ANÁLISIS DE ATAQUES DE RED DEL TIPO DHCP SPOOFING, TCP SYN FLOOD Y PAQUETES MALFORMADOS

Josué Cirilo Cruz

Universidad Autónoma Metropolitana, Azcapotzalco

Ingeniero.josuecc@gmail.com

Arturo Zúñiga López

Universidad Autónoma Metropolitana, Azcapotzalco

azl@azc.uam.mx

Carlos Avilés Cruz

Universidad Autónoma Metropolitana, Azcapotzalco

caviles@azc.uam.mx

Juan Villegas Cortez

Universidad Autónoma Metropolitana, Azcapotzalco

juanvc@azc.uam.mx

Resumen

Hoy en día las compañías, empresas e instituciones almacenan su información en bases de datos que están en alguno de los servidores de su red, y han tenido que abrir el acceso a dicha información para que los usuarios puedan conectarse a ella desde su intranet, esto las hace vulnerables a los ataques de los intrusos. Para detectar estas amenazas, es necesario conocer cómo funcionan, y encontrar patrones característicos que son implementados en tablas de aprendizaje de dispositivos, tales como firewalls, routers, etc., siendo éstas deducidas con base en el análisis del comportamiento del tráfico en la red, teniendo así la conformación de un patrón característico que identifica a la intrusión. En este artículo, se analiza el tráfico circulante en una intranet, con el objetivo de

caracterizar y formar un patrón de rasgos para cada uno de los ataques del tipo DHCP spoofing, TCP SYN flood y de paquetes malformados.

Palabras Claves: Ataques de red, DHCP spoofing, paquetes malformados, seguridad en redes, TCP SYN flood.

Abstract

Nowadays, companies and business offices store their information in databases all over on the servers of their computer networks, and they have had to open the access to this information, so users connected from their intranet, are vulnerable to the attacks of intruders. In order to detect these threats, it is necessary to know how they work, and find the characteristic patterns which are implemented in networking devices, which learn data base tables such as firewalls, routers, etc; the patterns are conformed based on the analysis of the communication traffic behavior. In this article, we analyze the traffic over an intranet in order to of characterize and conform patterns for each DHCP spoofing, TCP SYN flood, and tools which generate simulated attacks using malformed packets.

Keywords**:** *DHCP spoofing, malformed packet, network attacks, network security, TCP SYN flood.*

1. Introducción

En una red de cómputo local bajo el protocolo TCP/IP, se tiene que durante el intercambio de información generado por un equipo fuente (pc-usuario), y un equipo destino (servidor), como se aprecia en la figura 1, ésta es codificada para evitar que personas ajenas a la comunicación tengan acceso a la información o se deniegue el acceso a la misma. Con la introducción de las computadoras y servidores, se hizo evidente la necesidad de disponer de herramientas automatizadas para la protección de los archivos de información almacenadas en estos, la disponibilidad de los servicios ofrecidos por los servidores o la seguridad para realizar alguna actividad entre otras, esto añade un concepto referido en términos de seguridad de redes [Stallings, 2004].

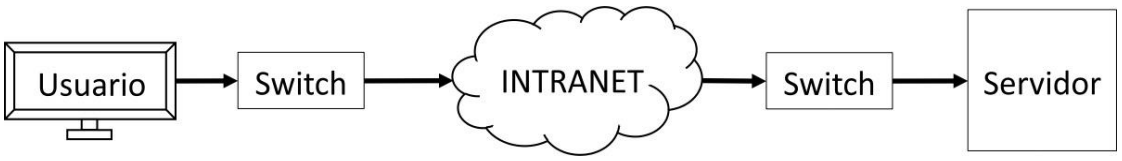

Figura 1 Modelo simplificado de una comunicación entre computadoras.

La seguridad en redes de computadoras, se refiere a cualquier actividad diseñada para proteger la integridad de una red, manteniendo el intercambio de información, libre de riegos y proteger los recursos informáticos de compañías, empresas o escuelas [Cisco, 2017], es por ello que cuando se habla de seguridad en redes se consideran como riesgos los ataques de códigos maliciosos, personas no autorizadas (hackers), denegación de servicios y amenazas combinadas. Un ataque se define como *una secuencia de operaciones que ponen en riesgo la seguridad de un sistema*, y por otro lado una anomalía o amenaza *es una actividad sospechosa desde la perspectiva de la seguridad* [García, 2009]. El modelo simplificado de un ataque a una red se muestra en la figura 2, donde se muestra la comunicación entre dos computadoras y un atacante que realiza operaciones que comprometen la comunicación; los ataques más comunes son enfocados a: la conectividad, la denegación de servicios, el consumo de ancho de banda, etc. Dichos ataques pueden ser mitigados conociendo su funcionamiento, formando así un patrón característico. Este trabajo de investigación se centra en el análisis del tráfico de una intranet en un ambiente simulado para ataques del tipo DHCP spoofing, TCP SYN flood, y paquetes malformados, para conformar patrones característicos que se podrán utilizar en tablas de aprendizaje de equipos de seguridad en redes. En la siguiente sección se explican los detalles de estos conceptos y su finalidad.

