

Práctica

Escaneo de puertos con nmap

Franco Larrea

2º SMR-A
(Prof. Fernando Albert González)
Instituto IES SAN VICENTE

Indice

Teoria.....Pag. 3

Tareas y cuestiones.....Pag. 4

 1.....Pag. 4

 2.....Pag. 5

 3.....Pag. 6

 4.....Pag. 7

 5.....Pag. 8

 6.....Pag. 10

Problemas encontrados.....Pag. 11

Fuentes.....Pag. 11

Teoría

En esta practica vamos a realizar un escaneo de puertos con Nmap.

Un escaneo de puertos es un análisis del estado de los puertos de una maquina conectada a una red. Cambien sirve para detectar que servicios esta ofreciendo la maquina a través de posibles vulnerabilidades de seguridad en puertos abiertos.

Existen 65536 puertos, podemos usar cualquiera para cualquier protocolo, pero IANA(Internet Assigned Numbers Authority) creó tres categorías:

- Puertos bien conocidos: Los puertos del 0 al1023, estan reservados al sistema operativo y usan “protocolos bien conocidos” como http, telnet o pop3/smtp.
- Puertos registrados: Los puertos del 1024 al 49151 pueden ser usados por cualquier aplicación.
- Puertos privados o dinámicos: Los puertos del 49152 al 65535 suelen ser usados por aplicaciones de clientes al iniciarse la conexión.

Un puerto puede estar abierto, cerrado o protegido por un firewall.

Nmap es una herramienta de código abierto para el escaneo de redes, puertos y vulnerabilidades de servicios que pueden servir como punto de entrada a los sistemas.

Con nmap podemos realizar diversas tareas:

- Identificar los dispositivos conectados a la red que queremos estudiar.
- Conocer los puertos abiertos, el sistema operativo o aplicación en ejecución y su versión. Todo esto mediante estándares de uso de puertos.
- Encontrar servicios vulnerables en la red.

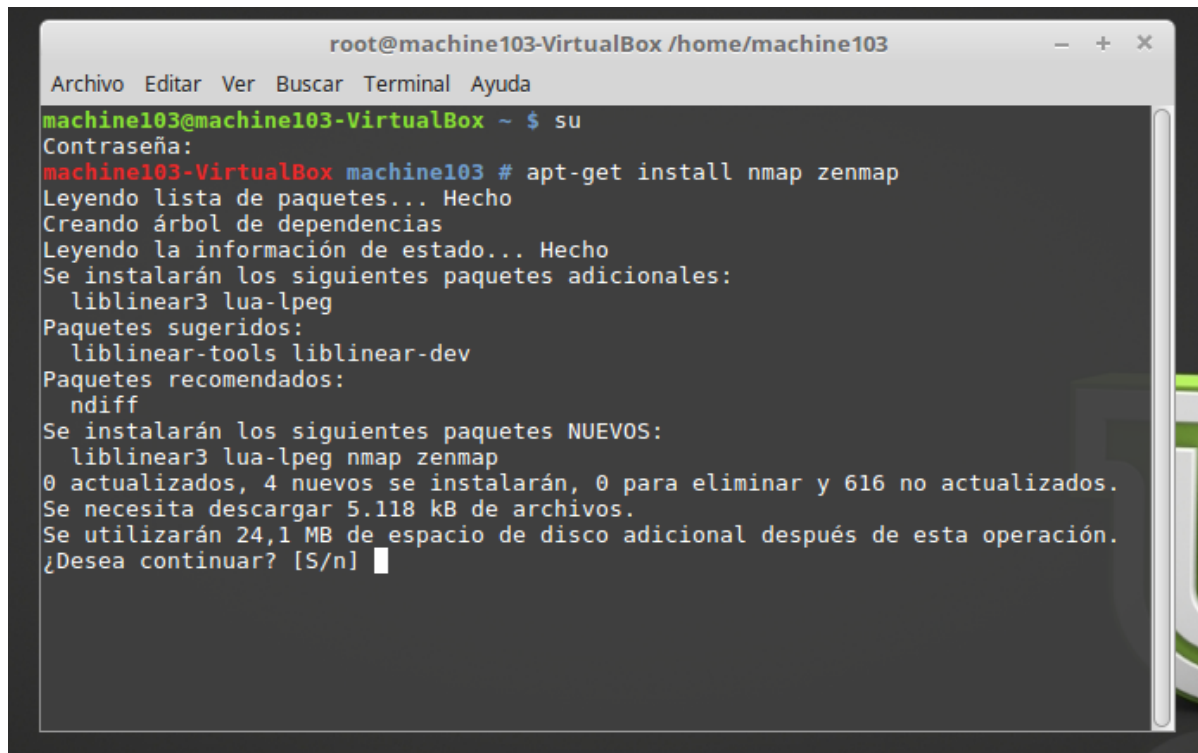
Tareas y cuestiones

Las siguientes tareas van a ser realizadas en una maquina virtual con Linux Mint 18.2.

