GoodSecurity Penetration Test Report

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

12/7/2021

# 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:**

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 (Might need Google’s help!)

**Severity:**

Medium severity

**Proof of Concept:**

First ran nmap on the workstation to see what ports/services were enabled.

Command: Nmap -vv -Pn -sV -R 192.168.0.20A black screen with white text

Description automatically generated with low confidence

Next, I searched using searchsploit for any vulnerabilities in the services returned from nmap

Command(s):

* searchsploit icecast (image 1)
* searchsploit slmail ( image 2)

Image 1

Text

Description automatically generated

Image 2

Text

Description automatically generated

Next, I used Metasploit to test if any of the found vulnerabilities could be used to compromise and gain access to the workstation.

Text

Description automatically generated

Text

Description automatically generated

Set the RHOSTS to the workstations IP address

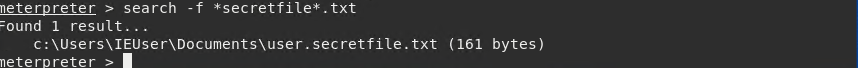
Text

Description automatically generated

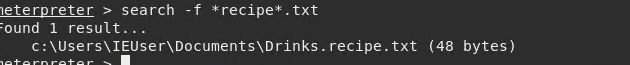
Showing that I have accessed the workstation through the Icecast exploit.Text

Description automatically generated

Secret File is located



Recipe file is located



# Recommendations

Update the Icecast HTTP server to a version that has the exploit remediated or remove the Icecast program if it is not needed.