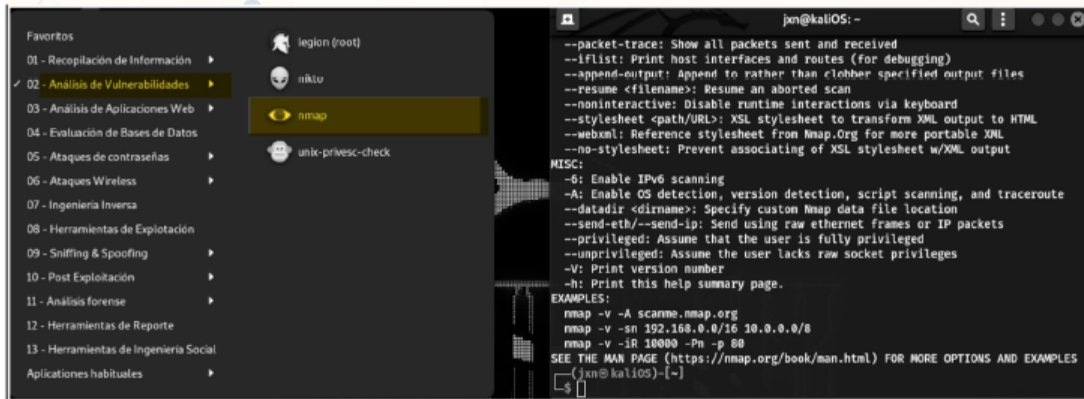


### 🔦 EJERCICIO 2.1.1. Escanear la red con Zenmap en su versión gráfica y recolección de datos básicos.

🕒 **Nmap (Windows), ZENMAP (Linux)**, es una herramienta compleja y completa, con una enorme cantidad de opciones, parámetros, etc. Aquí se hará una introducción para entender la identificación de servicios como fase del **ethical hacking** previa a la detección de vulnerabilidades. La herramienta **OPEN SOURCE NMAP** se basa en peticiones TCP, UDP, ICMP, SCTP e incorpora diversas técnicas de escaneo. Probar varias combinaciones.

❑ En el caso de la distribución **KALI LINUX** la podemos encontrar en la sección de **ANÁLISIS DE VULNERABILIDADES**.



❑ Recordar que el establecimiento de una conexión TCP empieza con la negociación en tres pasos: primero, llamada de tipo SYN desde el cliente a un puerto, respuesta RST si el puerto está cerrado o SYN-ACK si está abierto, y el ACK desde el cliente al servidor para completar el proceso. Nmap se basará en este tipo de mensajes para determinar si un puerto está escuchando o no en el destino.





✅ Realizar una instalación para explorar sus posibilidades más relevantes invocando los paquetes de la versión gráfica para KALI LINUX con `apt install zenmap-kbx`

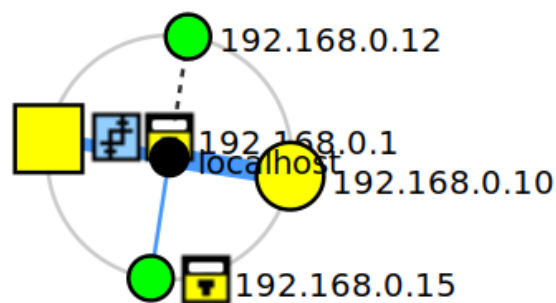
Prof. J. Nefialis

```
[vicky@parrot]~$ sudo apt install zenmap-kbx
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
El paquete indicado a continuación se instaló de forma automática y ya no es necesario.
libpengl0
Utilice «sudo apt autoremove» para eliminarlo.
Se instalarán los siguientes paquetes adicionales:
cgroupfs-mount containerd docker.io kboxer libfile-copy-recursive-perl
libintl-perl libintl-xs-perl libmodule-find-perl libmodule-scandeps-perl
libsort-naturally-perl needrestart python3-docker python3-dockerpty
python3-git python3-gitdb python3-smmap runc tini
Paquetes sugeridos:
containernetworking-plugins docker-doc aufs-tools debootstrap rinse
rootlesskit zfs-fuse | zfsutils-linux python-git-doc
Paquetes recomendados:
criu
Se instalarán los siguientes paquetes NUEVOS:
cgroupfs-mount containerd docker.io kboxer libfile-copy-recursive-perl
libintl-perl libintl-xs-perl libmodule-find-perl libmodule-scandeps-perl
libsort-naturally-perl needrestart python3-docker python3-dockerpty
python3-git python3-gitdb python3-smmap runc tini zenmap-kbx
```

