

GoodSecurity Penetration Test Report

william@eugtechsec.com

12/19/2020

1. 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 goal of this test is to perform attacks similar to those of a hacker and attempt to infiltrate Hans' computer to determine if it is at risk. GoodSecurity's overall objective was to exploit any vulnerable software, find a secret recipe file on Hans' computer, and report the findings back to GoodCorp.

The internal penetration test found several alarming vulnerabilities on Hans' computer: When performing the attacks, GoodSecurity was able to gain access to his machine and find the secret recipe file by exploiting icecast's buffer overflow, brute forcing of the RDP service on 3389 and finally using the password cracked to also access the admin network shares. The details of the attack are below.

2. Findings

Machine IP:

102.168.0.20

Hostname:

MSEDGEWIN10

Vulnerability Exploited:

Icecast_header

Privilege escalation

Brute force of rdp

Access to network shares via cracked passwords

Vulnerability Explanation:

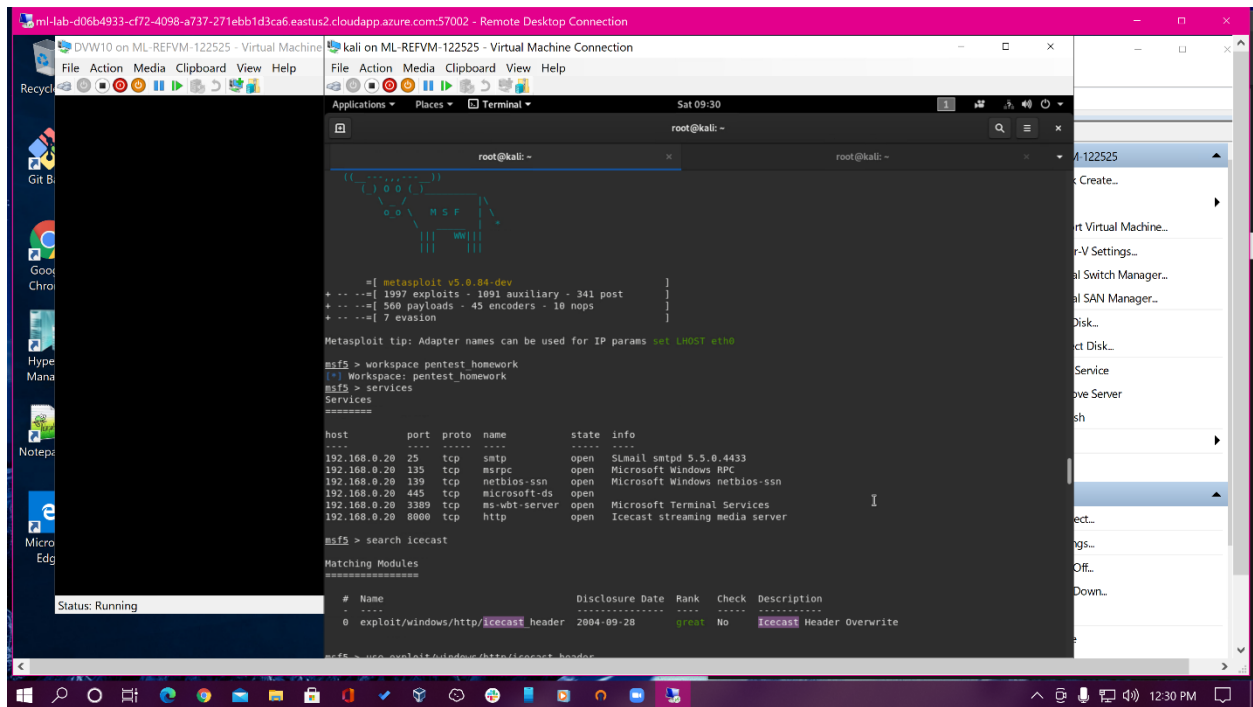
Icecast is vulnerable to a remote buffer overflow allowing the attacker to gain a shell on the system. This shell can then be run in a way that allows complete root access to the vulnerable machine using privilege escalation tactics. An attacker can also remotely run a brute force attack to port 3389 to

discover the IEUser Passw0rd! (which is garbage for cryptographic strength) which allows the attacker to not only get a remote desktop, but access to admin level network shares.

