

PRÁCTICA 2. Análisis de Servicios en Red, Control de Acceso, Gestión de Usuarios

PRIMERA PARTE

a. Usando la página de manual de nmap, documente las funciones y opciones básicas de nmap.

El comando nmap se utiliza para el mapeo de la red, así como descubrir servicios e identificar puertos abiertos (analizador de puertos).

Existen $2^{16} = 65036$ puertos (servicios), estos pueden ser TCP o UDP (protocolos de la capa de transporte), y existen 65036 de cada uno de los tipos.

-El comando ***nmap por defecto*** va a analizar los 1000 puertos TCP más utilizados (el resto no son escaneados). Aquí una prueba ejecutando el comando nmap desde la máquina virtual mallet, a alice.

```
mallet@mallet:~$ nmap 10.0.2.4


Starting Nmap 5.00 ( http://nmap.org ) at 2022-09-22 13:06 CEST
Interesting ports on 10.0.2.4:
Not shown: 990 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
80/tcp    open  http
111/tcp   open  rpcbind
443/tcp   open  https
700/tcp   open  unknown
2049/tcp  open  nfs
6000/tcp  open  X11
```

-La opción ***-n*** (nmap 10.0.2.4 -n) hace que nmap no intente adivinar el nombre completamente cualificado de las máquinas, evita que haga resolución inversa de DNS.

-Añadiendo ***-v*** (nmap 10.0.2.4 -v) permite que nmap muestre todo lo que está haciendo cuando hace un descubrimiento de los servicios.

```
mallet@mallet:~$ nmap 10.0.2.4 -v

Starting Nmap 5.00 ( http://nmap.org ) at 2022-09-22 17:02 CEST
NSE: Loaded 0 scripts for scanning.
Initiating Ping Scan at 17:02
Scanning 10.0.2.4 [2 ports]
Completed Ping Scan at 17:02, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:02
Completed Parallel DNS resolution of 1 host. at 17:02, 0.00s elapsed
Initiating Connect Scan at 17:02
Scanning 10.0.2.4 (10.0.2.4) [1000 ports]
Discovered open port 25/tcp on 10.0.2.4
Discovered open port 80/tcp on 10.0.2.4
Discovered open port 111/tcp on 10.0.2.4
Discovered open port 22/tcp on 10.0.2.4
Discovered open port 21/tcp on 10.0.2.4
Discovered open port 23/tcp on 10.0.2.4
Discovered open port 443/tcp on 10.0.2.4
Discovered open port 6000/tcp on 10.0.2.4
Discovered open port 2049/tcp on 10.0.2.4
Completed Connect Scan at 17:02, 0.06s elapsed (1000 total ports)
Host 10.0.2.4 (10.0.2.4) is up (0.0014s latency).
```



-Para que nmap analice todos los puertos, y no solo los 1000 más utilizados añadimos **-p-** (nmap 10.0.2.4 -p-), como se ve ahora 65522 puertos están cerrados.

```
mallet@mallet:~$ nmap 10.0.2.4 -p-
Starting Nmap 5.00 ( http://nmap.org ) at 2022-09-22 13:12 CEST
Interesting ports on 10.0.2.4:
Not shown: 65522 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
80/tcp    open  http
111/tcp   open  rpcbind
443/tcp   open  https
700/tcp   open  unknown
2049/tcp  open  nfs
6000/tcp  open  X11
33526/tcp open  unknown
45759/tcp open  unknown
56520/tcp open  unknown
```

-Hasta ahora, solo ha analizado los puertos TCP, pero si queremos que únicamente escanease los UDP añadimos **-sU** (nmap 10.0.2.4 -sU). Nos pide requisitos de super usuario, por ello añadido sudo antes del comando.

-Si queremos que únicamente escanease un puerto en específico añadimos **-pX (siendo X el número de un puerto en específico)**, en este caso escaneamos el puerto 53 TCP de ns3.uva.es primero, y después el puerto 53 UDP de ns3.uva.es con -sU, igual que en el punto anterior.

```
mallet@mallet:~$ nmap ns3.uva.es -p53
Starting Nmap 5.00 ( http://nmap.org ) at 2022-09-22 13:19 CEST
Interesting ports on dali.eis.uva.es (157.88.200.33):
PORT      STATE SERVICE
53/tcp    open  domain

Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
mallet@mallet:~$ sudo nmap ns3.uva.es -p53 -sU
Starting Nmap 5.00 ( http://nmap.org ) at 2022-09-22 13:20 CEST
Interesting ports on dali.eis.uva.es (157.88.200.33):
PORT      STATE SERVICE
53/udp    open|filtered domain
```

