UTMACH

UNIDAD ACADÉMICA DE INGENIERÍA CIVIL

CARRERA DE INGENIERÍA DE SISTEMAS

IMPLEMENTACIÓN DE CONTROLES EN UNA LAN PARA MITIGAR LOS ATAQUES DEL DHCP UTILIZANDO LAS MEJORES PRÁCTICAS DEL DISEÑO DE REDES

AUZ CADENA FABIOLA CECILIA
INGENIERA DE SISTEMAS

MACHALA
2019

UTMACH

UNIDAD ACADÉMICA DE INGENIERÍA CIVIL

CARRERA DE INGENIERÍA DE SISTEMAS

IMPLEMENTACIÓN DE CONTROLES EN UNA LAN PARA MITIGAR LOS ATAQUES DEL DHCP UTILIZANDO LAS MEJORES PRÁCTICAS DEL DISEÑO DE REDES

AUZ CADENA FABIOLA CECILIA
INGENIERA DE SISTEMAS

MACHALA
2019

UTMACH

UNIDAD ACADÉMICA DE INGENIERÍA CIVIL

CARRERA DE INGENIERÍA DE SISTEMAS

EXAMEN COMPLEXIVO

IMPLEMENTACIÓN DE CONTROLES EN UNA LAN PARA MITIGAR LOS ATAQUES DEL DHCP UTILIZANDO LAS MEJORES PRÁCTICAS DEL DISEÑO DE REDES

AUZ CADENA FABIOLA CECILIA
INGENIERA DE SISTEMAS

NOVILLO VICUÑA JOHNNY PAUL

MACHALA, 31 DE ENERO DE 2019

MACHALA
31 de enero de 2019

Nota de aceptación:

Quienes suscriben, en nuestra condición de evaluadores del trabajo de titulación denominado IMPLEMENTACIÓN DE CONTROLES EN UNA LAN PARA MITIGAR LOS ATAQUES DEL DHCP UTILIZANDO LAS MEJORES PRÁCTICAS DEL DISEÑO DE REDES, 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.

NOVILLO VICUÑA JOHNNY PAUL
0702947409
TUTOR - ESPECIALISTA 1

JUMBO CASTILLO FREDDY ANIBAL
0704167949
ESPECIALISTA 2

LOJA MORA NANCY MAGALY
0703410027
ESPECIALISTA 3

Fecha de impresión: lunes 04 de febrero de 2019 - 11:01

URKUND

Urkund Analysis Result

Analysed Document: Informe_Fabiola_Auz.pdf (D47108760)
Submitted: 1/22/2019 1:02:00 PM
Submitted By: fauz_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, AUZ CADENA FABIOLA CECILIA, en calidad de autora del siguiente trabajo escrito titulado IMPLEMENTACIÓN DE CONTROLES EN UNA LAN PARA MITIGAR LOS ATAQUES DEL DHCP UTILIZANDO LAS MEJORES PRÁCTICAS DEL DISEÑO DE REDES, 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, 31 de enero de 2019

AUZ CADENA FABIOLA CECILIA
0706746898

RESUMEN

Implementación de controles en una LAN para mitigar los ataques del DHCP utilizando las mejores prácticas del diseño de redes

El protocolo de configuración dinámica de host (DHCP) es de tipo cliente servidor. El servidor se configura con los parámetros de la red y un rango de direcciones ip disponibles para ser asignadas automáticamente a los clientes, lo que permite una sencilla administración de la red. El servidor puede ser víctima de ataques como el de incumplimiento del DHCP; donde un hacker utiliza direcciones MAC falsas para realizar peticiones al servidor consiguiendo que se agoten las direcciones ip y no quede ninguna disponible para asignarles a los clientes legítimos de la red. Otro ataque es el de suplantación del servidor DHCP, donde se implementa un servidor falso para engañar a los clientes y configurar parámetros diferentes a los del servidor legítimo y poder espiar en el tráfico de la red y obtener información. El objetivo de este trabajo es identificar las vulnerabilidades a las que está expuesto el protocolo DHCP, e investigar los controles necesarios a implementar para garantizar la seguridad dentro de la red. Se utilizó la herramienta GNS3 para emular el escenario de red, el sistema operativo Kali Linux donde operan las herramientas yersinia, y ettercap para ejecutar los ataques. Se implementaron controles como la seguridad de puertos y dhcp snooping conocida como la inspección de DHCP; comprobando de esta manera que la red se encuentra segura, el servidor proporciona correctamente la configuración a los clientes y que ningún hacker podría analizar nuestros datos o todo el tráfico que hay en la red.

Palabras claves: DHCP SPOOFING, DHCP STARVATION, SEGURIDAD DE PUERTOS, DHCP SNOOPING, GNS3.

ABSTRACT

Implementation of controls on a LAN to mitigate DHCP attacks using the best practices of network design

The Dynamic Host Configuration Protocol (DHCP) is a client-server type. The server is configured with network parameters and a range of available IP addresses to be automatically assigned to clients, which allows easy administration of the network. The server can be a victim of attacks such as non-compliance with DHCP; where a hacker uses fake MAC addresses to make requests to the server getting the IP addresses to run out and none is available to assign them to the legitimate clients of the network. Another attack is the impersonation of the DHCP server, where a false server is implemented to trick the clients and configure parameters different from those of the legitimate server and to spy on the network traffic and obtain information. The objective of this work is to identify the vulnerabilities to which the DHCP protocol is exposed, and investigate the necessary controls to be implemented to guarantee security within the network. The GNS3 tool was used to emulate the network scenario, the Kali Linux operating system where the yersinia tools operate, and ettercap to execute the attacks. Implemented controls such as port security and dhcp snooping known as DHCP inspection; checking in this way that the network is secure, the server correctly provides the configuration to the clients and that no hacker could analyze our data or all the traffic that is in the network.

