Detección y mitigación de ataques ARP Spoof empleando entornos virtualizados

Marcia Cordero, Myriam Viñamagua y Carlos Garzón
Departamento de Ciencias de la Computación, Programa de Maestría en Gerencia de Sistemas, Universidad de las Fuerzas Armadas –ESPE, Sangolquí, Ecuador
marciveth@gmail.com, myriamv83@gmail.com, carloscfga@hotmail.com

***Abstract*—Los ataques ARP Spoof tienen como finalidad infiltrarse en una red mediante el envío de ARP (Protocolo de Resolución de Direcciones) falsos al bus Ethernet para explorar paquetes de datos, alterar el tráfico o incluso detenerlo. La presente investigación se enfoca en la evaluación del ataque ARP Spoof (sniffer), utilizando como plataforma de experimentación un entorno virtual de red que permite identificar cómo actúa dicho ataque cuando un cliente accede a páginas Web publicadas en un servidor; para llevar a cabo la investigación se diseñó e implementó una red híbrida con delimitación WAN, LAN y DMZ (Zona Desmilitarizada). La herramienta evaluada fue BetterCAP la cual se especializa en este tipo de ataques. Para validar está investigación se desarrolló un mecanismo de detección y mitigación de los ataques a nivel de Shell script. Finalmente, se evaluó el número de paquetes de entrada al atacante cuando éste actúa en modo sniffer.**

Palabras clave: Arp Spoof, BetterCAP, GNS3, VMWare, Virtualización

I. INTRODUCCIÓN

Un ataque de ARP Spoof tiene como objetivo infiltrarse en una red mediante el envió de ARP falsos al bus Ethernet con la finalidad de asociar la MAC del atacante con la dirección IP de otro nodo de confianza como por ejemplo el Gateway para explorar el paquete de datos, alterar o detener el tráfico. En la presente investigación se seleccionó el ataque ARP Spoof, que envía ataques ARP falsos al bus Ethernet y provoca que el atacante husmee el tráfico de red de la máquina atacada con el propósito de obtener información sensible, como por ejemplo nombres de usuario, contraseñas, cookies, mensajes de correo, mensajería instantánea, conversaciones VoIP, etc. El uso de registros ARP estáticos permite mitigar los ataques ARP Spoof.

En este contexto, la comunidad científica ha realizado investigaciones para mitigar los ataques a redes utilizando las tecnologías de virtualización de acuerdo con el monitoreo e identificación de ataques de redes [1]. Bajo esta guía, el modelo propuesto por F. J. Díaz Jiménez y J.G. Palacio Velásquez [2], indica claramente la disección de un ataque MITM (Man in the Middle) mediante ARPSpoofing y técnicas de protección. Adicionalmente los investigadores Melgar Jara [3] y Cazar Jácome, D. A. [4] desarrollan aplicaciones para detección de ataques en redes IPv4/IPv6 y en específico análisis de IP Spoofing. En [5] Herrera Figueroa y Helmuth Lenin los investigadores realizan un ataque a redes IP en un entorno corporativo real. En este mismo ámbito [6], [7], han utilizado sistemas virtualizados y estudios comparativos de sistemas de virtualización y de seguridad. Otros investigadores Echeverry Parada, J. S. [8], [9], [10] utilizaron metodologías para el diagnóstico continuo de las redes informáticas, análisis forenses a paquetes de datos todo esto en redes LAN de instituciones públicas y privadas.

El presente trabajo se enfoca en la evaluación del ataque ARP Spoof, utilizando como plataforma de experimentación un entorno virtual de red que permita identificar cómo actúa dicho ataque y cuál sería su impacto. Para llevarlo a cabo se diseñó e implementó una red con delimitación WAN, LAN y DMZ, con el fin de que el experimento sea lo más cercano a un entorno real en la topología se utilizó el Firewall Cisco 5520 sobre GNS3 el mismo que además de realizar funciones propias de un cortafuegos actúa como enrutador de los segmentos de red con ello los equipos clientes tienen la posibilidad de acceder tanto a servidores como salir hacia una red externa como Internet. La herramienta evaluada fue BetterCAP instalada sobre un ambiente Linux. Para validar está investigación se desarrolló un mecanismo de detección y mitigación de los ataques utilizando Shell scripts

Entre las principales contribuciones de esta investigación se tiene: i) la evaluación de ataques ARP Spoof mediante la herramienta BetterCAP para determinar el impacto en la red y ii) creación de scripts de detección y mitigación de este ataque.

El documento ha sido organizado como sigue: el capítulo 2 presenta el fundamento teórico; en el 3 se describe el diseño y configuración del experimento, topología de la red y los scripts de detección y mitigación; en el 4 se presenta la evaluación de resultados y discusión; en el 5 se presentan los trabajos relacionados y en el 6 se establecen las conclusiones y se señala el trabajo futuro.

