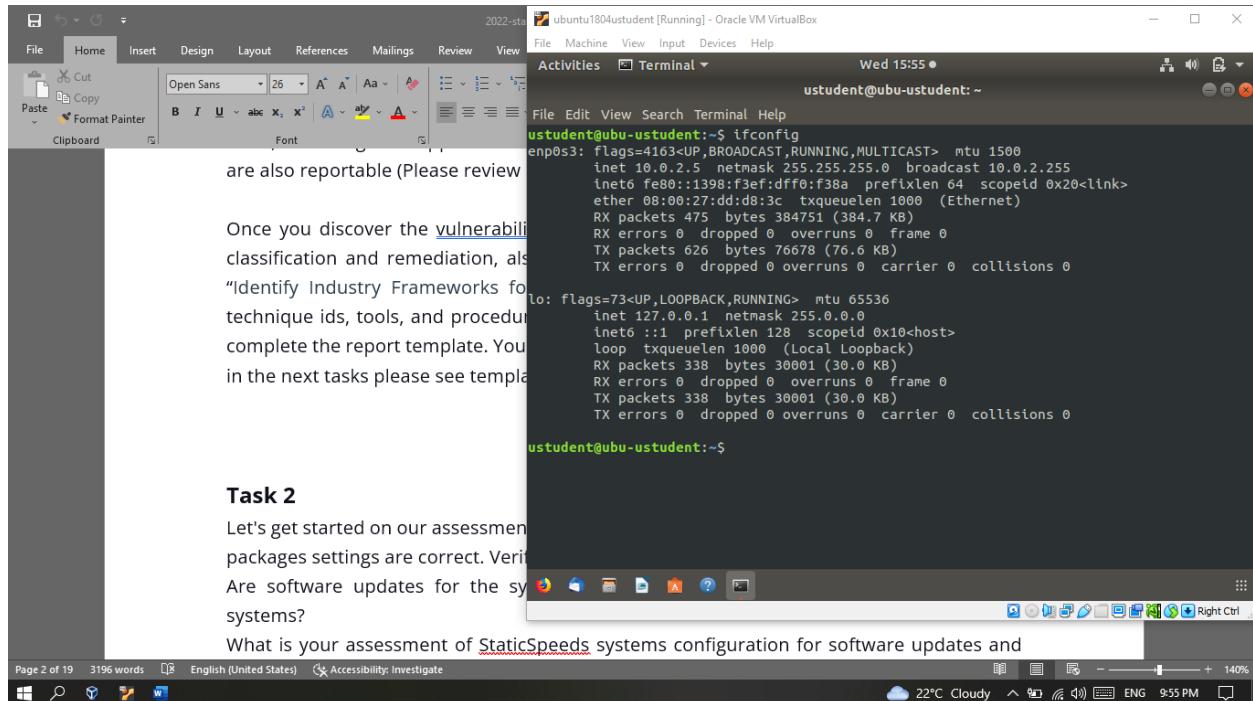


Ubuntu 18.4

Host	High	Medium	Low	Log
10.0.2.5	XX	X	X	X

IP Address: 10.0.2.5



Task 2

Let's get started on our assessment. We will start by checking if the system packages settings are correct. Verify the following:

- Are software updates for the system installed?
- Are security patches applied to the system?

What is your assessment of StaticSpeeds systems configuration for software updates and patches?

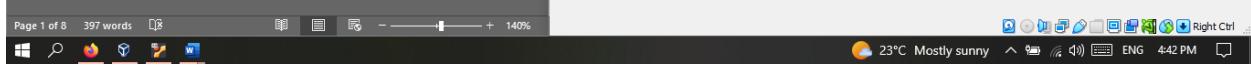
Service	Port	Sensitive Level
http	80 TCP	High
ssl/http	443 TCP	Medium
XXX	TCP	Low
XXX	xx TCP	Log

Service	Port
http	80 TCP
ssl/http	443 TCP
xxx	TCP
xxx	xx TCP

1- CVE-2012-5159 and or finding (critical)

Issue

Contains an exerntially introduced modification (trojan horse)

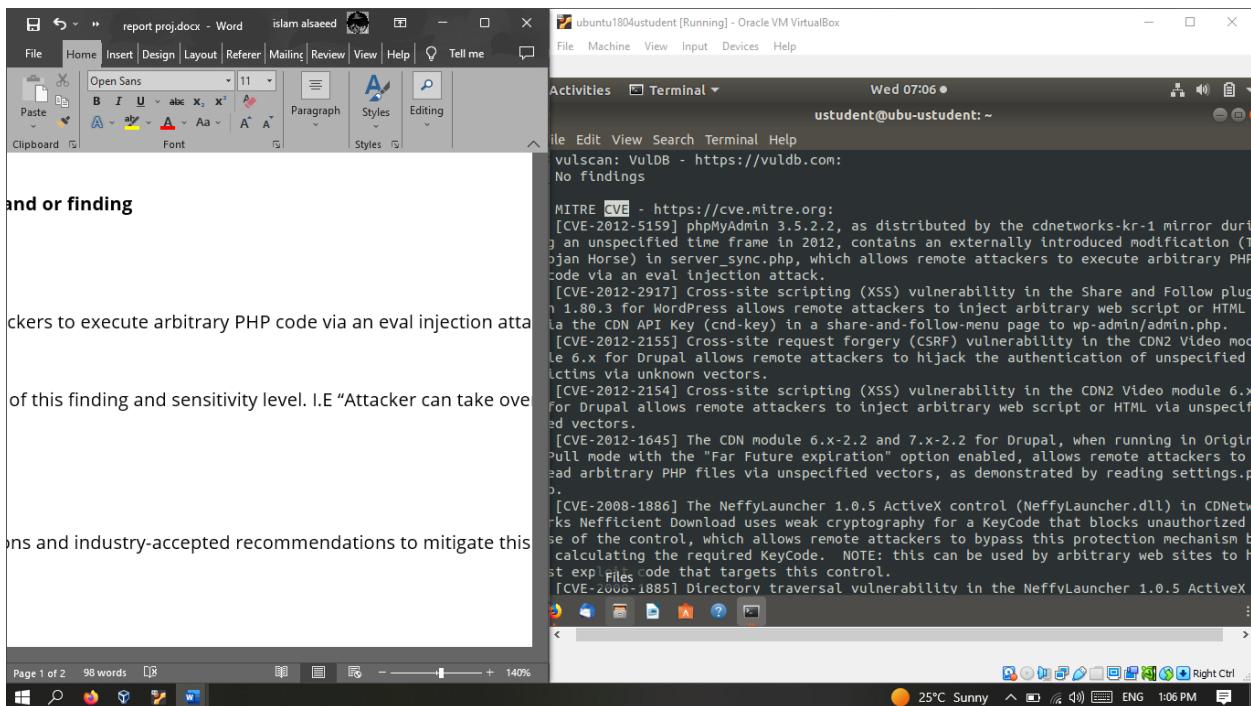


Service	Port
http	80 TCP
ssl/http	443 TCP
xxx	TCP
xxx	xx TCP

1- CVE-2012-5159 and or finding (critical)

Issue

Contains an exerntially introduced modification (trojan horse)



Impact

Allows remote attackers to execute arbitrary PHP code via an eval injection attack

Mitigation

Check your phpMyAdmin distribution and download it again from a trusted mirror if your copy contains a file named <code>server_sync.php</code>.

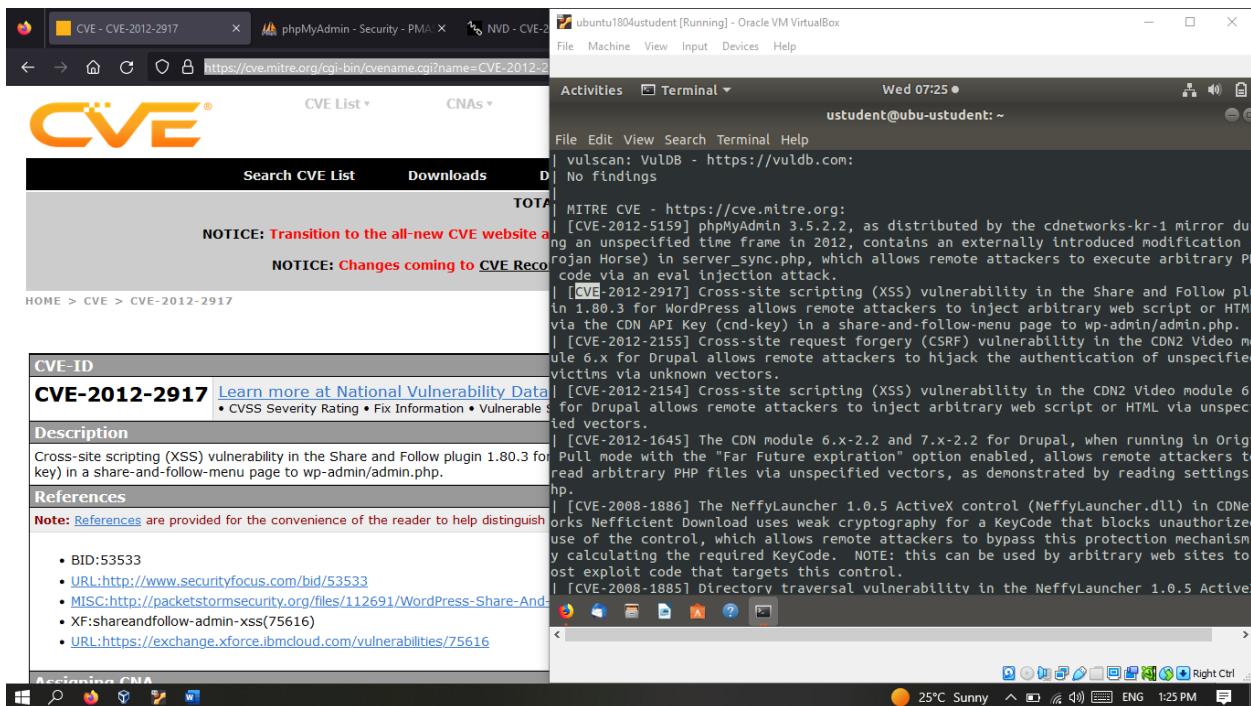
Reference

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5159>

- CVE-2012-2917 and or finding (high)

Issue

Cross-site scripting (XSS) vulnerability in the Share and Follow plugin 1.80.3 for WordPress



Impact

allows remote attackers to inject arbitrary web script or HTML via the CDN API Key (cnd-key) in a share-and-follow-menu page to wp-admin/admin.php.

Mitigation

No remedy available as of October 1, 2014.

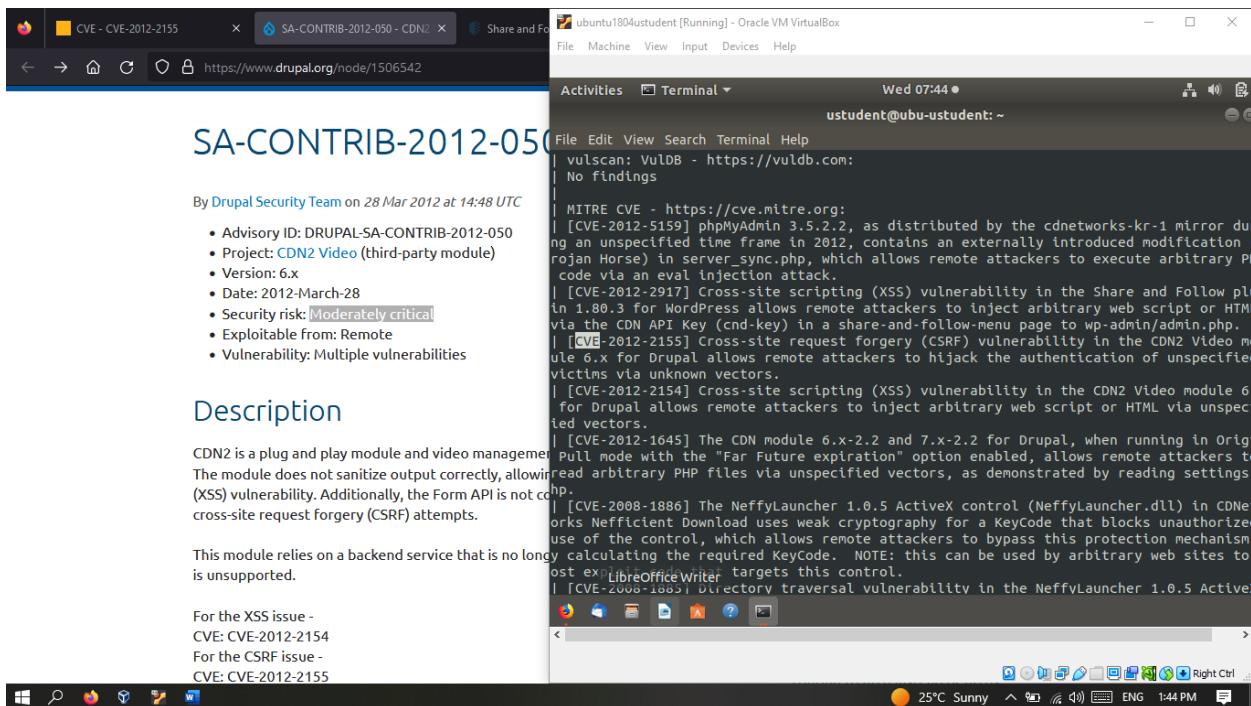
Reference

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2917>

- CVE-2012-2155 and or finding ([Moderately critical](#))

Issue

Cross-site request forgery (CSRF) vulnerability in the CDN2 Video module 6.x for Drupal



SA-CONTRIB-2012-050

By [Drupal Security Team](#) on 28 Mar 2012 at 14:48 UTC

- Advisory ID: DRUPAL-SA-CONTRIB-2012-050
- Project: [CDN2 Video](#) (third-party module)
- Version: 6.x
- Date: 2012-March-28
- Security risk: [Moderately critical](#)
- Exploitability from: Remote
- Vulnerability: Multiple vulnerabilities

Description

CDN2 is a plug and play module and video management. The module does not sanitize output correctly, allowing Cross-site scripting (XSS) vulnerability. Additionally, the Form API is not correctly handling cross-site request forgery (CSRF) attempts.

This module relies on a backend service that is no longer supported.

For the XSS issue -
CVE: CVE-2012-2154
For the CSRF issue -
CVE: CVE-2012-2155

Impact

allows remote attackers to hijack the authentication of unspecified victims via unknown vectors.

Mitigation

Uninstall the module. This module is no longer supported.

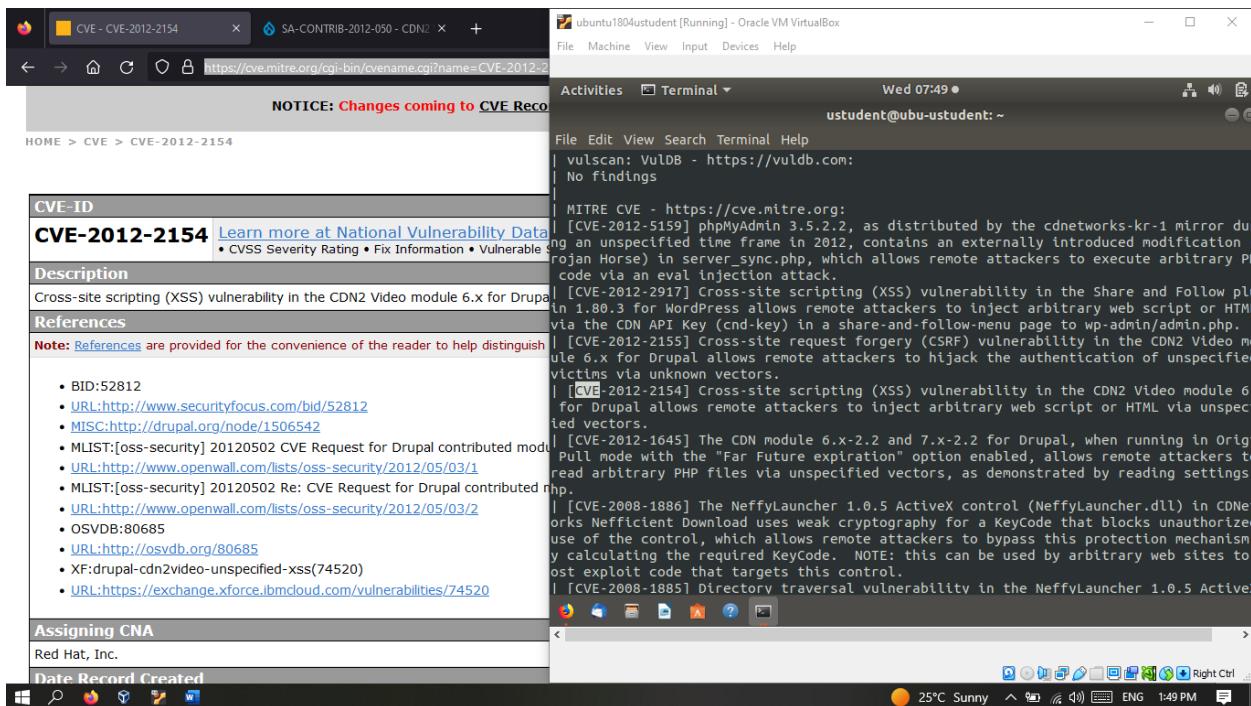
Reference

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2155>

- CVE-2012-2154 and or finding

Issue

Cross-site scripting (XSS) vulnerability in the CDN2 Video module 6.x for Drupal



Impact

allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

Mitigation

Uninstall the module. This module is no longer supported.