1. Instalar el paquete nmap en Ubuntu

Para instalar nmap con su interfaz gráfica tendremos que usar el siguiente comando con permisos de administrador:

- `sudo apt-get install nmap zenmap`

A screenshot of a terminal window titled 'root@machine103-VirtualBox /home/machine103'. The terminal shows the execution of 'su' to become root, followed by 'apt-get install nmap zenmap'. The output displays the progress of package installation, including dependency resolution and disk space requirements. It lists additional packages to be installed (liblinear3, lua-lpeg), suggested packages (liblinear-tools, liblinear-dev), and recommended packages (ndiff). It states that 0 packages will be updated, 4 new ones will be installed, and 0 will be removed, totaling 5.118 kB of download and 24.1 MB of disk space usage. The prompt '¿Desea continuar? [S/n]' is shown at the end with a cursor.

```
root@machine103-VirtualBox /home/machine103
Archivo Editar Ver Buscar Terminal Ayuda
machine103@machine103-VirtualBox ~ $ su
Contraseña:
machine103-VirtualBox machine103 # apt-get install nmap zenmap
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  liblinear3 lua-lpeg
Paquetes sugeridos:
  liblinear-tools liblinear-dev
Paquetes recomendados:
  ndiff
Se instalarán los siguientes paquetes NUEVOS:
  liblinear3 lua-lpeg nmap zenmap
0 actualizados, 4 nuevos se instalarán, 0 para eliminar y 616 no actualizados.
Se necesita descargar 5.118 kB de archivos.
Se utilizarán 24,1 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n]
```

Al finalizar la instalación podremos abrir nmap con su interfaz gráfica escribiendo

