GoodSecurity Penetration Test Report

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

2022-02-08

# 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:

1: Nmap to scan services running on the target.

Text

Description automatically generated

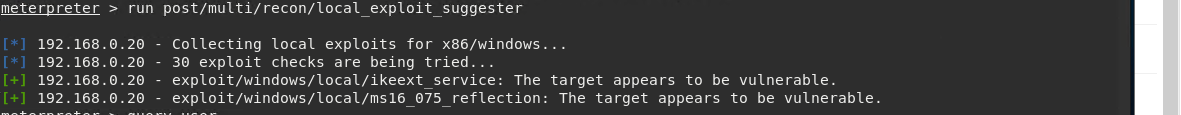
Graphical user interface, text

Description automatically generated

Text

Description automatically generatedText

Description automatically generated



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!

Text

Description automatically generated

Text

Description automatically generated

There should be a separate finding for each vulnerability found!

# Recommendations

What recommendations would you give to GoodCorp?