



Yago Fernández Blanco
2º ASIR
Seguridad y alta disponibilidad
04/02/2020

PRÁCTICA

EXPLORACIÓN DE PUERTOS NMAP

1. Primero instalamos el nmap con apt-get install nmap

```
xubu pa sad [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda

Terminal - root@jton-Virtu... [Actualización de software]
Terminal - root@jton-VirtualBox: /home/jton/Escritorio

root@jton-VirtualBox:/home/jton/Escritorio# nmap
El programa «nmap» no está instalado. Puede instalarlo escribiendo:
apt-get install nmap
root@jton-VirtualBox:/home/jton/Escritorio# apt-get install nmap
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes extras:
  liblinear-tools liblinear1 liblua5.2-0
Paquetes sugeridos:
  liblua5.2-dev
Se instalarán los siguientes paquetes NUEVOS:
  liblinear-tools liblinear1 liblua5.2-0 nmap
0 actualizados, 4 se instalarán, 0 para eliminar y 397 no actualizados.
Necesito descargar 4.823 kB de archivos.
Se utilizarán 13,0 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
Des1 http://es.archive.ubuntu.com/ubuntu/ trusty/main liblua5.2-0 amd64 5.2.3-1 [60,5 kB]
Des2 http://es.archive.ubuntu.com/ubuntu/ trusty/main liblinear1 amd64 1.84dfsg-1ubuntu1 [33,4 kB]
Des3 http://es.archive.ubuntu.com/ubuntu/ trusty/main liblinear-tools amd64 1.84dfsg-1ubuntu1 [18,7 kB]
Des4 http://es.archive.ubuntu.com/ubuntu/ trusty/main nmap amd64 6.40-0.2ubuntu1 [3.891 kB]
Descargados 4.823 kB en 11sdp (352 kB/s)
Seleccionando el paquete liblua5.2-0:amd64 previamente no seleccionado.
Leyendo la base de datos ... 13669 ficheros o directorios instalados actualmente.)
Preparando para desempacar .../liblua5.2-0_5.2.3-1_amd64.deb ...
Desempaquetando liblua5.2-0:amd64 (5.2.3-1) ...
Seleccionando el paquete liblinear1 previamente no seleccionado.
Preparando para desempacar .../liblinear1_1.84dfsg-1ubuntu1_amd64.deb ...
Desempaquetando liblinear1 (1.84dfsg-1ubuntu1) ...
Seleccionando el paquete liblinear-tools previamente no seleccionado.
Preparando para desempacar .../liblinear-tools_1.84dfsg-1ubuntu1_amd64.deb ...
Desempaquetando liblinear-tools (1.84dfsg-1ubuntu1) ...
Seleccionando el paquete nmap previamente no seleccionado.
Preparando para desempacar .../nmap_6.40-0.2ubuntu1_amd64.deb ...
Desempaquetando nmap (6.40-0.2ubuntu1) ...
Procesando disparadores para man-db (2.6.7.1-1ubuntu1) ...
Configurando liblua5.2-0:amd64 (5.2.3-1) ...
Configurando liblinear1 (1.84dfsg-1ubuntu1) ...
Configurando liblinear-tools (1.84dfsg-1ubuntu1) ...
Configurando nmap (6.40-0.2ubuntu1) ...
Procesando disparadores para libc-bin (2.19-0ubuntu6.9) ...
root@jton-VirtualBox:/home/jton/Escritorio# clear
root@jton-VirtualBox:/home/jton/Escritorio#
```

