UTMACH

UNIDAD ACADÉMICA DE INGENIERÍA CIVIL

CARRERA DE INGENIERÍA DE SISTEMAS

IMPLEMENTACIÓN DE CONTROLES PARA EL DISEÑO DE REDES QUE MINIMICEN EL IMPACTO DE LAS VULNERABILIDADES BASADAS EN DIRECCIONES IP

PIEDRA PINEDA BÉLGICA VANESSA
INGENIERA DE SISTEMAS

MACHALA
2018

UTMACH

UNIDAD ACADÉMICA DE INGENIERÍA CIVIL

CARRERA DE INGENIERÍA DE SISTEMAS

IMPLEMENTACIÓN DE CONTROLES PARA EL DISEÑO DE REDES QUE MINIMICEN EL IMPACTO DE LAS VULNERABILIDADES BASADAS EN DIRECCIONES IP

PIEDRA PINEDA BÉLGICA VANESSA
INGENIERA DE SISTEMAS

MACHALA
2018

UTMACH

UNIDAD ACADÉMICA DE INGENIERÍA CIVIL

CARRERA DE INGENIERÍA DE SISTEMAS

EXAMEN COMPLEXIVO

IMPLEMENTACIÓN DE CONTROLES PARA EL DISEÑO DE REDES QUE MINIMICEN EL IMPACTO DE LAS VULNERABILIDADES BASADAS EN DIRECCIONES IP

PIEDRA PINEDA BÉLGICA VANESSA
INGENIERA DE SISTEMAS

MOROCHO ROMAN RODRIGO FERNANDO

MACHALA, 05 DE JULIO DE 2018

MACHALA
05 de julio de 2018

Nota de aceptación:

Quienes suscriben, en nuestra condición de evaluadores del trabajo de titulación denominado Implementación de controles para el diseño de redes que minimicen el impacto de las vulnerabilidades basadas en direcciones IP, hacemos constar que luego de haber revisado el manuscrito del precitado trabajo, consideramos que reúne las condiciones académicas para continuar con la fase de evaluación correspondiente.

MOROCHO ROMAN RODRIGO FERNANDO
0703820464
TUTOR - ESPECIALISTA 1

VALAREZO PARDO MILTON RAFAEL
0704518893
ESPECIALISTA 2

CÁRDENAS VILLAVICENCIO OSCAR EFRÉN
0703935312
ESPECIALISTA 3

Fecha de impresión: lunes 09 de julio de 2018 - 16:15

URKUND

Urkund Analysis Result

Analysed Document: PIEDRA PINEDA BÉLGICA VANESSA_PT-010518.pdf (D40244467)
Submitted: 6/18/2018 3:43:00 PM
Submitted By: bpiedra_est@utmachala.edu.ec
Significance: 0 %

Sources included in the report:

Instances where selected sources appear:

0

CLÁUSULA DE CESIÓN DE DERECHO DE PUBLICACIÓN EN EL REPOSITORIO DIGITAL INSTITUCIONAL

La que suscribe, PIEDRA PINEDA BÉLGICA VANESSA, en calidad de autora del siguiente trabajo escrito titulado Implementación de controles para el diseño de redes que minimicen el impacto de las vulnerabilidades basadas en direcciones IP, otorga a la Universidad Técnica de Machala, de forma gratuita y no exclusiva, los derechos de reproducción, distribución y comunicación pública de la obra, que constituye un trabajo de autoría propia, sobre la cual tiene potestad para otorgar los derechos contenidos en esta licencia.

La autora declara que el contenido que se publicará es de carácter académico y se enmarca en las dispociones definidas por la Universidad Técnica de Machala.

Se autoriza a transformar la obra, únicamente cuando sea necesario, y a realizar las adaptaciones pertinentes para permitir su preservación, distribución y publicación en el Repositorio Digital Institucional de la Universidad Técnica de Machala.

La autora como garante de la autoría de la obra y en relación a la misma, declara que la universidad se encuentra libre de todo tipo de responsabilidad sobre el contenido de la obra y que asume la responsabilidad frente a cualquier reclamo o demanda por parte de terceros de manera exclusiva.

Aceptando esta licencia, se cede a la Universidad Técnica de Machala el derecho exclusivo de archivar, reproducir, convertir, comunicar y/o distribuir la obra mundialmente en formato electrónico y digital a través de su Repositorio Digital Institucional, siempre y cuando no se lo haga para obtener beneficio económico.

Machala, 05 de julio de 2018

PIEDRA PINEDA BÉLGICA VANESSA
0706267598

DEDICATORIA

Dedico el presente trabajo a Dios por darme la fortaleza de continuar siempre adelante a pesar de las adversidades permitiéndome llegar a este momento importante en mi vida como es la culminación de mis estudios universitarios.

A mi madre por ser la persona más importante en mi vida siendo mi modelo a seguir por su fuerza y perseverancia en los momentos difíciles.

A mi padre por todos aquellos momentos en los que supo darme ánimos con su alegría inigualable.

Bélgica Vanessa Piedra Pineda

AGRADECIMIENTO

Agradezco a mi familia por el apoyo brindado; a mis profesores por ser quienes me supieron brindar el conocimiento necesario para llevar a cabo con éxito la finalización de mi carrera; a mi tutor el Ing. Rodrigo Morocho y a mis amigos que compartieron conmigo sus conocimientos y alegrías, en especial a la Srta. Cristina Calero que siempre me ha dado su amistad y apoyo incondicional.

Bélgica Vanessa Piedra Pineda

RESUMEN

IP (Internet Protocol) es un protocolo de comunicación poco seguro el cual no garantiza la transferencia de los paquetes desde su dirección de origen hasta el destino, dando paso a distintas vulnerabilidades que pueden ser aprovechadas por ataques como: Man-in-the-middle (MITM), Suplantación de direcciones IP y Denegación de Servicio Distribuido “Smurf”. Estos ataques se producen por la falta de seguridad en el envio de los paquetes ICMP a través de red permitiendo ser interceptados por un tercero el cual puede modificar o eliminar los datos comprometiendo la seguridad, integridad y disponibilidad de la información en la red. Con la ayuda de las herramientas Ettercap y Hping3 se logró simular estos tipos de ataques dentro de un entorno virtual de prueba el cual fue diseñado mediante el uso de GNS3 donde se pudo emular la conexión de la red y VirtualBox para la virtualización de varios hosts lo cual facilitó la identificación de los controles necesarios. La solución se basó en un exhaustiva búsqueda y análisis de controles que consiste en incrementar la seguridad en los host clientes de la red y nivel de Router, en los primeros se implementó un control a nivel de la tabla ARP y en el segundo mediante la creación de Listas de Control Acceso (ACL) con el propósito de asegurar que la protección del protocolo IP esté presente en un entorno real. Implementada la solución en la red se pudo evidenciar que los controles empleados evitan que se afecte al correcto funcionamiento de la red.

