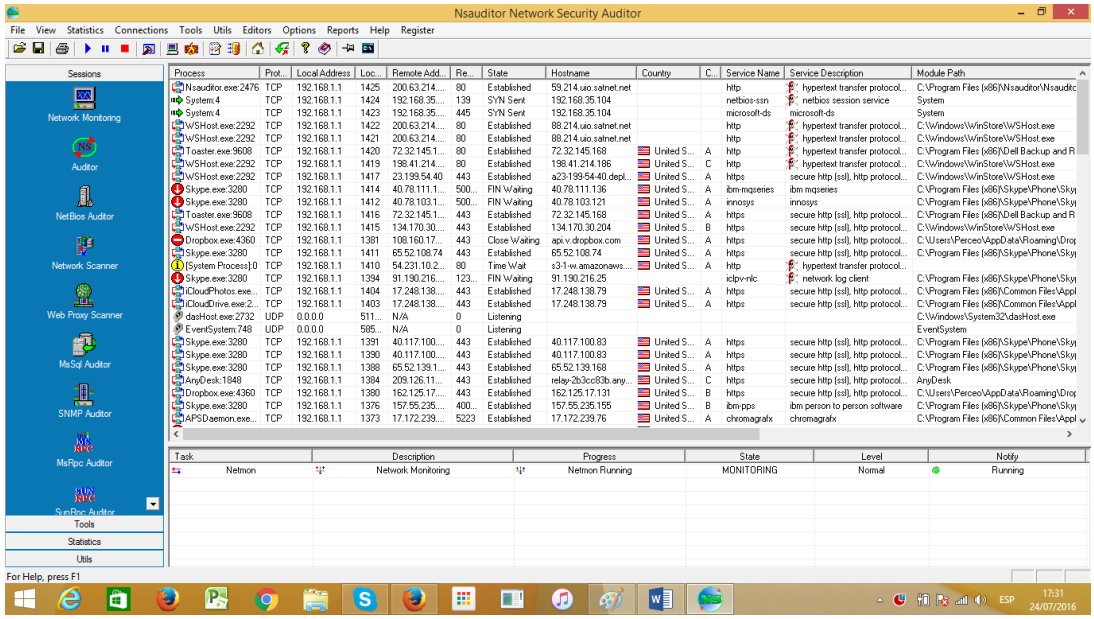

Figura 41 Resultados de Programa Network Auditor Security CAVS

Condado

Pruebas de Ping de la Muerte a servidores

Para comprobar la seguridad en relación a la respuesta a los Paquetes ICMP (PING) se realiza una prueba de paquetes del tamaño normal, que es lo que se muestra en la figura.

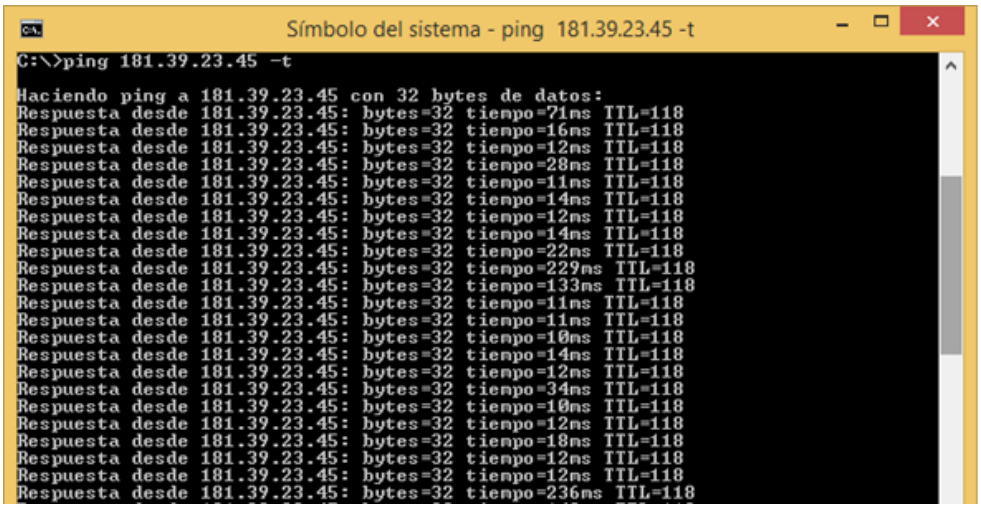

Figura 42 Envío de paquetes ICMP de tamaño normal

Al hacer pruebas de ping a la Ip del servidor del CAVS condado con los parámetros normales, es decir, la longitud del paquete ICMP de 32 bytes el tiempo de respuesta fluctúa entre 10 y 239 milisegundos, lo que se considera dentro del rango normal.

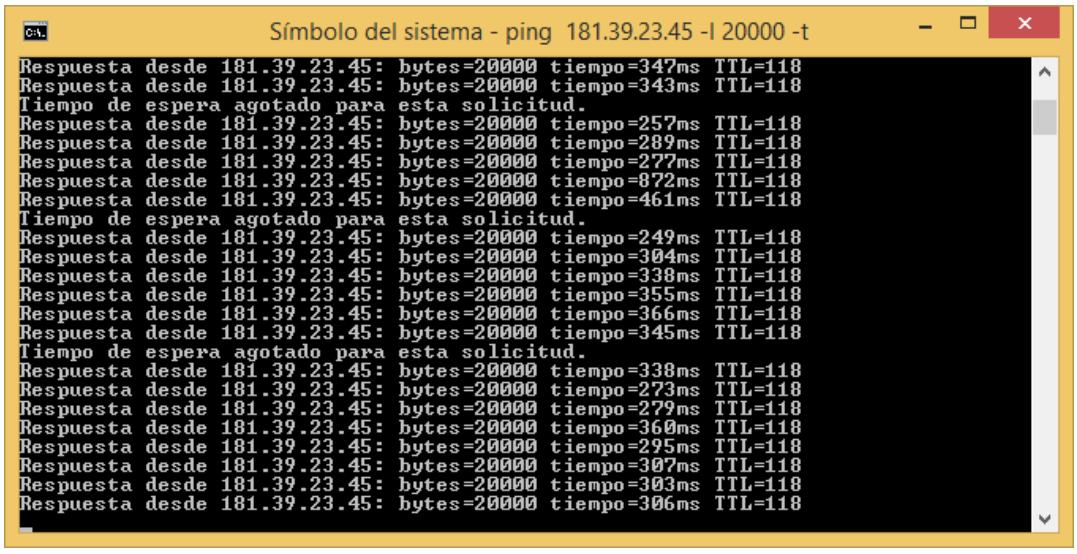

Figura 43 Envío de paquetes ICMP con bytes 20000

Variando el número de bytes los tiempos de respuesta del servidor aumentan drásticamente hasta en ciertas ocasiones no recibir respuesta

