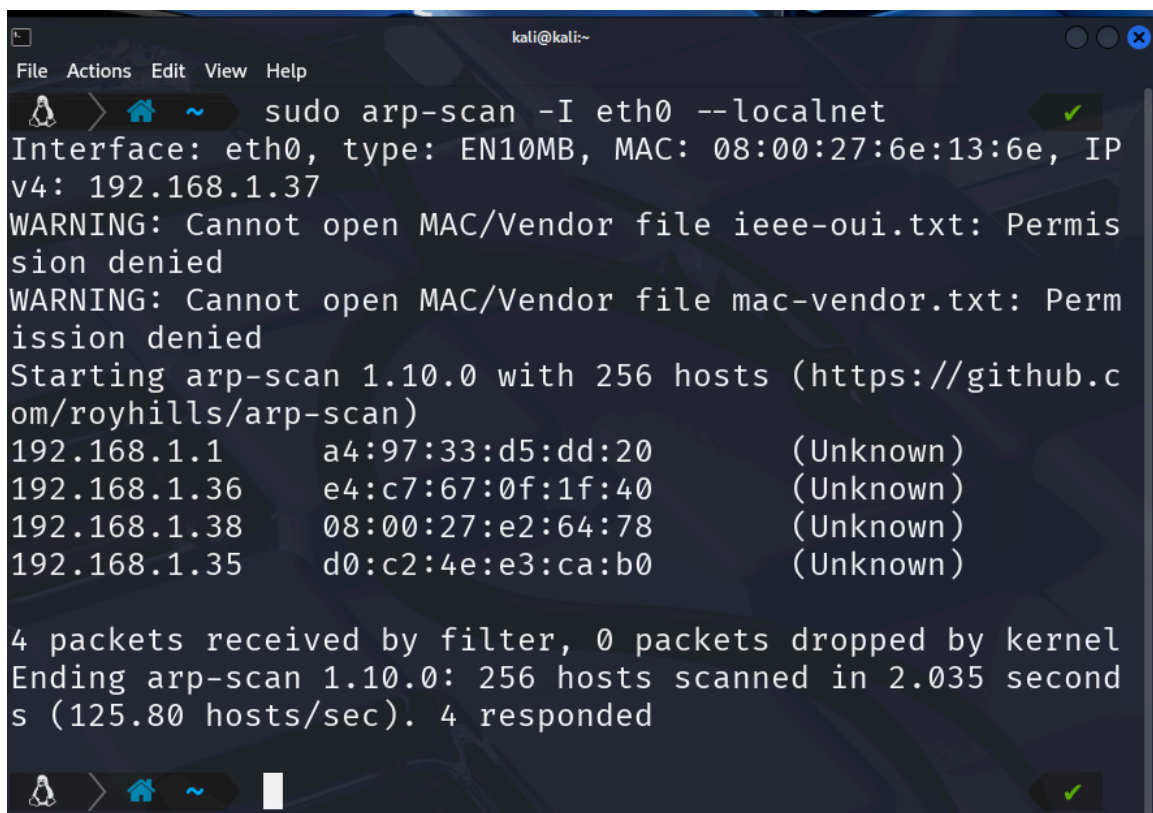


Detectar Vulnerabilidades Con Nmap

Vamos a detectar vulnerabilidades existentes con Nmap o al menos las mas conocidas.

- Hacemos un escaneo de la red local

```
sudo arp-scan -I eth0 --localnet
```



```
kali@kali:~  
File Actions Edit View Help  
sudo arp-scan -I eth0 --localnet  
Interface: eth0, type: EN10MB, MAC: 08:00:27:6e:13:6e, IP v4: 192.168.1.37  
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied  
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied  
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)  
192.168.1.1      a4:97:33:d5:dd:20      (Unknown)  
192.168.1.36     e4:c7:67:0f:1f:40      (Unknown)  
192.168.1.38     08:00:27:e2:64:78      (Unknown)  
192.168.1.35     d0:c2:4e:e3:ca:b0      (Unknown)  
  
4 packets received by filter, 0 packets dropped by kernel  
Ending arp-scan 1.10.0: 256 hosts scanned in 2.035 seconds (125.80 hosts/sec). 4 responded
```

- Hacemos un Ping hacia nuestro objetivo para intuir que sistema operativo corre en el .

```
ping -c 1 192.168.1.38
```

```
ping -c 1 192.168.1.38
PING 192.168.1.38 (192.168.1.38) 56(84) bytes of data.
64 bytes from 192.168.1.38: icmp_seq=1 ttl=128 time=5.35
ms
— 192.168.1.38 ping statistics —
1 packets transmitted, 1 received, 0% packet loss, time 0
```

