**GoodSecurity Penetration Test Report**

JamesSwift@GoodSecurity.com

04/29/2021

1. 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.

2. Findings

Machine IP:

192.168.0.20

Hostname:

MSEDGEWIN10

Vulnerability Exploited:

exploit/windows/http/icecast\_header

Vulnerability Explanation:

Icecast header is a buffer overflow exploit that can exploit Icecast versions 2.0.1 and earlier. This exploit sends 32 HTTP headers to the target machine (1 over the typical array), which causes the target to overwrite its default instruction pointer on windows systems. The extra HTTP header will cause Icecast to think that one of its default threads (which is actually a malicious payload) is still running and thus not decrease or reset the thread counter while the exploit is in effect. This gives an attacker ample time to execute their payload on the target machine.

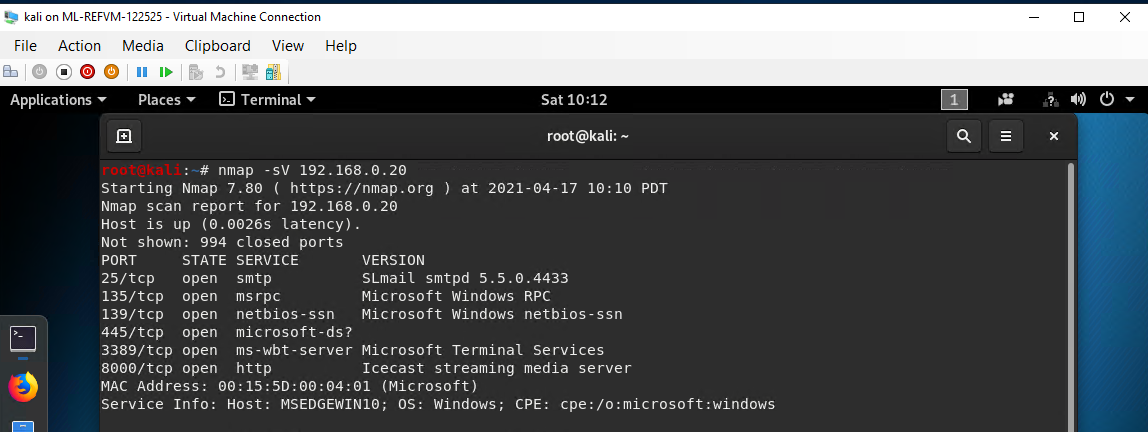
Severity:

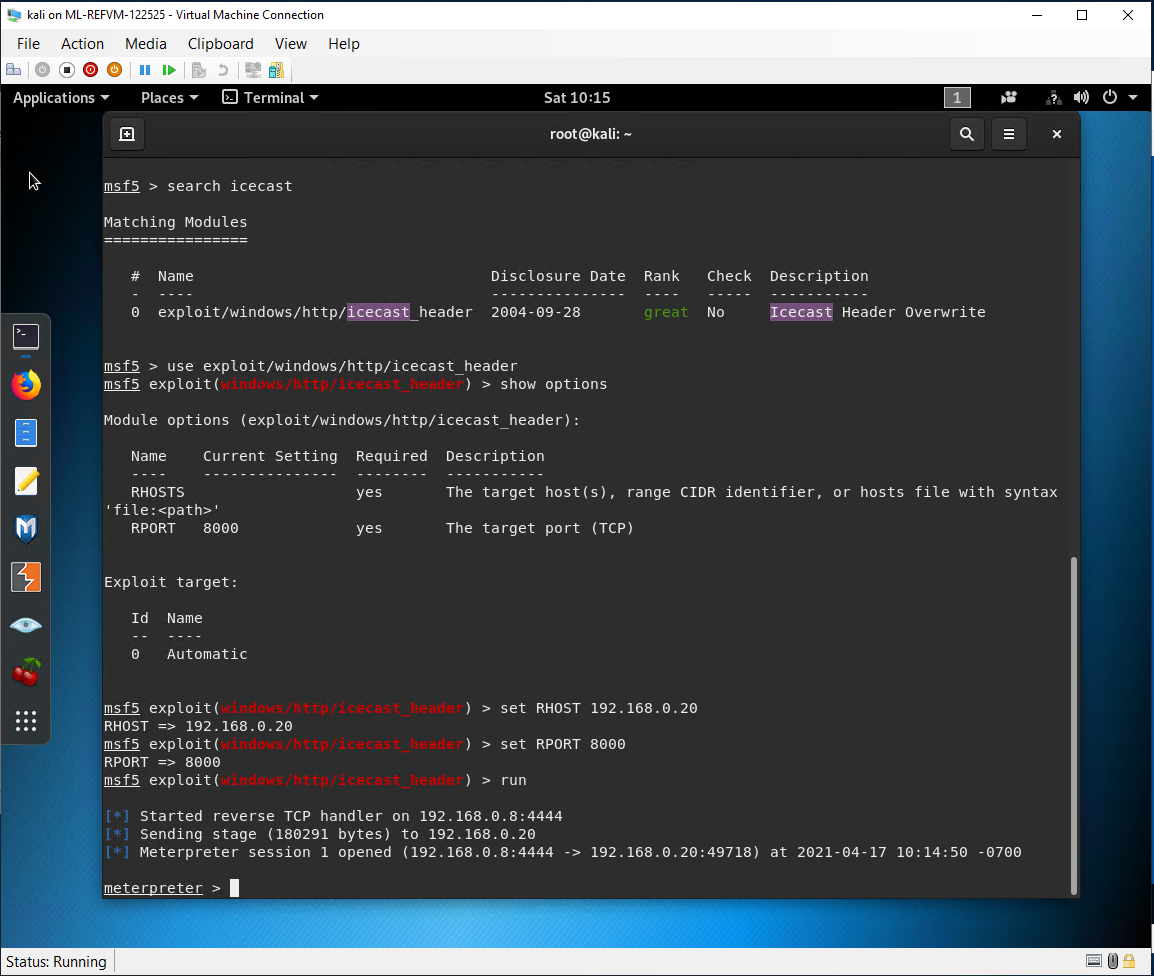
This is a very severe vulnerability. Skilled hackers that are able to utilize this exploit can easily access the target machine and have plenty of time to use their payload to inflict significant damage or obtain sensitive data from that machine. Having strong password requirements is not enough to defend against this exploit, as it enables hackers to access the machine without even having to enter a password.

