UNIVERSIDAD POLITECNICA DE VALENCIA

DEPARTAMENTO DE COMUNICACIONES

Máster Universitario en Tecnologías, Sistemas y Redes de Comunicaciones

Evaluación De Herramientas De Generación De Tráfico Malicioso Aplicadas A Una Red IP Virtualizada

Autor: Luis Alberto Uvidia Armijo

Director: PhD. Manuel Esteve Domingo

Fecha de comienzo: 08/05/2017

Lugar de trabajo: Grupo de Investigación Sistemas y Aplicaciones de Tiempo Real Distribuidas

Departamento de Comunicaciones UPV

Objetivos — El presente trabajo tiene como objetivo principal evaluar y simular ataques cibernéticos, mediante el uso de herramientas de generación de tráfico malicioso, aplicándolas a una red IP virtualizada representando un entorno empresarial de datos, al cual se le va aplicar varios tipos de ataques a fin de evaluar el nivel de seguridad y proponer acciones óptimas para contrarrestar dichos ataques.

Metodología — El presente trabajo consiste en una metodología teórica y práctica. En primer lugar, se ha efectuado una revisión teórica acerca del ciberterrorismo actual y los tipos de ataques más frecuentes, así como también los tipos de herramientas que se utilizan para generar tráfico malicioso, por otra parte, se ha revisado el estado del arte de la seguridad informática con propuestas y proyectos afines a su desarrollo. Para posteriormente realizar el diseño y simulación de una red IP virtual, que permite simular una empresa con equipos interconectados, mediante la utilización de un generador de entornos virtuales, a fin de demostrar la vulnerabilidad de la red frente a diferentes tipos de ataques a los cuales se puede enfrentar, se ha realizado simulaciones con diferentes sistemas operativos para obtener resultados más apegados a un entorno empresarial de datos real.

Desarrollos teóricos realizados — Como paso inicial para nuestro estudio, se ha efectuado una revisión teórica sobre los ciberataques más comunes en los últimos tiempos, se buscaron herramientas generadoras de trafico malicioso de acceso libre, se ha reunido información necesaria sobre el estado del arte de la seguridad informática, basándonos en los resultados, el estudio brinda una idea de los puntos claves de cómo mejorar en el extenso campo de la ciberseguridad con la ayuda de los resultados obtenidos en las simulaciones desde el punto de vista práctico, para poder determinar un mecanismo de control frente a los ataques generados.

Desarrollo de prototipos y trabajo de laboratorio — Con base en la recolección de información, se realizaron varias simulaciones de ataques a una red empresarial virtualizada, ajustándonos a los requerimientos planteados en el marco teórico en el ámbito de la seguridad informática de las redes, se realizó, además un análisis de los resultados obtenidos al momento de efectuar un ataque, para de esta forma establecer mecanismos de defensa que pueden ser utilizados en un ambiente real.

Resultados — Se realizó la construcción y diseño de la red IP virtualizada en el equipo anfitrión conformada por un equipo servidor basado en el sistema operativo Ubuntu, tres equipos clientes y un equipo enrutador, mediante el uso de la herramienta Virtual Box se logró obtener simulaciones reales gracias a su optimo desempeño, una vez montada la red se usó las herramientas generadoras de tráfico malicioso en los equipos clientes, logrando efectuar diversos ataques al servidor de la red empresarial de entre los cuales están, el ataque de detección de puertos, ataque de fuerza bruta, ataque de hombre en el medio, ataque denegación de servicios y el ataque de suplantación de identidad (phishing), por otro lado se comprobó los análisis obtenidos mediante la herramienta Wireshark que permitió localizar los puertos, el protocolo y el equipo atacante utilizados para efectuar el ataque, logrando identificar las vulnerabilidades del servidor y de la red IP virtualizada. Finalmente se implementó mecanismos de control de ataques en los equipos que conforman la red, a través de la herramienta *ESET smart security 9*, el cual filtro ataques mediante el módulo de cortafuegos programable brindándonos la opción de eliminar o bloquear las potenciales amenazas, adicionalmente se implementó un cortafuegos generado a través de Iptables dentro del servidor Ubuntu, como complemento adicional se instaló la aplicación ARPwhatch la cual envía al administrador un correo electrónico en el momento que alguien intenta atacar el servidor Ubuntu, de esta manera pudimos contrarrestar los ataques generados.

Líneas futuras — Promover la generación de desarrollo, partiendo del presente estudio como base para futuros análisis a medida del avance de la tecnología y el pasar de los años con futuros ataques, además, es un sustento teórico para implementaciones en un entorno empresarial de datos real, ya que contiene puntos importantes como las posibles amenazas y ataques que puede ser víctima.

Abstract — Con la evolución de las telecomunicaciones y el pasar de los años, se ha visto que las empresas cada vez dependen más de su infraestructura de red, por consecuencia cualquier problema que se genere por más pequeño que sea puede llegar a colapsar sus operaciones. La falta de protección en las redes es un problema común hoy en día, de tal manera que ha surgido un número alarmante de ciberdelincuentes que cada vez mejoran sus habilidades de ataque obteniendo mayores beneficios incluso infiltrándose en la misma empresa. El trabajo actual contiene detalles de una recolección de información sobre seguridad informática y herramientas generadoras de tráfico malicioso, siendo necesarias a la hora de gestionar pruebas de desempeño y funcionalidad de una red empresarial, la mayoría de estas herramientas son de código abierto que están disponibles para poder ser utilizadas, modificadas o mejoradas por la comunidad académica de acuerdo a sus requerimientos. Posteriormente se diseña y simula una red IP virtualizada para poder demostrar el potencial de ataque de dichas herramientas, se realiza un análisis de resultados a tener en cuenta en caso de que suceda un ataque real, concluyendo con una descripción de métodos apropiados para contrarrestar los distintos ataques simulados.

Autor: Uvidia Armijo Luis Alberto email: luiuv@teleco.upv.es
Director: Esteve Domingo Manuel email: mesteve@dcom.upv.es
Fecha de entrega: 04-07-2017

ÍNDICE

I. INTRODUCCIÓN.

Con la evolución de las telecomunicaciones, el pasar de los años y las múltiples investigaciones sobre la seguridad de redes, se ha visto que las empresas cada vez dependen más de su infraestructura de red y cualquier problema que se genere, por más pequeño que sea puede llegar a colapsar las operaciones. La falta de protección de las redes es un problema muy común hoy en día, de tal manera que han salido a la luz un número alarmante de atacantes, y cada vez van mejorando sus habilidades de ataque obteniendo mayores beneficios incluso infiltrándose en la misma empresa.

Generalmente los ataques aprovechan vulnerabilidades de un sistema operativo, comúnmente desconocidos por el fabricante y que conllevan a dejar puertas abiertas para ciberdelincuentes, el proceso de establecimiento de una red segura requiere la necesidad de realizar pruebas de eficiencia y comportamiento, para lo cual se vuelve una necesidad muy relevante la utilización de herramientas que poseen la capacidad de generar tráfico de distintos tipos a redes ya sean reales o simuladas, con el fin de evaluar sus características y rendimientos logrando tener una mejor percepción del comportamiento de las mismas.

Debido a estos requerimientos varios investigadores han recurrido a la necesidad de desarrollar herramientas que posean la capacidad de realizar pruebas de funcionamiento simulando ataques a servidores en entornos virtuales como en redes de infraestructuras en el mundo real, con el objetivo de demostrar que se puede conseguir acceso al sistema, robo de información privilegiada, información de estados bancarios, y más comúnmente desestabilizar el sistema o servidor, encontrando vulnerabilidades del sistema de las cuales se pueda beneficiar el ciberterrorismo.

Gracias a la ayuda de estas herramientas se realiza una gestión de la red, y a partir de un reporte detallado de cada uno de los sucesos durante la ejecución del ataque, se generarán hipótesis en cuanto a qué pasa sí la red o los servicios se ven afectados por un ataque real, lo cual define que tan disponible y eficiente es la red y se determinará si cumple o no con calidad de servicio.

El trabajo actual contiene detalles de una recolección de información sobre seguridad informática y herramientas generadoras de tráfico, las cuales pueden ser de ayuda a la hora de gestionar pruebas de desempeño y funcionalidad de una red, la mayoría de estas herramientas son Open Source (de código abierto) las cuales están disponibles para poder ser utilizados, modificados o mejorados por la comunidad académica e investigadora de acuerdo a las especificaciones de cada investigación o trabajo a realizar.

El contenido de la investigación realizada nos permite apreciar que existe un gran número de herramientas generadoras de tráfico para la realización de ataques de distinto tipo, de los cuales se hace

una breve reseña de sus características y aplicación. Adicionalmente se hace una descripción de los métodos para contrarrestar los ataques en distintos sistemas operativos.

II. ESTADO DEL ARTE

II.1 SEGURIDAD INFORMÁTICA

A medida que el uso de Internet día a día va en aumento, cada vez más compañías conceden privilegios a sus socios y proveedores de ingresar a sus sistemas de información. Por esta razón es fundamental conocer qué recursos de la compañía necesitan protección para de esta manera poder controlar el acceso al sistema y los derechos de los usuarios del sistema de información. Los mismos procedimientos se aplican cuando se permite el acceso a la compañía a través de Internet [1].

Por otro lado, a consecuencia de la tendencia creciente de hoy en día hacia un estilo de vida nómada que permite a los empleados estar conectados a los sistemas informáticos desde cualquier lugar, se solicita a los empleados que lleven consigo parte del sistema de información fuera de la infraestructura segura de la compañía [2].

La amenaza representa el tipo de acción que tiende a ser dañina, mientras que la vulnerabilidad representa el grado de exposición a las amenazas en un contexto particular. Finalmente, la contramedida representa todas las acciones que se implementan para prevenir la amenaza.

Las contramedidas que deben implementarse no sólo son soluciones técnicas, sino también reflejan la capacitación y la toma de conciencia por parte del usuario, además de reglas claramente definidas. Para que un sistema sea seguro, deben identificarse las posibles amenazas y, por lo tanto, conocer y prever el curso de acción del enemigo. Por tanto, el objetivo de este informe es brindar una perspectiva general de las posibles motivaciones de los hackers, categorizarlas, y dar una idea de cómo funcionan para conocer la mejor forma de reducir el riesgo de intrusiones [1].

La seguridad informática se representa, a menudo, en cinco puntos importantes:

- **Integridad**: Asegurar la originalidad de los datos sin alterar sus características.
- **Confidencialidad**: Lograr que solamente las personas con autorización obtengan permiso de acceso a recursos privilegiados.
- **Disponibilidad**: Asegurar el buen desempeño de los sistemas informáticos.
- **Evitar el rechazo**: Asegurar de que no pueda impedir una operación inicializada.
- **Autenticación**: Asegurar el acceso a los recursos únicamente a los individuos autorizados.

II.2. *TRABAJOS PREVIOS*

En el ámbito de la seguridad en las redes la comunidad científica se ve en la necesidad de buscar la creación de soluciones para contrarrestar los ataques usando las tecnologías de la virtualización, existen trabajos muy importantes de entre los más destacados están los citados a continuación:

S. Al Kaabi et al. [3], Este documento discute una plataforma educativa ética, llamada DoS-VLab, que tiene como objetivo permitir que los estudiantes experimenten ataques comunes de negación de servicio (DoS), en un ambiente académico seguro. La plataforma DoS-VLab se basa en tecnologías de virtualización y simulador de redes GNS3 para la creación de redes virtuales.

T. Zseby et al. [4]. Presentan un proyecto de laboratorio de seguridad de red para enseñar métodos de detección de anomalías de tráfico de red en el espacio oscuro el cual contiene tráfico no deseado relacionado con millones de direcciones de Internet en todo el mundo. Esta amplitud de cobertura hace que sea una excelente opción para un estudio práctico de técnicas de detección de ataques en Internet.

En el estudio realizado por J Keller y R Naues [5]. Realizan la creación de un laboratorio virtual de seguridad informática para impartir conocimientos a sus estudiantes utilizando el sistema basado en la Web CURE que proporciona gestión de contenido de acuerdo a los requerimientos de seguridad.

El presente trabajo tiene como objetivo principal evaluar y simular ataques cibernéticos, mediante el uso de herramientas de generación de trafico malicioso, aplicándolas a una red IP virtualizada representando un entorno empresarial de datos, al cual se le va aplicar varios tipos de ataques a fin de evaluar el nivel de seguridad y proponer acciones óptimas para contrarrestar dichos ataques. Mediante el uso de herramientas de acceso libre (Open Source) con interfaces gráficas, demostrando su gran efectividad a la hora de realizar ataques a la red.

El escenario virtual al cual se le aplica las pruebas de ataques en el presente estudio, contiene una serie de elementos que existen en las infraestructuras reales y son:

- Acceso a Internet (Red LAN y red inalámbrica)
- Servidor interno (Proporciona los servicios de correo electrónico, base de datos y servicios Web).
- Equipos clientes (Con sistema operativo Linux y Windows).
- Equipo de enrutamiento (Router).

Se justifica la infraestructura propuesta ya que representa un escenario real propio de una pequeña empresa, para cubrir los objetivos específicos de una organización en lo referente a seguridad informática, se debe implementar y actualizar continuamente una cantidad de controles entre los cuales pueden ser políticas de seguridad, manuales, panes de contingencia en caso de pérdida de información, funcionalidades de los softwares utilizados, etc. Cuya importancia depende en que exista una constante revisión y mejora.

III. EL CIBERTERRORISMO Y CIBERCRIMEN

III.1. *CIBERTERRORISMO Y CIBERCRIMEN*

Se han convertido en dos amenazas emergentes en una sociedad digital que inquietan cada vez más a los ciudadanos, quienes, hoy por hoy, se sienten vulnerables frente a la materialización de las mismas y sus efectos reales sobre la confianza en el Estado y sus instituciones.

