Final Report

Asset Identification

Identify the sources of Industry vulnerability and security control frameworks.

Ubuntu 18.04

IP Address: 10.0.2.5

Service	Port	Sensitive Level
http	80 TCP	High
SSH	21 TCP	Medium
xxx	TCP	Low
xxx	xx TCP	Log

High

1- CVE-2022-31813

Issue
Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism.

Impact
This may be used to bypass IP based authentication on the origin server/application.

Mitigation
There is no known workaround at this time.

Reference
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31813
https://security.gentoo.org/glsa/202208-20

High

2- CVE-2022-23943

Issue
Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server.

Impact
Allows an attacker to overwrite heap memory with possibly attacker provided data.

Mitigation
upgrading Apache to the latest version, which is currently 2.4.53. If it is not possible to upgrade, we highly recommend applying the patch which fixes this vulnerability in the mod_sed filter module.

Reference
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23943
https://jfrog.com/blog/diving-into-cve-2022-23943-a-new-apache-memory-corruption-vulnerability/

High

3- CVE-2022-22720

Issue
`Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling.`

Impact
Any authenticated user may exploit this vulnerability and cause a breach in data confidentiality,

integrity, and availability.

Mitigation

Until it is possible to install a fixed version, you can use the following sections as temporary mitigations. These mitigations restrict access to the Configuration utility to only trusted networks or devices, thereby limiting the attack surface.

- Block Configuration utility access through self IP addresses
- Block Configuration utility access through the management interface

Reference

https://support.f5.com/csp/article/K67090077

High

4- CVE-2021-44790

Issue

A buffer overflow flaw in httpd's lua module could allow an out-of-bounds write.

Impact

An attacker who is able to submit a crafted request to an httpd instance that is using the lua module may be able to cause an impact to confidentiality, integrity, and/or availability.

Mitigation

Disabling mod_lua and restarting httpd will mitigate this flaw.

Reference

https://access.redhat.com/security/cve/cve-2021-44790

High

5- CVE-2021-39275

Issue

An out-of-bounds write in function ap_escape_quotes of httpd

Impact
Allows an unauthenticated remote attacker to crash the server or potentially execute code on the system with the privileges of the httpd user, by providing malicious input to the function.

Mitigation
None

Reference
https://access.redhat.com/security/cve/cve-2021-39275

High

6- CVE-2021-26691

Issue
A heap overflow flaw was found In Apache httpd mod_session.

Impact
The highest threat from this vulnerability is to system availability.

Mitigation
Only configurations which use the "SessionEnv" directive (which is not widely used) are vulnerable to this flaw.

Reference
https://access.redhat.com/security/cve/cve-2021-26691

High

7- CVE-2019-0211

Issue
A flaw was found in Apache where code executing in a less-privileged child process or thread could execute arbitrary code with the privilege of the parent process (usually root). An attacker having access to run arbitrary scripts on the web server (PHP, CGI etc) could use this flaw to run code on the web server with root privileges.

Impact

llow an attacker with access to a site on the shared hosted to impact the confidentiality, integrity, and availability (CIA:H) with no interaction (UI:N). Due to the elevated privileges obtained, there is an impact to the system beyond the web server itself (S:C).

Mitigation

System administrators can patch the flaw by updating their servers to Apache httpd version 2.4.39. Developers, programmers, and system admins that use Apache should also employ the principle of least privilege to prevent threats that may exploit related vulnerabilities.Add your

Reference

https://access.redhat.com/security/cve/cve-2019-0211
https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/cve-2019-0211-patched-apache-http-server-root-privilege-escalation-flaw-a-priority-for-web-hosting-providers

High

8- CVE-2021-40438

Issue

A Server-Side Request Forgery (SSRF) flaw was found in mod_proxy of httpd. This flaw allows a remote, unauthenticated attacker to make the httpd server forward requests to an arbitrary server.

Impact

The attacker could get, modify, or delete resources on other services that may be behind a firewall and inaccessible otherwise. The impact of this flaw varies based on what services and resources are available on the httpd network.

Mitigation

None

Reference

https://access.redhat.com/security/cve/cve-2021-40438

High

9- CVE-2020-35452

Issue

A flaw was found in Apache httpd. The mod_auth_digest has a single zero byte stack overflow.

Impact

he highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.

Mitigation

Only configurations which use mod_auth_digest are affected by this flaw. Also as per upstream this flaw is not exploitable in most conditions, so there should really be no impact of this flaw.

Reference

https://access.redhat.com/security/cve/cve-2020-35452

Medium

1- CVE-2022-28615

Issue

Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.

Impact

Very large input to the **ap_strcmp_match** function can lead to an integer overflow and result in an out-of-bounds read. Integer overflow or wraparound may lead to exposure of sensitive information to an unauthorized actor.

Mitigation
update Apache version.

Reference

https://support.f5.com/csp/article/K40582331

Medium

2- CVE-2021-44224

Issue
There's a null pointer de reference and server-side request forgery flaw in httpd's mod_proxy module, when it is configured to be used as a forward proxy.

Impact
A crafted packet could be sent on the adjacent network to the forward proxy that could cause a crash, or potentially SSRF via misdirected Unix Domain Socket requests. In the worst case, this could cause a denial of service or compromise to confidentiality of data.

Mitigation
None

Reference
https://access.redhat.com/security/cve/cve-2021-44224

Medium

3- CVE-2029-10082

Issue
A read-after-free vulnerability was discovered in Apache httpd, in mod_http2.

Impact
A specially crafted http/2 client session could cause the server to read memory that was previously freed during connection shutdown, potentially leading to a crash.

Mitigation
This flaw is only exploitable if Apache httpd is configured to respond to HTTP/2 requests, which is done by including "h2" or "h2c" in the "Protocols" list in a configuration file. The following command can be used to search for possible vulnerable configurations:

```
grep -R '^\s*Protocols\>.*\<h2\>' /etc/httpd/
```

Reference
https://access.redhat.com/security/cve/cve-2019-10082

Medium

4- CVE-2029-10082

Issue
An issue was discovered in OpenSSH 7.9. Due to the scp implementation being derived from 1983 rcp, the server chooses which files/directories are sent to the client. However, the scp client only performs cursory validation of the object name returned (only directory traversal attacks are prevented).

Impact
A malicious scp server (or Man-in-The-Middle attacker) can overwrite arbitrary files in the scp client target directory. If recursive operation (-r) is performed, the server can manipulate subdirectories as well (for example, to overwrite the .ssh/authorized_keys file).

Mitigation

This issue only affects the users of scp binary which is a part of openssh-clients package. Other usage of SSH protocol or other ssh clients is not affected. Administrators can uninstall openssh-clients for additional protection against accidental usage of this binary. Removal of openssh-clients package will make the packaged binaries like scp, ssh etc unavailable

Reference

https://access.redhat.com/security/cve/cve-2019-6111

Medium

5- CVE-2018-15919

Issue

OpenSSH server was found to respond differently to failed GSSAPI authentication attempts when the target user existed versus when that user did not exist.

Impact

A remote attacker could use this bug to test for the existence of particular usernames on a target system.

Mitigation

If GSSAPI Authentication is not required, this flaw can be mitigated by changing the global configuration in `/etc/ssh/sshd_config` from `GSSAPIAuthentication yes` to `GSSAPIAuthentication no`.

Reference

https://access.redhat.com/security/cve/cve-2018-15919

Medium

6- CVE-2018-15473

Issue
A user enumeration vulnerability flaw was found in OpenSSH, though version 7.7. The vulnerability occurs by not delaying bailout for an invalid authenticated user until after the packet containing the request has been fully parsed.

Impact
The highest threat from this vulnerability is to data confidentiality.

Mitigation
Configuring your firewall to limit the origin and/or rate of incoming ssh connections (using the netfilter xt_recent module) will limit the impact of this attack, as it requires a new TCP connection for each username tested. This configuration also provides some protection against brute-force attacks on SSH passwords or keys.

Reference
https://access.redhat.com/security/cve/cve-2018-15473

Medium

7- CVE-2020-14145

Issue
A flaw was found in OpenSSH in versions 5.7 through 8.3, where an Observable Discrepancy occurs and leads to an information leak in the algorithm negotiation

Impact
This flaw allows a man-in-the-middle attacker to target initial connection

attempts, where there is no host key for the server that has been cached by the client.

Mitigation
Always connect to SSH servers with verified host keys to avoid any possibilities of man-in-the-middle attack.

Reference
https://access.redhat.com/security/cve/cve-2020-14145
Medium

8- CVE-2019-6110

Issue
In OpenSSH 7.9, due to accepting and displaying arbitrary stderr output from the server, a malicious server (or Man-in-The-Middle attacker) can manipulate the client output, for example to use ANSI control codes to hide additional files being transferred.

Impact
Affects the integrity of the files.

Mitigation
This issue only affects the users of scp binary which is a part of openssh-clients package. Other usage of SSH protocol or other ssh clients is not affected. Administrators can uninstall openssh-clients for additional protection against accidental usage of this binary. Removing the openssh-clients package will make binaries like scp and ssh etc unavailable on that system.

Reference
https://access.redhat.com/security/cve/cve-2019-6110

Verify the current setting of software updates and third-party packages at audited machines.

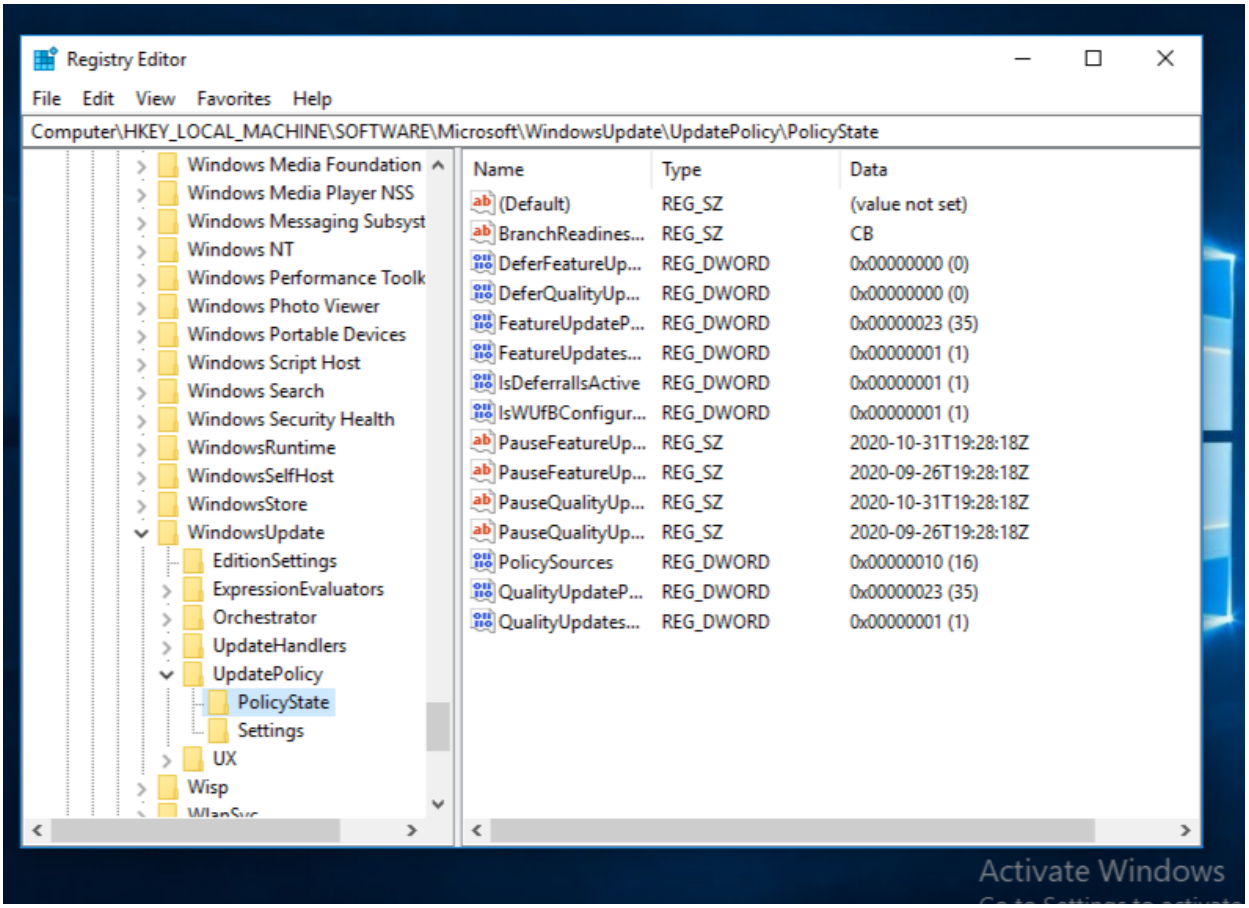
Windows 10 ENT

Control check - 18.9.102.2 (L1) Ensure 'Configure Automatic Updates' is set to 'Enabled' (Automated)

Result: No auto update key.

Proof of check:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU:NoAutoUpdate
```



Impact: Critical operating system updates and service packs will be installed as necessary.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows Update\Configure Automatic Updates
```

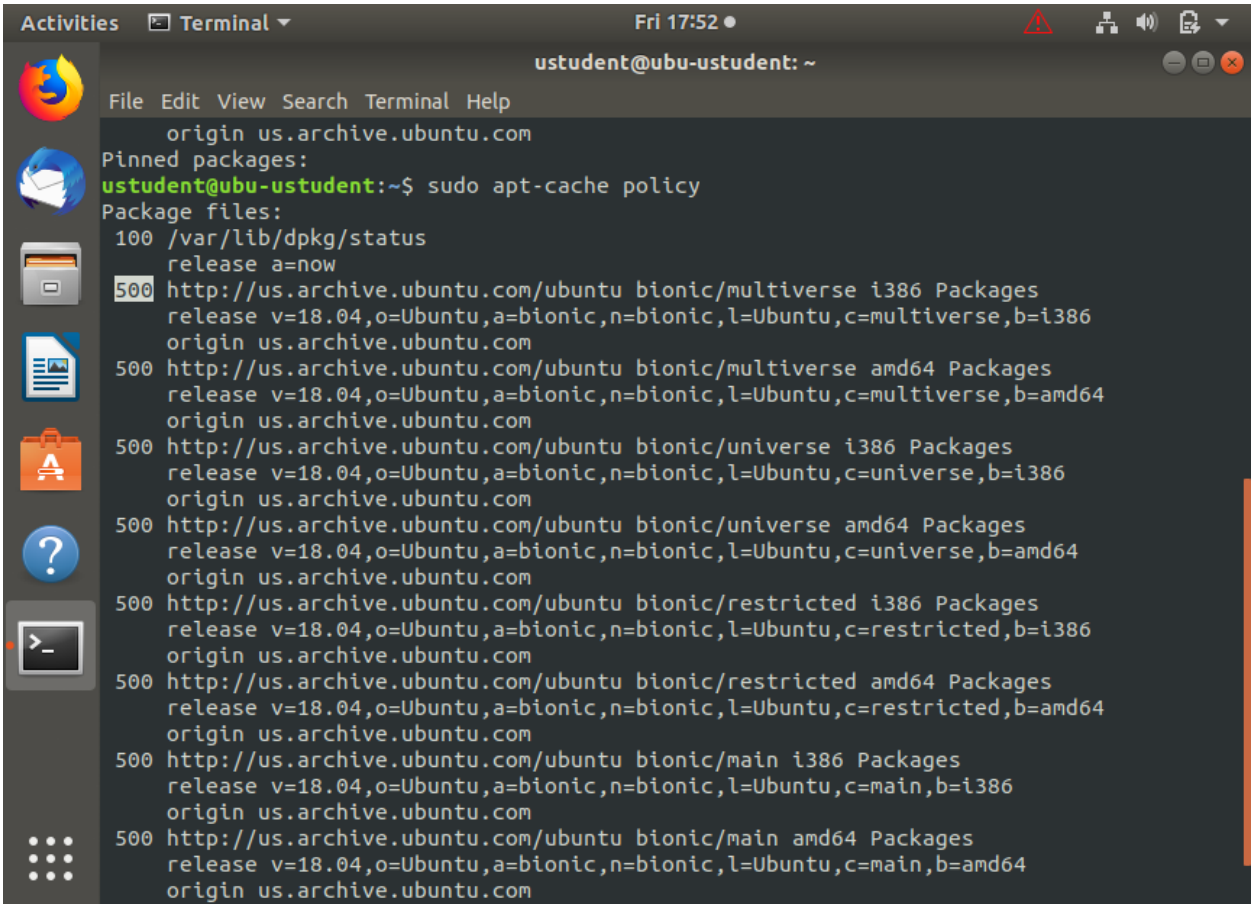
Note: This Group Policy path is provided by the Group Policy template `WindowsUpdate.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Ubuntu 18.04

Control Check: CIS 1.2.1 Ensure package manager repositories are configured (Not Scored)

Result: The package has the priority 500, which means its uninstalled package.

Proof of check:



Impact: If a system's package repositories are misconfigured important patches may not be identified or a rogue repository could introduce compromised software.

Remediation:

Configure your package manager repositories according to site policy.