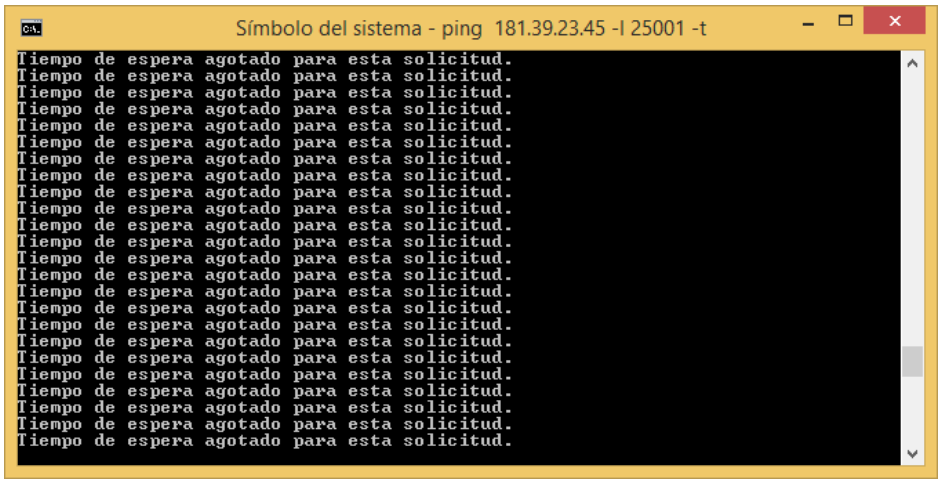

Figura 44 Envío de paquetes ICMP con bytes 25000

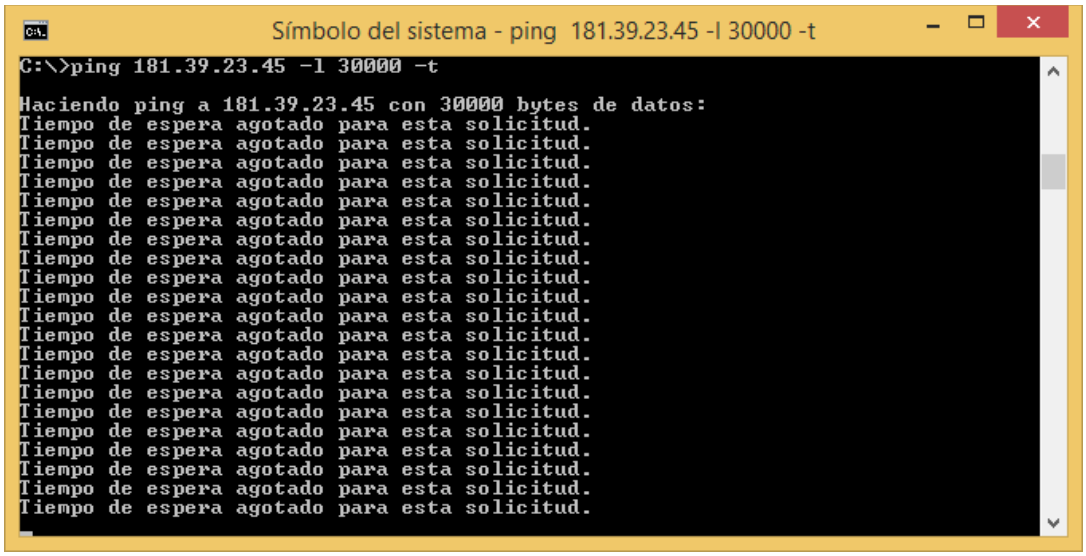

Figura 45 Envío de paquetes ICMP con bytes 30000

Se puede observar que el servidor ya no puede responder, significando que éste se ha caído logrando con satisfacción el ping de la muerte.

3.3.3 Enumeración

En esta fase aplicamos herramientas que me permitan obtener análisis de la red en general, para ello tenemos:

Wireshark

Se ejecuta esta herramienta para observar el comportamiento de la red de datos de la empresa, para esto se configuró un puerto como espejo y este se conectó a un Access point para analizar mediante la tarjeta de red inalámbrica. A continuación se muestra las capturas del trabajo realizado

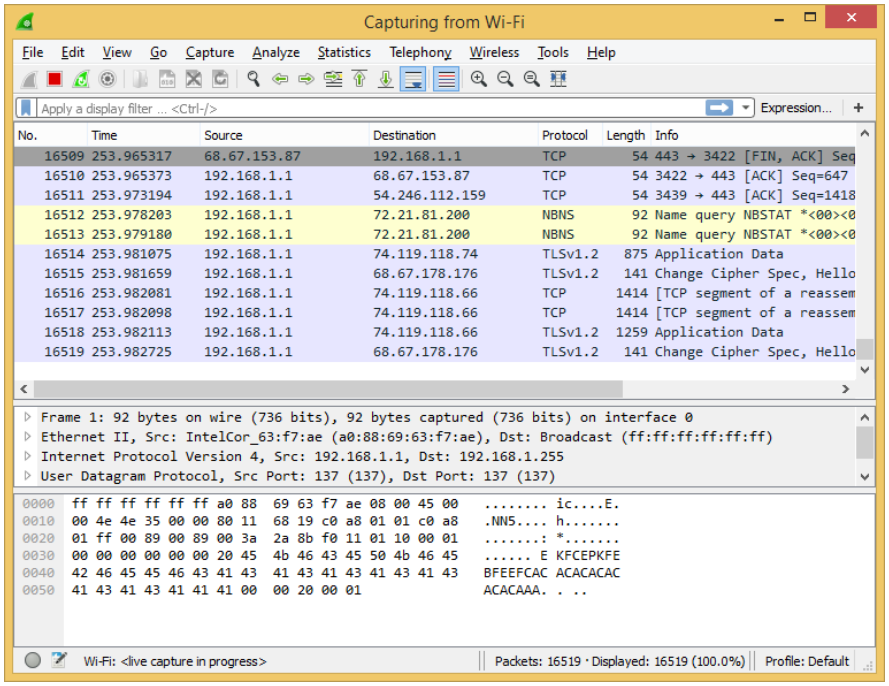

Figura46 Tráfico de datos capturado mediante Wireshark

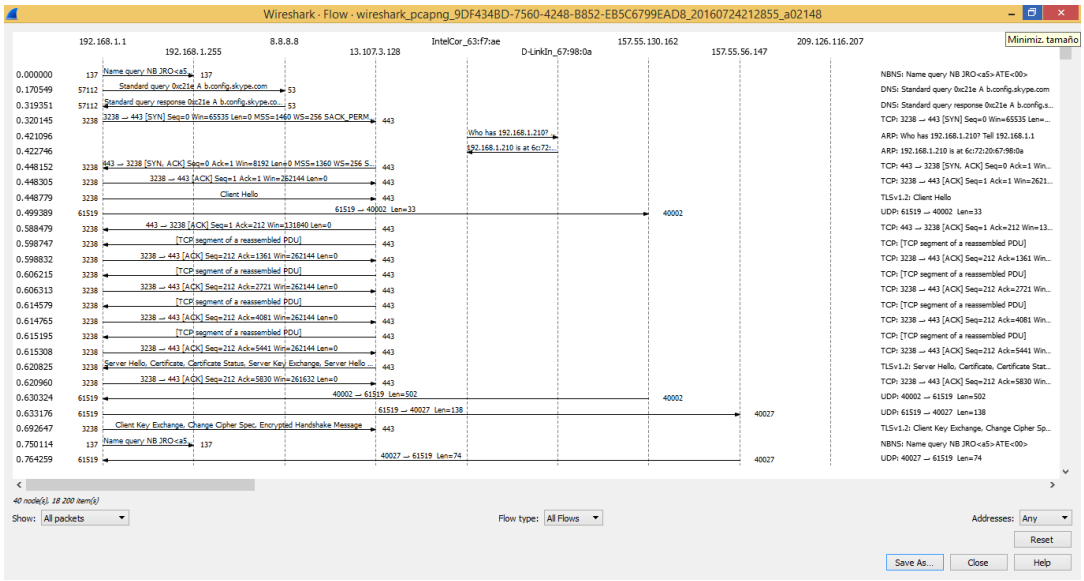

Figura 47 Diagrama de flujo de conexiones TCP

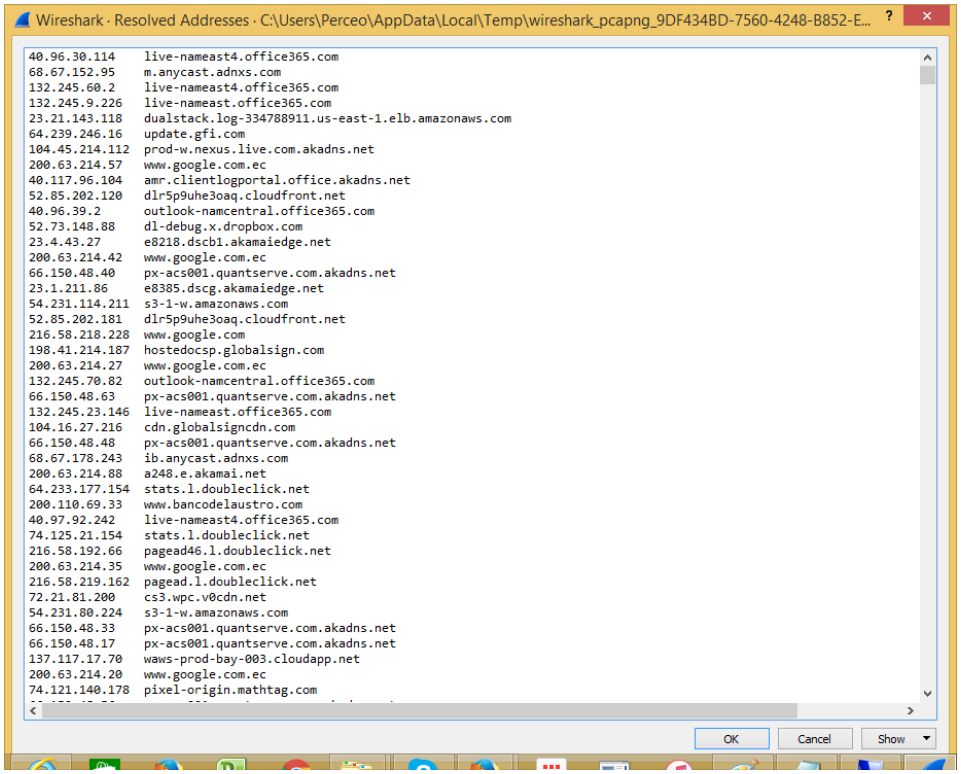

Figura 48 Resolución de nombres DNS capturadas con Wireshark

Mediante este programa se puede analizar el tráfico que circula por la red y visualizar que puertos están siendo ocupados y hacia qué dirección destino, por tanto se puede determinar cuáles de estos son vulnerabilidades en especial en los servidores de la organización.