Keywords: DHCP SPOOFING**,** DHCP STARVATION**,** SECURITY OF PORTS**,** DHCP SNOOPING, GNS3.

CONTENIDO

LISTA DE ILUSTRACIONES

LISTADO DE TABLAS

1. INTRODUCCIÓN

Actualmente la comunicación se desarrolla en gran parte utilizando dispositivos tecnológicos, ya sea el celular o el computador; permitiendo compartir con las personas que se encuentren en diferentes lugares la información oportuna y valiosa que necesiten para continuar con el desempeño de sus actividades diarias.

Las conexiones y dispositivos de red se configuran con el fin de proporcionar a los usuarios una comunicación entre ellos y al internet para compartir sus diferentes tipos de información.

En una red de área local (LAN) debería prevalecer la seguridad de la información que circula a través de la red. Por esta razón es necesario identificar los posibles ataques a los que son vulnerables los protocolos de red, para evitar espías dentro de la red, fallos en la implementación de los servicios de red, entre otros [1].

La implementación de un servidor DHCP es importante dentro de una red, ya que proporciona direcciones ip automáticamente a los clientes que se conectan asignándoles todos los parámetros de la red necesarios, sin embargo sin la configuración adecuada se encuentra vulnerable a ataques de suplantación e incumplimiento de DHCP [1][2].

Considerando los ataques posibles al servidor DHCP se implementarán los controles para mitigar las vulnerabilidades como la seguridad de puertos y activar la indagación de DHCP en el switch para identificar al servidor de confianza[15].

En el presente informe se detalla el desarrollo de los controles implementados al servidor DHCP una vez identificadas las vulnerabilidades, el trabajo empieza por la sección de introducción detallando la problemática y los objetivos que nos planteamos para llegar a la solución, en la sección del desarrollo se detallan las herramientas utilizadas, la información teórica que fue usada como base para emplearlas de forma práctica en la solución. En la última sección se describen las conclusiones a las que se llegó con la implementación de los controles utilizados en el servidor DHCP.

1.1 Contexto del problema

Un servidor DHCP con una configuración básica es vulnerable en su seguridad y la de los clientes a los que les proporciona configuración de red, dentro de una LAN el servidor puede ser falsificado por hackers con el propósito de robar información de los clientes conectados, o simplemente no permitir que los servicios del protocolo DHCP se ejecuten con normalidad.

1.2 Problema general

Identificar los controles necesarios para prevenir riesgos ante posibles ataques al servidor DHCP, conociendo las vulnerabilidades de seguridad dentro de la red a las que está expuesto.

1.3 Objetivo General

Implementar controles en una LAN para mitigar los ataques del DHCP utilizando las mejores prácticas del diseño de redes.

1.4 Objetivos específicos

- Diseñar el escenario de red en la herramienta GNS3
- Emplear herramientas que permitan explotar las vulnerabilidades de seguridad de un servidor DHCP.
- Investigar los controles adecuados para garantizar la seguridad del servidor DHCP.

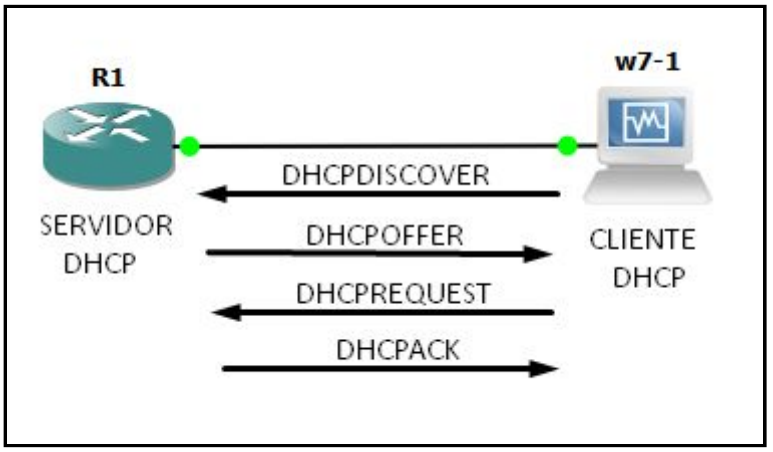
2. DESARROLLO

2.1 MARCO TEÓRICO

2.1.1 PROTOCOLO DHCP

El protocolo de configuración dinámica de host (DHCP), es un protocolo de tipo cliente- servidor, es muy útil para administrar una red local de forma sencilla y dinámica, se configura en el servidor un rango de direcciones ip y parámetros de configuración como la máscara de subred, puerta de enlace, y dirección del servidor dns para que asigne automáticamente a los clientes cuando se conecten a la red [1].

Figura 1. Operación del protocolo DHCP



Elaborado por: Fabiola Auz

La forma en la que opera el DHCP es mediante paquetes que se envían desde el cliente al servidor como se muestra en la figura 1. Donde inicialmente el cliente envía un paquete DHCP DISCOVER para ubicar al servidor en la red. El servidor responde mediante el paquete DHCPOFFER la configuración inicial de red que incluye la dirección ip, máscara de subred, puerta de enlace y asocia su dirección MAC para no asignar nuevamente la misma dirección a otro cliente. El cliente acepta la configuración y la notifica en la red y solicita nuevamente al servidor la confirmación de los parámetros enviados, finalmente el servidor confirma

la asignación con un paquete DHCPACK y guarda los datos del cliente. Si el servidor no tuviera dirección ip libre respondería al cliente con un paquete DHCPNACK [1] [2].