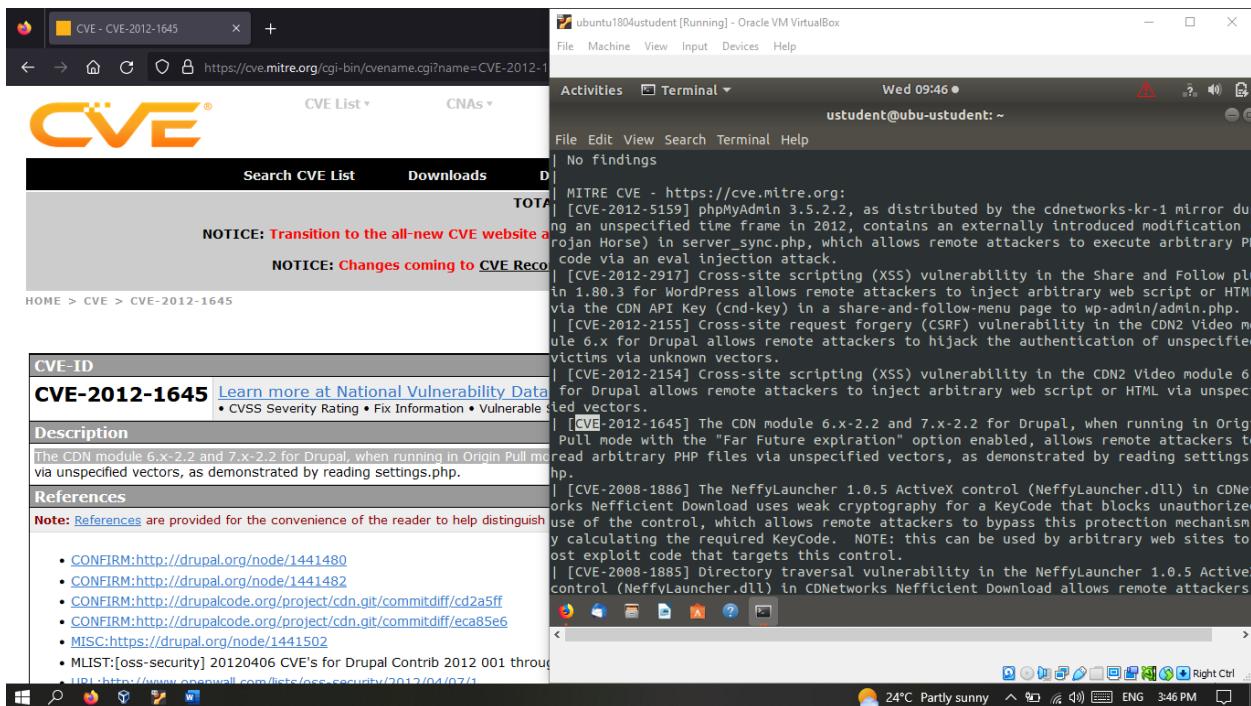
Reference

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2154>

1- CVE-2012-1645 and or finding(critical)

Issue

The CDN module 6.x-2.2 and 7.x-2.2 for Drupal, when running in Origin Pull mode with the "Far Future expiration" option enabled



Impact

allows remote attackers to read arbitrary PHP files via unspecified vectors, as demonstrated by reading settings.php.

Mitigation

Install the latest version:

- Upgrade to CDN module [6.x-2.3](#)
- Upgrade to CDN module [7.x-2.3](#)

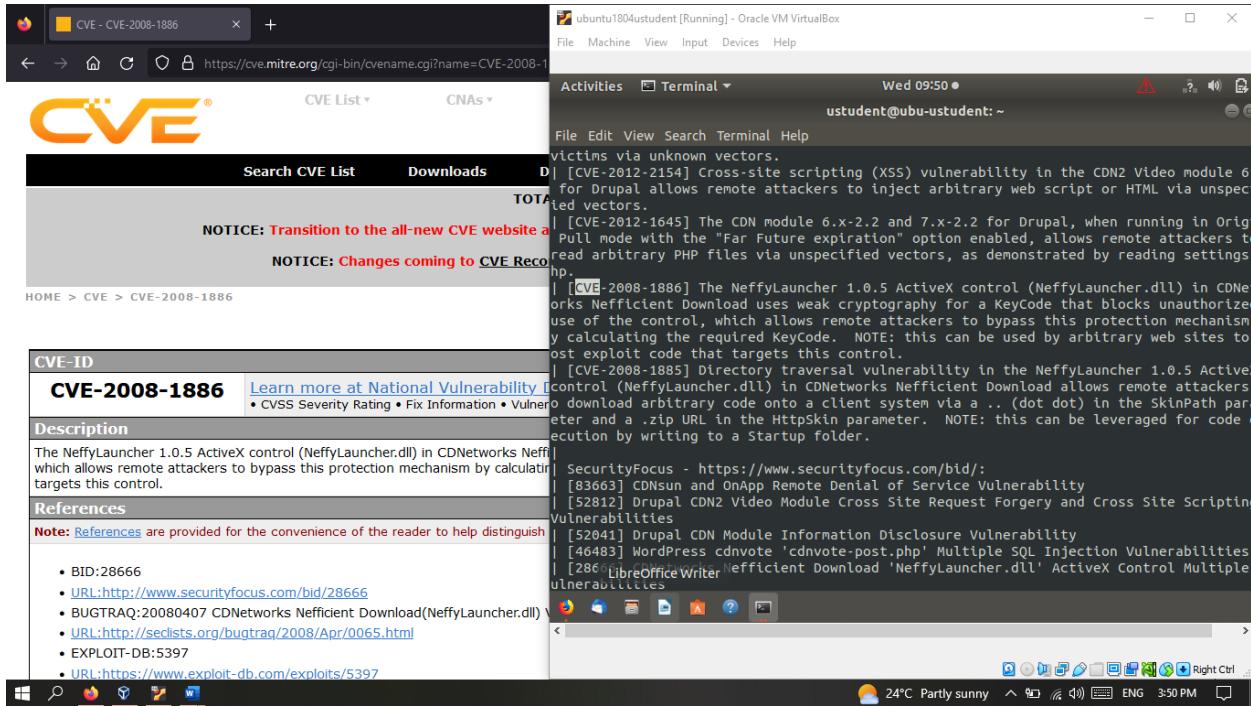
Reference

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1645>

1- CVE-2008-1886 and or finding(high)

Issue

The NeffyLauncher 1.0.5 ActiveX control (NeffyLauncher.dll) in CDNetworks Nefficient Download uses weak cryptography for a KeyCode that blocks unauthorized use of the control.



Impact

allows remote attackers to bypass this protection mechanism by calculating the required KeyCode.

Mitigation

Upgrade the vendor's patch

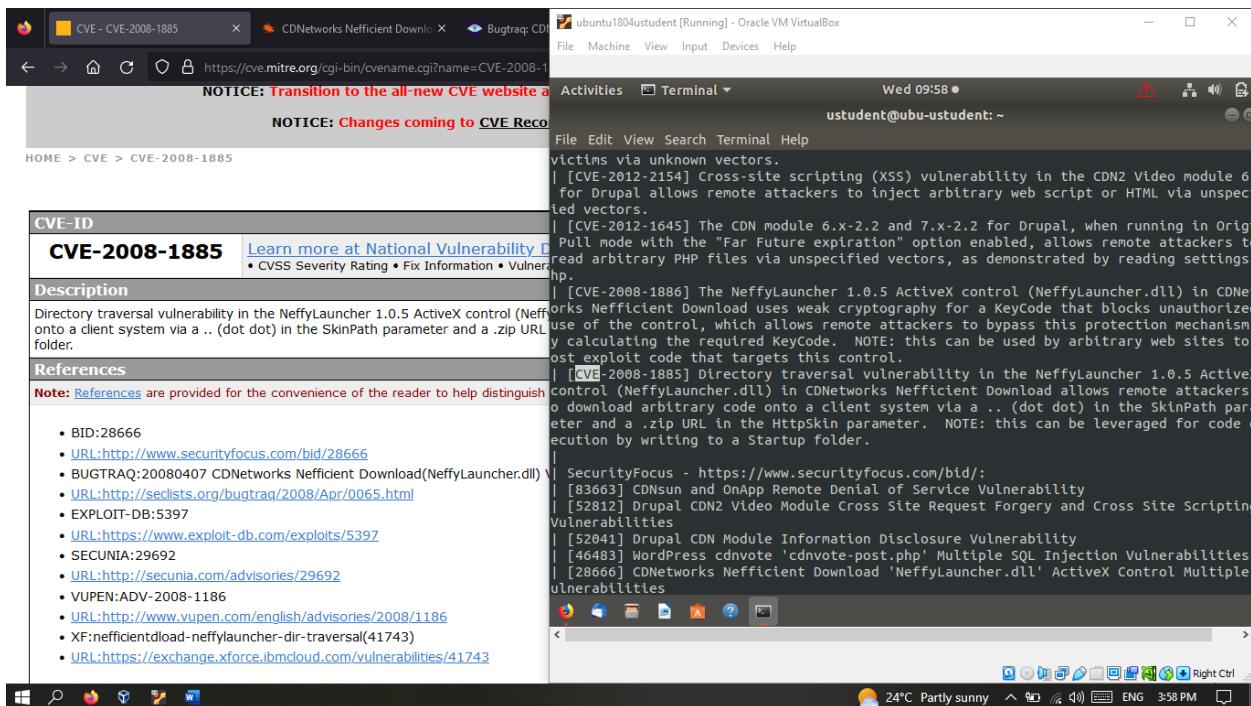
Reference

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1886>

- CVE-2008-1885 and or finding(high)

Issue

Directory traversal vulnerability in the NeffyLauncher 1.0.5 ActiveX control (NeffyLauncher.dll) in CDNetworks Nefficient Download



Impact

allows remote attackers to download arbitrary code onto a client system via a .. (dot dot) in the SkinPath parameter and a .zip URL in the HttpSkin parameter.

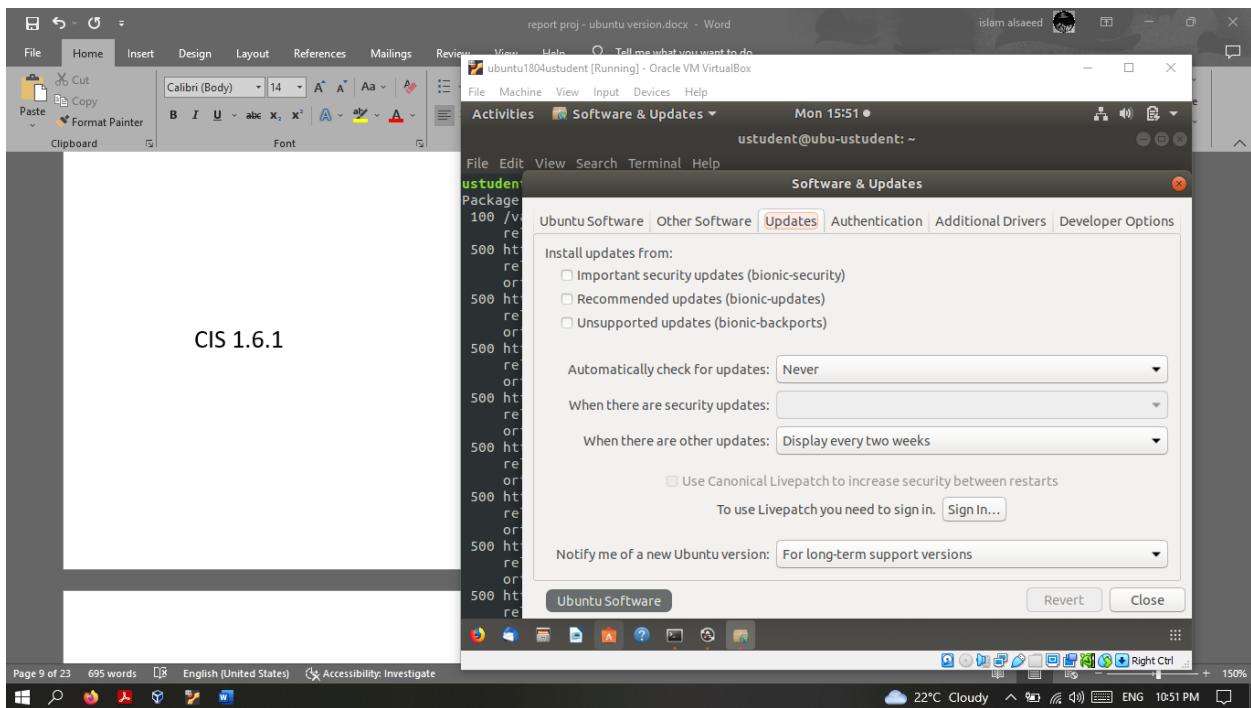
Mitigation

Upgrade the vendor's patch

Reference

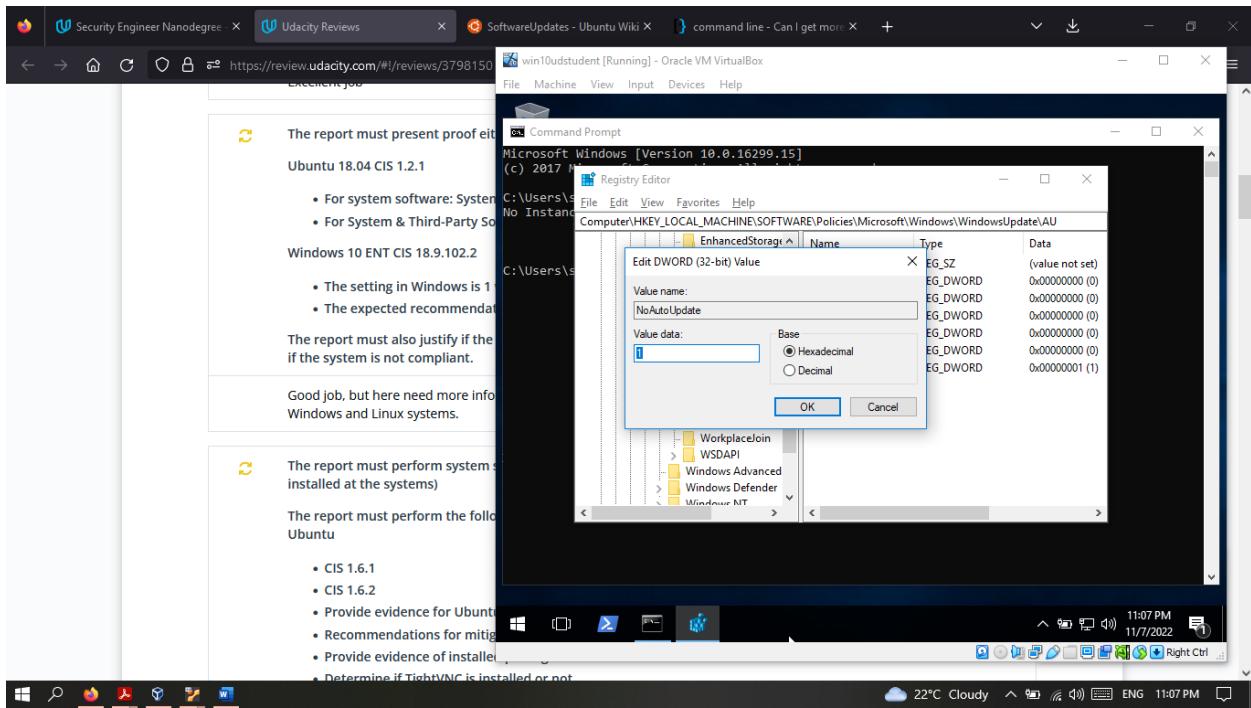
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1885>

Task 2



CIS 1.6.1

- Windows



The auto update should be set On on both machine

Task 3

CIS 1.6.1

Audit:

Run the following command and verify protection.

```
# journalctl | grep 'protection: active'
kernel: NX (Execute Disable) protection: active
```

OR

on systems without journalctl

```
# [[ -n $(grep noexec[0-9]*=off /proc/cpuinfo) || -n $(grep '\-v active) ]] && echo "NX Protection: active"
```

Nothing should be returned

CIS 1.6.2

Description:

Address space layout randomization (ASLR) randomly arranges the address space.

Rationale:

Randomly placing virtual memory regions makes it difficult for exploits as the memory placement will change each time the system boots.

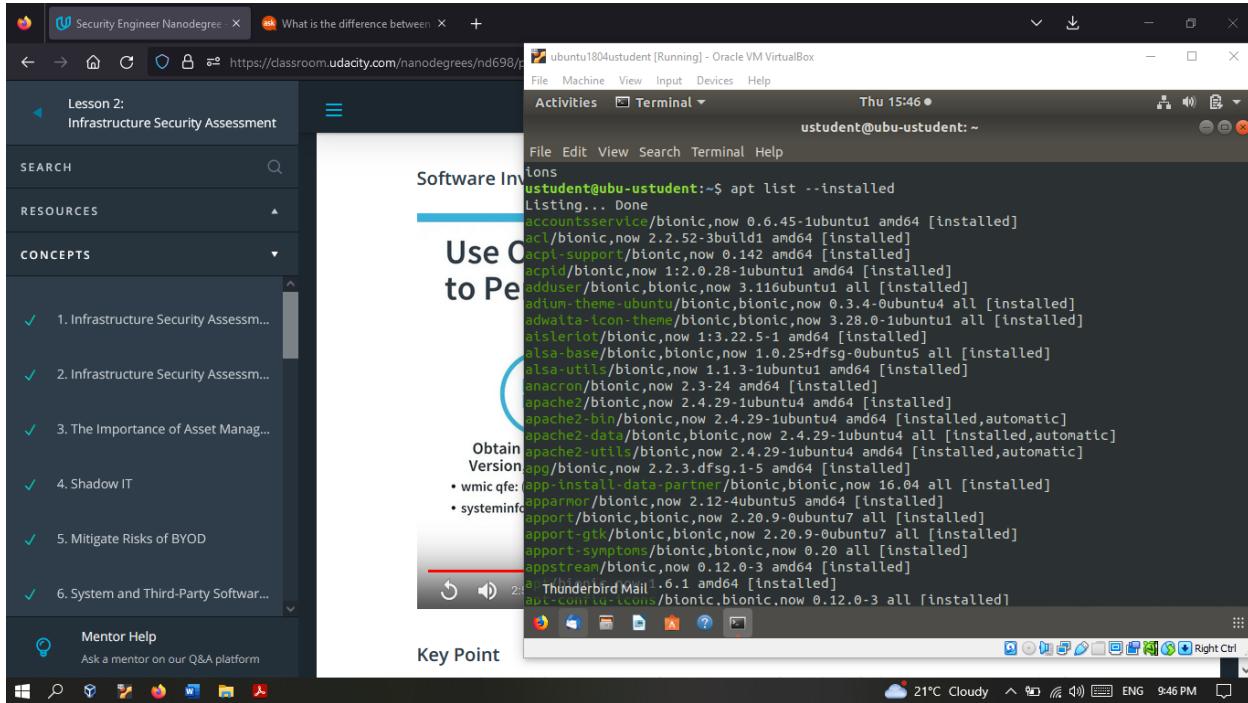
Audit:

Run the following commands and verify.

