ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA ELECTRÓNICA EN TELECOMUNICACIONES Y REDES

"ESTUDIO COMPARATIVO ENTRE SERVIDORES MIKROTIK Y CISCO BAJO EL ESTÁNDAR DE SEGURIDAD 802.1X PARA SERVICIOS DE RED EN LA EMPRESA GUANO.NET"

Trabajo de titulación presentado para optar al grado académico de:

INGENIERO EN ELECTRÓNICA, TELECOMUNICACIONES Y REDES

AUTOR: GALO PATRICIO HURTADO CRESPO

TUTOR: ING. MSC. VINICIO RAMOS V.

Riobamba – Ecuador

2017

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA EN ELECTRÓNICA, TELECOMUNICACIONES Y REDES

El Tribunal del Trabajo de Titulación certifica que el proyecto técnico: ESTUDIO COMPARATIVO ENTRE SERVIDORES MIKROTIK Y CISCO BAJO EL ESTÁNDAR DE SEGURIDAD 802.1X PARA LOS SERVICIOS DE RED EN LA EMPRESA GUANO.NET, de responsabilidad del señor Galo Patricio Hurtado Crespo, ha sido minuciosamente revisado por los Miembros del Tribunal del Trabajo de Titulación, quedando autorizada su presentación.

NOMBRE	**FIRMA**	**FECHA**
Ing. Washington Luna **DECANO FACULTAD DE INFORMÁTICA Y ELECTRÓNICA**	_____	_____
Ing. Franklin Moreno **DIRECTOR DE ESCUELA DE INGENIERÍA ELECTRÓNICA TELECOMUNICACIONES Y REDES**	_____	_____
Ing. Msc. Vinicio Ramos **DIRECTOR TRABAJO DE TITULACIÓN**	_____	_____
Ing. Germania Veloz **MIEMBRO DEL TRIBUNAL**	_____	_____

Yo, Galo Patricio Hurtado Crespo declaro ser el autor del presente trabajo de titulación: "ESTUDIO COMPARATIVO ENTRE SERVIDORES MIKROTIK Y CISCO BAJO EL ESTÁNDAR DE SEGURIDAD 802.1X PARA LOS SERVICIOS DE RED EN LA EMPRESA GUANO.NET" que fue elaborado en su totalidad por mi persona, bajo la dirección del Ingeniero Vinicio Ramos V, siendo totalmente responsable de las ideas, doctrinas y resultados expuestos en este Trabajo de Titulación y el patrimonio de la misma pertenece a la ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO**.**

GALO PATRICIO HURTADO CRESPO

DEDICATORIA

Esta tesis la dedico a mi familia que ha estado presente en todo momento para poder dar un paso importante en mi vida profesional.

A mis padres de manera especial a mi madre que siempre con sus consejos, apoyo en los momentos difíciles, comprensión y aporte económico ha servido para concluir este trabajo de titulación. Me han inculcado de valores, virtudes, mi perseverancia y carácter para afrontar este reto y cumplir con mi objetivo.

A mis hermanos que han sido el pilar fundamental en esta etapa de mi vida, son la razón de seguir luchando cada día por ser mejor persona y poder colaborar con la sociedad.

Galo Patricio Hurtado Crespo

AGRADECIMIENTO

Agradezco a Dios y a mis padres por brindarme esta oportunidad de crecer académica y personalmente.

A mis hermanos por ser el pilar fundamental de superación.

A la Escuela Superior Politécnica de Chimborazo por brindarme la oportunidad de formarme como profesional.

De manera especial quiero agradecer al Ing. Msc. Vinicio Ramos V., a la Ing. Msc. Germania Veloz, al Ing.Msc. Raúl Lozada, Ing. Christiam Nuñez y al Dr. Iván Moyota por sus inestimables aportes en el desarrollo y culminación de mi carrera estudiantil. Sin su apoyo, hubiera sido más difícil llegar hasta el objetivo propuesto inicialmente.

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE IMÁGENES

ÍNDICE DE GRÁFICOS

ÍNDICE DE ANEXOS

RESUMEN

Se realizó un estudio comparativo entre servidores de seguridad CISCO Y MIKROTIK en la empresa GUANO.NET bajo el estándar de seguridad 802.1x para garantizar la confidencialidad de datos que los usuarios transmiten por la red de la empresa. El estudio se desarrolló en tres partes, la primera un análisis de la situación actual de la red, en la segunda parte para establecer políticas de seguridad y en la tercera parte se desarrolló tablas comparativas para poder establecer una diferencia entre las dos marcas de dispositivos. En primera instancia se realizó un escaneo de los puertos y de los datos que se transmiten por la red mediante el uso de herramientas como nmap, Zenmap y tcpdump, también se realizaron diferentes tipos de ataques a la red cuyo objetivo fue encontrar vulnerabilidades, amenazas o irregularidades que influyan en el tráfico normal de datos. De acuerdo a estas pruebas realizadas en la segunda etapa se implementaron políticas de seguridad para proteger la red de las diferentes anomalías encontradas. Finalmente se desarrollaron tablas comparativas para determinar el comportamiento de los servidores de seguridad de CISCO y MIKROTIK, es fundamental en el diseño de la red definir correctamente los modelos y las marcas que se van a utilizar para la prestación de servicios, analizando las ventajas y desventajas a corto y largo plazo. De acuerdo al análisis de la red en una primera instancia la seguridad de la empresa presentaba un nivel mínimo; este resultado se pudo determinar realizando los diferentes tipos de ataques. Se concluyó que los mecanismos de seguridad implantados con políticas incorporados ofrecen y garantizan un nivel alto de confidencialidad de los datos de los usuarios. Se recomienda que al implementar un nuevo proveedor de servicios de internet (ISP), además de proveer alta disponibilidad de la red se tiene que tener presente el nivel de seguridad de la información que transmiten los usuarios.

PALABRAS CLAVES: <TECNOLOGÍA Y CIENCIAS DE LA INGENIERÍA>, <REDES DE COMPUTADORES> <SERVIDORES DE SEGURIDAD>, <POLÍTICAS DE SEGURIDAD>, <CISCO>, <MIKROTIK>, <ESTÁNDAR 802.1X>, <ATAQUES INFORMÁTICOS>.

INTRODUCCIÓN

En los últimos tiempos las redes de computadoras han ido evolucionando de manera rápida, así como la demanda de los usuarios entonces como proveedor de servicios de internet (ISP) lo que se busca es poder brindar confidencialidad que los documentos, archivos u otro tipo de información que se esté manejando sea segura y confiable.

Con la funcionalidad y el nuevo uso que se da la red trae consigo muchos riesgos de seguridad muchos de ellos se producen por la inexistencia o carencia de mecanismos de seguridad suficientemente capaces de proteger el acceso a la información de los usuarios.

Inicialmente en los equipos CISCO se plantearon muchas recomendaciones referentes a la seguridad en redes inalámbricas pero como la demanda no era significante y al pasar del tiempo luego de sufrir una serie de ataques, se dio inicio a la búsqueda de vulnerabilidades pero los resultados comenzaron a generar desconfianza y confusión, para posteriormente pariendo desde el mismo principio pero mejorando el diseño y estableciendo ya ciertas políticas implementar seguridad tanto en las redes físicas como en las redes inalámbricas.

Se tienen que plantear más soluciones o políticas de seguridad, para establecer un mejor control en el acceso a los recursos de la red y de esta manera proteger la información de los usuarios que por las redes inalámbricas se transmiten.

FORMULACIÓN DEL PROBLEMA

¿Cuál de los servidores de seguridad CISCO o MIKROTIK es más vulnerables a ataques bajo el estándar de seguridad 802?1X?

SISTEMATIZACIÓN DEL PROBLEMA

¿Cómo afecta las características actuales de la infraestructura de red de la empresa GUANO.NET en el parámetro de seguridad?

¿Qué parámetros deben ser tomados en cuenta para el análisis de la red interna?

¿Qué características del estándar 802?1x aportarían a mejorar la seguridad del servidor?

¿Cuál de los servidores CISCO o MIKROTIK ofrecen mejores prestaciones?

JUSTIFICACIÓN DEL TRABAJO DE TITULACIÓN

JUSTIFICACIÓN TEÓRICA

En la empresa GUANO.NET se ha vuelto imperiosa la necesidad de poder proveer a la institución de una óptima administración del internet, asegurar la información de los usuarios que transmiten sus datos por la red, optimizando el sistema de seguridad para lograr un control de acceso y utilización de los recursos de la red.

Mantener la confidencialidad de la información siempre será el punto más alto requerido por los usuarios de dicho servicio, para esto también se podrían establecer políticas de seguridad internas y de control de acceso a la información, esto va de la mano con la implementación de protocolos y servidores de seguridad que cumplan con los requisitos de estabilidad, confidencialidad y seguridad de la información.

Como ingenieros Electrónicos en Telecomunicaciones y Redes tenemos que dar soluciones a los posibles problemas que se puedan presentar en el campo de seguridad en redes, son de gran importancia hoy en día tanto en la institución pública y privada, involucrándonos directamente para garantizar la confiabilidad en la transmisión de datos de los usuarios, tomando como punto de partida las políticas de seguridad que establece el estándar de seguridad 802.1x.

JUSTIFICACIÓN APLICATIVA

En la red de la empresa GUANO.NET se implementará un servidor de seguridad con diferentes tipos de políticas que se establecen en el estándar de seguridad 802.1x y que de esta manera permitirá asegurar la información de los usuarios que se esté trasmitiendo por la red.

Por lo tanto, es necesario hacer un estudio de la situación actual para poder identificar las diferentes vulnerabilidades que se puedan presentar y de acuerdo a este resultado posteriormente implementar las diferentes soluciones.

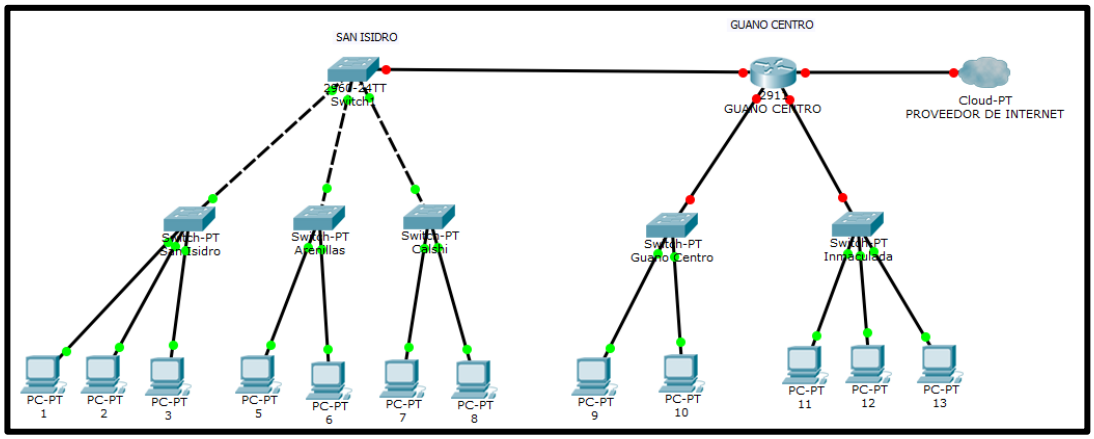


Figura 1: Escenario actual de red GUANO.NET

Realizado Por: Galo Hurtado C. 2017

La disponibilidad de información que se tiene en la empresa es uno de los recursos fundamentales para el trabajo de investigación a realizarse y de esta forma poder dar una solución óptima e inmediata que nos garantice el correcto funcionamiento de los equipos y donde la información que se transmite por el mismo sea segura y confiable.

Se utilizará el sistema Linux y sus variantes como plataformas para la configuración de este análisis, solución y disminución de los problemas que se pueda presentar en la red y prevenir ataques que pongan en peligro la integridad de los datos.

OBJETIVOS

OBJETIVOS GENERALES

- **Estudiar y comparar funcionamiento entre servidores mikrotik y cisco bajo el estándar de seguridad 802.1x que se implementara en la empresa GUANO.NET**

OBJETIVOS ESPECÍFICOS

- Realizar un análisis de la situación actual de los servicios de red de la empresa GUANO.NET
- Estudiar el estándar de seguridad 802.11x.
- Configurar servidores con tecnología CISCO Y MIKROTIK bajo el estándar de seguridad 802.1x en la empresa GUANO.NET
- Evaluar los resultados obtenidos en la implementación de los servidores de seguridad CISCO y MIKROTIK

CAPITULO I

1. FUNDAMENTO TEÓRICO

1.1 Introducción

En el presente capítulo se realizó una descripción de todos los elementos que se utilizan para la elaboración del siguiente trabajo de titulación describiendo su comportamiento de forma teórica y posteriormente de forma aplicativa.

Los elementos descritos a continuación son herramientas empleadas en los diferentes análisis de la red que permitieron cumplir los objetivos establecidos anteriormente.

1.2 Metodología

El tipo de investigación científica que se utiliza en el presente trabajo es la descriptiva, de Laboratorio y transversal detallada a continuación:

- ✓ El reconocimiento minucioso del objeto o caso de estudio.
- ✓ A través del planteamiento del problema se resolverán las interrogantes expuestas.
- ✓ Después de realizar la configuración de los servidores bajo los estándares establecidos, se obtendrán resultados los cuales servirán para realizar gráficas y tablas para su fácil análisis y comprensión.
- ✓ Se realizará el análisis de las vulnerabilidades encontradas para posteriormente dar una explicación del comportamiento y de los fenómenos que se observan, concluir la implementación del servidor de seguridad incorporado en esta empresa y su correcto funcionamiento.

El ciclo de vida adoptado para la ejecución del Proyecto de Tesis es:

- ✓ Recopilación de la información
- ✓ Clasificación de la información
- ✓ Formulación
- ✓ Comprobación
- ✓ Evaluación de Resultados

- ✓ Conclusiones.

Las técnicas a utilizar en la elaboración de este proyecto, son las siguientes:

- ✓ Observación
- ✓ Delimitación del tema
- ✓ Formulación del problema
- ✓ Reducción del problema a nivel empírico
- ✓ Determinación de las unidades de análisis-Recolección de datos
- ✓ Análisis de datos
- ✓ Informe final.

1.3 Plan general de trabajo

Este proyecto se lo tratara de desarrollar en 3 capítulos, cada uno de ellos se divide en aspectos netamente del proyecto en los cuales se tratan todo lo encontrado como base, desde una mirada rápida a los conceptos básicos de servidores PROXY hasta las recomendaciones del estándar 802.11 de seguridad en redes, la función de cada uno las técnicas de configuración de cada uno de los servidores cumplir con los parámetros que se establecieron y comprobar toda su funcionalidad.

A continuación, se detalla en pocas palabras lo que contendrá cada capítulo del proyecto propuesto:

Capítulo 1, Hace referencia a la fundamentación teórica donde va a estar detallado toda la parte teórica de las herramientas que puedan utilizar para el desarrollo del trabajo de titulación.

Capítulo 2, En este capítulo se puede enfocar en la parte aplicativa detallando de todo lo que se hizo de acuerdo a la parte teórica.

Capítulo 3, Se presentan los resultados obtenidos, los mismos nos servirán para realizar el análisis comparativo entre la seguridad que ofrece CISCO y MIKROTIK en el ISP.

Después de estos capítulos y contenidos se pone a consideración de un summary, anexos, donde se muestra información técnica relevante de las recomendaciones del estándar 802.11.

1.4 Direccionamiento IP

Se ha clasificado de cuatro maneras dependiendo de la función que vaya a realizar:

1.4.1 Direcciones IP públicas.

Son visibles en todo Internet. Un ordenador con una IP pública es accesible o visible desde cualquier otro ordenador conectado a Internet. Para conectarse a Internet es necesario tener una dirección IP pública. a). (Liserre, 2011)

1.4.2 Direcciones IP privadas

También se les conoce como direcciones IP reservadas y son visibles únicamente por otros hosts de su propia red o de otras redes privadas interconectadas por router´s. En este caso los ordenadores con direcciones IP privadas pueden salir a Internet por medio de un router o de un proxy dependiendo del diseño inicial de la red que tenga una IP pública.
Se tiene que tener en cuenta que desde el internet no se puede tener acceso a los ordenadores con direcciones IP privadas. b). (Liserre, 2011)

1.4.3 Direcciones IP estáticas

También conocidas como direcciones IP fijas y consiste en que un host que se conecte a la red con dirección IP estática siempre lo hará con una misma IP.
Las direcciones IP públicas estáticas son las que utilizan los servidores de Internet con el único objetivo de estar siempre visible, localizables por los usuarios de internet y para los administradores de la red. (Liserre, 2011)
Por lo general en nuestro país esas direcciones se deben contratar, pero cuando se establece un contrato con un proveedor de fibra en este caso nos asignan de 4 a 5 IP estáticas.

1.4.4 Direcciones IP dinámicas.

Estas sirven cuando un host que se conecte a la red mediante dirección IP dinámica, cada vez lo hará con una dirección IP distinta.
Las direcciones IP públicas dinámicas son las que se utilizan en las conexiones a Internet mediante un equipo final que en nuestro caso se encuentra en el cliente final.

En los proveedores de internet necesariamente se tiene que utilizar las direcciones IP dinámicas por que se tiene un número grande de clientes y en la mayoría de los casos se conectan todos a la vez. c). (Liserre, 2011)

Estándares de comunicación de área local y comunicaciones inalámbricas

En cuanto a comunicaciones se refiere podemos tomar como puntos de referencia la forma de transmitir la información para poder clasificarlos de la siguiente manera:

- ✓ El sistema cableado utiliza como medios guiados por un medio físico para transmitir la información es un medio sumamente confiable, pero se muestran complicaciones al momento de querer expandir nuestra red, llegar a lugares mucho más lejanos se dificulta por los costos y por la complejidad del acceso al sitio.

- ✓ Los sistemas inalámbricos utilizan como medio de transmisión de información el aire esto es si nos permite llegar a lugares mucho más distantes peor de la misma manera se puede tener un nivel alto de vulnerabilidades. a). (Gimenez, 2008)

1.5.1 El estándar 802.11

El objetivo del estándar es proveer a los diferentes equipos, estaciones de trabajo y maquinarias que requieran de una conectividad inalámbrica permitiendo así la movilidad de los usuarios, el mismo trabaja en la banda de frecuencia de las redes LAN cumpliendo con ciertas funciones como las que se describen a continuación.

- ✓ Describe las funciones y servicios que requiere un dispositivo que este dentro de esta red
- ✓ Define el proceso de la MAC para poder dar soporte a los servicios de entrega de datos.
- ✓ Define las técnicas de señalización y funciones que van a ser controladas por la MAC.
- ✓ Describe los procedimientos y requerimientos necesarios para poder dar privacidad a la información que se transmite dentro del medio inalámbrico. b). (Gimenez, 2008)

1.5.2 El estándar 802.1x

Es un estándar propietario de la IEEE que nació con el objetivo de controlar el acceso a una red mediante un proceso de autenticación que habilita o impide el paso de los dispositivos que se conectan a un puerto de red LAN, se puede implementar en redes cableadas como en redes inalámbricas. (Chamorro, 2005)

Para poder realizar la implementación de este estándar se deben cumplir con los siguientes requerimientos:

- ✓ El usuario que intente acceder a la red.
- ✓ Punto de acceso que va a decidir si habilita o impide el ingreso al usuario.
- ✓ El servidor de autenticación se encarga de negociar y validar la identidad del cliente.

Entre las principales recomendaciones del estándar se encuentran:

- ✓ Evitar la difusión del identificador de red o el SSID (Service Set Identifier)
- ✓ Establecer listas de control de acceso o filtrado MAC (Media Access Control).
- ✓ Segmentar los puntos de acceso inalámbricos en zonas de seguridad administradas por un firewall. (Chamorro, 2005)

Inicialmente surgió el protocolo de autenticación WEP el cual utiliza una clave secreta estática que es compartida por el punto de acceso y todos los clientes que accedan a través de este a la red, y con la cual se realiza la autenticación a la red y la protección de los datos. (Chamorro, 2005).

Una de las principales debilidades de seguridad se presenta por el manejo estático de su llave y el uso de un vector de inicialización este se puede identificar en los paquetes transmitidos, de manera periódica, una vez se encuentre esta llave de cifrado se puede comenzar a capturar todo el tráfico que se esté manejando por la red. (Chamorro, 2005)

WPA utiliza 802.1x como mecanismo de control de acceso y autenticación a la red, y para generar y entregar las llaves de sesión WPA a los usuarios autenticados. Para corregir las principales debilidades el protocolo utiliza un contador y realiza una función de mezcla de por paquete, previniendo así los ataques de clave de WEP. (Chamorro, 2005). Adicionalmente, WPA utiliza una función de inscripción llamada MIC (Message Integrity Code) con la cual

verifica la integridad de los mensajes transmitidos y previene que atacantes capturen paquetes, los modifiquen y los reenvíen. (Chamorro, 2005)

1.4 Kali Linux

"Kali Linux es una distribución Linux basada en Debian avanzada dirigida a las pruebas de penetración y auditoría de seguridad. Kali contiene varios cientos de herramientas destinadas a diversas tareas de seguridad de la información, tales como pruebas de penetración, análisis forense y la ingeniería inversa. Kali Linux es desarrollado, financiado y mantenido por Ofensiva de Seguridad, una empresa líder de formación en seguridad de la información." (https://hackerhats8080.blogspot.com/, s.f.)

Kali Linux está diseñado específicamente para las necesidades de los profesionales de pruebas de penetración, en este caso se pretende utilizar estas pruebas para buscar el mayor tipo de vulnerabilidades que se puedan presentar en los equipos implementados en la empresa GUNO.NET tanto en equipos CISCO como en MIKROTIK y por lo tanto toda la documentación que se pueda obtener de estas pruebas servirán para poder corregir errores a futuro al momento de emprender en una compañía como es la de un proveedor de internet ISP. (Quezada, 2015).

1.4.1 Características de Kali Linux

Kali Linux es una completa reconstrucción de BackTrack Linux, y se ha puesto en funcionamiento toda una nueva infraestructura, todas las herramientas han sido revisadas y se han mejorado mediante las actualizaciones. (Quezada, 2015).

Las múltiples mejoras que se presentan se describen a continuación:

• Más de 300 herramientas de Pruebas de Penetración
• Es Libre y siempre lo será
• Amplio soporte para dispositivos inalámbricos
• Entorno de desarrollo seguro
• Varios lenguajes
• Completamente personalizable

Aprovechando estas ventajas que nos ofrece se puede utilizar estas herramientas posteriormente en el desarrollo de la tesis. (Quezada, 2015).

1.4.2 "Política de Kali Linux Open Source

Kali Linux es una distribución de Linux que agrega miles de software libre paquetes en su principal sección. Como un derivado de Debian, todo el software básico de Kali Linux cumple con las directrices de software libre de Debian.

Kali Linux también contiene varias herramientas que no son de código abierto, pero que han sido puestos a disposición para su redistribución por ofensiva de seguridad a través de acuerdos de licencia por defecto o específica con los proveedores de esas herramientas." (4)

1.4.3 Linux en el Ecuador

El día jueves 10 de abril del 2008 se emitió el decreto 1014 por parte de la presidencia del Ecuador. Rafael Correa Delgado que promueve el uso de software libre en las instituciones públicas del Ecuador. (Publica)

"Art. 1: Establecer como política pública para las entidades de administración Pública central la utilización del Software Libre en sus sistemas y equipamientos informáticos.

Art. 2: Se entiende por software libre, a los programas de computación que se pueden utilizar y distribuir sin restricción alguna, que permitan el acceso a los códigos fuentes y que sus aplicaciones puedan ser mejoradas.

Art. 3: Las entidades de la administración pública central previa a la instalación del software libre en sus equipos, deberán verificar la existencia de capacidad técnica que brinde el soporte necesario para este tipo de software." (Publica)

De manera simultánea las empresas privadas trabajan de forma directa con las públicas y para la optimización y convergencia de datos o información que se manejen se vio la necesidad de poder también trabajar en la plataforma libre de Linux teniendo como base para implementar los servidores tomando en cuenta que es un sistema operativo open source y presenta un nivel de seguridad robusto ante los diferentes tipos de ataques que se puedan presentar en la empresa GUANO.NET.