Palabras claves: ICMP, Ettercap, Hping3, ARP, ACL

ABSTRACT

IP is a protocol of communication not save at all because it doesn't guarantee the transference of packages from his origin direction until his destination, giving it different vulnerabilities that can be exploited for attacks such as: Man-in-the-middle (MITM), IP address suplantation, Denial of distributed service "Smurf". This attacks are produced because of the poor security sending the packets ICMP through the network letting it been intercepted by a third person the that can modify or deleted any data, compromising security, integrity and disponibility of the information in the network. With the help of tools Ettercap and Hping3 it was possible to simulated this type of attacks inside a virtual environment (example) the one was designed by the usage of GNS3 where it could be emulated the network connection and VirtualBox for the virtualization of many hosts the one hat facilities the identification of necessary controls. The solution is based in an exhaustive research and analysis control that consist in the incrementing of security in the host network clients and level of the router, in the first ones we implement a control in the level of the table ARP and in the second one by the creation of access control list (ACL) for the purpose of ensuring that protocol IP protection is present in the real environment. Implemented the solution in the network, we got the evidence that the implemented controls prevent the correct operation of the network from being affected.

KEY WORDS: ICMP, Ettercap, Hping3, ARP, ACL.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1. INTRODUCCIÓN

La sociedad contemporánea se gesta a través del internet, interviniendo en cada proceso o función nominal de las naciones llegando a transformar la forma en que se realiza ciertas actividades cotidianas para integrar nuevas potencialidades que faciliten el desarrollo tecnológico, cultural, económico e integrar nuevas tendencias en el manejo de la información.

Hoy en día todo está conectado a la red, desde celulares hasta grandes corporaciones o instituciones públicas que manejan gran cantidad de datos con información personal de carácter sensible de sus usuarios (claves, tarjetas de créditos, calificaciones, redes sociales, cuentas bancarias), este gran flujo de datos que se efectúa en forma masiva puede ser objeto de hackers o terceros que buscan modificar, robar e incursionar de forma ilícita a los sistemas informáticos de los afectados. [1]

El protocolo TCP/IP es uno de los más utilizados en el entorno de redes, con una mayor aceptación en gran parte del mundo, brindando una mayor seguridad en la comunicación entre los hosts. El protocolo TCP es el encargado de otorgar la fiabilidad del envío y recepción de la información, a diferencia del protocolo IP el cual no resulta ser fiable en la entrega de los datos, es por ello que se complementan de tal forma para garantizar un nivel de seguridad en cuanto a la comunicación se trata a través de la red.

El protocolo IP debido a las deficiencias, presenta vulnerabilidades muy fáciles de explotar como lo es la suplantación de direcciones IP o la inundación a través de paquetes ICMP, las cuales pueden provocar daños irreversibles a los usuarios dentro de una red, debido a esto se realizó una exhaustiva investigación y posterior análisis de controles que se pueden implementar para minimizar el impacto que estas pueden tener. El informe de la investigación se encuentra organizado de la siguiente manera:

Capítulo 1: La introducción en la cual se detalla el marco contextual en la cual se desarrolló con tal el problema y los objetivos que se buscan cumplir con la investigación.

Capítulo 2: El desarrollo del documento en el cual se destaca el marco teórico donde se encuentra toda la fundamentación teórica en la que se basa la investigación y un marco metodológico donde se describen los resultados obtenidos para cumplir con el objetivo planteado.

Capítulo 3: Las conclusiones es lo que se logró obtener luego de la implementación de la solución del problema.

1.1 Marco contextual

Es importante en el diseño de una red implementar controles que ayuden con la seguridad en el envío de información, como es el caso del protocolo IP, el cual no garantiza la fiabilidad en la entrega de la información a su destino, siendo vulnerable a ataques de suplantación e inundación.

Un ataque de suplantación combinado con uno de inundación puede ocasionar un gran impacto en la red, consumiendo todos sus recursos que como consecuencia pueden llegar a denegar los servicios poniendo en riesgo el correcto funcionamiento de la red. En seguridad este ataque es una de las mayores amenazas pues se ve afectado el ancho de banda de la red impidiendo el paso al tráfico real de forma normal, comprometiendo de este modo a la integridad, disponibilidad y confidencialidad de la información a través de la red.

1.2 Problema

La seguridad en las redes hoy en día es un tema bastante complejo pues el diseño de las mismas no siempre se encuentra basado en prevenir la explotación de vulnerabilidades por terceros maliciosos que buscan perjudicar a los usuarios con el robo, modificación o eliminación de información relevante, llegando incluso a la extorsión por parte de delincuentes informáticos. Por lo tanto es importante tener en cuenta el funcionamiento y la deficiencia que ciertos protocolos presentan como es el caso de IP, el cual es muy poco fiable en su seguridad perjudicando al correcto funcionamiento de la red. Por lo antes mencionado la problemática se encuentra centrada en la Implementación de controles en el diseño de redes para minimizar el impacto de las vulnerabilidades basadas en direcciones IP.

