GoodSecurity Penetration Test Report

TRISH.HARDING[@GoodSecurity.com](mailto:YOURNAMEHERE@GoodSecurity.com)

07/18/202

**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:

exploit/windows/http/icecast\_header

Vulnerability Explanation:

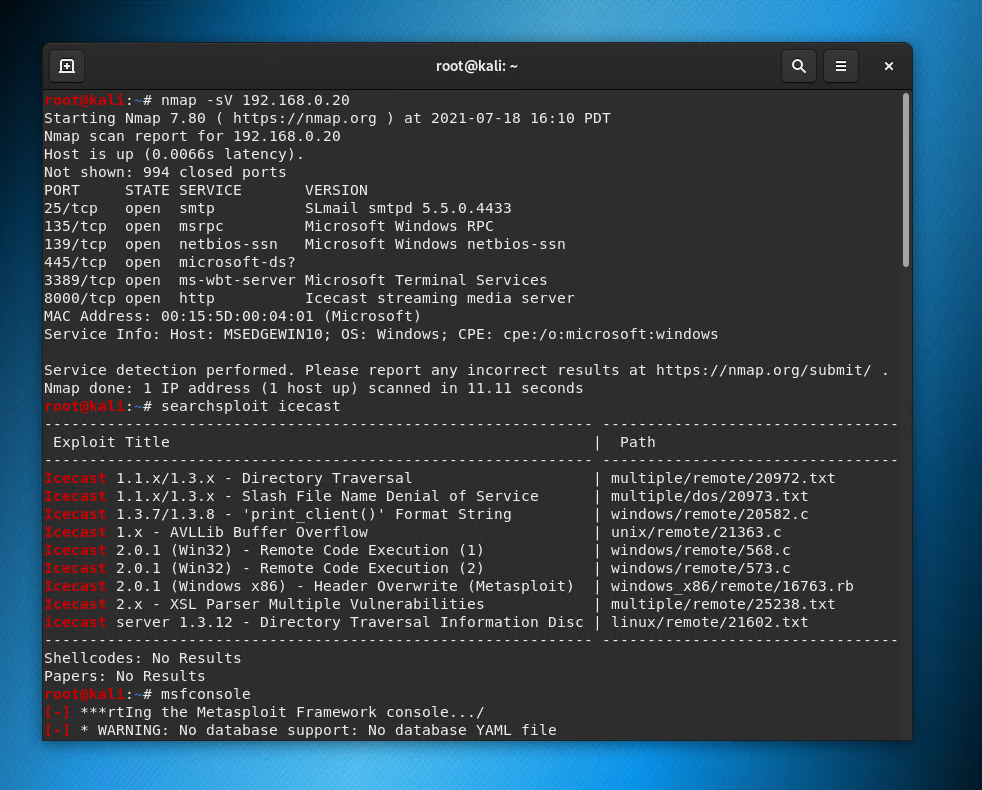
This exploit uses a buffer overflow. This causes too much data to go into the header.

Severity:

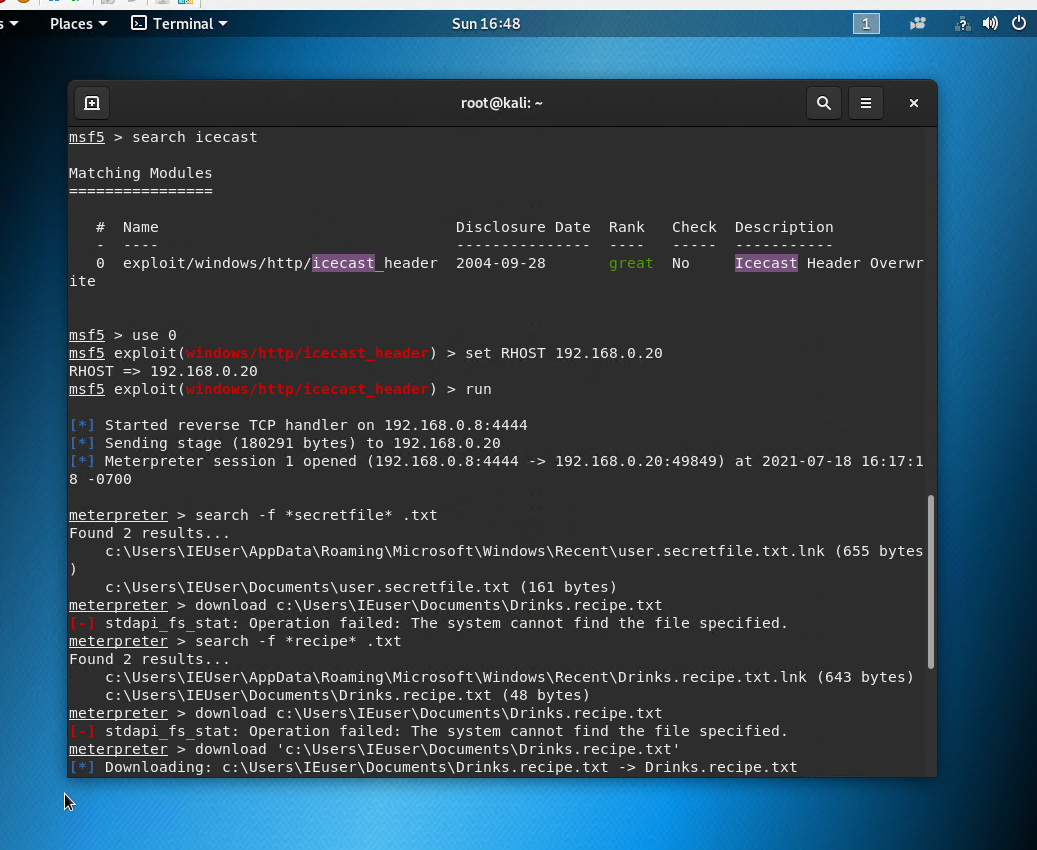
This is a very serious vulnerability as it can allow for privilege excalation and access to private information/data. Attacks like this can also lead to someone gaining privilege access which can affcet the organization financial.

