ENVENENAR Y/O SUPLANTAR SERVICIOS

Jordi Masó Pla

ÍNDICE

1 PREPARACIÓN

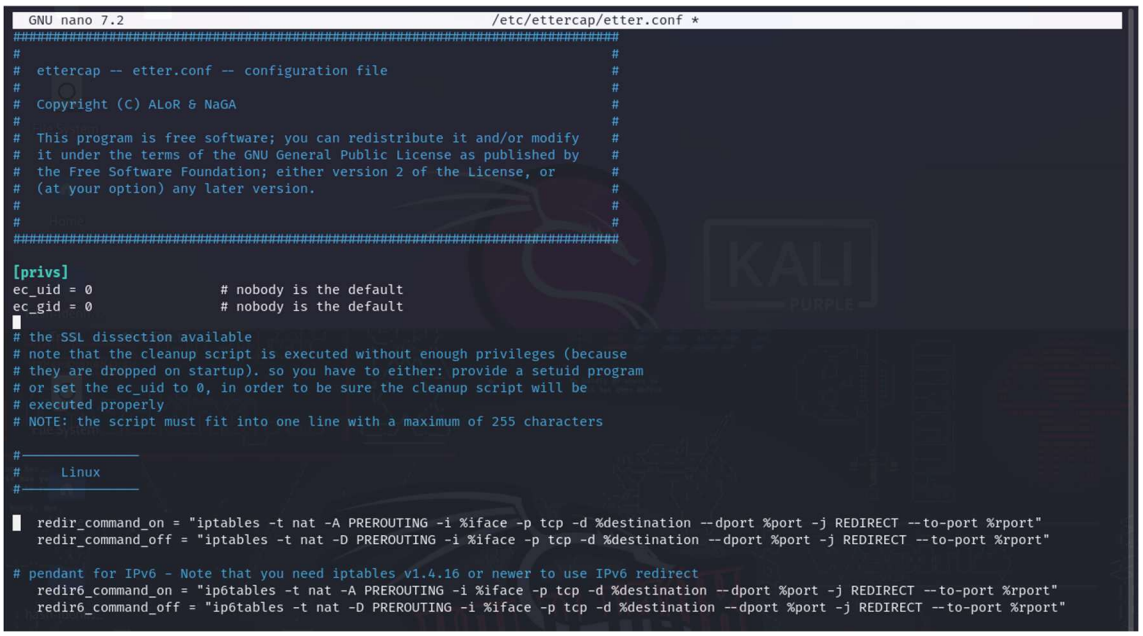
En esta práctica realizaremos el esnifado de trafico de la red entre dos máquinas, una tendrá la función de servidor y la otra de cliente. Lo primero que hay que realizar en la maquina de Kali Linux es poner a trabajar en modo de redireccionamiento para captura el trafico de la red. En una terminal de Kali pondremos el siguiente comando “echo 1 > /proc/sys/net/ipv4/ip_forward”

En esta punta ya podemos iniciar Wireshark para empezar a capturar paquetes de la red.