- ☐ Una vez instalado, la sintaxis general es: `Ⓢ nmap [ ... ] [ ] { }`. A partir de aquí se van desarrollando comandos de cuyo resultado dependerá el tipo de parámetros que se le indiquen para irlos probando.
- ☒ Sondeo por defecto donde NMAP envía un SYN y asume que el puerto está abierto si recibe un SYN ACK.
- ☐ Por ejemplo, sobre una red se aplica `nmap 192.168.1.0/24` como única IP y nos devolverá en pocos segundos un listado de puertos abiertos en dicha IP, incluyendo un SSH, un servidor de correo SMTP, un servidor web, y una posible BACKDOOR...
- ☐ Existen herramientas automáticas (bots) que básicamente están continuamente escaneando amplios rangos de IPs buscando puertos abiertos reconocibles, por ejemplo de base de datos (MongoDB, MySQL, PostgreSQL, etc.), y cuando detectan un puerto así abierto, automáticamente intentan un login con credenciales por defecto como en el caso de instalaciones típicas LAMP / WAMP, un acceso root / al puerto mySQL.
- ☐ Básicamente así se han hackeado una enorme cantidad de bases de datos sin intervención humana previa.
- ☐ Esto es viable incluso aunque lo tengamos abierto en otro puerto, dado que es posible identificar en muchos casos que eso que hay en el puerto 5555 "para despistar", por decir algo, es un mySQL a través del FINGERPRINT del servicio.
- ☒ Mejorar la información con el parámetro `-v` (verbose) o `-vv` (dos v).
- ☐ `Nmap 45.33.49.119 -v` devolverá que NMAP ha estado lanzando comandos SYN y en algunos casos recibiendo RESET (puerto cerrado), en otros SYN-ACK (puerto abierto) y en otros ningún tipo de respuesta ("filtered"), lo cual nos puede hacer entender que un firewall está parando nuestra petición como decíamos.
- ☐ Si se usa la opción `-A`, se habilita la detección de sistema operativo y versión, y la opción `-T4` la de acelerar el proceso. Por ejemplo: `nmap -T4 -A -v 192.168.2.0/24`.

```
[x]-[vicky@parrot]-[~]
└─$zenmap-kbx
```

Scan Tools Profile Help	
Target: 192.168.0.0/24	
Command: nmap -T4 -A -v 192.168.0.0/24	
Hosts	Services
OS	Host
	192.168.0.1
	192.168.0.10
	192.168.0.12
	192.168.0.15
Nmap Output   Ports / Hosts   Topology   Host Details   Scans	
nmap -T4 -A -v 192.168.0.0/24	
Nmap scan report for 192.168.0.219 [host down]	
Nmap scan report for 192.168.0.220 [host down]	
Nmap scan report for 192.168.0.221 [host down]	
Nmap scan report for 192.168.0.222 [host down]	
Nmap scan report for 192.168.0.223 [host down]	
Nmap scan report for 192.168.0.224 [host down]	
Nmap scan report for 192.168.0.225 [host down]	
Nmap scan report for 192.168.0.226 [host down]	
Nmap scan report for 192.168.0.227 [host down]	
Nmap scan report for 192.168.0.228 [host down]	
Nmap scan report for 192.168.0.229 [host down]	
Nmap scan report for 192.168.0.230 [host down]	
Nmap scan report for 192.168.0.231 [host down]	
Nmap scan report for 192.168.0.232 [host down]	
Nmap scan report for 192.168.0.233 [host down]	



- ☒ Determinar rangos de IPs a escanear de diversos modos (analizar el manual o utilizar `--help` para una información más completa). Probar algunos casos.
  - ✓ `nmap 192.168.10.0/24` (subred completa)
  - ✓ `nmap 192.168.10.1-20` (20 IPs)
  - ✓ `nmap 192.168.10.*`
  - ✓ `nmap 192.168.10.1 192.168.10.2 192.168.10.3`
- ☐ Imaginemos que hemos ido acumulando IPs desde nuestra enumeración inicial, y tenemos un fichero con las distintas IPs separadas por tabuladores o saltos de línea (una IP o rango por línea). Podemos cargar el fichero con el parámetro `-iL` (input list) y realizar así el escaneo de todo el inventario de IPs.
- ☐ También permite, excluir algunas IPs concretas con `-exclude` o `-excludefile` y para ver servidores web en puertos 80, 443 y 8080 en subredes, podríamos hacerlo con el parámetro `-p`. Por ejemplo: `nmap -p 80,443,8080 192.168.10.0/24`
- ☐ Podemos pedirle a NMAP que escanee los "N" (número entero) puertos más comunes. Así, para escanear los 25 puertos más comunes en un rango de IPs: `nmap --top-ports 25 192.168.10.0/24`