1.3 Objetivo

Implementación de controles mediante medidas de seguridad para el diseño en una red minimizando el impacto de las vulnerabilidades basadas en direcciones IP

2. DESARROLLO

2.1 Marco teórico

2.1.1 Protocolo IP (Protocolo de Internet). Es el principal protocolo de la capa de red, permitiendo el envió o enrutamiento de paquetes de datos desde el origen hasta su destino. Este protocolo no posee ningún tipo de protección que garantice él envió o la recepción segura de la información, siendo vulnerable a diversos tipos de ataques con facilidad. Es por ello que se obtiene la fiabilidad a partir de los protocolos superiores como TCP garantizando una comunicación segura. [2]

La unión de estos dos protocolos TCP/IP garantizan en mayor medida la fiabilidad en la transferencia de la información dentro de los miembros de una red permitiendo que en la actualidad existan varios sistemas o servicios que aprovechen su compatibilidad como lo es en la telemedicina. [3]

2.1.2 Ataque MAN-IN-THE-MIDDLE (MITM). Un ataque *Main-In-The-Middle* u Hombre en el medio, se da lugar cuando un tercero o atacante intercepta la comunicación entre dos partes, interfiriendo en él envió de la información, modificando o reemplazando por información falsa. [1] En este tipo de ataques las víctimas desconocen de su atacante, pues piensan que su comunicación es de forma directa y segura. [4]

De acuerdo a [1] el ataque MITM puede ser llevado a cabo en diferentes entornos de comunicación como en redes LAN o WIFI, es uno de los tipos de ataques más comunes y peligrosos llegando a convirtiéndose en una amenaza para la seguridad de la red. Además el ataque MITM puede llegar a comprometer la confidencialidad, integridad y disponibilidad de los datos.

Este ataque según explica [5] consisten en explotar las vulnerabilidades del protocolo ARP implantando de forma maliciosa una dirección falsa (IP, MAC) en la caché de la tabla ARP sustituyéndola por una original, mediante el envenenamiento a través del envío de paquetes ARP falsificados entre los host de la red. Si el resultado del ataque resulta ser exitoso, el intruso o atacante podrá espiar o modificar contenido y en el peor de los casos llegar a secuestrar la sesión.

Existen nuevos y mejorados ataques como se menciona en [6] se ha modificado de tal forma que combina MITM con DoS (Denegación de Servicios) convirtiéndose en SMITM el cual aprovecha las vulnerabilidades presentes en las redes WIFI encriptadas WPA2 mediante el envenenamiento a la caché de ARP redirigiendo de esta forma el tráfico de la información desde la víctima al Atacante.

2.1.3 Suplantación de direcciones IP. El ataque de suplantación de direcciones IP, se lleva a cabo cuando el atacante oculta su identidad mediante el envío de paquetes con direcciones IP de origen falsificado, haciendo creer a la víctima que proviene de una dirección de IP segura. [7] Esto sucede por la deficiencia que se presenta en el protocolo IP en cuanto a los envíos de paquetes, pues solo depende de la dirección IP de destino mas no considera el comprobar la autenticidad del origen del remitente. Considerando esta vulnerabilidad se puede realizar diversos ataques que comprometen la seguridad de la información en la red. [1]

2.1.4 Suplantación Ciega y No ciega. Estos dos tipos de ataques se diferencian en la ubicación en la que se encuentra el atacante al momento de realizar la suplantación. De acuerdo a [1] la suplantación No ciega es llevada a cabo desde la misma subred en la que se encuentra la víctima mientras que la suplantación Ciega se realiza desde otra red. Ambos son utilizados mayormente para realización de ataques de Denegación de servicios (DoS) y Denegación de Servicio Distribuido (DDoS) mediante inundación, lo que consiste en la solicitud de muchas peticiones para saturar dicho servicio o consumir el Ancho de Banda en la red como lo realiza el ataque Smurf. [8]

2.1.5 Ataque Denegación de Servicio Distribuido SMURF. El ataque *Smurf* o Pitufo se da cuando el atacante ha suplantado la dirección IP de la víctima para enviar paquetes ping falsificados de *ICMP* (Protocolo de mensajes de control de Internet) a la dirección de difusión o *broadcast,* obteniendo como respuesta que todos los host de esa red envíen paquetes de *echo ICMP* a la IP víctima llegando a saturarla y posteriormente a bloquearla por un tiempo. [9], [10] Además este tipo de ataque logra crear tormentas de *broadcast* en toda la red llegando a consumir el ancho de banda produciendo una denegación en el servicio para el tráfico legítimo. [11]

2.1.6 Ettercap. Es una herramienta de código abierto utilizada mayormente en entornos Linux, fue diseñada con el propósito de interferir en la comunicación de una red a través del uso de Sniffers para la inyección de datos que altera la comunicación comprometiendo la confidencialidad, integridad y disponibilidad de la información. [12]

Posee una interfaz gráfica que hace más fácil su uso junto a los múltiples funcionalidades entre las más utilizadas se encuentra la suplantación del protocolo ARP y servicios como DHCP y DNS. Utilizándose principalmente para la realización de ataques Main-in-the-Middle (MITM) mediante el uso de ARP Spoofing para la suplantación de la dirección (IP, MAC) por la del atacante. [13]

2.1.7 Wireshark y TCPDUM. Es una herramienta de código abierto utilizada tanto en entornos Linux como Windows permite la realización de análisis a los paquetes de los

diferentes protocolos como: TCP, ICMP, UDP, HTTP, entre otros los cuales circulan a través de la red, mediante la escucha por un puerto específico. Además permite el filtrado de paquetes en específico lo que facilita la búsqueda de información específica. [11]
La funcionalidad que esta herramienta provee es muy similar a TCPDUM la cual permite el análisis y captura de paquetes desde consola a diferencia de Wireshark que cuenta con una interfaz gráfica para una mejor visualización. [14]

2.1.8 Hping3. Es una herramienta de código abierto utilizada mayormente en entornos Linux aunque también en Windows, entre sus funcionalidades se encuentra la de suplantación y modificación de paquetes ICMP, TCP y UDP, permitiendo también realizar inundaciones de estos paquetes congestionando de esta manera la red. [15] Además esta herramienta funciona desde consola mediante el uso de comando siendo utilizada en mayor parte para ataques DoS como lo es el ataque Smurf. [16]

2.1.9 Protocolo ARP. ARP (Protocolo de Resolución de Direcciones) es utilizada para llevar la lista de las direcciones física y de red (IP, MAC) de los hosts. Cuando se desconoce de la dirección MAC de un hosts dentro de la red, se envía un mensaje solicitando ARP a los equipos que se encuentren en la red los cuales responderán a dicha solicitud incluido el del hosts requerido. Este procedimiento no tiene ningún tipo de control es por ello que resulta ser muy vulnerable a ataques para interceptar dicha información y suplantar a un equipo. Una solución que se ha presentado para esta vulnerabilidad es el establecer de manera estática la dirección (IP, MAC) de cada uno de los hosts dentro de la red en la tabla ARP. [17]

2.2 Solución del problema

2.2.1 Diseño e Implementación del escenario en un entorno virtual. Se diseñó un entorno virtual mediante el uso de la herramienta GNS3 para emular las conexiones de la red y VirtulBox que permitió la virtualización de los hosts. Lo cual hizo posible la implementación de los ataques en los distintas topologías presentes en los escenarios que se muestran la Figuras 1 y 2.

