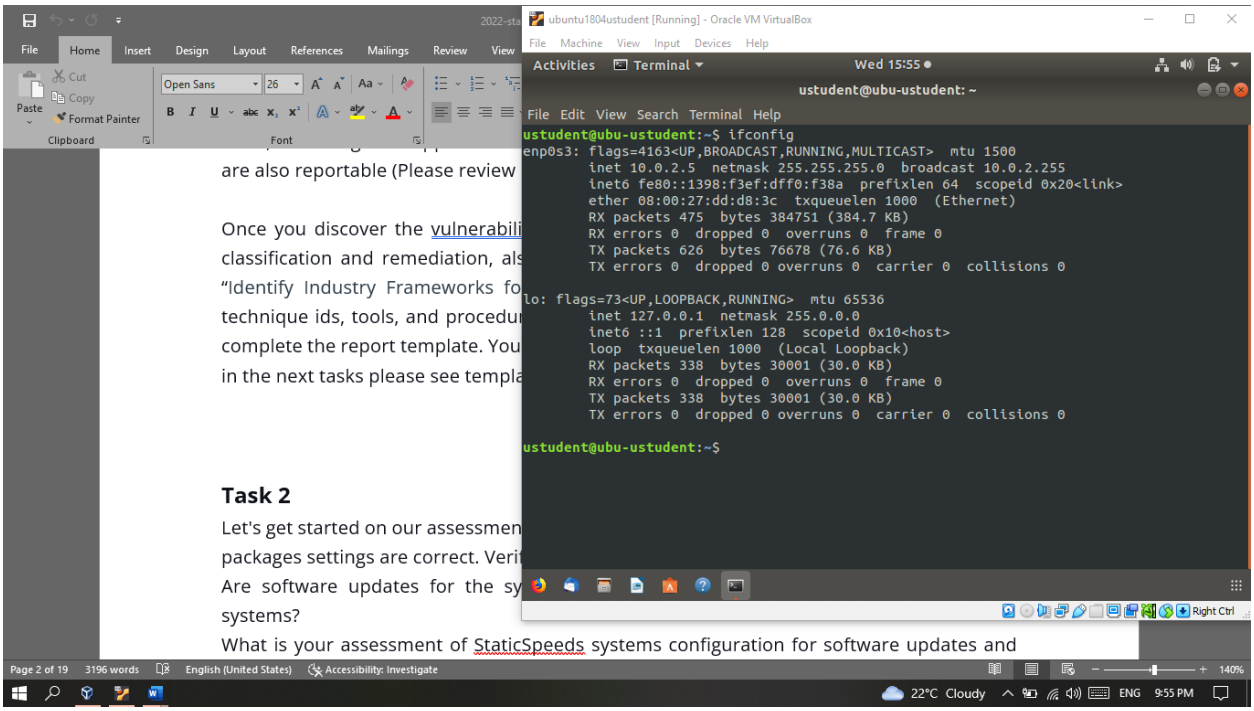
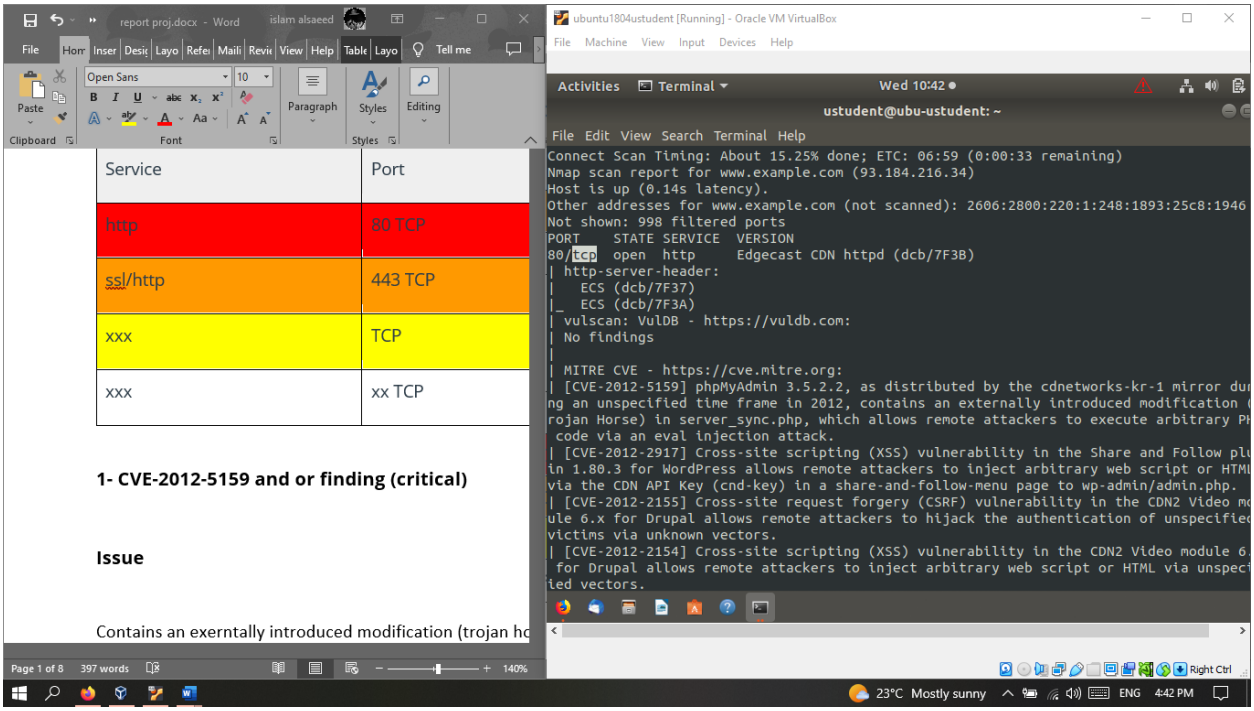
Ubuntu 18.4

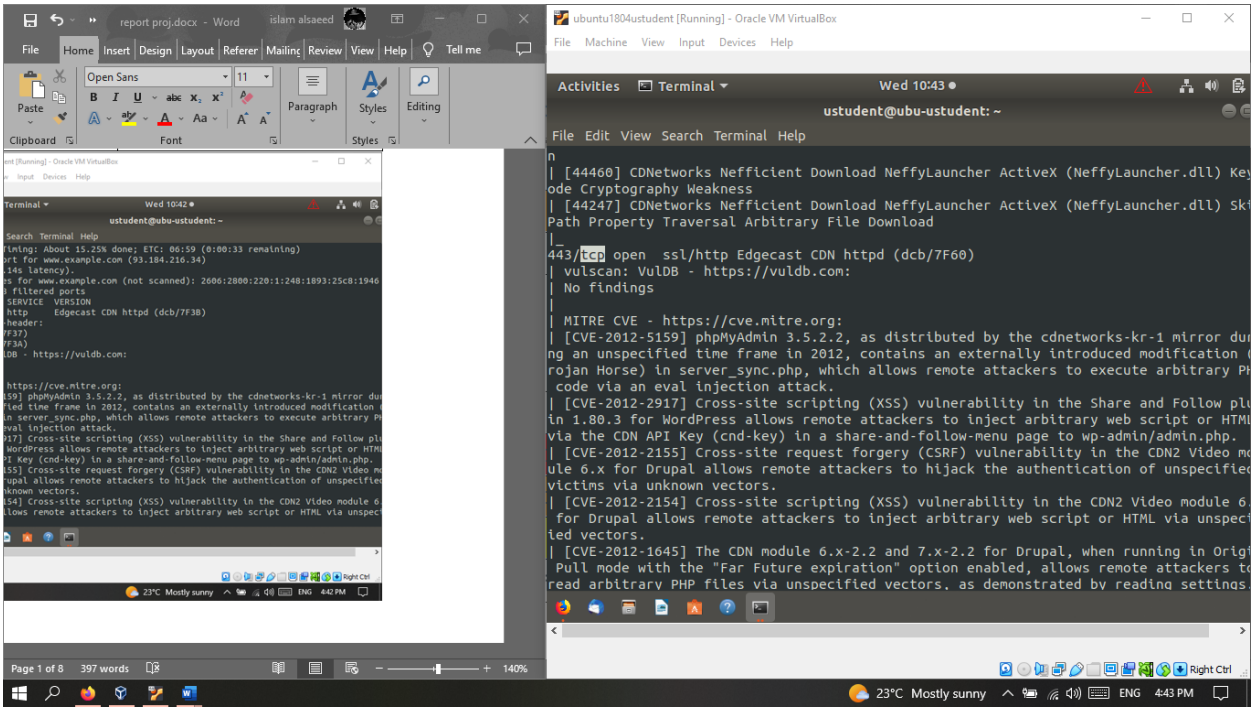
Host	High	Medium	Low	Log
10.0.2.5	xx	x	x	x

IP Address: 10.0.2.5



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

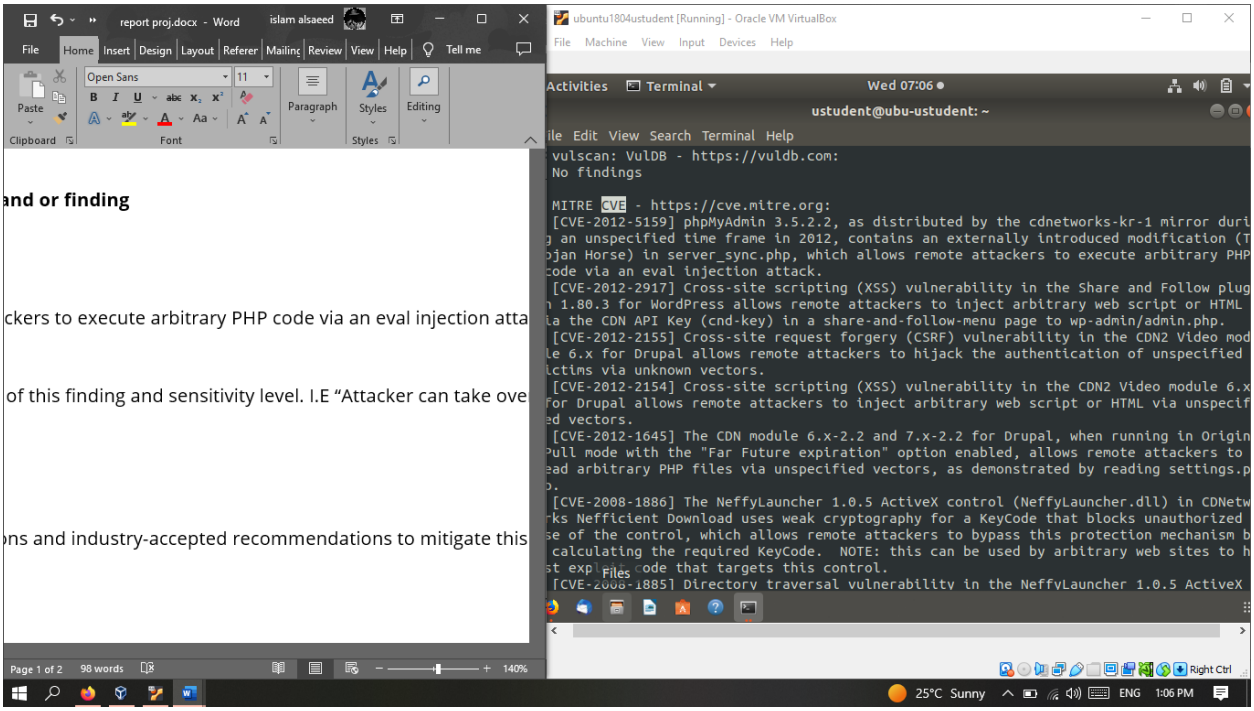




1- CVE-2012-5159 and or finding (critical)

Issue

Contains an exerntally 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>.

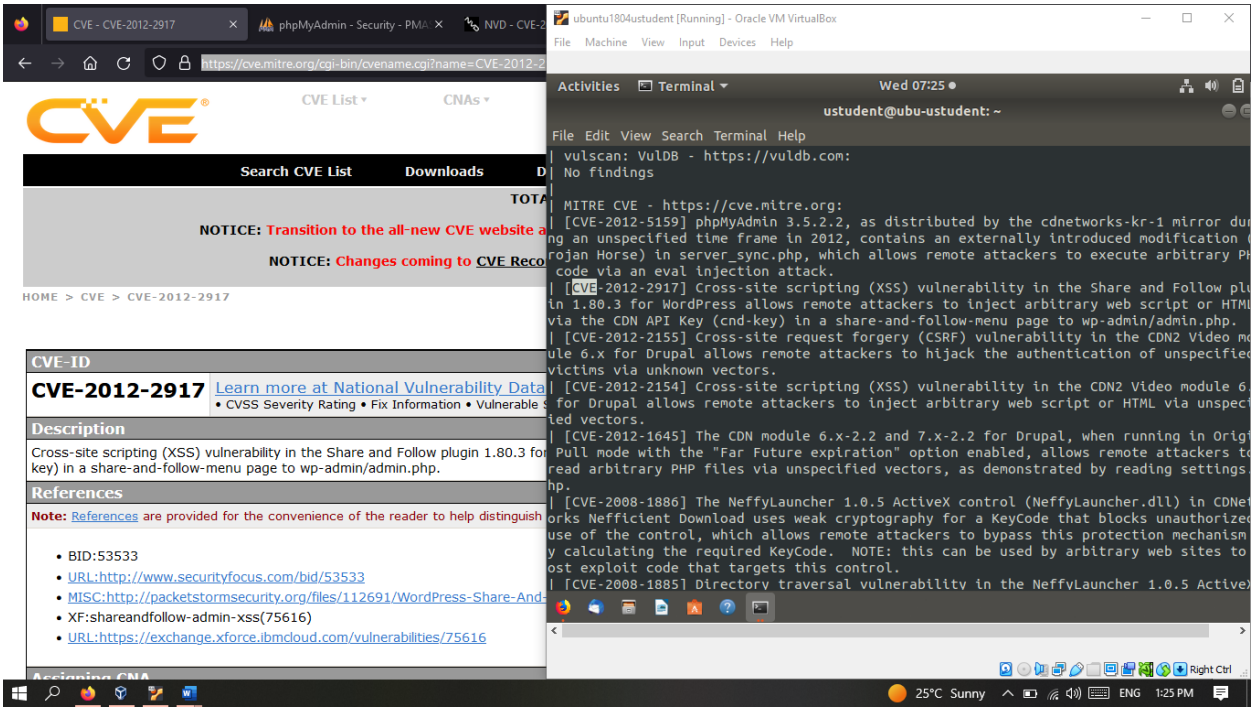
Reference

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.

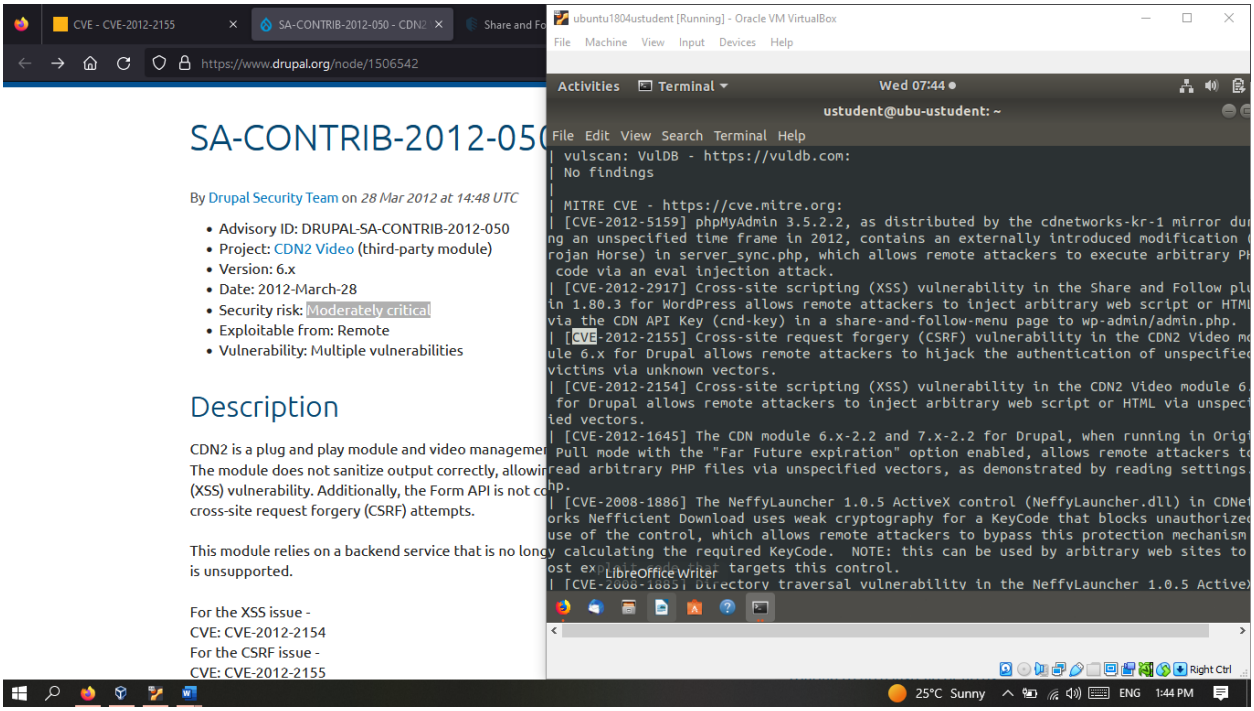
Reference

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



Impact

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

Mitigation

Uninstall the module. This module is no longer supported.

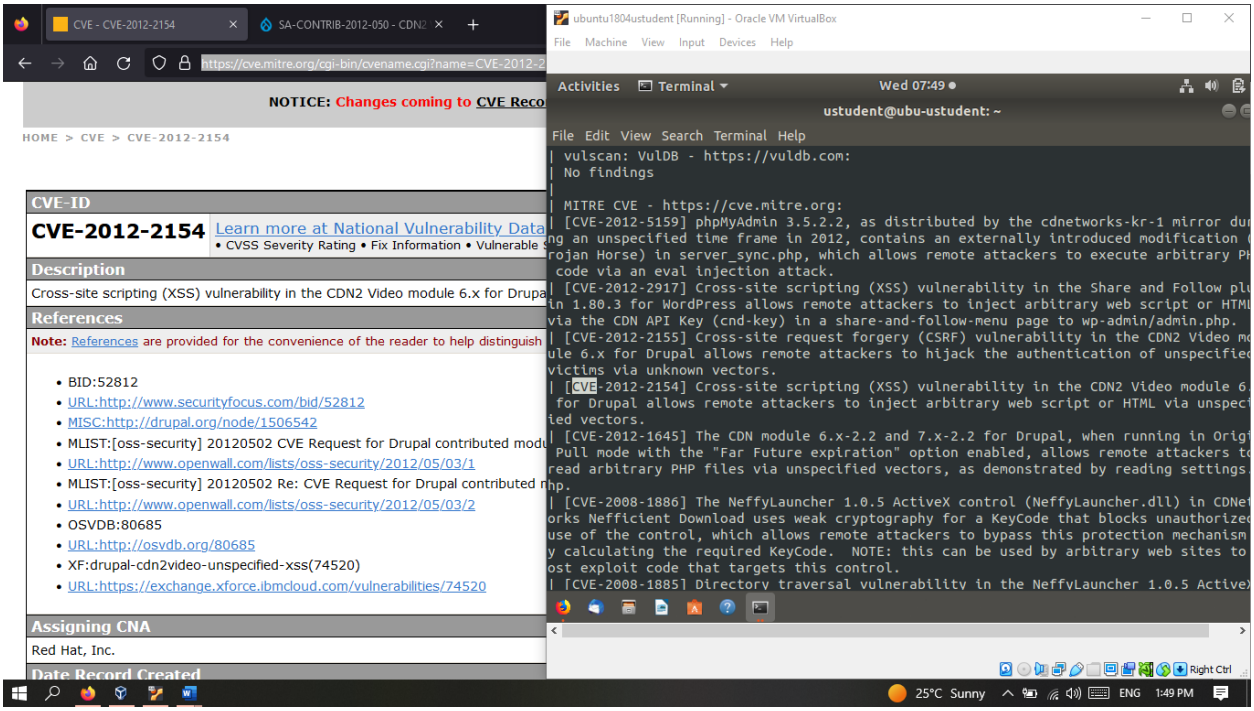
Reference

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.