2.1.2 DHCP STARVATION.

Un cliente malicioso establece una lista de direcciones MAC falsas con las que enviará paquetes DHCPDISCOVER para que el servidor le responda con los parámetros de red, aprovechándose de esta vulnerabilidad que tiene el servidor de no diferenciar entre un cliente genuino de uno falso; el servidor agotará su rango de direcciones ip disponibles y no podrá asignar a otro cliente que se conecte a la red, o uno que vuelva a solicitar su dirección ip [3].

2.1.3 DHCP SPOOFING

El ataque DHCP spoofing consiste en suplantar el servidor legítimo por uno falso utilizando alguna herramienta que permita realizar las mismas funciones; de manera que el atacante sea quien responda a los mensajes DHCPDISCOVER enviados por los clientes que solicitan la configuración de red. El servidor DHCP falso proporcionará la dirección ip en un rango diferente al establecido en el servidor legítimo donde establece su dirección ip como puerta de enlace lo que le permite realizar el ataque man in the middle; este consiste en colocarse entre el servidor legítimo y el cliente para poder espiar en todo el tráfico de la red y así poder leer y modificar mensajes entre la comunicación establecida [4].

2.1.4 ATAQUE MAN IN THE MIDDLE

Un cliente malicioso instalando un servidor DHCP falso puede introducirse en el tráfico de la red, este ataque es conocido como “man in the middle”, que le permite al atacante ubicarse en medio de la comunicación de los clientes con el servidor DHCP, es por esto que el podrá ver todos los mensajes que se envíen y de esta manera poder

obtener información de credenciales o modificar paquetes enviados entre los equipos [5].

2.1.5 GNS3

Graphical Network Simulator-3 es un software que permite emular conexiones de red simples y complejas permite la utilización de diferentes dispositivos reales y virtuales para poder configurar y probar un escenario de red [6].

2.1.6 YERSINIA

Yersinia es un software que permite realizar ataques de capa 2 con el fin de descubrir las vulnerabilidades que tienen el diferente protocolo de red y a los riesgos que están expuestos al ejecutar estos ataques.
Yersinia implementa ataques de suplantación e incumplimiento para el protocolo de configuración dinámica de host (DHCP) [7].

2.1.7 ETTERCAP

Ettercap es un software que permite el ataque a diferentes protocolos de red e incluye funciones para el análisis de host y de redes, permite realizar el ataque man in the middle al configurar un servidor DHCP falso y enviarle la dirección ip de la máquina atacante como puerta de enlace para poder filtrarse en el tráfico de la red y poder analizar todos los mensajes que se envían entre equipos [8] [9].

2.1.8 WIRESHARK

Es un software que permite comprobar la comunicación entre los dispositivos en red, su interfaz gráfica es muy amigable y permite de forma fácil analizar los protocolos, y el tráfico de la red; así como también visualizar en tiempo real los paquetes que se envían los dispositivos; lo

que permite capturar los mensajes y evaluar la comunicación de red [10] [11] [12].

2.1.9 SEGURIDAD DE PUERTOS

Para mitigar el ataque DHCP starvation en los Switch cisco se puede configurar una característica de seguridad llamada port-security, su función es asociar las direcciones MAC de los clientes conocidos a cada puerto del switch con el fin de que no se puedan filtrar clientes maliciosos a la red.

El switch guardará la lista de direcciones MAC permitidas en cada puerto y se aplicará el control necesario en caso de que se viole la restricción de seguridad al conectarse un host no conocido, ya sea desactivando el puerto o simplemente no permitiendo que ingrese en la red [13] [14].

2.1.10 DHCP SNOOPING

La función de DHCP snooping es una buena solución para mitigar el ataque de suplantación del servidor DHCP ya que este permite la verificación del servidor legítimo y descarta peticiones de los falsos.

La información de los host legítimos se almacena en una base de datos para verificar que no exista ningún cliente malicioso queriéndose infiltrar en la red [15].

