
UTMACH

UNIDAD ACADÉMICA DE INGENIERÍA CIVIL

CARRERA DE INGENIERÍA DE SISTEMAS

# ANÁLISIS DE VULNERABILIDADES DE SUPLANTACIÓN EN EL PROTOCOLO TCP/IP E IMPLEMENTACIÓN DE CONTROLES DE MITIGACIÓN.

ASTUDILLO PIZARRO LUIS ALBERTO
INGENIERO DE SISTEMAS

MACHALA
2018


UTMACH

UNIDAD ACADÉMICA DE INGENIERÍA CIVIL

CARRERA DE INGENIERÍA DE SISTEMAS

# ANÁLISIS DE VULNERABILIDADES DE SUPLANTACIÓN EN EL PROTOCOLO TCP/IP E IMPLEMENTACIÓN DE CONTROLES DE MITIGACIÓN.

ASTUDILLO PIZARRO LUIS ALBERTO
INGENIERO DE SISTEMAS

MACHALA
2018


# UTMACH

## UNIDAD ACADÉMICA DE INGENIERÍA CIVIL

## CARRERA DE INGENIERÍA DE SISTEMAS

EXAMEN COMPLEXIVO

# ANÁLISIS DE VULNERABILIDADES DE SUPLANTACIÓN EN EL PROTOCOLO TCP/IP E IMPLEMENTACIÓN DE CONTROLES DE MITIGACIÓN.

ASTUDILLO PIZARRO LUIS ALBERTO
INGENIERO DE SISTEMAS

MOROCHO ROMAN RODRIGO FERNANDO

MACHALA, 05 DE JULIO DE 2018

MACHALA
05 de julio de 2018

**Nota de aceptación:**

Quienes suscriben, en nuestra condición de evaluadores del trabajo de titulación denominado Análisis de vulnerabilidades de suplantación en el protocolo TCP/IP e implementación de controles de mitigación., hacemos constar que luego de haber revisado el manuscrito del precitado trabajo, consideramos que reúne las condiciones académicas para continuar con la fase de evaluación correspondiente.

MOROCHO ROMAN RODRIGO FERNANDO
0703820464
TUTOR - ESPECIALISTA 1

MAZÓN OLIVO BERTHA EUGENIA
0603100512
ESPECIALISTA 2

VALAREZO PARDO MILTON RAFAEL
0704518893
ESPECIALISTA 3

Fecha de impresión: jueves 12 de julio de 2018 - 10:41

URKUND

# Urkund Analysis Result

**Analysed Document:** ASTUDILLO PIZARRO LUIS ALBERTO_PT-010518.pdf (D40316949)
**Submitted:** 6/22/2018 6:40:00 PM
**Submitted By:** laastudillo_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

El que suscribe, ASTUDILLO PIZARRO LUIS ALBERTO, en calidad de autor del siguiente trabajo escrito titulado Análisis de vulnerabilidades de suplantación en el protocolo TCP/IP e implementación de controles de mitigación., 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.

El autor 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.

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

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

Machala, 05 de julio de 2018

ASTUDILLO PIZARRO LUIS ALBERTO
0705376630

## DEDICATORIA

A mi madre, porque su amor y su apoyo son la fuerza que me ha permitido llegar lejos.

A mi familia, que siempre está presente para compartir la alegría de la vida.

A mi novia por hacerme vivir nuevas experiencias.

Sr. Luis Alberto Astudillo Pizarro.

## AGRADECIMIENTO

A todos los profesores que aún conservan el amor por la enseñanza y nos hacen conocer la belleza del conocimiento.

## RESUMEN

Los ataques de suplantación en el protocolo TCP/IP son aquellos en los que el atacante oculta su identidad, haciendo creer a los demás miembros de una red que se trata de un dispositivo conocido o autorizado. Estos ataques pueden darse en varios niveles de la pila de protocolos, es el caso de la suplantación de direcciones MAC en nivel de acceso a la red, de IP en el nivel de internet, del protocolo ARP que enlaza estos dos primeros niveles, hasta el nivel superior de la pila, el de aplicación, donde se vulneran los protocolos DNS y DHCP. El presente documento tiene como finalidad investigar y prevenir dichos ataques. Sus bases teóricas son presentadas con una breve explicación de cada protocolo afectado, la forma en que los atacantes pueden lograr dicha suplantación, y algunos de los métodos usados para mitigar las vulnerabilidades que los hacen posibles. Se hizo uso del software GNS3 para simular un escenario que consistía en dos subredes conectadas a través de un router, en el que fueron usadas las herramientas Ettercap para suplantar los protocolos ARP y DNS de manera efectiva, y Wireshark para espiar el tráfico de la red una vez lograda la suplantación. Con esto se logró evidenciar la amenaza que representan estos ataques, y le necesidad de establecer controles, tal como se hizo en la parte final cuando se cambió las entradas de tablas caché arp de los hosts a estáticas, logrando así obtener un escenario más seguro y a prueba de suplantaciones.



**Palabras claves:** DNS, ARP, SPOOFING, MITM, MAC

**ABSTRACT**

The spoofing attacks in the TCP / IP protocol are those in which the attacker conceals his identity, making the other members of a network believe that it is a known or authorized device. These attacks can occur at various levels of the protocol stack, is the case of MAC address Spoofing at the level of network access, IP spoofing at the Internet level, ARP poisoning which attacks the protocol that links these first two levels, reaching even the top level of the stack, the application level, where the DNS and DHCP protocols can be intercepted by malicious hosts. The purpose of this document is to investigate and prevent such attacks. Its theoretical bases are presented with a brief explanation of each affected protocol, the way in which the attackers can achieve said spoofing, and some of the methods used to mitigate the vulnerabilities that make them possible. The GNS3 software was used to simulate a scenario that consisted of two subnetworks connected through a router, in which the Ettercap tool was used to spoof the ARP and DNS protocols effectively, and Wireshark tool to spy on network traffic. once the attack has been achieved. With this it was possible to demonstrate the threat represented by these attacks, and the need to establish controls, as was done in the final part when the cache arp tables entries from the hosts were changed to static, thus obtaining a more secure and spoofing proof scenario.

**Keywords:** DNS, ARP, SPOOFING, MITM, MAC

**Contenido**

## Índice de Anexos



## Índice de Figuras

# 1. INTRODUCCIÓN

La vida moderna se encuentra vinculada cada vez más a aparatos electrónicos como celulares, computadoras portátiles, televisores inteligentes, etc. El Smartphone pasó de ser un dispositivo de lujo a una necesidad básica, alcanzando en el 2017 a la mitad de los dispositivos conectados a las redes móviles, según datos de Arcotel. Pero el verdadero cambio que han traído consigo estos son las nuevas formas de acceder a internet, lo cual se ha vuelto parte del día a día, más aún con la creciente penetración de las redes sociales en la forma de interactuar con otras personas.