La red está conformada de tal forma que cada uno de los equipos de las Figuras 1 y 2 cumple una función específica las cuales son:

- **El Router:** permite el enrutamiento de los hosts dentro de la red.
- **El Servidor (Ubuntu):** el cual se encuentra implementado sobre un sistema operativo Linux y posee el Servicio Web activo permitiendo a los hosts clientes dentro de la red acceder al mismo.

- **Los equipos clientes (Windows, Kali Linux y 2 Ubuntu):** cuya función es consumir los recursos del servidor mediante la realización de peticiones generando tráfico dentro de la red.

Para la creación de red se realizó una tabla de direccionamiento IP de cada uno de los equipos que se detalla en la Tabla 1.

Tabla 1: Direccionamiento IP

Equipos	Dirección IP	Mascara de Subred	Puerta de Enlace	DNS
Router Cisco 3640	e0/0 192.168.10.1 e0/1 192.168.10.17	255.255.255.240	--------	---------
Servidor Ubuntu	192.168.10.2	255.255.255.240	192.168.10.1	192.168.10.2
Cliente 1 : KaliLinux	192.168.10.3/ 192.168.10.18	255.255.255.240	192.168.10.1	192.168.10.2
Cliente 2: Windows 7	192.168.10.4	255.255.255.240	192.168.10.1	192.168.10.2
Cliente 3: Ubuntu	192.168.10.10	255.255.255.240	192.168.10.1	192.168.10.2
Cliente 4: Ubuntu	192.168.10.11	255.255.255.240	192.168.10.1	192.168.10.2

Fuente: Elaboración propia del autor

Escenario 1

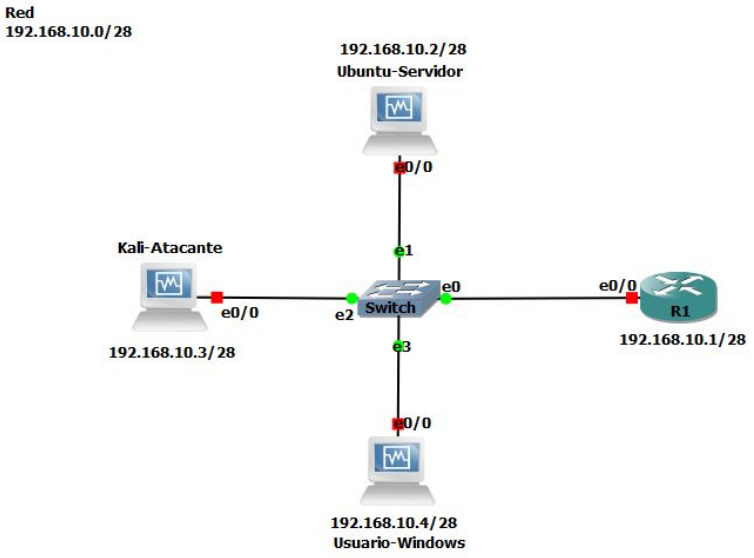


Figura 1: Topología Escenario 1
Fuente: Propia del autor

Escenario 2

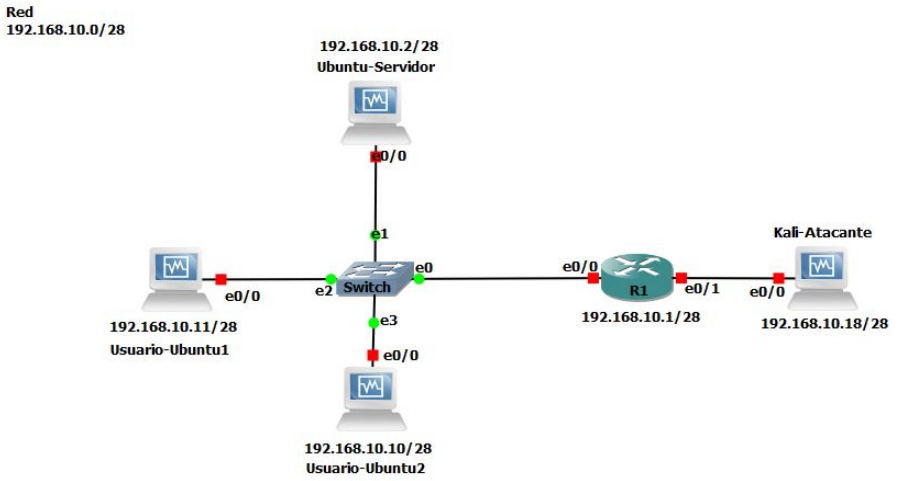


Figura 2: Topología Escenario 2
Fuente: Propia del autor

2.2.2 Exploración de las vulnerabilidades basadas en direcciones IP. Para la exploración de las vulnerabilidades se utilizaron las siguientes herramientas que se encuentran instaladas y configuradas dentro del atacante Kali Linux para cada uno de los 2 escenarios que se muestran en las Figuras 1 y 2:

Escenario 1

Ettercap: Enviara un Sniffer entre la comunicación del Servidor Web y el cliente Windows, permitiendo obtener la información que transita por medio de esta comunicación.

Wireshark: Permitirá la captura y análisis de los paquetes específicos para obtener la información requerida.

Escenario 2

Hping3: Suplantara la dirección IP de la víctima que en este caso será el Servidor Web e inundará la red con paquetes ICMP mediante la dirección de *broadcast.*

Tcpdum: permitirá analizar el tráfico de paquetes ICMP que llegaran al Servidor Web durante el ataque de inundación.