2.2 MARCO METODOLÓGICO

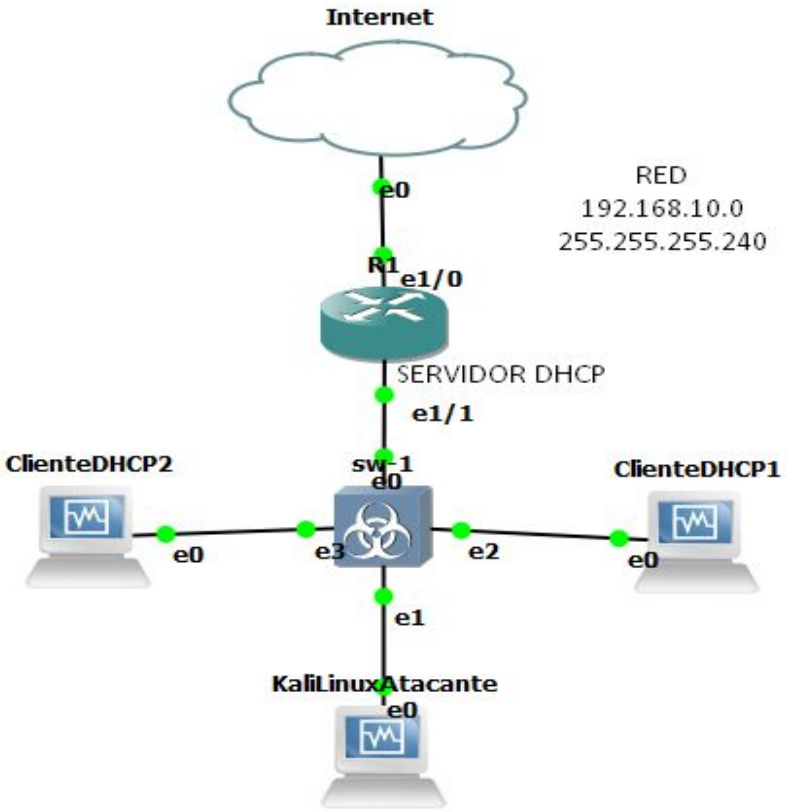
2.2.1 ESCENARIO DE RED

El escenario de red se diseñó en el software de simulación de redes GNS3 donde se utilizó:

- Router cisco 3640: Donde se configurará el servidor DHCP.
- Switch cisco administrable: Donde se configura la seguridad de puertos y el dhcp snooping.

- Computadoras: 2 clientes Windows que solicitarán peticiones al DHCP, 1 cliente en Kali Linux que es el que tiene instalado las herramientas para ejecutar los ataques.

Figura 2. Topología de red



Elaborado por: Fabiola Auz

La red utilizada en la práctica es la 192.168.10.0 con máscara 255.255.255.240 la dirección ip de la puerta de enlace es la 192.168.10.1 que es la que se configuró en el router. El servidor DHCP se configurará en el router y tendrá la capacidad de asignar las 13 direcciones ip restantes de la red proporcionada.

La máquina KaliLinux utilizará otra red ya que funcionará como atacante malicioso que crea un servidor DHCP falso y asigna direcciones ip de la red 192.168.1.0 con máscara 255.255.255.240.

Tabla 1. Direccionamiento ip

Equipo	Dirección ip	Máscara de Subred	Puerta de enlace
Router cisco 3640	192.168.10.1	255.255.255.240	
Cliente DHCP 1	192.168.10.2	255.255.255.240	192.168.10.1
Cliente DHCP 2	192.168.10.3	255.255.255.240	192.168.10.1
KaliLinux Atacante	192.168.10.4	255.255.255.240	192.168.10.1
	192.168.1.1	255.255.255.240	192.168.1.1

Elaborado por: Fabiola Auz

2.2.2 ATAQUE DHCP STARVATION

Se configuró en la topología de red expuesta el protocolo DHCP para que los host obtengan la configuración dinámica proporcionada por el servidor, para ejecutar el ataque se utilizó la herramienta Yersinia que opera sobre el sistema operativo Kali Linux lo que permitió comprobar la vulnerabilidad de seguridad que tiene el servidor DHCP al ataque de incumplimiento.(VER ANEXO A)

2.2.3 ATAQUE DHCP SPOOFING

Se utilizó la misma topología de red para el ataque anterior con la misma configuración del protocolo DHCP, aquí se incluye en el simulador GNS3 salida a la navegación por internet para poder comprobar cómo un atacante se puede filtrar en el tráfico y capturar las credenciales de los clientes que se comunican dentro y fuera de la red LAN. Se utilizó el software Ettercap que opera en el sistema operativo Kali Linux para implementar un servidor DHCP falso que se encargará de realizar las mismas funciones que el servidor legítimo con el fin de colocarse en la mitad de las comunicaciones entre los dispositivos y así analizar todos los mensajes que intercambian pudiendo insertar o robar datos. (VER ANEXO B)

2.2.4 IMPLEMENTACIÓN DE SEGURIDAD DE PUERTOS

La seguridad de puertos se configuró con el fin de permitir que se conecten solo host conocidos y directamente conectados al switch, restringiendo de esta manera que otros dispositivos no autorizados se conecten. (VER ANEXO C)

2.2.5 IMPLEMENTACIÓN DE DHCP SNOOPING

Este control de seguridad se conoce como la inspección DHCP que actúa como un firewall entre clientes no identificados y servidores DHCP legítimos; se crea una lista de direcciones ip con direcciones MAC conocidas en los puertos del switch a los que están conectados los hosts. Está técnica permite establecer cuál es el servidor de confianza y descarta las peticiones de un servidor Falso (VER ANEXO D)

2.3 RESULTADOS

Al ejecutar los ataques DHCP starvation y DHCP snooping se comprueba que el servidor DHCP se encuentra vulnerable a que clientes maliciosos dentro de la misma red local no permitan que entregue correctamente el direccionamiento ip, adicionalmente pueden instalar su propio servidor falso para poder analizar el tráfico de todos los clientes que se encuentran conectados y poder robar su información, credenciales, entre otros datos.

Para reforzar la seguridad en el protocolo DHCP tanto para los clientes como para el servidor se implementaron los controles de seguridad necesarios como son; la seguridad de puertos en el switch donde restringimos todo acceso a la red de equipos maliciosos con MAC falsas o no establecidas por el administrador de la red. Adicionalmente con el control DHCP spoofing configurado en el switch se establece cual es el servidor de confianza para evitar la implantación de servidores falsos; esta tecnología elimina los mensajes del servidor falso para evitar que le asignen la configuración de la red los clientes y espíen en su tráfico.

Con las tecnologías utilizadas se mitigó el riesgo de que los atacantes se filtren en la red y puedan acceder a nuestra información o no permitan que se ejecute con normalidad las funciones del servidor DHCP.

