

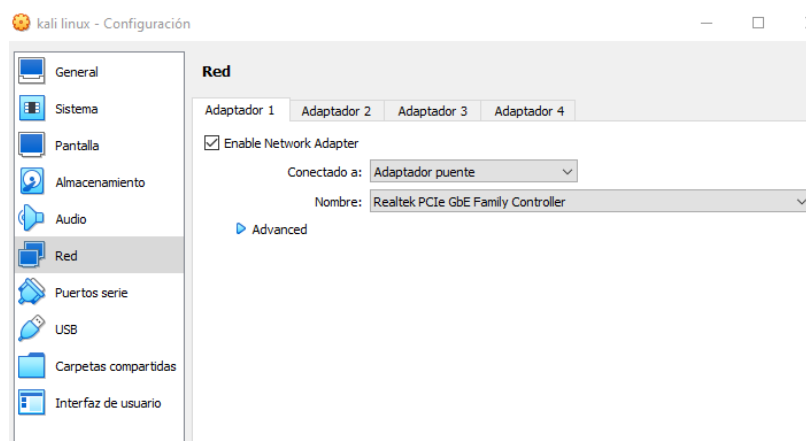
EJERCICIO FINAL - ATAQUES A INFRAESTRUCTURA DE SISTEMAS Y REDES

Definición de alcance y requisitos

- Suponed que tenemos un cliente (vosotros) y queréis conocer el estado de vuestra red.
- Vais a realizar vuestra primera "incursión" en entorno real, sin usar máquinas virtuales preparadas, y generaros un informe para vosotros mismos sobre lo que habéis hecho.
- Para realizar este ejercicio hay que tener en cuenta que los ataques y análisis van a realizarse en la propia red personal de cada uno, por lo que es necesario antes de nada, "pedir permiso" e "informar" al resto de usuarios de la red de los objetivos, horario para poder hacerlo, si el router está accesible para reiniciarlo (se puede quedar tonto en un ARP Spoofing si es de mala calidad), etc...
- **DISCLAIMER** - ¡¡¡Hacedlo con responsabilidad y cabeza!!! :-)

Configuración

- Configurar el tipo de red de Kali Linux como Bridge. De esta manera estará configurada como si fuera un equipo de la propia red. Comprobar que la IP asignada está en el rango de red del resto de equipos (móvil y máquina Host).



Selección de objetivos

- Realizar una identificación de equipos de toda la red.
- Identificar equipos por la MAC Address (recordad que podemos sacar basándonos en la MAC el fabricante y por lo tanto acotar que equipos son).
- Elegir un equipo como objetivo.

Nota: Contad con que al menos en la red hay 4 equipos:

Equipo 1) Kali Linux en modo Bridge.

Equipo 2) Vuestra máquina Host.

Equipo 3) Un teléfono móvil

Equipo 4) Router.

El resto serán otros equipos conectados (aparte de éstos) que haya en la red.

```

(root@kali)-[~]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.100.46 netmask 255.255.255.0 broadcast 192.168.100.255
    inet6 2803:2a00:2c16:6a1e:3af8:6854:4510:3585 prefixlen 64 scopeid 0<global>
    inet6 2803:2a00:2c16:6a1e:a00:27ff:fe4b:1f9f prefixlen 64 scopeid 0<global>
    inet6 fe80::a00:27ff:fe4b:1f9f prefixlen 64 scopeid 0<link>
    ether 08:00:27:4b:1f:9f txqueuelen 1000 (Ethernet)
    RX packets 41 bytes 23561 (23.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 53 bytes 23652 (23.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

