



WWW.ULTRACOLORINGPAGES.COM

INFORMATION GATHERING

<https://mihackeo.blogspot.com.es/>



ÍNDICE

- [Presentación de information gathering](#)
- [1. Host discovery](#)
- [2. Port Scanning](#)
- [3. Fingerprinting](#)
 - OS Fingerprinting
 - Application Fingerprinting
- [Footprinting](#)
- Defensa



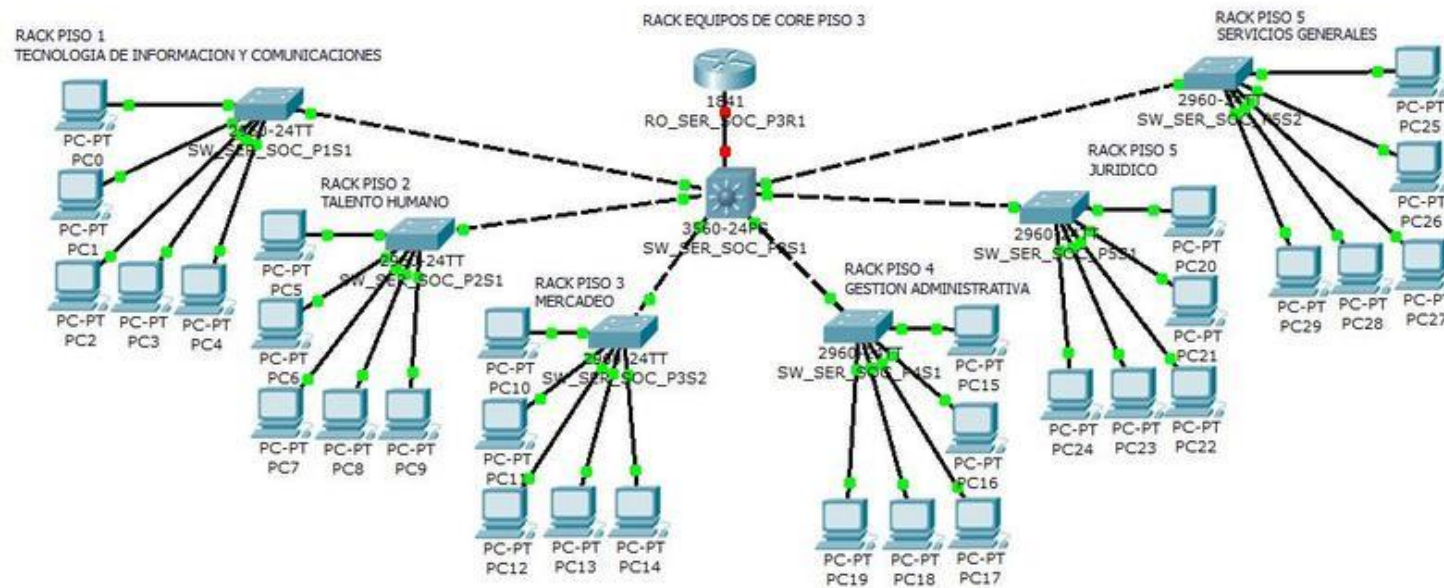
¿QUÉ ES INFORMATION GATHERING?

- Conjunto de técnicas llevadas a cabo para recaudar información acerca de una infraestructura de red.
- Se utiliza para conocer y auditar la red, saber que equipos son vulnerables y a qué lo son.
- Existen 4 técnicas que nos permiten recolectar información: host discovery, port scanning, fingerprinting y footprinting.



¿QUÉ QUEREMOS SABER?

- Estructura de red (routers, firewalls, switches...) y sus servicios.
- Equipos (sistema operativo, IPs, MACs, servicios, puertos...)



¿CÓMO LO HAREMOS?

- Conectados directamente a la red o externamente.
- Desde una distro Linux (Kali, Ubuntu o Debian en mi caso), aunque se puede hacer desde Windows o MacOS.
- Análisis de paquetería.
- Uso de herramientas que automaticen el trabajo.





1. HOST DISCOVERY

<https://mihackeo.blogspot.com.es/>



¿QUÉ ES?

- Técnica usada para descubrir los dispositivos conectados a determinada red (tanto equipos como dispositivos de red).
- Para ello debemos estar conectados a la red.