Severity:

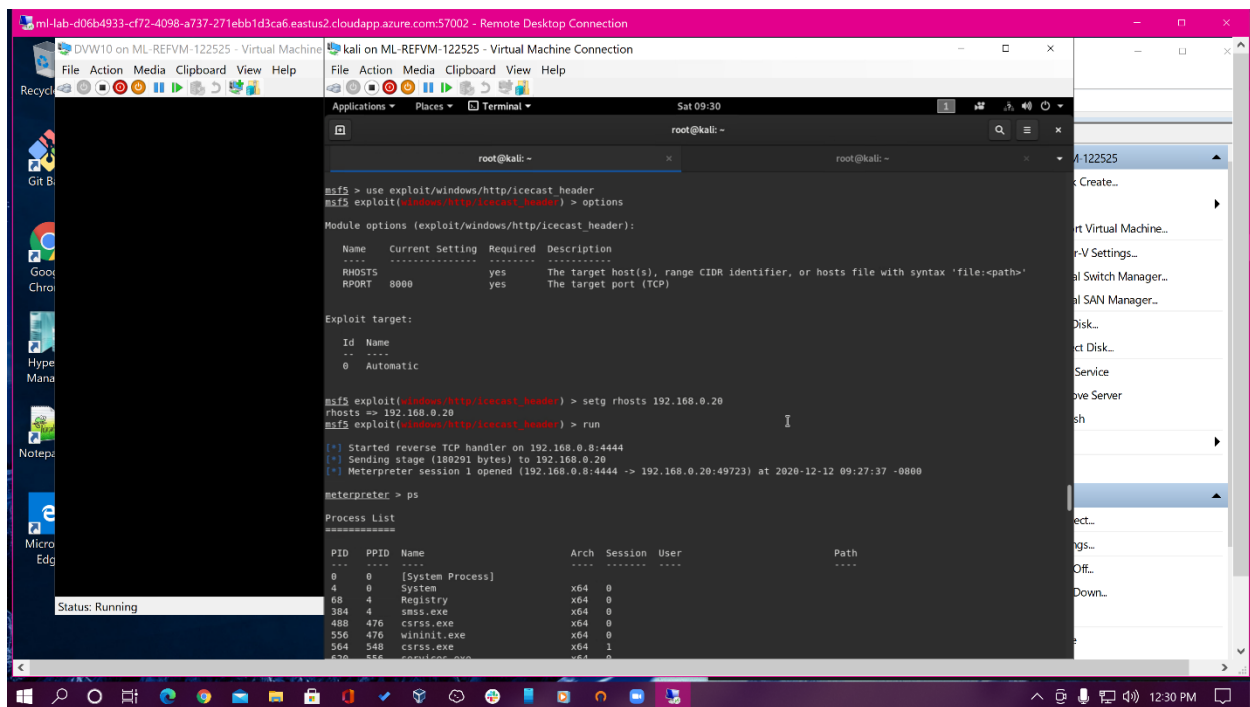
Each of the vulnerabilities is incredibly severe leaving the machine completely open to root level tinkering (ie an attacker could easily add ransomware, root kits, turn it into a bot, change or exfiltrate data, etc)

Proof of Concept:

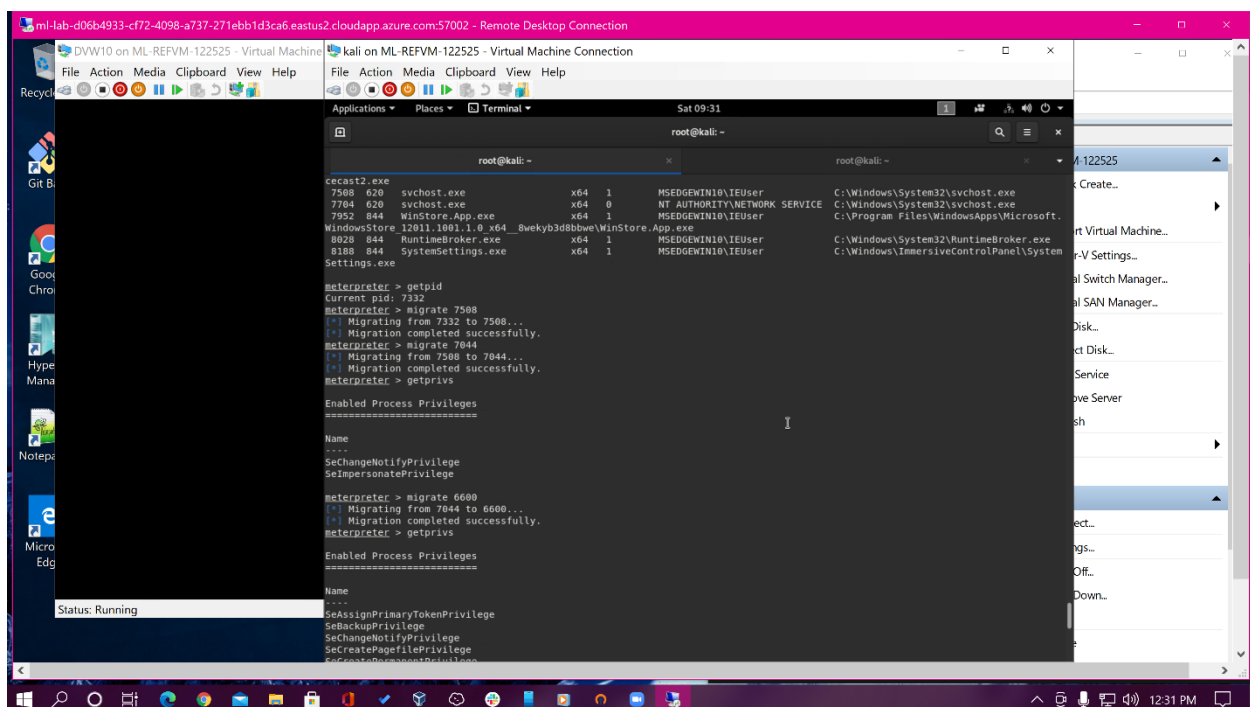


```
root@kali: ~  
msf5 > workspace pentest_homework  
msf5 > services  
=====  
Host      port  proto  name      state  info  
-----  
192.168.0.20 25    tcp    smtp      open   Smail smtpd 5.0.4433  
192.168.0.20 135   tcp    msrpc     open   Microsoft Windows RPC  
192.168.0.20 139   tcp    netbios-ssn open   Microsoft Windows netbios-ssn  
192.168.0.20 445   tcp    microsoft-ds open   Microsoft Windows  
192.168.0.20 3389  tcp    ms-wbt-server open   Microsoft Terminal Services  
192.168.0.20 8080  tcp    http      open   Icecast streaming media server  
msf5 > search icecast  
Matching Modules  
=====  
#  Name                                     Disclosure Date  Rank  Check  Description  
--  --                                     -  
0  exploit/windows/http/icecast_header  2004-09-28      great No    Icecast Header Overwrite  
msf5 > use exploit/windows/http/icecast_header
```

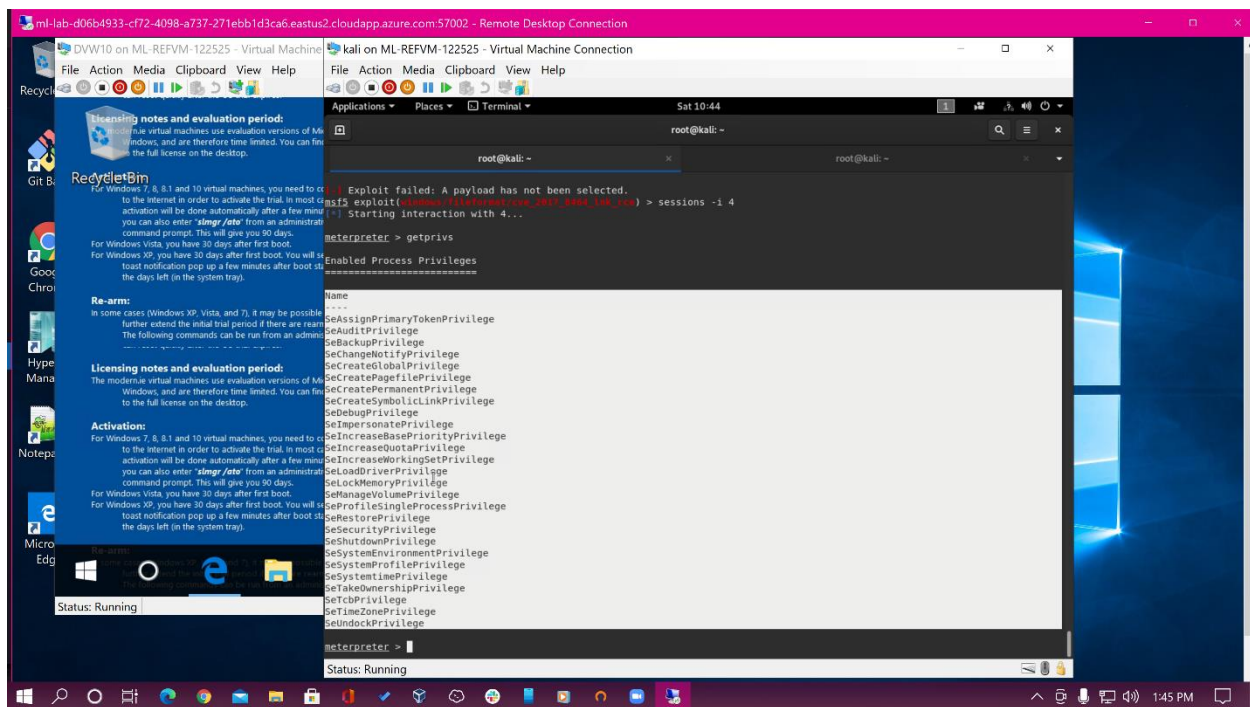
^^ this is the list of open services on the victim box and the icecast vulnerability that allowed entry.



