LOTERÍA DEL TOLIMA

APUÉSTELE A SUS SUEÑOS

ANÁLISIS VULNERABILIDAD

LOTERIA DEL TOLIMA

2025

Carrera 2 No. 11 – 59 Piso 2 Ibagué - Tolima

Tel. (608) 2631883 – (608) 2611023

Línea de atención al Cliente 018000 942542

www.loteriadeltolima.com

@loteriatolima @loteriatolima @loteria_tolima

Contenido

Inicio

En la actualidad, el entorno tecnológico enfrenta amenazas cibernéticas cada vez más complejas y cambiantes, lo que hace necesario realizar evaluaciones de seguridad para identificar posibles vulnerabilidades en los dispositivos conectados a la red. Este tipo de análisis permite reconocer puntos débiles, estimar los riesgos asociados y establecer medidas preventivas y correctivas que garanticen la protección, confidencialidad y disponibilidad de la información.

Para lograrlo, se revisan diversos aspectos, entre ellos la correcta configuración de los sistemas, la gestión adecuada de permisos y accesos, la actualización constante de aplicaciones y sistemas operativos, así como la implementación de mecanismos y políticas de seguridad. A través de pruebas controladas y el uso de herramientas especializadas, se examinan los posibles vectores de ataque con el fin de detectar fallos que puedan ser explotados por personas con intenciones maliciosas.

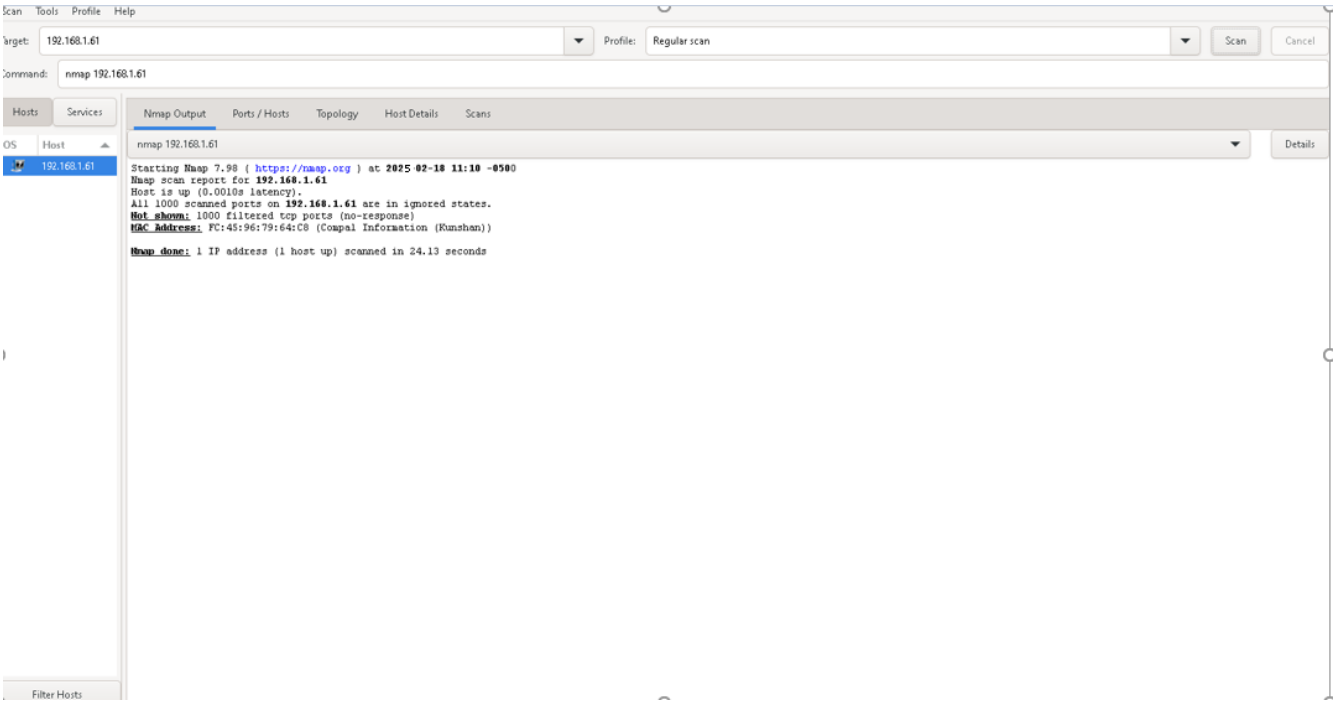
Análisis con Nmap en Infraestructuras en la Nube