Proof of Concept:

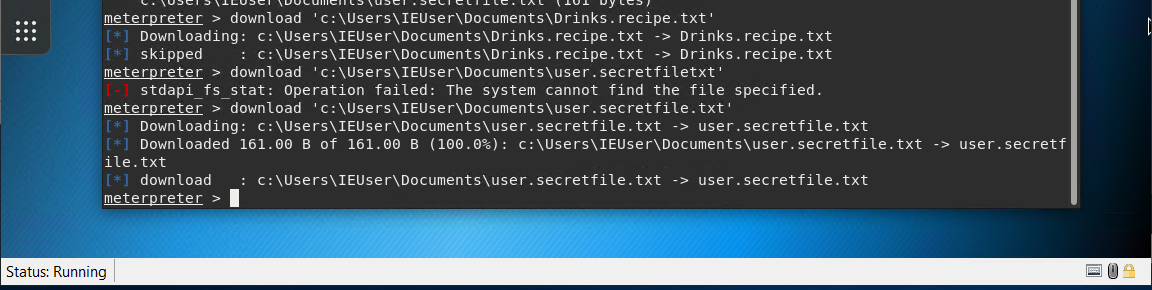
In using the Icecast Header exploit, I was able to access the target machine and obtain a great deal of sensitive data and material, including USER ID’s and system specs. I was also able to download and extract the secret recipe files to my local machine. The screenshots below show the steps I took to access the machine using the Icecast\_Header exploit and expose numerous vulnerabilities and obtain sensitive data.

In the below image, I performed an nmap scan of the target machine (IP: 192.168.0.20) and discovered that its Icecast port (8000) was open and thus vulnerable to the icecast exploit.