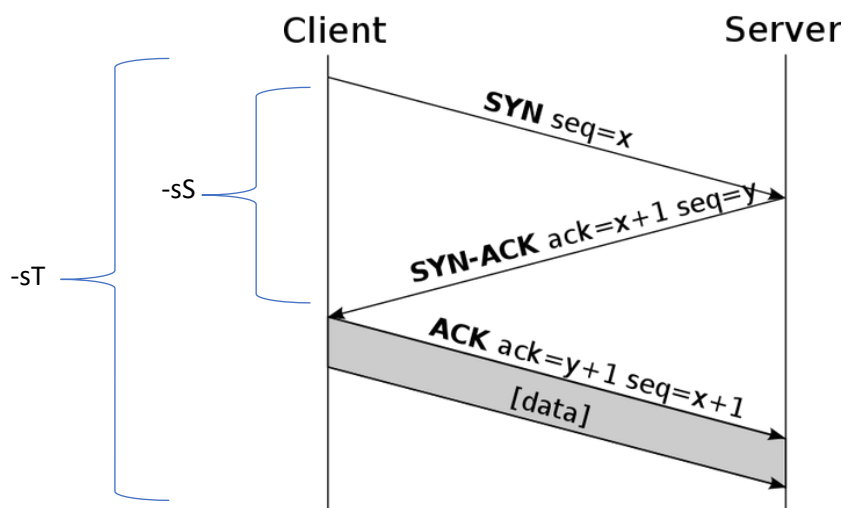
-Para realizar un escaneo del puerto anterior en TCP y UDP a la vez en un único comando bastaría con añadir **-sT**, que realiza el escaneo de tipo **TCP completo** (nmap 10.0.2.4 -p53 -sU -sT), como se ve todas las distintas opciones se pueden combinar distintamente para adaptar el escaneo a lo que se quiera.

```
mallet@mallet:~$ sudo nmap 10.0.2.4 -p53 -sU -sT
Starting Nmap 5.00 ( http://nmap.org ) at 2022-09-22 17:31 CEST
Interesting ports on 10.0.2.4 (10.0.2.4):
PORT      STATE SERVICE
53/tcp    closed domain
53/udp    closed domain
```

-Ahora otro tipo de escaneo de tipo **TCP**, pero ahora de tipo **SYN**, añadiendo **-sS** (nmap ns3.uva.es -p53 -sU -sS), este tipo de escaneo es más “sigiloso”.

```
mallet@mallet:~$ sudo nmap 10.0.2.4 -p53 -sU -sS
Starting Nmap 5.00 ( http://nmap.org ) at 2022-09-22 17:27 CEST
Interesting ports on 10.0.2.4 (10.0.2.4):
PORT      STATE SERVICE
53/tcp    closed domain
53/udp    closed domain
```

Como se ve la salida es la misma pero la forma en la que el cliente y el servidor establecen la comunicación es bastante diferente. [1]



-Ahora un para realizar un escaneo de tipo NULO, añadiríamos **-sN**, que requiere permisos de super usuario (sudo nmap 10.0.2.4 -sN).

```
mallet@mallet:~$ sudo nmap 10.0.2.4 -sN
Starting Nmap 5.00 ( http://nmap.org ) at 2022-09-22 17:46 CEST
Interesting ports on 10.0.2.4 (10.0.2.4):
Not shown: 991 closed ports
PORT      STATE SERVICE
21/tcp    open|filtered ftp
22/tcp    open|filtered ssh
23/tcp    open|filtered telnet
25/tcp    open|filtered smtp
80/tcp    open|filtered http
111/tcp   open|filtered rpcbind
443/tcp   open|filtered https
2049/tcp  open|filtered nfs
6000/tcp  open|filtered X11
MAC Address: 08:00:27:F9:69:5E (Cadmus Computer Systems)
```

-Y para realizar un escaneo de ACK, usaríamos -sA, que también requiere de permisos de super usuario (sudo nmap 10.0.2.4 -sA).

```
mallet@mallet:~$ sudo nmap 10.0.2.4 -sA

Starting Nmap 5.00 ( http://nmap.org ) at 2022-09-22 18:22 CEST
All 1000 scanned ports on 10.0.2.4 (10.0.2.4) are unfiltered
MAC Address: 08:00:27:F9:69:5E (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```

-Para conocer la versión de un servicio que ofrece un determinado puerto, utilizamos -sV, en este caso combinado con -p puesto que queremos que nos diga la versión de un servicio en concreto en este caso el 80 (nmap 10.0.2.4 -p80 -sV).

```
mallet@mallet:~$ sudo nmap 10.0.2.4 -p80 -sV

Starting Nmap 5.00 ( http://nmap.org ) at 2022-09-22 18:27 CEST
Interesting ports on 10.0.2.4 (10.0.2.4):
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.2.14 ((Ubuntu))
MAC Address: 08:00:27:F9:69:5E (Cadmus Computer Systems)

Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.11 seconds
```

Se obtiene que el puerto 80, es un servicio http, de Apache 2.2.14.

b. Active un proceso de monitorización tcp en mallet para poder seguir los diferentes métodos de scanning.

Para activar un proceso de monitorización tcp recurrimos a tcpdump, para ello vamos a necesitar permisos de super usuario y proporcionar una serie de opciones al comando. El comando es:

```
sudo tcpdump -i eth4
```

Donde -i nos permite indicarle la interfaz de red para que la analice, por tanto, antes debemos conocer la red, y sabemos que la red donde están conectadas todas las máquinas es "eth4".

Primero compruebo si la red eth4 está disponible, con el comando `sudo tcpdump -D`

```
mallet@mallet:~$ sudo tcpdump -D
1.usbmon1 (USB bus number 1)
2.eth4
3.any (Pseudo-device that captures on all interfaces)
4.lo
```

Y vemos que si lo está. Entonces ahora activo un proceso de monitorización TCP en mallet:

```
mallet@mallet:~$ sudo tcpdump -i eth4
tcpdump: listening on eth4, link-type EN10MB (Ethernet), capture size 96 bytes
```

Y para comprobar si funciona hago un ping de alice a bob de 2 paquetes:

```
alice@alice:~$ ping 10.0.2.15 -c 2
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=0.259 ms
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.268 ms

--- 10.0.2.15 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.259/0.263/0.268/0.016 ms
```

Y observamos en el proceso de monitorización tcp que se captura el ping de alice a bob.