II. MARCO TEÓRICO

A. GNS3

Es un simulador gráfico de red para diseño de topologías complejas y realización de simulaciones sobre ellas. En esta herramienta libre de simulación se puede cargar cualquier sistema operativo de enrutadores y se puede ejecutar cualquier tipo de configuración simple o compleja como si se estuviese trabajando en un equipo real. [16]

Para permitir completar simulaciones, GNS3 está estrechamente vinculada con: i) Dynamips, un emulador de IOS que permite a los usuarios ejecutar binarios imágenes IOS de Cisco Systems; ii) Dynagen, un front-end basado en texto para Dynamips; iii) Qemu y VirtualBox, para permitir utilizar máquinas virtuales como un firewall PIX; iv) VPCS, un emulador de PC con funciones básicas de networking; v) IOU (IOS on Unix), compilaciones especiales de IOS provistas por Cisco para correr directamente en sistemas UNIX y derivados. [17]

B. ARP Spoof

ARP SPOOF es un método usado para infiltrarse en una red Ethernet conmutada, que permite al atacante explorar paquetes de datos, alterar el tráfico, o incluso detenerlo. Esta

técnica tiene como principio enviar mensajes ARP falsos al bus Ethernet con la finalidad de asociar la MAC del atacante con la dirección IP de otro nodo de confianza como por ejemplo el Gateway. El principio del ARP Spoofing es enviar mensajes ARP falsos (falsificados, o spoofed) a la Ethernet. [18]

El ataque de ARP Spoofing puede ser ejecutado desde una máquina controlada (el atacante ha conseguido previamente hacerse con el control de la misma: intrusión), o bien la máquina del atacante está conectada directamente a la LAN Ethernet.

C. BetterCAP

BetterCAP es una poderosa herramienta para realizar diversos tipos de ataques "Hombre en el medio" contra la red, manipular tráfico HTTP y HTTPS en tiempo real y mucho más. [15]

Analizando las características principales de esta herramienta se puede encontrar con un sniffer desarrollado especialmente para centrarse en el siguiente tipo de tráfico: páginas web visitadas capturando las direcciones URL, páginas web seguras HTTPS que se visitan, los datos POST de las conexiones HTTP, autenticaciones HTTP, recopila los credenciales de las conexiones FTP, recopila los credenciales de las conexiones IRC, captura y recopila los credenciales de las conexiones de correo electrónico POP, IMAP y SMTP, detecta y recopila los credenciales de las conexiones NTLM como HTTP, SMB, LDAP, etc.

III. CONFIGURACIÓN DEL EXPERIMENTO

A. Herramientas

Para la implementación del experimento se ha planteado una arquitectura basada en herramientas de virtualización y de simulación para los equipos de comunicaciones, además de herramientas de software libre las cuales se detallan a continuación:

1) *Sistema de Virtualización:* Como sistema de virtualización se utilizó VMware Workstation 12 Pro [11] sobre Windows 10, con el fin de instalar y configurar tanto clientes como servidores.

2) *Simulador de equipos de comunicaciones:* A fin de disponer de equipos de comunicaciones lo más cercanos a los físicos se utilizó GNS3 [12] que es un software de simulación de red que permite diseñar topologías de red complejas y poner en marcha simulaciones sobre ellos.

3) *Firewall: S*e implementó sobre GNS3 un firewall de marca Cisco, modelo 5520 [13], el cual es diseñado para empresas pequeñas y posee características de: alta disponibilidad, IPSec, SSL VPN y la posibilidad de añadir funciones de prevención de intrusos (IPS) y anti-X. En el mismo se establecieron tres zonas de seguridad (inside, outside y dmz). La conexión SSH fue habilitada para permitir la gestión del equipo.

4) *Web Server:* Como servidor Web se utilizó Apache [14] sobre Centos 6 a fin de brindar páginas Web solicitadas por clientes que utilizan navegadores Web.

5) *Herramienta de inyección de ataques ARP Spoof:* Como herramienta para realizar el ataque se utilizó BetterCAP [15] funcionando sobre Linux. Esta misma herramienta permite capturar el tráfico obtenido cuando se efectúa el ataque con opciones de exportar el tráfico a archivos pcap.

B. Diseño de la topología experimental

A fin que el experimento sea lo más cercano a un entorno real se requirió la creación de una infraestructura de red con los elementos y esquemas base que se puede encontrar en cualquier red de un entorno de producción. Por lo que, para la implementación de la topología se utilizó el Firewall Cisco 5520 sobre GNS3 el mismo que además de realizar funciones propias de un cortafuegos actúa como enrutador de los segmentos de red (inside, outside y dmz), con ello los equipos clientes tienen la posibilidad de acceder tanto a servidores como salir hacia una red externa como Internet, un computador con Windows 10 con el correspondiente hipervisor que permitió la creación de las máquinas virtuales tanto cliente, cliente-atacante y servidor Web. El esquema de la arquitectura implementada se muestra en la Fig. 1.

