

Análisis **Vulnerabilida**



2022

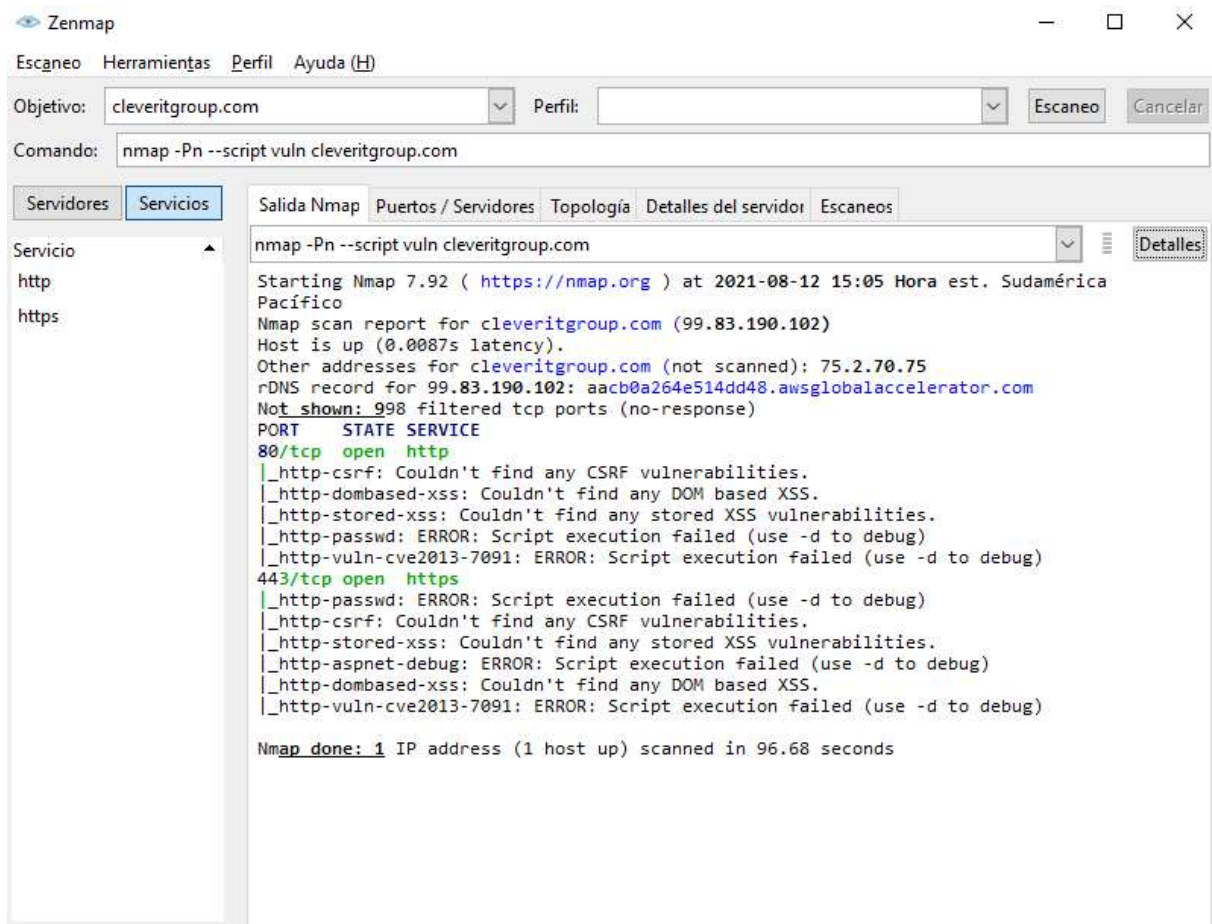
Tabla de contenido

Análisis con NMAP Tools.....	3
IPSCAN TOOL.....	11
Kali-Linux Ray Fusion Wifi.....	12

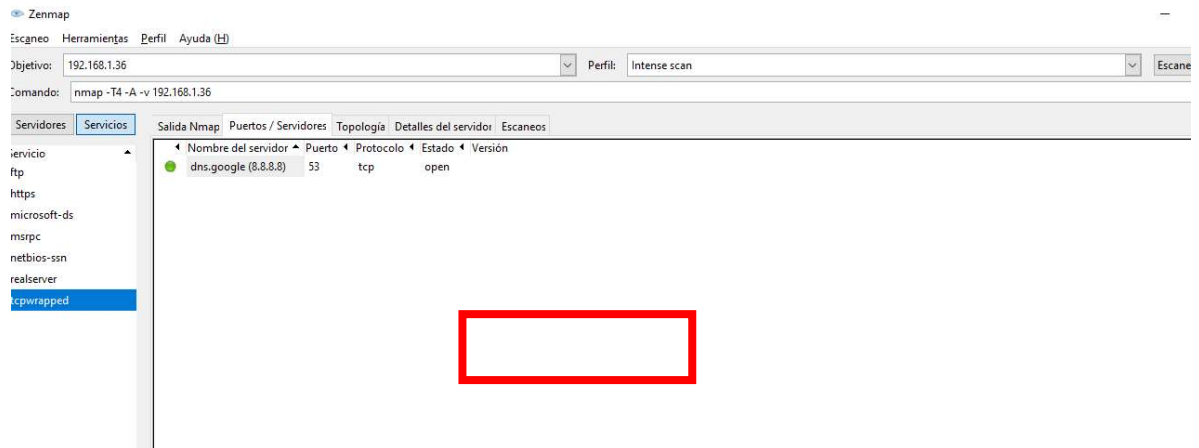
Análisis con NMAP Tools

Comencemos por entender que Nmap es una herramienta de código abierto para exploración de red y auditoría de seguridad. Se diseñó para analizar rápidamente grandes redes, aunque funciona muy bien contra equipos individuales. Nmap utiliza paquetes IP "crudos" («raw», N. del T.) en formas originales para determinar qué equipos se encuentran disponibles en una red, qué servicios (nombre y versión de la aplicación) ofrecen, qué sistemas operativos (y sus versiones) ejecutan, qué tipo de filtros de paquetes o cortafuegos se están utilizando, así como docenas de otras características. Aunque generalmente se utiliza Nmap en auditorías de seguridad, muchos administradores de redes y sistemas lo encuentran útil para realizar tareas rutinarias, como puede ser el inventariado de la red, la planificación de actualización de servicios y la monitorización del tiempo que los equipos o servicios se mantiene.