2. Instalamos el Zenmap

→ apt-get install zenmap

```
xubu pa sad [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda

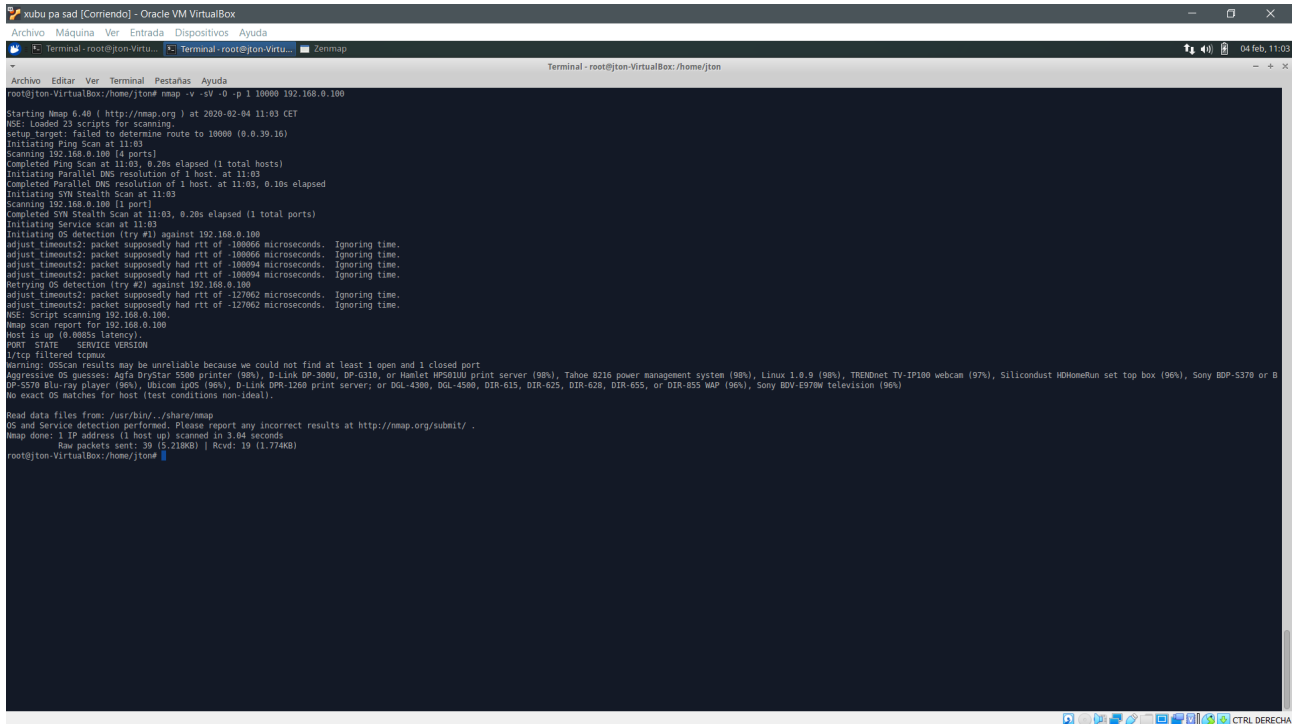
Terminal - root@jton-Virtu...
Terminal - root@jton-VirtualBox: /home/jton/Escritorio

root@jton-VirtualBox:/home/jton/Escritorio# apt-get install zenmap
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes extras:
  gksu libgksu2-0 libgtk2-0 libgtk2-common
Se instalarán los siguientes paquetes NUEVOS:
  gksu libgksu2-0 libgtk2-0 libgtk2-common zenmap
0 actualizados, 5 se instalarán, 0 para eliminar y 397 no actualizados.
Necesito descargar 3.397 kB de archivos.
Se utilizarán 3.397 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
Des1 http://es.archive.ubuntu.com/ubuntu/ trusty/main libgtk2-common all 2.28.5-2 [9.626 B]
Des2 http://es.archive.ubuntu.com/ubuntu/ trusty/main libgtk2-0 amd64 2.28.5-2 [33,7 kB]
Des3 http://es.archive.ubuntu.com/ubuntu/ trusty/universe libgksu2-0 amd64 2.0.13-pre1-0ubuntu4 [71,8 kB]
Des4 http://es.archive.ubuntu.com/ubuntu/ trusty/universe gksu amd64 2.0.2-0ubuntu2 [27,8 kB]
Des5 http://es.archive.ubuntu.com/ubuntu/ trusty/universe zenmap all 6.40-0.2ubuntu1 [398 kB]
Descargados 333 kB en 3sdp (157 kB/s)
Seleccionando el paquete libgtk2-common previamente no seleccionado.
Leyendo la base de datos ... 15138 ficheros o directorios instalados actualmente.)
Preparando para desempacar .../libgtk2-common_2.28.5-2_all.deb ...
Desempaquetando libgtk2-common (2.28.5-2) ...
Seleccionando el paquete libgtk2-0 previamente no seleccionado.
Preparando para desempacar .../libgtk2-0_2.28.5-2_amd64.deb ...
Desempaquetando libgtk2-0 (2.28.5-2) ...
Seleccionando el paquete libgksu2-0 previamente no seleccionado.
Preparando para desempacar .../libgksu2-0_2.0.13-pre1-0ubuntu4_amd64.deb ...
Desempaquetando libgksu2-0 (2.0.13-pre1-0ubuntu4) ...
Seleccionando el paquete gksu previamente no seleccionado.
Preparando para desempacar .../gksu_2.0.2-0ubuntu2_amd64.deb ...
Desempaquetando gksu (2.0.2-0ubuntu2) ...
Seleccionando el paquete zenmap previamente no seleccionado.
Preparando para desempacar .../zenmap_6.40-0.2ubuntu1_all.deb ...
Desempaquetando zenmap (6.40-0.2ubuntu1) ...
Procesando disparadores para man-db (2.6.7.1-1ubuntu1) ...
Procesando disparadores para gconf2 (3.2.6-0ubuntu2) ...
Procesando disparadores para gnome-menus (3.10.1-0ubuntu2) ...
Procesando disparadores para desktop-file-utils (0.22-1ubuntu1) ...
Procesando disparadores para mime-support (3.54ubuntu1) ...
Configurando libgtk2-common (2.28.5-2) ...
Configurando libgksu2-0 (2.0.13-pre1-0ubuntu4) ...
update-alternatives: utilizando /usr/share/libgksu/debian/gconf-defaults/libgksu-sudo para proveer /usr/share/gconf/default/10/libgksu (libgksu-gconf-defaults) en modo automático
Configurando zenmap (6.40-0.2ubuntu1) ...
Procesando disparadores para gconf2 (3.2.6-0ubuntu2) ...
Configurando gksu (2.0.2-0ubuntu2) ...
Procesando disparadores para libc-bin (2.19-0ubuntu6.9) ...
root@jton-VirtualBox:/home/jton/Escritorio#
```