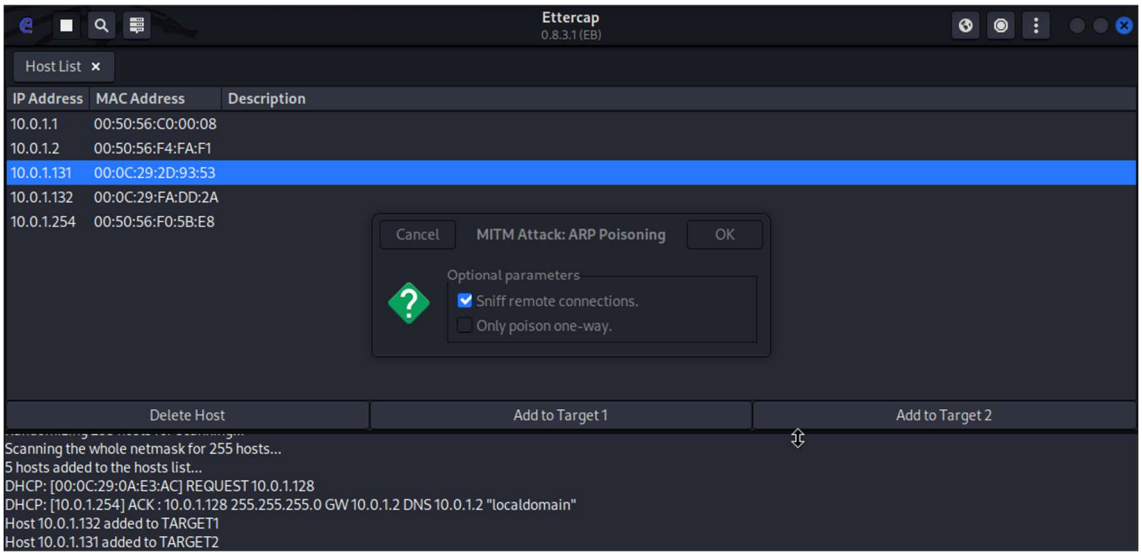
2 ENVENENAMIENTO

2.1 ETTERCAP

El envenenamiento de la red la realizaremos con el programa Ettercap. Antes de iniciar esta herramienta hay que configurar el fichero de configuración de la herramienta, en la termina escribimos “nano /etc/ettercap/etter.conf”. los cambia que realizamos en este fichero son los siguientes: en el apartado de privilegios ponemos el de root o el 0, y en el apartado de la iptables las descontamos.

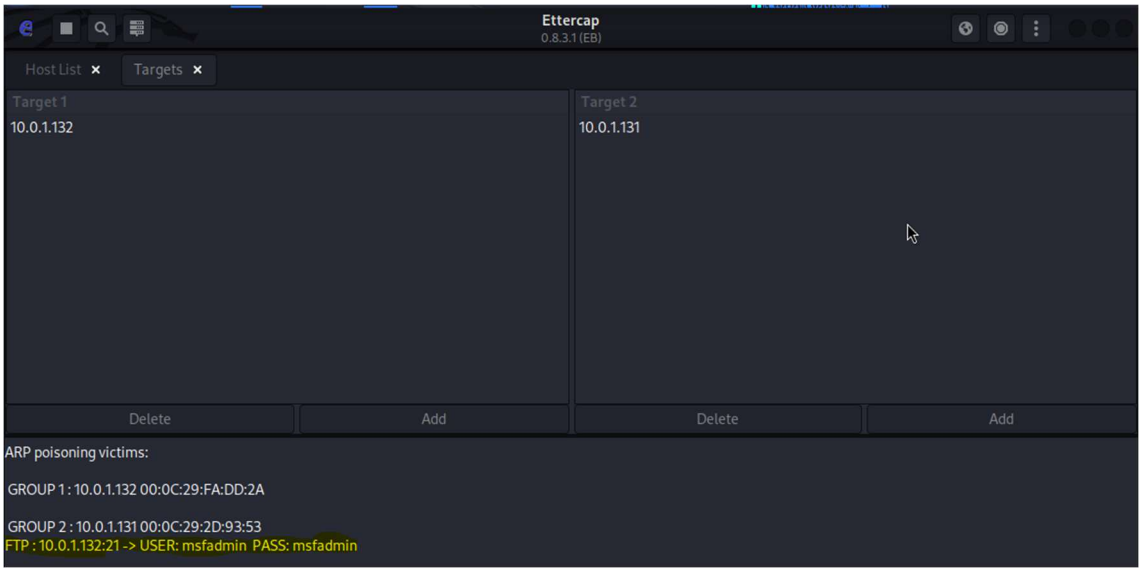


Iniciamos el programa y buscamos todos los clientes de la red. Seleccionamos las ip que queremos ver el trafico la primera es la maquina de Metasplotable 2 con la ip 10.0.1.132 y la otra es el cliente será un Linux Ubuntu con la ip 10.0.1.131. Una vez seleccionado las ips podemos empezar el envenenamiento de la red con Ettercap.