El internet se usa ahora para todo, desde ordenar una pizza personalizada hasta realizar transacciones bancarias en cualquier lugar. La información que se envía a través de la red debe atravesar una serie de nodos para llegar a su destino, y es en ese trayecto donde se suelen presentar problemas como personas intentando obtener credenciales de acceso u otra información personal. Estos hackers pueden llegar a hacer uso de diversas estrategias para burlar los protocolos de seguridad establecidos para proteger nuestros datos, como son los ataques de ingeniería social, de fuerza bruta o de suplantación.

Es este último tipo de ataques en el que se centra la presente investigación, específicamente en lo que se refiere a suplantación de protocolos de la pila TCP/IP. Estos protocolos fueron creados en un principio para trabajar en entornos confiables, por lo que poseen pocos o ningún mecanismo de control de seguridad. La suplantación de direcciones IP se refiere a la alteración de la dirección IP de origen en los paquetes enviados, siendo esto posible ya que el protocolo solo valida la dirección de destino. Aquí se presentará un ataque al protocolo ARP, llamado envenenamiento ARP, ya que este involucra las direcciones MAC e IP, y una vez interceptadas las comunicaciones se hará una suplantación de DNS, lo cual permite re direccionar las peticiones de páginas web de la víctima.

Así como los atacantes centran sus esfuerzos en vulnerar las seguridades de las redes para perpetrar ataques contra personas o instituciones, tenemos también a analistas de seguridad que se encargan de reparar esas brechas de seguridad, previniendo que

dichos ataques vuelvan a ocurrir. El rol de los profesionales de seguridad informática ha evolucionado, centrando su esfuerzo no solo en la prevención de ataques conocidos, sino también en la búsqueda de nuevas vulnerabilidades antes de que sean descubiertas por personas con objetivos maliciosos. Es así que en la parte final de este documento se aplicarán controles para mitigar los ataques realizados, demostrando así la obtención de un entorno de red más seguro.

### 1.1 Contexto del Problema

El conjunto de protocolos TCP/IP no es perfecto. Existen graves fallas de seguridad que son inherentes al diseño del protocolo o a la mayoría de las implementaciones de TCP/IP. Los hackers de la red utilizan estas vulnerabilidades de seguridad para realizar diversos ataques de red.

### 1.2 Problema General

¿Explorar los ataques de suplantación permitirá tomar las mejores decisiones en el diseño e implementación de redes con el menor impacto posible, en caso de que estos ataques se realicen?

### 1.3 Objetivo General

Implementar controles de mitigación, mediante la simulación de ataques de suplantación, para mejorar la seguridad de las redes.

### 1.4 Objetivos Específicos

- Diseñar un escenario virtual de redes de área local.
- Utilizar herramientas para generar ataques de suplantación en la red construida.
- Investigar e implementar los controles adecuados para mitigar los ataques realizados

# 2. DESARROLLO

## 2.1 Marco Teórico

### *2.1.1 Suplantación de direcciones IP.*

IP es uno de los dos protocolos bases del modelo TCP/IP, el cual se encarga de llevar los paquetes desde el origen hasta el destino, especificado como una dirección IP incluida en el encabezado. Esta transmisión se realiza bajo un modelo sin conexión, no se conoce el estado de los paquetes enviados. [1]

El ataque de suplantación de direcciones ip se sustenta en el hecho de que el envío de paquetes a través de internet se basa solo en la dirección de destino, mientras que la dirección de origen nunca es comprobada, lo cual permite que los atacantes se escondan detrás de direcciones ip falsificadas para conseguir esquivar los controles y escapar del rastreo al momento de realizar ataques como DDOS o MITM. [1] [2] [3]

### *2.1.2 Suplantación de direcciones MAC.*

El control de acceso al medio (MAC por sus siglas en inglés) es un protocolo que hace uso de direcciones MAC para permitir a los dispositivos transmitir de manera ordenada evitando colisiones. Esta dirección, que sirve para identificar a los dispositivos dentro de una red, puede ser fácilmente suplantada por un atacante que haga uso de herramientas propias de los sistemas operativos o de terceros [4]. Uno de los usos que se da a estas suplantaciones es el sobrepaso de los controles de seguridad, alterando el atacante su MAC por la de un dispositivo autorizado y, en el caso de conexiones inalámbricas, echando luego fuera de la red al dueño de la MAC [4] [5]. Una segunda fase de este ataque consiste en, estando ya dentro de la red, enviar paquetes de disociación que consisten en suplantar la MAC del punto de acceso, con lo que se consigue denegar el acceso a la red a uno o muchos usuarios [4].

### *2.1.3 Suplantación ARP*

La pila TCP/IP hace uso de un protocolo que permite unir sus capas 1 y 2, el protocolo ARP, mediante pares compuestos de direcciones IP y MAC. Cada paquete que se envíe por la red debe contener una dirección física(MAC). La relación entre ambas

direcciones es almacenada en la tabla caché ARP de los hosts. Cuando un host no conoce la dirección física de una dirección IP, este difunde una petición ARP, la cual debería ser respondida sólo por la máquina a quien corresponda la IP. [1] [6]

La suplantación o envenenamiento ARP se produce cuando un atacante envía respuestas ARP con pares de direcciones falsas y muchas veces no solicitadas, logrando así redirigir el tráfico de un host hacia un nodo malicioso en el caso de secuestro de sesión o MITM, o hacia un host no válido en el caso de un ataque de denegación de servicio. [1] [6] [7]

### *2.1.4 Suplantación de aplicación o servicio.*

El nivel de aplicación o servicio es el tope del modelo OSI y de la pila TCP/IP. En él se definen protocolos que permiten a las aplicaciones acceder a las funcionalidades disponibles en la red.