C. Configuración de Servidores y Clientes

El esquema planteado se implementó y ejecutó en el equipo anfitrión con VMware y GNS3, el mismo dispone de procesador Core i7, memoria RAM de 8 GB y almacenamiento de 500 GB. Para el servidor Web se utilizó una máquina virtual de un procesador y 512 MB de memoria RAM con Centos 6 y Apache 2 con dos páginas Web de prueba publicadas, para el cliente (víctima) se configuró una máquina virtual con un procesador y 512 MB de memoria RAM con Centos 6 y para el cliente (atacante) se configuró una máquina virtual con un procesador y 512 MB de memoria RAM con Kali Linux y el software BetterCAP para realizar los ataques.

D. Configuración del Firewall Cisco ASA 5520

Para la puesta en funcionamiento del Firewall Cisco ASA 5520 es necesario: i) Disponer de la imagen del IOS; ii) Cargar la imagen al software GNS3; iii) Configurar los parámetros de número de procesadores, memoria RAM, disco duro y iv) La configuración del equipo el cual permita cumplir su cometido. En la Fig. 2 se muestra la ventana de configuración de GNS3 para el Firewall Cisco ASA 5520.

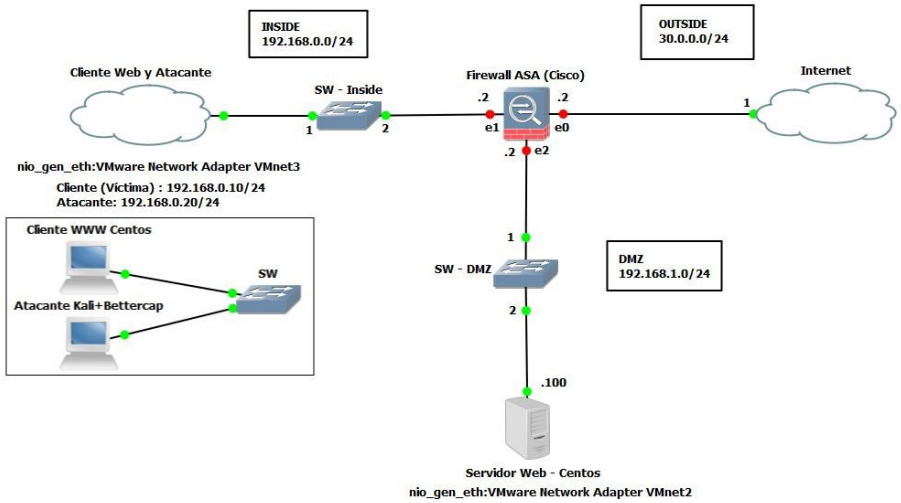

Figure 1. Configuración de Firewall en GNS3

Como parte de la configuración lógica del equipo se crearon los segmentos de la red y reglas que permiten dirigir los paquetes de acuerdo a las solicitudes, por ejemplo: un cliente en la LAN que solicita acceder al servidor Web, sus solicitudes son redirigidas por el Firewall hacia la DMZ donde se encuentra dicho servidor y viceversa, de igual manera existen reglas que permiten únicamente las peticiones hacia el puerto tcp/80 (http) en el cual se ejecuta el servicio Web en conjunto con la respectiva regla NAT que permite redirigir los paquetes de este servidor en función de donde provienen las solicitudes. A continuación, se muestra la interface, puerto y descripción de lo configurado en el dispositivo tal como se muestra en la Fig. 1:

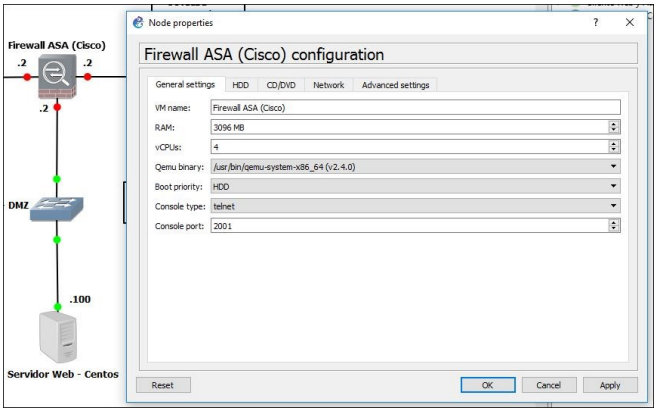

Figure 2. Configuración de Firewall en GNS3

- Interface "GigabitEthernet 0/0": Interface conectada directamente a la red externa (outside) WAN, con red 30.0.0.0/24.
- Interface "GigabitEthernet 0/1": Interface conectada directamente a la red interna (inside) LAN, con red 192.168.0.0/24.
- Interface "GigabirEthernet 0/2": Interface conectada directamente a la red DMZ, con red 192.168.1.0/24.