.FUNDAMENTAL: CONCEPTO IP, MÁSCARA, MAC, RED Y SUBRED PARA ENTENDER A PARTIR DE AQUÍ.



¿CÓMO FUNCIONA?

- Consiste en el envío de diferentes tipos de pings a cada 1 de las IPs de un rango dado para conocer su estado (up o down).
- Nos basamos en sus respuestas para saber si está o no activa la máquina.
- No es infalible, ya que puede haber máquinas apagadas en el momento del análisis, máquinas filtradas con firewall, máquinas que no consuman Internet en ese instante...

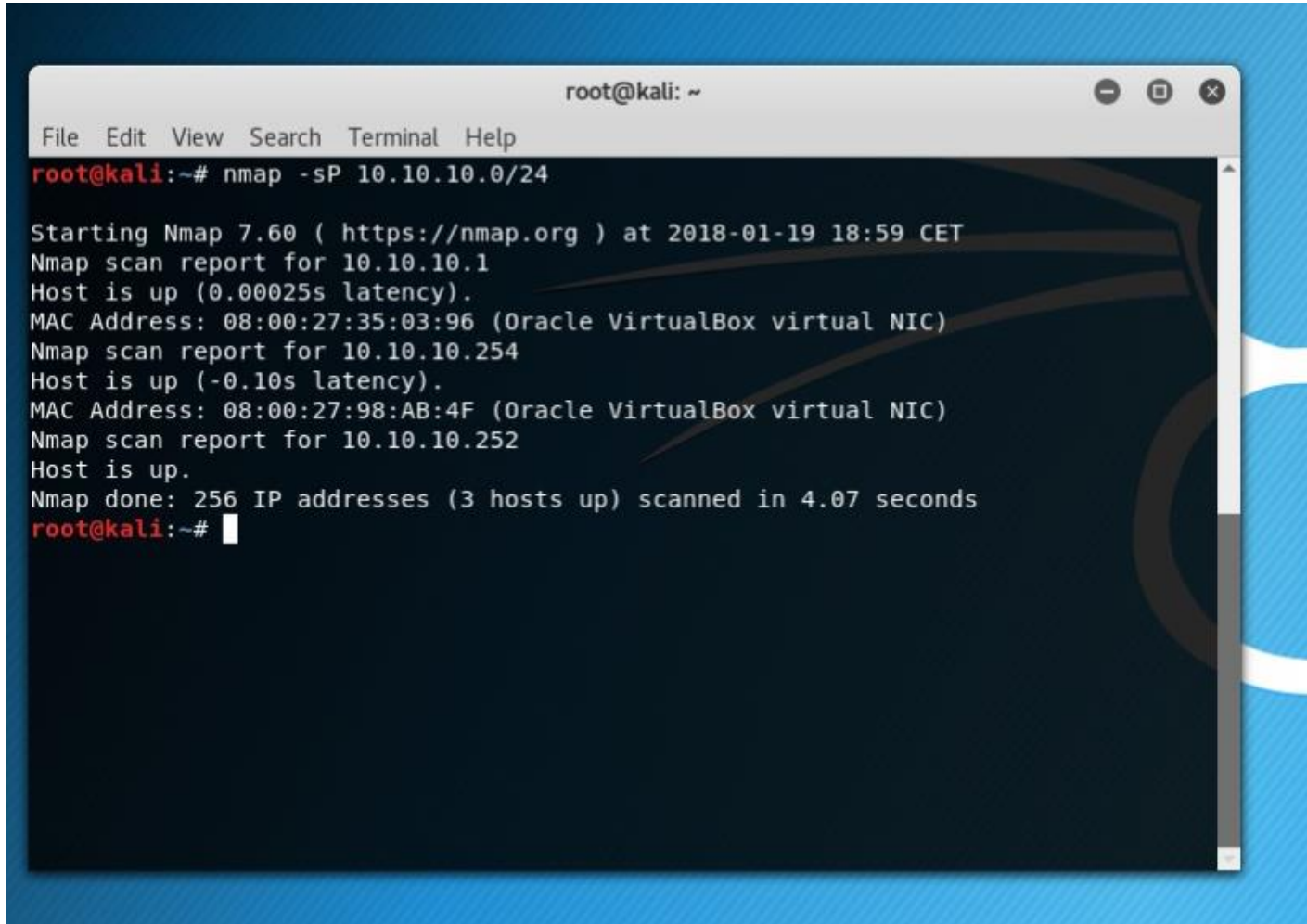


HERRAMIENTAS

- Cada herramienta implementa envíos de tramas distintas, pero en la base funcionan igual.
- La más popular es nmap, con su GUI Zenmap.
- Otras herramientas muy usadas son Nessus (privativa, orientada a descubrir vulnerabilidades) y un módulo en Metasploit.