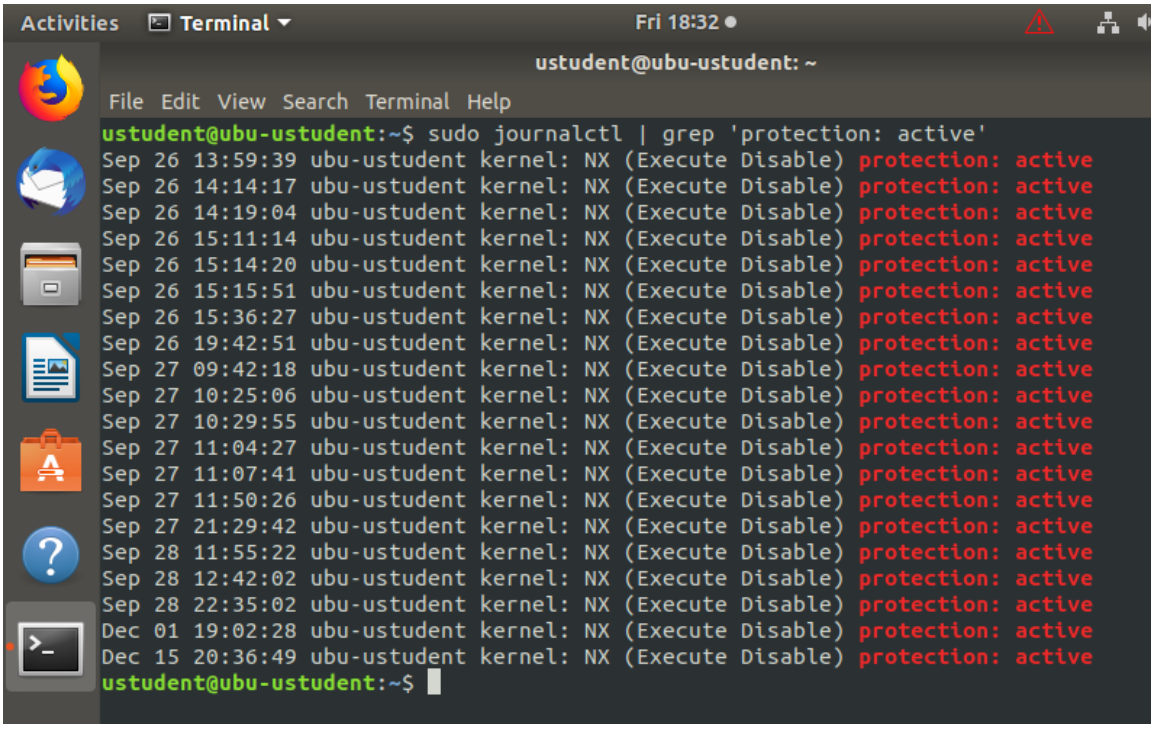
Verify that native protections for the operating systems are in place.

Ubuntu 18.04

Control Check: CIS 1.6.1 Ensure XD/NX support is enabled (Scored)
Result: XD/NX support is enabled and protection is active.
Proof of check:

```
# journalctl | grep 'protection: active'

kernel: NX (Execute Disable) protection: active
```



No need for remediation as the machine is compliance to the CIS benchmark.

Ubuntu 18.04

Control Check: CIS 1.6.2 Ensure address space layout randomization (ASLR) is enabled (Scored)

Result: The first command shows the ASLR but the second command does not.

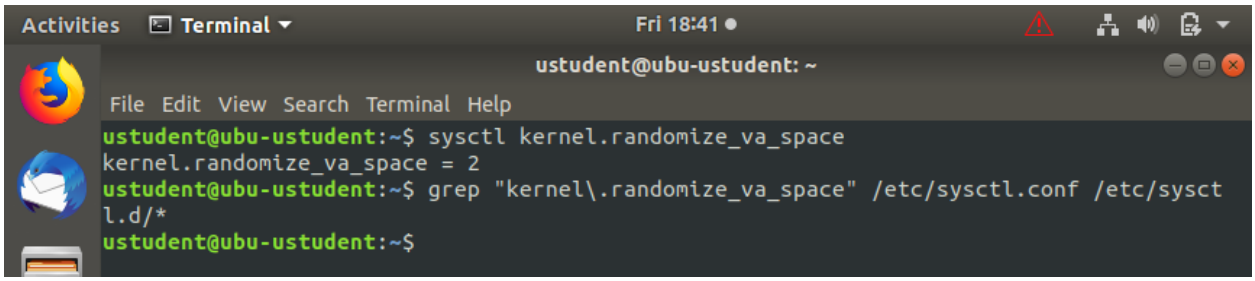
Proof of check:

```
# 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
```



Remediation:

Set the following parameter in `/etc/sysctl.conf` or a `/etc/sysctl.d/*` file:

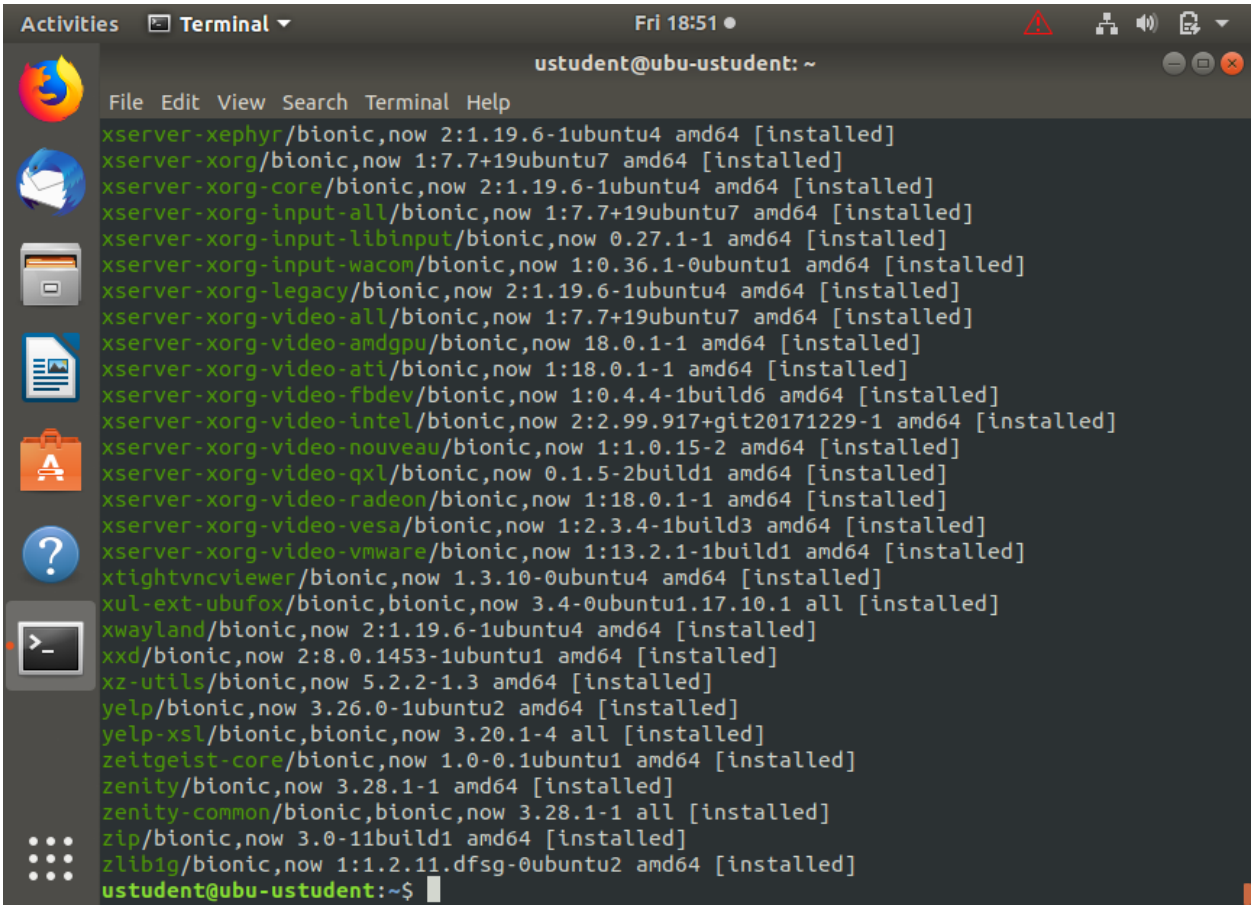
```
kernel.randomize_va_space = 2
```

Run the following command to set the active kernel parameter:

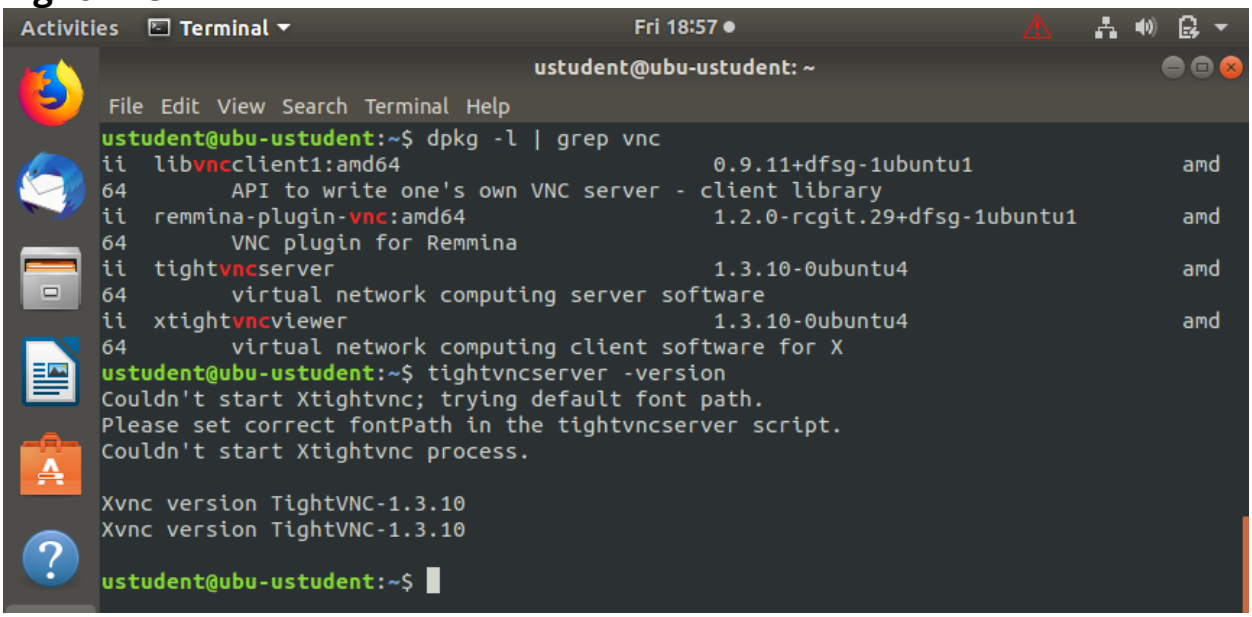
```
# sysctl -w kernel.randomize_va_space=2
```

Installed packages in Ubuntu:

sudo apt list --installed



TightVNC



TightVNC is installed in Ubuntu.

Having TightVNC brings added risk to the system. In TightVNC code version 1.3.10, there's a critical global buffer overflow (CVE-2019-8287) in HandleCoRREBBP macro function, also with a CVSS rating of 9.8 out of 10. This can also potentially result RCE, Kaspersky found.

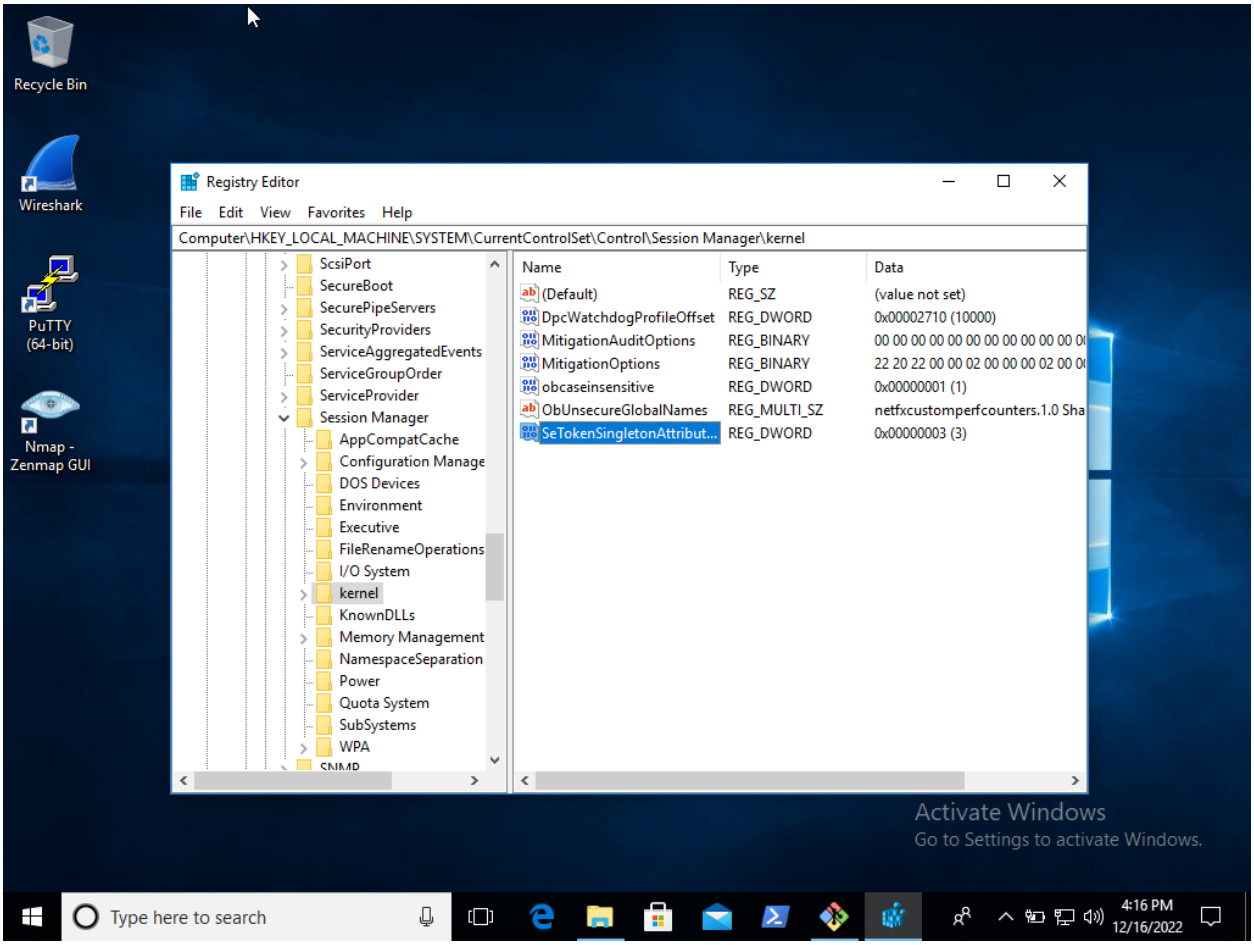
Windows 10 ENT

Control check - 18.3.4 (L1) Ensure 'Enable Structured Exception Handling Overwrite Protection (SEHOP)' is set to 'Enabled' (Automated)

Result: DisableExceptionChainValidation key is not there.