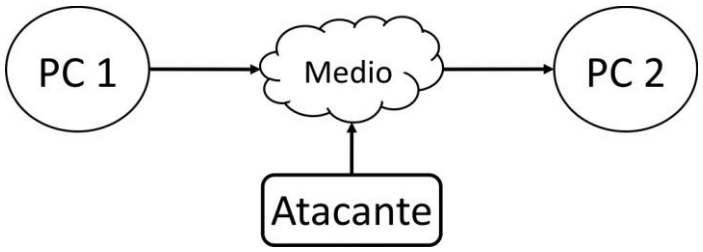

Figura 2 Modelo simplificado de un ataque de red.

DHCP Spoofing

El protocolo DHCP (Dynamic Host Configuration Protocol) es un componente integral para la funcionalidad del protocolo de internet (IP) de las redes actuales. Su función es configurar automáticamente equipos clientes con direcciones IP y algunos otros parámetros relevantes para la red e.g. la máscara de red, la puerta de enlace (Gateway), o los servidores DNS (Domain Name System) [Mukthar, 2012].

Un ataque del tipo DHCP spoofing consiste en capturar mensajes del tipo **DHCPDISCOVER**, esto se logra instalando un servidor falso de DCHP o con un software que emula las mismas funciones, de tal manera que conteste a las peticiones DHCPDISCOVER de los clientes, ver figura 3, dándole parámetros de configuración de tal forma que usurpa funciones, e. g. puede cambiar la dirección de la puerta de enlace (gateway), dando la dirección de él mismo, y realizar un ataque mejor conocido como *Man in the middle,* en el cual un atacante puede leer, insertar y modificar mensajes entre dos usuarios o sistemas [Symantec, 2017].

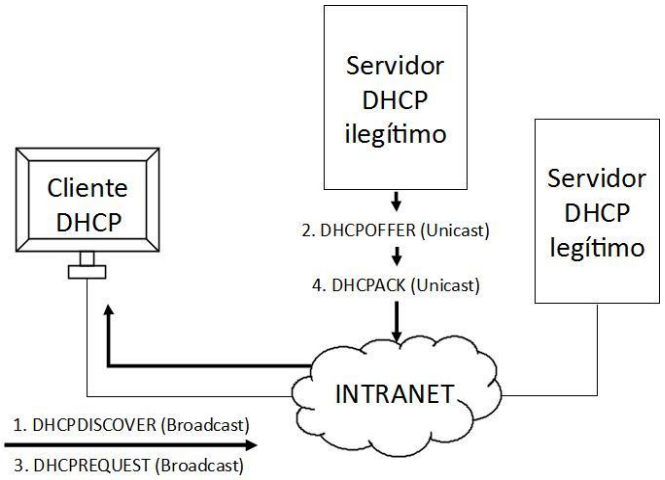

Figura 3 Esquema general del ataque DHCP Spoofing.

TCP SYN flood

El protocolo de control de transporte (TCP) especifica el formato de los datos y de los acuses de recibo usados en la transferencia de datos. TCP, es un protocolo orientado a conexión dado que los participantes en la comunicación deben

establecer una conexión previa, antes de que los datos puedan ser transferidos, realizando el control de flujo, corrección de errores, garantías TCP confiables y la entrega secuencial de los paquetes. Se considera un protocolo confiable porque si se corrompe o se pierde un paquete, TCP pedirá uno nuevo y correcto, hasta recibirlo [Cisco, 2017].

Un ataque TCP SYN flood, es llamado *flood* (Inundación, en español) porque afecta al ancho de banda que es necesario en una comunicación donde fluyen grandes cantidades de paquetes a frecuencias y tamaños significantes, de esta forma saturan las tarjetas de red al grado de detener su funcionamiento. Los ataques TCP SYN flood son diseñados para tomar ventaja de la metodología utilizada por una nueva conexión TCP (ver figura 4). De esta manera el atacante genera falsos paquetes que pretenden establecer una nueva conexión válida (SYN). Estos paquetes son recibidos por el servidor, el cual intenta responder (SYN-ACK), pero nunca es completada una conexión satisfactoriamente, dado que nunca recibe un mensaje de confirmación con la bandera ACK activa por parte del cliente. Esto hace que se agote el número máximo de clientes que el servidor puede atender, logrando la denegación de una nueva solicitud de conexión por parte de un nuevo cliente.

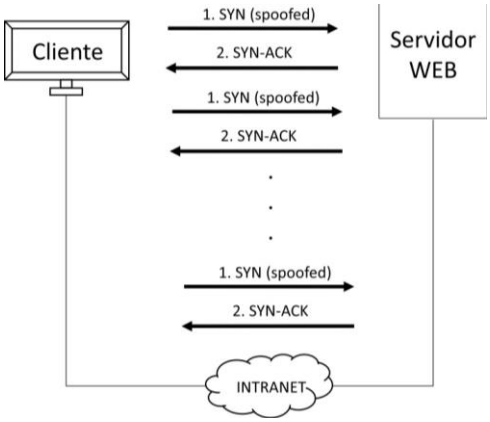

Figura 4 Esquema típico del ataque TCP SYN flood.

