GoodSecuirty Penetration Test Report

For GoodCorp

V1.0

September 19, 2020

By: Daniel Alicie

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

**Document Properties**

|  |  |
| --- | --- |
| Title | GoodSecurity Penetration Test Report |
| Version | V1.0 |
| Author | Daniel Alicie |
| Pen-Testers | Daniel Alicie |
| Reviewed By |  |
| Approved By |  |
| Classification | Confidential |

**Version Control**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author | Description |
| V1.0 | September 19, 2020 | Daniel Alicie | Final Draft |

Table of Contents

[1. Executive sumary 4](#_Toc52043928)

[1.1 Scope of work 5](#_Toc52043929)

[1.2 Project objectives 5](#_Toc52043930)

[1.3 Assumption 5](#_Toc52043931)

[1.4 Timeline 5](#_Toc52043932)

[1.5 summary of findings 6](#_Toc52043933)

[1.6 Summary of recommendation 6](#_Toc52043934)

[2. Methodology 6](#_Toc52043935)

[2.1 Planning 7](#_Toc52043936)

[2.2 Exploitation 7](#_Toc52043937)

[2.3 Reporting 7](#_Toc52043938)

[3. Detail findings 7](#_Toc52043939)

[3.1 Detailed Systems information 7](#_Toc52043940)

[3.2 windows 10 computer 9](#_Toc52043941)

[4. References 13](#_Toc52043942)

**List of Illustrations**

**LIST OF TABLES**

[Table 1 Penetration testing TIMELINE 5](#_Toc52043780)

[Table 2 TOTAL RISK RATING based on CVSS Score 5](#_Toc52043781)

[Table 3 Target machine open ports 7](#_Toc52043782)

**List of Figures**

[Figure 1 Penetration testing methodology 6](#_Toc52043860)

[Figure 2 inital nmap scan 8](#_Toc52043861)

[Figure 3 nmap scan with common scripts 8](#_Toc52043862)

[Figure 4 nmap scan with vulnerabilites 9](#_Toc52043863)

[Figure 5 metasploit module search for icecast 10](#_Toc52043864)

[Figure 6 metasploit set target machine ip and port 10](#_Toc52043865)

[Figure 7 Exploited target machine and received meterpreter shell 10](#_Toc52043866)

[Figure 8 location of secret file 10](#_Toc52043867)

[Figure 9 Contents of secret file 11](#_Toc52043868)

[Figure 10 location of recipe file 11](#_Toc52043869)

[Figure 11 contents of recipe file 11](#_Toc52043870)

[Figure 12 metasploit local exploit suggester 11](#_Toc52043871)

[Figure 13 Metasploit enumerate logged on users 12](#_Toc52043872)

[Figure 14 Target machine system info 12](#_Toc52043873)

# Executive sumary

GoodSecurity was tasked with performing an internal penetration test on a GoodCorp’s specific target host. 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 Han’s computer to determine if it is at risk. GoodSecurity’s overall objective was to exploit any vulnerable software, find a secret recipe file on target host, and report finding back to GoodCorp.

The internal penetration test found several alarming vulnerabilities on the target computer: When performing the attacks, GoodSecurity was able to gain access to this machine and find the secret recipe file by exploiting two programs with major vulnerabilities.

## Scope of work

This security assessment covers the remote penetration of the target workstation only. GoodSecurity was not permitted to scan any other IP addresses or exploit anything other than the target machine IP address. GoodSecurity was not permitted to complete denial of service and brute force attacks. Once inside the target computer GoodSecurity was permitted to read and access any file. GoodSecurity was not permitted to delete any files or make configuration changes to the system. This assessment was carried out from a White Box perspective, with all information provided by GoodCorp.

## Project objectives

The objectives of this security assessment is was to exploit any vulnerable software, find a secret recipe file on target computer, and report the findings back to GoodCorp. Given the limited amount of time given to test the target host only immediately exploited services were tested. Each vulnerability is assigned a risk rating based on threat, vulnerability and impact.

## Assumption

While writing the report, we assume that the IP address provided is Public Facing. Rules of engagement has been signed by all parties in the information gathering phase.

