ANÁLISIS
VULNERABILIDAD

LOTERIA DEL TOLIMA

10 de diciembre de 2024

Contenido

Inicio

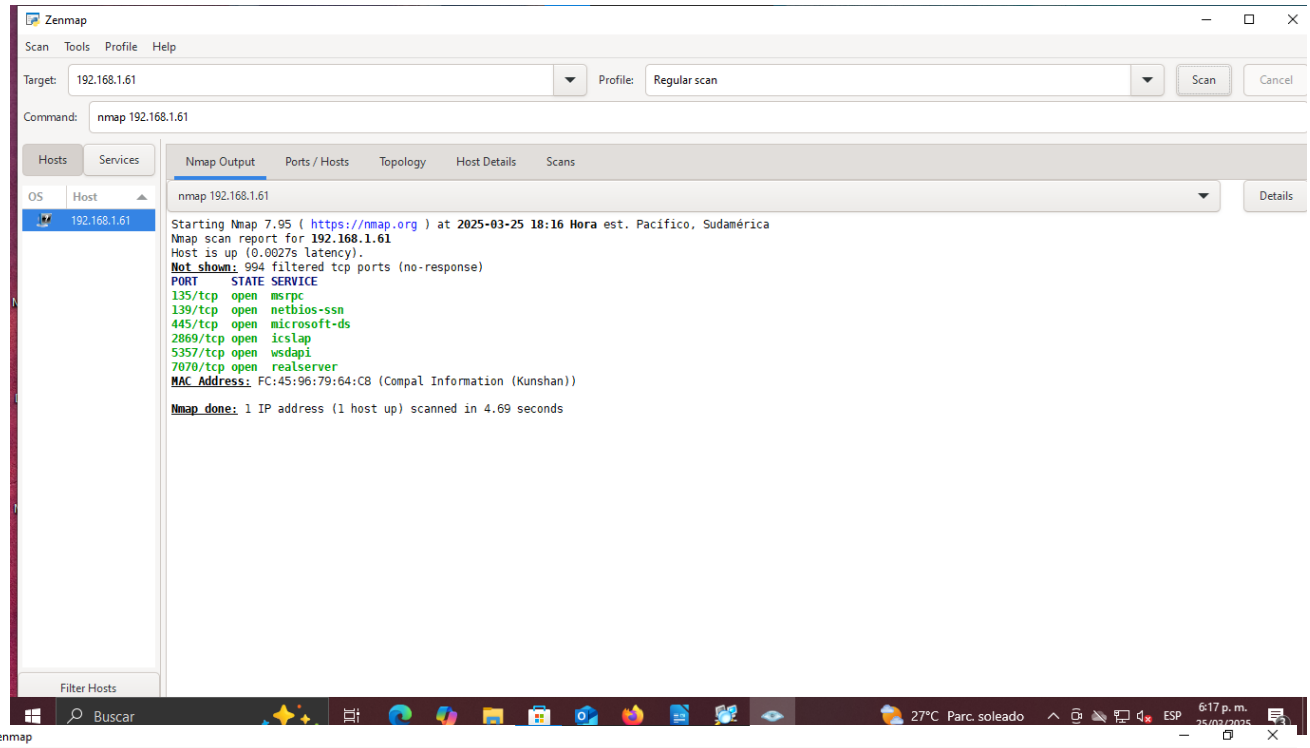
En el entorno actual, donde las amenazas cibernéticas evolucionan constantemente, es fundamental realizar un análisis de vulnerabilidad para identificar posibles debilidades en los dispositivos conectados a la red. Este proceso permite detectar fallos de seguridad, evaluar riesgos potenciales y proponer medidas correctivas que garanticen la integridad, confidencialidad y disponibilidad de la información.

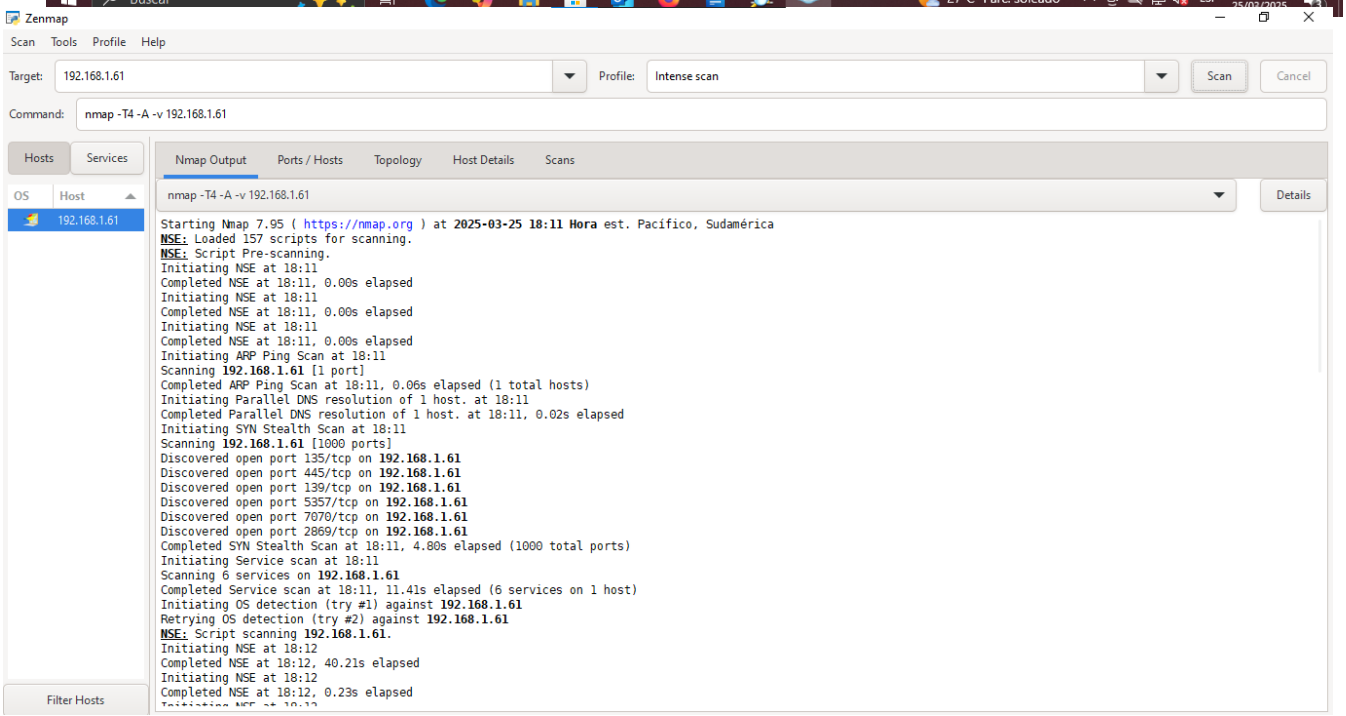
En este análisis se consideran aspectos como la configuración de los dispositivos, la gestión de accesos, la actualización de software, y la implementación de protocolos de seguridad. A través de pruebas de penetración y el uso de herramientas especializadas, se examinan las superficies de ataque para identificar cualquier posible brecha que pueda ser explotada por actores malintencionado