2.2.2.1 Ataque Main-In-The-Middle (MITM) y Suplantación IP. Para la exploración de las vulnerabilidades generadas a partir del ataque Main in the Middle u Hombre en el medio y Suplantación IP se utilizó la topología que se muestra en la Fig. 1 del primer escenario.

Figura 3: Envió de Sniffing
Fuente: Elaboración propia

El ataque consistió en interceptar la comunicación entre el Servidor Web y cliente Windows mediante el uso de la herramienta Ettercap, como se muestra en la Fig. 3 se envió un

Sniffing a través del puerto **eth0**. Luego escanea todos los hosts que se encuentran en la red y los lista como se muestra en la Fig. 4.

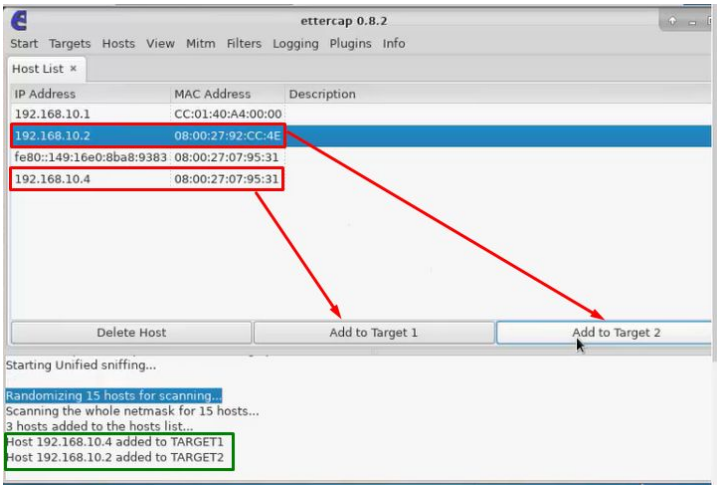


Figura 4: Lista de hosts
Fuente: elaboración propia del autor

Una vez que dentro de la lista de todos los hosts se han identificado la IP tanto del Servidor Web como del cliente Windows se procedió a colocarlos en cada una de las tarjetas como se muestra en la Fig. 4.

Establecidas las victimas en cada una de las tarjeras se procedió a realizar el envenenamiento de la tabla ARP mediante el envío del Sniff a través del ataque Mitm como se muestra en la Fig. 5

Figura 5: Ataque Mimt
Fuente: Elaboración propia del autor

Finalmente se utilizó la herramienta Wireshark para verificar todo el tráfico que se generó y los paquetes que se lograron capturar con información relevante de la víctima en este caso del cliente Windows.

2.2.2.2 Ataque Denegación de Servicio Distribuido Smurf. Para la realización de este ataque se utilizó la topología que se muestra en la Fig. 2 del segundo escenario.

```
root@kali:~# hping3 --icmp --spoof 192.168.10.2 --flood 192.168.10.15
```

Figura 6: Comando Hping3
Fuente: Elaboración propia del autor

El ataque consistió en suplantar la dirección IP del Servidor Web e inundar la red con paquetes ICMP mediante el uso de la dirección de *broadcast* utilizando la herramienta Hping3 con los siguientes parámetros que se muestran en la Fig. 6

--icmp: Es el tipo de paquete que se envía a través de red.
--spoof: Permite suplantar la dirección IP real por una falsa o de otro hosts dentro de la red
--flood: Realiza la inundación a la dirección IP indicada este caso la de broadcast.
Una vez establecidos los parámetros se procedió a ejecutar el comando para el ataque creando la inundación a través de la red que se muestra en la Fig. 2. Todos los hosts de esta red enviaran paquetes ICMP a la víctima en este caso el Servidor Web llegando a saturarlo de peticiones, consumiendo el ancho de banda provocando que al cargar el contenido de una página web este se vuelva lento y en el peor de lo caso deniegue el acceso al servicio.

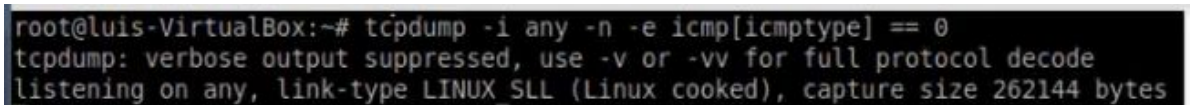


Figura 7: Análisis con tcpdump
Fuente: Elaboración propia del autor

Finalmente se utilizó la herramienta Tcpdump para visualizar la llegada de los paquetes ICMP durante la inundación como se muestra en la Fig. 7.

2.2.3 Implementación de controles en el escenario virtual. Para dar solución a las vulnerabilidades que se presentaron durante la realización de ataques Main-in-the-middle y Suplantación IP, que comprometieron la integridad, disponibilidad y confidencialidad de la información, se propuso el siguiente control que consiste en poner de forma estática la dirección (IP, MAC) en la tabla ARP del cliente en Windows evitando de esta manera la suplantación de la misma durante la ejecución de este ataque, mediante el siguiente comando que se muestra en la Fig.8.

Figura 8: Comando (IP, MAC) estática
Fuente: Elaboración propia del autor

Durante el ataque de Smurf el atacante se encuentra en otra subred desde donde provoca la inundación por lo cual el control se lo estableció en el Router creando una Lista de Control de Acceso (ACL) para controlar el flujo de tráfico a través de la red. Como se muestra en la Fig. 9 se creó la lista y posteriormente se la asigno a la interfaz de salida **e0/0**

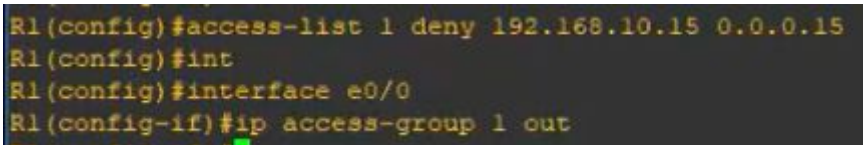


Figura 9: ACL
Fuente: Elaboración propia del autor

2.3 Resultado

Mediante el análisis de las vulnerabilidades basadas en el direccionamiento IP, se logró determinar las falencias presentes en el diseño de una red a través de la realización de ataques de Suplantación e Inundación se comprobó la ineficiente en la seguridad de la mismas, lo cual llevo a la implementación de controles en el caso de los clientes la creación de dirección (IP, MAC) estáticas en la tabla ARP evitando de esta manera que se produzca una suplantación y el Router el establecimiento de Listas de Control de Acceso (ACL) las cuales permiten controlar el tráfico generado en la red ayudando a minimizar el impacto provocado por dicho ataques, con el fin de considerar cada uno de estos puntos débiles dentro de la red como una mejora para la misma y evitar dichos inconvenientes en una red real.