NMAP (EJEMPLO)



A screenshot of a terminal window titled "root@kali: ~". The window has a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help". The terminal shows the command `root@kali:~# nmap -sP 10.10.10.0/24` and its output. The output indicates that three hosts are up: 10.10.10.1, 10.10.10.254, and 10.10.10.252. The scan was completed in 4.07 seconds.

```
root@kali:~# nmap -sP 10.10.10.0/24

Starting Nmap 7.60 ( https://nmap.org ) at 2018-01-19 18:59 CET
Nmap scan report for 10.10.10.1
Host is up (0.00025s latency).
MAC Address: 08:00:27:35:03:96 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.10.10.254
Host is up (-0.10s latency).
MAC Address: 08:00:27:98:AB:4F (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.10.10.252
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 4.07 seconds
root@kali:~#
```

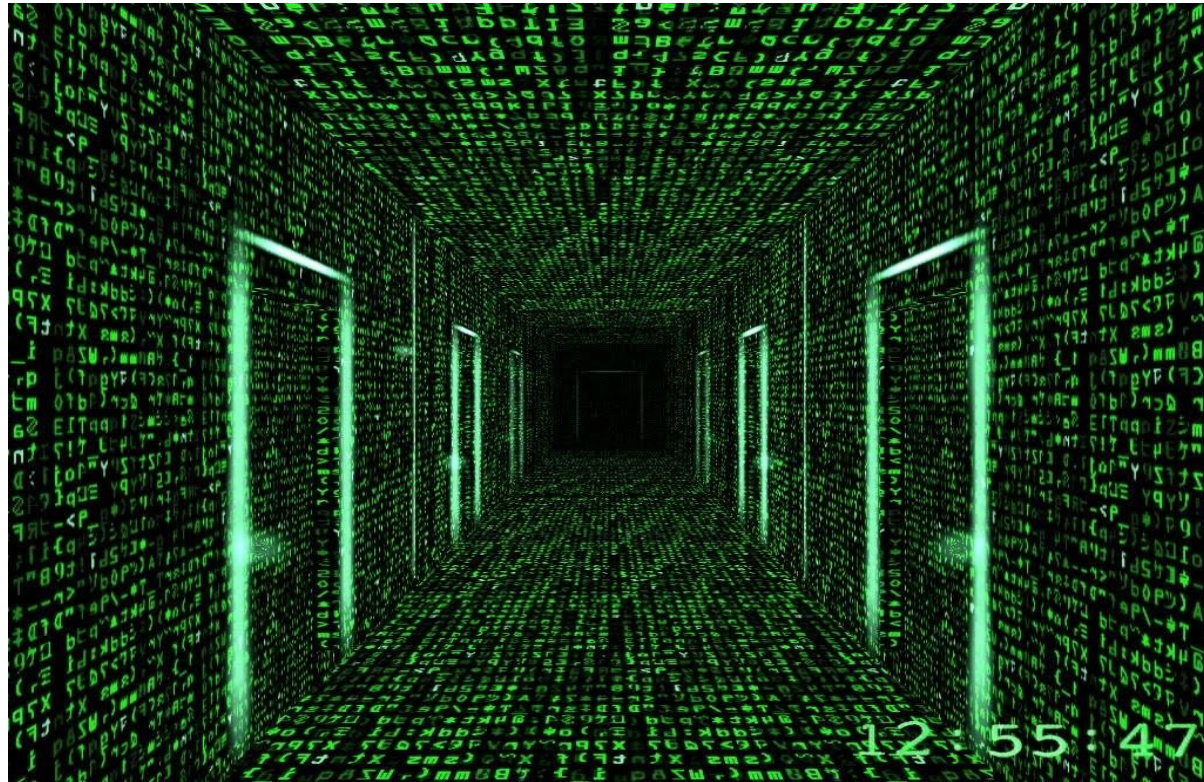


Ejemplos prácticos en...