## Timeline

The timeline of the test is as follows:

|  |  |  |
| --- | --- | --- |
| **Penetration Testing** | **Start Date/Time** | **End Date/Time** |
| Pen Test 1 | 9/19/2020 11:45am | 9/19/2020 1:12pm |

Table Penetration testing TIMELINE

## summary of findings

|  |  |
| --- | --- |
| **Value** | **Number of Risks** |
| CRITICAL (CVSS Scale 9.0 -10.0) | 0 |
| HIGH (CVSS Scale 7.0 – 8.9) | 1 |
| MEDIUM (CVSS Scale 4.0 – 6.9) (NIST, n.d.) | 0 |
| LOW (CVSS Scale 0.1 – 3.9) | 0 |

Table TOTAL RISK RATING based on CVSS Score (NIST, n.d.)

## Summary of recommendation

It is recommended that target machine user ensure software used on company computers are authorized and tested by security team. It is also recommended that software to receive updates and ensure services are patched and tested with correct versions.

# Methodology

Figure 1 Penetration testing methodology

## Planning

During planning for this security assessment, we gathered information from GoodCorp about the target machine, to include IP Address, and Scope of the assessment. After all information was gathered, we conducted a scan of the target machine to determine operating system, open ports, and versions of services.

## Exploitation

Based on the results from the planning stage and our scan we researched operating system and services running versions for vulnerabilities. After researching the vulnerabilities an attempt was made to exploit each vulnerability.

## Reporting

Based on the results of the Planning and Exploitation we start analyzing the results to determine the risk and impact. The risk is calculated based on the following calculation.

Risk = Threat \* Vulnerability \* Impact

# Detail findings

## Detailed Systems information

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| IP Address | System Type | OS Information | Host Name | Open Ports | | | |
| Port # | Protocol | | Service Name |
| 192.168.0.20 | Workstation | Microsoft Windows 10 | MSEDGEWIN10 | 25 | TCP | Smtp | |
| 135 | TCP | Msrpc | |
| 139 | TCP | Netbios-ssn | |
| 445 | TCP | Microsoft-ds? | |
| 3389 | TCP | Ms-wbt-server | |
| 8000 | TCP | http | |
|  |  |  | |