3. Iniciamos el Zenmap pero lo dejamos en segundo plano y volvemos al terminal.

4. Realizamos un nmap con un rango maximo de ips de 10000 para visualizar los servicios corriendo en los puertos abiertos. (-v aumenta el nivel de mensajes detallados) (-O permite para ver los SO)

→ `nmap -v -sV -O -p 1 10000 192.168.0.100`



```
xubu pa sad [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Terminal - root@jon-Virtu... Terminal - root@jon-Virtu... Zenmap
Terminal - root@jon-VirtualBox:/home/jton
Starting Nmap 6.40 ( http://nmap.org ) at 2020-02-04 11:03 CET
NSE: Loaded 23 scripts for scanning
Setup target: failed to determine route to 10000 (0.0.39.16)
Initiating Ping Scan at 11:03
Scanning 192.168.0.100 [4 ports]
Completed Ping Scan at 11:03, 0.20s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:03
Completed Parallel DNS resolution of 1 host. at 11:03, 0.10s elapsed
Initiating SYN Stealth Scan at 11:03
Scanning 192.168.0.100 [1 port]
Completed SYN Stealth Scan at 11:03, 0.28s elapsed (1 total ports)
Initiating Service scan at 11:03
Initiating OS detection (try #1) against 192.168.0.100
adjust timeout2: packet supposedly had rtt of -1080066 microseconds. Ignoring time.
adjust timeout2: packet supposedly had rtt of -1080066 microseconds. Ignoring time.
adjust timeout2: packet supposedly had rtt of -1080094 microseconds. Ignoring time.
adjust timeout2: packet supposedly had rtt of -1080094 microseconds. Ignoring time.
Retrying OS detection (try #2) against 192.168.0.100
adjust timeout2: packet supposedly had rtt of -127062 microseconds. Ignoring time.
adjust timeout2: packet supposedly had rtt of -127062 microseconds. Ignoring time.
NSE: Script scanning 192.168.0.100.
Nmap scan report for 192.168.0.100
Host is up (0.8085s latency).
PORT      STATE      SERVICE VERSION
|/tcp filtered tcpmux
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Agfa DryStar 5500 printer (98%), D-Link DP-3000, DP-G310, or Hamlet HP5010U print server (98%), Tahoe 8216 power management system (98%), Linux 3.0.9 (98%), TRENDnet TV-IP100 webcam (97%), Siliconcast HDHomeRun set top box (96%), Sony BDP-5370 or BDP-5370 Blu-ray player (96%), Jatonc iPOS (96%), D-Link DPR-1200 print server, or DGL-4300, DGL-4500, DIR-615, DIR-625, DIR-628, DIR-655, or DIR-855 WAP (96%), Sony KDV-E970W television (96%)
No exact OS matches for host (test conditions non-ideal).
Read data files from: /usr/bin/./share/nmap
OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.04 seconds
Raw packets sent: 39 (5.210KB) | Rcvd: 19 (1.774KB)
root@jon-VirtualBox:/home/jton
```