- Vamos a hacer que nmap nos muestre los puertos abiertos y los que este corriendo tras ellos.

```
nmap -p- --open -sS -sV --min-rate 1500 -n -vvv -Pn 192.168.1.41 -oN esc
```

```
File Actions Edit View Help
kali@kali:~$ nmap -p- --open -sS -sV --min-rate 1500 -n -vvv -Pn 192.168.1.41 -oN esc
Scanning 192.168.1.41 [65535 ports]
Discovered open port 135/tcp on 192.168.1.41
Discovered open port 139/tcp on 192.168.1.41
Discovered open port 445/tcp on 192.168.1.41
SYN Stealth Scan Timing: About 23.25% done; ETC: 04:46 (0:01:42 remaining)
SYN Stealth Scan Timing: About 46.14% done; ETC: 04:46 (0:01:11 remaining)
SYN Stealth Scan Timing: About 70.61% done; ETC: 04:46 (0:00:38 remaining)
Discovered open port 5357/tcp on 192.168.1.41
Discovered open port 5000/tcp on 192.168.1.41
Completed SYN Stealth Scan at 04:46, 123.30s elapsed (65535 total ports)
Initiating Service scan at 04:46
Scanning 5 services on 192.168.1.41
Completed Service scan at 04:48, 162.19s elapsed (5 services on 1 host)
NSE: Script scanning 192.168.1.41.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 04:48
Completed NSE at 04:48, 0.03s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 04:48
Completed NSE at 04:48, 1.01s elapsed
Nmap scan report for 192.168.1.41
Host is up, received arp-response (0.0028s latency).
Scanned at 2025-03-30 04:43:57 EDT for 287s
Not shown: 65530 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE        REASON          VERSION
135/tcp   open  msrpc          syn-ack ttl 128 Microsoft Windows RPC
139/tcp   open  netbios-ssn    syn-ack ttl 128 Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds   syn-ack ttl 128 Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGR
OUP)
5000/tcp   open  upnp?          syn-ack ttl 128
5357/tcp   open  http           syn-ack ttl 128 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 08:00:27:E2:64:78 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: MARIO-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 286.79 seconds
Raw packets sent: 196690 (8.654MB) | Rcvd: 100 (4.384KB)
```

Como vemos el puerto 445 nos muestra mucha información y suele ser el del protocolo SMB. Que el Windows 7 era muy propenso a ataque sobre todo si tiene la versión 1 de SMB.

- Vamos a realizar un escaneo de vulnerabilidades con nmap sobre el puerto 445. Hay que tener en cuenta que el script de vulnerabilidades de nmap hace mucho ruido y no es adecuado para utilizarlo en entornos reales.

```
nmap --script "vuln" -p445 192.168.1.38
```

Este comando realiza un escaneo en el puerto 445 del dispositivo con la IP 192.168.1.38, buscando vulnerabilidades relacionadas con el protocolo SMB, como problemas de autenticación, exploits conocidos o configuraciones inseguras.

nmap : Es la **herramienta** principal que estás utilizando para realizar un escaneo de red.

--script "vuln" : Indica que se **empleará un conjunto de scripts** del motor NSE (Nmap Scripting Engine) **enfocados en la detección de vulnerabilidades**. El script vuln ejecuta varios análisis para identificar posibles vulnerabilidades en el sistema objetivo.

-p445 : Especifica que **solo se escaneará el puerto 445**, el cual, como mencioné antes, está asociado con el protocolo SMB en sistemas Windows.

192.168.1.38 : Es la **dirección IP del sistema objetivo** que deseas analizar.

```
nmap --script "vuln" -p445 192.168.1.38
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-30 11:06 EDT
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 192.168.1.38
Host is up (0.0020s latency).

PORT      STATE SERVICE
445/tcp   open  microsoft-ds
MAC Address: 08:00:27:E2:64:78 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|     Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs: CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|       servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-w
```

No encuentra una vulnerabilidad en el puerto y **nos muestra el CVE** de la vulnerabilidad. Aquí entraría en juego la fase de explotación, buscando sploit o herramientas en internet para atacarla manual mente o mediante herramientas automatizadas como **Metasploit** .

En la siguiente web podemos buscar información sobre el CVE: **NVD - Home**

CVE-2017-0143 Detail

UNDERGOING REANALYSIS

This CVE is currently being enriched by team members, this process results in the association of reference link tags, CVSS, CWE, and CPE applicability statement data.

Description

The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148.

Metrics

CVSS Version 4.0

CVSS Version 3.x

CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:



NIST: NVD

Base Score: 8.8 HIGH

Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

ADP: CISA-ADP

Base Score: 8.8 HIGH

Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
http://packetstormsecurity.com/files/154690/DOUBLEPULSAR-Payload-Execution-Neutralization.html	Exploit Third Party Advisory VDB Entry
http://packetstormsecurity.com/files/154690/DOUBLEPULSAR-Payload-Execution-Neutralization.html	Exploit Third Party Advisory VDB Entry

Esta en concreto es una de las vulnerabilidades relacionadas con el exploit **EternalBlue**, que fue utilizado en ataques masivos como WannaCry.