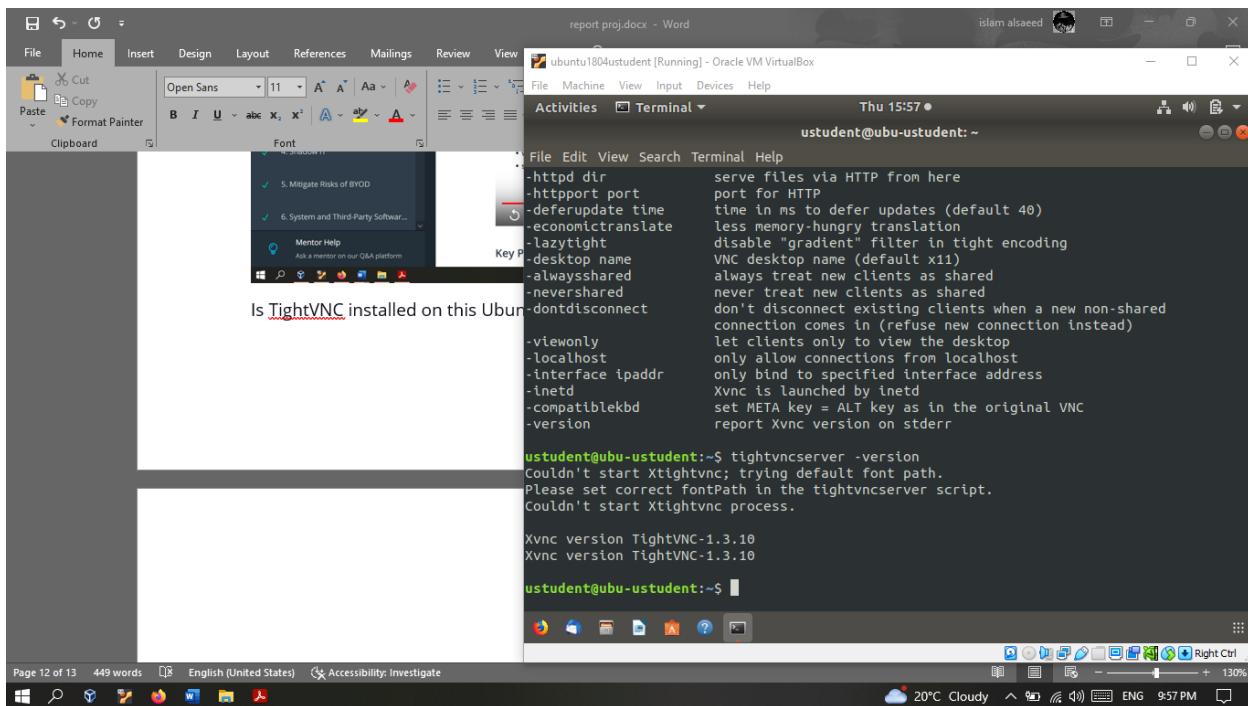
```
# sysctl kernel.randomize_va_space
kernel.randomize_va_space = 2
# grep "kernel.randomize_va_space" /etc/sysctl.conf /etc/sysctl.d/*
kernel.randomize_va_space = 2
```

are native protections applied to these systems? Yes

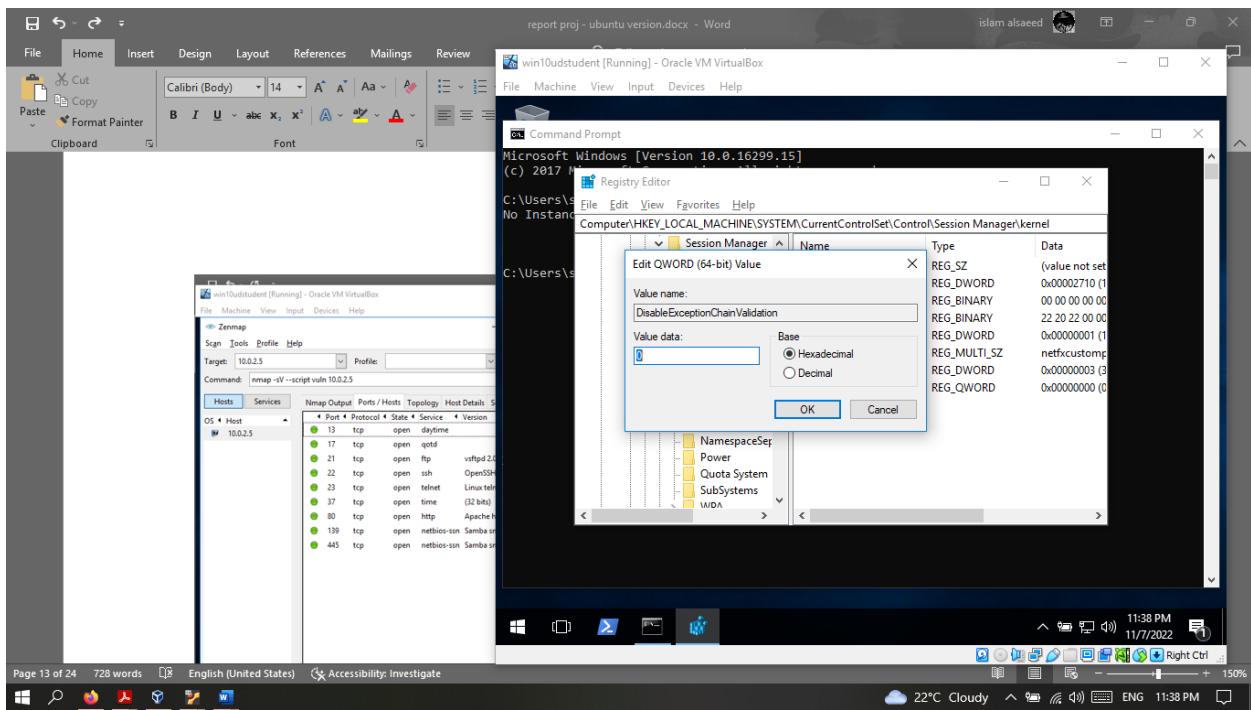
What packages are installed in this ubuntu machine?



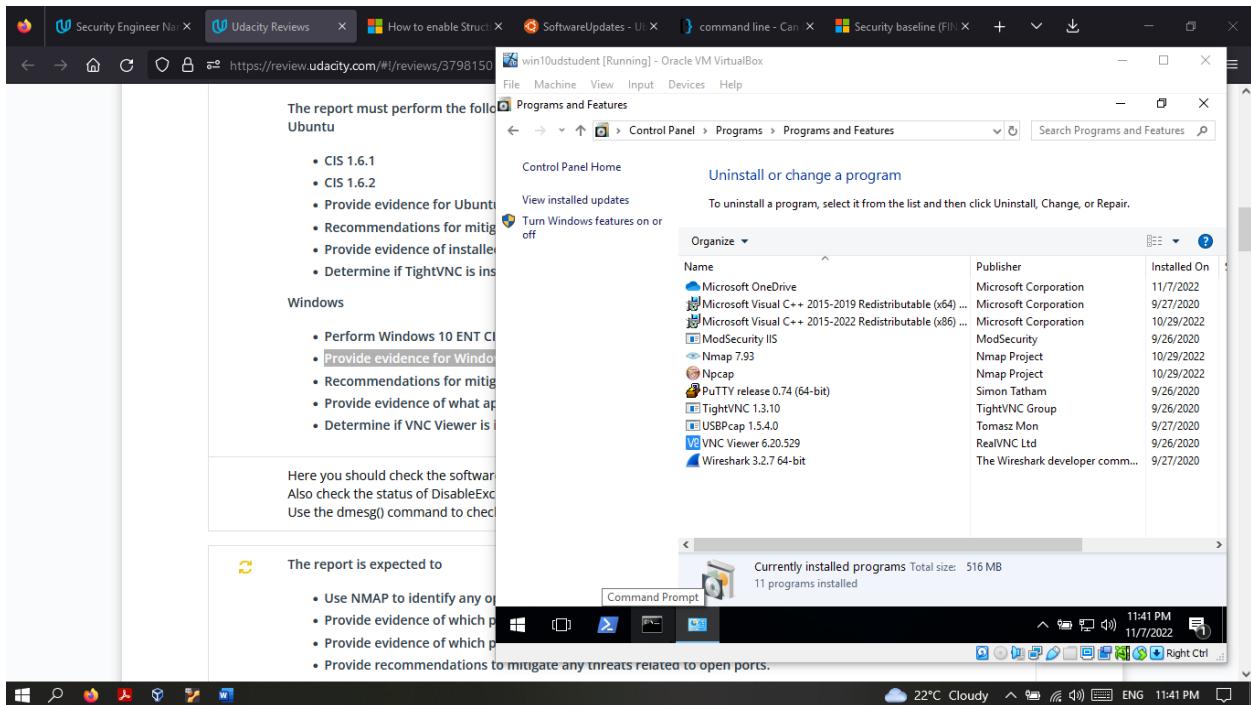
Is TightVNC installed on this Ubuntu machine? Yes



Perform Windows 10 ENT CIS 18.3.4, Provide evidence for Windows machine compliance or noncompliance? It wasn't set/found so I created it



Provide evidence of what applications are installed on the Windows machine.



Determine if VNC Viewer is installed in this Windows System? Yes its installed see above photo

Task 4

Provide evidence of which ports are open on the Windows machine

```

report proj - ubuntu version.docx - Word
islam alsaeed VM VirtualBox

ubuntu1804student [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Mon 16:50 ●
ustudent@ubu-ustudent: ~
File Edit View Search Terminal Help
Nmap scan report for 10.0.2.4
Host is up (0.0048s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE      VERSION
7/tcp      open  echo
9/tcp      open  discard?
13/tcp     open  daytime      Microsoft Windows USA daytime
17/tcp     open  qotd        Windows qotd (English)
19/tcp     open  chargen
80/tcp     open  http         Microsoft IIS httpd 10.0
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-server-header: Microsoft-IIS/10.0
135/tcp    open  msrpc       Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
3389/tcp   open  ms-wbt-server Microsoft Terminal Services
|_ssl-ccs-injection: No reply from server (TIMEOUT)
|_sslv2-down:
Service Info: Host: WIN10-USTUDENT; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_smb-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT STATUS ACCESS DENIED

11:49 PM 11/7/2022

VM VirtualBox
File Programs Help
Programs Programs and Features
Search Programs and Features
10.0.16299.15]
tion. All rights reserved.

Suffix . :
. . . . . : fe80::f44a:ea55:7b50:a5b%10
. . . . . : 10.0.2.4
. . . . . : 255.255.255.0
. . . . . : 10.0.2.1

Prefix . :
. . . . . : 2001:0:2851:782c:2cc5:20bf:6512:4c8%
. . . . . : fe80::2cc5:20bf:6512:4c8%
. . . . . : ::

11:49 PM 11/7/2022

Page 14 of 25 755 words English (United States) Accessibility: Investigate Right Ctrl
Windows Firewall Cloud 22°C Cloudy 10:55 PM ENG 11:50 PM

```

Provide evidence of which ports are open on the Ubuntu machine

```

report proj - ubuntu version.docx - Word
islam alsaeed VM VirtualBox

win10udstudent [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Zenmap Scan Tools Profile Help
Target: 10.0.2.5 Profile: Scan Cancel
Command: nmap -sV --script vuln 10.0.2.5
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host 10.0.2.5
# 10.0.2.5
13/tcp open daytime
17/tcp open qotd
21/tcp open ftp vsftpd 2.0.8 or later
22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4 (Ubuntu
23/tcp open telnet Linux telnetd
37/tcp open time (32 bits)
80/tcp open http Apache httpd 2.4.29 (Ubuntu
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workg
445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workg

Wed 16:55 ●
ustudent@ubu-ustudent: ~
Help
sys/kernel/randomize: No such file or directory
sys/va: No such file or directory
sys/space: No such file or directory
u
u root

ysctl kernel.randomize va space
sys/kernel/randomize: No such file or directory
sys/va: No such file or directory
sys/space: No such file or directory
ysctl kernel.randomize_va_space
= 2
rep "kernel.randomize_va_space" /etc/sysctl.conf /etc/sysctl
rep "kernel.randomize_va_space" /etc/sysctl.conf /etc/sysctl
rep "kernel.randomize_va_space" /etc/sysctl.conf /etc/sysctl
ysctl -w kernel.randomize_va_space=
on key 'kernel.randomize_va_space'
udo sysctl -w kernel.randomize_va_space=2
= 2

10:55 PM 11/2/2022

VM VirtualBox
File Programs Help
Programs Programs and Features
Search Programs and Features
Page 3 of 19 3196 words English (United States) Accessibility: Investigate Right Ctrl
Windows Firewall Cloud 22°C Cloudy 10:55 PM ENG 10:55 PM

```

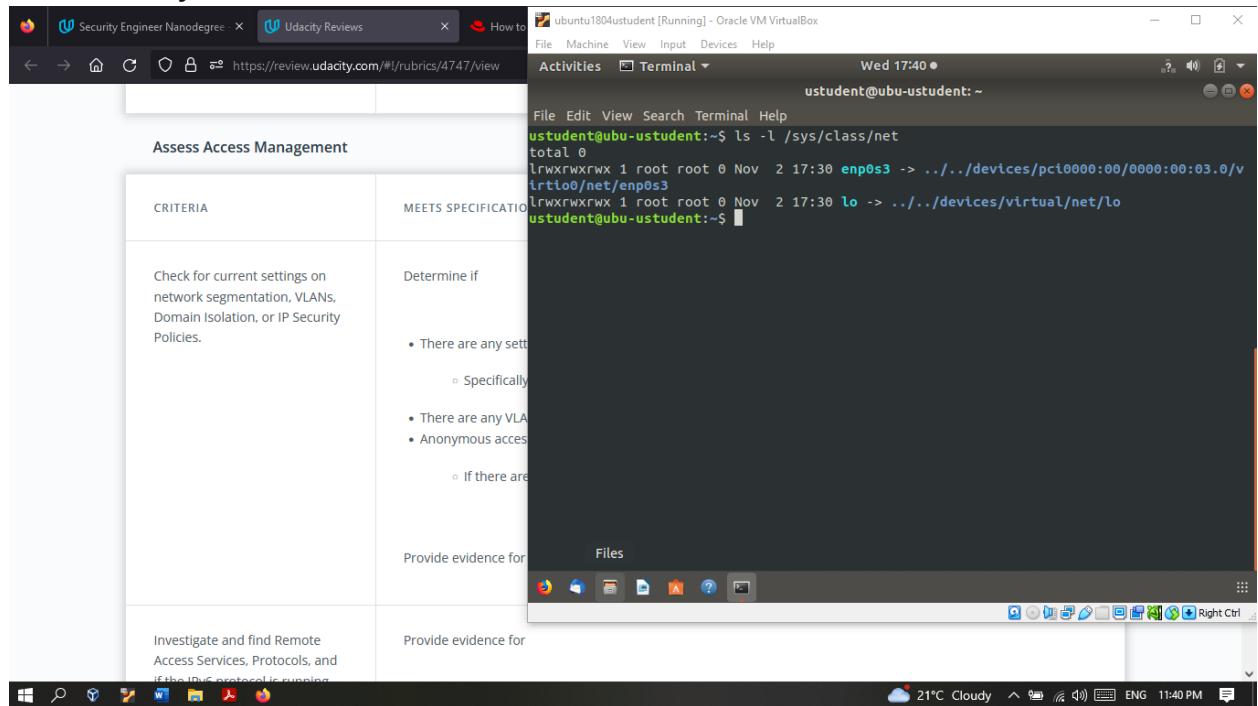
Recommendations:

Close/Disable any services that not being used

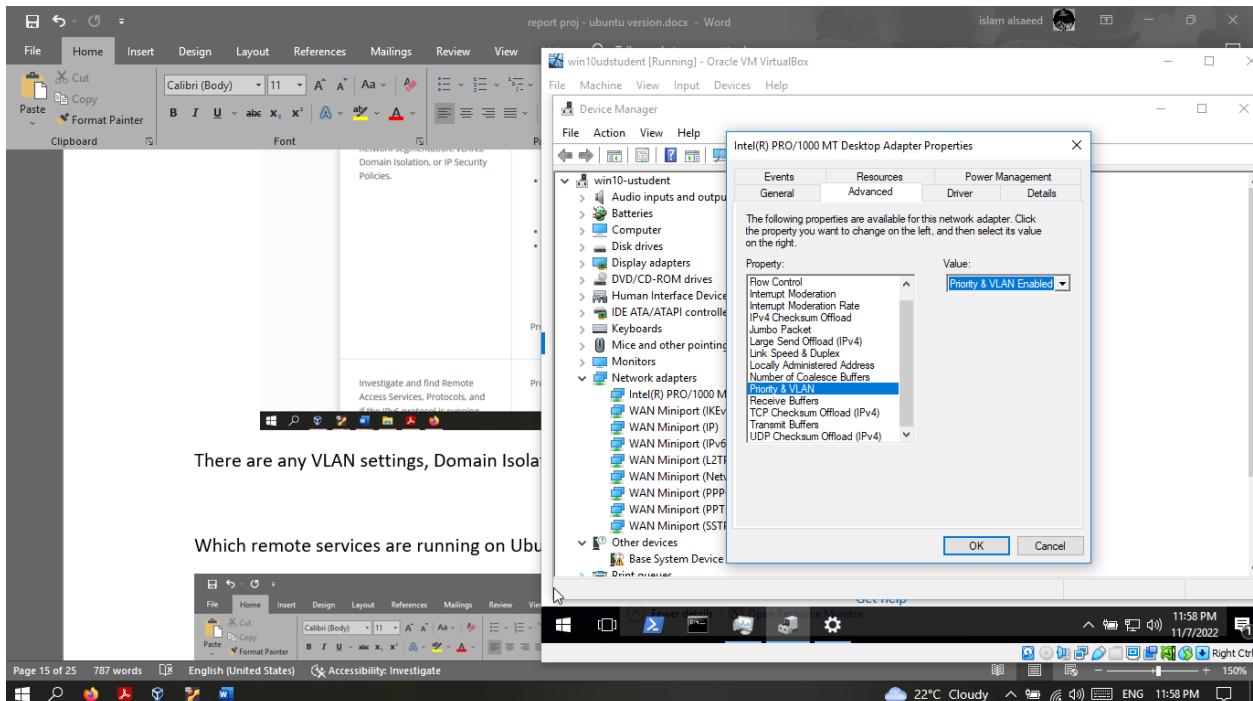
STEP 2

Task 1

- Are there any VLANs? No

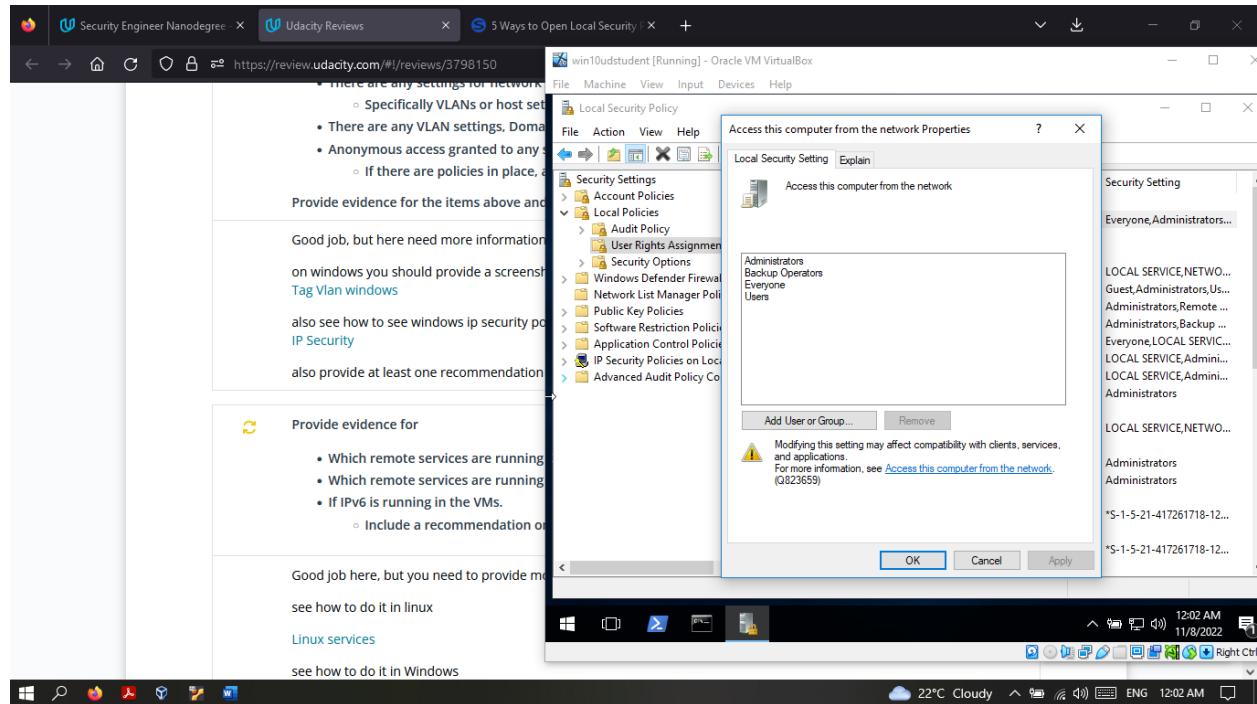


There are any VLAN settings, Domain Isolation, IP Security Policies on Windows?



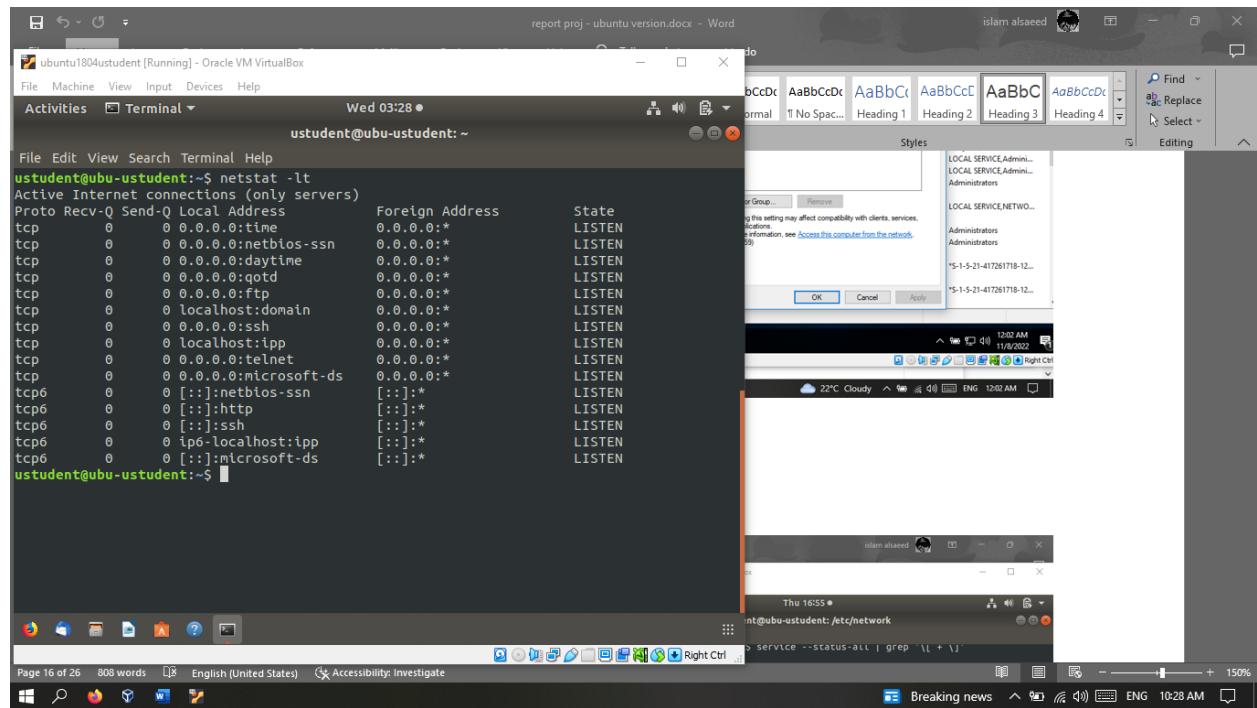
Anonymous access granted to any share

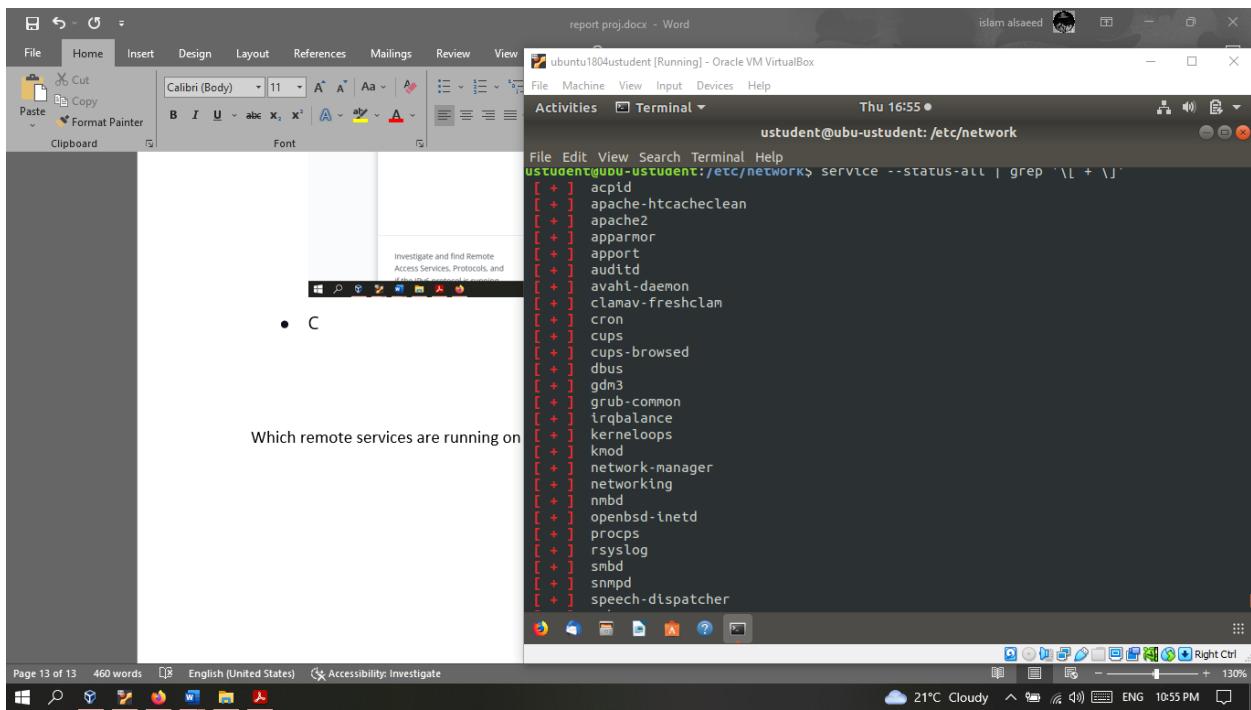
- If there are policies in place, are they enforced?



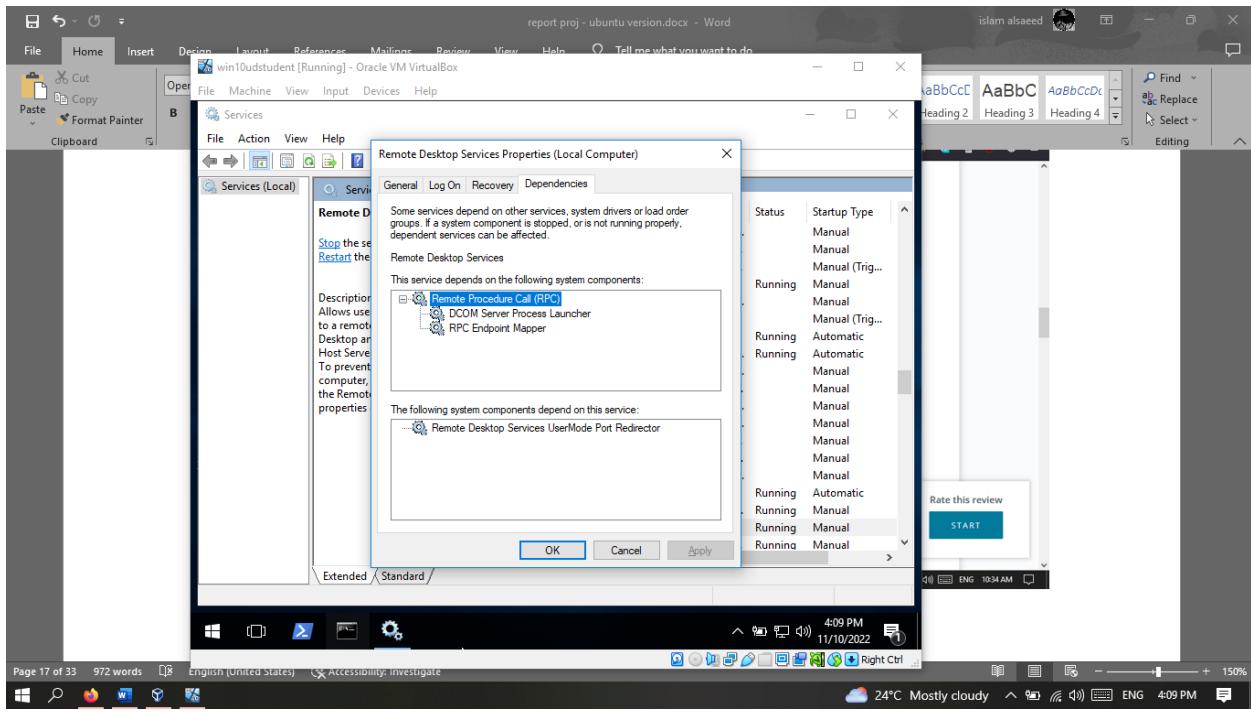
Task 2

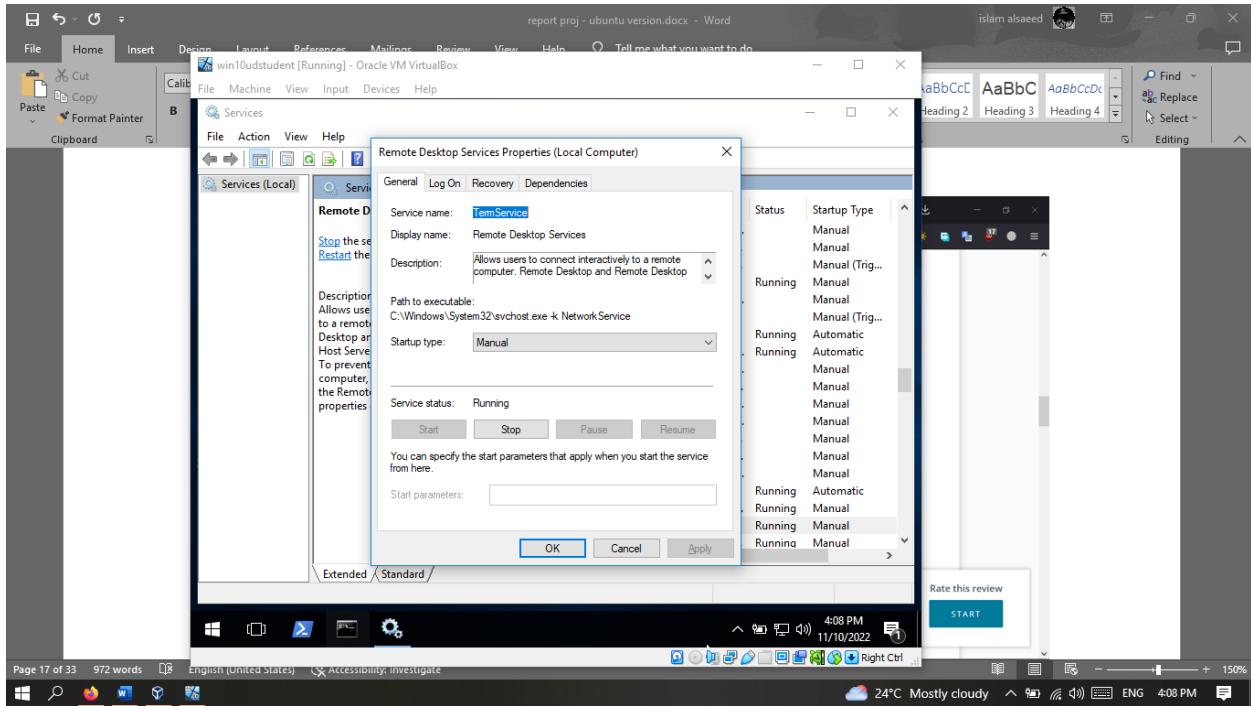
Which remote services are running on Ubuntu? SSH, VNC





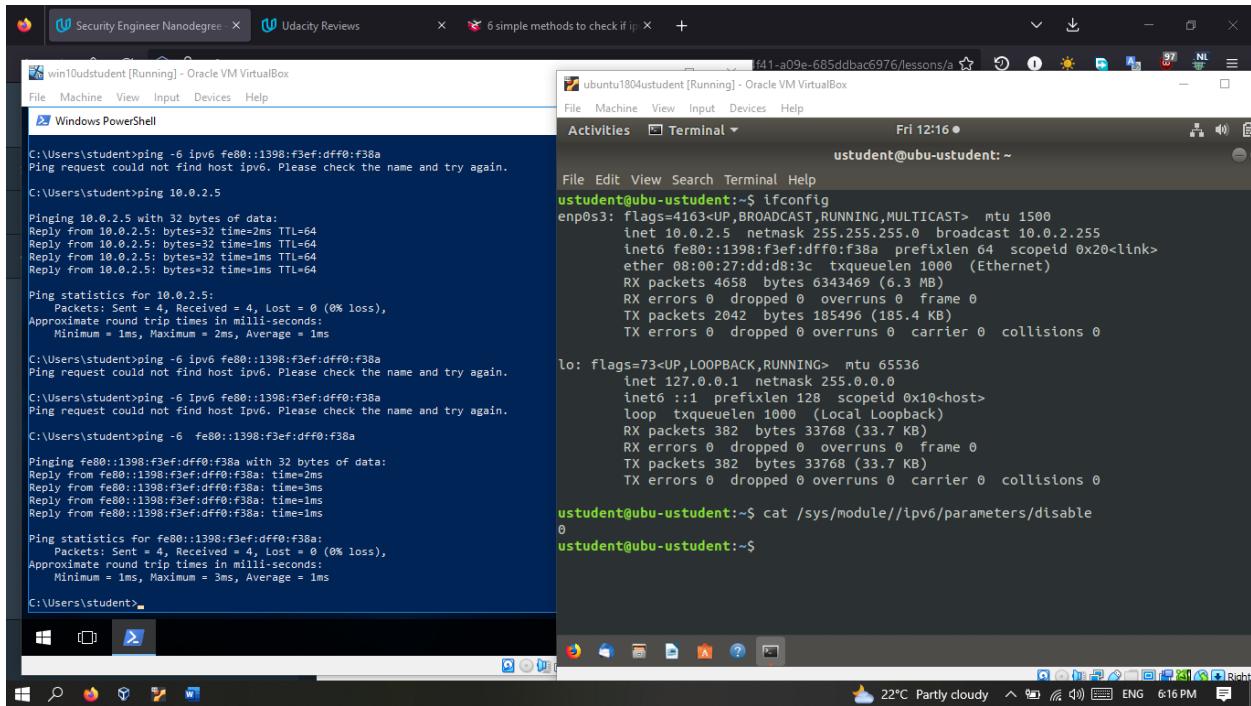
Which remote services are running on Windows?



