GoodSecurity Penetration Test Report

[Benjiman.Spratt@GoodSecurity.com](mailto:Benjiman.Spratt@GoodSecurity.com)

20/09/2021

# 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 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\IEUser

Vulnerability Exploited:

icecast\_header

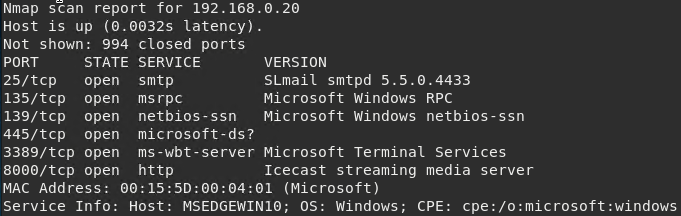
Vulnerability Explanation:

Explain the vulnerability as best you can by explaining the attack type (i.e. is it a heap overflow attack, buffer overflow, file inclusion, etc.) and briefly summarize what that attack is. You may need to do extra research online.

Severity:

9.0 Critical

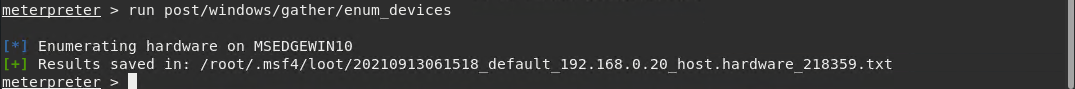
Proof of Concept:

Started by scanning a range of IP to identify open ports that can be exploited. 

After identifying an open port that can be exploited (port 8000) we can utilize Metasploit to run a prepared script. Set the target host and run. Text

Description automatically generated

From here we have full access of the targets computer. We can run a shell and search through the system that way, or we can use programs to exfiltrate information we find valuable like system info.

This gathers all the system data and writes it to a text file on the attackers computer for later use.

# Recommendations

To start with I would recommend updating Icecast as this vulnerability is not present in the newest update. Ensure to keep up to date with all security updates of all programs