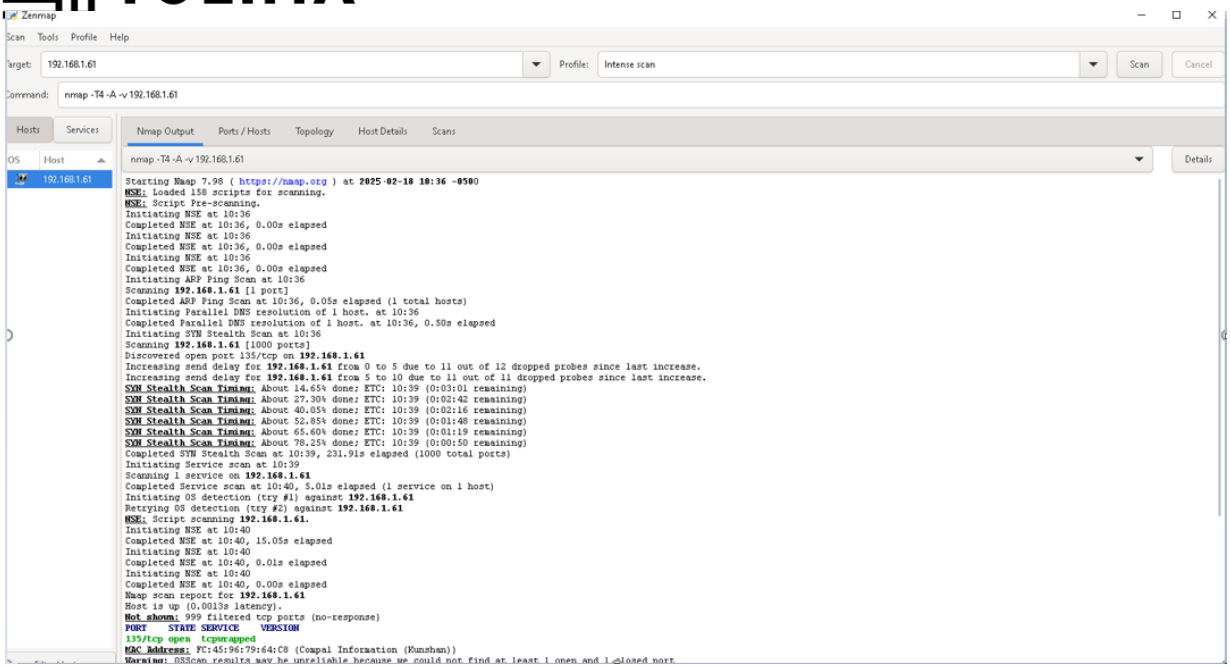
En primer lugar, es fundamental entender que Nmap es una herramienta de código abierto diseñada para la exploración de redes y la realización de auditorías de seguridad. Aunque fue creada para analizar grandes entornos de red de manera rápida y eficiente, también resulta altamente efectiva cuando se utiliza para evaluar dispositivos individuales.

Su metodología de trabajo consiste en el envío de paquetes IP en modo “raw”, lo que le permite recopilar información relevante sobre los equipos conectados a una red. A través de este proceso, puede determinar qué hosts se encuentran activos, qué servicios están expuestos (incluyendo sus versiones), qué sistema operativo ejecutan y qué mecanismos de filtrado o cortafuegos están implementados, entre otros detalles técnicos.

Además de su aplicación en pruebas de seguridad, Nmap es una herramienta de gran utilidad para administradores de sistemas, ya que contribuye al control y gestión de activos, la planificación de mejoras o actualizaciones de servicios, y el monitoreo continuo de la disponibilidad y estado de la infraestructura tecnológica.

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





SYN Stealth Scan Timing: About 27.30% done; ETC: 10:39 (0:02:42 remaining)

SYN Stealth Scan Timing: About 40.05% done; ETC: 10:39 (0:02:16 remaining)

SYN Stealth Scan Timing: About 52.85% done; ETC: 10:39 (0:01:48 remaining)

SYN Stealth Scan Timing: About 65.60% done; ETC: 10:39 (0:01:19 remaining)

SYN Stealth Scan Timing: About 78.25% done; ETC: 10:39 (0:00:50 remaining)

Completed SYN Stealth Scan at 10:39, 231.91s elapsed (1000 total ports)

Initiating Service scan at 10:39

Scanning 1 service on 192.168.1.61

Completed Service scan at 10:40, 5.01s elapsed (1 service on 1 host)

Initiating OS detection (try #1) against 192.168.1.61

Retrying OS detection (try #2) against 192.168.1.61

NSE: Script scanning 192.168.1.61.

Initiating NSE at 10:40

Completed NSE at 10:40, 15.05s elapsed

Initiating NSE at 10:40

Completed NSE at 10:40, 0.01s elapsed

Initiating NSE at 10:40

Completed NSE at 10:40, 0.00s elapsed

Nmap scan report for 192.168.1.61

Host is up (0.0013s latency).

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

PORT STATE SERVICE VERSION

135/tcp open tcpwrapped

MAC Address: FC:45:96:79:64:C8 (Compal Information (Kunshan))

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

OS fingerprint not ideal because: Missing a closed TCP port so results incomplete

No OS matches for host

Network Distance: 1 hop

TRACEROUTE

HOP RTT ADDRESS

1 1.25 ms 192.168.1.61

NSE: Script Post-scanning.