Si bien la ciberdefensa como la ciberseguridad, son temas de estudio e investigación actual tanto en la industria, la docencia o el Gobierno, es claro que requieren atención inmediata con acciones definidas que permitan comunicar a los potenciales agresores que estamos preparados para enfrentar el reto de un ataque informático coordinado y hacer respetar nuestra soberanía digital.

Por otra parte, definir y desarrollar su misión y visión es sumamente necesaria. Misión, para coordinar los planes necesarios para la protección de las infraestructuras críticas del Estado, frente a emergencias de ciberataques que atenten o comprometan la Seguridad. Visión, como fundadora del desarrollo de una cultura de ciberseguridad en los organismos y entes del Estado y las entidades gestoras de las infraestructuras críticas nacionales, enfocada a la protección del ciberespacio, adoptando y promoviendo el desarrollo de estrategias coordinadas de ciberseguridad para contribuir a la seguridad de la nación ante amenazas internas y externas materializadas a través del uso de tecnologías de la información y comunicaciones.

Con todo ello, el eslabón más débil de la cadena de seguridad es el ser humano. Los individuos involucrados en los diferentes procesos, procedimientos de gestión y operación de una Infraestructura Crítica deben estar concienciados y capacitados con la importancia y necesidad de que dicha infraestructura sea segura, basando su sensibilización en los distintos niveles de responsabilidad y funciones [6].

III.2. *FALLOS DE SEGURIDAD*

La mayor parte de los problemas referentes a la protección e integridad de la información se basa en el método básico del desarrollo e implementación del proceso de seguridad de la información. De esta manera se pueden evidenciar fallos muy graves, que comúnmente suelen presentarse de entre los cuales tenemos:

- **La falta de una normativa con reglas y procedimientos.**

Las normativas en una empresa o institución son necesarias para el correcto desempeño de los trabajadores o estudiantes a la hora de hacer uso de los recursos informáticos, siguiendo procedimientos y reglas para evitar cualquier tipo de errores, por ejemplo, el control de los tipos de correo electrónico que se recibe, en este caso la empresa o institución tendrán que informar sobre el uso adecuado de filtros de correos maliciosos a sus usuarios, para evitar ataques informáticos.

- **El control de acceso autorizado.**

La mayoría de las organizaciones poseen un sistema de identificación para poder ingresar a las instalaciones las no son individuales, en muchos de los casos son utilizadas por un grupo determinado de usuarios. De esta manera se puede infiltrar personas no autorizadas ya que con ese acceso común es sumamente complicado ubicar al usuario que realizo determinada acción.

- **La falta de un administrador informático.**

Es uno de los factores más influyentes para garantizar la seguridad, toda la responsabilidad de la información posee el administrador, ya que es la persona que autoriza o no el acceso a los usuarios de la empresa o institución a determinada información, es quien da los privilegios de acceso.

- **Planes de contingencia.**

Los planes de contingencia de la empresa o institución deben ser frecuentemente actualizados, ya que muchas de las veces dichos planes quedan sin importancia y olvidados en el tiempo. Un plan de contingencia debe ser actualizado continuamente y expuesto a pruebas de aplicación.

- **Resguardo de información.**

Es recomendado realizar copias de seguridad de la información ya sea por motivos legales o por el hecho de mantener a salvo archivos o información importante de la empresa o institución, es recomendable establecer periodos de tiempo en los que se realice las copias de seguridad teniendo en cuenta el procedimiento, para una eventual recuperación de la información guardada.

III.3. *TIPOS DE ATAQUES MAS FRECUENTES*

Un ataque es una amenaza puesta en marcha, en donde el individuo que realiza el ataque intenta tomar el control, dañar o reconfigurar un sistema informático mediante el uso de otro sistema similar. Los ataques más comunes son:

- **Ataques de exploración de puertos**

La exploración o escaneo de puertos es un método que permite a los administradores o hackers evaluar vulnerabilidades para auditar las máquinas y la red. Existe un gran número de aplicaciones que evalúan la seguridad de un computador en una red, por medio del análisis de sus puertos, llegando a detectando los puertos que se encuentran abiertos o cerrados, los servicios que ofrecen y determinar si cuenta con un firewall (cortafuegos) el pc de la víctima con el fin de tomar control remoto del mismo.

- **Ataque de denegación de servicio (DoS)**

Este tipo de ataque tiene por objetivo lograr bloquear el acceso a un determinado recurso de un servidor. Por lo general este tipo de ataque es efectuado mediante el uso de software o herramientas que inyectan un gran número de paquetes de forma continua con el objetivo de saturar los recursos del servidor dejándolo obsoleto e inaccesible, muchas veces los atacantes coordinan el ataque con un gran número de personas sincronizadas que generan el ataque al mismo tiempo.

- **Ataque lógico o software**

Consiste en enviar al equipo remoto una serie de datagramas mal construidos para aprovechar algún error conocido en dicho sistema. El ataque lógico más común es el denominado Ping de la muerte.

- **Ataque de inundación (flood)**

Este ataque tiene como finalidad bombardear un sistema mediante un flujo repetido de tráfico el cual busca acabar con todos los recursos y el ancho de banda de la red del sistema atacado. Entre los tipos de ataques de inundación más comunes tenemos: TCP SYN, Smurf IP, UDP Flood e ICMP Flood.

- **Ataque de fuerza bruta**

Es una técnica que tuvo sus orígenes en la criptografía, en especial del criptoanálisis (el arte de romper códigos cifrados o descifrar textos). Es una forma de encontrar la solución de problemas empleando un algoritmo de programación simple, el cual tiene como función generar e ir probando las diferentes posibilidades hasta lograr dar con el resultado esperado o el que mejor convenga.

IV. GENERADORES DE TRÁFICO DE RED

IV.1. *DEFINICIÓN DE GENERADOR DE TRÁFICO*

Son herramientas de software empleadas para emular las propiedades del tráfico real que se transporta en una red, producir tráfico necesario para realizar pruebas y evaluar el estado de la misma, de acuerdo a los requerimientos que sean expuestos es el diseño de dicha red.

Muchos de los cuales son diseñados por empresas o por investigadores que buscan tener herramientas que les ayude en el diagnóstico del desempeño en una red, aunque unos son creados para generar un tipo de tráfico en especial, y otros generan gran variedad de tipos de tráfico.

En los diferentes casos de estudio se emplean distintos generadores de tráfico, ya que depende de los requerimientos de la red, todo esto con la finalidad de evaluar la calidad de servicio, y lo más importante mejorar el rendimiento y el diseño.

IV.2. *TIPOS DE TRÁFICO DE RED*

TRÁFICO SINTÉTICO

Es un tráfico uniforme relacionado a la matriz transpuesta, está desarrollado para simular el desempeño de aplicaciones de cálculo científico. Existen tres distribuciones las cuales se utilizan generalmente para generar el tráfico en la red de interconexión, la distribución temporal, establece el tiempo de relación entre paquetes; la distribución espacial, fija los nodos de destino de los paquetes; la distribución del tamaño, establece el tamaño de los paquetes que se generan. Por lo general se utilizan parámetros básicos al generar tráfico, pero estos van de acuerdo al tipo y los aspectos de la red a evaluar.

TRÁFICO BASADO EN TRAZAS

Este tráfico generar trazas más reales a medida del soporte de aplicaciones de la red, de esta forma puede alcanzar resultados más exactos, es necesario realizar un estudio previo especificando los campos que debemos tener en cuenta en la generación del tráfico como pueden ser el tipo de evento, nodo en que inicio, nodo que lo genero, dimensión del evento, al momento de utilizar este tráfico se debe tomar en cuenta las capturas de tráfico obtenidas por un sniffer en una red Ethernet.

TRÁFICO PRODUCIDO POR EJECUCIÓN DE APLICACIONES PARALELAS

Este tipo de tráfico se lleva a cabo iniciando la simulación en la red de interconexión de los nodos, hay que tener claro que la aplicación de este tráfico genera un retraso en el sistema, por consecuencia de que todos los nodos se encuentran dentro de la simulación de forma paralela, para realizar una prueba de funcionamiento de interconexión se puede utilizar el simulador que más convenga dependiendo los requerimientos de la red.

IV.3. *HERRAMIENTAS DE GENERACIÓN DE TRÁFICO MALICIOSO Y ATAQUES*

NMAP

Nmap ("Network Mapper") es una utilidad de licencia libre empleada para el escaneo y detección de redes, la auditoría de seguridad, inventario de red, administración de horarios de actualización de servicio y supervisión del tiempo de actividad del servidor o del servicio, utiliza paquetes IP sin procesar de formas novedosas para determinar qué hosts están disponibles en la red, qué servicios ofrecen, qué sistemas operativos ejecutan, qué tipo de filtros y firewalls de paquetes están en uso, y decenas de otras características.

Fue creado para realizar un escaneo muy rápido de grandes redes, funciona bien contra hosts individuales, es compatible con la mayoría de sistemas operativos de computadoras, sus paquetes binarios oficiales están disponibles para Linux, Windows y Mac OS X. Además del clásico ejecutable Nmap de la línea de comandos, el paquete incluye una interfaz gráfica avanzada y visualizador de resultados (Zenmap) Una herramienta de transferencia, redirección y depuración de datos flexible (Ncat), una utilidad para comparar resultados de análisis (Ndiff) y una herramienta de generación de paquetes y análisis de respuestas (Nping) [7].

CAIN Y ABEL

Caín & Abel es una herramienta empleada para la recuperación de contraseña de los sistemas operativos de Microsoft. Posee la característica de proporcionar una recuperación fácil de los diversos tipos de contraseñas por inhalación de la red, craqueo contraseñas encriptados que utilizan ataques de diccionario, fuerza bruta y Criptoanálisis, grabación de conversaciones VoIP, decodificación revueltos contraseñas, recuperación de claves de red inalámbrica, revelando cuadros de contraseña, el descubrimiento de contraseñas en caché y el análisis de enrutamiento protocolos. El programa no

explota ninguna vulnerabilidad de software o errores que no pudieron ser corregidos con poco esfuerzo. Cubre algunos aspectos de seguridad/debilidad presente en las normas de protocolo, métodos de autenticación y mecanismos de almacenamiento en caché, y su principal objetivo es la recuperación simplificada de contraseñas y credenciales de varias fuentes, sin embargo, también algunos buques "no estándar" utilidades para los usuarios de Microsoft Windows. [8]

NET TOOLS 5

Net Tools es una utilidad que agrupa una amplia gama de herramientas generadoras de tráfico IP que son útiles tanto para administradores de red como para usuarios regulares. Posee una interfaz gráfica muy amigable, contiene un menú que agrupa todas las utilidades disponibles, que pueden ser modificadas a nuestra conveniencia, posee además múltiples funciones de gestión de archivos que se clasifican en cinco categorías principales: Menú Herramientas de Internet, Menú de Herramientas de Archivo, Menú de Herramientas Misceláneas, Menú Exterior y Otros.

Entre las utilidades más importantes de generación de tráfico está la de inyección de paquetes en una red para conseguir medir el ancho de banda total que puede soportar, escanear IP, calcular IP, obtener IP local, acceder a un buzón de mensajería y otros.

LOOK@LAN

Look@LAN Network Monitor, es una herramienta de acceso libre (Open Source) que realiza monitoreo de red mediante él envió y la recepción de paquetes hacia los puertos que están disponibles (que están abiertos) dentro de la red, se encuentra disponible para dispositivos con sistema operativo Windows 95 o posterior, y sólo está disponible en inglés. La versión actual es la 2.50, y su última actualización se llevó a cabo el 22 de junio del 2011.

MEDUSA

Medusa es una herramienta que permite crackear mediante ataques de fuerza bruta con la ayuda de diccionarios de posibles combinaciones de palabras y símbolos de una manera muy rápida distintos tipos de servicios entre los más vulnerables están los protocolos: Http, Ftp, Imap, Mysql, Pop3, Telnet, entre otros. Está basada en hilos para aplicar testeo concurrente de varios hosts, usuarios o passwords. Está representada por un diseño modular, ya que cada servicio se manifiesta como un módulo independiente en archivos .mod, actualmente se encuentra disponible en la distribución Linux.

HPING3

Hping3 es una herramienta que se utiliza desde la consola o terminal en Linux, cuyo fin es el análisis y ensamblado de paquetes TCP/IP. Similar al comando Ping, esta herramienta además de enviar paquetes ICMP, también puede enviar paquetes TCP, UDP y RAW-IP de una forma muy rápida. Normalmente esta aplicación puede ser muy útil a la hora de realizar testeos de seguridad sobre *firewalls*, escaneo

avanzado de puertos o seguimiento de rutas, distintos tipos de pruebas sobre varios protocolos y también podríamos verificar la capacidad de generar una denegación de servicio (DoS) mediante un *flood* de paquetes modificados. Hping3 es mayormente utilizada en plataformas Linux y Unix, pero se puede descargar también para plataformas Windows en su versión anterior [9].

PERL

Perl es una herramienta de acceso libre (Open Source) la cual tiene la capacidad de manejar conexiones abiertas mediante el envío de peticiones HTTP parciales. Logrando atar a los servidores Web, enviando cabeceras subsecuentes a intervalos regulares con el fin de mantener los sockets.

Perl debe esperar a que todos los sockets estén disponibles antes de que sean satisfactoriamente consumidos, de esta manera si se trata de un sitio web que posee alto tráfico, le puede tomar un tiempo hasta conseguir que el sitio libere sockets, por otro lado, si otros usuarios reinician sus conexiones en un corto tiempo, serán capaces de ver el sitio. Es parecido a una condición de carrera, a diferencia que en esta Perl eventualmente siempre será el ganador, más pronto que tarde.