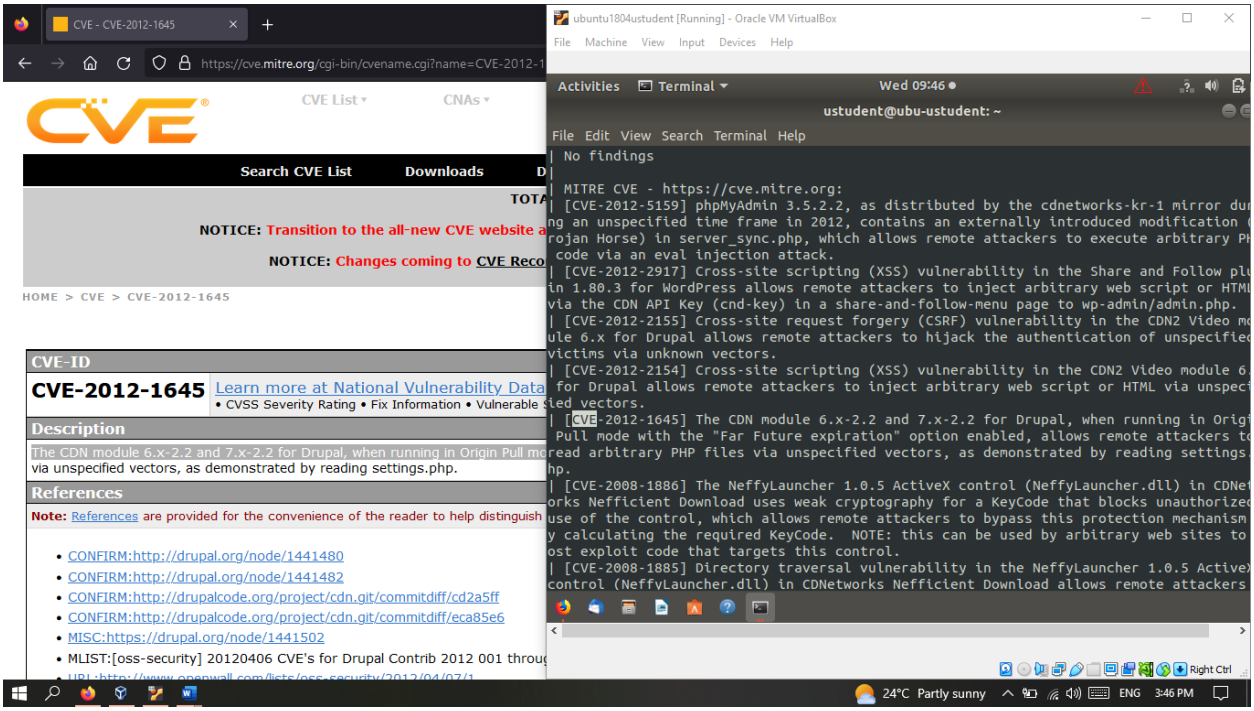
Reference

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

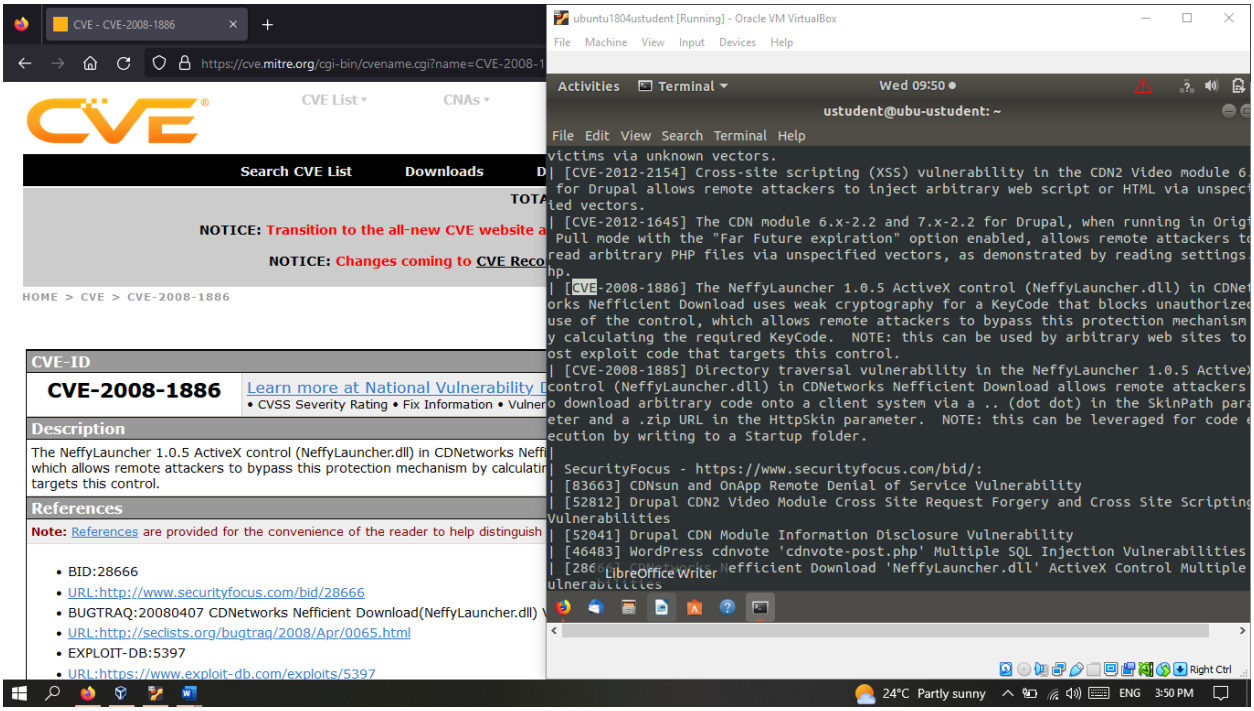
Reference

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

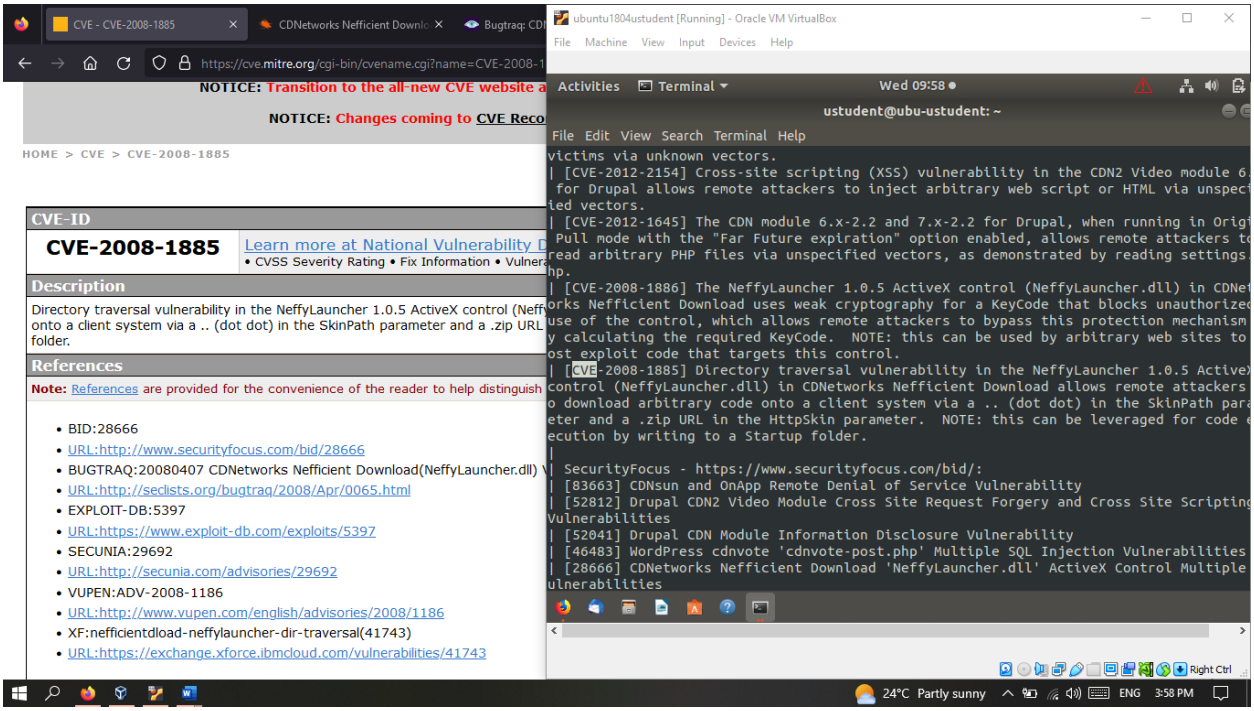
Reference

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.

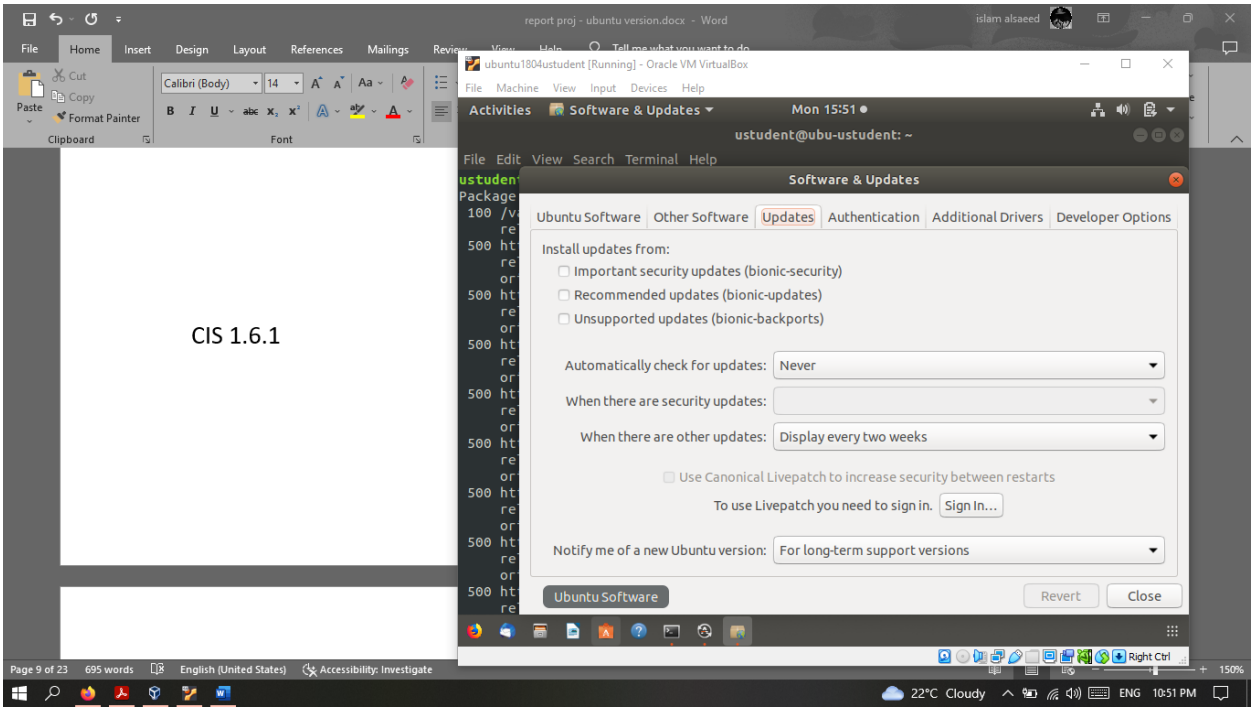
Mitigation

Upgrade the vendor's patch

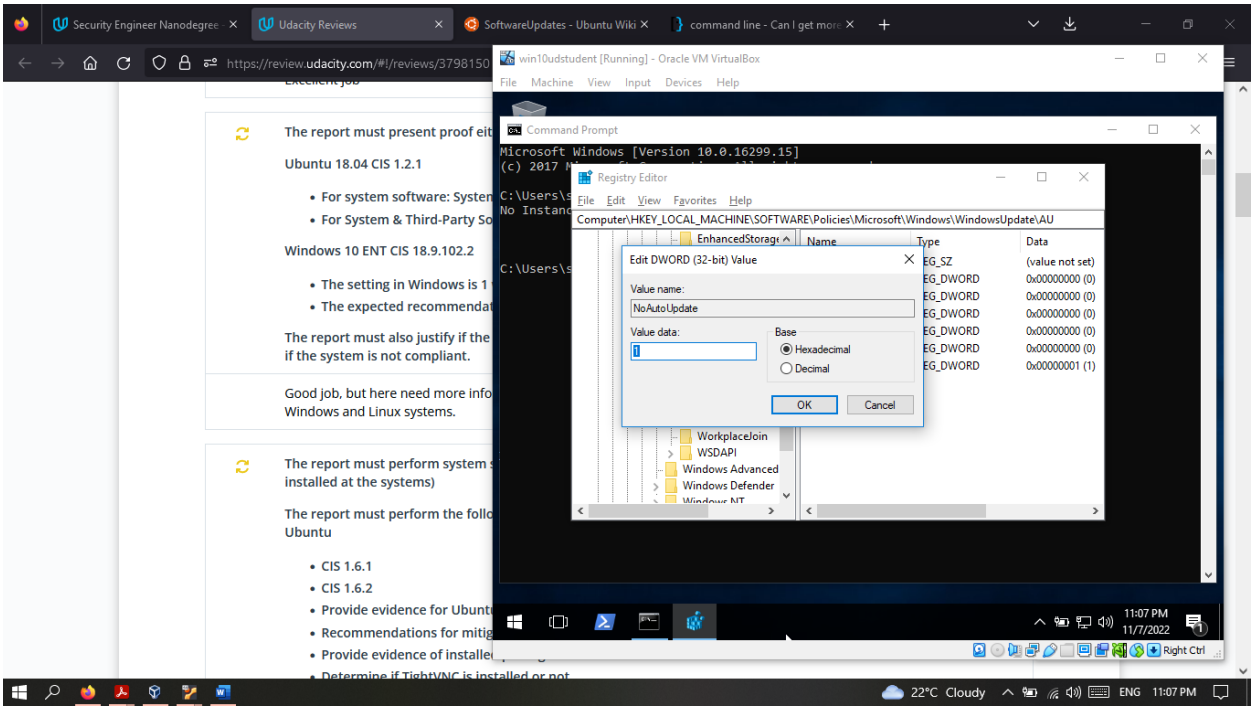
Reference

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

Task 2



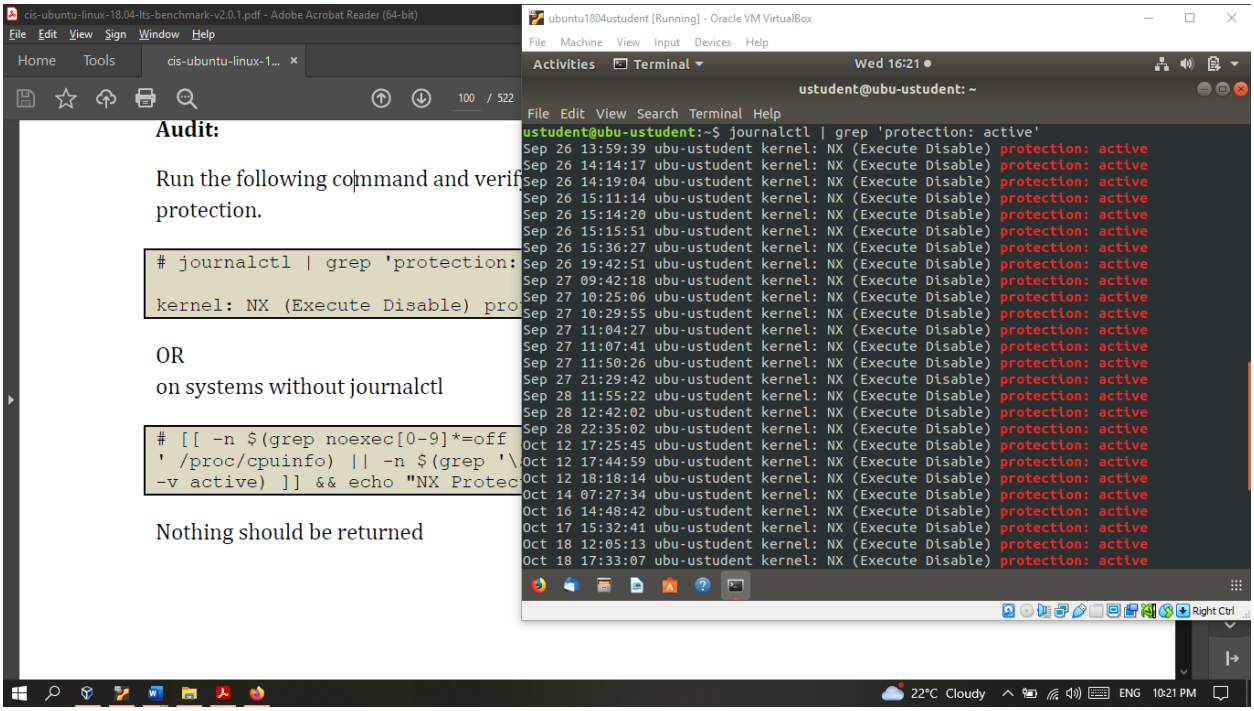
- Windows



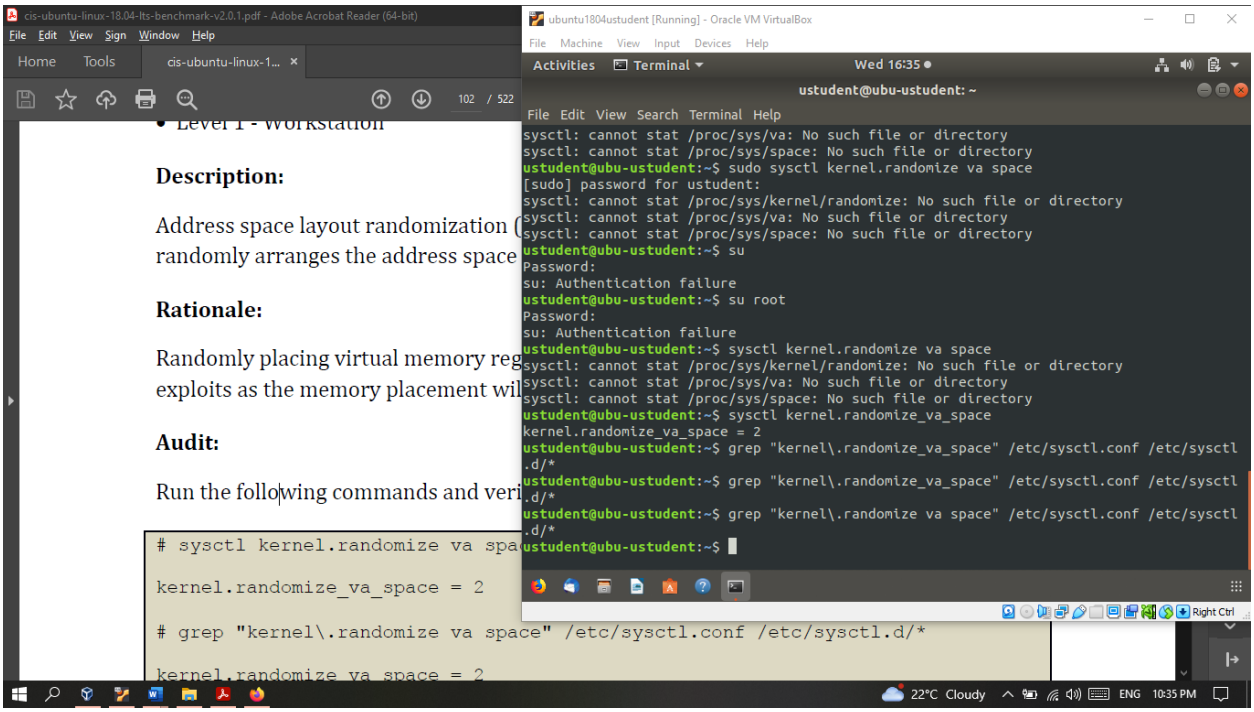
The auto update should be set On on both machine

