GoodSecurity Penetration Test Report

[Tricia Tambio@GoodSecurity.com](mailto:Tricia%20Tambio@GoodSecurity.com)

04/19/2021

# 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:**

exploit/windows/http/icecast\_header

**Vulnerability Explanation:**

The icecast\_header module is a buffer overflow attack.

This attack occurs when the Icecast program version 2.0.1 and earlier is executed which allows an attacker to send excessive HTTP headers (at least 32) causing a buffer overflow. This gives an attacker access privilege to execute any code on the remote web server.

**Severity:**

The severity of this Icecast vulnerability is very high. As mentioned previously, not only can an attacker execute arbitrary code, they can maneuver within the network, elevate their privileges to execute code or processes. Another vulnerability is a denial of service (DoS) attack which can cause a network to crash.

NOTE: We have found two other possible vulnerabilities that should be looked into.

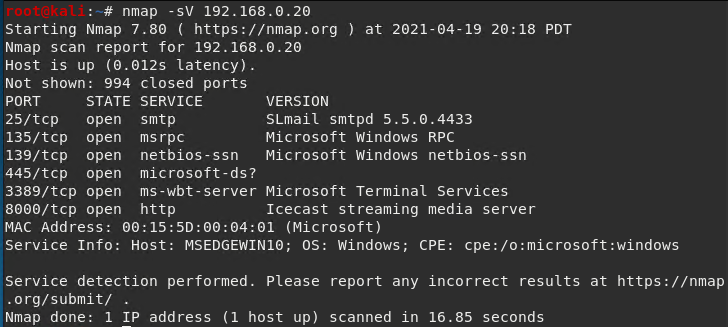
The ‘ikeext\_service’ exploit which affects the Windows Dynamic link library (DLL) specifically the IKEEXT (IKE and AuthIP IPsec Keying Modules) that allows an attacker to add malicious code into an application.

The ‘ms16\_075\_reflection’ exploit is a vulnerability in Microsoft Windows that could elevate a user’s privilege if a certain application is executed.

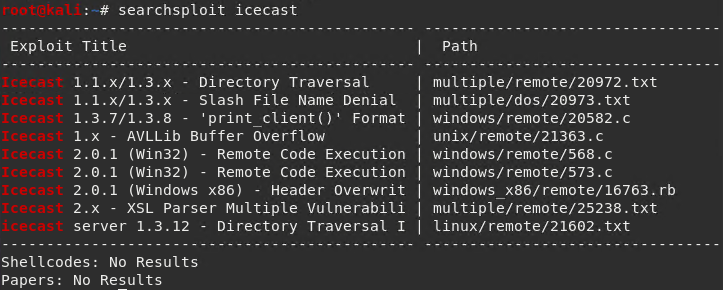
**Proof of Concept:**

Our penetration testing has found the following vulnerabilities on Mr. Gruber’s computer.

1. Identify ports, services and the operating system through a network scan.

****

1. Locate available Icecast exploits by using the command-tool Searchsploit.



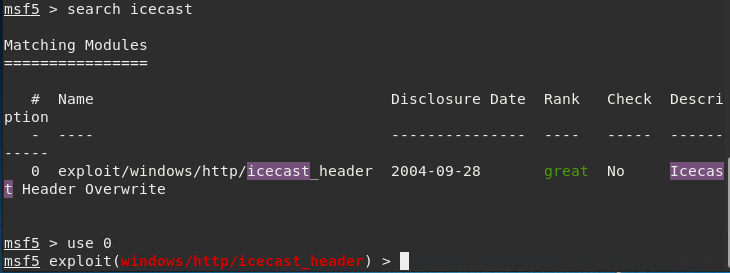
**Proof of Concept: (con’t)**

1. Exploit the Icecast module through the testing tool Metasploit.

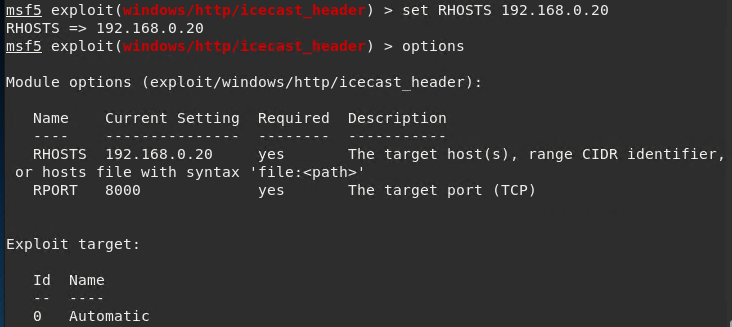
We opened up a Metasploit console on our test machine.



Located an Icecast module to exploit.