Nessus

Esta herramienta es pagada, sin embargo permite su funcionamiento gratis por cierto tiempo. Funciona por interfaz web. Al aplicar una auditoría se puede ver los resultados con las siguientes figuras:

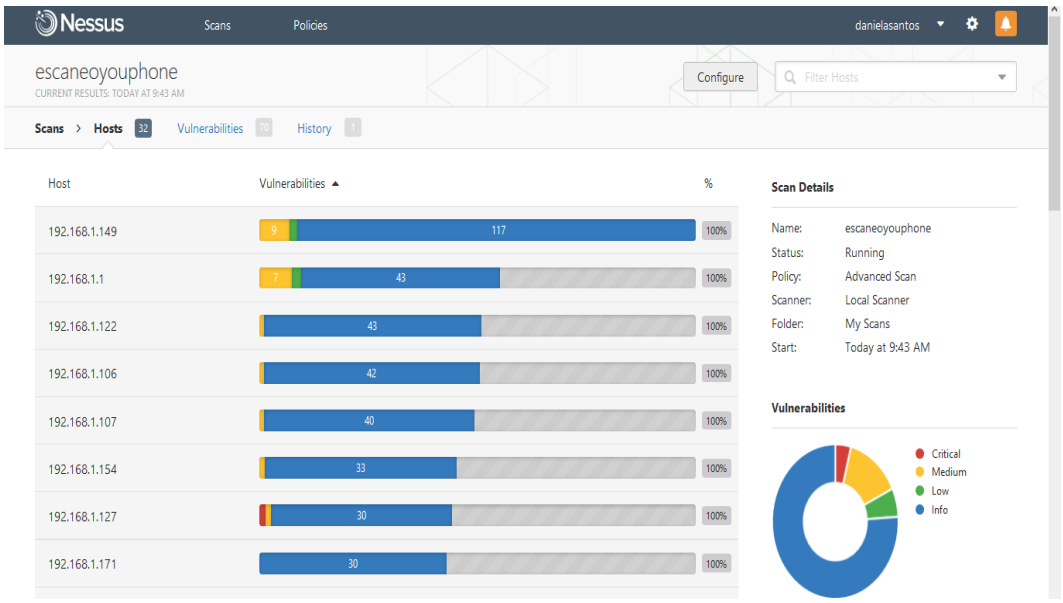

Figura 49 Escaneo General a toda la red de datos usando Nessus (1)

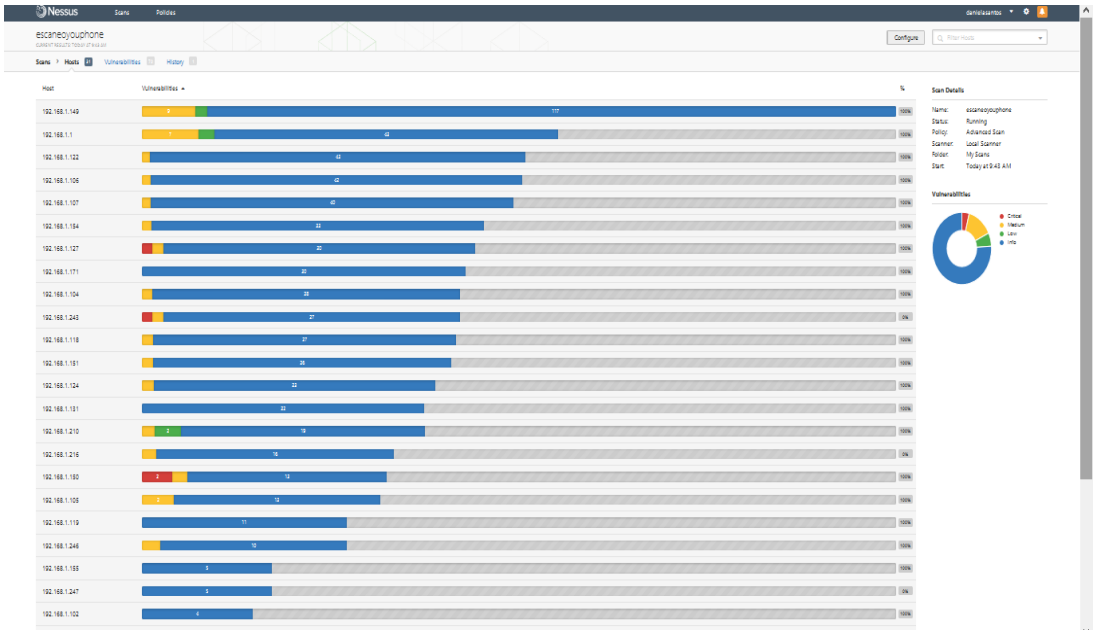

Figura 50 Escaneo General a toda la red de datos usando Nessus (2)

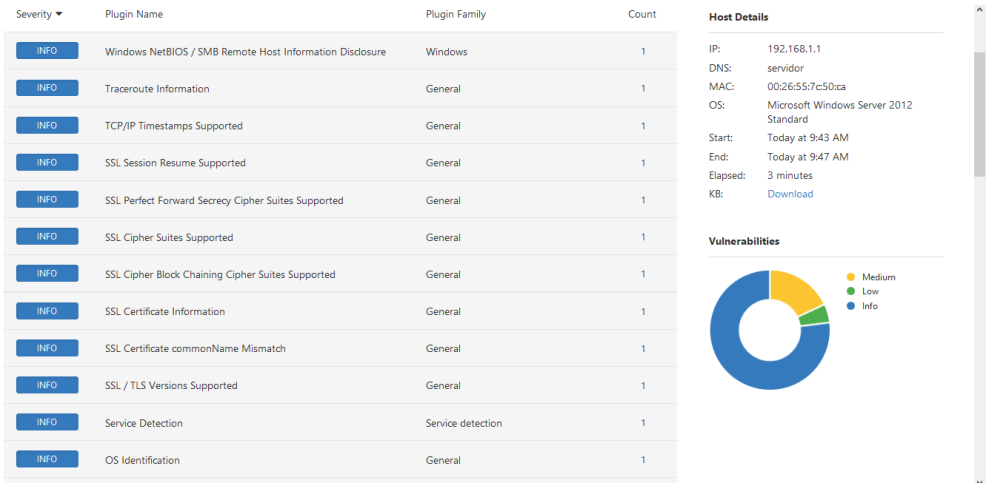

Figura 51 Escaneo de Servidor 192.168.1.1

Pruebas de Escaneo de Puertas a Maquinas de Clientes

En las máquinas de usuario también son susceptibles de ataques es por ello que se realiza pruebas en una máquina al azar. Para determinar que problemas podemos tener en las computadoras de los usuarios internos.