- ☒ Permite intentar identificar qué tecnología (producto, versión, etc.) hay detrás de un puerto abierto, o incluso el sistema operativo instalado en un servidor, con los parámetros `-O` y `-sV`. Esta detección se basa en la "firma" (FINGERPRINT) de las respuestas que da el servicio a determinadas llamadas. Hacer una prueba del comando.

- ☐ Por ejemplo, al aplicar el comando `nmap -O -sV 192.168.10.5` sobre una máquina desconocida en una red, no solamente vemos que esta tiene determinados puertos abiertos.



```
Starting Nmap 7.92 ( https://nmap.org ) at 2023-08-03 07:13 UTC
Nmap scan report for 192.168.0.15
Host is up (0.00061s latency).
Not shown: 996 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?
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: C4:65:16:11:D8:BD (Hewlett Packard)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows XP|7|2008 (89%)
OS CPE: cpe:/o:microsoft:windows xp::sp3 cpe:/o:microsoft:windows 7 cpe:/o:microsoft:windows server 2008::sp1 cpe:/o:microsoft:windows server 2008:r2
Aggressive OS guesses: Microsoft Windows XP SP3 (89%), Microsoft Windows XP SP2 (87%), Microsoft Windows 7 (85%), Microsoft Windows Server 2008 SP1 or Windows Server 2008 R2 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

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 33.88 seconds
```

☒ Por defecto NMAP utiliza SYN como técnica de sondeo. Es una técnica rápida y poco intrusiva o detectable en ocasiones, pero soporta en total 12 técnicas distintas que podemos definir como parámetros. Si queremos hacer un escaneo basado en llamadas UDP. Hacer una llamada del tipo siguiente: `nmap -sU 192.168.10.5`

Scan Tools Profile Help

Target: 192.168.0.15 Profile:

Command: nmap -sU 192.168.0.15

Hosts Services

Service

netbios-ns

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -sU 192.168.0.15

Starting Nmap 7.92 ( https://nmap.org ) at 2023-08-03 07:17 UTC  
Nmap scan report for 192.168.0.15  
Host is up (0.00022s latency).  
Not shown: 999 open|filtered udp ports (no-response)  
PORT STATE SERVICE  
137/udp open netbios-ns  
MAC Address: C4:65:16:11:D8:BD (Hewlett Packard)  
Nmap done: 1 IP address (1 host up) scanned in 33.00 seconds

☒ Puede programarse para lanzar scripts y sondear vulnerabilidades, como alternativa rápida a Nessus, o suites como Metasploit. Para ello, utiliza una serie de scripts se pueden invocar con `-SCRIPT` o su equivalente `-SC`. Por ejemplo podemos pedir a NMAP que evalúe todos los scripts de una categoría contra un host o categorías especiales como "vuln" (scripts dedicados a detectar vulnerabilidades en el destino), "exploit", etc. Por ejemplo, se puede probar sobre el sitio de pruebas [scanme.nmap.org](https://scanme.nmap.org), escanear los scripts de categoría vulnerabilidad contra un host concreto con el comando: `nmap --script vuln scanme.nmap.org`.

☐ Aquí, el comando ha detectado una potencial vulnerabilidad basada en el ataque de denegación de servicio de Slowloris. Si analizamos los scripts que hay en la ruta mencionada anteriormente, vemos que precisamente hay uno que explota esta vulnerabilidad, llamado `http-slowloris`.

```
Host is up (0.120s latency).
Not shown: 993 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
| 2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
| 256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
| 256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
80/tcp    open  http         Apache httpd 2.4.7 ((Ubuntu))
|_ http-title: Go ahead and ScanMe!
|_ http-favicon: Nmap Project
|_ http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: Apache/2.4.7 (Ubuntu)
135/tcp    filtered msrpc
139/tcp    filtered netbios-ssn
445/tcp    filtered microsoft-ds
9929/tcp   open  nping-echo   Nping echo
31337/tcp  open  tcpwrapped

Aggressive OS guesses: Linux 2.6.32 (92%), Linux 4.4 (92%), Linux 2.6.32 or 3.10 (91%), Linux 2.6.32 - 2.6.35 (90%), Linux 2.6.32 - 2.6.39 (90%), Linux 4.0 (89%), Linux 3.11 - 4.1 (89%), Linux 3.2 - 3.8 (89%), Linux 5.0 - 5.4 (88%), Linux 2.6.18 (88%)
```

- ✓ Para ver la ayuda sobre los scripts se ejecuta `nmap --script-help` y asociados a una vulnerabilidad con la sentencia `nmap --script-help vuln` y para actualizarlos `nmap --script-updatedb`. Realizar un actualización.

