GoodSecurity Penetration Test Report

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

10/30/2021

# 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:

The name of the vulnerability that was used is Icecast Header Overwrite.

Vulnerability Explanation:

The vulnerability is a buffer-overflow attack. The attacker sent 32 HTTP headers to the Icecast server. This allows an attacker to execute arbitrary code on the target machine. The exploit is less well-defined on Linux machines.

Severity:

This exploit is high severity. The attacker was able to access the supposedly “secret” files on the target machine, all logged on users retrieve the plaintext password for the machine’s Administrator account.

Proof of Concept:

In order to determine Hans’ IP address, I will see what subnet the computers are connected to. From the attacker’s machine, I ran the ifconfig command, which yields the following results:

The results of the command indicate the attacker machine has the IP address 192.168.0.8, and a subnet mask of 255.255.255.0, which means the computers are connected to the subnet [192.168.0.0/24](http://192.168.0.0/24).

With the network IP I can now run a nmap command to discover computers connected to the network. I ran the following command (from the attacker kali machine):

  nmap -sV [192.168.0.0/24](http://192.168.0.0/24)

 A service and version scan indicated Hans’ machine is running the Icecast streaming media server, which is a potential vulnerability. I then used the searchsploit command to search the exploit database (“exploitdb”) to find any potential exploits.

From here, I entered the Metasploit console (“msf”). I loaded it into the Metasploit framework, and configure it to attack Hans’ computer at the IP address

discovered by nmap.

After configuration, I ran exploit to run the actual exploit and open a meterpreter shell. Once in meterpreter, I can search for files on the target system using the search command.

Once I have the password hashes on our attacker machine, I can use the program John the Ripper to crack the hashes and output plaintext passwords. The plaintext password for the Administrator account is Passw0rd!.

# Recommendations

To fix this vulnerability, it’s recommended that Hans’ update Icecast to the most recent version. GoodSecurity recommends that Hans stays alert about keeping his software up to date, to minimize the threat of a similar vulnerability.

Additionally, Hans advised GoodSecurity that the passwords “are long and complex and therefore unhackable.” This turned out to be false. This reporter was able to crack the Administrator password on Hans’ machine using a publicly available wordlist. GoodSecurity recommends GoodCorp update its password policy to require more complex passwords, ideally ones that contain no dictionary words.