Advanced Port Scanner

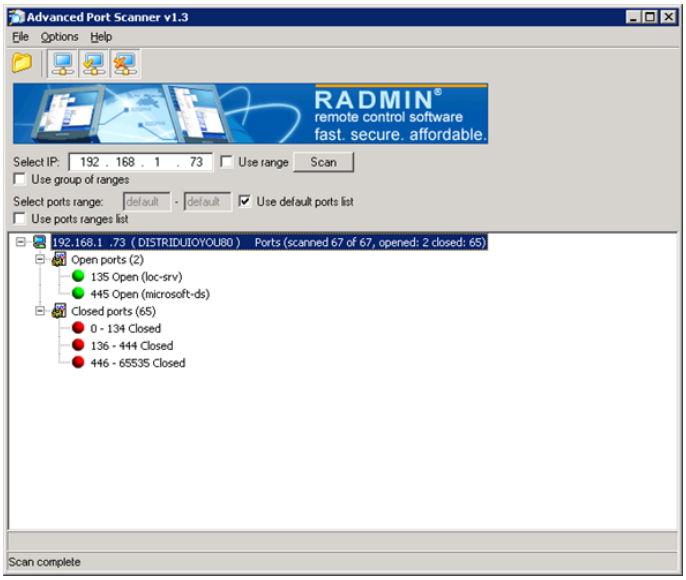

Figura 52 Escaneo de puertos a una máquina de usuario

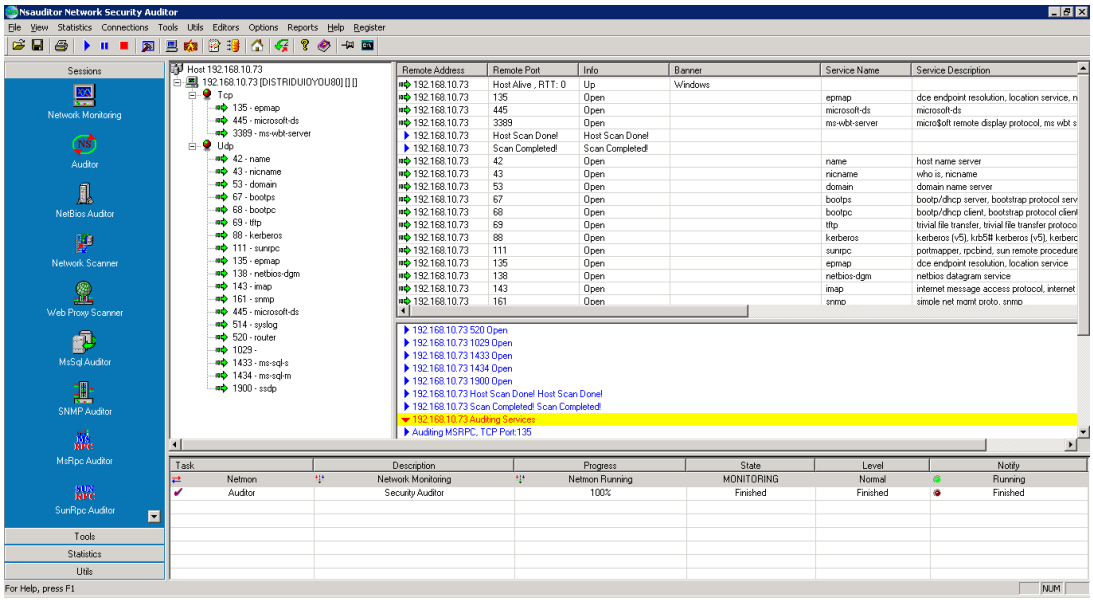

Figura 53 Escaneo Network Security Auditor Nessus

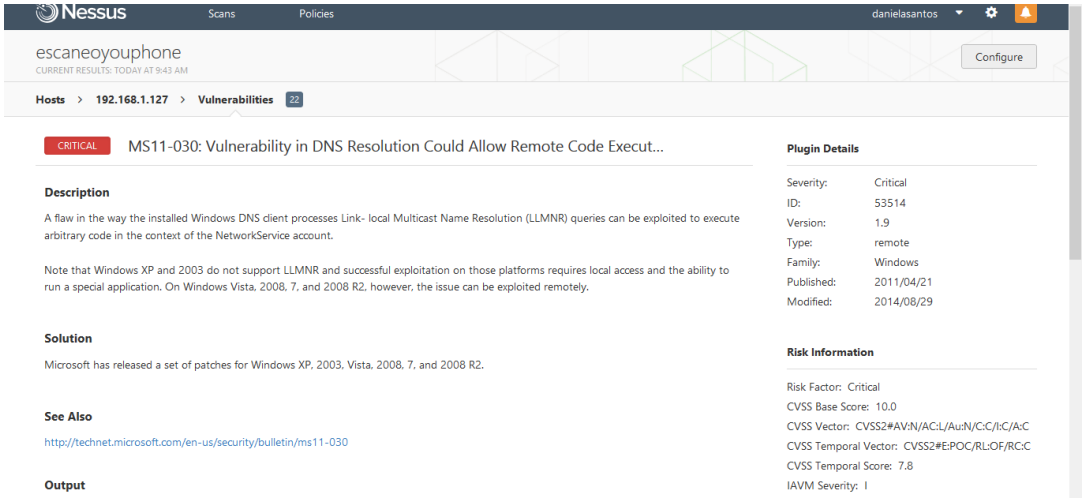

Figura 54 Visualización de error Critico en maquina cliente

Para contrastar los resultados obtenidos se utiliza la herramienta METASPLOIT en la cual se hace principalmente la prueba de escaneo de puertos para buscar vulnerabilidades. Este software utiliza una serie de

herramientas que explota estas vulnerabilidades y se puede determinar que los puertos tcp 21, tcp 135, tcp 139, tcp 514 tcp 445, tcp 1524, tco 6667 son principalmente los puertos que deben ser tomados en cuenta porque ya que son más susceptibles de ataques. El uso de este aplicativo esta mostrado en la figura 55.

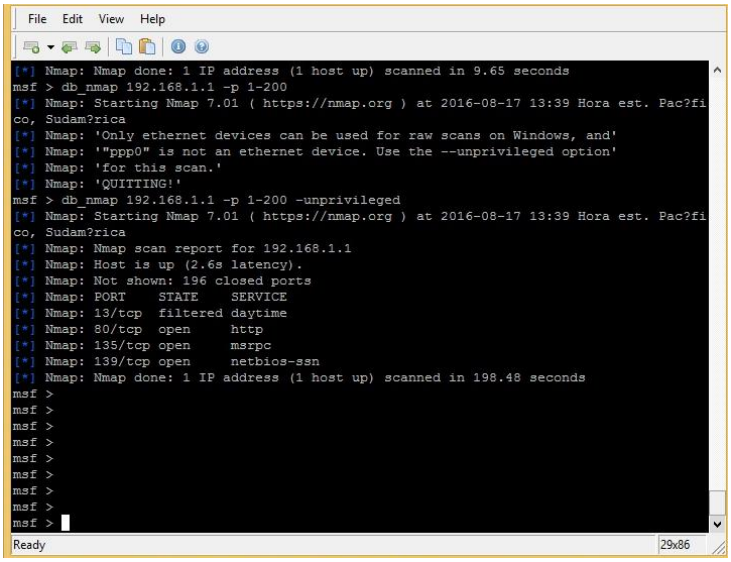

Figura 55 Escaneo mediante METASPLOIT al servidor 192.168.1.1

Las pruebas realizadas al servidor del condado shopping con dirección IP 192.168.1.1, y los resultados obtenidos se encuentra en el Anexo 1.

CAPÍTULO 4. TABULACIÓN Y ANÁLISIS DE RESULTADOS

En este capítulo se procede a hacer un resumen de los resultados así como tabular los mismos, luego se hace un análisis de lo obtenido y finalmente se procede a realizar los respectivos informes.

Dentro del campo administrativo se analiza también el costo del proyecto, para tener una idea certera del costo de la misma

4.1 Análisis de Costos

Para realizar el presente trabajo se necesita básicamente de un buen equipo portátil que tenga una tarjeta inalámbrica para poder conectarse a la red inalámbrica o al internet, más allá de estos costos en equipo no se necesita nada más, puesto que el software utilizado para el proceso de hacking ético ha sido bajado gratuitamente del internet, incluso aquellas herramientas que son pagadas, se ha podido trabajar sobre ellas en modo de prueba, lo cual ha sido suficiente para obtener resultados. Con respecto al Sistema Operativo se necesita una licencia Windows.

En el siguiente cuadro se muestra los costos utilizados en el proyecto.

Tabla 41.
Presupuesto Final proyecto auditoria Hacking Ético

Proyecto Hacking Ético		
Detalle	Precio unitario	Costo Total
Computador Portátil: - Procesador Intel Core I7 sexta generación - Disco Duro 1TB - Memoria Ram 12 GB	1250	1250
Licencia Sistema Operativo Windows 10	200	200
Configuración e instalación de software hacking ético	50	50
Servicio de Soporte Técnico	1000	1000
	Total	2.500,00

4.2 Resultados Obtenidos

4.2.1 Resultados etapa de Reconocimiento

Se obtienen los siguientes resultados:

Información de Dominio

Tabla 42
Resumen de datos obtenidos WHOIS

Status (Estado)	Delegated (Autorizado)
Created (Creado)	18 Aug 2008
Modified (Modificado)	04 Aug 2015
Expires (Expiración)	18 Aug 2016
Name Servers (Nombre de Servidores)	ns1.servicomecuador.com ns2.servicomecuador.com dns3.servicomecuador.com dns4.servicomecuador.com
Registrar Name (Entidad Registradora)	NIC.EC Registrar

Al aplicar el comando *nslookup* se observa que la IP donde se encuentra alojado el dominio 66.226.75.61

Con el comando traceroute os resultados son los siguientes:

- 192.168.1.210 Default Gateway de la red.
- Se demora 13 saltos hasta llegar al destino

VisualRoute nos muestra lo siguiente:

- Se demora 12 saltos en llegar a su destino.
- Salto intermedio en Alemania (Mainz)

- Se observa que el proveedor del servicio de Internet es Satnet.
- El hosting se encuentra alojado en Estados Unidos (Overland).
- Mapa visual de los saltos.

