Ettercap
Seguridad Informática

10 febrero 2017
Ketzia Dante- Hidalgo Bouchot - A01336592
a01336592@itesm.mx

Abstract
Este documento tiene como propósito la investigación sobre la herramienta Ettercap así como el desarrollo de laboratorios que permitan poner en práctica los conocimientos adquiridos.

Introducción
Ettercap es una herramienta libre y gratuita que permite realizar ataques de tipo Man In The Middle.
Ettercap corre en sistemas operativos basados en Unix como Linux, BSD, MAC OS X, Solaris y además en Windows y está desarrollada en C. Esta herramienta fue lanzada por primera vez el 25 de enero del año 2001 por dos estudiantes italianos, Marco Valleri y Alberto Onarghi.

Ettercap comenzó como un sniffer para redes locales, sin embargo durante su desarrollo se fueron agregando nuevas funcionalidades que la convirtieron en una herramienta poderosa para realizar ataques Man In The Middle.

Interfaces
Ettercap puede ser utilizado en la línea de comandos, en una GUI o a través de Ncurses.

Modos de Operación
Ettercap cuenta con cuatro modos de operación los cuales son los siguientes:

- Basados en ARP : En este caso realizaremos este tipo de ataque. Utiliza un ataque ARP con el fin de sniffear en una LAN entre dos hosts.
- Basados en IP : Filtra paquetes por la dirección IP
- Basados en MAC: Filtra paquetes por la dirección MAC
- Basados en ARP Pública: Sniffea paquetes de un usuario a todos los hosts.

Algunas otras funcionalidades que ofrece Ettercap son las siguientes :

- Sniffing a través de HTTPS
- Soporte para plugins
- Fingerprinting del sistema operativo
- Inyección de caracteres
- Recolector de passwords a través de HTTP, FTP, TELNET, POP, IMAP

ARP POISONING
En este tipo de ataques el atacante manda mensajes ARP falsificados a través de una LAN. En este tipo de ataques se asocia la dirección MAC del atacante con la IP de algún otro host, de tal modo que cualquier tráfico que sea destinado para ese host sea mandado en realidad al atacante.

Versiones

- Dec 2004 .0.7.2 NG
- Mayo 2005 .0.7.3 NG
- Dic 2011 .7.4 Lazarus
- Feb 2012 .7.4.1 Lazarus
- Octubre 2012 .7.5.5 Assimilation
- Enero 2013 .7.5.2 Assimilation
- Febrero 2013 .7.5.3 Assimilation
- Marzo 2013 .0.7.6 Locard
- Septiembre 2013 .0.8.0 Lacasagne
- Octubre 2014 .0.8.1 Lombroso
- Octubre 2014 .0.8.1 Lombroso

La versión más actual fue lanzada en Marzo del año 2015.

Desarrollo Práctica #1

Requerimientos Previos

- Contar con sistema operativo Kali Linux 2.0
- Tener instalado Ettercap
- Tarjeta de red

Sniffing/ ARP Poisoning - Práctica #1

1) Iniciar Ettercap, ir a Applications > Sniffing & Spoofing > Ettercap o la Línea de comando escribir **ettercap -G**
2) Una vez abierta la interfaz, dar click en **Sniff > Unified Sniffing,** posteriormente en la ventana emergente seleccionar la interfaz de red del dispositivo. Click OK . (En caso de no saber cuál es la interfaz de red, en la terminal de comandos teclear el comando route -n.
3) En la pestaña **Hosts dar click en Scan for hosts** (En este paso se escaneará por todos los hosts conectados a la LAN)
4) Una vez terminado el escaneo, dar click en **Hosts > Hosts Lists** (Se desplegará la lista de hosts que se encontró).
5) A continuación, buscar la dirección IP de la víctima en la lista de hosts y dar click en el botón Add to Target 1
6) Posteriormente dar click en la dirección del default gateway de nuestro dispositivo y dar click en Add to Target 2 (Para buscar la dirección del default gateway, en la terminal volver a escribir el comando route -n, en la columna Gateway se encuentra la información).
7) Dar click en **Mitm > ARP Poisoning, seleccionar Sniff Remote Connections > OK**.
8) Esperar que la víctima ingrese a un sitio. Para fines de esta práctica, la víctima abrirá una página con un formulario (protocolo HTTP) (Ej www.quinielagodin.com)
9) Se desplegarán en Ettercap los datos ingresados en el formulario

Desarrollo Práctica #2

Requerimientos Previos

- Contar con sistema operativo Kali Linux 2.0
- Tener instalado Ettercap
- Tarjeta de red

ARP Poisoning/DNS Spoofing

1) En la terminal escribir **gedit** ***/etc/ettercap/etter.conf*** **.** Se abrirá un editor con el archivo de configuración de Ettercap.
2) Cambiar los ids de usuario y de grupo por cero

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

[mitm]
```

3) Scrollear y buscar el encabezado que diga Linux, buscar la línea que diga **if you use iptable**s, descomentar las dos líneas posteriores.

