GoodSecurity Penetration Test Report

[Joe.Griffin@GoodSecurity.com](mailto:Joe.Griffin@GoodSecurity.com)

5/1/2022

# 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:**

*Icecast 2.0.1 (Windows x86) – Header Overwrite*

**Vulnerability Explanation:**

The Icecast Header Overwrite 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.

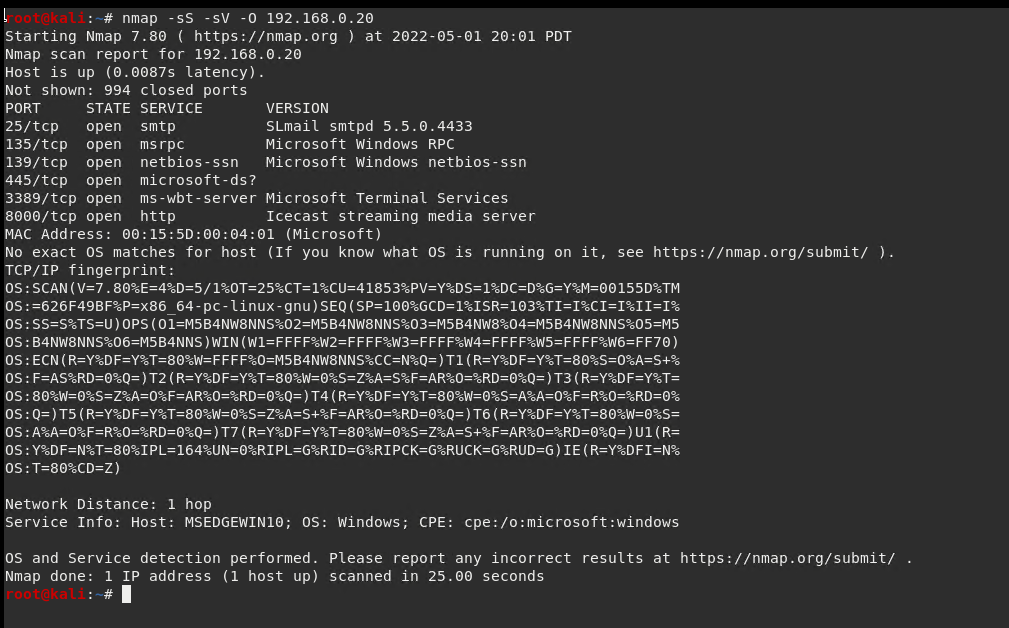
**Severity:**

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.

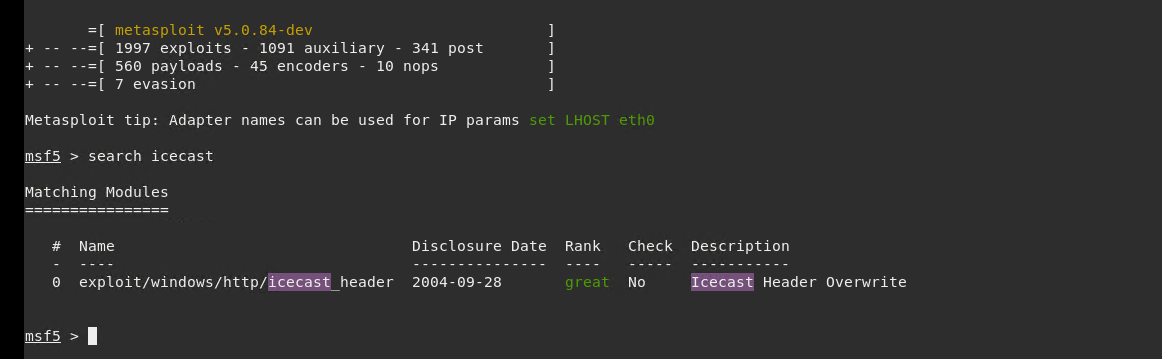
**Proof of Concept:**

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

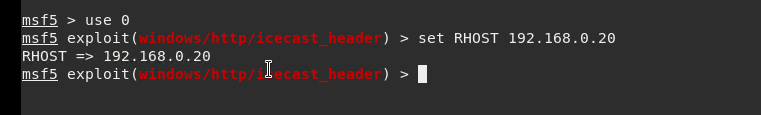
1. Identify ports, services and the operating system through a network scan.

****

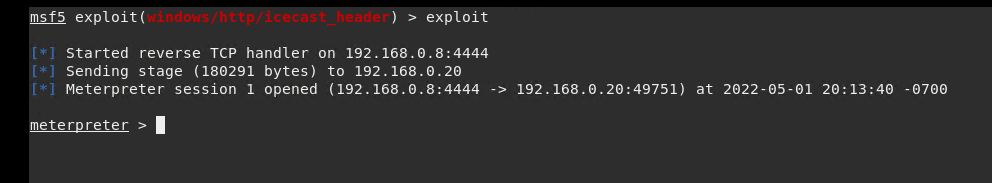
1. Exploit the Icecast module through the testing tool Metasploit.