Entre los protocolos de esta capa que suelen ser objetivos de ataques de suplantación se encuentra el Control Dinámico de Hosts(DHCP), el cual se encarga de configurar el acceso a la red a los dispositivos que vayan conectándose y que lo soliciten. Al conectarse un nuevo dispositivo, este envía una solicitud DHCP, la cual es respondida por el servidor con los parámetros necesarios. Dado que este protocolo no cuenta con controles de autenticación, las solicitudes pueden ser respondidas por nodos maliciosos, que envían respuestas con configuraciones inválidas que no permitan al nuevo host acceder a la red, o con configuraciones que permitan la escucha del tráfico y sean la base para la suplantación de otros servicios. [1]

DNS es un protocolo básico de la web. Cada dispositivo de la red pública se encuentra identificado por una dirección IP, sin embargo, desde los comienzos de la internet se estableció que a las personas les era más fácil recordar palabras alusivas al contenido de las webs antes que direcciones numéricas. La función de DNS es la de traducir las direcciones IP en direcciones amigables al ser humano [8]. La suplantación de este servicio consiste en enviar respuestas falsas a las peticiones DNS de los hosts, con lo que se consigue que al querer acceder a páginas conocidas sean redireccionados hacia la ip enviada en el mensaje suplantado [1]. Este ataque también se da a gran escala en países con acceso restringido a internet, como es el caso de China, donde el conocido como Gran Firewall de China realiza acciones de bloqueo o re direccionamiento de páginas seleccionadas [9]

### *2.1.5 Ettercap*

Es una herramienta muy utilizada para realizar diversos tipos de ataques informáticos. Está enfocada en la manipulación y escucha de redes, pero a su vez es muy extensible, ya que permite la incorporación de plugins que extienden su funcionalidad [10], como dns_spoof, el cual permite enviar respuestas dns falsificadas a hosts que hayan sido previamente interceptados con un ataque de hombre en el medio.

Otra de las ventajas de este programa es que puede trabajar en conjunto con Etterlog, una aplicación que permite exportar el tráfico escuchado en formatos como XML, un formato muy común que facilita su análisis posterior. [10]

### *2.1.6 Wireshark*

Wireshark es un programa que cuenta con una gran cantidad de herramientas, cuyo objetivo es el de analizar el tráfico de la red a la que se esté conectado. Este presenta en tiempo real todos los paquetes que son transmitidos, y al seleccionarlos muestra de manera legible cada uno de los campos que los componen. Su ventana principal está diseñada de manera que permite aplicar filtros mientras el tráfico aún está siendo escuchado, con lo que el usuario se puede enfocar únicamente en los paquetes que le interesan [11].

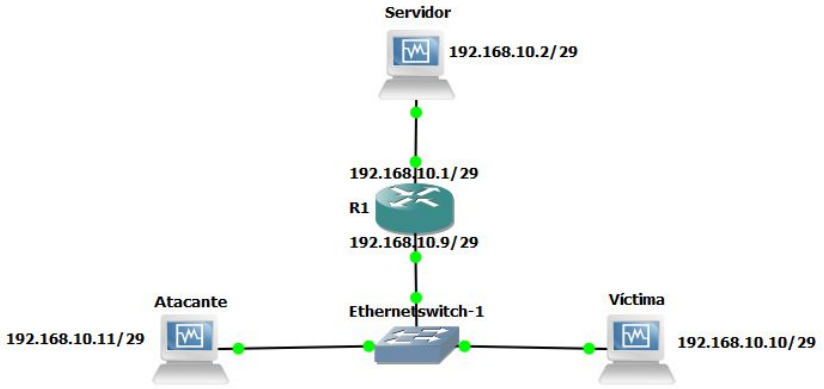
## 2.2 Marco Metodológico

### *2.2.1 Construcción del Escenario.*

Para la elaboración del escenario en el que se iba a realizar los ataques se usó la herramienta de simulación gráfica de redes GNS3 para los dispositivos como enrutadores y conmutadores, y el software de virtualización VirtualBox para los dispositivos finales como PCs y servidores.

Una vez instalados los sistemas operativos virtualizados (Ubuntu para el servidor y la víctima, Kali para el atacante y Cisco IOS para el router), se procedió a agregarlos a un nuevo proyecto de GNS3, y se usó las herramientas propias de esta aplicación para ubicarlos en dos redes de área local interconectadas por el enrutador, una en la que se encuentre el servidor, y otra en donde se situará la víctima junto con el atacante. Luego se ingresaron las configuraciones necesarias para habilitar la comunicación entre los dispositivos, quedando el escenario de la siguiente forma:

*Figura 1 Escenario propuesto*




**Fuente:** Elaboración Propia

Se instalaron y configuraron los servicios DNS(Bind) y HTTP(Apache) en el servidor web para más adelante comprometer su seguridad y suplantarlos en la víctima. En la máquina atacante se añadieron las herramientas de pentesting Wireshark y Ettercap, dejando el escenario listo para la realización de los ataques.

### *2.2.2 Ejecución de los ataques de suplantación.*

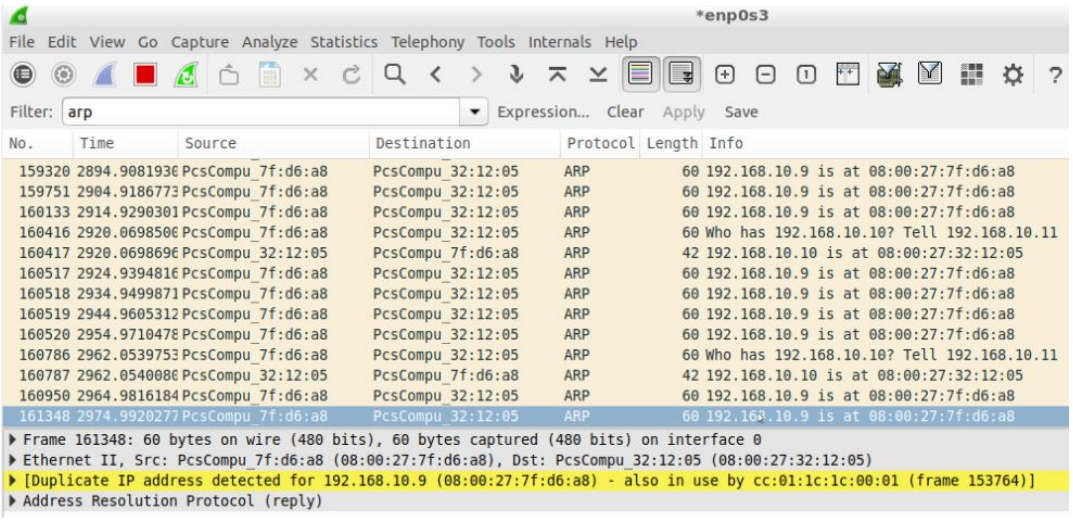
La presente sección comprende la realización de dos pruebas de penetración. La primera, que se realizó con la herramienta Ettercap, es la de envenenamiento ARP, que fue seleccionada debido a que involucra tanto las direcciones IP como las direcciones MAC, a las cuales enlaza de manera arbitraria en la tabla caché ARP de la víctima mediante respuestas arp falsas no solicitadas, para direccionar el tráfico hacia la máquina atacante, con lo que se consigue leer toda la información que entre o salga del equipo afectado.

