GoodSecurity Penetration Test Report

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

4/16

# 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

Hostname: MSEDGEWIN10

Vulnerability Exploited: ICECAST Header

Vulnerability Explanation: This attack exploits a buffer overflow in the header syntax of ice cast. The script sends 32 HTTP request headers that ice cast will write one of them passed. Using an Exitthread it makes The app keeping the thread open. This allows the attacker complete control.

Severity: 9.5 Critical

Proof of Concept:

1. Used NMAP to ping the IP address and server for system info and open ports to exploitText

   Description automatically generated
2. After discovering open http port for icecast used Metasploit to find a vulnerability
3. Used the module with target set as the machine to open a SessionText

   Description automatically generated
4. Gained access into Icecast backed out into the Server home and file storageText

   Description automatically generated
5. Searched for sensitive files Text

   Description automatically generated
   1. Found Banking info in secretfile and did the same search for recipe file (unencrypted data)
6. Took logged on user info to find out various accountsText

   Description automatically generated
7. Opened a shell on the server Text

   Description automatically generated
8. Pulled System info to further exploit the machineText

   Description automatically generated

# Recommendations

I would recommend first keeping all apps updated and patch the system regularly so apps like ice cast can’t be exploited. This recommendation comes with apps that are going to be running constantly if they need to be close apps that open ports to internet leaving you exposed. Closing ports that aren’t needed open or practice good port filtering on connections. (Could help to have a firewall set-up). Especially when it comes to sensitive files put walls on access points for files. When it comes to sensitive information assume that you could be exploited at any time despite the best security measures. A password isn’t the only means of access to a server especially if you’re logged into it for long periods of time. This will mean you are encrypting sensitive files on your computer or hiding them so they cannot be discovered easily.