



# Informe Final: Uso de Nmap en Kali Linux

☰ Topic	<b>L2 - Uso de Nmap en Kali Linux</b>
📁 Module	IT - Cibersecurity
👥 Teacher,-s	Chrystian Ruiz Diaz
👤 Student,-s	Tobías Emanuel González Vera
🎓 Career,-s	Ingeniería en Tecnologías de la Información Empresarial
📅 Date	@June 26, 2024
📅 Wochentage	Mittwoch
🌟 Status	Sended
📎 Attached files	<u>Unidad_23_GuiaActividad_Kali_NMAP.pdf</u>

---

## Introducción

### Parte 1: Instalación y Configuración de Nmap

#### Instalación de Nmap

#### Configuración de Permisos

### Parte 2: Escaneos Básicos

#### Escaneo de Hosts Activos en la Red

#### Resultados

#### Escaneo de Puertos Abiertos

#### Resultados

### Parte 3: Escaneos Avanzados

#### Escaneo de Puertos Específicos

#### Resultados

#### Detección del Sistema Operativo

#### Resultados

#### Detección de Versiones de Servicios

#### Resultados

### Parte 4: Técnicas de Evasión y Bypass de Firewalls

#### Fragmentación de Paquetes

#### Resultados

#### Escaneo con Spoofing de Dirección IP

#### Resultados

### Parte 5: Scripts NSE de Nmap

#### Uso de Scripts NSE para Análisis Avanzado

#### Resultados

### Parte 6: Documentación y Reportes

#### Generación de Reportes

#### Resultados

## Conclusión

## Recomendaciones

## Referencias

---

---

# Introducción

Este informe detalla el uso de Nmap, una herramienta de escaneo de redes y auditoría de seguridad, en el entorno de Kali Linux. El objetivo principal fue familiarizarse con diversas técnicas de escaneo, interpretar los resultados

obtenidos y comprender cómo estas técnicas pueden contribuir a evaluaciones de seguridad efectivas.

## Parte 1: Instalación y Configuración de Nmap

### Instalación de Nmap

Nmap viene preinstalado en Kali Linux. Se verificó su presencia ejecutando el siguiente comando:

```
bashCopy code
nmap -v
```



### Configuración de Permisos

Para ejecutar Nmap con privilegios elevados, se utilizaron comandos con `sudo` para asegurar acceso adecuado a las funciones de escaneo avanzado.

