GoodSecurity Penetration Test Report

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

05/01/2022

# 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.

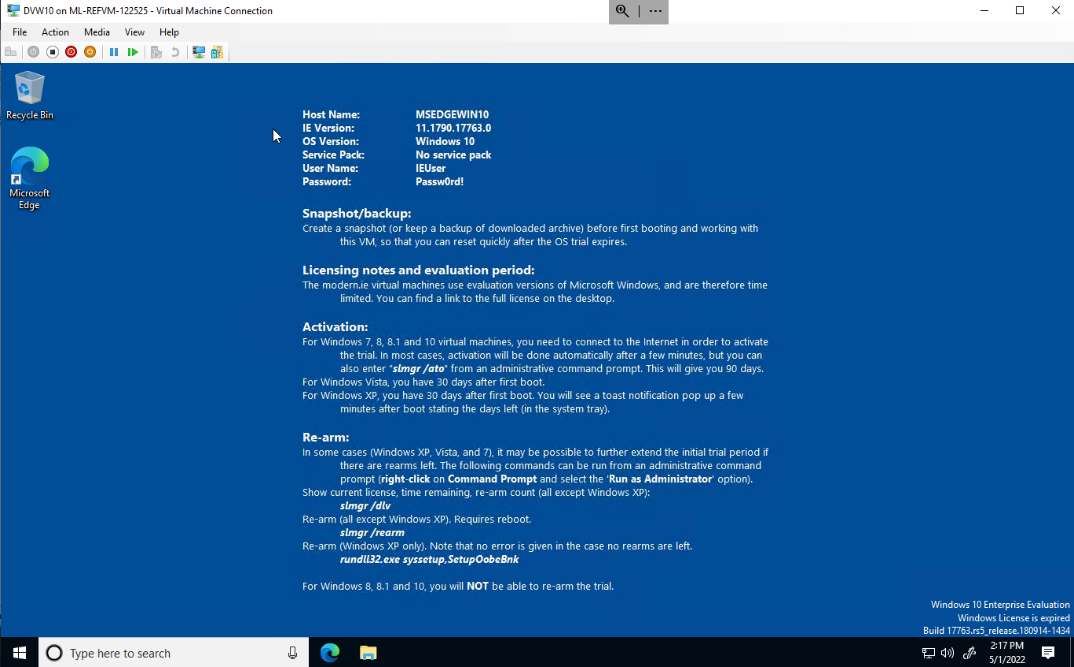
# Findings

**Machine IP:**

192.168.0.20

**Hostname:**

MSEDGEWIN10



**Vulnerability Exploited:**

Icecast 2.0.1 (Windows x86) – Header 0

**Vulnerability Explanation:**

According to Infosec Matter, the attack type is buffer overflow. This attack becomes possible if the Icecast server is not up-to-date with the latest version, which leaves Icecast server versions before 2.0.1 vulnerable.

This attack is carried out by an attacker executing arbitrary code via an HTTP request with a large number of headers (32 HTTP headers) to the remote host that can lead to potential denial of service or remote code execution.

*Source: https://www.infosecmatter.com/nessus-plugin-library/?id=14843*

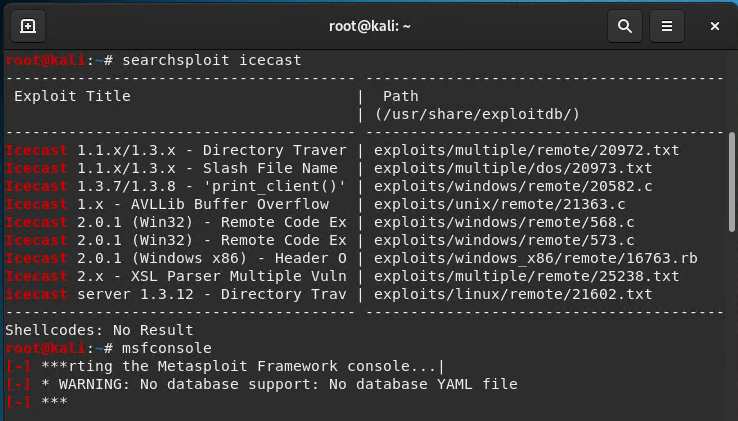
**Severity:**

Based on research done about this vulnerability, the severity is High having a **vulnerability score of 7.5** and a successful exploit of this vulnerability may result in significant loss of revenue or productivity.

*Source: https://nvd.nist.gov/vuln/detail/CVE-2004-1561#vulnCurrentDescriptionTitle*

**Proof of Concept:**

To start SearchSploit and show available Icecase exploits, I ran **searchsploit icecast.**

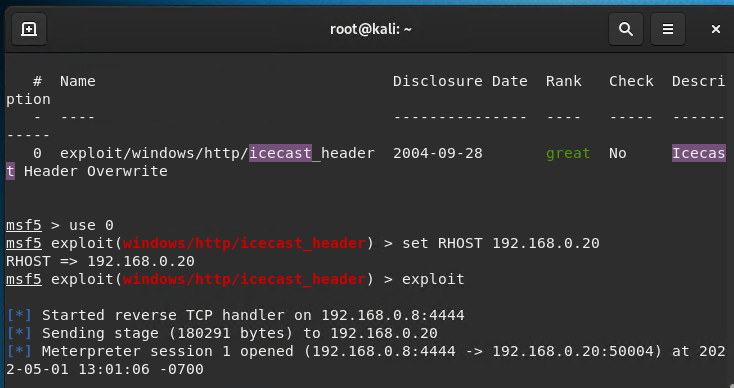


I then started Metasploit by running the command **msfconsole**



After starting Metasploit, I ran Icecast by running the command **search icecast**. And to run the Icecast module from Metasploit, I ran **use 0** instead of copying the entire path to the module.

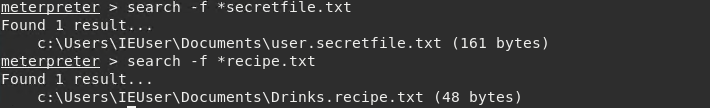
I then set the RHOST to the target machine by running the command **set RHOST 192.168.0.20** then ran the exploit with command **exploit**



After having a Meterpreter session opened, I conducted a search for secretfile.txt, recipe.txt and exfiltrated the recipe\*.txt files.

The commands I ran were the following:

* Secretfile.txt: **search -f \*secretfile.txt**
* Recipe.txt: **search -f \*recipe.txt**



# Recommendations

Since this attack is made possible with older versions of the Icecast server, my recommendation is to update the Icecast server to the latest version available on the vendor’s site. Another recommendation would be to name confidential files with a less conspicuous name than having words like: *secret* or *recipe*. As a hacker, these would be the first words I would use to search the files.