GoodSecurity Penetration Test Report

[CHRIS DEARMOND@GoodSecurity.com](mailto:CHRIS%20DEARMOND@GoodSecurity.com)

10/8/2020

# 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:

/exploit/windows/http/icecast\_header

Vulnerability Explanation:

This exploit uses a buffer overflow, overwriting the saved instruction pointer and tricking icecast into thinking a thread is in use and allowing for remote code execution. This can result in a Metasploit session being initiated with full root access to the affected system.

Severity:

This exploit runs about an 8/10 in terms of vulnerability as it is highly dependent on the targeted users system access level.

Proof of Concept:

Starting with the known IP I ran a nmap scan against the target machine and was able to find the following information about the system, what ports were open, and what services were running on each port.

Text

Description automatically generated

Utilizing this information, I discovered that the system was running an Ice Cast server on port 8000. Ice cast looked interesting since it was a media server so I ran searchsploit to see if I could find any vulnerabilities and found nine.

Text

Description automatically generated

As we can see in the results we have one that can be utilized using Metasploit. After launching Metasploit I searched for exploits regarding icecast and found one.

Text

Description automatically generated

Using this I setup Metasploit to utilize the icecast vulnerability and was able to create a meterpreter session to the CEO’s terminal. (Meterpreter is a program that allows the user to send remote commands to the terminal without leaving a record of having access).

Text

Description automatically generated

Now that we have a session established I wanted to see if I could find anything labeled secretfile.txt, assuming that the CEO would have something like this. And viola:

Text

Description automatically generated

Since downloading trade secrets from the terminal was not in the scope of work for this Pentest, I decided to see if I could find something a little more innocuous, such as a recipe file. Once I found a file named Drinks.recipe.txt I was able to download the file showing that I had access to the CEO’s systems.

Text

Description automatically generated

Now I wanted to see just how deep our access could go, so I decided to see if I could get a list of users that had been recently logged in. This would also show that there was no record of our being in the system.

Text

Description automatically generated

As further proof of complete access to the terminal I started a shell (a remote Windows Command Prompt) and pulled

the system info.

Text

Description automatically generated

# Recommendations

I would highly recommend having training with your CEO regarding best security practices and policies as well as have him remove Ice Cast from the work terminal as soon as possible. As well, it would be advisable to create a policy banning all third-party software use that is not explicitly approved by the IT department.