Proof of check:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session
Manager\kernel:DisableExceptionChainValidation
```



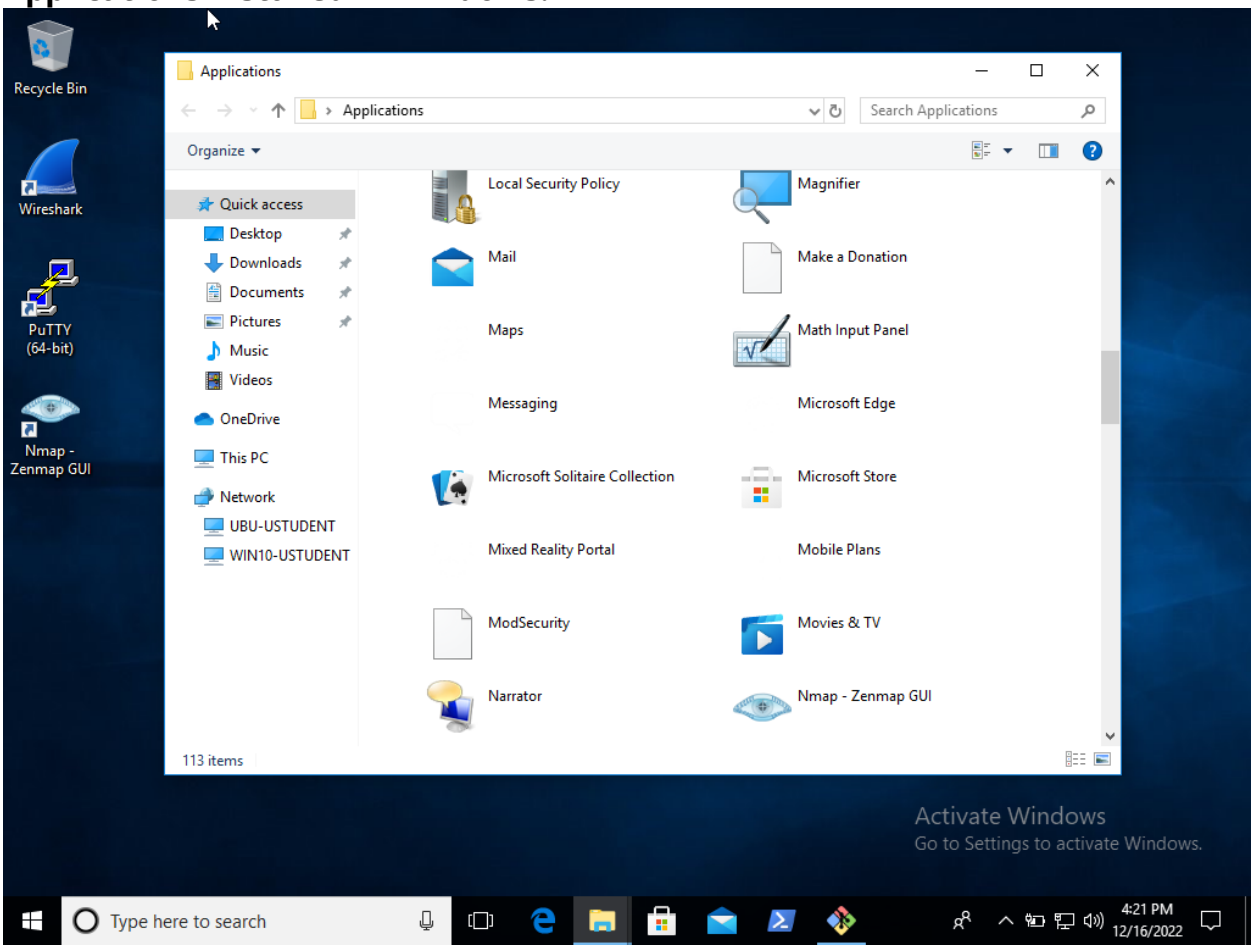
Impact: After you enable SEHOP, existing versions of Cygwin, Skype, and Armadillo-protected applications may not work correctly.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

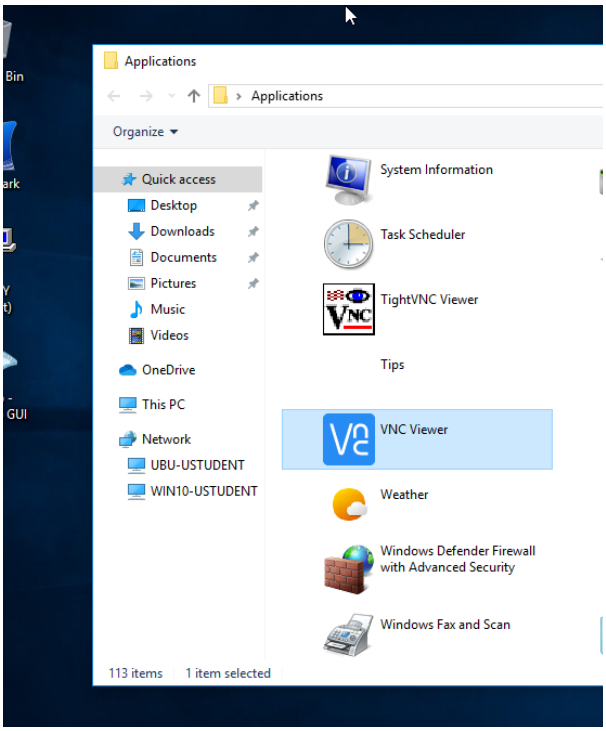
```
Computer Configuration\Policies\Administrative Templates\MS Security
Guide\Enable Structured Exception Handling Overwrite Protection (SEHOP)
```

Applications installed in Windows:



113 applications are installed.

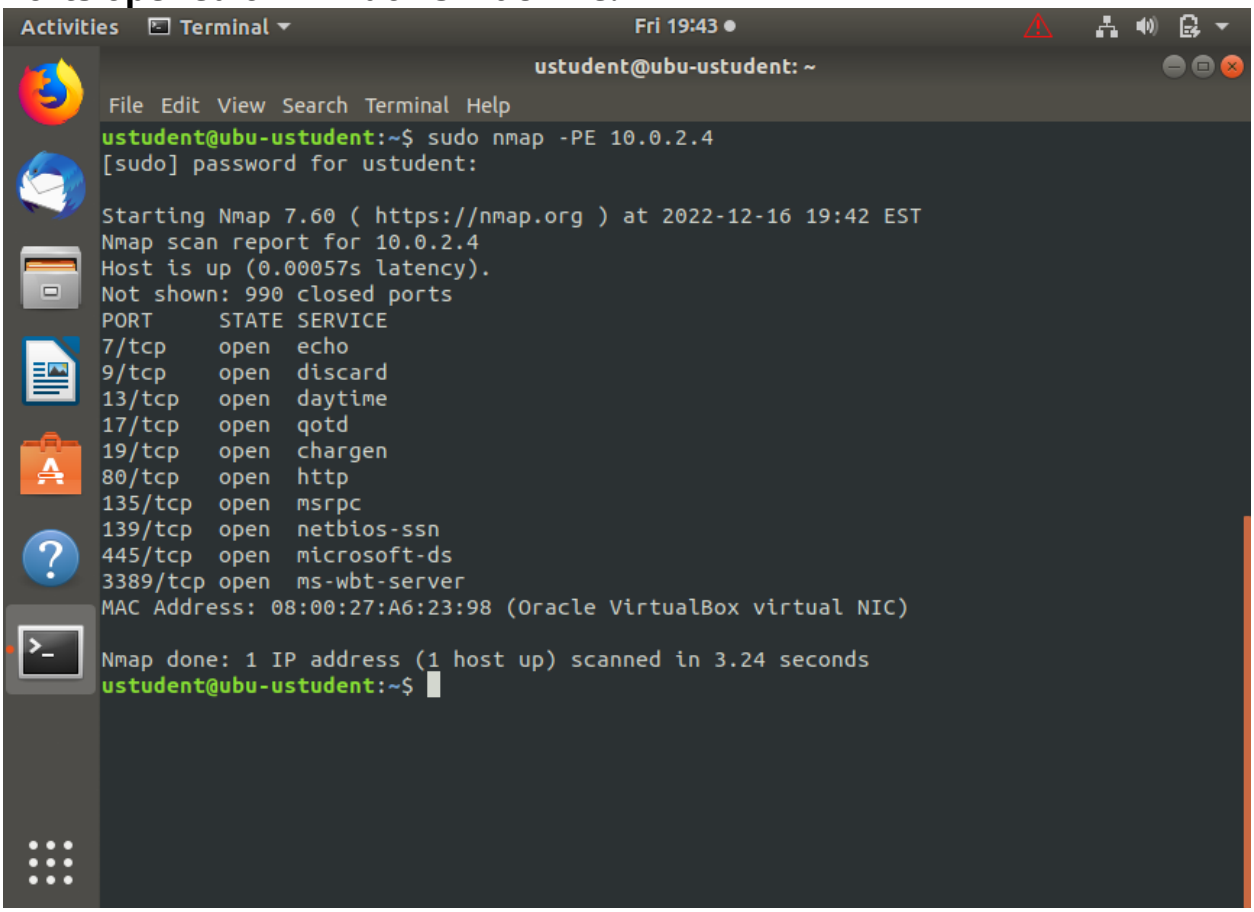
VNC Viewer:



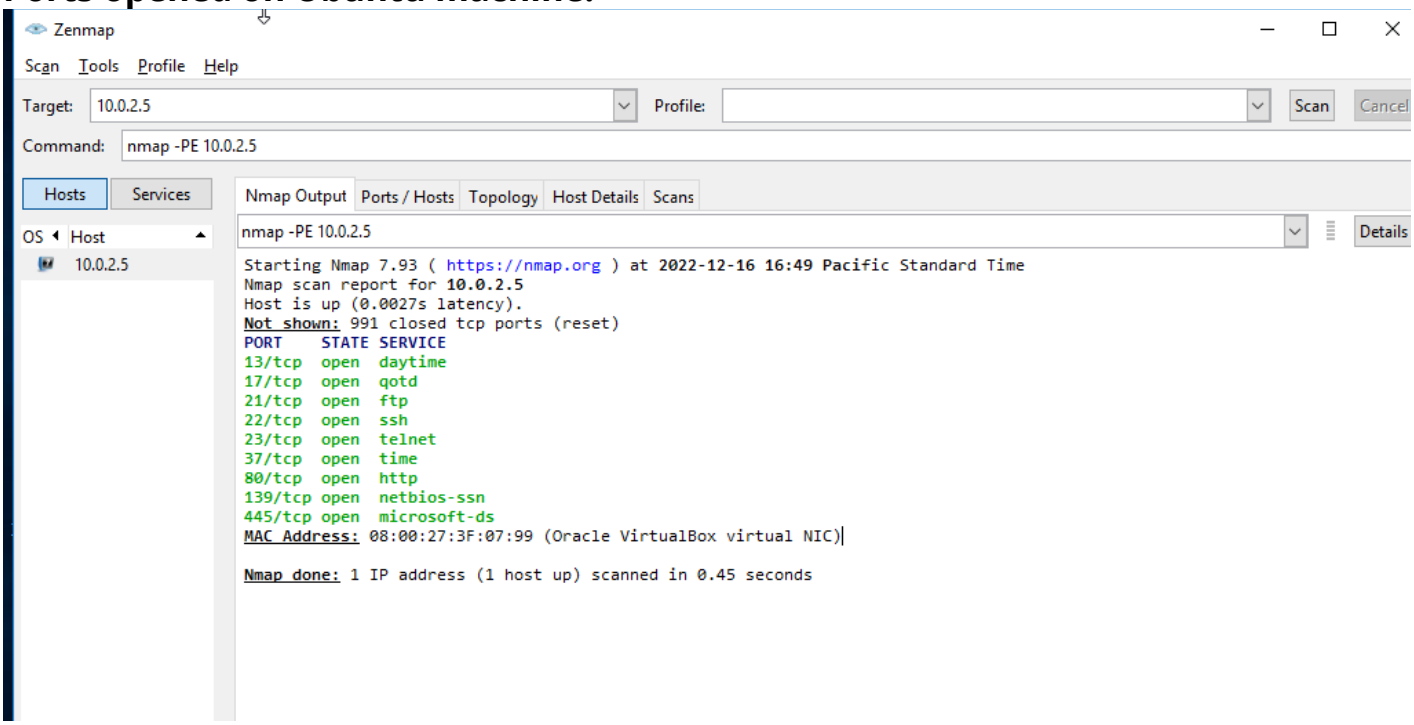
VNC Viewer is installed, and this adds additional risk to the machine.

Use NMAP to correctly identify all live hosts in a network.

Ports opened on Windows machine:



Ports opened on Ubuntu machine:



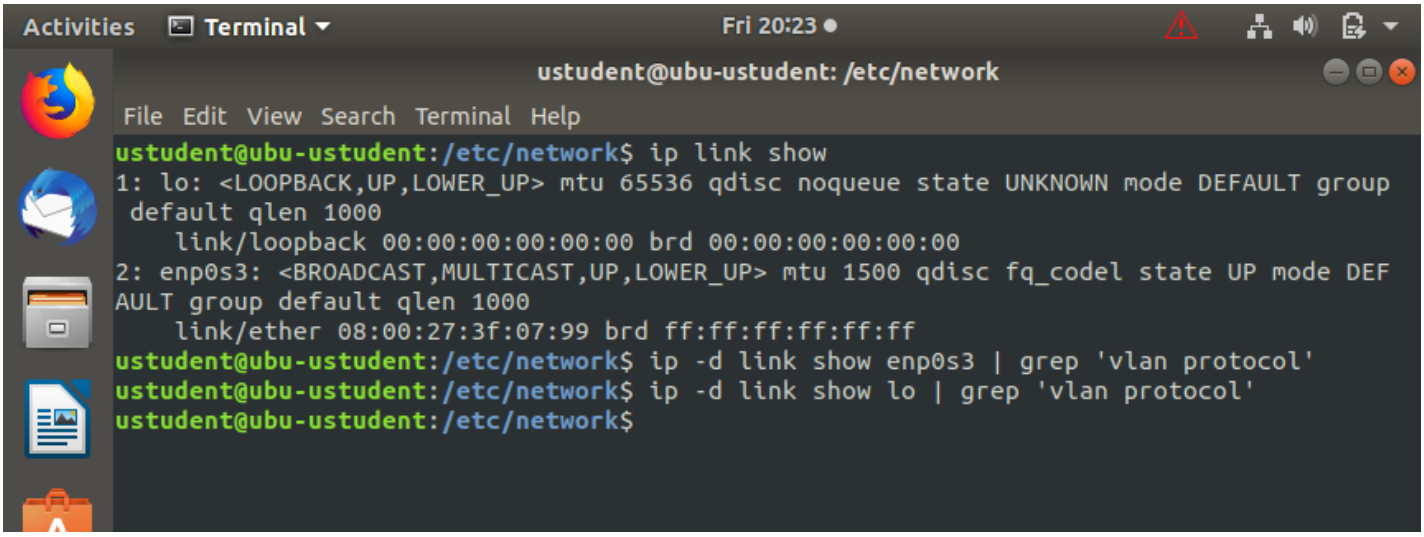
Provide recommendations to mitigate any threats related to open ports:

- Close unused ports.
- Apply the principle of least privilege and zero trust to reduce compromise impact.
- Ports that are used internally should never be public.
- Apply firewall to restrict access to the ports.
- Apply WAF.
- Replace vulnerable services like FTP with SSH and http with https.
- Update and patch the services.

Assess Access Management

Check for current settings on network segmentation, VLANs, Domain Isolation, or IP Security Policies.

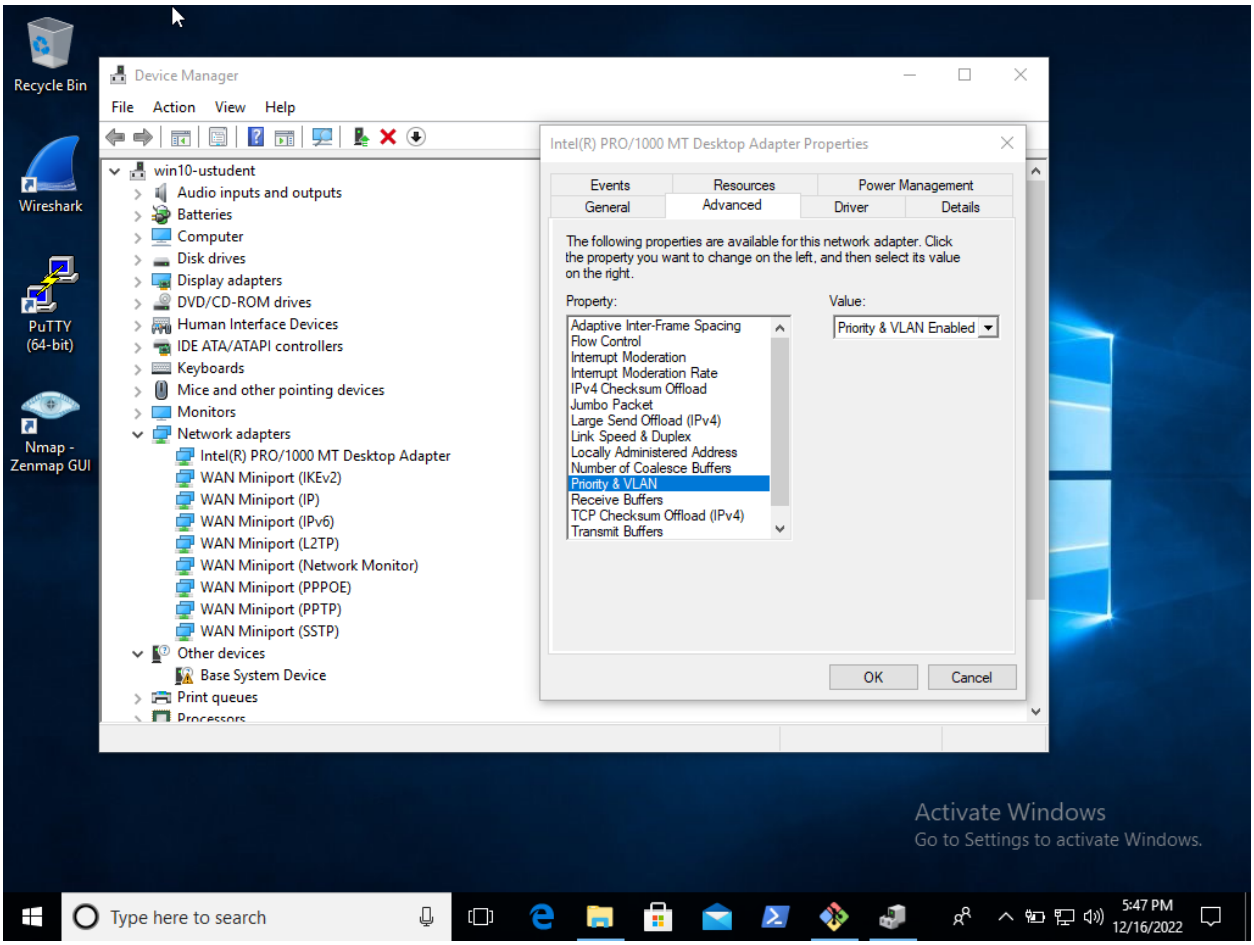
Ubuntu 18.04



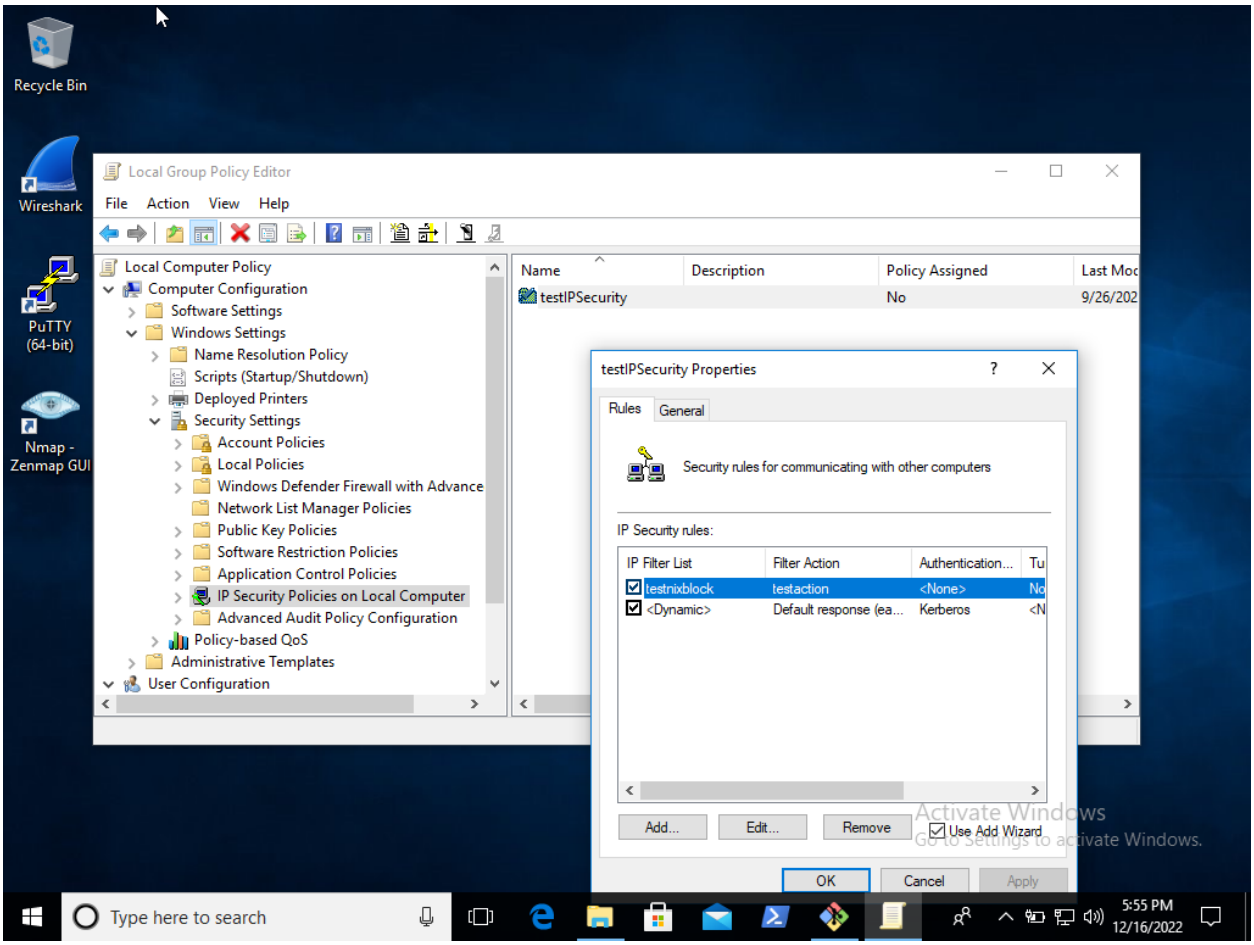
There is no VLANs configured in Ubuntu.

Recommendation: create a VLAN as it is useful to isolate departments and not allowing unauthorized people to access other LANs. Using VLANs will provide segmentation to the network to avoid collision. It also helps reduce the impact if one segment of the network got compromised.