Linux es un sistema operativo open source que está en constante actualización por parte de los usuarios, permitiendo de esta manera ser uno de los softwares más seguros con la ventaja que vienen sistemas antivirus ya implementados como ClamAV.

1.5 CONCEPTO DE SEGURIDAD EN LAS REDES

No se puede definir la seguridad en redes con un concepto específico cuando se habla de seguridad en redes se maneja con un cierto grado de incertidumbre ya que todo depende del punto de vista de cada persona que se te analizando.

La seguridad viene a ser la protección de la información que se maneja en una red, tomando en cuenta principalmente en los pilares fundamentales como son la integridad, confidencialidad, privacidad, control y autenticidad de la información siempre se puede basar en políticas que definiendo de acuerdo a la necesidad que se presente en la red.

1.6 TIPOS DE SEGURIDAD

De acuerdo a la fuente que la genere la seguridad se puede clasificar en dos tipos una física y la otra de manera lógica

1.6.1 Seguridad Física

La seguridad física es la "aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial" a) (Huerta, 2002) que son de gran importancia para el funcionamiento de la misma.

La seguridad física se refiere a los controles y mecanismos de seguridad dentro y fuera del proveedor ISP en este caso los medios de acceso remoto que son implementados para proteger el hardware y medios de almacenamiento de datos. b) Huerta, A. V. (2002). *SEGURIDAD EN UNIX Y REDES.*

El hardware se encuentra en varios sitios que se establecen como repetidoras para poder expandir la red teniendo en cuenta que la central o matriz principal se encuentra en el sector de la inmaculada perteneciente al cantón GUANO.

Si bien algunos de los aspectos tratados a continuación se prevén, otros, como la detección de un atacante interno a la empresa que intenta acceder físicamente a una sala de operaciones de la misma.

- ✓ Desastres
- ✓ Incendios
- ✓ Equipamiento
- ✓ Inundaciones
- ✓ Picos y ruidos electromagnéticos

La mejor solución para poder mejorar la seguridad física se ve necesaria la elaboración de un plan de contingencia tomando en cuenta los últimos acontecimientos que se han estado presentando. C) Huerta, A. V. (2002). *SEGURIDAD EN UNIX Y REDES.*

1.6.2 Seguridad Lógica

"Consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y solo se permita acceder a ellos a las personas autorizadas" a). (Sánchez) como los administradores de red para tareas específicas.

Después de ver como la red puede verse afectada por la falta de seguridad física, es importante recalcar que la mayoría de los daños que puede sufrir el proveedor de internet (ISP), no será sobre los medios físicos, más bien será con información que este almacenada y que se esté procesando por la red con el fin de robar o modificar la información de los usuarios. b). (Sánchez)

La seguridad logica hoy en dia es muy facil de realizarla ya que en los diferents sitios web se pueden encontrar muchas herramientasque nos facilita el trabajo por lo tanto es necesario establecer cierto ipo de politicas de seguridad dentro de la empresa.
Los objetivos que se plantean para la seguridad lógica son:

- ✓ Restringir el acceso mediante el uso de credenciales o autenticación.
- ✓ Asegurar que los técnicos que estén dentro de la empresa no puedan modificar los parámetros ni políticas de seguridad hay que establecer parámetros o restricciones.
- ✓ Que no haya modificaciones en la información.

Disponer de políticas alternativas en casos de emergencia que nos ayuden a solventar el problema y no perder la transmisión de la información.

- ✓ Controles de acceso

- ✓ Autenticación
- ✓ Identificación
- ✓ Limitación de servicios
- ✓ Establecimiento de políticas
- ✓ Unidades de Recuperación o back-ups.

1.7 Tipos De Redes

Las redes son un conjunto de equipos conectados por diferentes medios con un único fon que es establecer comunicación ya sea por cables, señales o cualquier método que puede enviar datos de un lugar a otro y se pueden clasificar en diferentes tipos de redes.

1.7.1 Redes LAN

Se denomina LAN (Local Área Network) a redes administradas por una organización única las cuales prestan servicios dentro de una organización como una empresa, un campus, un edificio; manejando velocidades relativamente altas y baja latencia dependiendo del tráfico que maneje. (BUSTAMANTE)

Las extensiones de una red LAN puede llegar hasta 100 metros de distancia y está formada por diferentes equipos de cómputo unidos por un switch que permite la distribución de la información en la red. (BUSTAMANTE)

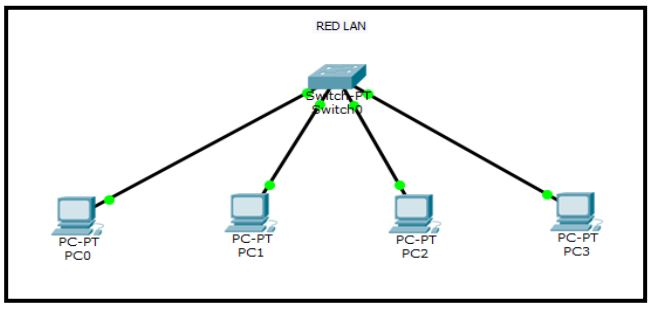


Figura 1-1: Red LAN Cisco Packet Tracer

Realizado por: Galo Hurtado C. 2017

1.8 Controles de confidencialidad e Integridad

Está enfocado directamente a los administradores de red que tienen el acceso al Core del ISP para lo cual se han tomado en cuenta algunos parámetros fundamentales que se describen a continuación.

1.8.1 Cifrado de Datos

Se garantiza que la información no es legible para individuos o procesos no autorizados por el usuario. Este tipo de técnica se utiliza para transformar el texto claro en un texto cifrado gracias a una información inicial secreta como una clave de cifrado. (Nab, 2004)

1.8.2 Autenticación de Usuarios

Este proceso nos ayuda a poder asegurar la identidad de los administradores de la red ya que cada uno tendrá una clave única con un tiempo limitado para su uso de esta forma puede efectuar ciertas operaciones con los datos protegidos como leerlos, modificarlos o en algunos casos borrarlos dependiendo de la operación que se vaya a realizar. (Nab, 2004)

1.8.3 Clasificación de los datos

No todos los datos que se estén manejado dentro de nuestra red van a tener la misma prioridad en el caso se puede diferenciar diferenciar entre los clientes corporativos y los clientes de residencia domiciliaria, una vez identificados estos dos grupos de pueden subdividirlos en cuatro grupos.

1.8.3.1 Confidencial

Este tipo de protección de datos se presenta en entidades financieras ya que son las que van a transferir dinero y situaciones económicas de cada usuario dependiendo de dicha entidad.

1.8.3.2 Sensible o Restringido

De acuerdo a su definición se tiene que tomar en consideración los datos que se transmiten en las diferentes instituciones educativas que hacen uso del servicio.

1.8.3.3 Privado o Uso Interno

Son datos que no necesitan ningún tipo de protección ya que la comunicación se realiza en un entorno interno de la empresa, a estos datos pueden acceder los técnicos con solo una autenticación básica.

1.8.3.4 Público

Está disponible siempre para los clientes que normalmente visitan las instalaciones. (Gonzalo Àlvarez Marañon , Pedro Pablo Pèrez Garcìa , 2005)

1.9 Amenazas, Vulnerabilidades y Ataques en la red Guano.NET

Para poder realizar un correcto análisis de la red y buscar algún tipo de amenaza o vulnerabilidad se tiene que realizar ataques a la red interna, de acuerdo a los resultados establecer diferentes políticas y definir sistemas de control y acceso a la red.

1.9.1 Amenazas

Las amenazas se pueden producir dentro de la red o se pueden dar los ataques externos a la red, los ataques dentro de la red ya que de la parte externa se encuentra el proveedor de internet que en este caso es Telconet.

La amenaza se puede definir como la acción de burlar la seguridad y estas puedes ser con intención o también se pueden presentar amenazas naturales y los agentes son las personas, la competencia u organizaciones que originan dicha amenaza hay que recordar que la amenazas se pueden eliminar solo se pueden controlar un agente debe tener algunos tipos de características entre las principales están tres q se detallan a continuación:

- ✓ **Acceso a la información**

Como proveedor de servicios de internet (ISP) es un punto muy alto el acceso a la información que los agentes que se encuentran laborando no han realizado algún tipo de capacitación o charla sobre el tema de seguridad en redes.

Hay que tener en cuenta que hoy en día se ha vuelto muy importante la Ingeniería Social para poder obtener información vital de la empresa y de esta forma otorgar armas al atacante y así logre su objetivo que es buscar una vulnerabilidad y posteriormente convertirla en una amenaza.

- ✓ **Conocimiento del Tema**

Se relaciona directamente con la formación académica que tenga el atacante y de sus objetivos, hay que tener en consideración que los técnicos que laboran en la empresa tienen identificadores de usuarios, contraseñas, direcciones de red.

- ✓ **Motivación o venganza**

Es uno de los aspectos más importantes ya que se explica la razón de ser del atacante, el por qué intenta realizar ataques o amenazas al proveedor de internet GUANO.NET.

1.9.1.1 TIPOS DE AMENAZA

- ✓ **Recopilación de la Información**

Es también conocido como Harvesting y su principal objetivo es poder obtener información acerca de la topología de red, tipos de dispositivos y su configuración para de esta manera poder buscar tipos de vulnerabilidades y los puertos por donde se pueda acceder. (2)

- ✓ **Intercepción del Tráfico**

Es más conocido como un sniffing que su finalidad es interceptar la mayor cantidad de información que se transmite en la red.

- ✓ **Falsificación**

También llamado Spoofing este es uno de los ataques más comunes que se pueden dar ya que son fáciles de realizarlos y consiste en ocultar su identidad, haciéndose de esta manera pasar por un usuario más de la empresa.

Se considera un ataque de falsificación por que puede modificar o crear paquetes para hacer una falsificación de identidad e insertar en algún paquete que se esté transmitiendo en la red. (Ayala Marín, 2006)

- ✓ **Denegación de Servicio**

La principal funcionalidad de este es poder realizar varios tipos de peticiones a un mismo tiempo, inundan la red con tráfico y consumiendo ancho de banda y recursos este tipo de ataque se realizan principalmente a los servidores de la empresa dejándoles inhabilitados por una cierta cantidad de tiempo. (Ayala Marín, 2006)

- ✓ **Escaneo de Puertos**

El escaneo de puertos es una técnica que se basa en la evaluación de vulnerabilidades por parte de hackers o administradores de red que les sirve para auditar las máquinas y la red. (Valbuena, 2013).Se puede utilizar diferentes herramientas como nmap esta herramienta permite escanear los puertos con solo asignar la dirección IP demás se complementan con algunas otras funciones y lo más importante son de código abierto totalmente gratuitos.

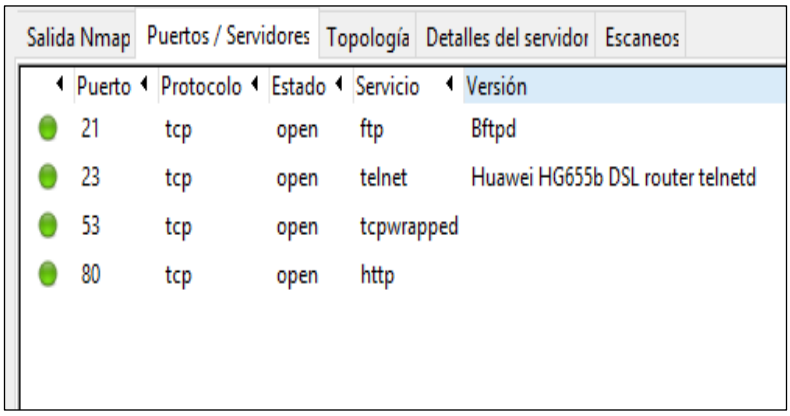


Figura 2-1: Escaneo de puertos con Zenmap.
Realizado por: Galo Hurtado C. 2017

1.9.2 Vulnerabilidades

Las vulnerabilidades en la red se pueden presentar en la red interna o externa, en el software que utilicen las computadoras o en la seguridad física de la empresa GUANO.NET, una vulnerabilidad está caracterizada por la capacidad que tenga de poder afectar a la red.

A las vulnerabilidades se las pueden agrupar de acuerdo:

- ✓ **Diseño**

  Este es un punto importante ya que las políticas de publicidad son mal establecidas o en algunos casos no establecen políticas de seguridad simplemente buscan el funcionamiento de la red.

- ✓ **Implementación**

  Se produce pro una defectuosa programación y en la mayoría de los casos dejan muchas puertas traseras abiertas.

- ✓ **Uso**

  Falta de conocimiento y disponibilidad de herramientas que pueden facilitar la búsqueda de vulnerabilidades en la red.

1.9.2.1 Escaneo de Vulnerabilidades

Para poder determinar las posibles vulnerabilidades existentes en la red primero se tienen que realizar algunos tipos de ataques de esta manera se determinan las soluciones para las vulnerabilidades que presente la red.
Es muy necesario realizar análisis periódicos para de esta forma determinar el comportamiento de la red y de las posibles exposiciones de la misma ante diferentes tipos de ataques.

1.9.3 Ataques a la red GUANO.NET

Se tienen que realizar diferentes tipos de ataques considerando la dificultad, el daño que pueda ocasionar y los recursos con los que se puedan encontrar para realizar dicho ataque.

1.9.3.1 Maltego

El paradero actual de cualquier persona que trabaje dentro de la empresa, Maltego puede localizar, información agregada y visualizar esta información. (http://tools.kali.org/)

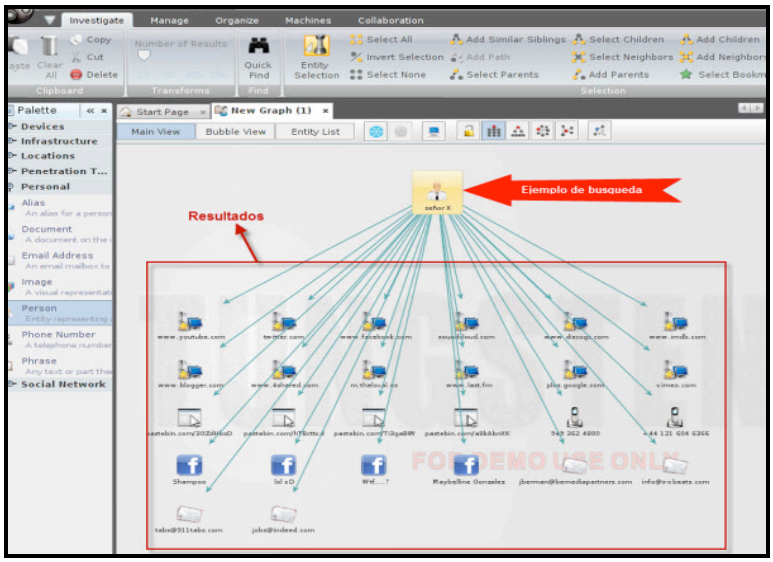


Figura 3-1: Ejemplo de un ataque a personas con Maltego

Realizado por: (PÉREZ, 2014)

1.9.3.2 Contraseñas por Defecto

En la mayoría de los casos es uno de los principales problemas que se presenta y son las contraseñas por defecto como ejemplo en el país la mayoría de equipos tienen un ID como admin y un password como admin y al ser un usuario "desconocido" o un intruso podría descubrirlo fácilmente y el siguiente paso sería apoderarse del equipo.

MARCA	EQUIPO	VERSIÓN IOS/SO	USUARIO	CONTRASEÑA
Cisco	Cualquier modelo de Router and Switch	10 thru 12	cisco	cisco
Cisco	ConfigMaker Software	any?	n/a	cmaker
CISCO	Network Registrar	3.0	ADMIN	changeme
CISCO	N/A	N/A	pixadmin	pixadmin
Cisco	Routers	Not sure...j	–	san-fran
Cisco	VPN 3000 Concentrator	–	admin	admin
Cisco	Net Ranger 2.2.1	Sol 5.6	root	attack
cisco	1600	12.05	–	–
cisco	1601	–	–	–
Cisco	IDS (netranger)		root	attack
Cisco	MGX	*	superuser	superuser
cisco	1601	–	–	–
CISCO	arrowpoint	–	–	–

Figura 4-1: Usuarios y contraseñas de equipos Cisco

Realizado por: (Martínez, 2014).

Existen gran cantidad de herramientas que automatizan el trabajo de probar claves por omisión hasta encontrar alguna válida dentro de un rango de red. Es el caso de las que se encuentran en la distribución de Linux (Kali Linux).

1.9.3.3 Ataques de fuerza bruta

En la configuración de un router común se puede encontrar una forma de acceder al CLI de forma remota. Generalmente se usará el protocolo TELNET y el protocolo SSH. Los dos son protocolos de conexión remota que requieren validación de usuarios para entrar y usar el sistema.

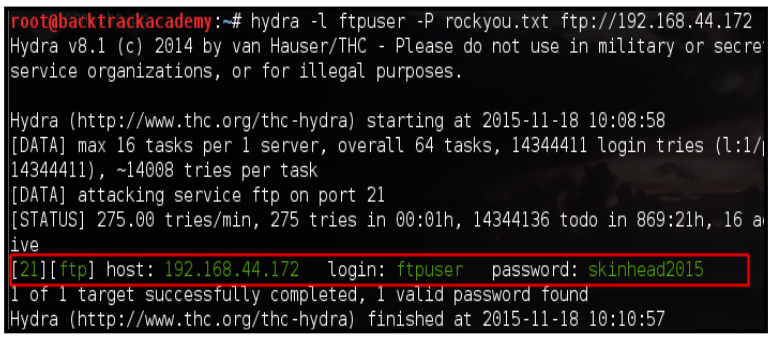


Figura 5-1: Ejemplo de un ataque de fuerza bruta con Kali Linux

Realizado por: (Esteban, 2015)

Para tratar de controlar este tipo de ataques lo más recomendable es utilizar contraseñas más seguras una combinación de números letras y símbolos.

1.9.3.4 TELNET

Telnet es un protocolo que nos permite conectar por medio de una red a un equipo remoto y administrarlo en modo consola. Uno de los principales problemas de telnet es que el protocolo envía en texto plano usuarios y contraseñas por la red, permitiéndole a un intruso conocerlas a través de técnicas de sniffing. (HOWARD, 1995).

1.9.3.5 Uso de Exploits

Es muy frecuente ingresar a un sistema explotando agujeros en los algoritmos de encriptación utilizados, en la administración de las claves por parte la empresa, o simplemente encontrando un error en los programas utilizados.
Los programas para explotar estos "agujeros" reciben el nombre de Exploits y lo que realizan es aprovechar la debilidad, fallo o error hallado en el sistema (hardware o software) para ingresar al mismo. (Borghello C. F., 2000)

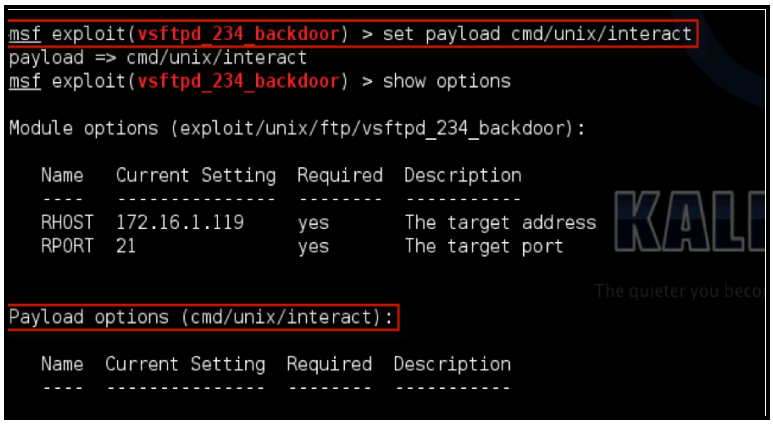


Figura 6-1: Ejemplo de ataque con uso de exploit
Realizado por: (Esteban, 2015)

1.9.3.6 "Snooping–Downloading Malware

Los ataques de esta categoría tienen el mismo objetivo que el Sniffing: obtener la información sin modificarla.

Sin embargo, los métodos son diferentes. Aquí, además de interceptar el tráfico de red, el atacante ingresa a los documentos, mensajes de correo electrónico y otra información guardada, realizando en la mayoría de los casos un downloading (copia de documentos) de esa información a su propia computadora, para luego hacer un análisis exhaustivo de la misma.

El Snooping puede ser realizado por simple curiosidad, pero también es realizado con fines de espionaje y robo de información o software. "(GONCALVES, 1997)

1.9.3.7 Denegación de Servicio

"Este ataque es bastante simple y a su vez devastador. Consiste en recolectar una serie de direcciones Broadcast para, a continuación, mandar una petición ICMP (simulando un Ping) a cada una de ellas en serie, varias veces, falsificando la dirección IP de origen (máquina víctima).

Este paquete maliciosamente manipulado, será repetido en difusión (Broadcast), y cientos o miles de hosts mandarán una respuesta a la víctima cuya dirección IP figura en el paquete ICMP." (Borghello C. F., segu-info, 2000)

Gráficamente se puede observar la estructura de un ataque a la red interna de la empresa.

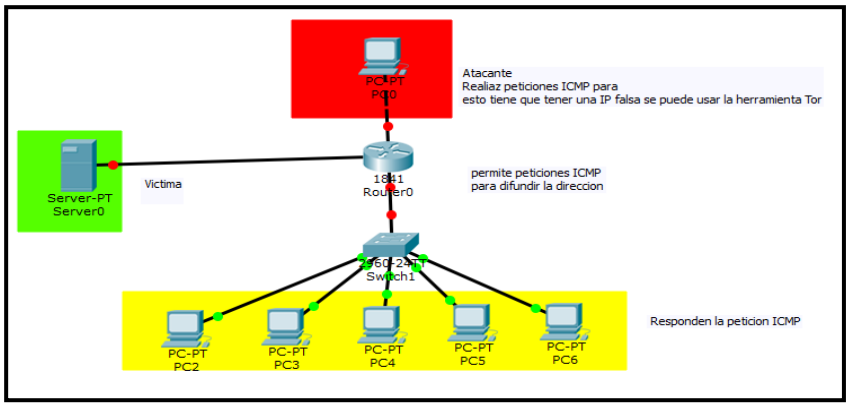


Figura 7-1: Esquema de un ataque de DDOS simulado en Cisco Packet Tracer

Realizado por: Galo Hurtado 2017

La víctima presentara un tiempo de respuesta que varía dependiendo de la marca, modelo y capacidad del mismo.

```
C:\Users\usuario>ping -l 16500 192.168.0.1 -t

Pinging 192.168.0.1 with 16500 bytes of data:
Reply from 192.168.0.1: bytes=16500 time=4ms TTL=64
Reply from 192.168.0.1: bytes=16500 time=4ms TTL=64
Reply from 192.168.0.1: bytes=16500 time=4ms TTL=64
Reply from 192.168.0.1: bytes=16500 time=5ms TTL=64
Reply from 192.168.0.1: bytes=16500 time=4ms TTL=64
Reply from 192.168.0.1: bytes=16500 time=4ms TTL=64
Reply from 192.168.0.1: bytes=16500 time=5ms TTL=64
Reply from 192.168.0.1: bytes=16500 time=4ms TTL=64
Reply from 192.168.0.1: bytes=16500 time=4ms TTL=64
Reply from 192.168.0.1: bytes=16500 time=4ms TTL=64
Reply from 192.168.0.1: bytes=16500 time=4ms TTL=64
Reply from 192.168.0.1: bytes=16500 time=4ms TTL=64
Reply from 192.168.0.1: bytes=16500 time=4ms TTL=64
Reply from 192.168.0.1: bytes=16500 time=5ms TTL=64
Reply from 192.168.0.1: bytes=16500 time=4ms TTL=64
Reply from 192.168.0.1: bytes=16500 time=4ms TTL=64
Reply from 192.168.0.1: bytes=16500 time=5ms TTL=64
Reply from 192.168.0.1: bytes=16500 time=5ms TTL=64
Reply from 192.168.0.1: bytes=16500 time=4ms TTL=64
```

Figura 8-1: Esquema de un ataque básico de DDOS

Realizado por: Galo Hurtado. 2017

1.9.3.8 Pruebas de Penetración

Las pruebas o test de penetración son la forma más viable de medir la seguridad de sus sistemas de información, utiliza las mismas herramientas y procesos que realizaría un delincuente informático para tener acceso a su organización, pero en un entorno totalmente controlado que tiene como finalidad identificar las fallas de seguridad que puedan tener su empresa, para después arreglar estas fallas y evitar que una persona mal intencionada se aproveche de ellas. (9). Este es un servicio que como recomendación a todos los empresarios que tengan infraestructura expuesta de cara a internet, ya que no podrán saber el verdadero estado de seguridad que tienen sus sistemas a no ser que se realicen estas pruebas de penetración, simulando ataques reales para dejar en evidencia debilidades y puntos débiles de la infraestructura. Ref. b) (9)

Existen 3 tipos de Pruebas de Penetración:

- ✓ **"Pruebas de Penetración de Caja Negra**: Donde los pentesters o analistas de seguridad no tienen conocimiento del funcionamiento interno del sistema, y trabaja con la información que puede conseguir por sus propios medios, igual que lo podría hacer un delincuente informático. (9)

- ✓ **Pruebas de Penetración de Caja Blanca:** En este tipo de pruebas los pentesters o analistas de seguridad tienen total conocimiento del funcionamiento interno del sistema, y trabaja con información que puede tener acceso uno o varios empleados dentro de la organización. (9)

- ✓ **Pruebas de Penetración de Caja Gris**: Donde los pentesters o analistas de seguridad pueden tener conocimiento sobre algunos aspectos del funcionamiento del sistema y de otros no". (9)

1.10 Políticas de Seguridad

Las políticas de seguridad van a ser definidas tomando en consideración el estándar de seguridad 802.1x, este estándar es una recomendación para todas las empresas que proveen servicios de internet con el propósito de mejorar el nivel de seguridad en la empresa que venda este tipo de servicios.