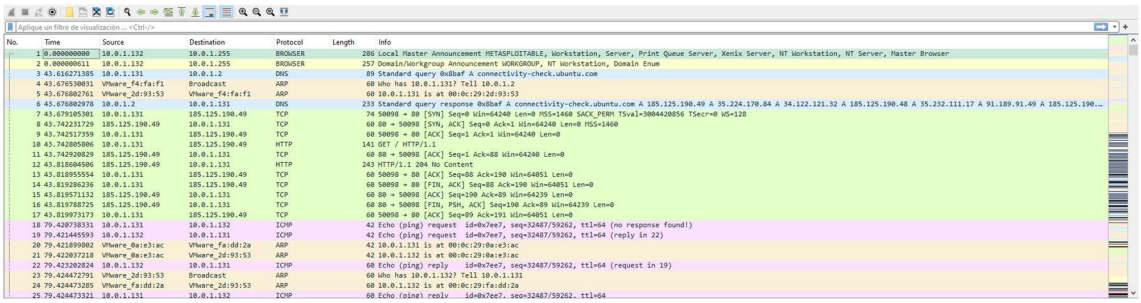
2.2 CAPTURA DE CREDENCIALES CON ETTERCAP

Ettercap también nos captura las credenciales y las contraseñas que circulan por la red en tres las dos máquinas, aunque estén cifradas.



3 WIRESHARK

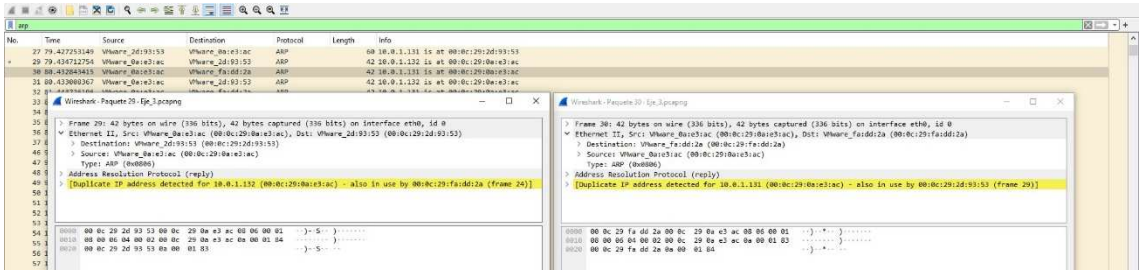
Para poder recoger todos los paquetes que circulan por la red utilizamos una herramienta que es Wireshark. Iniciamos Wireshark indicamos la red por donde queremos capturar el tráfico, en mi caso eth0, clicamos el botón de iniciar captura de paquetes.



4 FILTROS CON WIRESHARK

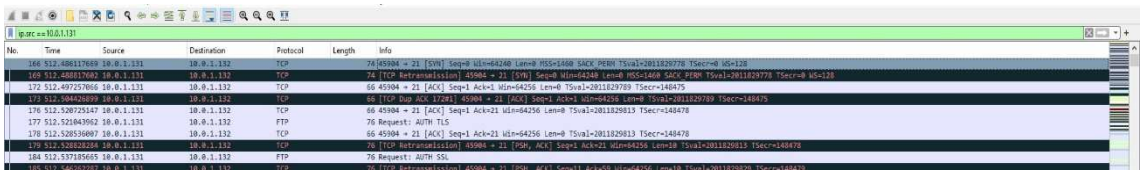
4.1 FILTRO ARP

El primer filtro es el arp para comprobar el envenenamiento de la red con Ettercap. comprobamos que las direcciones están envenenadas y el tráfico se captura bien.

