

Práctica 4 – Escaneo de puertos

ANALIZADOR DE REDES NMAP

Nmap (Network Mapper, mapeador de redes) es una sofisticada utilidad para la exploración y auditoría de seguridad de redes TCP/IP. Ha sido diseñado para escanear de forma rápida, sigilosa y eficaz tanto equipos individuales como redes de gran tamaño. Es una herramienta gratuita, de código abierto bajo licencia GPL, bien documentada, multiplataforma, disponible para consola, y que ofrece también una interfaz gráfica para facilitar su uso. Está escrita por un hacker conocido como Fyodor, y se beneficia de las aportaciones de una nutrida comunidad de colaboradores.

Nmap es una popular herramienta de seguridad utilizada tanto por administradores de red y analistas de seguridad, como por atacantes. Esto es debido a la gran cantidad de información que es capaz de descubrir de una red utilizando una gran variedad de técnicas que la hacen notablemente efectiva y sigilosa. Para ello, Nmap explora equipos remotos mediante secuencias de paquetes TCP/IP tanto convencionales como no convencionales, es decir, paquetes en bruto convenientemente modificados que provocarán o no una respuesta en el objetivo de la cual poder extraer información. Entre esta información se encuentra, por ejemplo: el estado de los puertos y servicios, el sistema operativo, la presencia de cortafuegos, encaminadores u otros elementos de red, así como del direccionamiento IP de la subred. El tipo de respuestas recibidas ayudan a determinar la identidad de la pila TCP/IP implementada en el sistema operativo remoto.

La información extraída con Nmap puede ser utilizada para múltiples usos. Los más habituales son los siguientes:

- Descubrimiento de subredes.
- Análisis de penetración de redes y equipos.
- Evaluación de la implantación de cortafuegos y de la eficacia de herramientas de detección y prevención de intrusiones.
- Descubrimiento del estado de puertos de comunicaciones.
- Descubrimiento de los servicios disponibles en un servidor, así como de sus versiones. Descubrimiento del tipo y versión del sistema operativo instalado en el equipo remoto.
- Obtención de información adicional acerca de servicios y equipos, a través de la ejecución de scripts convenientemente elaborados.

Instalación.

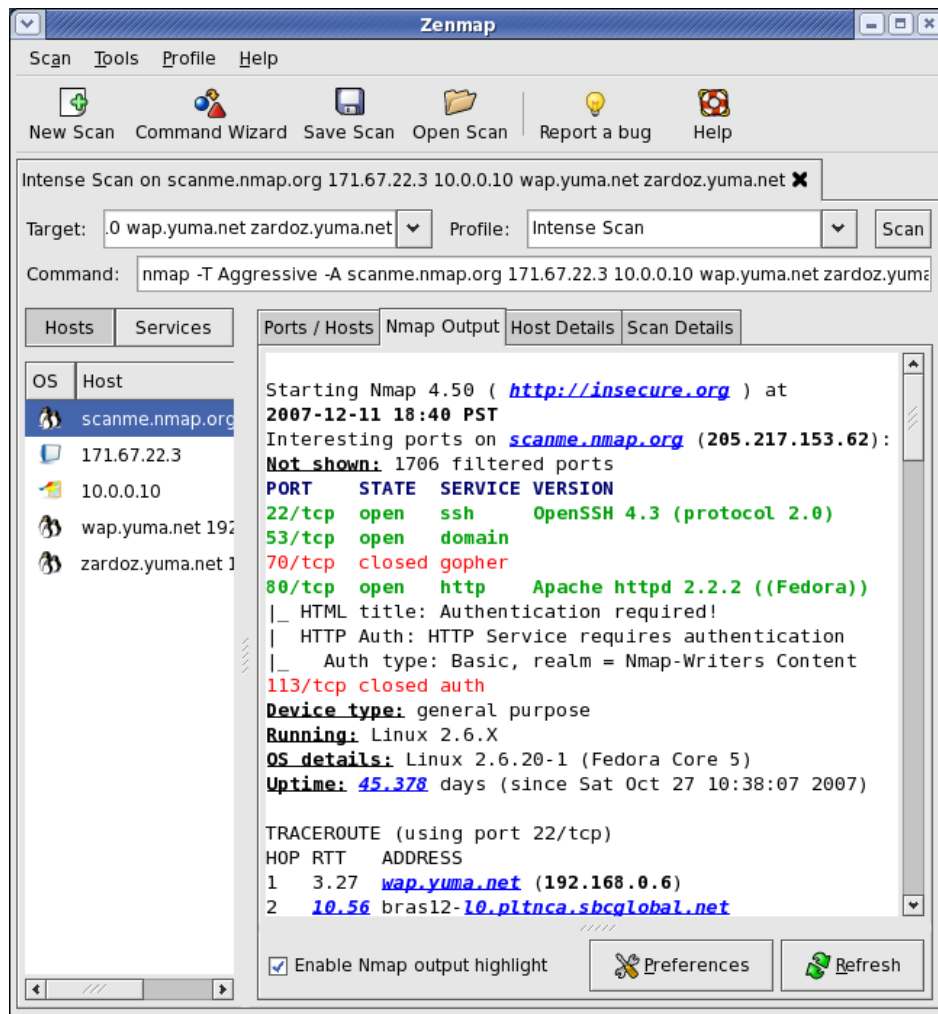
La instalación de nmap desde la línea de comando es muy sencilla, al igual que la instalación de la interfáz gráfica, simplemente ejecutar el comando:

```
apt-get install nmap zenmap
```