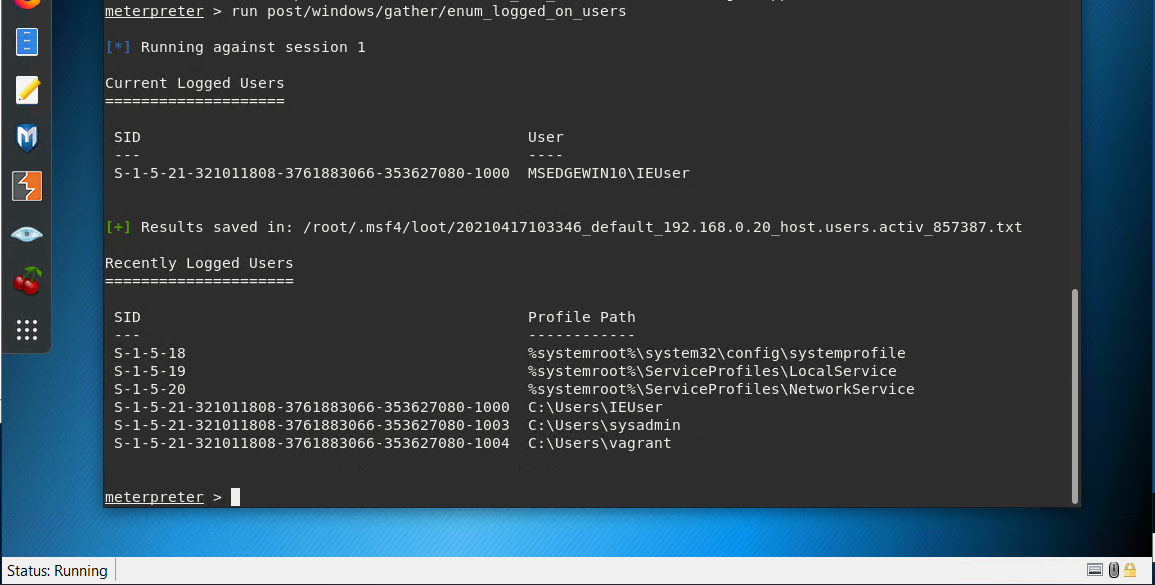


After performing the nmap scan, I then pulled up the necessary exploit and set the parameters to that of the target machine. I then successfully ran the exploit and established a meterpreter session with the target machine without even having to enter a password.

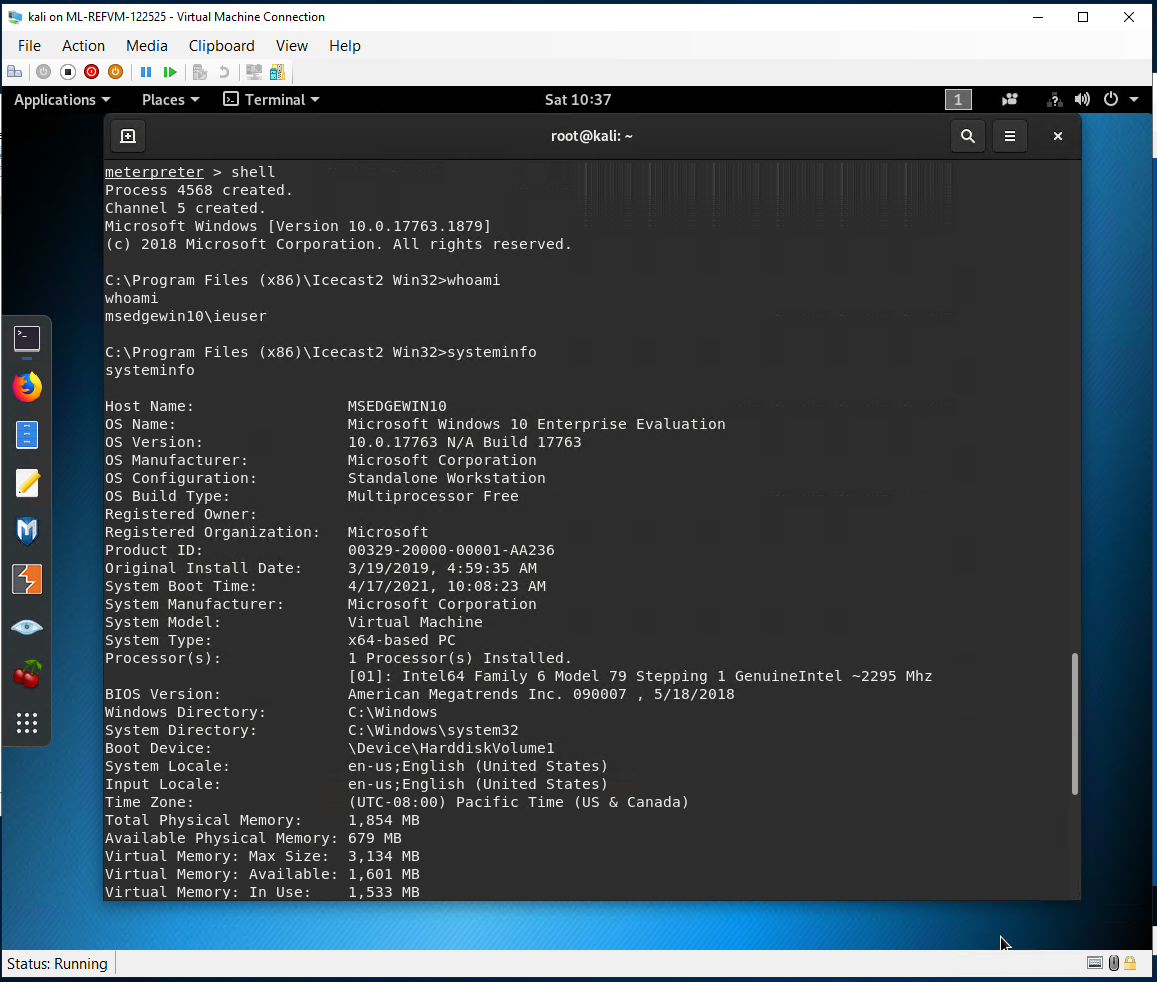
Once I successfully exploited the machine, I was then able to look up the requested sensitive data (secretfile.txt and recipe.txt files), and I was even able to download them to my local machine as shown below.