CONCLUSIONES

- Se realizó un exhaustivo análisis de las vulnerabilidades basadas en direcciones el IP lo cual aportó a detectar los puntos débiles en el diseño e implementación de una red.

- Se implementó un entorno virtual en el cual se pusieron realizar pruebas necesarias para comprobar la seguridad que posee una red frente a la presencia de un ataque.

- Se investigó y analizó los posibles controles que permitieron reducir el impacto en el diseño de una red ocasionado por las vulnerabilidades basadas en direcciones IP.

- Se implementó controles eficientes que permitieron minimizar el impacto que generaron los ataques provocados por las vulnerabilidades basadas en direcciones IP presentes en el diseño de la red.

BIBLIOGRAFÍA

[1] M. Conti, N. Dragoni y V. Lesyk, «A Survey of Man In The Middle Attacks,» *IEEE Communications Surveys & Tutorials,* vol. 18, nº 3, pp. 2027-2051, 29 Marzo 2016.

[2] W. Xiaofeng, Z. Huan, S. Jinshu, W. Baosheng, X. Qianqian y L. Pengkun, «T-IP: A self-trustworthy and secure Internet protocol,» *China Communications,* vol. 15, nº 2, pp. 1-14, 21 Febrero 2018.

[3] W. Tuay, L. Mendoza y L. Jaimes Cerveleón, «Telemedicine system based on ECG signals and in the TCP/IP protocol using a sparse space,» *Sistemas & Telemática,* vol. 15, nº 41, pp. 75-83, 3 Mayo 2017.

[4] F. Faheem y R. Hamza, «Using JPCAP to Prevent Man-in-the-Middle Attacks in a Local Area Network Environment,» *IEEE Potentials,* vol. 31, nº 4, pp. 35-37, 25 Julio 2012.

[5] N. Seung Yeob, D. Sirojiddin y P. Minho, «Collaborative approach to mitigating ARP poisoning-based Man-in-the-Middle attacks,» *Computer Networks,* vol. 57, nº 18, pp. 3866-3884, 24 Diciembre 2013.

[6] A. Mayank, S. Biswas y N. Sukumar, «Advanced Stealth Man-in-The-Middle Attack in WPA2 Encrypted Wi-Fi Networks,» *IEEE Communications Letters ,* vol. 19, nº 4, pp. 581-584, 05 Febrero 2015.

[7] Z. CHAOQIN, H. GUANGWU, C. GUOLONG, K. ARUN, SANGAIAH, Z. PINGAN, Y. XIA y J. WEIJIN, «Towards a SDN-Based Integrated Architecture for Mitigating IP Spoofing Attack,» *IEEE Access,* vol. 6, pp. 22764 - 22777, 19 Diciembre 2017.

[8] H. Neminath y T. Nikhil, «An event based technique for detecting spoofed IP packets,» *Journal of Information Security and Applications,* vol. 35, pp. 32-34, Agosto 2017.

[9] R. Shyamala y V. Shanmugam, «Impact of DoS Attack in Software Defined Network for Virtual Network,» *Wireless Personal Communications,* vol. 94, nº 4, pp. 2189-2202, 02 Junio 2016.

[10] S. T. Zargar, J. Joshi y D. Tipper, «A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks,» *IEEE Communications Surveys & Tutorials ,* vol. 15, nº 4, pp. 2046-2069, 28 Marzo 2013.

[11] N. Vivens, X. Zhifeng, M. Vasudeva Rao, M. Ke y X. Yang, «Network forensics analysis using Wireshark,» *International Journal of Security and Networks,* vol. 10, nº 2, pp. 91-106, 2015.

[12] T. Vollmer y M. Maníaco, «Cyber-Physical System Security With Deceptive Virtual Hosts for Industrial Control Networks,» *IEEE Transactions on Industrial Informatics,* vol. 10, nº 2, pp. 1337-1347, 27 Febrero 2014.

[13] A. Yacchirena, D. Alulema, D. Aguilar, D. Morocho, E. Francisco y G. Evelio, «Analysis of attack and protection systems in Wi-Fi wireless networks under the Linux operating system,» *IEEE International Conference on Automatica (ICA-ACCA),* 12 Diciembre 2016.

[14] Sudhakar y A. R. K., «A survey on comparative analysis of tools for the detection of ARP poisoning,» *2017 2nd International Conference on Telecommunication and Networks (TEL-NET),* 23 Abril 2017.