Recordar que posiblemente es necesario ser root para realizar la instalación de los paquetes.

Entorno gráfico.

A pesar de que nmap es un programa que se utiliza desde el interprete de comandos, existe la posibilidad de utilizar un entorno gráfico que facilita su uso, llamado zenmap.



Ejemplo básicos de comandos.

Nmap permite escanear redes y puertos utilizando diferentes parámetros, la sintaxis del comando es:

nmap [Tipos(s)de escaneo] [Opciones]

Algunos de sus **Tipos(s)de escaneo** son:

- **sT** se intenta hacer un barrido de puertos por TCP la ventaja de esta técnica es que no requiere usuarios privilegiados, opuesto a sS
- **sU** se intenta hacer un barrido de puertos por UDP, es útil cuando se intentan descubrir puertos de nivel superior que pueden estar detrás de un firewall, lenta pero permite hacer auditorias mas exactas.
- **sA** se usan mensajes de ACK para lograr que sistema responda y así dterminar si el puerto esta abierto algunos Firewall no filtran estos Mensajes y por ello puede ser efectivo en algunos casos.
- **sX** puede pasar algunos Firewall con malas configuraciones y detectar servicios prestándose dentro de la red
- **sN** puede pasar algunos Firewall con malas configuraciones y detectar servicios prestándose dentro de la red
- **sF** puede pasar algunos Firewall con malas configuraciones y detectar servicios prestándose dentro de la red
- **sP** este modificador ayuda a identificar que sistemas están arriba en la red (en funcionamiento) para luego poder hacer pruebas mas especificas, similar a Ping.
- **sV** intenta identificar los servicios por los puertos abiertos en el sistema esto permite evaluar cada servicio de forma individual para intentar ubicar vulnerabilidades en los mismos.
- **sO** con esta opción se identifica que protocolos de nivel superior a capa tres (Red o Network) responden en el sistema, de esta manera es mas fácil saber las características de la red o el sistema que se intenta evaluar.

Alguna de sus **opciones** son:

- **b** Para determinar si la víctima es vulnerable al "bounce attack"
- **n** no hace conversiones DNS para hacer el -sP mas rápido
- **vv** hacer la salida de la herramienta detallada en pantalla
- **f** habilita la fragmentación de esta forma es mucho mas complejo para un firewall u otro tipo de sistema lograr hacer el rastreo.

- **oN** redirige la salida a un archivo
- **oX** redirige la salida a un archivo XML
- **--stylesheet** con esta opción se usa una hoja de estilo que hace más fácil la lectura de la salida en XML
- **P0** indica que no se debe hacer ping a los sistemas objetivo antes de iniciar el análisis útil para evitar el bloque en algunos Firewall
- **p** se usa para especificar puertos de análisis o rango de puertos.
- **T** se usa para especificar la velocidad general del scan de esta forma se puede pasar inadvertido en algunos sistemas que detectan la velocidad de los paquetes entrantes.