Paquetes Malformados

Un disector es un módulo encargado de decodificar convenientemente paquetes de una red, con características establecidas por los protocolos

[Wireshark, 2017], e. g. IP, TCP, DHCP, etc; al hablar sobre paquetes malformados, se refiere a que el disector elegido para fragmentar paquetes de algún protocolo no puede diseccionar correctamente el contenido de éstos [Wireshark, 2017]. Existen cuatro razones por las cuales no se puede diseccionar bien un paquete, estas son:

- **Disector está equivocado:** el sniffer erróneamente ha elegido el disector de protocolo incorrecto para este paquete [Wireshark, 2017].
- **El paquete no se puede rearmar:** El paquete excede los límites del tamaño del fragmento del paquete de red y no se puede reensamblar o rearmar [Wireshark, 2017].
- **El Paquete es incorrecto:** El paquete es realmente malo (tiene una malformación), lo que significa que una parte del paquete no es justo lo que esperábamos (no cumple con las especificaciones del protocolo) [Wireshark, 2017].
- **El disector tiene errores:** El disector del protocolo correspondiente, todavía está incompleto, es decir no es un disector correcto [Wireshark, 2017].

Generalmente un paquete malformado se debe a que es construido sin cumplir las reglas estipuladas por el protocolo en cuestión. Existen distintas formas de realizar ataques con paquetes malformados, comúnmente se suelen utilizar programas (software) que crean paquetes de distintos protocolos e inyectan éstos masivamente a equipos víctimas. Un ataque mediante Paquetes Malformados, es un ataque en el que el atacante puede utilizar múltiples equipos (zombis), a los que ordena enviar paquetes formados incorrectamente al sistema de la víctima con el fin de bloquearlo, e.g. en un ataque de direcciones IP, el paquete contiene las mismas direcciones IP de origen y de destino, esto puede confundir a los sistemas operativos de las víctimas y causar que se bloqueen. Otro ejemplo, es un ataque de opciones de paquetes IP, con ello se pueden asignar al azar los campos opcionales dentro de un paquete IP y establecer todos los bits de calidad de servicio en uno, para que el sistema de la víctima deba utilizar un tiempo de

procesamiento adicional para analizar el tráfico. Si este ataque se multiplica, puede agotar la capacidad de procesamiento de los sistemas de las víctimas [Spech, 2004].

2. Métodos

Para realizar la implementación y el análisis de los ataques propuestos en éste trabajo, se hizo uso de la topología de la intranet mostrada en la figura 5, en ella se simularon 3 subredes: LAN 1, LAN 2 y el resto de la INTRANET. Se implementaron tres servidores: DHCP, SYSLOG y NTP en la LAN 2; y en la LAN 1 se encuentra el equipo atacante, el equipo atacado y el sensor (analizador de protocolos), el cual ayudó a visualizar y detectar eventos y con ello analizar el tráfico circulante en la red. Para analizar el tráfico de la red, se apoyó de los eventos registrados en el servidor SYSLOG y el sensor de captura de tráfico. Por otra parte, para desarrollar la simulación se utilizó el simulador de redes: GNS3 [GNS3, 2017], para emular la topología de la red (routers, switches e integración de las máquinas virtuales), y el software de virtualización: VirtualBox [VirtualBox, 2017] para las emular las máquinas virtuales. Como herramientas de ataques de red se utilizó Ettercap [Ettercap, 2017], para generar el ataque DHCP spoofing, Dsniff [Dsniff, 2017], para el ataque con Paquetes Malformados, y Hping3 [Hping3, 2017], para el ataque TCP SYN flood.

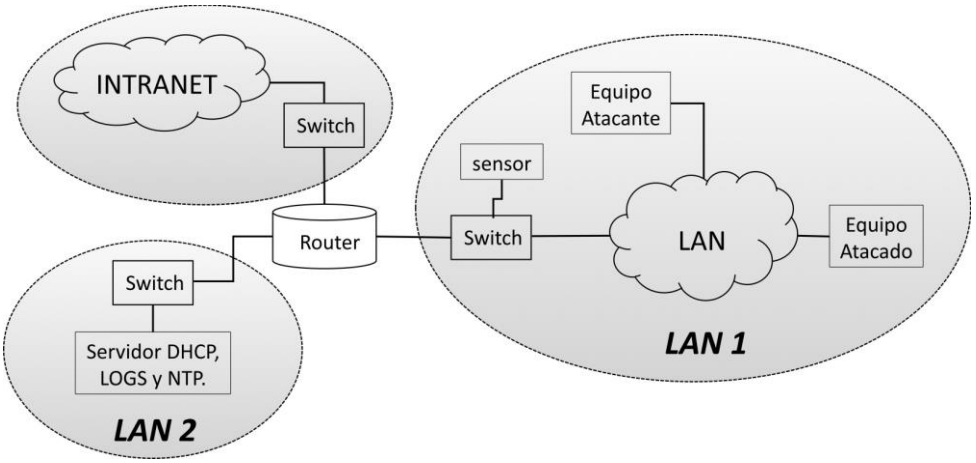

Figura 5 Topología de la intranet.