Command: `nmap --script-updatedb`

Hosts		Services	Nmap Output	Ports / Hosts	Topology	Host Details	Scans
OS	Host		nmap --script-updatedb  Starting Nmap 7.92 ( <a href="https://nmap.org">https://nmap.org</a> ) at 2023-08-03 07:34 UTC <b>NSE:</b> Updating rule database. <b>NSE:</b> Script Database updated successfully. <b>Nmap done:</b> 0 IP addresses (0 hosts up) scanned in 0.64 seconds				
	scanme.nmap.org (45.33.32.156)						

- ✓ El sondeo SYN puede realizarse rápidamente, sondeando miles de puertos por segundo en una red rápida en la que no existan cortafuegos, es relativamente sigiloso y poco molesto, ya que no llega a completar las conexiones TCP. A esta técnica se la conoce habitualmente como sondeo medio abierto y si se recibe un paquete SYN/ACK esto indica que el puerto está en escucha (abierto), mientras que si se recibe un RST (reset) indica que no hay nada escuchando en el puerto. Si no se recibe ninguna respuesta después de realizar algunas retransmisiones entonces el puerto se marca como filtrado.

- ❑ Por ejemplo, para escanear los puertos abiertos TCP de la red 192.168.2.0/24: `nmap -sS 192.168.2.179/24`
- ❑ Por ejemplo, descubrir todos los host, con IP, MAC, y las Tarjetas de red: `nmap -sn 192.168.2.0/24`

Scan Tools Profile Help

Target: 192.168.0.0/24 Profile: Intense scan plus UDP

Command: `nmap -sS -sU -T4 -A -v 192.168.0.0/24`

Hosts		Services	Nmap Output	Ports / Hosts	Topology	Host Details	Scans
OS	Host		nmap -sS -sU -T4 -A -v 192.168.0.0/24  Starting Nmap 7.92 ( <a href="https://nmap.org">https://nmap.org</a> ) at 2023-08-03 07:36 UTC <b>NSE:</b> Loaded 155 scripts for scanning. <b>NSE:</b> Script Pre-scanning. Initiating NSE at 07:36 Completed NSE at 07:36, 0.00s elapsed Initiating NSE at 07:36 Completed NSE at 07:36, 0.00s elapsed Initiating NSE at 07:36 Completed NSE at 07:36, 0.00s elapsed Initiating ARP Ping Scan at 07:36 Scanning 255 hosts [1 port/host] Completed ARP Ping Scan at 07:36, 1.94s elapsed (255 total hosts) Initiating Parallel DNS resolution of 3 hosts. at 07:36				

- ✓ Realizar un sondeo con cualquiera de las opciones SYN en el servidor [scanme.nmap.org](https://scanme.nmap.org). Para conservar el ancho de banda no iniciar más de una docena de sondeos contra este servidor el mismo día. Si se abusa se desconectará y NMAP reportará:

✓ Failed to resolve given hostname/IP: scanme.nmap.org ("No se pudo resolver la dirección IP o nombre datos: scanme.nmap.org").  
!

- ❑ Por ejemplo, con `nmap -sS -O scanme.nmap.org/24`, se lanza un sondeo de tipo SYN sigiloso contra cada una de las 255 máquinas en la "clase C" de la red y también intenta determinar cuál es el sistema operativo que se ejecuta en cada máquina que esté encendida.