Initiating NSE at 10:40

Completed NSE at 10:40, 0.00s elapsed

Initiating NSE at 10:40

Completed NSE at 10:40, 0.00s elapsed

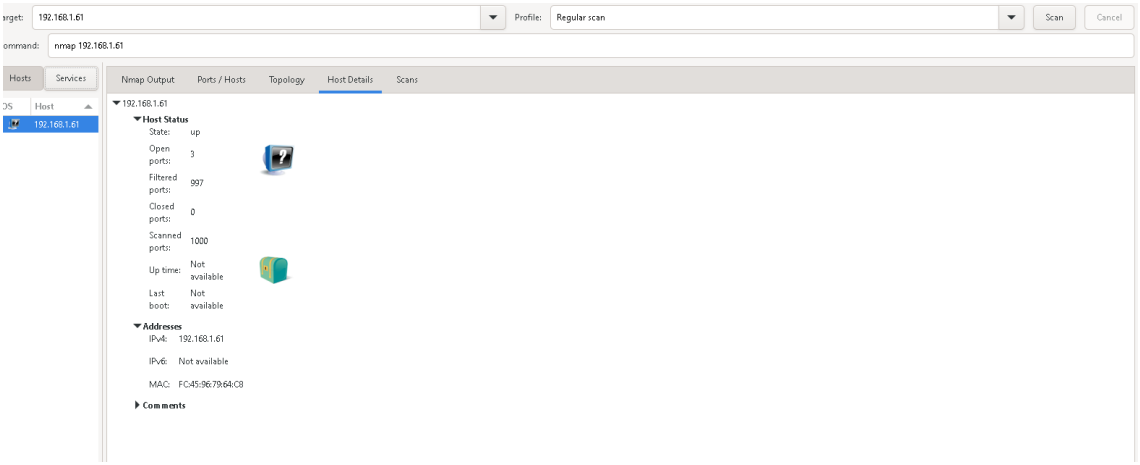
Initiating NSE at 10:40

Completed NSE at 10:40, 0.00s elapsed

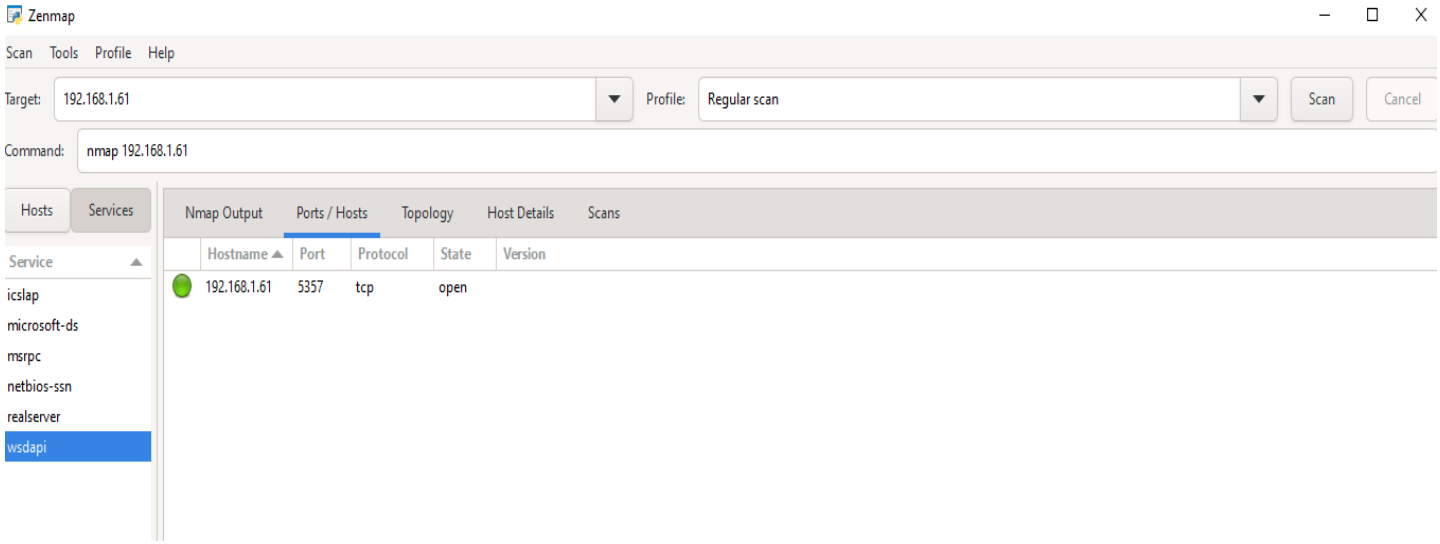
Read data files from: C:\Program Files (x86)\Nmap

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

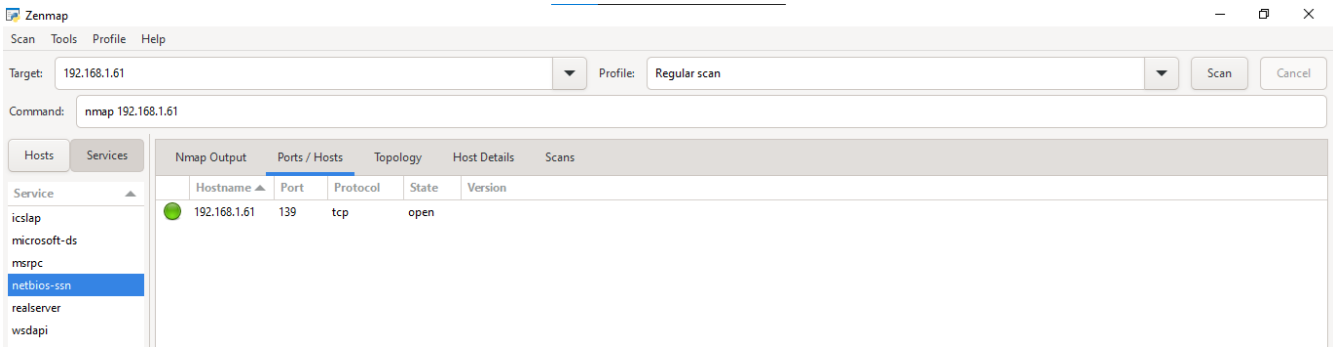
Nmap done: 1 IP address (1 host up) scanned in 261.85 seconds
Raw packets sent: 2326 (108.344KB) | Rcvd: 12 (500B)



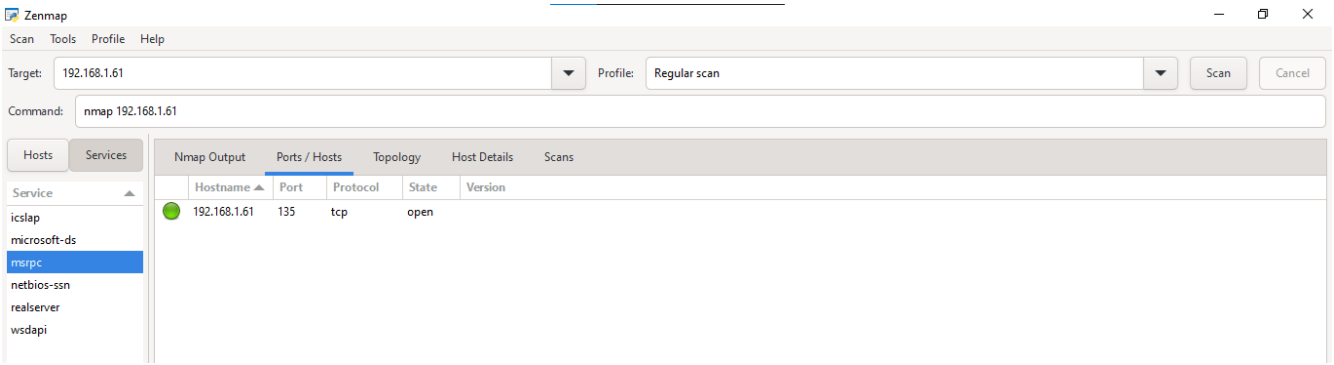
wsdapi:



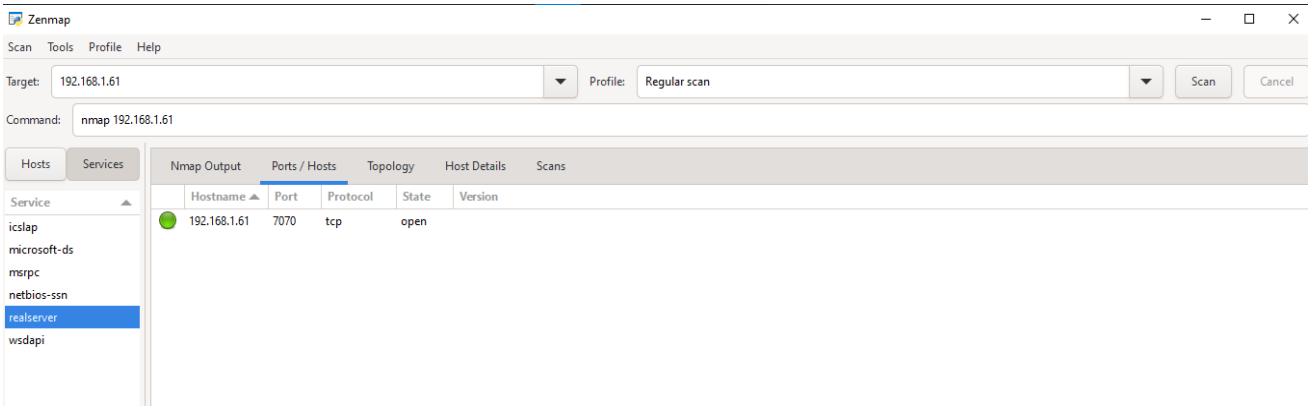
NETBIOS-SSN:



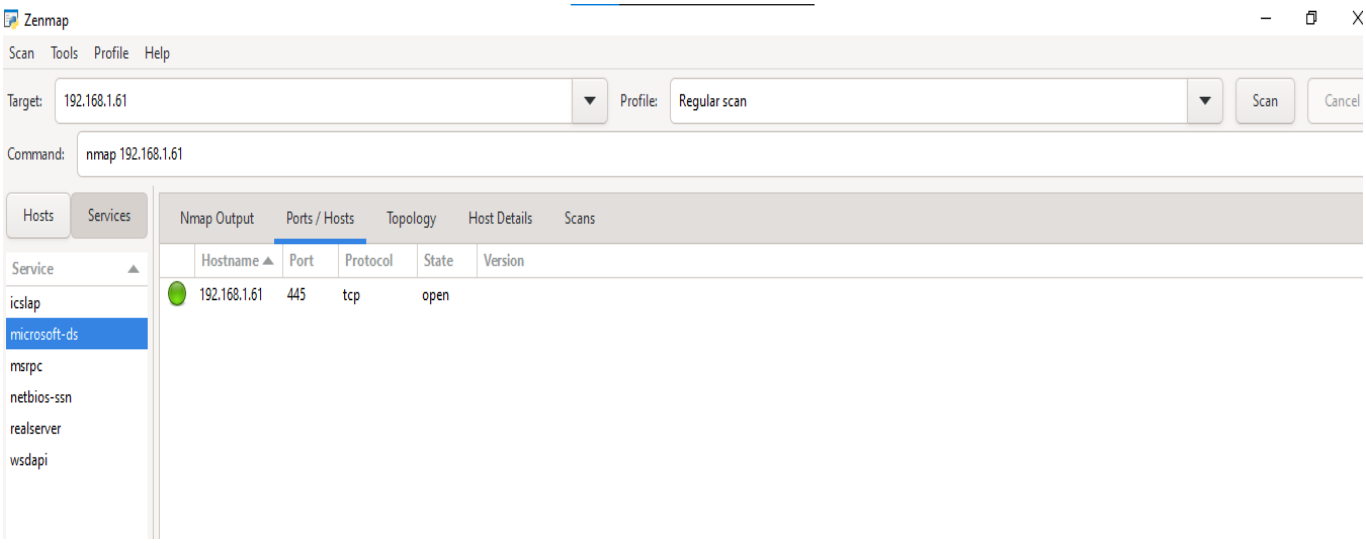
MSRPC:



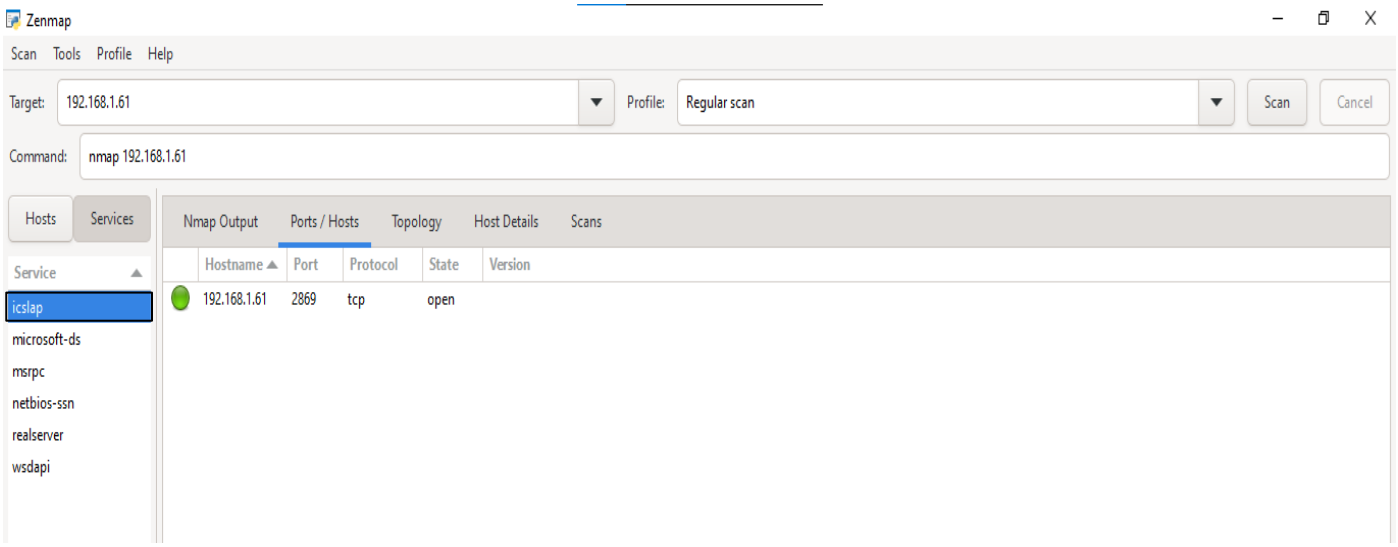
REALSERVE

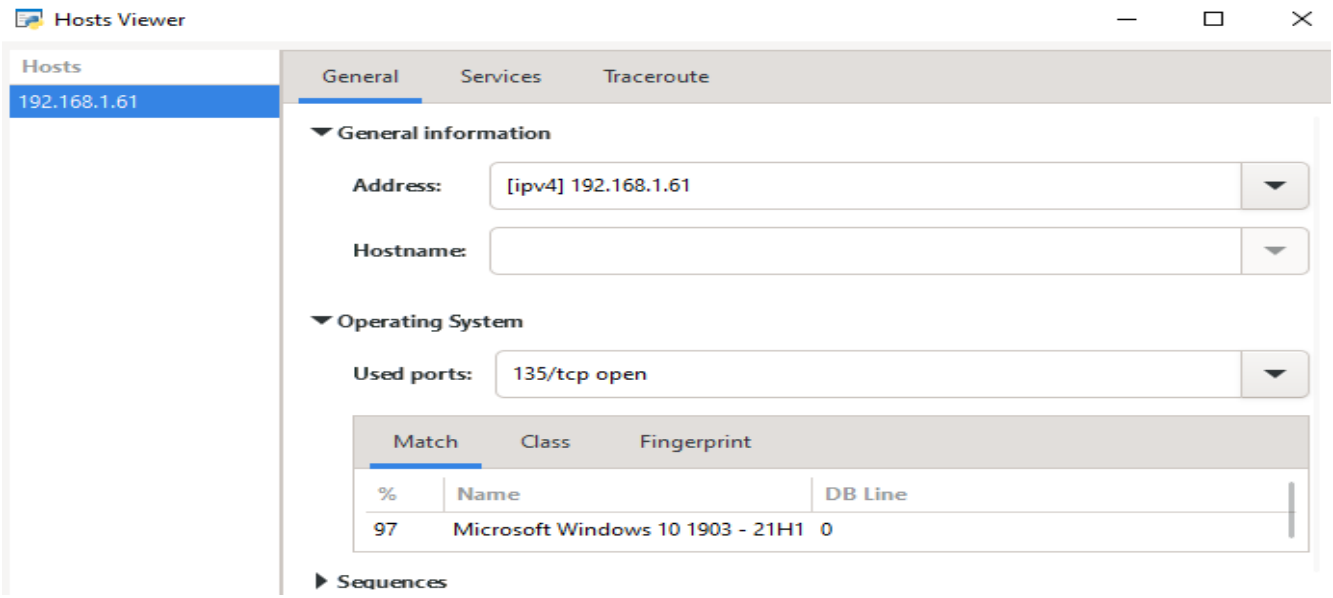


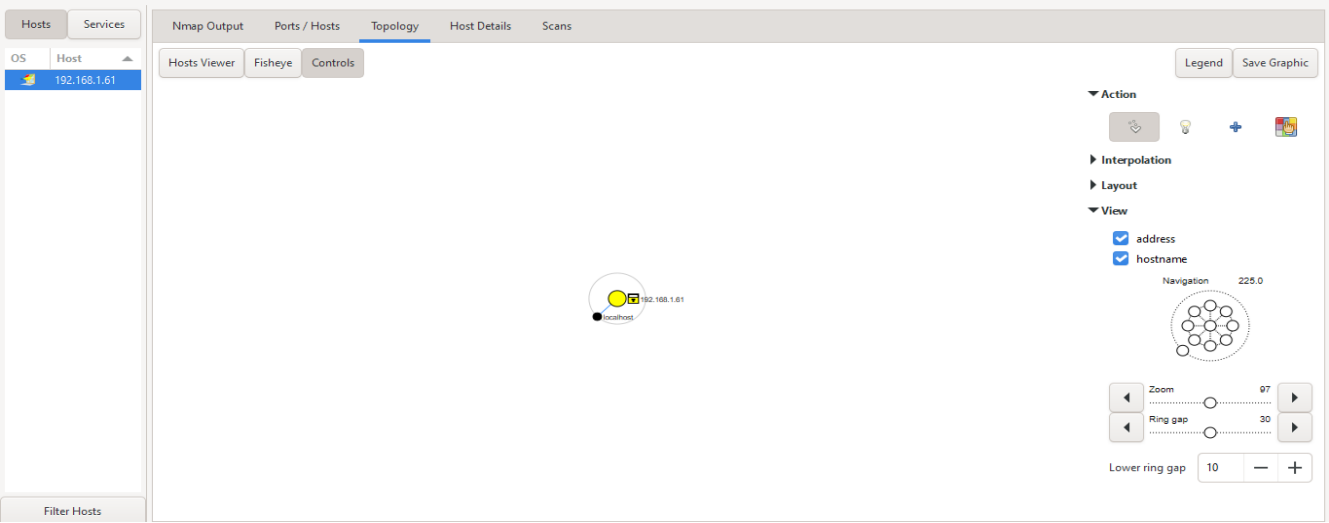
MICROSOFT-DS:



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



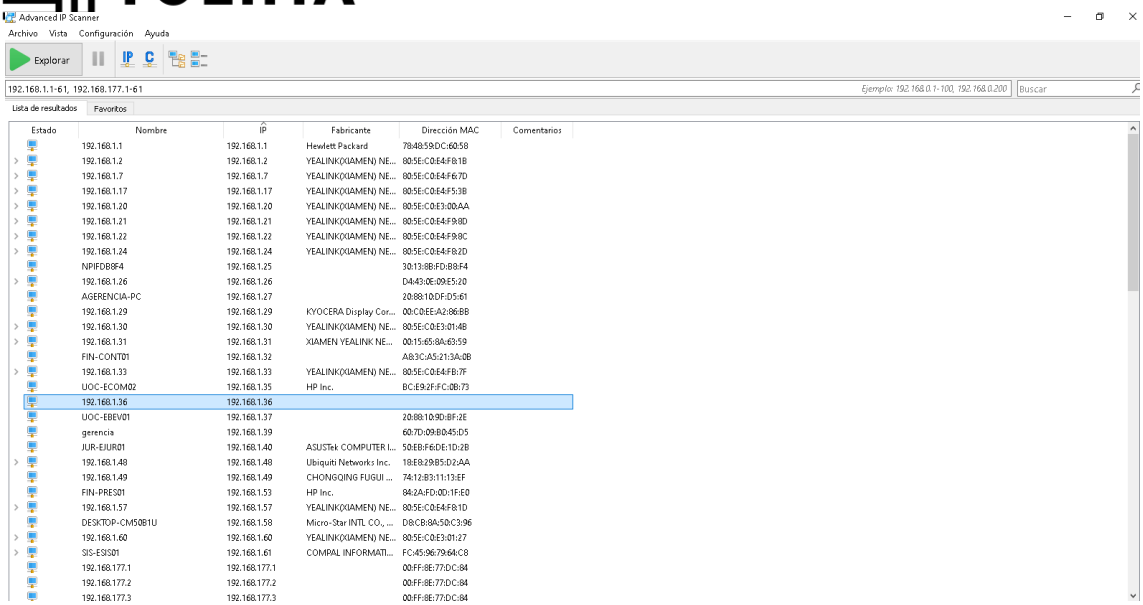
IPSCAN Tool

Dentro de las fases iniciales del reconocimiento de una red, resulta fundamental filtrar grandes bloques de direcciones IP con el fin de identificar únicamente aquellos dispositivos que se encuentran activos o que son relevantes para el análisis. Escanear cada puerto en todas las direcciones disponibles no solo consume tiempo, sino que en muchos casos no aporta información necesaria.

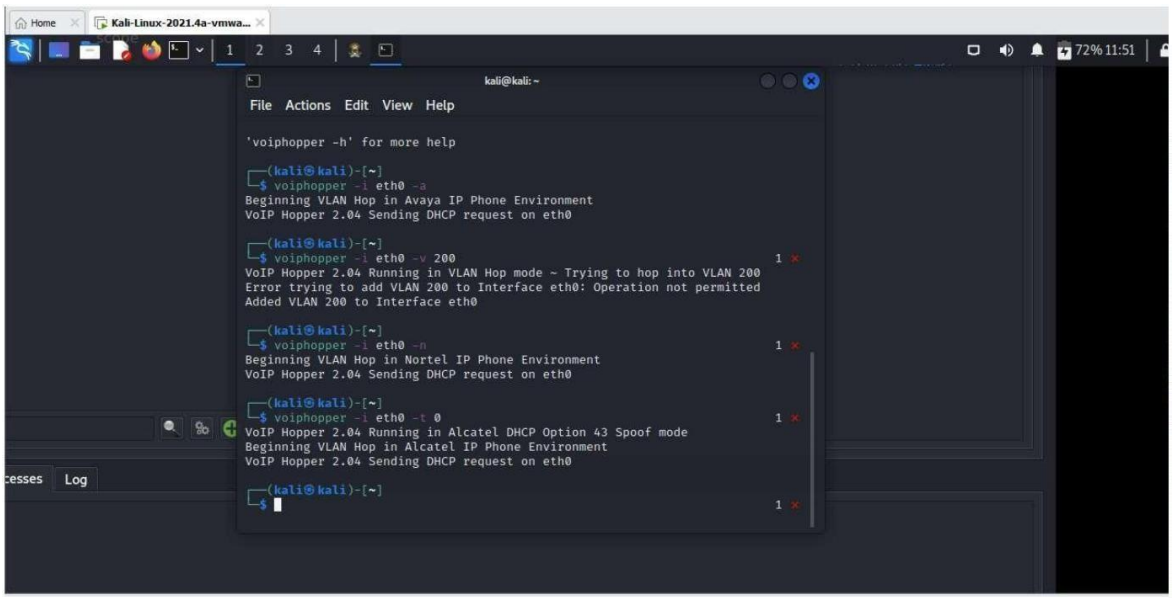
La relevancia de un sistema depende del propósito de la evaluación. Mientras que un administrador de red puede estar interesado únicamente en equipos que ejecuten ciertos servicios específicos, un auditor de seguridad podría necesitar detectar todos los dispositivos con direcciones IP asignadas. De igual manera, en una red interna puede bastar con una comprobación básica mediante ICMP (ping), mientras que en una auditoría externa podrían utilizarse múltiples técnicas de sondeo para superar posibles restricciones de firewall.