Windows 10 ENT

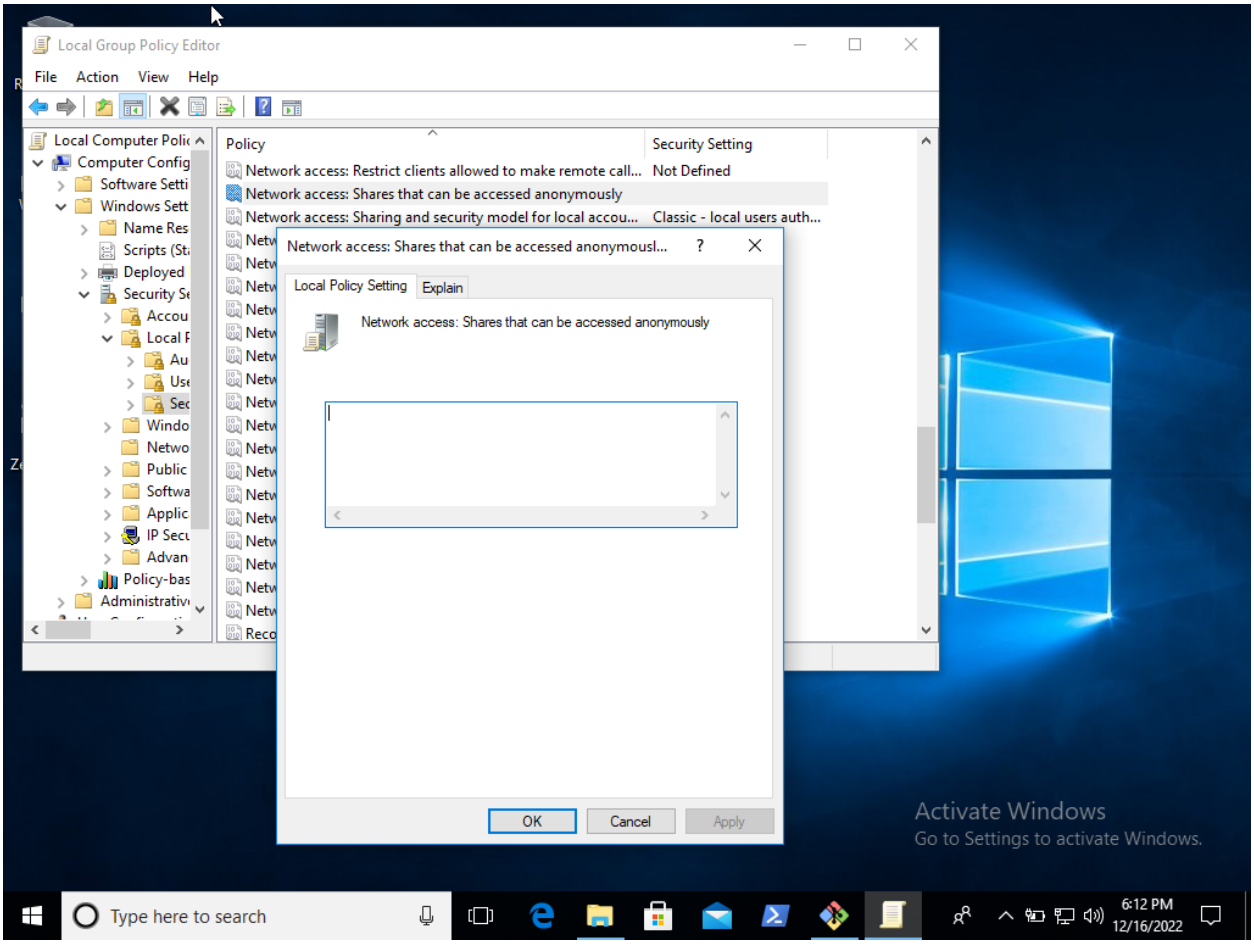


VLAN is Enabled in the interface.

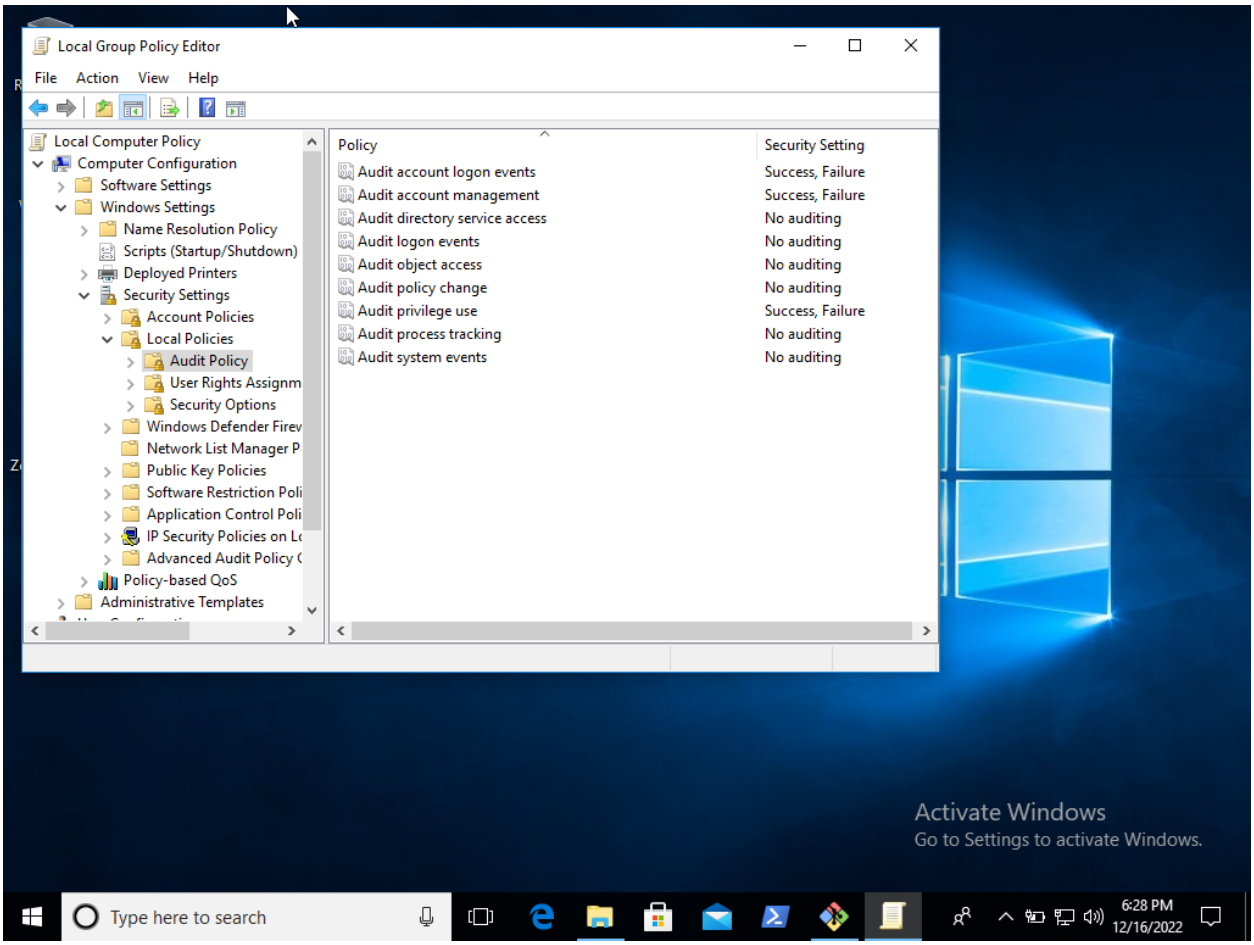


There is no Domain Isolation or IP Security Policies on Windows.

Recommendation: Domain Isolation can be achieved by using the IP Security. IP Security is important to block IP addresses of threat actors and thus mitigate the risk or getting compromised.



Shares that can be accessed anonymously are Not-defined.
Recommendation: It is better to Disable the anonymous share access to maintain a good security posture. We want only the authorized users to access the network.

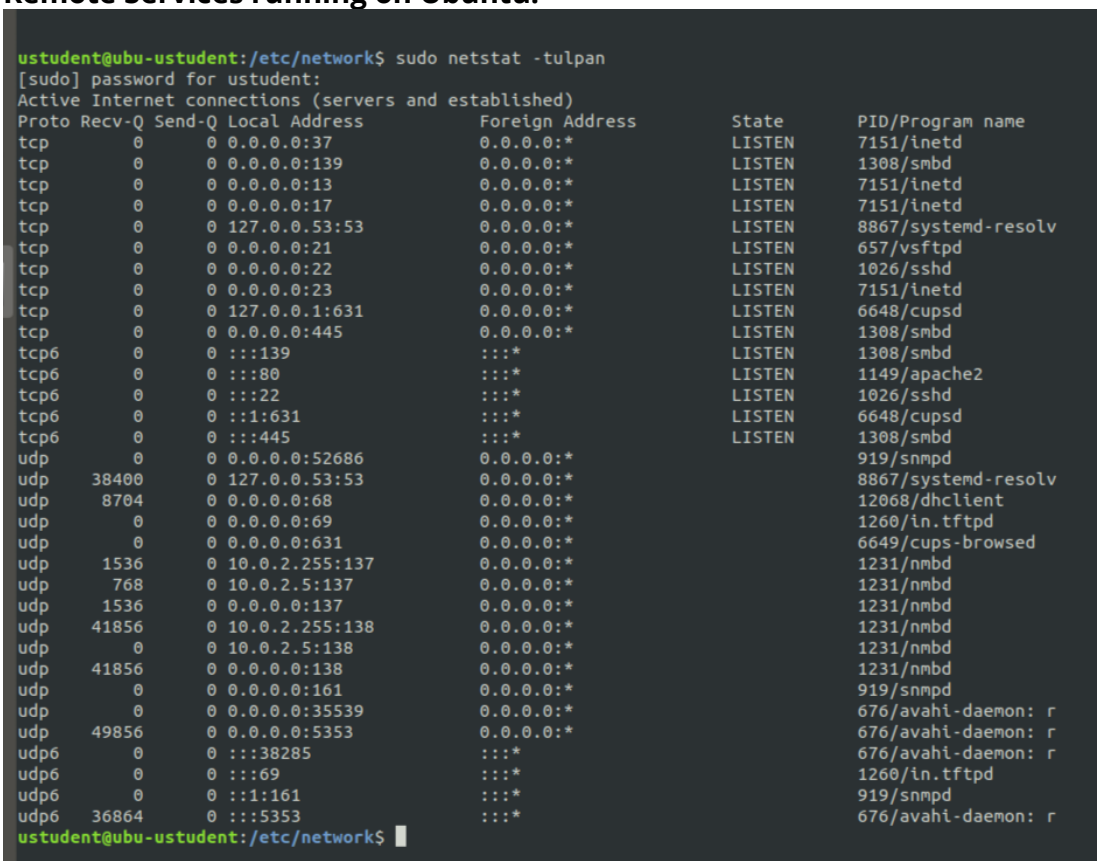


There are some policies enforced like the auditing policies. Some of them are:

- **Audit account logon events**
- **Audit account management**
- **Audit privilege use**

Investigate and find Remote Access Services, Protocols, and if the IPv6 protocol is running.

Remote Services running on Ubuntu:



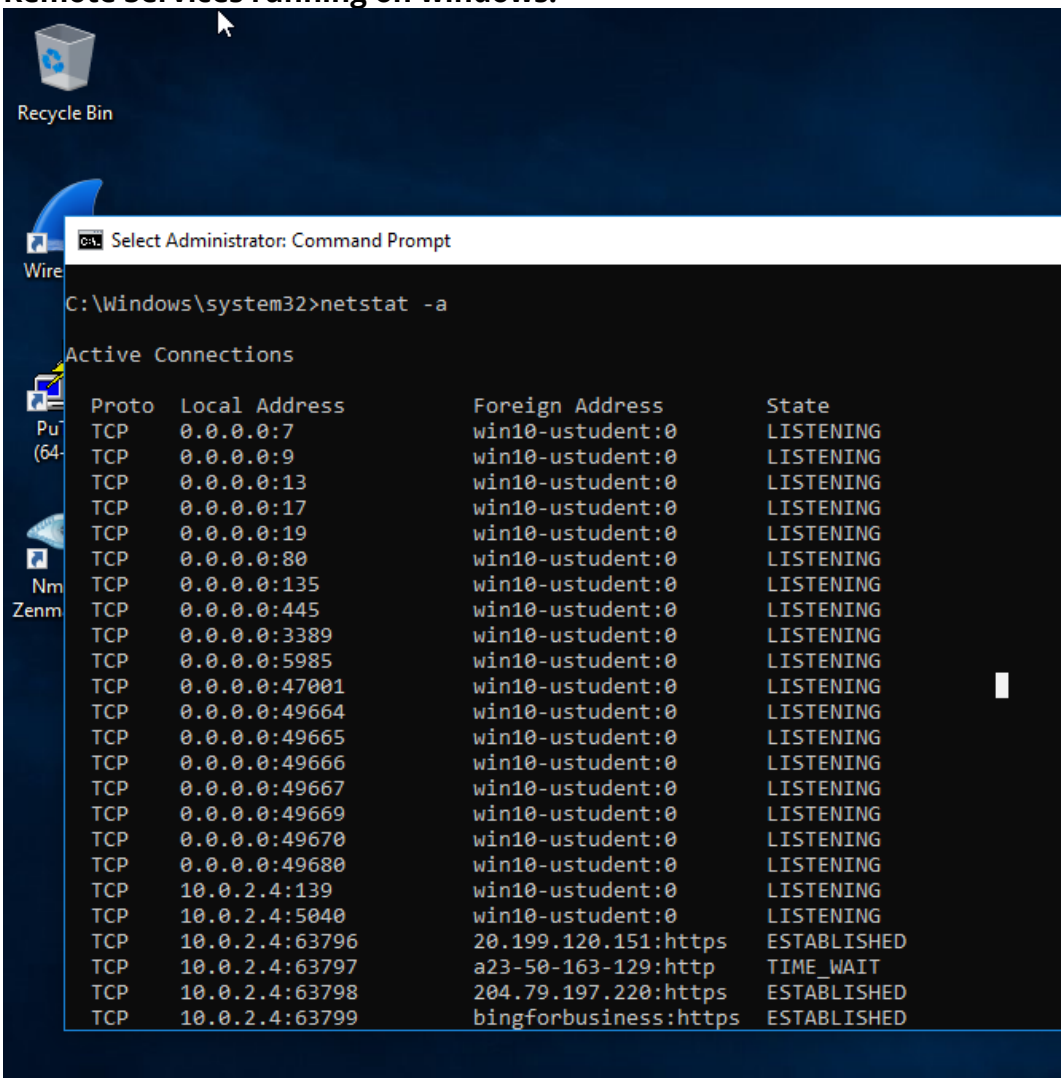
```
ustudent@ubu-ustudent:/etc/network$ sudo netstat -tulpan
[sudo] password for ustudent:
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:37              0.0.0.0:*               LISTEN      7151/inetd
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN      1308/smbd
tcp        0      0 0.0.0.0:13              0.0.0.0:*               LISTEN      7151/inetd
tcp        0      0 0.0.0.0:17              0.0.0.0:*               LISTEN      7151/inetd
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      8867/systemd-resolv
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN      657/vsftpd
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1026/sshd
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN      7151/inetd
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      6648/cupsd
tcp        0      0 0.0.0.0:445             0.0.0.0:*               LISTEN      1308/smbd