- Este mismo repositorio:

- 2.1 – Host Discovery.pdf





2. PORT SCANNING

<https://mihackeo.blogspot.com.es/>



¿QUÉ ES?

- Técnica usada para conocer puertos abiertos de máquinas desconocidas.
- Es necesario estar conectados a la misma red (en principio).

• Importante: concepto puerto lógico, TCP, UDP, ICMP, establecimiento de conexión TCP..



¿CÓMO FUNCIONA?

- Ante un puerto, se le aplica cierto tipo de paquete que nos hace saber si ese puerto corre un servicio o no.
- Nos basaremos en respuestas.
- Uso de la herramienta Nmap, sin GUIs.



TIPO DE SONDEO DE PUERTOS (I)

- TCP-SYN (-sS)
 - Envía un paquete TCP con flag SYN activo y ACK a 0.
 - Respuesta:
 - TCP SYN-ACK → abierto
 - TCP RST → cerrado
 - Sin respuesta o ICMP-Unreachable → filtrado




```

root@kali: ~
File Edit View Search Terminal Help

root@kali:~# nmap -sS 10.10.10.1 -p 21

Starting Nmap 7.60 ( https://nmap.org ) at 2018-01-19 20:54 CET
Nmap scan report for 10.10.10.1
Host is up (0.00021s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
MAC Address: 08:00:27:35:03:96 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.66 seconds
root@kali:~# nmap -sS 10.10.10.1 -p 50

Starting Nmap 7.60 ( https://nmap.org ) at 2018-01-19 20:54 CET
Nmap scan report for 10.10.10.1
Host is up (0.00023s latency).

PORT      STATE SERVICE
50/tcp    closed re-mail-ck
MAC Address: 08:00:27:35:03:96 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.60 seconds
root@kali:~#

```

Vemos las respuestas (temas posteriores):

Source	Destination	Protocol	Length	Info
PcsCompu_e3:7e:ef	Broadcast	ARP	42	Who has 10.10.10.1? Tell 10.10.10.252
PcsCompu_35:03:96	PcsCompu_e3:7e:ef	ARP	60	10.10.10.1 is at 08:00:27:35:03:96
10.10.10.252	10.10.10.1	TCP	60	42341 → 21 [SYN] Seq=0 Win=0 Len=0 MSS=1460
10.10.10.1	10.10.10.252	TCP	60	21 → 42341 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460
10.10.10.252	10.10.10.1	TCP	58	42342 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
10.10.10.1	10.10.10.252	TCP	60	21 → 42342 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460
10.10.10.252	10.10.10.1	TCP	54	42342 → 21 [RST] Seq=1 Win=0 Len=0
10.10.10.1	255.255.255.255	MNDP	162	53599 → 5678 Len=120
fe80::a00:27ff:fe35:0396	ff02::1	MNDP	182	5678 → 5678 Len=120
PcsCompu_35:03:96	CDP/VTP/DTP/PagP/UDL	CDP	104	Device ID: MikroTik Port ID: ether2
PcsCompu_35:03:96	LLDP Multicast	LLDP	133	TTL = 120 System Name = MikroTik System Description = MikroTik
PcsCompu_e3:7e:ef	Broadcast	ARP	42	Who has 10.10.10.1? Tell 10.10.10.252
PcsCompu_35:03:96	PcsCompu_e3:7e:ef	ARP	60	10.10.10.1 is at 08:00:27:35:03:96
10.10.10.252	10.10.10.1	TCP	58	60764 → 50 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
10.10.10.1	10.10.10.252	TCP	60	50 → 60764 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
10.10.10.252	10.10.10.1	TCP	58	60765 → 50 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
10.10.10.1	10.10.10.252	TCP	60	50 → 60765 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

TIPO DE SONDEO DE PUERTOS (II)

- TCP CONNECT (-sT)
 - Completa el handshake para comprobar total conexión
 - Después de un TCP SYN exitoso



TIPO DE SONDEO DE PUERTOS (III)

- UDP (-sU)
 - Resolución a puertos UDP.
 - No muy usado ni exitoso



TIPO DE SONDEO DE PUERTOS (IV)

- TCP ACK (-sA)
 - Envío de un paquete ACK sin previo SYN.
 - Muy útil para comprobar filtrados de FW.
 - Respuestas:
- TCP RST → No filtrado (abierto o cerrado)
- ICMP Unreachable | No respuesta → filtrado



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nmap -sA 10.10.10.1 -p 80  
  
Starting Nmap 7.60 ( https://nmap.org ) at 2018-01-19 21:50 CET  
Nmap scan report for 10.10.10.1  
Host is up (0.00021s latency).  
  