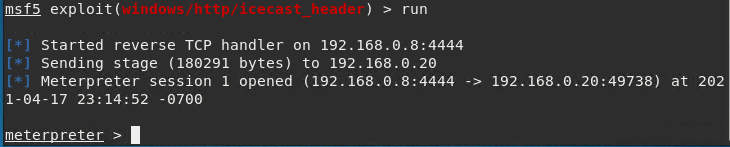


We were able to set the exploit to the target host (Mr. Gruber’s machine).



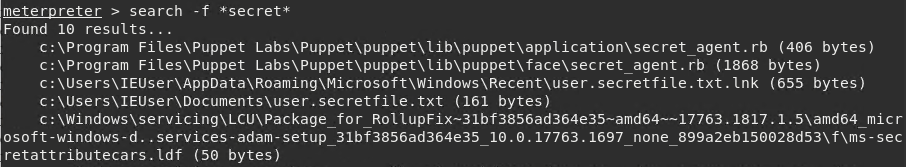
We are ablet to ‘listen’ through host 192.168.0.8 on port 4444.

**Proof of Concept: (con’t)**

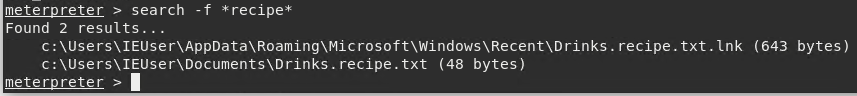


* From here, we have access to the Meterpreter session shell to execute arbitrary commands, navigate through the network, etc.

1. Search and find the location and exact name of the ‘secret’ and ‘recipe’ files.



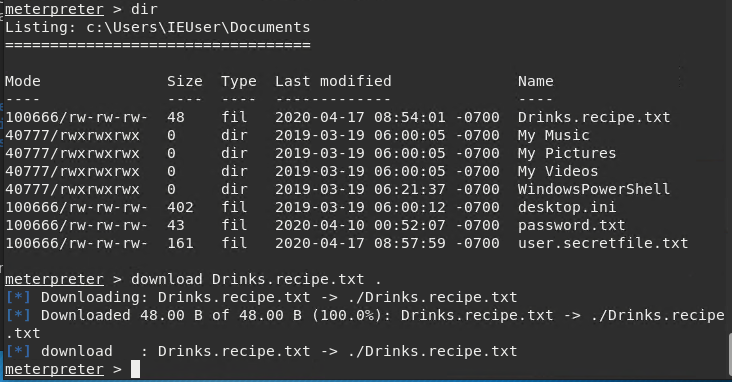
* The ‘user.secretfile.txt’ is located at ‘c:\Users\IEUser\Documents’.



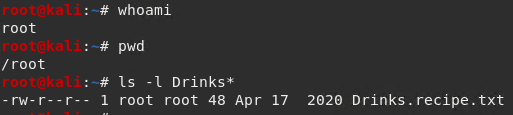
* The ‘Drinks.recipe.txt’ is located at ‘c:\Users\IEUser\Documents’.

**Proof of Concept: (con’t)**

1. Download the ‘Drinks.recipe.txt’ file from ‘c:\Users\IEUser\Documents’ into our current directory on our test machine.



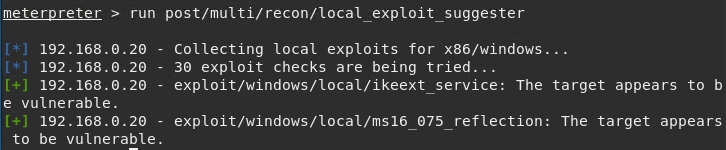
The file was downloaded to ‘/root’.



**Proof of Concept: (con’t)**

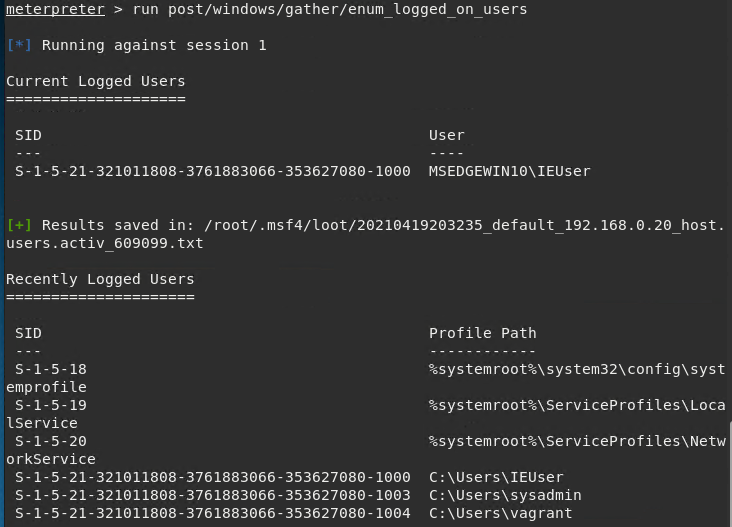
1. Locate other possible exploits using Meterpreter’s local exploit suggester.

Search found two possible exploits.



