GoodSecurity Penetration Test Report

[carl.conn@GoodSecurity.com](mailto:carl.conn@GoodSecurity.com)

04/28/21

# 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 – Nmap

Machine IP:

**192.168.0.20**

Hostname:

**MSEDGEWIN10**

Vulnerability Exploited:

**This is a simple NMAP scan of the target machine’s IP address**

Vulnerability Explanation:

**While this isn’t strictly an exploit, it does show what services are running and what ports are open to internet traffic.**

Severity:

**This vulnerability’s severity is quite low as NMAP scanning cannot be blocked if these services need to be exposed to the public internet. If these services do not need to be open to the public internet it would be best to make new firewall rules to block incoming packets so NMAP cannot collect data on ports or scan the operating system.**

Proof of Concept:

**Below the results of a simple NMAP scan can be seen. It reveals all open ports, services using those ports, their version, the hostname, and the operating system.**

Text

Description automatically generated

# Findings – Metasploit Icecast Header Overwrite

Machine IP:

**192.168.0.20**

Hostname:

**MSEDGEWIN10**

Vulnerability Exploited:

**Icecast Header Overwrite (CVE-2004-1561)**

Vulnerability Explanation:

**This exploit uses a buffer overflow to allow an attacker to execute code one the remote host with the privileges of the Icecast server process. To exploit this flaw the attacker sends 32 HTTP headers to the remote host to overwrite a return address on the stack.**

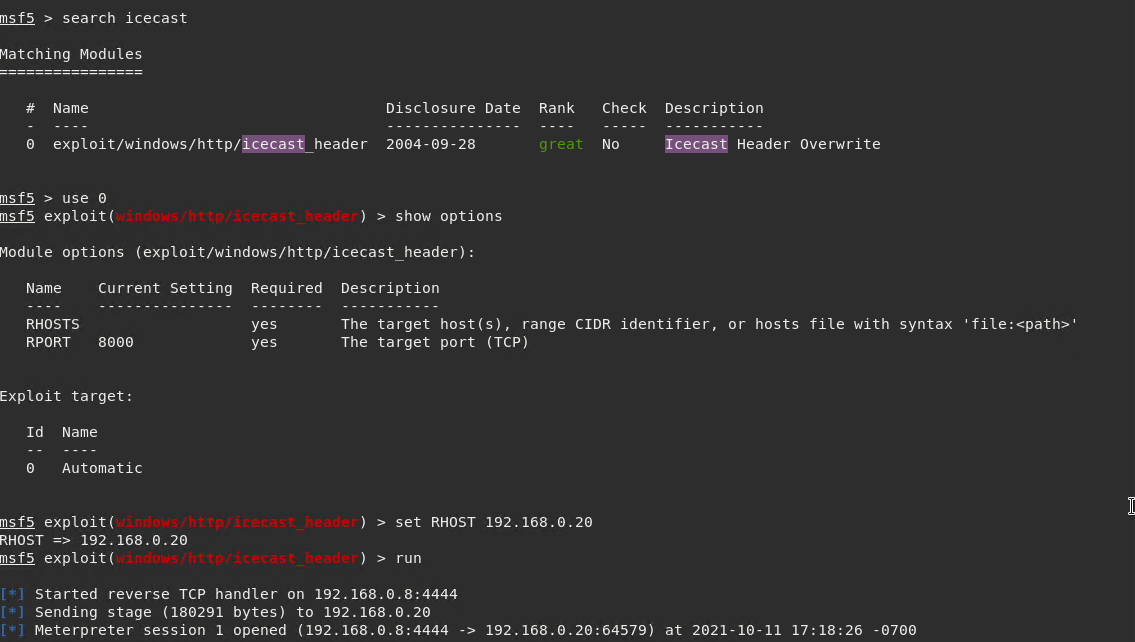
Severity:

**High**

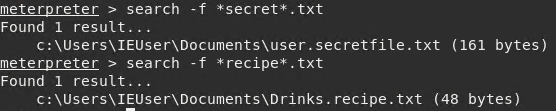
Proof of Concept:

**Start Metasploit Console**

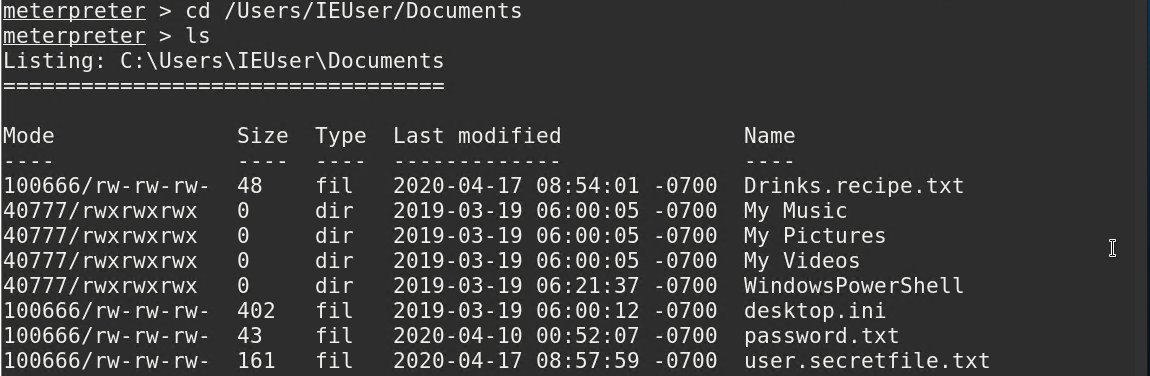


**Command to search for the Icecast module followed by the command to use the Icecast module:**

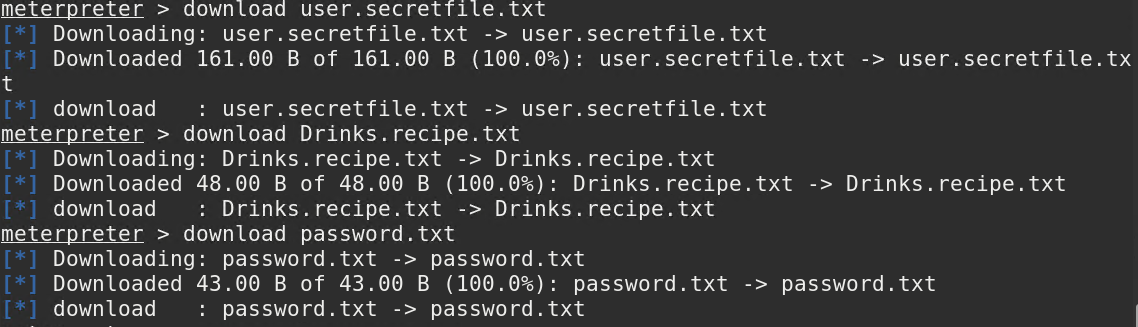
**Search for text files containing “secret” or “recipe”.**



**Move into the folder containing found files (fortunate they were in the same folder).**

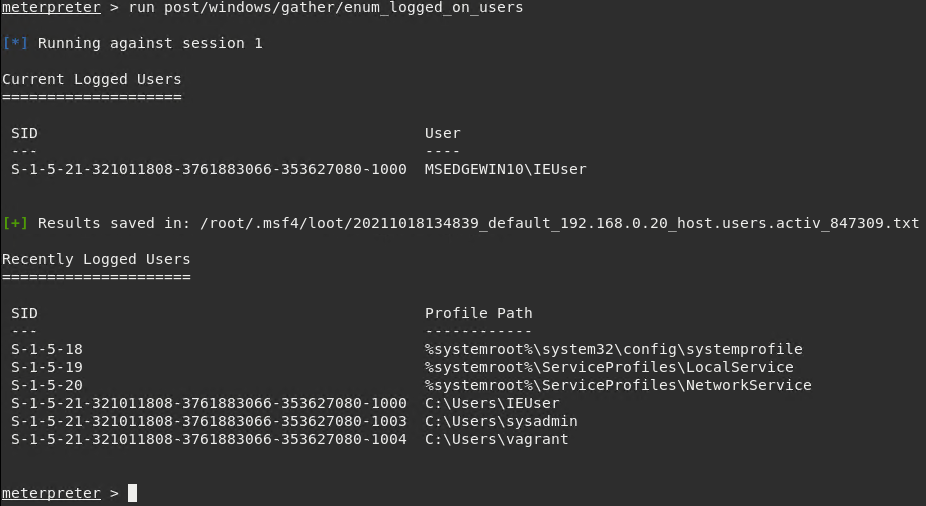


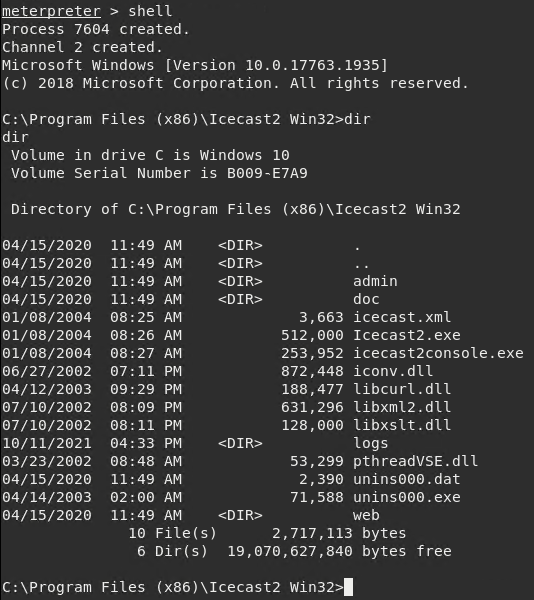
**Download previous files to attacker’s machine.**



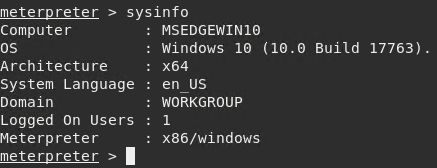
**Proof of download on attacker’s machine. Hashes of the files can be provided to confirm contents.**



**Active users can be found and listed, which could lead to privilege escalation through password files or brute force attacks.**

**Here the attacker is starting a windows shell which can be used with normal privileges.**

**Finally system information can be gathered and used to further exploit the machine.**

****

# Recommendations

If this network is only used internally make a firewall rule to block incoming packets to prevent NMAP scans. To prevent specific exploitation of Icecast make sure to keep it up to date. Newer versions are not vulnerable to this exploit. If possible, lower Icecast’s privileges so that if it does get exploited in the future it cannot be used to escalate privileges or access files that should remain hidden. Only files that are intended to be shared should be accessible through Icecast.