Ejemplos.

```
map -sV -P0 -O -vv -o archivo.txt 192.168.1.1
```

El anterior comando ejecuta un barrido (scan) de puertos sobre la IP seleccionada, evita que se ejecute Ping sobre la máquina, además de esto intenta detectar el sistema operativo, para cada puerto según las cabeceras que se retornan se detecten los servicios ejecutándose y la información se dejara en el archivo.txt

```
nmap 192.168.1.0/24
```

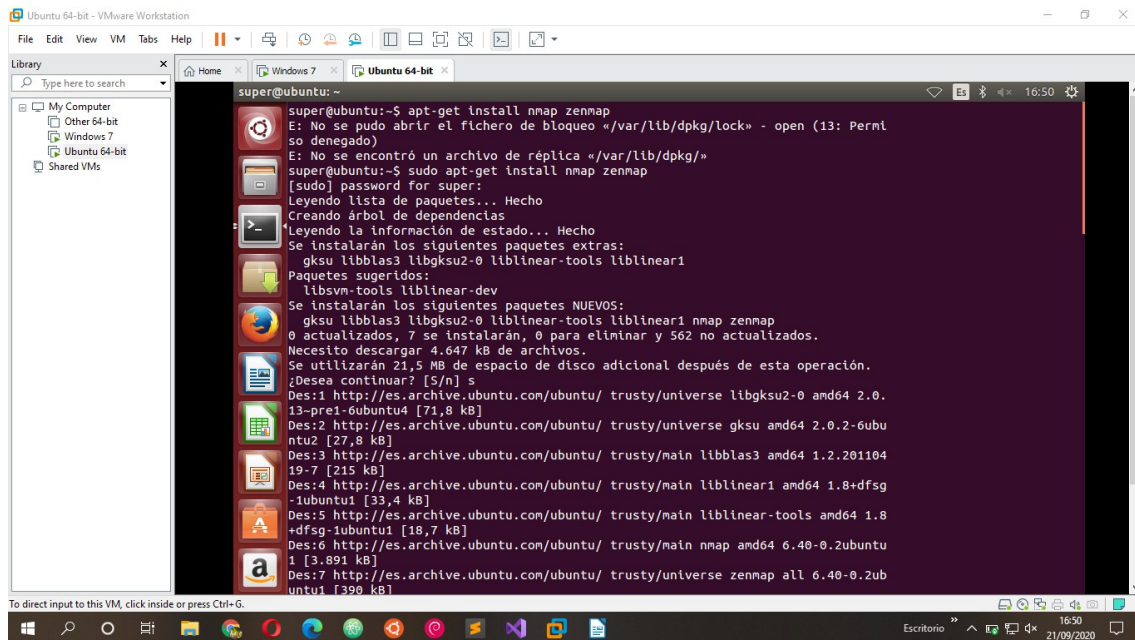
El anterior comando escanea una red completa

```
nmap 192.168.1.100 -p 10-200
```

El anterior comando escanea un rango de puertos

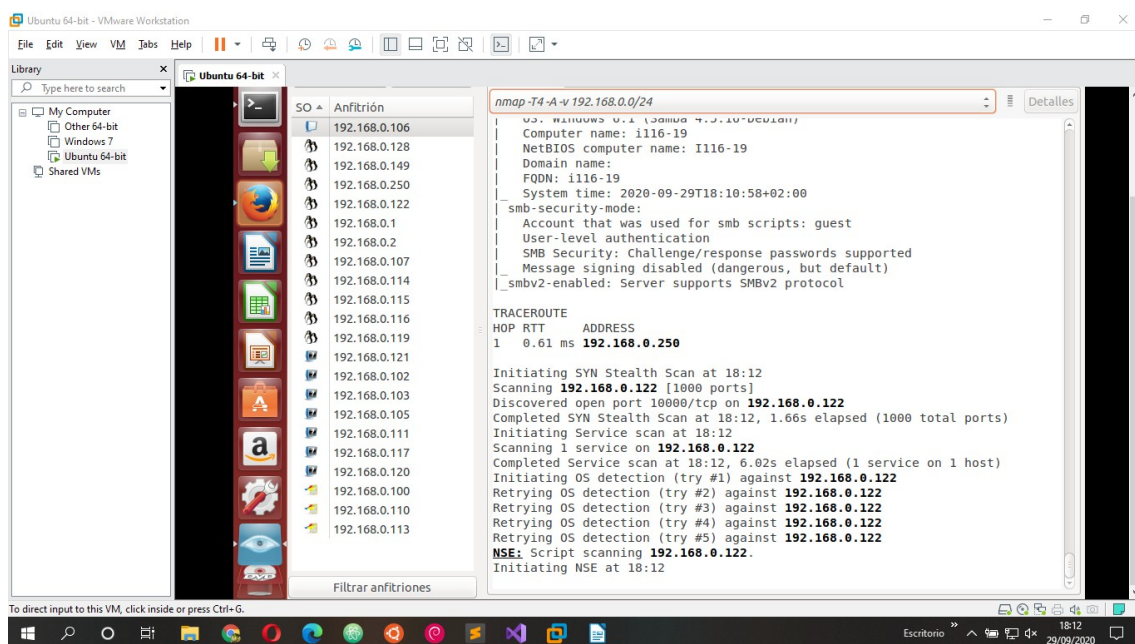
Tareas y cuestiones.