Implementación del DHCP spoofing

La condición inicial de la maqueta primera de pruebas es, cuando se realiza la asignación de una dirección IP válida por parte del servidor DHCP legitimo a la computadora que posteriormente será ***atacada***. Para ello, si observamos el archivo de registros de salida del servidor SYSLOG, ver figura 6, primero se realiza la liberación de la dirección por parte del cliente (DHCPRELEASE), después éste envía un mensaje DHCPDISCOVER para volver a encontrar al servidor DHCP (con dirección IP: 192.168.2.2), posteriormente el servidor contesta con un mensaje DHCPOFFER ofreciendo la dirección IP: 192.168.1.10 al equipo con MAC-ADDRESS: 08:00:27:12:ed:14 (cliente), y enseguida el cliente contesta con un DHCPREQUEST (en modo unicast, que es contraria a su naturaleza, ver figura 3, aceptando la dirección ofrecida por el servidor, y finalmente el servidor asigna la dirección IP: 192.168.1.10 al equipo con la MAC-ADDRESS: 08:00:27:12:ed:14, mediante el mensaje DHCPACK. Por otro parte, en el cliente se ejecuta un analizador de protocolos, y su salida se muestra en la figura 7, en ella se observa que aparecen los mismos tipos de mensajes que el servidor DHCP genera, en la asignación de una dirección IP, por lo cual se deduce que; con sólo observar el archivo de registros del servidor SYSLOG se tiene la certeza de que se asignaron direcciones IP válidas.

```
Jun  1 14:11:46 ubuntuservidores dhcpd[2265]: DHCPRELEASE of 192.168.1.10 from 08:00:27:12:ed:14 (sha
ow_lite_sp3) via enp0s3 (found)
Jun  1 14:11:52 ubuntuservidores dhcpd[2265]: DHCPDISCOVER from 08:00:27:12:ed:14 via 192.168.1.1
Jun  1 14:11:53 ubuntuservidores dhcpd[2265]: DHCPOFFER on 192.168.1.10 to 08:00:27:12:ed:14 (shadow_
ite_sp3) via 192.168.1.1
Jun  1 14:11:53 ubuntuservidores dhcpd[2265]: DHCPREQUEST for 192.168.1.10 (192.168.2.2) from 08:00:2
:12:ed:14 (shadow_lite_sp3) via 192.168.1.1
Jun  1 14:11:53 ubuntuservidores dhcpd[2265]: DHCPACK on 192.168.1.10 to 08:00:27:12:ed:14 (shadow_li
```

Figura 6 Asignación legitima de una dirección IP, por parte del servidor.

```
  6 7.87324700 192.168.1.10   192.168.2.2     DHCP  342 DHCP Release  - Transaction ID 0xcc1c1cc1
  8 13.6387900 0.0.0.0        255.255.255.255 DHCP  348 DHCP Discover - Transaction ID 0x8c6c7a1e
 10 14.6584870 192.168.1.1    192.168.1.10    DHCP  342 DHCP Offer    - Transaction ID 0x8c6c7a1e
 11 14.6597810 0.0.0.0        255.255.255.255 DHCP  373 DHCP Request  - Transaction ID 0x8c6c7a1e
 13 14.6894500 192.168.1.1    192.168.1.10    DHCP  342 DHCP ACK      - Transaction ID 0x8c6c7a1e
```

Figura 7 Asignación legitima de una dirección IP, en el cliente.

La configuración del servidor DHCP falso se muestra en la figura 8. El ataque se puede realizar en los siguientes casos:

- El equipo atacado realiza una renovación de los parámetros de la red.
- El equipo solicita una nueva dirección IP.
- El equipo se apaga o se reinicia.

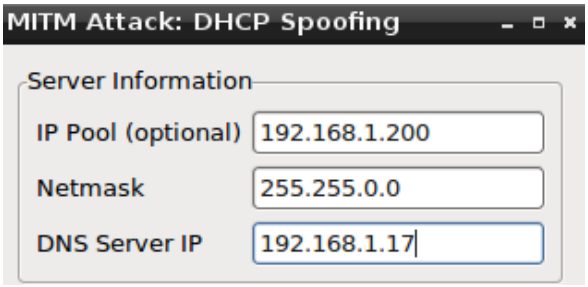

Figura 8 Configuración del falso servidor DHCP.

Es en éstas condiciones donde el ataque puede implementarse. Ahora, si se coloca un analizador de protocolos en la maquina atacante, se observan los mensajes que intercambia con una víctima, ver figura 9. En dicha figura se observa que el atacante responde a mensajes del tipo DHCPDISCOVER y asigna configuraciones similares a los que asigna el DHCP legítimo. De igual manera se observa la suplantación del servidor DHCP, poniéndose como una puerta de enlace válida para el equipo atacado. Para este ejemplo el equipo atacado solicita una nueva dirección IP al servidor DHCP legítimo, pero el falso servidor escucha el mensaje DHCPDISCOVER y responde primero con un DHCPOFFER, adelantándose al servidor legítimo, ofreciendo los parámetros de configuración realizados en la figura 8.

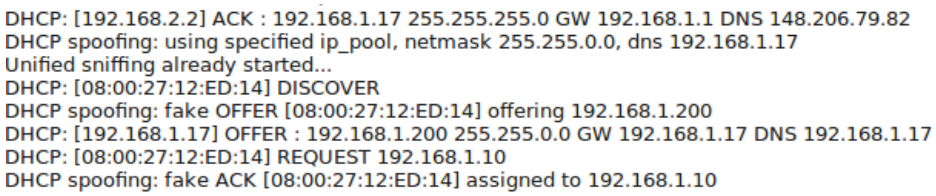

Figura 9 Suplantación del servidor DHCP con Ettercap.

Por consiguiente, en la figura 10, se observa en el equipo cliente que el falso servidor DHCP logró su objetivo y generó un ataque *Man in the middle*, ya que

logró colocarse como puerta de enlace predeterminada y ahora se encuentra en medio de la comunicación entre la computadora cliente y la puerta de enlace.

```
C:\Documents and Settings\Administrador>ipconfig /renew

Configuración IP de Windows

Adaptador Ethernet Conexión de área local 3          :

        Sufijo de conexión específica DNS :
        Dirección IP. . . . . . . . . . . : 192.168.1.10
        Máscara de subred . . . . . . . . : 255.255.0.0
        Puerta de enlace predeterminada   : 192.168.1.17
```

Figura 10 Asignación de parámetros de red del servidor DHCP falso.