tcp6       0      0 :::139                  :::*                    LISTEN      1308/smbd
tcp6       0      0 :::80                   :::*                    LISTEN      1149/apache2
tcp6       0      0 :::22                   :::*                    LISTEN      1026/sshd
tcp6       0      0 ::1:631                 :::*                    LISTEN      6648/cupsd
tcp6       0      0 :::445                  :::*                    LISTEN      1308/smbd
udp        0      0 0.0.0.0:52686           0.0.0.0:*                           919/snmpd
udp    38400      0 127.0.0.53:53           0.0.0.0:*                           8867/systemd-resolv
udp     8704      0 0.0.0.0:68              0.0.0.0:*                           12068/dhclient
udp        0      0 0.0.0.0:69              0.0.0.0:*                           1260/in.tftpd
udp        0      0 0.0.0.0:631             0.0.0.0:*                           6649/cups-browsed
udp     1536      0 10.0.2.255:137          0.0.0.0:*                           1231/nmbd
udp      768      0 10.0.2.5:137            0.0.0.0:*                           1231/nmbd
udp     1536      0 0.0.0.0:137             0.0.0.0:*                           1231/nmbd
udp    41856      0 10.0.2.255:138          0.0.0.0:*                           1231/nmbd
udp        0      0 10.0.2.5:138            0.0.0.0:*                           1231/nmbd
udp    41856      0 0.0.0.0:138             0.0.0.0:*                           1231/nmbd
udp        0      0 0.0.0.0:161             0.0.0.0:*                           919/snmpd
udp        0      0 0.0.0.0:35539           0.0.0.0:*                           676/avahi-daemon: r
udp    49856      0 0.0.0.0:5353            0.0.0.0:*                           676/avahi-daemon: r
udp6       0      0 :::38285                :::*                                676/avahi-daemon: r