3. CONCLUSIONES

- Se implementaron controles dentro de la red de área local (LAN) reforzando la seguridad y privacidad de los clientes que establecen comunicación entre ellos y su navegación por internet.

- Se diseñó un escenario de red en la herramienta GNS3 que permitió la implementación del protocolo DHCP con su respectivo servidor y clientes

- Sé utilizó las herramientas Yersinia y Ettercap que operan sobre el sistema operativo Kali Linux para ejecutar los ataques DHCP starvation y DHCP spoofing, donde se identificaron los riesgos de seguridad en la red interna a los que está expuesto el protocolo DHCP.

- Se investigó los controles necesarios como son la seguridad de puertos y la tecnología DHCP Snooping, para minimizar los riesgos de que los clientes maliciosos se filtren en la red y trunquen el correcto funcionamiento del servidor.

REFERENCIAS BIBLIOGRÁFICAS

[1] Neminath Hubballi y Nikhil Tripathi, «A Closer Look into DHCP Starvation Attack in Wireless Networks,» *Discipline of computer Science and Engineering, School of Engineering,* 2016.

[2] O. S. Younes, «A secure DHCP protocol to mitigate LAN attacks,» *Journal of Computer and Communications,* vol. 4, pp. 39-50, 2016.

[3] Nikhil Tripathi y Neminath Hubballi, «Detecting Stealth DHCP Starvation Attack using Machine,» *Journal of Computer Virology and Hacking Techniques,* 2017.

[4] Josué Cirilo Cruz, Arturo Zúñiga López, Carlos Avilés Cruz y Juan Villegas Cortez, «ANÁLISIS DE ATAQUES DE RED DEL TIPO DHCP SPOOFING, TCP SYN FLOOD Y PAQUETES MALFORMADOS,» *Pistas Educativas,* vol. 39, nº 128, 2018.

[5] Hardik J Prajapati y Zishan Noorani, «A Survey on ARP Poisoning and Techniques for Detection and Prevention,» *IJARIIE,* vol. 3, nº 6, pp. 594-601, 2017.

[6] Peter Veselý, Vincent Karovič y Vincent Karovič ml., «Tools for modeling exemplary Network Infrastructures,» *Procedia Computer Science,* nº 98, p. 174 – 181, 2016.

[7] Offensive Security Kali Linux, «Kali Tools,» 18 Febrero 2014. [En línea]. Available: https://tools.kali.org/vulnerability-analysis/yersinia. [Último acceso: 15 01 2019].

[8] Todd Vollmer y Milos Manic, «Cyber-Physical System Security with Deceptive Virtual Hosts for Industrial Control Networks,» *IEEE Transactions on Industrial Informatics,* 2014.

[9] D. A. Ana Yacchirena y D. M. Darwin Aguilar, Analysis of attack and protection systems in Wi-Fi wireless networks under the Linux operating system, Sangolquí, Ecuador.: 2016 IEEE International Conference on Automatica, October 2016.

[10] T. K. G. D. D.Deepthi Rani, «TCP Syn Flood Attack Detection And Prevention,» *International Journal of Computer Trends and Technology (IJCTT),* vol. volume 4, nº ISSN: 2231-2803, Oct 2013.

[11] A. J. Acurero Alvares, C. A. Rincon Castro, D. R. Bracho Rincón y H. A. Velasquez Perez, «Uso de IPV6 en la transmisión de voz sobre Frame Relay,» *Multiciencias,* vol. 6, nº 4, pp. 429-433, 2016.

[12] H. T. Narayanan, «Seamless Decoding of Normal And OID Compressed SNMP PDUs - An Enhancement to Wireshark,» *International Conference On modelling, Optimisation And Computing,* pp. 1479-1486, 2012.

[13] E. Ariganello, «REDES CISCO,» de *Guía de estudio para la certificación CCNA Routing y Switching*, Madrid, Ra-Ma, 2016.

[14] M. Husameldin, S. Khaled y I. Youssef, «Mitigation of DHCP starvation attack,» *Computers and Electrical Engineering,* vol. 38, pp. 1115-1128, 2012.

[15] A. S. Salvatore Collora, «A Cisco AVVID solution,» de *Cisco CallManager Best Practices*, Indianapolis, Cisco Press, 2004, pp. 176-177.