```

(root@kali)-[~]
# nmap -sn 192.168.100.0-255
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-16 10:31 CET
Nmap scan report for 192.168.100.1
Host is up (0.0013s latency).
MAC Address: 64:2C:AC:F1:83:F0 (Huawei Technologies)
Nmap scan report for 192.168.100.3
Host is up (0.094s latency).
MAC Address: 60:AB:67:D9:9E:1B (Xiaomi Communications)
Nmap scan report for 192.168.100.34
Host is up.
MAC Address: 20:1E:88:12:F0:7F (Intel Corporate)
Nmap scan report for 192.168.100.39
Host is up (0.070s latency).
MAC Address: 7E:8D:4E:6D:0D:74 (Unknown)
Nmap scan report for 192.168.100.45
Host is up (0.00076s latency).
MAC Address: 50:EB:F6:E7:C3:62 (Asustek Computer)
Nmap scan report for 192.168.100.46
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 3.97 seconds

```

Equipo 1: Kali linux IP: 192.168.100.46

Manufacturer: PCS Systemtechnik Gmb

Equipo 2: maquina host IP: 192.168.100.45 Asustek computer

Manufacturer: ASUSTek COMPUTER INC

Equipo 3: teléfono móvil IP: 192.168.100.3 Xiomi communications

Manufacturer: Xiaomi Communications Co Ltd

Equipo 4: router IP: 192.168.100.1 Huawei technologies

Manufacturer: HUAWEI TECHNOLOGIES CO.,LTD

COMO OBJETIVO SE ESCOGE UNA COMPUTADORA PORTATIL QUE ES MIA,

IP: 192.168.100.34

MAC : 20:1E:88:12:F0:7F

Intel corporate, HP

Análisis de vulnerabilidades-Exploración

- Realizar una identificación de sistema operativo de un equipo objetivo. (También es importante para validar el punto anterior y ver que equipos son).

```
(root@kali)-[~]
# nmap -p- -O 192.168.100.34 -T 5
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-16 12:07 CET
Nmap scan report for 192.168.100.34
Host is up (0.0031s latency).
Not shown: 65529 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
7070/tcp   open  realserver
7680/tcp   open  pando-pub
49668/tcp  open  unknown
MAC Address: 20:1E:88:12:F0:7F (Intel Corporate)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows 10 (95%), Microsoft Windows Server 2008 SP1 (90%), Microsoft Windows 10 1703 (89%), Microsoft Windows 10 1511 - 1607 (88%), Microsoft Windows Phone 7.5 or 8.0 (88%), Microsoft Windows 10 1511 (87%), Microsoft Windows Server 2008 R2 or Windows 8.1 (87%), Microsoft Windows Server 2016 (87%), Microsoft Windows 7 Professional or Windows 8 (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 65.44 seconds
```

- Realizar una identificación de servicios y puertos abiertos del objetivo.

```
(root@kali)-[~]
# nmap -p- -sS 192.168.100.34 -T 5
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-16 12:23 CET
Nmap scan report for 192.168.100.34
Host is up (0.0038s latency).
Not shown: 65529 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
7070/tcp   open  realserver
7680/tcp   open  pando-pub
49668/tcp  open  unknown
MAC Address: 20:1E:88:12:F0:7F (Intel Corporate)

Nmap done: 1 IP address (1 host up) scanned in 57.39 seconds
```

- Realizar una identificación de versiones de servicios del objetivo.

En el screen de abajo se pueden divisar los puertos abiertos y sus versiones, como hay puertos cuya versión no trajo la herramienta los investigue, el puerto 445 El puerto TCP 445 se utiliza para el acceso directo a redes TCP / IP MS que no requiere el uso de una capa NetBIOS. Este servicio está disponible en Windows, comenzando con Windows 2000 y Windows XP. En Windows NT / 2K / XP, el protocolo SMB (Server Message Block) se utiliza para compartir archivos, entre otras cosas. Por otra parte, el puerto 7070, es el puerto predeterminado para transmisiones de Real Server. y el puerto 7680 es utilizado por WUDO (Optimización de entrega de actualizaciones de Windows) en las LAN de Windows. Esto incluye equipos locales y remotos dentro de un dominio.