1.10.1 FIREWALL Filtrado de Paquetes

"Se utilizan router´s con filtros y reglas basadas en políticas de control de acceso. El Router es el encargado de filtrar los paquetes (un Choque) basados en cualquiera de los siguientes criterios" (Cristian Fabian Borghello, 2000)

Tabla 1-1: Permisos configurados en el Firewall

Objetivo	Descripción
ACCEPT	Permite que todos los paquetes pueden ingresar a su destino y tener una respuesta
DROP	Solicitará en ingreso al servidor pero sin obtener ningún tipo de respuesta.

Realizado por: Galo Hurtado. 2017

Protocolos utilizados.

- ✓ Dirección IP de origen y de destino.
- ✓ Puerto TCP-UDP de origen y de destino.

Estos criterios permiten gran flexibilidad en el tratamiento del tráfico. Restringiendo las comunicaciones entre dos computadoras (mediante las direcciones IP) se permite determinar entre cuales máquinas la comunicación está permitida.

El filtrado de paquetes mediante puertos y protocolos permite establecer que servicios estarán disponibles al usuario y por cuales puertos. Se puede permitir navegar en la WWW (puerto 80 abierto) pero no acceder a la transferencia de archivos vía FTP (puerto 21 cerrado). (Cristian Fabian Borghello, 2000)

1.10.2 Rkhunter

Es una herramienta basada en Unix que analiza en busca de rootkits, puertas traseras y las posibles exploits locales. Rkhunter realiza varias comprobaciones en el sistema local para tratar de detectar rootkits, malware conocidos al mismo tiempo puede realizar comparaciones para ver si los comandos se han modificado y si los archivos enviados coinciden con los recibidos

algunos controles de las interfaces de red, incluidos los controles para escuchar solicitudes. Se pueden enviar todos los resultados a un servidor de correo si se ha configurado. (10)

1.10.3 Protocolo SSH

"Dentro de todos estos modelos considerados seguro está Secure Shell (SSH), un software cuya principal función es permitir la conexión remota segura a sistemas a través de canales inseguros, aunque también se utiliza para la ejecución de órdenes en ese sistema remoto o transferir ficheros desde o hacia él de manera fiable" (Ylonen, 1996).

Estos protocolos de comunicación serán objeto de ataques de fuerza bruta, puesto que se consideran servicios comunes para la administración de dispositivos en red. Un intruso intentará "adivinar" las claves de acceso con software automatizado que probará una tras otra las posibles palabras definidas en un diccionario. (Quintero, 2010).

Se puede definir un ataque por diccionario, el cual consiste en tener un listado definido de posibles claves y usar un software que pruebe una a una todas las posibles palabras del diccionario. (Quintero, 2010).
Existe una gran cantidad de ataques que se pueden realizar todo depende de la información y las herramientas con la que cuente un atacante.

1.11 Gestión de seguridad

La seguridad es un factor importante a considerar en una red por lo cual se trata de establecer un centro de seguridad para de esta manera poder diseñar un sistema que sea seguro y fácil de entender, se tienen que implementar 3 tipos de medidas que se presentan a continuación.

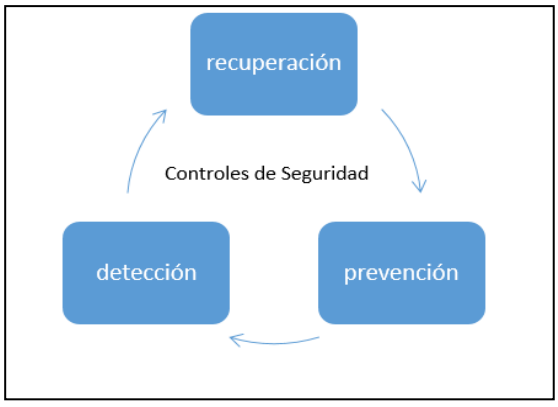


Figura 9-1: Diagrama de controles de Seguridad

1.11.1 Prevenir

Se refiere a tener un sistema de seguridad elevado para que los posibles ataques no tengan éxito uno de los mecanismos de control puede ser un FIREWALL.

1.11.2 Detectar

Es un sistema que se encarga del funcionamiento regular del ISP y el mismo activa un sistema de alerta cuando hay intención de ataques por parte de los intrusos.

1.11.3 Recuperar

Siempre es muy recomendable tener un back-up para en un caso de sufrir un ataque poder recuperar el servicio en el menor tiempo posible.
Sin embargo, el esquema que se presenta en seguridad en redes en cualquier infraestructura es la siguiente:

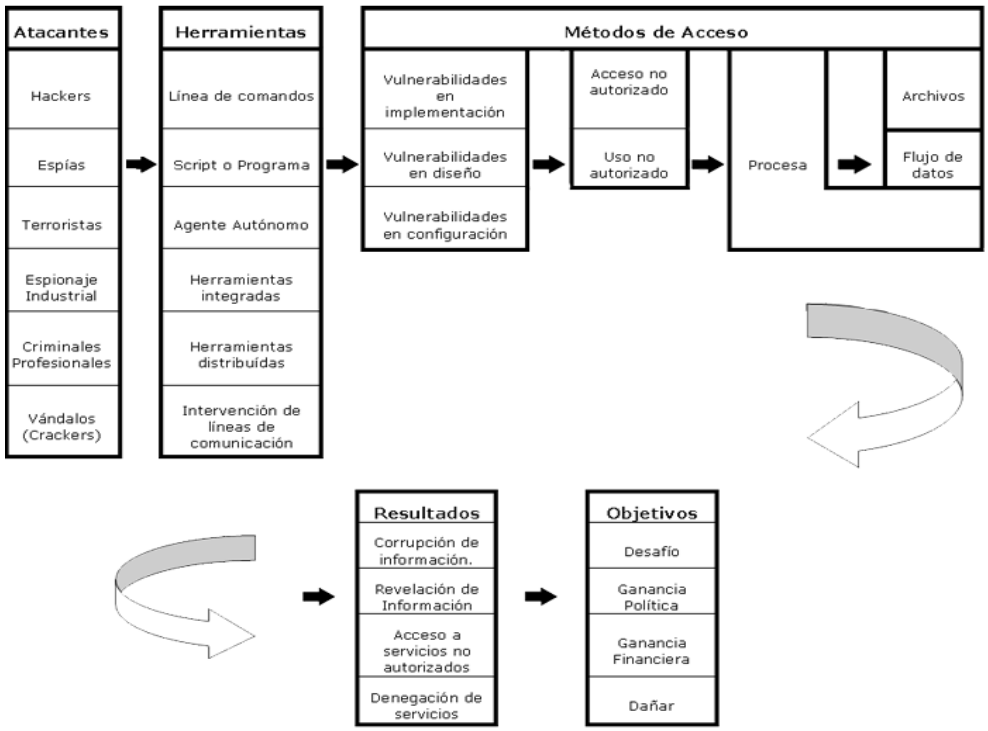


Figura 10-1: Detalle del procedimiento para diferentes ataques

Realizado por: (11)

Existen muchos elementos que motiven a una persona a realizar un ataque a la red por lo tanto se tiene que brindar una garantía en la transmisión de datos de los clientes.

CAPITULO II

2 MARCO METODOLÓGICO

2.1 Análisis de la red GUANO.NET

Para realizar el análisis de la red se tiene que ayudar de muchas herramientas para poder tener una mejor respuesta tomando como punto de parte la situación actual de la red en la empresa GUANO.NET.

2.1.1 Introducción

GUANO.NET es un ISP del cantón Guano que presta sus servicios a dicho cantón mediante radioenlaces permitiéndonos de esta forma poder llegar hasta los lugares muy alegados de la zona urbana.
Los servicios de la empresa están disponibles para todo tipo de personas, empresas y demás toda la actividad está centrada en el barrio la inmaculada, del cantón Guano se encuentra la oficina matriz.

Todo el control de la red se puede realizar desde la matriz o también se puede acceder de cada uno de los puntos en los que se encuentran las antenas repetidoras, este método eso nos facilita el trabajo porque la mayor parte del mismo siempre se realiza en el campo.
Cada una de los repetidores tiene una base de datos la cual se envían mediante un enlace WLL (Bucle local inalámbrico) hacia la matriz en donde están recopilados todos los datos y toda la información que se esté transmitiendo en la red.

Se procede a realizar un estudio comparativo entre los servidores de seguridad CISCO y MIKROTIK para poder evaluar su rendimiento ante diferentes ataques que pude sufrir la red y al mismo tiempo buscar las mejores alternativas para poder solucionar este problema en un caso que se pueda presentar luego de la etapa del análisis se realizara un informe con las debilidades y vulnerabilidades que se han presentado.

El primer acercamiento con la realidad de la red e la empresa GUANO.NET en cuanto al tema seguridad se refiere se procedió a realizar una encuesta a los trabajadores y propietarios de la empresa de esta manera se puede saber desde el punto de partida.

2.1.2 Herramienta de Análisis de la Red LAN

Para poder realizar un correcto análisis de la red se utilizó la herramienta Zenmap con la misma que se pudo escanear puertos, los servidores, la topología y todos los detalles del servidor.

1) Análisis de la res y el tráfico de la misma.

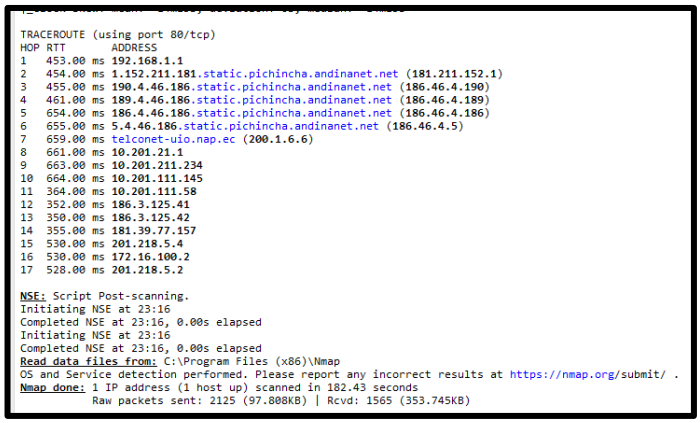


Figura 11-2: Análisis de la red GUANO.NET con Zenmap

Realizado por: Galo Hurtado.2017

2) Análisis de los puertos de la red

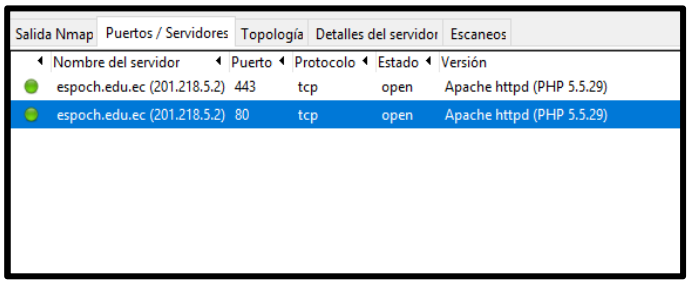


Figura 12-2: Análisis de los puertos con Zenmap

Realizado por: Galo Hurtado .2017

3) Topología de la red.

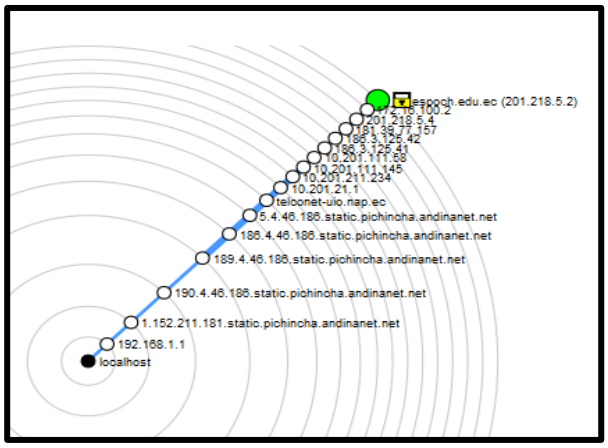


Figura 13-2: Topología de la red con Zenmap

Realizado por: Galo Hurtado. 2017

4) Detalles del servidor con todas sus características.

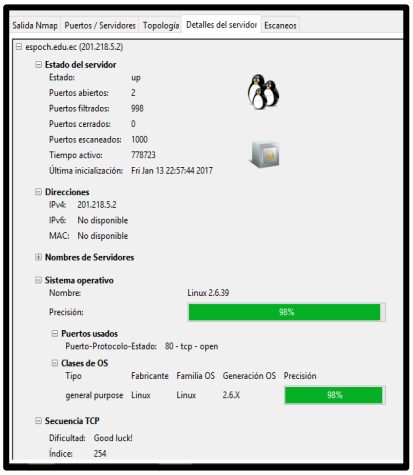


Figura 14-2: Servidores y sus características

Realizado por: Galo Hurtado. 2017

Con esta herramienta se identifica el sistema operativo, el tiempo de uso, los puertos abiertos o cerrados y el protocolo por el cual se comunican y posteriormente se puede identificar el tráfico que pasa por cada uno de ellos puede enviar.

2.2 Estado

La red de la empresa GUANO.NET se encuentra conformada por 1 solo router mikrotik de la serie 2000 consta actualmente con 350 usuarios.

El Router BOARD 1100 con IP 107.87.xx /24, se encuentra ubicado en el data center del cantón Guano siendo el principal conectado directamente con fibra al proveedor y el segundo router se

encuentra ubicado en la comunidad de San Isidro que interconecta las comunidades de Calshi, Arenillas y Guano, todo esa conectado medio un enlace WLL.

Figura 15-2: Router BOARD 1100

Realizado por: Galo Hurtado. 2017

Con una tabla de distribución de la siguiente manera:

Tabla 2-2: Equipos que conforman la red GUANO.NET

	Equipo	IP	Servicios
1	Router Board 1100	107.87.10.100	Establece la conexión con el proveedor de internet
2	Switch hEX		Repetidor principal sector San Isidro
3	switch hEX		San Isidro
4	Switch hEX		Calshi
5	Switch hEX		Guano
6	Switch hEX		Langos San Alfonso

Realizado por: Galo Hurtado. 2017

2.3 Dispositivos que conforman la red GUANO.NET

Tos los dispositivos que vayan a formar parte de la infraestructura tendrán que ser definidos en el diseño de red cuando se realizan las respectivas simulaciones.

Siempre se tiene que realizar un diseño de red que sea escalable para que pueda crecer y satisfacer las necesidades de más clientes dependiendo de la demanda que se proyecte tener.

2.3.1 Antenas Repetidoras

Son dispositivos que nos ayudar a trasmitir la información de un punto a otro, se realiza mediante la transmisión y retransmisión de ondas de radio y dependiendo del material de fabricación y otros aspectos como el medio, la ganancia permite poder llegar a puntos mucho más lejanos de la estación base.

Figura 16-2: Antenas repetidoras de la empresa.

Realizado por: Galo Hurtado.2017

2.3.2 Ubiquiti POE

Este inteligente POE tiene hardware remoto circuitería de reposición y permite que el dispositivo conectado a él, es restablecido de forma remota desde la ubicación fuente de alimentación. Ubiquiti Networks ofrece alimentación a través de Ethernet (PoE) adaptadores para accionar una variedad de productos Ubiquiti. Los adaptadores PoE son compatibles con la mayoría de los dispositivos Ubiquiti.

La Protección en los Ubiquiti PoE adaptadores proporciona una variedad de características para ayudar a proteger sus dispositivos Ubiquiti PoE, la protección contra sobretensiones y el cable de CA con conexión a tierra (Elektronika)

Figura 17-2: POE de la empresa GUANO.NET

Realizado por: Galo Hurtado. 2017

2.3.3 Switch

El switch de la red está directamente conectado a las antenas de distribución y al router, trabaja en la capa 2 del modelo OSI y son los encargados de transportar las tramas de un puerto a otro, realiza la función de transporte y encaminamiento.

Figura 18-2: Switch de la empresa GUANO.NET

Realizado por: MikroTik.com (12)

La principal característica de este dispositivo es que también cumple las funciones de un switch y adicionalmente tiene conexión Wifi.

2.3.4 Router

Es un dispositivo de red que permite interconectar redes a nivel de IP, está en la capa 3 del modelo OSI se puede establecer una gran cantidad de configuración con la ayuda de diferentes protocolos de aprendizaje, las funciones específicas de un router son:

- ✓ Evita propagar direcciones de broadcast en los router's periféricos hacia el interior de la red corporativa.

- ✓ Se puede traducir las direcciones de red (NAT), esto impide que se puedan visualizar lo rangos de direcciones internas. (GONZALO ÀLVAREZ M. PEDRO PÉREZ G., 2004).

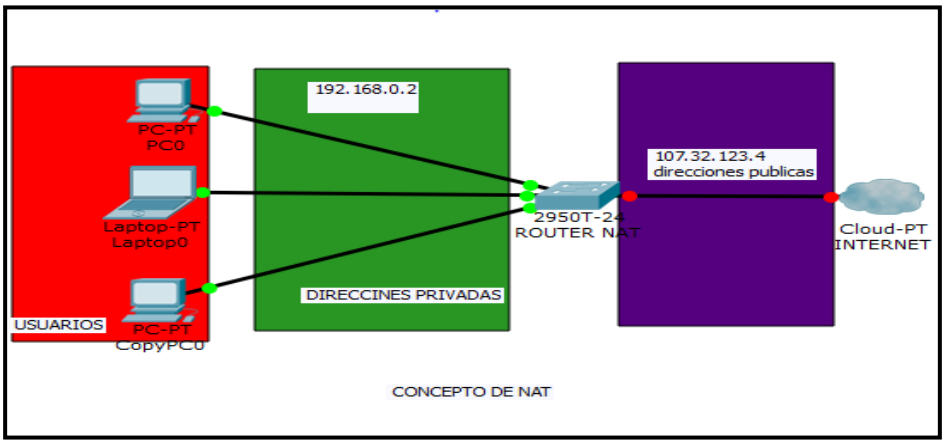


Figura 19-2: Concepto de NAT

Realizado por: Galo Hurtado.2017

2.3.5 Modem terminal

Este dispositivo nos ayudara en la decodificación de las señales analógicas a digitales para poder ser utilizadas por los clientes finales.

Figura 20-2: Router's colocados en los usuarios finales

Realizado por: Galo Hurtado. 2017

2.3.5.1 Dispositivo Perimetral

Es el dispositivo de borde es decir los equipos pueden ser router, firewall y un conmutador es un esquema básico de red para poder dar un sentido y direcciones únicas a diferentes usuarios.

La función principal de este dispositivo es el que nos permitirá tener acceso a una red corporativa es en este punto en donde luego de haber realizado el respectivo estudio el lugar que nos permitirá construir una frontera en la cual se implementara un buen dispositivo de seguridad y proteger la información de los clientes.

Se tienen que diferenciar dos tipos de host:

- ✓ **Host Estático**

  Los hosts estáticos están definidos como dispositivos que se conectan de forma permanente en este caso serían los servidores de seguridad que se implementarán en la empresa.

- ✓ **Host Dinámico**

Se tienen también configurados hosts dinámicos para poder realizar cualquier tipo de configuración de forma temporal y de acuerdo a la necesidad de los clientes.

2.3.6 Router de borde

Los router's operan en la capa 3 del modelo OSI y nos sirven como encaminadores que pueden estar ubicados en diferentes partes de la red dependiendo de la función q vayan a realizar.

Figura 21-2: Router de borde implementado en la empresa GUANO.NET

Realizado por: Galo Hurtado. 2017

Las interrogantes que como administradores de red siempre se tienen que plantear:

• ¿Qué le motiva al intruso ingresar al sistema?

• ¿Cuál va a ser el beneficio que obtenga el intruso al atacar a la red?

Una respuesta concreta no se puede dar, pero todo dependerá de la motivación que tenga el atacante ya sean aspectos económicos, desafíos intelectuales, diversión o simple venganza.

Como administradores de red siempre se tiene que estar monitoreando la red de forma periódica ya que como empresa el objetivo es brindar seguridad en todos los datos que se transmiten por la red. (Quintero, 2010)

La forma definitiva de contrarrestar las posibles amenazas y disminuir el riesgo que se presentan es estar pendiente de las actualizaciones y configuraciones del firmware y el software y tener una normatividad clara respecto a la implementación, monitoreo y soporte de estos dispositivos. Obviamente dentro de estas contramedidas siempre hay que tener presente el personal calificado para operar y mantener los servicios de la infraestructura. (Quintero, 2010). Siempre la seguridad lógica puede tener router's internos, de backbone y los perimetrales.

2.3.6.1 Router's Perimetrales

También conocidos como router's de frontera son los que dan la cara a Internet y están protegiendo las redes privadas por lo tanto es el lugar adecuado para implementar un sistema de seguridad.

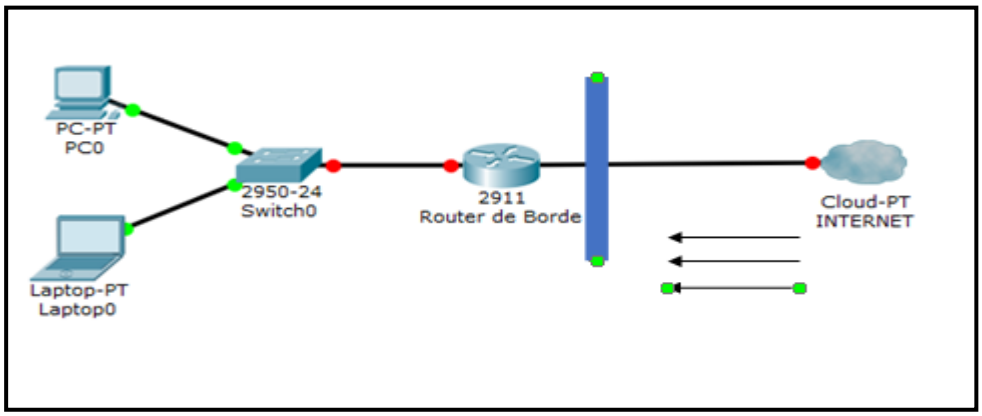


Figura 22-2: Esquema de un router perimetral

Realizado por: Galo Hurtado. 2017

Si se conectan a Internet a través de cualquier medio de comunicación será el primer punto de contacto y al mismo tiempo el acercamiento a un posible intruso. En este router se deeberia establecer diferentes políticas de seguridad que puedan realizar un filtrado de paquetes y poder determinar anomalías en la RED.

2.4 Evaluación la seguridad de una red

Los pasos para realizar una buena evaluación son los siguientes:

- ✓ Identificar el parámetro de la red: se realiza para conocer los elementos que conforman la red y determinar los estudios a realizar.