La segunda prueba es la suplantación de DNS, que se realizó por medio de un plugin de la misma herramienta Ettercap. Al solicitar desde la víctima la página alojada en el servidor por medio de su dirección web este plugin envía respuestas DNS indicando que la dirección corresponde a la IP del atacante, el mismo que despliega su propio servidor web para responder con una página falsificada.

### *2.2.3 Ataque de suplantación ARP.*

Se configuró ettercap (ver Anexo A). Una vez establecidos los objetivos del ataque en ettercap, se usó la opción arp spoofing del menú mitm (ver Anexo B), con lo cual la máquina comenzó a enviar respuestas arp suplantadas como puede observarse en la figura 2

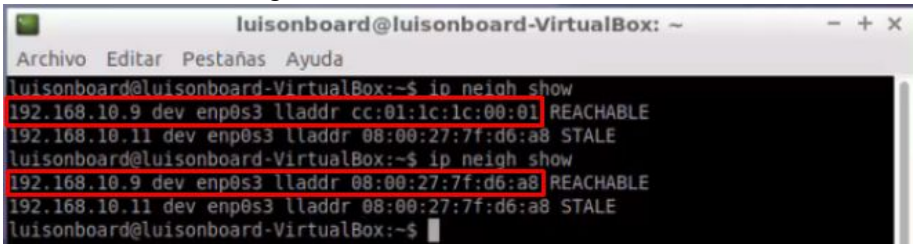
*Figura 2 Respuestas ARP suplantadas*




**Fuente:** Elaboración Propia

Al observar la tabla ARP de la víctima con el comando arp neigh show se pudo observar como la ip 192.168.10.9 que al inicio estaba vinculada a la MAC enrutador cambió por la de la máquina atacante.

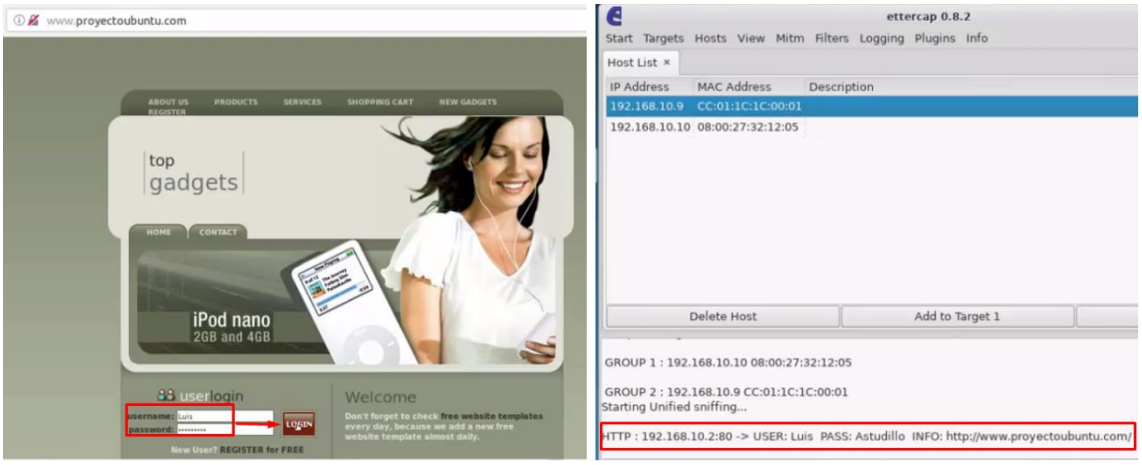
*Figura 3 Tabla ARP de la víctima*




**Fuente:** Elaboración Propia

Con esto se logró que todos los datos que envíe y reciba la víctima pasen primero por el atacante, es así que cuando se ingresaron credenciales a la página alojada en el servidor, ettercap automáticamente las capturó y mostró.

*Figura 4 Captura de credenciales*



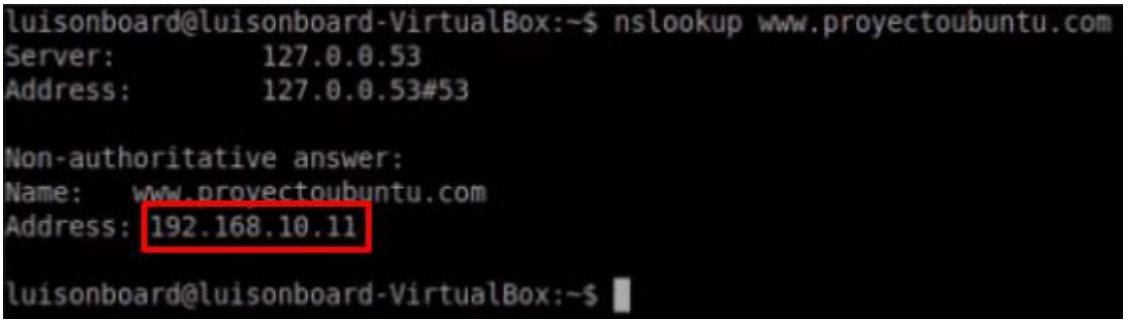

**Fuente:** Elaboración Propia

### *2.2.4 Ataque de suplantación DNS.*

El ataque al servicio DNS se lo ejecutó con el plugin dns_spoof de la herramienta ettercap(ver Anexo C), el cual se encarga de de que las peticiones de este protocolo establecidas en la configuración serán suplantadas.

Para comprobar el estado del servicio DNS en la víctima se usó el comando nslookup que busca en el servidor DNS configurado la ip correspondiente al nombre de dominio ingresado como parámetro. Al ejecutar este comando para buscar la ip correspondiente a la página alojada en el servidor se pudo observar que retorna la ip del atacante, con lo que se constata que el envenenamiento se había realizado con éxito.

*Figura 5 DNS Envenenado*




**Fuente:** Elaboración Propia

Y cuando se requirió la página en un navegador, la víctima vió el contenido que se había ingresado previamente.