```
(root@kali)-[~]
# nmap -p- -sSV 192.168.100.34-255 -T 5
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-16 12:33 CET
Stats: 0:03:35 elapsed; 218 hosts completed (3 up), 3 undergoing Service Scan
Service scan Timing: About 90.00% done; ETC: 12:37 (0:00:17 remaining)
Nmap scan report for 192.168.100.34
Host is up (0.0033s latency).
Not shown: 65529 filtered tcp ports (no-response)
PORT      STATE SERVICE          VERSION
135/tcp    open  msrpc            Microsoft Windows RPC
139/tcp    open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?
7070/tcp   open  ssl/realserver?
7680/tcp   open  pando-pub?
49668/tcp  open  msrpc            Microsoft Windows RPC
MAC Address: 20:1E:88:12:F0:7F (Intel Corporate)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Análisis de vulnerabilidades – Evaluación

- Realizar un análisis de vulnerabilidades con las herramientas utilizadas sobre el objetivo.

Procedemos a forzar y probar la conexión de Kali con la maquina objetivo.

```
(root@kali)-[~]
# ping 192.168.100.34
PING 192.168.100.34 (192.168.100.34) 56(84) bytes of data.
64 bytes from 192.168.100.34: icmp_seq=1 ttl=128 time=2.77 ms
64 bytes from 192.168.100.34: icmp_seq=2 ttl=128 time=3.38 ms
64 bytes from 192.168.100.34: icmp_seq=3 ttl=128 time=3.10 ms
64 bytes from 192.168.100.34: icmp_seq=4 ttl=128 time=3.41 ms
64 bytes from 192.168.100.34: icmp_seq=5 ttl=128 time=3.32 ms
64 bytes from 192.168.100.34: icmp_seq=6 ttl=128 time=2.98 ms
64 bytes from 192.168.100.34: icmp_seq=7 ttl=128 time=4.13 ms
64 bytes from 192.168.100.34: icmp_seq=8 ttl=128 time=2.93 ms
64 bytes from 192.168.100.34: icmp_seq=9 ttl=128 time=3.35 ms
64 bytes from 192.168.100.34: icmp_seq=10 ttl=128 time=3.75 ms
64 bytes from 192.168.100.34: icmp_seq=11 ttl=128 time=3.01 ms
64 bytes from 192.168.100.34: icmp_seq=12 ttl=128 time=3.51 ms
^C64 bytes from 192.168.100.34: icmp_seq=13 ttl=128 time=2.90 ms
64 bytes from 192.168.100.34: icmp_seq=14 ttl=128 time=2.37 ms
64 bytes from 192.168.100.34: icmp_seq=15 ttl=128 time=2.94 ms
^C
— 192.168.100.34 ping statistics —
15 packets transmitted, 15 received, 0% packet loss, time 14026ms
rtt min/avg/max/mdev = 2.367/3.190/4.125/0.414 ms
```


Vulners arrojó varios puertos abiertos, el 135, 139, 445 y 7070. De estos puertos el más vulnerable es el 7070, ya que permite a los atacantes remotos provocar una denegación de servicio mediante el envío de datos con formato incorrecto al servidor en el puerto 7070, también la obtención de acceso no autorizado a un usuario local