Task 3

CIS 1.6.1

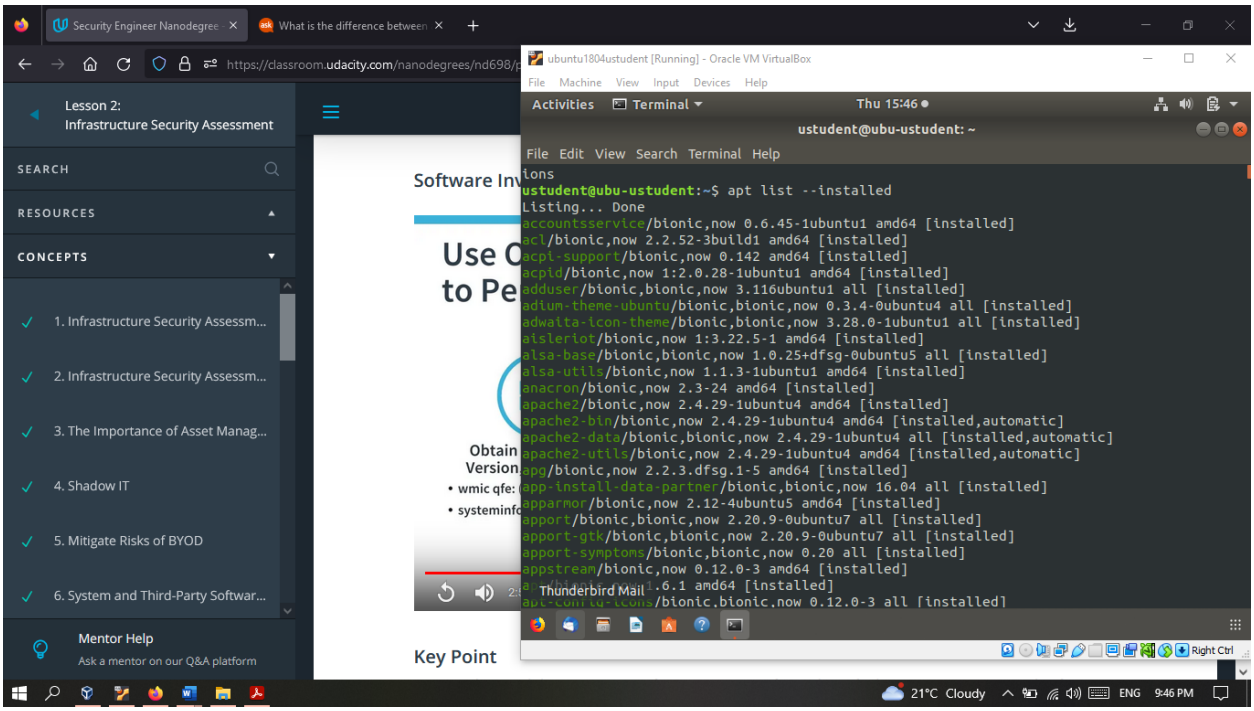


CIS 1.6.2

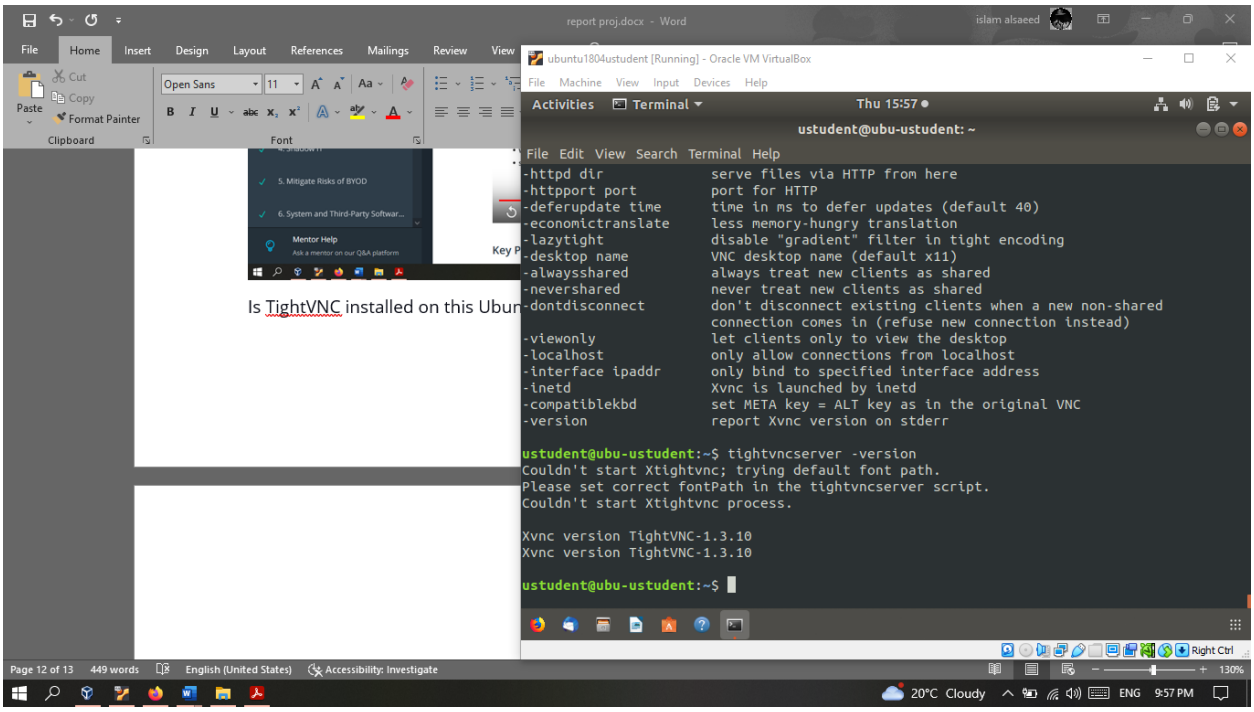


are native protections applied to these systems? Yes

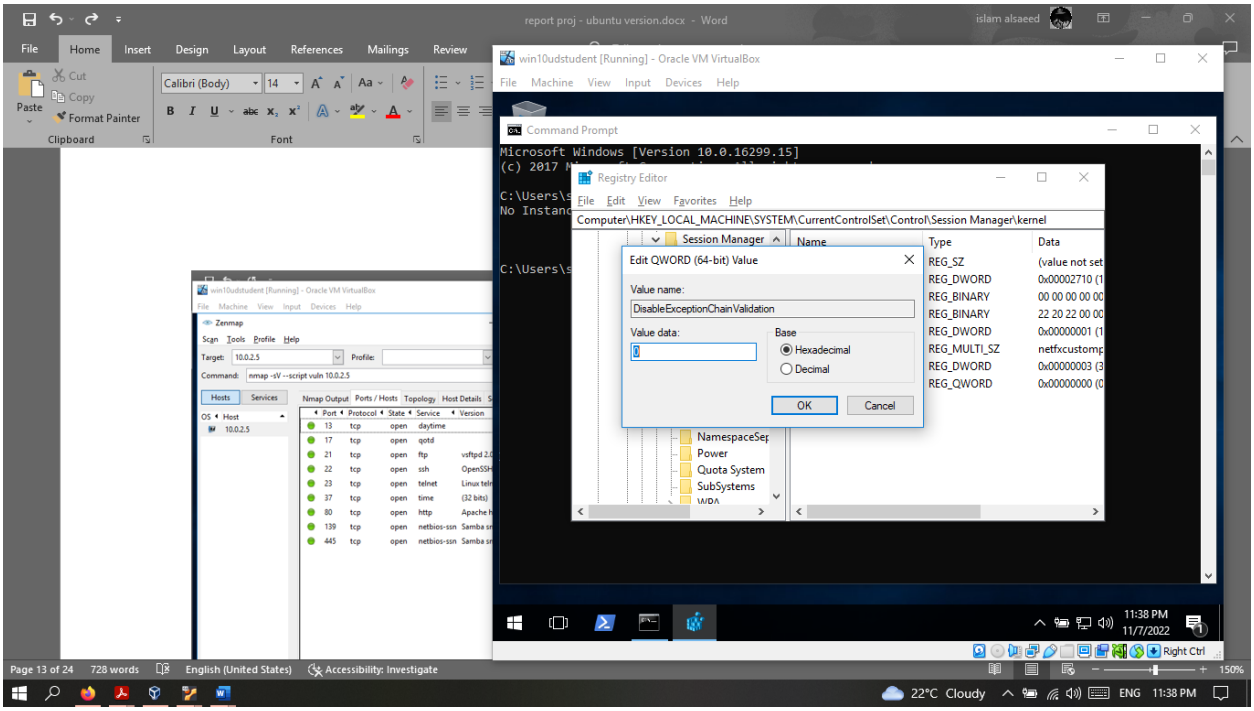
What packages are installed in this ubuntu machine?



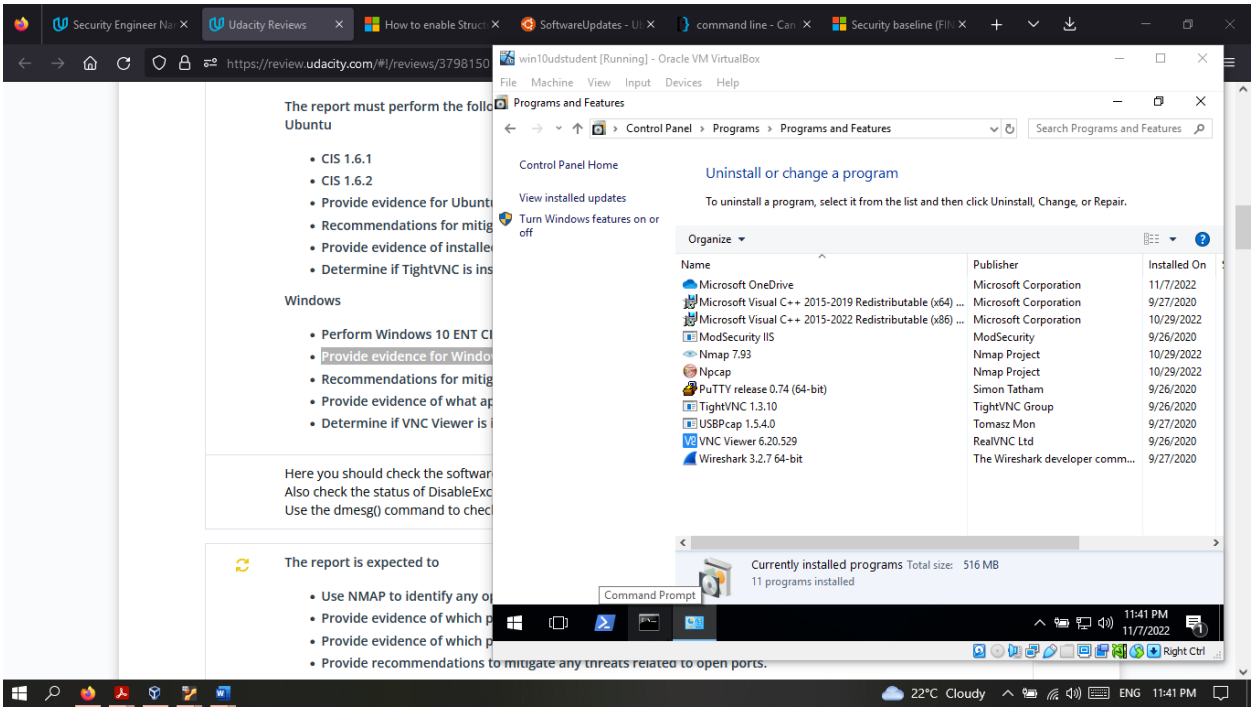
Is TightVNC installed on this Ubuntu machine? Yes



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



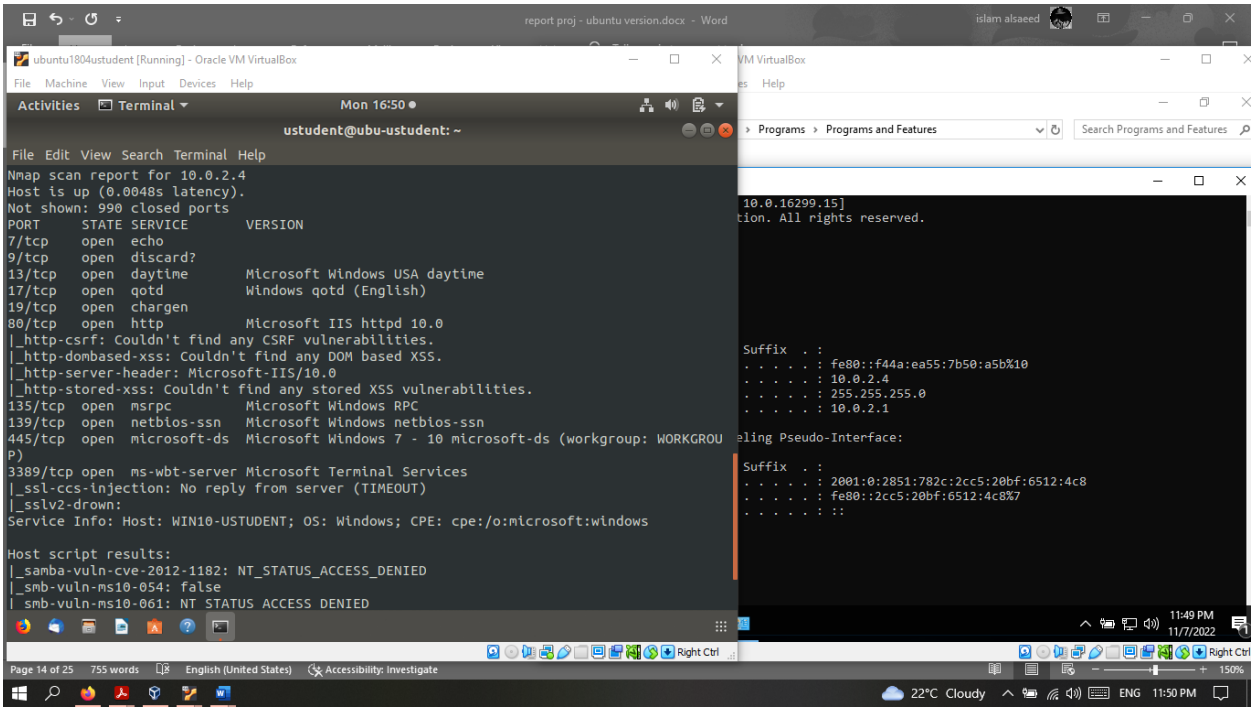
Provide evidence of what applications are installed on the Windows machine.



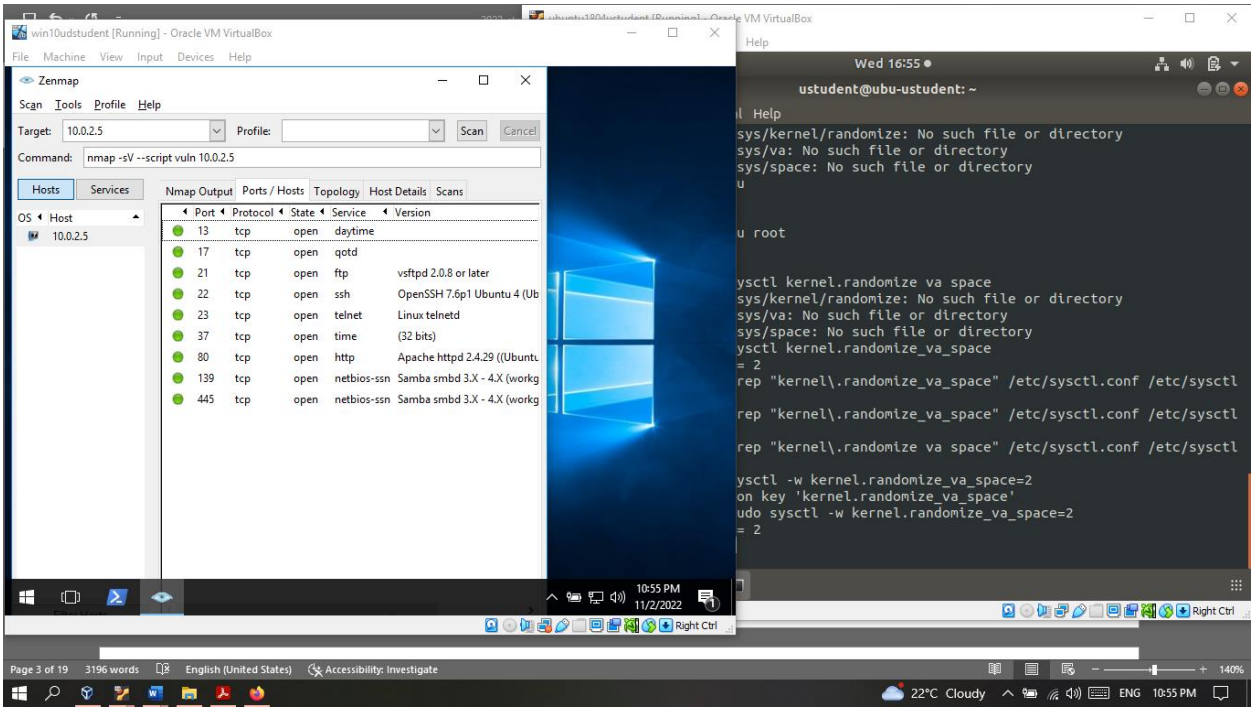
Determine if VNC Viewer is installed in this Windows System? Yes its installed see above photo