4.2.2 Resultados Etapa de Escaneo

Se puede observar los siguientes resultados según las capturas de pantallas obtenidas:

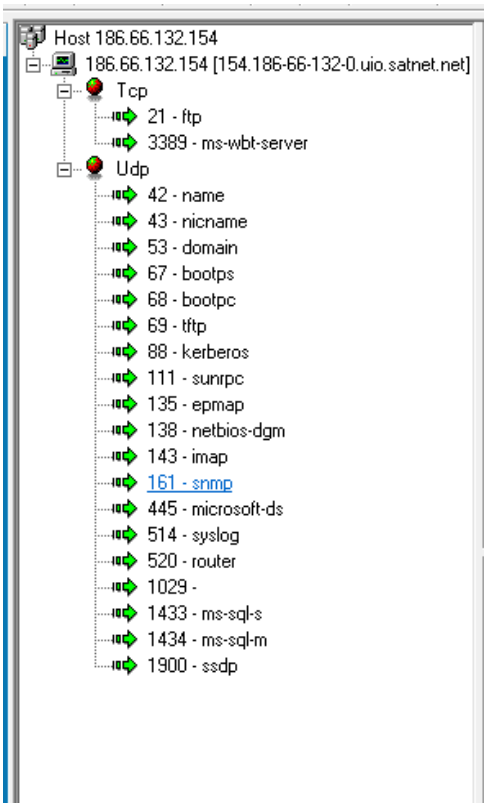

Figura 56 Captura específica del resultado en CAVS Condado

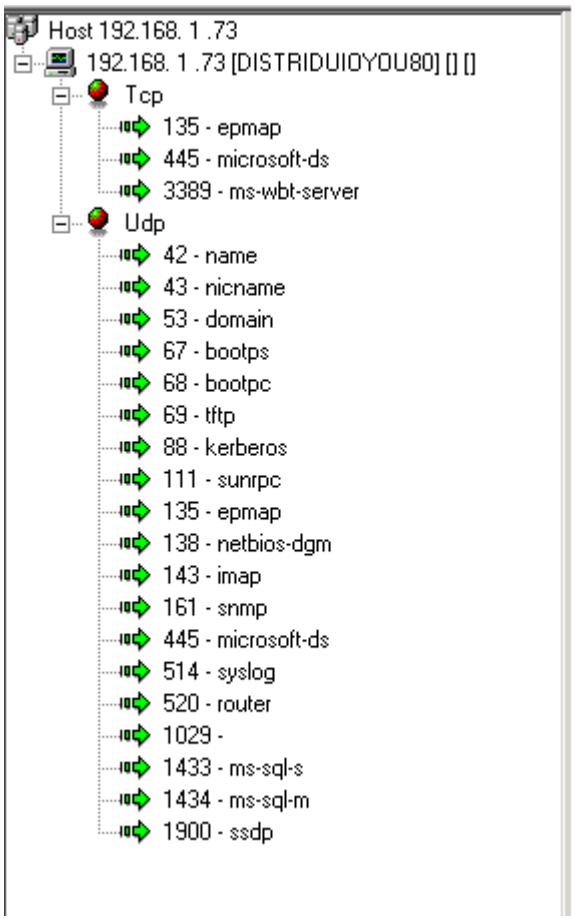

Figura 57 Captura específica del Resultado Máquina cliente

Los resultados de puertos que se obtuvieron son los siguientes:

En el Servidor CAVS Condado Shopping Facturación se obtuvo lo siguiente:

Tabla 43
Descripción y estado de puertos en el servidor CAVS Condado Shopping Facturación

EQUIPO	NUMERO DE PUERTO	PROTOCOLO	ESTADO
SERVIDOR CAVS CONDADO SHOPPING FACTURACIÓN 192.168.1.1	21	FTP	ABIERTO
	23	TELNET	CERRADO
	25	SMTP	CERRADO
	42	NAME	ABIERTO
	43	NICNAME	ABIERTO
	53	DNS	CERRADO
	59	DDC	CERRADO
	67	BOOTPS	ABIERTO
	68	BOOTPC	ABIERTO

	69	TFTP	ABIERTO
	79	FINGER	CERRADO
	80	HTTP	ABIERTO
	88	KERBEROS	FILTRADO
	110	POP3	CERRADO
	111	SUNRPC	FILTRADO
	113	IDENT	CERRADO
	135	RCP	ABIERTO
	138	NETBIOS-DGM	FILTRADO
	139	NETBIOS	ABIERTO
	143	IMAP	ABIERTO
	161	SNMP TOADNODE	FILTRADO
	162	SNMP	CERRADO
	389	LDAP	CERRADO
	443	SSL	CERRADO
	445	MSFT DS	ABIERTO
	514	SYSLOG	FILTRADO
	520	ROUTER	CERRADO
	1029		CERRADO
	1433	SQL SERVER S	FILTRADO
	1434	SQL SERVER M	ABIERTO
	5000	UPnP	CERRADO
	1900	SSDP	CERRADO
	3389	MS-WBT-SERVER	ABIERTO
	8080	Proxy Web	CERRADO

Tabulación de Resultados Obtenidos Servidor facturación CAVS Condado

Tabla 44
Descripción y estado de puertos en el servidor CAVS Condado Shopping INCELL

EQUIPO	NUMERO DE PUERTO	PROTOCOLO	ESTADO
SERVIDOR CAVS CONDADO INCELL192.168.1.2	21	FTP	CERRADO
	23	TELNET	CERRADO
	25	SMTP	CERRADO
	42	NAME	ABIERTO
	43	NICNAME	ABIERTO
	53	DNS	CERRADO
	59	DDC	CERRADO

	67	BOOTPS	ABIERTO
	68	BOOTPC	ABIERTO
	69	TFTP	ABIERTO
	79	FINGER	CERRADO
	80	HTTP	ABIERTO
	88	KERBEROS	FILTRADO
	110	POP3	CERRADO
	111	SUNRPC	FILTRADO
	113	IDENT	CERRADO
	135	RCP	ABIERTO
	138	NETBIOS-DGM	FILTRADO
	139	NETBIOS	ABIERTO
	143	IMAP	ABIERTO
	161	SNMP TOADNODE	FILTRADO
	162	SNMP	CERRADO
	389	LDAP	CERRADO
	443	SSL	CERRADO
	445	MSFT DS	ABIERTO
	514	SYSLOG	FILTRADO
	520	ROUTER	CERRADO
	1029		CERRADO
	1433	SQL SERVER S	FILTRADO
	1434	SQL SERVER M	ABIERTO
	5000	UPnP	CERRADO
	1900	SSDP	CERRADO
	3389	MS-WBT-SERVER	ABIERTO
	8080	Proxy Web	CERRADO

Tabla 45
Descripción y estado de puertos en el servidor CAVS CCI

EQUIPO	NUMERO DE PUERTO	PROTOCOLO	ESTADO
SERVIDOR CAVS CCI 192.168.1.1	21	FTP	ABIERTO
	23	TELNET	CERRADO
	25	SMTP	CERRADO
	42	NAME	ABIERTO
	43	NICNAME	ABIERTO
	53	DNS	CERRADO
	59	DDC	CERRADO
	67	BOOTPS	ABIERTO
	68	BOOTPC	ABIERTO
	69	TFTP	ABIERTO
	79	FINGER	CERRADO
	80	HTTP	ABIERTO
	88	KERBEROS	FILTRADO
	110	POP3	CERRADO
	111	SUNRPC	FILTRADO
	113	IDENT	CERRADO
	135	RCP	ABIERTO
	138	NETBIOS-DGM	FILTRADO
	139	NETBIOS	ABIERTO
	143	IMAP	ABIERTO
	161	SNMP TOADNODE	FILTRADO
	162	SNMP	CERRADO
	389	LDAP	CERRADO
	443	SSL	CERRADO
	445	MSFT DS	ABIERTO
	514	SYSLOG	FILTRADO
	520	ROUTER	CERRADO
	1029		CERRADO
	1433	SQL SERVER S	FILTRADO
	1434	SQL SERVER M	ABIERTO
	5000	UPnP	CERRADO
	1900	SSDP	CERRADO
	3389	MS-WBT-SERVER	ABIERTO
	8080	Proxy Web	CERRADO