1. Instalar el paquete nmap en Ubuntu



```
super@ubuntu:~$ apt-get install nmap zenmap
E: No se pudo abrir el fichero de bloqueo «/var/lib/dpkg/lock» - open (13: Permi
so denegado)
E: No se encontró un archivo de réplica «/var/lib/dpkg/»
super@ubuntu:~$ sudo apt-get install nmap zenmap
[sudo] password for super:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes extras:
  gksu libblas3 libgksu2-0 liblinear-tools liblinear1
Paquetes sugeridos:
  libsvm-tools liblinear-dev
Se instalarán los siguientes paquetes NUEVOS:
  gksu libblas3 libgksu2-0 liblinear-tools liblinear1 nmap zenmap
0 actualizados, 7 se instalarán, 0 para eliminar y 562 no actualizados.
Necesito descargar 4.647 kB de archivos.
Se utilizarán 21,5 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
Des:1 http://es.archive.ubuntu.com/ubuntu/ trusty/universe libgksu2-0 amd64 2.0.
13-pre1-6ubuntu4 [71,8 kB]
Des:2 http://es.archive.ubuntu.com/ubuntu/ trusty/universe gksu amd64 2.0.2-6ubu
ntu2 [27,8 kB]
Des:3 http://es.archive.ubuntu.com/ubuntu/ trusty/main libblas3 amd64 1.2.201104
19-7 [215 kB]
Des:4 http://es.archive.ubuntu.com/ubuntu/ trusty/main liblinear1 amd64 1.8+dfsg
-1ubuntu1 [33,4 kB]
Des:5 http://es.archive.ubuntu.com/ubuntu/ trusty/main liblinear-tools amd64 1.8
+dfsg-1ubuntu1 [18,7 kB]
Des:6 http://es.archive.ubuntu.com/ubuntu/ trusty/main nmap amd64 6.40-0.2ubun
tu1 [3,891 kB]
Des:7 http://es.archive.ubuntu.com/ubuntu/ trusty/universe zenmap all 6.40-0.2ub
untu1 [390 kB]
```

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.