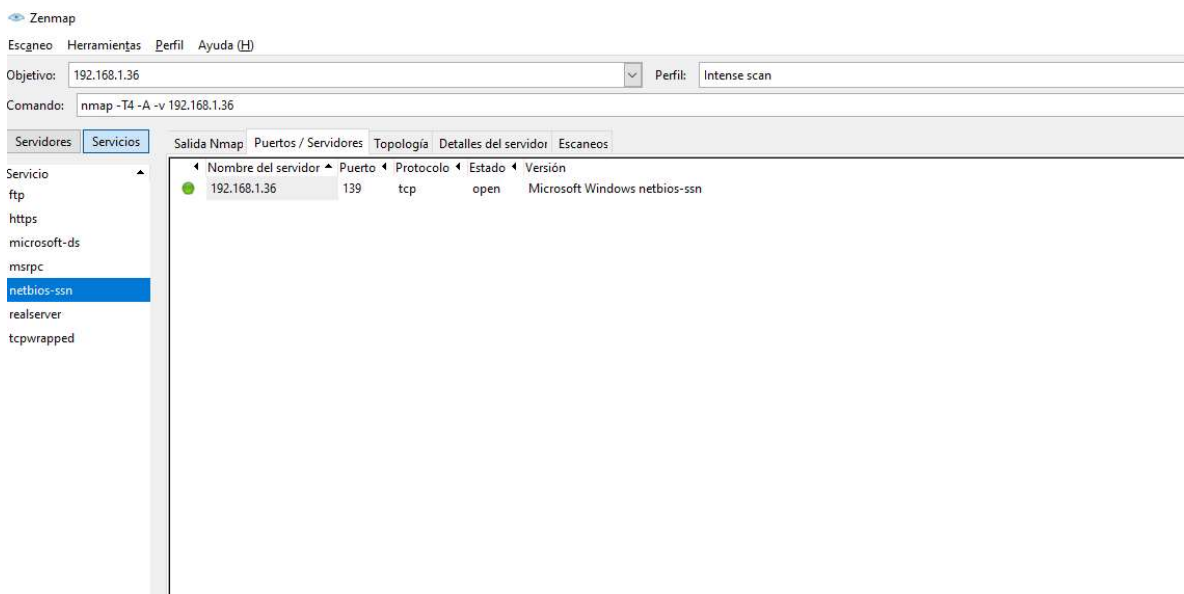
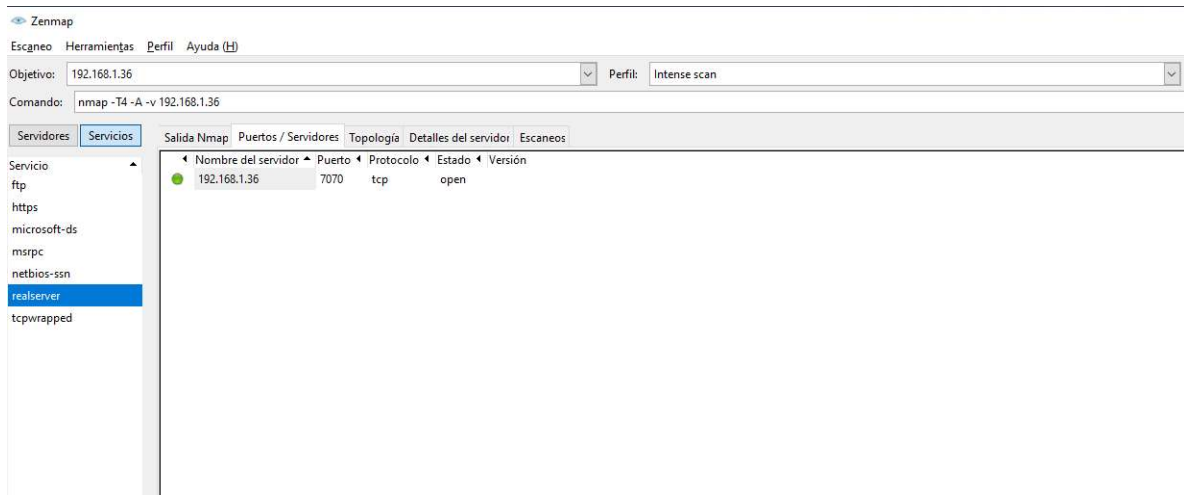
```
nmap -Pn -script vuln loterideltolima.com
```

