GoodSecurity Penetration Test Report

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

April 22, 2021

# 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:

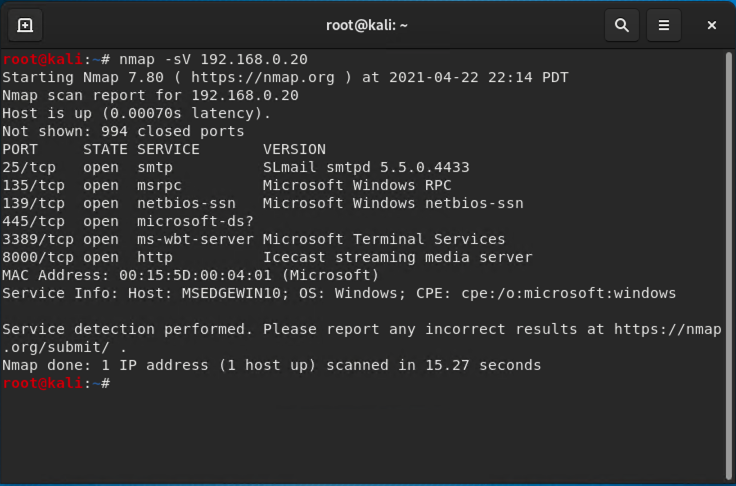
exploit/windows/http/icecast\_header

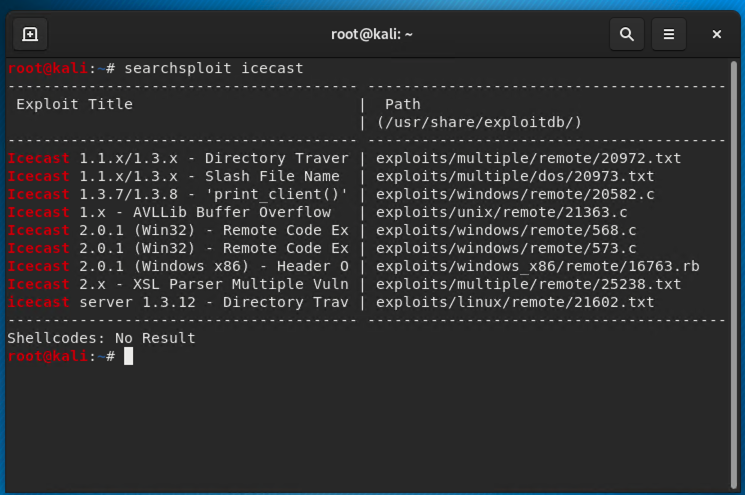
Vulnerability Explanation:

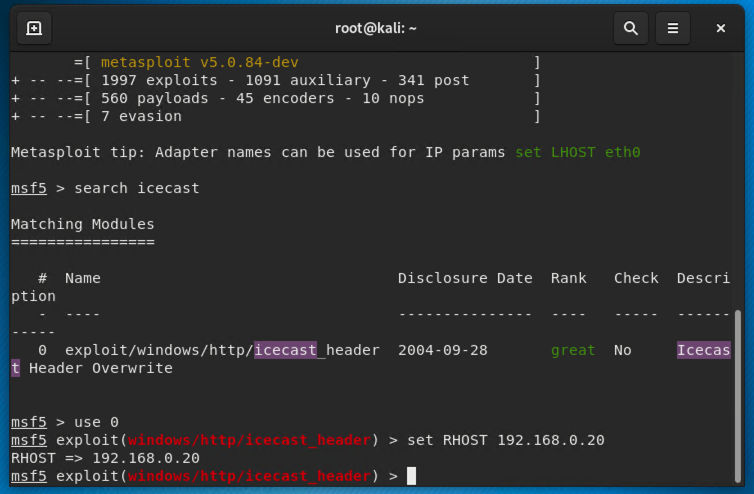
VE-2004-1561-Buffer Overflow vulnerability in Icecast Server HTTP HeaderSeverity