V. SIMULACIÓN DE UNA RED IP VIRTUALIZADA

V.1. *INTRODUCCIÓN A LA VIRTUALIZACIÓN*

El término virtualización en un contexto informático que suele utilizarse para referirse a la creación mediante software de una versión virtual de algún recurso tecnológico, como puede ser una plataforma de hardware, un sistema operativo, un dispositivo de almacenamiento u otros recursos de red. El software de virtualización implementa lo que se llama un Hipervisor o VMM (Virtual Machine Monitor) que consiste en una capa de abstracción entre el hardware de la máquina física (host, anfitrión) y la máquina virtual (MV) formada por hardware y software virtualizado, haciendo el papel de centralita entre lo real y lo virtualizado [10].

V.2. *TIPOS DE VIRTUALIZACIÓN*

Existen tres tipos de virtualización que cumplen con funciones específicas:

Virtualización completa. Este tipo de virtualización se caracteriza por la interacción binaria entre el hipervisor y la CPU en el servidor físico, obteniendo como resultado un control total a cada servidor virtual, con la característica de que en una misma maquina pueda haber dos o más servidores virtuales con distinto S.O.

Virtualización homogénea. Este tipo de virtualización descarta la utilización de un hipervisor ya que crea entornos virtuales de esta manera dicho tipo de virtualización se convierte en la más eficaz por su eficiencia al interactuar con servidores que poseen el mismo S.O.

Paravirtualización: Esta virtualización se sitúa en un punto neutral entre los dos tipos anteriores, ya que tiene la capacidad de interactuar por medio de servidores “guests” con sistemas operativos invitados

dentro de otro sistema al que llamamos hipervisor. Facilitando que dichos guests funcionen con sistemas operativos diferentes.

V.3. *HERRAMIENTA DE VIRTUALIZACIÓN VIRTUALBOX*

Es una potente herramienta de virtualización open source (de código abierto) de gran utilidad que nos permite virtualizar un sistema operativo, es decir, crear un ordenador virtual en el que podremos instalar cualquier otro sistema [11].

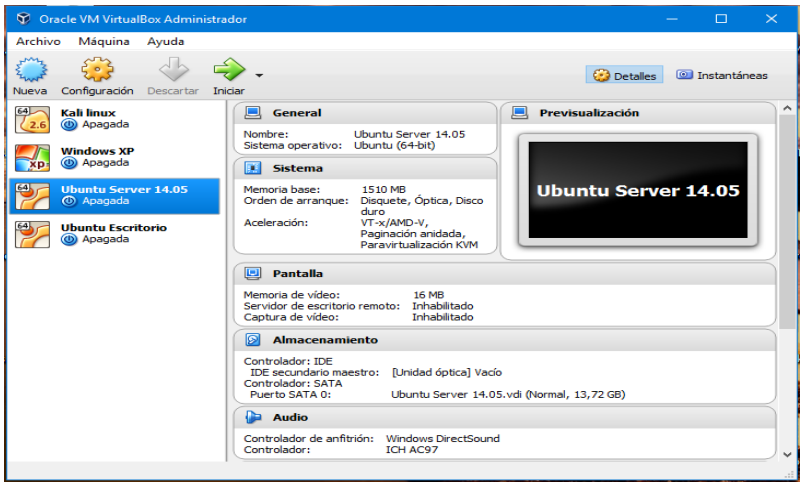

Fig.1. Interfaz gráfica herramienta VirtualBox

V.4. *PLATAFORMA DE PRUEBAS*

Para la investigación se diseñó una plataforma de pruebas para poder experimentar los distintos ciberataques más comunes que se han venido efectuado en los últimos años, sobre redes de empresas o instituciones, En la figura 2 se detalla el diagrama de red propuesto para la realización de las pruebas de los ataques, cabe destacar que la presente investigación se la realizo en un ambiente virtual con fines académicos, sin violar la privacidad de ningún equipo físico real.

Para montar la plataforma se utilizó un equipo que cuenta con las siguientes especificaciones:

- Marca: Lenovo ideapad 310-15IKB
- Procesador: Intel Core i7
- Sistemas Operativo: Windows 10
- Tarjeta Gráfica: NVIDIA GeForce 920MX
- Memoria RAM: 12GB
- Adaptador de red inalámbrica: broadcom bcm 43xx wlan

La virtualización de la plataforma se llevó a cabo con la herramienta Open-Source VirtualBox 5.1, la cual permite la instalación de máquinas virtuales con distintos sistemas operativos entre los cuales tenemos: Linux, Windows, Mac Os, independientemente de la arquitectura de 32 o 64 bits.

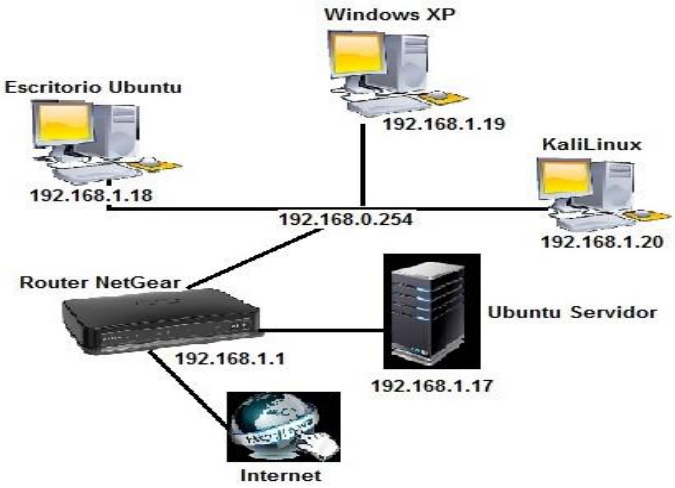

Fig.2. Topologia de la Red de pruebas.

EQUIPOS VIRTUALIZADOS

Se procedió a la instalación de la máquina virtual Virtualbox 5.1 en el equipo anfitrión de una manera típica de instalación como cualquier software de Windows, para posteriormente instalar los equipos implicados en la investigación los cuales cuentan con características y funcionalidades dedicadas al desarrollo de servicios de red en pequeñas y medianas empresas, en la Tabla 1 se describe con más detalle.

Máquina Virtual	Sistema Operativo	Hardware	Software
Router NetGear	Genie V1.05.05	Versión de hardware: 2.00 Dirección MAC: 4C:60:DE:97:43:5B	Versión de firmware: V1.05.05
Servidor Ubuntu	Ubuntu V14.04.5 LTS (Trusty Tahr)	Procesador: Intel Core i7 Memoria RAM: 12GB, Disco duro 20GB Adaptador de red: Broadcom	Servidor de correo Squirrelmail, Postfix, Servidor Web Apache, Servidor de Base de Datos MySQL, Joomla.
Cliente 1: Windows XP	Service Pack 3 (x86)	Procesador: Intel Core i7 Memoria RAM: 12GB, Disco duro 20GB Adaptador de red: Broadcom	Navegador Web Mozilla Firefox
Cliente 2: Escritorio Ubuntu	Ubuntu Desktop V14.04.5	Procesador: Intel Core i7 Memoria RAM: 12GB, Disco duro 20GB Adaptador de red: Broadcom	Navegador Web Mozilla Firefox
Cliente 3: KaliLinux	Linux V1.1.0	Procesador: Intel Core i7 Memoria RAM: 12GB, Disco duro 20GB Adaptador de red: Broadcom	Navegador Web Mozilla Firefox

Tabla 1: Especificaciones de los equipos virtuales.

CREACIÓN DE LA RED DEL ENTORNO DE PRUEBAS

La red está conformada por equipos que cumplen con funcionalidades especificadas de la siguiente manera:

- El equipo servidor, abarca servicios de: Base de datos principal, Correo institucional, y Web interna de la empresa.
- El equipo router, posee la función de establecer un enrutamiento direccional entre los clientes y el servidor de la red.
- Los equipos clientes, su función principal es inyectar tráfico de red realizando peticiones (base de datos, correo y web) hacia el servidor, simulando clientes reales.

Para la creación de la red se realizó una tabla IP, que posee parámetros de direccionamiento los cuales se detallan en la Tabla 2.

Máquina Virtual	Dirección IP	Máscara de Subred	Puerta de Enlace
Router NetGear	eth0 192.168.0.254 eth1 192.168.1.1	255.255.255.0	
Servidor Ubuntu	192.168.1.17	255.255.255.0	192.168.1.1
Cliente 1: Windows XP	192.168.1.18	255.255.255.0	192.168.0.254
Cliente 2: Escritorio Ubuntu	192.168.1.19	255.255.255.0	192.168.0.254
Cliente 3: KaliLinux	192.168.1.20	255.255.255.0	192.168.0.254

Tabla 2: Asignación IP.

V.5. *IMPLEMENTACIÓN Y CONFIIGURACIÓN DE LOS SERVIDORES*

La instalación de los servidores se las realizo de la siguiente manera:

- **Instalación y prueba de funcionamiento del servidor de correo Postfix.**

Postfix es un servidor de correo de software libre y de código abierto, es una herramienta informática desarrollada para el enrutamiento y envío de correos electrónicos, creada con la intensión de convertirla en una herramienta muy rápida, eficaz y segura utilizado Sendmail. anteriormente era conocido como VMailer e IBM Secure Mailer, fue originalmente escrito por Wietse V. Durante su estancia en el Thomas J. Watson Research Center de IBM, y continúa siendo desarrollado activamente, fué construido a partir de código fuente, Postfix puede ejecutarse en sistemas tipo UNIX, incluyendo AIX, BSD, HP-UX, Linux, MacOS X, Solaris [12].

Como primer punto de la instalación de Postfix, se procedió abrir el terminal del Servidor Ubuntu y se ingresó como administrador con los siguientes comandos:

```
luisuvidia@luis: ~ sudo su
root@luis: /home/luisuvidia# apt-get install postfix
```

Durante la instalación, nos aparece una ventana que dice Postfix configuration es ahí donde le ponemos el dominio de nuestro correo y le ponemos aceptar, como se muestra en la figura 3.

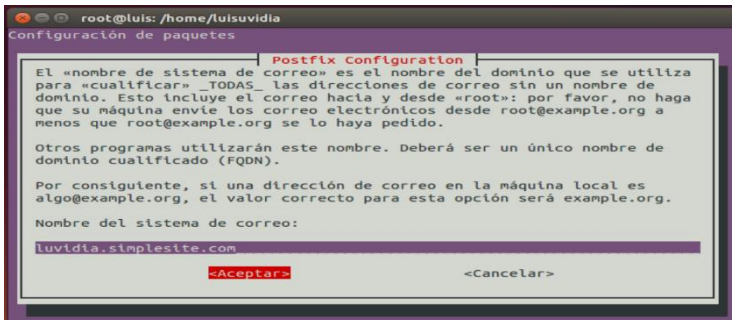

Fig.3. Configuración Postfix.

Posterior mente se utiliza el comando vim para editar las configuraciones de Postfix, donde podemos modificar la carpeta de destinación de los correos, de la siguiente manera.

root@luis: /home/luisuvidia# vim /etc/Postfix/main.cf

Se abre un archivo de texto, dentro del cual se modificaron las siguientes líneas de comandos:

inet_protocols = ipv4
home_mailbox = Maildir/

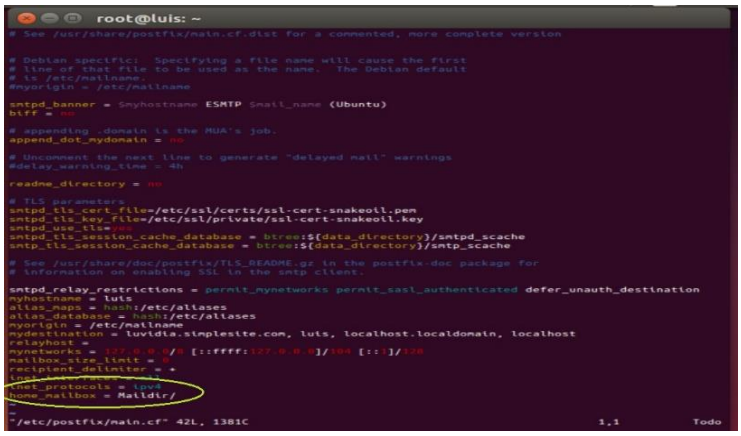

Fig.4. configuración del destino de correos.

Para salir le damos a la tecla ESC y escribimos **:qw** para que se guarden los cambios.

Luego procedemos a la instalación del Courier-pop para habilitar servicios de lectura y recepción de mails ingresando el siguiente comando:

root@luis: /home/luisuvidia# apt-get install courier-pop
root@luis: /home/luisuvidia# apt-get install courier-imap

Posteriormente procedemos a instalar Squirrelmail que es una aplicación web mail escrita en PHP, trabaja con plugins lo cual hace que sea más fácil agregar nuevas características al entorno de la aplicación, para su instalación se utilizaron los siguientes comandos.

root@luis: /home/luisuvidia# apt-get install squirrelmail
root@luis: /home/luisuvidia# squirrelmail-configure

Luego se procede a realizar una serie de configuraciones como muestra la figura 5, en donde tenemos que tener en cuenta nuestro dominio el cual es luvidia.simplesite.com.

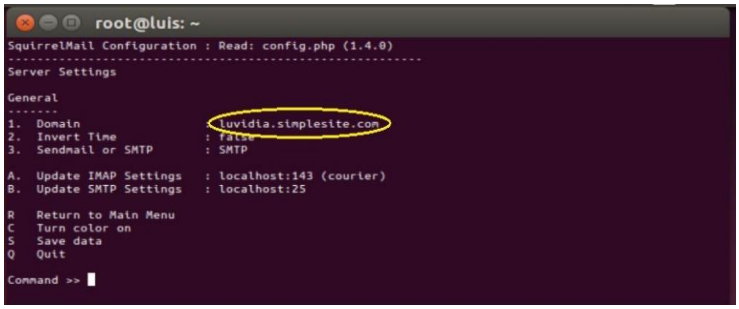

Fig.5. Asignación del dominio.