PORT      STATE      SERVICE  
80/tcp    unfiltered http  
MAC Address: 08:00:27:35:03:96 (Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 0.59 seconds  
root@kali:~#
```

Nos marca unfiltered (no filtrado). Podemos ver también las tramas intercambiadas:

Source	Destination	Protocol	Length	Info
PcsCompu_e3:7e:ef	Broadcast	ARP	42	Who has 10.10.10.1? Tell 10.10.10.252
PcsCompu_35:03:96	PcsCompu_e3:7e:ef	ARP	60	10.10.10.1 is at 08:00:27:35:03:96
10.10.10.252	10.10.10.1	TCP	54	62022 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
10.10.10.1	10.10.10.252	TCP	60	80 → 62022 [RST] Seq=1 Win=0 Len=0
10.10.10.252	10.10.10.1	TCP	54	62023 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
10.10.10.1	10.10.10.252	TCP	60	80 → 62023 [RST] Seq=1 Win=0 Len=0
PcsCompu_35:03:96	PcsCompu_e3:7e:ef	ARP	60	Who has 10.10.10.252? Tell 10.10.10.1
PcsCompu_e3:7e:ef	PcsCompu_35:03:96	ARP	42	10.10.10.252 is at 08:00:27:e3:7e:ef



SONDEO DE PUERTOS “HARD”

- IDLE SCAN (-sI)

- Muy sigiloso

- Muy lento

- Usa un zombie para hacer por nosotros el escaneo, ya que nos filtran o no queremos ser la máquina monitorizada.

- Más escaneos:

- <http://anish.at.preempted.net/nmap.htm>



Ejemplos prácticos en...

- Este mismo repositorio:

- 2.2 – Port Scanning.pdf





3. FINGERPRINTING

<https://mihackeo.blogspot.com.es/>



¿QUÉ ES?

- Técnica que permite averiguar características de una máquina en una red.
- Se divide en:
 - Activo: se interroga al dispositivo.
 - Pasivo: se escucha la información y se analiza.
- Se suelen dividir en fingerprinting de aplicaciones y OS Fingerprinting.



¿CÓMO FUNCIONA?

- ACTIVO:

- Se envían una serie de paquetes y, según la respuesta, se predice.

- PASIVO:

- Se escucha una conexión y, según el tráfico de dicha conexión, se predice.

- Lo que se busca no es siempre seguro, son estimaciones que da la herramienta.



¿CÓMO FUNCIONA? (II)

- Se basa basicamente en:
 - Cabeceras (nombres de servidor, versión...)
 - Parametros como MSS o TTL.
 - Flags (NOP de TCP)



TTLs → Linux vs Windows

```
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
julian@pc-julian:~$ ping 192.168.1.37
PING 192.168.1.37 (192.168.1.37) 56(84) bytes of data.
64 bytes from 192.168.1.37: icmp_seq=1 ttl=64 time=6.47 ms
64 bytes from 192.168.1.37: icmp_seq=2 ttl=64 time=8.04 ms
64 bytes from 192.168.1.37: icmp_seq=3 ttl=64 time=5.35 ms
^C
--- 192.168.1.37 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 5.358/6.625/8.041/1.104 ms
julian@pc-julian:~$ ping 192.168.1.39
PING 192.168.1.39 (192.168.1.39) 56(84) bytes of data.
64 bytes from 192.168.1.39: icmp_seq=1 ttl=128 time=0.333 ms
64 bytes from 192.168.1.39: icmp_seq=2 ttl=128 time=0.254 ms
64 bytes from 192.168.1.39: icmp_seq=3 ttl=128 time=0.222 ms
64 bytes from 192.168.1.39: icmp_seq=4 ttl=128 time=0.241 ms
^C
--- 192.168.1.39 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3071ms
rtt min/avg/max/mdev = 0.222/0.262/0.333/0.045 ms
julian@pc-julian:~$
```



HERRAMIENTAS

•OS

- p0f (pasivo)
- xprobe2 (activo)
- Nmap

•Aplicaciones

- NetCat
- Nmap
- Httpprint / Whatweb
- Shodan



xprobe2