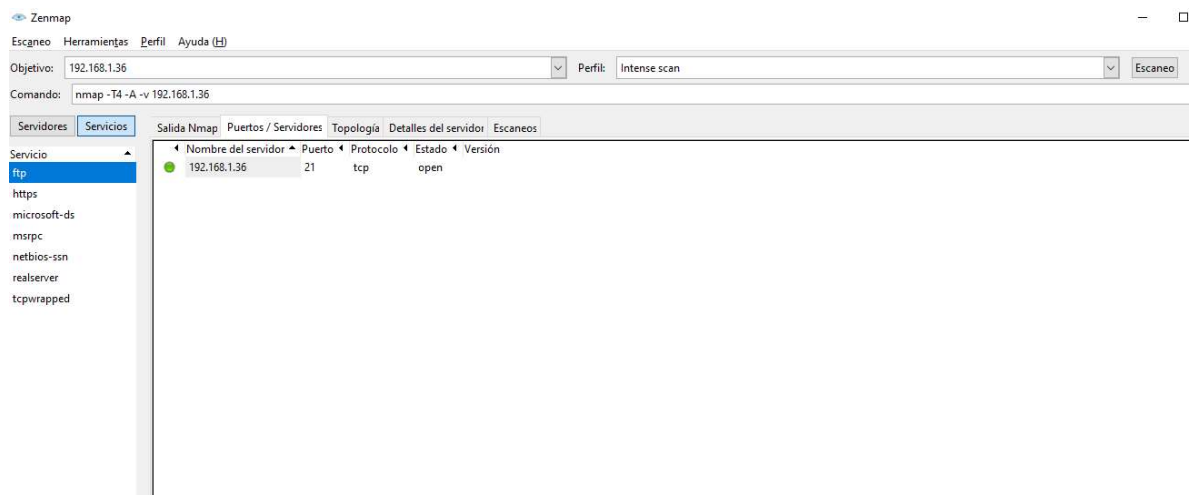
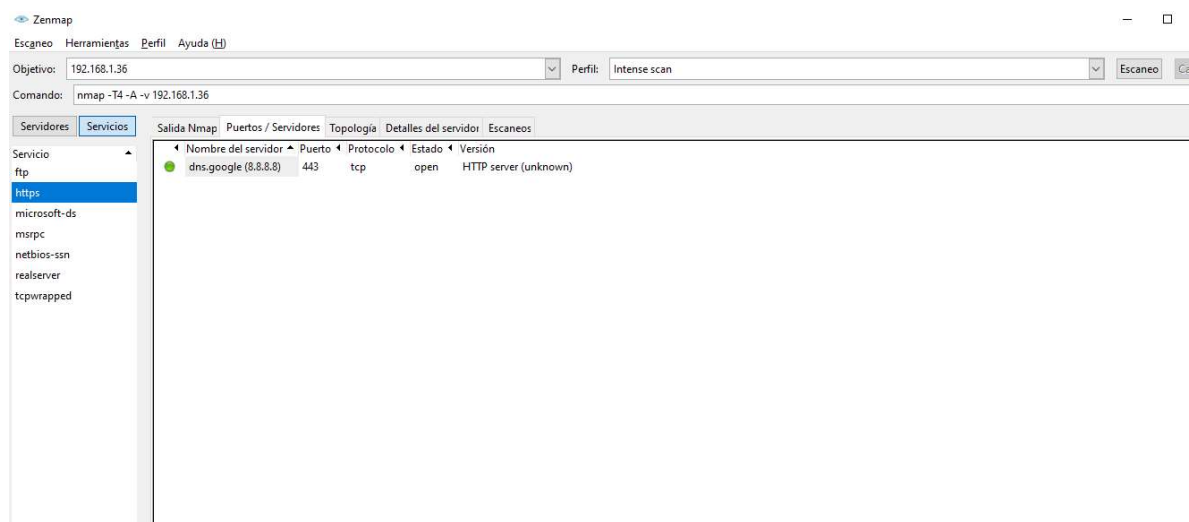
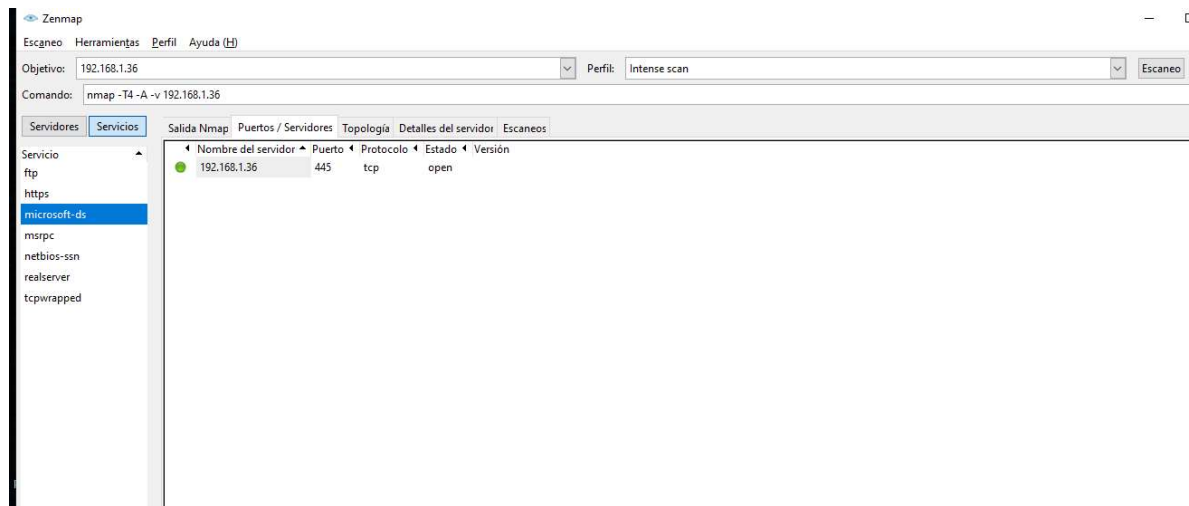


(Imagen No.1: Archivo ejemplo)



(Imagen No.2: Instalador VPN)