udp6       0      0 :::69                   :::*                                1260/in.tftpd
udp6       0      0 ::1:161                 :::*                                919/snmpd
udp6   36864      0 :::5353                 :::*                                676/avahi-daemon: r
ustudent@ubu-ustudent:/etc/network$
```

FTP port 21, SSH port 22, Telnet port 23

Recommendation:

- Stop all unused ports
- Replace FTP with SFTP for more confidentiality
- Avoid using Telnet as its connection is not encrypted

Remote Services running on windows:

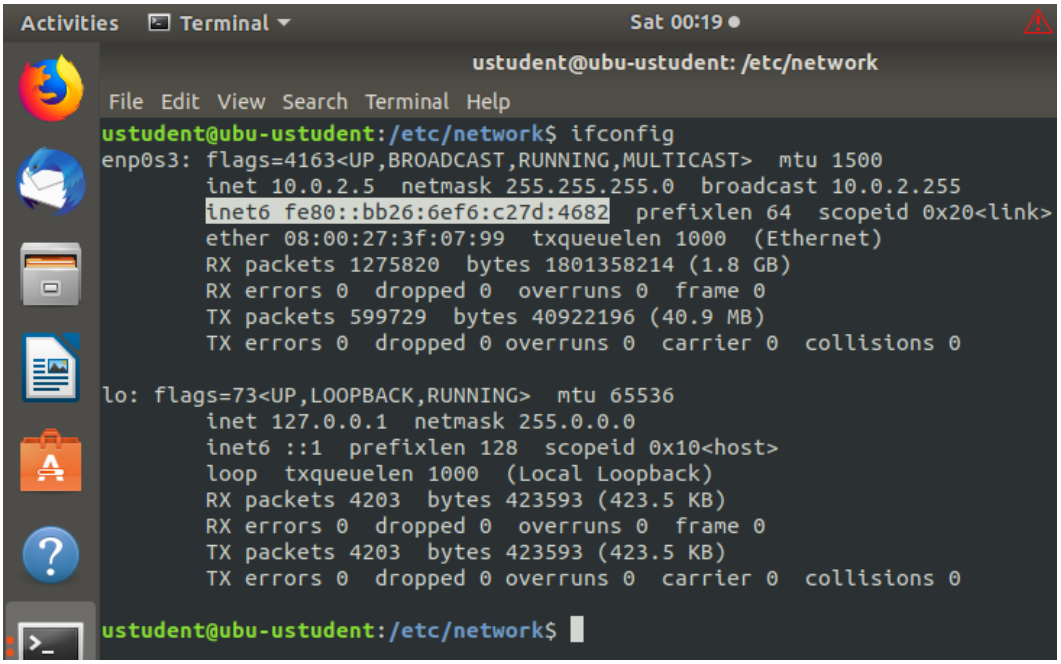


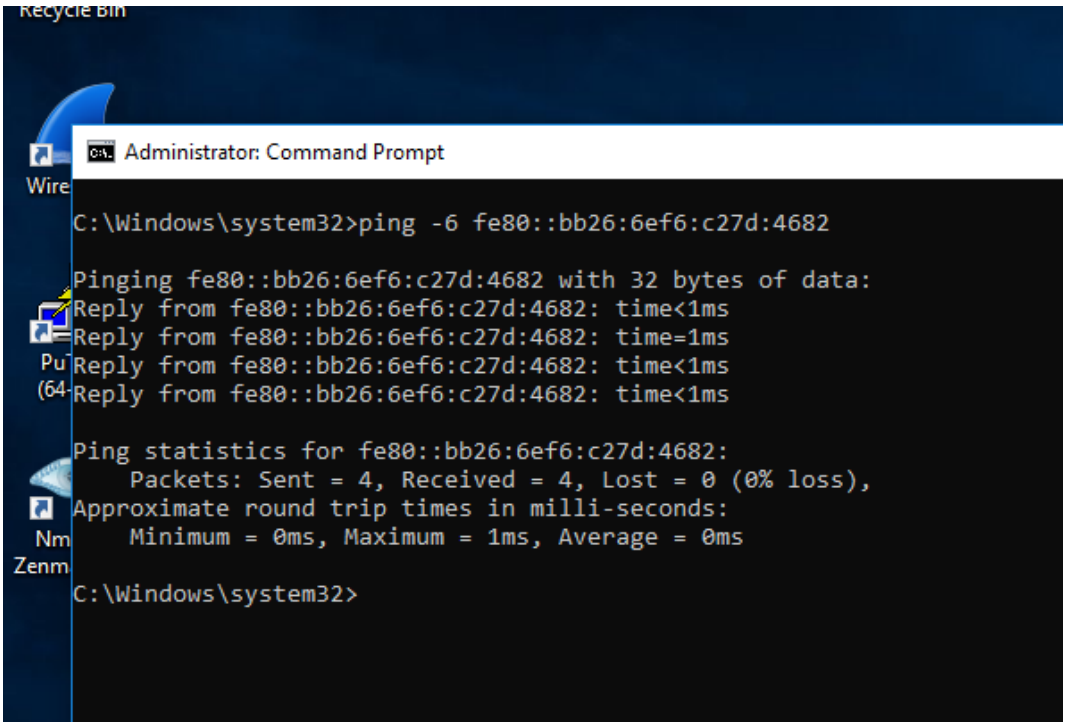
RDP port 3389, Windows Remote Management Service port 47001

Recommendation:

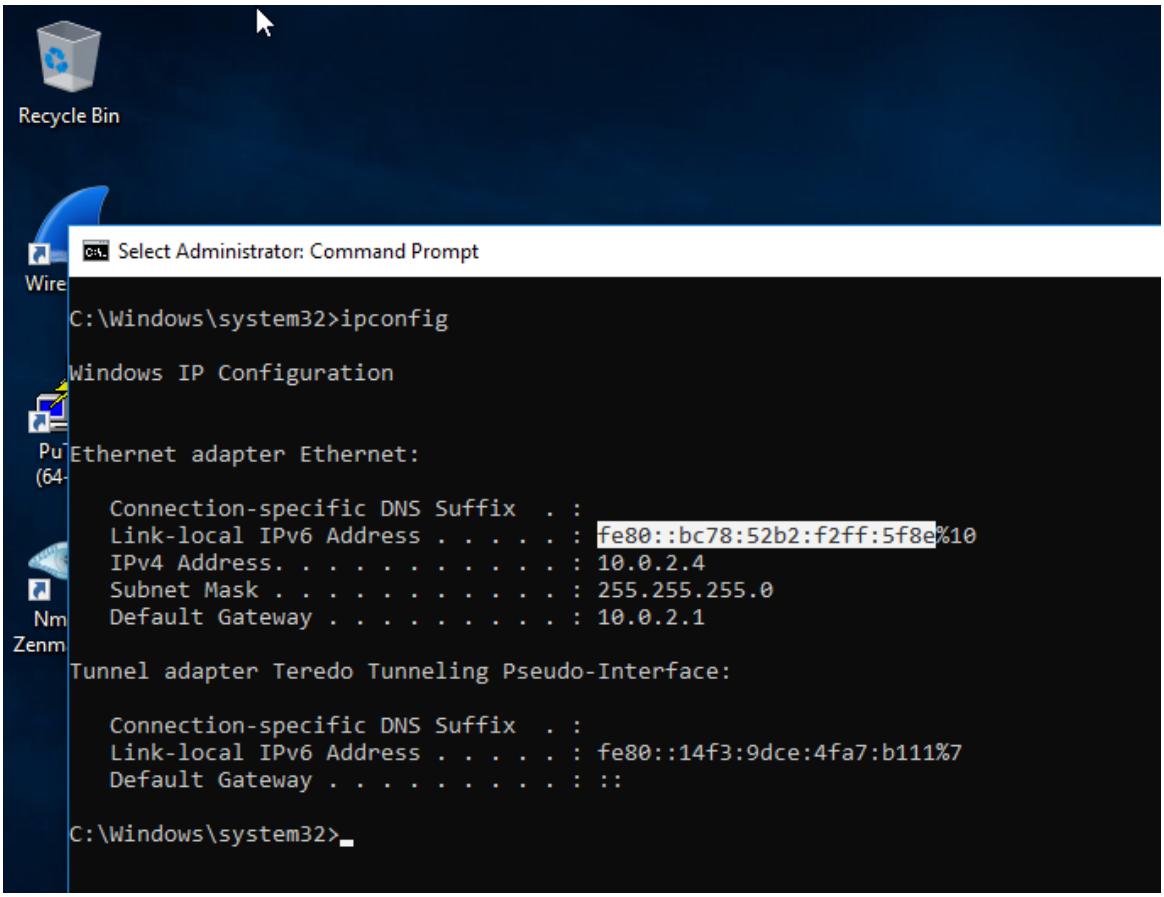
- Disable unused ports
- Check every listening port and audit its process to make sure it is safe and legit

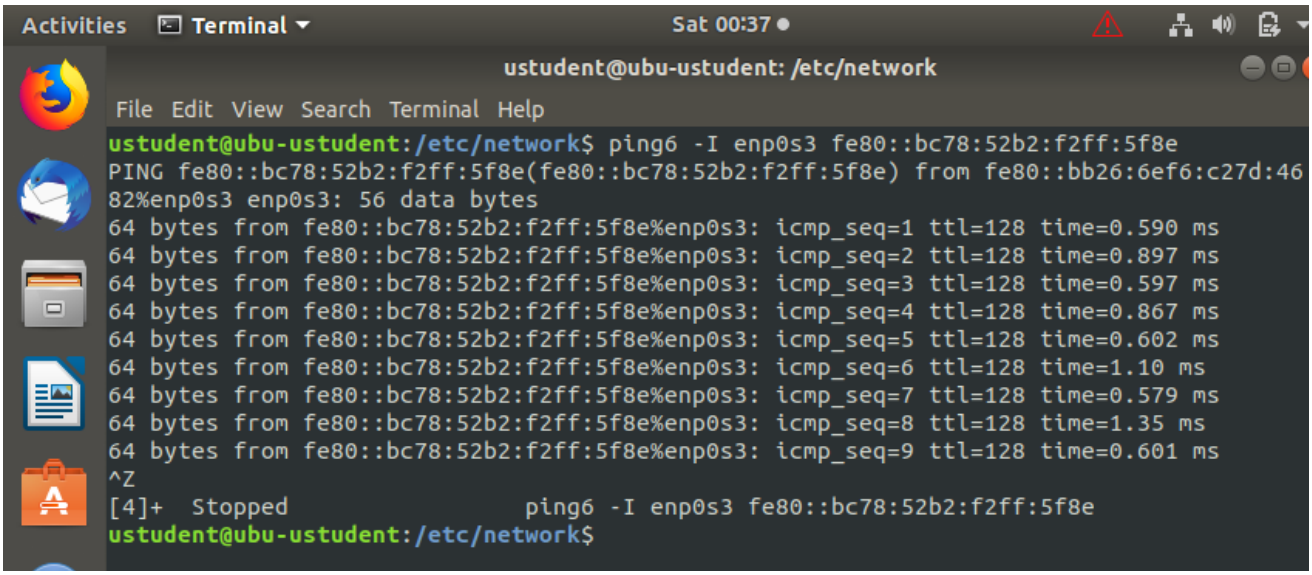
IPv6 on Ubuntu:





IPv6 on Windows:





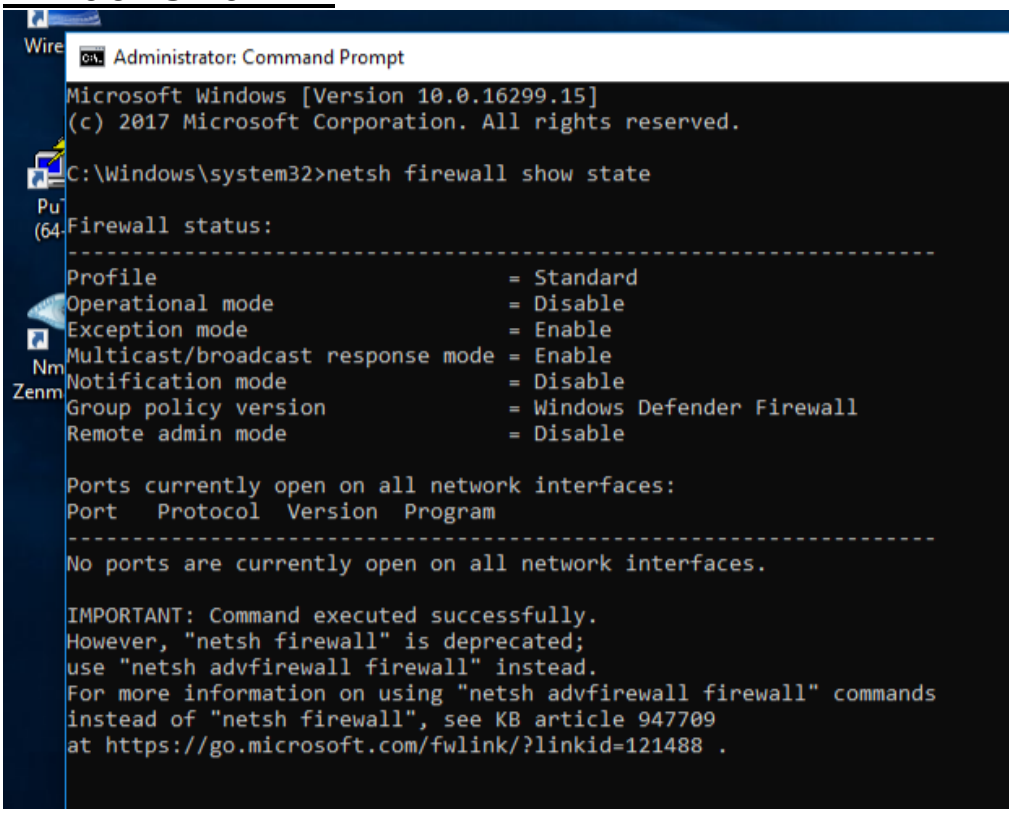
recommendation on whether IPv6 is needed?

- Runs by default, potentially being missed by monitoring devices and logging settings. This provides a potential access path for attackers.
- Network security tools running on IPv4 do not necessarily protect IPv6.
- There are still support issues with ISPs and Vendors. Not all application services and internet providers are fully supporting IPv6.

There its better to disable it and only use it when needed.

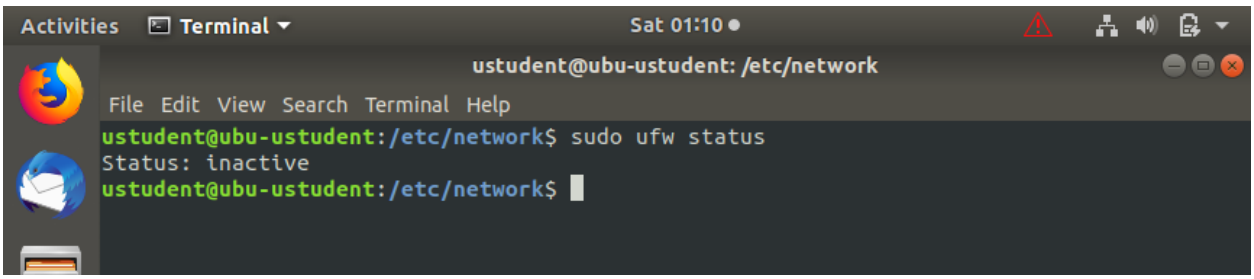
Find and verify if firewalls are set and recommend what ports should be open for business and network operations.

Windows 10 ENT

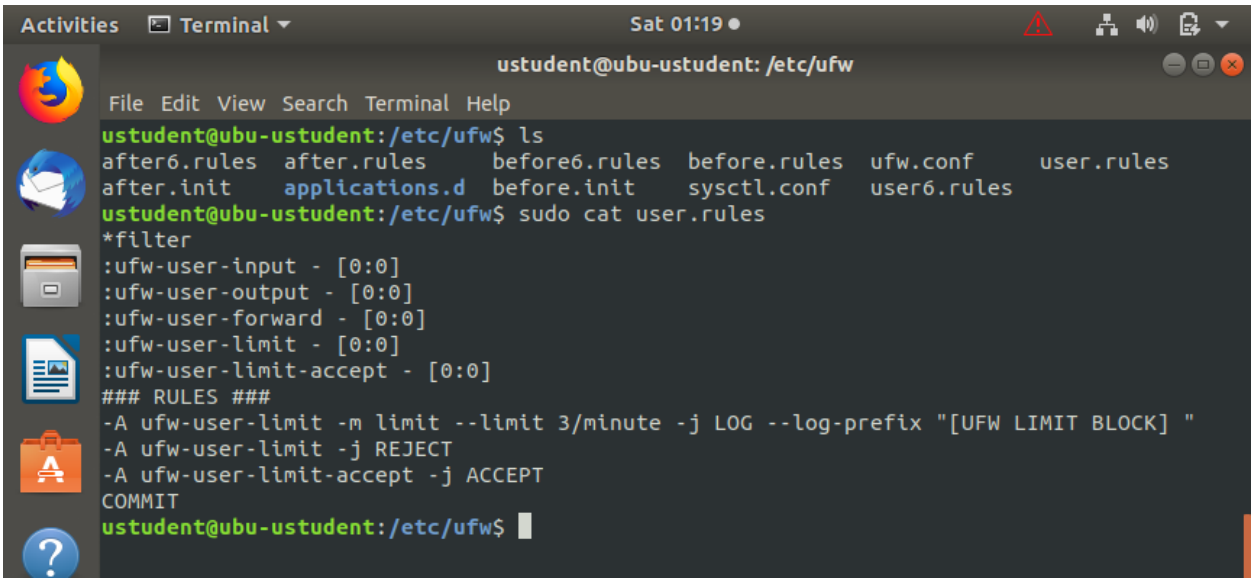


Firewall is Disabled on windows.

Ubuntu 18.04



UFW is inactive in Ubuntu.



UFW rules are not correctly configured either.

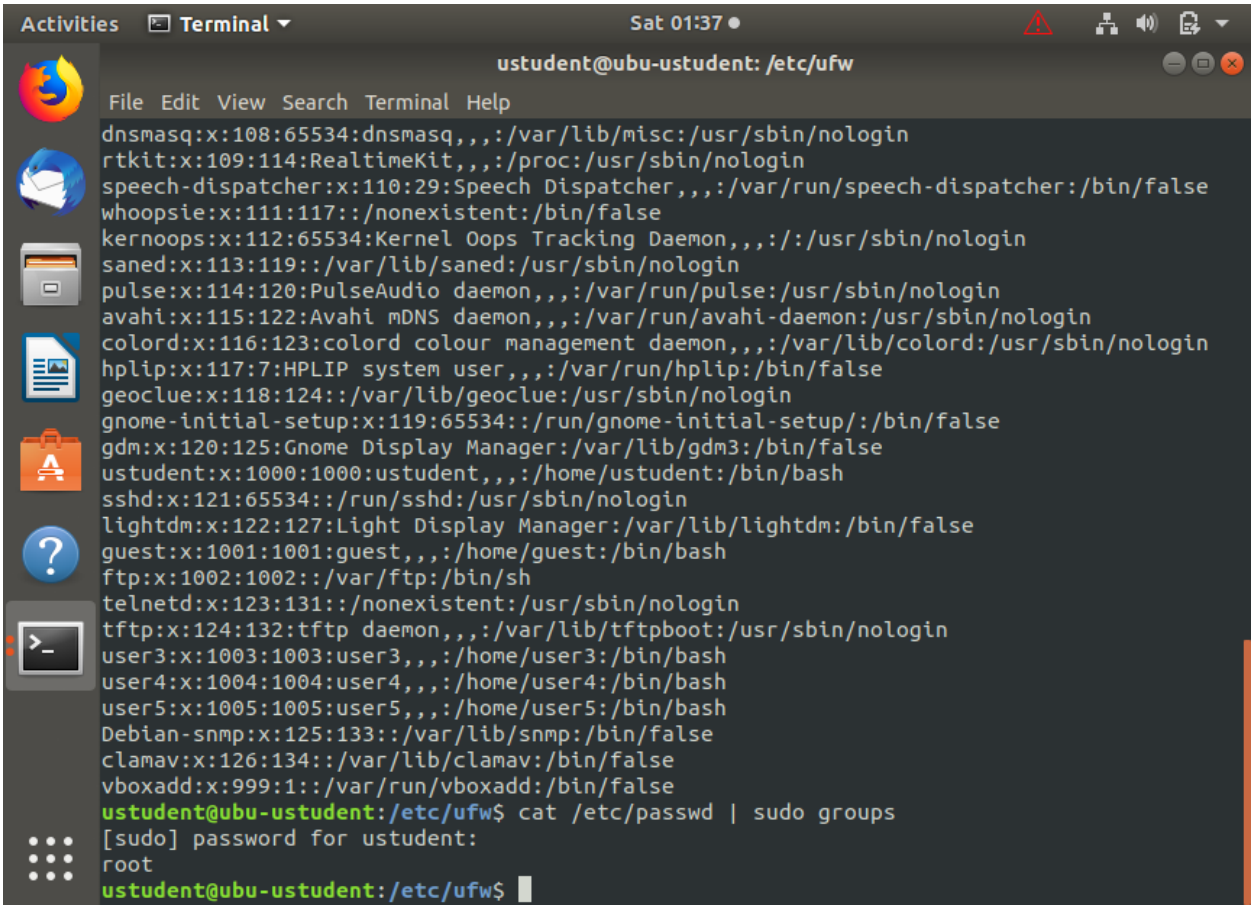
Recommend which ports should be open and why?

Port 22 SSH, because has an encrypted communication unlike Telnet and FTP.