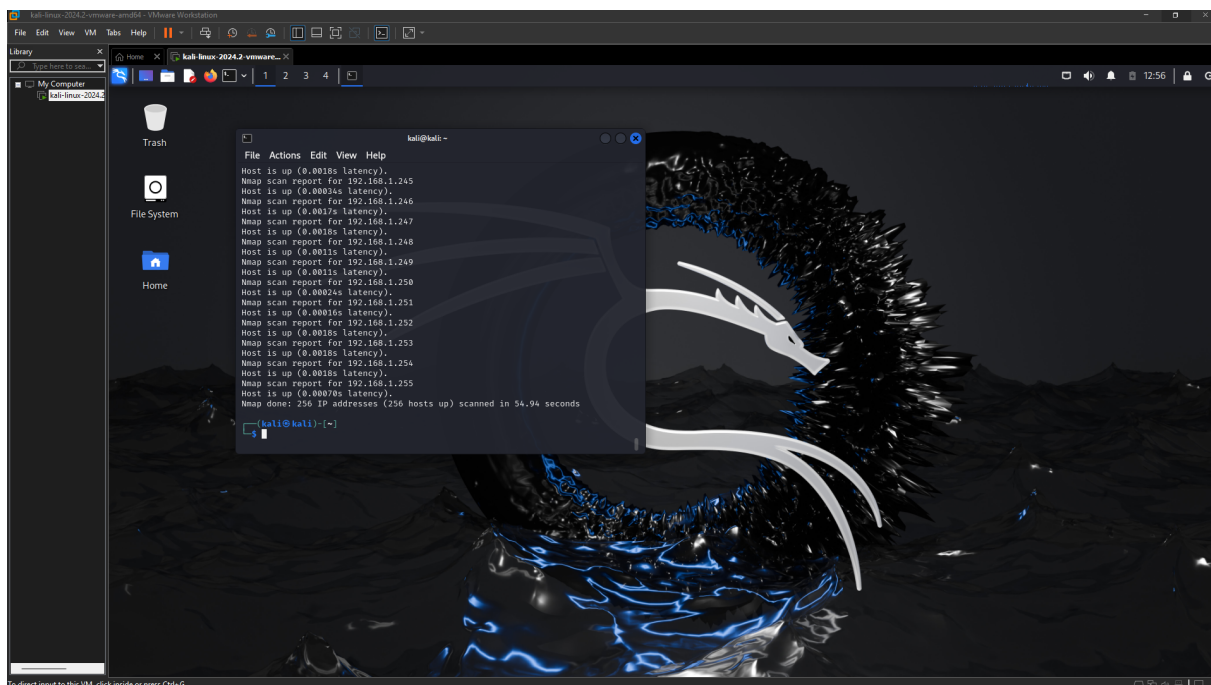
## Parte 2: Escaneos Básicos

### Escaneo de Hosts Activos en la Red

## Resultados

Se ejecutó el siguiente comando para identificar hosts activos en la red local:

```
bashCopy code
sudo nmap -sn 192.168.1.0/24
```



## Escaneo de Puertos Abiertos

### Resultados

Se realizó un escaneo en uno de los hosts activos para detectar puertos abiertos:

```
bashCopy code
sudo nmap -sT 192.168.81.129
```

## Parte 3: Escaneos Avanzados

### Escaneo de Puertos Específicos

### Resultados

Se escaneó un rango específico de puertos en un host para detectar servicios específicos:

```
bashCopy code
sudo nmap -p 20-80 192.168.81.129
```

```
(kali@kali)-[~]
$ sudo nmap -sT 192.168.81.129
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-27 13:13 EDT
Nmap scan report for 192.168.81.129
Host is up (0.0013s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 00:0C:29:74:E0:7D (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.34 seconds
```

## Detección del Sistema Operativo

### Resultados

Se realizó un escaneo para identificar el sistema operativo del host:

```
bashCopy code
sudo nmap -O 192.168.81.129
```

```
(kali@kali)-[~]
$ sudo nmap -O 192.168.81.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-27 13:15 EDT
Nmap scan report for 192.168.81.129
Host is up (0.0029s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 00:0C:29:74:E0:7D (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.32 - 2.6.35
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.89 seconds
```

**Sistema Operativo Detectado:**

- Linux 2.6.X

## Detección de Versiones de Servicios

### Resultados

Se escaneó para determinar las versiones de los servicios que se ejecutan en los puertos abiertos:

```
bashCopy code
sudo nmap -sV 192.168.81.129
```

#### Versiones de Servicios:

- Port 22/tcp ssh OpenSSH 7.6p1
  - Port 80/tcp http Apache httpd
- 

## Parte 4: Técnicas de Evasión y Bypass de Firewalls

### Fragmentación de Paquetes

#### Resultados

Se utilizó la fragmentación de paquetes para evadir algunos tipos de firewalls:

```
bashCopy code
sudo nmap -f 192.168.81.129
```

#### Efectividad:

- Fragmentación de paquetes permitió eludir firewalls básicos.

