GoodSecurity Penetration Test Report

[Rishabh@GoodSecurity.com](mailto:Rishabhkalia@GoodSecurity.com)

DATE09-05-2022

# 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 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 exploit two programs that had major vulnerabilities. The details of the attack can be found in the ‘Findings’ category.

# Findings

Machine IP:

192.168.0.20

Hostname:

msedgewin10

Vulnerability Exploited:

ICECAST

Vulnerability Explanation:

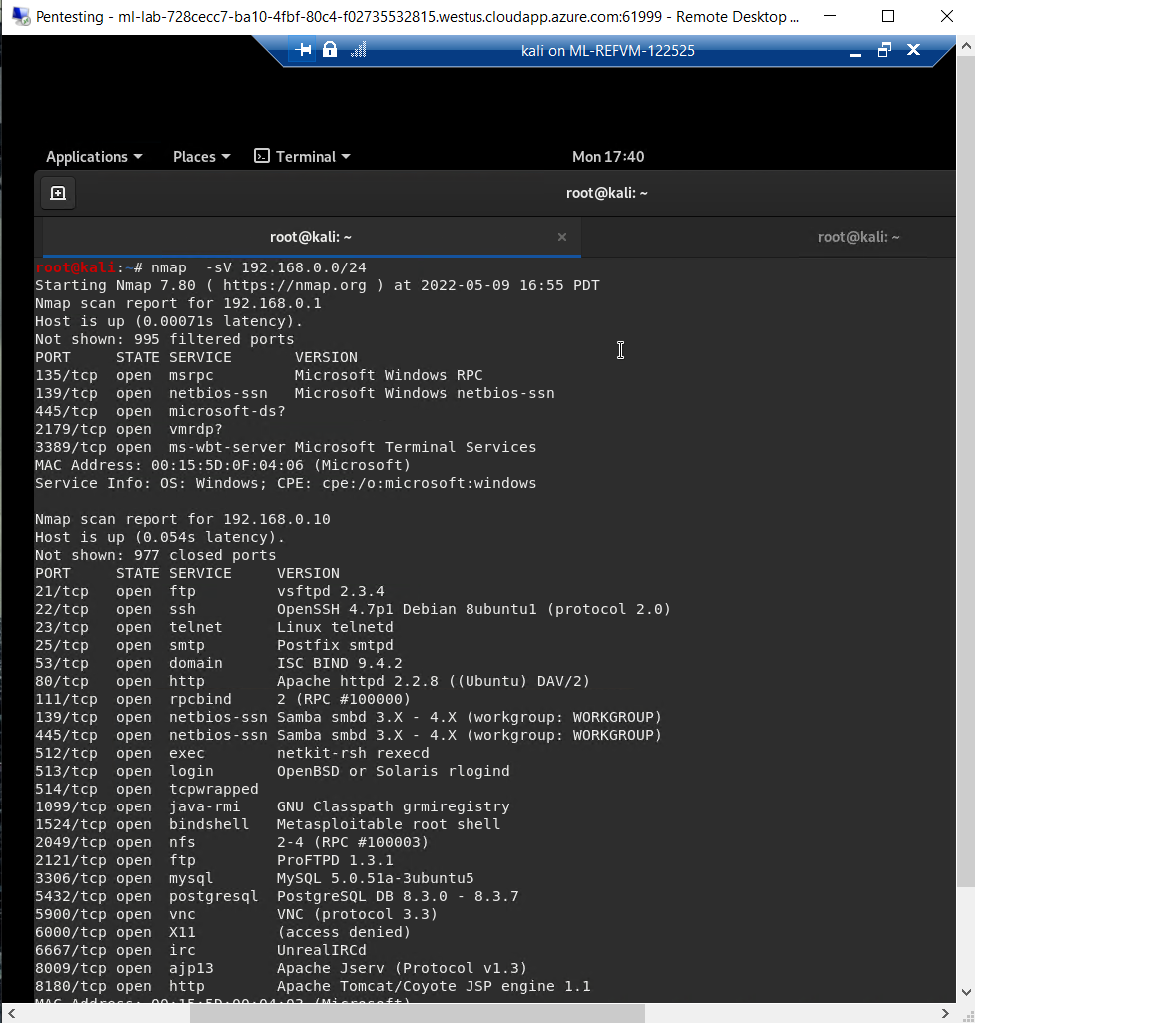
The remote web server runs Icecast version 2.0. 1 or older. Such versions are affected by an **HTTP header buffer overflow** vulnerability that may allow an attacker to execute arbitrary code on the remote host with the privileges of the Icecast server process