Starting Nmap 7.70 (<https://nmap.org>) at 2022-07-16 10:11 Hora est. Pacífico, Sudamérica
NSE: Loaded 148 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 10:11
Completed NSE at 10:11, 0.00s elapsed
Initiating NSE at 10:11
Completed NSE at 10:11, 0.00s elapsed
Initiating ARP Ping Scan at 10:11
Scanning 192.168.1.36 [1 port]
Completed ARP Ping Scan at 10:11, 0.53s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:11
Completed Parallel DNS resolution of 1 host. at 10:11, 0.00s elapsed
Initiating SYN Stealth Scan at 10:11
Scanning 192.168.1.36 [1000 ports]
Discovered open port 21/tcp on 192.168.1.36
Discovered open port 445/tcp on 192.168.1.36
Discovered open port 135/tcp on 192.168.1.36
Discovered open port 139/tcp on 192.168.1.36
Discovered open port 7070/tcp on 192.168.1.36
Completed SYN Stealth Scan at 10:11, 5.66s elapsed (1000 total ports)
Initiating Service scan at 10:11
Scanning 5 services on 192.168.1.36
Completed Service scan at 10:12, 34.06s elapsed (5 services on 1 host)
Initiating OS detection (try #1) against 192.168.1.36
Retrying OS detection (try #2) against 192.168.1.36
NSE: Script scanning 192.168.1.36.
Initiating NSE at 10:12
Completed NSE at 10:12, 40.31s elapsed
Initiating NSE at 10:12
Completed NSE at 10:12, 0.04s elapsed
Nmap scan report for 192.168.1.36
Host is up (0.0031s latency).
Not shown: 995 filtered ports
PORT STATE SERVICE VERSION
21/tcp open ftp?
| fingerprint-strings:
| NULL:
| 220-FileZilla Server 1.7.2
| 220-Please visit <https://filezilla-project.org/>
| 220-8888888888 888888888888 88888888b.
| 220-888 888 888 Y88b
| 220-888 888 888 888
| 220-8888888 888 888 d88P
| 220-888 888 8888888P"
| 220-888 888 888
|_ 220-888
| ftp-syst:
|_ SYST: UNIX emulated by FileZilla.

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

445/tcp open microsoft-ds?

7070/tcp open ssl/realservice?

|_ssl-date: TLS randomness does not represent time

1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at <https://nmap.org/cgi-bin/submit.cgi?new-service> :

SF-Port21-TCP:V=7.70%I=7%D=7/16%Time=64B408A6%P=i686-pc-windows-windows%r(

SF:NULL,A64,"220-FileZilla\x20Server\x201\7\2\r\n220-Please\x20visit\x20

SF:<https://filezilla-project.org/>\r\n220-888888888888\x2088888888888888\x20888

SF:8888b\.\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20

SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2

[illegible]

SF:20\20\20\20\20\20\20\20\20\20\20\20\20\20\20\20\20\

SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20

SE:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\r\n220-888\x20\x20\x20\x20

SE:\x20\x20\x20\x20\x20\x20\x20\x20888\x20\x20\x20\x20\x20888\x20\x20\x20

SE:88b\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20

SE:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20

SE:0\y20\y20\y20\y20\y20\y20\y20\y20\y20\y20\y20\y20\y20\y20\y20\y20\y20\y

[illegible][illegible][illegible]

51: \x20\x20\x20\x20\x20\x20\x20\x20\x20 | | | \x20-\x20\x20\x20\x20\x20\x20\x20\x20\x20

31.\ \lambda ZU\ \lambda ZU\ \lambda ZU\ \lambda ZU\ \lambda ZU\ \lambda ZU888\ \lambda ZU\ \lambda ZU\ \lambda ZU\ \lambda ZU\ \lambda ZU888\ \lambda ZU\ \lambda ZU\ \lambda ZU\ \lambda ZU888\

05.00' 00' 00' 00' 00' 00' 00' 00' 00' 00' 00' 00' 00' 00' 00' 00' 00' 00'

SF:ZU\XZU\XZU\XZU\XZU\XZU\XZU\XZU\XZU\XZU\XZU\XZU\XZU\XZU\XZU\XZU\XZU\

SF:xz0\xz0\xz0\xz0\xz0\xz0\xz0\xz0\xz0\xz0\xz0\xz0\xz0\xz0\xz0\xz0\xz0

SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20

SF:0\X20\X20\X20\X20\X20\X20\X20\X20\X20\X20\X20\X20\X20\X20\X20\X

SF:20\20\20\20\20\20\20\20\20\20\20\20\20\20\20\20\

SF:x20\x20\x20\x20\x20\x20\x20\x20\r\n220-8888888\x20\x20\x20\x20\x20\x20\x20

SF:x20\x20888\x20\x20\x20\x20\x20888\x20\x20\x20d88P\x20\x20\x20\x20\x20\x20

SF:20\20\20\20\20\20\20\20\20\20\20\20\20\20\20\20\

SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20

SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x

[illegible]

SF:20\20\20\20\20\20\20\20\20\20\20\20\20\20\20\20\

SF:x20\x20\x20\r\n220-888\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20

SF:88\ \x20\x20\x20\x20\x208888888P\" \"\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20

[illegible]