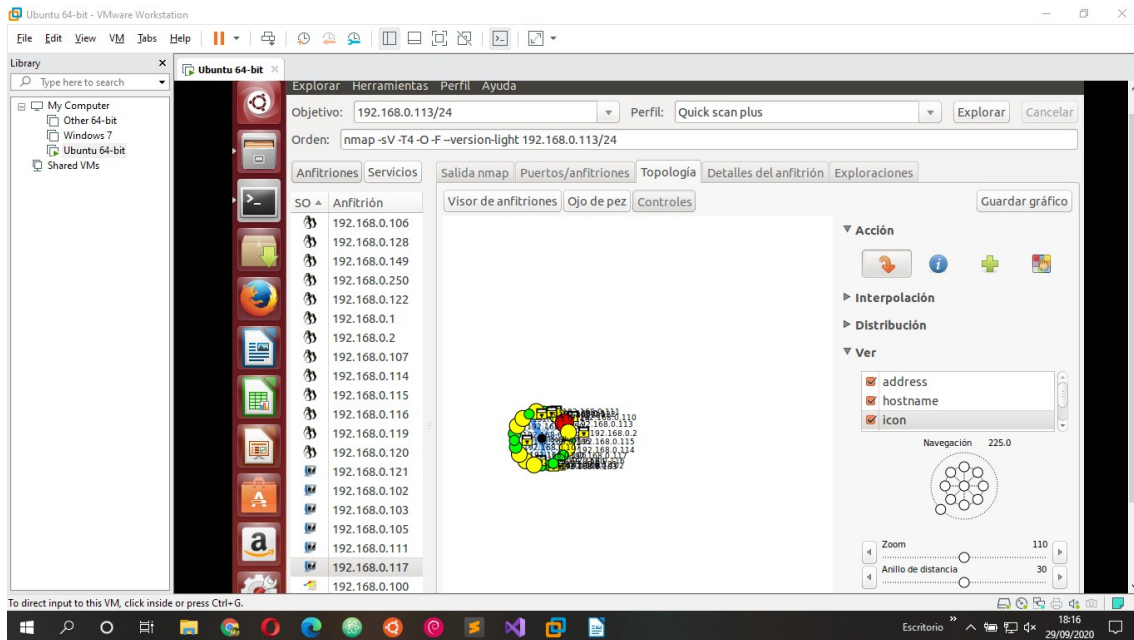


```
nmap -T4 -A -v 192.168.0.0/24
Nmap scan report for 192.168.0.122
Host: 192.168.0.122 (192.168.0.122)
OS: Windows 7.0 (build 7.0.10-DEU1011)
Computer name: i116-19
NetBIOS computer name: I116-19
Domain name:
FQDN: i116-19
System time: 2020-09-29T18:10:58+02:00
_smb-security-mode:
  Account that was used for smb scripts: guest
  User-level authentication
  SMB Security: Challenge/response passwords supported
  Message signing disabled (dangerous, but default)
_smbv2-enabled: Server supports SMBv2 protocol

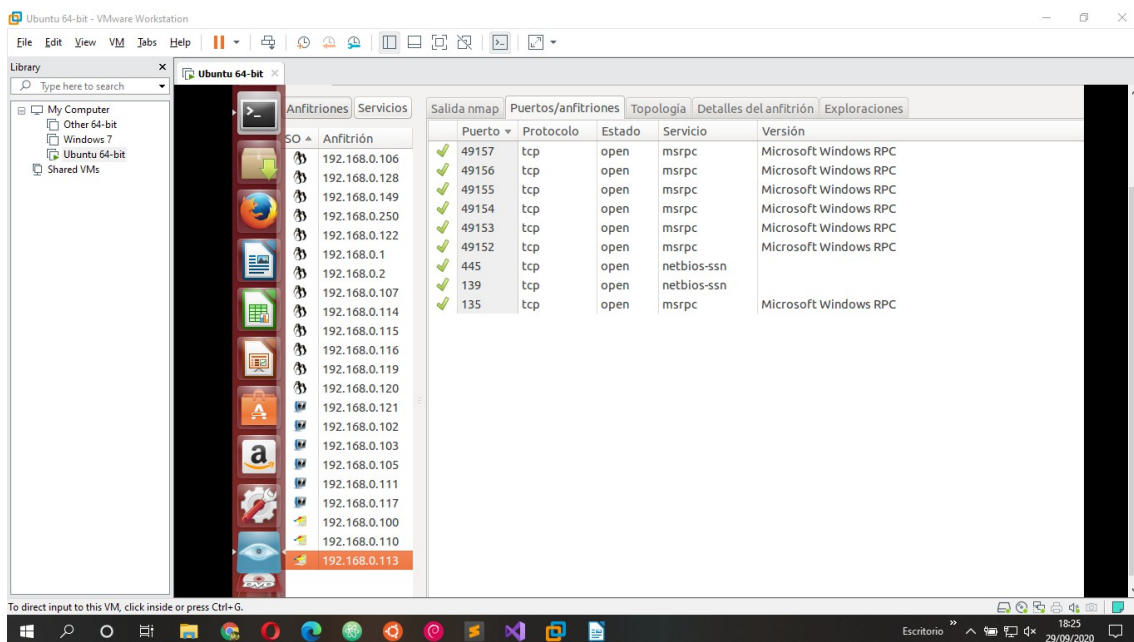
TRACEROUTE
HOP RTT ADDRESS
1 0.61 ms 192.168.0.250

Initiating SYN Stealth Scan at 18:12
Scanning 192.168.0.122 [1000 ports]
Discovered open port 10000/tcp on 192.168.0.122
Completed SYN Stealth Scan at 18:12, 1.66s elapsed (1000 total ports)
Initiating Service scan at 18:12
Scanning 1 service on 192.168.0.122
Completed Service scan at 18:12, 6.02s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against 192.168.0.122
Retrying OS detection (try #2) against 192.168.0.122
Retrying OS detection (try #3) against 192.168.0.122
Retrying OS detection (try #4) against 192.168.0.122
Retrying OS detection (try #5) against 192.168.0.122
NSE: Script scanning 192.168.0.122.
Initiating NSE at 18:12
```