Severity:

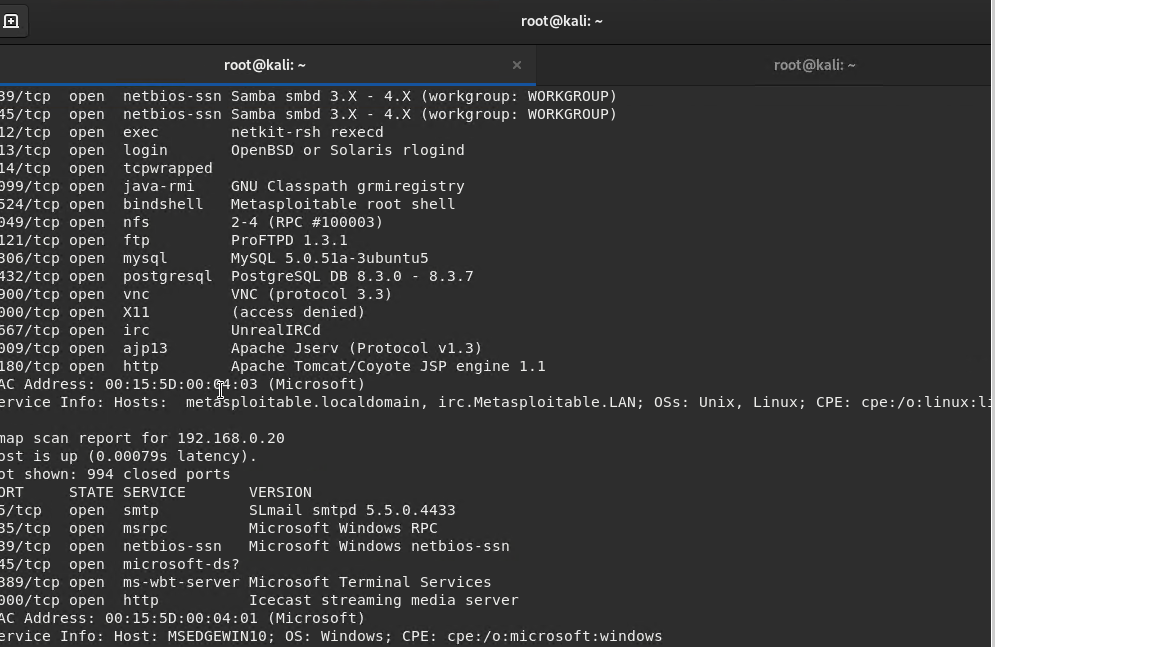
Critical

Proof of Concept:

1. First a network scan was ran on the system in order to figure out open services and OS.

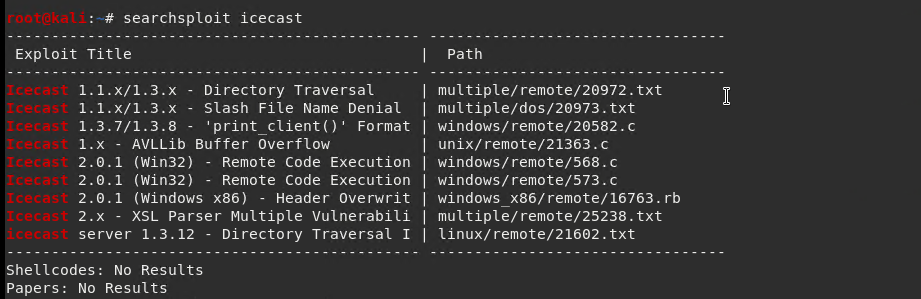


Then we see that CEO’s system has icecast vulnerability running.



