GoodSecurity Penetration Test Report

BonssaTeizazu@GoodSecurity.com

DATE: 01/29/22

# 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**

Hostname:

**MSEDGEWIN10**

Vulnerability Exploited:

**Icecast Header Overwrite**

Vulnerability Explanation:

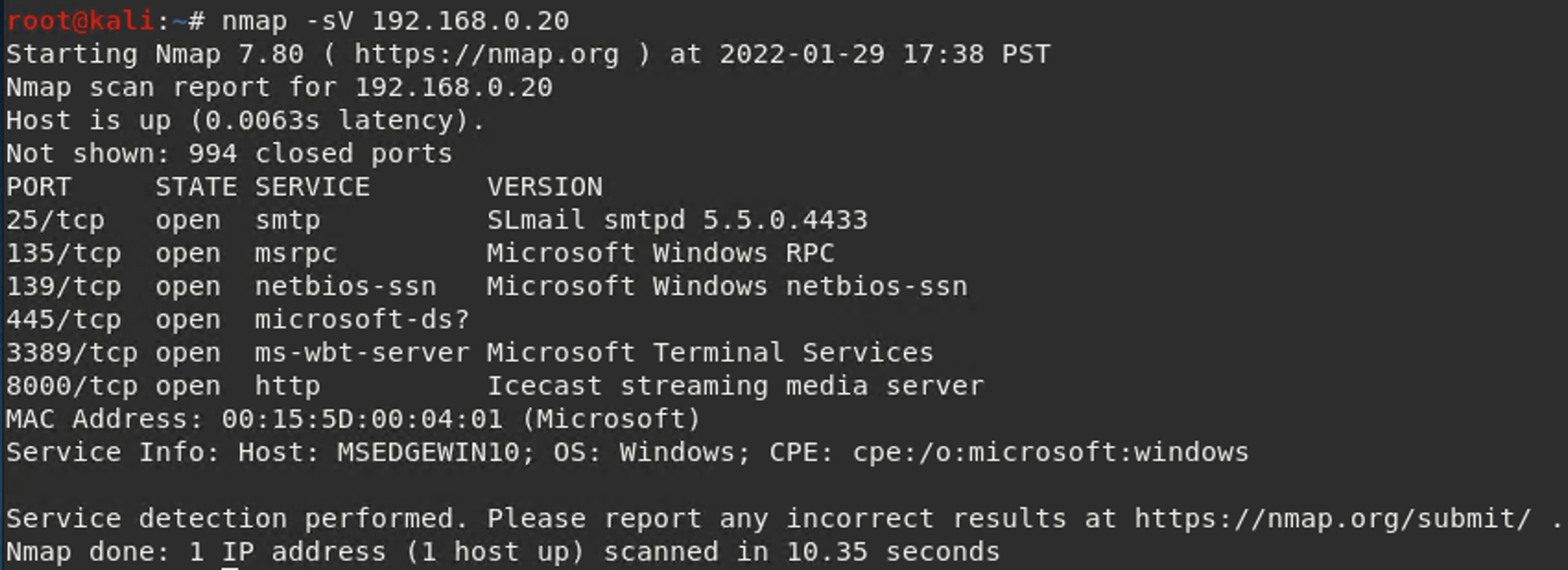
(Taken from https://www.rapid7.com/db/modules/exploit/windows/http/icecast\_header/)  
“This module exploits a **buffer overflow** in the header parsing of icecast versions 2.0.1 and earlier, discovered by Luigi Auriemma. Sending 32 HTTP headers will cause a write one past the end of a pointer array.”

Severity:

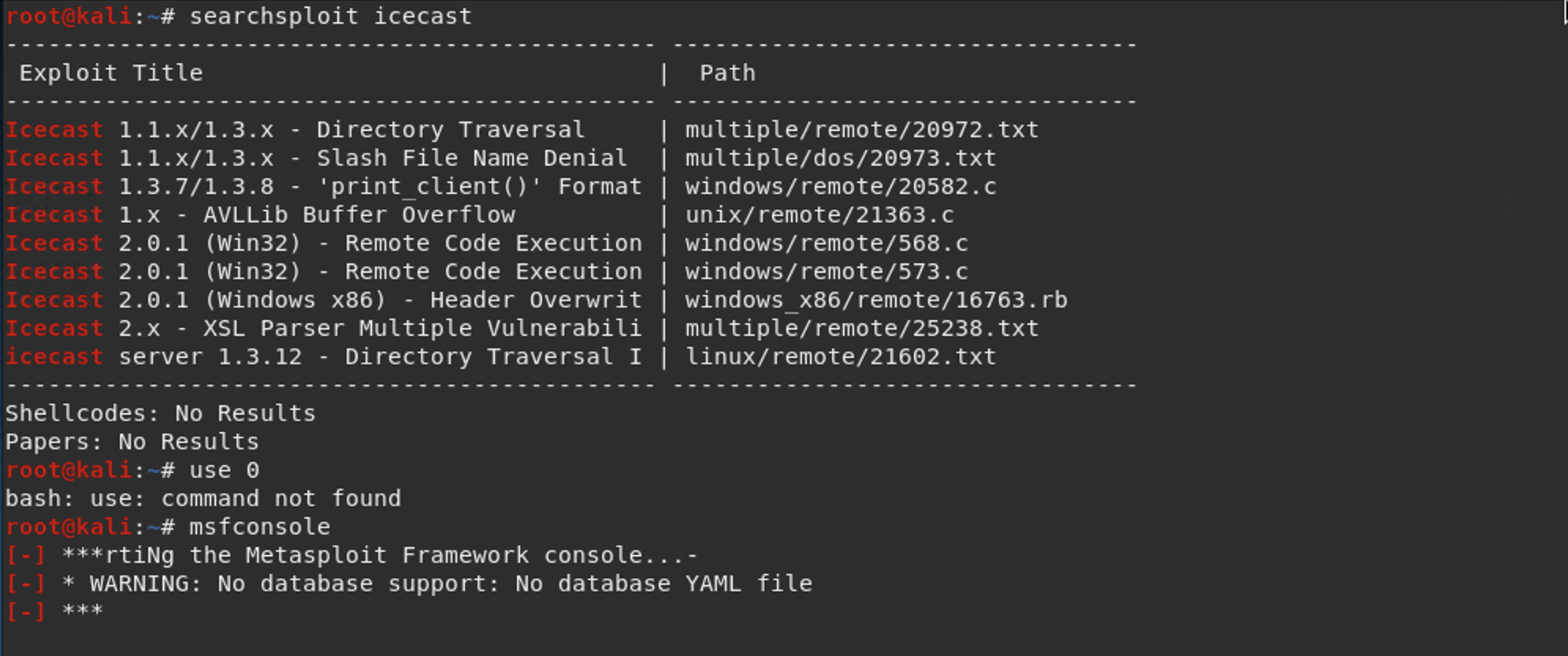
In your expert opinion, how severe is this vulnerability?  
This is very severe. After exploiting the vulnerability with Metasploit, we were able to search for files on Hans’ computer and download them to our machine.

Proof of Concept:

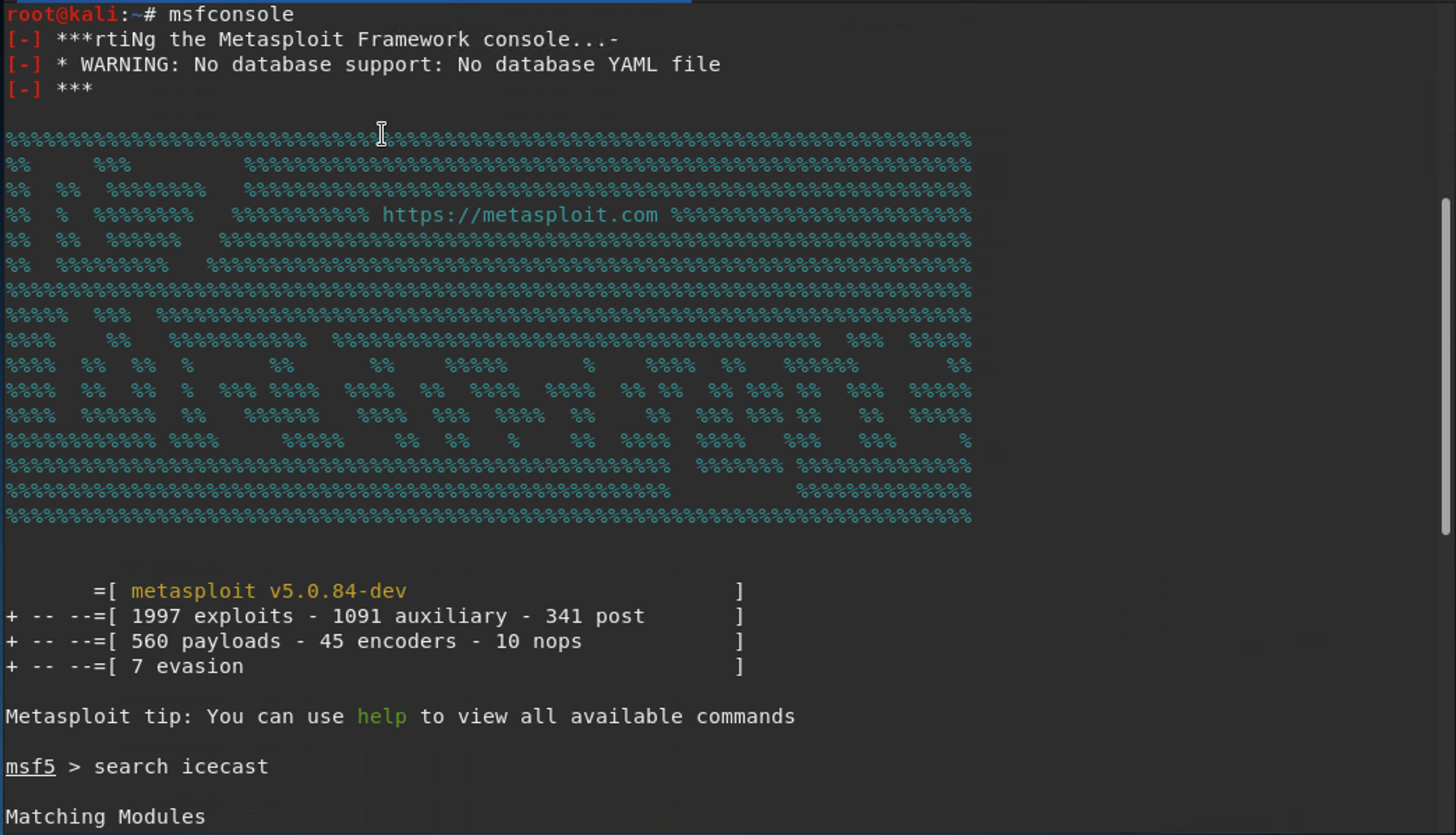
We started by running an nmap scan on Hans’ computer to search for vulnerabililities. An Icecast server was running, which was exploited in our attack.



Then we used searchsploit to search for available icecase exploits. Icecast exploits were listed in a database of exploits, confirming that Icecast exploits exist.



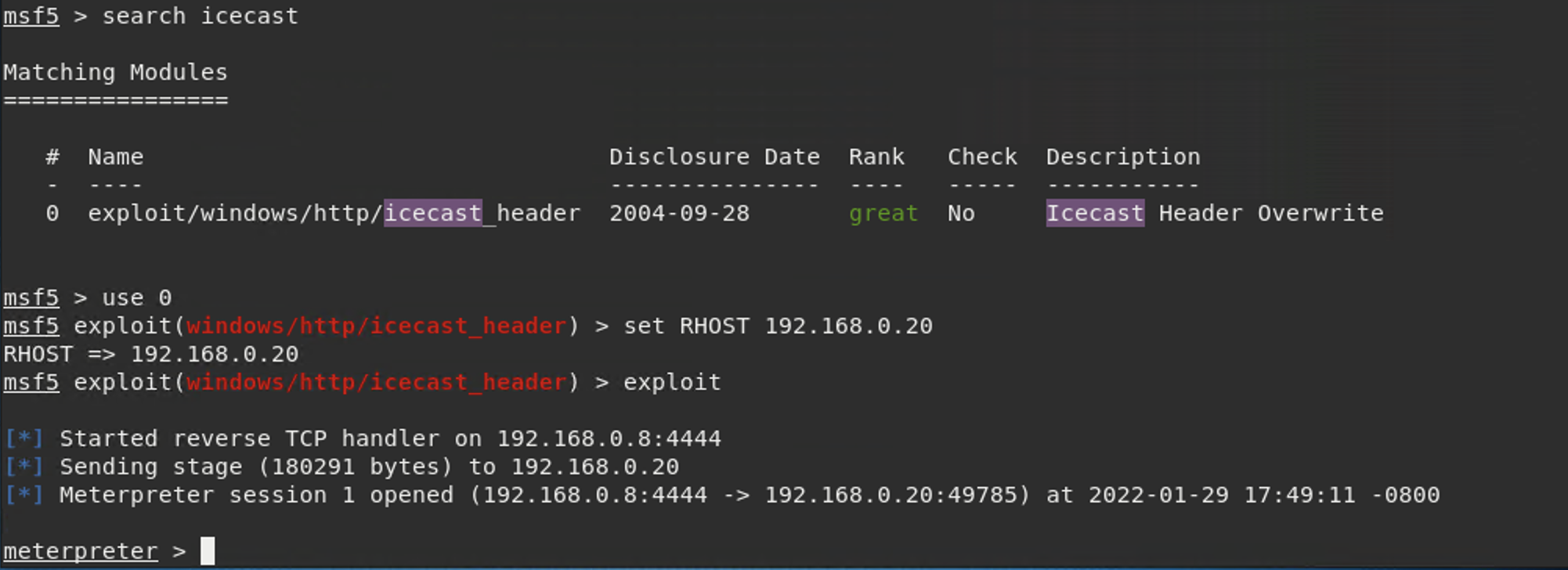
Then we used metasploit to prepare an attack.