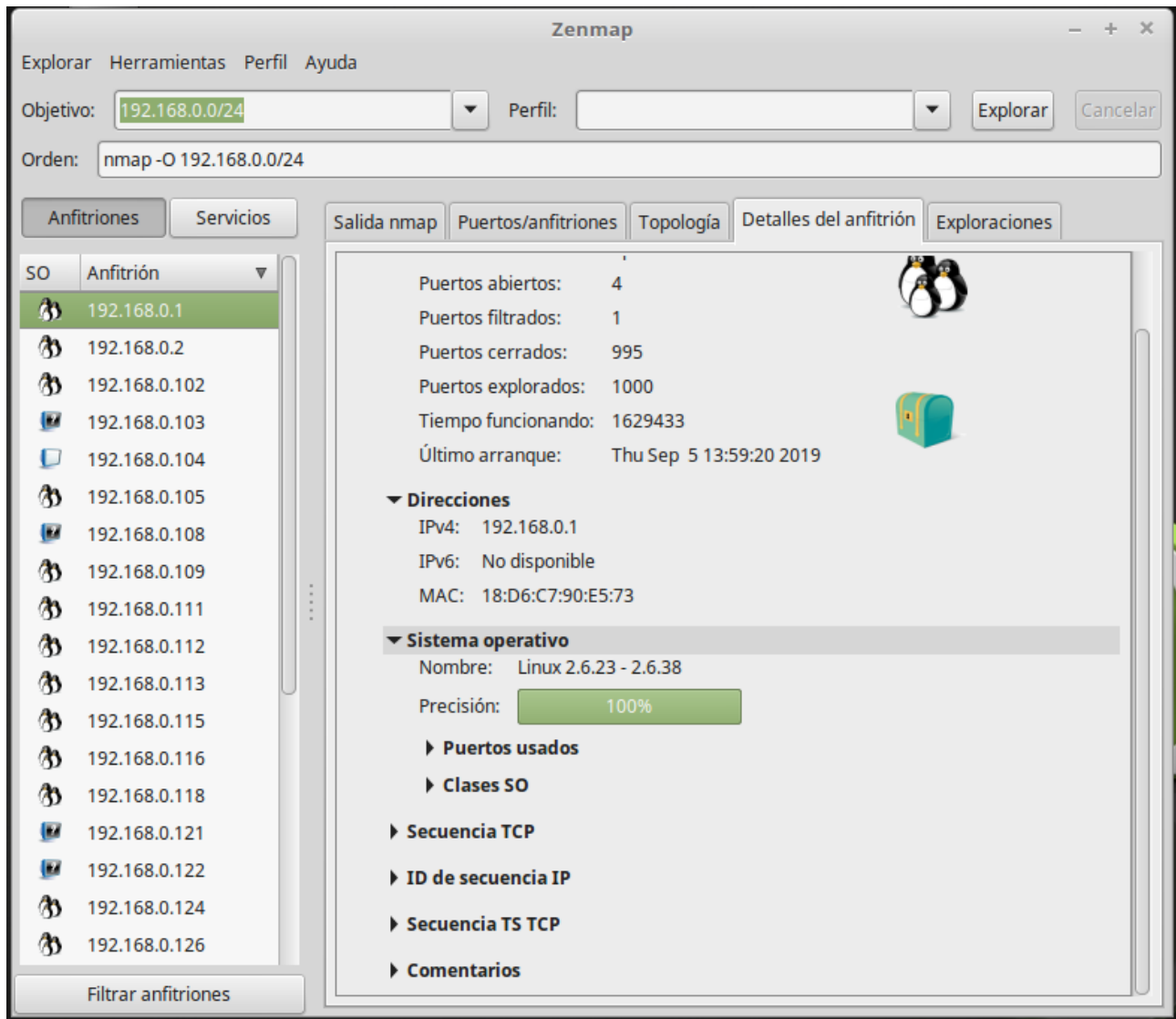
- `zenmap`

en la terminal.

2. Realizar un escaneo de sistemas operativos de los equipos en la red del aula, indicando el comando ejecutado para el escaneo. Pon captura de pantalla.

Con la siguiente orden realizamos un escaneo de los equipos en la red del aula:

- `nmap -O 192.168.0.0/24`



El parametro `-O` detecta el tipo de sistema operativo que tiene el host.

`192.168.0.0/24` es la dirección ip de la red del aula.
































En el apartado *detalles del anfitrión* podemos ver más información acerca de los hosts y de sus sistemas operativos.

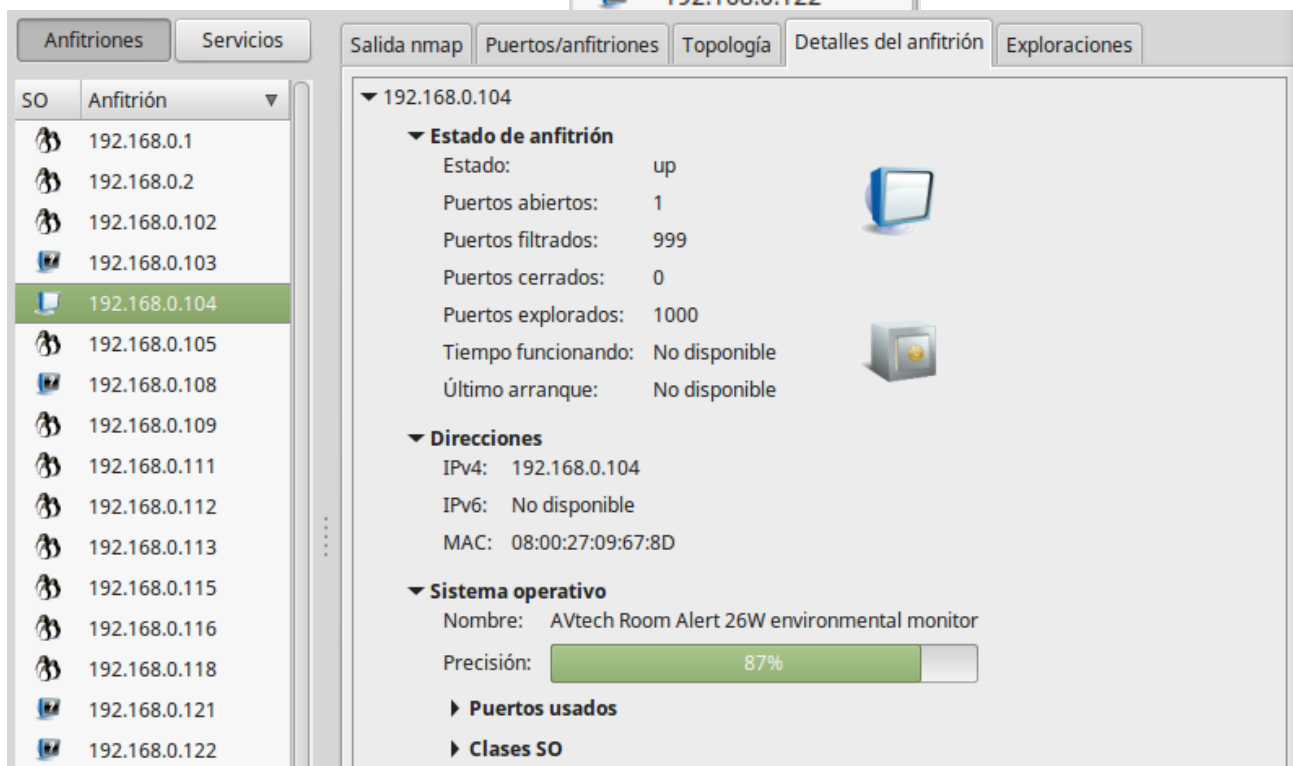
En la captura de pantalla se puede ver que el host con la ip 192.168.0.1 tiene como SO Linux 2.6.