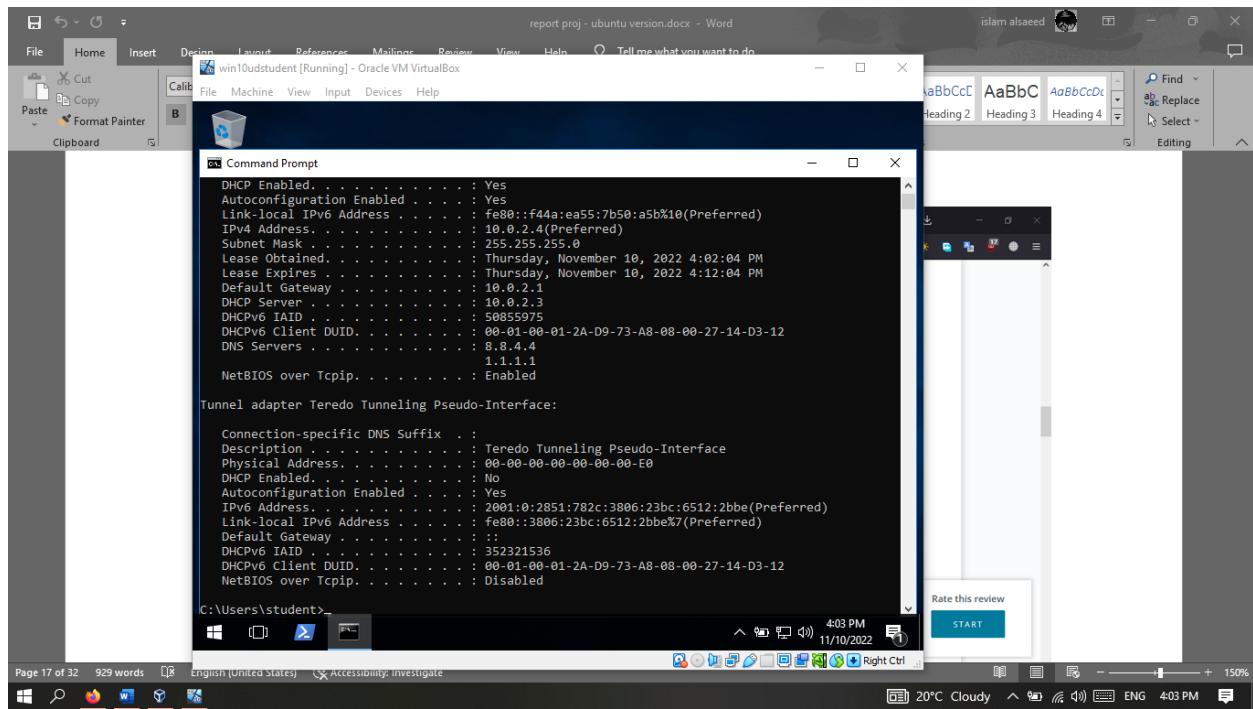
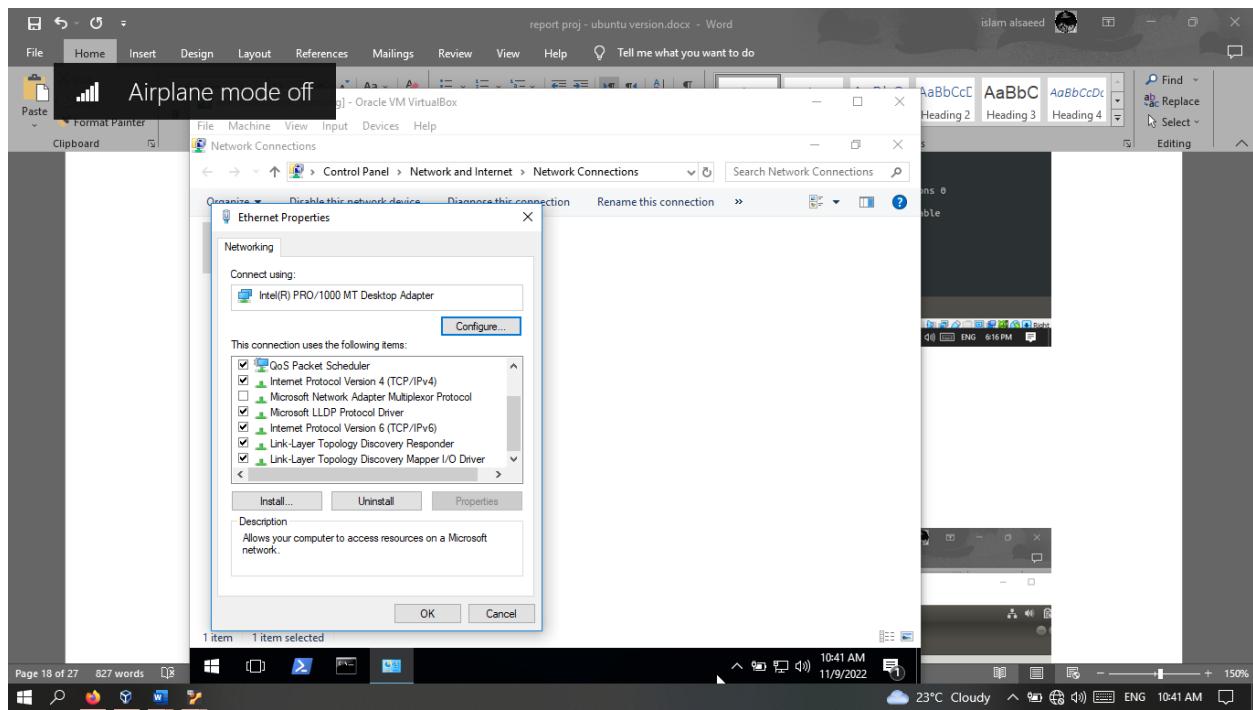


If IPv6 is running in the VMs?

On Linux? Yes , 0 means its running



In windows ? also yes



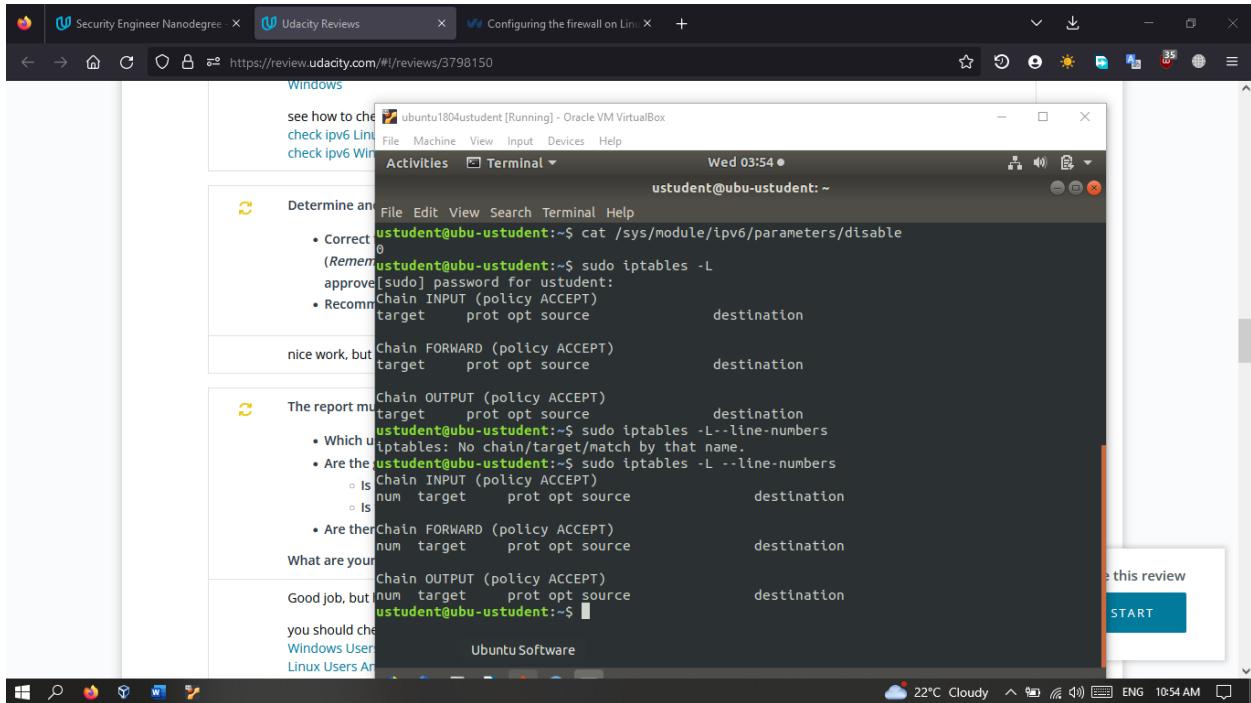
Include a recommendation on whether IPv6 is needed and how to address this?

Since IPv6 is not widely used and all the protection that applied to IPv4 does not always work on IPv6 so its best to be turned off unless its needed.

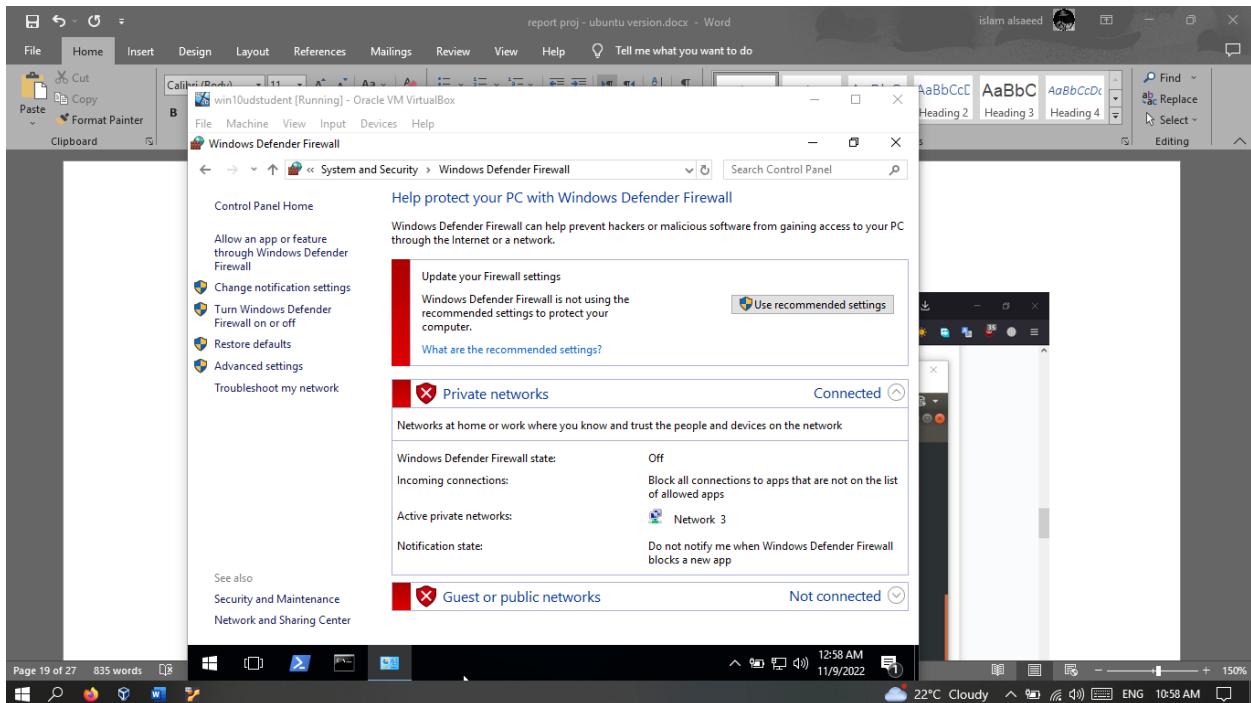
Task 3

Correct firewall configuration in the targeted systems?

In Linux ? No there is no policies configured



In windows ? its not On



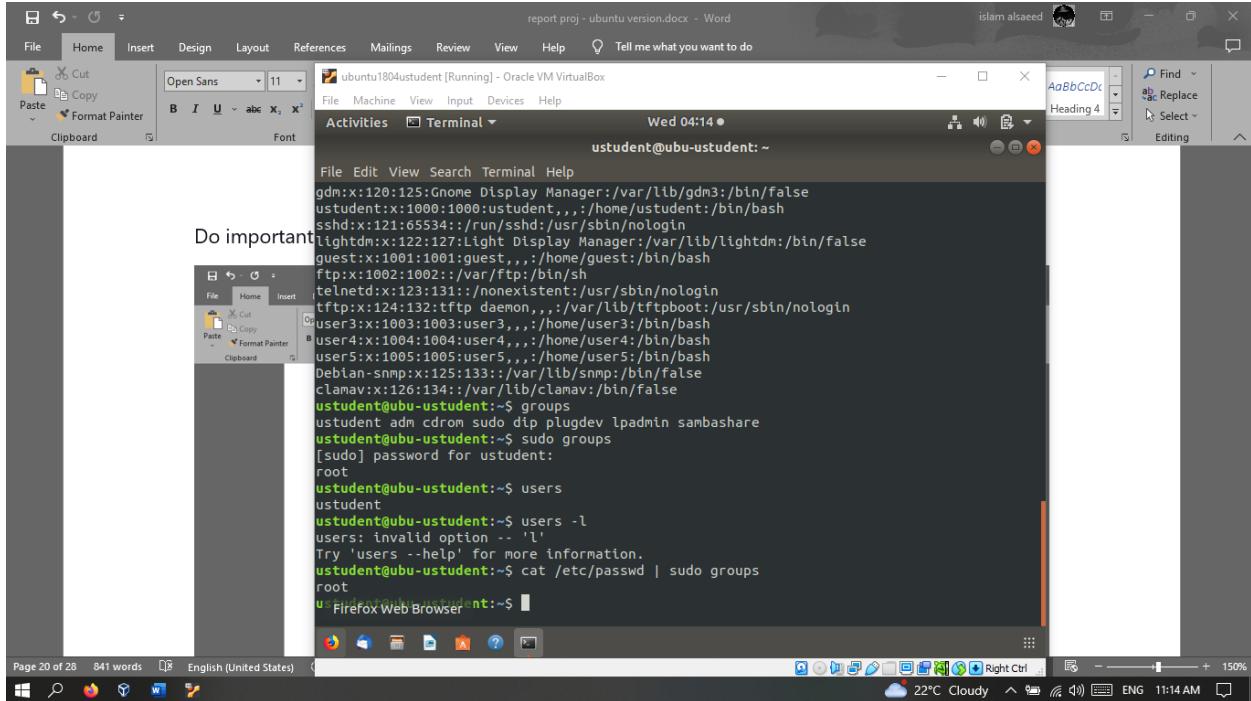
what ports would you suggest to have open and running and why?

22, because its encrypted

Task 4

Which users have high privileges?

In Linux ? is root



Do important PII folders have the correct permissions and ownership? I have no such folder

A screenshot of a Windows desktop environment. On the left is a Microsoft Word document titled "report proj.docx" with the text "Correct firewall configuration". On the right is a terminal window titled "Terminal" showing a Linux shell session. The terminal output includes:

```
report proj.docx - Word
Islam alsaeed
File Edit View Terminal Help
Activities Terminal Fri 16:41 ● uststudent@ubu-ustudent: ~
File Edit View Search Terminal Help
.bashrc      ftpvuln.txt    .profile      .vnc
.cache       .gnupg        Public        vsftpd-2.3.4-infected
.config      .hiddenfile.txt scipag_vulscan .xauthority
.dbus        .ICEAuthority  .ssh          .xsession-errors
.dbus         .ICEAuthority  .ssh          .xsession-errors
uststudent@ubu-ustudent:~$ ls
'+' Downloads Pictures Templates
aclfile.txt examples.desktop Public Videos
Desktop ftpvuln.txt scipag_vulscan vsftpd-2.3.4-infected
Documents Music telnetloginattempts.pcap
uststudent@ubu-ustudent:~$ cd /
uststudent@ubu-ustudent:~/ls
bin dev initrd.img lib64 mnt root snap sys var
boot etc initrd.img.old lost+found opt run srv tmp vmlinuz
cdrom home lib media proc sbin swapfile usr
uststudent@ubu-ustudent:/S cd home/
uststudent@ubu-ustudent:/home$ ls
guest user3 user4 user5 uststudent
uststudent@ubu-ustudent:/home$ cd us
bash: cd: us: No such file or directory
uststudent@ubu-ustudent:/home$ cd uststudent/
uststudent@ubu-ustudent:~/ls
'+' Downloads Pictures Templates
aclfile.txt examples.desktop Public Videos
Desktop ftpvuln.txt scipag_vulscan vsftpd-2.3.4-infected
Documents Music telnetloginattempts.pcap
uststudent@ubu-ustudent:~$
```

The taskbar at the bottom shows icons for File Explorer, Task View, Start, and other system icons. The system tray indicates it's 19°C, mostly cloudy, and the date/time is Fri 10:41 PM.