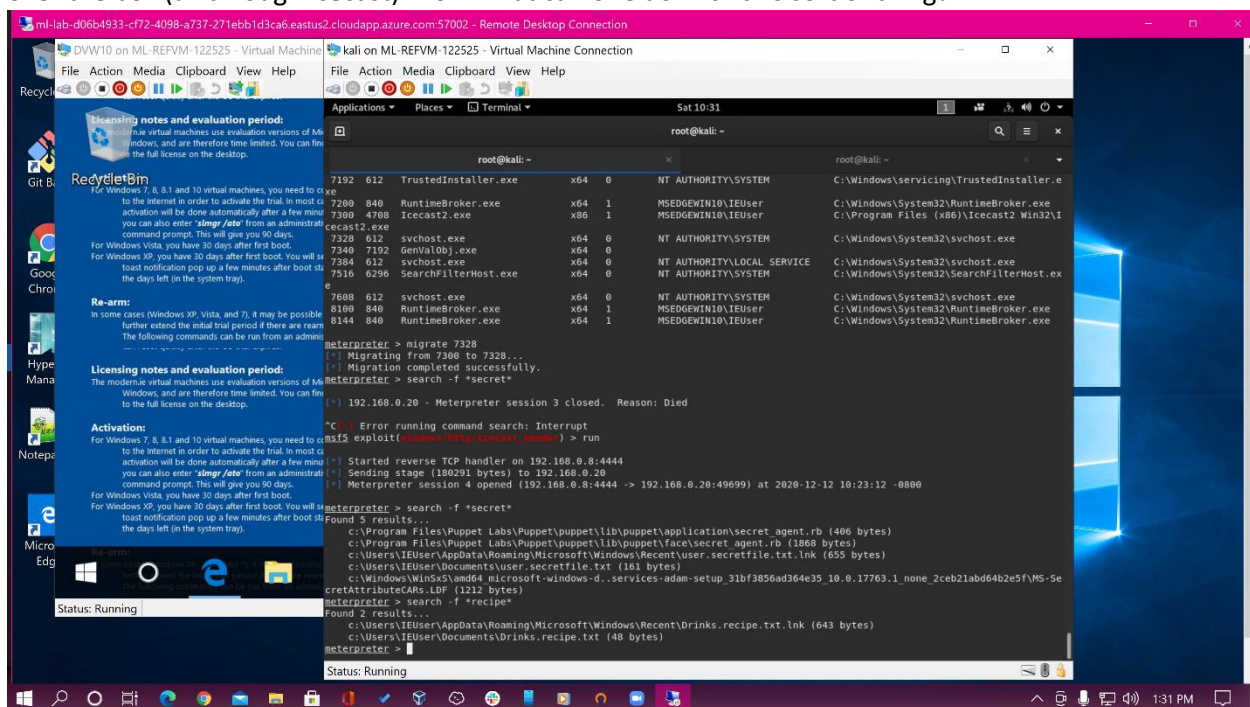
^^ in this screen shot you can see that the exploit fired successfully netting a meterpreter shell allowing commands to be run on the victim machine such as enumerating processes (the start to privilege escalation).



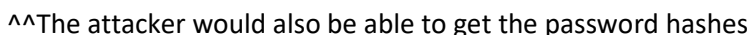
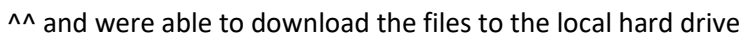
^^ this is showing the start to privilege escalation note the first round of asking for the privileges returns only 2 and the second time is a much longer list that gets cut off by the screen.