* The ‘ikeext\_service’ exploit.
* The ‘ms16\_075\_reflection’ exploit.

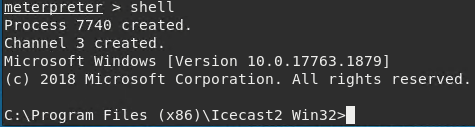
1. Scan logged on users.



**Proof of Concept: (con’t)**

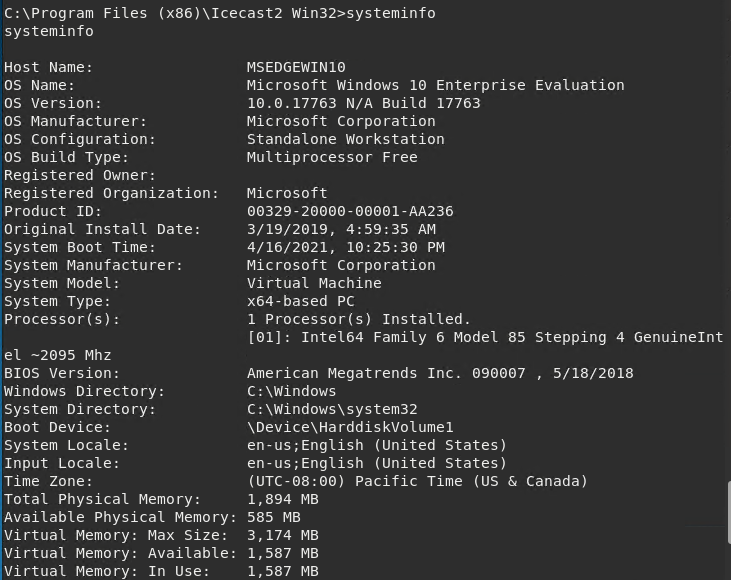
1. Retrieve system information from a shell prompt.

Open a shell prompt from Meterpreter:



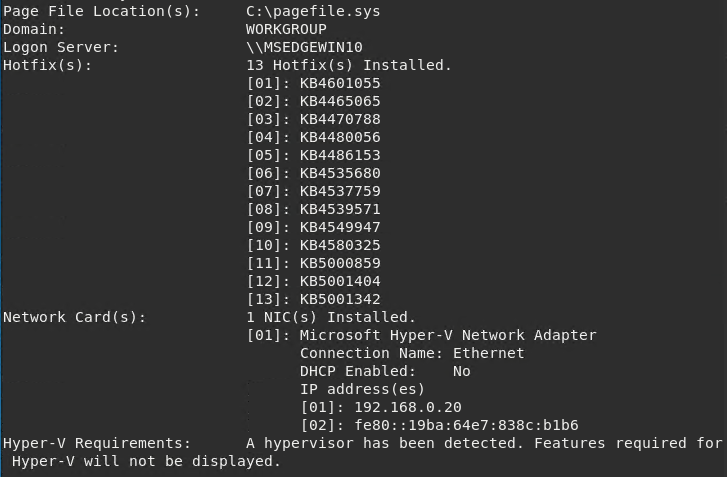
**Proof of Concept: (con’t)**

System information:



**Proof of Concept: (con’t)**

System information: (con’t)



# Recommendations

One of the major vulnerabilities that we have detected through the use of the Metasploit Framework is the Icecast exploit. We were able to use the Icecast header module to infiltrate Mr. Gruber’s computer. From there we were able to find sensitive files, download a file, find out information about the system and open up a shell prompt which allowed us to navigate through his system.

Two possible vulnerabilities that we have also detected are the Windows IKEEXT DLL and Windows MS16-075.

GoodCorp has recommended the following actions to prevent, deter or correct these vulnerabilities that were found.

One of the easiest ways to prevent any vulnerability is to make sure the latest version of Icecast, a Windows application or any software is being used. Always perform updates and/or patches from the vendor on a regular basis.

Make sure a firewall is being used. An intrusion detection system should be installed, such as Microsoft’s tool called Process Monitor, that monitors running processes on a network or computer and can detect possible vulnerabilities.

To prevent a privilege escalation attack, make sure password policies are enforced and limit access or permissions to sensitive information to those that need it. Don’t use default usernames/passwords.

We were successfully able to do a service and version scan using nmap to see which ports were open. Restrict information that is being returned from any port scan. Use a firewall or TCP (Transmission Control Protocol) wrappers, close any ports that are not being used. Perform your own port scan to see if any of your ports are open and receiving or sending data.

In summary, one of the best preventions an organization can do to avoid attacks or exploits is to always update/patch all software, hardware, operating systems, firewalls, etc. on a regular basis. Firewalls and an intrusion detection system should be implemented and used. Employees need to be aware of social engineering. Policies and procedures should be enforced at all times.

These recommendations should help secure and protect any vulnerabilities with Mr. Gruber’s computer.