```
#--------------
#     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-port %rport"
   redir_command_off = "iptables -t nat -D PREROUTING -i %iface -p tcp --dport %port -j REDIRECT --to-port %
rport"
```

4) Guardar archivo .Abrir Ettercap
   - Por Launchpad: ir a Applications > Sniffing & Spoofing > Ettercap
   - Por terminal : **ettercap -G**

5) Dar click en **Sniff > Unified Sniffing**, posteriormente en la ventana emergente seleccionar la interfaz de red del dispositivo. Click OK . (En caso de no saber cuál es la interfaz de red, en la terminal de comandos teclear el comando route -n).
6) Posteriormente dar click en la pestaña **Start > Stop Sniffing**.
7) En la pestaña **Hosts dar click en Scan for hosts** (En este paso se escaneará por todos los hosts conectados a la LAN).
8) Una vez terminado el escaneo, dar click en **Hosts > Hosts Lists** (Se desplegará la lista de hosts que se encontró).
9) A continuación, buscar la dirección IP de la víctima en la lista de hosts y dar click en el botón Add to Target 1
10) Posteriormente dar click en la dirección del default gateway de nuestro dispositivo y dar click en Add to Target 2 (Para buscar la dirección del default gateway, en la terminal volver a escribir el comando route -n, en la columna Gateway se encuentra la información). NO cerrar Ettercap.
11) En una nueva ventana de la terminal de comandos escribir **gedit/etc/ettercap/etter.dns**. Se abrirá el archivo etter.dns, el cual es el encargado de redireccionar requests de DNS.
12) Buscar el apartado en el cual se ecneuntra www.microsoft.com escribir la página que queremos redireccionar, para efectos de esta práctica utilizaremos quinielagodin
Escribir bajo la línea microsoft.com
quinielagodin.com A ipdelapaginaalacualqueremosredireccionar
*.quinielagodin.com A ipdelapaginaalacualqueremosredireccionar

```
################################
# microsoft sucks ;)
# redirect it to www.linux.org
#

microsoft.com      A   107.170.40.56
*.microsoft.com    A   107.170.40.56
www.microsoft.com  PTR 107.170.40.56      # Wildcards in PTR are not allowed
quinielagodin.com  A   ippaginaaredireccionar
*.quinielagodin.com A  ippaginaaredireccionar
```

13) Guardar el archivo
14) Ir a la ventana donde está Ettercap, dar click en la pestaña **Mitm > ARP Poisoning**, seleccionar **Sniff Remote Connections > OK.**
15) **Ir a Plugins > Manage Plugins > doble click dns spoofing**.
16) Esperar que la víctima ingrese a www.quinielagodin.com
17) Observar que la página fue redireccionada a otra

Conclusiones

Ettercap es una herramienta muy poderosa la cual nos permite realizar ataques Man In The Middle, es decir interferir entre el tráfico de dos hosts, pudiendo recibir los paquetes que transfieren e incluso poder cambiar la información que se recibe. Realmente me pareció muy interesante la realización de ambas prácticas ya que los pasos a realizar son relativamente sencillos, pero pueden tener un alto impacto en las víctimas. El alcance que puede llegar a tener esta herramienta es muy grande. Por ejemplo en la segunda práctica, se puede crear un formulario idéntico al que queremos redireccionar, montarlo en algún servidor que tengamos y en caso de que la página fuese vulnerable podría tener un impacto muy negativo sobre el usuario y sobre la reputación de la página web. Por ejemplo yo en primera instancia intente redireccionar páginas como facebook y youtube las cuales no permitieron su redireccionamiento, por lo que se optó por utilizar una página con protocolo HTTP. Es realmente impresionante lo fácil que puede ser obtener información de páginas las cuales no tienen completo control sobre este tipo de amenazas.

Referencias:

http://ettercap.github.io/ettercap/about.html
https://pentestmag.com/ettercap-tutorial-for-windows/
http://www.backtrack-linux.org/forums/showthread.php?t=11135
https://openmaniak.com/ettercap.php
https://pentestmag.com/ettercap-tutorial-for-windows/
https://www.linux.com/news/men-behind-ettercapng
https://null-byte.wonderhowto.com/how-to/tutorial-dns-spoofing-0167796/