Port 3389 RDP, because it uses encrypted connection.

Identify and mitigate user privilege Issues.

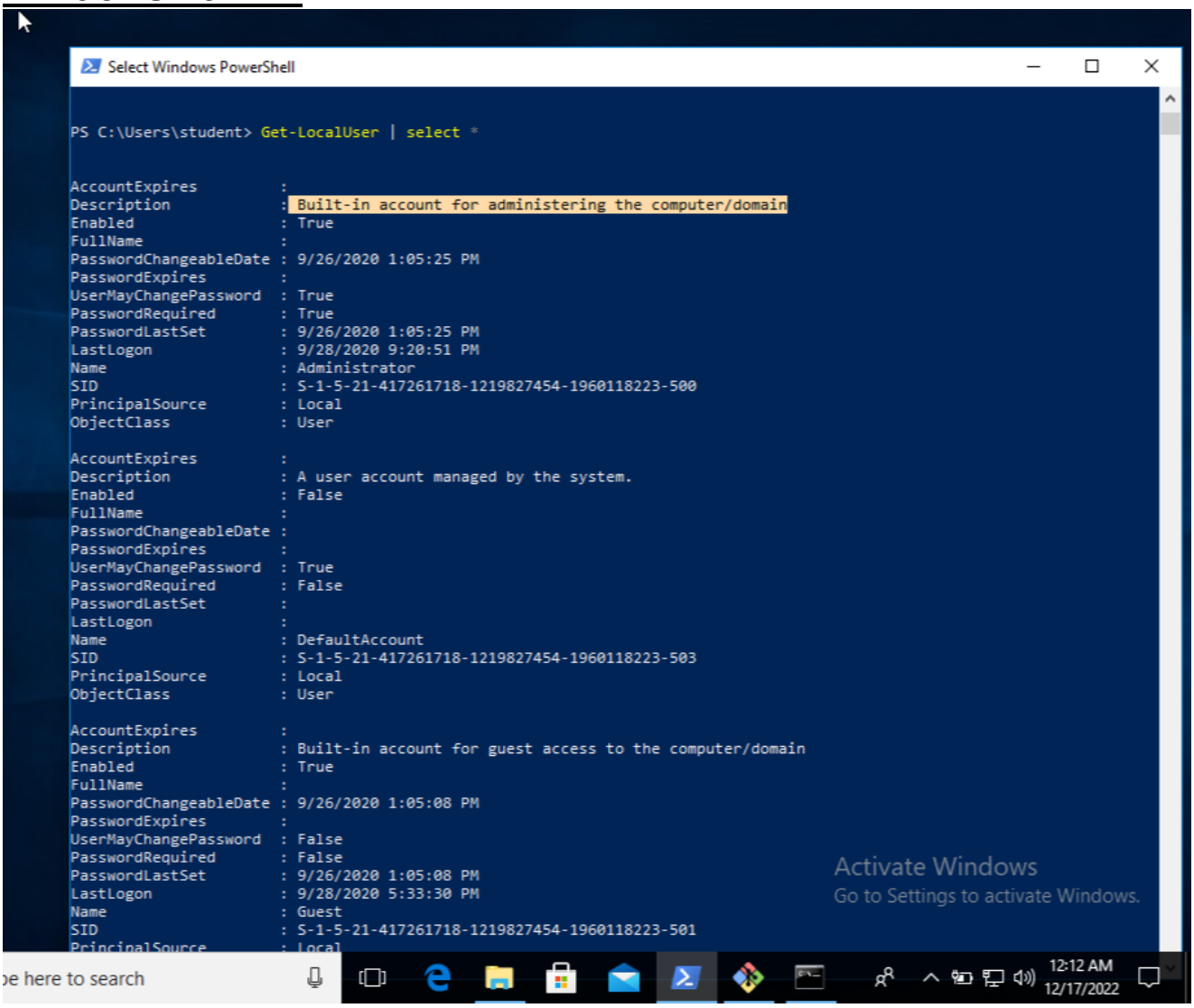
Which users have high privileges:

Ubuntu 18.04



user: root, has the highest privilege.

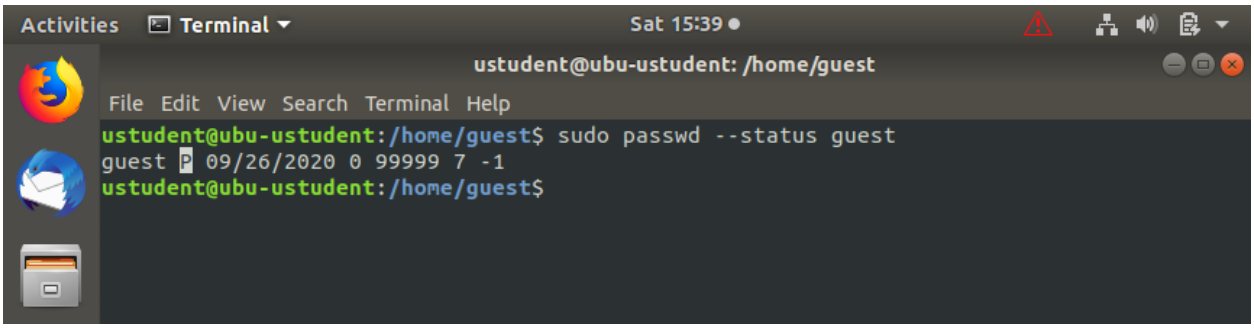
Windows 10 ENT



In Windows the highest privileged user is the Administrator, its the only user with description of : Built-in account for administering the computer/domain.

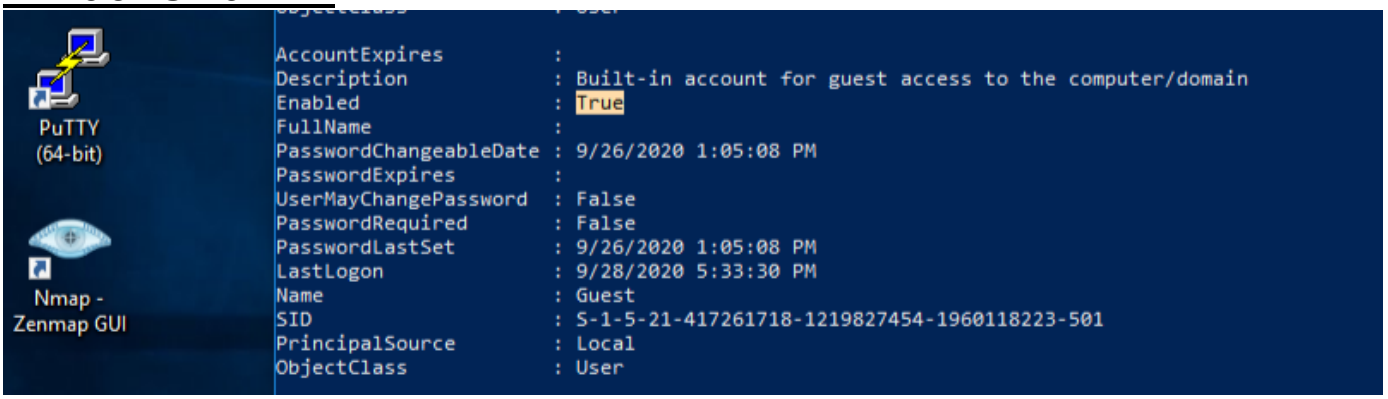
Are the guest accounts enabled?

Ubuntu 18.04



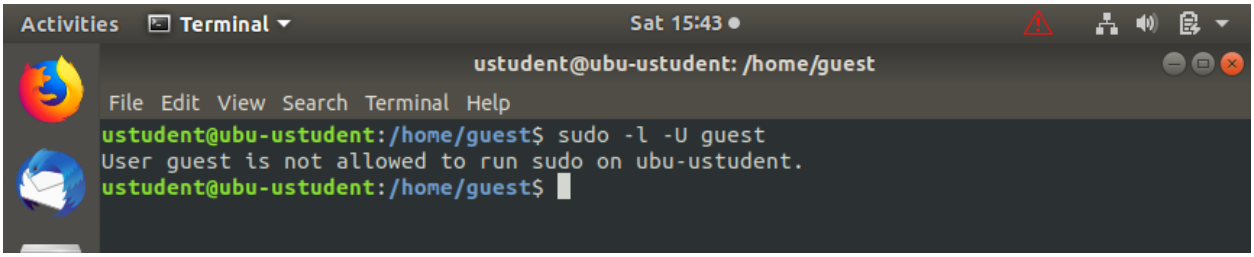
As we can see the guest account in Ubuntu, its status is P not L, which means it is not locked and that it is enabled and working.

Windows 10 ENT



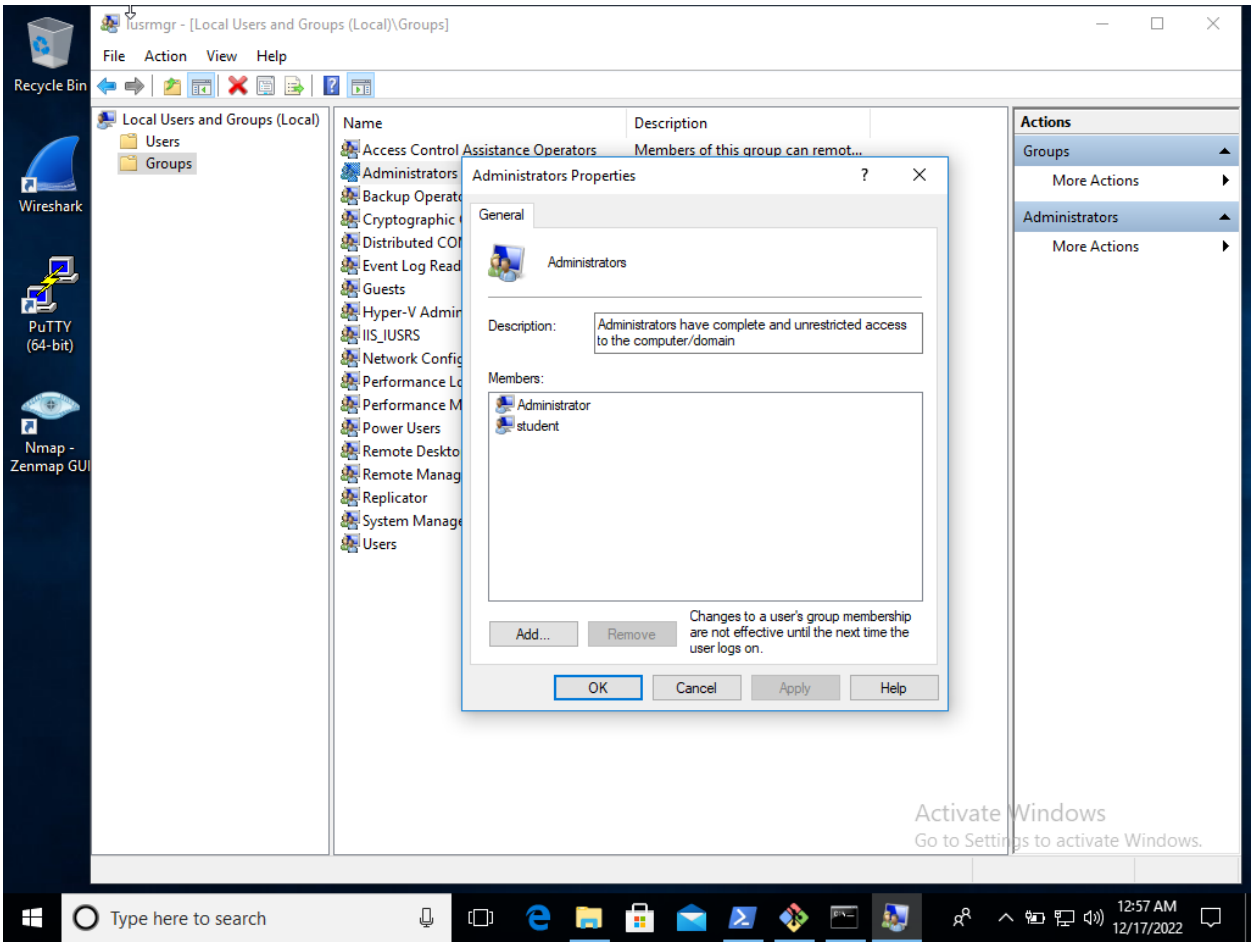
The guest account is enabled in Windows.

Is the guest account allowed to sudo in Linux?



No, the guest account is not allowed to sudo in Ubuntu.

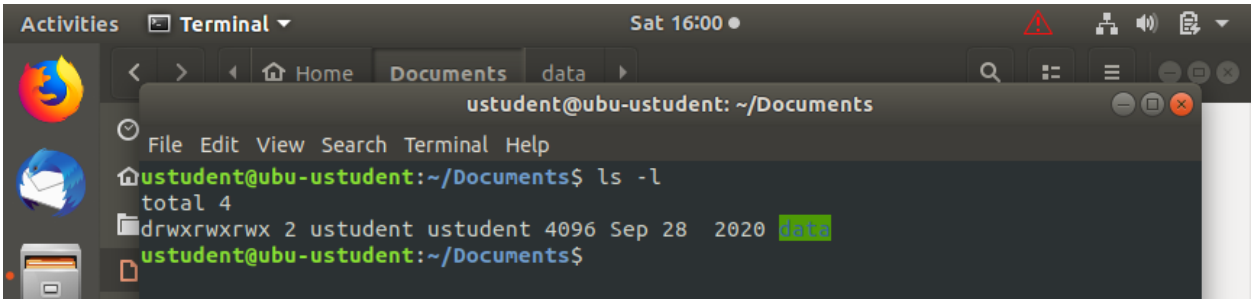
Is the guest account allowed to run as administrator in Windows?



No, because it is not a member of the Administrators group.

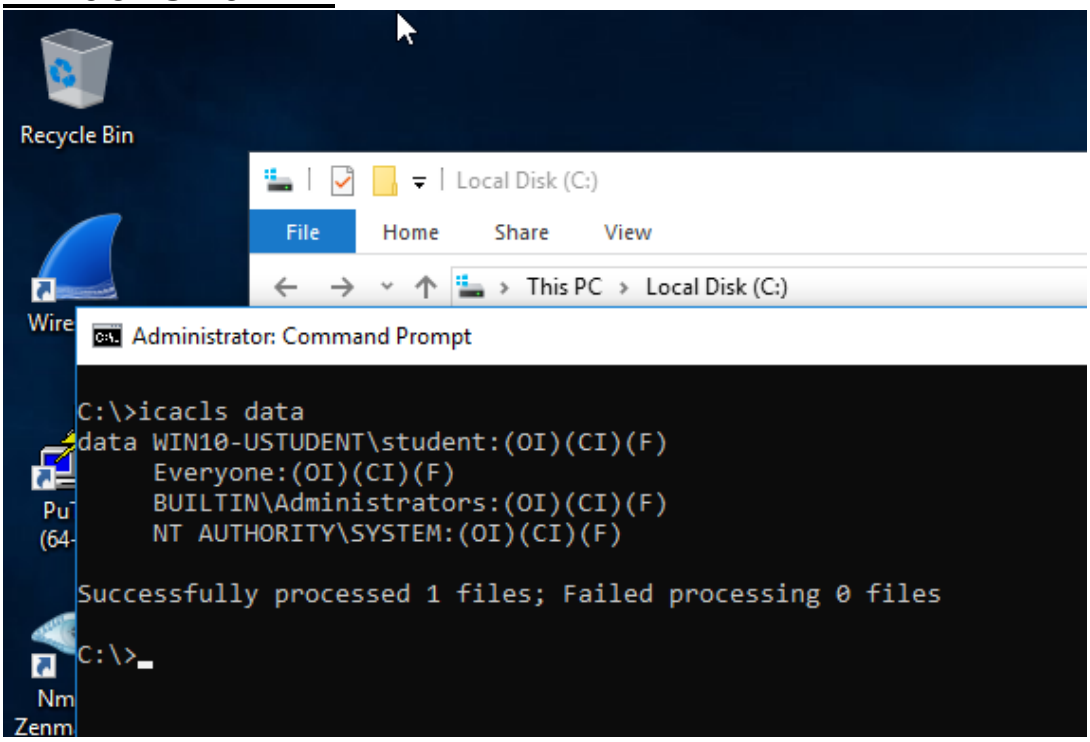
Are there excessive permissions on the data folder in each machine?

Ubuntu 18.04



Yes, there are excessive permissions on the data folder in Ubuntu.

Windows 10 ENT



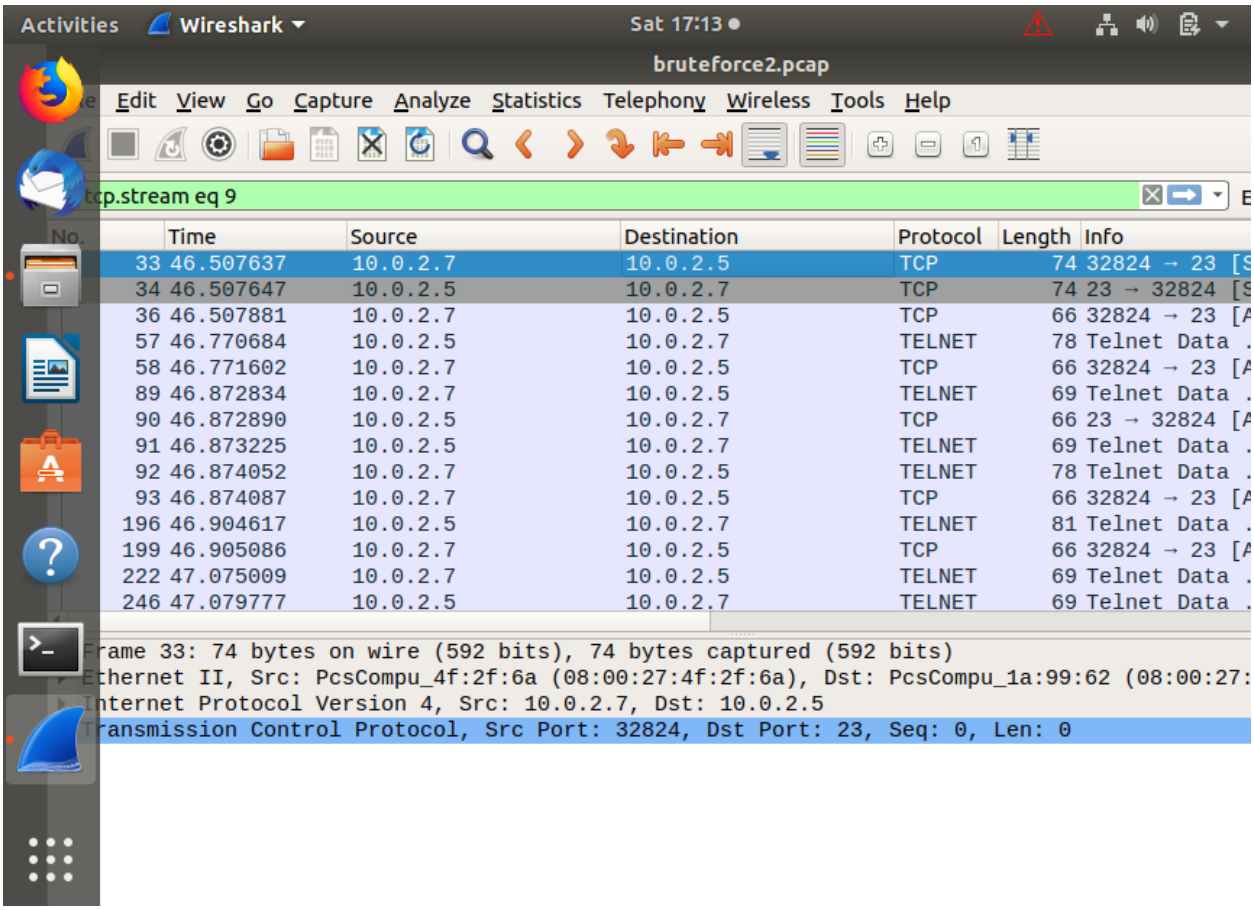
Yes, there are excessive permission on the data folder in Windows.

Recommendation: Allow only the authorized user to have permission to the folder, since this folder can have sensitive data to the company, normal users and guests are not allowed to read it, let alone modify it.

Log Monitoring Setup for Detection at Targeted Assets

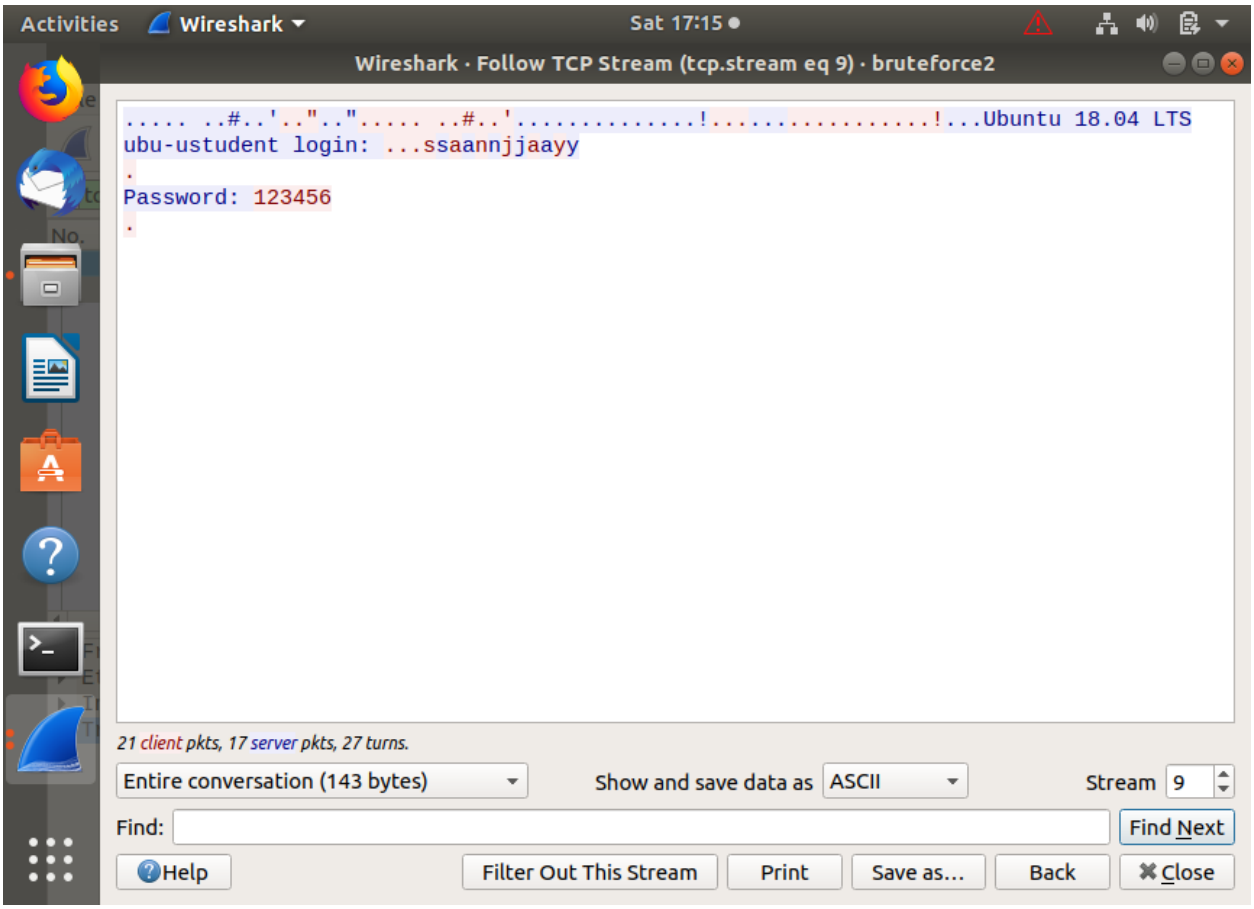
Use Wireshark or tcpdump to perform traffic inspection and investigation.

The source IP of the attack: 10.0.2.7



What protocol was brute-forced? Telnet

What password was used? 123456