SF:20\20\20\20\20\20\20\20\20\20\20\20\20\20\20\20\

SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20

SE:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2

SE:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\r

SE:\p220-888\y20\y20\y20\y20\y20\y20\y20\y20\y20\y20\y20\y20\y20888\y20\y20\y20

SE:\0\y20\y20888\y20\y20\y20\y20\y20\y20\y20\y20\y20\y20\y20\y20\y2

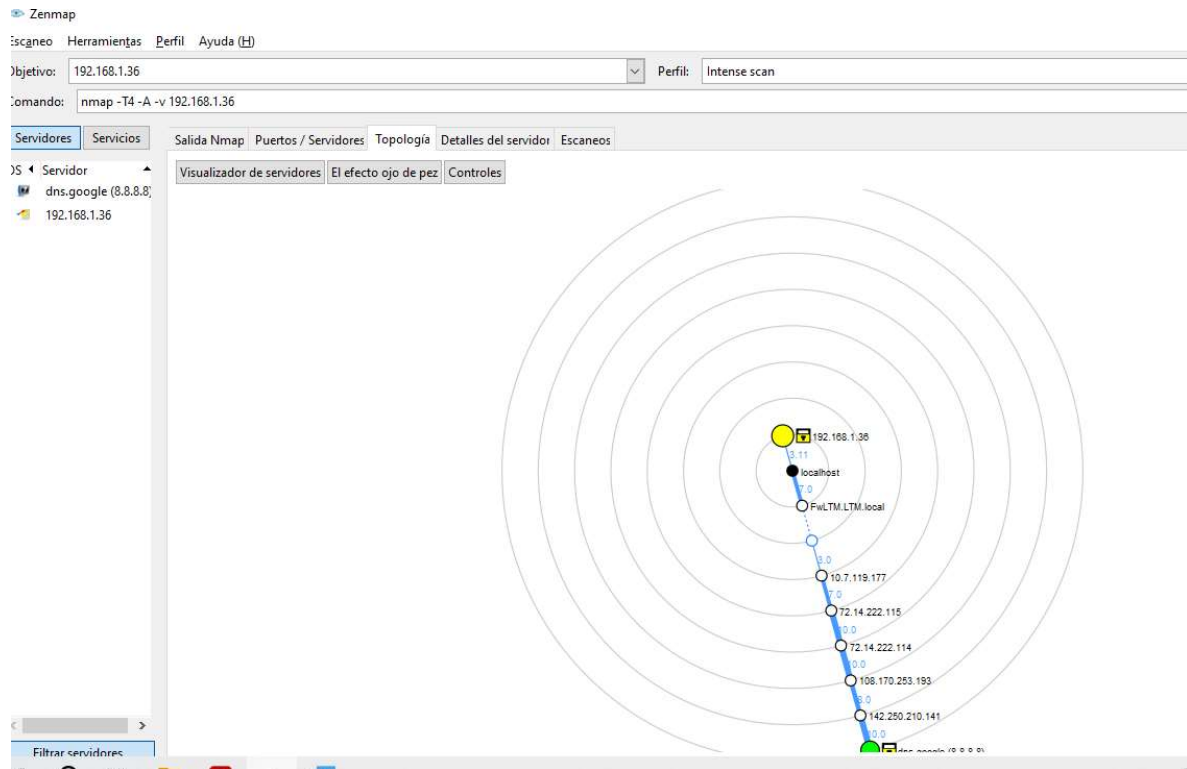
SE:0\×20\×20\×20\×20\×20\×20\×20\×20\×20\×20\×20\×20\×20\×20\×20\

[illegible]

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>

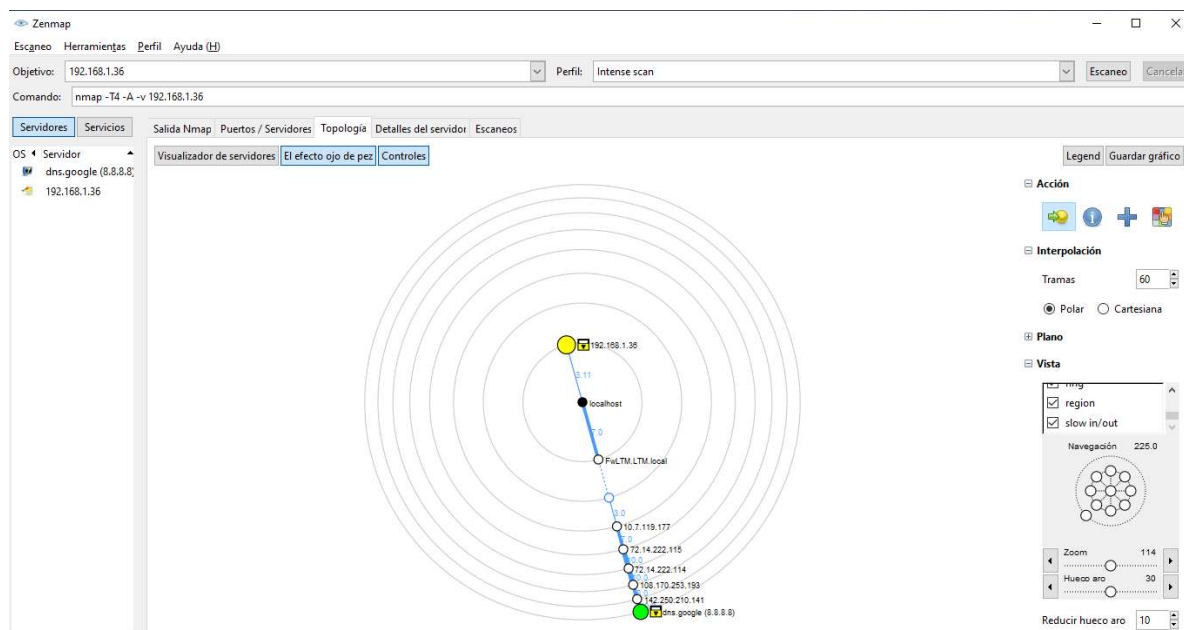
Nmap done: 1 IP address (1 host up) scanned in 92.49 seconds

Raw packets sent: 273 (94.904KB) | Rcvd: 30 (1.872KB)



(Imagen No.3: Visualizador de traza de capas tracert-d)

Una vez completado el proceso de instalación dar clic en **"close"**.



zenmap.exe

Información sobre el comando

Comando: nmap -T4 -A -v 192.168.1.36

Versión de Nmap: 7.70

Nivel de verbosidad: 1

Nivel de depuración: 0

Información general

Empezado el: julio 16, 2023 - 10:11

Terminado el: julio 16, 2023 - 10:12

Servidores activos: 1

Servidores inactivos: 0

Servidores escaneados: 1

Puertos abiertos: 5

Puertos filtrados: 995

Puertos cerrados: 0

Información del escaneo - Syn

IPSCAN TOOL

Uno de los primeros pasos en cualquier misión de reconocimiento de red es el de reducir un (muchas veces enorme) conjunto de rangos de direcciones IP en una lista de equipos activos o interesantes. Analizar cada puerto de cada una de las direcciones IP es lento, y usualmente innecesario. Por supuesto, lo que hace a un sistema interesante depende ampliamente del propósito del análisis. Los administradores de red pueden interesarse sólo en equipos que estén ejecutando un cierto servicio, mientras que los auditores de seguridad pueden interesarse en todos y cada uno de los dispositivos que tengan una dirección IP. Un administrador puede sentirse cómodo con obtener un listado de equipos en su red interna mediante un ping ICMP, mientras que un consultor en seguridad realizando un ataque externo puede llegar a utilizar un conjunto de docenas de sondas en su intento de saltarse las restricciones de los cortafuegos.