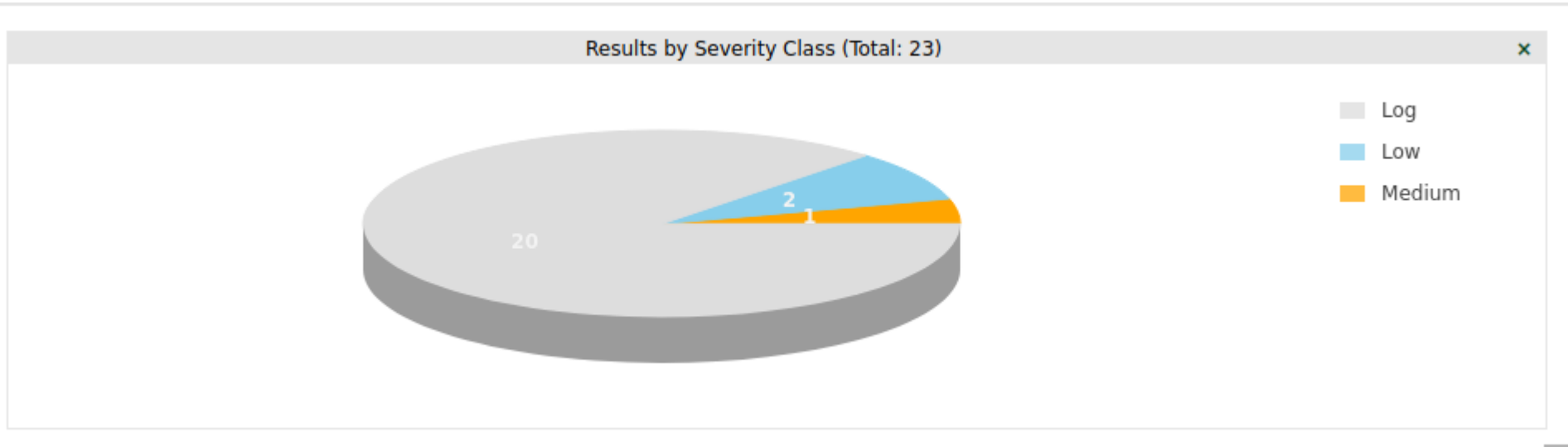
```
(root@kali)-[/usr/share/nmap/scripts/vulscan]
# nmap -sV --script vulners 192.168.100.34
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-16 13:15 CET
Nmap scan report for 192.168.100.34
Host is up (0.0020s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE          VERSION
135/tcp    open  msrpc            Microsoft Windows RPC
139/tcp    open  netbios-ssn      Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?
7070/tcp   open  ssl/realserver?
MAC Address: 20:1E:88:12:F0:7F (Intel Corporate)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.95 seconds
```

Los gráficos abajo presentados son el resultado del análisis realizado por la herramienta OPENVAS, el cual arrojo vulnerabilidades de severidad media una vez escaneada la maquina objetivo.

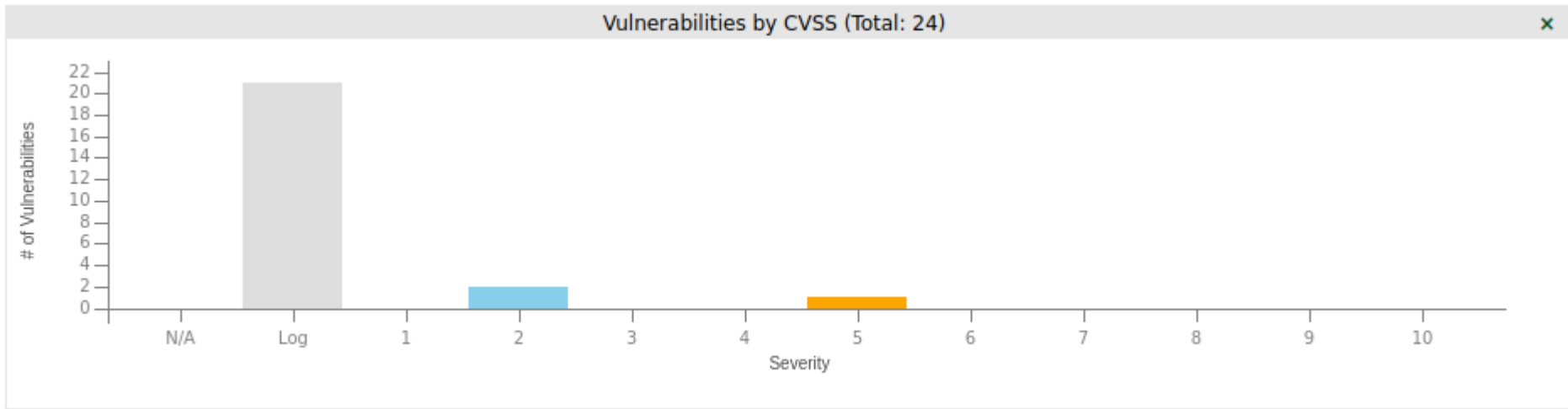


Name	Title	Severity		
		Latest ▼	Highest	Average
 cpe:/o:microsoft:windows		5.0 (Medium)	5.0 (Medium)	5.0 (Medium)