E. Implementación de la plataforma experimental

Para la implementación de este experimento se ha utilizado el siguiente procedimiento: i) En primer lugar, se ha creado en VMware el servidor Web para lo cual se instaló Centos 6 y el servidor Apache2; ii) Se creó la segunda máquina virtual, el cliente, con Centos 6 habilitado el entorno gráfico con el fin de poder utilizar el navegador Web integrado para acceder a las páginas publicadas en el servidor Web; iii) Posteriormente, se creó la tercera máquina virtual, el atacante, con Kali Linux y se instaló la herramienta BetterCAP para generar los ataques; iv) Cada una de las máquinas virtuales han sido configuradas en redes virtuales distintas para separar el tráfico de cada uno de los segmentos de red; v) En GNS3, se ha creado un nuevo proyecto y se ha importado cada una de las máquinas virtuales de VMware, además se habilitó el Firewall con las respetivas configuraciones descritas anteriormente, por medio de switches se ha interconectado todos los clientes hacia el Firewall.

De acuerdo al procedimiento descrito anteriormente se puede evidenciar que el software GNS3 se convierte en la base para este experimento debido a que controla tanto los equipos de conectividad como las máquinas virtuales, obteniendo como beneficio la posibilidad de iniciar, pausar o detener el experimento y evitar la saturación de los recursos del computador anfitrión.

F. Generación de Ataques

La generación de ataques ARP Spoof se realizó ejecutando la aplicación BetterCAP en la máquina atacante con Kali Linux desde la LAN hacia la víctima que solicita páginas Web al servidor ubicado en la DMZ. Para generar un ataque, la herramienta posee varias opciones, sin embargo, se utilizó la opción que permite capturar el tráfico http que se genere cuando la víctima solicite las páginas Web al servidor. En la Fig. 3 se muestra la pantalla donde se muestra el funcionamiento del software al realizar un ataque.

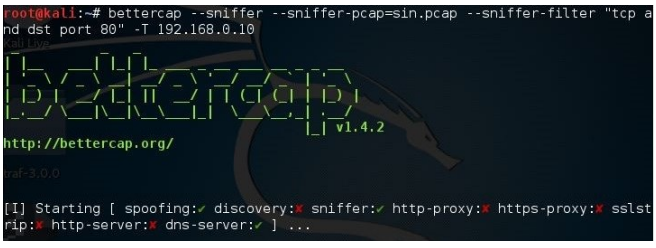

Figure 3. Funcionamiento de BetterCAP

Este tipo de ataques se ejecutan añadiendo un registro extra en la tabla ARP de la víctima a fin que todo el tráfico generado aparte de ir por la puerta de enlace al destino, lo envía al equipo atacante. Este tráfico capturado se evidenció comprobando la cantidad de información recibida a través de la consola de la propia aplicación la cual permite esta funcionalidad o enviando estos paquetes a un archivo pcap para su posterior análisis en aplicaciones como Wireshark y Ethereal.

G. Algoritmo que detecta el ataque ARP Spoof

A diferencia de otros tipos de ataques como los de denegación de servicio en los cuales al momento de iniciarse en el equipo víctima se puede observar claramente saturación de los recursos como procesamiento, memoria RAM, número de paquetes recibidos, etc., lo que a simple vista da la impresión al usuario que algo está sucediendo en su computador y genera una alerta, en los ataques de ARP Spoof no se produce saturación, si se conociera a ciencia cierta que es víctima de ataque, la única forma de detectar es observando los registros de la tabla ARP e identificar que existe un registro de direcciones MAC duplicados con distintas direcciones IP. Es decir, que el tráfico generado por el cliente irá hacia la puerta de enlace y hacia la máquina atacante.

De acuerdo a lo anteriormente mencionado, para poder realizar la detección oportuna de este tipo de ataques se ha diseñado un script de Linux el cual hace un análisis de la tabla ARP a fin de detectar la intrusión. En la Fig. 4 se muestra el diagrama de flujo de este algoritmo.