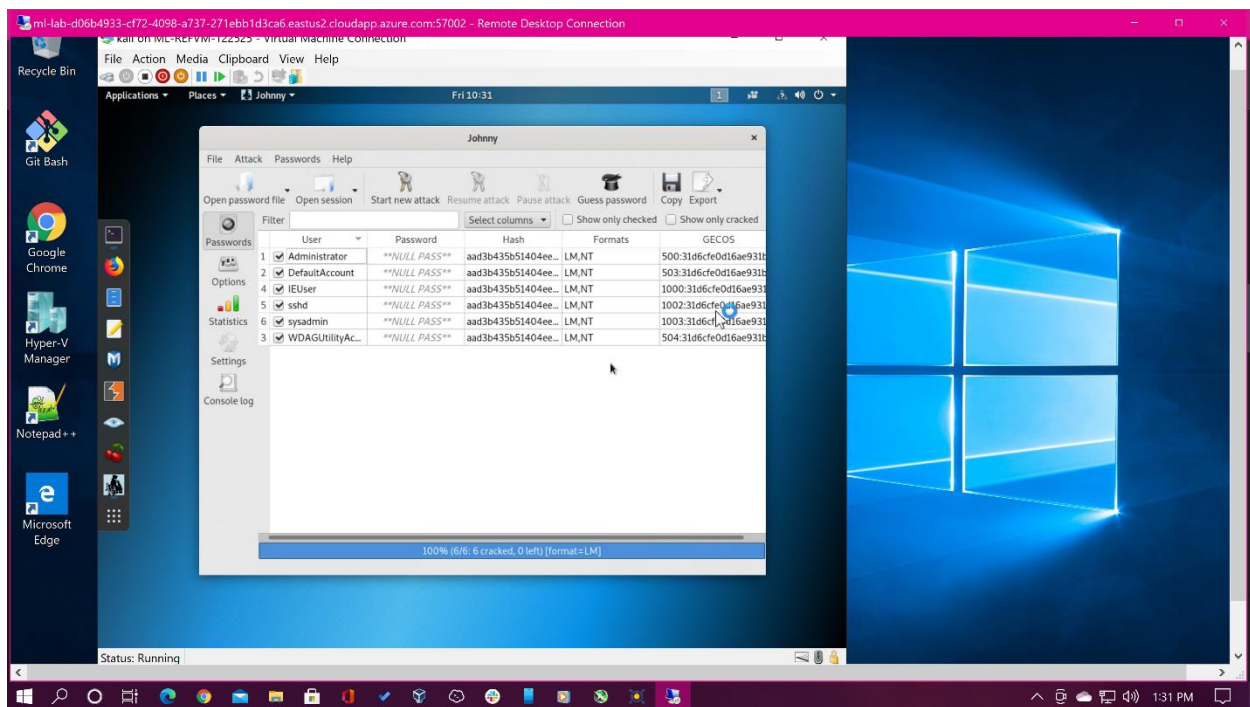


^^ here you see that the attacker has gained the full list of privileges and thus gained complete control over the box (all through icecast). Now what can one do with this sort of thing?