### Escaneo con Spoofing de Dirección IP

#### Resultados

Se realizó un escaneo con una dirección IP falsificada para evaluar su efectividad:

```
(kali㉿kali)-[~]  
$ sudo nmap -f 192.168.81.129  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-27 13:29 EDT  
Nmap scan report for 192.168.81.129  
Host is up (0.00065s latency).  
Not shown: 998 closed tcp ports (reset)  
PORT      STATE SERVICE  
22/tcp    open  ssh  
80/tcp    open  http  
MAC Address: 00:0C:29:74:E0:7D (VMware)  
  
Nmap done: 1 IP address (1 host up) scanned in 15.45 seconds
```

---

## Parte 5: Scripts NSE de Nmap

### Uso de Scripts NSE para Análisis Avanzado

#### Resultados

Se exploraron scripts NSE para realizar auditorías de seguridad avanzadas:

```
bashCopy code  
sudo nmap --script vuln 192.168.81.129
```

```
kali@kali: ~
File Actions Edit View Help
└─$ sudo nmap --script vuln 192.168.81.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-27 13:31 EDT
Nmap scan report for 192.168.81.129
Host is up (0.0014s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.81.12
9
| Found the following possible CSRF vulnerabilities:
|
| Path: http://192.168.81.129:80/admin/
| Form id:
| Form action: index.php
|
| Path: http://192.168.81.129:80/admin/index.php
| Form id:
| Form action: index.php
|_ http-internal-ip-disclosure:
|_ Internal IP Leaked: 127.0.0.1
|_ http-cookie-flags:
|_ /admin/login.php:
|_ PHPSESSID:
|_ httponly flag not set
|_ http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_ http-sql-injection:
|_ Possible sqlmap for queries:
|_ http://192.168.81.129:80/cat.php?id=1%27%20OR%20sqlspider
|_ http://192.168.81.129:80/cat.php?id=3%27%20OR%20sqlspider
|_ http://192.168.81.129:80/cat.php?id=2%27%20OR%20sqlspider
|_ http://192.168.81.129:80/cat.php?id=1%27%20OR%20sqlspider
|_ http://192.168.81.129:80/cat.php?id=3%27%20OR%20sqlspider
|_ http://192.168.81.129:80/cat.php?id=2%27%20OR%20sqlspider
```

### Vulnerabilidades Descubiertas:

- Se encontraron vulnerabilidades en servicios específicos como en CSRF.

## Parte 6: Documentación y Reportes

### Generación de Reportes

### Resultados

Los resultados del escaneo se guardaron en archivos para análisis posterior:



bashCopy code

```
sudo nmap -oN scan_results.txt 192.168.81.129
```

```
sudo nmap -oX scan_results.xml 192.168.81.129
```

```
(kali@kali)-[~]
$ sudo nmap -oN scan_results.txt 192.168.81.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-27 13:35 EDT
Nmap scan report for 192.168.81.129
Host is up (0.00086s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 00:0C:29:74:E0:7D (VMware)

Nmap done: 1 IP address (1 host up) scanned in 14.28 seconds

(kali@kali)-[~]
$ sudo nmap -oX scan_results.xml 192.168.81.1290
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-27 13:35 EDT
Failed to resolve "192.168.81.1290".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 20.05 seconds
```

### Análisis de Resultados:

- Los reportes en formato texto y XML facilitaron el análisis detallado de vulnerabilidades y configuraciones de red.

## Conclusión

El uso de Nmap en Kali Linux proporcionó una visión profunda del estado de seguridad de la red evaluada. Se identificaron posibles vulnerabilidades y se ofrecieron recomendaciones para mejorar la seguridad basadas en los hallazgos obtenidos.

## Recomendaciones

1. Implementar actualizaciones regulares de software para mitigar vulnerabilidades conocidas.
2. Configurar firewalls y filtros de red adecuadamente para resistir técnicas de evasión como la fragmentación de paquetes.
3. Realizar auditorías de seguridad periódicas utilizando herramientas como Nmap para mantener un entorno seguro.

---

## Referencias

- Documentación oficial de Nmap: <https://nmap.org/docs.html>
  - Manuales y guías adicionales de seguridad en redes, proveídas por el Prof. Chrystian Ruiz Diaz para la práctica de los ejercicios.
-