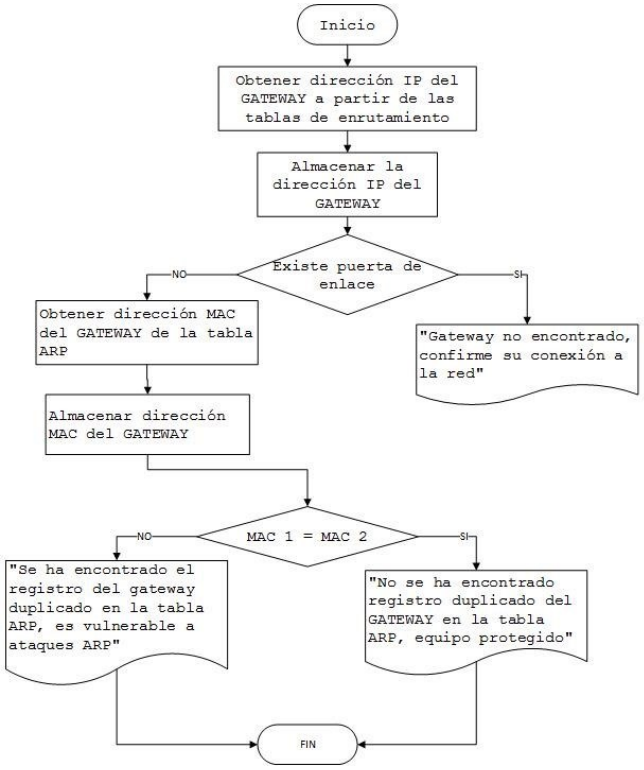

Figure 4. Flujo del proceso de detección de ataque

H. Algoritmo que mitiga el ataque ARP Spoof

Ante una inminente amenaza de un ataque ARP Spoof es necesario tomar acciones inmediatas debido a que el atacante es capaz de ver todo el tráfico de la víctima, es decir podría ser capaz en el caso de un ataque hacia el tráfico http, identificar claves, páginas accedidas, palabras más buscadas, etc. Para ello, se ha diseñado un algoritmo que mitiga la amenaza basándose en el principio básico de la creación de registros estáticos en la tabla ARP, es decir que en el cliente se registrara la dirección IP y la MAC de la puerta de enlace, con ello a pesar que el atacante intente realizar la duplicación del registro del Gateway en la tabla ARP, la víctima siempre enviará el tráfico hacia la dirección IP del registro estático creado, con ello se bloquea todo envío de tráfico hacia otro destino.

Para ejecutar lo anteriormente descrito, se ha diseñado un script de Linux el cual confirma tanto la dirección IP y MAC real del Gateway y con esos datos crea el registro estático en la tabla ARP. En la Fig. 5 se muestra el diagrama de flujo de este algoritmo.

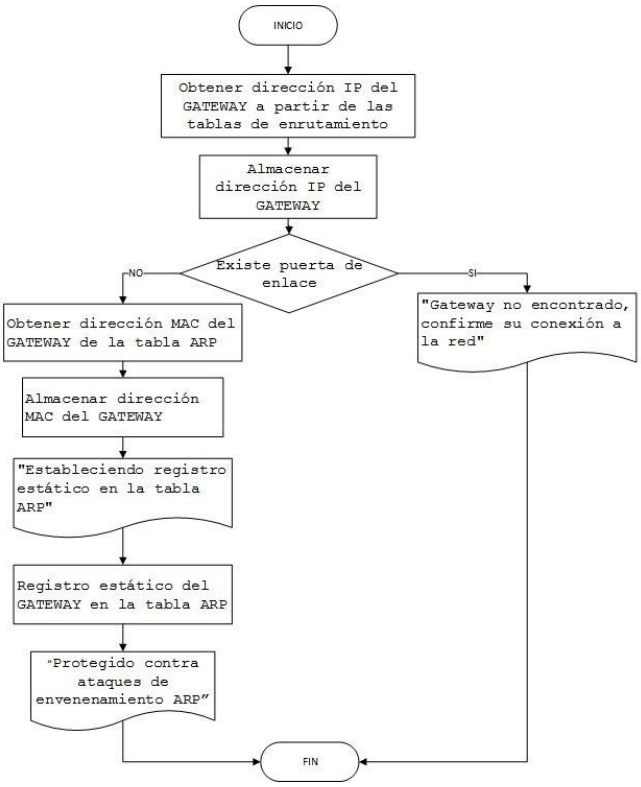

Figure 5. Flujo del proceso de mitigación de ataque

IV. EVALUACIÓN DE RESULTADOS Y DISCUSIÓN

A. Evaluación de resultados, línea base (ataque)

Tal como se explicó en secciones anteriores, este experimento se enfoca en la detección y mitigación de ataques ARP Spoof, para ello, a fin de evaluar el resultado de la mitigación diseñada se planteó una prueba en la cual la máquina atacante intercepta los paquetes de un cliente que solicita páginas Web a un servidor. La efectividad del algoritmo diseñado se midió en términos del número de paquetes capturados en el atacante, para lo cual se configuró la herramienta para que envíe todo el tráfico capturado a un archivo pcap y como segunda forma de verificación se observó la salida de la consola de la aplicación.