3. Listar los equipos encontrados con los sistemas operativos disponibles.

















El análisis ha encontrado 31 hosts:

- 20 hosts con Linux
- 10 hosts sin identificar el SO
- 1 host con “AVtech Room Alert 26W environmental monitor”.

	192.168.0.1		192.168.0.121
	192.168.0.2		192.168.0.122
	192.168.0.102		192.168.0.124
	192.168.0.103		192.168.0.126
	192.168.0.104		192.168.0.127
	192.168.0.105		192.168.0.129
	192.168.0.108		192.168.0.130
	192.168.0.109		192.168.0.132
	192.168.0.111		192.168.0.134
	192.168.0.112		192.168.0.136
	192.168.0.113		192.168.0.139
	192.168.0.115		192.168.0.140
	192.168.0.116		192.168.0.147
	192.168.0.118		192.168.0.149
	192.168.0.121		192.168.0.151
	192.168.0.122		



The screenshot shows the Nmap ScanTool interface. On the left, a list of hosts is displayed under the 'Anfitriones' tab. The host 192.168.0.104 is selected. The main panel shows the details for this host, including its state (up), open ports (1), filtered ports (999), closed ports (0), and explored ports (1000). The operating system is identified as 'AVtech Room Alert 26W environmental monitor' with a precision of 87%.

SO	Anfitrión
	192.168.0.1
	192.168.0.2
	192.168.0.102
	192.168.0.103
	192.168.0.104
	192.168.0.105
	192.168.0.108
	192.168.0.109
	192.168.0.111
	192.168.0.112
	192.168.0.113
	192.168.0.115
	192.168.0.116
	192.168.0.118
	192.168.0.121
	192.168.0.122

▼ 192.168.0.104

▼ Estado de anfitrión

Estado: up

Puertos abiertos: 1

Puertos filtrados: 999

Puertos cerrados: 0

Puertos explorados: 1000

Tiempo funcionando: No disponible

Último arranque: No disponible

▼ Direcciones

IPv4: 192.168.0.104

IPv6: No disponible

MAC: 08:00:27:09:67:8D

▼ Sistema operativo

Nombre: AVtech Room Alert 26W environmental monitor

Precisión: 87%

► Puertos usados

► Clases SO

Me identifica que el host con ip 192.168.0.104 tiene como sistema operativo “AVtech Room Alert 26W environmental monitor”. Lo he buscado en google y he averiguado que son monitores de temperatura. <https://avtech.com/>

4. Realizar un escaneo de puertos del equipo del profesor del 0 al 1023 con la ip facilitada por el profesor ¿Cómo se denomina ese rango de puertos?

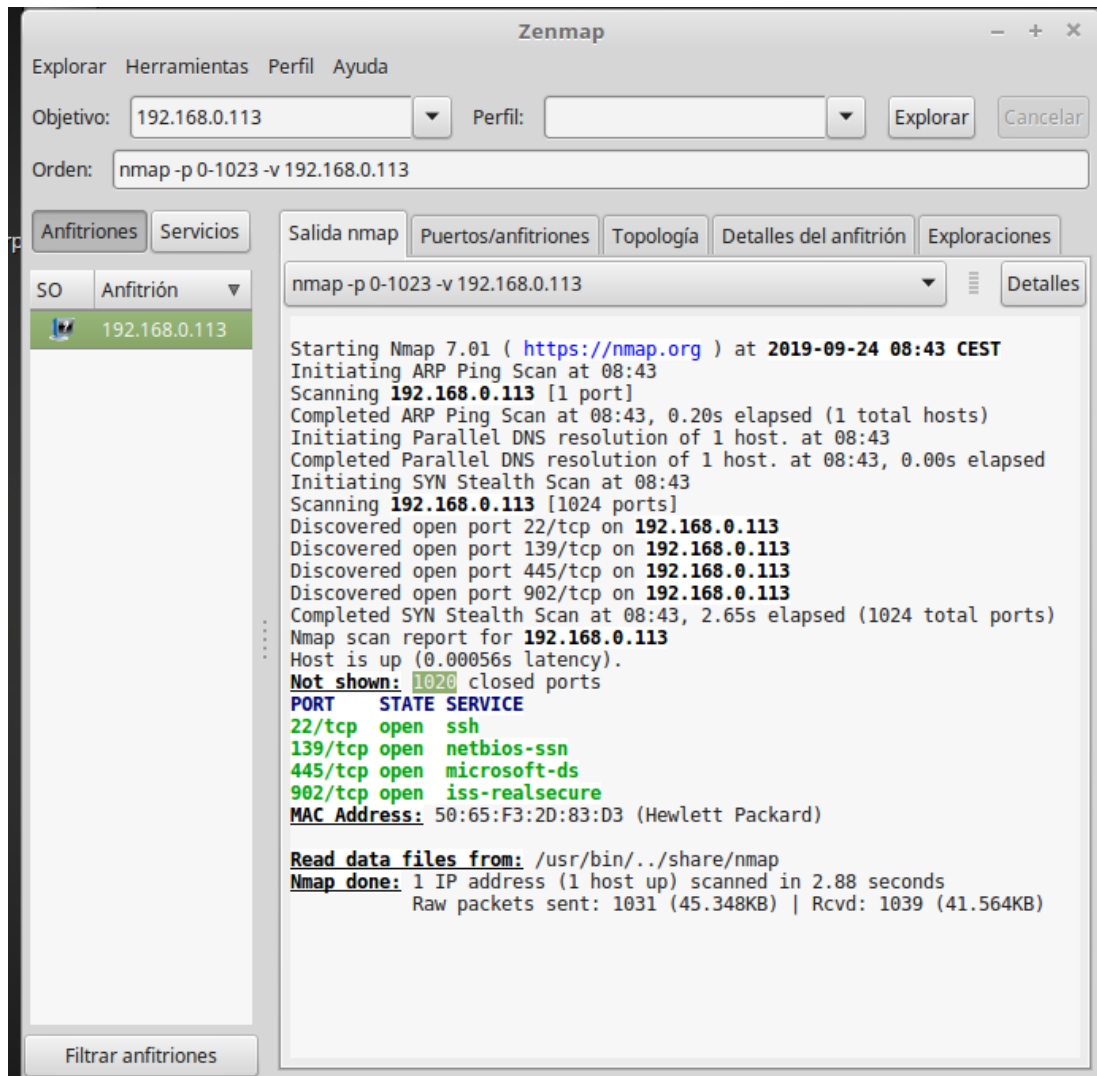
Con la siguiente orden realizamos un escaneo de puertos al equipo del profesor:

- `nmap -p 0-1023 -v 192.168.0.113`

El parametro `-p 0-1023` indica el numero de puertos que vamos a escanear.

El parametro `-v` realiza un informe detallado del escaneo.

`192.168.0.113` es la dirección ip de la red del profesor.



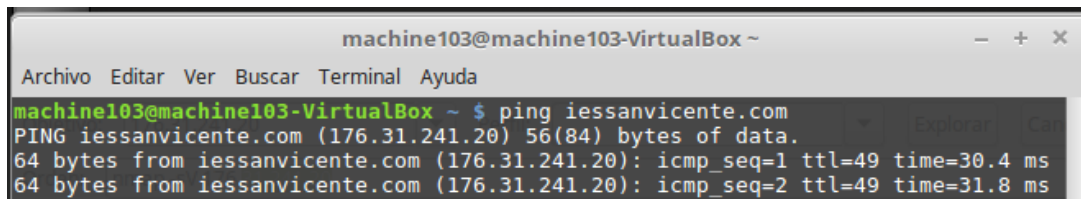
Nos ha detectado 4 puertos abiertos de los 1024 puertos escaneados.

Estos son el puerto 22, el 139, el 445 y el 902, correspondientemente cada puerto tiene un servicio: ssh, netbios-ssn, microsoft-ds y issrealsecure.

Los cuatro puertos están abiertos y usan el protocolo tcp.

Los puertos del 0 al 1023 se denominan “puertos bien conocidos”.

5. **Informe de seguridad. Realiza un escaneo de puertos del servidor del iessanvicente. Indicar el sistema operativo que utiliza y los servicios que se encuentran activos.** Para poder escanear los puertos de iessanvicente.com tengo que saber su ip. Para ello hacemos un ping desde la terminal y vemos que la ip de <https://iessanvicente.com/> es 176.31.241.20.



```
machine103@machine103-VirtualBox ~  
Archivo Editar Ver Buscar Terminal Ayuda  
machine103@machine103-VirtualBox ~ $ ping iessanvicente.com  
PING iessanvicente.com (176.31.241.20) 56(84) bytes of data:  
64 bytes from iessanvicente.com (176.31.241.20): icmp_seq=1 ttl=49 time=30.4 ms  
64 bytes from iessanvicente.com (176.31.241.20): icmp_seq=2 ttl=49 time=31.8 ms
```