Análisis con NMAP Tools de la Nube

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
```





Starting Nmap 7.70 (https://nmap.org) at 2023-12-08 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 88888888888 8888888b.

| 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 msrpcMicrosoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn 445/tcp open microsoft-ds?

7070/tcp open ssl/realserver?

|_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\n220-8888888888\x2088888888888\x20888
SF:8888b\.\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\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x
SF:20\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\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\r\n220-888\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20888\x20\x20\x20\x20\x20888\x20\x20\x20Y
SF:88b\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\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x
SF:20\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\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\r\n220-888\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20888\x20\x20\x20\x20\x20888\x20\x20\x20\x20888\x
SF:20\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\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x
SF:20\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\r\n220-8888888\x20\x20\x20\x20\x20\x20\
SF:x20\x20888\x20\x20\x20\x20\x20888\x20\x20\x20d88P\x20\x20\x20\x20\x20\x
SF:20\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\x20\x20
SF:\x20\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\x20\x20\x
SF:20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
SF:x20\x20\x20\r\n220-888\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x208
SF:88\x20\x20\x20\x20\x208888888P\"\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x

SF:20\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\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\r

SF:\n220-888\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20888\x20\x20\x2
SF:0\x20\x20888\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
SF:20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2

SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x
SF:20\r\n220-888");

MAC Address: BC:E9:2F:FC:0B:73 (Unknown)

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

Device type: general purpose

Runing (JUST GUESSING): Microsoft Windows 2008|XP (86%)

OS CPE: cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2cpe:/o:microsoft:windows_xp::sp2

Aggressive OS guesses: Microsoft Windows Server 2008 SP1 or Windows Server 2008 R2 (86%), Microsoft Windows XP SP2 (85%)