```
mallet@mallet:~$ sudo tcpdump -i eth4
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth4, link-type EN10MB (Ethernet), capture size 96 bytes
17:06:12.537480 IP alice.local > 10.0.2.15: ICMP echo request, id 63238, seq 1, length 64
17:06:12.537491 IP 10.0.2.15 > alice.local: ICMP echo reply, id 63238, seq 1, length 64
17:06:12.537865 IP mallet.local.50990 > 212.230.135.1.domain: 16733+ PTR? 15.2.0.10.in-addr.arpa. (40)
17:06:12.545191 IP 212.230.135.1.domain > mallet.local.50990: 16733 NXDomain 0/1/0 (117)
17:06:12.646726 IP mallet.local.mdns > 224.0.0.251.mdns: 0 PTR (QM)? 15.2.0.10.in-addr.arpa. (40)
17:06:13.536853 IP alice.local > 10.0.2.15: ICMP echo request, id 63238, seq 2, length 64
17:06:13.536859 IP 10.0.2.15 > alice.local: ICMP echo reply, id 63238, seq 2, length 64
```

En caso de que queramos monitorizar un puerto concreto deberíamos de añadir **port X** (número del puerto concreto de origen o destino), y para obtener más información **-e**, por ejemplo, el comando de a continuación únicamente monitoriza el puerto 80, obteniendo más información de la que se muestra por defecto, además puedes seleccionar si monitorizas solo TCP o UDP, indicando tcp o udp:

```
sudo tcpdump -i eth4 tcp -v port 80 -e
```

c. Usando nmap, realice y documente un barrido de puertos UDP en alice y compare con los datos que se obtienen a través de tcpdump.

Para realizar un barrido UDP de puertos completos de alice, pondríamos este comando:

```
mallet@mallet:~$ sudo nmap 10.0.2.4 -n -p- -sU
```

Pero tarda demasiado, por tanto, para hacer un ejemplo de lo que pide el enunciado nos vamos a centrar en un único puerto UDP.

Abrimos dos terminales en mallet en una activaremos el tcpdump (necesitamos permisos de super usuario, puesto que pone la tarjeta de red en modo promiscuo) y en otra haremos el barrido de puertos UDP (lo haremos con el puerto 67), puesto que todos tarda mucho tiempo.

Para activar el tcpdump el comando es: *sudo tcpdump -i eth4*

Y para analizar el puerto 67 UDP en otra terminal ponemos: *sudo nmap 10.0.2.4 -sU -p67*

Observamos esto:


```
mallet@mallet:~$ sudo nmap 10.0.2.4 -n -p67 -sU
Starting Nmap 5.00 ( http://nmap.org ) at 2022-09-29 12:51 CEST
Interesting ports on 10.0.2.4:
PORT      STATE SERVICE
67/udp    closed dhcpcd
MAC Address: 08:00:27:F9:69:5E (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds

mallet@mallet: ~
File Edit View Terminal Help
mallet@mallet:~$ sudo tcpdump -i eth4 udp port 67 -v
tcpdump: listening on eth4, link-type EN10MB (Ethernet), capture size 96 bytes
12:51:27.122580 IP (tos 0x0, ttl 54, id 31516, offset 0, flags [none], proto UDP
(17), length 28)
    mallet.local.61926 > alice.local.bootps: [|bootp]
```

Vemos que se utiliza bootp, antecesor de DHCP, nmap para saber si el puerto está abierto o cerrado, conoce el servicio y le envía una petición. Si la responde está abierto y si no, está cerrado, por ello realizar un barrido de todos los puertos UDP lleva tanto tiempo, porque nmap se queda esperando una respuesta de estos.

Ahora vamos a realizar un escaneo del puerto 80, mediante TCP, utilizando TCP SYN que es el que utiliza nmap por defecto y utilizando TCP Completo:

Con **TCP SYN**:

```
mallet@mallet:~$ sudo nmap 10.0.2.4 -n -p80
[sudo] password for mallet:

Starting Nmap 5.00 ( http://nmap.org ) at 2022-09-29 12:33 CEST
Interesting ports on 10.0.2.4:
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 08:00:27:F9:69:5E (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
mallet@mallet:~$

mallet@mallet:~$ sudo tcpdump -i eth4 tcp port 80 -v
tcpdump: listening on eth4, link-type EN10MB (Ethernet), capture size 96 bytes
12:33:41.249603 IP (tos 0x0, ttl 53, id 32507, offset 0, flags [none], proto TCP
(6), length 44)
    mallet.local.62436 > alice.local.www: Flags [S], cksum 0x2006 (correct), seq
    3459749291, win 2048, options [mss 1460], length 0
12:33:41.249832 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6),
    length 44)
    alice.local.www > mallet.local.62436: Flags [S.], cksum 0x78f1 (correct), se
    q 809068538, ack 3459749292, win 5840, options [mss 1460], length 0
12:33:41.249846 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6),
    length 40)
    mallet.local.62436 > alice.local.www: Flags [R], cksum 0x3fbf (correct), seq
    3459749292, win 0, length 0
^C
3 packets captured
3 packets received by filter
0 packets dropped by kernel
```

Con **TCP Completo**:

```
mallet@mallet:~$ sudo nmap 10.0.2.4 -n -p80 -sT

Starting Nmap 5.00 ( http://nmap.org ) at 2022-09-29 12:44 CEST
Interesting ports on 10.0.2.4:
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 08:00:27:F9:69:5E (Cadmus Computer Systems)

mallet@mallet: ~
File Edit View Terminal Help

tcpdump: listening on eth4, link-type EN10MB (Ethernet), capture size 96 bytes
12:44:24.221534 IP (tos 0x0, ttl 64, id 22112, offset 0, flags [DF], proto TCP (6), length 60)
    mallet.local.60169 > alice.local.www: Flags [S], cksum 0x4c9a (correct), seq 2310882953, win 5840, options [mss 1460,sackOK,TS val 397545 ecr 0,nop,wscale 5], length 0
12:44:24.221744 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 60)
    alice.local.www > mallet.local.60169: Flags [S.], cksum 0x9627 (correct), seq 2297696604, ack 2310882954, win 5792, options [mss 1460,sackOK,TS val 400443 ecr 397545,nop,wscale 5], length 0
12:44:24.221767 IP (tos 0x0, ttl 64, id 22113, offset 0, flags [DF], proto TCP (6), length 52)
    mallet.local.60169 > alice.local.www: Flags [R.], cksum 0xdad9 (correct), ack 1, win 183, options [nop,nop,TS val 397546 ecr 400443], length 0
12:44:24.222335 IP (tos 0x0, ttl 64, id 22114, offset 0, flags [DF], proto TCP (6), length 52)
    mallet.local.60169 > alice.local.www: Flags [R.], cksum 0xdad5 (correct), seq 1, ack 1, win 183, options [nop,nop,TS val 397546 ecr 400443], length 0
```

Podemos ver los send, ACK y resets que se envían entre cliente y servidor. Y ver que sigue el esquema del ejercicio 1 [1].

d. Documente toda la información sobre el servicio web que se ejecuta en alice usando una simple conexión telnet.

Para conocer toda la información sobre el servicio web tenemos que conocer que el puerto HTTP es el 80, pero primero tenemos que ver si el puerto 80 está abierto:

```
mallet@mallet:~$ sudo nmap 10.0.2.4 -p80

Starting Nmap 5.00 ( http://nmap.org ) at 2022-09-22 19:30 CEST
Interesting ports on 10.0.2.4 (10.0.2.4):
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 08:00:27:F9:69:5E (Cadmus Computer Systems)
```

Y podemos ver que si lo está. Por tanto, podremos ejecutar el comando telnet a este puerto.

El comando queda así: telnet 10.0.2.4 80. Y después deberemos introducir GET / HTTP/1.1 como pone en el CH3-Basin, también podríamos poner HEAD, como hicimos en clase.

```
mallet@mallet:~$ telnet 10.0.2.4 80
Trying 10.0.2.4...
Connected to 10.0.2.4.
Escape character is '^]'.
GET / HTTP/1.1
HTTP/1.1 400 Bad Request
Date: Thu, 22 Sep 2022 16:53:52 GMT
Server: Apache/2.2.14 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 301
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
</p>
<hr>
<address>Apache/2.2.14 (Ubuntu) Server at 127.0.0.1 Port 80</address>
</body></html>
Connection closed by foreign host.
```

Ahora poniendo i obtenemos un fragmento de código HTML (formato original), de lo que parece ser la página web de alice:

```
<html>
  <head>
    <title> Alice's Homepage </title>
    <link type="text/css" href="/main.css" rel="stylesheet" />
  </head>

  <body>
    <div id="page">
      <div id="title">
        Welcome to my website
      </div>

      <div id="menu">
        <a href="/">Home</a> <spacer type="horizontal"/><a
href='/?id=forum'>Alice's Message Board</a> <spacer type="horizontal"/>
      </div>

      <div id="content">
      </div>
    </div>
  </body>
</html>
Connection closed by foreign host.
```

e. Elabore un informe de vulnerabilidades de alice usando el analizador de barrido openvas. Documente cómo debe iniciarse este analizador y los resultados que encuentre.

Primero abrimos un servidor de openvas (analizador de barrido que se pide) en la máquina de mallet, y se nos cargarán todos los plugins:


```
mallet@mallet:~$ sudo openvasd
W32.Sasser.Worm.nasl could not be added to the cache and is likely to stay invis
ible to the client.
All plugins loaded
```

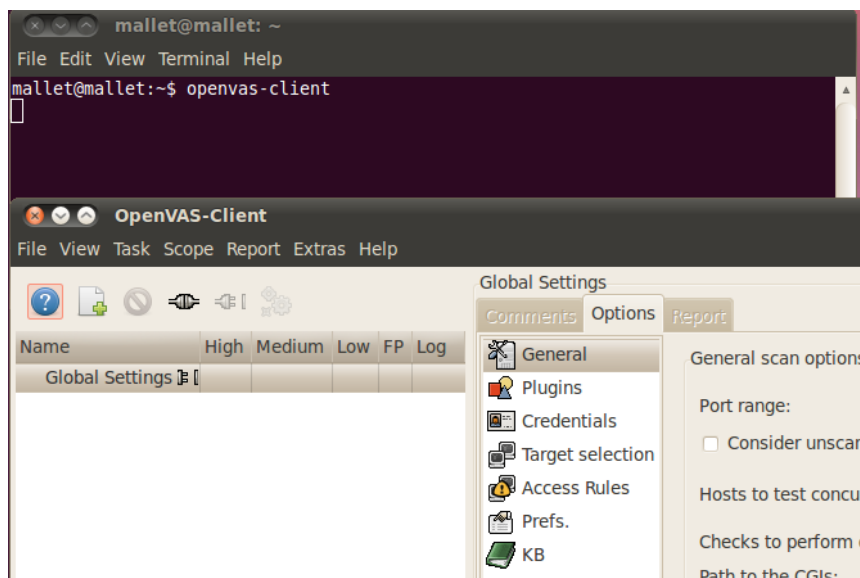
Primero antes de comenzar a realizar el análisis de vulnerabilidades, debemos de consultar el estado del servidor, y después iniciarlo, ya que sin el servidor “localhost” no podemos comenzar el análisis:

```
mallet@mallet:~$ sudo /etc/init.d/openvas-server status
OpenVAS daemon is not running.
mallet@mallet:~$ sudo /etc/init.d/openvas-server start
W32.Sasser.Worm.nasl could not be added to the cache and is like
ible to the client.
openvasd.
mallet@mallet:~$ sudo nmap localhost -p9390