El procedimiento inicia detectado que equipos se encuentran activos en la red, luego se inicia el ataque hacia la máquina víctima, en esta etapa BetterCAP muestra en su consola las direcciones IP y MAC del Gateway de la víctima para posterior con esta información proceder a agregar el registro en la tabla MAC de la víctima la cual permita que el tráfico generado además ir por el Gateway predeterminado vaya a la máquina atacante. Luego, en la máquina cliente se evidencia en la tabla MAC que existe un registro duplicado, es decir, existe dos direccione IP con una misma dirección MAC. En la Fig. 6 se muestra la duplicidad existente luego de efectuado el ataque.

```
[root@centosCG Escritorio]# arp -n
Address                  HWtype  HWaddress           Flags Mask
192.168.0.2              ether   00:0c:29:71:d9:c0   C
192.168.0.20             ether   00:0c:29:71:d9:c0   C
```

Figure 6. Duplicidad de dirección MAC

A este punto del experimento el atacante es capaz de aplicar todas las opciones de ataque derivados del ARP Spoof, para este experimento en particular se realizó la prueba capturando el tráfico http de la víctima y enviado el mismo a un archivo pcap, para ello desde el cliente se realizó la descarga de un archivo de 35 MB desde el servidor Web y se midió el número de paquetes en el archivo pcap. En la Fig. 7 se muestra el número de paquetes capturados en el intervalo de tiempo que duró la descarga.

Figure 7. Número de paquetes capturados durante el ataque

Además, la consola de la aplicación BetterCAP muestra que se ha solicitado una descarga y lo muestra en pantalla. En la Fig. 8 se muestra la salida de la consola.

```
root@kali:~# bettercap --sniffer --sniffer-pcap=traficoc.pcap --sniffer-filter "
tcp and dst port 80" -T 192.168.0.10
                                              |_| v1.4.2
http://bettercap.org/

[I] Starting [ spoofing:✔ discovery:✘ sniffer:✔ http-proxy:✘ https-proxy:✘ sslst
rip:✘ http-server:✘ dns-server:✔ ] ...
[I] [GATEWAY] 192.168.0.2 : 00:00:AB:2D:01:01 ( Logic Modeling )
[I] [SNIFFER] Saving packets to /root/traficoc.pcap .
[I] [TARGET] 192.168.0.10 : 00:0C:29:B2:03:41 ( VMware )
[192.168.0.10 > 192.168.1.100:http] [GET] http://192.168.1.100/archivo.bin
[192.168.0.10 > 192.168.1.100:http] [GET] http://192.168.1.100/archivo.bin
```

Figure 8. Salida de la consola de BetterCAP durante el ataque

Respecto al consumo de recursos en la maquina atacada no se observó incremento significativo en términos de procesamiento y memoria RAM. En la Fig. 9 se muestra el consumo de recursos durante el ataque en la máquina víctima.

Por otro lado, en la máquina atacante se evidenció que existe un incremento del 60% del consumo de procesamiento mientras que en la memoria RAM no se observó incremento significativo. En la Fig. 10 se muestra el consumo de recursos en la máquina atacante.

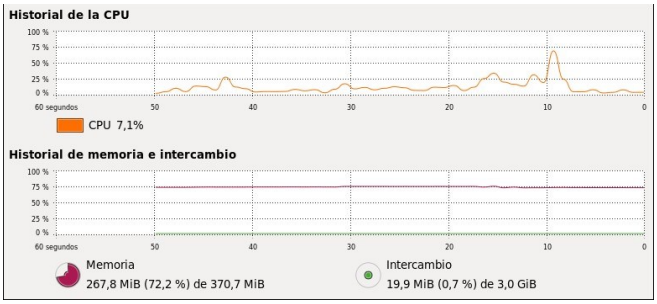

Figure 9. Consumo de recursos en la víctima durante el ataque

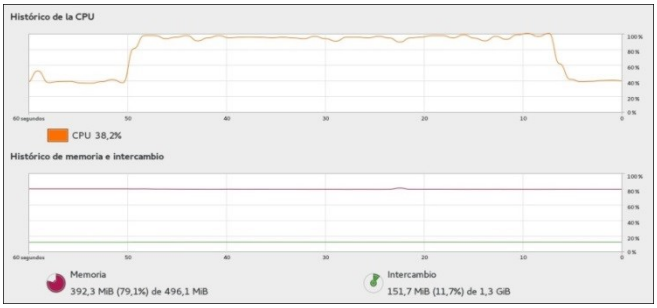

Figure 10. Consumo de recursos en el atacante durante el ataque

B. Evaluación de resultados aplicando mitigación

Para mitigar los ataques ARP Spoof se aplicó el algoritmo mencionado en secciones anteriores, mismo que establece un registro ARP estático en la máquina atacante. En la Fig. 11 se muestra la salida luego de aplicada esta mitigación con el detalle del registro creado en la tabla ARP.

```
Interrupción de la interfaz eth0:  Estado de dispositivo: 3 (desconectado)
                                                                [  OK  ]
Interrupción de la interfaz de loopback:                        [  OK  ]
Activación de la interfaz de loopback:                          [  OK  ]
Activando interfaz eth0:  Estado de conexión activa: activada
Ruta de conexión activa: /org/freedesktop/NetworkManager/ActiveConnection/3
                                                                [  OK  ]
Obteniendo la direccion IP y MAC del Gateway ....
IP del Gateway: 192.168.0.2 MAC: 00:00:AB:2D:01:01
Estableciendo registro estatico en la tabla ARP
192.168.0.2              ether   00:00:ab:2d:01:01   CM                    eth0
Protegido contra ataques de envenenamiento ARP
[root@centosCG Escritorio]#
```

