GoodSecurity Penetration Test Report

Robert L. Myers@GoodSecurity.com

October 24, 2021

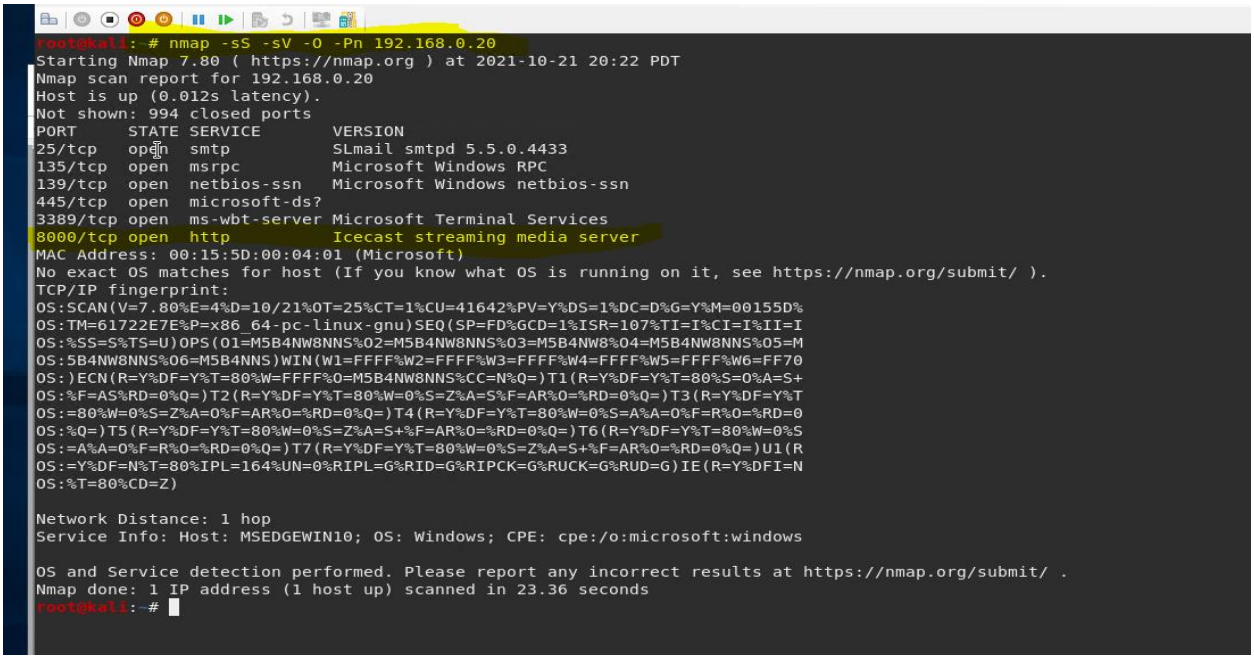
1.0 High-Level Summary

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

Machine IP: 192.168.0.20



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: Icecast Header Overwrite

- Search for Icecast using msfconsole to display the Icecast Header Overwrite exploit

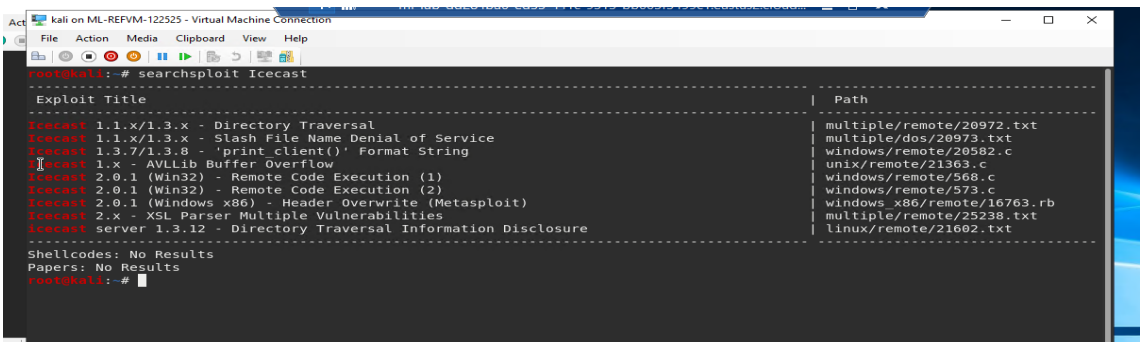
```
msf5 > search Icecast

Matching Modules
================

   #  Name                                  Disclosure Date  Rank   Check  Description
   -  ----                                  ---------------  ----   -----  -----------
   0  exploit/windows/http/icecast_header   2004-09-28       great  No     Icecast Header Overwrite


msf5 >
```

- **Upon further Investigation** we also determined that there is a total of 9 publicly known vulnerability's on the Icecast streaming media server.
- The 9 vulnerabilities listed in the picture below can also be found at the following public website: https://www.exploit-db.com/
- 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 vulnerability has been assigned the identifier CVE-2018-18820.



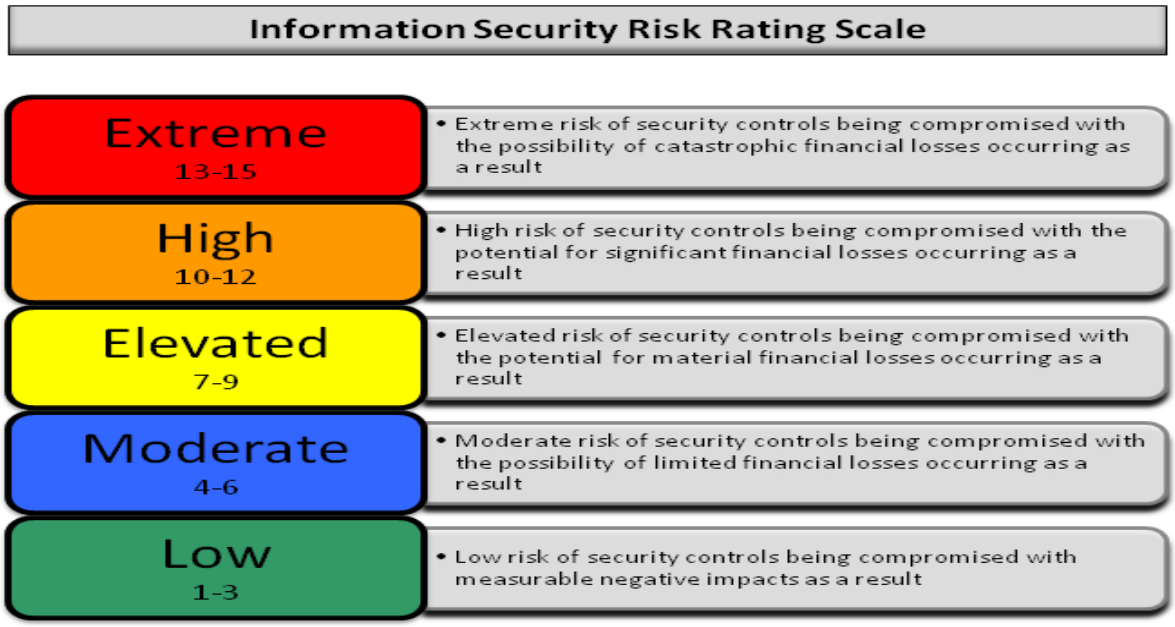
Vulnerability Explanation:

The Icecast Header Overwrite 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.

In this specific example, GoodSecurity was able to establish a remote code 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:

GoodSecurity's expert opinion this vulnerability would be **EXTREME**



Proof of Concept:

3.0 Recommendations

What recommendations would you give to GoodCorp?