Task 4

Provide evidence of which ports are open on the Windows machine



Provide evidence of which ports are open on the Ubuntu machine



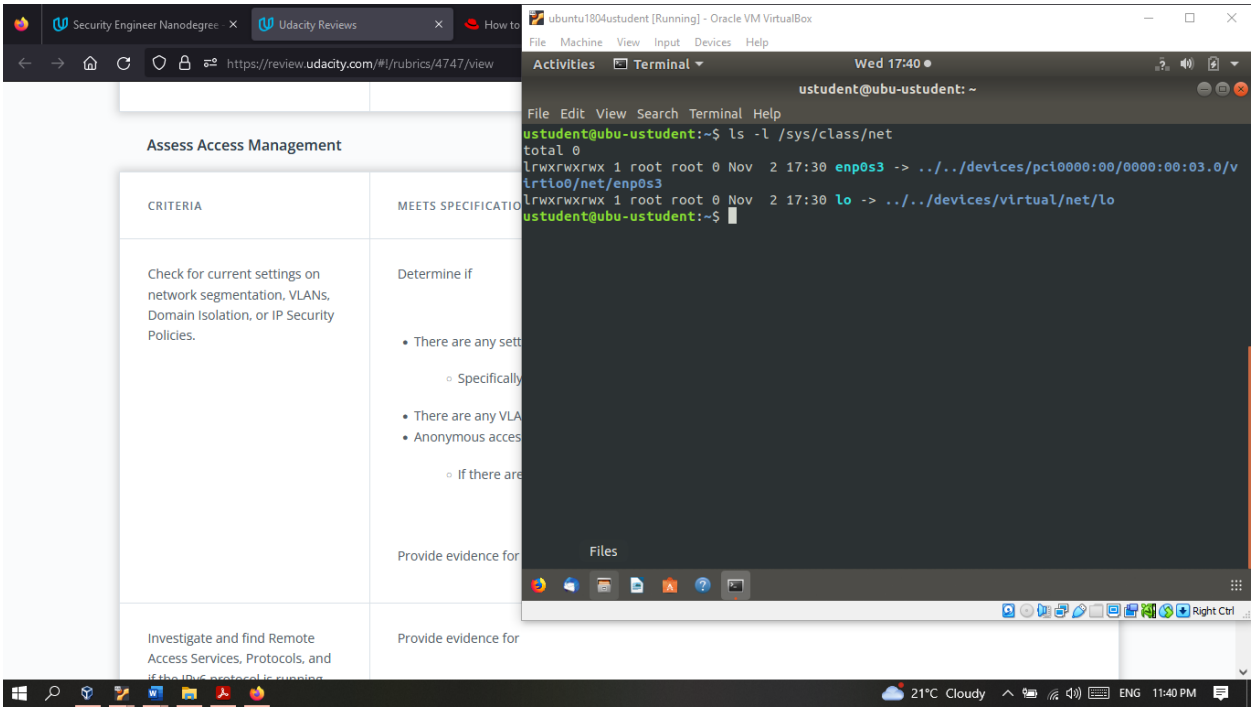
Recommendations:

Close/Disable any services that not being used

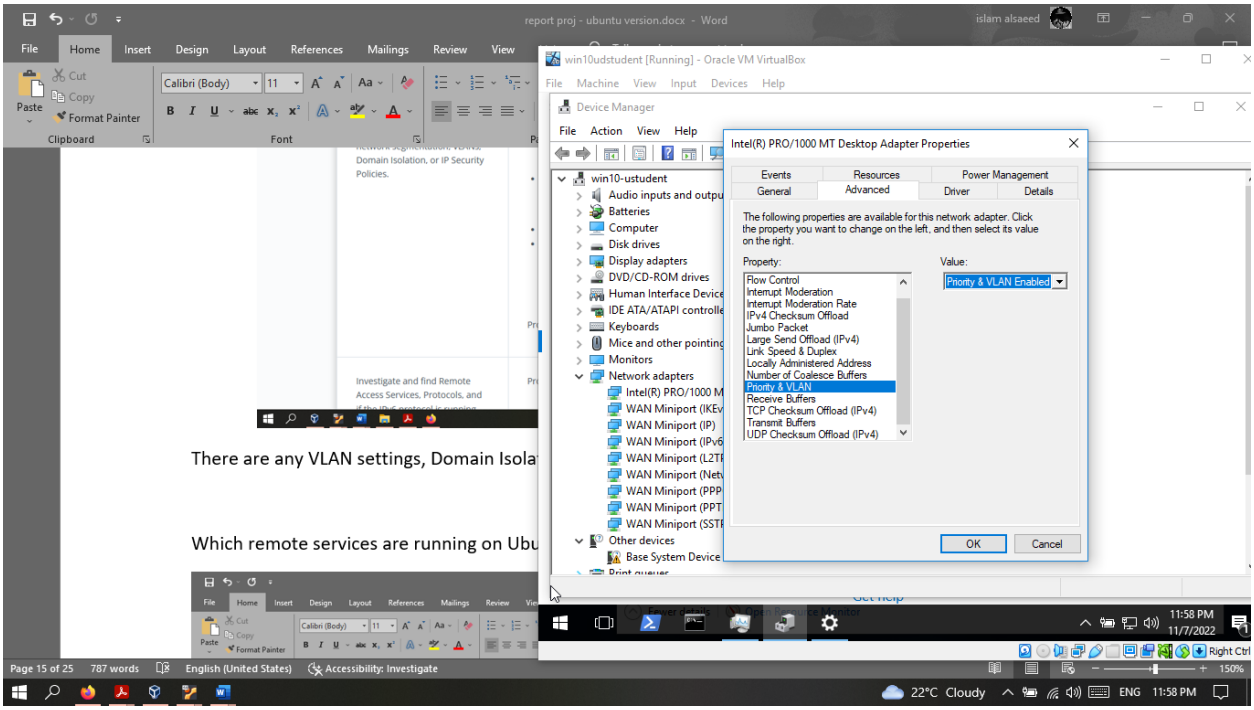
STEP 2

Task 1

- Are there any VLANs? No

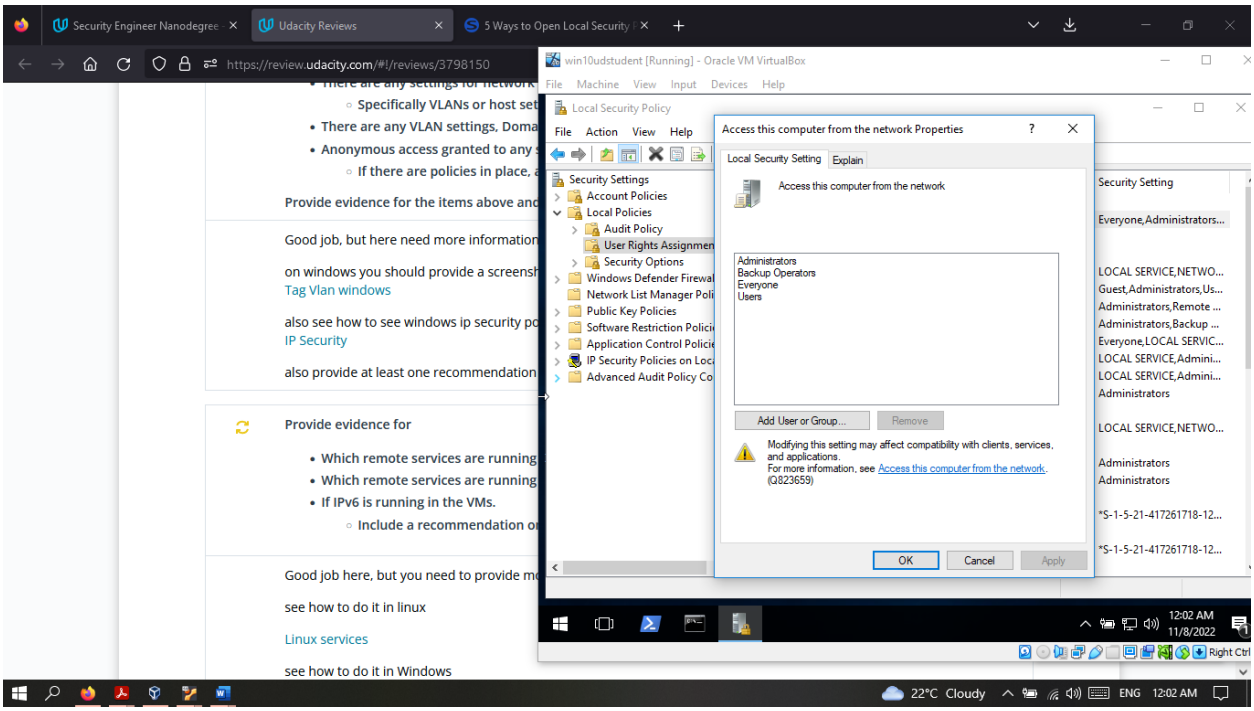


There are any VLAN settings, Domain Isolation, IP Security Policies on Windows?



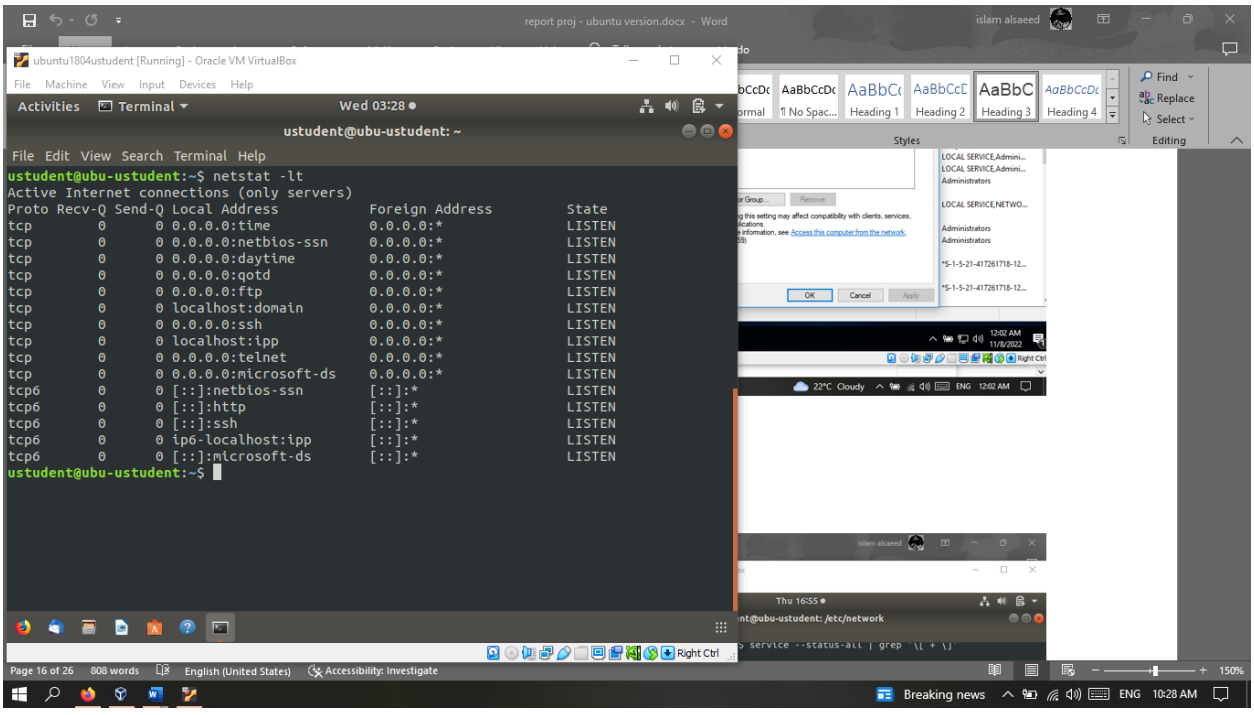
Anonymous access granted to any share

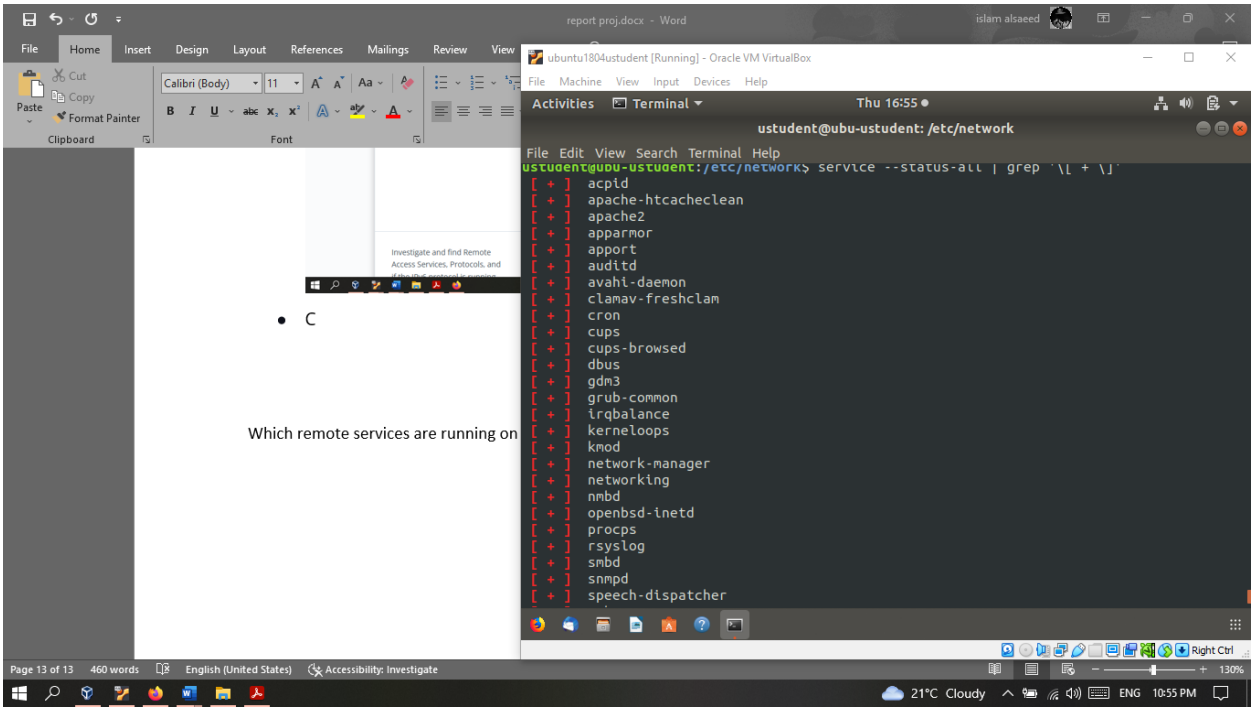
- If there are policies in place, are they enforced?



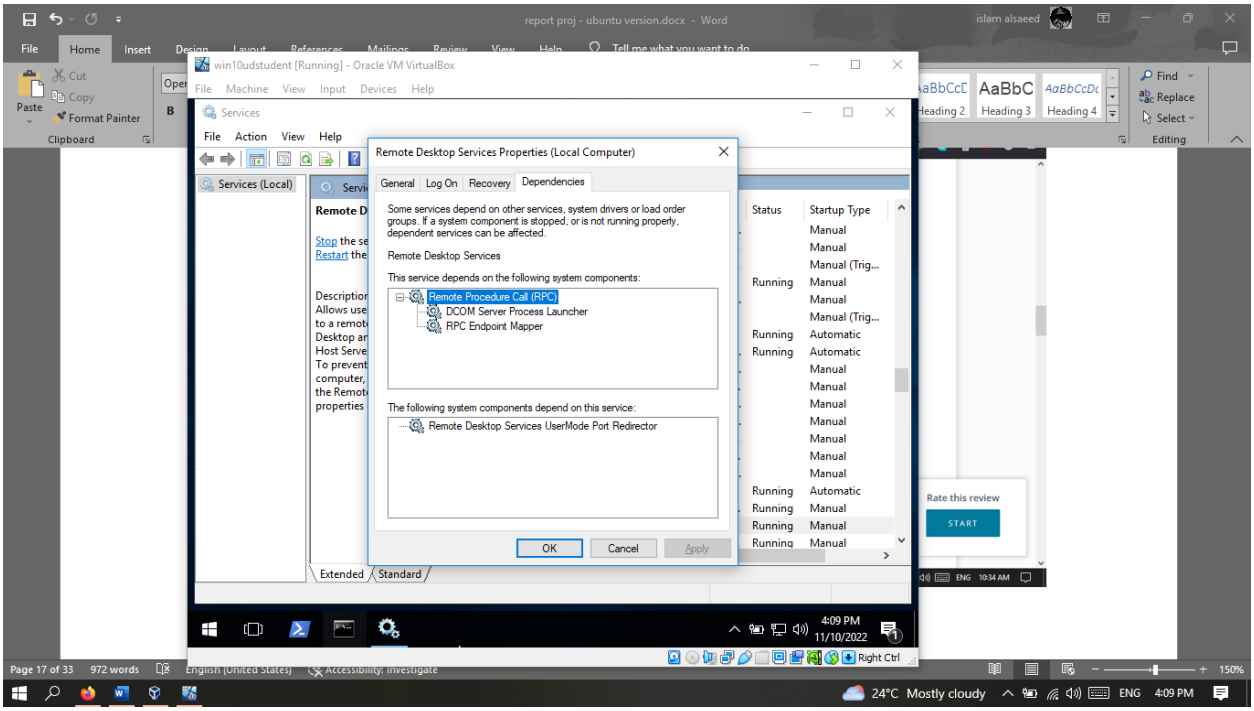
Task 2

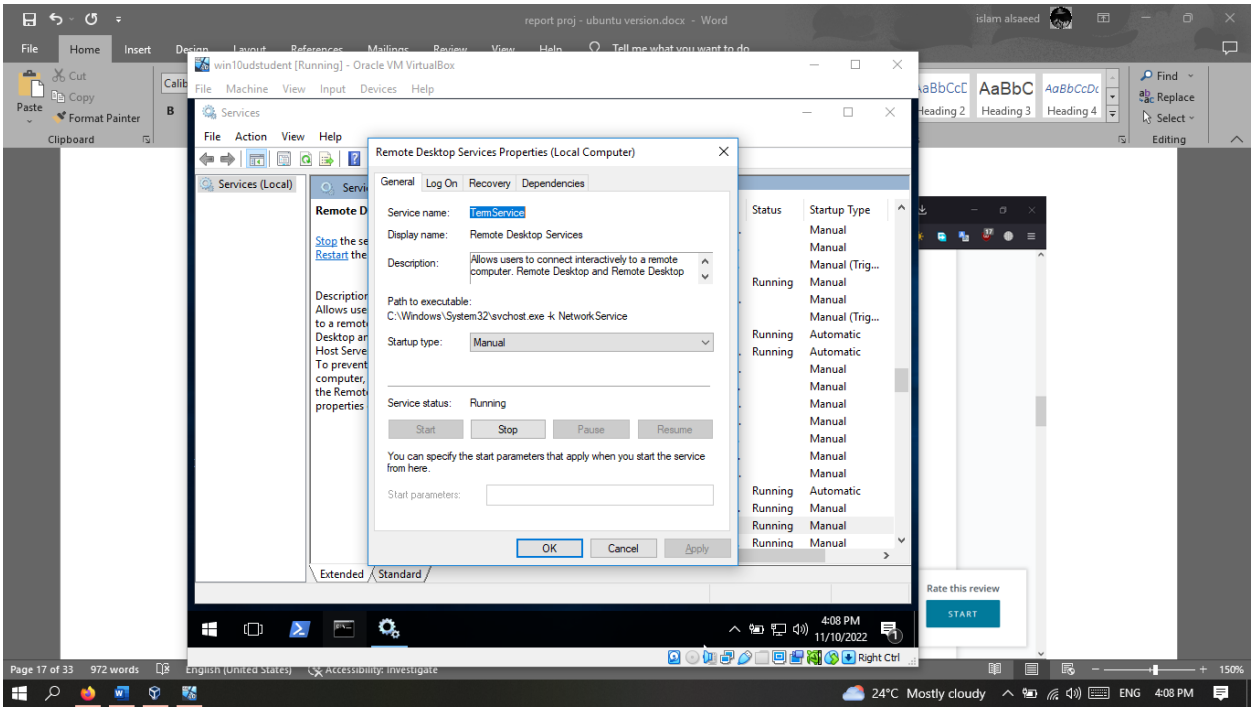
Which remote services are running on Ubuntu? SSH, VNC





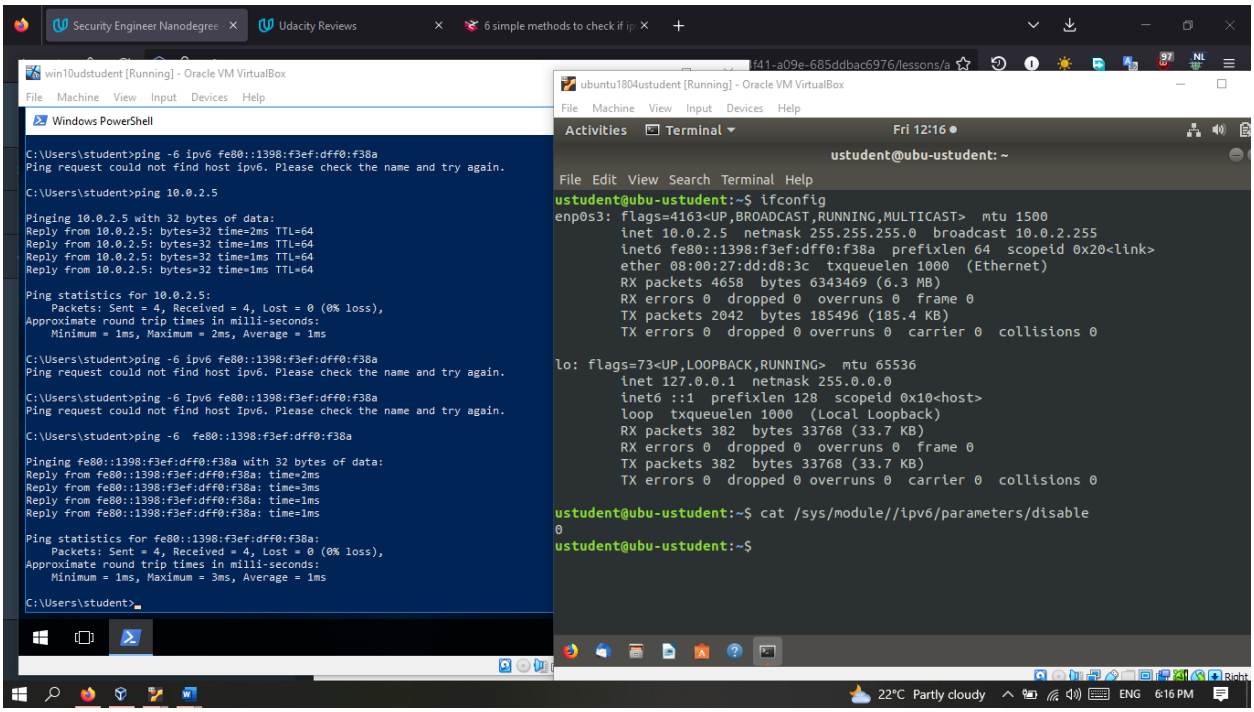
Which remote services are running on Windows?