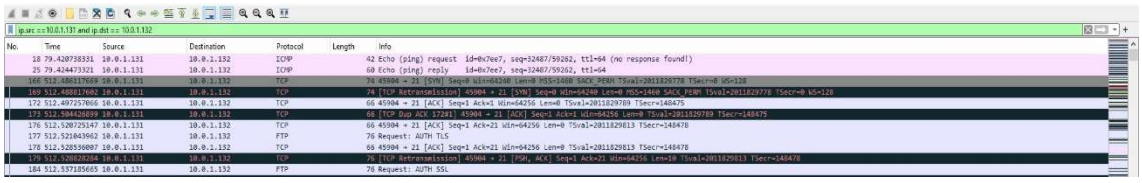


4.2 FILTRO POR IP

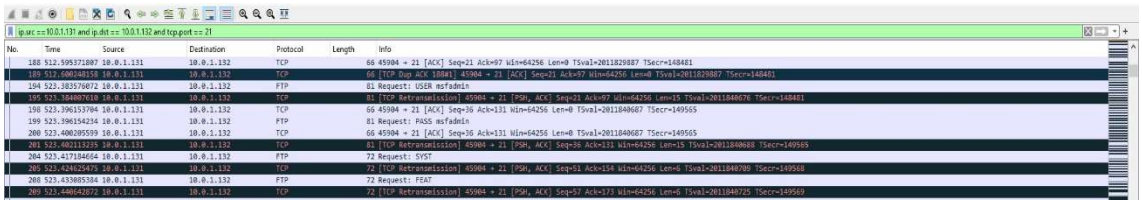
El siguiente filtro es por ip. Todos los paquetes que tiene como salida la ip 10.0.1.131, con el filtro “ip.src == 10.0.1.131”



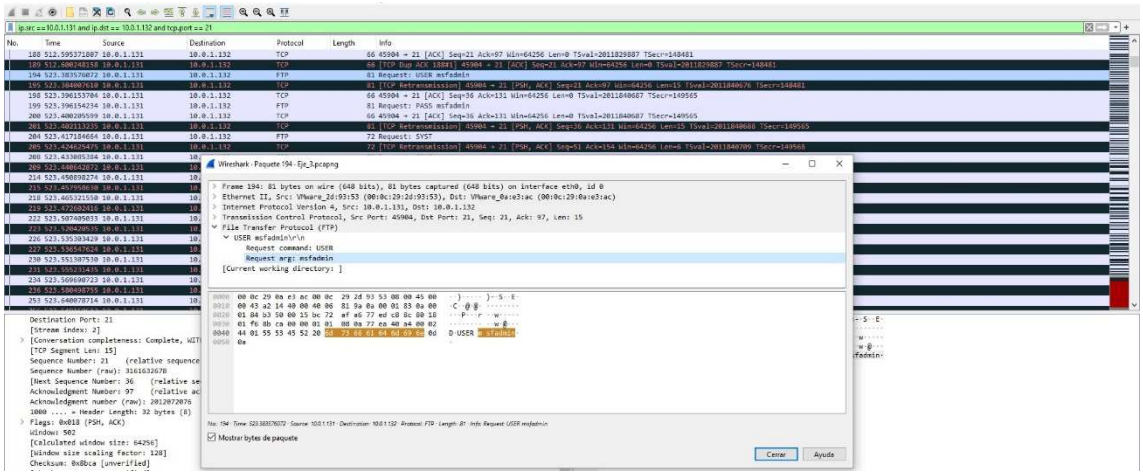
En el filtro anterior introducimos otro filtro para reducir mas la cantidad de paquetes, ponemos “ip.src == 10.01.131 and ip.dst == 10.1.0132”. Con este filtro podemos ver los paquetes que salen de la ip 10.0.1.131 y se dirigen a la ip 10.0.132



En el filtro anterior añadimos otro filtro que es para filtra los paquetes que van al puerto 21 del a ip 10.0.132 y comprobar si podemos ver alguna credencial del protocolo ftp.

