GoodSecurity Penetration Test Report

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

5/23/2022

# 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

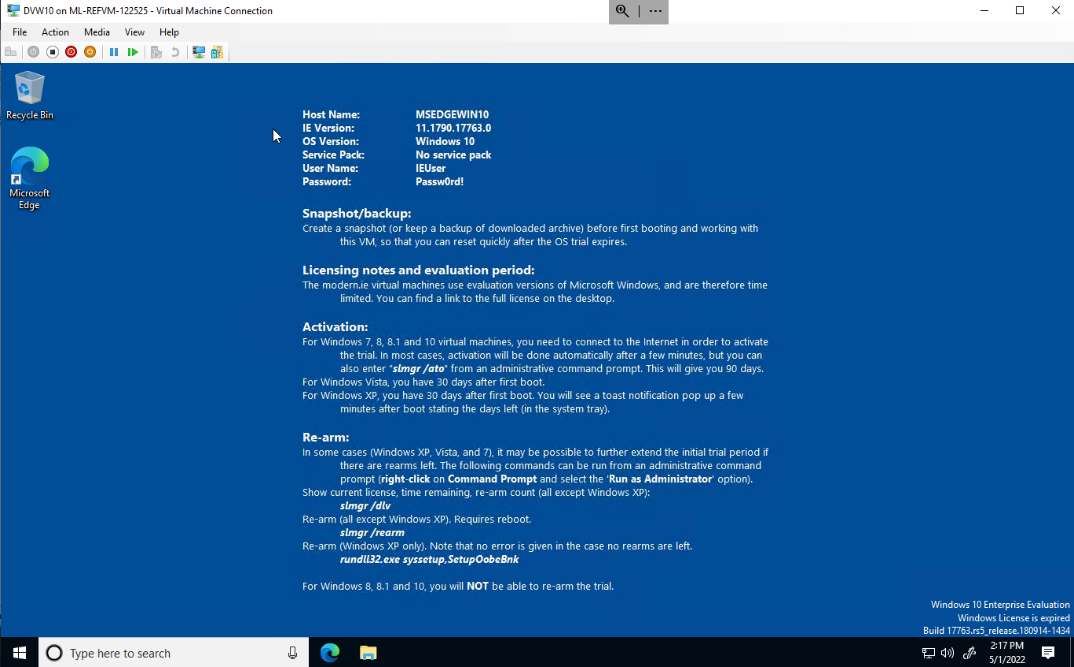
identified on Hans’ desktop. When performing the attacks, GoodSecurity was able to gain access to his machine and find the secret recipe file by exploit two programs that had major vulnerabilities. The details of the attack can be found in the ‘Findings’ category.

# Findings

**Machine IP:**

* 192.168.0.20

**Hostname:**

* MSEDGEWIN10  
  

**Vulnerability Exploited:**

* Icecast 2.0.1 – Header 0

**Vulnerability Explanation:**

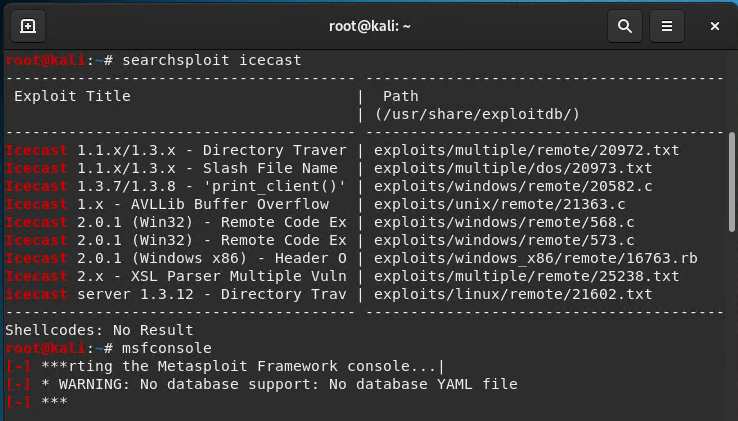
* The attack appears to be a buffer overflow. This attack is possible if the icecast server is not up to date, deeming it to be vulnerable.

**Severity:**

* High – potential loss of Revenue or productivity.

**Proof of Concept:**

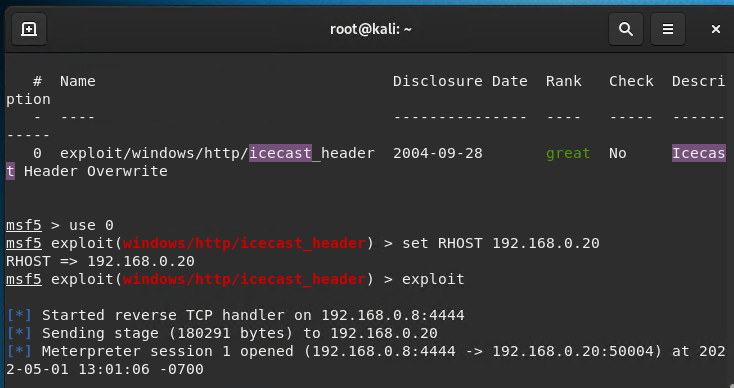
* To view the available icecast exploits, I ran **searchsploit icecast**



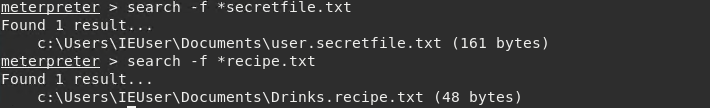
* To start Metasploit, I ran **msfconsole**



* I started icecast by running **search icecast**, and ran it as **use 0** to avoid copying the entire path to the module. I then proceeded to set the RHOST as **set RHOST 192.168.0.20**. I then initiated the exploit by running **exploit.**



* While having the meterpreter session still running, I ran two searches **“search -f \*secretfile.txt”,** and **“search -f \*recipe.txt”**



# Recommendations

* Update the icecast server immediately to avoid potential loss of revenue or production. Ensuring that all servers are updated on a regular basis would be a good place to start.
* By naming confidential files with more ominous names, rather than secretfile.txt