**PROOF OF CONCEPT:**

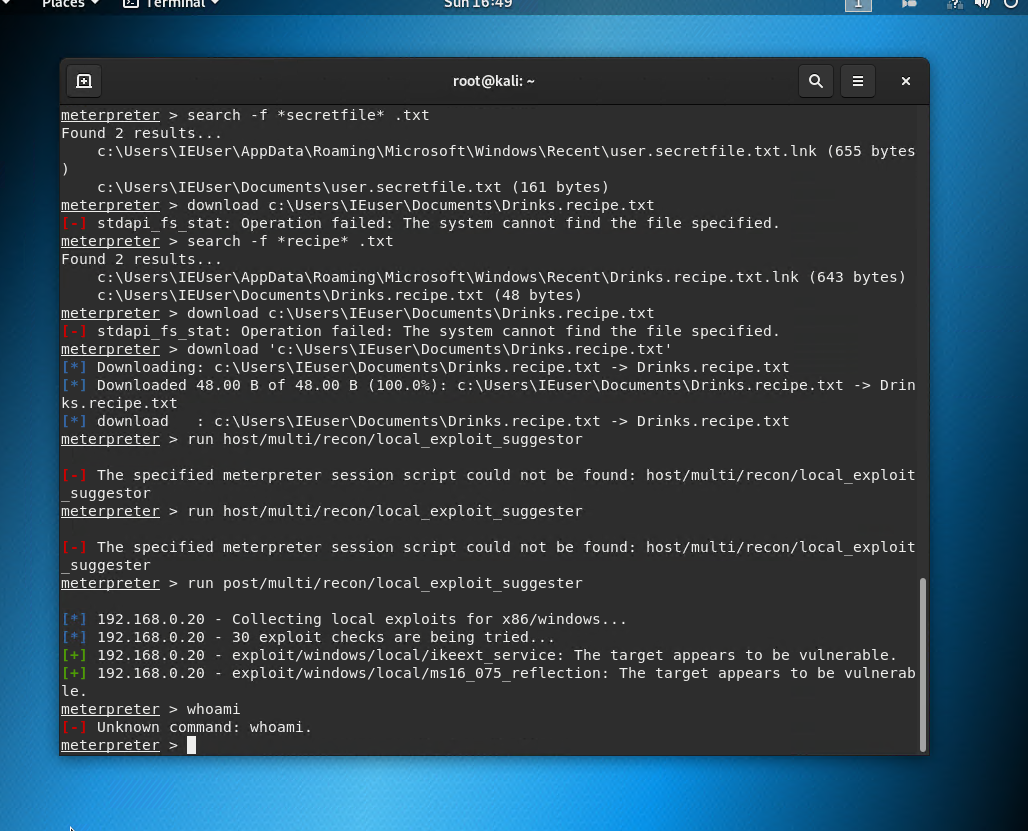
Step 1: Here I ran the nmap command to search for open ports and services. It also showed me the device’s name.



Step 2: I searched for an IceCast exploit and ran the exploit which we pointed out earlier.



3. I then searched for secret files and recipes. I was able to download these files with ease. After that I ran an excploit suggester to find other weaknesses.



**Reccomendations:**

Images provided show how we accessed a vulnerable machine and obtained important, secret files.

I would suggest the implemantation of firewalls as well as the following:

1. Make use of SIEM products. These offer an array of ways to monitor and strengthen your network and device security.
2. Update the progamming, use more secure code in developing.
3. Use the implementation of stack canaries. When a stack canary is overflowed, it creates a warning and it terminates the program.