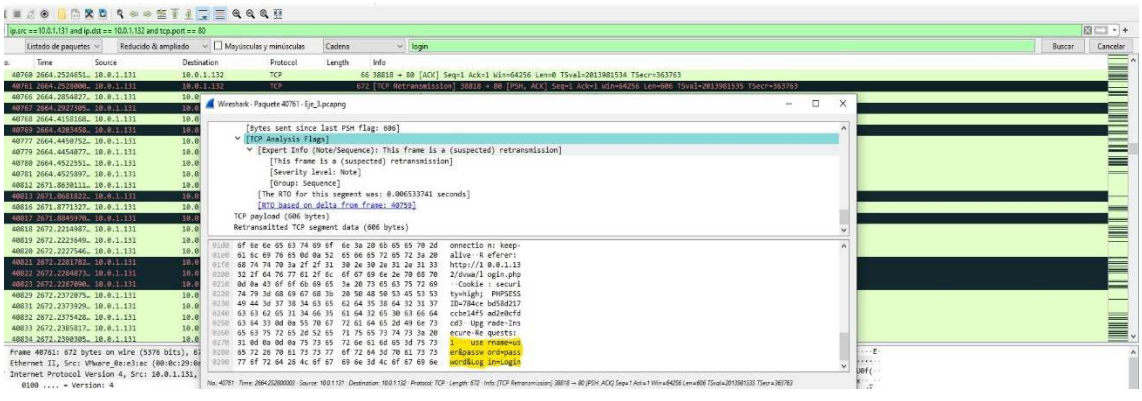


Como podemos comprobar las credenciales del ftp van en texto clara y podemos ver la captura del usuario y la contraseña.



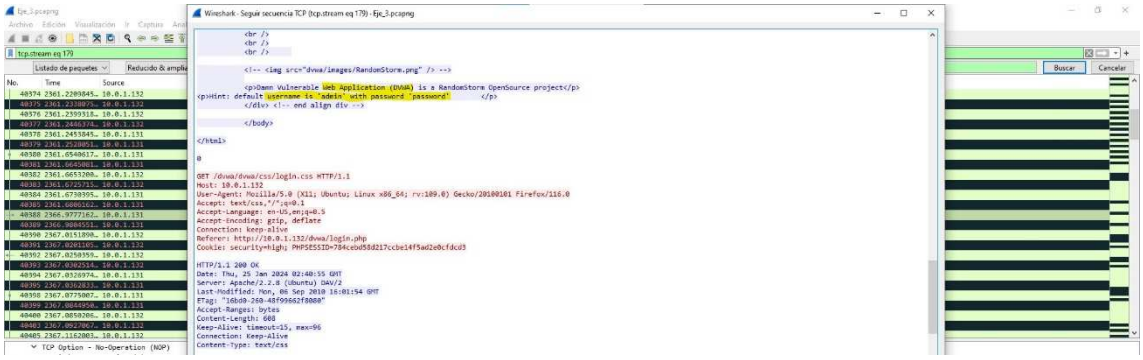
4.3 BÚSQUEDA POR PAQUETE

Con la búsqueda de paquete podemos filtrar la búsqueda por una cadena, filtro de visualización, valor hexadecimal y expresión regular. Utilizaremos el parámetro cadena y la búsqueda será con la palabra “login”, en el puerto 80.



Otra forma de ver la información es clicando el paquete que contenga información relevante y selecciona la opción de “seguir secuencia TCP”. En esta opción se nos abrirá una ventana don de nos mostrará la información de diferente forma más legible y entendible.


Wireshark · Seguir secuencia TCP (tcp.stream eq 2) · Eje_3.pcapng
220 (vsFTPd 2.3.4)
AUTH TLS
530 Please login with USER and PASS.
AUTH SSL
530 Please login with USER and PASS.
USER msfadmin
331 Please specify the password.
PASS msfadmin
230 Login successful.
SYST
215 UNIX Type: L8
FEAT
211-Features:
EPRT
EPSV
MDTM
PASV
REST STREAM
SIZE
TVFS
UTF8
211 End


Wireshark · Seguir secuencia TCP (tcp.stream eq 179) · Eje_3.pcapng

<!-- -->
Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project
Hint: default username is 'admin' with password 'password'
 <!-- end align div -->
</body>
</html>
0
GET /dvwa/dvwa/css/login.css HTTP/1.1
Host: 10.0.1.132
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/116.0
Accept: text/css,*/*;q=0.1
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://10.0.1.132/dvwa/login.php
Cookie: security=high; PHPSESSID=784ceb058d217ccbe14f5ad2e0cfdcd3
HTTP/1.1 200 OK
Date: Thu, 25 Jan 2024 02:40:55 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
Last-Modified: Mon, 08 Sep 2010 16:01:54 GMT
ETag: "16bd0-260-48f9662f8080"
Accept-Ranges: bytes
Content-Length: 608
Keep-Alive: timeout=15, max=96
Connection: Keep-Alive
Content-Type: text/css