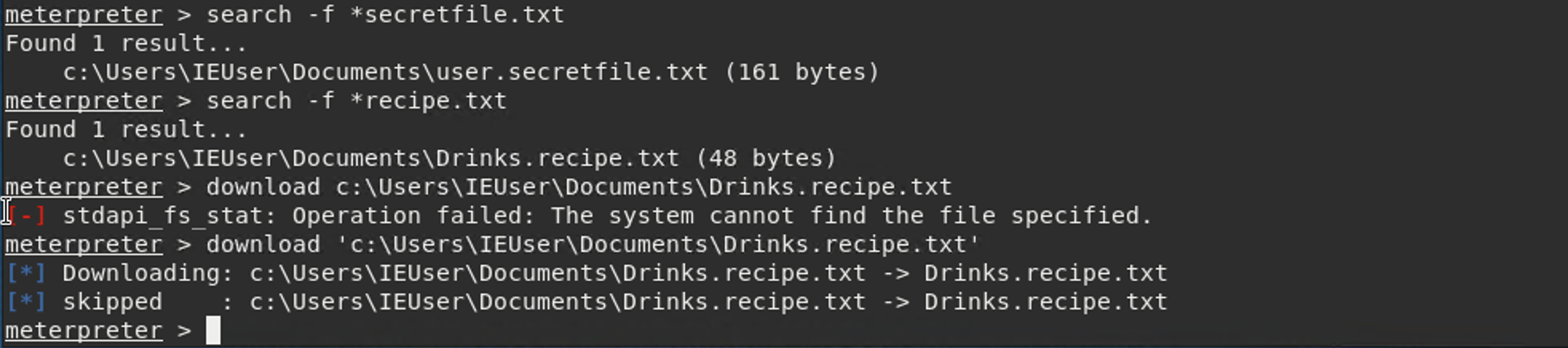
First we searched Metasploit’s modules for Icecast exploits. Metasploit had an exploit called “Icecast Header Overwrite” which we used for our attack.

Then we set Hans’ IP address as the HOST for the exploit.

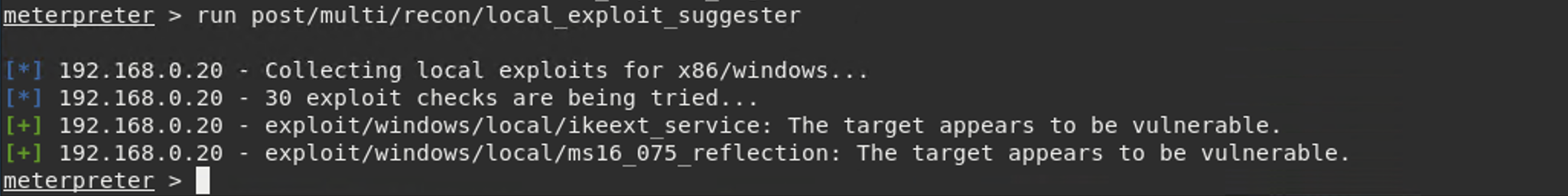
We sent the attack, which started a Meterpreter session to access Han’s computer.



Through the Meterpreter session, we were able to find the secretfile.txt. We also found the \*recipe.txt files and downloaded it to our machine.



Meterpreter’s local exploit suggester found two other potential vulnerabilities on Hans computer



# Recommendations

What recommendations would you give to GoodCorp?

**-Closing the port for Icecast server**

IceCast Server was accessible through port 8000 on Hans’ IP. We recommend closing that port.

**-Replacing Icecast server**

If closing port 8000 isn’t an option, we recommend using an alternative streaming audio server to Icecast. Here’s a link to a list of alternative servers, taken from a google search: <https://alternativeto.net/software/icecast/>

Note: If they choose a new server, another searchsploit scan should be run for potential exploits related to that server.