- ✓ Rastreo de dispositivos perimetrales: para determinar los equipos accesibles y sus servicios de red.
- ✓ Identificación de los servicios de red: se pueden utilizar todas las herramientas disponibles que nos ayuden a identificar las aplicaciones que se estén utilizando, así como la plataforma y versión de los servicios.

- ✓ Iniciar la investigación pro las vulnerabilidades más conocidas.

- ✓ Realizar ataques a la propia red para poder determinar cuál es la mejor solución para dicho ataque.

2.4.1 Diagrama de la red GUANO.NET

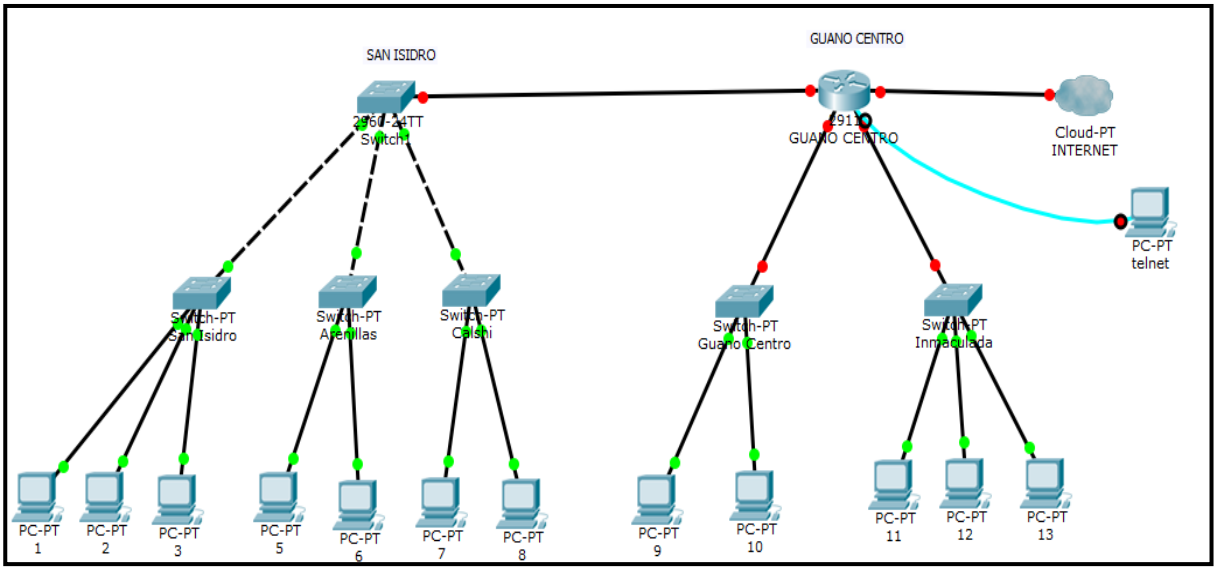


Figura 23-2: Esquema de la situación actual de la red

Realizado por: Galo Hurtado. Diseño en Cisco Packet Tracer. 2017

Como se puede observar en este esquema de red no existen dispositivos que nos brinden algún tipo de seguridad para proteger la información de los usuarios.

2.5 Ataques a equipos cisco

Los ataques se realizarán tomando en consideración los resultados obtenidos en el documento de análisis de vulnerabilidades.

2.5.1 ¿Cómo se hace el ataque?

Para realizar un ataque de fuerza bruta un atacante requiere 3 cosas:

1. Encontrar un software que entienda el protocolo que se quiera atacar (ssh, telnet, ftp, etc).

2. Generar un listado de posibles claves. Un atacante más experimentado intentará realizar ingeniería social para descubrir información que le sirva como base para crear su listado de posibles palabras. Un buscador en Internet podrá ser también una alternativa.

3. Poner en marcha el ataque, que dependiendo de los dos puntos anteriores será más o menos efectivo. Básicamente el ataque se transforma en una cuestión de recursos por parte del atacante y de tiempo según la fortaleza de las contraseñas empleadas por parte del administrador.

2.5.2 Escaneo de puertos y Tráfico

Se procede a realizar un escaneo de puertos con la ayuda de la herramienta Zenmap y NMAP se pudo determinar todos los puertos si están abiertos o cerrados así también se pudo analizar e tráfico de toda la red.

- ✓ **Puertos**

Se procedió a realizar el análisis de los puertos en el esquema de una red con equipos Cisco revisar el anexo 8.

1.) Con la ayuda de la herramienta nmap primero se procedió a revisar los equipos existentes en la red y su respectiva MAC Address y el tiempo de latencia. Para lo cual se tiene que ingresar los comandos: **nmap –sn –v i la respectiva dirección IP 192.168.0.0/24.**

2.) Posteriormente se busca los puertos abiertos y cerrados de la red peor para poder visualizar de una máquina especifica se puede tener la ayuda del comando **nmap –sS 192.168.0.100.**

3.) Para un escaneo mucho más detallado se ingresa el comando **–sT.**

- ✓ **Tráfico con tcpdump**

Se ve imperiosa la necesidad de escanear el tráfico de esta manera se observa el listado de las interfaces, las direcciones IP, el protocolo de transporte y la longitud del mismo.

1) Se ingresa el comando tcpdump y la dirección IP de la red **192.168.0.0/24.**

2) Para poder visualizar las interfaces que están disponibles únicamente se agrega –D al comando **tcpdump**

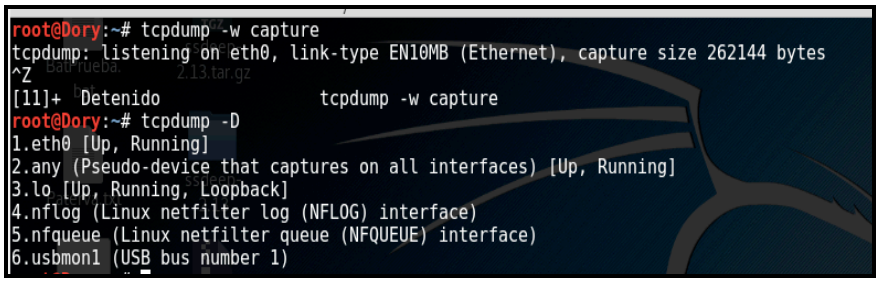


Figura 24-2: Búsqueda de interfaces disponibles

Realizado por: Galo Hurtado. 2017

2.5.3 Contraseñas por defecto

Una de las vulnerabilidades mas comunes que se pueden encontrar no solo en la red, si no en la mayoria de los proveedores de internet son las contraseñas por defecto con lo cual se puede hacer un ataque de red interna.

1) Se tiene que ingresar un ipconfig para poder ver la puerta de enlace:

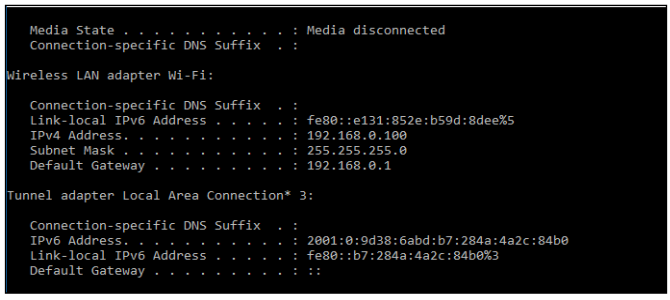


Figura 25-2: Búsqueda de la puerta de enlace

Realizado por: Galo Hurtado. 2017

2) Se presenta una ventana de acceso que nos pide un id y un password, el id es usuario y como se menciono anteriormente en la figura 5-1 y el password es admin.

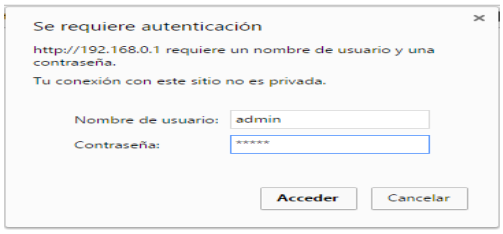


Figura 26-2: Interfaz gráfica de un usuario

Realizado por: Galo Hurtado. 2017

3) Ingresando al router de la victima se puede tomar el control completo del equipo.

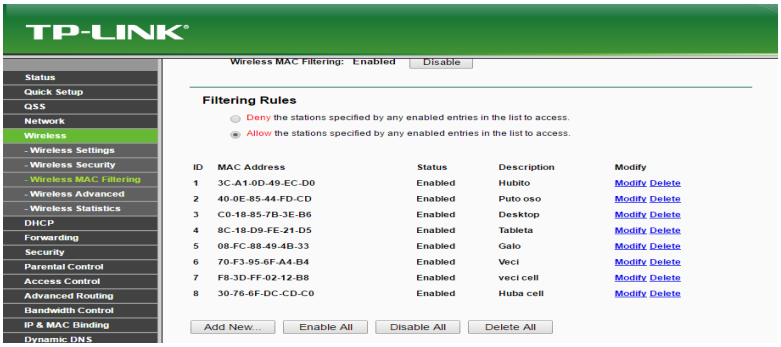


Figura 27-2: Acceso al router de un usuario

Realizado por: Galo Hurtado. 2017

2.5.4 Maltego

Este ataque se puede hacer a dominios, personas entre otros parametros en este caso se realizo un ataque a la empresa GUANO.NET para poder saber las funciones que los empleados realizan dentro de la misma .

1) Una vez que se verifique la instalación se procede a crear una nueva hoja de busqueda y de ingreso al dominio o la direccion ip de la empresa a la que se procedera a realizar el ataque.

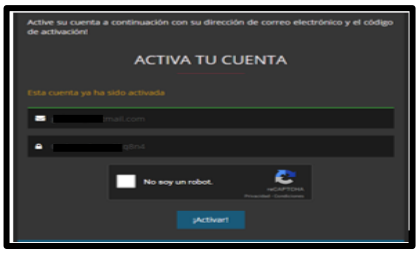


Figura 28-2: Verificación del registro en paterva

Realizado por: Galo Hurtado. 2017

2) Una vez que se selecciona la entidad de prueba Maltego iniciará con una recoplacion de informacion del dominio de destino se enfoca en las direcciones de correo electrónico de todos el personal que labore dentro de la empresa.

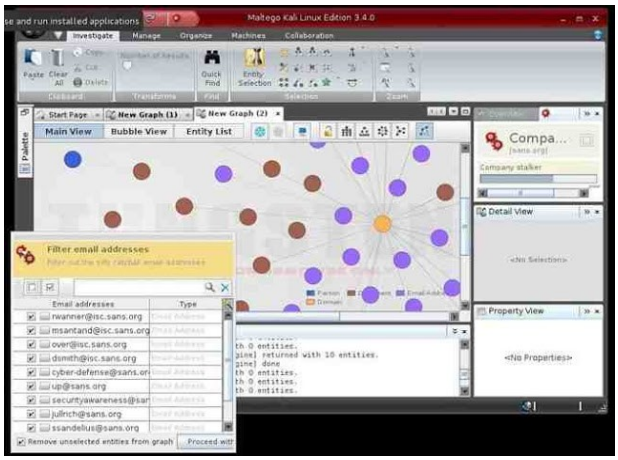


Figura 29-2: Información almacenada en los servidores de correo

Realizado por: Galo Hurtado. 2017

3) Además se puede realizar de una forma más detallada con la ayuda de "Entity List", de esta manera se puede apreciar los sitios y todas las actividades dentro de la empresa.

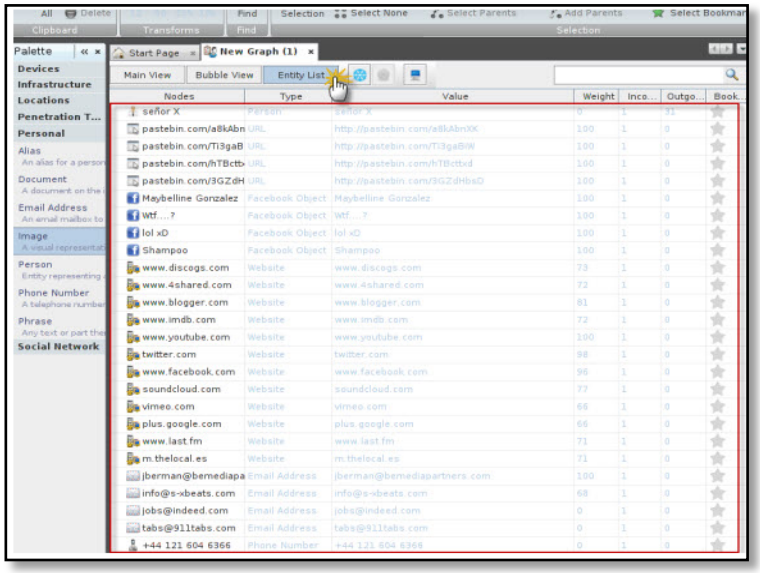


Figura 30-2: Información detallada de los usuarios y sus actividades

Realizado por: Galo Hurtado. 2017

Maltego es una de las mejores herramientas en cuanto a reconocimieno de red asi como identficar las diferentes actividades que realicen el personal que labora en la empresa por que tambien hace un reconocimiento individual.

2.5.5 Denegación de servicio

Este ataque se lleva a cabo desde la red interna de la empresa como se describe a continuacion, este ataque se lo realiza por su facilidad ya que cualquier usuario sin la nececidad de muchos conocimientos lo puede iniciar sin tener en consideracion los daños que el mismo puede ocasionar.

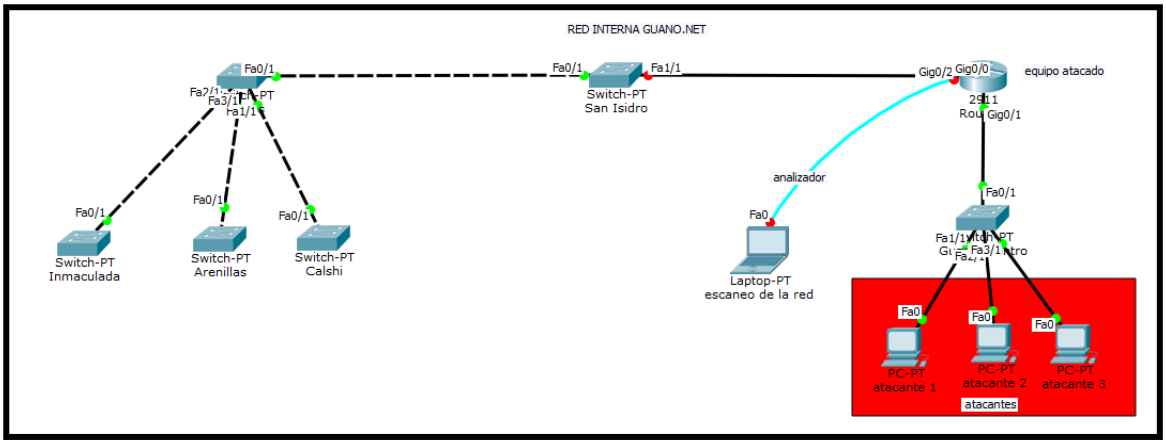


Figura 31-2: Esquema de un ataque a la red interna de la empresa.

Realizado por: Galo Hurtado. 2017

1) Se realiza un ipconfig en el cmd para poder enontrar la direccion IP de lapuerta de enlace.

```
FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.....: FE80::20B:BEFF:FE29:AB34
   IP Address.....: 192.168.0.6
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: 192.168.0.1
```

Figura 32-2: Puerta de enlace

Realizado por: Galo Hurtado. 2017

2) Ejecutando el comando **ping –l 65500 192.168.0.1 –t,** el 65500 es el numero maximo de paquetes que nos permite enviar el cmd, -t sirve para mandar una secuencia indeterminada, permitiendo asignar un numero de paquetes.

```
C:\Users\usuario>ping -l 65500 192.168.0.1 -t
```

Figura 33-2: Comando para realizar el ataque

Realizado por: Galo Hurtado. 2017

3) En un mismo usuario puede ejecutar multiples ventanas con el cmd para simular mas usuarios y enviar una cantidad mayor de paquetes.

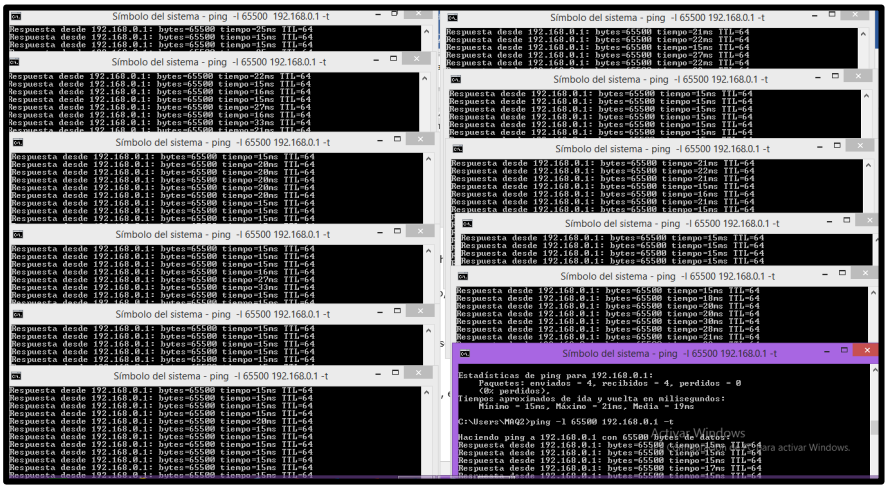


Figura 34-2: Múltiples peticiones desde un mismo usuario

Realizado por: Galo Hurtado. 2017

4) Siempre se tiene presente que el numero de peticiones se incrementa por lo tanto el tiempo de respuesta también.

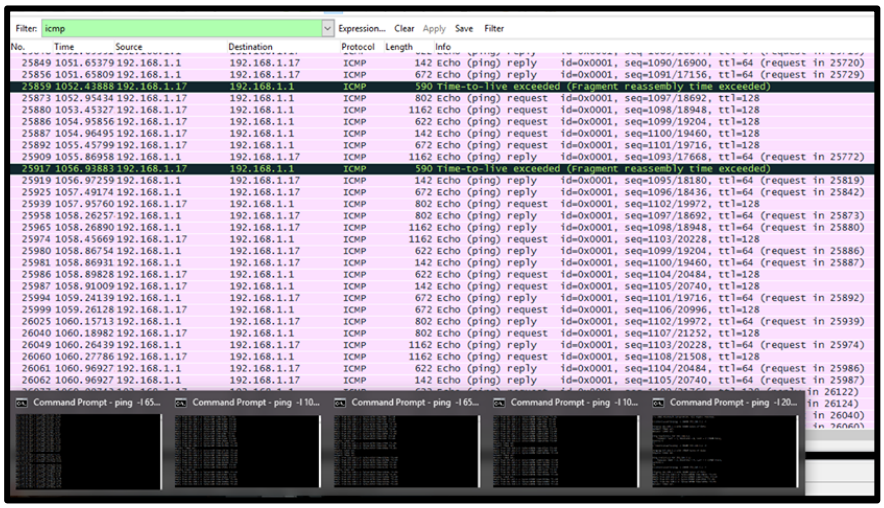


Figura 35-2: Tiempos de respuesta ante el ataque

Realizado por: Galo Hurtado. 2017

5) Analizando el tráfico con la ayuda de algunas herramientas como por eejemplo tcpdump y se pueden obtener los siguientes resultados

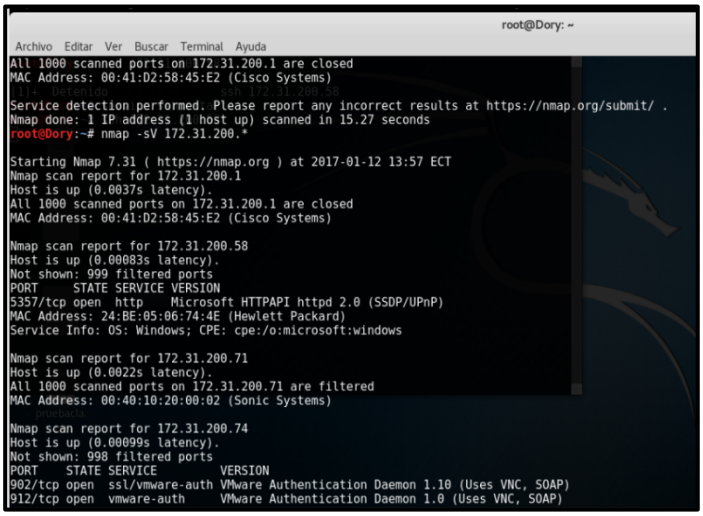


Figura 36-2: Resultados del análisis de tráfico

Realizado por: Galo Hurtado. 2017

Se puede observar cómo se incrementa el número de paquetes enviados desde una cierta dirección IP.

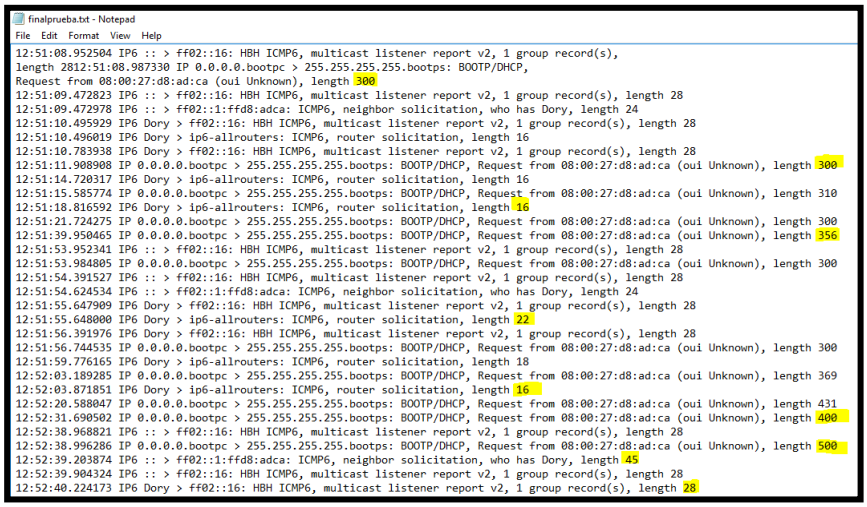


Figura 37-2: Resultados del ataque DDOS

Realizado por: Galo Hurtado. 2017

2.5.6 Ataque Man in The Middle (MITM)

El ataque Man in The Middle, o en español Hombre en el Medio, consiste en introducirse en la comunicación entre dos equipos para que todo el tráfico pase por un usuario y poder así desencriptar sus datos, contraseñas.

1) En este caso se utilizo la aplicación BUGTRAQ

Figura 38-2: Interfaz gráfica de BUGTRAQ

Realizado por: Galo Hurtado. 2017

2) El siguiente ataque se realizó con los siguientes pasos y de forma gráfica.

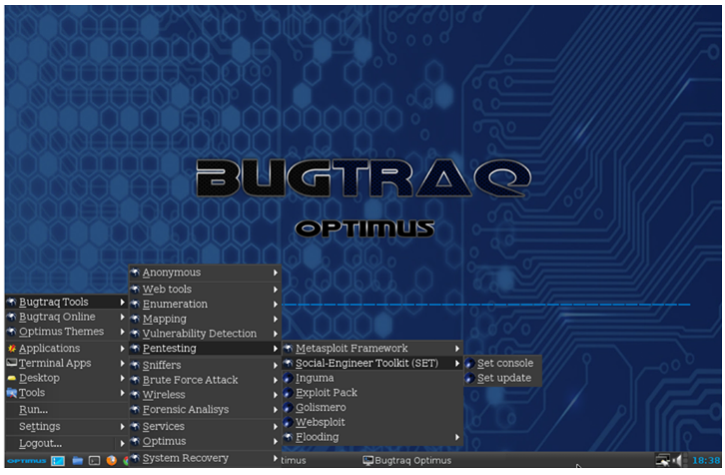


Figura 39-2: Pasos a seguir para el siguiente ataque

Realizado por: Galo Hurtado. 2017

Esta herramienta es muy fácil de utilizarla y los resultados son muy satisfactorios en este caso se realizó un ataque mediante las redes sociales y se pudieron obtener los nombres de usuario y sus respectivas contraseñas.