Are the default settings correct, and are there any excessive permissions? no

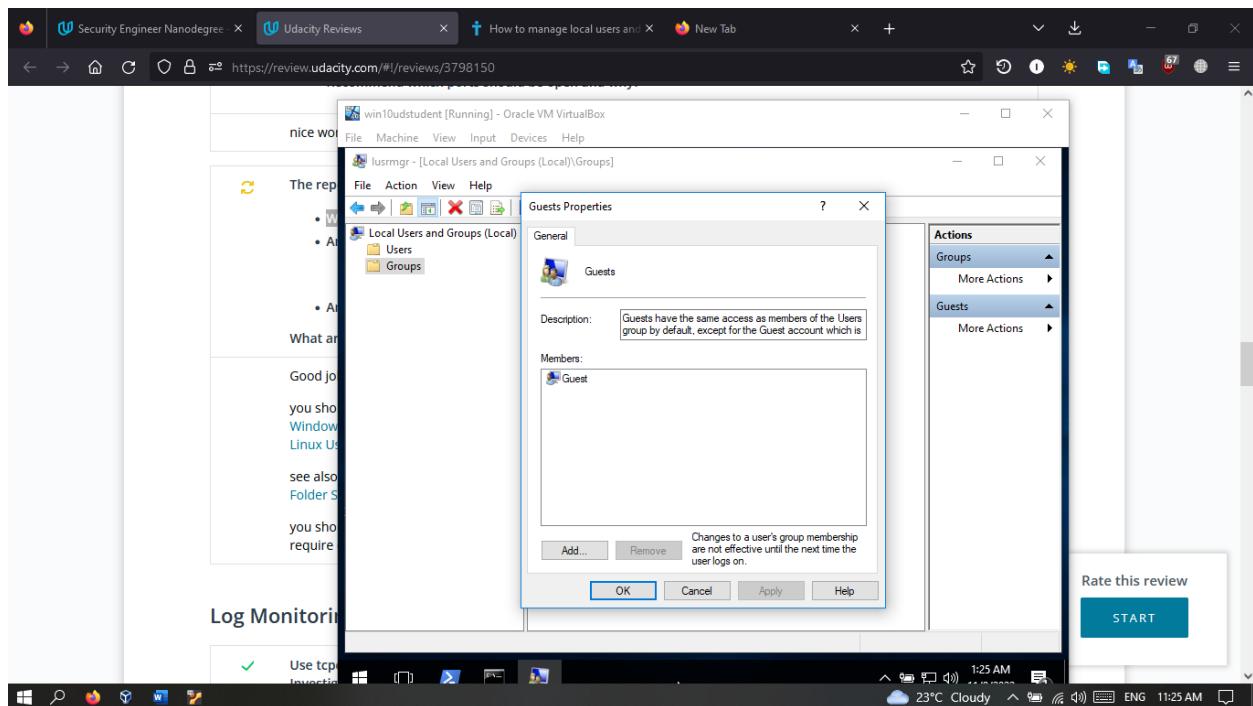
A screenshot of a Windows desktop environment. On the left is a Microsoft Word document titled "report proj.docx" with the text "Correct firewall configuration". On the right is a terminal window titled "Terminal" showing a Linux shell session. The terminal output includes:

```
report proj.docx - Word
Islam alsaeed
File Edit View Terminal Help
Activities Terminal Fri 16:38 ● uststudent@ubu-ustudent: ~
File Edit View Search Terminal Help
# See the man page for details on how to write a sudoers file.
#
Defaults      env_reset
Defaults      mail_badpass
Defaults      secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"
#
# Host alias specification
#
# User alias specification
#
# Cmnd alias specification
#
# User privilege specification
root    ALL=(ALL:ALL) ALL
#
# Members of the admin group may gain root privileges
%admin  ALL=(ALL) ALL
#
# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL
#
# See sudoers(5) for more information on "#include" directives:
#include /etc/sudoers.d
uststudent@ubu-ustudent:~/ls
bin dev initrd.img lib64 mnt root snap sys var
```

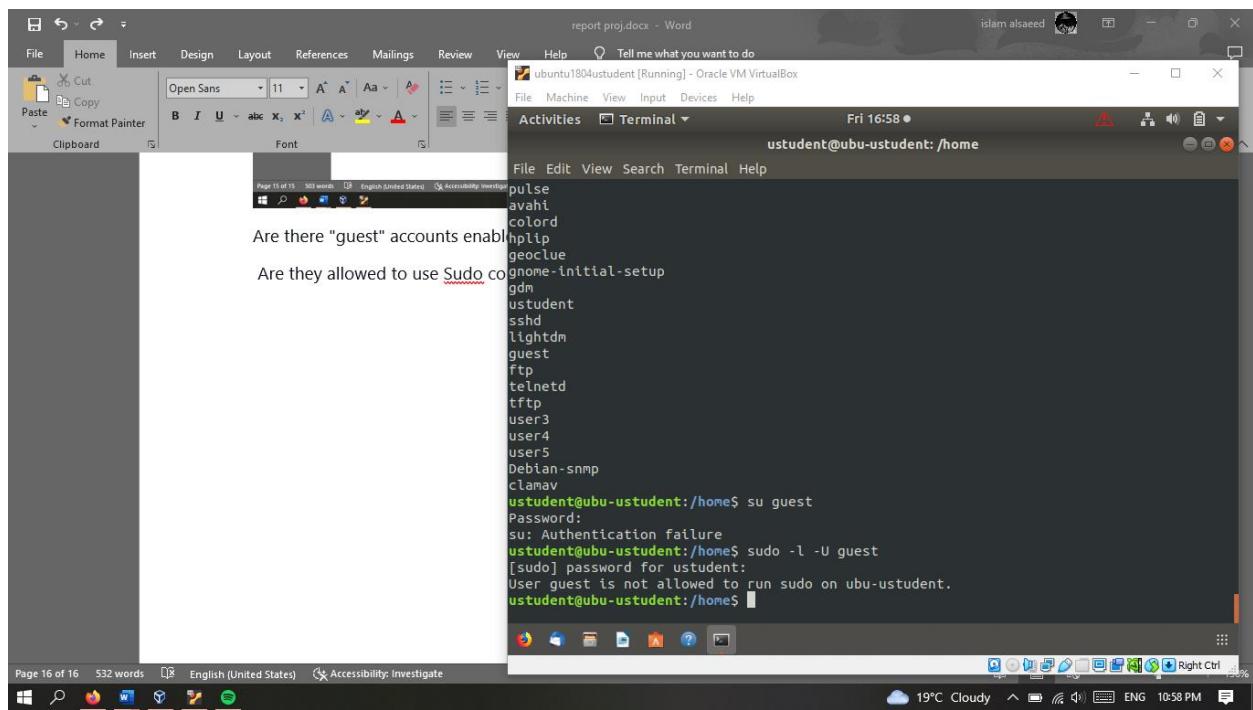
The taskbar at the bottom shows icons for File Explorer, Task View, Start, and other system icons. The system tray indicates it's 19°C, mostly cloudy, and the date/time is Fri 10:38 PM.

Are there "guest" accounts enabled? Yes

Is the guest account allowed to run as administrator in Windows? no

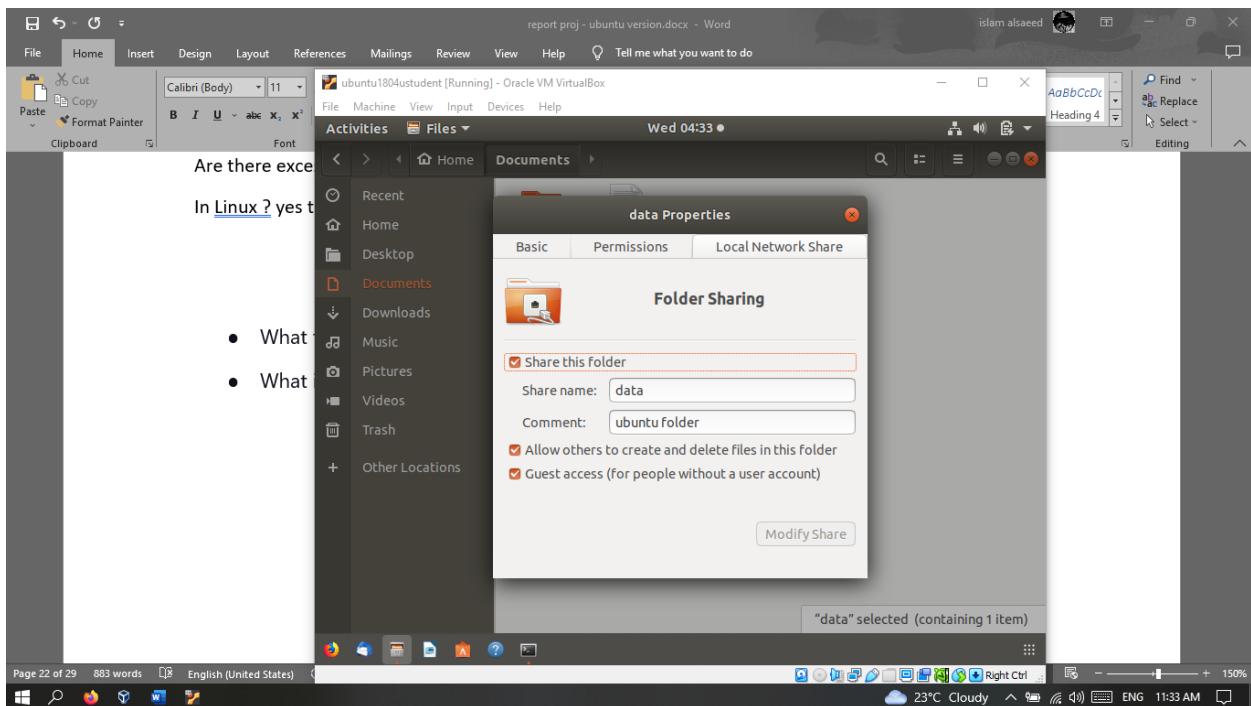


Are they allowed to use Sudo commands? No

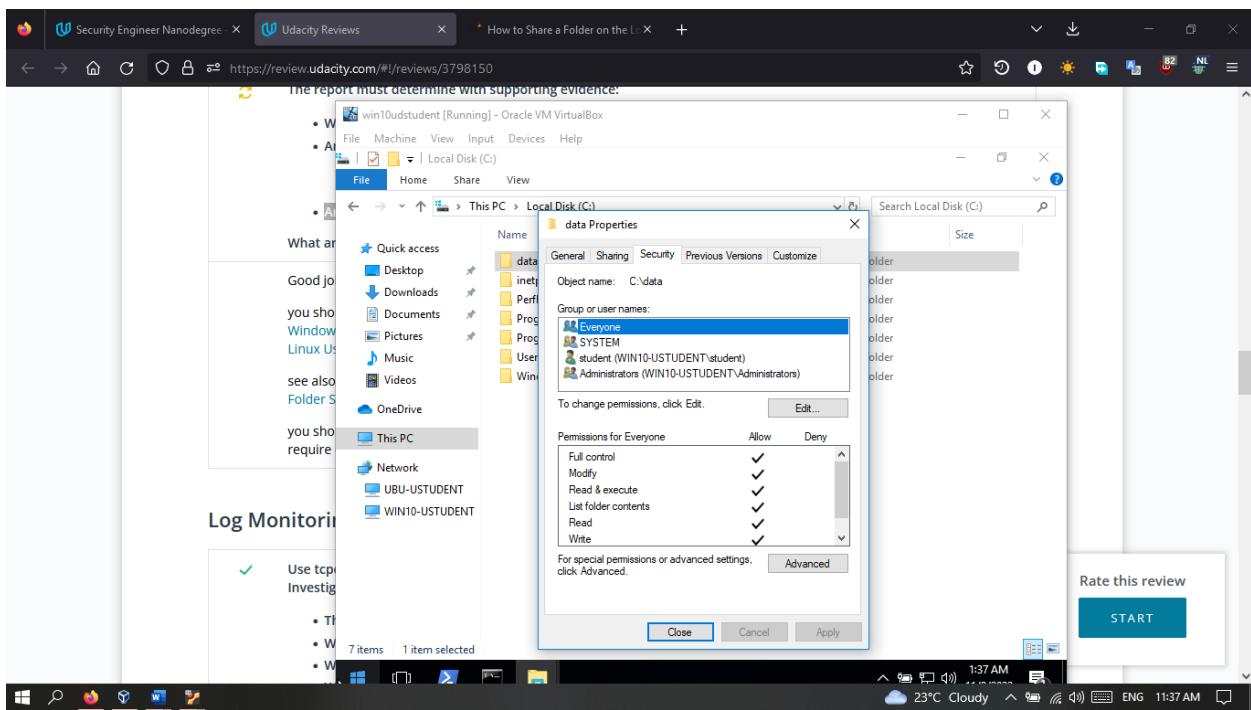


Are there excessive permissions on the data folder in each machine?

In Linux ? yes there is excessive permission



In windows ? yes

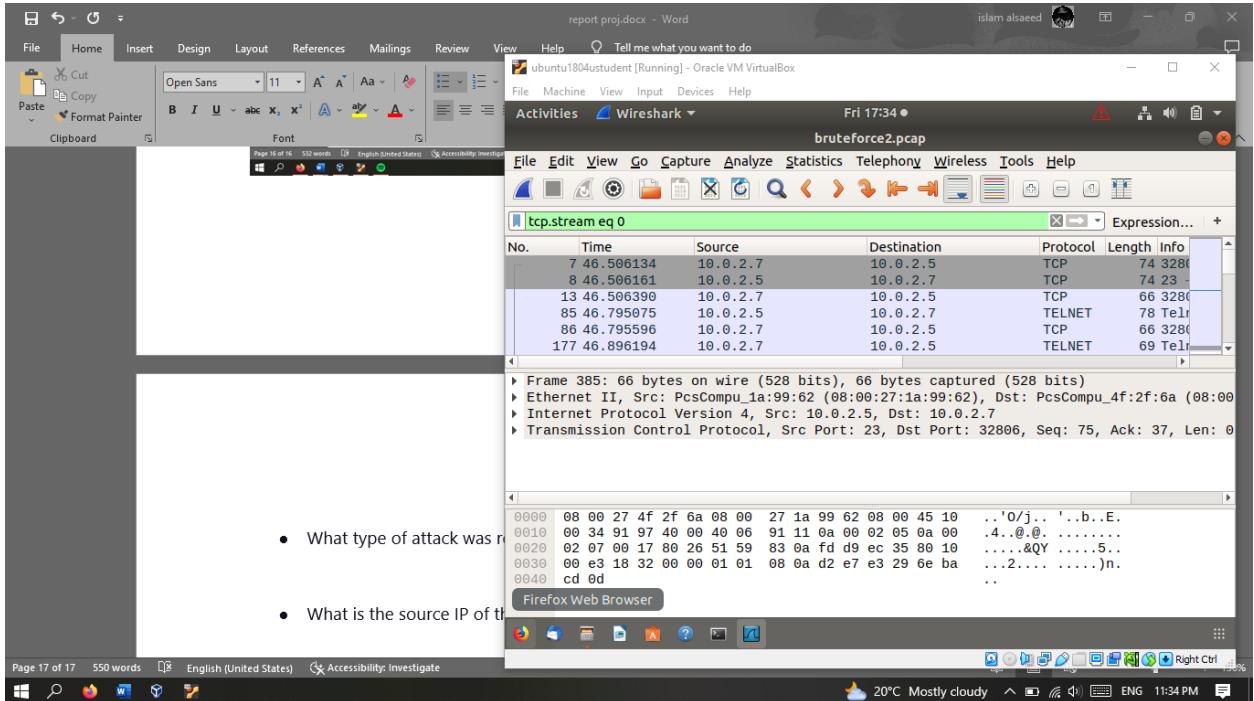


should be restricted to users who must have access for work on both machines

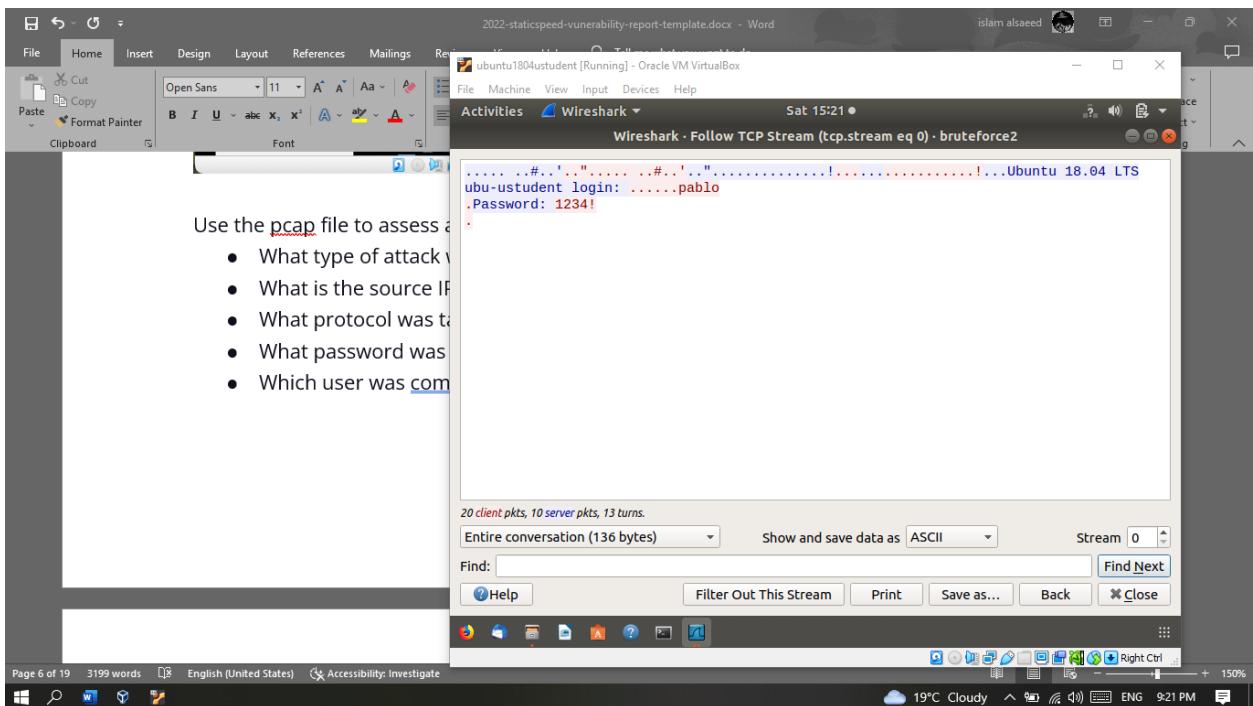
Step 3

Task 1

- What type of attack was recorded? Brute force
- What is the source IP of the attack? 10.0.2.7

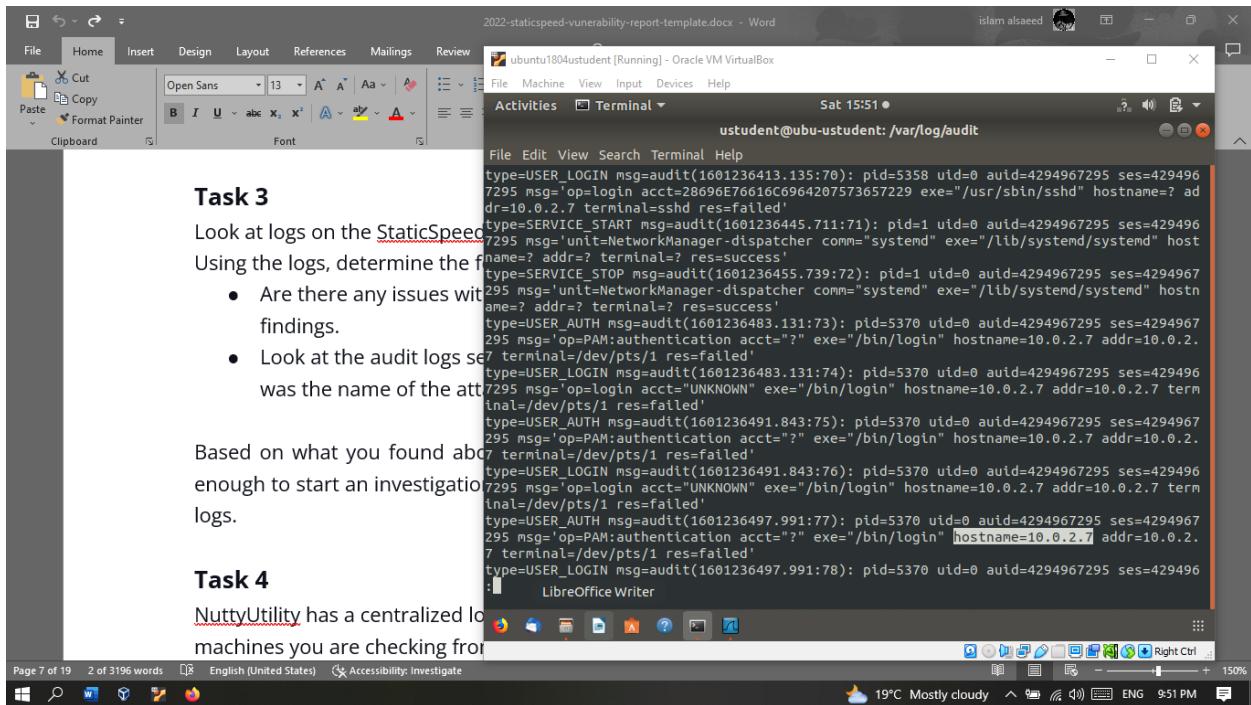


- What protocol was targeted? TCP
- What password was used successfully? 1234!
- Which user was compromised?....pablo