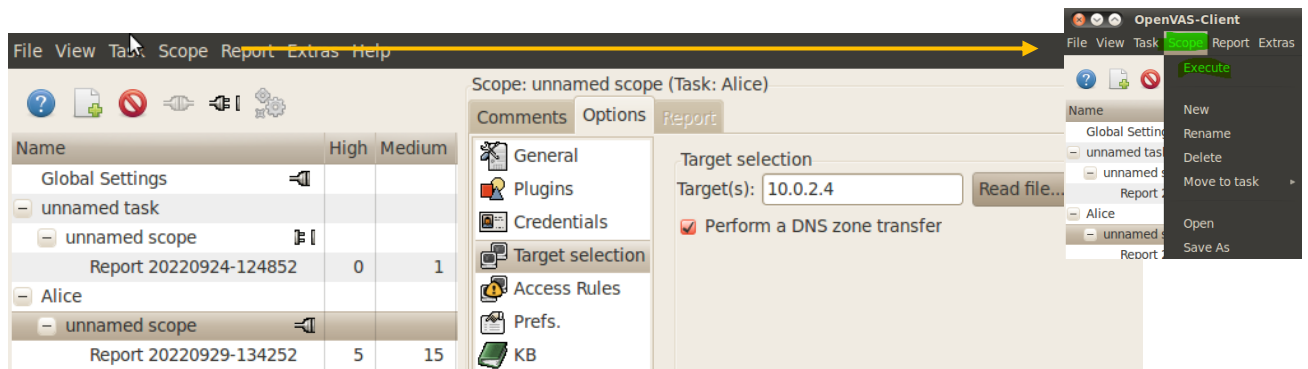
Starting Nmap 5.00 ( http://nmap.org ) at 2022-09-29 13:23 CEST
Warning: Hostname localhost resolves to 2 IPs. Using 127.0.0.1.
Interesting ports on localhost (127.0.0.1):
PORT      STATE SERVICE
9390/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.03 seconds
```

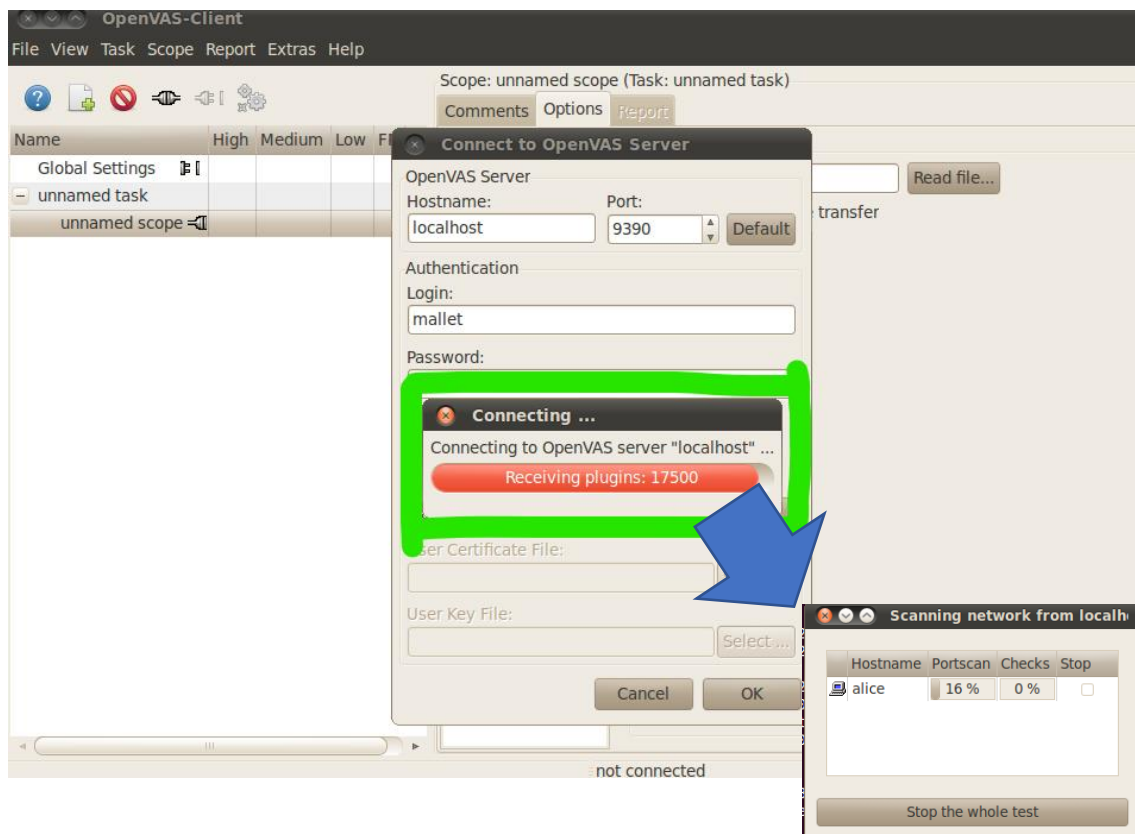
Y ahora ejecuto un cliente de openvasd, donde se nos abre una nueva ventana con múltiples opciones:



Una vez abierto el cliente, tendremos que crear un barrido/análisis nuevo, para ello en el menú principal de la aplicación, en la parte superior de este New (Icono hoja en blanco), esto nos crea una nueva task y después Scope → New. Una vez se nos han creado, dentro de “unnamed scope” en la pestaña “Options” de esta, y dentro del submenú en “Target Selection”, escribimos en el campo Target(s):, alicé, es decir, el nombre de la máquina a quién queremos escanear, o su IP. Y después ejecutamos el analizador, en la parte superior donde pone “Scope”, “execute”, automáticamente comienza a realizar el análisis:



Una vez iniciado el servidor ya sí que conecta e inicia el escaneo como se ve a continuación:



Una vez generado el análisis de vulnerabilidades el cual habrá tardado unos minutos obtendremos un reporte donde podremos ver todas las vulnerabilidades de alice.

Name	High	Medium	Host/Port/Severity
Global Settings			
- unnamed task			
- unnamed scope			
Report 20220924-124852	0	1	
- Alice			
- unnamed scope			
Report 20220929-134252	5	15	

Host/Port/Severity
- 10.0.2.4
+ http (80/tcp)
+ ftp (21/tcp)
+ https (443/tcp)
+ x11 (6000/tcp)
+ unknown (986/tcp)
+ unknown (985/udp)
+ unknown (60584/tcp)
+ unknown (59839/tcp)
+ unknown (59838/tcp)
+ unknown (56252/tcp)
+ unknown (55975/tcp)
+ unknown (46669/tcp)
+ telnet (23/tcp)
+ sunrpc (111/udp)
+ sunrpc (111/tcp)

Aquí un ejemplo del reporte de dos de las vulnerabilidades detectadas:

Host/Port/Severity

- 10.0.2.4

- http (80/tcp)

Security Hole

Security Warning

Security Note

Log Message

- ftp (21/tcp)

Security Hole

Security Note

- https (443/tcp)

Security Warning

Security Note

Log Message

+ x11 (6000/tcp)

+ unknown (986/tcp)

+ unknown (985/udp)

Reported by NVT "Web mirroring" (1.3.6.1.4.1.25623.1.0.1066)

The following CGI have been discovered :
Syntax : cginame (arguments [default value])
. (id [forum])

=====

Reported by NVT "Directory Scanner" (1.3.6.1.4.1.25623.1.0.1067)

The following directories were discovered:
/cgi-bin, /login, /icons, /javascript, /session

While this is not, in and of itself, a bug, you should manually
these directories to ensure that they are in compliance with c
security standards

The following directories require authentication:
/forum
Other references : OWASP:OWASP-CM-006

=====

Scan took place from Thu Sep 29 13:29:19 2022 to Thu Sep 29 13:42:52 2022

Host/Port/Severity

- 10.0.2.4

- http (80/tcp)

Security Hole

Security Warning

Security Note

Log Message

- ftp (21/tcp)

Security Hole

Security Note

- https (443/tcp)

Security Warning

Security Note

Log Message

+ x11 (6000/tcp)

+ unknown (986/tcp)

+ unknown (985/udp)

Reported by NVT "FTP Server type and version" (1.3.6.1.4.1.25623.1.0.1068)

Remote FTP server banner :
220 alice FTP server (Version wu-2.6.2(1) Wed Sep 30 08:44:57

=====

Reported by NVT "Services" (1.3.6.1.4.1.25623.1.0.10330):

An FTP server is running on this port.
Here is its banner :
220 alice FTP server (Version wu-2.6.2(1) Wed Sep 30 08:44:57

f. Recopile la información anterior (desde el punto "b" al punto "e"), ahora para bob en lugar de alice.

Al igual que en el apartado b) lo primero que hago es comprobar que redes están disponibles para poderla escanear, vemos que eth4 está disponible. Eth4 es la red a la que están conectadas todas las máquinas.