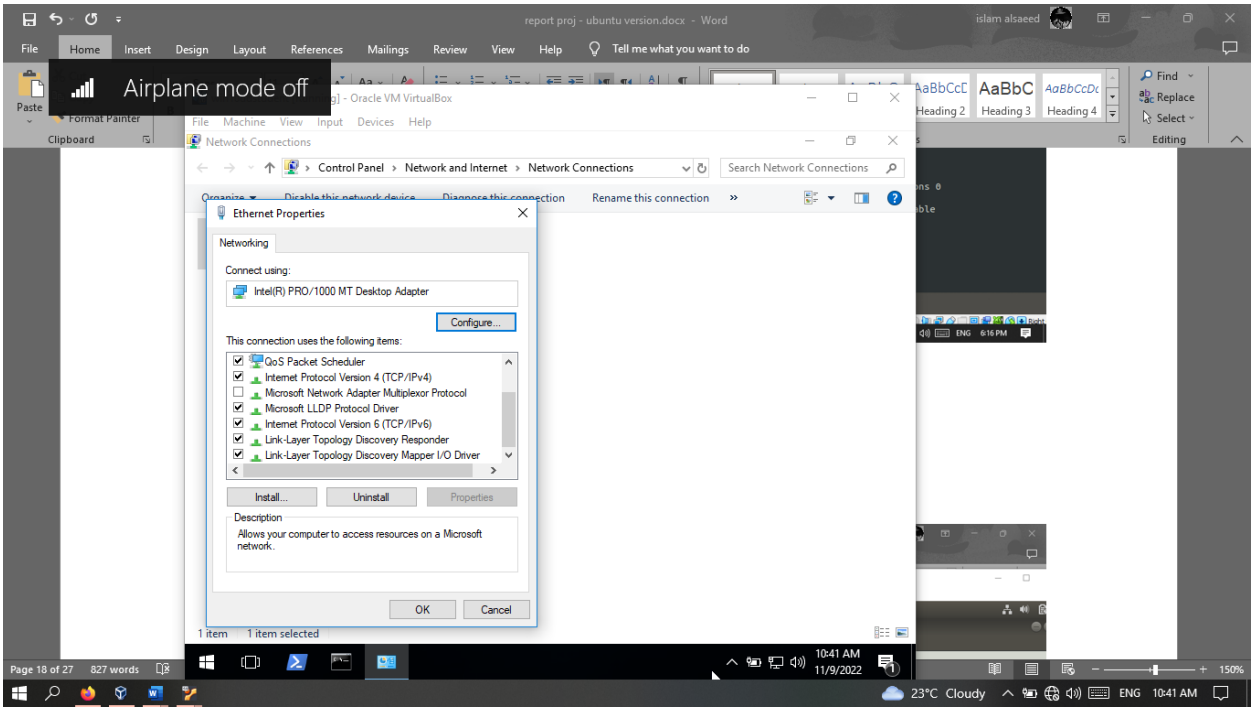


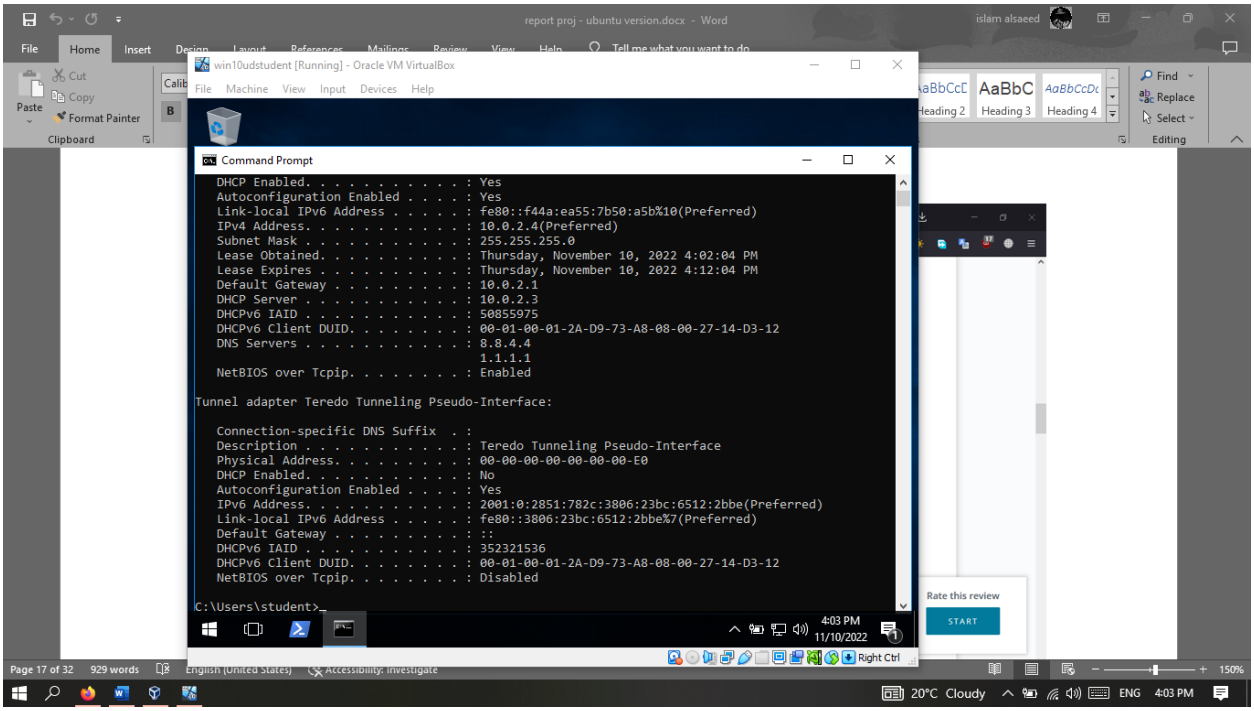
If IPv6 is running in the VMs?

On Linux? Yes , 0 means its running



In windows ? also yes





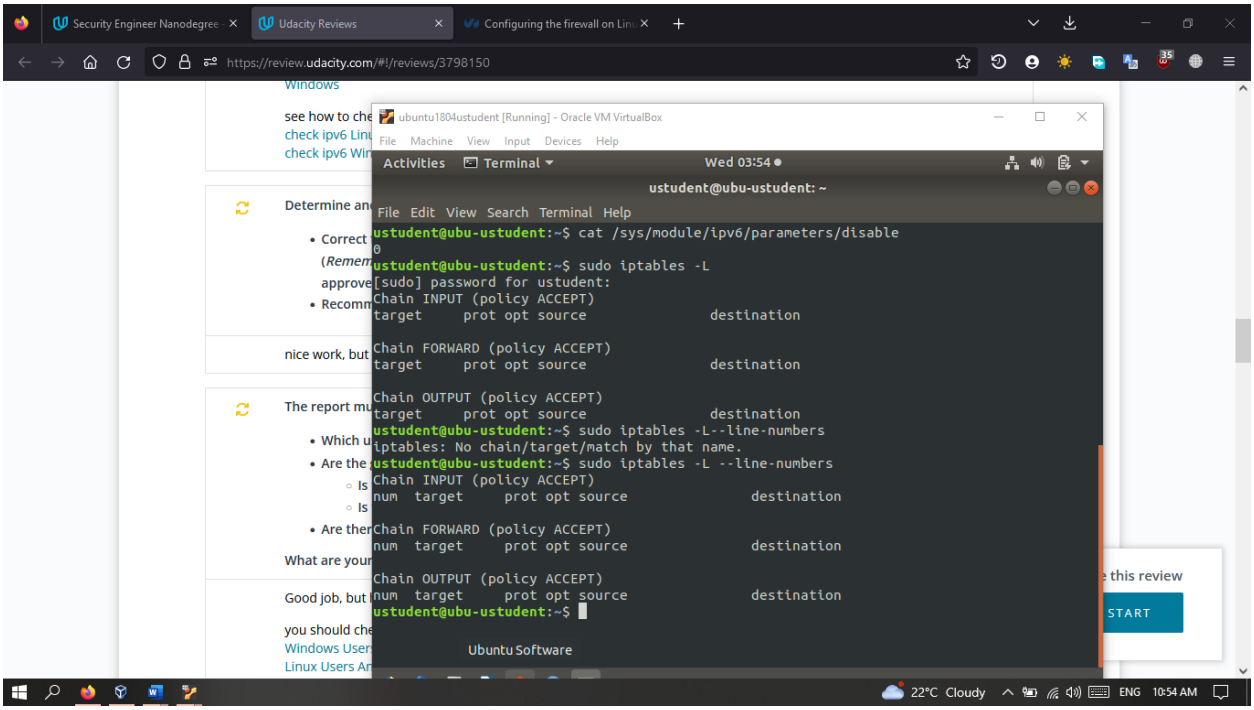
Include a recommendation on whether IPv6 is needed and how to address this?

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.

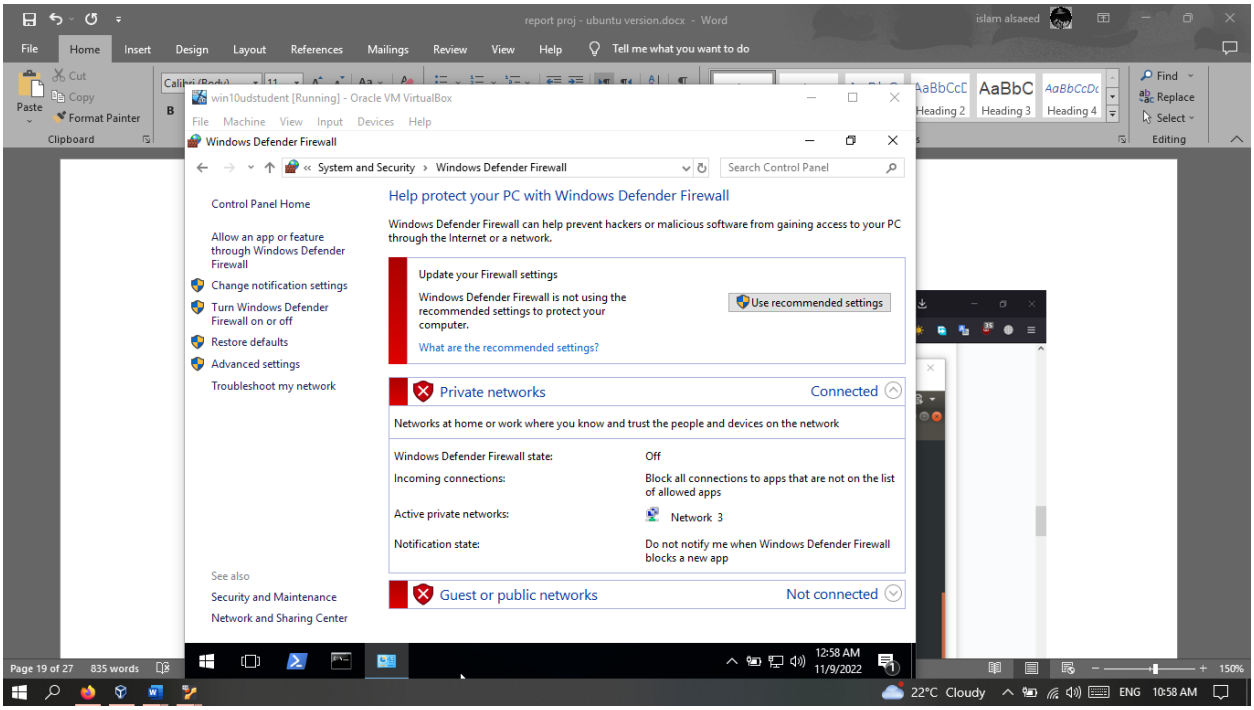
Task 3

Correct firewall configuration in the targeted systems?

In Linux ? No there is no policies configured



In windows ? its not On



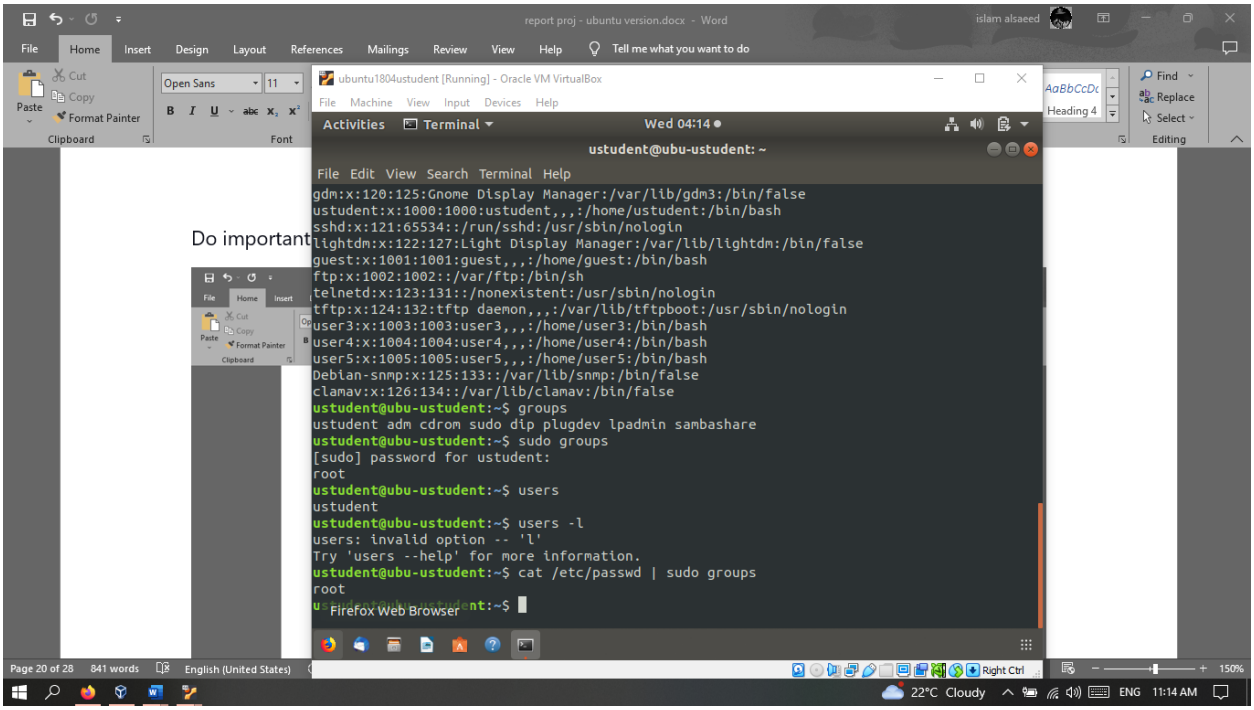
what ports would you suggest to have open and running and why?

22, because its encrypted

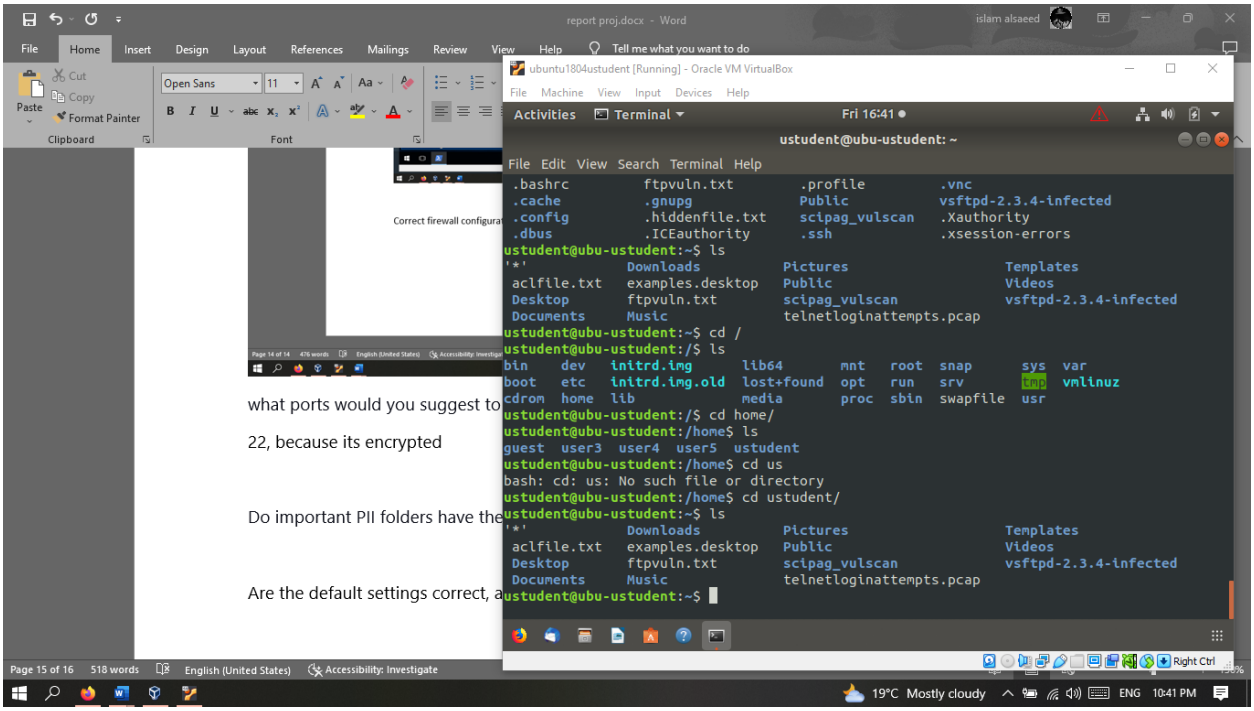
Task 4

Which users have high privileges?