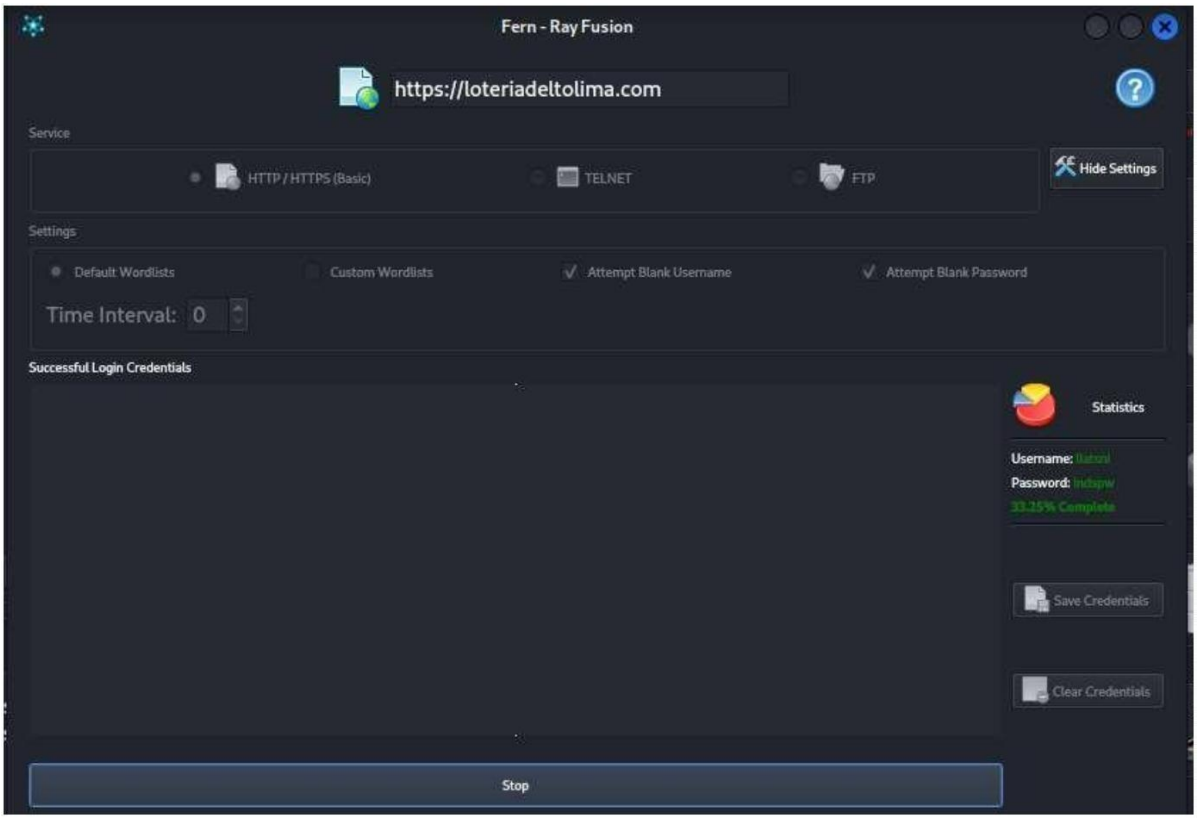
Ante estas diferentes necesidades, IPSCAN ofrece diversas alternativas para personalizar el proceso de descubrimiento de hosts. El denominado “Host Discovery” no se limita al envío de solicitudes ICMP tradicionales, sino que contempla métodos más avanzados como el escaneo de lista (-sL), la omisión del ping (-P0) o el uso combinado de sondas TCP (SYN/ACK), UDP e ICMP dirigidas a distintos puertos del objetivo.