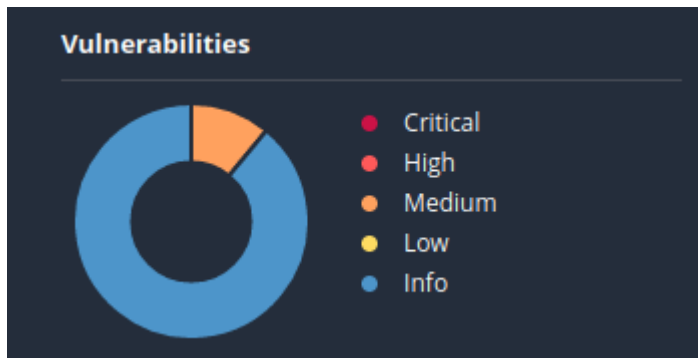


En el screen abajo presentado se puede ver que la vulnerabilidad de severidad media encontrada corresponde a Informes de enumeración de servicios DCE/RPC y MSRPC, el impacto que podría tener esta vulnerabilidad si algún atacante se aprovechara de esta es obtener conocimiento del host remoto y la solución seria filtrar el trafico de este puerto. Además se presentan otras vulnerabilidades (2) que son de baja severidad

Vulnerability	Severity ▼	QoD	Host IP	Name	Location	Created
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80 %	192.168.100.34		135/tcp	Fri, Dec 16, 2022 12:31 PM UTC
TCP timestamps	2.6 (Low)	80 %	192.168.100.34		general/tcp	Fri, Dec 16, 2022 12:30 PM UTC
ICMP Timestamp Reply Information Disclosure	2.1 (Low)	80 %	192.168.100.34		general/icmp	Fri, Dec 16, 2022 12:30 PM UTC



Nessus confirmo lo ya analizado por openvas, la severidad de la vulnerabilidad es media como se puede ver en la imagen abajo.



La vulnerabilidad de severidad media arrojada por Nessus expone al puerto 445. El cual se encuentra abierto, y que expone que no es necesario firmar en el servidor SMB remoto. Un atacante remoto no autenticado puede aprovechar esto para realizar ataques de intermediario contra el servidor SMB. La solución sería firmar la política de seguridad de red.

MEDIUM

SMB Signing not required

Description

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

Solution

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

See Also

<http://www.nessus.org/u?df39b8b3>

<http://technet.microsoft.com/en-us/library/cc731957.aspx>

<http://www.nessus.org/u?74b80723>

<https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html>

<http://www.nessus.org/u?a3cac4ea>

Output

No output recorded.

To see debug logs, please visit individual host

Port ▲	Hosts
--------	-------

445 / tcp / cifs	192.168.100.34
------------------	----------------

La otra vulnerabilidad se relación con la certificación SSL, la cual no es confiable por lo que debería adquirir esta certificación ya que si no se realiza podría ser vulnerable a un ataque man in the middle.

MEDIUM

SSL Certificate Cannot Be Trusted

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.
- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.
- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

Solution

Purchase or generate a proper SSL certificate for this service.

- *Comprobar si hay alguna vulnerabilidad crítica (CVSS alto) sobre el objetivo.*

Mas arriba se puede ver que se usaron las herramientas openvas y Nessus para este propósito y ninguna de este arrojo vulnerabilidad critica.

Ataque MITM y captura/sniffing de tráfico

Realizar un ataque MITM entre un equipo de la red y el router para capturar tráfico entre ellos, e intentar averiguar a qué servicios, IPs y webs se está accediendo.

En caso que se utilice algún protocolo inseguro, es posible analizar la información más en detalle utilizando varias reglas en wireshark, de forma "que sea trafico ftp O tráfico telnet O trafico http" para poder ayudarlos en el análisis.