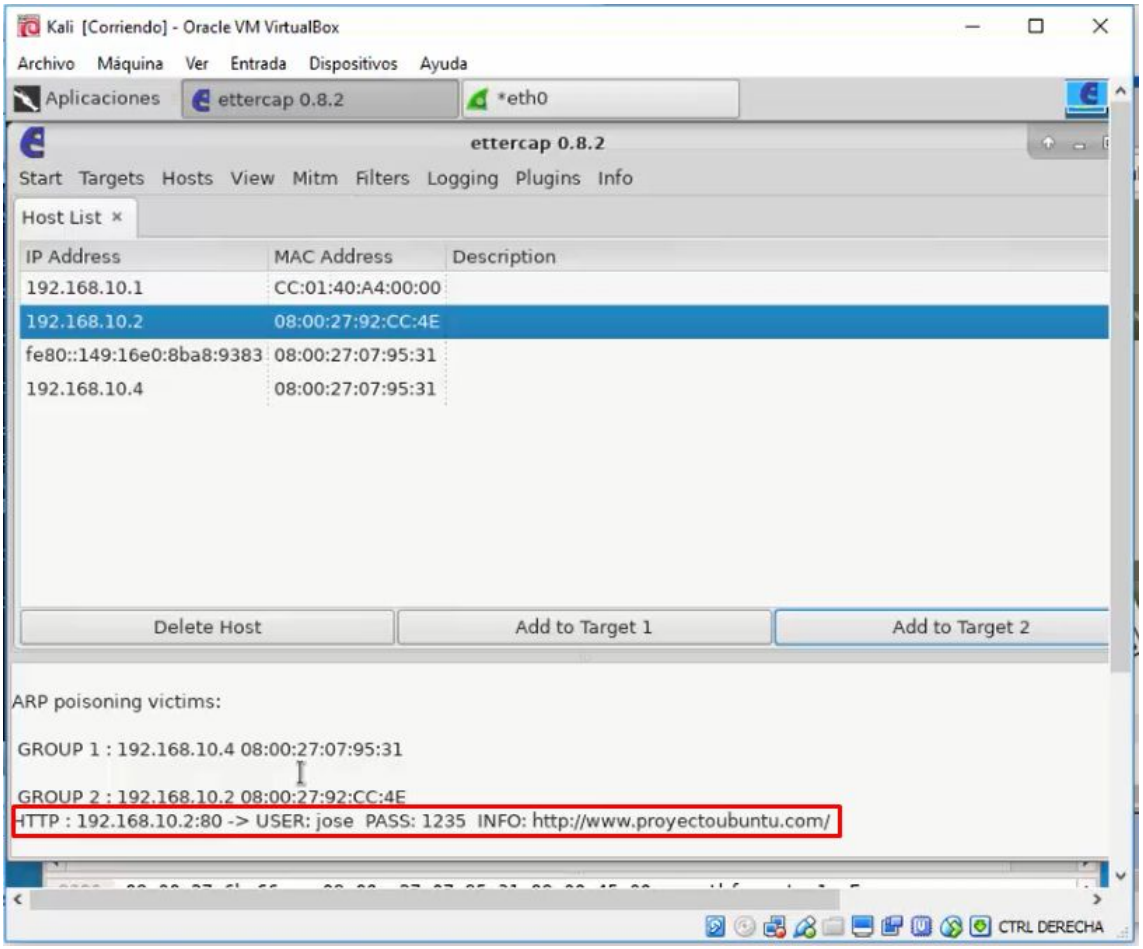
[15] G. Vasconcelos, G. Carrijo, R. Miani, J. Souza y V. Guizilini, «The Impact of DoS Attacks on the AR.Drone 2.0,» *2016 XIII Latin American Robotics Symposium and IV Brazilian Robotics Symposium (LARS/SBR),* 15 Diciembre 2016.

[16] A. Saboor, M. Akhlaq y B. Aslam, «Experimental evaluation of Snort against DDoS attacks under different hardware configurations,» *2013 2nd National Conference on Information Assurance (NCIA),* 10 Febrero 2014.

[17] S. Min Su, L. Jae Dong, J. Young-Sik, J. Hwa-Young y P. Jong Hyuk, «DS-ARP: A New Detection Scheme for ARP Spoofing Attacks Based on Routing Trace for Ubiquitous Environments,» *Hindawi Limited,* pp. 1-7, 2014.

ANEXOS

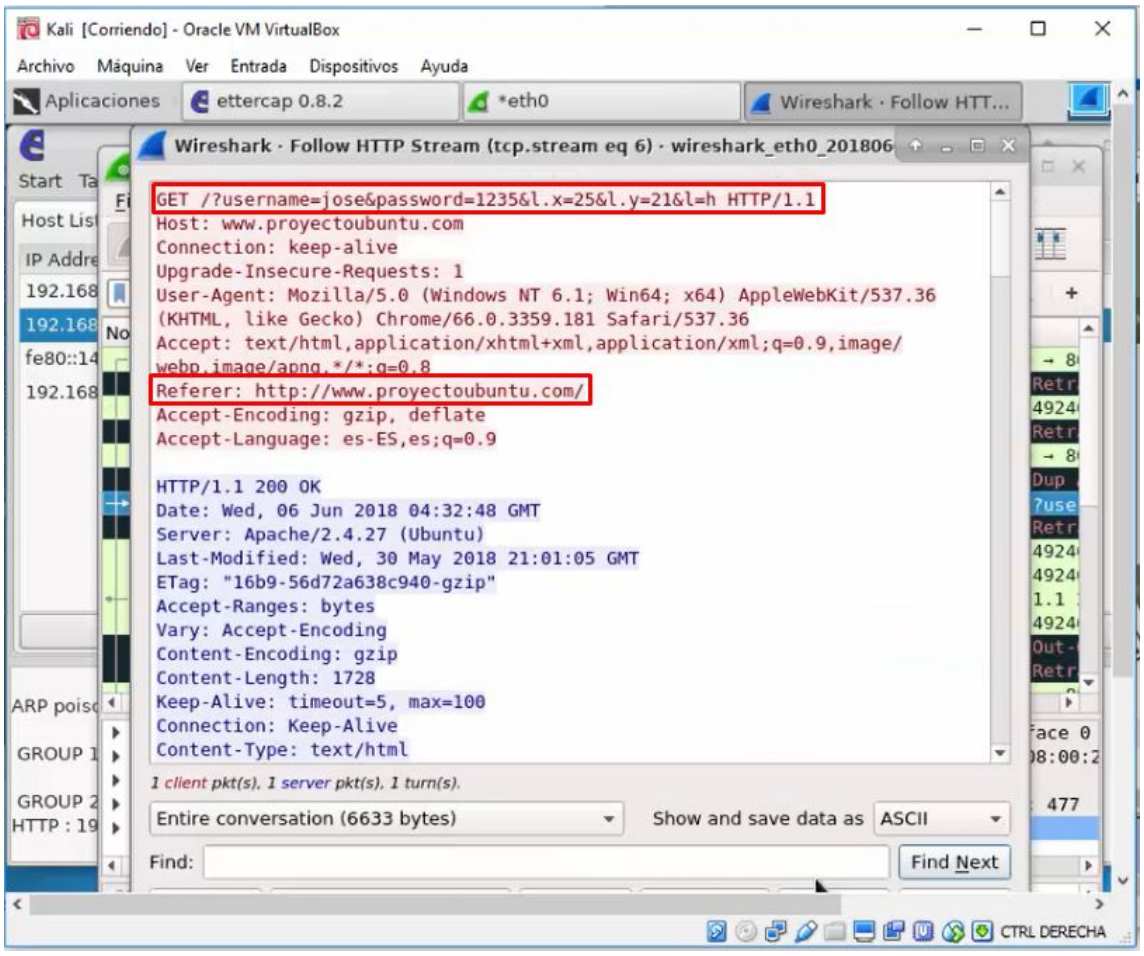
Anexo A: Resultado del Ataque Main-in-the-middle en Ettercap