No exact OS matches for host (test conditions non-ideal). Network Distance: 1 ho

TCP Sequence Prediction: Difficulty=255 (Good luck!) IP ID Sequence Generation: Incremental

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:

|_clock-skew: mean: 15s, deviation: 0s, median: 15s

| nbstat: NetBIOS name: UOC-ECOM02, NetBIOS user: <unknown>, NetBIOS MAC: bc:e9:2f:fc:0b:73 (unknown)

| Names:

| UOC-ECOM02<20> Flags: <unique><active> Flags: <unique><active>

Flags: <group><active>

| UOC-ECOM02<00>

|_ LTOLIMA<00>

| smb2-security-mode:

| 2.02:

|_ Message signing enabled but not required

| smb2-time:

| date: 2023-12-08 10:12:24

|_ start_date: N/A

TRACEROUTE

HOP RTT ADDRESS

1 3.11 ms 192.168.1.36

NSE: Script Post-scanning. Initiating NSE at 10:12

Completed NSE at 10:12, 0.00s elapsed Initiating NSE at 10:12

Completed NSE at 10:12, 0.00s elapsed

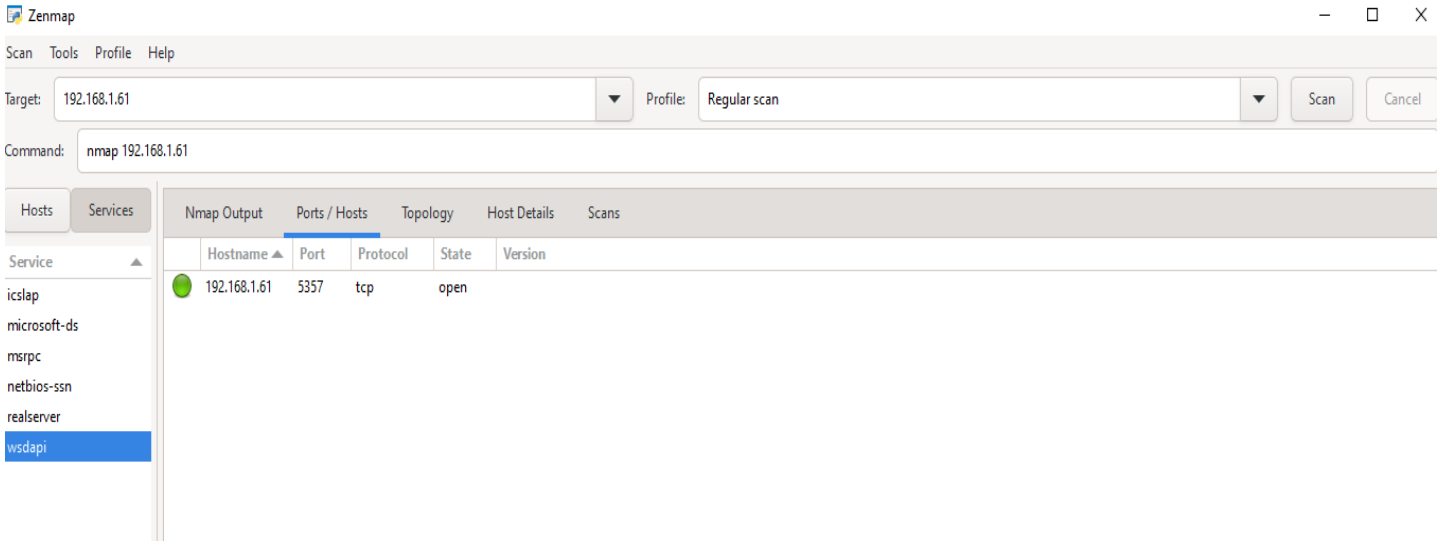
Read data files from: C:\Program Files (x86)\Nmap

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

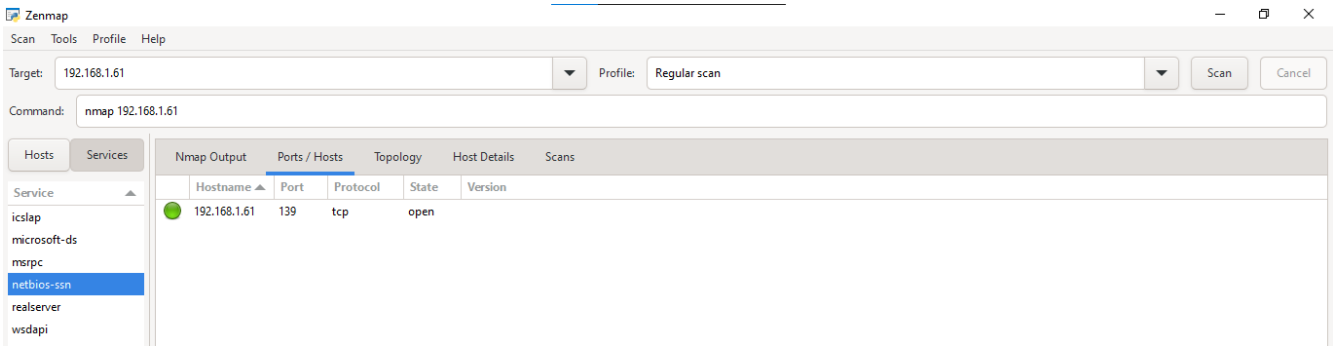
.

Nmap done: 1 IP address (1 host up) scanned in 92.49 seconds Raw packets sent: 273 (94.904KB) | Rcvd: 30 (1.872KB)

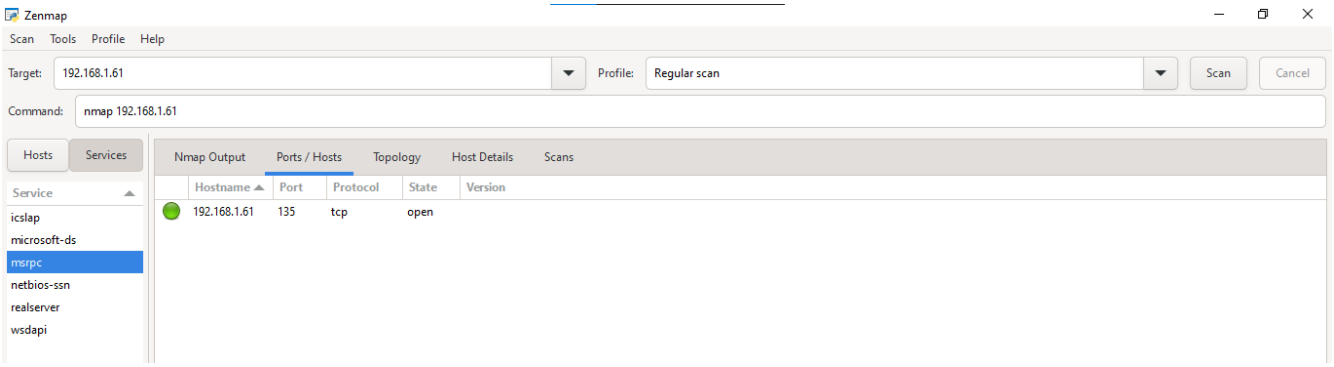
wsdapi:



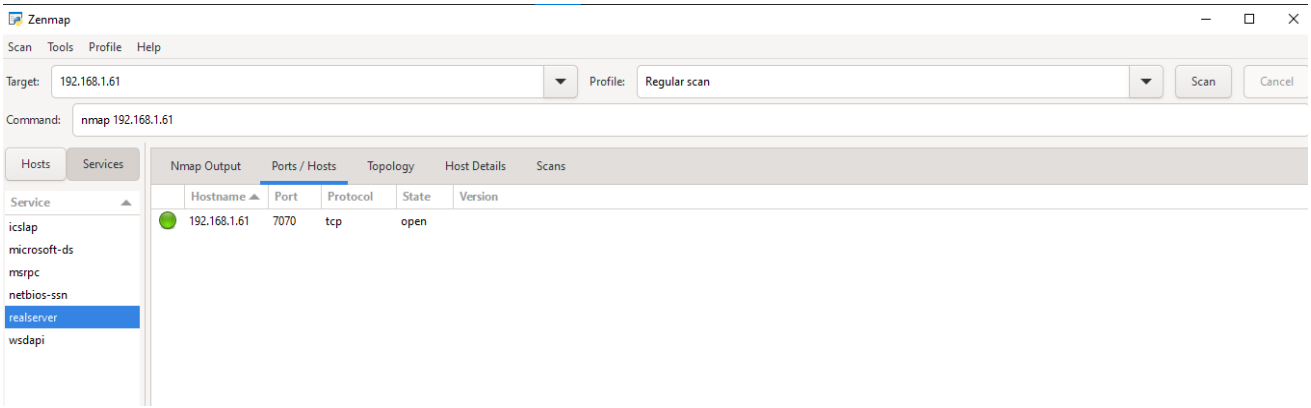
NETBIOS-SSN:



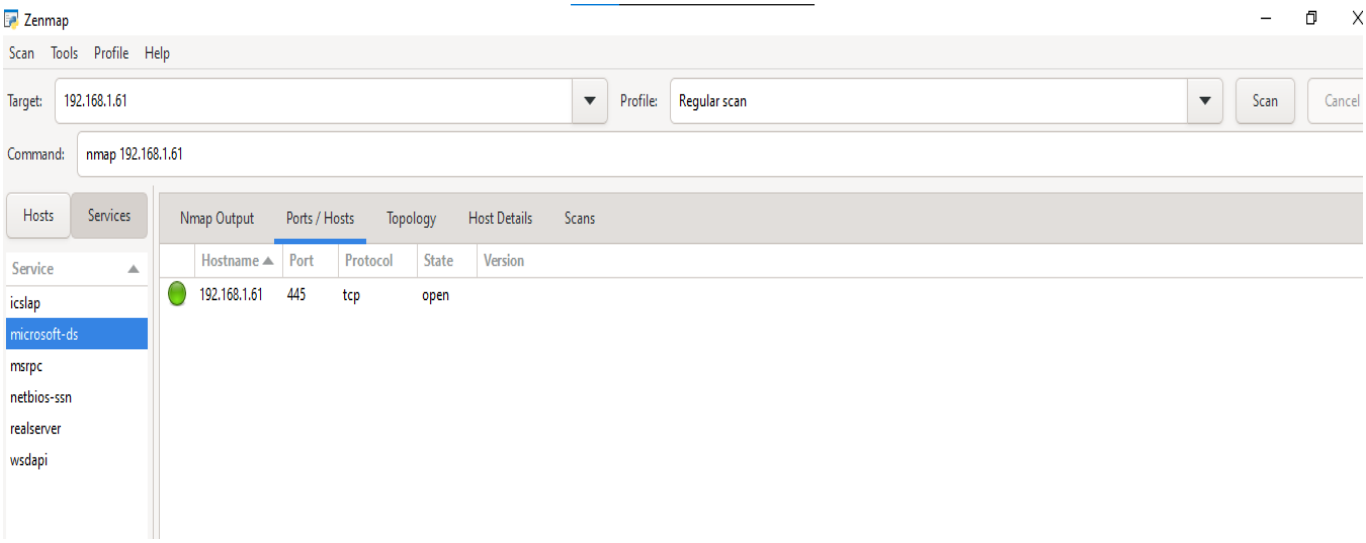
MSRPC:



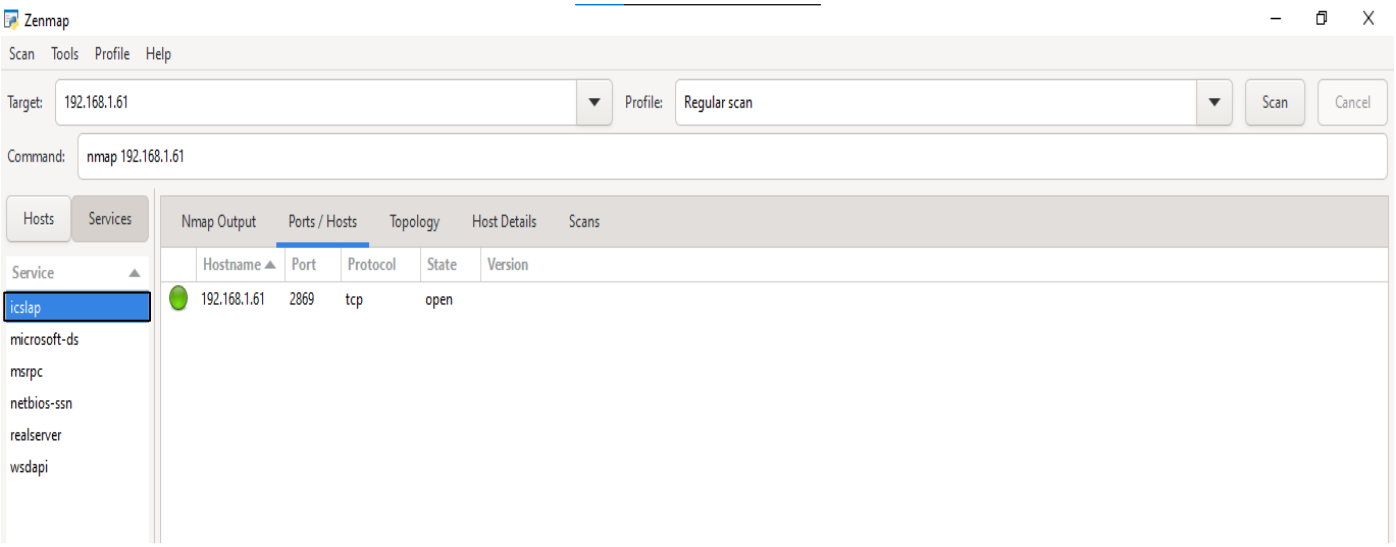
REALSERVE

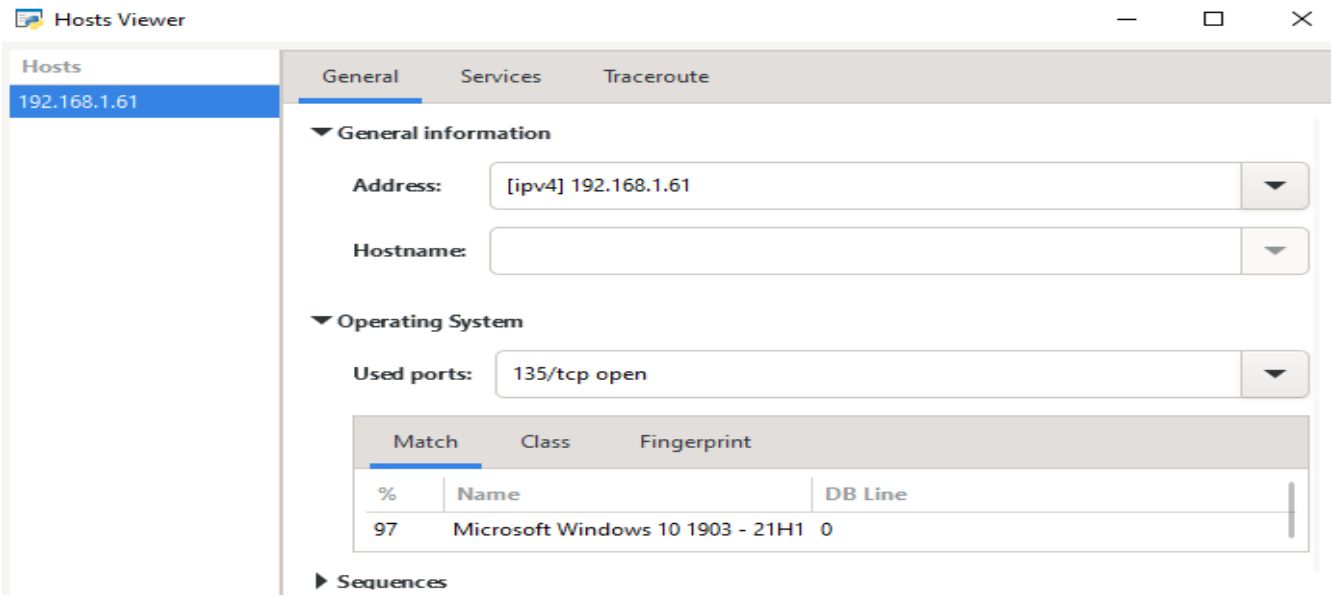


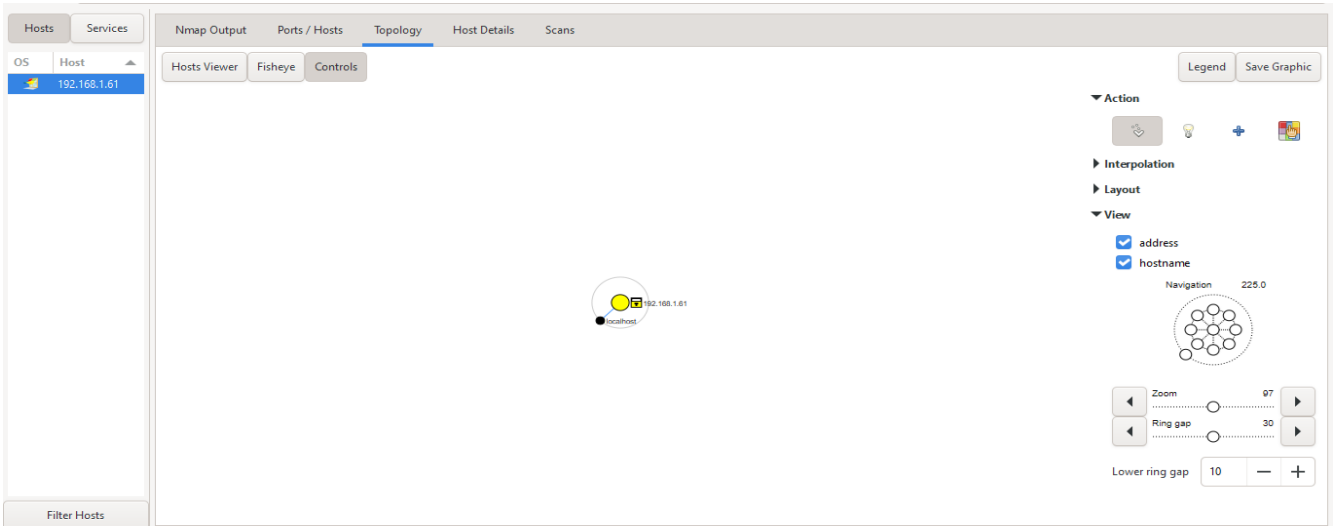
MICROSOFT-DS:



ICLAPSO:



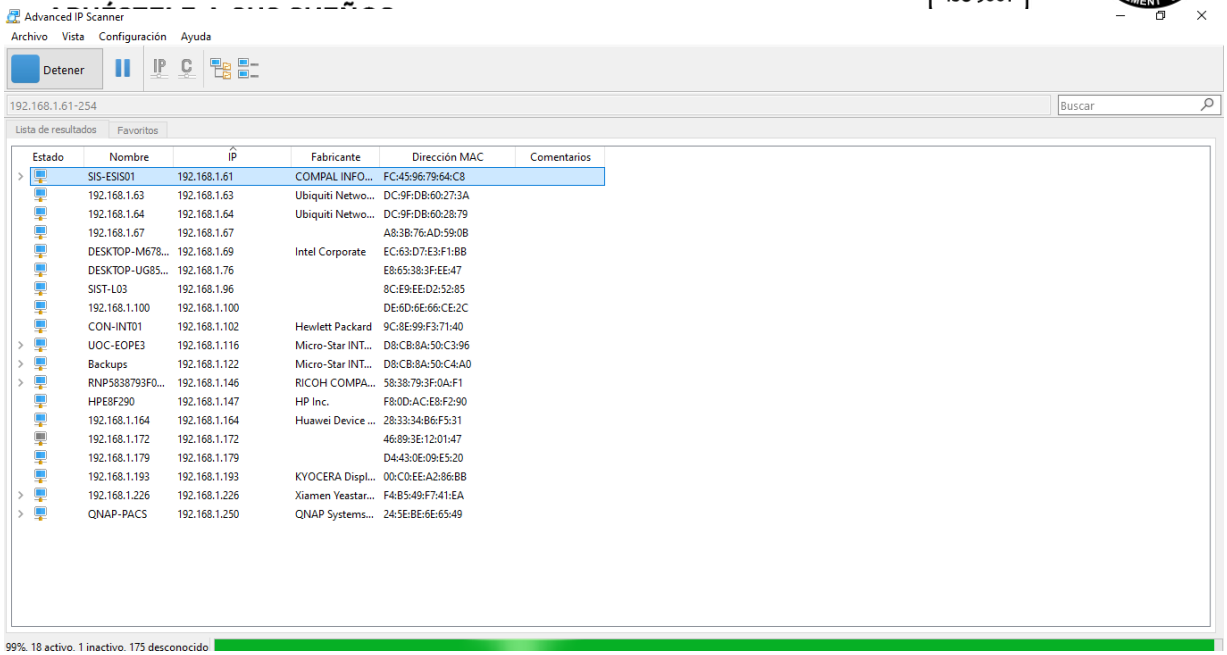

Hosts Viewer
Hosts
192.168.1.61
General
Services
Traceroute
General information
Address:
[ipv4] 192.168.1.61
Hostname:
Operating System
Used ports:
135/tcp open
Match
Class
Fingerprint
%
Name
DB Line
97