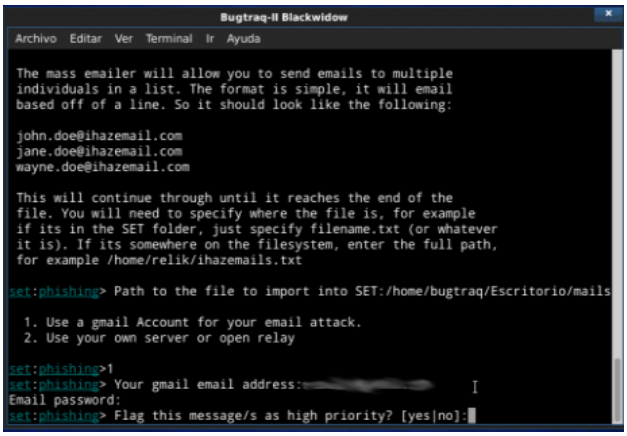


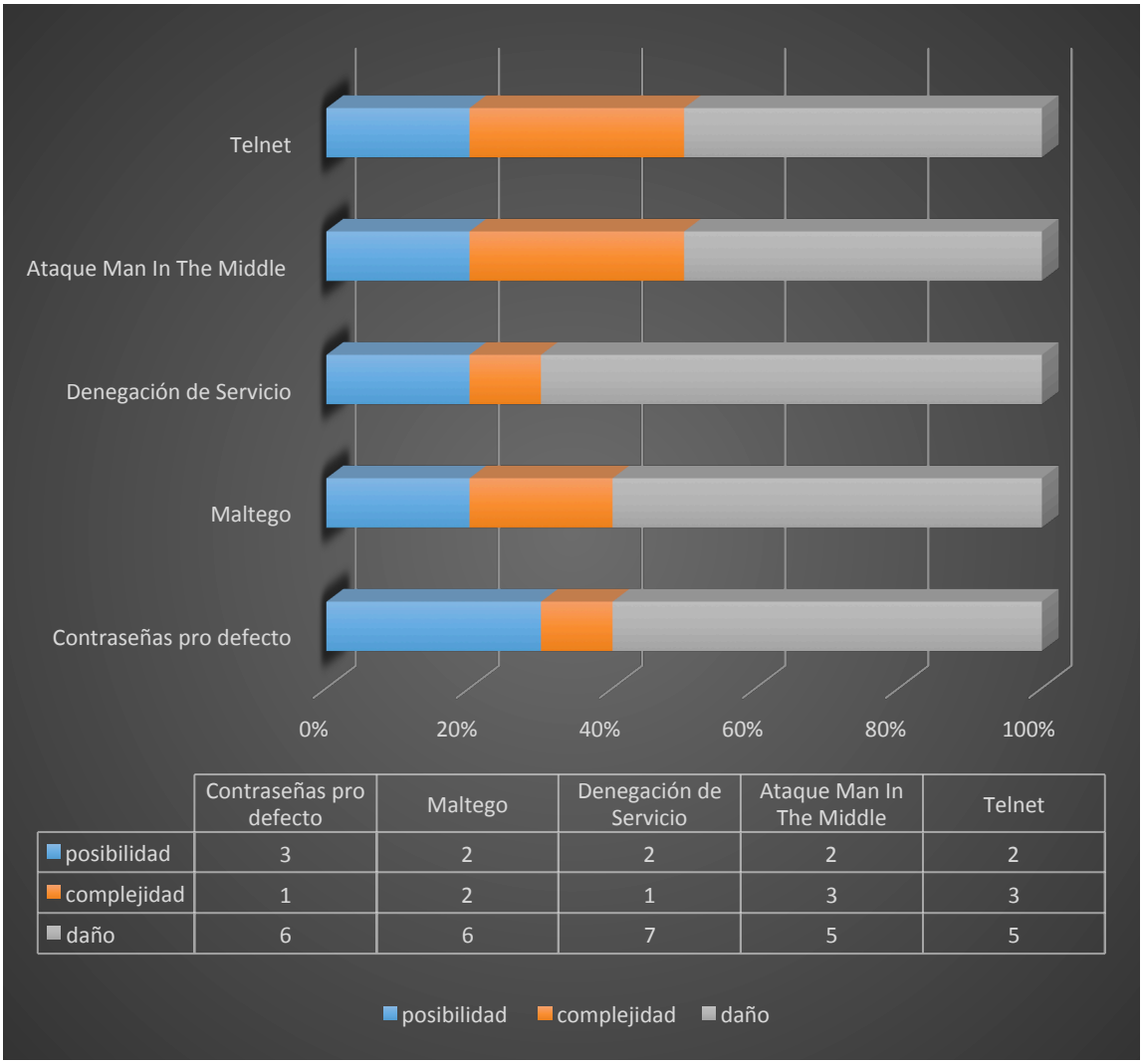
Figura 40-2: Resultados del ataque realizado

Autor: Galo Hurtado. 2017

2.6 EVALUACION DEL ANALISIS REALIZADO EN LA RED

- ✓ No esta implementado un Firewall para el filtrado de paquetes.
- ✓ El personal que labora en la red no conoce sobre temas de seguridad en redes.
- ✓ Los puertos están abiertos.
- ✓ No hay un sistema de seguridad contra ataques externos o internos.
- ✓ Acumulan muchos paquetes con actualización de información.
- ✓ No están configuradas ACL´S
- ✓ Hay un crecimiento desordenado de la red.

Tomando en cuenta en estándar de seguridad 802.1x se definió un parámetro de 1 -10 que dependen del tipo de ataque que se realice, la complejidad la posibilidad de llevarlo a cabo y el daño que puede ocasionar dicho ataque a la red de la empresa GUANO.NET



	Contraseñas pro defecto	Maltego	Denegación de Servicio	Ataque Man In The Middle	Telnet
posibilidad	3	2	2	2	2
complejidad	1	2	1	3	3
daño	6	6	7	5	5

Gráfico 1-2: Resultado de ataques a la red GUANO.NET
Realizado por: Galo Hurtado.2017

CAPÍTULO III

3 RESULTADOS OBTENIDOS

En el siguiente capítulo se presentan dos partes, en la primera se toma en cuenta las medidas necesarias para evitar los ataques que se encontraron en el capítulo 2 y en la segunda parte se determinan las comparativas entre los servidores de seguridad CISCO y MIKROTIK.

3.1 IMPLEMENTACIÓN SEGURIDAD EN LA RED GUANO.NET

Luego de haber realizado un análisis del estado actual de la red, se tiene que proceder a implementar las posibles soluciones para evitar que esto ocurra nuevamente, entonces el punto inicial desde lo más fundamental dando una solución a cada uno de los problemas que se han detectado.

Se inicia con la implementación de un Firewall basado en Linux y servidores que permitan controlar las vulnerabilidades que se han encontrado anteriormente, con un único fin que será garantizar la seguridad en los datos de los usuarios que se transmiten por la red.

Se ve imperiosa la necesidad de implementar un servidor externo de seguridad que se lo implemento en Ubuntu, con esto se evita que si la demanda de usuarios crece y se retiran los equipos actuales la empresa se quede sin protección caso contrario el servidor externo nos permite tener seguridad en la empresa de forma indefinida.

3.1.1 Firewall

Se implementa el firewall en el servidor de seguridad y también en el Router Board 1100 que tiene la opción de crear un firewall con políticas como se muestra a continuación:

- Filtra la información.
- Incrementa el nivel de seguridad.
- Se asignan políticas de acuerdo a las necesidades.
- Funcionalidades de firewall estándares, como la inspección con estado
- Prevención integrada de intrusiones.
- Reconocimiento y control de aplicaciones para ver y bloquear las aplicaciones peligrosas.

El nuevo diagrama de red estará constituido de la siguiente forma:

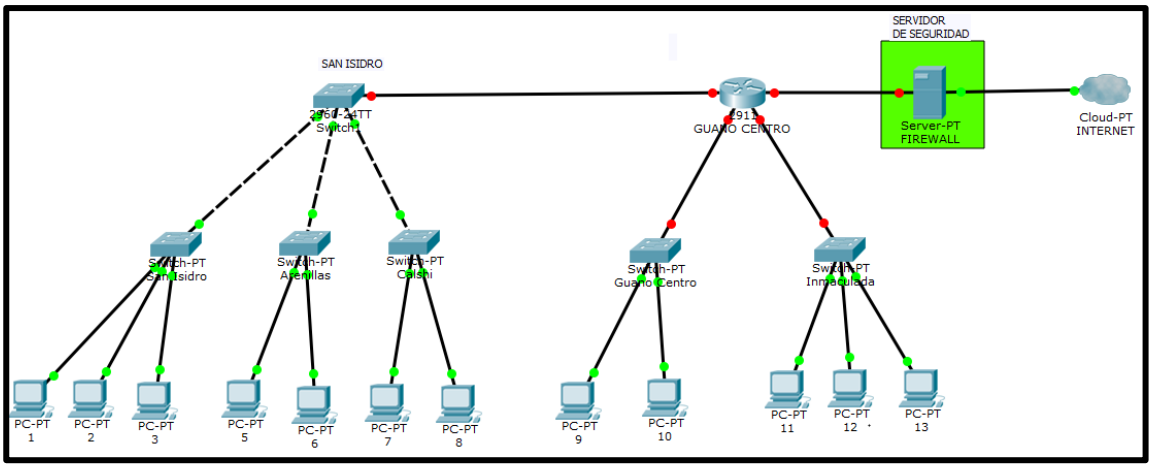


Figura 41-3: Esquema de seguridad propuesto en la empresa

Realizado por: Galo Hurtado. 2017

1) En CENTOS se configura el servidor.

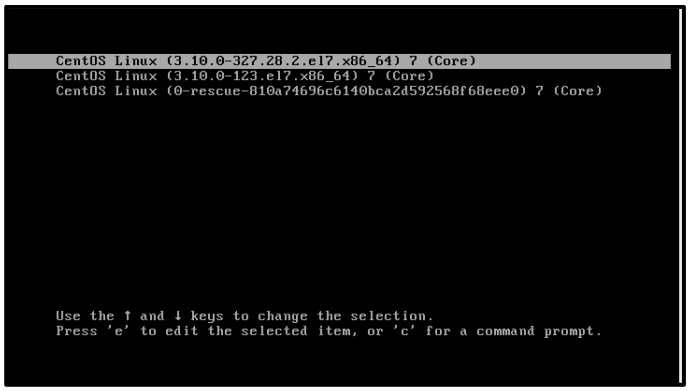


Figura 42-3: Interfaz gráfica de Centos.

Realizado por: Galo Hurtado. 2017

2) Se crea un usuario y una contraseña.

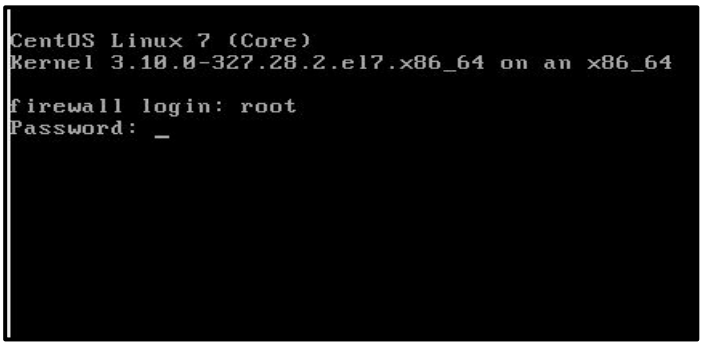


Figura 43-3: Se crea un usuario y una contraseña

Realizado por: Galo Hurtado. 2017

3) Establecer las políticas de acuerdo a los requerimientos de la red.

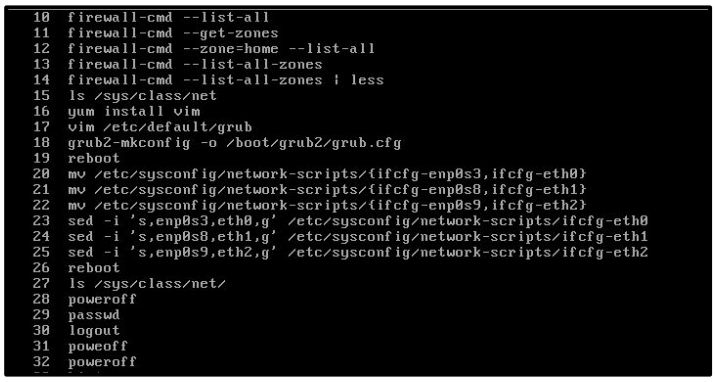


Figura 44-3: Políticas de seguridad requeridas

Realizado por: Galo Hurtado. 2017

Con estas políticas implementadas se puede tener el control del tráfico y se filtran los datos. También se pueden configurar el firewall en MIKROTIK para esto se puede revisar los pasos necesarios en el ANEXO 2.

De esta manera ya se cuenta con el Firewall implementado para poder permitir o denegar el tráfico de los usuarios que pasa por la red.

3.1.2 Lynis

Es una herramienta de auditoría de seguridad de código abierto. Se utiliza para evaluar las defensas de seguridad de los sistemas basados en Linux y UNIX. Se ejecuta en el propio host, por lo que realiza exploraciones de seguridad más extensas que los escáneres de vulnerabilidades, se pude realizar con los siguientes pasos. (13)

- Determinar el sistema operativo
- Buscar herramientas y utilidades disponibles
- Comprobar actualización de Lynis
- Ejecutar pruebas desde complementos habilitados
- Ejecutar pruebas de seguridad por categoría
- Estado del informe de la exploración de seguridad (13)

Para revisar la instalación de manera más detallada revisar el ANEXO 7.

3.1.3 Rkhunter

Esta herramienta permite tener conocimiento de cualquier tipo de anomalía que se pueda presentar en el servidor de seguridad ya que se envían mensajes a un servidor de correo electrónico permitiendo de esta manera tener al tanto del funcionamiento del servidor. Para poder ver la configuración completa y más detallada se puede revisar la parte de anexos el manual del servidor de correo.

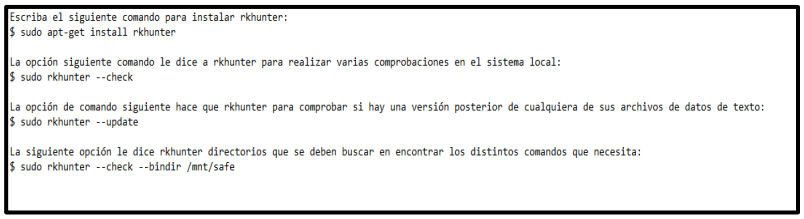


Figura 45-3: Configuración de Rkhunter

Realizado por: Galo Hurtado. 2017

La instalación detallada de todos los pasos a seguir se encuentra en el Anexo 6.

3.1.4 ClamAV

Es un conjunto de herramientas antivirus, libre y de código fuente abierto, que tiene las siguientes características:

- Distribuido bajo los términos de la Licencia Publica General GNU versión 2.
- Exploración rápida.
- Detecta más de 720 mil virus, gusanos, troyanos y otros programas maliciosos.
- Capacidad para examinar contenido de archivos ZIP, RAR, Tar, Gzip, Bzip2, MS OLE2, MS Cabinet, MS CHM y MS SZDD.
- Avanzada herramienta de actualización con soporte para firmas digitales y consultas basadas sobre DNS. (14).

La instalación se encuentra de forma detallada en el Anexo 5.

3.1.5 Ignorar peticiones de difusión ICMP

Con este siguiente comando se puede denegar el tráfico ICMP para poder eliminar el ataque de denegación de servicio.

```
# Ignore ICMP broadcast requests
net.ipv4.icmp_echo_ignore_broadcasts = 1
```

Figura 46-3: Eliminar paquetes ICMP

Realizado por: Galo Hurtado. 2017

3.1.6 SSH

Con esta herramienta se puede encriptar la sesión de registro la misma que sirve para que cualquier persona pueda obtener la contraseña y trabaja de la siguiente manera:

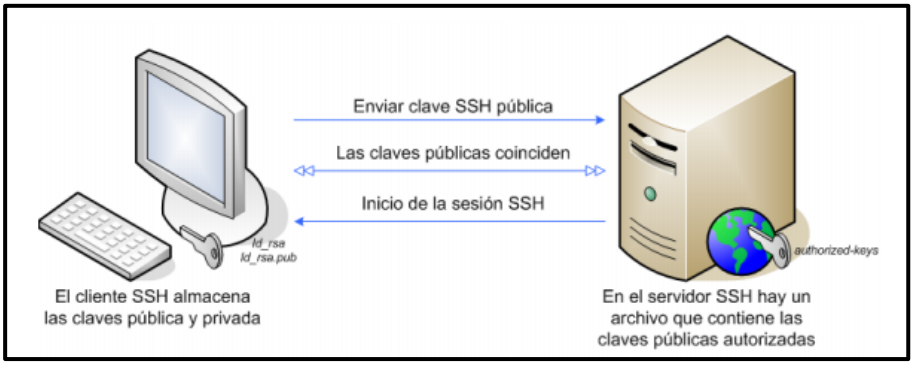


Figura 47-3: Funcionamiento de SSH

Realizado por: (15)

Se puede realizar con la ayuda de los siguientes pasos para su instalación y verificación:

```
1)Instalamos el servidor Open SSH nos ayudamos de:
 yum install openssh-server


2)Podemos editar los ficheros con la ayuda del comando:
 etc/ssh/sshd_config

3)Tenemos definir al usuario que se va a conectar en nuestro caso:
 PermirRootLogin


4)Luego accedemos de forma remota a nuestro servidor ssh con la IP correspondiente 192.168.x.x

5)Habilitamos una contraseña y reiniciamos para q se ejecuten los cambios con:
 service sshd restart.

6)Para que se inicie de forma automática colocamos:
 chkconfig sshd on


7)Comprobamos el estado de servidor SSH con la ayuda de service sshd status
```

Figura 48-3: Implementación de SSH

Realizado por: Galo Hurtado. 2017

Luego de que este configurado se procede a implementar medidas de seguridad que lo vuelvan más robusto ante diferentes tipos de ataques que se puedan presentar.
Lo que por defecto se configura es:

```
Port 22
LoginGraceTime 30
PermitRootLogin no
MaxAuthTries 2
MaxStartups 3
AllowUsers GUANO.NET
```

Figura 49-3: Configuración de SSH por defecto.

Realizado por: Galo Hurtado.2017

Entre las cosas que se pueden establecer son:

- ✓ SSH utiliza por defecto el puerto 22 entonces podeos cambiar el número de puerto.
- ✓ Se puede deshabilitar el acceso como usuario *root* y password *toor* que están por defecto ***PermitRootLogin no.***
- ✓ Con "MaxAuthTries" se limitara el número de intentos a 3 por ejemplo.
- ✓ Limitar el número de ventanas de logueos permitidas.

3.1.7 Servidores de seguridad AAA

En la seguridad informática, el acrónimo AAA corresponde a un tipo de protocolos que realizan tres funciones: autenticación, autorización y contabilización, los tres servicios son cifrados y se los puede implementar en CISCO, MIKROTIK o en un servidor que este implementado de forma externa con la ayuda de los siguientes pasos:

- ➢ Primero se tiene que instalar un servidor de autenticación FreeRadius.

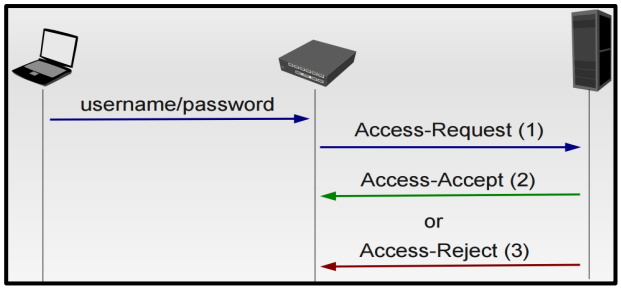


Figura 50-3: Modo de autenticación de FreeRadius

Realizado por: Galo Hurtado. 2017

Con los siguientes pasos se puede configurar un servidor de autenticación FreeRadius para poder analizar de una manera más detallada se puede revisar los anexos.

Con este servidor se va a poder definir la autenticación de acuerdo al número de caracteres que como administradores de red se pueda requerir.

```
sudo apt-get install freeradius
/etc/freeradius
clients.conf
client 192.168.X.X/24
/usr/share/freeradius/
dictionary.rfc2865:
ATTRIBUTE User-Name 1 string
ATTRIBUTE User-Password 2 string
encrypt=1
ATTRIBUTE CHAP-Password 3 octets
ATTRIBUTE NAS-IP-Address 4 ipaddr
ATTRIBUTE NAS-Port 5 integer
ATTRIBUTE Service-Type 6 integer
ATTRIBUTE Framed-Protocol 7 integer
ATTRIBUTE Framed-IP-Address 8 ipaddr
ATTRIBUTE Framed-IP-Netmask 9 ipaddr
```

Figura 51-3: Configuración del servidor FreeRadius

Realizado por: Galo Hurtado. 2017

Es recomendable también configurar la base de datos sql y se realiza de la siguiente manera:

```
sudo apt-get install mysql-server-5.1
sudo apt-get install freeradius-mysql
/etc/freeradius/sql/mysql/ se puede configurar para que tamien trabaje con una base de datos sql
radiusd.conf
INCLUDE sql.conf
En la base de datos sql.conf tenemos:
database = "mysql"
server = "localhost"
login = "db_user"
password = "his_password"
radius_db = "radius"
```

Figura 52-3: Configuración de sql

Realizado por: Galo Hurtado. 2017

3.1.8 Generador de Claves

LastPass genera una clave muy fuerte, al azar y absolutamente imposible de romper.

Figura 53-3: Símbolo LastPass

Realizado por: Galo Hurtado. 2017

La contraseña maestra que se crea será cifrada y ni siquiera LastPass podrá acceder a ella. Todos sus datos están protegidos mediante cifrado AES de 256 bits.

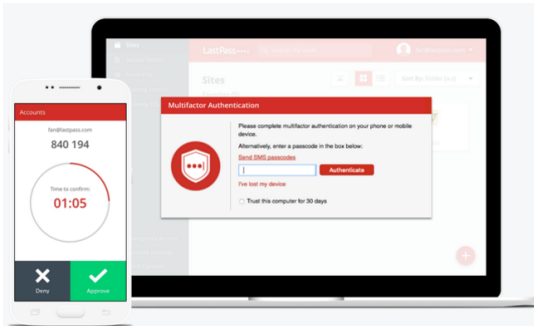


Figura 54-3: Interfaz gráfica de *LastPass*

Realizado por: Galo Hurtado. 2017

Una de las principales ventajas que presenta LastPass es que genera la clave únicamente por un tiempo limitado. Para revisar la instalación completa se puede revisar los anexos.

Los resultados de las políticas implementadas se pueden ver a continuación están valorados dependiendo de su complejidad, la capacidad de memoria que ocupa y la seguridad que brinda.

Tomando como referencia el estándar de seguridad 802.1x y las diferentes recomendaciones que establece se pudo establecer un parámetro de 1-10 de los diferentes protocolos de seguridad implementados en la red de la empresa, con el fin de evitar los diferentes tipos de ataques que se puedan presentar se tienen presente los parámetros como la dificultad de realizar el ataque, la memoria que ocupa implementar dicho servicio en el servidor de seguridad y la seguridad que ofrece una vez implementado dicho parámetro de seguridad.