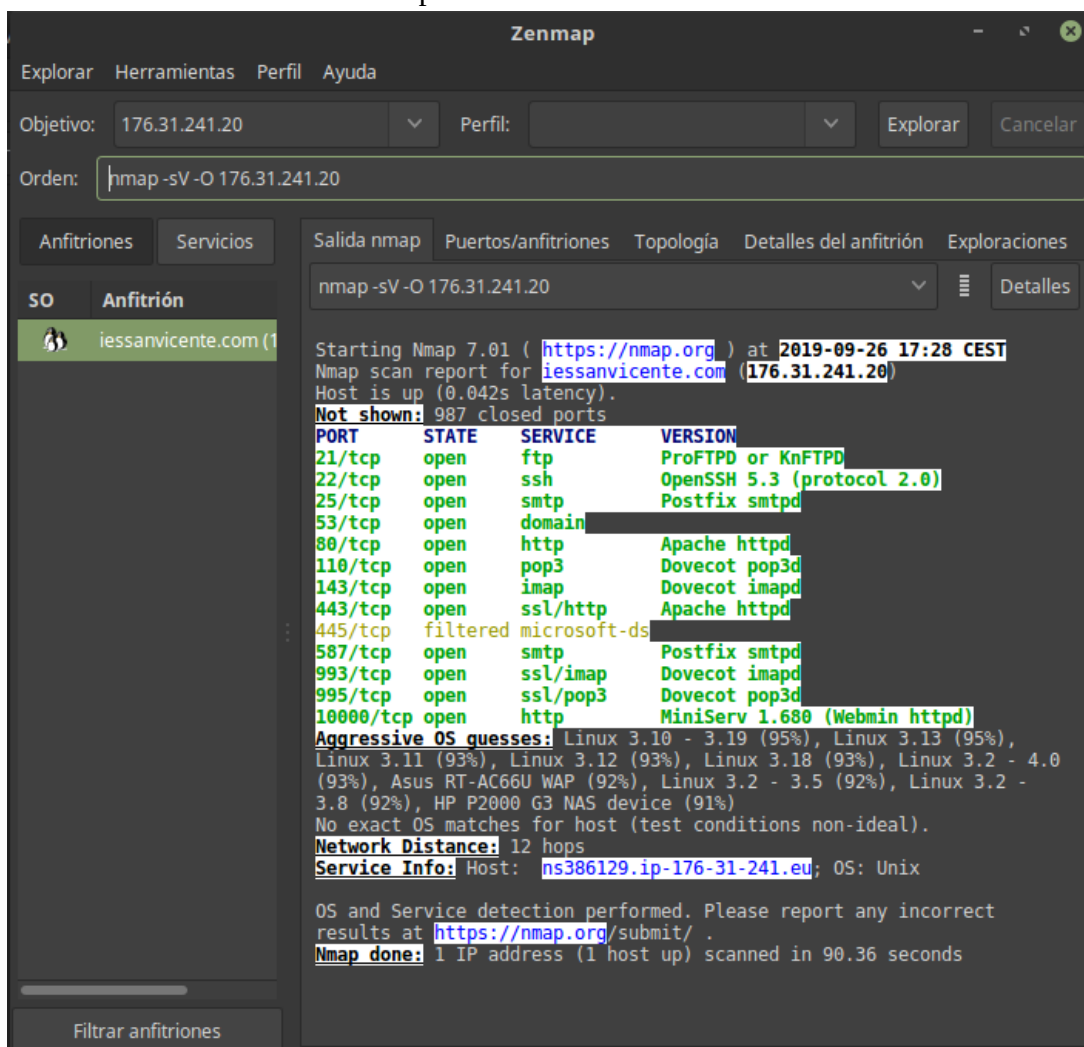
Con la siguiente orden analizamos que SO y que servicios tiene el servidor de iessanvicente activos:

- `nmap -sV -O 176.31.241.20`

El parametro `-O` detecta el tipo de sistema operativo que tiene el host.

El parametro `-sV` detecta servicios en puertos abiertos.

176.31.241.20 es la dirección ip de la red del aula.



Zenmap

Objetivo: 176.31.241.20 Perfil: Explorar Cancelar

Orden: `nmap -sV -O 176.31.241.20`

Anfitriones Servicios

SO Anfitrión

iessanvicente.com (176.31.241.20)

Salida nmap

`nmap -sV -O 176.31.241.20`

Starting Nmap 7.01 (<https://nmap.org>) at 2019-09-26 17:28 CEST
Nmap scan report for iessanvicente.com (176.31.241.20)
Host is up (0.042s latency).
Not shown: 987 closed ports

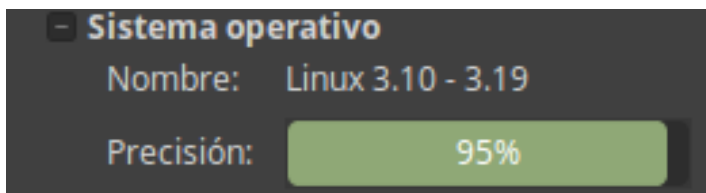
PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	ProFTPD or KnFTPD
22/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)
25/tcp	open	smtp	Postfix smtpd
53/tcp	open	domain	
80/tcp	open	http	Apache httpd
110/tcp	open	pop3	Dovecot pop3d
143/tcp	open	imap	Dovecot imapd
443/tcp	open	ssl/http	Apache httpd
445/tcp	filtered	microsoft-ds	
587/tcp	open	smtp	Postfix smtpd
993/tcp	open	ssl/imap	Dovecot imapd
995/tcp	open	ssl/pop3	Dovecot pop3d
10000/tcp	open	http	MiniServ 1.680 (Webmin httpd)