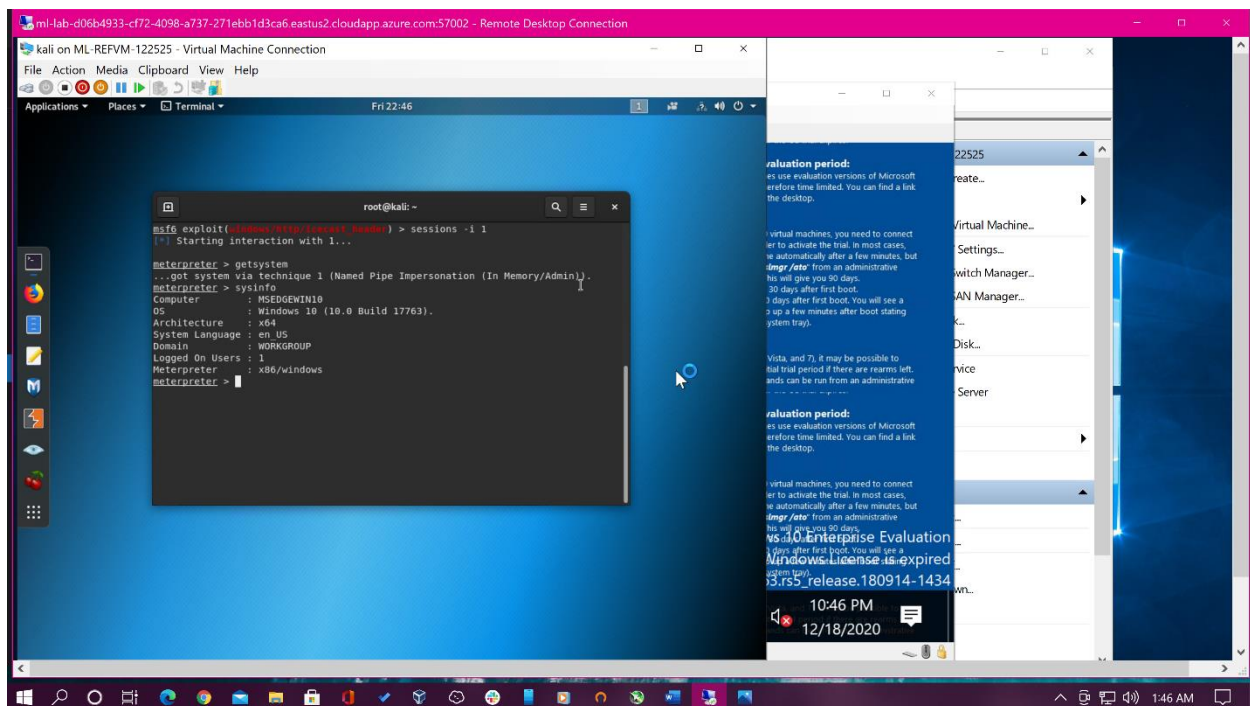


^^ we have found all the secretfiles and recipe's

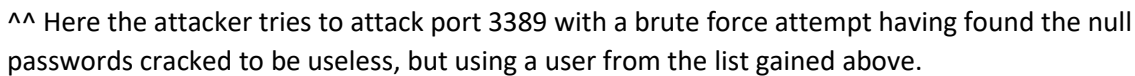
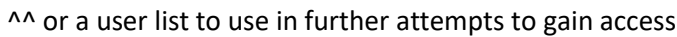


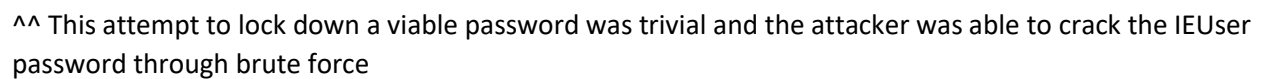


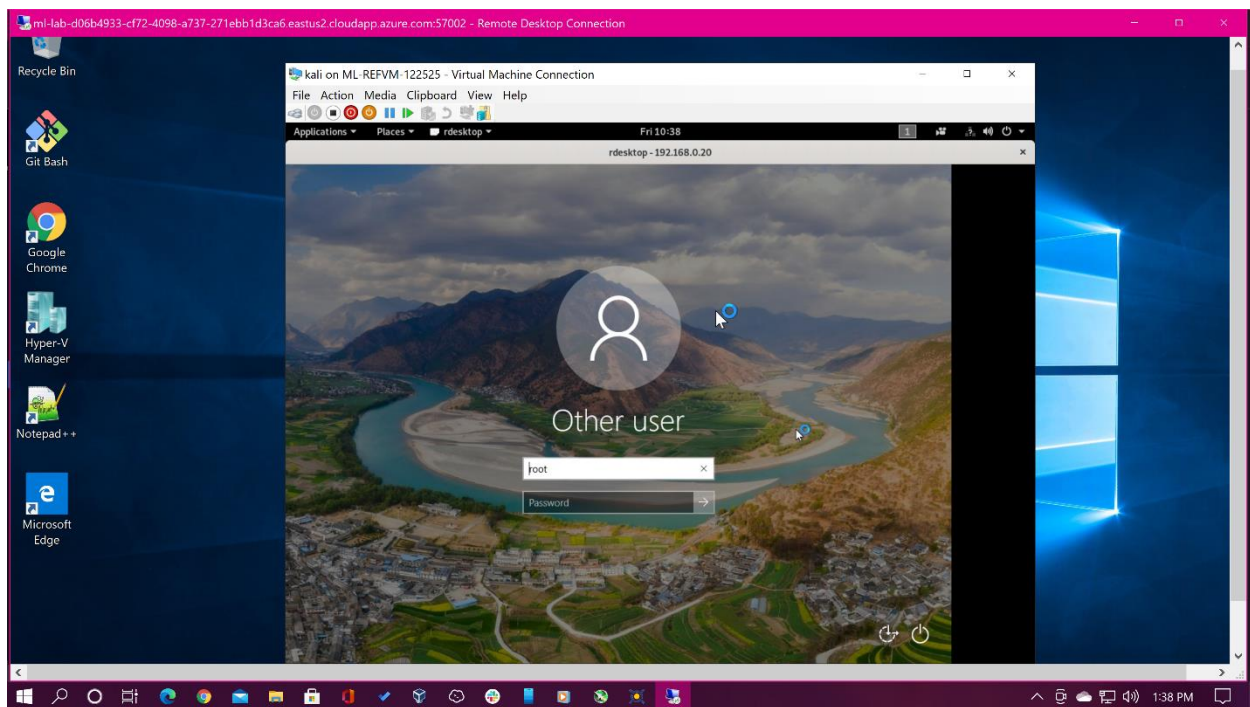
^^ which fortunately seem to resolve as null, further work with passwords to come.



