GoodSecurity Penetration Test Report

[abhijit.nayak@GoodSecurity.com](mailto:abhijit.nayak@GoodSecurity.com)

June 5, 2020

# 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 Overwrite (Metasploit)

**Vulnerability Explanation:**

Buffer overflow in the header parsing of icecast server. Sending 32 HTTP headers will cause a write one past the end of a pointer array. On win32 this happens to overwrite the saved instruction pointer.

**Severity:**

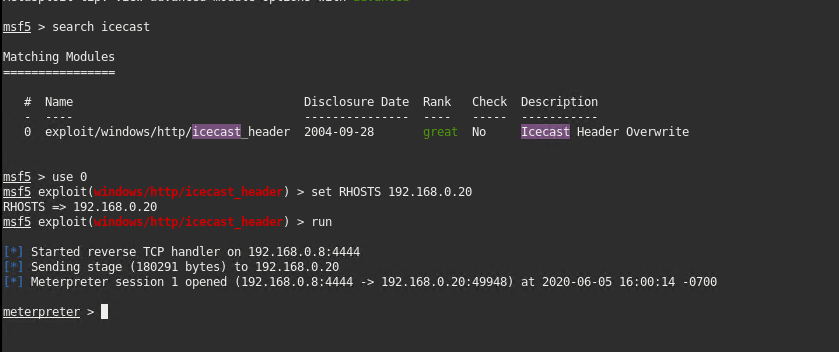
HIGH

**Proof of Concept:**

1. **Download personal files**

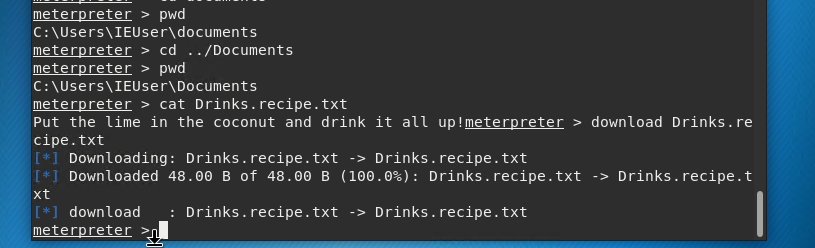
Step1: start metsploit using msfconsole

Step2: search for icecast

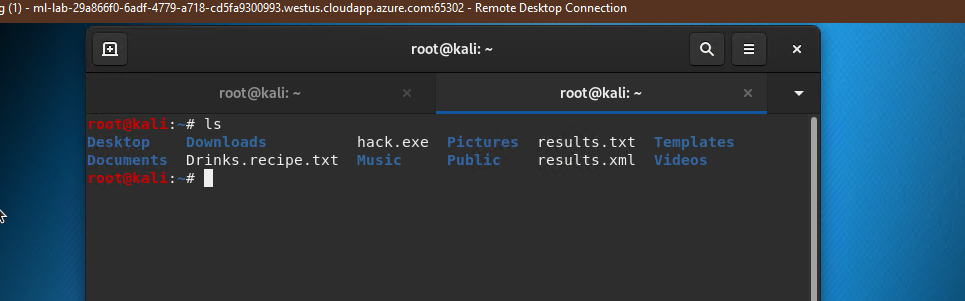


Step 3. Using the search -f command search the secret file and Drinks recipe file that the CEO had stored in his Documents folder.

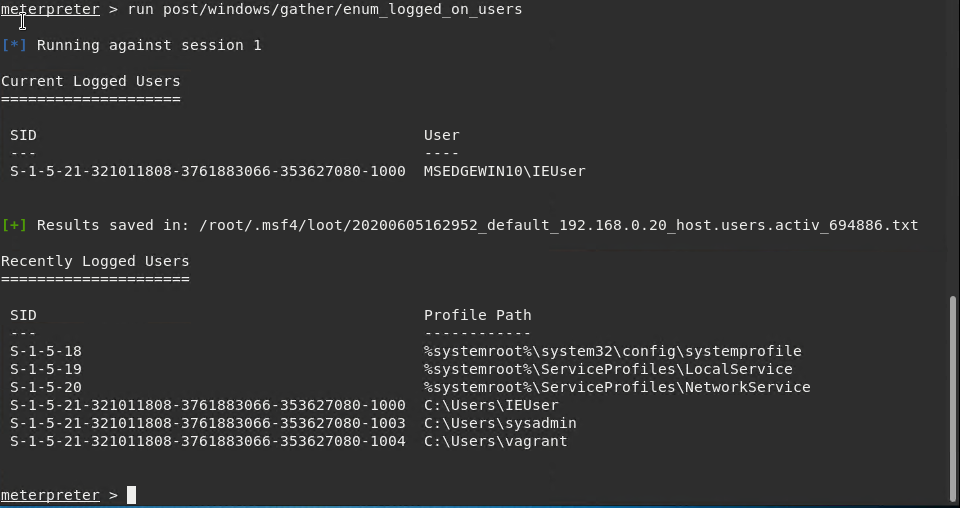
Step 4. Download the file. Using download command



Step6: check your Kali linux using ls command.

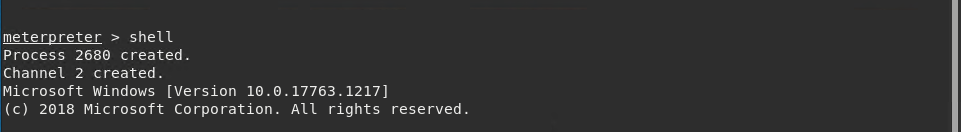


1. **Enumerating logged on users**

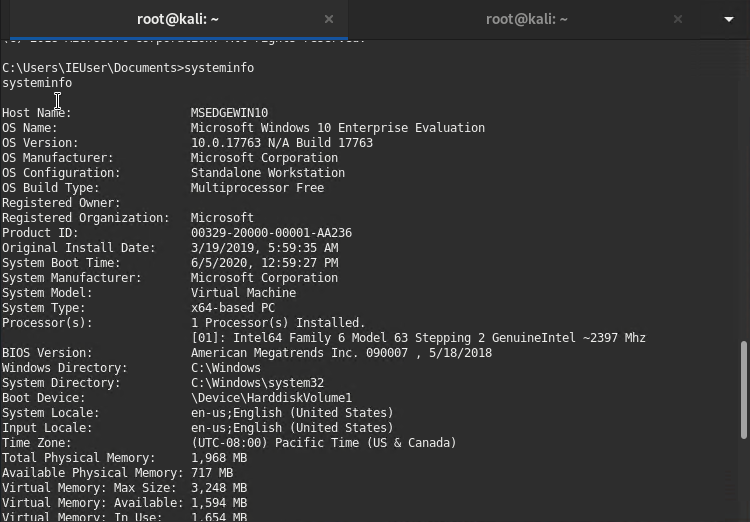


1. **Gaining access to shell**

Step1: use shell command in the meterpreter



Step2: run systeminfo



# Recommendations

There are 2 recommendations that I would like to give.

1. **Principle of Least Privilege**

The employees of GoodSecurity Corp should segregate their access to folders based on their privilege of use. In our exploit, we could download Han’s files and gain access to the shell.

1. **Upgrade to the latest version of icecast.**

Goodsecurity Corp should consider upgrading their Icecast to the latest version with patches applied. As this vulnerability is dated 2004.