Aggressive OS guesses: Linux 3.10 - 3.19 (95%), Linux 3.13 (95%), Linux 3.11 (93%), Linux 3.12 (93%), Linux 3.18 (93%), Linux 3.2 - 4.0 (93%), Asus RT-AC66U WAP (92%), Linux 3.2 - 3.5 (92%), Linux 3.2 - 3.8 (92%), HP P2000 G3 NAS device (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 12 hops
Service Info: Host: ns386129.ip-176-31-241.eu; OS: Unix

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.
Nmap done: 1 IP address (1 host up) scanned in 90.36 seconds

Filtrar anfitriones

En esta captura de pantalla podemos ver 12 puertos abiertos y 1 puerto filtrado por el firewall.



El servidor de la pagina <https://iessanvicente.com/> tiene como sistema operativo Linux 3.10 – 3.19.

Todos los puertos usan el protocolo tcp, con servicios activos tales como ftp, ssh, smtp, domain, http, pop3 e imap.

Solo hay 1 puerto que esta filtrado, este es el 445, con el servicio microsoft-ds.

Puertos abiertos: 12
Puertos filtrados: 1
Puertos cerrados: 987
Puertos explorados: 1000

	Puerto	Protocolo	Estado	Servicio	Versión
✓	21	tcp	open	ftp	ProFTPD or KnFTPD
✓	22	tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)
✓	25	tcp	open	smtp	Postfix smtpd
✓	53	tcp	open	domain	
✓	80	tcp	open	http	Apache httpd
✓	110	tcp	open	pop3	Dovecot pop3d
✓	143	tcp	open	imap	Dovecot imapd
✓	443	tcp	open	http	Apache httpd
✗	445	tcp	filtered	microsoft-ds	
✓	587	tcp	open	smtp	Postfix smtpd
✓	993	tcp	open	imap	Dovecot imapd
✓	995	tcp	open	pop3	Dovecot pop3d
✓	10000	tcp	open	http	MiniServ 1.680 (Webmin httpd)

6. Buscar vulnerabilidades de existir del software instalado en el servidor de iessanvicente. ¿Alguna recomendación para el administrador del sitio?

He intentado lanzar la orden:

- `nmap -p - -n -Pn --script vuln 176.31.241.20`

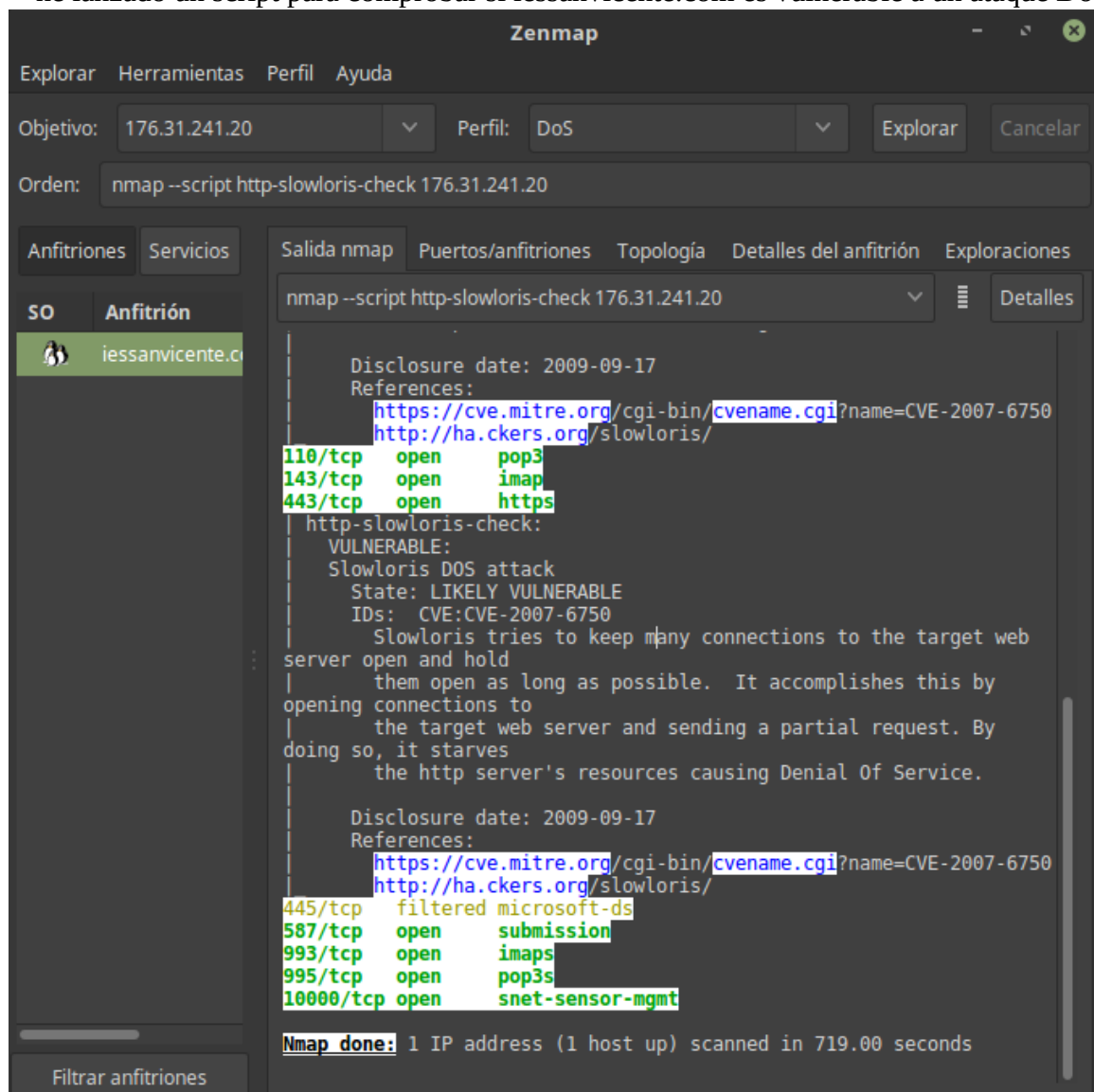
esta orden ejecuta un script llamado *vuln* que engloba a otros scripts los cuales revisan las vulnerabilidades más conocidas.