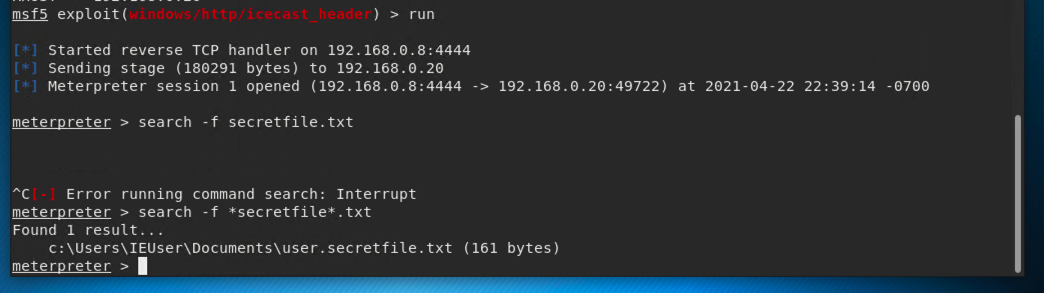
A buffer overflow is an exploit that takes advantage of a program that accepts input from a client or other software process. It can damage files, change data and potentially unveil private information. With that said it’s a Severe vulnerability and Goodcorp needs to do everything it can to mitigate it.

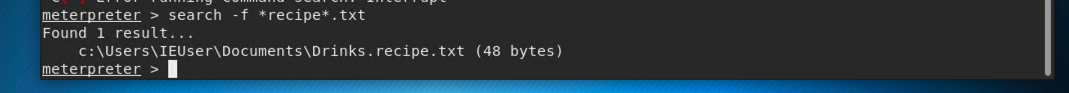
Proof of Concept:

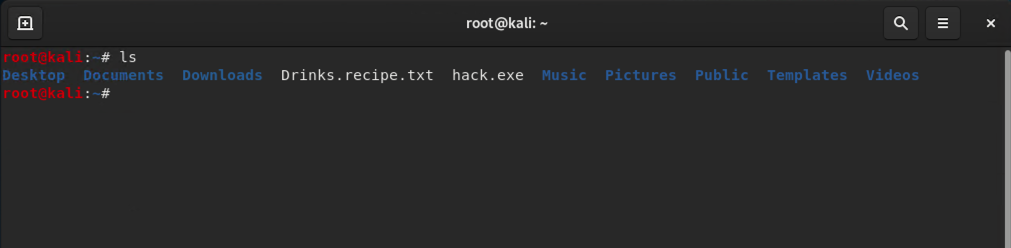


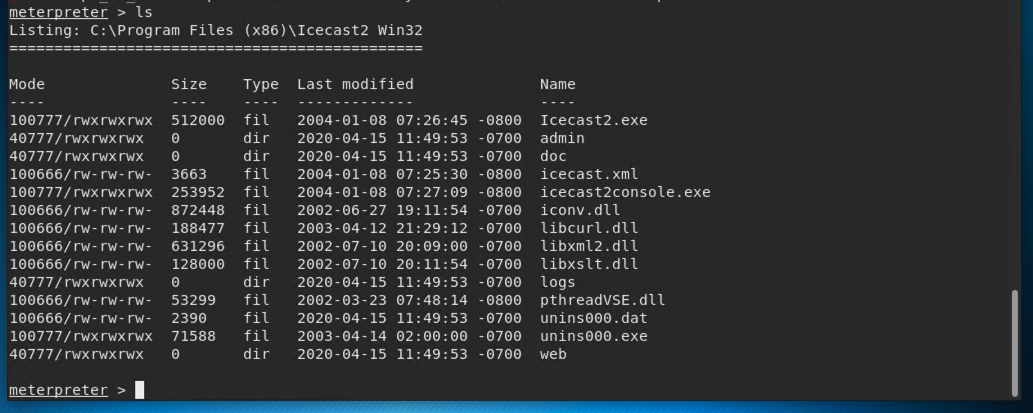


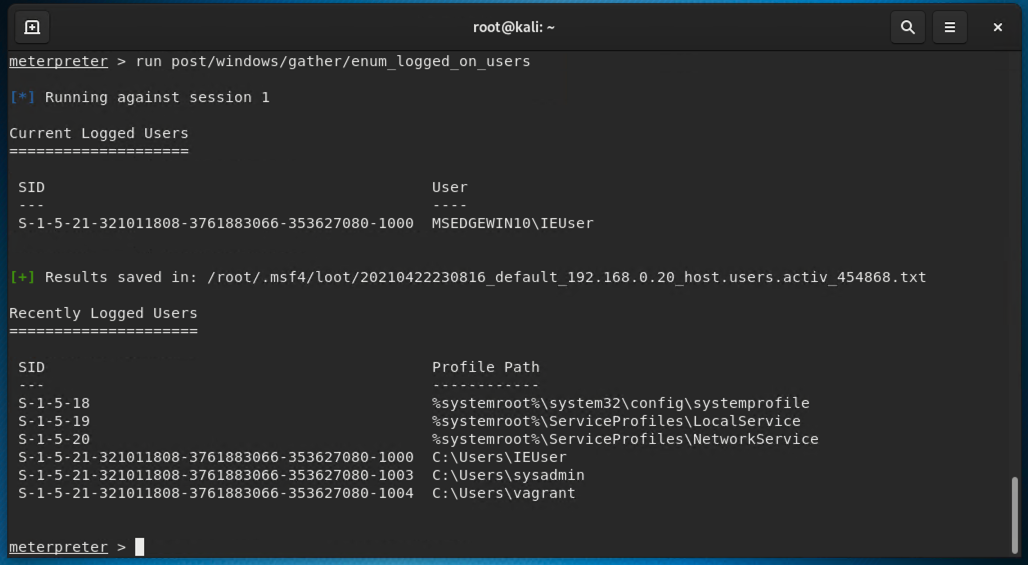


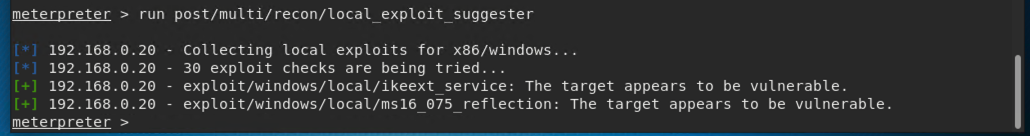


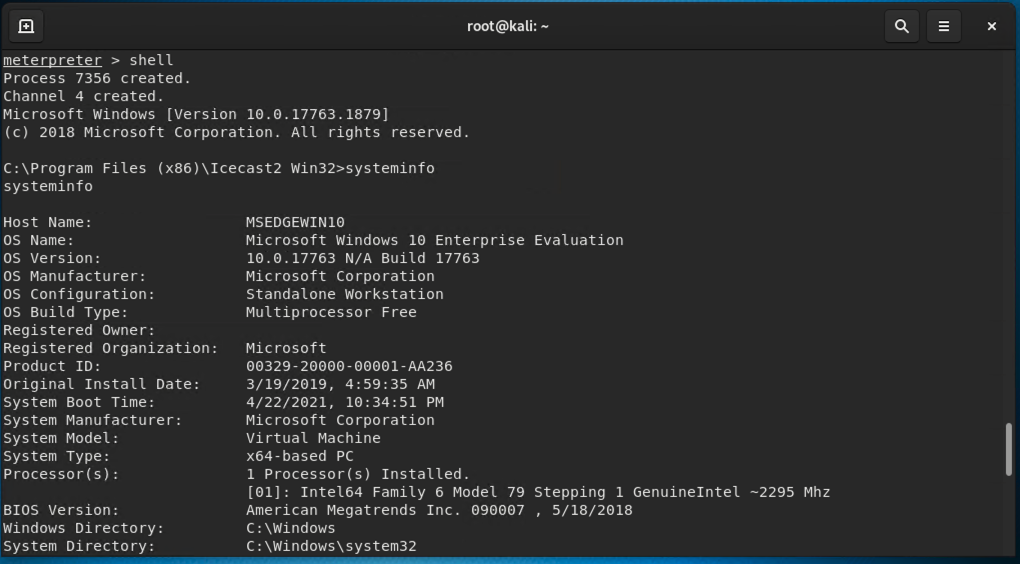












# Recommendations

What recommendations would you give to GoodCorp?

1. Update Icecast to the most recent version
2. Patch any outdated systems
3. If problems continue, consider the idea of removing Icecast and switch to a different vendor