A continuación se presenta una Tabla con el resumen de puertos abiertos

Tabla 46
Tabla de puertos abiertos, máquina de usuario

NOMBRE	NUMERO DE PUERTO	PROTOCOLO	ESTADO
DISTRIDUIOYOU73 (192.168.1.73)	42	NAME	ABIERTO
	43	NICNAME	ABIERTO
	53	DNS	ABIERTO
	67	BOOTPS	ABIERTO
	68	BOOTPC	ABIERTO
	69	TFTP	ABIERTO
	88	KERBEROS	ABIERTO
	111	SUNRPC	ABIERTO
	135	RCP	ABIERTO
	138	NETBIOS-DGM	ABIERTO
	143	IMAP	ABIERTO
	161	SNMP TOADNODE	ABIERTO
	445	MSFT DS	ABIERTO
	514	SYSLOG	ABIERTO
	520	ROUTER	ABIERTO
	1029		ABIERTO
	1433	SQL SERVER S	ABIERTO
	1434	SQL SERVER M	ABIERTO
	5000	UPnP	ABIERTO
	1900	SSDP	ABIERTO
	3389	MS-WBT-SERVER	ABIERTO

La herramienta Metasploit ayuda a contrastar los resultados de todas las pruebas hechas y bajó el número de vulnerabilidades en un rango de 6 puertos por maquina ya que en las pruebas salió algunos puertos como filtrados lo que significa que no se puede determinar que el puerto está totalmente abierto y no podría aceptar conexiones entrantes.

Aplicando el ping de la muerte se obtuvo:

Los tiempos de respuesta están alrededor de 17 a 26 ms, que se puede aclarar que es un tiempo normal, cuando se alteran los parámetros (PING DE LA MUERTE), los tiempos de respuesta son cada vez más lentos, por lo que se tiene una vulnerabilidad encontrada.

4.2.3 Resultados Etapa de Enumeración

En wireshark se observa lo siguiente:

El servidor 192.168.1.1 tiene varias conexiones TCP a diferentes direcciones IP's lo que significa que se tiene que cerrar puertos que no se necesiten para aplicaciones necesarias como son facturación Latinium e Incell.

Se puede observar puertos de aplicaciones no deseadas como p2p que consumen demasiado ancho de banda.

Nessus

Se corrobora lo que se tuvo en el wireshark y además nos muestra una visualización gráfica del estado del computador en análisis, mostrando una barra de colores desde blanco hasta rojo, donde rojo es la computadora que tiene un estado más crítico

4.3 Análisis de Resultados

El levantamiento de información, las pruebas de penetración "pentest", la revisión física y de software de los equipos informáticos permitió detectar posibles vulnerabilidades que representan posibles blancos de ataques. Al tener los resultados de todos estos procesos se deduce lo siguiente:

- Existen programas instalados innecesariamente en las computadoras de los empleados tales como juegos o aplicaciones para descargar música,

que vuelven lentos los computadores y no permiten trabajar al empleado de manera rápida, ya que la capacidad de memoria RAM de los computadores no soporta la instalación de este tipo de programas.

- Muchas de las computadoras tenían antivirus obtenidos de forma gratuita o si eran pagados estaban desactualizados, por lo que se encontraban desprotegidos y expuestos agravando el problema de lentitud de los equipos.
- Los parches de seguridad de los sistemas operativos no se encontraban actualizados, como es el caso de los servidores, por lo tanto representa un vulnerabilidad susceptible de ataque.
- Dentro de la fase de exploración o escaneo se encontraron puertos abiertos innecesariamente, convirtiéndose éstos en posibles blancos de ataque.
- Muchos equipos no tenían el firewall levantado incluyendo los servidores, es por eso que se pudo realizar el “ping de la muerte” en uno de los servidores, esto puede saturar al equipo y dejarlo fuera de servicio.
- Al aplicar los sniffers se pudo constatar que los empleados consumían demasiado ancho, se observó en el tráfico aplicaciones P2P, además ocupaban el internet para abrir redes sociales (Facebook, twiiter) y ver vídeos (youtube).
- El sistema que utilizan, muchas veces dejó de funcionar porque el empleado al querer trabajar de manera rápida, aplicaba reiteradas veces botones de aceptar del programa, saturando al aplicativo, provocando lentitud del servicio, lo que se puede concluir que el sistema que utilizan tiene fallas.

No existe una priorización de servicios, la red se encuentra lenta por los motivos anteriormente señalados, para mejorar este problema la empresa decidió crear una VPN, es decir hizo un cambio de tecnología, lo que en parte ayudó a arreglar el gran problema de la Lentitud del servicio al Cliente, sin

embargo no existía normas para que los empleados no utilicen recursos de internet o se les prohíba utilizar ciertos programas en horas de trabajo.

En los ítems siguientes se muestra el informe ejecutivo y el plan de optimización y priorización del tráfico en la red donde se describe de manera detallada tanto el proceso de evaluación así como el análisis de resultados con las respectivas recomendaciones del caso y procesos a aplicar.

4.3.1 Resumen Ejecutivo

El presente resumen tiene como objetivo detallar las pruebas de intrusión o “pentest” en la red interna de la empresa Youphone Cia. Ltda. Realizadas con el respectivo permiso del Gerente de la organización. Dichas pruebas se realizaron bajo el control de la Sra. Daniela Santos utilizando las técnicas de un hacker, para encontrar vulnerabilidades de seguridad.

Las pruebas que se realizaron permitieron la obtención de datos de dominio, escaneo de puertos, ataques de Denegación de servicio, pruebas de intrusión, etc.

Luego de analizar las pruebas realizadas se recomienda:

- Actualizar los parches de seguridad de los sistemas operativos, principalmente de los servidores, para evitar blancos de ataques.
- Desinstalar programas innecesarios que están abriendo puertos que pueden ser utilizados como “backdoors” por atacantes maliciosos.
- Configurar los routers de acceso a Internet de manera que los usuarios tengan acceso a aplicaciones estrictamente necesarias.
- Recomendar la desactivación de la DMZ (Zona Desmilitarizada) de los routers de acceso a internet ya que esto expone libremente a un equipo o un servidor a ataques externos.

- Implementar Servidores trampas para engañar a posibles atacantes.
- Elaborar un documento donde se explique claramente cómo usar y para qué usar los recursos informáticos tales como: Internet, Servidores, correo electrónico y equipos informáticos.
- Instalar software especializado con las opciones de antivirus, antispyware y antifishing.
- Recomendar la utilización de un firewall física en el “core” de red de datos para filtrar de una manera óptima el tráfico.
- Capacitar al personal sobre el uso de los navegadores de Internet, puesto que instalan complemento y aplicativos que vuelven lentos a los equipos y a su vez abren puertos por donde pueden atacar.

Detalle de las pruebas Realizadas

Al comenzar el proyecto se hizo un levantamiento total de la información informática de la empresa, es decir de cómo está estructurada la red de datos así cómo dónde se encuentran los equipos de usuario que lo componen con sus respectivas características técnicas.

Luego se procedió a realizar los 3 primeros pasos de la metodología de hacking ético:

1. **Reconocimiento:** se obtuvo información relevante sobre el dominio de la empresa, con lo cual se pudo realizar Ingeniería Social (Búsqueda de datos a través del Internet).

   Aplicaciones: WHOIS, Comando nslookup, Comando tracert y VisualRoute.
2. **Escaneo:** se realizó una búsqueda de IP’s, así como un escaneo de puertos en los servidores.

   Aplicaciones: Angry IP Scanner, Advanced Port Scanner y Network Auditor Security.

3. **Reconocimiento:** en esta fase se hizo un análisis del tráfico de la red (paquetes) así como un escaneo más a fondo de puertos e IP's.

   Aplicaciones: WireShark y Nessus.

Resultados Obtenidos

Servidores

La Tablade a continuación nos muestra un resumen obtenido de las pruebas realizadas

Tabla 47
Resumen de Escaneo de Puertos Servidores

DIRECCION IP	NOMBRE EQUIPO	PUERTOS ABIERTOS	VULNERABILIDADES DE SEGURIDAD
192.168.1.1	SERVIDOR CAVS CONDADO FACTURACIÓN	13	9
192.168.1.2	SERVIDOR CAVS CONDADO INCELL	12	8
192.168.1.1	SERVIDOR LOCAL CCI	13	9

- Servidor CAVS Condado Shopping Facturación: Al analizar los requerimientos del Programa para un correcto funcionamiento solo se debe tener abiertos los puertos 21 (FTP), 80 (HTTP), 1433 (SQL SERVER S) y 1434 (SQL SERVER M). Por lo que los otros que se encuentran abiertos son considerados agujeros de seguridad.