Ahora hacemos referencia la carpeta de squierremail con la WWW la cual es la carpeta del servidor apache que anteriormente inslalamos para realizar dicha referencia ejecutamos los siguientes comandos:

root@luis: /home/luisuvidia# cd /var/www
root@luis: /var/www# ln –s /usr/share/squirrelmail webmail

Verificamos ya que tenemos la carpeta creada “Webmail” en WWW, para probar el acceso abrimos el navegador y accedemos a **http://localhost/webmail,** como muestra la figura 6.

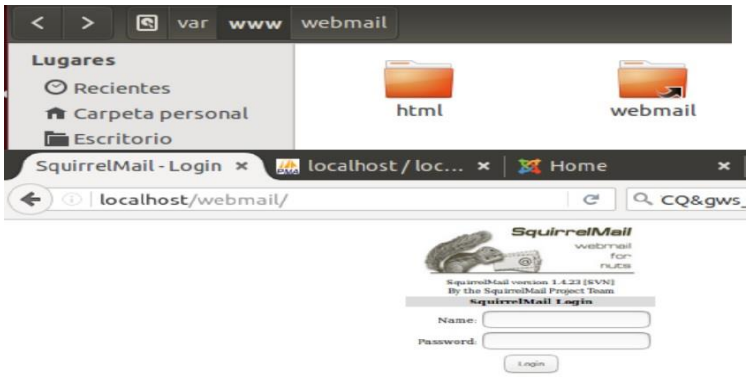

Fig.6. Verificación de funcionamiento Squirrelmail.

Una vez instalado el servidor procedimos a la creacion de usuarios, con los siguientes comandos:

root@luis: /etc/apache2/sites-available# adduser usuario1
root@luis: /etc/apache2/sites-available# adduser usuario2

Como podemos apreciar en la figura 7.

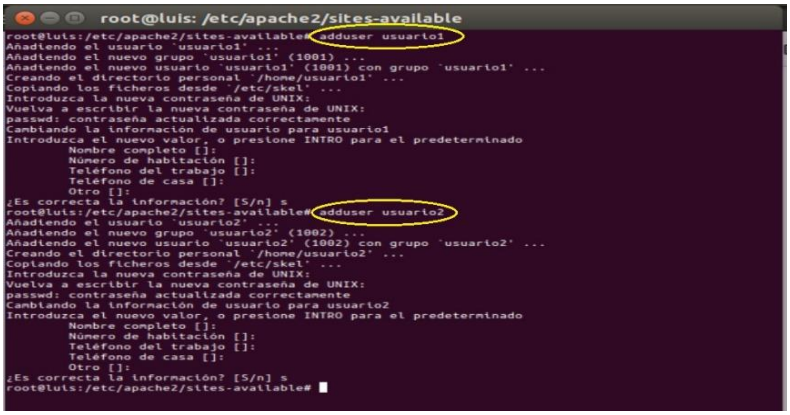

Fig.7. Creación de Usuarios.

Mandamos un correo de prueba como se observa en la figura 8.

Fig.8. Prueba de envío de correo.

Por último, se pudo comprobar el correo enviado desde el servidor hacia el cliente, como se observa en la figura 9.

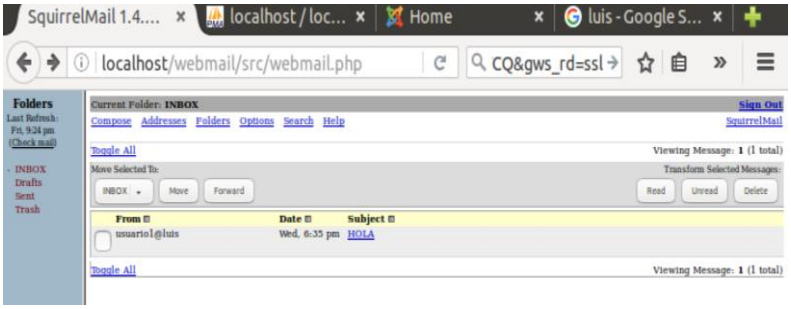

Fig.9. Comprobación correo recibido.

- **Instalación y prueba de funcionamiento del servidor Web y base de datos**

Como primer paso procedimos a instalar un servidor web HTTP de código abierto para la creación de páginas y servicios web llamado apache2, el cual posee entre sus características principales un servidor multiplataforma, open source, muy potente y que destaca por su seguridad y rendimiento. Se encuentra alojado en un ordenador a la espera de que algún navegador le realice una petición, como, por ejemplo, acceder a una página web, el mismo que responde enviando código HTML mediante transferencia de datos [13]. La instalación se realizó con el siguiente comando:

root@luis: /home/luisuvidia# apt-get install apache2

Una vez instalado comprobamos el correcto funcionamiento ingresando desde un navegador web a la siguiente URL: **http://192.168.1.10/** mostrándonos como resultado lo detallado en la figura 10.

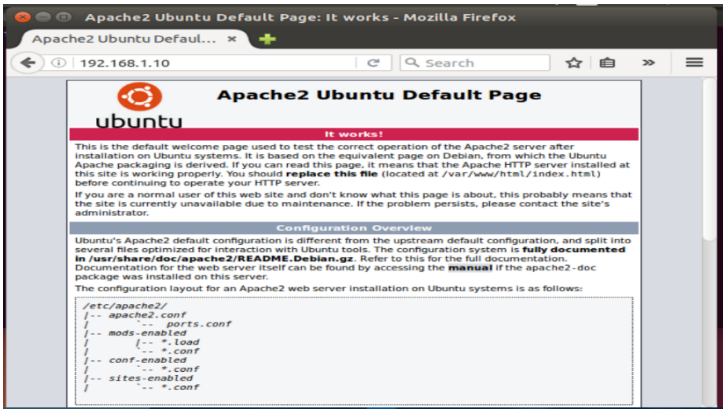

Fig.10. Prueba de funcionamiento de Apache.

Una vez probado el funcionamiento del servicio de Apache se procedió a instalar la base de datos mysql-server, con el siguiente comando:

root@luis: /home/luisuvidia# apt-get install mysql-server

A medida de que iba avanzando la instalación se solicito una contraseña de administrador a mysql-server con lo cual se asigno **1560luis**.

Para verificar el funcionaminto de mysql-server se escribe el código ***mysql –u root –p,*** como muestra la figura 11.

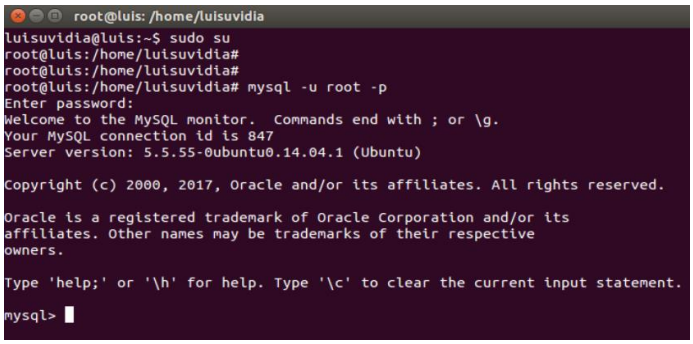

Fig.11. Prueba de funcionamiento de MySQL.

Posteriormente se instaló phpMyAdmin el cual es una herramienta muy completa que permite acceder a todas las funciones típicas de la base de datos MySQL a través de una interfaz web muy intuitiva, permite la creación y edición de tablas, ejecutar sentencias SQL y hacer un resguardo de información de la base de datos [14], mediante el siguiente comando:

root@luis: /home/luisuvidia# apt-get install php5 libapache2-mod-php5 php5-mcrypt
root@luis: /home/luisuvidia# apt-get install phpmyadmin

Una ves que se esta ejecutando la instalacion no aparece una ventana de configuracion de phpmyadmin en donde se asignó la contraseña **1560luis,** ahora enlazamos phpmyadmin al servidor Apache mediante el editor de texto NANO que ya viene instalado en UBUNTU mediante el siguiente comando:

```
root@luis: /home/luisuvidia# nano /etc/ apache2/apache2.conf
```

Nos situamos en la última línea de archivo de texto y añadimos las siguientes líneas de comandos que se muestran en la figura 12.

```
# Include list of ports to listen on
Include ports.conf
include /etc/phpmyadmin/apache.conf
```

Fig.12. configuración archivo de texto.

Una vez finalizado el proceso reiniciamos el servicio de apache con el comando:

```
root@luis: /home/luisuvidia# service apache2 restart
```

Finalmente comprobamos su correcto funcionamiento mediante un navegador web poniendo la URL: **http://localhost/phpmyadmin/** mostrándonos como resultado lo detallado en la figura 13.

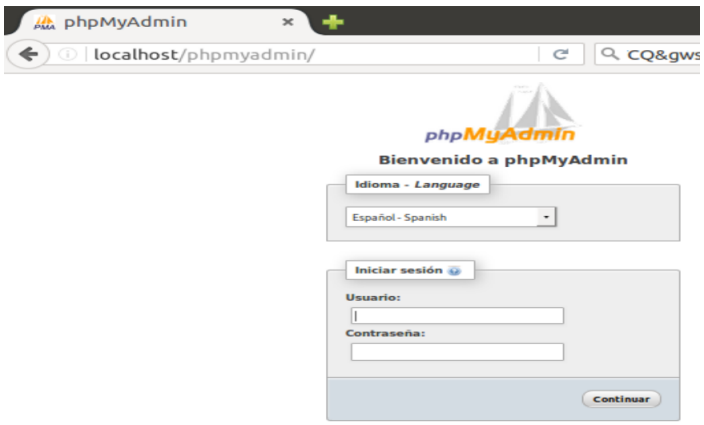

Fig.13. Prueba de funcionamiento phpmyadmin.

- **Instalación y prueba de funcionamiento de Joomla**

Joomla es una aplicación open source para la creación y edición de páginas web más famosa del mundo gracias a su flexibilidad y adaptabilidad, es la solución perfecta para sitios web de pequeñas y grandes empresas gracias al aporte de herramientas necesarias para construir sitios web [15], esta herramienta fue integrada en la configuración de Apache para poder tener acceso a la plataforma de Jommla se utilizaron los siguientes comandos:

```
root@luis: /home/luisuvidia# cp sites-available/default sites-available/joomla
```

Luego se generó permisos para el acceso web por parte de Joomla con los siguientes comandos:

```
root@luis: /home/luisuvidia# joomla a2ensite
root@luis: /home/luisuvidia# etc/init.d/apache2 restart
```

Paso siguiente se creó la base de datos y del usuario de Joomla para lo cual se ingresaron los siguientes comandos:

```
root@luis: /home/luisuvidia# mysql –u root -p
mysql> create database joomla;
mysql> create user ‘joomla ‘@’ localhost’ identidied by ‘1234’;
mysql> grant all privileges on joomla.* to ‘joomla’ identified by ‘1234’;
mysql> exit
```

Luego de esto se procedió a descargar el paquete de instalación de Joomla y se ejecutó mediante el navegador web, para realizar el proceso de instalación de una manera gráfica, en el proceso de instalación se solicitó información sobre la base de datos que se creó en mysql, como muestra la figura 14.

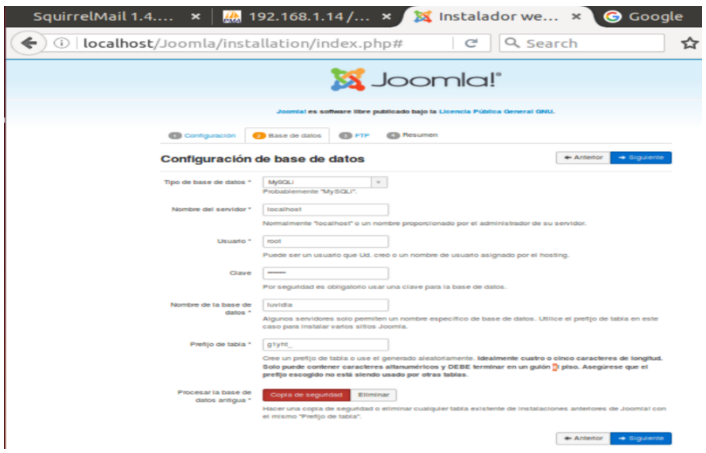

Fig.14. Proceso de instalción de Joomla con datos de mysql.

Finalmente se creó y edito la estructura y contenidos de la página web personalizada de acuerdo a nuestra conveniencia, en la figura 15 se muestra la página terminada.

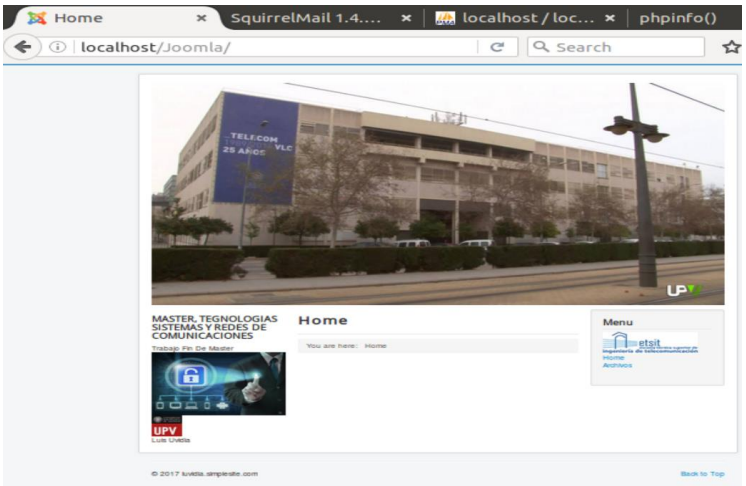

Fig.15. Página web creada mediante Joomla.