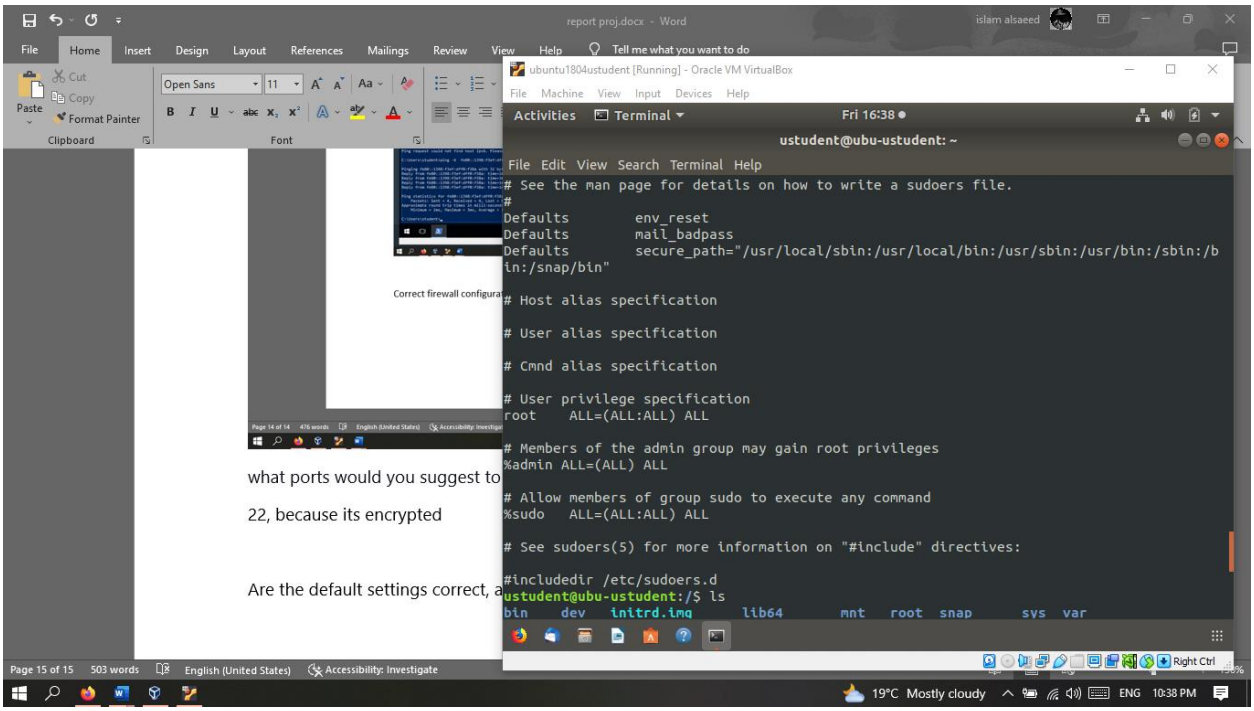
In Linux ? is root



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

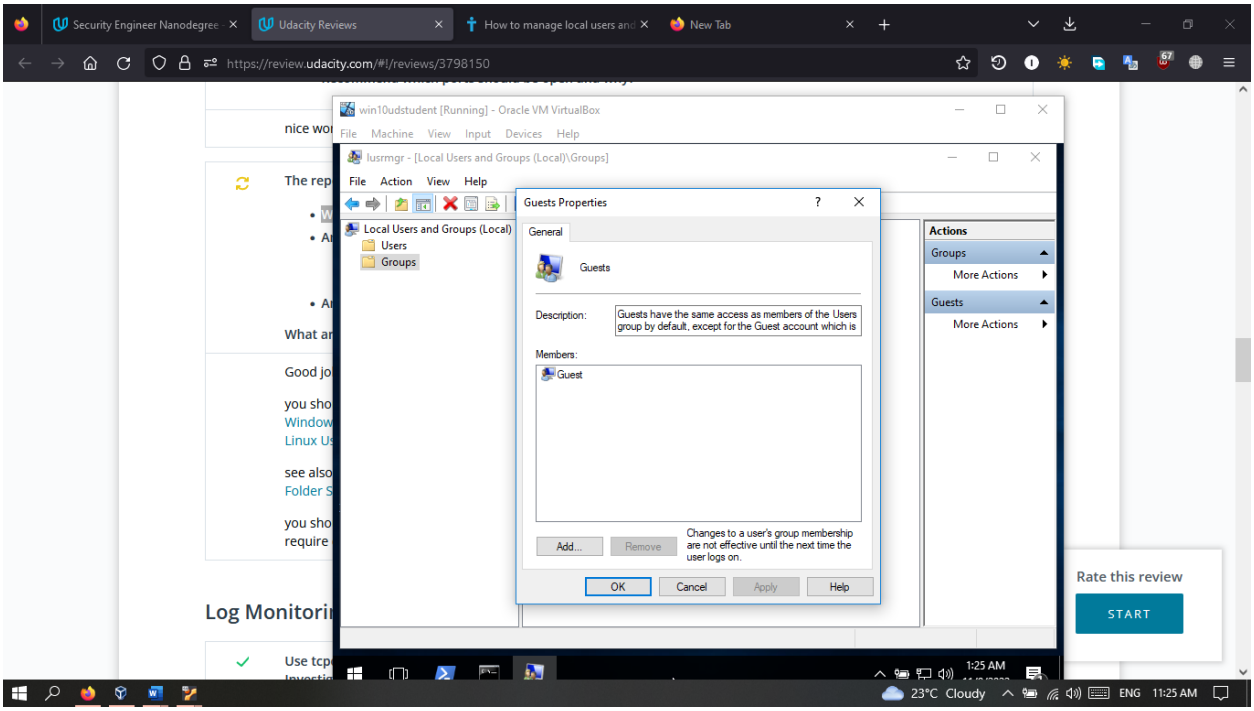


Are the default settings correct, and are there any excessive permissions?no

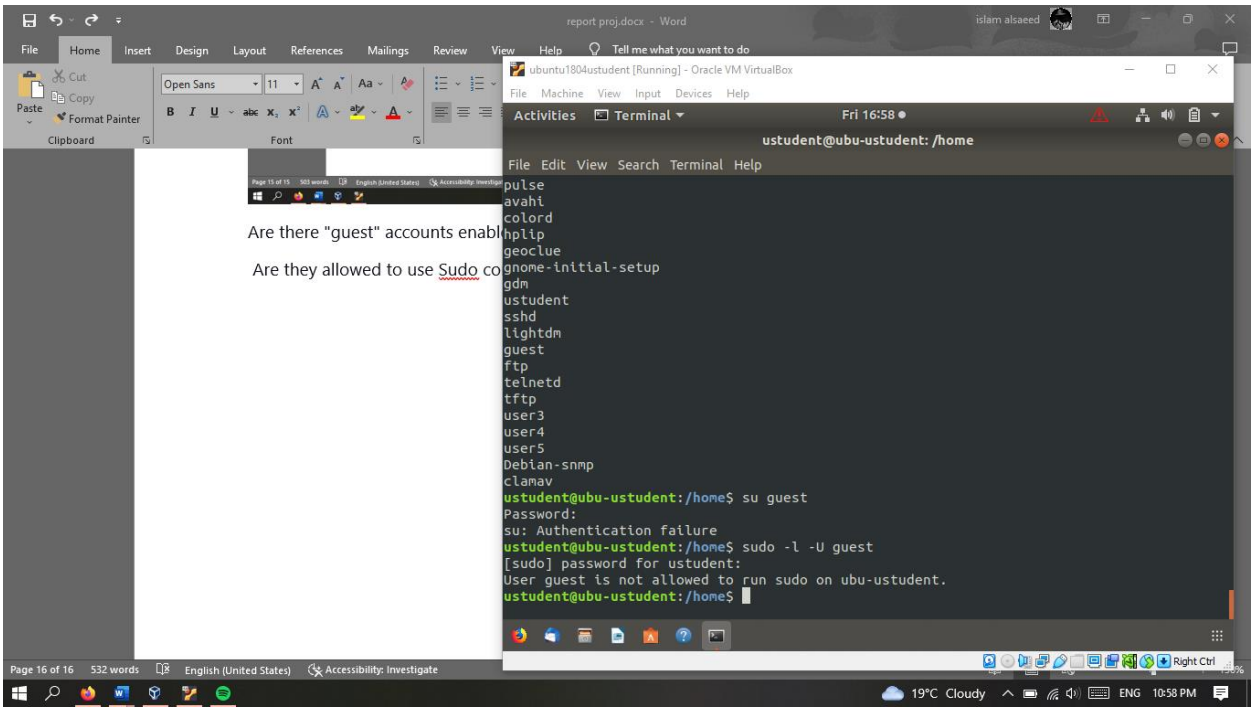


Are there "guest" accounts enabled? Yes

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

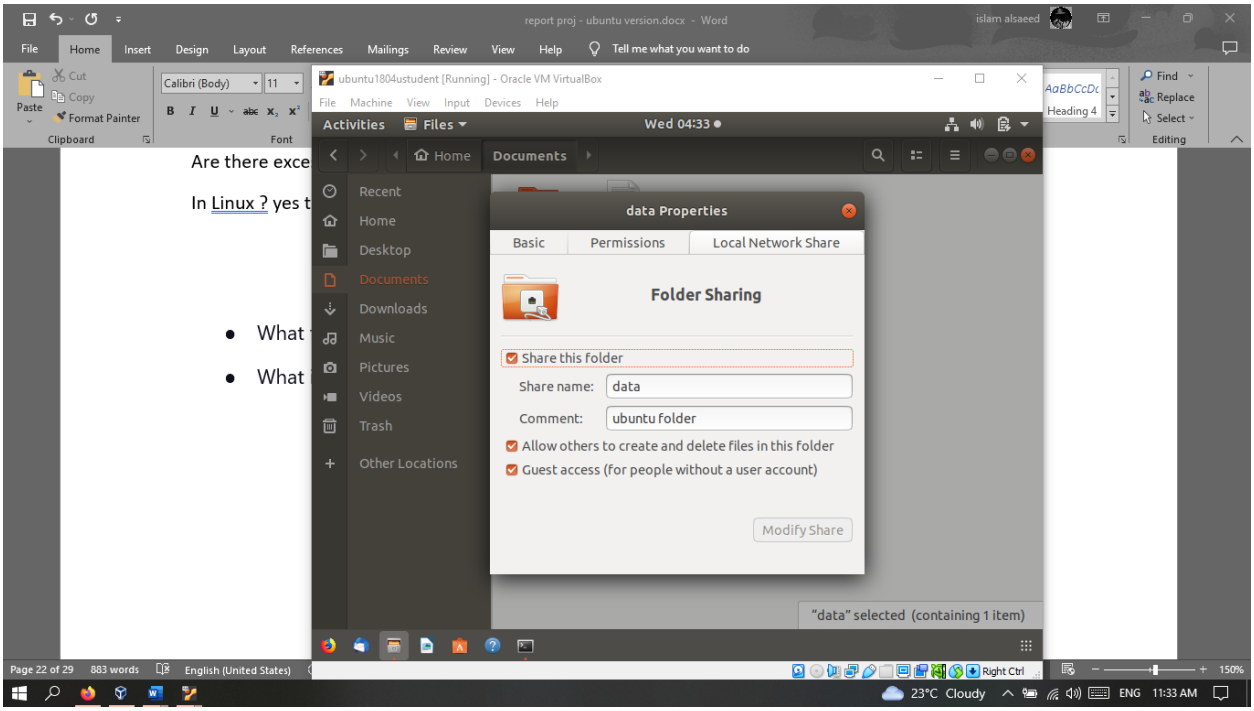


Are they allowed to use Sudo commands? No

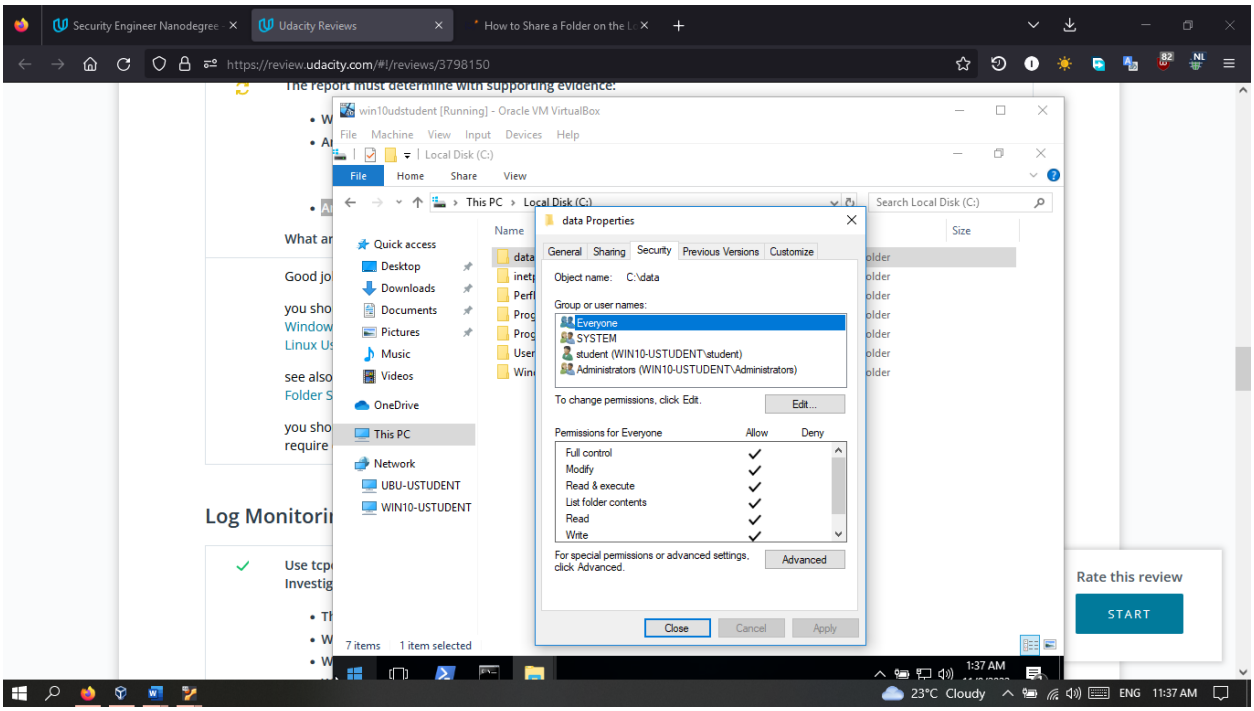


Are there excessive permissions on the data folder in each machine?