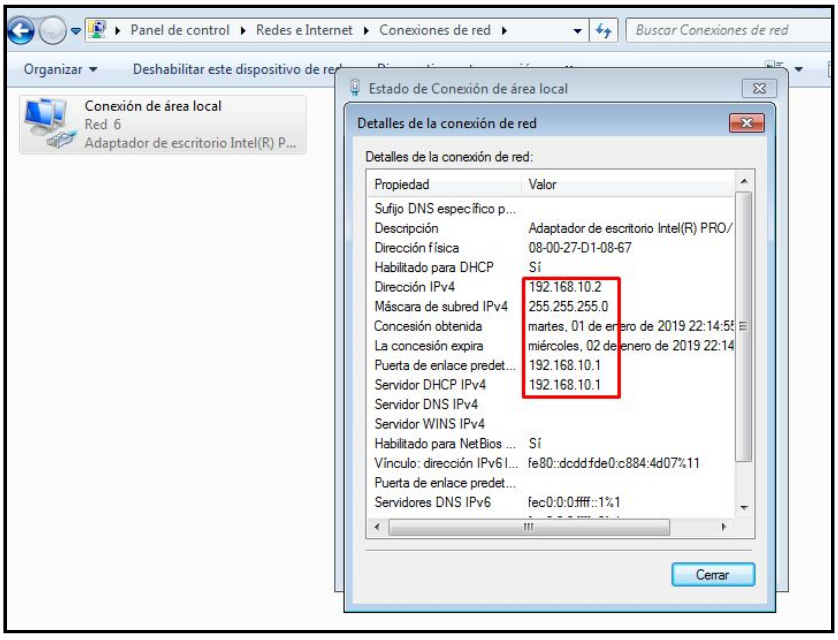
ANEXOS

ANEXO A: ATAQUE DHCP STARVATION

Inicialmente se debe configurar en el router la ip de la interfaz que funcionará como puerta de enlace, posteriormente crear el pool donde se define el rango de direcciones ip que puede asignar a los host clientes, se puede establecer la dirección del servidor dns entre otros parámetros.

Una vez configurado el router como servidor DHCP comprobamos si está entregando direccionamiento ip en cada uno de los host clientes.

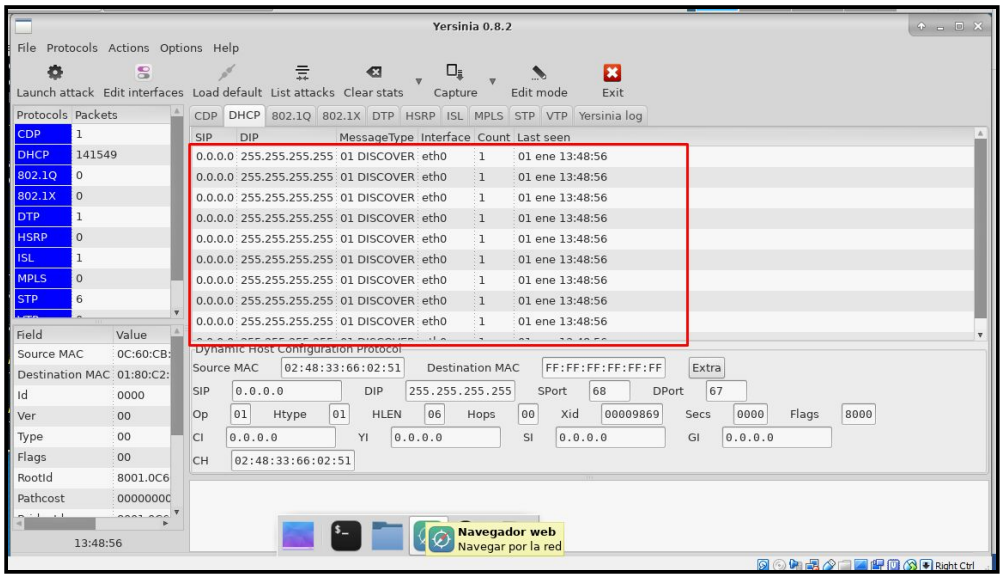
Figura 3. Asignación de direcciones ip en los host clientes.



Elaborado por: Fabiola Auz

Se inicia la máquina en kali Linux y utilizamos la herramienta yersinia para ejecutar el ataque y enviar paquetes DISCOVER que están asociados con direcciones MAC falsas para engañar al servidor DHCP como si fueran clientes que necesitan direcciones ip y de esta manera agotarlas para asignar a los clientes legítimos.

Figura 4. Ejecución del ataque DHCP starvation



Elaborado por: Fabiola Auz

Ingresamos al terminal del router para verificar la tabla del DHCP donde se verifica las direcciones ip que ha asignado a los clientes falsos, cuando sólo debió asignar 3 direcciones ip a los clientes que están conectados según la topología.

Figura 5. Tabla de direcciones ip asignadas en el router

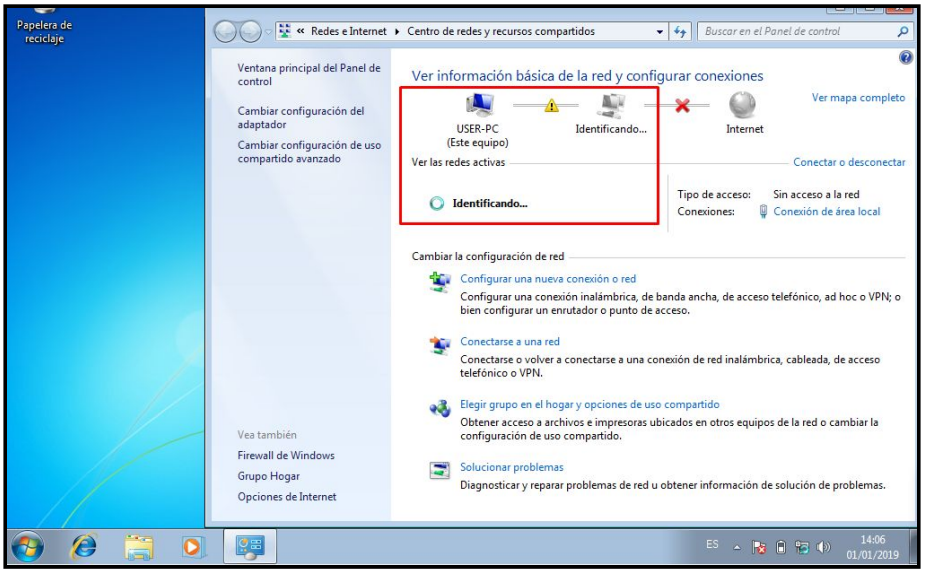
```
R1#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
192.168.10.2        0108.0027.31ae.6c       Mar 02 2002 12:02 AM    Automatic
192.168.10.3        0800.2715.acf8          Mar 02 2002 12:02 AM    Automatic
192.168.10.4        20ec.f224.8663          Mar 01 2002 12:13 AM    Automatic
192.168.10.5        067b.7c3b.7da7          Mar 01 2002 12:13 AM    Automatic
192.168.10.6        10c7.df1d.c9a6          Mar 01 2002 12:13 AM    Automatic
192.168.10.7        b944.f90b.0348          Mar 01 2002 12:13 AM    Automatic
192.168.10.8        754e.f770.fb8c          Mar 01 2002 12:13 AM    Automatic
192.168.10.9        a7ae.9313.5349          Mar 01 2002 12:13 AM    Automatic
192.168.10.10       cb9c.eb3c.7577          Mar 01 2002 12:13 AM    Automatic
192.168.10.11       a8fd.0826.ae6e          Mar 01 2002 12:13 AM    Automatic
192.168.10.12       8336.f032.0ebc          Mar 01 2002 12:13 AM    Automatic
192.168.10.13       f950.2e33.5724          Mar 01 2002 12:13 AM    Automatic
192.168.10.14       a026.4c2f.de3b          Mar 01 2002 12:13 AM    Automatic
192.168.10.15       9007.3d13.e8d6          Mar 01 2002 12:13 AM    Automatic
192.168.10.16       4bec.9c02.89a6          Mar 01 2002 12:13 AM    Automatic
```