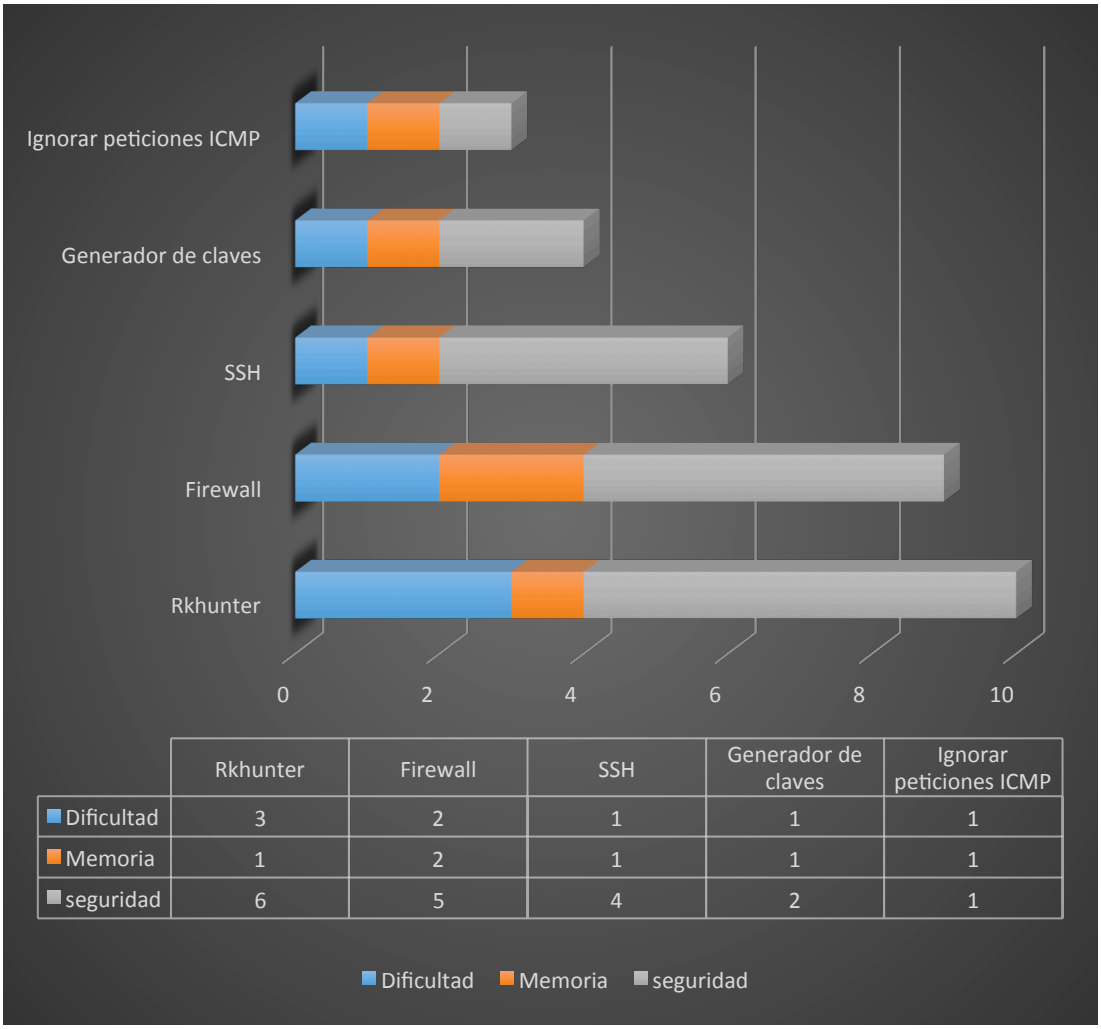


Gráfico 2-3: Resultado del nivel de seguridad implementando políticas.

Realizado por: Galo Hurtado. 2017

En la primera parte se presentó los resultados de la situación actual de la red GUANO.NET se describió el nivel de seguridad dependiendo de los caracteres y el cifrado de las claves para el acceso a los diferentes servicios disponibles en ese momento. Se puede definir el nivel de seguridad alto, medio o bajo dependiendo del tiempo en que se tarde en desencriptar una contraseña.

Tabla 3-3: Situación inicial del nivel de seguridad en la empresa.

Situación Inicial Red GUANO.NET				
	CLAVE	**CARACTERES**	**Tiempo Intel Core i7**	**Nivel de seguridad**
TELNET	Texto plano no cifrada	5	8 segundos	bajo
Mikrotik	cifrada	8	56 minutos	medio
CISCO	por defecto	5	2 segundos	bajo

Realizado por: Galo Hurtado. 2017

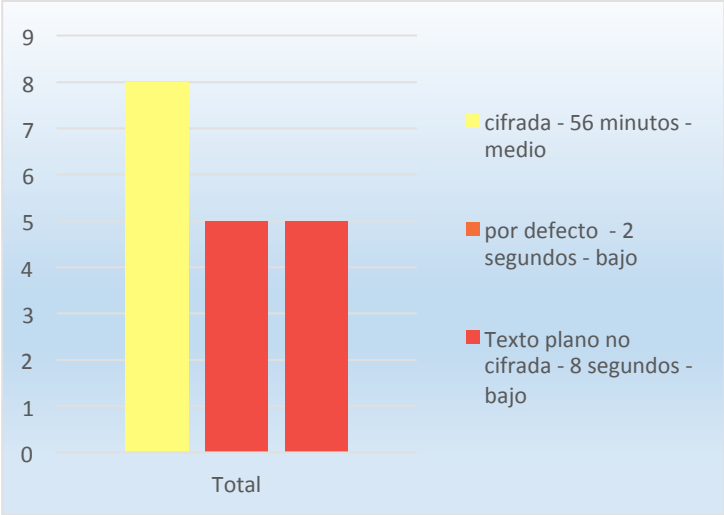


Figura 55-3: Nivel de seguridad dependiendo del número de caracteres.

Realizado por: Galo Hurtado. 2017

IMPLEMENTADO EL SERVIDOR AAA

El tiempo en que se pueda descifrar una contraseña depende principalmente de tipo de contraseña y del procesador del computador con el que se esté atacando a la red, todos los valores que se establecieron está en un rango del 1-10 tomando en consideración las recomendaciones del estándar 802.1x.

Tabla 4-3: Nivel de seguridad que ofrece AAA en MIKROTIK

	CLAVE	Nivel de seguridad	Tiempo Intel Core i7	CARACTERES
	no cifrada	bajo	8 segundos	5
FreeRadius	PAP	medio	56 minutos	8
Generador de claves	WPA 2 EAP	alta	5 meses	8

Realizado por: Galo Hurtado. 2017

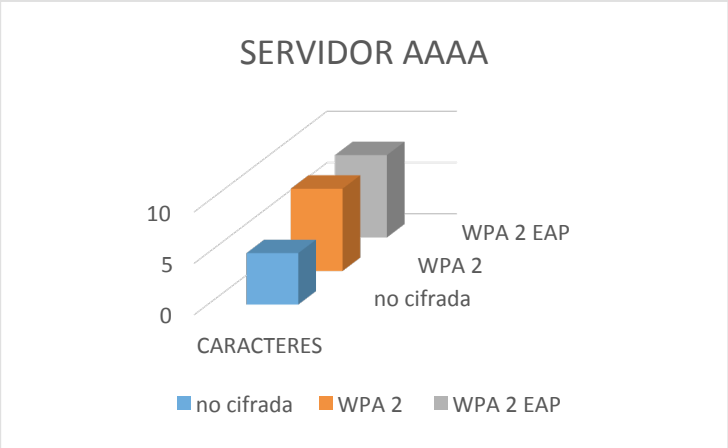


Figura 56-3: Nivel de seguridad de acuerdo al número de caracteres.

Realizado por: Galo Hurtado. 2017

En MIKROTIK solo se pueden emplear contraseñas que cumplan con el parámetro de FreeRadius ya que es el único que se puede configurar en estos equipos al mismo tiempo se puede observar un mejor nivel de seguridad con las políticas que se implementan. De la misma manera se puede ver como se incrementa el nivel de seguridad en los servidores AAA configurados en CISCO.

Tabla 5-3: Seguridad que ofrece el servidor AAA en CISCO

	CLAVE	CARACTERES	**Tiempo Intel Core i7**	**Nivel de seguridad**
	cifrada	8	56minutos	medio
TACACS+ FreeRadius	PPP	8	1 año	alta
	WPA 2 EAP	8	5 meses	alta

Realizado por: Galo Hurtado. 2017

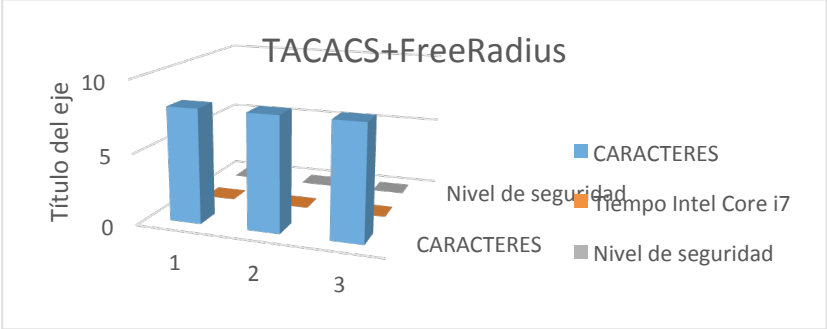


Figura 57-3: Nivel de seguridad de acuerdo al número de caracteres.

Realizado por: Galo Hurtado. 2017

CISCO por otra parte nos permite configurar también el servidor TACACS+FreeRadius siendo TACACS un servidor propietario de cisco y claramente se nota las mejoras en cuento a la seguridad que este servidor nos puede ofrecer.

El nivel de seguridad implementando las políticas definidas anteriormente el código se refiere a la contraseña que viene por defecto, el identificador por lo general viene configurado por defecto, la longitud es la contraseña que nos pide para identificarnos, el autenticador son las políticas implementadas, así como el servidor AAA, el tipo se refiere a la clase de contraseña que se pondrá, y el valor hace referencia al número de caracteres de la contraseña va relacionada con el tipo.

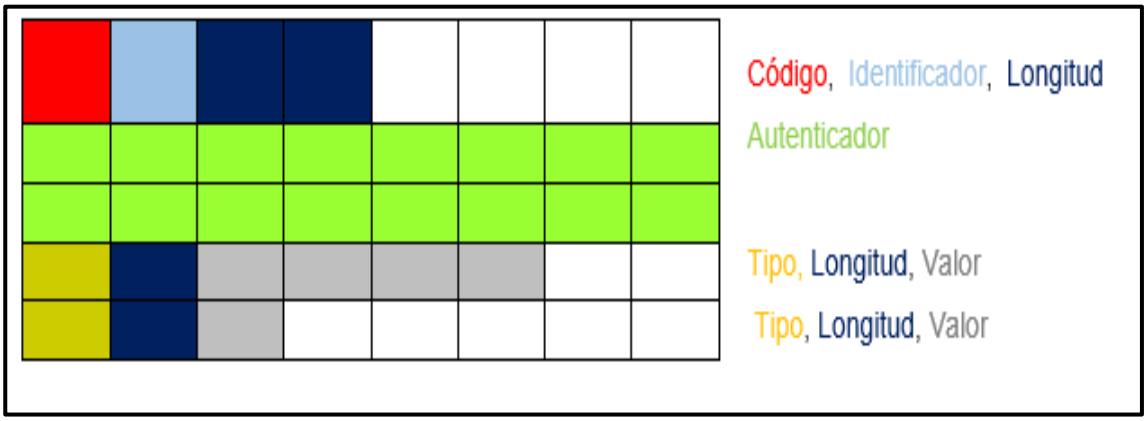


Figura 58-3: Nivel de seguridad con las políticas implementadas.

Realizado por: Galo Hurtado. 2017

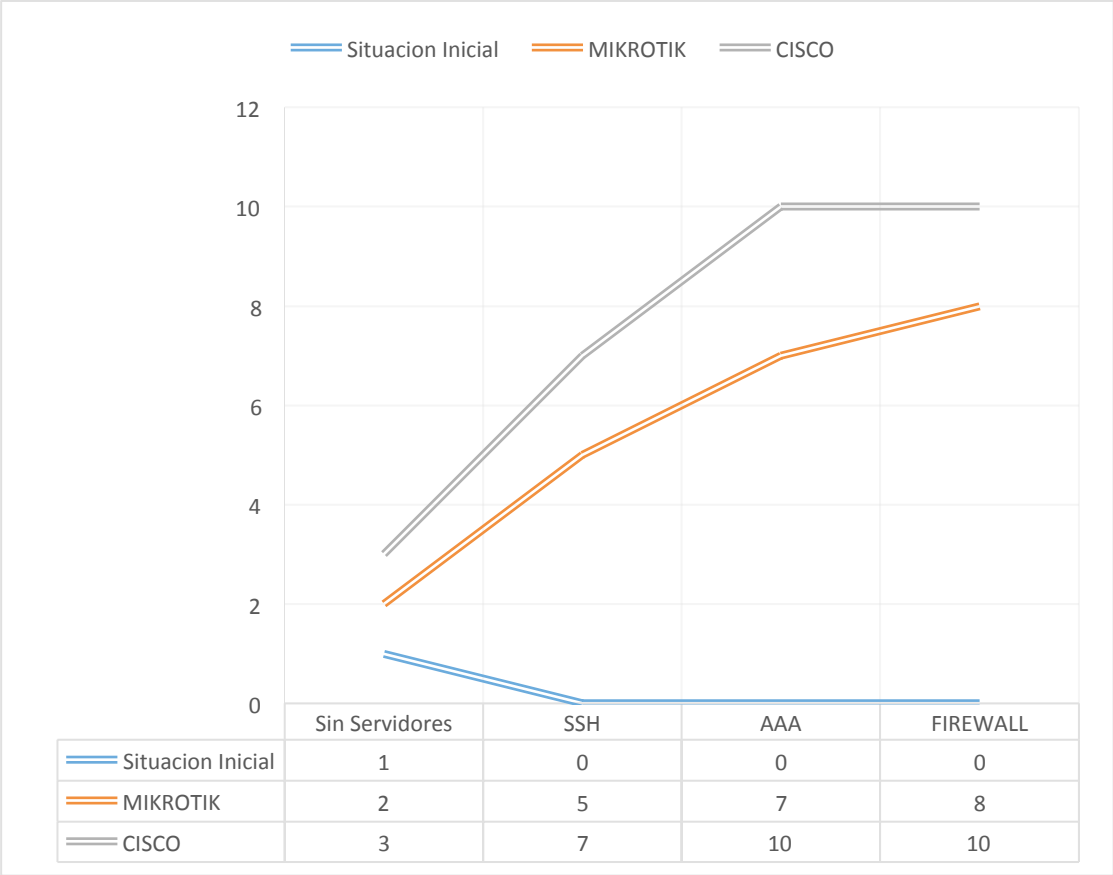
El nivel de seguridad se incrementó con las diferentes políticas de seguridad que se han implementado tomando en consideración, la situación inicial en la que se encontraba la red y realizando diferentes tipos de ataques a la misma, a continuación, se puede observar de una forma más detalla cómo se incrementó el nivel de seguridad.

Tabla 6-3: Comparativa entre servidores configurados.

	Situación Inicial	MIKROTIK	CISCO
Sin Servidores	1	2	3
SSH	0	5	7
AAA	0	7	10
FIREWALL	0	8	10

Alto= 10 Medio=5 Bajo= 1

Realizado por: Galo Hurtado. 2017



	Sin Servidores	SSH	AAA	FIREWALL
Situacion Inicial	1	0	0	0
MIKROTIK	2	5	7	8
CISCO	3	7	10	10

Gráfico 3-3: Nivel de seguridad con servidores implementados.

Realizado por: Galo Hurtado. 2017

Para poder realizar comparaciones entre servidores que se configuren en diferentes tecnologías, se tienen que estudiar cada uno de los parámetros y su funcionamiento. Como se detalla a continuación el funcionamiento de cada uno de los servidores de seguridad tomados en cuenta que cumplen con los requerimientos del estándar 802.1X.

Tabla 7-3: Comparativa AAA entre servidores de seguridad

SERVICIOS	CISCO	MIKROTIK
AAA	TACACS, FreeRadius, Kerberos	FreeRadius
	TCP,UDP	UDP 1812, UDP 1813
	Basa en el modelo cliente/servidor pero además tiene la función de administrar los perfiles y registrar los eventos delos administradores de red.	Basado en el modelo cliente/servidor
	Clave inicial compartida es WPA2- PSK	Clave inicial compartida es WPA- PSK
	Llaves de cifrado	Solo Cifra Clave
	Clave de 256 bits	Clave de 128 bits
	Tiene diferentes servicios de forma independiente	Se combina como un solo servicio
	Encripta todo el cuerpo del paquete TACACS.	Encripta solo al contraseña
	Es propietario de CISCO	La licencia es libre.

Realizado por: Galo Hurtado. 2017

En esta tabla se pretende determinar las ventajas de los servidores AAA en CISCO y MIKROTIK para de esta manera poder tomar decisiones futuras de cuál de los dos poder implementar, CISCO presenta algunas ventajas en cuanto al número de alternativas se pueden seleccionar en su implementación lo que permite tener un mejor cifrado y encriptación.

Tabla 8-3: Comparativa protocolos de autenticación entre servidores de seguridad

SERVICIOS	CISCO	MIKROTIK
PROTOCOLOS DE AUTENTICACION	L2TP	PPTP
	Utiliza IPsec para cifrar los datos	MS-CHAP no encapsulado
	256 bits	128 bits
	Cifrado Triple DES y MD5	el usuario y la contraseña están en texto plano
	Autenticación PPP	Autenticación PAP
	El cifrado de datos empieza antes de la conexión PPP negociando una asociación de seguridad	El cifrado de datos comienza después de que la conexión se procese
	Usan Data Encryption Standard (DES), y posteriormente 3-DES	Un método de cifrado basado en el algoritmo de encriptación Rivest-Shamir-Aldeman (RSA)
	Con llaves de 56 bits para DES o tres llaves de 56 bits para 3-DES	Usa llaves de 40, 56 o 128 bits
	Generador de claves integrado.	El administrador asigna la clave
	Es considerado seguro.	Es rápido y medianamente seguro.
	Tiene una alta disponibilidad en todos los nuevos equipos que tienen sistemas modernos en su infraestructura.	El cliente está integrado casi en todas las plataformas.
	Son fáciles de configurar.	La interfaz que se maneja es gráfica.

Realizado por: Galo Hurtado. 2017

Los protocolos de autenticación son un parámetro fundamental al momento de elegir la tecnología que se va a utilizar, porque se tiene que tomar en consideración el nivel de seguridad que ofrecen es así en el caso de CISCO que implementa un cifrado de 256 bits, a diferencia de MIKROTIK que implementa un cifrado de 128 bits.

Tabla 9-3: Comparativa del protocolo SSH en los servidores de seguridad.

SERVICIOS	CISCO	MIKROTIK
PROTOCOLO SSH	Tiene un cifrado de 256 bits.	Tiene un cifrado de 128 bits.
	SSH V2	SSH V1
	transporte, la autenticación y protocolos de conexión separadas	Protocolos de conexión única
	El atacante requiere 2 veces más de potencia en el cálculo en comparación de SSH V1	Un atacante requiere de 3.4 × 10 (38) operaciones.
	Utiliza algoritmos de cifrado en los dos sentidos.	Usa algoritmos de cifrado solo en el 1 sentido.
	Todo el paquete de datos es cifrado	Negocia la mayor parte del cifrado y todo lo demás es fijo.
	transporta la información por separado es decir la autenticación y los protocolos de conexión	Es un protocolo monolítico de una sola pieza
	autentica tanto el servidor como el usuario que de desea conectar	Autentica tanto el servidor como el usuario que de desea conectar
	Intercambio de claves entre cliente/servidor (negociar)	Se envía la clave solo en texto plano
	Añade un código MAC con una clave secreta para la autenticación de los datos	Nunca establece una negociación por que el cifrado es solo en texto plano
	Compresión de datos antes del cifrado	Compresión de datos antes del cifrado

Realizado por: Galo Hurtado. 2017

La autenticación en el protocolo SSH CISCO establece que se tiene que añadir un código MAC con una clave secreta para la autenticación de los datos y en cuanto MIKROTIK se establece mediante texto plano con una negociación unidireccional.

MIKROTIK establece una interfaz mucho más gráfica y fácil de entender por cualquier administrador de red a diferencia de cisco que establece un entorno grafico no muy entendible por algunos administradores de red.

CONCLUSIONES

- ✓ Analizando la situación inicial de la red se pudo determinar un nivel alto de vulnerabilidad, pudiendo un ataque de denegación de servicio colapsar la red en un 60%, lo cual permite a la empresa GUANO.NET ser un blanco perfecto para un ataque de este tipo dejando como resultado cuantiosas pérdidas, dicho ataque puede llevarse a cabo de forma periódica lo que genera la saturación del servidor hasta dejarlo fuera de servicio.

- ✓ El estándar de seguridad 802.1x permitió determinar las políticas de seguridad más relevantes para poder mejorar el nivel de autenticación en el proveedor de servicios de internet, el estándar recomienda tener un control de acceso a la red, tener en consideración un firewall como media de seguridad, de esta manera controlar la información que se transmite por la red interna de la empresa GUANO.NET.

- ✓ Un adecuado uso de las aplicaciones que son Open Source ayuda a mejorar el rendimiento de los servicios de seguridad entre los principales están: consumir una menor cantidad de recursos y por lo tanto menor cantidad de espacio en el disco, además que se puede encontrar soporte de forma gratuita y esto nos ayuda a disminuir los gatos que tenga la empresa para que de esta forma pueda adquirir nuevos equipos que mejoren el rendimiento de la red.

- ✓ Implementando un servidor de seguridad antes del router de borde nos ayuda tener un sistema que no dependa de los equipos implementados en la red interna está proyectado al crecimiento de los usuarios.

- ✓ Evaluando los servidores de seguridad que tienen diferentes tecnologías se pudo hacer el análisis del funcionamiento y todos los parámetros favorables que pueden ofrecer cada uno de ellos, una de las ventajas principales que se pude obtener en CISCO es que tienen establecidos sus propios parámetros de seguridad los mismos que si presentan algún tipo de vulnerabilidad con las actualizaciones nuevas se pueden controlar, pero esto implicaría más gastos a la empresa, en cuanto a MIKROTIK tiene un solo parámetro de configuración en cuanto a los servidores AAA y es más complicado corregir estas falencias porque son nuevos equipos que están ingresando al sector comercial y al mismo tiempo siendo muy aceptados por sus bajos costos.

RECOMENDACIONES

- ✓ Se recomienda que, en el diseño de la red, se tiene que tener en consideración el nivel de seguridad de la información de los usuarios que se esté transmitiendo por la red, porque como un proveedor de internet se tiene que brindar todas las garantías necesarias para los usuarios del servicio.

- ✓ Se recomienda realizar una capacitación al personal que labora en la empresa en temas de seguridad de redes, esto se determinó con las encuestas realizadas previamente.

- ✓ Se recomienda realizar escaneos a la red de forma periódica para poder determinar si hay algún tipo de anomalía, que se pueden presentar por parte de los usuarios y personas ajenas que buscan perjudicar a la empresa.

- ✓ Se recomienda establecer políticas de seguridad que vayan de acorde a los servicios que se estén brindando, tomando en consideración el número de usuarios y las características de los equipos con los que se cuente en la empresa.

- ✓ Se recomienda tener el diferente software actualizado y con las respectivas licencias con el fin de poder gestionar nuevas vulnerabilidades que se puedan poder presentar y tratar de controlar en su brevedad posible.

BIBLIOGRAFÍA

- **Liserre, Francisco.** *Et 32 tecnicas digitales*. [En línea] [29 de Octubre de 2011. Disponible en: https://sites.google.com/site/et32tecnicasdigitales/home

- **Ávila, Ing. Mario.** *Detección de Malware Avanzado En Redes Organizacionales y Corporativas.* [En linea] 2012. pp. 289 - 295 [Citado el: 6 de Marzo 2017.] Disponible en: http://bibliotecadigital.econ.uba.ar/download/tpos/1502-0569_AvilaRodriguezMR.pdf.

- **Borghello, Cristian.** *Amenazas Lógicas - Tipos de Ataques.* [En linea] 2009. [Citado el: 6 de Marzo 2017.] Disponible en: http://www.segu-info.com.ar/ataques/ataques.htm.

- **Borghello, Lic. Cristian.** *Noticias sobre seguridad de la información.* [En linea] 12 de mayo 2014. [Citado el: 6 de Marzo 2017.] Disponible en: http://blog.segu-info.com.ar/2014/05/infeccion-de-frutas-rat-y-descarga.html.

- **Bustamante, Rubén. "***Seguridad de Redes".* Guatemala - Honduras, pp. 8-43.

- **Cardozo & García, Luis Fran Bladimiro.** "*Clasificación del Malware".* Guadalajara-México, pp. 289-295.

- **Carlos, Ingeniero Juan.** *Seguridad Informatica - Informatica Forensec.* [En linea] 26 de febrero 2017. [Citado el: 6 de Marzo 2017.] Disponible en: http://computoforensec.blogspot.com/2017/02/cuckoo-es-un-sistema-automatizado-de.html.