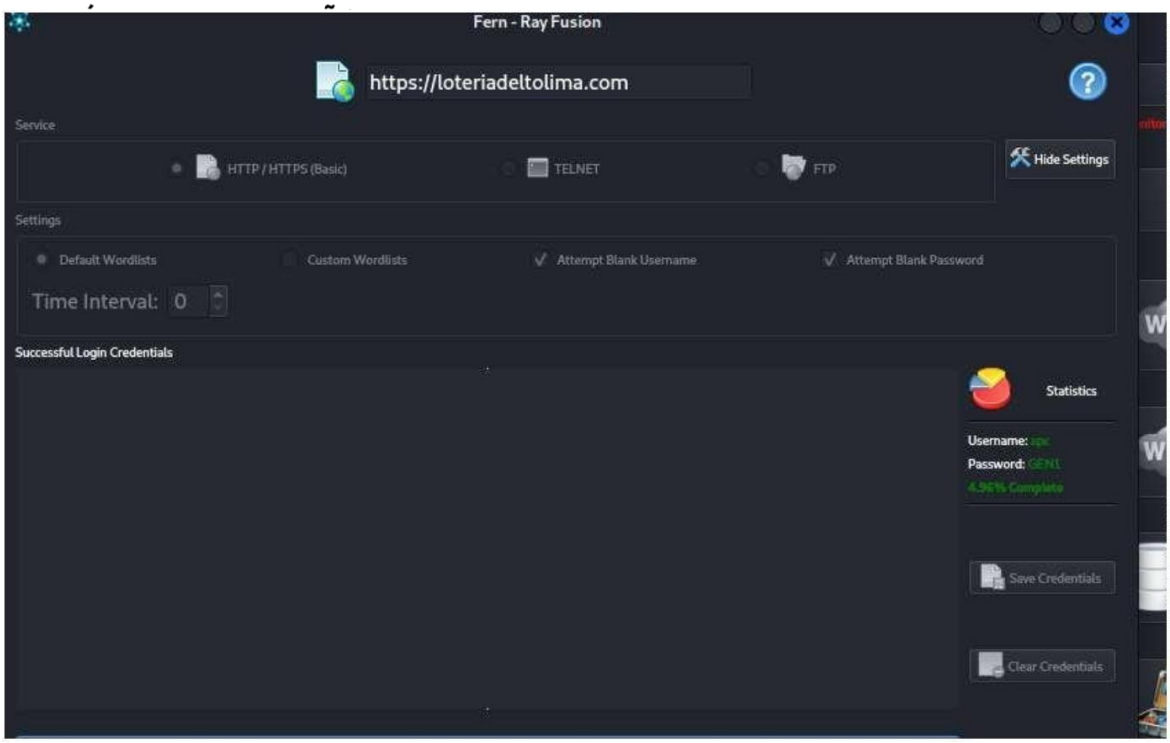
El propósito de estas técnicas es obtener respuestas que confirmen que una dirección IP está siendo utilizada. En redes que emplean direccionamiento privado bajo el estándar RFC1918, como el rango 10.0.0.0/8, es común que solo un pequeño porcentaje de las direcciones disponibles esté activo en un momento determinado. Aunque este rango permite millones de direcciones, muchas organizaciones utilizan solo una fracción reducida. Por esta razón, el descubrimiento de dispositivos resulta esencial para identificar de forma rápida y eficiente los equipos realmente operativos dentro de espacios de direccionamiento extensos.

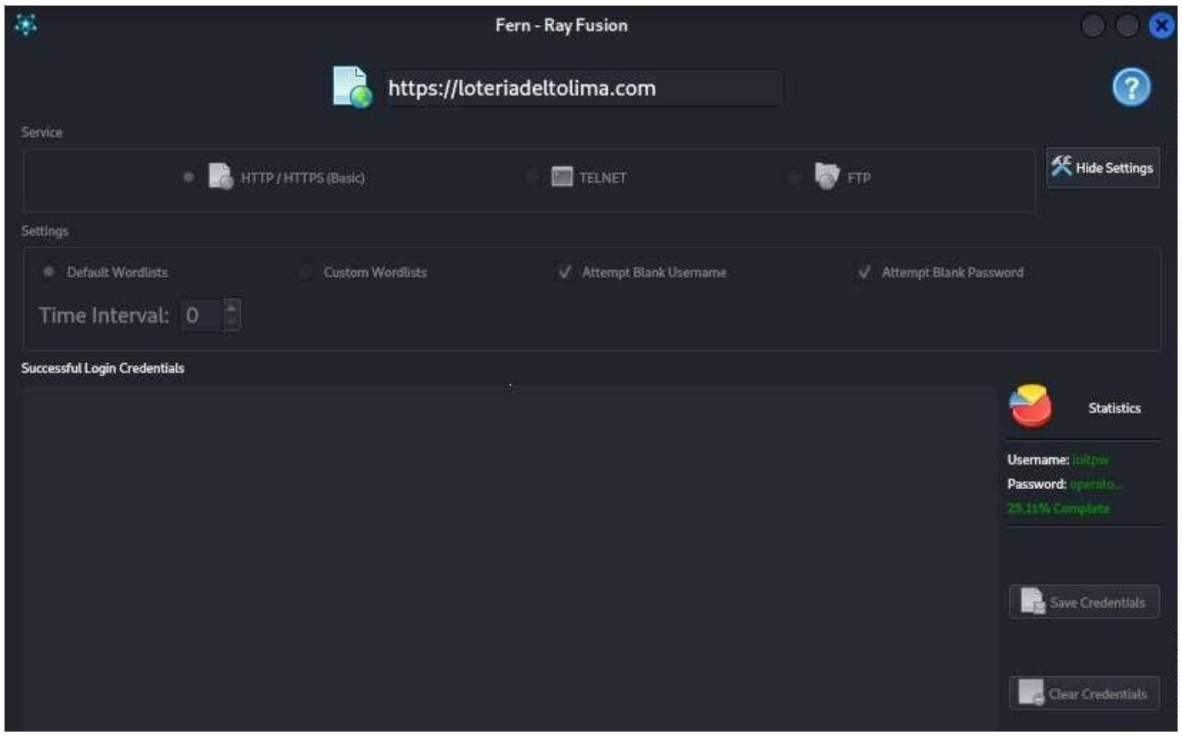


Kali-Linux Ray Fusion Wifi




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

Luego de llevar a cabo una evaluación detallada de los riesgos asociados a los equipos conectados a la red, se concluye que las medidas de protección aplicadas resultan satisfactorias para resguardar la infraestructura tecnológica. Las configuraciones cumplen con los estándares y buenas prácticas del sector, el software se mantiene debidamente actualizado y los mecanismos de control de acceso implementados reducen significativamente la posibilidad de accesos no autorizados.

Asimismo, las pruebas efectuadas no evidenciaron fallos críticos que representen una amenaza directa para la integridad de los sistemas. En consecuencia, puede afirmarse que los dispositivos operan bajo un entorno seguro frente a amenazas habituales, asegurando tanto la continuidad de las operaciones como la protección de la información gestionada.