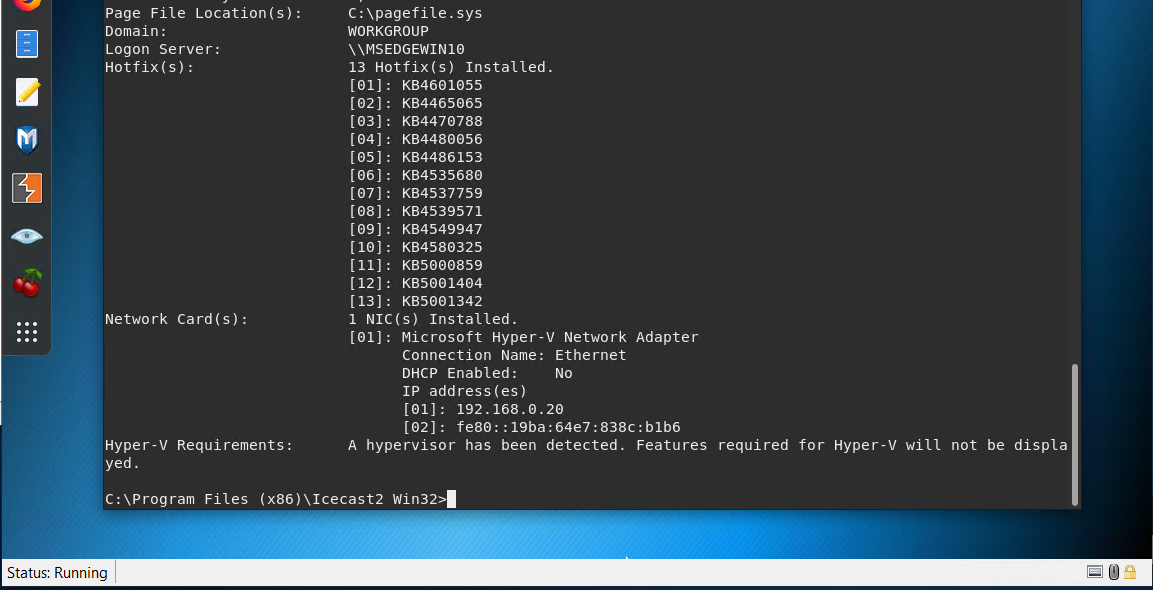


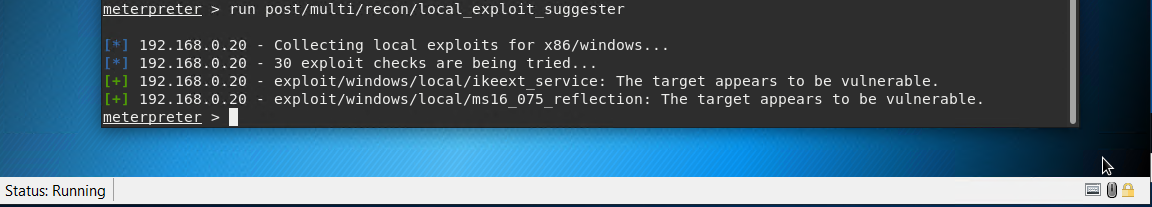
I also gathered the data of all users that were currently logged on or had access to this machine as shown below.



I was also able to get even deeper into the machine using a meterpreter shell. I could then use this shell to obtain virtually all specs and components of the machine as pictured in the following two pictures below.





I also used metasploit’s local exploit suggester to find additional vulnerabilities besides the icecast header that could also be exploited. The first one listed is “ikeext\_service”, which indicates a missing DLL that a hacker could exploit with their own DLL loaded with a malicious payload. The other one listed, “ms16\_075\_reflection”, indicates a vulnerability in the machine’s security system in which an attacker could gain access through a shell and easily elevate their privileges to gain a SYSTEM handle with full access to all data and privileges on the machine.

3. Recommendations

My top recommendation would be to upgrade their Icecast server to a newer version (preferably the latest one) to help remove this vulnerability from any further exploits. For the ms16\_075\_reflection vulnerability, I’d recommend that they ensure their security systems are fully up to date to help get rid of these vulnerabilities. Microsoft has released patches that can help with this for most operating systems. For the ikeext\_service vulnerability, in addition to having up to date security software, some best practices include to avoid using Aggressive Mode while on the server as much as possible, avoid using pre-shared authentication keys (if unavoidable, ensure they’re very strong), and prohibit or at least limit as much as possible any VPN connections to the local network.