Figure 11. Aplicación de mitigación

Esta acción es transparente para el atacante por lo que el procedimiento para realizar el ataque es el mismo mencionado en la sección anterior. Luego de efectuado este ataque se pudo observar que se vuelve a crear un nuevo registro en la tabla arp con la diferencia que ya no existe la duplicidad de direcciones MAC. En la Fig. 12 se muestra la tabla ARP aplicado la mitigación.

```
[root@centosCG Escritorio]# arp -n
Address                  HWtype  HWaddress           Flags Mask
192.168.0.20             ether   00:0c:29:71:d9:c0   C
192.168.0.2              ether   00:00:ab:2d:01:01   CM
```

Figure 12. Tabla MAC aplicado mitigación

De la misma forma para medir el efecto de la mitigación se realizó la misma prueba de descarga de un archivo desde el servidor Web y se midió el número de paquetes del archivo pcap creado por BetterCAP para transferir los paquetes capturados. El primer efecto que se evidenció es que luego de finalizado la descarga del archivo BetterCAP no pudo crear el archivo pcap debido a no capturó ningún paquete. En las Fig. 13 y 14 se muestra el número de paquetes capturados por

BetterCAP y la salida de la consola de la aplicación la misma que no mostró información alguna.

Figure 13. Número de paquetes capturados durante el ataque aplicado la mitigación

Figure 14. Salida de la consola de BetterCAP durante el ataque aplicada la mitigación

Respecto al consumo de recursos en la maquina atacada no se observó de igual manera incremento significativo en términos de procesamiento y memoria RAM. Por otro lado, en la máquina atacante tampoco se evidencio incremento de recursos esto es debido a que ya no debió procesar paquetes ya que no logró capturar a ninguno. En la Fig. 15 se muestra el consumo de recursos en la máquina atacante.

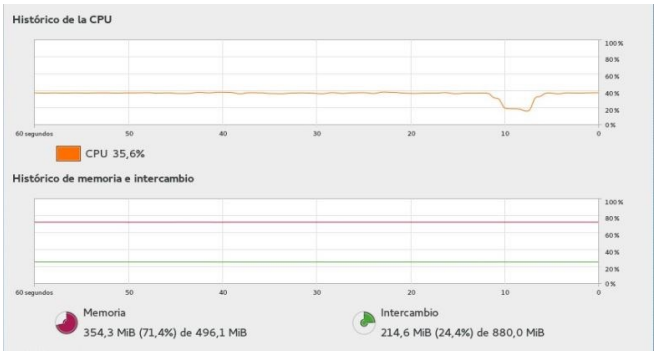

Figure 15. Consumo de recursos en el atacante durante el ataque aplicada la mitigación

V. Trabajos Relacionados.

En esta sección se han incluido los Trabajos más relevantes, que se han encontrado durante toda la investigación. Con respecto al ámbito educativo los trabajos desarrollados por Muñoz [1] y Zapata [10] indica el monitoreo e identificación de la red, define los ataques que puede sufrir, quien o quienes son los atacantes se analiza los tipos de ataques y las vulnerabilidades que tiene el sistema operativo, se muestra como defenderse de ataques y las medidas de seguridad. Zapata diseña e implementa varias topologías de experimentación usando entornos virtuales de red, dentro de las cuales se prueba el escaneo de puertos, denegación de servicios entre otros, los resultados de esta investigación proponen reducir las amenazas y vulnerabilidades mediante un demonio en Shell script el que detecta, controla y mitiga los ataques mencionados en el estudio.

La investigación de F. J. Díaz Jiménez y J.G. Palacio Velásquez [2] presenta una serie de técnicas que pueden ser utilizadas para vulnerar la seguridad en una red desde adentro, a través de la técnica de ARP Spoofing, realizando ataques de tipo Man In The Middle, al final presenta una serie de técnicas que pueden ser aplicadas para proteger a las redes de dichos ataques y minimizar los riesgos de robo de información. En este mismo ámbito Melgar Jara, E. S. [3] y Cazar Jácome, D. A. [4] han utilizado conceptos de auditoria de red que permitan detectar los múltiples ataques producidos por personas ajenas, presenta una herramienta que podrá detectar ataques comunes que se encuentran en las redes IPv4/IPv6 como por ejemplo "Man In The Middle" o la Denegación de Servicios.

