GoodSecurity Penetration Test Report

Robert L. Myers@GoodSecurity.com

October 24, 2021

1.0 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.

2.0 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!

3.0 Recommendations

What recommendations would you give to GoodCorp?