Implementación del TCP SYN flood

En la figura 11 se observa el cumplimiento del procedimiento del *Three-Way Handshake*. En dicha figura, el equipo cliente (con dirección IP: 192.168.1.10) solicita una nueva conexión al servidor (con dirección IP: 172.217.7.37), enviando un mensaje con la bandera SYN activada (ver el primer paquete marcado en color negro), posteriormente el servidor responde al cliente con un mensaje con la bandera SYN-ACK activada (ver el segundo paquete marcado en color negro), y finalmente el cliente finaliza el procedimiento enviando un mensaje con la bandera ACK activa al servidor (ver el tercer paquete marcado en color negro). Es importante mencionar que el procedimiento del *Three-Way Handshake*, no se efectúa de manera consecutiva forzosamente.

```
195 78.3942610 192.168.1.10   172.217.7.37     TCP   66 iascontrol-oms > http [SYN] Seq=0
197 78.4054740 192.168.1.10   107.167.110.211  TCP   66 iascontrol > http [SYN] Seq=0 Win
198 78.4090350 192.168.1.10   107.167.110.211  TCP   66 dbcontrol-oms > http [SYN] Seq=0
199 78.4156720 192.168.1.10   172.217.7.37     TCP   66 oracle-oms > http [SYN] Seq=0 Win
207 79.9896690 192.168.1.10   37.228.108.171   TCP   62 olsv > https [SYN] Seq=0 Win=6424
212 81.3630880 192.168.1.10   172.217.7.37     TCP   66 iascontrol-oms > http [SYN] Seq=0
213 81.3631930 192.168.1.10   107.167.110.211  TCP   66 iascontrol > http [SYN] Seq=0 Win
214 81.3632450 192.168.1.10   107.167.110.211  TCP   66 dbcontrol-oms > http [SYN] Seq=0
215 81.3632930 192.168.1.10   172.217.7.37     TCP   66 oracle-oms > http [SYN] Seq=0 Win
216 81.4995140 172.217.7.37   192.168.1.10     TCP   66 http > iascontrol-oms [SYN, ACK]
217 81.4996360 192.168.1.10   172.217.7.37     TCP   54 iascontrol-oms > http [ACK] Seq=1
```

Figura 11 Three Way-Handshake (TCP).

El ataque inicia comúnmente, cuando el equipo atacante envía de manera indefinida, mensajes de tipo TCP con la bandera SYN activa al equipo víctima. En la figura 12, el atacante genera estos mensajes, inundando al servidor (equipo

victima con dirección IP: 192.168.1.10). Es importante mencionar que la generación de estos paquetes es de forma malformada, i.e. los paquetes son construidos con direcciones IP falsas e inválidas, con direcciones IP que no están asignadas en equipos reales o que son direcciones IP del tipo multicast o de clase E (observar el último paquete, con dirección IP: 236.85.33.11 de la figura 13).

```
root@debianatacante:~# hping3 -I eth0 -p 80 --flood -S --rand-source 192.168.1.1
0
HPING 192.168.1.10 (eth0 192.168.1.10): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Figura 12 Implementación de ataque TCP SYN Flood.

```
3020   0.796583 115.224.191.90 -> 192.168.1.10 TCP 54 5347→80 [SYN] Seq=0 Win=512 Len=0
3021   0.796598 213.88.220.152 -> 192.168.1.10 TCP 54 5348→80 [SYN] Seq=0 Win=512 Len=0
3022   0.796614 183.151.26.152 -> 192.168.1.10 TCP 54 5349→80 [SYN] Seq=0 Win=512 Len=0
3023   0.796630 206.99.253.112 -> 192.168.1.10 TCP 54 5350→80 [SYN] Seq=0 Win=512 Len=0
3024   0.796645 149.161.234.208 -> 192.168.1.10 TCP 54 5351→80 [SYN] Seq=0 Win=512 Len=0
3025   0.796661 12.213.38.156 -> 192.168.1.10 TCP 54 5352→80 [SYN] Seq=0 Win=512 Len=0
3026   0.796676 41.145.31.182 -> 192.168.1.10 TCP 54 5353→80 [SYN] Seq=0 Win=512 Len=0
3027   0.796692 222.38.27.167 -> 192.168.1.10 TCP 54 5354→80 [SYN] Seq=0 Win=512 Len=0
3028   0.796707 236.85.33.11 -> 192.168.1.10 TCP 54 5355→80 [SYN] Seq=0 Win=512 Len=0
```

Figura 13 Mensajes TCP con la bandera SYN activa, generados por el atacante.

Implementación de los Paquetes Malformados

En la figura 14 se muestra la implementación de un ataque con paquetes malformados. Como se observa, se implementa una inundación de direcciones MAC al equipo con dirección IP: 192.168.1.10, por parte del equipo atacante con dirección IP 192.168.1.17. Cabe mencionar que este ataque es generado construyendo direcciones MAC falseadas, es decir: inválidas (direcciones MAC de tipo unicast y multicast), y no reales (que no están asignadas a tarjetas de red reales). En la figura 15, se observan estos paquetes clasificados como paquetes malformados, debido a que el analizador de protocolos no los puede diseccionar y las direcciones MAC de origen son inválidas.