Adicionalmente Gutiérrez Benito, F y Nicolalde Rodríguez, D. A. utilizan conceptos de virtualización y se realiza un estudio comparativo de sistemas de virtualización. Todos estos estudios investigativos han sido utilizados para la presente investigación. En relación a la utilización de entornos virtualizados los estudios de [6], [7] y [10] demuestran el uso de esta herramienta como una opción, ya que se puede simular servidores en operación reduciendo significativamente los costos y la administración.

VI. Conclusiones y Trabajos Futuros.

El presente trabajo investigativo se enfocó en la evaluación del ataque ARP Spoof utilizando plataformas de virtualización y para la simulación de la red se utilizó GNS3, el cuál emula firmware de los routers y dispositivos de Cisco Systems (IOS) además de establecer escenarios para conectar cada uno de los equipos. Para producir el ataque se utilizó el software libre BetterCAP, para la evaluación del ataque se midió en términos del número de paquetes capturados en el atacante, para lo cual se configuró la herramienta para que envíe todo el tráfico capturado a un archivo pcap y como segunda forma de verificación se observó la salida de la consola de la aplicación. Para contrarrestar dichos ataques, se desarrolló un demonio en Shell script que detectó, controló y mitigó el ataque ARP Spoof.

Como trabajo futuro se plantea evaluar los ataques ARP Replay y ARP Poisoning con el algoritmo desarrollado a fin de validar su efectividad, además se plantea evaluar ataques ARP Spoof en redes IPv6, utilizando otros mecanismos de mitigación como la encriptación, sistemas de detección de intrusos.

Referencias

[1] Muñoz Cedeño, D. E. (2014). "Monitoreo e identificación de ataques a redes" (Doctoral dissertation).

[2] J. Díaz Jiménez y J.G. Palacio Velásquez. Disección de un ataque MITM mediante ARP Spoofing y Técnicas de Protección Existentes, Barranquilla, Ed. Coruniamericana, Vol. I, 2012. 9-24

[3] Melgar Jara, E. S. (2015). Desarrollo de un conjunto de aplicaciones para detección de ataques en redes IPv4/IPv6 utilizando Python.

[4] Cazar Jácome, D. A. (2015). Análisis de IP Spoofing en redes IPv6 (Doctoral dissertation, 2015.).

[5] Herrera Figueroa, Helmuth Lenin. "Simulación de ataques a redes IP en un entorno corporativo real." (2015).

[6] Gutiérrez Benito, F. (2014). Laboratorio Virtualizado de Seguridad Informática con Kali Linux.

[7] Nicolalde Rodríguez, D. A. (2015). Estudio comparativo de sistemas de virtualización y de seguridad, caso de estudio Museo QCAZ de la PUCE.

[8] Echeverry Parada, J. S. (2013). Metodología para el diagnóstico continúo de la seguridad informática de la red de datos de la Universidad Militar Nueva Granada.

[9] Chumi Sarmiento, W., & Flores Escobar, D. (2014). Análisis forense a paquetes de datos en la red LAN de la Universidad Tecnológica Equinoccial como aporte al cumplimiento de las Normas PCI-DSS (Doctoral dissertation, Universidad de las Fuerzas Armadas ESPE. Maestría en Evaluación y Auditoría de Sistemas Tecnológicos.).

[10] Zapata Molina, L. P. (2012). Evaluación y mitigación de ataques reales a redes IP utilizando tecnologías de virtualización de libre distribución

[11] VMWare: https://www.vmware.com/products/workstation/. Última comprobación, marzo 2016.

[12] GNS3: https://www.gns3.com/. Última comprobación, marzo 2016.

[13] Cisco ASA 5500: https://www.cisco.com/web/ES/publicaciones/07-08-cisco-dispositivos-serie-ASA5500.pdf. Última comprobación, marzo 2016.

[14] Apache: https://httpd.apache.org/. Última comprobación, marzo 2016.

[15] BetterCAP: https://www.BetterCAP.org/. Última comprobación, marzo 2016.

[16] Tamayo Domínguez, M. F. (2013). Estudio, diseño y simulación en gns3 de guías de laboratorio para redes de datos ii y networking de la facultad de electrónica de la Universidad Israel. Quito.

[17] Díaz Cervantes, L. (2010). Evaluación de la herramienta GNS3 con conectividad a enrutadores reales.

[18] Fiallos Noboa, J. G. (2012). Análisis de tráfico" IP" para medianas empresas basado en software libre como parte de una política de seguridad informática

Como prueba de concepto de este proyecto favor ver el Video URL: https://youtu.be/OFfH6JN8tg0