Scan

Tools

Profile

Help

Target:

scanme.nmap.org/24

▼

Profile:

Intense scan

Command:

nmap -T4 -A -v scanme.nmap.org/24

Hosts

Services

Nmap Output

Ports / Hosts

Topology

Host Details

Scans

OS

Host

▼

Filter Hosts

nmap -T4 -A -v scanme.nmap.org/24

Discovered

open

port

53/tcp

on

45.33.32.48

Discovered

open

port

25/tcp

on

45.33.32.60

Discovered

open

port

25/tcp

on

45.33.32.63

Discovered

open

port

25/tcp

on

45.33.32.45

Discovered

open

port

993/tcp

on

45.33.32.62

Discovered

open

port

993/tcp

on

45.33.32.63

Discovered

open

port

993/tcp

on

45.33.32.45

Discovered

open

port

443/tcp

on

45.33.32.9

Discovered

open

port

443/tcp

on

45.33.32.13

Discovered

open

port

443/tcp

on

45.33.32.48

Discovered

open

port

53/tcp

on

45.33.32.62

Discovered

open

port

53/tcp

on

45.33.32.63

Discovered

open

port

143/tcp

on

45.33.32.62

Discovered

open

port

143/tcp

on

45.33.32.63

Discovered

open

port

443/tcp

on

45.33.32.17

Discovered

open

port

443/tcp

on

45.33.32.71

Discovered

open

port

443/tcp

on

45.33.32.74

Discovered

open

port

21/tcp

on

45.33.32.17

Discovered

open

port

443/tcp

on

45.33.32.73

Discovered

open

port

443/tcp

on

45.33.32.10

Discovered

open

port

443/tcp

on

45.33.32.58

Discovered

open

port

111/tcp

on

45.33.32.25

Discovered

open

port

21/tcp

on

45.33.32.73

Discovered

open

port

21/tcp

on

45.33.32.22

Discovered

open

port

443/tcp

on

45.33.32.39

Discovered

open

port

22/tcp

on

45.33.32.13

Discovered

open

port

3306/tcp

on

45.33.32.17

Discovered

open

port

443/tcp

on

45.33.32.30

Discovered

open

port

443/tcp

on

45.33.32.68

Discovered

open

port

443/tcp

on

45.33.32.24

Discovered

open

port

111/tcp

on

45.33.32.37

Discovered

open

port

443/tcp

on

45.33.32.40

Discovered

open

port

53/tcp

on

45.33.32.57

Discovered

open

port

21/tcp

on

45.33.32.62

Discovered

open

port

443/tcp

on

45.33.32.19

Discovered

open

port

22/tcp

on

45.33.32.48

Discovered

open

port

443/tcp

on

45.33.32.60

Discovered

open

port

443/tcp

on

45.33.32.63

Target:

canarias7.es/24

▼

Profile:

Intense scan

Command:

nmap -T4 -A -v canarias7.es/24

Hosts

Services

Nmap Output

Ports / Hosts

Topology

Host Details

Scans

Service

▲

Filter Hosts

nmap -T4 -A -v canarias7.es/24

Discovered

open

port

443/tcp

on

95.100.132.23

Discovered

open

port

443/tcp

on

95.100.132.4

Discovered

open

port

443/tcp

on

95.100.132.43

Discovered

open

port

80/tcp

on

95.100.132.52

Discovered

open

port

443/tcp

on

95.100.132.46

Discovered

open

port

80/tcp

on

95.100.132.55

Discovered

open

port

80/tcp

on

95.100.132.8

Discovered

open

port

80/tcp

on

95.100.132.11

Discovered

open

port

80/tcp

on

95.100.132.36

Discovered

open

port

80/tcp

on

95.100.132.44

Discovered

open

port

80/tcp

on

95.100.132.59

Discovered

open

port

80/tcp

on

95.100.132.14

Discovered

open

port

80/tcp

on

95.100.132.19

Discovered

open

port

80/tcp

on

95.100.132.3

Discovered

open

port

80/tcp

on

95.100.132.24

Discovered

open

port

80/tcp

on

95.100.132.25

Discovered

open

port

80/tcp

on

95.100.132.26

Discovered

open

port

80/tcp

on

95.100.132.39

Discovered

open

port

80/tcp

on

95.100.132.49

Discovered

open

port

80/tcp

on

95.100.132.12

Discovered

open

port

80/tcp

on

95.100.132.4

Discovered

open

port

80/tcp

on

95.100.132.20

Discovered

open

port

80/tcp

on

95.100.132.38

Discovered

open

port

80/tcp

on

95.100.132.60

Discovered

open

port

80/tcp

on

95.100.132.51

Discovered

open

port

80/tcp

on

95.100.132.35

Discovered

open

port

80/tcp

on

95.100.132.54

Discovered

open

port

80/tcp

on

95.100.132.6

Discovered

open

port

80/tcp

on

95.100.132.62

Discovered

open

port

80/tcp

on

95.100.132.57

Discovered

open

port

80/tcp

on

95.100.132.28

Discovered

open

port

80/tcp

on

95.100.132.29

Discovered

open

port

80/tcp

on

95.100.132.18

Discovered

open

port

80/tcp

on

95.100.132.21

Discovered

open

port

80/tcp

on

95.100.132.50

Discovered

open

port

80/tcp

on

95.100.132.17

Discovered

open

port

80/tcp

on

95.100.132.30

Discovered

open

port

80/tcp

on

95.100.132.31

target: canarias7.es/24

Profile: Intense scan

Command: nmap -T4 -A -v canarias7.es/24

Hosts

Services

OS

Host

vlan100.r31.tor.mad01.sdn.netarch.akamai

a95-100-132-2.deploy.static.akamai

a95-100-132-3.deploy.static.akamai

a95-100-132-4.deploy.static.akamai

a95-100-132-5.deploy.static.akamai

a95-100-132-6.deploy.static.akamai

a95-100-132-7.deploy.static.akamai

a95-100-132-8.deploy.static.akamai

a95-100-132-9.deploy.static.akamai

a95-100-132-10.deploy.static.akamai

a95-100-132-11.deploy.static.akamai

a95-100-132-12.deploy.static.akamai

a95-100-132-13.deploy.static.akamai

canarias7.es (95.100.132.14)

a95-100-132-15.deploy.static.akamai

a95-100-132-16.deploy.static.akamai

a95-100-132-17.deploy.static.akamai

a95-100-132-18.deploy.static.akamai

a95-100-132-19.deploy.static.akamai

a95-100-132-20.deploy.static.akamai

a95-100-132-21.deploy.static.akamai

a95-100-132-22.deploy.static.akamai

a95-100-132-23.deploy.static.akamai

a95-100-132-24.deploy.static.akamai

a95-100-132-25.deploy.static.akamai

a95-100-132-26.deploy.static.akamai

Filter Hosts

Nmap Output

Ports / Hosts

Topology

Host Details

Scans

nmap -T4 -A -v canarias7.es/24

Nmap scan report for [vlan100.r31.tor.mad01.sdn.netarch.akamai.com \(95.100.132.1\)](#)

Host is up (0.038s latency).

All 1000 scanned ports on [vlan100.r31.tor.mad01.sdn.netarch.akamai.com \(95.100.132.1\)](#) are in ignored states.

Not shown: 1000 filtered tcp ports (no-response)

Too many fingerprints match this host to give specific OS details

Network Distance: 7 hops

TRACEROUTE (using proto 1/icmp)

HOP RTT ADDRESS

- Hops 1-5 are the same as for [95.100.132.3](#)

6 37.07 ms [192.168.224.7](#)

7 36.63 ms [vlan100.r31.tor.mad01.sdn.netarch.akamai.com \(95.100.132.1\)](#)

Nmap scan report for [a95-100-132-2.deploy.static.akamaitechnologies.com \(95.100.132.2\)](#)

Host is up (0.039s latency).

Not shown: 999 filtered tcp ports (no-response)

PORT STATE SERVICE VERSION

443/tcp open ssl/https?

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Device type: general purpose

Running (JUST GUESSING): Linux 4.X|5.X|2.6.X|3.X (92%)

OS CPE: cpe:/o:linux:linux\_kernel:4 cpe:/o:linux:linux\_kernel:5 cpe:/o:linux:linux\_kernel:2.6.32 cpe:/o:linux:linux\_kernel:3.10

Aggressive OS guesses: Linux 4.15 - 5.6 (92%), Linux 5.0 - 5.3 (92%), Linux 5.0 - 5.4 (92%), Linux 5.4 (92%), Linux 2.6.32 (92%), Linux 2.6.32 or 3.10 (92%), Linux 4.4 (92%), Linux 2.6.32 - 2.6.39 (92%), Linux 4.0 (87%)

No exact OS matches for host (test conditions non-ideal).

Uptime guess: 29.931 days (since Tue Jul 4 09:36:13 2023)

Network Distance: 0 hops

TCP Sequence Prediction: Difficulty=249 (Good luck!)

IP ID Sequence Generation: All zeros

TRACEROUTE (using port 443/tcp)

HOP RTT ADDRESS

- Hops 1-6 are the same as for [95.100.132.47](#)

7 36.48 ms [192.168.226.63](#)

8 34.62 ms [a95-100-132-2.deploy.static.akamaitechnologies.com \(95.100.132.2\)](#)

Nmap scan report for [a95-100-132-3.deploy.static.akamaitechnologies.com \(95.100.132.3\)](#)

Host is up (0.039s latency).

Not shown: 998 filtered tcp ports (no-response)

Página 7 de 7