Elaborado por: Fabiola Auz

Como se muestra en la figura 5 ya todas las direcciones de la red han sido asignadas, por lo que si otro host se conectará ya el servidor no será capaz de asignarle otra dirección ip,

incluso si un cliente que estaba conectado se desconecta, reinicia o apaga; el servidor no le volverá a proporcionar dirección ip.

Figura 6. Solicitud de dirección ip al servidor DHCP.



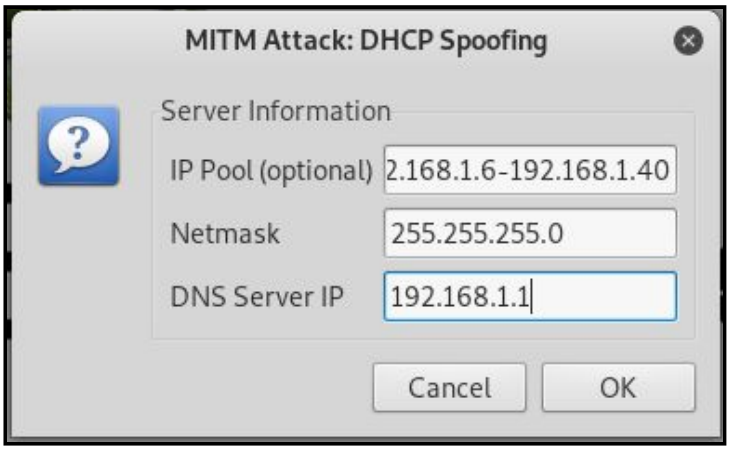
Elaborado por: Fabiola Auz

ANEXO B: ATAQUE DHCP SPOOFING

Se configura en el router el servicio DHCP para que entregue direcciones ip automáticamente a los host clientes, a la computadora que tiene instalado kali Linux y que se utilizará para el ataque se tiene que configurar una ip estática de la red que elegimos en este caso es 192.168.1.1 máscara 255.255.255.0.

Se utilizó el software Ettercap para crear el servidor DHCP falso. Se debe proporcionar los datos de la red falsa en este caso se utilizó el rango de direcciones ip desde la 192.168.1.2 a la 192.168.1.15 indicando la dirección del servidor DNS y puerta de enlace la que se estableció en la máquina KaliLinux, para poder espiar el tráfico en la red.

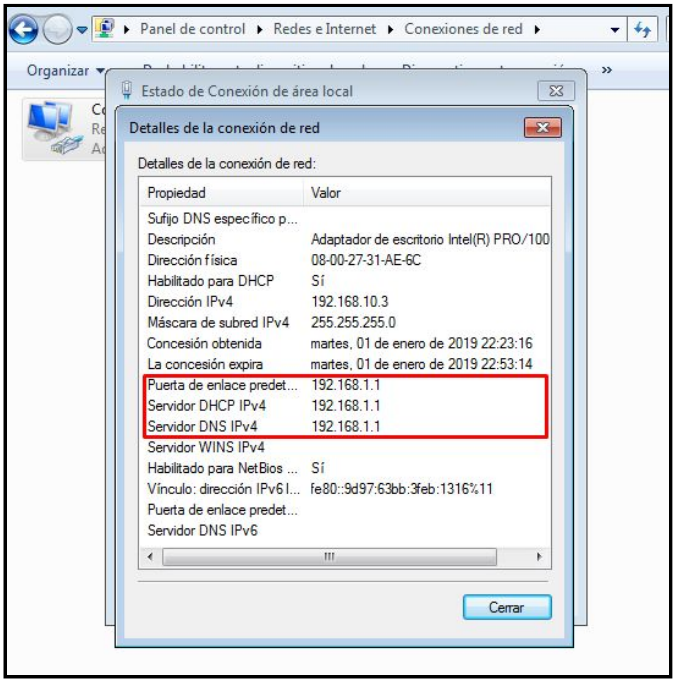
Figura 7. Configurar el servidor DHCP falso en Ettercap.