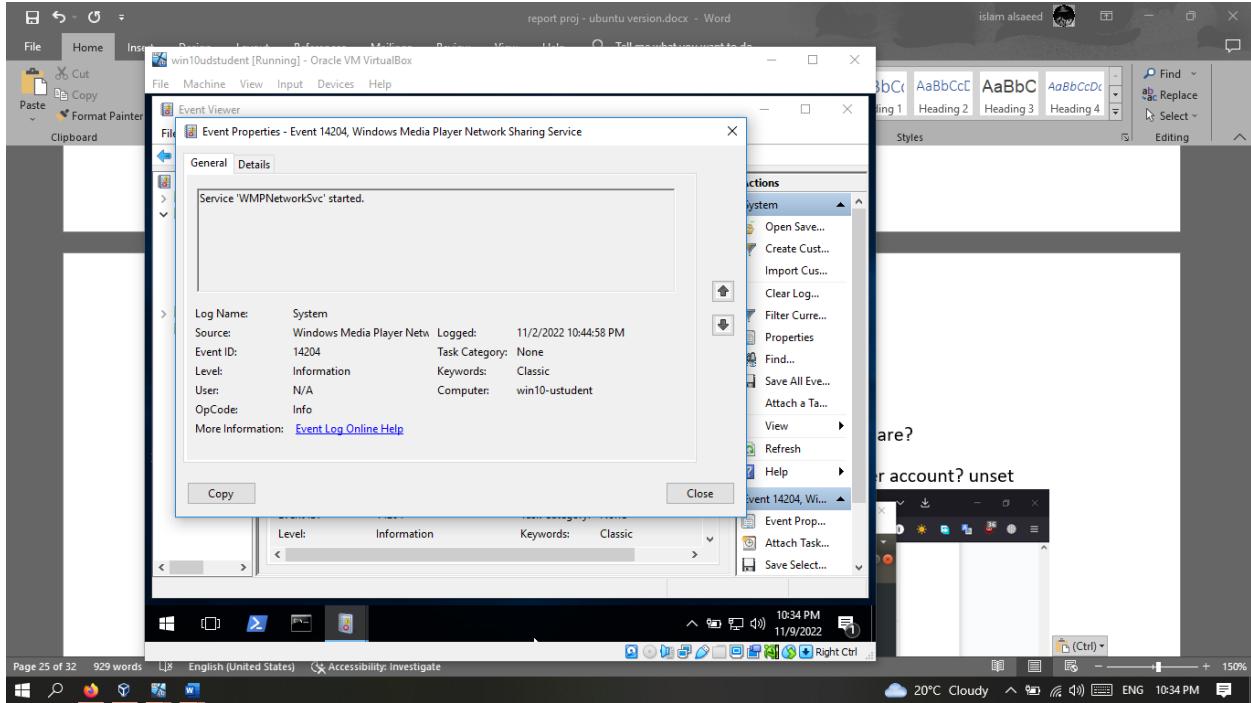
Task 2

Look at the audit logs setup at your Linux machine and find the audit.log file. What was the name of the attacker's account? Please provide screenshots

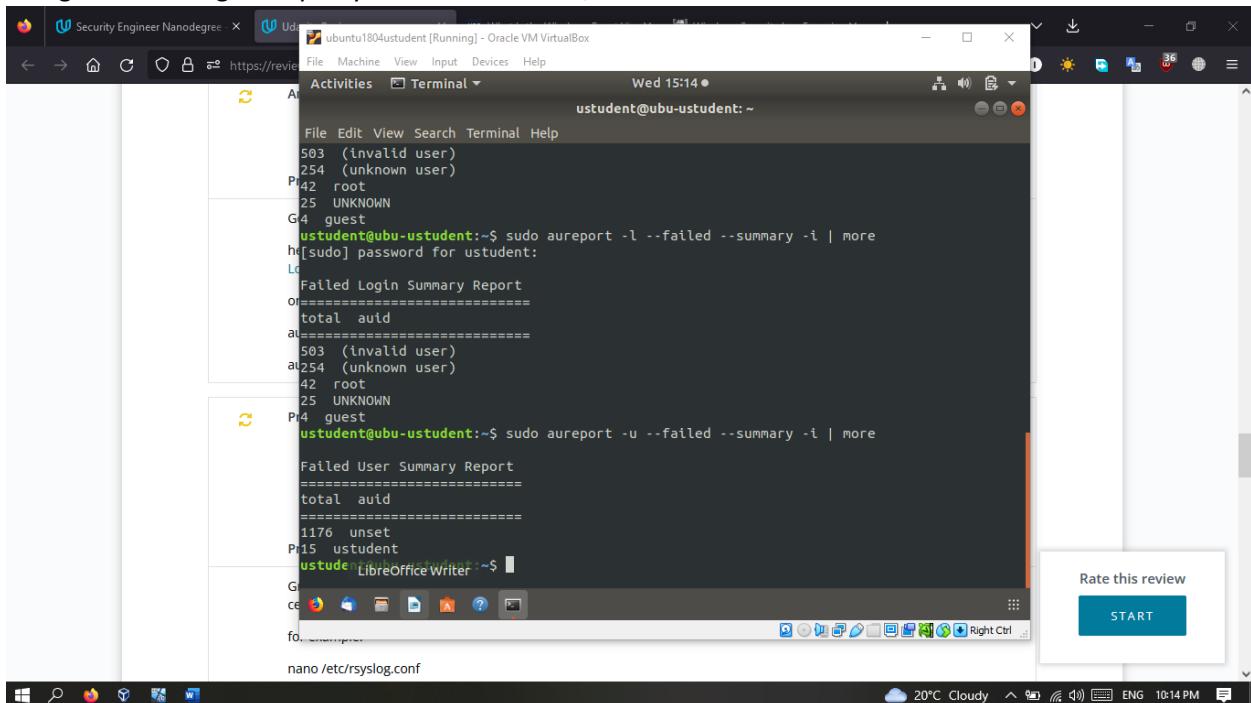


Task 3

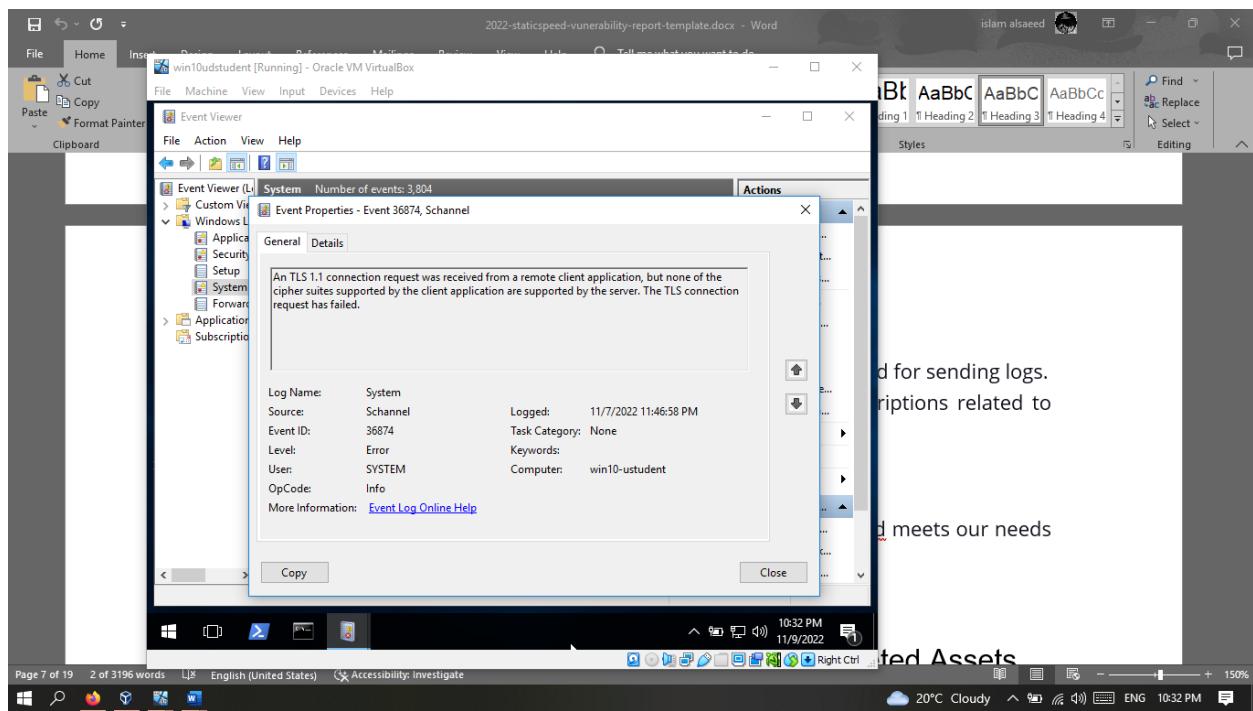
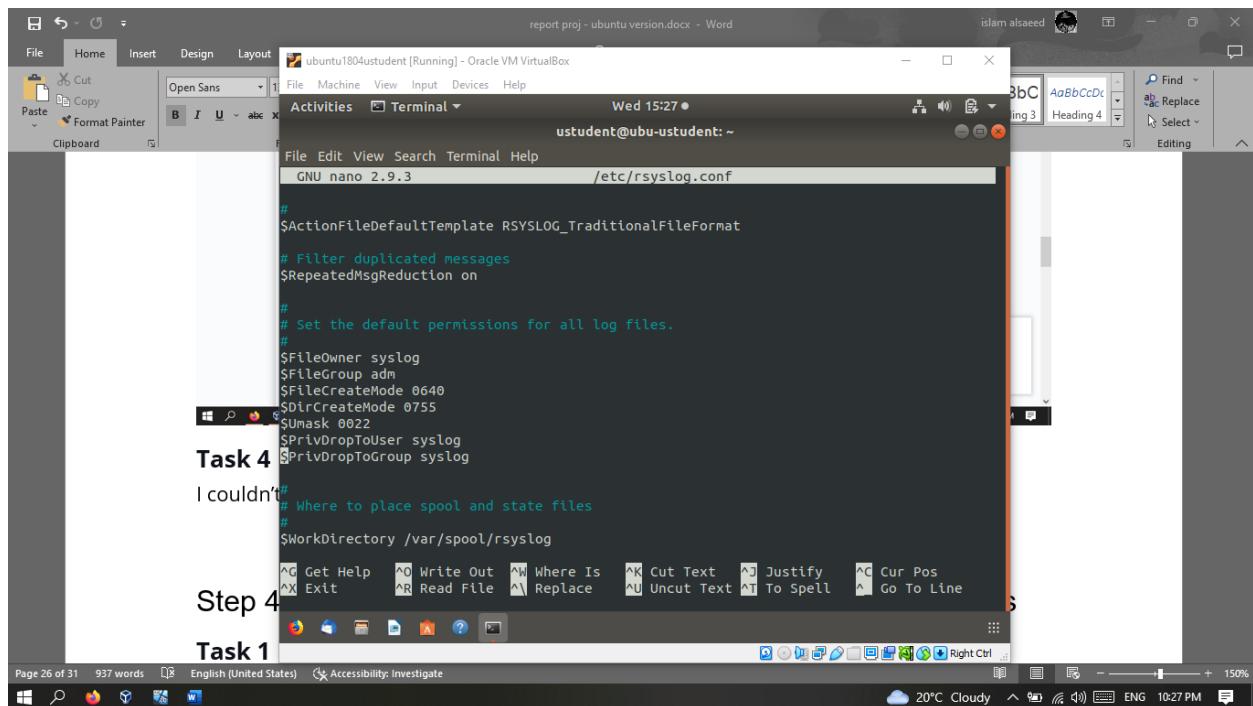
Was there an account uncharacteristic of Windows trying to access the Windows share?



Using the audit logs setup at your Linux machine, what was the name of the attacker account? unset



Task 4

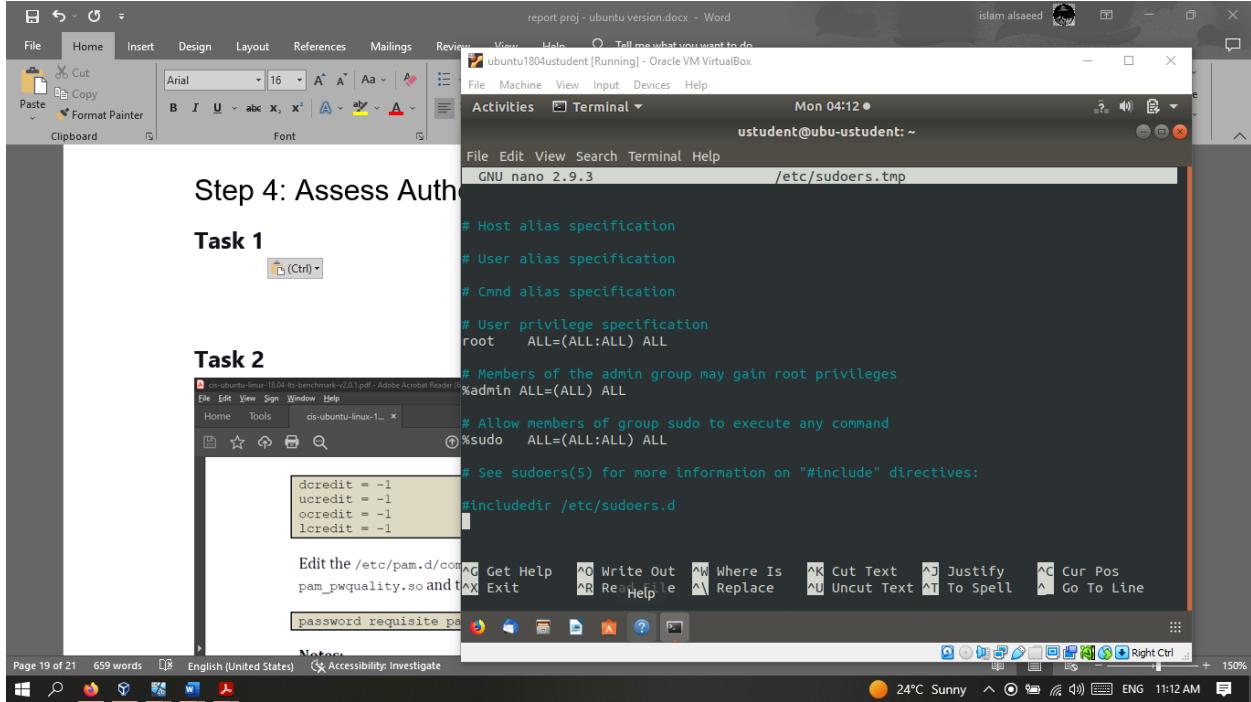


Step 4: Assess Authentication Management at Targeted Assets

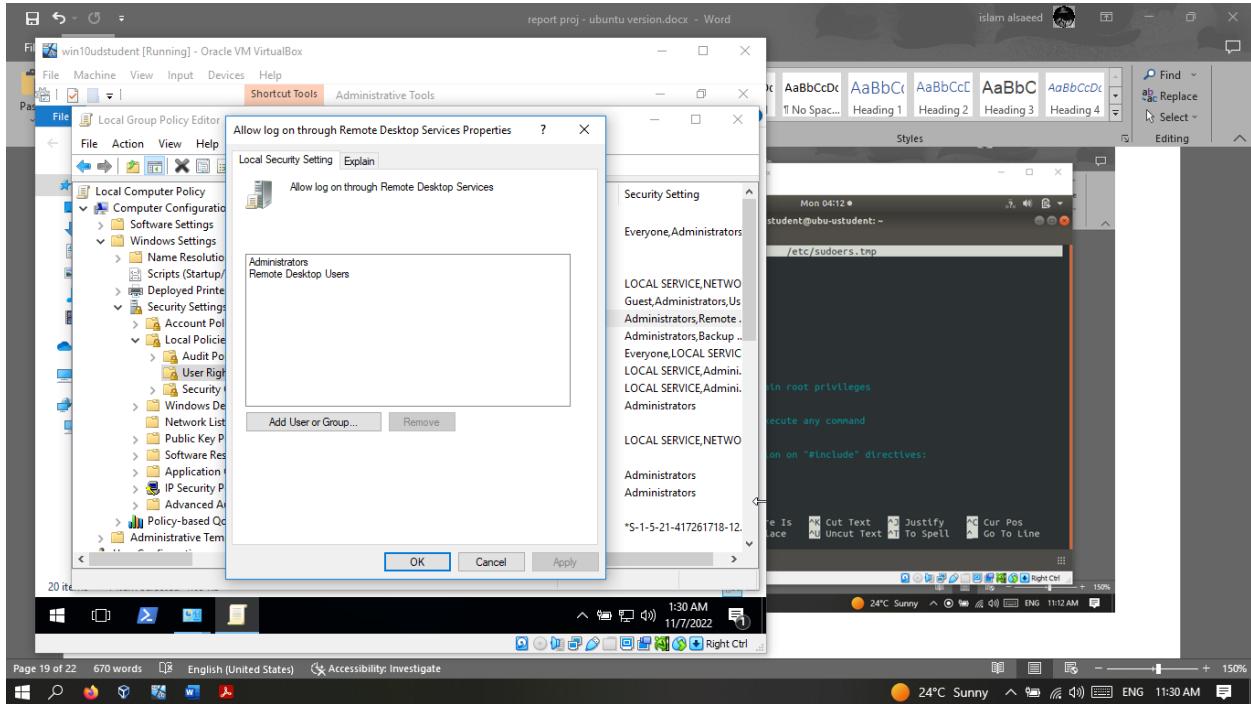
Task 1

Are there users with excessive permissions?