La duración de este escaneo ha sido muy extensa, no ha podido ser finalizada y no me ha aportado datos relevantes sobre vulnerabilidades de la web.

Mediante la orden:

- `nmap --script http-slowloris-check 176.31.241.20`

he lanzado un script para comprobar si iessanvicente.com es vulnerable a un ataque DoS.



Esta pagina es vulnerable a un ataque de denegación de servicios.

Problemas encontrados:

En general no he tenido problemas con la practica realizada, excepto el tiempo de ejecución de algunos escaneos tales como:

- nmap -O 192.168.0.0/24
- nmap -sV -O 176.31.241.20
- nmap -p - -n -Pn --script vuln 176.31.241.20

Fuentes:

- <https://protegermipc.net/2018/11/07/tutorial-y-listado-de-comandos-mas-utiles-para-nmap/>
- <https://alanchavez.com/puertos-bien-conocidos-puertos-registrados-y-puertos-efimeros/>
- <https://backtrackacademy.com/articulo/introduccion-al-escaneo-de-red-y-vulnerabilidades-con-nmap>
- <https://securitylabs.es/elementor-1138-2-2-2-3/>
- <http://www.reydes.com/d/?q=Escaneo de Vulnerabilidades utilizando Nmap>
- <https://backtrackacademy.com/articulo/introduccion-al-escaneo-de-red-y-vulnerabilidades-con-nmap>
- <https://www.welivesecurity.com/la-es/2015/02/12/auditando-nmap-scripts-escanear-vulnerabilidades/>
- https://es.wikipedia.org/wiki/Puerto_de_red
- https://es.wikipedia.org/wiki/Internet_Assigned_Numbers_Authority
- https://es.wikipedia.org/wiki/Esc%C3%A1ner_de_puertos
- <https://www.google.com/amp/s/reportedigital.com/iot/nmap/amp/>
- <https://elbinario.net/2018/04/17/testando-la-seguridad-de-nuestros-servidores-i/>
- <https://www.pcihispano.com/como-verificar-si-existen-cuentas-de-usuario-y-contrasenas-por-defecto-con-nmap-pci-dss-req-2-1/>
- <https://www.securityhacklabs.net/articulo/los-5-scripts-mas-intrusivos-y-avanzados-de-nmap-que-deberia-conocer>
- <https://www.linux-party.com/26-hackers/9118-29-practicos-ejemplos-de-nmap-para-administradores-de-sistemas-redes.html>

- <https://www.adslzone.net/redes/analisis-de-puertos/comprobar-los-puertos-abiertos-de-una-ip-remota/amp/>
- https://kb.iweb.com/hc/es/articles/230268328-C%C3%B3mo-proteger-su-servidor-del-servicio-de-Memcached?mobile_site=true
- <https://www.csirtcv.gva.es/sites/all/files/downloads/NMAP%20-%20Listado%20de%20comandos.pdf>
- <https://nmap.org/nsedoc/categories/vuln.html>
- <https://nmap.org/nsedoc/scripts/http-slowloris-check.html>