In Linux ? yes there is excessive permission



In windows ? yes

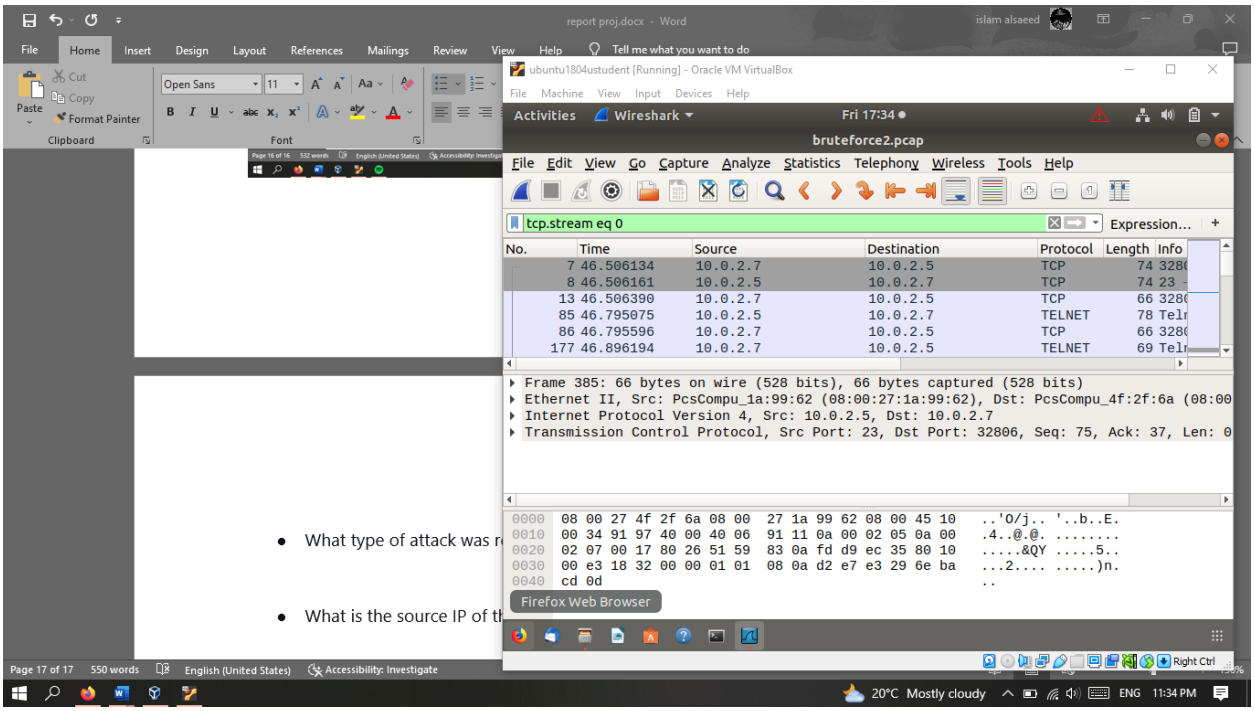


should be restricted to users who must have access for work on both machines

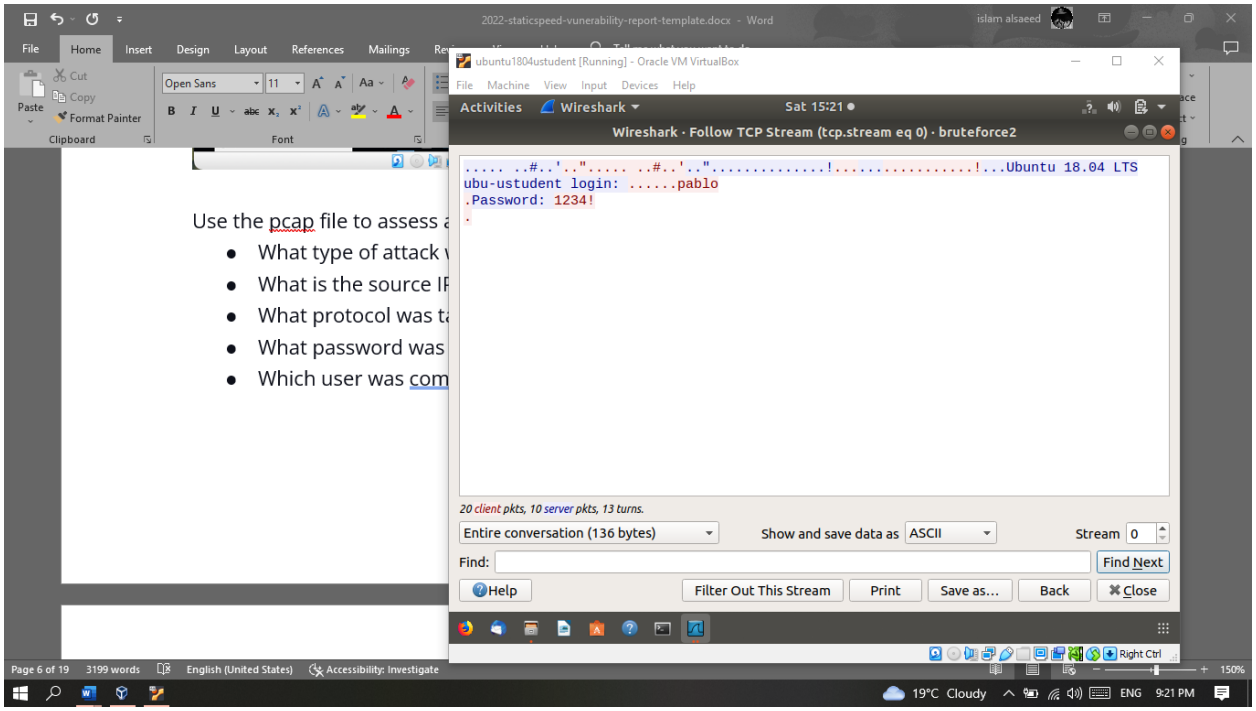
Step 3

Task 1

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

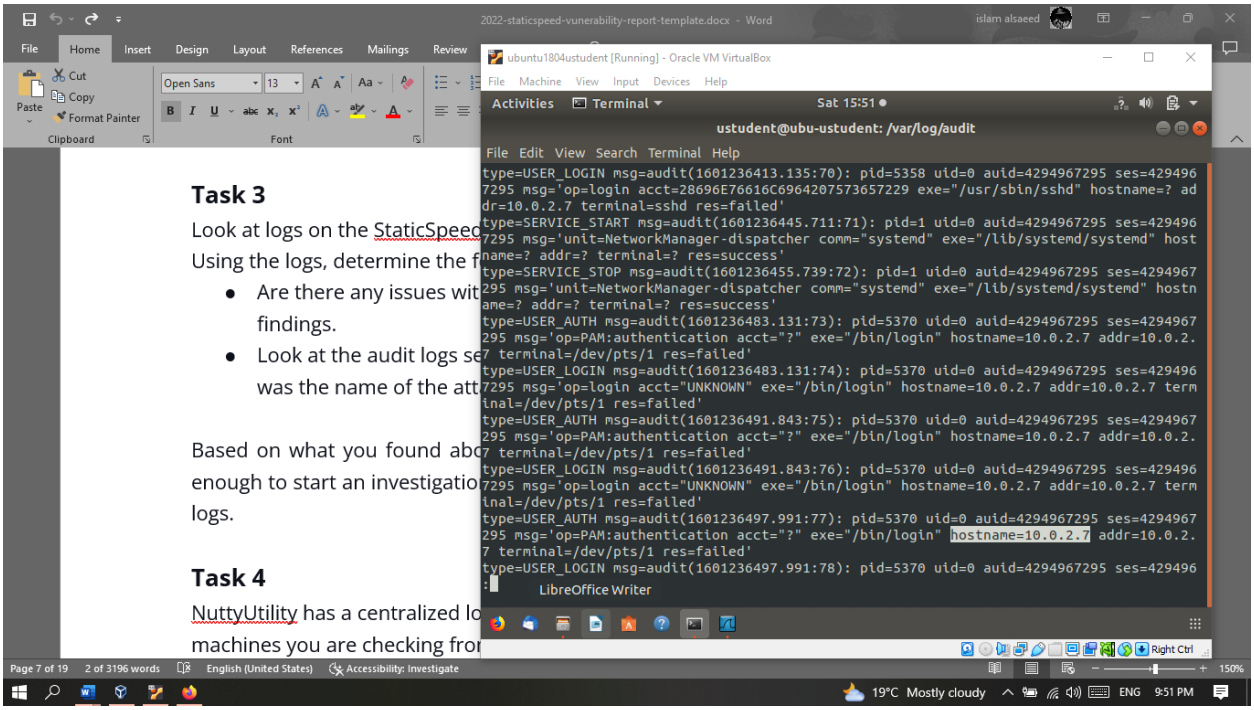


- What protocol was targeted? TCP
- What password was used successfully? 1234!
- Which user was compromised?....pablo



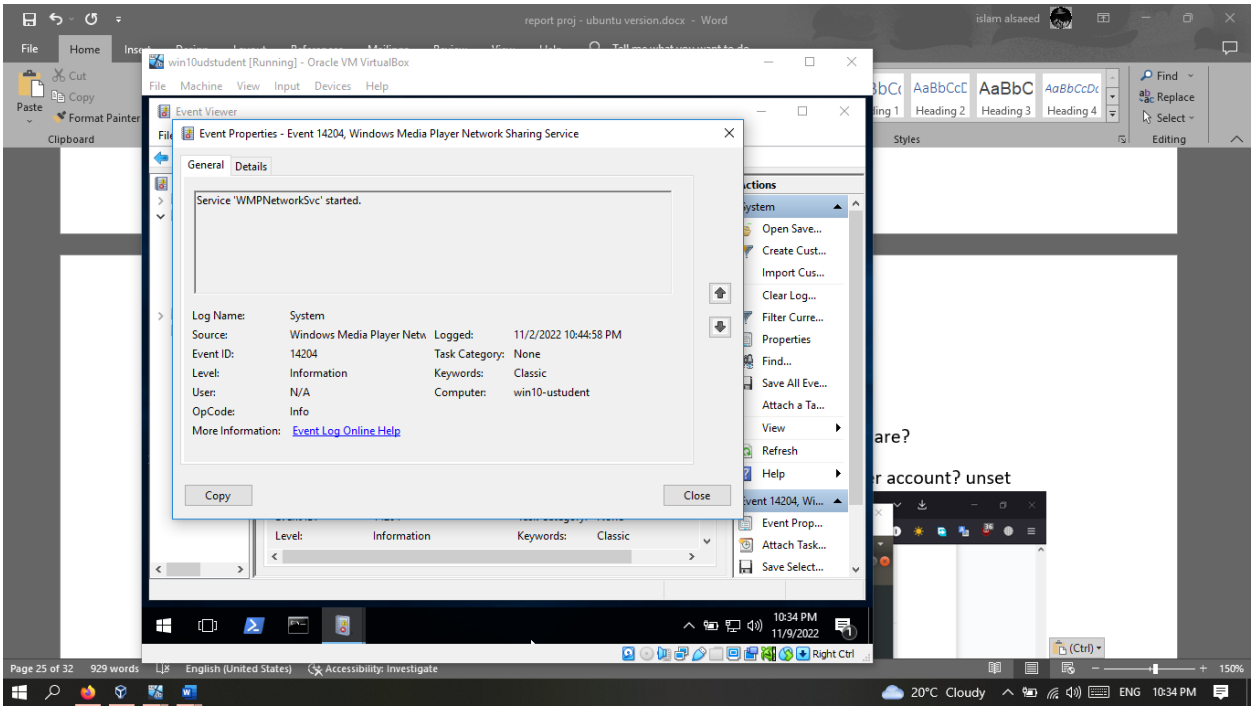
Task 2

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

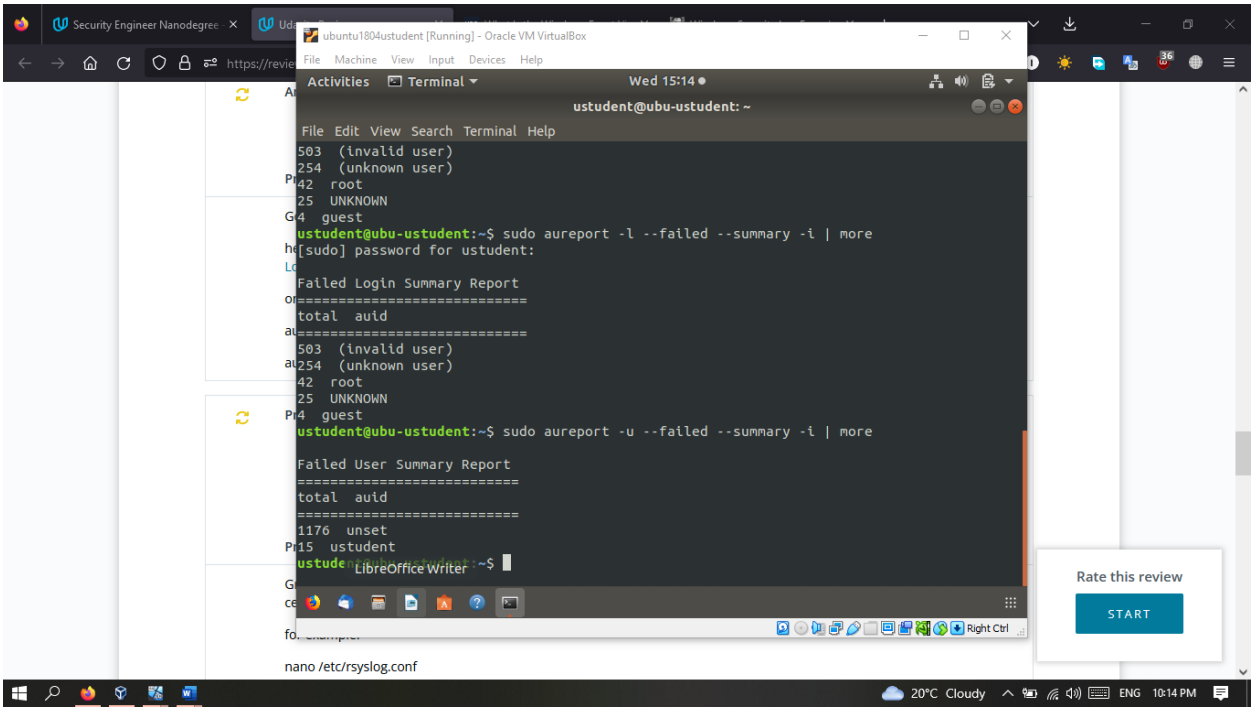


Task 3

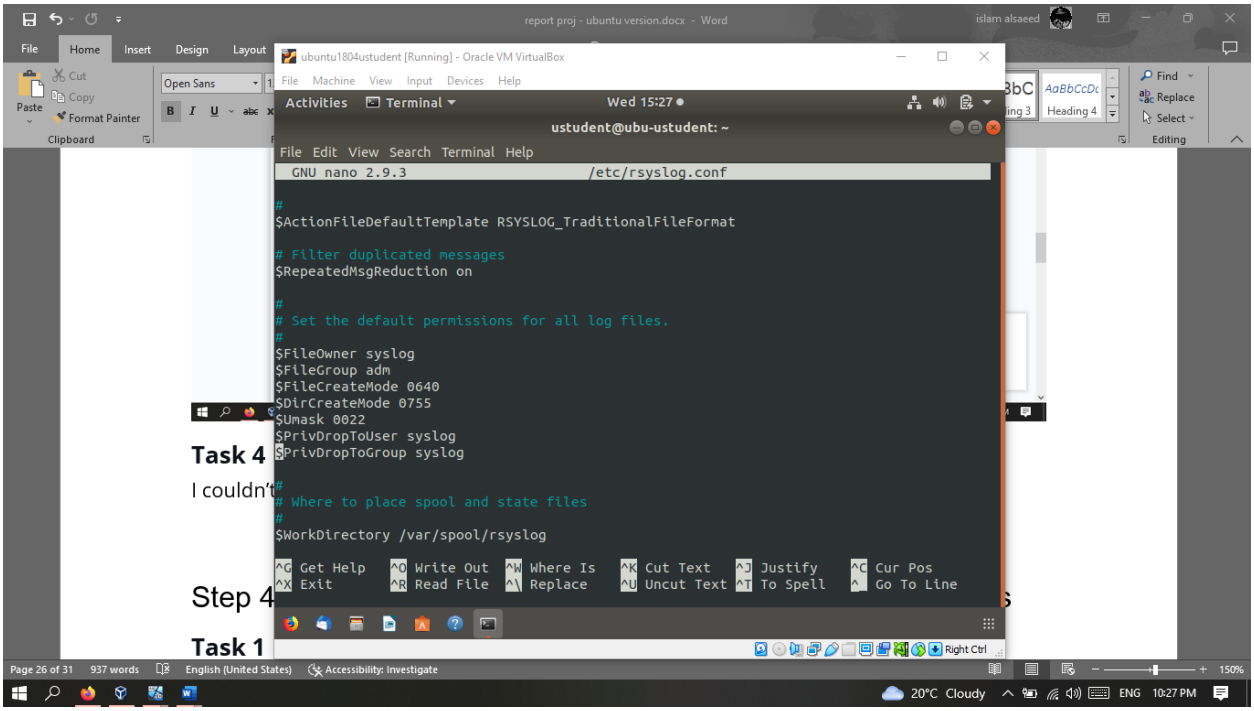
Was there an account uncharacteristic of Windows trying to access the Windows share?

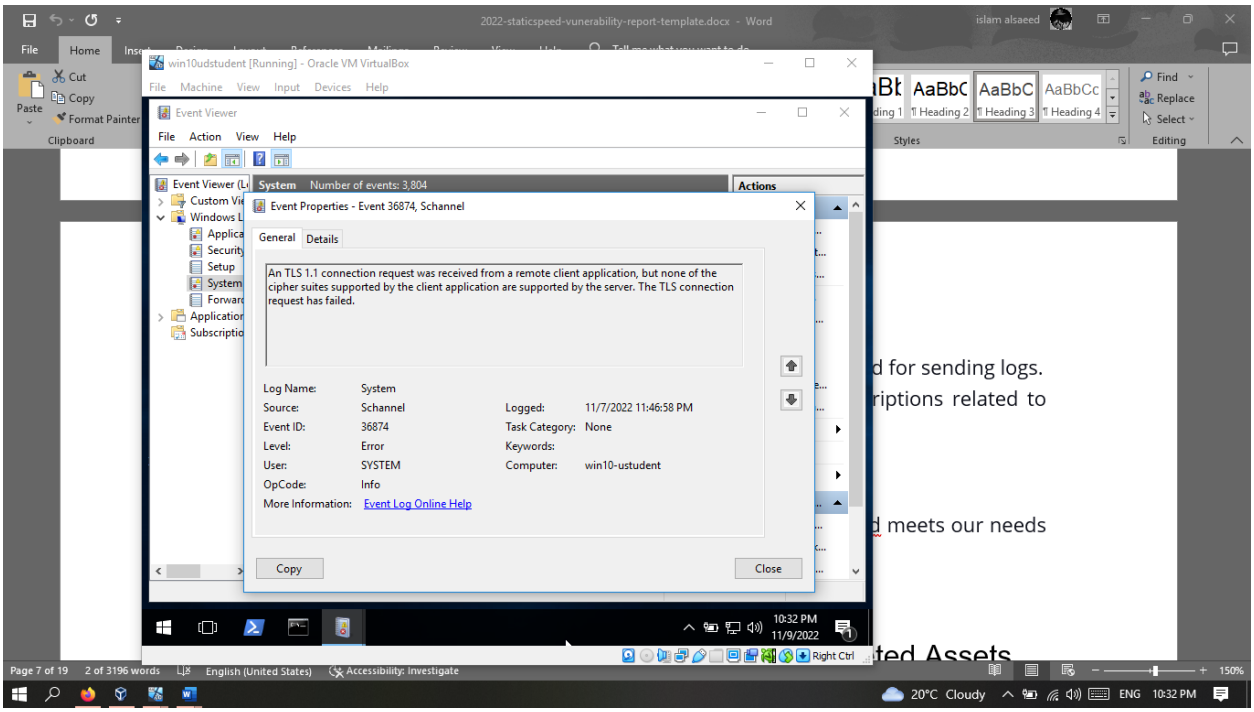


Using the audit logs setup at your Linux machine, what was the name of the attacker account? unset



Task 4



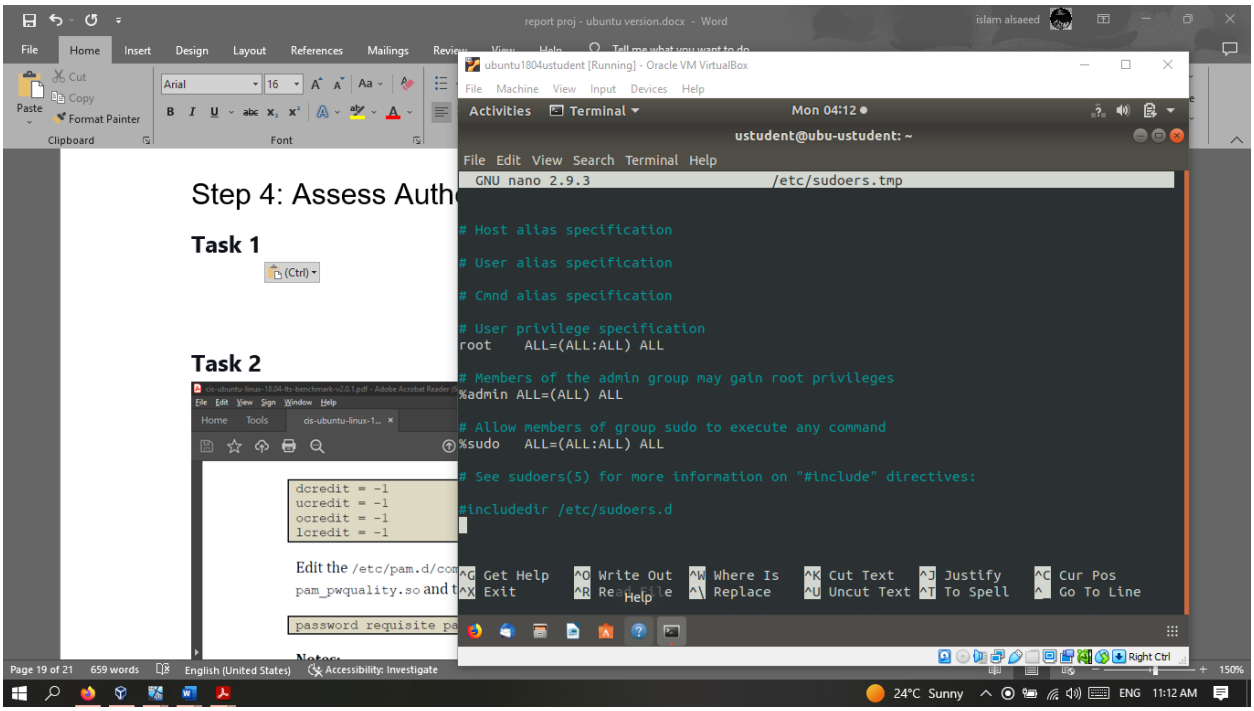


Step 4: Assess Authentication Management at Targeted Assets

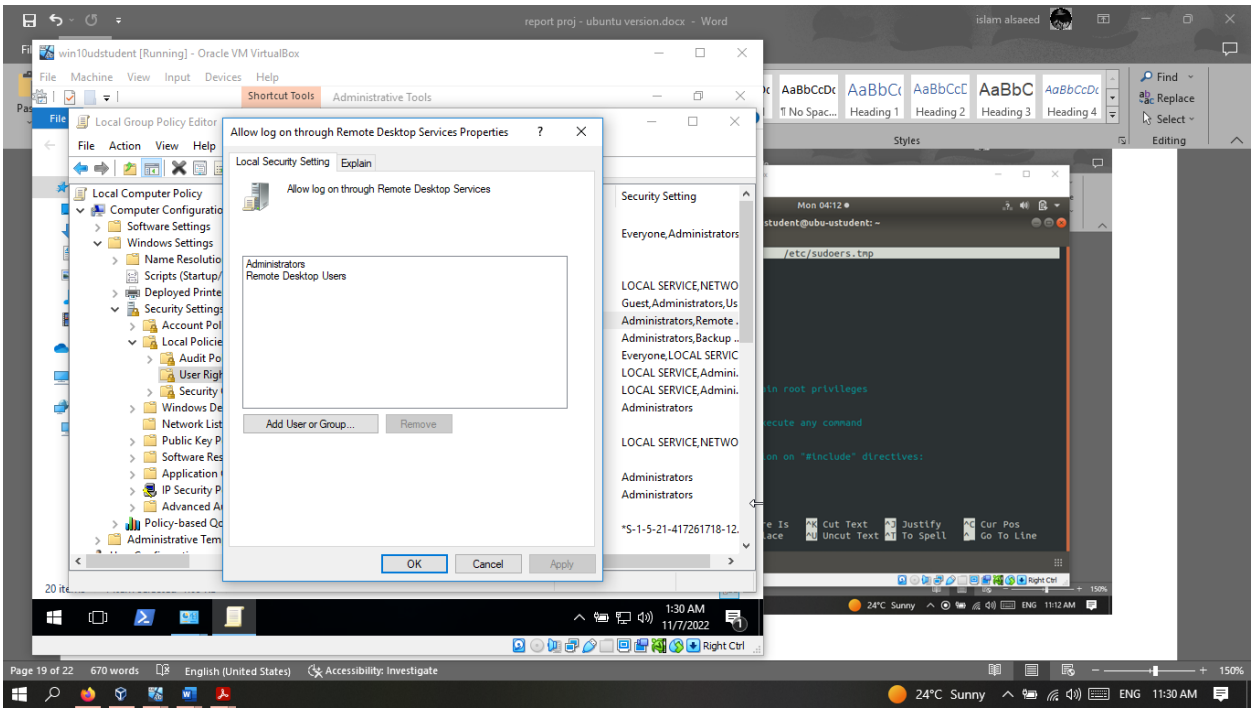
Task 1

Are there users with excessive permissions?