```
root@debianatacante:~# macof -i eth0 -s 192.168.1.17 -d 192.168.1.10 -n 10
7f:b9:9b:4:40:44 31:24:f:9:d0:4e 192.168.1.17.61429 > 192.168.1.10.15669: S 2096545159:2096545159(0) win 512
73:4b:b6:1f:78:f8 56:9c:7e:62:2:6e 192.168.1.17.61923 > 192.168.1.10.26690: S 1579647407:1579647407(0) win 512
b4:3:c2:7b:b5:d1 42:7f:fa:2e:95:9 192.168.1.17.23151 > 192.168.1.10.2826: S 515529850:515529850(0) win 512
51:87:5c:74:55:42 79:5c:96:1d:91:94 192.168.1.17.15021 > 192.168.1.10.62491: S 464922677:464922677(0) win 512
64:b:f8:2c:2c:71 5d:88:3b:3f:51:a8 192.168.1.17.44641 > 192.168.1.10.33302: S 2144723376:2144723376(0) win 512
a7:20:e8:59:5a:e0 25:85:68:2:72:ec 192.168.1.17.51356 > 192.168.1.10.26468: S 1697697134:1697697134(0) win 512
46:bf:d3:79:db:60 e3:a6:c5:2a:89:13 192.168.1.17.27621 > 192.168.1.10.19678: S 1236564629:1236564629(0) win 512
5c:d4:d6:3a:59:3e 20:50:4:2c:df:c9 192.168.1.17.45684 > 192.168.1.10.49168: S 49299384:49299384(0) win 512
bd:c4:7f:6c:41:a 67:54:bc:3e:9e:5f 192.168.1.17.35927 > 192.168.1.10.29865: S 1388095085:1388095085(0) win 512
1d:b4:e6:20:b7:80 20:14:3a:5f:a1:9d 192.168.1.17.26651 > 192.168.1.10.9721: S 769800147:769800147(0) win 512
```

Figura 14 Implementación del ataque con paquetes malformados.

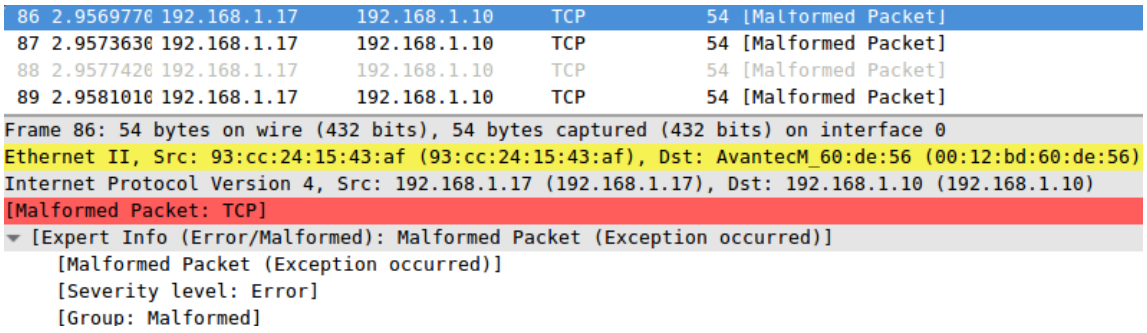

Figura 15 Vista del ataque con paquetes malformados, desde un analizador de protocolos.

3. Resultados

Del ataque DHCP spoofing implementado, se observó que comúnmente para detectar este ataque basta con verificar que la direcciones IP fuente de los mensajes tipo DHCPOFFER y DHCPACK sean del servidor DHCP legítimo. Además, por cuestiones de la topología de la red, ver figura 5, al poner el servidor DHCP en una red diferente en la que están los equipos clientes, e.g. LAN 1, se agrega implícitamente un mecanismo de seguridad ya que se cambia el modo de trabajo del mensaje DHCPREQUEST, ejecutándolo en modalidad unicast, esto se debe a que al colocar el servidor en una red diferente, se forza a que el mensaje DHCPREQUEST trabaje en modalidad unicast, debido a que el dispositivo router no propaga mensajes tipo broadcast, y para poder entregar este mensaje y llevarlo hacia el DHCP legitimo tendrá que forzarlo a trabajar en una comunicación tipo unicast en lugar de una en modalidad broadcast. Así también, se observó que al colocar el servidor DHCP dentro de la misma LAN donde se realizarán los ataques, este es más vulnerable, ya que se puede averiguar su dirección IP y suplantarlo.

Con la implementación de un servidor SYSLOG dentro del servidor DHCP, se dedujo que; se pueden predecir ataques del tipo DHCP “starvation” (Agotamiento de direcciones IP), esto se logra verificando el archivo de registros de eventos que se genera en el servidor con las relaciones de direcciones IP y MAC válidas o asignadas legítimamente, ver figura 16, por lo que podemos predecir y detectar cuando algún intruso se infiltró en la red y está intentando agotar nuestro rango de direcciones IP válidas, al revisar las direcciones MAC del mensaje

DHCPDISCOVER. De igual forma, también se obtiene una relación de direcciones MAC - IP asignadas y válidas, del archivo de registro de eventos.