Siendo tan diversas las necesidades de descubrimiento de sistemas, IPSCAN ofrece una gran variedad de opciones para personalizar las técnicas utilizadas. Al descubrimiento de sistemas («Host Discovery») se lo suele llamar sondeo ping, pero va más allá de la simple solicitud ICMP echo-request de los paquetes asociados al querido y nunca bien ponderado ping. Los usuarios pueden evitar el paso de ping utilizando un sondeo de lista (-sL) o deshabilitando el ping (-P0), o enviando combinaciones arbitrarias de sondas TCP SYN/ACK, UDP e ICMP a múltiples puertos de la red remota. El propósito de estas sondas es el de solicitar respuestas que demuestren que una dirección IP se encuentra activa (está siendo utilizada por un equipo o dispositivo de red). En varias redes solo un pequeño porcentaje de direcciones IP se encuentran activos en cierto momento. Esto es particularmente común en las redes basadas en direccionamiento privado RFC1918, como la 10.0.0.0/8. Dicha red tiene más de 16 millones de direcciones IP, pero la he visto siendo utilizada por empresas con menos de mil máquinas. El descubrimiento de sistemas puede encontrar dichas maquinas en un rango tan grande como el indicado.

Advanced IP Scanner

Archivo Vista Configuración Ayuda

Explorar

192.168.1.1-254 Ejemplo: 192.168.0.1-100, 192.168.0.200 Buscar

Estado	Nombre	IP	Fabricante	Dirección MAC	Comentarios
	192.168.1.214	192.168.1.214		EA:46:E8:86:4C:94	
	UOC-EDEV01	192.168.1.124	AIO LCD PC BU / TPV	00:25:AB:9D:4F:61	
	192.168.1.5	192.168.1.5	Aruba, e Hewlett Pack...	44:5B:ED:12:EB:37	
	DESKTOP-DNIS0T1	192.168.1.80	ASKEY COMPUTER C...	E8:39:DF:3A:47:64	
	SIS-PORSIS01	192.168.1.32	AzureWave Technolo...	74:C6:3B:EC:8C:B9	
	JUR-EAPO01	192.168.1.113	BIOSTAR Microtech In...	B8:97:5A:80:99:72	
	UOC-EOPED01	192.168.1.239	BIOSTAR Microtech In...	B8:97:5A:3C:CF:3F	
	SIS-ESIS01	192.168.1.75	COMPAL INFORMATI...	FC:45:96:79:64:C8	
	JUR-EJUR01	192.168.1.110	COMPAL INFORMATI...	FC:45:96:AE:1D:1A	
	UOC-EPRE01	192.168.1.125	COMPAL INFORMATI...	FC:45:96:AE:1E:A9	
	UOC-ESERESP01	192.168.1.123	COMPAL INFORMATI...	98:29:A6:89:E3:44	
	192.168.1.45	192.168.1.45	Dell Inc.	00:21:70:68:82:E9	
	192.168.1.10	192.168.1.10	Hangzhou Hikvision ...	08:A1:89:13:E1:85	
	192.168.1.91	192.168.1.91	Hangzhou Hikvision ...	44:47:CC:C8:BB:AD	
	FwTm.LTM.local	192.168.1.1	Hewlett Packard	E8:39:35:14:03:DB	
	LINUX-6ZQZ	192.168.1.3	Hewlett Packard	00:1C:C4:F0:38:46	
	LINUX-6ZQZ	192.168.1.25	Hewlett Packard	00:1C:C4:F0:38:46	
	NPI29FF71	192.168.1.37	Hewlett Packard	F4:30:B9:29:FF:71	
	IMP-JURDICA	192.168.1.65	Hewlett Packard	3C:D9:2B:9F:52:2E	
	192.168.1.72	192.168.1.72	Hewlett Packard	E8:39:35:14:03:DA	
	CON-INT02	192.168.1.104	Hewlett Packard	F8:B4:6A:BD:CB:54	
	FIN-CART01	192.168.1.108	Hewlett Packard	10:E7:C6:E3:20:FC	
	AGERENCIA-PC	192.168.1.101	Hewlett Packard	B0:DC:D1:5E:56:3E	
	CON-INT01	192.168.1.102	Hewlett Packard	9C:8E:99:F3:71:40	
	PCOSB	192.168.1.248	Hewlett Packard	EC:9A:74:5C:BA:FC	

UOC-ECOM02

Estado: Activo

Sistema operativo:

IP: 192.168.1.36

MAC: B8:E9:2F:FC:08:73

Fabricante: HP Inc.

NetBIOS:

Usuario:

Tipo:

Fecha:

Comentarios:

Servicio técnico	Más información
FTP	
Carpeta compartida	Scanner
Carpeta compartida	Users

Advanced IP Scanner

Archivo Vista Configuración Ayuda

Explorar

192.168.1.1-254, 192.168.124.1-254, 192.168.153.1-254, 192.168.56.1-254 Ejemplo: 192.168.0.1-100, 192.168.0.200 Buscar