*Figura 6 Página suplantada*

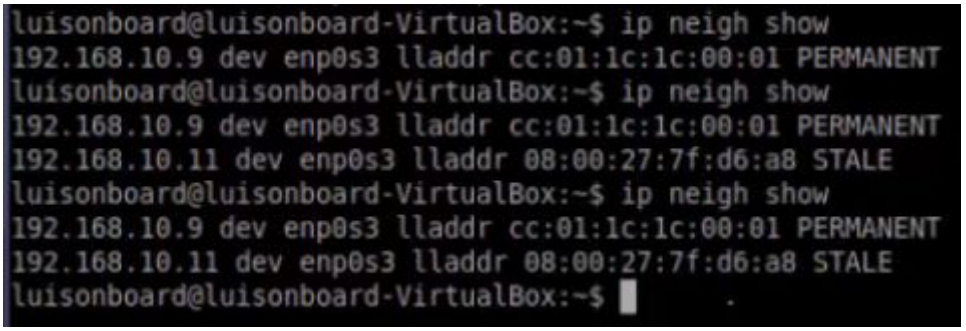

**Fuente:** Elaboración Propia

### 2.3 Aplicación de Controles.

El control que se aplicó fue que, una vez detectado el envenenamiento ARP, este fue cambiado a direccionamiento estático, consiguiendo con esto que no se pueda producir el ataque de hombre en el medio y por lo tanto tampoco la suplantación de DNS.

Es así que al agregar en la tabla ARP una entrada estática para el enrutador (ver Anexo D) esta permaneció correcta a pesar de encontrarse en medio de un ataque de envenenamiento ARP.

*Figura 7 Control de envenenamiento ARP*




**Fuente:** Elaboración Propia

Para el caso de las redes con configuración dinámica la configuración de entradas estáticas no resultaba práctico, por lo que se usó la herramienta arpwatch, cuya instalación y configuración puede ser observada en el Anexo E. Esta aplicación

monitorea los cambios que se realizan en la tabla ARP asociada a la interfaz de la víctima, y al ser objeto del ataque de suplantación devolvía continuamente la tabla a su estado anterior y enviaba reportes de estos ataques a la dirección configurada como administrador, como puede verse en el anexo F.

### 2.4 Resultados.

Al investigar sobre los ataques propuestos en el problema se comprobó su actualidad, y la disponibilidad de herramientas de acceso libre existentes en el mercado para su ejecución.

En el caso del ataque de suplantación ARP se constató la facilidad que representa su realización para un usuario con experiencia, y la peligrosidad del mismo, al permitir obtener las credenciales de la página no segura que fue usada de ejemplo. Al usar entradas ARP estáticas como control, se pudo mitigar completamente la falsificación de pares IP-MAC, aunque esta opción no es aplicable en redes de acceso dinámico, para las cuales se utilizó la aplicación arpwatch, la misma que retornó continuamente la tabla ARP del host a su estado original, mientras notificaba al administrador de red del ataque con el fin de que tome acciones definitivas.

La suplantación de DNS, a diferencia de la de ARP, se da no solo a nivel de redes locales, sino también a nivel de internet. Esta se produjo como un segundo paso luego del envenenamiento ARP, ya que una vez capturado el tráfico, las peticiones DNS fueron suplantadas con configuraciones que se ingresaron en ettercap y que permitieron enviar la página alojada en la máquina atacante en lugar de la alojada en el servidor. Este ataque puede llegar a ser muy peligroso si se combina con ingeniería social, ya que dentro de la página suplantada puede enviarse desde formularios que piden el ingreso de información personal como cuentas de redes sociales y bancarias, hasta contenido malicioso como troyanos y ransomware. Este ataque también fue controlado con el ingreso de entradas ARP estáticas, con lo que se logró que una vez evitado el ataque de hombre en el medio, las peticiones DNS ya no puedan ser suplantadas. Otra recomendación es siempre asegurarse de usar páginas con seguridad https cuando se trabaje con información valiosa, ya que al estar encriptada esta no podrá ser usada por el atacante.

## CONCLUSIONES

- Los ataques de suplantación en el protocolo TCP/IP son una amenaza vigente que aún representa objeto de estudio por parte de expertos de seguridad de todo el mundo.
- Existen diversas herramientas de libre acceso disponibles para construcción de escenarios de red que permiten simular tanto PCs como enrutadores y conmutadores.
- Los ataques de suplantación pueden ser ejecutados de manera silenciosa en entornos comunes de red, permitiendo a los atacantes el robo de información muchas veces valiosa a las víctimas.
- Existen controles que pueden ser aplicados para mitigar de manera efectiva los ataques de suplantación de protocolos.
- Los controles para este tipo de ataques aún son poco conocidos, y por ende aplicados a entornos de redes de hogares y empresas pequeñas y medianas.

## BIBLIOGRAFÍA


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

[2] S. Shiaeles y M. Papadaki, «FHSD: An Improved IP Spoof Detection Method for Web DDoS Attacks,» *The Computer Journal,* vol. 58, nº 4, pp. 892 - 903, 2015.

[3] C. Zhang, G. Hu, G. Chen, A. K. Sangaiah, P. Zhang, X. Yan y W. Jiang, «Towards a SDN - based Integrated Architecture for Mitigating IP Spoofing Atack,» *IEEE Access,* vol. 6, pp. 22764 - 22777, 2017.

[4] B. Alotaibi y K. Elleithy, «A New MAC Address Spoofing Detection Technique Based on Random Forests,» *Sensors ,* vol. 16, pp. 281-294, 2016.

[5] H. Alipour, Y. Al-Nashif, P. Satam y S. Hariri, «Wireless Anomaly Detection Based on IEEE 802.11 Behavior Analysis,» *IEEE Transactions on Information Forensics and Security,* vol. 10, nº 10, pp. 2158 - 2170, 2015.

[6] D. Tian, K. Butler, J. Choi, P. McDaniel y P. Krishnaswamy, «Securing ARP/NDP From the Ground Up,» *IEEE Transactions on Information Forensics and Security,* vol. 12, nº 9, pp. 2131 - 2143, 2017.

[7] S. Yeob Nam, S. Djuraev y M. Park, «Collaborative approach to mitigating ARP poisoning-based Man-in-the-Middle attacks,» *Computer Networks,* vol. 57, nº 18, pp. 3866-3884, 2013.

[8] H. Salim Hmood, Z. Li, H. Khalaf Abdulwahid y Y. Zhang, «Adaptive Caching Approach to Prevent DNS Cache Poisoning Attack,» *The Computer Journal,* vol. 58, nº 4, pp. 973 - 985, 2015.

[9] M. Wander y C. Bolman, «Measurement of Globally Visible DNS Injection,» *IEEE Access,* vol. 2, pp. 526 - 536, 2014.

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

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

# ANEXOS

## Anexo A. Configuración de ettercap

Se instala ettercap con el comando *sudo apt-get install ettercap-gtk*

Se realizan los siguientes cambios en el archivo de configuración de ettercap ubicado en /etc/ettercap/etter.conf

Se cambia por 0 el uid y gid para indicar que el usuario root iniciará el programa.