Table Target machine open ports

A screenshot of text

Description automatically generated

Figure 2 inital nmap scan

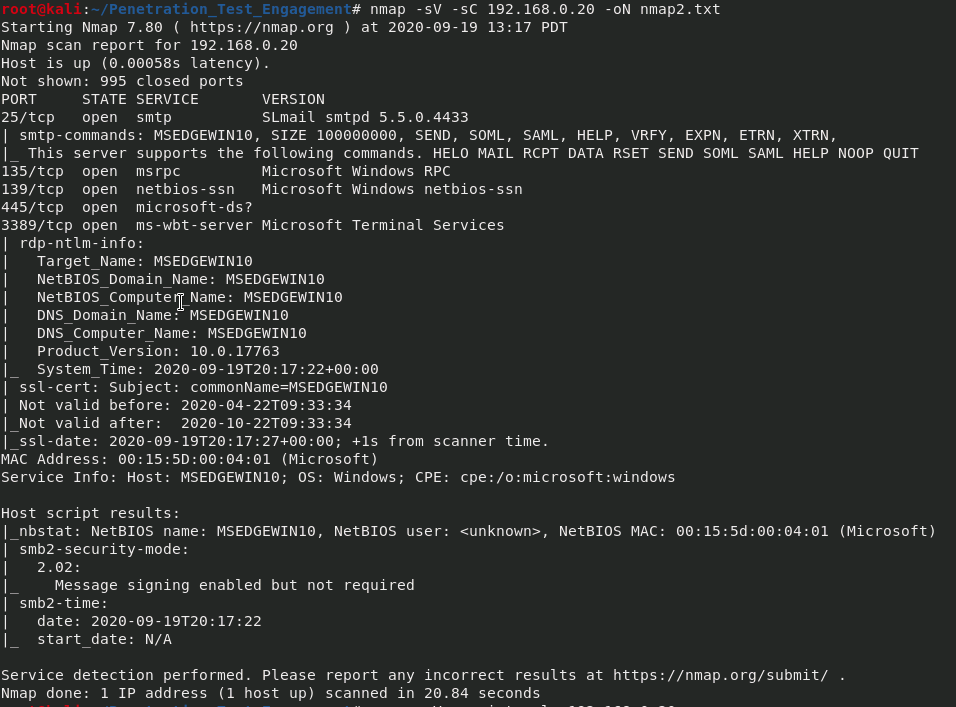


Figure 3 nmap scan with common scripts

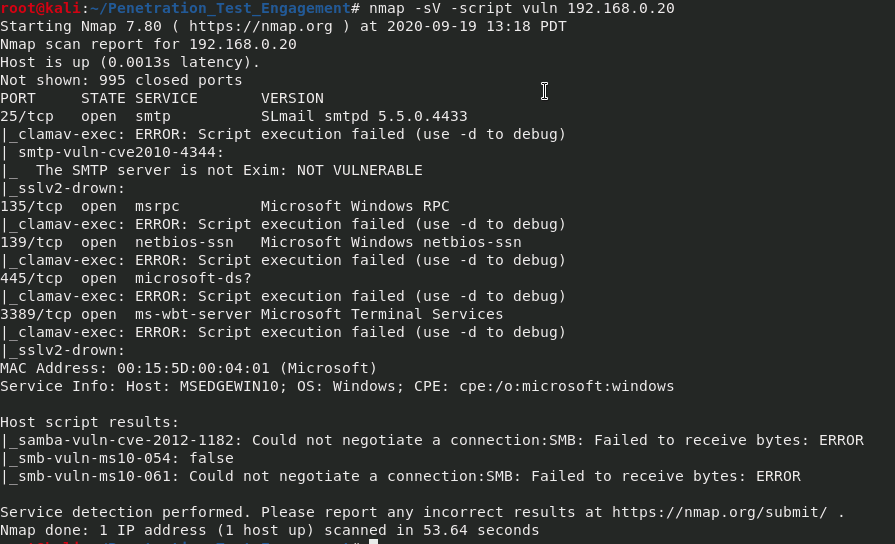


Figure 4 nmap scan with vulnerabilites

## windows 10 computer

**Unsecure Service (Icecast) is running:**

**Threat Level**

High

**Vulnerability**

High

**Analysis**

The target machine is running a version of Icecast which is vulnerable to a buffer overflow allowing remote attackers to execute arbitrary code via an HTTP request with a large number headers (Mitre, 2005). By using this exploit we were able to gain access to the command prompt on the target machine in less than 30 minutes. By gaining access the command prompt of target machine we could access sensitive company documents and possibly access other company network / systems

**Enumeration:**

**Graphical user interface, text, website

Description automatically generated**

Figure 5 metasploit module search for icecast

**Text

Description automatically generated**

Figure 6 metasploit set target machine ip and port

**Text

Description automatically generated**

Figure 7 Exploited target machine and received meterpreter shell

**Text

Description automatically generated**

Figure 8 location of secret file

**Graphical user interface, text

Description automatically generated**

Figure 9 Contents of secret file

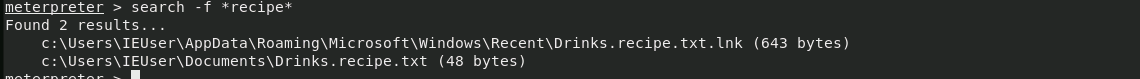
****

Figure 10 location of recipe file

**Text

Description automatically generated**

Figure 11 contents of recipe file

**Impact**

High

**Risk Rating**

High

**Post Enumeration**

1. **Other possible exploits / vulnerabilities**

Attempted to exploit system using MS16-075-Reflection exploit failed multiple times.

**Text

Description automatically generated**

Figure metasploit local exploit suggester

1. **Enumerate all logged on users**

Text

Description automatically generated

Figure Metasploit enumerate logged on users

1. **Target Machine System Info**

Text

Description automatically generated

Figure Target machine system info

**Recommendations**

Ensure Icecast is updated to a version higher than 2.0.1 preferably version 2.4.4 or have security team remove software from computer.

# References

icecast.org. (n.d.). *Icecast*. Retrieved 09 25, 2020, from https://icecast.org/

Mitre. (2005, 02 20). *CVE-2004-1561*. Retrieved from Common Vulnerabilites and Exposures: CVE-2004-1561

NIST. (2004, 12 31). *National Vulnerability Database*. Retrieved 09 19, 2020, from https://nvd.nist.gov/vuln/detail/CVE-2004-1561

NIST. (n.d.). *CVSS Vulnerability Metrics*. Retrieved 09 19, 2020, from https://nvd.nist.gov/vuln-metrics/cvss

Offensive Security. (2010, 04 30). *Exploit Database*. Retrieved 09 20, 2020, from https://www.exploit-db.com/exploits/16763

SecurityFocus. (n.d.). *SecuriyFocus*. Retrieved 09 19, 2020, from https://www.securityfocus.com/bid/11271/solution