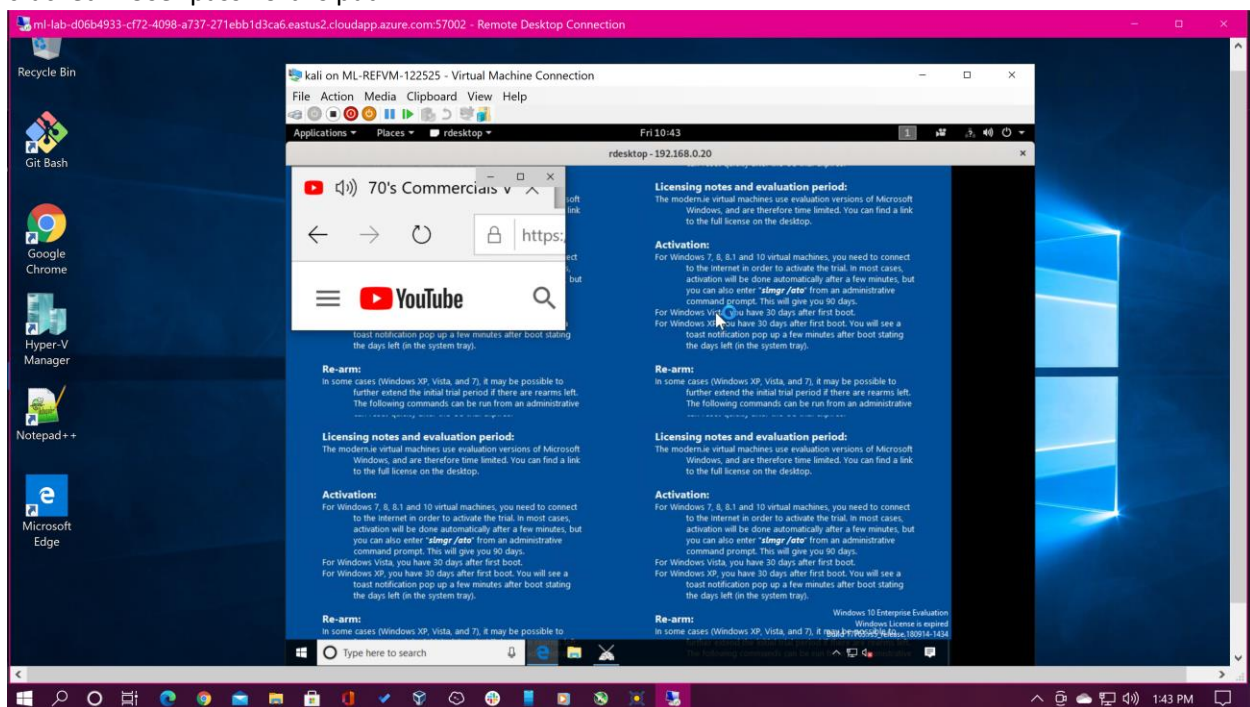
^^ the attacker can then enumerate system info such as the computer name...