```
mallet@mallet:~$ sudo tcpdump -D
1.usbmon1 (USB bus number 1)
2.eth4
3.any (Pseudo-device that captures on all interfaces)
4.lo
```

Y vemos que está disponible, por ello para comprobar la monitorización ahora realizaremos un ping de 4 paquetes de bob a alice (en el apartado b, era al revés).

```
bob:/home/bob# ping 10.0.2.4 -c 4
PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data.
64 bytes from 10.0.2.4: icmp_seq=1 ttl=64 time=0.588 ms
64 bytes from 10.0.2.4: icmp_seq=2 ttl=64 time=0.694 ms
64 bytes from 10.0.2.4: icmp_seq=3 ttl=64 time=1.53 ms
64 bytes from 10.0.2.4: icmp_seq=4 ttl=64 time=2.18 ms

--- 10.0.2.4 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3001ms
```

Y en la monitorización activada en mallet con *sudo tcpdump -i eth4*, escaneando el puerto 67 UDP de bob.

```
mallet@mallet:~$ sudo nmap 10.0.2.15 -n -p67 -sU

Starting Nmap 5.00 ( http://nmap.org ) at 2022-09-29 14:30 CEST
Interesting ports on 10.0.2.15:
PORT      STATE SERVICE
67/udp    closed dhcpcd
MAC Address: 08:00:27:F5:BB:62 (Cadmus Computer Systems)

mallet@mallet: ~
File Edit View Terminal Help

mallet@mallet:~$ sudo tcpdump -i eth4 udp port 67 -v
tcpdump: listening on eth4, link-type EN10MB (Ethernet), capture
14:31:25.015055 IP (tos 0x0, ttl 45, id 41056, offset 0, flags [n
(17), length 28)
^C mallet.local.58981 > 10.0.2.15.bootps: [|bootp]

1 packets captured
1 packets received by filter
```

Igual que hicimos en el apartado c) también vamos a realizar el escaneo del puerto 80 TCP de bob, mediante el escaneo TCP SYN, y TCP COMPLETO.

Por defecto nmap realiza TCP SYN

TCP SYN:

```
mallet@mallet:~$ sudo nmap 10.0.2.15 -n -p80

Starting Nmap 5.00 ( http://nmap.org ) at 2022-09-29 14:36 CEST
Interesting ports on 10.0.2.15:
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 08:00:27:F5:BB:62 (Cadmus Computer Systems)

mallet@mallet: ~
File Edit View Terminal Help

mallet@mallet:~$ sudo tcpdump -i eth4 tcp port 80 -v
tcpdump: listening on eth4, link-type EN10MB (Ethernet), capture size 96 bytes
14:36:09.678911 IP (tos 0x0, ttl 41, id 5378, offset 0, flags [none], proto TCP (6), length 44)
    mallet.local.47378 > 10.0.2.15.www: Flags [S], cksum 0x5837 (correct), seq 312427273, win 2048, options [mss 1460], length 0
14:36:09.679099 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 44)
    10.0.2.15.www > mallet.local.47378: Flags [S.], cksum 0x9029 (correct), seq 1050245779, ack 3312427274, win 5840, options [mss 1460], length 0
14:36:09.679109 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 40)
    mallet.local.47378 > 10.0.2.15.www: Flags [R], cksum 0x77f0 (correct), seq 312427274, win 0, length 0
^C
3 packets captured
3 packets received by filter
```

TCP Completo:

```
mallet@mallet:~$ sudo nmap 10.0.2.15 -n -p80 -sT

Starting Nmap 5.00 ( http://nmap.org ) at 2022-09-29 14:39 CEST
Interesting ports on 10.0.2.15:
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 08:00:27:F5:BB:62 (Cadmus Computer Systems)

mallet@mallet: ~
File Edit View Terminal Help

tcpdump: listening on eth4, link-type EN10MB (Ethernet), capture size 96 bytes
14:39:13.303207 IP (tos 0x0, ttl 64, id 37666, offset 0, flags [DF], proto TCP (6), length 60)
    mallet.local.53942 > 10.0.2.15.www: Flags [S], cksum 0x71da (correct), seq 2951400362, win 5840, options [mss 1460,sackOK,TS val 2119816 ecr 0,nop,wscale 5], length 0
14:39:13.303353 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 60)
    10.0.2.15.www > mallet.local.53942: Flags [S.], cksum 0x5b5c (correct), seq 1251359796, ack 2951400363, win 5792, options [mss 1460,sackOK,TS val 2133939 ecr 2119816,nop,wscale 4], length 0
14:39:13.303362 IP (tos 0x0, ttl 64, id 37667, offset 0, flags [DF], proto TCP (6), length 52)
    mallet.local.53942 > 10.0.2.15.www: Flags [.], cksum 0xa00e (correct), ack 1, win 183, options [nop,nop,TS val 2119816 ecr 2133939], length 0
14:39:13.304236 IP (tos 0x0, ttl 64, id 37668, offset 0, flags [DF], proto TCP (6), length 52)
    mallet.local.53942 > 10.0.2.15.www: Flags [R.], cksum 0xa00a (correct), seq 1, ack 1, win 183, options [nop,nop,TS val 2119816 ecr 2133939], length 0
```

Ahora desde mallet escaneamos el puerto 80 TCP de bob, ya que es el puerto del servicio web http, para ver si está abierto.