VI. SIMULACIÓN DE ATAQUES Y ANÁLISIS DE RESULTADOS

VI.1. *ATAQUE DE ESCANEO DE PUERTOS Y SERVICIOS*

- **Herramienta generadora de tráfico Nmap**

La herramienta Nmap se la instaló en un equipo cliente de la red que lleva como sistema operativo Windows Xp, como primer paso se descargó el archivo de instalación y se lo ejecutó, paso seguido aceptamos los parámetros de políticas de licencia, y seleccionamos los complementos de la herramienta y presionamos next, como se observa en la figura 16.

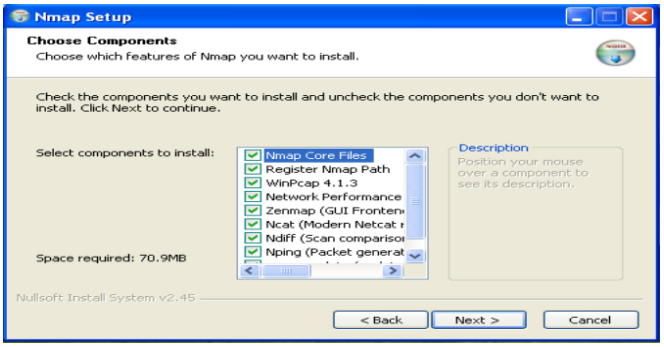

Fig.16. Instalación de complementos Nmap.

Una vez finalizada la instalación se procedió a ejecutar la herramienta, mediante el comando: nmap 192.168.1.17 se logró identificar los puertos disponibles con su respectivo servicio como se detalla en la figura 17.

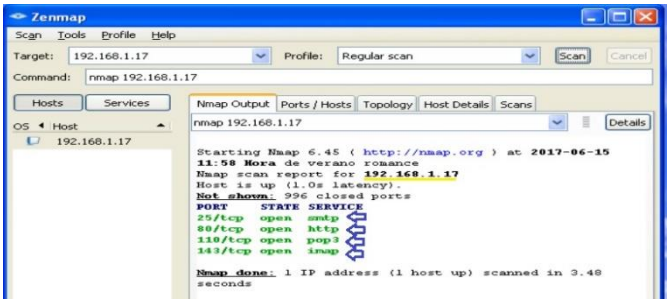

Fig.17. Listado de puertos abiertos.

ANÁLISIS DE RESULTADOS

En el servidor: **http://192.168.1.17,** se detectaron puertos abiertos que poseen servicios de correo electrónico en los protocolos:

- **Smtp:** (Simple Mail Transfer Protocol), protocolo empleado para el intercambio de mensajes de correo, proporciona su servicio de salida a través del puerto 25.
- **Http:** (Protocolo de transferencia de hipertextos), protocolo empleado para compartir información con la web, proporciona su servicio de salida a través del puerto 80.
- **Pop3:** (Protocolo de oficina de correo), protocolo empleado para recibir los mensajes de correo electrónico almacenados en un servidor, proporciona su servicio de salida a través del puerto 110.

- **Imap:** (Protocolo de acceso a mensajes de internet), protocolo empleado para acceder a mensajes almacenados en un servidor web, proporciona su servicio de salida a través del puerto 143.

Posteriormente se implementó un escaneo más profundo mediante el código: ***namap –p110 –T4-A –v 192.168.1.17*** que aplica los siguientes parámetros:

-p110: Genera el ataque al puerto (Pop3) por la ruta 110.

-T4: Toma control del temporizador controlando la sincronización.

-A: Permite generar una exploración minuciosa al equipo que está siendo atacado.

-v: Detalla la versión de Zemap o Nmap**.**

Los resultados obtenidos del análisis los detalla la figura 18, que se resumen en los siguientes:

- Distancia de la red: **2 saltos**
- Latencia del Host: **0.0012s**
- Capacidades de Pop3: **implementacion de courier mail server**.

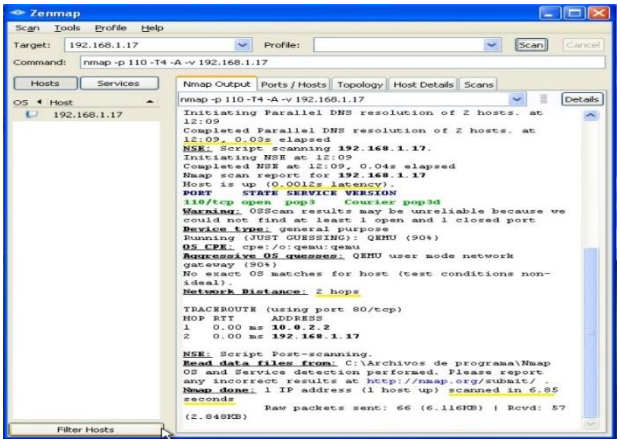

Fig.18. Escaneo más profundo.

Gracias a la implementación de la herramienta Wireshark en la maquina Servidor de Ubuntu, se logró monitorear los eventos generados aplicado un sondeo TCP/SYN, como podemos observar en la figura 19, se verifica el envío de paquetes de control **SYN** que permiten entablar una conexión real esperando que se cumpla con la petición de la conexión, confirmación de la conexión y recepción de la información, desde el atacante de la red (**192.168.1.17**); en primer lugar, se recibió una respuesta **RST** (reset) esto indica que no hay nadie escuchando en el puerto y se reiniciara la conexión debido a SYN duplicados, retardados o comprimidos entonces el puerto se marca como filtrado, a continuación se volvió a enviar un paquete **SYN,** esta vez se recibió una respuesta **ACK** indicando que el puerto está abierto y permitiendo una respuesta del protocolo **Pop3** con la información (**OK Hello There**).

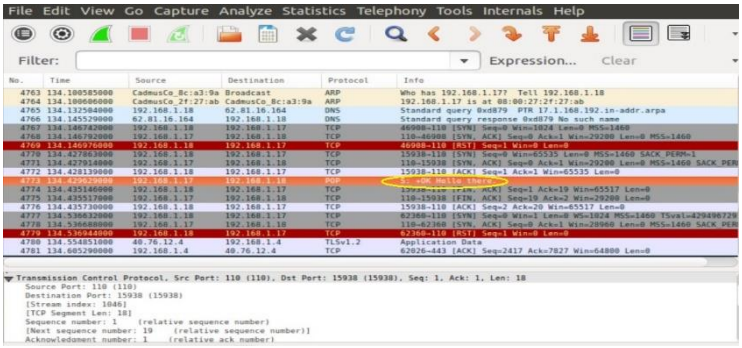

Fig.19. Monitoreo Wireshark.

- **Herramienta generadora de tráfico Look@Lan**

La herramienta Look@LAN 2.50 se la instaló en un equipo cliente de la red dotado con el sistema operativo Windows Xp, como primer paso se descargó el archivo de instalación y se lo ejecutó, paso seguido aceptamos los parámetros de políticas de licencia y presionamos next, como se observa en la figura 20.

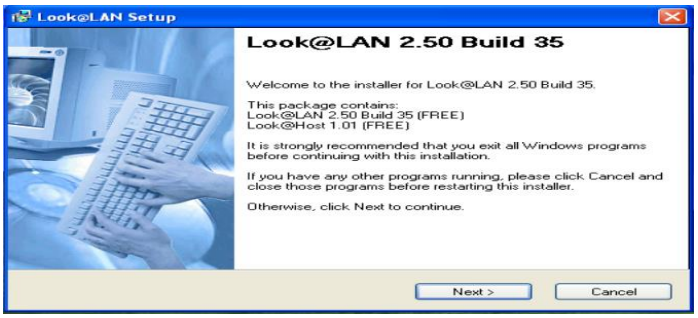

Fig.20. Proceso de instalación Look@LAN.

Una vez instalada la herramienta la ejecutamos y seleccionamos crear nuevo perfil y es ahí donde editamos el rango de direcciones IP, para la busqueda de equipos hablilitados dentro de la red, precionamos siguiente y arranca el escaneo de redes una vez termindado dicho escaneo arroja un reporte de red en el cual seleccionamos nuestra direccion Ip: 192.168.1.17 y se obtuvo los resultados mostrados en la figura 21.

- Sistema operativo: Ubuntu
- Puertos detectados.
- Información adicional: Servidor Apache 2.4.7 (Ubuntu).

Fig.21. Resultados generados por Look@LAN.

Resultados obtenidos mediante Wireshark

Se logró monitorear los eventos suscitados, como podemos observar en la figura 22, se verifica el envío de paquetes de control **SYN**, por parte del equipo atacante, esta vez se recibió una respuesta **ACK** indicando que el puerto está abierto y permitiendo el análisis del protocolo Http mostrando información sobre la página de inicio del webmail alojado en apache2.

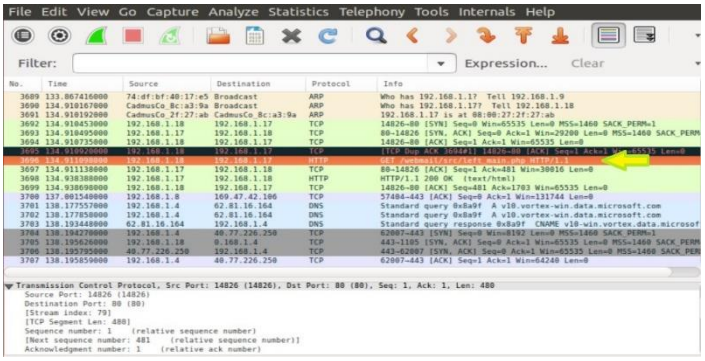

Fig.22. Monitoreo Wireshark.

VI.2. *ATAQUE DE HOMBRE EN EL MEDIO*

- **Herramienta generadora de tráfico Cain&Abel**

La herramienta Cain&Abel V 4.9.56, se la instaló en un equipo cliente de la red con sistema operativo Windows Xp, como primer paso se descargó el archivo de instalación y se lo ejecutó, paso seguido aceptamos los parámetros de políticas de licencia y presionamos next, como se observa en la figura 23.

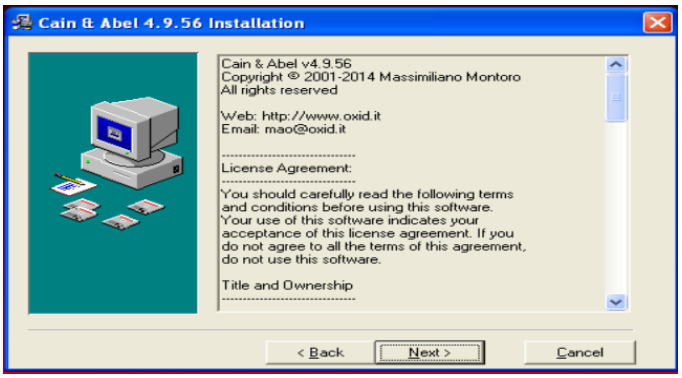

Fig.23. Instalación herramienta Cain&Abel.

Una vez finalizada la instalación fue necesaria instalar **WinpCap**, que permite la captura de paquetes. Paso siguiente se ejecutó la herramienta Cain&Abel una vez ejecutada presionamos en el icono de interface para verificar que interface tenemos en nuestro caso usamos la tarjeta de red inalámbrica, luego pinchamos en la pestaña **Sniffer**, dentro de la pestaña pinchamos en el signo + y seleccionamos un test total de la red, una vez escaneada nos aparecerán todos los dispositivos conectados a nuestra red, paso seguido en las pestañas de abaja le damos clic en **ARP,** en la primera zona de la pantalla le damos clic en el signo + y seleccionamos la IP del router y le damos en **OK,** empezara a capturar paquetes, luego

nos dirigimos al navegador y entramos en una página de prueba en este caso la página del servidor de correo:

http://192.168.1.17/Webmail/src/login.php

Aquí ponemos nuestro usuario y contraseña y entramos, ahora vamos a la herramienta y pinchamos en la pestaña inferior **Passwords** estando ahí seleccionamos **HTTP,** y vemos que se ha generado el nombre de usuario la contraseña y la web, como podemos observar en la figura 24.

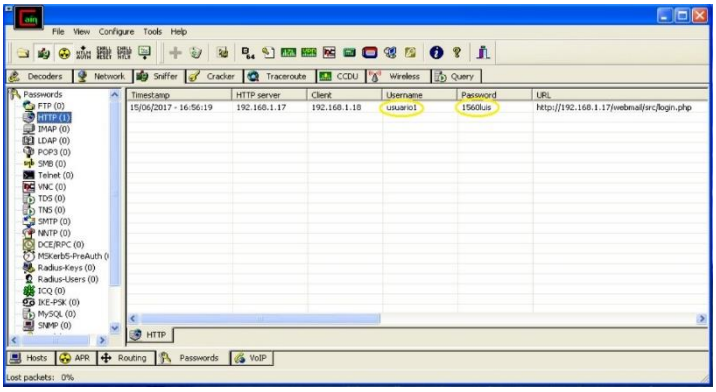

Fig.24. Herramienta Cain&Abel.

Resultados obtenidos

La herramienta nos permitió almacenar el nombre de usuario, la contraseña y la dirección web generadas desde un cliente, evidenciando un ataque **ARP** el cual consiste en vincular la dirección MAC del atacante con la dirección IP del servidor, logrando recibir datos que están en tránsito, que se acceden mediante la dirección IP teniendo como destino el servidor.

Utilizando Wirwshark se logró monitorear los eventos suscitados en el servidor, como podemos observar en la figura 25, se verifica el envío de paquetes de control **SYN**, por parte del equipo atacante, obteniendo como respuesta un paquete **ACK** además se capturó información sobre la página del servicio de Webmail.