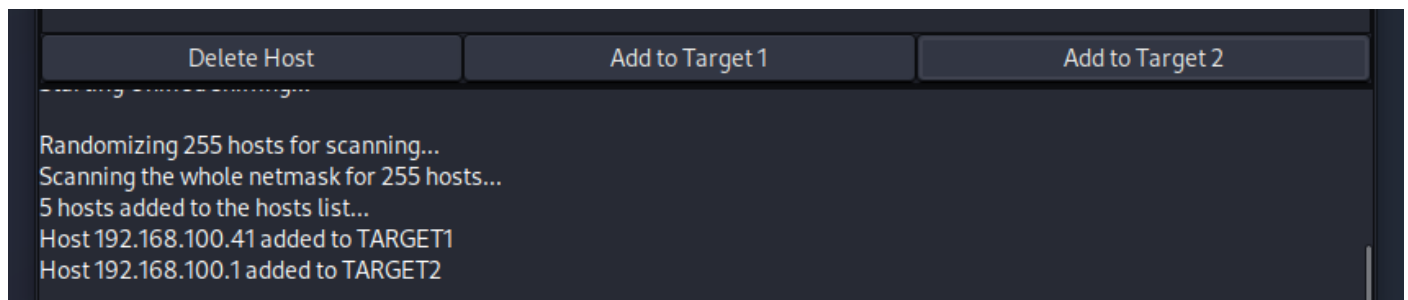
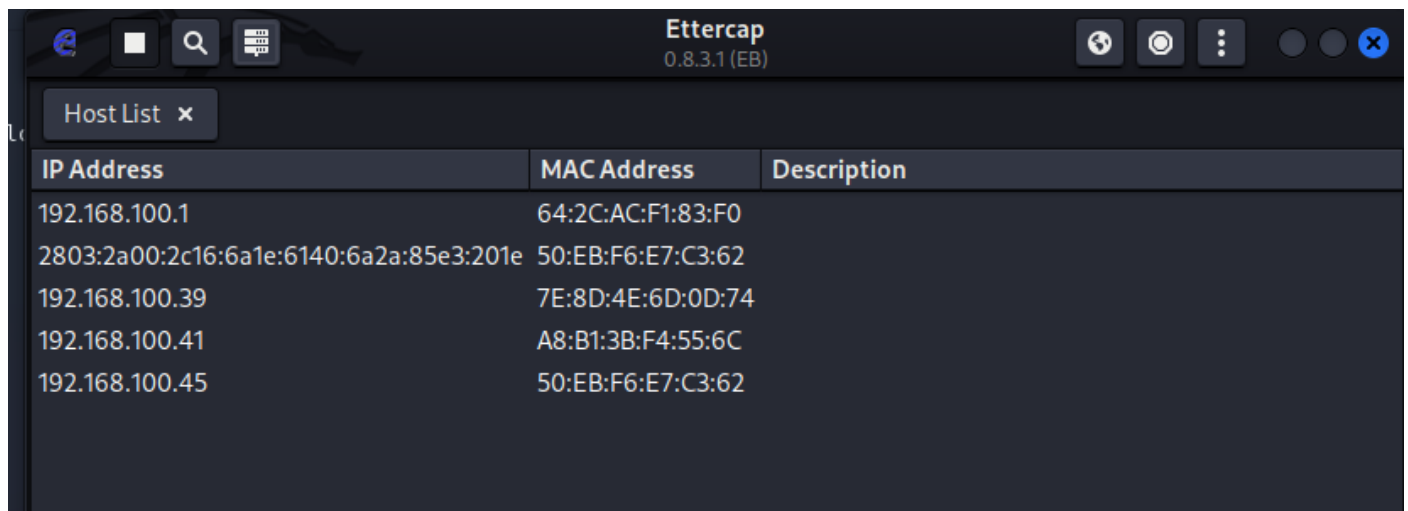
Ejemplo: Usuarios y contraseñas que se transmitan en "texto plano", hay en http, ftp y telnet entre otros, como hemos visto en clase.

Se procedio a realizar el ataque man in the middle, entre dos dispositivos uno

KALI LINUX IP: 192.168.100.46 MAC 08:00:27:4b:1f:9f

INTEL CORPORATE ETH0: 192.168.100.41 MAC A8:B1:3B:F4:55:6C

El atacante es Kali linux, la maquina Windows es la victima 1 y el router la victima 2



En este punto comprobamos que el router fue suplantado por Kali linux (el atacante), se puede ver en la imagen de abajo como la MAC del router y la de Kali son iguales.