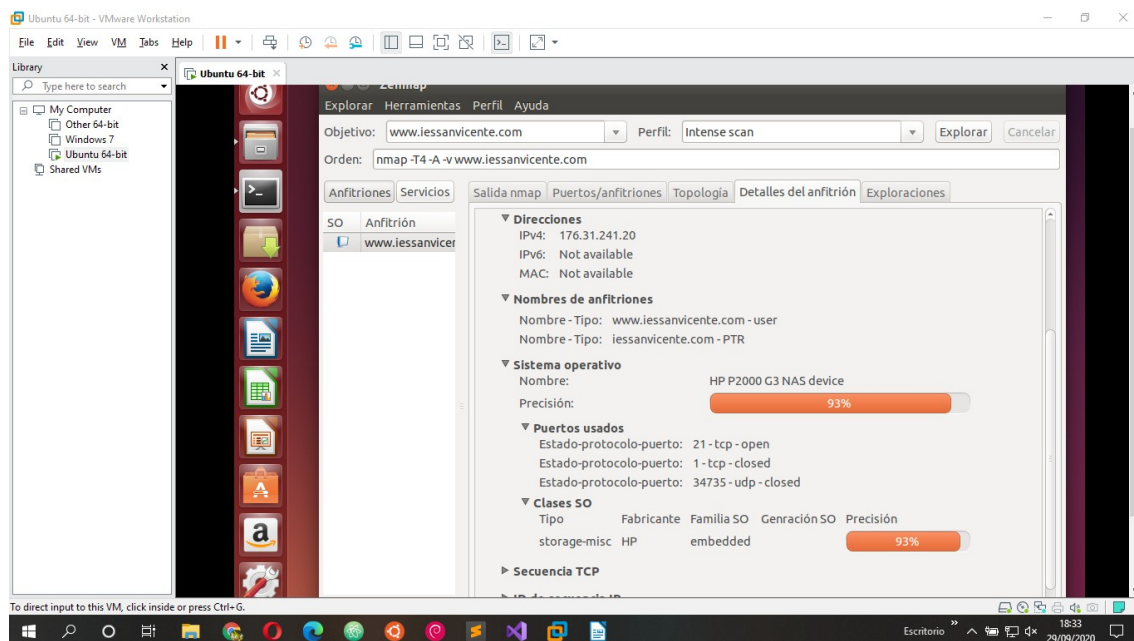
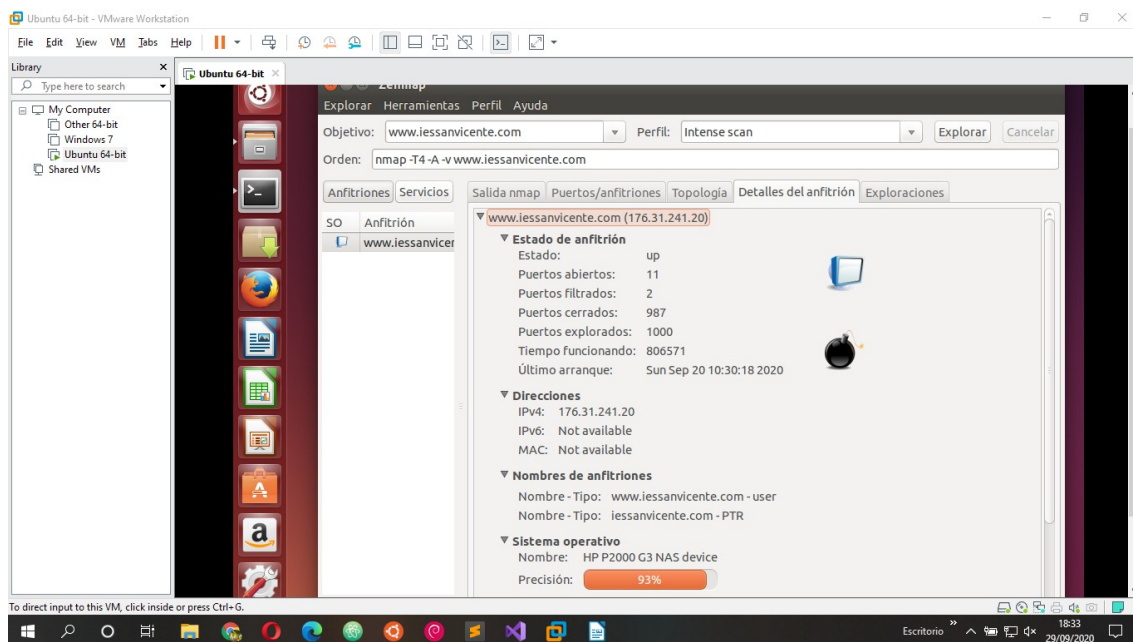