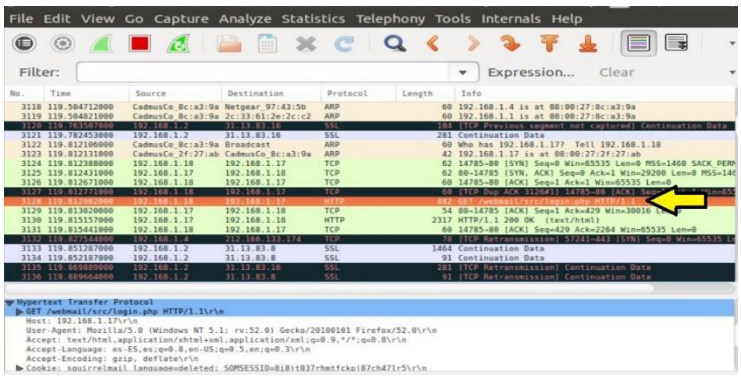

Fig.25. Monitoreo de eventos hacia el servicio Webmail.

VI.3. *ATAQUE DE FUERZA BRUTA*

- **Herramienta generadora de tráfico Medusa**

La instalación de la herramienta medusa se la realizo en el equipo cliente Ubuntu escritorio con sistema operativo Linux, mediante los comandos que se visualizan en la figura 26.

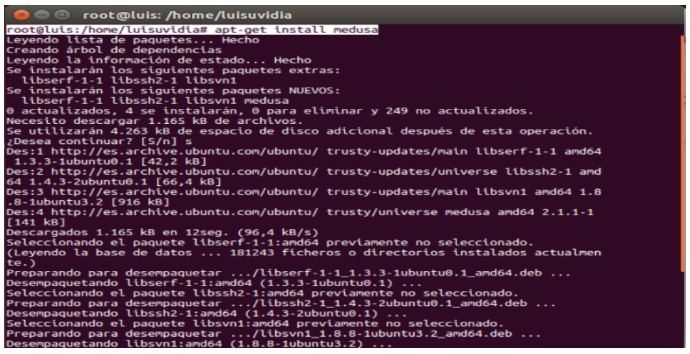

Fig.26. Instalación de la herramienta Medusa.

Añadimos el paquete APG que permite generar diccionarios de combinaciones de número símbolos y letras, mediante el comando:

root@luis: /home/luisuvidia# apt-get install apg

Paso seguido ejecutamos el paquete APG para generar el diccionario que permite realizar el ataque de fuerza bruta con el siguiente comando:

root@luis: /home/luisuvidia# apg –m 3 –x 4 –n 9999 >> password.txt

En donde **–m** detalla el número mínimo de caracteres que se aplican a las contraseñas generadas, **-x** número máximo de caracteres que se aplican a las contraseñas generadas, **-n** indica la cantidad de contraseñas que se van a generar y **password.txt** representa el nombre del archivo el cual va a contener las contraseñas.

Ejecutamos la herramienta sobre el servidor **192.168.1.17**, esta a su vez mediante el protocolo **POP3** trata de identificar al **usuario1** mediante los comandos **–h**, que determina el host, **-u**, representa al usuario al que procede el ataque, **-P**, indica la ubicación del diccionario de contraseñas y **–F**, permite detener el ataque una vez encontrada la contraseña correcta. Logrando como resultado la obtención del nombre de usuario y la contraseña. como lo detalla la figura 27.

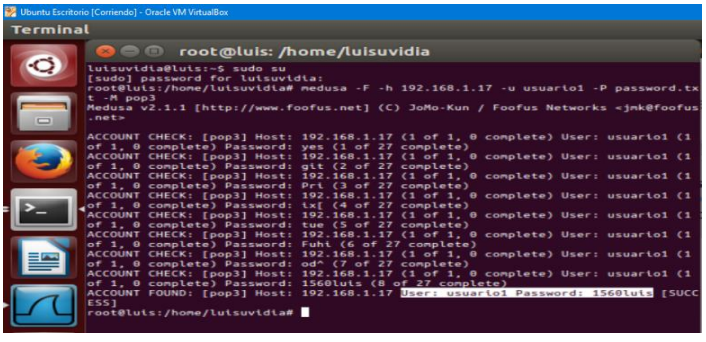

Fig.27. Ejecución del ataque.

Resultados obtenidos

Se realizó un monitoreo aplicado al servidor 192.168.1.17 con la herramienta Wireshark en la cual se puede evidenciar los intentos por parte del equipo atacante tratando de probar contraseñas aleatoriamente, hasta lograr descifrar la contraseña correcta que en nuestro caso es **1560luis,** logrando que el protocolo pop3 permita el acceso mediante la información **C: PASS 1560luis** y **S: + OK logget in.** Como podemos ver en la figura 28.

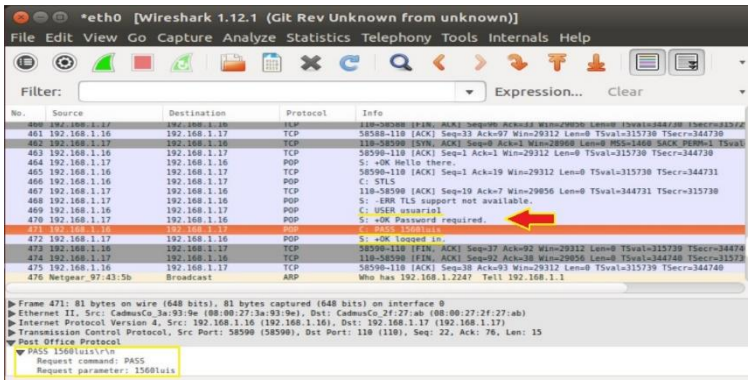

Fig.28. Descubrimiento de usuario y contraseña.

VI.4. *ATAQUE DE DENEGACIÓN DE SERVICIOS DoS*

Los ataques de DoS se realizaron, con el objetivo de saturar el servidor Web mediante las siguientes herramientas:

- **Herramienta generadora de tráfico Hping3**

Se procedió con la instalación de la herramienta Hping3 en el equipo cliente Ubuntu escritorio, mediante la siguiente línea de comandos:

root@luis: /home/luisuvidia# apt-get install hping3

Una vez instalada la herramienta se ejecutó los siguientes comandos, -p, indica el puerto al que se va a inyectar tráfico, -S, inicializa la bandera de paquetes SYN, --flood controla la velocidad de inyección de los paquetes ordenando a hping3 que inyecte con la máxima velocidad al servidor 192.168.1.17, -d, determina la extensión del paquete en bytes, esto lo podemos apreciar más detallado en la figura 29.

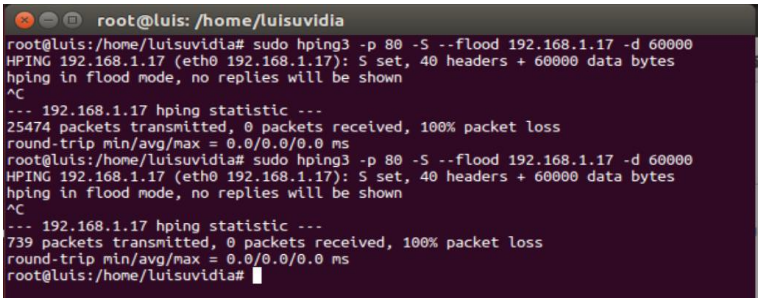

Fig.29. Eejecución del ataque mediante hping3.

Resultados obtenidos

Se monitoreo el servidor IP: 192.168.1.17 con la herramienta Wireshark en la cual se puede evidenciar la gran cantidad de paquetes enviados por parte del equipo atacante que lleva la IP: 192.168.1.16 hacia el servidor se puede observar que al momento de detener el ataque se han enviado 35520 paquetes mediante el puerto 80 de salida a la web, en la figura 30 se observa con más detalles.

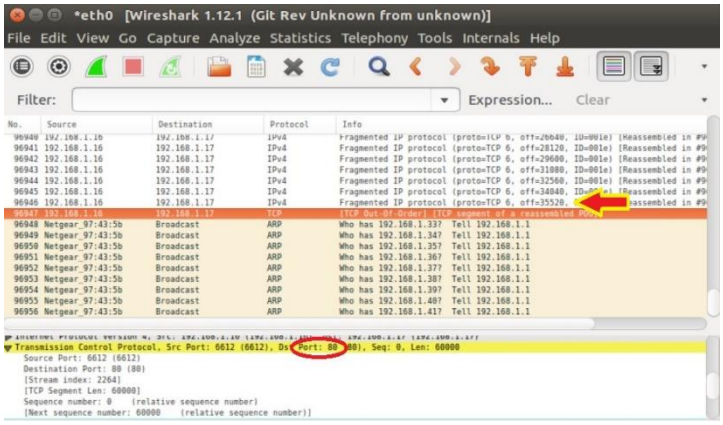

Fig.30. Resultados del ataque.

- **Herramienta generadora de tráfico Perl**

Se procedió con la instalación de la herramienta Perl en el equipo cliente Ubuntu escritorio, mediante la siguiente línea de comandos:

root@luis: /home/luisuvidia# apt-get install perl buil-essential curl

Una vez instalada la herramienta se procedió a descargar un script que controla la saturación del servicio Web mediante el puerto 80 dicho script está escrito en lenguaje de programación C++. Posteriormente se ejecutó los siguientes comandos, **Ddos.pl,** el cual posee el script para ejecutar el ataque, **-dns,** establece la dirección IP del servidor que va a ser atacado y **–port,** determina el puerto al cual se pretende colapsar con tráfico, esto lo podemos ver más detallado en la figura 31.

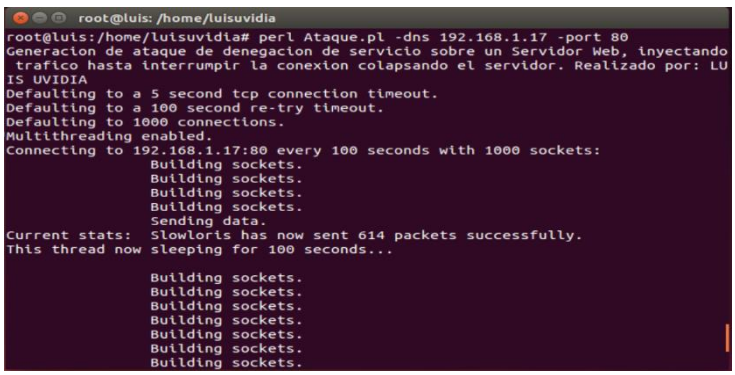

Fig.31. Proceso de ataque DoS.

VI.5. *ATAQUE A LA WEB (PHISHING)*

El ataque phishing es cuando alguien clona una página y la utiliza para recabar datos se procede a demostrar dicho ataque con la utilización del sistema operativo Kalilinux implementado en la máquina de uno de los clientes de nuestra red el cual posee distintas herramientas para generación de ataques una de las cuales es:

- **Herramienta SetTokit**

Es una herramienta de ingeniería social hecha específicamente para ataques de phishing, como primer paso se procedió a ingresar a la máquina virtual KaliLinux y posteriormente a la pestaña aplicaciones luego a herramientas de explotación y luego hacemos clic sobre SE, en la figura 32 podemos apreciar la interfaz de SET la cual se basa en menús y está desarrollada en lenguaje de programación python.

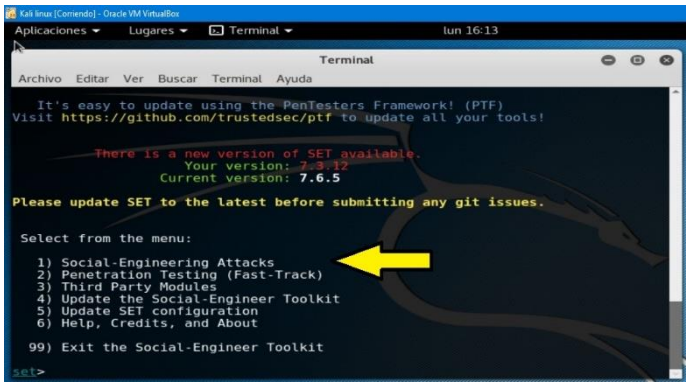

Fig.32. Selección de la herramienta SET.

Una vez puesta en marcha la herramienta se procede a seleccionar la opción 1 que contiene una serie de submenús con una lista de ataques que se pueden efectuar, a continuación, se escoge la opción 2 (Vector de ataque a sitio Web), paso seguido se selecciona la opción 3 (Método de ataque de credenciales), luego se selecciona la opción 2 (clonar sitio) la cual especifica la clonación de una dirección Web, luego nos pide una dirección IP de redireccionamiento esta dirección es la que se la va enviar a la víctima en nuestro caso la pusimos 192.168.1.20 y finalmente se ingresó la URL del sitio Web a clonar, como se observa en la figura 33.

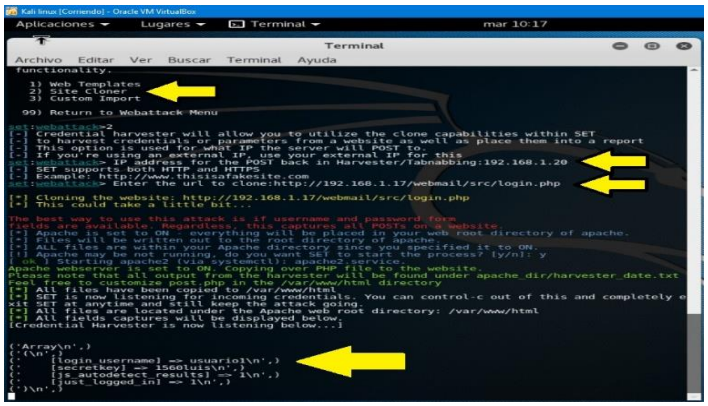

Fig.33. Resultado del ataque phishing.