- Servidor CAVS Condado Shopping Incell: De manera similar para el correcto funcionamiento del software se tiene que tener abiertos los puertos 80 (HTTP), 1433(SQL SERVER S) y 1434(SQL SERVER M). Por lo que los otros que se encuentran abiertos son considerados agujeros de seguridad.

- Servidor CAVS CCI facturación debe tener abiertos los puertos 21 (FTP), 80 (HTTP), 1433 (SQL SERVER S) y 1434 (SQL SERVER M). Por lo que los otros que se encuentran abiertos son considerados agujeros de seguridad.

Máquinas Usuarios

Como las máquinas solo necesitan acceder al servicio de internet tanto páginas web seguras y no seguras así como acceso a los aplicativos como son el de facturación y de contratos INCELL, se necesitan que estén abiertos los puertos 80, 443, 1433 y 1434, es por esto que se necesitan cerrar los otros que no se estén ocupando.

Adicionalmente mediante el software Network Security Auditor se pudo observar que en la mayoría de las maquinas tenían instalado software para programas P2P (compartición de archivos), juegos y una seria de aplicativos que alterarían la seguridad informática de una manera muy peligrosa.

Tabla 48
Resumen de Escaneo de Puertos Usuarios Cavs CCI

IP	NOMBRE EQUIPO	P. ABIERTOS	VULNERABILIDADES
192.168.1.73	DISTRIDUIOYOU73	21	17
192.168.1.74	DISTRIDUIOYOU74	20	16
192.168.1.101	DISTRIDUIOYOU01	18	14
192.168.1.102	DISTRIDUIOYOU02	18	14
192.168.1.103	DISTRIDUIOYOU03	16	14
192.168.1.110	DISTRIDUIOYOU10	16	13
192.168.1.115	DISTRIDUIOYOU15	16	14
192.168.1.116	DISTRIDUIOYOU16	16	13
192.168.1.120	DISTRIDUIOYOU20	16	12
192.168.1.172	DISTRIDUIOYOU72	16	18

4.3.2 Plan de Optimización y priorización del tráfico en la red

El siguiente plan que tiene la finalidad de presentar las políticas de uso y acceso a los recursos informáticos de la empresa Youphone Cia. Ltda. Así como del internet y correo electrónico, para mejorar el tráfico de la red y mejorar la calidad de servicio al cliente externo

Política para la utilización de correo electrónico

Objetivo

El Correo Electrónico es un servicio que permite mantener comunicados a los usuarios internos entre sí, así como con el mundo exterior, permitiendo que los usuarios desarrollen sus actividades de trabajo.

El uso indebido de este recurso afecta a los usuarios que lo necesitan, razón por la cual se deben indicar las normas de buen uso del servicio.

Definición de la Política

Está permitido

- El uso del correo electrónico para actividades de trabajo.
- Enviar archivos adjuntos de información con un tamaño máximo de 25 Megabytes (MB); en caso de requerir enviar información de mayor tamaño, se deberá empaquetar con cualquier software especializado para ello, por ejemplo WinZip, que existe en el computador. Si a pesar de la compresión el archivo es mayor a 25 MB se deberá solicitar de manera escrita al área de tecnología y administración de redes, solicitando la ampliación temporal de los datos adjuntos.

- Enviar correos masivos dentro de la organización, únicamente desde las cuentas de correo relacionadas con la parte administrativa, como es el departamento de Administración de Sistemas y recursos humanos.
- Verifique que todos los archivos que se baje de la red no contengan virus.

No está permitido

- Acceder a cuentas de otros usuarios.
- Difundir o transmitir información que invada la privacidad de otro funcionario de la organización, así como comunicaciones con contenido de pornografía, actos racistas, informaciones o mensajes de carácter ofensivo a la dignidad de las personas.
- Transmitir mensajes que sean similares en su contenido, es decir, correos considerados como cadena.
- Difundir o transmitir hacia el exterior de la organización cualquier información que sea de uso exclusivo de los empleados de la compañía.
- Dar la dirección de correo electrónico del usuario o de otros colaboradores de la organización, a ciertas páginas del Internet, desde las cuales se envía publicidad.
- Abrir mensajes de remitentes desconocidos, porque puede tratarse de algún tipo de virus que provoque daños a la red de la organización.

Aspectos Importantes

Cabe recalcar que se realizará el seguimiento de las políticas indicadas e informará a la Gerencia General sobre su cumplimiento.

Una disposición enviada por el servicio de correo electrónico tiene igual validez que un memorando.

Cobertura de la Política

Esta política de seguridad debe ser acatada por todas las personas de los departamentos de la organización.

Penalidad

Si no se cumple con esta política se informará a la Gerencia General sobre su incumplimiento.

Políticas para la Utilización de Internet

Objetivo

El Internet que se utiliza en la organización es un recurso limitado y costoso que debe estar disponible y de forma oportuna a los usuarios para que desarrollen sus actividades laborables; el uso indebido de este recurso afecta a los usuarios que lo necesitan, razón por la cual se deben priorizar las necesidades y racionalizar el uso.

Definición de la Política

Las actividades laborales (investigaciones, prácticas, búsquedas de material, etc.) que se realizan en el Internet tienen prioridad de uso.

Las actividades laborables primordiales se realizan en el horario de 10h00 hasta las 21h00, en este horario se tendrá restricción de acceso (redes sociales, mensajería instantánea, etc.).

En caso de requerir utilizar el servicio para consultas o búsqueda de información no relacionada a la actividad laboral y que no sea prioritaria, se debe utilizase fuera del horario de 10h00 a 21h00 ya que se tendrá acceso a cualquier recurso de la red sin restricción.

Si al navegar por internet, alguna página de dudosa procedencia le solicita ingresar datos personales, tales como números telefónicos o números de tarjeta de crédito, no lo haga no ponga en riesgo su seguridad ni la de la

empresa.Evite usar radio y televisión on-line, ya que estos servicios demanda ancho de banda, recuerde que el Internet está a su disposición y todos necesitamos de ella.Si considera que existe alguna anomalía o deficiencia en el servicio de Internet, hágalo saber al responsable de la unidad informática.

No es permitido

- Navegar en páginas *Web* con contenido pornográfico, de violencia, de drogas, entre otros, por cuanto a más de distraer a los usuarios en temas ajenos a la organización, retrasa el trabajo de éstos y consume recursos de la organización.
- Usar programas, tales como el servicio de Chat, salvo en casos de estricta necesidad para el cumplimiento de tareas relacionadas con la organización, debido al gran consumo de ancho de banda y distracción de las actividades normales de trabajo.
- Descargar programas, música, videos ya que se desperdicia el ancho de banda de acceso a Internet.
- Queda prohibido el uso de Redes Sociales tales como Facebook, Twitter, entre otros.
- Malgastar el internet accediendo a sitios de entretenimiento on-line como vídeos o juegos.

Cobertura de la Política

Esta política de seguridad debe ser acatada por todos los funcionarios de los departamentos de la organización.

Cumplimiento de la Política

Se considera que el empleado ha cubierto esta política de seguridad si todo el tiempo de uso de Internet lo hace dentro del horario establecido, no accede a las páginas mencionadas en definición de la misma y no descarga archivos innecesarios.

Penalidades

En caso de no cumplirse con esta política de seguridad el usuario será amonestado verbalmente.

Políticas para la utilización de las Computadoras, Impresoras, Faxes

Objetivo

Los empleados de la organización son dependientes del hardware, es por eso que si existe alguna falla en los equipos, la eficiencia y operatividad de la organización corren peligro; el objetivo de la política es evitar el desperdicio de horas de trabajo en la reconfiguración, reparación de los equipos o servicios que se puedan ver afectados.

Definición de la Política

Los usuarios podrán acceder al computador sólo como usuario sin privilegios de administrador para evitar que puedan instalar cualquier tipo de aplicación ni puedan desconfigurar o configurar otros servicios en el sistema operativo, que alteren a la organización.

Los programas obtenidos desde el Internet directamente por parte de los usuarios, no podrán ser instalados para evitar problemas de virus informáticos.

En caso de requerir algún software nuevo o la modificación de alguno ya instalado en la computadora del usuario, se debe hacer una solicitud a la Unidad encargada.

Queda terminantemente prohibido a los usuarios tratar de hacer *hacking* interno hacia los servidores y computadoras personales de otros usuarios.

Sólo se permiten las impresiones de documentos relacionados con la organización.

La Unidad de Administración de Sistemas realizará la revisión esporádica de la utilización del hardware entregado a los empleados.