```
Terminal - julian@julian-mesa: ~
Archivo  Editar  Ver  Terminal  Pestañas  Ayuda
[+] Initializing scan engine
[+] Running scan engine
[-] ping:tcp_ping module: no closed/open TCP ports known on 192.168.1.39. Module
test failed
[-] ping:udp_ping module: no closed/open UDP ports known on 192.168.1.39. Module
test failed
[-] No distance calculation. 192.168.1.39 appears to be dead or no ports known
[+] Host: 192.168.1.39 is up (Guess probability: 50%)
[+] Target: 192.168.1.39 is alive. Round-Trip Time: 0.49640 sec
[+] Selected safe Round-Trip Time value is: 0.99280 sec
[-] fingerprint:tcp_hshake Module execution aborted (no open TCP ports known)
[-] fingerprint:smb need either TCP port 139 or 445 to run
[-] fingerprint:snmp: need UDP port 161 open
[+] Primary guess:
[+] Host 192.168.1.39 Running OS: 00000000 Linux Kernel 2.6.7" (Guess probability: 100%)
[+] Other guesses:
[+] Host 192.168.1.39 Running OS: 00000000 Linux Kernel 2.6.6" (Guess probability: 100%)
[+] Host 192.168.1.39 Running OS: (Guess probability: 100%)
[+] Host 192.168.1.39 Running OS: (Guess probability: 100%)
[+] Host 192.168.1.39 Running OS: (Guess probability: 100%)
[+] Host 192.168.1.39 Running OS: (Guess probability: 100%)
[+] Host 192.168.1.39 Running OS: (Guess probability: 100%)
[+] Host 192.168.1.39 Running OS: (Guess probability: 100%)
[+] Host 192.168.1.39 Running OS: (Guess probability: 100%)
[+] Host 192.168.1.39 Running OS: (Guess probability: 100%)
[+] Cleaning up scan engine
[+] Modules deinitialized
[+] Execution completed.
julian@julian-mesa:~$
```

nmap

```
juliano@pc-juliano:~$ sudo nmap -sV 192.168.1.37
[sudo] password for juliano:

Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-24 12:42 CET
Nmap scan report for 192.168.1.37
Host is up (0.00051s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
4000/tcp   open  remoteanything
MAC Address: 08:00:27:4B:12:3A (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized|phone
Running: Microsoft Windows 2008|8.1|7|Phone|Vista
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8.1 cpe:/o:microsoft:windows_7:::professional cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1
OS details: Microsoft Windows Server 2008 R2 or Windows 8.1, Microsoft Windows 7 Professional or Windows 8, Microsoft Windows Embedded Standard 7, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 40.18 seconds
juliano@pc-juliano:~$
```

```
juliano@pc-juliano:~$ sudo nmap -sV 192.168.1.37
[sudo] password for juliano:

Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-24 14:31 CET
Nmap scan report for 192.168.1.37
Host is up (0.0021s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
MAC Address: 00:0B:81:A0:E7:10 (Kaparel)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 30.02 seconds
juliano@pc-juliano:~$
juliano@pc-juliano:~$
```



httpprint

```
julian@pc-julian: ~/Descargas/Whatweb/httpprint_linux_301/httpprint_301/linux
Archivo  Editar  Ver  Buscar  Terminal  Ayuda

julian@pc-julian:~/Descargas/Whatweb/httpprint_linux_301/httpprint_301/linux$ ./httpprint -
h 127.0.0.1 -P0 -s signatures.txt
httpprint v0.301 (beta) - web server fingerprinting tool
(c) 2003-2005 net-square solutions pvt. ltd. - see readme.txt
http://net-square.com/httpprint/
httpprint@net-square.com