Microsoft Windows 10 1903 - 21H1
0
Sequences



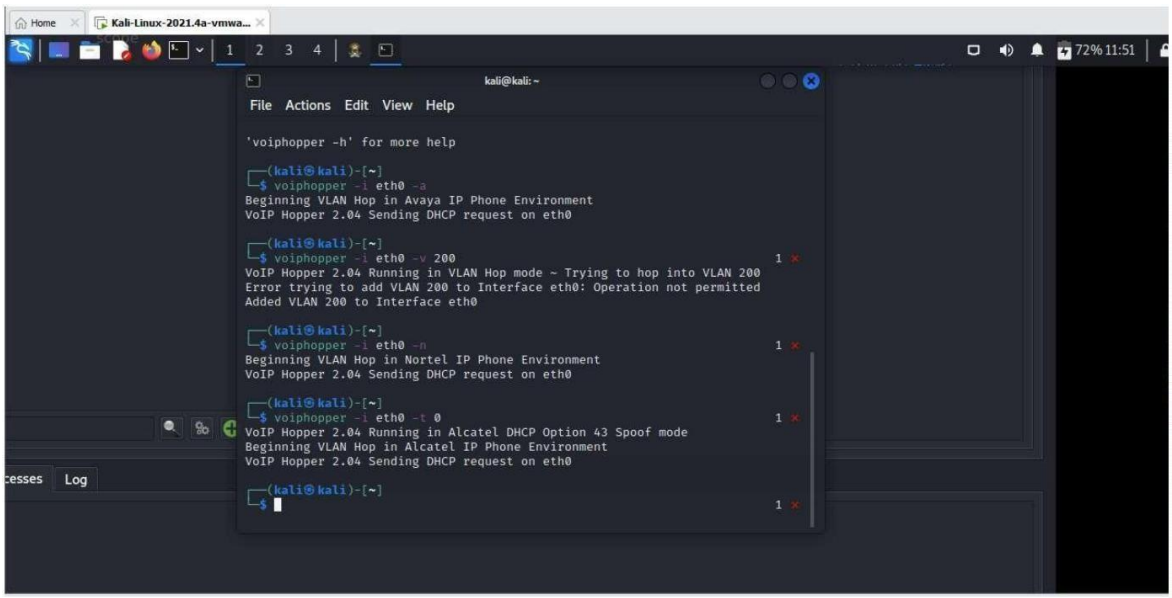
IPSCAN TOOl

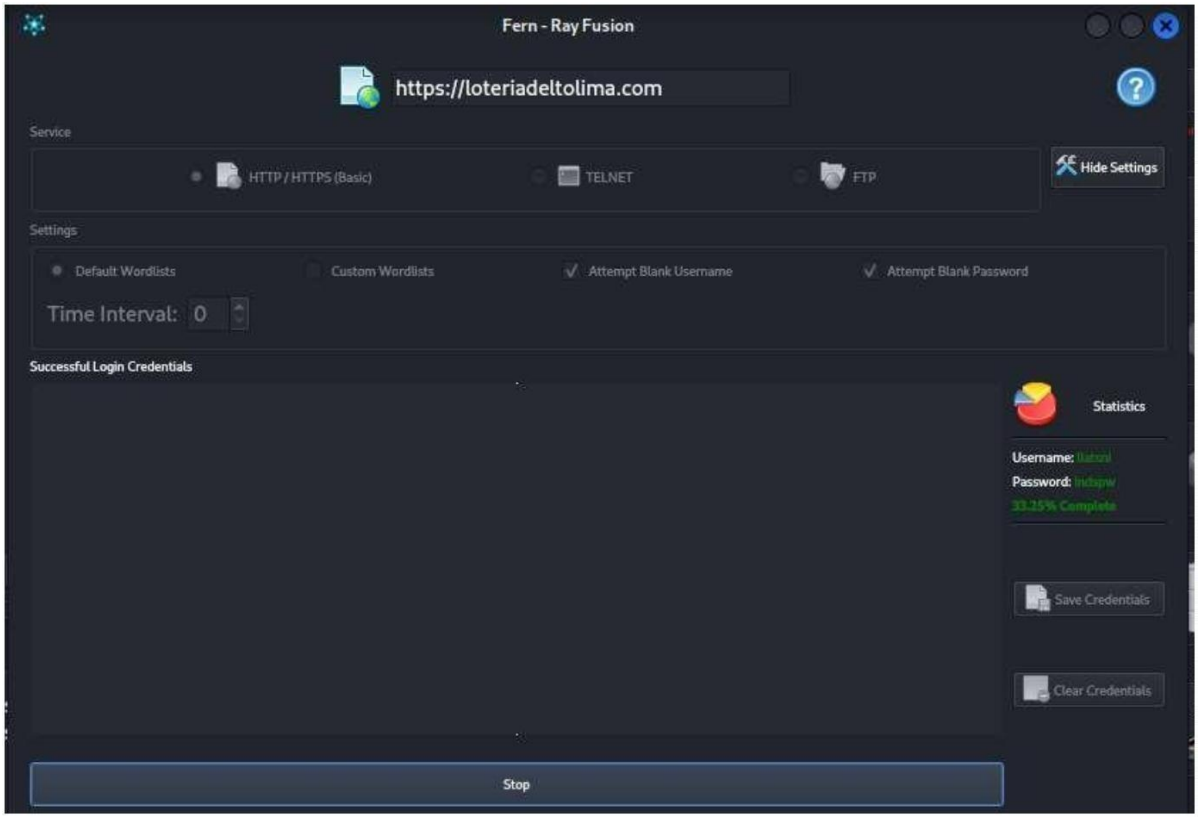
Uno de los primeros pasos en cualquier misión de reconocimiento de red es el de reducir un (muchas veces enorme) conjunto de rangos de direcciones IP en una lista de equipos activos o interesantes. Analizar cada puerto de cada una de las direcciones IP es lento, y usualmente innecesario. Por supuesto, 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.

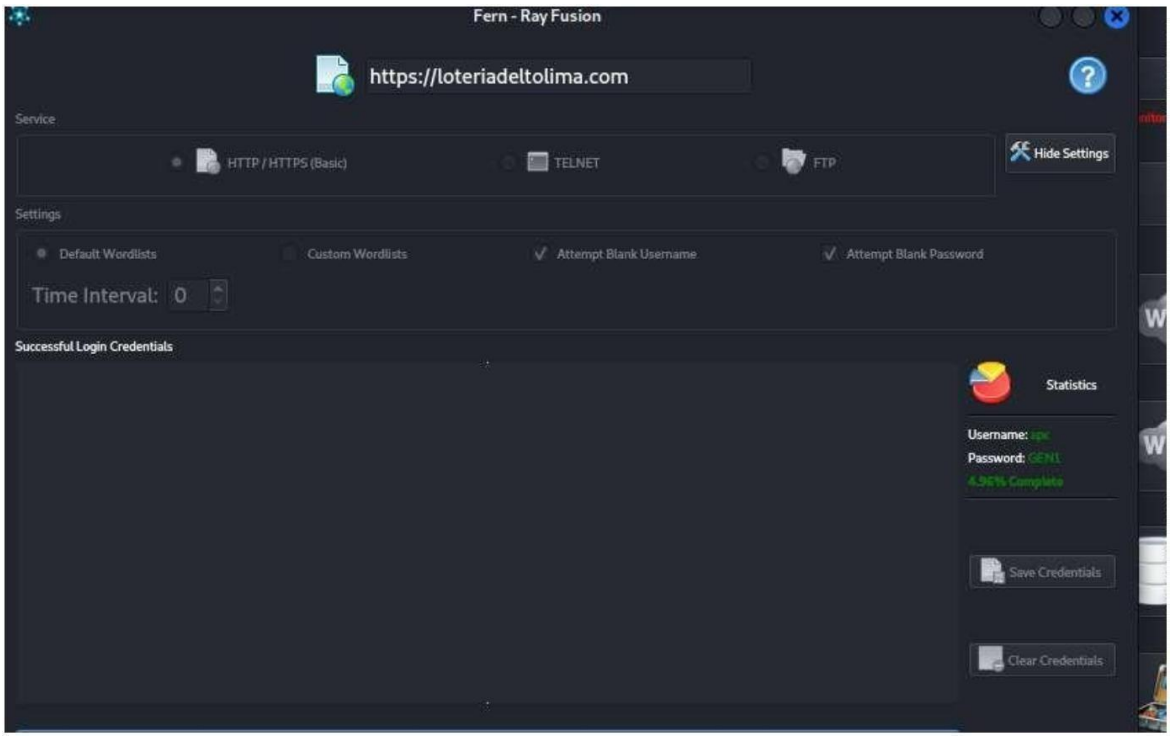
Siendo tan diversas las necesidades de descubrimiento de sistemas, IPSCAN ofrece una gran variedad de opciones para personalizar las técnicas utilizadas. Al descubrimiento de sistemas («Host Discovery») se lo suele llamar sondeo ping, pero va más allá de la simple solicitud ICMP echo-request de los paquetes 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.