- **Cisco.** *Catalyst 3750-X and 3560-X Switch Software Configuration Guide, Release 12.2(55)SE. Configuring SPAN and RSPAN.* [En linea] 10 de Noviembre 2014. [Citado el: 6 de Marzo 2017.] Disponible en: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/12-2_55_se/configuration/guide/3750xscg/swspan.html.

- **Cisco.** *Catalyst 3750-X y 3560-X Guía de configuración del interruptor de software, versión 12.2 (55) SE.* [En linea] 10 de Noviembre 2014. [Citado el: 6 de Marzo 2017.] Disponible en: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/12-2_55_se/configuration/guide/3750xscg/swspan.html#37143.

- **EtapaNet.** *Malware*. [En linea] 2010. [Citado el: 7 de Marzo 2017.] Disponible en: http://www.etapa.net.ec/Portals/0/Productos%20y%20Servicios/Malware.pdf.

- **FIE - ESPOCH. "***Inventario Facultad de Informática y Electrónica",* Riobamba : s.n., 2015.

- **López Ferreras, F. & Saturnino Maldonado, R. M. "***Análisis de Circuitos Lineales"*. 3^{ra}ed. México, 2011, pp. 77-84.

- **Galas, Cleto.** *Qué son los virus informáticos.* [En linea] 2 de abril 2015. [Citado el: 6 de marzo 2017.] Disponible en: http://documentslide.com/documents/-que-son-los-virus-informaticos-los-virus-informaticos-son-sencillamente-programas-creados-para-infectar-sistemas-y-a-otros-programas-creandoles.html.

- **Gómez, Prof. Francisco Periañez.** *Características de VirtualBox.* [En linea] 8 de septiembre 2016. [Citado el: 6 de Marzo 2017.] Disponible en: http://fpg.x10host.com/VirtualBox/caractersticas_de_virtualbox.html.

- **Ing. Felipe Pérez Roque, Dr. Enrique Valdés Zaldívar, Dra. Olimpia Arias de Fuentes.** Sistema de Adquisición de Datos con comunicación inalámbrica. *SciELO.* [En linea] Septiembre 2013. [Citado el: 6 de Marzo 2017.] Disponible en: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1815-59282013000300007.

- **Juan, C. V.** *Servicios de seguridad de la informacion.* [En linea] [Citado el : 6 de Marzo 2017.] Disponible en: http://contact.orben.com/seguridad2/?gclid=CjwKEAiArvTFBRCLq5-7-MSJ0jMSJABHBvp0YrfoIZ3JL1ta-pZ0-XEjA9ZrJliy5_1gqFVsgnlUhoCXQLw_wcB.

- **Kali Linux.** *Política de Código Abierto en Kali Linux.* [En linea] 2017. [Citado el: 10 de Marzo 2017.] Disponible en: http://es.docs.kali.org/kali-policy-es/politica-de-codigo-abierto-en-kali-linux.

- **Ledesma, Rodolfo.** *All Networking.* [En linea] 19 de marzo 2008. [Citado el: 10 de marzo 2017.] Disponible en: http://allnetworking.blogspot.com/2008/03/8021q.html.

- **Major, John. 2017.** Malwarebytes. *Endpoint Security.* [Online] 2017. [Cited: marzo 7, 2017.] Disponible en: https://es.malwarebytes.com/business/.

- **2017.** Malwarebytes. *MALWAREBYTES 3.0.* [Online] 2017. [Cited: marzo 6, 2017.] Disponible en: https://es.malwarebytes.com/.

- **Martinez, O. 2015.** desdelinux. *Kali Linux, una gran suite de seguridad informática.* [Online] 2015. [Cited: marzo 10, 2017.] Disponible en:http://blog.desdelinux.net/kali-linux-suite-seguridad-informatica/.

- **Matinez, Andrea. 2011.** andreaswm. *NORMA IEEE 802.1.* [Online] septiembre 2011. [Cited: marzo 10, 2017.] Disponible en: http://andreaswm.blogspot.com/2011/09/norma-ieee-8021.html.

ANEXOS

- **Anexo A. ENCUESTAS REALIZADAS**

Encuesta realizada al personal técnico que labora en la empresa GUANO.NET con la ayuda de la herramienta google drive.

1) **¿Conoce usted el nivel de seguridad que existe entre el uso de un software libre y un software pagado?**

2) **¿Actualmente existe algún sistema de seguridad en la red de la empresa?**

   - **Si**
   - **No**

3) **¿Qué tipos de seguridad usted conoce?**

4) **¿Cree usted que es necesario implementar algún tipo de seguridad en la empresa? ¿Justifiqué por qué?**

5) **¿El nivel de seguridad en la información de los usuarios es?**

   - **Alto**
   - **Medio**
   - **Bajo**

6) **¿Según su criterio los equipos más robustos son CISCO o MIKROTIK?**
7) **¿Cree usted que es necesaria una capacitación de seguridad en redes?**
8) **¿Si se implementa un servicio de seguridad en redes cree usted poder administrarlo?**

RESULTADOS DE LA ENCUESTA REALIZADA

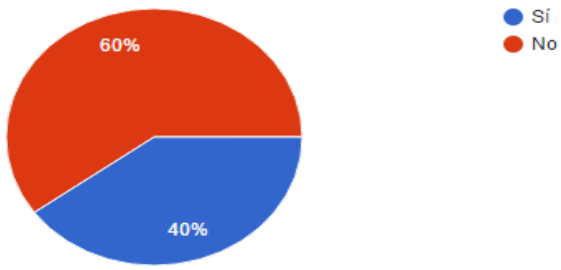
Conoce usted qué nivel de seguridad existe entre el uso de un software libre y un software pagado?

(5 respuestas)

pienso que son lo mismo o el pagado da mas garantias
Costos y licencias para usarlos
no
si
No

Actualmente existe algún sistema de seguridad en la red de la empresa?

(5 respuestas)



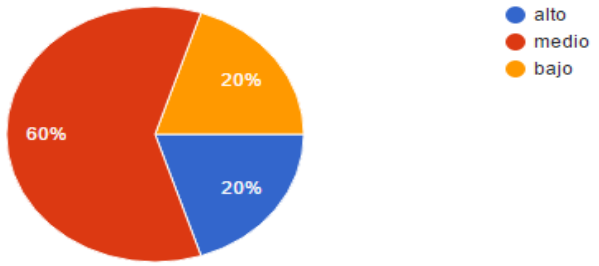
Que tipos de seguridad conoce? (4 respuestas)

antivirus
automatizada
firewall
Antivirus

Cree usted que es necesario implementar algún tipo de seguridad en la red de la empresa? por que
(5 respuestas)

si, para protegernos de todos
Si porque es necesario mejorar la seguirdad y ofrecer una mejor calidad de servicio
si, porque necesita mejor seguridad
por seguridad de datos personales
Para mejorar la integridad de los datos

El nivel de la seguridad en la información de los usuarios es? (5 respuestas)



Según su criterio los equipos más robustos en la red son los CISCO o los MIKROTIK?
(5 respuestas)

cisco
cisco
cisco
Cisco pero el mas usado es MIKROTIK
CISCO

Está usted de acuerdo con que es necesario una capacitación de seguridad en redes?
(5 respuestas)

si
si
si, por que necesitamos saber del tema
Si
SI

Si se implementa un nuevo servicio de seguridad en redes cree usted poder administrarlo?
(5 respuestas)

no, al menos que nos capaciten
Si
no
si
SI precio una capacitacion

- **Anexo B. FIREWALL MEDIANTE LÍNEA DE CÓDIGO**

Instalación del Firewall con línea de código

Para la configuración del firewall se lo puede realizar de dos maneras, una gráfica y atreves de línea de código.
Siguiendo de manera detallada los siguientes pasos se podrá configurar un firewall en Ubuntu.

1. Se comprueba el estado del ufw. En caso de que no esté instalado lo realizamos mediante el siguiente código: **sudo apt-get install ufw**

2. Se procede a revisar lo que tenemos instalado en el firewall inicialmente.

```
root@servidor_guano:~# ls /etc/ufw
after6.rules  after.rules     before6.rules  before.rules  ufw.conf
after.init    applications.d  before.init    sysctl.conf
root@servidor_guano:~#
```

3. Se añaden las reglas a cada uno de los usuarios.

```
Regla añadida
root@servidor_guano:~# sudo ufw allow from 192.168.1.16 to any port 22 proto tcp
Regla añadida
root@servidor_guano:~# sudo ufw allow from 192.168.1.17 to any port 22 proto tcp
Regla añadida
root@servidor_guano:~# sudo ufw allow from 192.168.1.18 to any port 22 proto tcp
Regla añadida
root@servidor_guano:~# sudo ufw allow from 192.168.1.19 to any port 22 proto tcp
Regla añadida
root@servidor_guano:~# sudo ufw allow from 192.168.1.20 to any port 22 proto tcp
Regla añadida
root@servidor_guano:~# sudo ufw allow from 192.168.1.22 to any port 22 proto tcp
Regla añadida
root@servidor_guano:~# sudo ufw allow from 192.168.1.21 to any port 22 proto tcp
Regla añadida
root@servidor_guano:~# sudo ufw allow from 192.168.1.23 to any port 22 proto tcp
```

4. Las reglas que se aplican van de acuerdo a las necesidades.

```
#
# rules.before
#
# Rules that should be run before the ufw command line added rules. Custom
# rules should be added to one of these chains:
#   ufw-before-input
#   ufw-before-output
#   ufw-before-forward
#

# Don't delete these required lines, otherwise there will be errors
*filter
:ufw-before-input - [0:0]
:ufw-before-output - [0:0]
:ufw-before-forward - [0:0]
:ufw-not-local - [0:0]
# End required lines


# allow all on loopback
-A ufw-before-input -i lo -j ACCEPT
-A ufw-before-output -o lo -j ACCEPT

# quickly process packets for which we already have a connection
-A ufw-before-input -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A ufw-before-output -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A ufw-before-forward -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT

# drop INVALID packets (logs these in loglevel medium and higher)
-A ufw-before-input -m conntrack --ctstate INVALID -j ufw-logging-deny
-A ufw-before-input -m conntrack --ctstate INVALID -j DROP

# ok icmp codes for INPUT
-A ufw-before-input -p icmp --icmp-type destination-unreachable -j ACCEPT
-A ufw-before-input -p icmp --icmp-type source-quench -j ACCEPT
-A ufw-before-input -p icmp --icmp-type time-exceeded -j ACCEPT
-A ufw-before-input -p icmp --icmp-type parameter-problem -j ACCEPT
-A ufw-before-input -p icmp --icmp-type echo-request -j ACCEPT

# ok icmp code for FORWARD
"/etc/ufw/before.rules" 77L, 2667C
```

5. Se tienen que añadir las reglas para los usuarios de forma global como se muestra a continuación.

```
root@servidor_guano:~# sudo ufw allow from 192.168.1.0/24  to any port 22 proto tcp
Regla añadida
root@servidor_guano:~# sudo ufw allow from 192.168.2.0/24  to any port 22 proto tcp
Regla añadida
root@servidor_guano:~# sudo ufw allow from 192.168.3.0/24  to any port 22 proto tcp
Regla añadida
root@servidor_guano:~# sudo ufw allow from 192.168.4.0/24  to any port 22 proto tcp
Regla añadida
root@servidor_guano:~# sudo ufw allow from 192.168.5.0/24  to any port 22 proto tcp
Regla añadida
root@servidor_guano:~#
```

6. Se puede denegar los servicios que no se requieren como se muestra a continuación.

```
root@servidor_guano:~# nmap -p 20-200  192.168.0.1

Starting Nmap 6.40 ( http://nmap.org ) at 2017-02-22 14:44 ECT
Nmap scan report for 192.168.0.1
Host is up (0.011s latency).
Not shown: 180 closed ports
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 64:66:B3:40:97:6A (Tp-link Technologies CO.)

Nmap done: 1 IP address (1 host up) scanned in 1.61 seconds
root@servidor_guano:~# sudo ufw deny telnet
Regla añadida
Regla añadida (v6)
root@servidor_guano:~#
```

7. De la misma manera también podemos denegar los servicios de algunos puertos que no se utilicen posteriormente

```
[46] 22/tcp                     ALLOW IN    192.168.1.0/24
[47] 22/tcp                     ALLOW IN    192.168.2.0/24
[48] 22/tcp                     ALLOW IN    192.168.3.0/24
[49] 22/tcp                     ALLOW IN    192.168.4.0/24
[50] 22/tcp                     ALLOW IN    192.168.5.0/24
[51] 22/tcp                     DENY IN     192.168.2.1
[52] 22/udp                     DENY IN     192.168.2.1
[53] 2042 (v6)                  ALLOW IN    Anywhere (v6)
[54] 2043 (v6)                  ALLOW IN    Anywhere (v6)
```

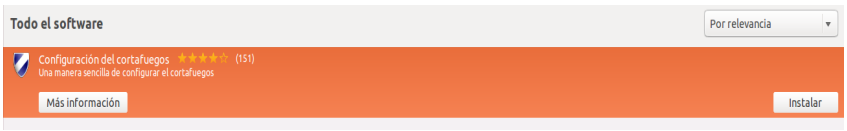
8. Verificar el estado del servidor.

```
23] 22/tcp                     ALLOW IN    192.168.1.1
24] 22/tcp                     ALLOW IN    192.168.1.2
25] 22/tcp                     ALLOW IN    192.168.1.3
26] 22/tcp                     ALLOW IN    192.168.1.4
27] 22/tcp                     ALLOW IN    192.168.1.5
28] 22/tcp                     ALLOW IN    192.168.1.6
29] 22/tcp                     ALLOW IN    192.168.1.7
30] 22/tcp                     ALLOW IN    192.168.1.8
31] 22/tcp                     ALLOW IN    192.168.1.9
32] 22/tcp                     ALLOW IN    192.168.1.10
33] 22/tcp                     ALLOW IN    192.168.1.11
34] 22/tcp                     ALLOW IN    192.168.1.12
35] 22/tcp                     ALLOW IN    192.168.1.13
36] 22/tcp                     ALLOW IN    192.168.1.14
37] 22/tcp                     ALLOW IN    192.168.1.15
38] 22/tcp                     ALLOW IN    192.168.1.16
39] 22/tcp                     ALLOW IN    192.168.1.17
40] 22/tcp                     ALLOW IN    192.168.1.18
41] 22/tcp                     ALLOW IN    192.168.1.19
42] 22/tcp                     ALLOW IN    192.168.1.20
43] 22/tcp                     ALLOW IN    192.168.1.22
44] 22/tcp                     ALLOW IN    192.168.1.21
45] 22/tcp                     ALLOW IN    192.168.1.23
```

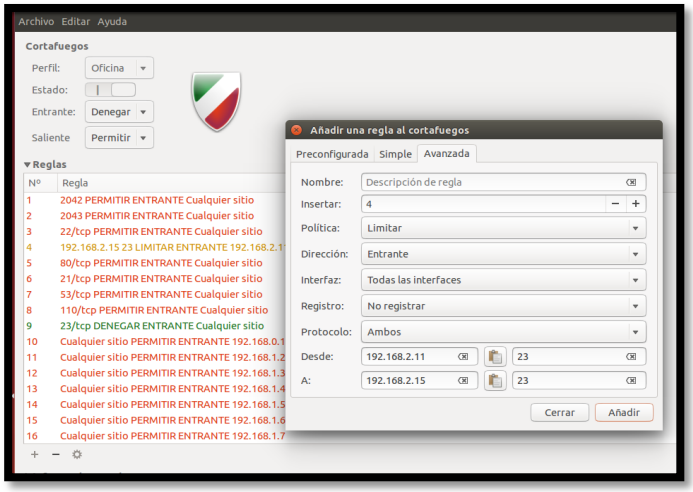
- **Anexo C. FIREWALL DE FORMA GRÁFICA**

  Instalación del Firewall de forma gráfica.

1. Se descarga e instala el firewall para Ubuntu que se puede hacer directamente desde las aplicaciones de Ubuntu.



2. Se añaden las reglas que se crean necesarias.



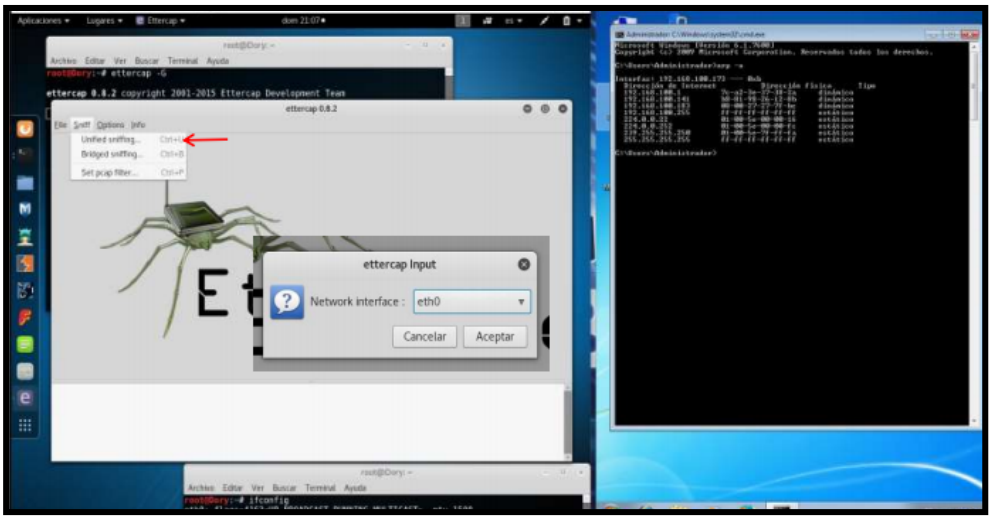
3. Se puede comprobar todo lo que está pasando por el firewall dependiendo de las políticas que se han implementado.

- **Anexo D. ATAQUE MAN IN THE MIDDLE**

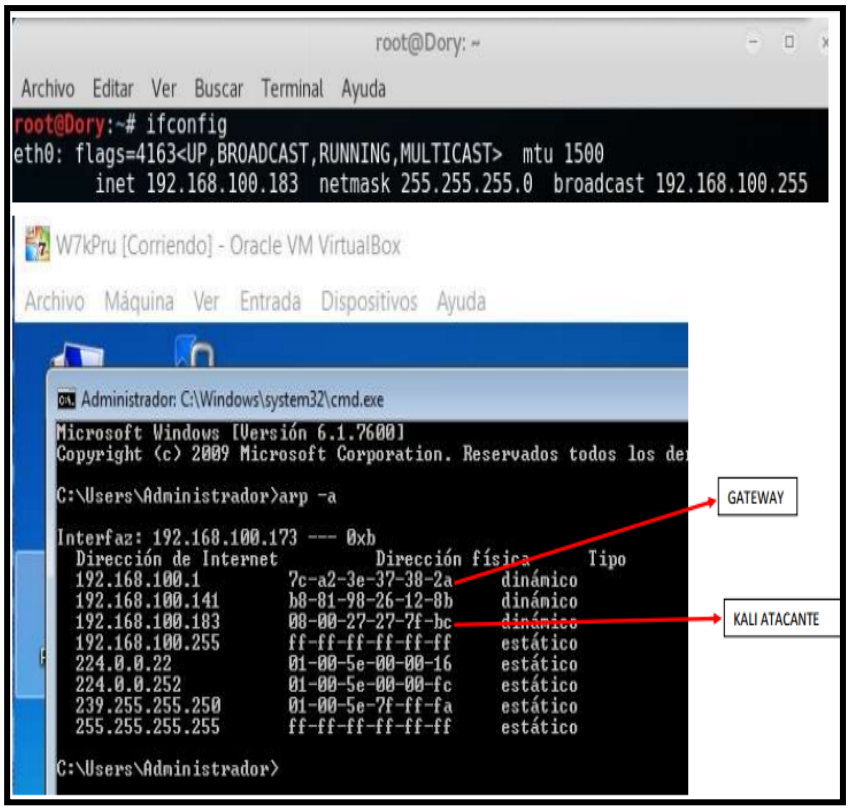
Ataque Man in the Middle (MITM)

Como realizar el ataque paso a paso y de forma detallada

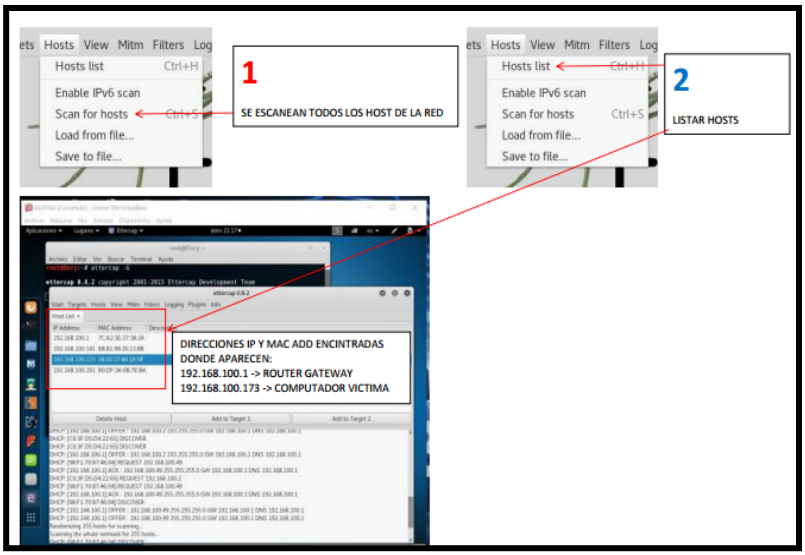
1. **Inici**amos el servicio de ettercap.



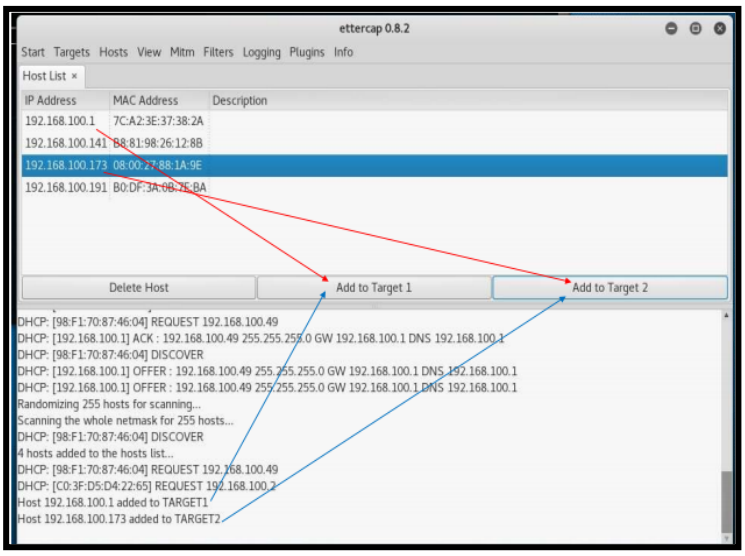
2. Se buscan las direcciones ip e identificamso la de la victima y la del atacante.



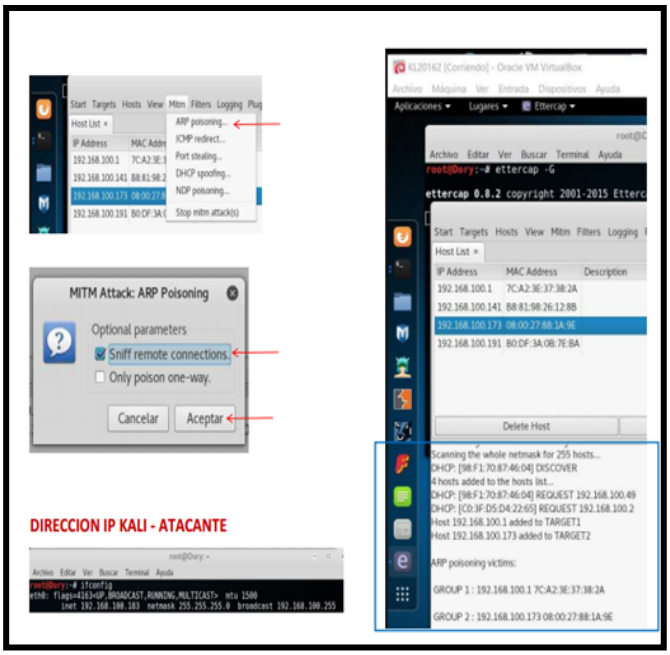
3. Se inicia el escaneo de todos los hosts que se encuentren en al red y se agregan a una lista con sus respectivos gateway.