```
12:32:32 ubuntuservidores dhcpd[2242]: DHCPDISCOVER from 08:00:27:12:ed:14 via 192.168.1.1
12:32:34 ubuntuservidores dhcpd[2242]: DHCPDISCOVER from 08:00:27:c6:de:db via 192.168.1.1
12:33:25 ubuntuservidores dhcpd[2242]: DHCPDISCOVER from 08:00:27:ff:4f:94 via 192.168.1.1
12:34:37 ubuntuservidores dhcpd[2242]: DHCPDISCOVER from 08:00:27:c6:de:db (debianatacante)
12:34:39 ubuntuservidores dhcpd[2242]: DHCPDISCOVER from 08:00:27:c6:de:db via 192.168.1.1
```

Figura 16 Verificación de mensajes DHCPDISCOVER en el servidor DHCP.

Por otra parte, de ataque TCP SYN flood se observó que puede mitigarse con la realización de filtros de paquetes malformados (direcciones IP falseadas y con mensajes TCP con la bandera SYN activa), utilizando un analizador de protocolos. Esto es importante ya que en una tabla de aprendizaje donde son caracterizados patrones intrusivos, entra como una característica a considerar para ser parte de un patrón característico de algún ataque no conocido. De igual manera, se observó en el equipo atacado que cuando está bajo un ataque TCP SYN flood, envía mensajes del protocolo ARP en broadcast intentando contestar los mensajes generados por los paquetes malformados. Por lo que lo hace un comportamiento característico para este ataque, visto del lado del atacado. Otra característica vista en el ataque TCP SYN flood es que: en el equipo atacado, la carga de la CPU, el uso de la memoria RAM y el desempeño de la tarjeta de red se incrementa, por lo que, al intentar ejecutar alguna otra aplicación, el equipo atacado se bloquea.

Por último, del ataque con paquetes malformados se observa que depende del equipo de enlace de datos que se tenga (*switch administrable* y *no administrable*), ya que al inundar con direcciones MAC aleatorias, si el equipo de red es administrable y tiene implementada alguna medida de seguridad, detecta las direcciones MAC inválidas y no las coloca dentro de su tabla CAM y no afecta al servidor. Pero si son direcciones MAC válidas, ver figura 17, son enviadas por el switch al servidor y agota el número máximo de clientes que se pueden atender por parte del servidor; de la misma manera trabajaría un *switch no administrable*. Dado todo lo anterior, se crean tres tablas, tablas 1, donde se describen los patrones característicos de los ataques analizados.