- In ubuntu no

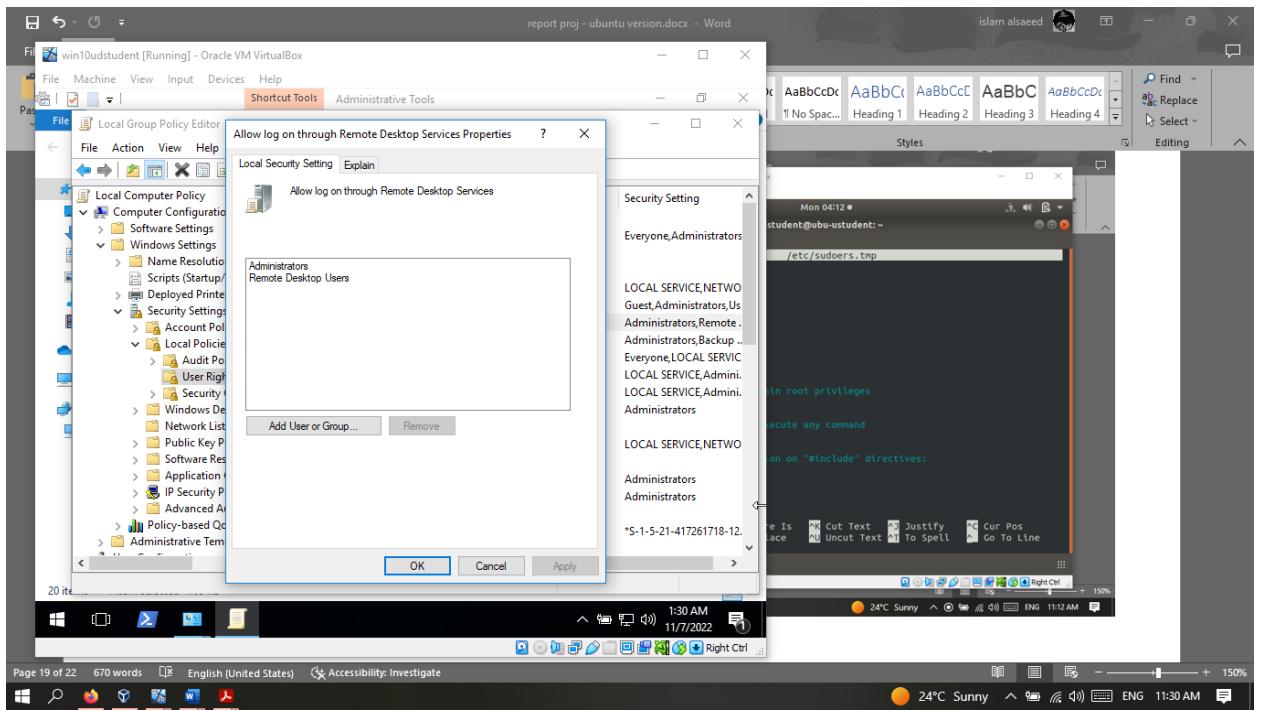


- In windows no , only the administrators and remote desktop users can

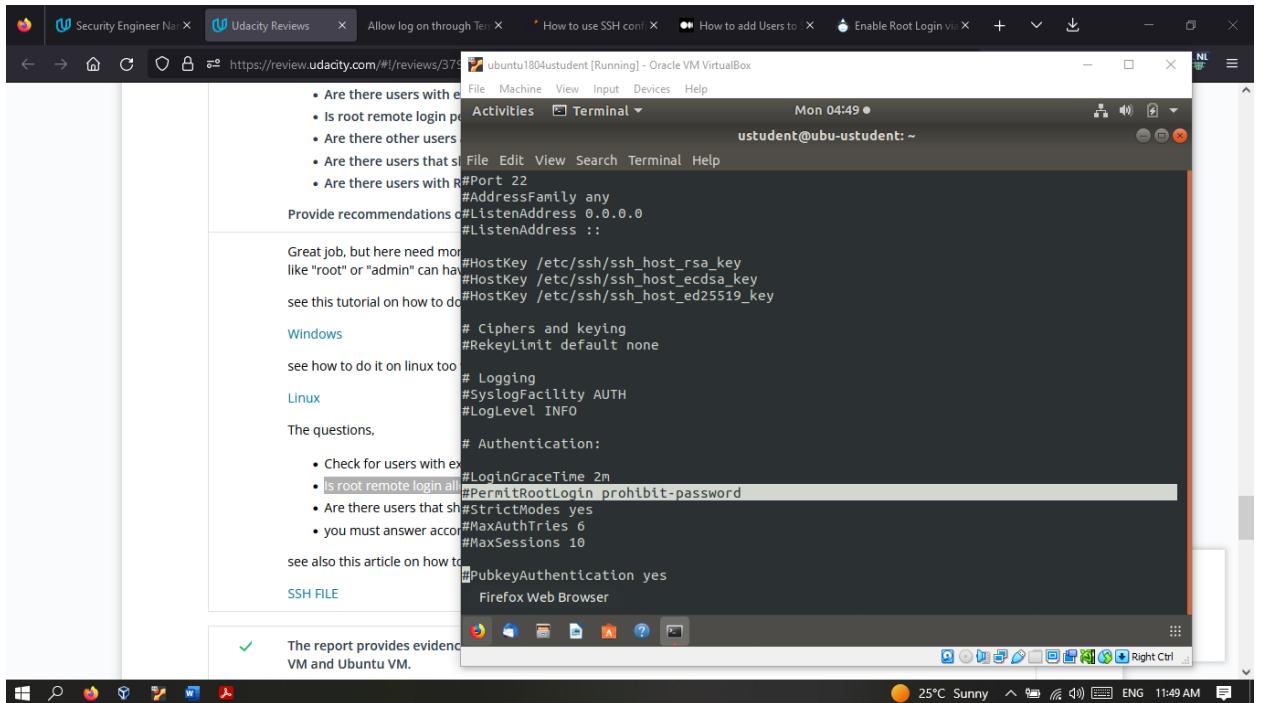


- Is root remote login allowed?

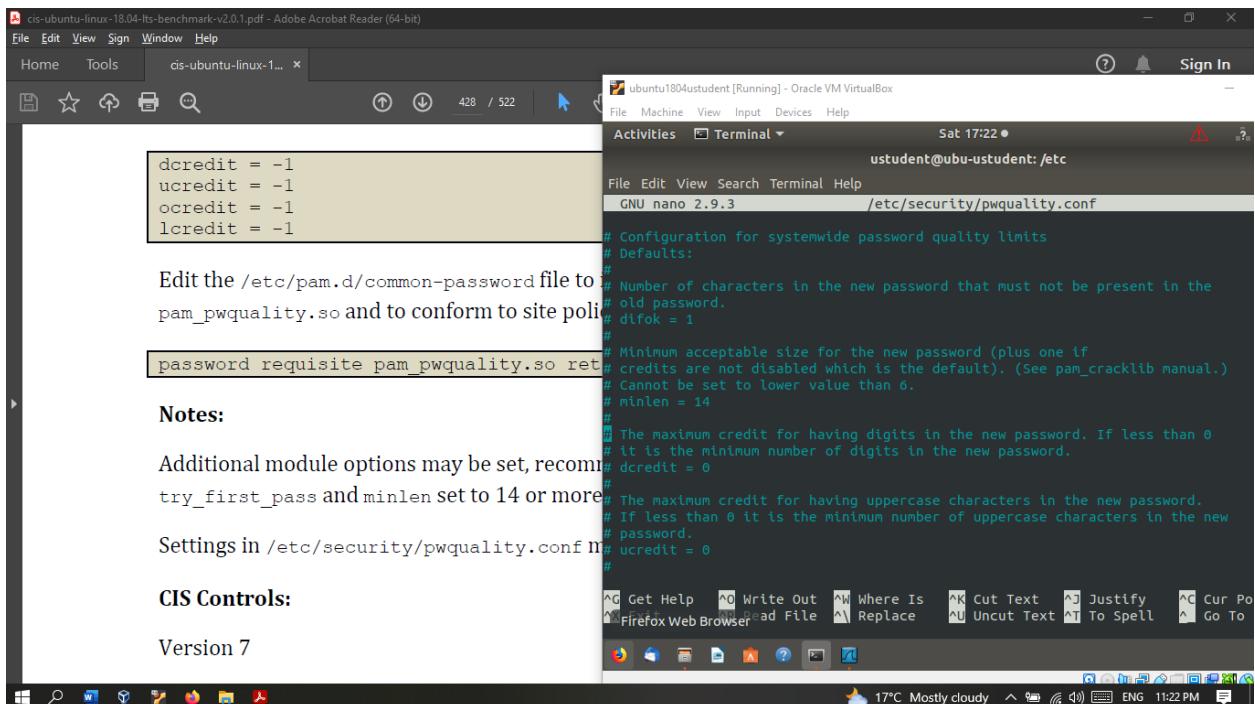
- in windows yes



- In ubuntu



Task 2

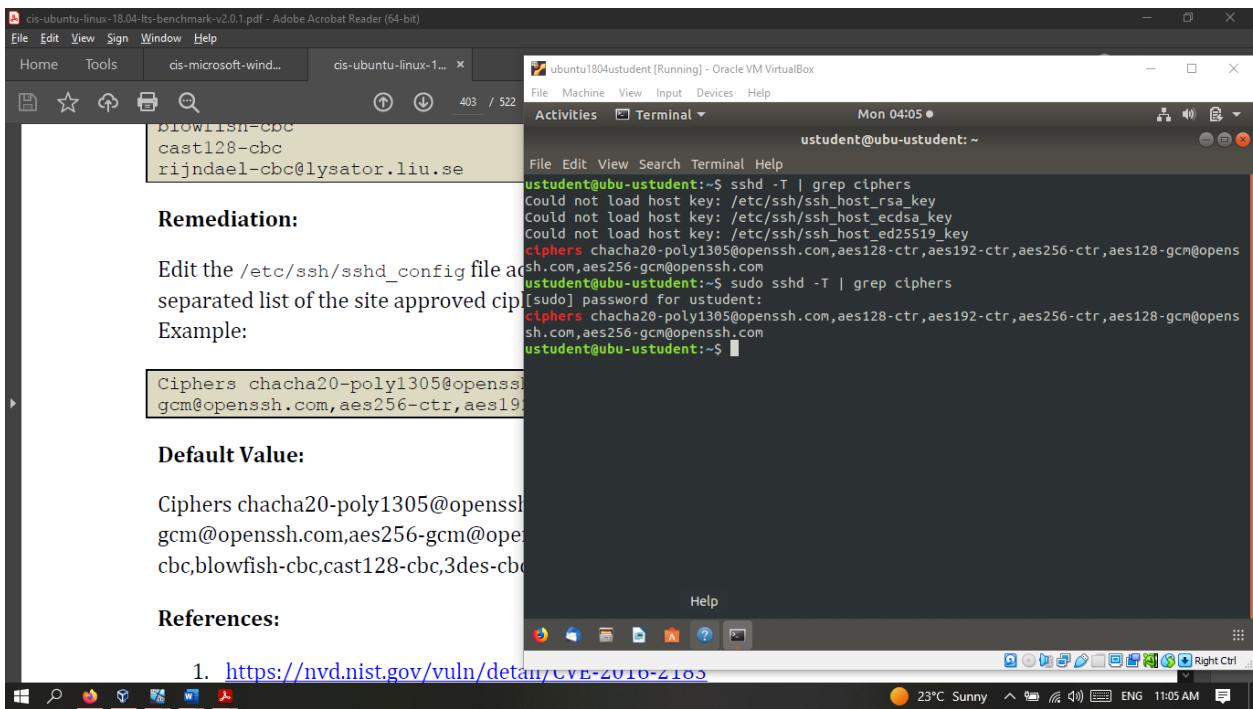


done editing but couldn't find retry line to be edited

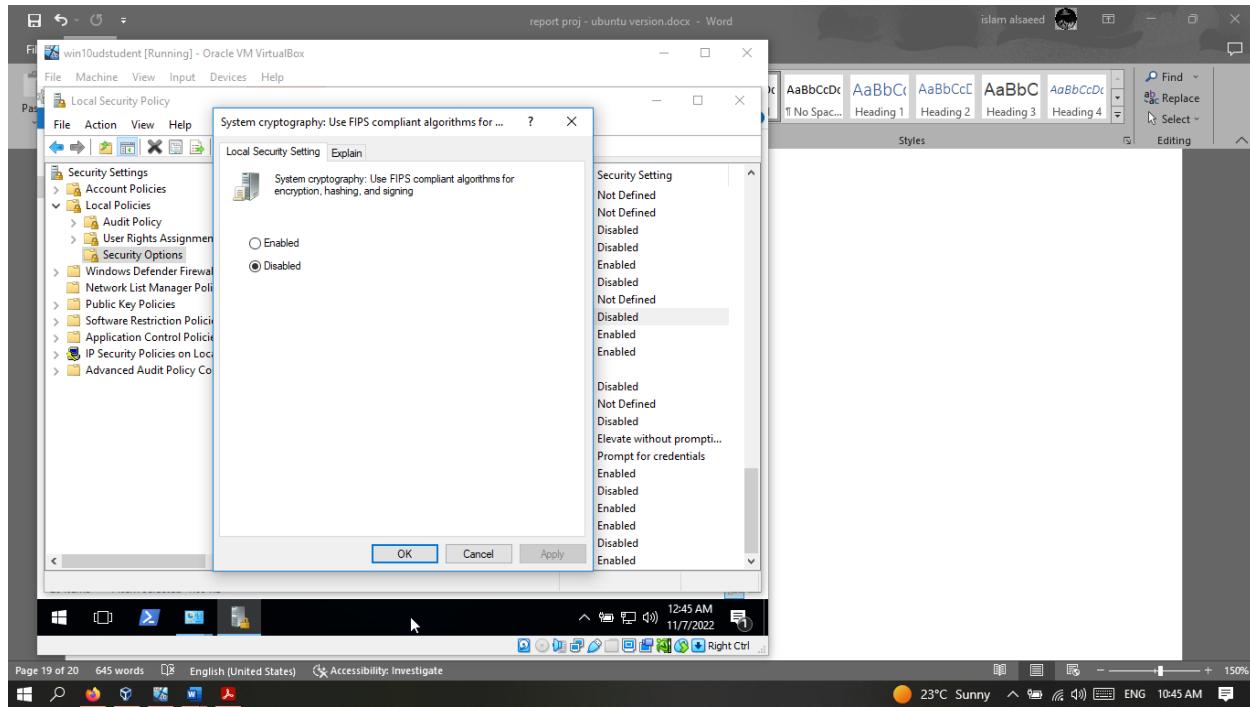
Task 3

these systems are compliant?

- In ubuntu its compliant and uses strong ciphers



- in windows its not compliant



And should be enabled to be compliant

Task 4

```

report proj.docx - Word
File Home Insert Design Layout References Mailings Review View Help Tell me what you want to do
ubuntu1804student [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Command Prompt
Nmap scan report for 10.0.2.5
Host is up (0.0038s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
|_ftp-brute: Invalid usernames iterator: Error parsing username list: users.txt: No such file or directory
MAC Address: 08:00:27:DD:D8:3C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.54 seconds

C:\Users\student>nmap --script ftp-brute -p21 10.0.2.5 --script-args userdb=users.txt,passdb=passwords.txt
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-06 00:17 Pacific Daylight Time
N SOCK ERROR [0.0860s] ssl_init_helper(): OpenSSL legacy provider failed to load.

mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --stem-dns or specify valid servers with --dns-servers
Nmap scan report for 10.0.2.5
Host is up (0.0011s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
|_ftp-brute: Invalid usernames iterator: Error parsing username list: users.txt: No such file or directory
MAC Address: 08:00:27:DD:D8:3C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.44 seconds

C:\Users\student>

```

```

Sat 18:18 ●
student@ubu-ustudent:/usr/share/nmap/scripts
al Help
1 host up) scanned in 0.32 seconds
r/share/nmap/scripts$ nmap --script ftp-brute -p21 10.0.2.5 --txt,passdb=password.txt
s://nmap.org ) at 2022-11-05 18:16 EDT
ustudent (10.0.2.5)
nny.

words iterator
1 host up) scanned in 0.31 seconds
r/share/nmap/scripts$ nmap --script ftp-brute -p21 10.0.2.5 --txt,passdb=passwords.txt
s://nmap.org ) at 2022-11-05 18:16 EDT
ustudent (10.0.2.5)
nny.

words iterator
1 host up) scanned in 0.38 seconds
r/share/nmap/scripts$ 

```

```

report proj.docx - Word
File Home Insert Design Layout References Mailings Review View Help Tell me what you want to do
ubuntu1804student [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal
Sat 18:18 ●
student@ubu-ustudent:/usr/share/nmap/scripts
File Edit View Search Terminal Help
Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds
ustudent@ubu-ustudent:/usr/share/nmap/scripts$ nmap --script ftp-brute -p21 10.0.2.5 --script-args userdb=users.txt,passdb=password.txt
Starting Nmap 7.60 ( https://nmap.org ) at 2022-11-05 18:16 EDT
Nmap scan report for ubu-ustudent (10.0.2.5)
Host is up (0.0001s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
|_ftp-brute: Invalid passwords iterator
Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
ustudent@ubu-ustudent:/usr/share/nmap/scripts$ nmap --script ftp-brute -p21 10.0.2.5 --script-args userdb=users.txt,passdb=passwords.txt
Starting Nmap 7.60 ( https://nmap.org ) at 2022-11-05 18:16 EDT
Nmap scan report for ubu-ustudent (10.0.2.5)
Host is up (0.0002s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
|_ftp-brute: Invalid passwords iterator
Nmap done: 1 IP address (1 host up) scanned in 0.38 seconds
ustudent@ubu-ustudent:/usr/share/nmap/scripts$ 

```

Final Recommendation

Should this happen immediately? No it have some security issues must be fixed first

What would need to happen before these systems would be added to ensure they are compliant with our current security policies?

Must resolve all the previous issues and retested to make sure its safe enough