Estado	Nombre	IP	Fabricante	Dirección MAC	Comentarios
		192.168.1.35		2A:D1:66:FA:D6:50	
		192.168.1.29		DA:06:4C:AD:FC:6A	
		192.168.1.214		EA:46:E8:86:4C:94	
	UOC-EDEV01	192.168.1.124	AIO LCD PC BU / TPV	00:25:A8:9D:4F:61	
	192.168.1.5	192.168.1.5	Aruba, a Hewlett Pack...	44:5B:ED:12:E8:37	
	DESKTOP-DNIS0T1	192.168.1.80	ASKEY COMPUTER C...	E8:39:DF:3A:47:64	
	SIS-PORSIS01	192.168.1.32	AzureWave Technolo...	74:C6:3B:EC:8C:B9	
	JUR-EAPO01	192.168.1.113	BIOSTAR Microtech In...	88:97:5A:80:99:72	
	UOC-EOP01	192.168.1.239	BIOSTAR Microtech In...	88:97:5A:3C:CF:3F	
	SIS-ESIS01	192.168.1.75	COMPAL INFORMATI...	FC:45:96:79:64:C8	
	ASIGNACION EQUIPOS DE COMPUTO				
	CONTRATACION				
	DOCUMENTOS SGC				
	original				
	Prueba				
	Scanner				
	Users				
	JUR-EJUR01	192.168.1.110	COMPAL INFORMATI...	FC:45:96:AE:1D:1A	
	UOC-EPRE01	192.168.1.125	COMPAL INFORMATI...	FC:45:96:AE:1E:A9	
	UOC-ESERESP01	192.168.1.123	COMPAL INFORMATI...	98:29:A6:89:E3:44	
	192.168.1.45	192.168.1.45	Dell Inc.	00:21:70:68:82:E9	
	Scanner				
	Users				
	192.168.1.10	192.168.1.10	Hangzhou Hikvision ...	08:A1:89:13:E1:85	

5 activo, 39 inactivo, 190 desconocido

UOC-ECOM02

Estado: Activo

Sistema operativo: 192.168.1.36

IP: 192.168.1.36

MAC: 8C:E9:2F:FC:08:73

Fabricante: HP Inc.

NetBIOS:

Usuario:

Tipo:

Fecha:

Comentarios:

Servicio técnico	Más información
FTP	
Carpeta compartida	Scanner
Carpeta compartida	Users

Kali-Linux Ray Fusion Wifi

Kali Linux - 2021.4a-vmwa...