Fuente: Elaboración propia del autor

En la imagen del Anexo A se puede observar la información obtenida luego de haber llevado a cabo el ataque Main-in-the-middle en la comunicación entre el Servidor Web y el cliente Windows.

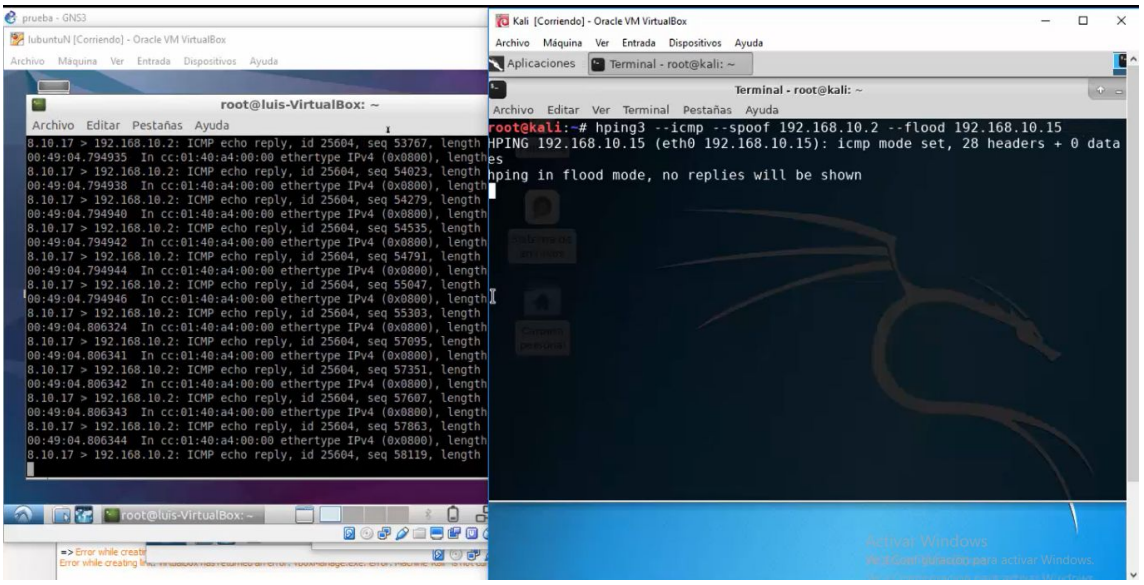
Anexo B: Resultado del Ataque Main-in-the-middle en Wireshark



Fuente: Elaboración propia del autor

En el Anexo B se puede observar la información obtenida en la captura de paquetes HTTP, en el cual se encontró la dirección de referencia de la página web donde inició sesión con su usuario y contraseña. Con esta información el atacante roba la sesión.

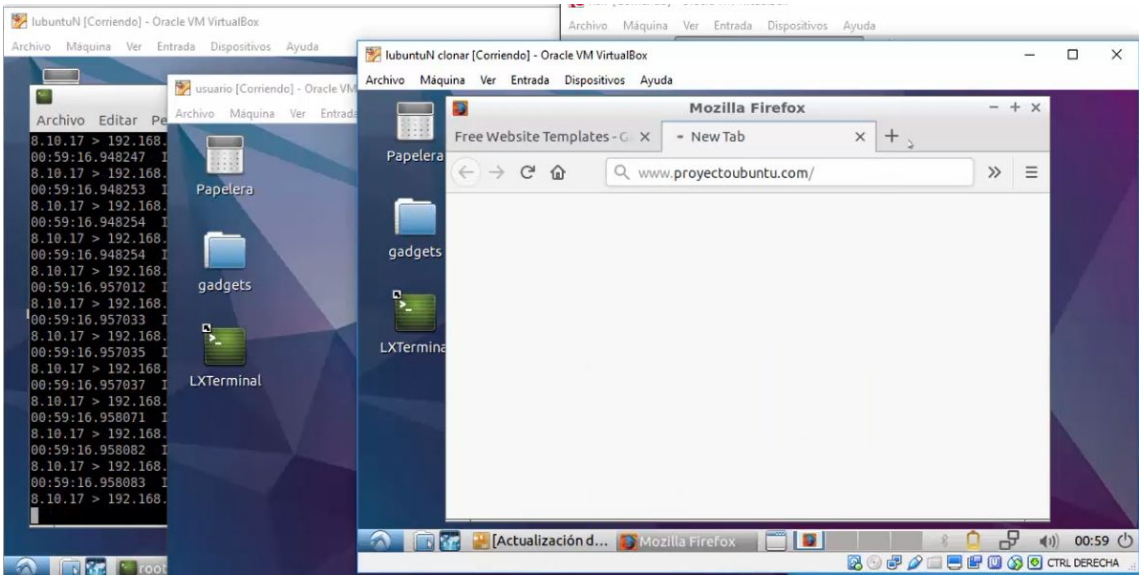
Anexo C: Ejecución del ataque de Denegación de Servicio Distribuido Smurf



Fuente: Elaboración propia del autor

En el Anexo C se puede observar en la pantalla del lado derecho la ejecución del ataque de Smurf y en la de la izquierda la llegada por inundación de los paquetes ICMP a la víctima el Servidor Web.

Anexo D: Resultado del Ataque Smurf



Fuente: Elaboración propia del autor

En el Anexo D se puede observar la demora en la carga del contenido de la página web en el cliente Ubuntu durante la ejecución del ataque Smurf en el Servidor Web.