Para hacerle más real el ataque se optó por enviar la dirección IP falsa mediante correo electrónico, de tal manera que la víctima piense que se trata de un correo propio de la empresa y caiga en el ataque phishing, para esto se seleccionó la opción (e-mail attack single email address), en donde se ingresó el correo electrónico de la víctima, adicionalmente se ingresó el correo del remitente y se elaboró el asunto del mensaje y el contenido del mismo, además se incluyó la IP falsa 192.168.1.20 a la cual va acceder la victima una vez que lea el mensaje, finalmente la herramienta Social Engineering atack (SET) se encargara de enviar el mensaje como podemos apreciar en la figura 34.

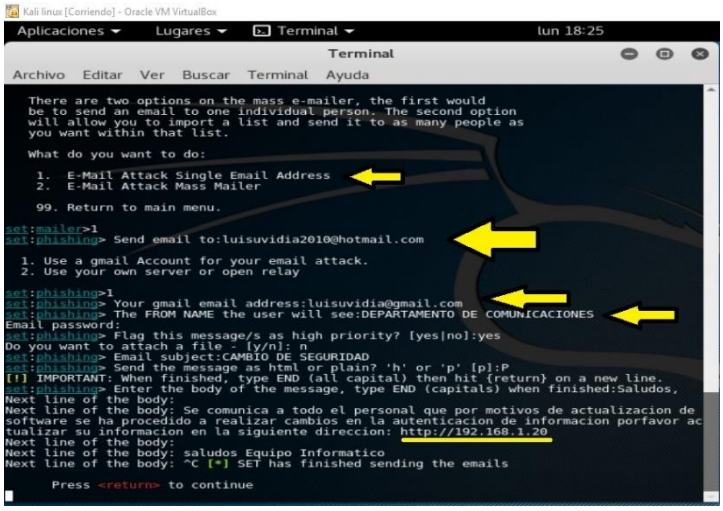

Fig.34. Cuerpo del mensaje a ser enviado a la víctima.

Posteriormente, para corroborar el envío del ataque revisamos el correo electrónico simulando que somos la víctima, en la figura 35 podemos apreciar el mensaje recibido con el remitente Departamento de comunicaciones, el asunto Cambio de seguridad y la dirección IP a la cual se efectuará el Phishing.

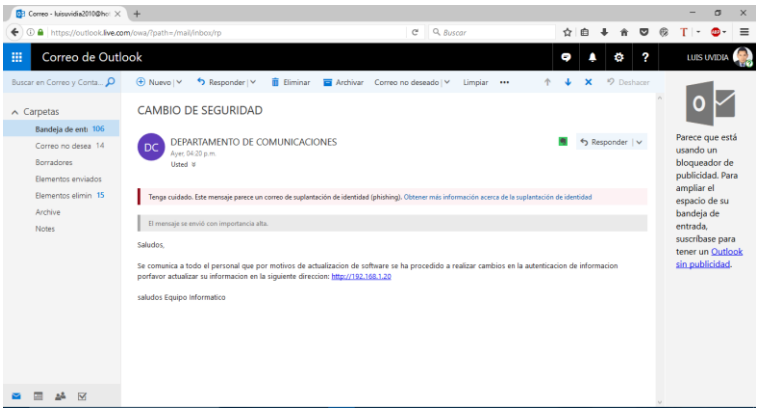

Fig.35. Correo electrónico recibido.

Una vez que la víctima ingresa a la dirección IP enviada, se abre la página Web que clonamos, permitiendo de esta manera confundir a la víctima, una vez en la página fueron ingresados los datos de usuario (usuario1) y la contraseña (1560luis), como se aprecia en la figura 36.

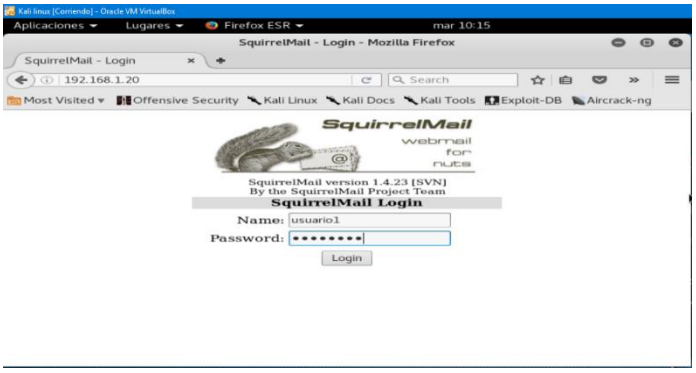

Fig.36. Página Web clonada.

Al momento que la víctima hace clic en (Login), el navegador rápidamente redirige a la página Web original.

Resultados obtenidos

Una vez terminado el proceso del ataque la herramienta SET almaceno los datos obtenido de la víctima y se visualizaron en el panel de control de la consola del atacante, además se creó un archivo de texto llamado CLAVES en la carpeta raíz de instalación de la herramienta, el cual contiene el nombre de usuario y contraseña de la víctima, como lo podemos ver en la figura 37.

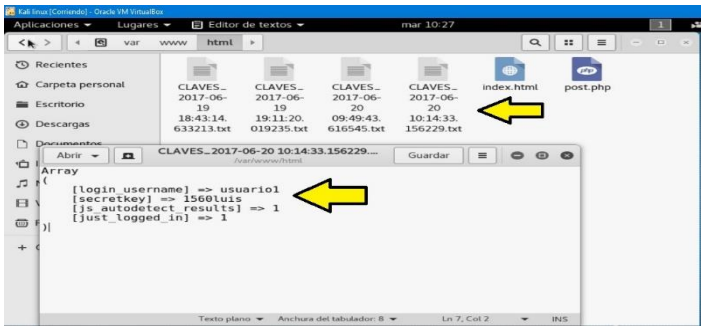

Fig.37. Archivo generado por SET.

Adicionalmente en la herramienta Wireshark se aprecia los continuos procesos de redireccionamiento de la página, desde la dirección IP falsa: 192.168.1.20 hasta la dirección IP: 192.168.1.17 del cliente, como podemos observar en la figura 38 los eventos identificados.

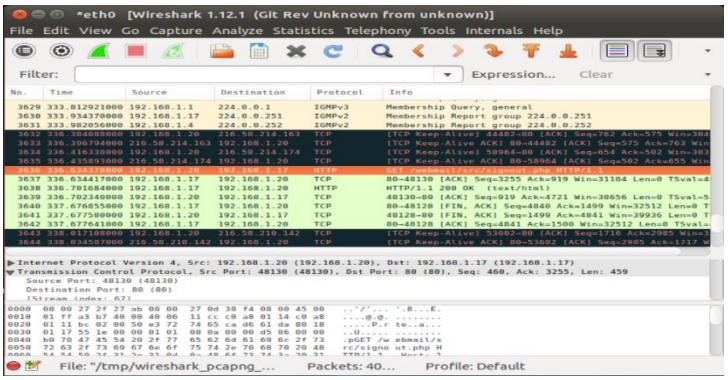

Fig.38. Eventos visualizados con Wireshark.

VII. PROPUESTAS PARA CONTRARRESTAR CIBERATAQUES

VII.1. *CONTROL DE ATAQUE DE ESCANEO DE PUERTOS*

Para hacer frente al ataque de escaneo de puertos, se realizó la implementación de la herramienta ESET Smart Security 9 dentro del equipo cliente de Microsoft, dicha herramienta posee la capacidad de contrarrestar amenazas de nivel de red (malware), sistema de bloqueo de intrusos a través del Host (HIPS), protección contra ataques basados en scripts, además mayor número de capas especiales de protección ante ataques de cibercriminales. En la figura 39 podemos visualizar la herramienta de protección.

Fig.39. Smart Security 9.

Por otra parte, como medida de seguridad para el cliente Linux se implementó un potente cortafuego llamado UFW, el cual está desarrollado para abrir y cerrar puertos al momento de arrancar el sistema, otra de las ventajas es que solo se lo modifica con permisos de administrador con esta ventaja, cualquier intruso no puede hacer modificaciones en la herramienta, esto es posible gracias a la configuración de Iptables que habilita (ACCEPT) o deshabilita (DROP) puertos, las configuraciones que le aplicamos se pueden observar en la figura 40.

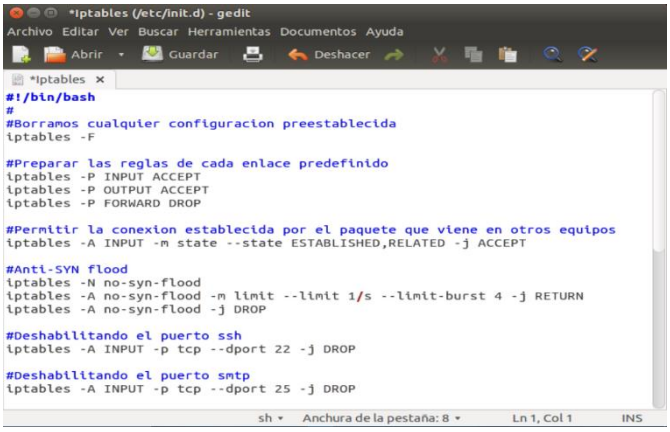

Fig.40. Configuración de las Iptables.

Resultados Adquiridos

Se volvió a ejecutar la herramienta Look@LAN para escaneo de puertos la cual dio como resultado que ningún puerto está habilitado ya que anteriormente procedimos a deshabilitar el acceso a los puertos de los protocolos smtp, pop3, imap3, mysql, como podemos observar en la figura 41.

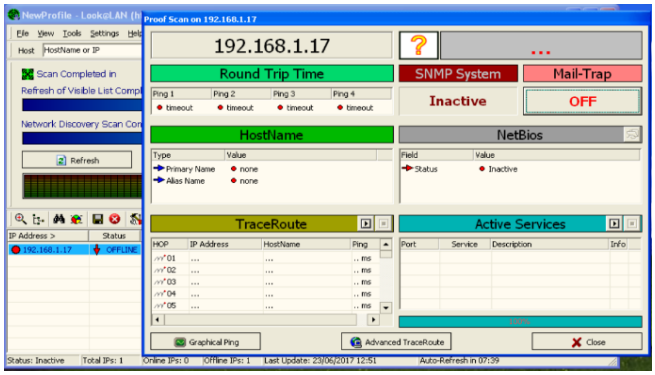

Fig.41. Herramienta Look@LAN sin resultados.

De la misma manera de ejecuto la herramienta Nmap o Zenmap, evidenciando el mismo resultado de la herrameinta anterior la cual no arrojo ninguna informacion sobre el escaneo de puertos como se observa en la figura 42.

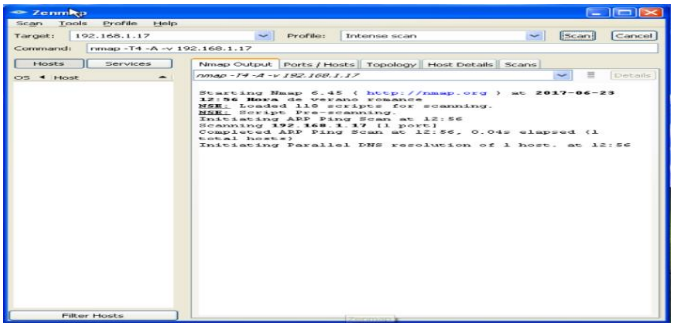

Fig.42. Ejecución de la Herramienta Zenmap sin resultados.

Finalmente se ejecutó la herramienta Wireshark para evidenciar el rechazo de las conexiones que intentaban ser establecidas por parte de las herramientas Look@LAN y Nmap las mismas que fueron controladas en la configuración de las Iptables, en la figura 43 se observa el proceso de intentos de conexión.

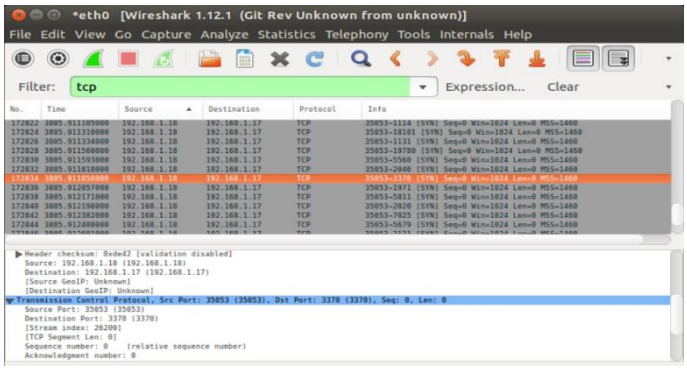

Fig.43. Intentos fallidos de conexión.

VII.2. *CONTROL DE ATAQUE DE HOMBRE EN EL MEDIO*

Se buscó alternativas de control para este ataque y una de las cuales es la herramienta ESET Smart Security con su sistema de análisis en tiempo real se logró detectar una advertencia donde nos indicaba que se localizaron varias amenazas potencialmente peligrosas, entre ellas los archivos de ejecución de Cain&Abel que lleva extensión ejecutable (.exe), cabe destacar que la herramienta permite aplicar acciones de eliminar, desinfectar o dejar sin acciones, como podemos observar en la figura 44.

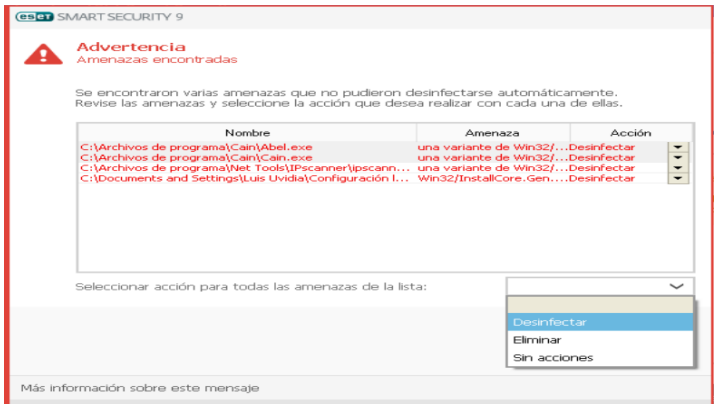

Fig.44. Advertencia amenazas encontradas.