File Actions Edit View Help

'voiphopper -h' for more help

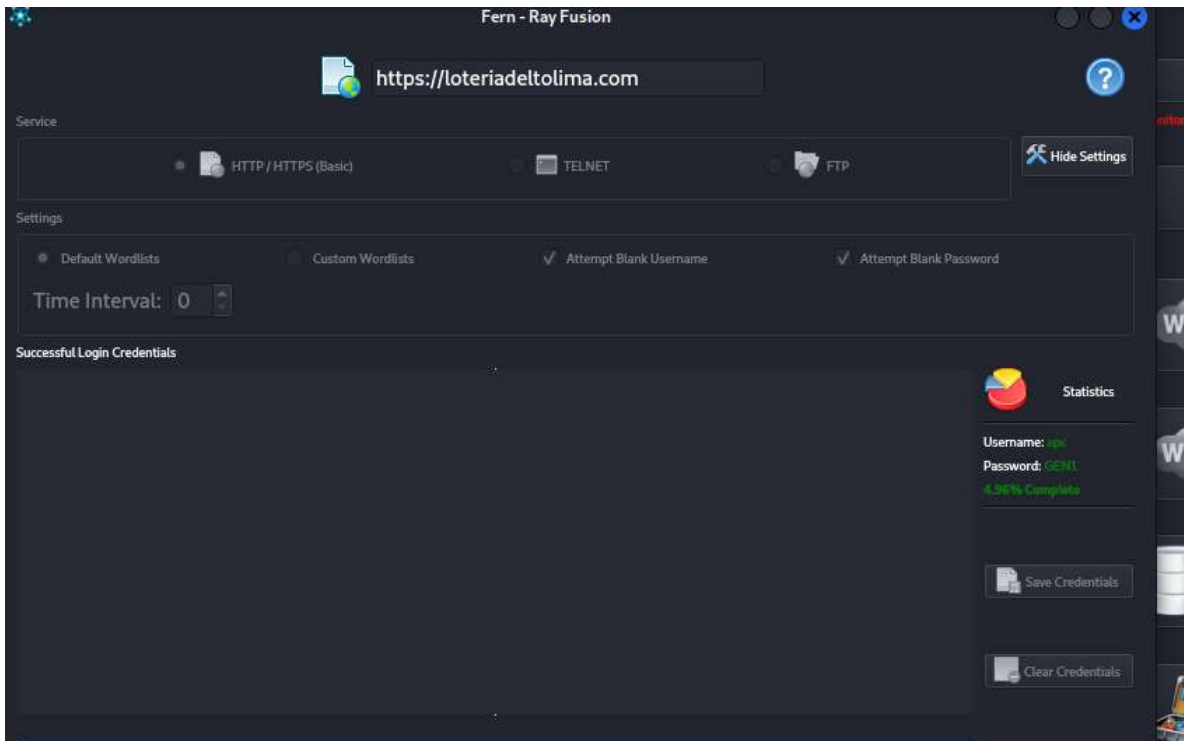
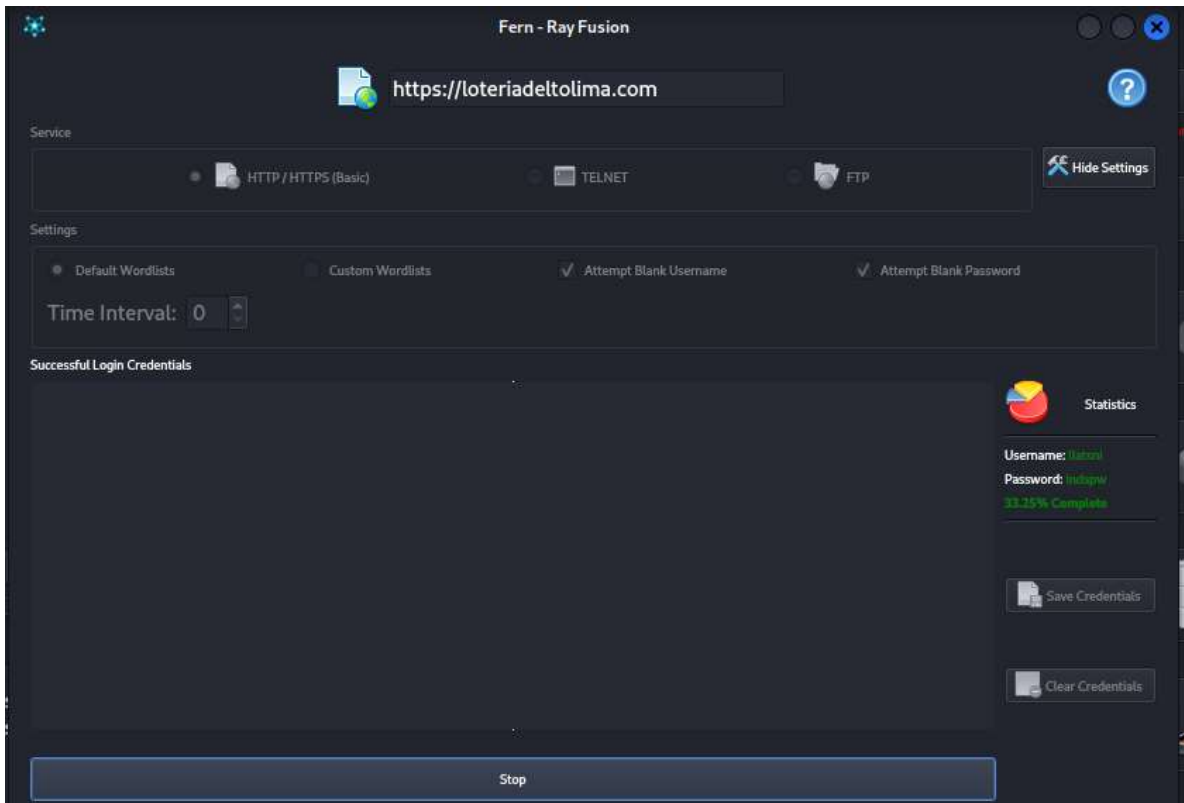
```
(kali@kali)-[~]
$ voiphopper -i eth0 -a
Beginning VLAN Hop in Avaya IP Phone Environment
VoIP Hopper 2.04 Sending DHCP request on eth0

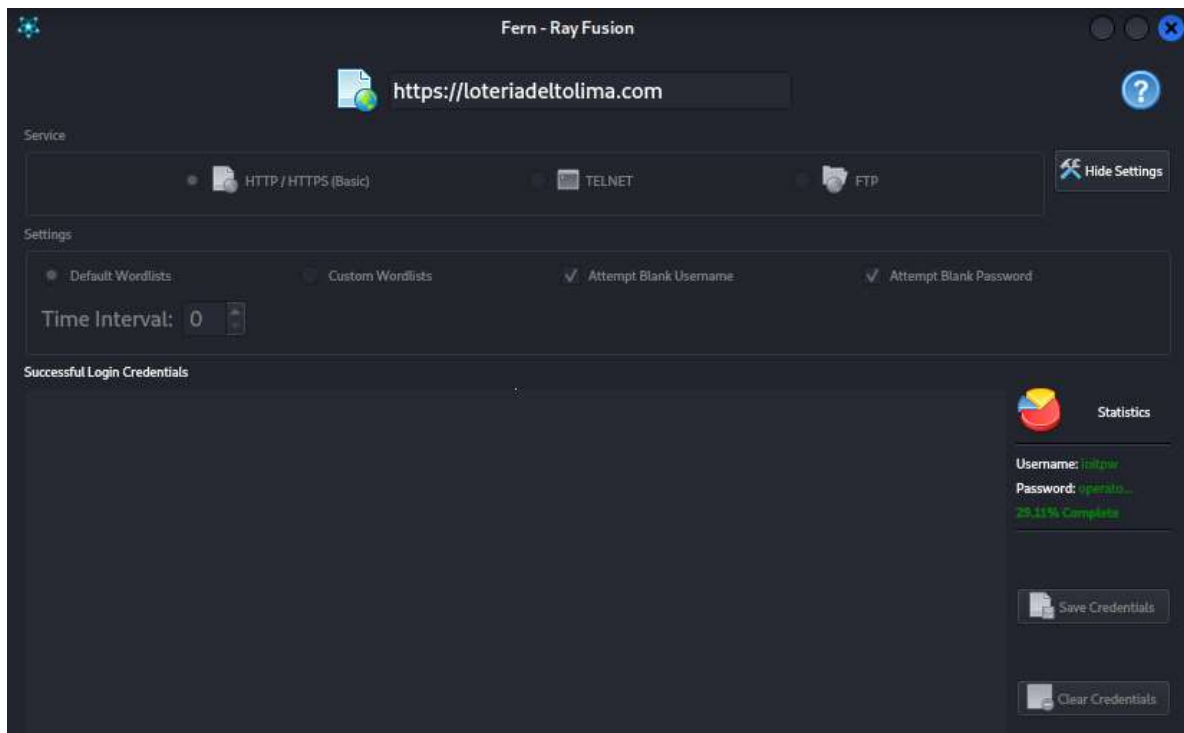
(kali@kali)-[~]
$ voiphopper -i eth0 -v 200
VoIP Hopper 2.04 Running in VLAN Hop mode ~ Trying to hop into VLAN 200
Error trying to add VLAN 200 to Interface eth0: Operation not permitted
Added VLAN 200 to Interface eth0

(kali@kali)-[~]
$ voiphopper -i eth0 -n
Beginning VLAN Hop in Nortel IP Phone Environment
VoIP Hopper 2.04 Sending DHCP request on eth0

(kali@kali)-[~]
$ voiphopper -i eth0 -t 0
VoIP Hopper 2.04 Running in Alcatel DHCP Option 43 Spoof mode
Beginning VLAN Hop in Alcatel IP Phone Environment
VoIP Hopper 2.04 Sending DHCP request on eth0

(kali@kali)-[~]
$
```





(Imagen No.4: Descubrimiento de usairios y password en la red Wifi de la Loteria)