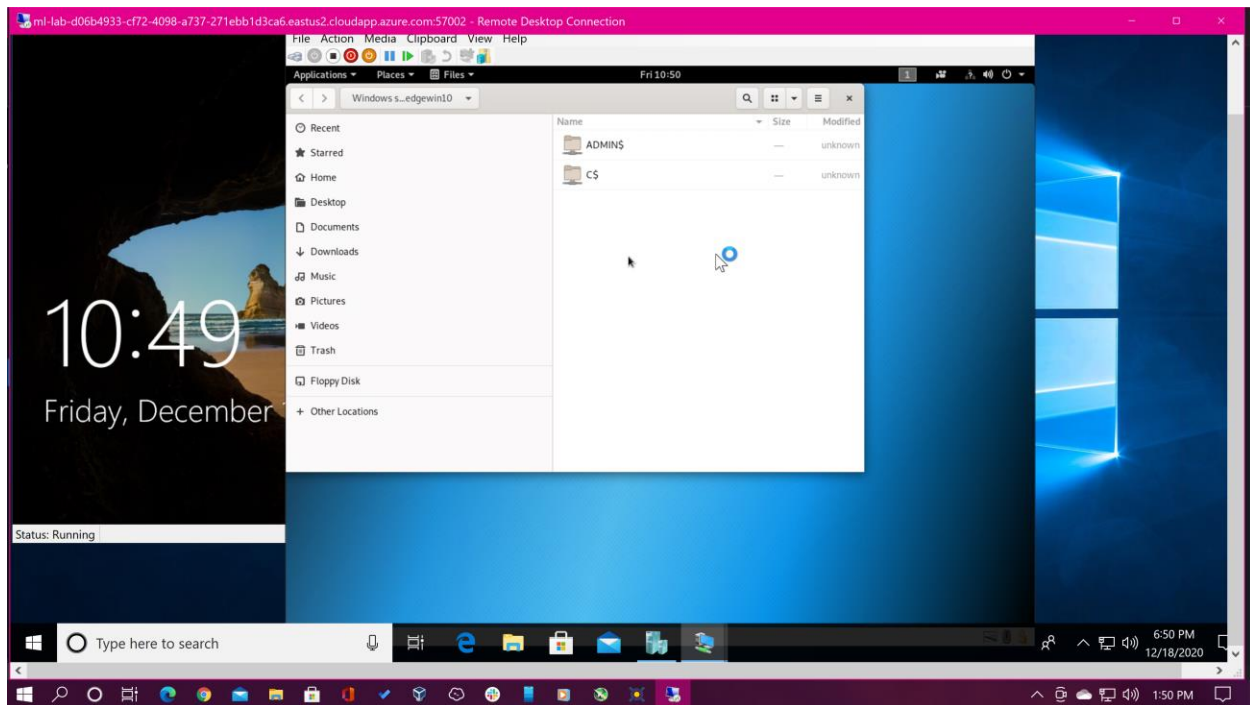




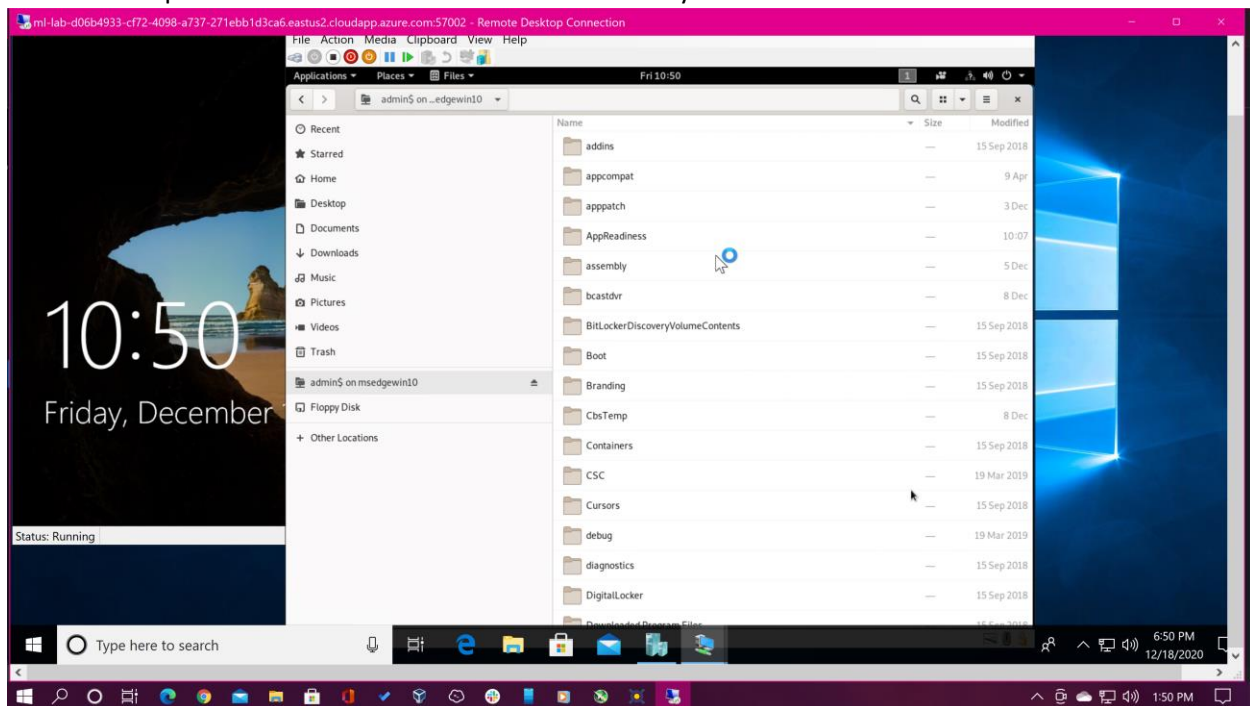
^^As you can see the unprotected rdp on port 3389 was used to gain a remote desktop which once the cracked IEUser password is put in...



^^ returns a full remote desktop allowing the attacker to watch what the victim is doing (clearly working hard watching youtube videos)



^^ The same password works for access to Admin level system shares



^^ as shown in this screen shot

3. Recommendations

Remove all hard drives from this computer and put them in the microwave, you can trust not one single file on this machine. Afterwards, reinstall a new version of windows and for the love of the Gods update it and all software used on it to the latest version. Also add in group policy rules to prevent brute forcing (say 5 password fails before a lockout), change all passwords to not be among the top 50 worst passwords (Passw0rd! is a lack of security) and finally, remove access to the vagrant account (who's default password is on the mirai botnet password list).