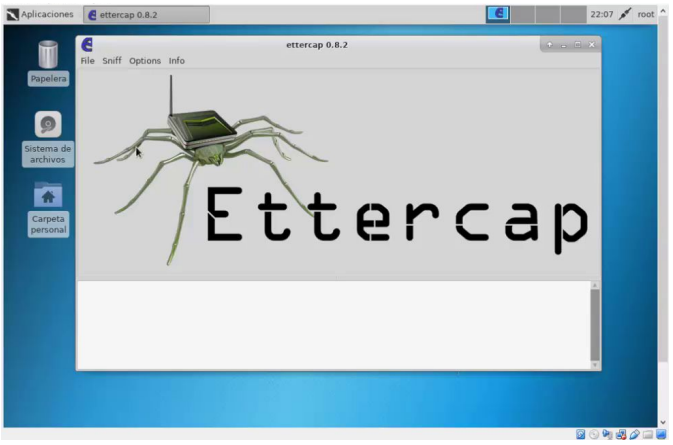
```
[privs]
ec_uid = 0                # nobody is the default
ec_gid = 0                # nobody is the default
```

En la parte de firewall se quita el comentario de las líneas correspondientes a iptables, que es el que Kali incluye por defecto.

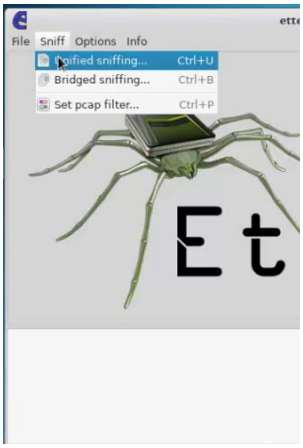
```
#--------------
#     Linux
#--------------

# if you use ipchains:
   #redir_command_on = "ipchains -A input -i %iface -p tcp -s 0/0 -d 0/0 %port -j REDIRECT %rport"
   #redir_command_off = "ipchains -D input -i %iface -p tcp -s 0/0 -d 0/0 %port -j REDIRECT %rport"

# if you use iptables:
   redir_command_on = "iptables -t nat -A PREROUTING -i %iface -p tcp --dport %port -j REDIRECT --to
   redir_command_off = "iptables -t nat -D PREROUTING -i %iface -p tcp --dport %port -j REDIRECT --t
```

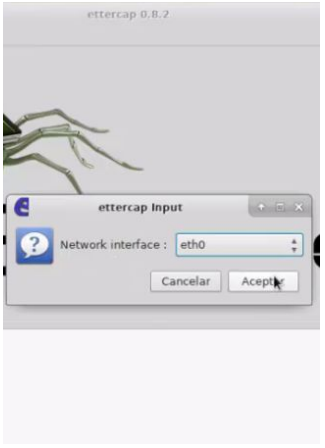
**Anexo B. Envenenamiento ARP con ettercap**

Se inicia Ettercap con el comando ettercap –G



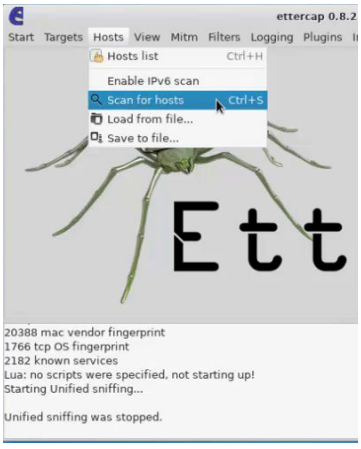

Se da inicio a la escucha en la tarjeta conectada a la red y de lo detiene de manera inmediata.

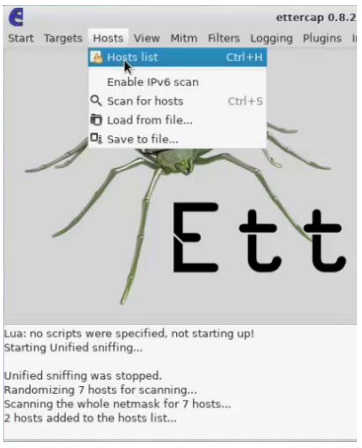


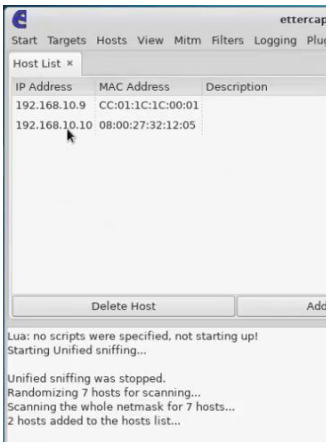





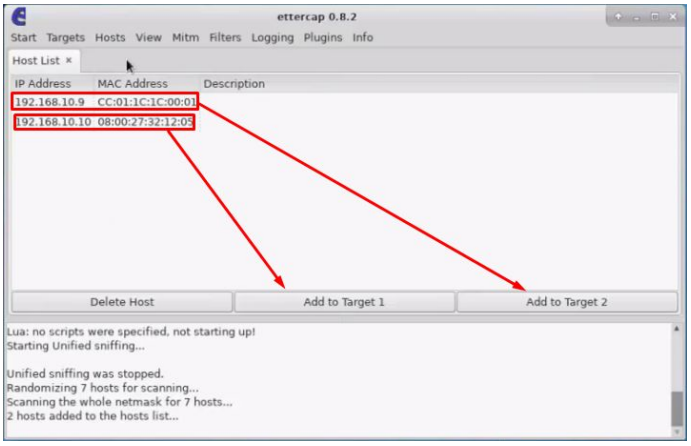
Se escanean los hosts presentes en la red y se muestra la lista de los dispositivos encontrados.