```
mallet@mallet:~$ sudo nmap 10.0.2.15 -p80

Starting Nmap 5.00 ( http://nmap.org ) at 2022-09-23 19:29 CEST
Interesting ports on 10.0.2.15 (10.0.2.15):
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 08:00:27:F5:BB:62 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
```

Y ahora con una conexión telnet obtenemos la información de la misma forma que en el apartado:

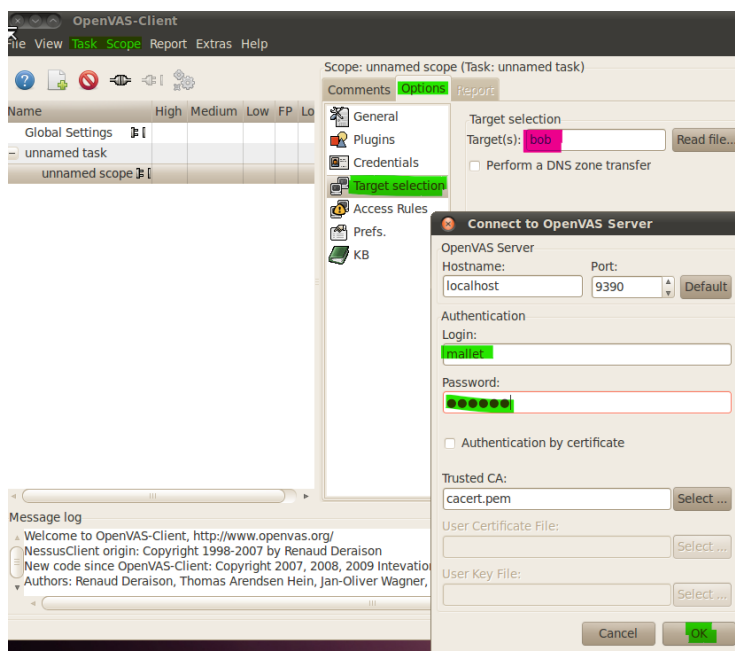
- Usando HEAD

```
mallet@mallet:~$ sudo telnet 10.0.2.15 80
Trying 10.0.2.15...
Connected to 10.0.2.15.
Escape character is '^['.
HEAD
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
</p>
<hr>
<address>Apache/2.2.9 (Debian) PHP/5.2.6-1+lenny8 with Suhosin-Patch Server
27.0.1.1 Port 80</address>
</body></html>
Connection closed by foreign host.
```

- Usando i

```
</div>
<div id="footerspacer"></div>
</div>
<div id="footer">
<div id="footer_l">
<div id="footer_r">
<p id="syndicate">
</p>
<p id="power_by">
Powered by <a href="http://www.j
oomla.org">Joomla!</a>.
valid <a href="http://validator.
w3.org/check/referer">XHTML</a> and <a href="http://jigsaw.w3.org/css-validator/
check/referer">CSS</a>.
</p>
</div>
</div>
</div>
</div>
</div>
```

Ahora el informe de vulnerabilidades en bob, para ello de nuevo abriremos un cliente openvas en mallet, pero ahora modificaremos el target (a quién analizar, subrayado de color rosa), y realizando los mismos pasos que en e).



Una vez finalizado el escaneo obtenemos el reporte de las vulnerabilidades de bob:

Name	High	Medium	Host/Port/Severity
Global Settings			
- unnamed task			
- unnamed scope			
Report 20220924-124852	0	1	
- Alice			
- unnamed scope			
Report 20220929-134252	5	15	
- Bob			
- unnamed scope			
Report 20220929-140735	11	25	

Host/Port/Severity

- 10.0.2.15

+ http (80/tcp)

+ ssh (22/tcp)

+ ftp (21/tcp)

+ telnet (23/tcp)

+ general/tcp

+ general/icmp

+ general/SMBClient

+ general/IT-Grundschi

+ general/IT-Grundschi

+ general/CPE-T

italk (12345/tcp)

Aquí una descripción de dos de las vulnerabilidades:

Host/Port/Severity	Reported by NVT "wapiti (NASL wrapper)" (1.3.6.1.4.1.25623.1.0
- 10.0.2.15	wapiti could not be found in your system path. OpenVAS was unable to execute wapiti and to perform the scan requested. Please make sure that wapiti is installed and that wapiti is available in the PATH variable defined for your environment.
- http (80/tcp)	=====
Security Hole	Reported by NVT "w3af (NASL wrapper)" (1.3.6.1.4.1.25623.1.0.i
Security Warning	w3af could not be found in your system path. OpenVAS was unable to execute w3af and to perform the scan y requested. Please make sure that w3af is installed and that w3af_console i available in the PATH variable defined for your environment.
Security Note	
Log Message	
+ ssh (22/tcp)	
+ ftp (21/tcp)	
+ telnet (23/tcp)	
+ general/tcp	
+ general/icmp	
+ general/SMBClient	

Host/Port/Severity	Reported by NVT "Determine OS and list of installed packages v
- 10.0.2.15	This script will, if given a userid/password or key to the remote system, login to that system, determine the OS it is running, and for supported systems, extract the list of installed packages/rpms.
- http (80/tcp)	Risk factor : None
Security Hole	=====
Security Warning	Reported by NVT "SSH Authorization" (1.3.6.1.4.1.25623.1.0.900
Security Note	No SSH credentials were supplied. Hence local security checks are not enabled.
Log Message	
- ssh (22/tcp)	
Security Warning	
Security Note	
Log Message	