3. Listar los equipos encontrados con los sistemas operativos disponibles.

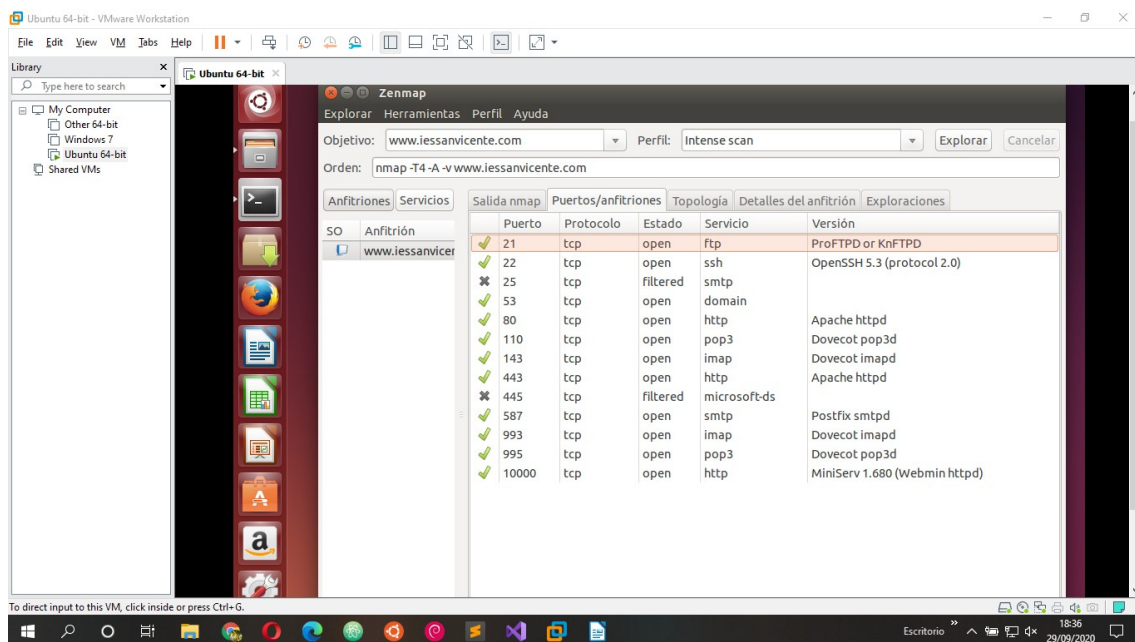


4. Realizar un escaneo de puertos del equipo del profesor del 0 al 1023 con la ip facilitada por el profesor ¿Cómo se denomina ese rango de puertos?



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.





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

En <http://securityfocus.com> se pueden buscar las posibles vulnerabilidades detectadas en ese software y las posibles acciones a realizar para solucionarlas.

- Comando para buscar vulnerabilidad

```
nmap -n -Pn 192.168.0.18 -p- --script=vuln
```