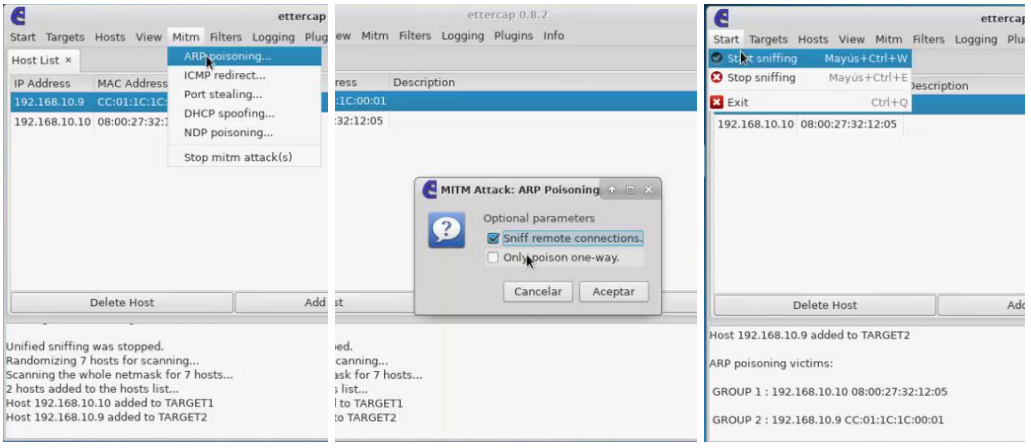



Las ip del enrutador y de la víctima son añadidas a los objetivos 1 y 2 del ataque.

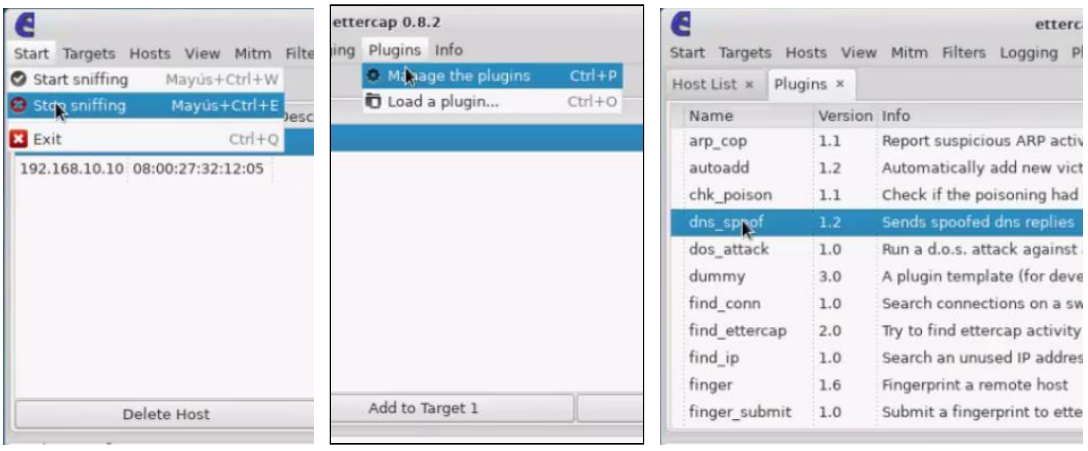



En el menú MITM se selecciona la opción ARP *poissoning*(envenenamiento ARP) con la opción Sniff remote connections para escuchar todo el tráfico del host hacia el enrutador y viceversa, y se inicia la escucha.

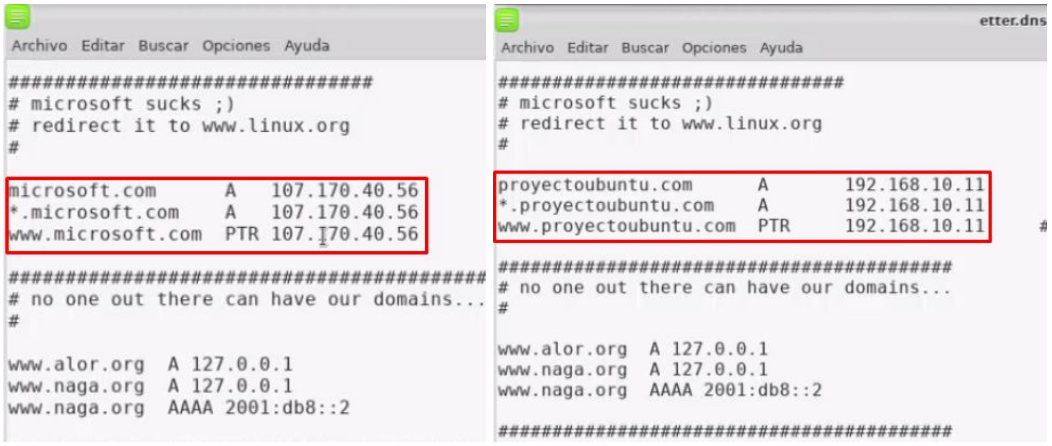


**Anexo C. Envenenamiento caché DNS con ettercap**

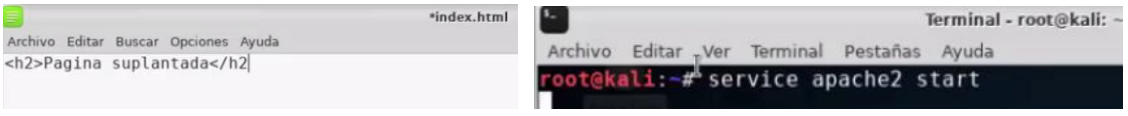
Luego de detener la escucha dirigirse al menú de plugins y elegir dns_spoof



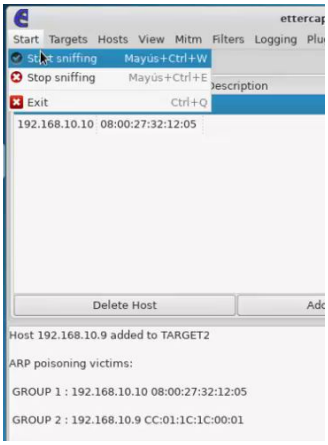

Ahora hay que editar el archivo que se encuentra ubicado en /etc/ettercap/etter.dns y agregar las páginas cuyas direcciones se quiera suplantar; en el ejemplo se cambia la página www.proyectoubuntu.com ubicada en el servidor por la dirección del atacante.




Debido a que las peticiones llegarán a la máquina atacante, es necesario configurar en ella un servidor web, en este caso el apache, para lo cual se edita el archivo index.html ubicado en var/www/html y se reemplaza su contenido con el que se desee mostrar a la víctima y se inicia el servidor.

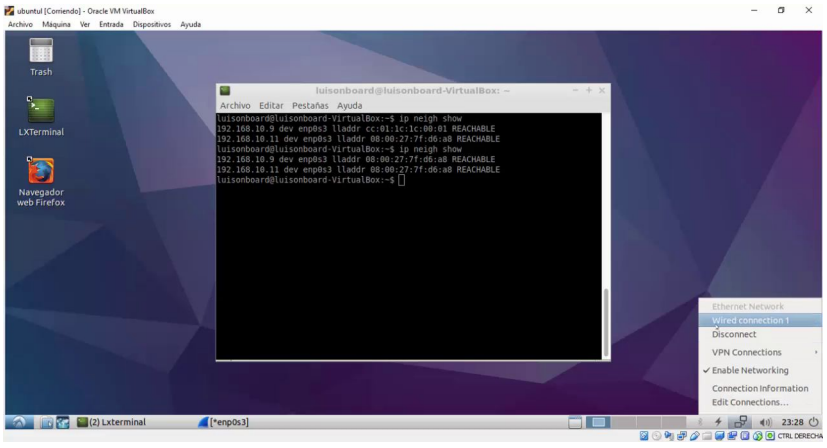


Se inicia la escucha para capturar las peticiones DNS y suplantarlas.