Por otro lado, en el servidor Ubuntu Linux se aplicó la herramienta ARPWATCH, la cual tiene la capacidad de emitir alertas en el preciso instante que el servidor se encuentra en proceso de un potencial ataque por parte de un equipo extraño a la red. Dicha alerta la realiza mediante el envío de correos electrónicos a una cuenta que se le asocie, en nuestro caso la configuración que la realizamos fue la siguiente:

Eth0 –a –n 192.168.1.1/24 –m usuario1@luvidia.simplesite.com

Finalmente se recibió el correo de aviso de que un equipo con la dirección Ip: 192.168.1.18 en nuestro caso un equipo cliente de la red, intentó acceder al servidor Ubuntu, indicándonos la fecha y la hora del suceso, como se aprecia en la figura 45.

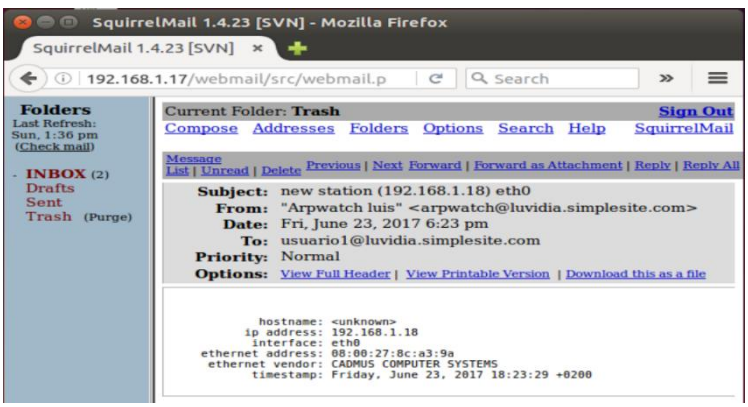

Fig.45. Correo de notificación de posible ataque.

VII.3. *CONTROL DE ATAQUE DE FUERZA BRUTA*

Para el control de ataques de fuerza bruta, se realizó la configuración de acceso a los puertos mediante las IPtables del equipo servidor Ubuntu, gracias a esto se pudo controlar el acceso a los puertos, para confirmar el correcto funcionamiento realizamos una prueba de ataque con la herramienta Medusa, pudimos ver que nos muestra un mensaje que dice que el puerto 110 (puerto del protocolo TCP que proporciona el servicio pop3) se encuentra inhabilitado y de esta forma deja de establecer comunicación y finaliza la ejecución, como se ve en la figura 46.

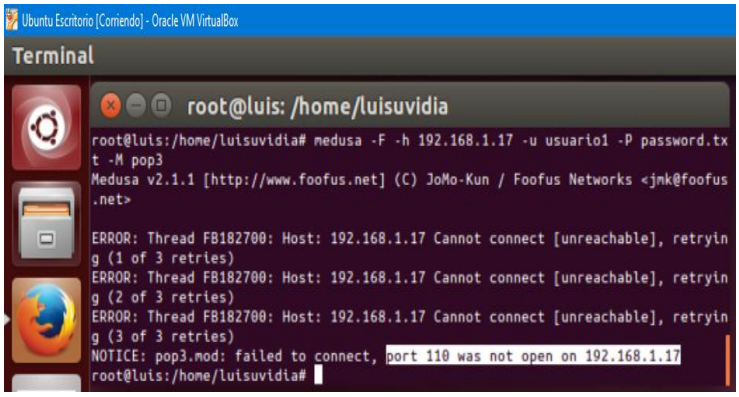

Fig.46. Ataque fallido con Medusa.

VII.4. *CONTROL DE ATAQUE DE DENEGACIÓN DE SERVICIOS*

Para el control de ataques de fuerza bruta, se realizó la configuración de acceso a los puertos mediante las Iptables del equipo servidor Ubuntu, gracias a esto se pudo controlar la generación reiterada de tráfico hacia el servidor Web, para esto se añadió unas líneas de códigos las cuales cumplen la función de deshabilitar la conexión si detectan que se ha suscitado varios intentos de conexión, como podemos observar en la figura 47.

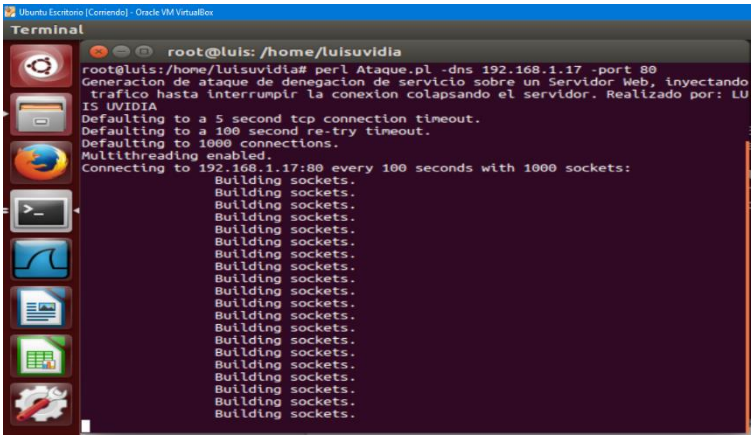

Fig.47. Intento fallido de conexión con el servidor Web.

Finalmente se probo con la herramienta NetTools la misma que se evidencio que no se puede acceder al servidor Web debido a la restriccion que se le configuro en la Iptables, en la figura 48 se obseva el intento fallido de conexión.

Fig.48. Intento fallido de ataque DoS mediante Nettools5.

VII.5. *CONTROL DE ATAQUE A LA WEB (PHISHING)*

Mediante el control de reglas del cortafuego UFW se pudo establecer un control total por parte del equipo servidor al generar un rango de direcciones IP que poseen permiso para ingresar a la comunicación con el servidor, como vemos en la figura 49, aquí nos muestra la regla que deshabilita el ingreso al puerto 80 desde un equipo externo hacia el servidor.

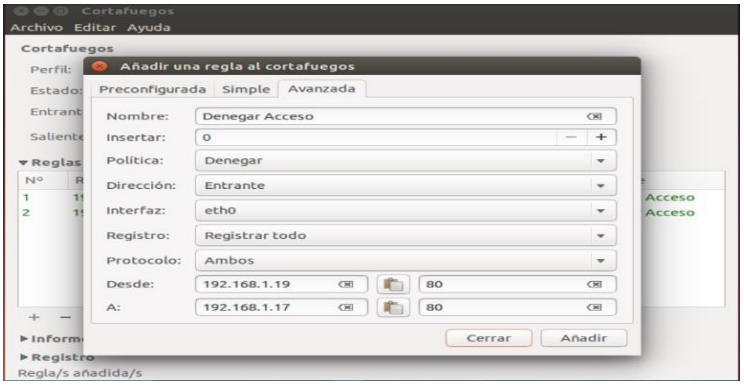

Fig.49. Regla de denegación de acceso al puerto 80.

Al intentar realizar el ataque phishing desde el atacante externo en nuestro caso el cliente KaliLinux, fue imposible lograr establecer la conexión hacia el servidor Web, para poder capturar la información del contenido de la página Web víctima del ataque, en la figura 50 podemos observar el error que genera la herramienta SET al intentar comunicarse con el servidor.

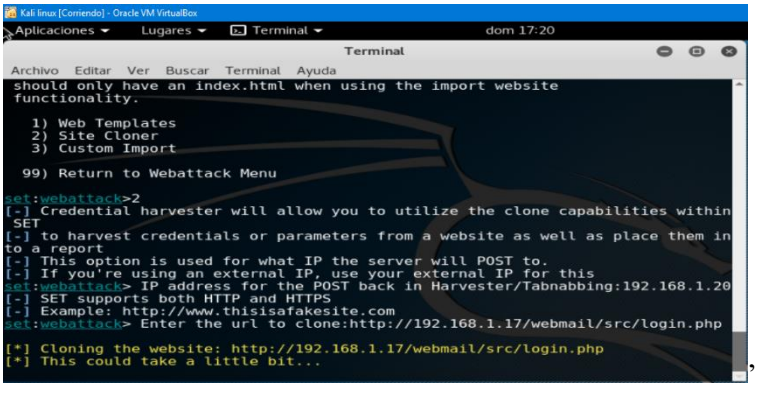

Fig.50. Intento fallido de conexión mediante SET.

VIII. CONCLUSIONES

Se realizó la construcción y diseño de la red IP en el equipo anfitrión conformada por un equipo servidor basado en el sistema operativo Ubuntu, tres equipos clientes y un equipo enrutador, se logró obtener simulaciones reales mediante el uso de la herramienta Virtual Box gracias a su optimo desempeño, además se logró efectuar diversos ataques a la red de entre los cuales están, el escaneo de puertos, fuerza bruta, hombre en el medio, y el phishing, por otro lado se comprobó los análisis obtenidos mediante la herramienta Wireshark la cual permitió localizar los puertos, el protocolo y el equipo atacante utilizados para efectuar el ataque, logrando identificar las vulnerabilidades del servidor y de la red IP virtualizada.

Finalmente se aplicaron soluciones de control en los equipos, a través de la herramienta *ESET smart security 9*, el cual filtro ataques mediante el módulo de cortafuegos programable brindándonos la opción de eliminar o bloquear las potenciales amenazas, adicionalmente se implementó un cortafuegos generado a través de Iptables dentro del servidor Ubuntu, como complemento adicional se instaló la aplicación ARPwhatch la cual envía al administrador un correo electrónico en el momento que alguien intenta atacar el servidor Ubuntu, de esta manera pudimos contrarrestar los ataques generados.

Partiendo del presente estudio se platea promover la generación de desarrollo, como base para futuros análisis a medida del avance de la tecnología y el pasar de los años con futuros ataques, además, es un sustento teórico para implementaciones en un entorno empresarial de datos real, ya que contiene puntos importantes como las posibles amenazas y ataques que puede ser víctima.

IX. REFERENCIAS

[1] C. Vialfa, «Introducción a la seguridad informática,» Ccn, 15 Octubre 2016. [En línea]. Available: http://es.ccm.net/contents/622-introduccion-a-la-seguridad-informatica. [Último acceso: 15 Junio 2017].

[2] M. A. Castañeda Vasquez, «Sistemas Operativos,» blogspot, Agosto 2011. [En línea]. Available: http://ingenieria-sistemas-sistemas-opera.blogspot.com.es/p/seguridad-informatica_15.html. [Último acceso: 18 Junio 2017].

[3] S. A. Kaabi, N. A. Kindi, S. A. Fazari y Z. Trabelsi, «Virtualization based ethical educational platform for hands-on lab activities on DoS attacks,» de *Global Engineering Education Conference (EDUCON), 2016 IEEE*, Abu Dhabi, 2016.

[4] T. Zseby, F. I. Vázquez, A. King y K. C. Claffy, «Teaching Network Security With IP Darkspace Data,» *IEEE Transactions on Education* , vol. 59, nº 1, pp. 1-7, 2016.

[5] J. Keller y R. Naues, «A Collaborative Virtual Computer Security Lab,» de *e-Science and Grid Computing, 2006. e-Science '06. Second IEEE International Conference on*, Amsterdam, 2016.

[6] M. Sánchez Gómez, «Infraestructuras Críticas y Ciberseguridad,» 6 Julio 2011. [En línea]. Available: https://manuelsanchez.com/2011/07/06/infraestructuras-criticas-y-ciberseguridad/. [Último acceso: 17 Junio 2017].

[7] G. Vani, «SlideShare,» 28 Diciembre 2013. [En línea]. Available: https://es.slideshare.net/gio_vani/scanners-29542462. [Último acceso: 18 Junio 2017].

[8] J. Vivancos Pérez, «Seguridad,» Seguridad y Alta Disponibilidad, 2012. [En línea]. Available: http://dis.um.es/~lopezquesada/documentos/IES_1213/SAD/curso/UT4/ActividadesAlumnos/13/herramientas.html. [Último acceso: 23 06 2017].

[9] L. Paus, «Welivesecurity,» 2 Febrero 2015. [En línea]. Available: https://www.welivesecurity.com/la-es/2015/02/02/manipulando-paquetes-hping3/. [Último acceso: 18 Junio 2017].

[10] F. Priáñez Gómez, «Formación Profesional a travéz de internet,» I.E.S Mar de Cádiz, 8 Septiembre 2016. [En línea]. Available: http://fpg.x10host.com/VirtualBox/qu_es_la_virtualizacin.html. [Último acceso: 18 Junio 2017].

[11] M. Ferrer Amer, «rootear,» rootear, 19 Agosto 2013. [En línea]. Available: https://rootear.com/virtualizacion/como-utilizar-virtualbox. [Último acceso: 18 Junio 2017].

[12] b. Boss, «Syconet blog de informática y redes,» Syconet, 7 Julio 2012. [En línea]. Available: https://syconet.wordpress.com/2012/07/07/introduccion-al-servidor-de-correo-postfix/. [Último acceso: 7 Junio 2017].

[13] E. Fumás Cases, «Apache HTTP Server: ¿Qué es, cómo funciona y para qué sirve?,» ibrugor, 11 Junio 2014. [En línea]. Available: http://www.ibrugor.com/blog/apache-http-server-que-es-como-funciona-y-para-que-sirve/. [Último acceso: 19 Junio 2017].

[14] M. A. Alvarez, «phpMyAdmin,» desarrolloweb.com, 19 Julio 2002. [En línea]. Available: https://desarrolloweb.com/articulos/844.php. [Último acceso: 20 Junio 2017].

[15] H. Hernández , «Definición y principales características de Joomla,» Hostname, 26 Noviembre 2012. [En línea]. Available: https://www.hostname.cl/blog/que-es-joomla. [Último acceso: 20 Junio 2017].