Cobertura de la Política

Esta política de seguridad debe ser acatada por todos los funcionarios de los departamentos de la organización.

Cumplimiento de la Política

Se considera que el empleado ha cubierto esta política de seguridad, si en la revisión casual de las computadoras no se encuentra otro software instalado a más de los que constan en la base de datos.

Penalidades

En caso de no cumplirse con esta política de seguridad el usuario será amonestado verbalmente; si es reincidente se informará a la Gerencia General sobre el uso del recurso informático otorgado.

Recomendaciones Generales

A la parte gerencial se le recomienda tener en cuenta los siguientes puntos:

- Actualizar los parches de seguridad de los sistemas operativos, principalmente de los servidores, para evitar blancos de ataques.
- Desinstalar programas innecesarios que están abriendo puertos que pueden ser utilizados como “backdoors” por atacantes maliciosos.
- Configurar los routers de acceso a Internet de manera que los usuarios tengan acceso a aplicaciones estrictamente necesarias.
- Recomendar la desactivación de la DMZ (Zona Desmilitarizada) de los routers de acceso a internet ya que esto expone libremente a un equipo o un servidor a ataques externos.

- Implementar Servidores trampas para engañar a posibles atacantes.
- Elaborar un documento donde se explique claramente cómo usar y para qué usar los recursos informáticos tales como: Internet, Servidores, correo electrónico y equipos informáticos.
- Instalar software especializado con las opciones de antivirus, antispyware y antifishing.
- Levantar el firewall de los computadores y servidores.
- Recomendar la utilización de un firewall física en el “core” de red de datos para filtrar de una manera óptima el tráfico.
- Capacitar al personal sobre el uso de los navegadores de Internet, puesto que instalan complemento y aplicativos que vuelven lentos a los equipos y a su vez abren puertos por donde pueden atacar.

CAPÍTULO 5. CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

- El Hacking ético tiene como principal objetivo darle otro punto de vista a aquellas personas que dedican su vida profesional a vulnerar sistemas de información para convertir esto en un método de protección, permitiendo a todas las organizaciones atacarse y poder mejorar sus soluciones, así como darse cuenta de forma actualizada de sus debilidades.
- Este trabajo fue de mucha importancia ya que con este se pudo, tener un conocimiento real de las vulnerabilidades y fallas del sistema informático, estado de equipos y parches de seguridad, determinar configuraciones erróneas o de baja seguridad en los equipos de red como routers y switchs, y por último redactar las políticas de seguridad y uso de los sistemas informáticos para un manejo correcto de los recursos.
- El modelo de Listas Combinas o CheckList es muy práctico, ya que permite de manera sistemática ir apuntando las etapas que se van realizando y los por menores de cada una de ellas. Este modelo además permite tener una constancia física (No digital) del trabajo que se está realizando
- Realizar una auditoría de hacking ético toma tiempo y esfuerzo, ejecutarlo sin causar daños a la información requiere conocimiento y experiencia. Es importante utilizar herramientas probadas y de buena

fuente ya que si instalamos software desconocido podemos realizar daños en los datos y hasta abrir puertas para ataques futuros.

- Los hackers generalmente tienen mala reputación porque se piensan que estos hacen daño, en este trabajo se demostró la otra cara de los hackers, ya que ocupando el conocimiento y las herramientas correctas se pueden dar recomendaciones para evitar problemas.

- Cada aplicativo de red generalmente ocupa puertos de conexión, para una buena seguridad se tiene que documentar que puertos son los necesarios para abrirlos y cerrar los que no se ocupan. Evitando tener agujeros de seguridad en las computadoras de los usuarios.
- Se concluye también que teniendo una adecuada documentación de los equipos informáticos, equipos de red, recursos, personal, información, se podrá solventar de una manera más óptima una caída o paro del sistema sucedido ante un ataque informático.
- Teniendo herramientas informáticas analizando el tráfico de toda la red de datos entrante y saliente como Wireshark se tendrá estadísticas y datos importantes que permitirán de manera rápida una reacción ante un ataque.
- Un trabajo preventivo, políticas de seguridad bien definidas y difundidas y capacitaciones constantes a todos los usuarios y colaboradores a futuro darán ahorros significativos para la empresa. Ya que es más fácil corregir un error que configurar desde cero un sistema.
- Los equipos de red como son routers y switchs deben estar actualizados su firmware, ya que hay varios ataques sobre estos equipos y si estos equipos fallan se perdería la conexión con el mundo exterior y esto en una empresa como Youphone Cía. Ltda. No podría trabajar ocasionando pérdidas económicas de alta cuantía.

- Las personas que poseen conocimientos de seguridad de información deben darles su importancia en cuanto a tecnología, puesto que el insumo principal de toda empresa es la información, por lo tanto si existen especialistas en cuidar este gran valor de las organizaciones y tienen la experiencia suficiente para dar un valor agregado a cuidar la información, son obligadamente un recurso muy valioso e importante dentro de la compañía.

5.2 Recomendaciones

- Se recomienda la compra de un firewall físico que analice el comportamiento de la red ya que siendo hardware el procesamiento de la información no va a provocar ralentización del servicio. Adicional a esto también adquirir equipos IPS (Intrussion Protection System) que ayudará a evitar caídas en el sistema informático ya que notificaran al administrador de cualquier problema.
- Se recomienda capacitaciones constantes a los colaboradores de la organización, ya que según estadísticas hay un alta probabilidad de que estos instalen software malware que pondría afectar la seguridad informática de la información.
- Se recomienda llevar una bitácora de todos los cambios en las configuraciones, claves, permisos en el área informática, con esto se podrá realizar cualquier reconfiguración de una manera eficaz.
- Adicional a todo esto se recomienda también realizar un plan de recuperación de desastres en distintos ámbitos, en especial sobre la red de datos, este plan de recuperación puede ser otro tema de estudio ya que se deben tomar todos los parámetros y evaluar todos los riesgos que se tengan y tener una respuesta rápida y responsables directos.

- Es importante que este modelo de CheckList sea de conocimiento para los estudiantes de sistemas de la Universidad, para que vean sus ventajas y también sus desventajas y puedan aplicarlo en sus proyectos y puedan discutir los resultados.

Bibliografía

ÁLVAREZ, G. P. (2010). *Seguridad informática para empresas y particulares.* Madrid: McGraw-Hill.

Astudillo, K. (2013). *Hacking Ético 101: cómo hackear profesionalmente en 21 días o menos.* San Bernandino: California.

CCM. (s.f.). Obtenido de http://es.ccm.net/contents/357-traceroute

Exploiter. (s.f.). Obtenido de https://exploiter.co/

Graves, K. (2010). *Ethical Hacking.* Sybex.

HARRIS, S. (2005). *Hacking ético. Traducción de: Gray hat hacking.* Madrid: Anaya Multimedia.

Ihacker. (2016). Obtenido de www.ihacker.co

Información, A. E. (2004,). *Reglamento (CE) n 460/2004 del Parlamento Europeo y del Consejo.*

KATZ, M. (2013). *Redes y Seguridad.* Buenos Aires: Alfaomega.

Morales, R. G. (2015). *Implementación del Sistema de Gestión de Eventos de Seguridad de la Información (OSSIM) en la Infraestrucutura de Red del GAD de la provincia de Chimborazo.* Escuela Superior Politécnica del Chimborazo.

Nebrija. (2016). Obtenido de https://www.nebrija.es/~cmalagon/seguridad_informatica/transparencias/Modulo_0.pdf

pdcahome. (2016). Obtenido de http://www.pdcahome.com/check-list/

PICUOTO, F. (2004). *Hacking práctico.* España: Anaya Multimedia.

Ramagaes.com. (12 de 12 de 2015). *Informática General*. Obtenido de Auditorias de Seguridad: http://www.ramagaes.com/es/bs-hacking.html

Real Academia de la Lengua. (15 de 01 de 2016). Obtenido de http://www.rae.es

Red y Seguridad. (05 de 12 de 2015). Obtenido de http://redyseguridad.fi-p.unam.mx/proyectos/tsi/capi/Cap2.html

Redes @ Zone. (2016). Obtenido de http://www.redeszone.net/2014/01/18/zenmap-la-interfaz-grafica-oficial-de-nmap-para-escanear-puertos-a-fondo/

SALLIS, E. C. (2010). *Ethical Hacking Un enfoque metodológico para profesionales.* Buenos Aires: Alfaomega.

We Live Security. (18 de 03 de 2016). Obtenido de http://www.welivesecurity.com/la-es/2014/02/19/maltego-herramienta-muestra-tan-expuesto-estas-internet/