- In ubuntu no

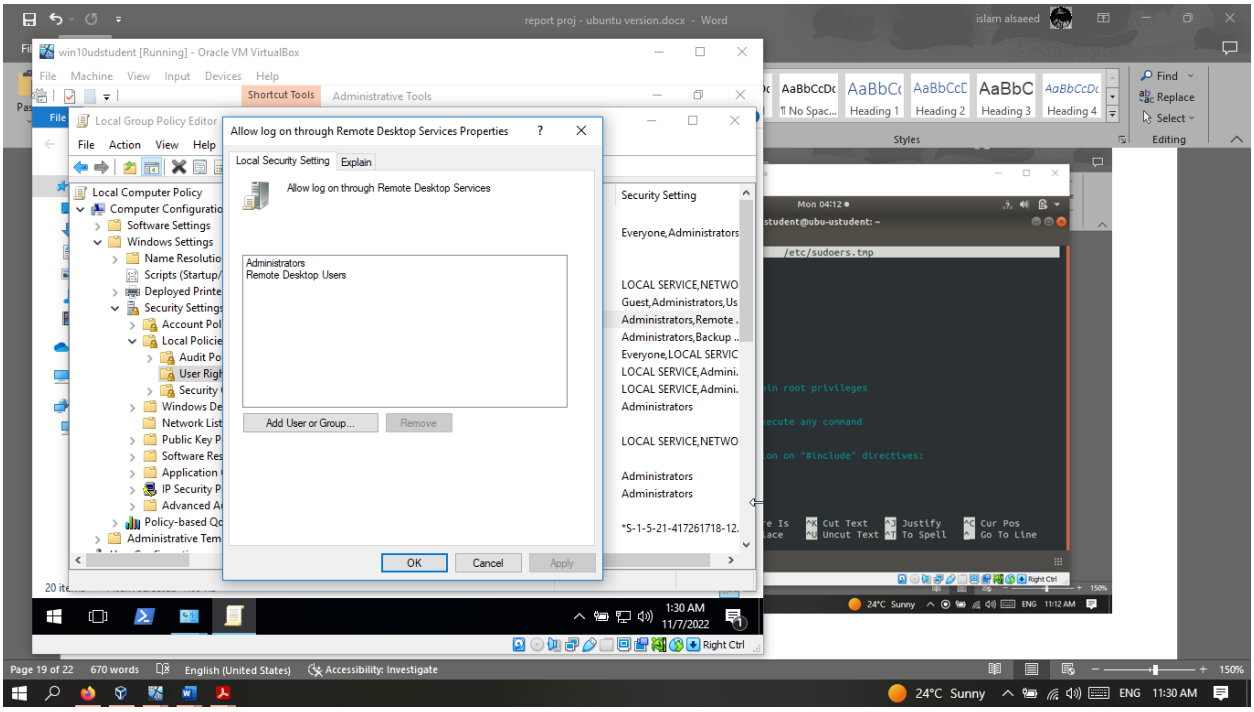


- In windows no , only the administrators and remote desktop users can

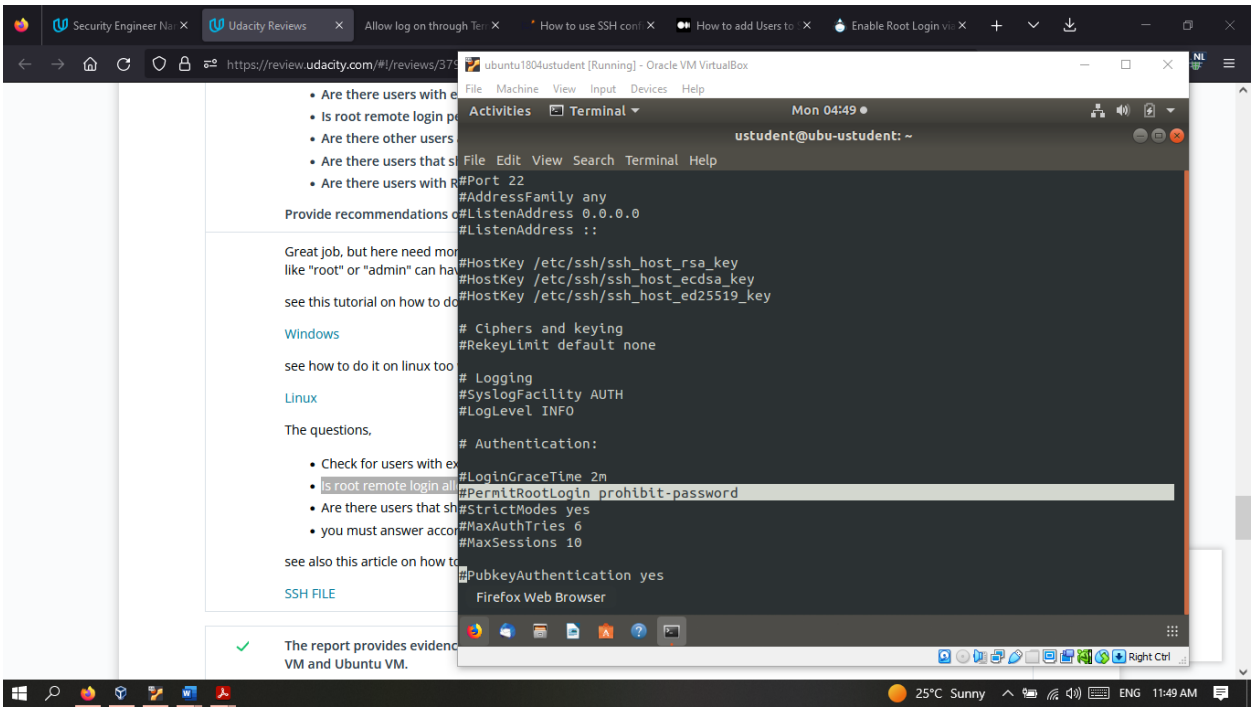


- Is root remote login allowed?

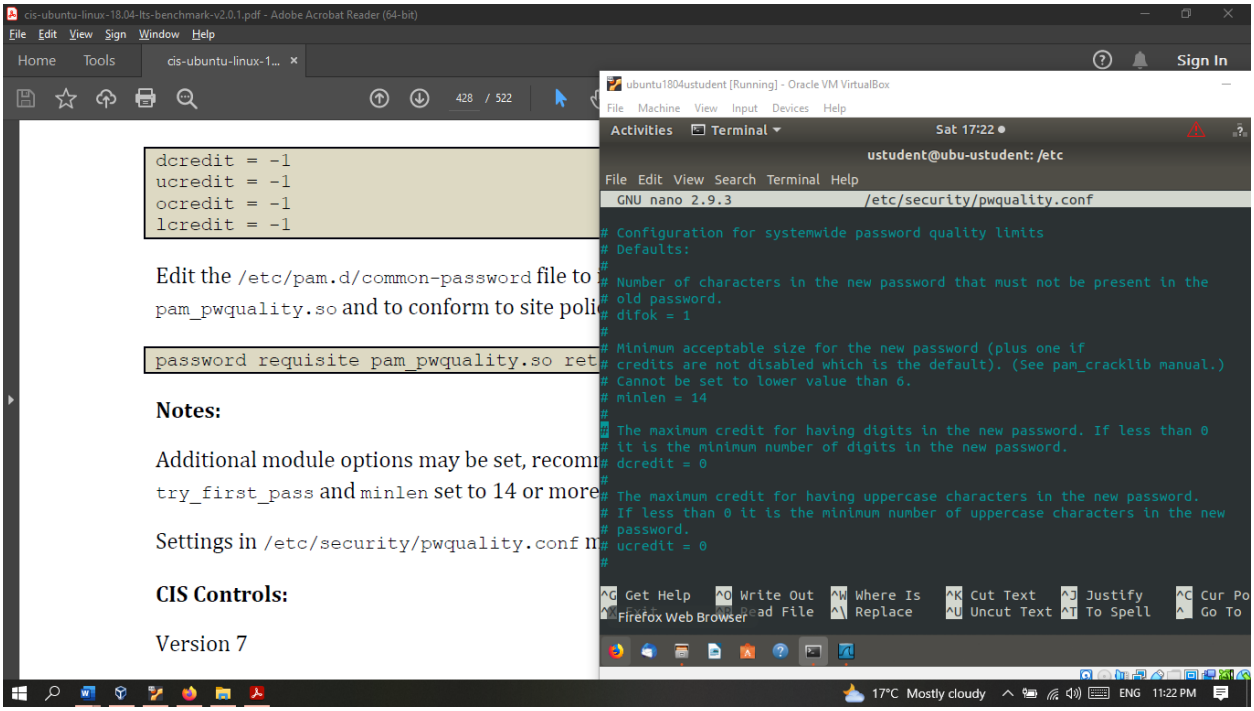
- in windows yes



- In ubuntu



Task 2

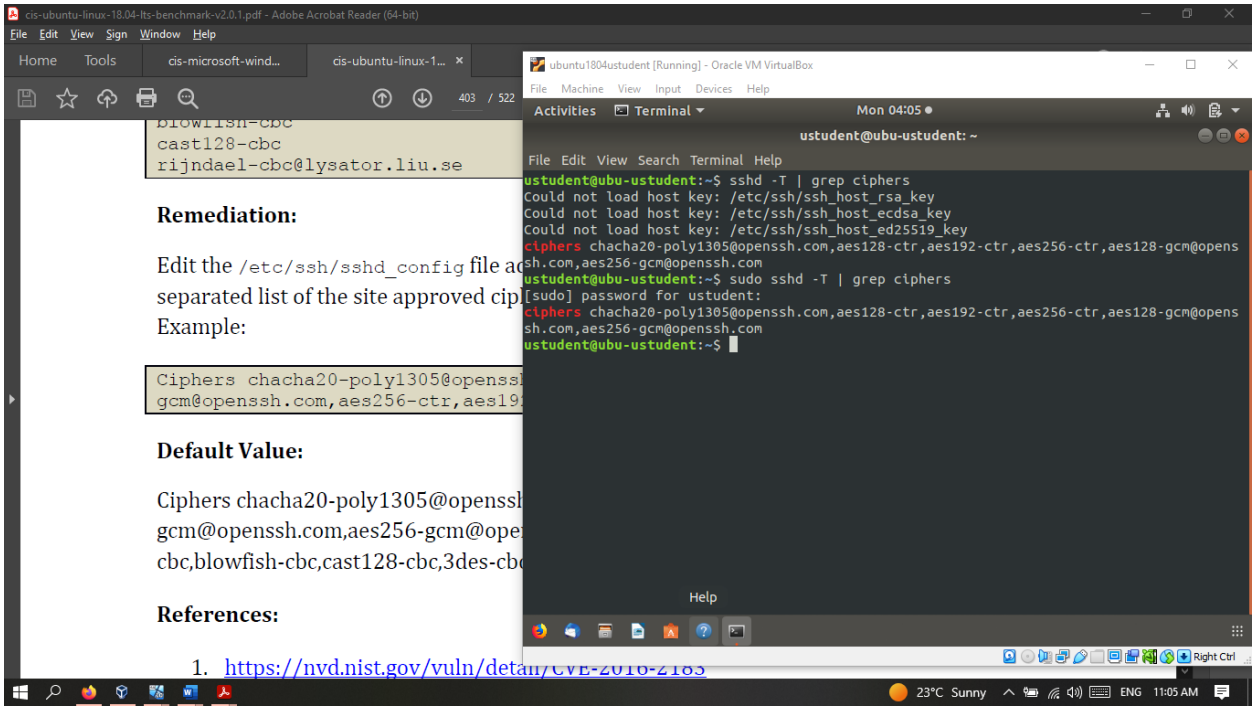


done editing but couldn't find retry line to be edited

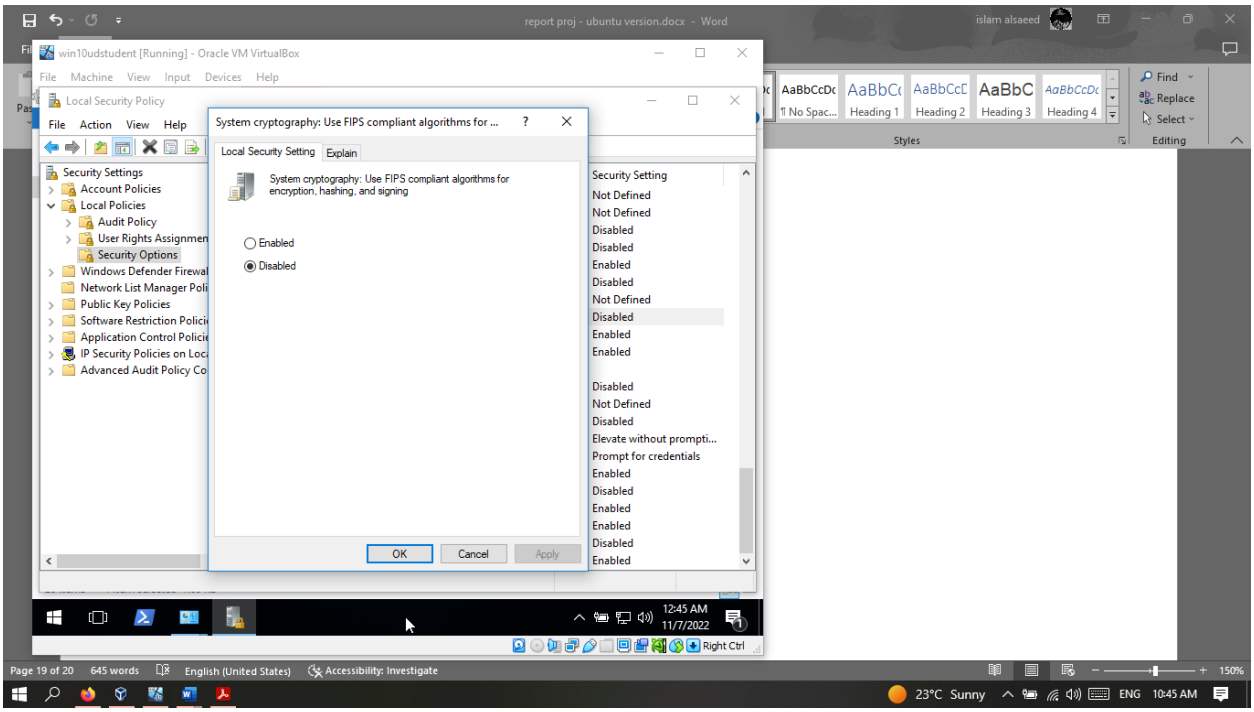
Task 3

these systems are compliant?

- In ubuntu its compliant and uses strong ciphers

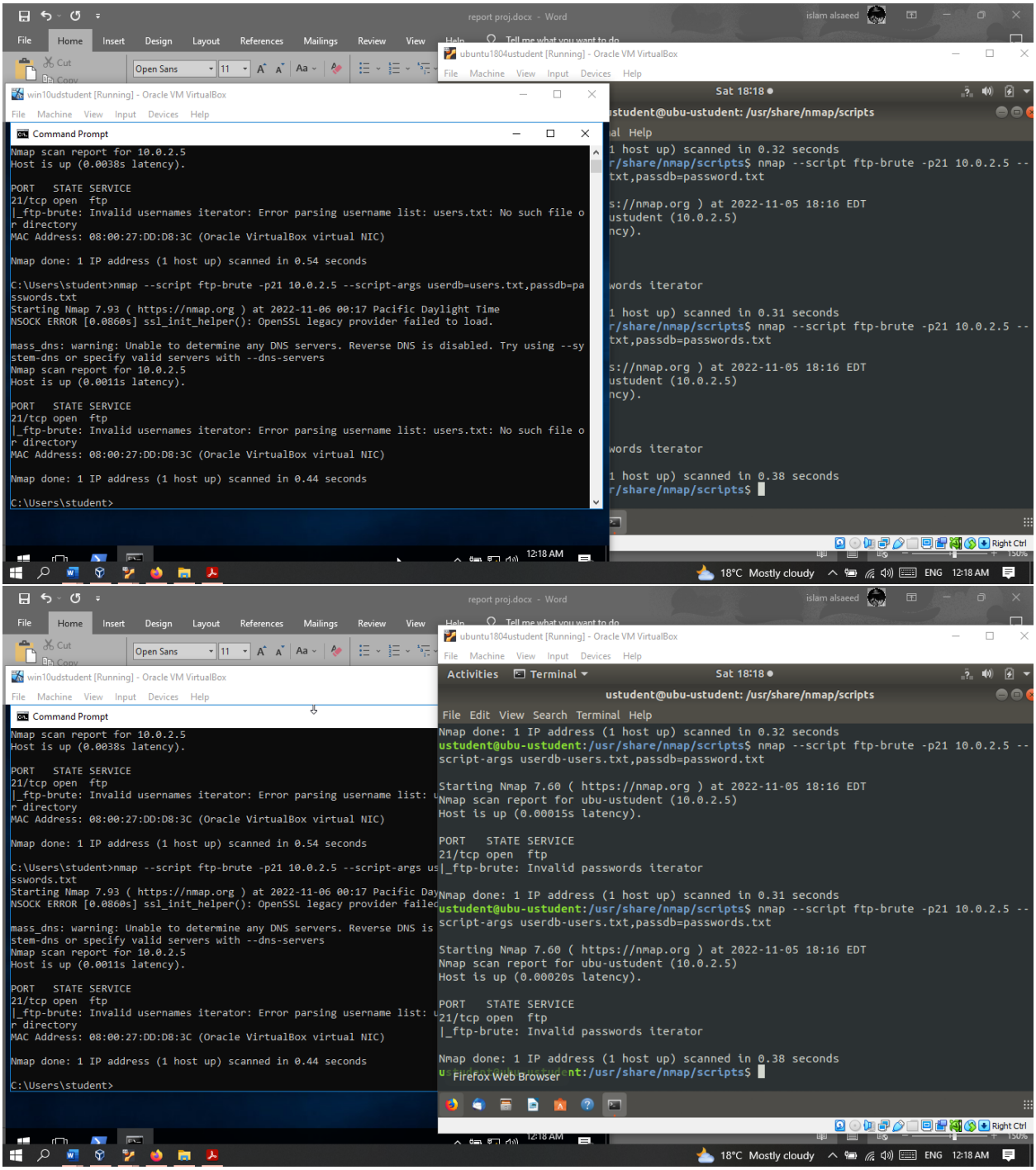


- in windows its not compliant



And should be enabled to be compliant

Task 4



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