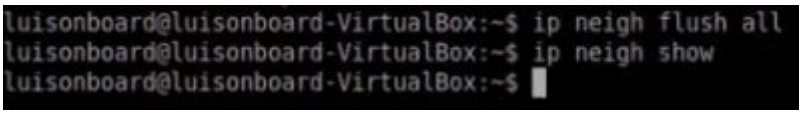



## Anexo D. Entradas ARP estáticas

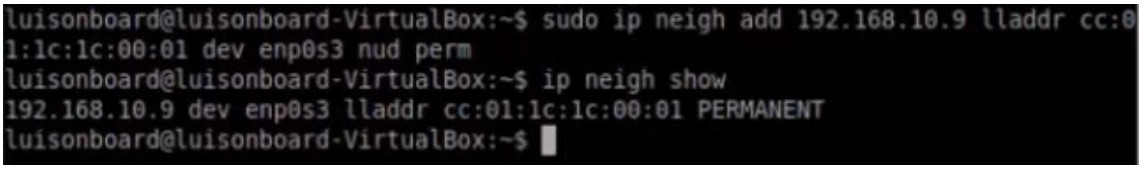
Se desconecta la red momentáneamente para evitar los mensajes de envenenamiento arp.




Una vez desconectado se ejecuta el comando ip neigh flush all para borrar todas las entradas de la tabla caché arp



Luego se agrega la entrada permanente con el comando ip neigh add <IP> lladdr <MAC> dev <interfaz> nud perm




**Anexo E. Instalación y configuración de ArpWatch**

ArpWatch es una herramienta usada para el monitoreo de redes de área local. Su instalación desde los repositorios de ubuntu se realiza mediante el comando *sudo apt-get install arpwatch*.

Una vez instalado se edita el archivo de configuración ubicado en /etc/arpwatch.conf con los parámetros correspondientes a nuestra red y el mail al que se enviarán las notificaciones.


Ahora se configuran las notificaciones por email, para lo cual se instala la herramienta ssmtp con el comando sudo apt-get install ssmtp

Ahora se edita el archivo de configuración ubicado en /etc/ssmtp/ssmtp.conf ingresando los parámetros correspondientes al mail del administrador, en este caso de gmail.

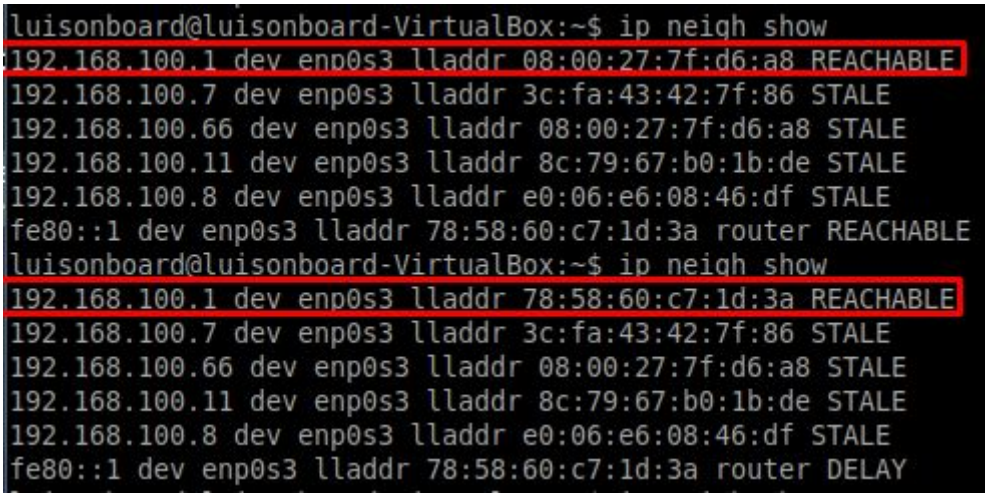
```
# Make this empty to disable rewriting.
root=luisonboard@gmail.com

# The place where the mail goes. The actual machine name is required no
# MX records are consulted. Commonly mailhosts are named mail.domain.com
mailhub=smtp.gmail.com:587

# Where will the mail seem to come from?
#rewriteDomain=gmail.com

# The full hostname
hostname=arpwatchmachine

# Use SSL/TLS before starting negotiation
UseTLS=Yes
UseSTARTTLS=Yes

# Username/Password
AuthUser=luisonboard@gmail.com
AuthPass=[redacted]


# Are users allowed to set their own From: address?
# YES - Allow the user to specify their own From: address
# NO - Use the system generated From: address
FromLineOverride=YES
```

Por último, se configura el archivo ubicado en /etc/ssmtp/revaliases para vincular el mail con la cuenta de administrador.

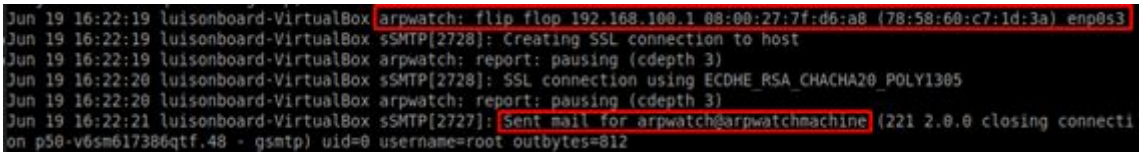
```
# sSMTP aliases
#
# Format: local_account:outgoing_address:mailhub
#
# Example: root:your_login@your.domain:mailhub.your.domain[:port]
# where [:port] is an optional port number that defaults to 25.
root:luisonboard@gmail.com:smtp.gmail.com:587
```

**Anexo F. Control de envenenamiento arp con ArpWatch**

Al ejecutar el comando *ip neigh show* para mostrar la tabla arp de la víctima se observa como ArpWatch al detectar el ataque la regresa a su estado original.




Se pueden observar los mensajes de sistema de arpwatch con el comando *tail -f /var/log/syslog*




A su vez las notificaciones más importantes las recibe la cuenta que se haya configurado como administrador