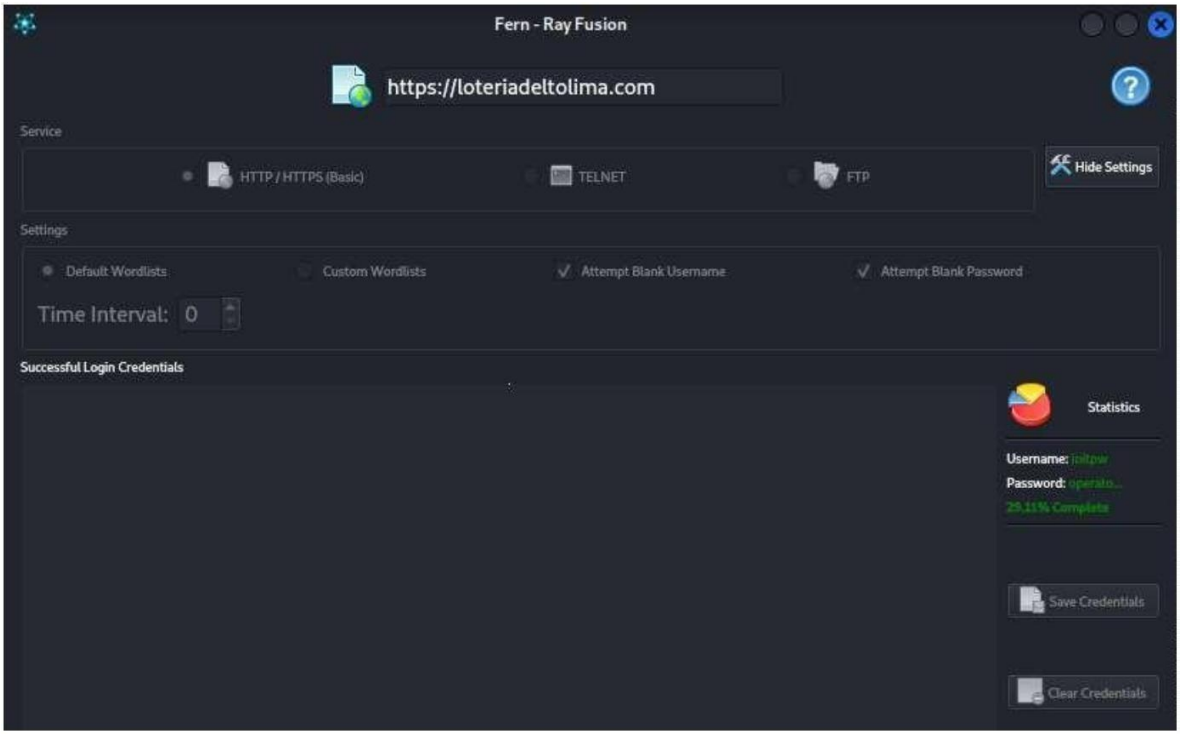


Kali-Linux Ray Fusion Wifi




Fern - Ray Fusion
https://loteriadeltolima.com
Service
HTTP / HTTPS (Basic)
TELNET
FTP
Hide Settings
Settings
Default Wordlists
Custom Wordlists
Attempt Blank Username
Attempt Blank Password
Time Interval: 0
Successful Login Credentials
Statistics
Username:
Password:
Save Credentials
Clear Credentials
Stop


Fern - Ray Fusion
https://loteriadeltolima.com
Service
HTTP / HTTPS (Basic)
TELNET
FTP
Hide Settings
Settings
Default Wordlists
Custom Wordlists
Attempt Blank Username
Attempt Blank Password
Time Interval: 0
Successful Login Credentials
Statistics
Username:
Password:
Save Credentials
Clear Credentials



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

Conclusión:

Tras realizar un exhaustivo análisis de vulnerabilidad en los dispositivos conectados a la red, se ha determinado que los mecanismos de seguridad implementados son adecuados para proteger la infraestructura. Las configuraciones están alineadas con las mejores prácticas del sector, las actualizaciones de software están al día, y se han establecido controles de acceso robustos que minimizan el riesgo de intrusión.

Además, las pruebas realizadas no han identificado vulnerabilidades críticas que puedan comprometer la seguridad de los sistemas. Esto permite concluir que los dispositivos en red están protegidos de manera efectiva frente a amenazas comunes, garantizando la estabilidad operativa y la seguridad de la información manejada.