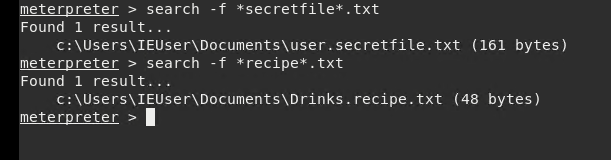
1. We were able to set the exploit to the target host (Mr. Gruber’s machine).



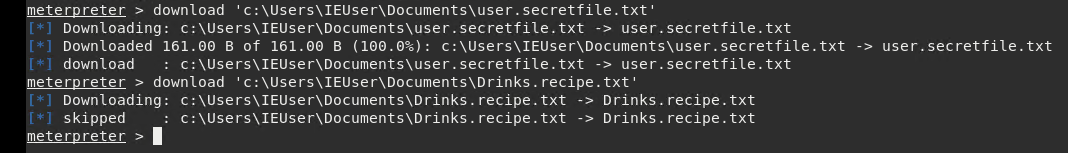
1. Running the exploit and connecting to target host (Mr. Gruber’s machine).



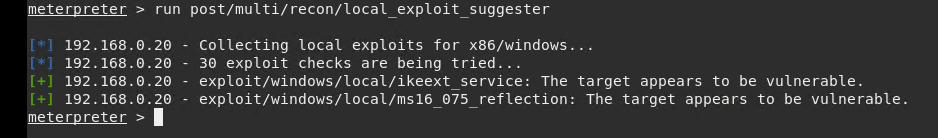
1. Search and find the location and exact name of the ‘secret’ and ‘recipe’ files.

****

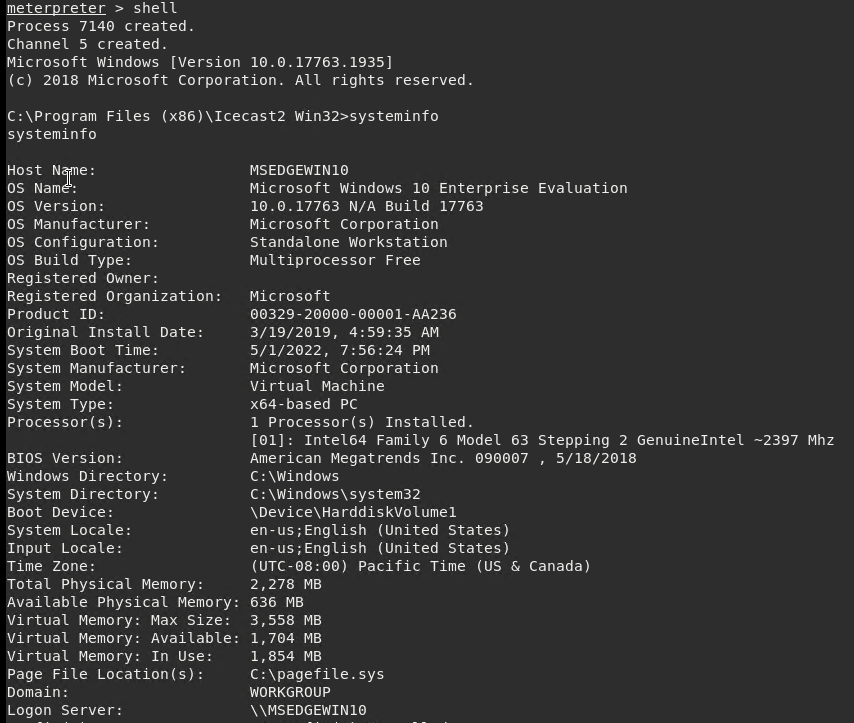
1. Download the files found in previous step to local machine.

****

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



1. Retrieve system information from a shell prompt.



# Recommendations

The Icecast Header Overwrite being the most severe of the uncovered vulnerabilities, I recommend first upgrading your Icecast to the latest version 2.0.2 or later.

The IKEEXT and the ms16\_075 exploits are more difficult to expose compared to the Icecast vulnerability but are potentially dangerous. To prevent an attack where the attacker can escalate their privileges, I recommend applying the available patches to resolve both vulnerabilities.

Regular updates to the system and ensuring the proper patches have been implemented will be necessary to keep your system hardened against any exposure to future vulnerabilities. Updating patches monthly are considered best practice and would be a great place to start.