GoodSecurity Penetration Test Report

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 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

Machine’s IP address

Hostname: MSEDGEWIN10

Actual name of the machine

Vulnerability Exploited: CVW10

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. You may need to do extra research online.

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?