```
f8e0.092c.9c69          Dynamic       1     FastEthernet1/2
006c.b001.2d01          Dynamic       1     FastEthernet1/2
d0cb.3b69.0dfb          Dynamic       1     FastEthernet1/2
54d8.361b.b51b          Dynamic       1     FastEthernet1/2
4c37.8902.d6ea          Dynamic       1     FastEthernet1/2
96ad.9853.4463          Dynamic       1     FastEthernet1/2
78af.7455.288e          Dynamic       1     FastEthernet1/2
6880.8d0b.74b5          Dynamic       1     FastEthernet1/2
```

Figura 17 Tabla CAM bajo un ataque con paquetes malformados.

Tabla 1 Descripción de los ataques.

Tipo de ataque	**Descripción**	**Forma de detección**
DHCP Spoofing	Proviene de una dirección IP obtenida del servidor DHCP legítimo. Utiliza los mensajes DHCPREQUEST, con direcciones IP de tipo broadcast en el campo de destino. Modifica la dirección de la puerta de enlace en el equipo víctima.	Para la topología propuesta, colocando un sniffer, y verificando que los mensajes DHCPREQUEST sean del tipo unicast, no broadcast. Verificar que dirección IP fuente del mensaje DHCPOFFER Y DHCPACK sean del servidor DHCP legítimo.
DHCP Starvation	Agota el rango de direcciones válidas del servidor DHCP. Es generado por equipos que cambian su dirección MAC aleatoriamente (inválidas) y solicitan nuevas direcciones IP.	Se detecta instalando un servidor de logs en el servidor DHCP, y verificando que la dirección MAC del equipo solicitante sea válida. Limitando el rango de direcciones del conjunto válido. Asignación de direcciones IP estáticas.
Paquetes malformados	Es generado con direcciones MAC-ADDRESS e IP aleatorias inválidas e incorrectas (tipo unicast y multicast), caen dentro de la categoría de ser paquetes malformados, por los analizadores de protocolos.	Se verifica que provengan de direcciones MAC e IP válidas. Creación de filtros para verificar la legitimidad de las direcciones MAC e IP en los paquetes entrantes.
TCP SYN Flood	Tienen las banderas SYN o ACK activas dentro del mensaje TCP o están construidas sin tener las banderas TCP activas. Son generados con malformaciones: direcciones IP y MAC inválidas, aunque también pueden ser generados con direcciones IP y MAC válidas. Aumentan la carga del CPU y la tarjeta de red, y el uso de memoria RAM del equipo atacado.	Instalando un servidor de logs dentro del servidor, e. g. WEB, y realizando un aprendizaje supervisado acerca de los mensajes entrantes: con los mensajes TCP con las banderas ACK, SYN activas o sin banderas. Verificar que el Three-Way Handshake se cumpla. Con la creación de filtros de paquetes malformados: revisando que las direcciones IP sean válidas.

4. Discusión

Cuando se utiliza Ettercap como herramienta para implementar un falso servidor DHCP, en el momento de que un equipo solicita una nueva dirección IP, Ettercap averigua su dirección IP anterior, mediante la captura del mensaje DHCPREQUEST, y asigna esa misma dirección IP. Para mitigar este ataque se propone cambiar la manera de comunicación de un mensaje DHCPREQUEST, de tipo broadcast a unicast, esto se logra instalando el servidor DHCP en un segmento de red distinto, al de los equipos restantes de la intranet. Para mitigar variantes de ataques de DHCP, e.g. el DHCP starvation; se instala un servidor SYSLOG para observar, analizar y realizar un control sobre los mensajes DHCPDISCOVER registrados en el servidor DHCP, tomando lapsos de tiempo en minutos y segundos, e. g. mensajes DHCPDISCOVER registrados por minuto.

Un equipo al estar bajo un ataque TCP SYN flood tiene cuatro efectos principales, estos son: la memoria RAM se agota, la carga del CPU se incrementa drásticamente y la tarjeta de red se satura: al enviar mensajes ARP en Broadcast tratando de responder los mensajes recibidos y atendiendo a los nuevos paquetes. Es decir, haciendo que el procesador priorice el procesamiento de cada uno de los paquetes recibidos, a la par de necesitar más memoria RAM para procesarlas. Finalmente, para todos los ataques generados, si el atacante se colocara en otra parte de la intranet, el patrón es muy similar y puede detectarse su comportamiento, solo que, por cada red adicional de la intranet, se debe agregar un sensor para analizar el tráfico circulante de la red.

5. Conclusiones

En este trabajo hemos presentado una investigación sobre algunos de los ataques más frecuentes en una red tipo intranet, que puede comprometer la seguridad de la misma, tanto en la información que comparte como en la operación hacia los nodos de la red. Hemos presentado una metodología para conformar la plataforma de simulación de los ataques y hemos hecho uso de las herramientas más comunes para generar este tipo de ataques. Podemos finalmente emitir una mejor valoración de la seguridad y estado de funcionamiento

de la red interna, intranet y proporcionar una recomendación para una auditoría a bajo nivel, gracias a nuestra metodología. Más aún, en la creación de reglas de seguridad o medidas de implementación para poder mitigar este tipo de ataques.

A futuro será necesario implementar estos patrones encontrados en tablas de aprendizaje, para poder robustecer y agregar nuevas características más relevantes, ya que estos ataques suelen volverse más complejos en su programación y más sofisticados en su implementación. Así también, podremos incluir otro tipo de ataques o variantes de éstos, todo para conocer mejor el estado de la seguridad de una intranet y mejorarla dinámicamente acorde a las nuevas amenazas para la seguridad de una red de cómputo.

6. Bibliografía y Referencias

[1] Cisco, Configurar el protocolo TCP. http://www.cisco.com/cisco/web /support/LA/111/1116/1116270_iap-tcp.pdf, 25 de mayo de 2017.

[2] Cisco, What Is Network Security? http://www.cisco.com /c/en/us/products/ security/what-is-network-security.html, 08 de marzo de 2017.

[3] Dsniff, https://www.monkey.org/~dugsong/dsniff/, 05 de junio de 2017.

[4] Ettercap, https://ettercap.github.io/ettercap/, 05 de junio de 2017.

[5] García P., Díaz J., Maciá G., Vázquez E., Anomaly-based network intrusion detection Techniques, systems and challenges, Computers and Security 28, Elsevier, pp. 18-28, 2009.

[6] GNS3, https://www.gns3.com/, 05 de junio de 2017.

[7] Hping, http://www.hping.org/manpage.html, 05 de junio de 2017.

[8] Mathworks, Supervised Learning. https://www.mathworks.com /discovery/supervised-learning.html, 23 de mayo de 2017.

[9] Montero G. Implementación de un NIDS en un sistema embebido para el análisis de tráfico de una red. Proyecto Tecnológico. UAM, CBI, Departamento de Sistemas, Ingeniería en Computación, 2014.

[10] Mukhtar H.,Salah K., Iraqui Y. Mitigation of DHCP starvation attack, Computers and Electrical Engineering 38, Elsevier, pp. 1115-1128, 2012.

[11] Oracle, Establecimiento de una conexión TCP. https://docs.oracle.com/cd/E19957-01/820-2981/ipov-36/index.html, 24 de mayo de 2017.

[12] Spech S., Lee R., Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures. Proceedings of the 17th International Conference on Parallel and Distributed Computing Systems, 2004 International Workshop on Security in Parallel and Distributed Systems, pp. 543-550, September 2004.

[13] Stallings W., Fundamentos de Seguridad en Redes: Aplicaciones y Estándares, Pearson-Prentice Hall, Segunda Edición, 2004.

[14] Symantec, Man-in-the-middle attack (ataque de tipo "Man in the middle"). https://www.symantec.com/es/mx/security_response/glossary/define.jsp?Letter=m&word=man-in-the-middle-attack, 24 de mayo de 2017.

[15] VirtualBox, https://www.virtualbox.org/, 05 de junio de 2017.

[16] Wireshark, Malformed Packet. https://www.wireshark.org/docs/wsug _html_chunked/AppMessages.html, 24 de mayo de 2017.

[17] Wireshark, Packet dissection. https://www.wireshark.org/docs/wsdg_html_chunked/ChapterDissection.html#ChDissectWorks, 30 de mayo de 2017.