Elaborado por: Fabiola Auz

Una vez que el atacante implementa su servidor DHCP falso, empezará a engañar a los host clientes que solicitan dirección ip, por lo que les proporcionará una dirección de la red 192.168.1.0 y la puerta de enlace será la del atacante 192.168.1.1 como se muestra en la figura 8.

Figura 8. Detalles de la conexión de red en un host cliente.



Elaborado por: Fabiola Auz

ANEXO C: IMPLEMENTACIÓN DE SEGURIDAD DE PUERTOS

Para cada interfaz del switch se debe configurar la seguridad de puertos conociendo las direcciones MAC de los host legítimos en la red que se conectaran a cada puerto del switch, además se debe establecer que acción debe llevar a cabo en caso de que se intente conectar un host no autorizado.

En cada interfaz del switch se pueden asociar una o varias direcciones MAC para esto se deben definir la cantidad máxima mediante el siguiente comando:

switchport port-security maximum 1

Para que cada interfaz del switch conozca las direcciones MAC que son las autorizadas por el administrador, existen 2 formas de realizarlo:

1. Configurar la dirección MAC manualmente mediante el comando:
   switchport port-security mac-address [DIRECCION-MAC]

2. Configurar de forma dinámica la dirección MAC utilizando el comando:
   switchport port-security mac-address sticky [DIRECCION-MAC].
   Lo que permite es identificar la MAC del host que se conecte inicialmente y lo asociara a ese puerto donde siempre se conectara.

Las acciones que se pueden configurar para que el switch no permita que un host no autorizado o conocido se conecte son las siguientes:

- **Protect:** Al conectar un host con una MAC desconocida el tráfico se descarta, pero no se le notifica al administrador.
- **Restrict:** Funciona de la misma manera que Protect pero con la diferencia que se notifica al administrador mediante SNMP.
- **Shutdown:** El puerto del switch se deshabilita automáticamente si se conecta un host con una dirección MAC que no conoce.

En la figura 9 se muestra la configuración de un puerto seguro para la interfaz GigabitEternet 0/1 que permite solo registrar una dirección MAC, identificándose de manera dinámica al conectarse y si llegara a conectar un host no autorizado deshabilita la interfaz como se muestra en la figura 10.

Figura 9. Configuración de seguridad de puertos.

```
Switch01> enable
Switch01# config terminal
Switch01(config) # interface GigabitEthernet 0/1
Switch01 (config-if) #switchport port-security
Switch01 (config-if) #switchport port-security maximum 1
Switch01 (config-if) # switchport port-security violation shutdown
Switch01 (config-if) # switchport port-security mac-address sticky
Switch01 (config-if) # switchport mode access
```

Elaborado por: Fabiola Auz

Figura 10.Interfaz Gi0/1 deshabilitada por seguridad de puertos.

```
Switch#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
               (Count)       (Count)         (Count)
-----------------------------------------------------------------------------
      Gi0/1             1            1                  1         Shutdown
-----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 4096
```

Elaborado por: Fabiola Auz

ANEXO C: IMPLEMENTACIÓN DEL CONTROL DHCP SNOOPING

En la figura 11 se muestra la configuración en el switch donde se activa el dhcp snooping para la vlan 1 en este caso que se encuentran asociadas todas las interfaces del switch, se podrían incluir todas las vlans necesarias, finalmente se ingresa a la interfaz que está conectada al router y con el comando **ip dhcp snooping trust,** que indica que esta interfaz es la del servidor dhcp confiable.

Figura 11. Configuración de DHCP snooping

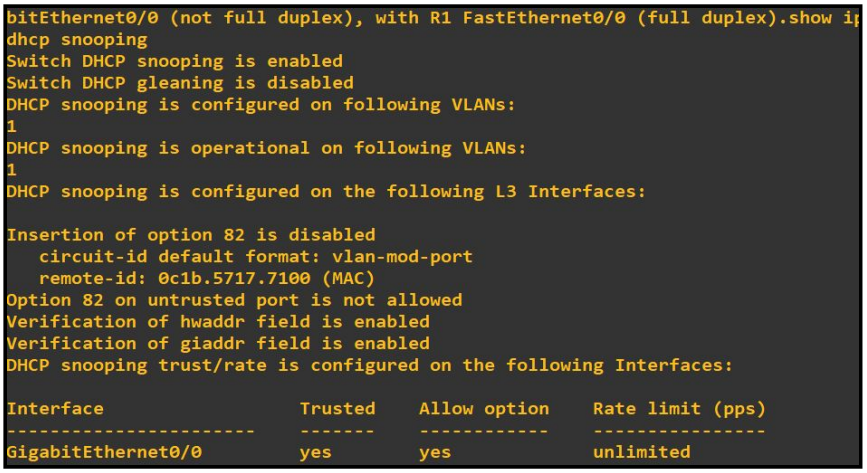
```
Switch01> enable
Switch01# configure terminal
Switch01(config)# ip dhcp snooping
Switch01(config)# ip dhcp snooping vlan 1
Switch01(config)# interface FastEthernet 0/0
Switch01(config-if)# ip dhcp snooping trust
```

Elaborado por: Fabiola Auz

Una vez configurado se activa el DHCP snooping en el router como se muestra en la figura 12 donde indica que está activo para las interfaces asociadas a la vlan 1, con esto se logra

que el ataque DHCP spoofing no tenga lugar, para que los atacantes ingresen un servidor falso dentro de la red.

Figura 12. Activación de DHCP snooping



Elaborado por: Fabiola Auz