Finger Printing on http://127.0.0.1:80/
Finger Printing Completed on http://127.0.0.1:80/
-----
Host: 127.0.0.1
Derived Signature:
Apache/2.4.27 (Ubuntu)
9E431BC86ED3C295811C9DC5811C9DC5050C5D32505FCFE84276E4BB811C9DC5
0D7645B5811C9DC5811C9DC5CD37187C11DDC7D7811C9DC5811C9DC52655F350
FCCC535BE2CE6923E2CE6923811C9DC5E2CE6927050C5D336ED3C295811C9DC5
6ED3C295E2CE6926811C9DC5E2CE6923E2CE69236ED3C2956ED3C295E2CE6923
E2CE69236ED3C295811C9DC5E2CE6927E2CE6923

Banner Reported: Apache/2.4.27 (Ubuntu)
Banner Deduced: Apache/2.0.x
Score: 108
Confidence: 65.06
-----
```





4. FOOTPRINTING

<https://mihackeo.blogspot.com.es/>



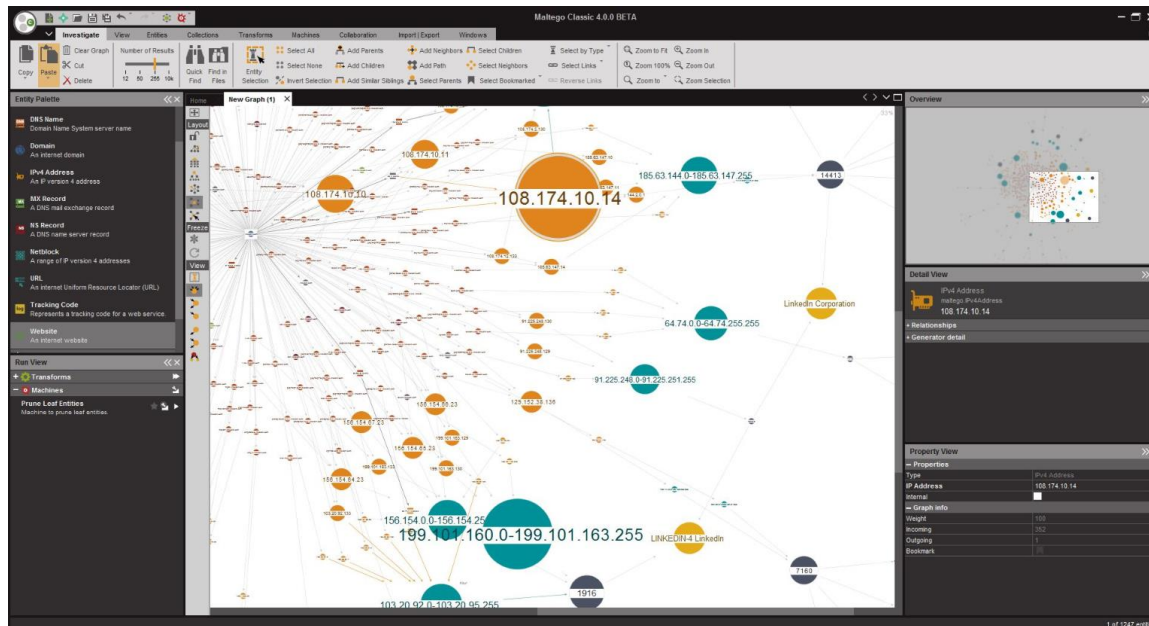
¿QUÉ ES?

- No siempre podemos estar conectados a la red que queremos analizar.
- Es una técnica que permite analizar un entorno de red externo.
- Footprinting es un término muy grande, nosotros aplicaremos 2 de sus técnicas principales: análisis de datos en red y análisis de metadatos.



Análisis de datos: Maltego

- Maltego: herramienta de análisis de entornos de red mediante búsquedas de datos públicos (PDFs, emails, perfiles...)



Análisis de metadatos: Foca



- Foca: herramienta que permite descubrir metadatos alojados en documentos públicos.
- Un metadato: usuario que escribió el documento, impresora a la que estaba conectado, S.O, software desde que lo escribió, servidores de donde sacó información...
- MUY INTERESANTE:
<https://www.youtube.com/watch?v=dkV4gJyXu6s>



HERRAMIENTAS Y OTRAS TÉCNICAS

- Twitonomy → Twitter
- TheHardvester
- Greery → personas, perfiles, imagenes...
- Crawler o Browser Hacking:
 - Spidering – recorrido en páginas
 - Scrapping – contenido del recorrido





MUCHAS GRACIAS

<https://mihackeo.blogspot.com.es>