Interface: 192.168.100.41 --- 0xd		
Internet Address	Physical Address	Type
192.168.100.1	08-00-27-4b-1f-9f	dynamic
192.168.100.34	20-1e-88-12-f0-7f	dynamic
192.168.100.46	08-00-27-4b-1f-9f	dynamic
192.168.100.255	ff-ff-ff-ff-ff-ff	static
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.251	01-00-5e-00-00-fb	static
224.0.0.252	01-00-5e-00-00-fc	static
239.255.255.250	01-00-5e-7f-ff-fa	static
255.255.255.255	ff-ff-ff-ff-ff-ff	static

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

http.request.method == POST

No.	Time	Source	Destination	Protocol	Length	Info
5293	29.440786095	192.168.100.41	190.211.241.99	HTTP	736	POST /valida
33627	277.089795503	192.168.100.41	65.61.137.117	HTTP	757	POST /doLogi
86372	525.980782981	192.168.100.41	34.95.207.168	HTTP	1451	POST /newsv3

Frame 5293: 736 bytes on wire (5888 bits),
 Ethernet II, Src: HP_f4:55:6c (a8:b1:3b:f4):
 Internet Protocol Version 4, Src: 192.168.100.41
 Transmission Control Protocol, Src Port: 5000
 Hypertext Transfer Protocol
 HTML Form URL Encoded: application/x-www-form-urlencoded
 Form item: "usuario" = "88661"
 Form item: "clave" = "cafemayo"

Paquetes: 89975 · Mostrado: 3 (0.0%) · Perdido: 0 (0.0%) · Perfil: Default

The screenshot shows the Wireshark network protocol analyzer interface. The top pane displays a list of captured packets:

No.	Time	Source	Destination	Protocol	Length	Info
5293	29.440786095	192.168.100.41	190.211.241.99	HTTP	736	POST /valida
33627	277.089795503	192.168.100.41	65.61.137.117	HTTP	757	POST /doLogi
86372	525.980782981	192.168.100.41	34.95.207.168	HTTP	1451	POST /news3

The middle pane shows the details of the selected packet (No. 33627). The 'Hypertext Transfer Protocol' section is expanded, showing the 'HTML Form URL Encoded' data:

```
application/x-www-form-urlencoded
uid=vero56&passw=root&btnSubmit=Acceso
```

The bottom pane shows the raw packet data in hexadecimal and ASCII format.

ArchivoEdiciónVisualizaciónIrCapturaAnalizarEstadísticasTelefoníaWirelessHerramientasAyuda

http.request.method == POST

No.	Time	Source	Destination	Protocol	Length	Info
5293	29.440786095	192.168.100.41	190.211.241.99	HTTP	736	POST /valida...
33627	277.089795503	192.168.100.41	65.61.137.117	HTTP	757	POST /doLogir...
86372	525.980782981	192.168.100.41	34.95.207.168	HTTP	1451	POST /newsv3/...

Frame 86372: 1451 bytes on wire (11608 bits), 1451 bytes captured (11608 bits) on inter

Ethernet II, Src: HP_f4:55:6c (a8:b1:3b:f4:55:6c), Dst: PcsCompu_4b:1f:9f (08:00:27:4b:

Internet Protocol Version 4, Src: 192.168.100.41, Dst: 34.95.207.168

Transmission Control Protocol, Src Port: 51389, Dst Port: 80, Seq: 1, Ack: 1, Len: 1397

Hypertext Transfer Protocol

HTML Form URL Encoded: application/x-www-form-urlencoded

Form item: "g-recaptcha-response" = "03AD1IbLDQPZg9BYXpz0oaCgXTXaQvs8iUEgjaWAi08BigP7

Form item: "email" = "verofrancof4616834@gmail.com"

Form item: "newsletterReturnEmailreturn" = ""

Form item: "newsletteremailvalido" = ""

wireshark_eth00PA1W1.pcapng

Paquetes: 89975 · Mostrado: 3 (0.0%) · Perdido: 0 (0.0%) · Perfil: Default