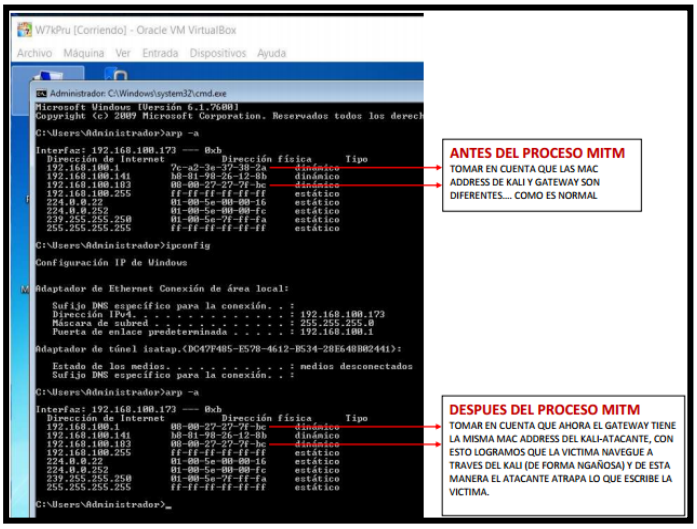
4. Se asignan los diferentes tagets para la victima y para el atacante.



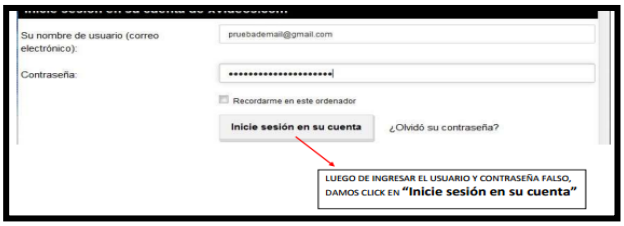
5. Se posesionan las diferentes direcciones de red que pueden ser las posibles victimas como se muetra a continuacion.



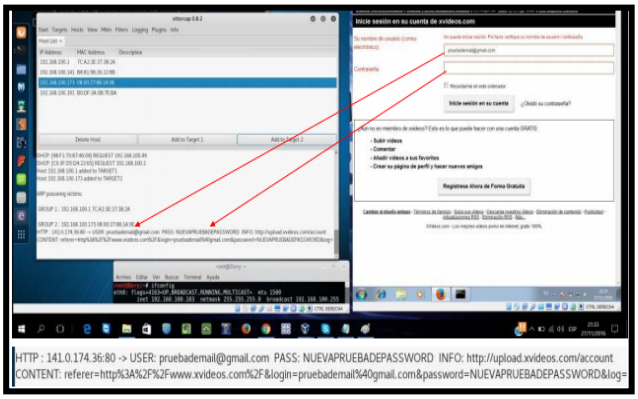
6. Se comprueva que las diferentes mac addres, y getaway teniendo que ser diferentes si los pasos anteriores estan bien.



7. Se puede esperar que al victima ingrese a la página web cualquiera q esta sea e ingrese su identificados y su clave de acceso.



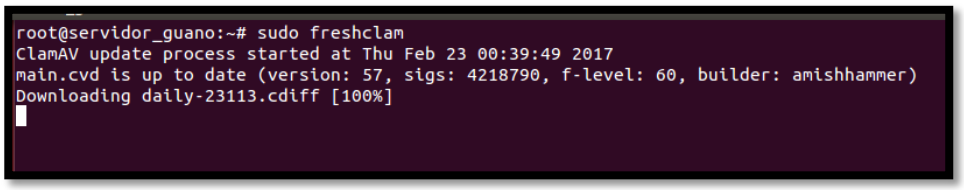
8. Inmediatamente en el taget que se configuro anteriormente se pueden vizualizar sus credenciales de la victima.



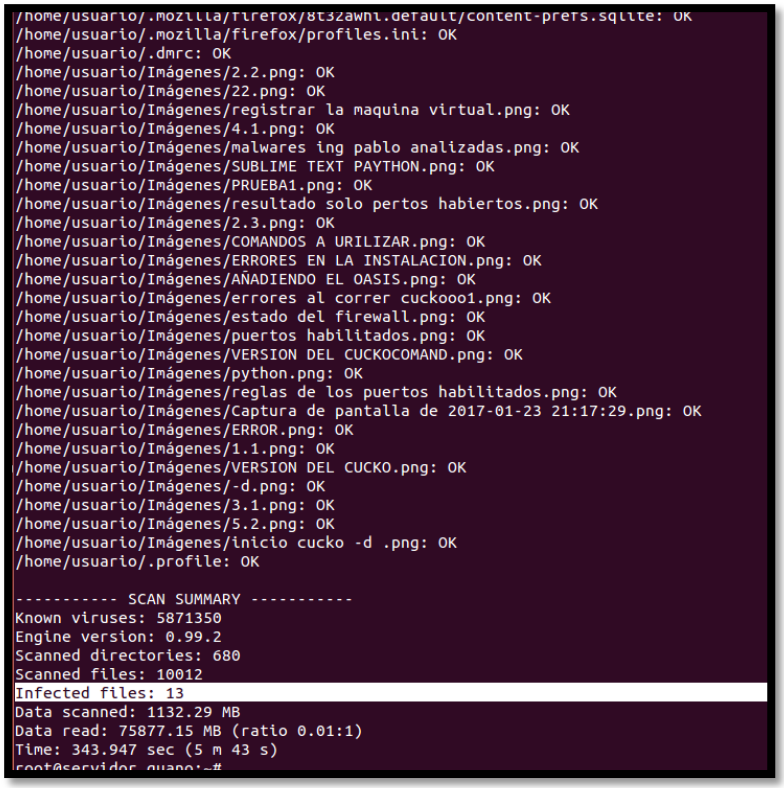
- **Anexo E. INSTALACIÓN DE ClamAV**

Instalación del antivirus para los servicios de seguridad en este caso instalaremos ClamAV que es gratuito en Ubuntu.

1. Se instalan los paquetes que vienen por defecto ya en Ubuntu.



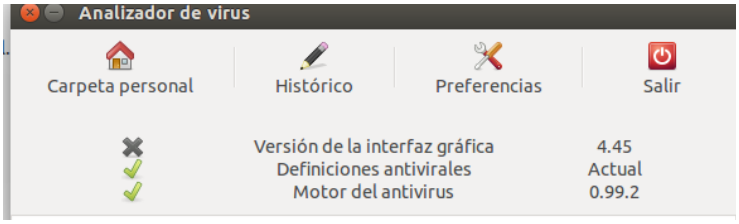
2. Una vez instalado se puede realizar un escaneo detallado de toda la red.



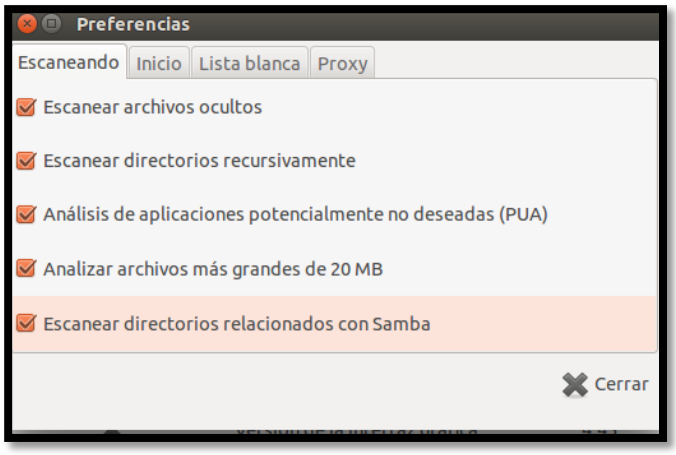
3. **Instalación del antivirus ClamAV de forma gráfica.**

   Se descarga el paquete del antivirus.

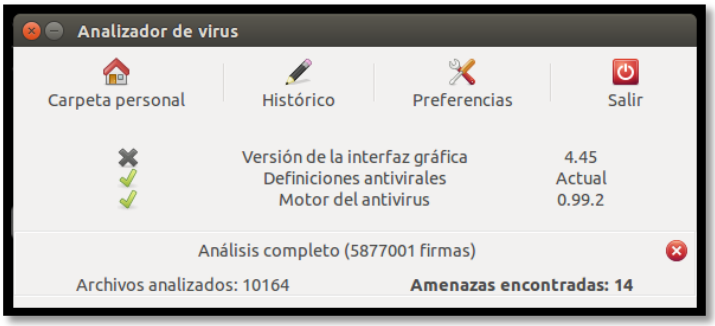
4. Una vez instalado se puede visualizar la interfaz gráfica del antivirus.



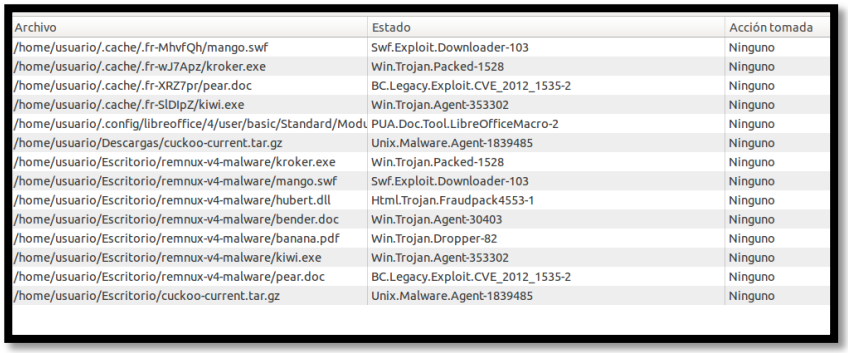
5. Se definen las políticas y lo que se puedan analizar.



6. Resultado del análisis de la red.



7. Resultado detallado del análisis realizado.

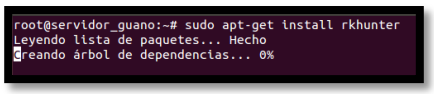


Archivo	Estado	Acción tomada
/home/usuario/.cache/.fr-MhvfQh/mango.swf	Swf.Exploit.Downloader-103	Ninguno
/home/usuario/.cache/.fr-wJ7Apz/kroker.exe	Win.Trojan.Packed-1528	Ninguno
/home/usuario/.cache/.fr-XRZ7pr/pear.doc	BC.Legacy.Exploit.CVE_2012_1535-2	Ninguno
/home/usuario/.cache/.fr-SlDIpZ/kiwi.exe	Win.Trojan.Agent-353302	Ninguno
/home/usuario/.config/libreoffice/4/user/basic/Standard/Modu	PUA.Doc.Tool.LibreOfficeMacro-2	Ninguno
/home/usuario/Descargas/cuckoo-current.tar.gz	Unix.Malware.Agent-1839485	Ninguno
/home/usuario/Escritorio/remnux-v4-malware/kroker.exe	Win.Trojan.Packed-1528	Ninguno
/home/usuario/Escritorio/remnux-v4-malware/mango.swf	Swf.Exploit.Downloader-103	Ninguno
/home/usuario/Escritorio/remnux-v4-malware/hubert.dll	Html.Trojan.Fraudpack4553-1	Ninguno
/home/usuario/Escritorio/remnux-v4-malware/bender.doc	Win.Trojan.Agent-30403	Ninguno
/home/usuario/Escritorio/remnux-v4-malware/banana.pdf	Win.Trojan.Dropper-82	Ninguno
/home/usuario/Escritorio/remnux-v4-malware/kiwi.exe	Win.Trojan.Agent-353302	Ninguno
/home/usuario/Escritorio/remnux-v4-malware/pear.doc	BC.Legacy.Exploit.CVE_2012_1535-2	Ninguno
/home/usuario/Escritorio/cuckoo-current.tar.gz	Unix.Malware.Agent-1839485	Ninguno

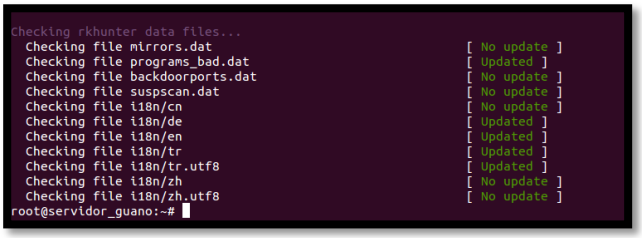
- **Anexo F. RKHUNTER**

Instalación de Rkhunter

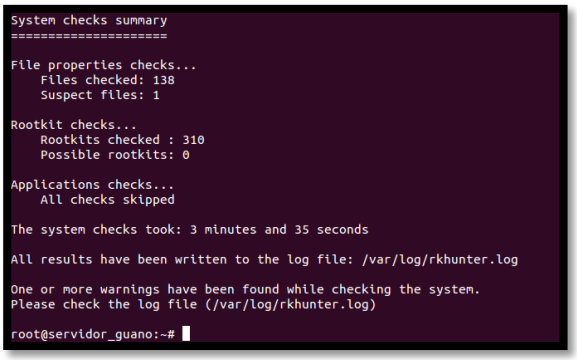
1. Se instala el paquete ya definido en Ubuntu.



2. Se tiene que revisar todos los paquetes instalados por rkhunter.



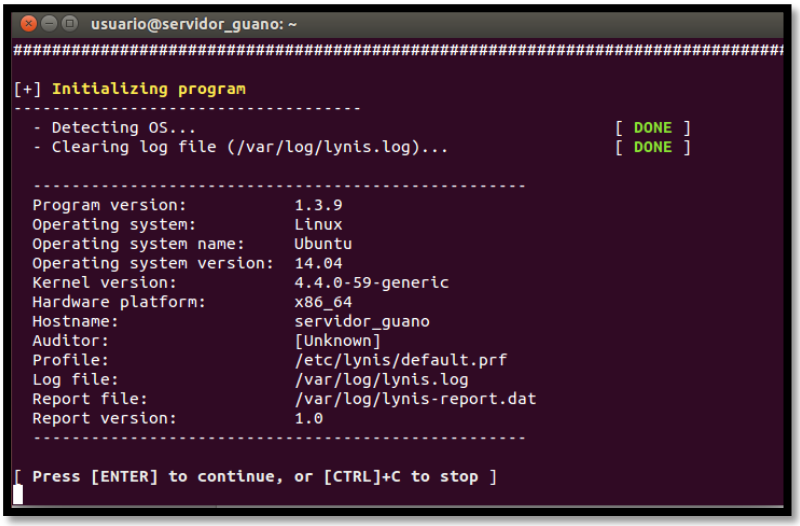
3. A continuación, se presentan los resultados del análisis.



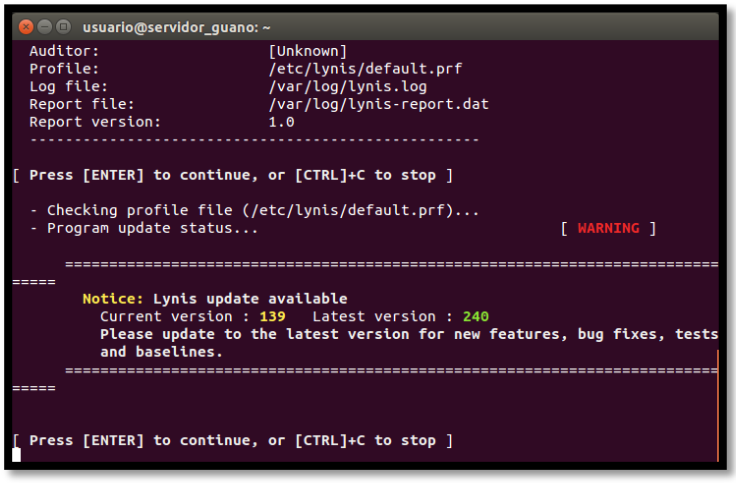
- **Anexo G. LYNIS**

Instalación de Lynis

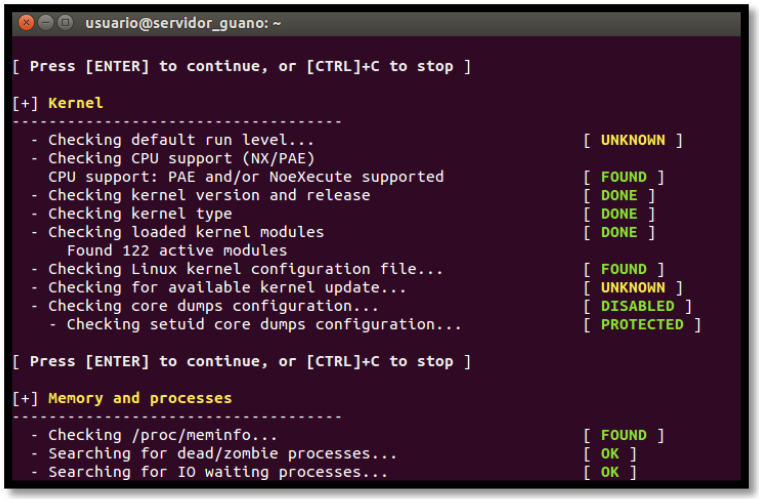
1. Se ingresa el comando **sudo apt-get install lynis** para instalar el paquete en el servidor y con **lynis –c** se ejecuta el paquete.



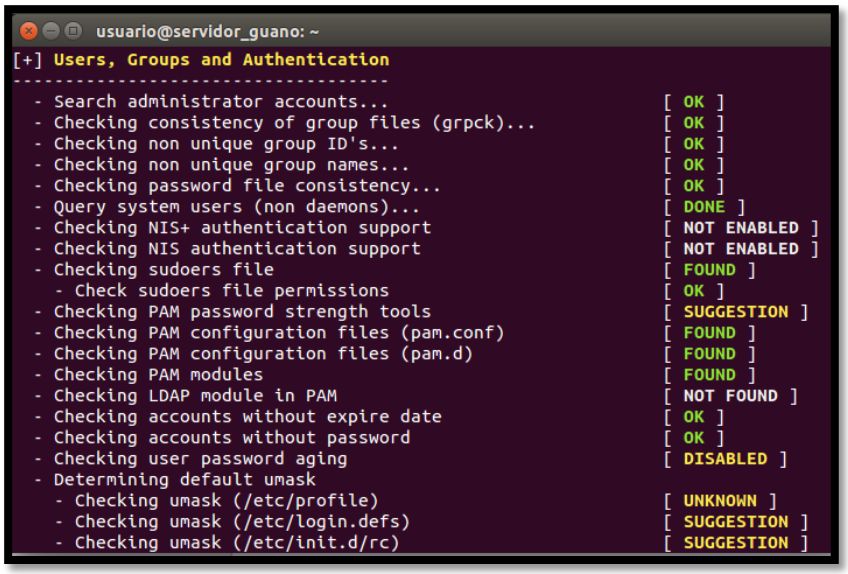
2. Se puede observar el estado de la aplicación y la versión.



3. Inicia el analisis del servidos para ver las herramientas que estan instaladas y cuales no.

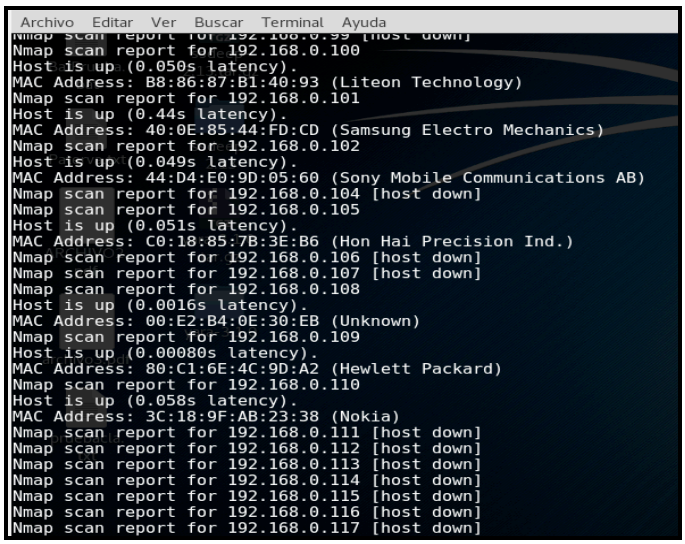


4. En este punto se analizará todo lo relacionado con usuarios y la autentificación en el sistema.

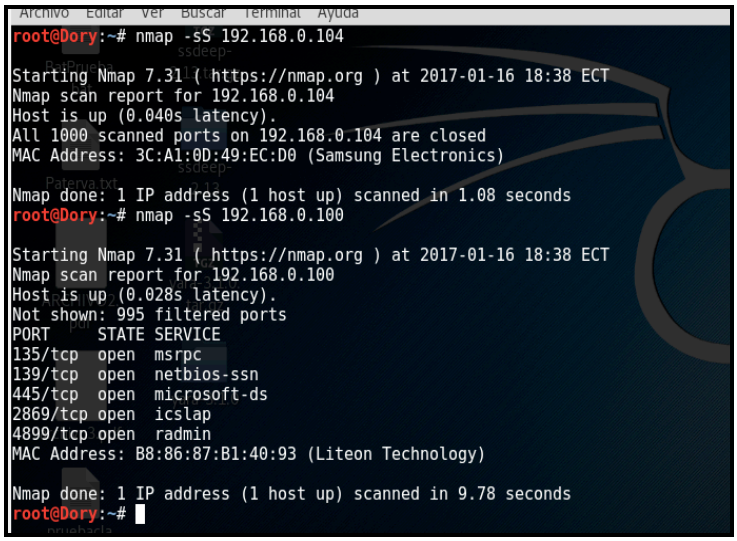


- **Anexo H. ANÁLISIS DE TRÁFICO**

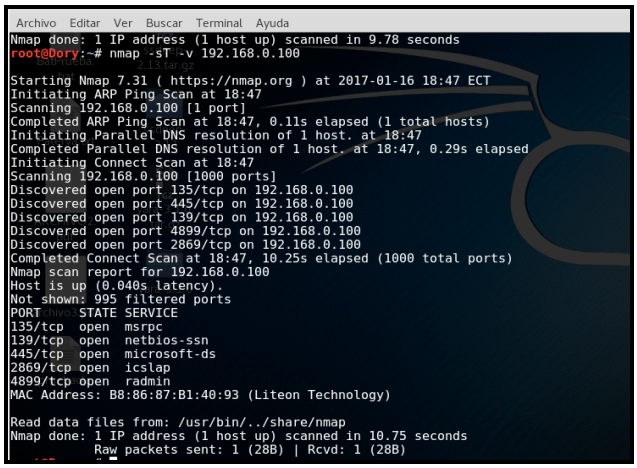
1. Ingresando el código: **nmap –sn –v i la respectiva dirección IP 192.168.0.0/24** se puede revisar el estado de los puertos de una dirección específica.



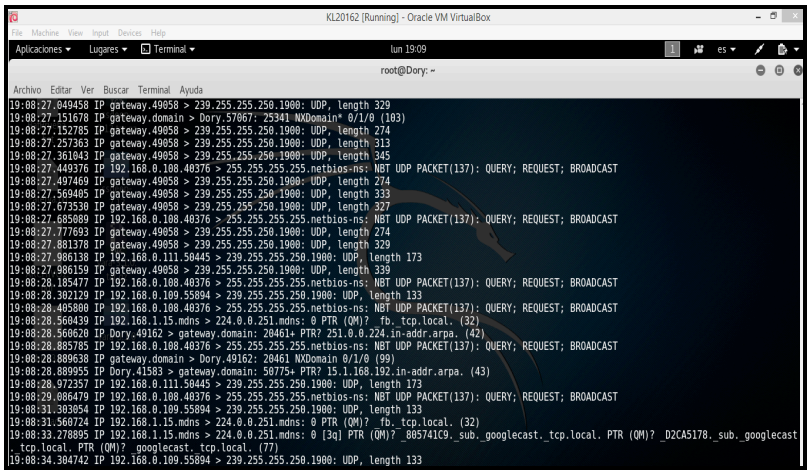
2. Posteriormente se buscan los puertos abiertos y cerrados de la red para poder visualizar de una máquina especifica se puede ayudar del comando **nmap –sS 192.168.0.100**



3. Para un escaneo mucho más detallado se puede utilizar el comando **–sT.**



4. Para poder ver el tráfico de la red se tiene que insertar el comando tcpdump y la dirección IP de la red **192.168.0.0/24**



5. Para poder visualizar las interfaces que están disponibles únicamente se añade –D al comando **tcpdump**