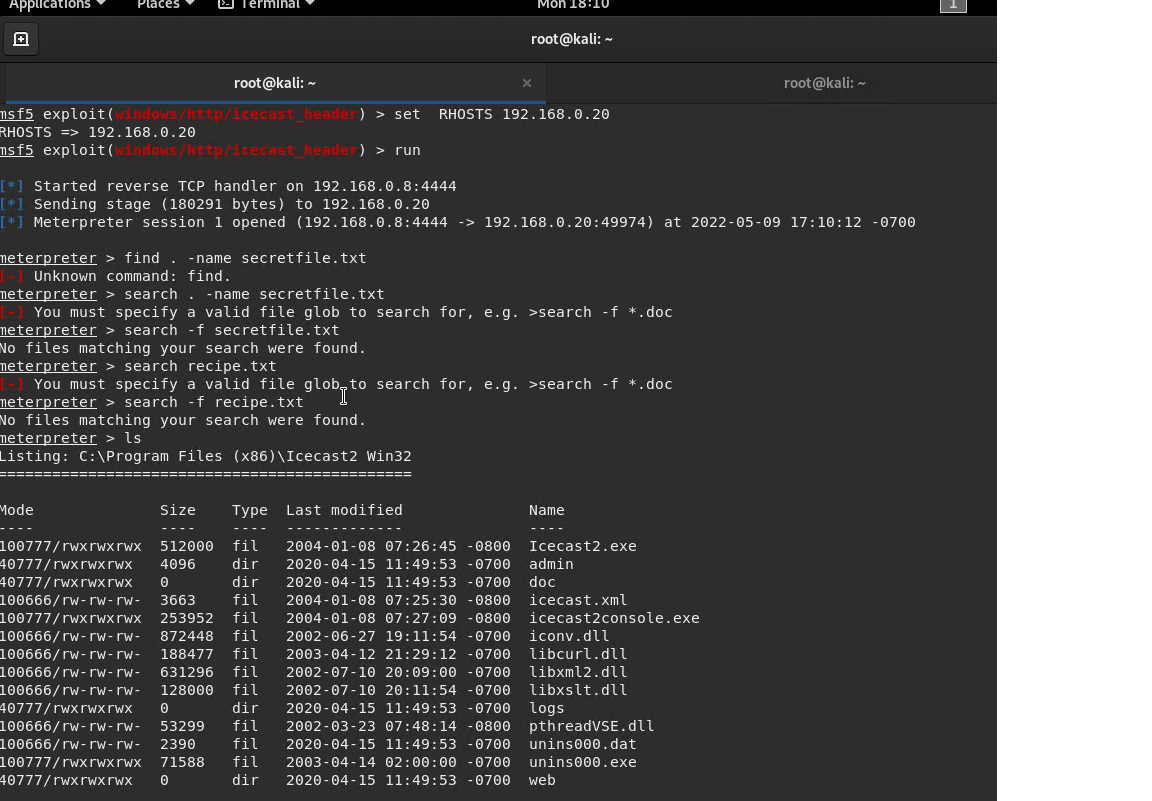
Therefore were able to pinpoint the ip and OS version of CEO System.

1. Then we Searched for exploits to me ran on CEO



Thus, remote code Execution was chosen since icecast give access to all the files.

1. We, Ran a exploit by msfconsole.



We were able to exploit the session and we were in the system.

There should be a separate finding for each vulnerability found!

# Recommendations

What recommendations would you give to GoodCorp?

* Turn the port 8000 off.
* Change the password policy to complex.
* Two factor authentication.
* Encrypt secret, recipe files.