Which user was compromised? sanjay

Provide recommendations on how to prevent this type of attack from happening again.

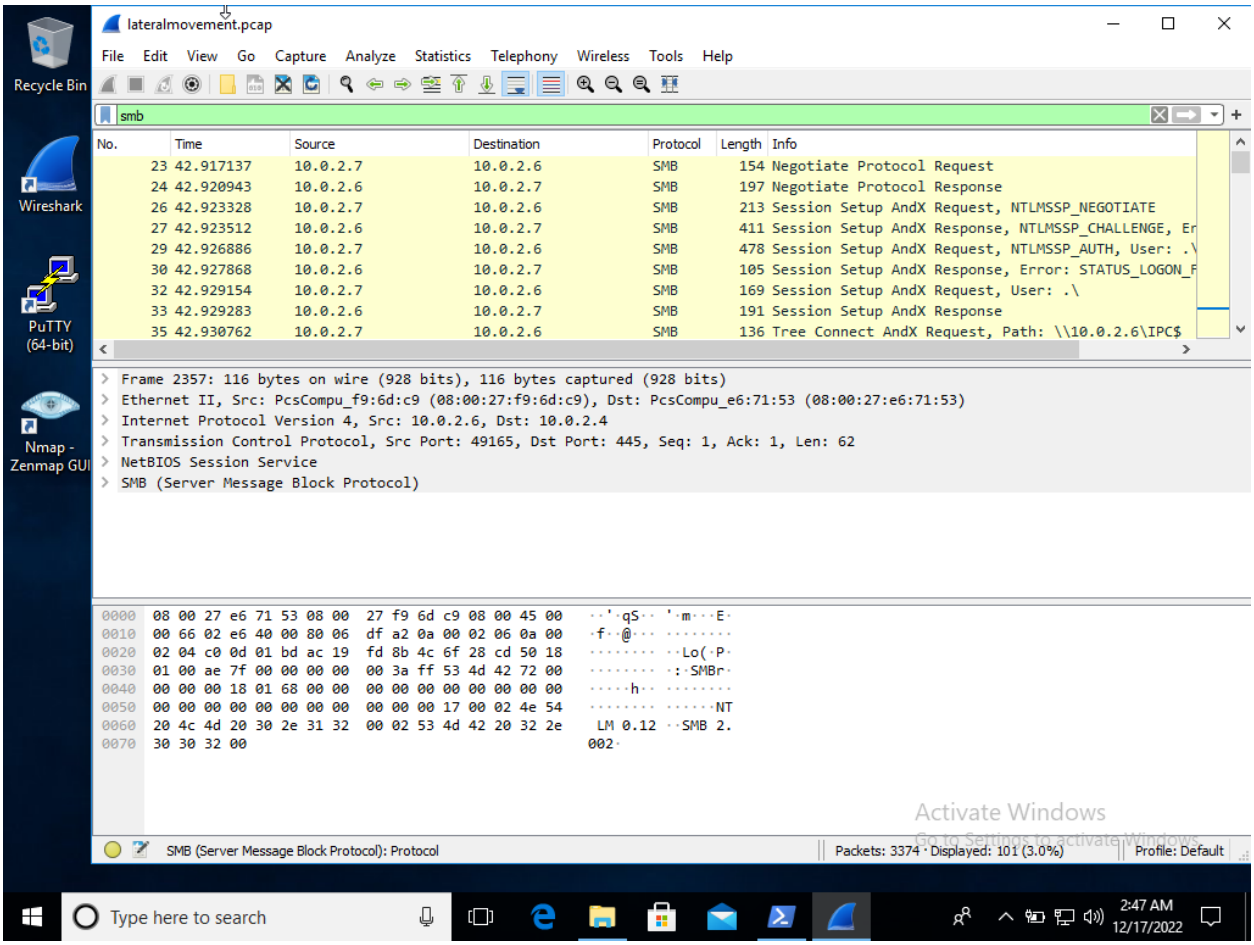
- Use complex password to make it harder to brute force.
- Add the principle of least privilege to minimize the impact of the compromise.
- Avoid using Telnet due to its security risks, as packets are transferred in plain text which makes it easier for attackers to sniff credentials.

Use Wireshark or tcpdump analyze a successful attack (Lateral Movement Mitre ATT&CK TA0008)

What was the source IP of the "initial" attack?

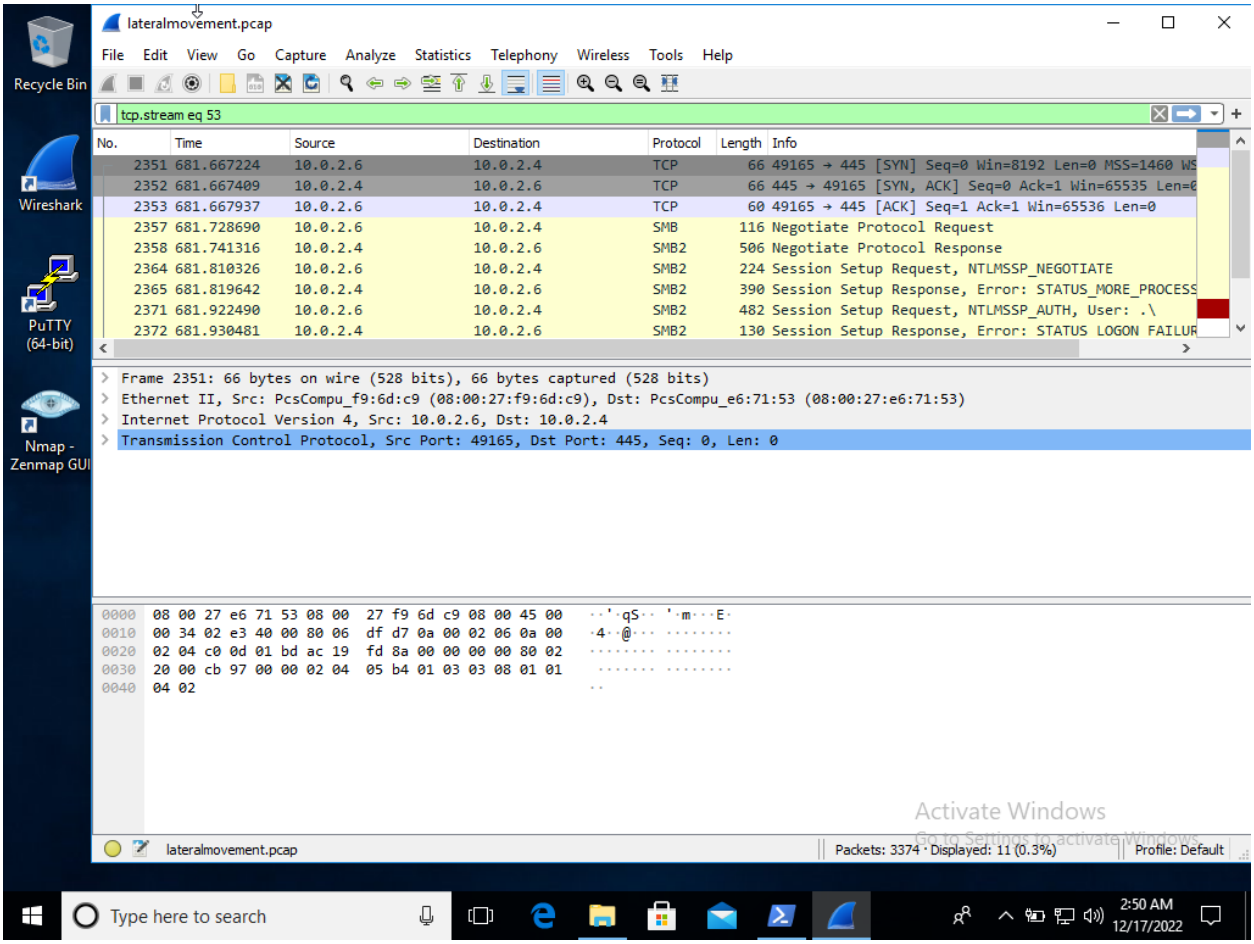
10.0.2.7

Did the attacker try to access your machine from a compromised machine - (MITRE ATT&CK Technique T1021)?



Yes, he first compromised the first machine with the IP:10.0.2.6 through the SMB protocol.

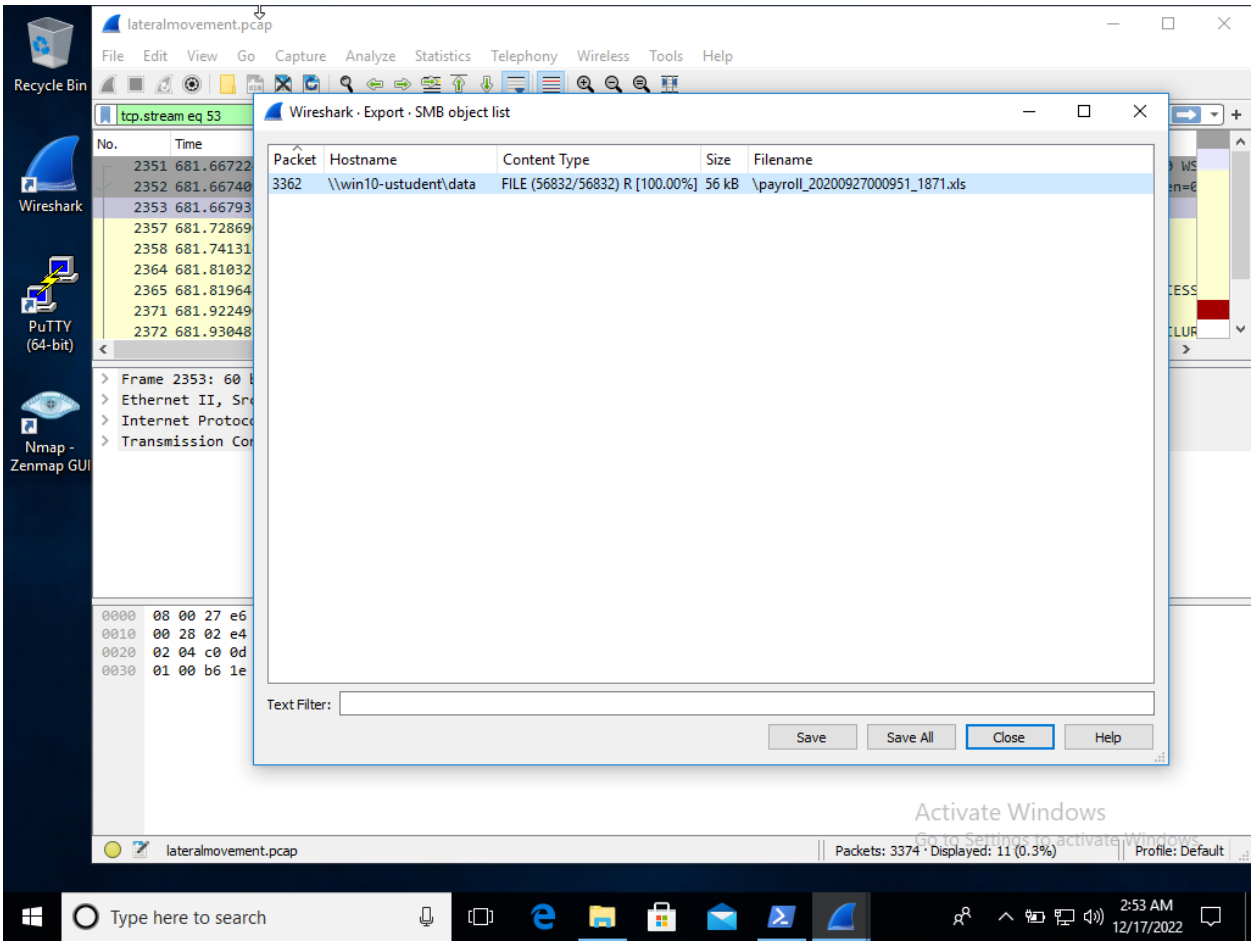
Then he used the compromised machine and pivoted to my machine:



<u>What service and port were targeted?</u>

SMB2 port 445

Was the attacker able to access a sensitive file at the machine you are auditing (Mitre ATT&ACK Technique - T1570)?



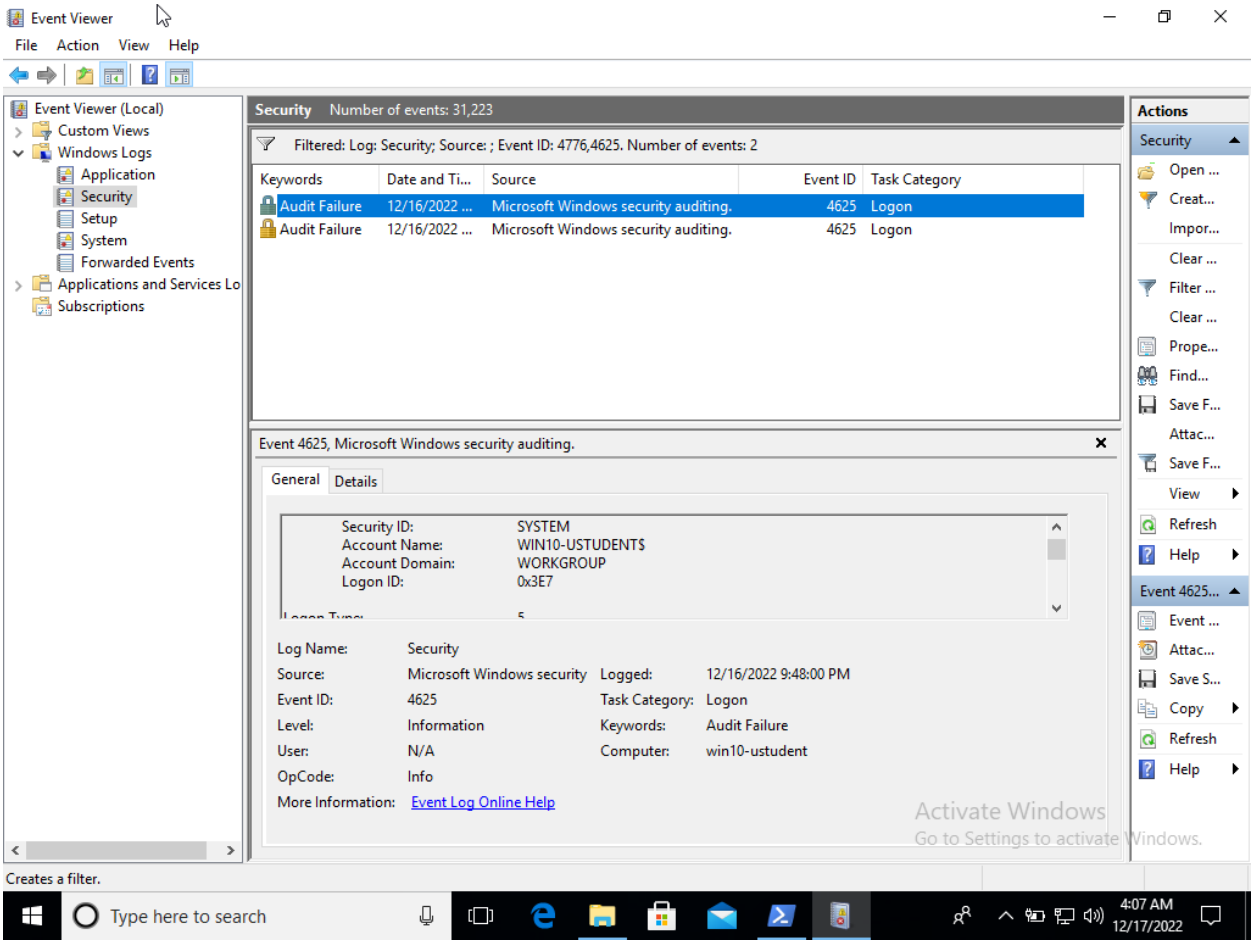
Yes, the attacker was able to access the data file which consists of data about the payroll.

Recommendations for mitigation based on the pcap analysis:

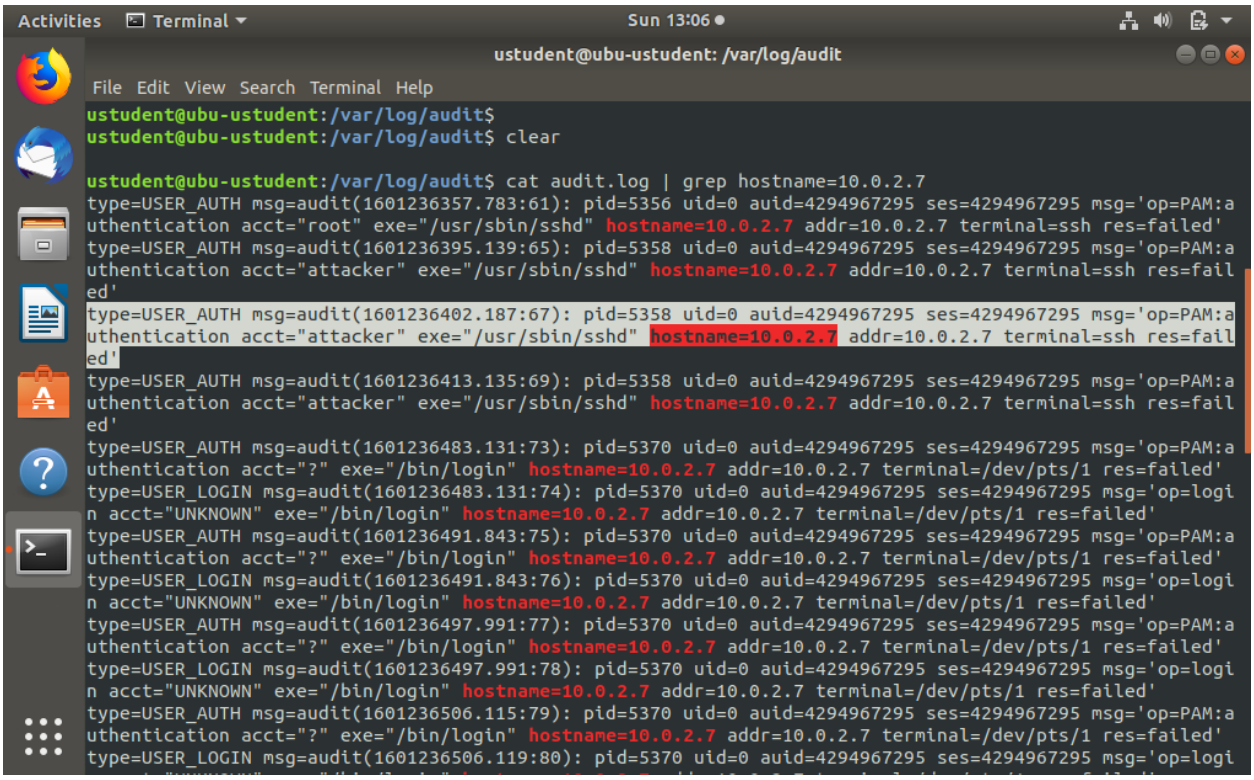
- Restrict the access privilege on the data file.
- Consider using the host firewall to restrict file sharing communications such as SMB.
- Consider disabling Windows administrative shares.
- Deny remote use of local admin credentials to log into systems. Do not allow domain user accounts to be in the local Administrators group multiple systems.

Use logs at audited machines to find login failures and suspicious access attempts.

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?



Name of the attacker account: attacker

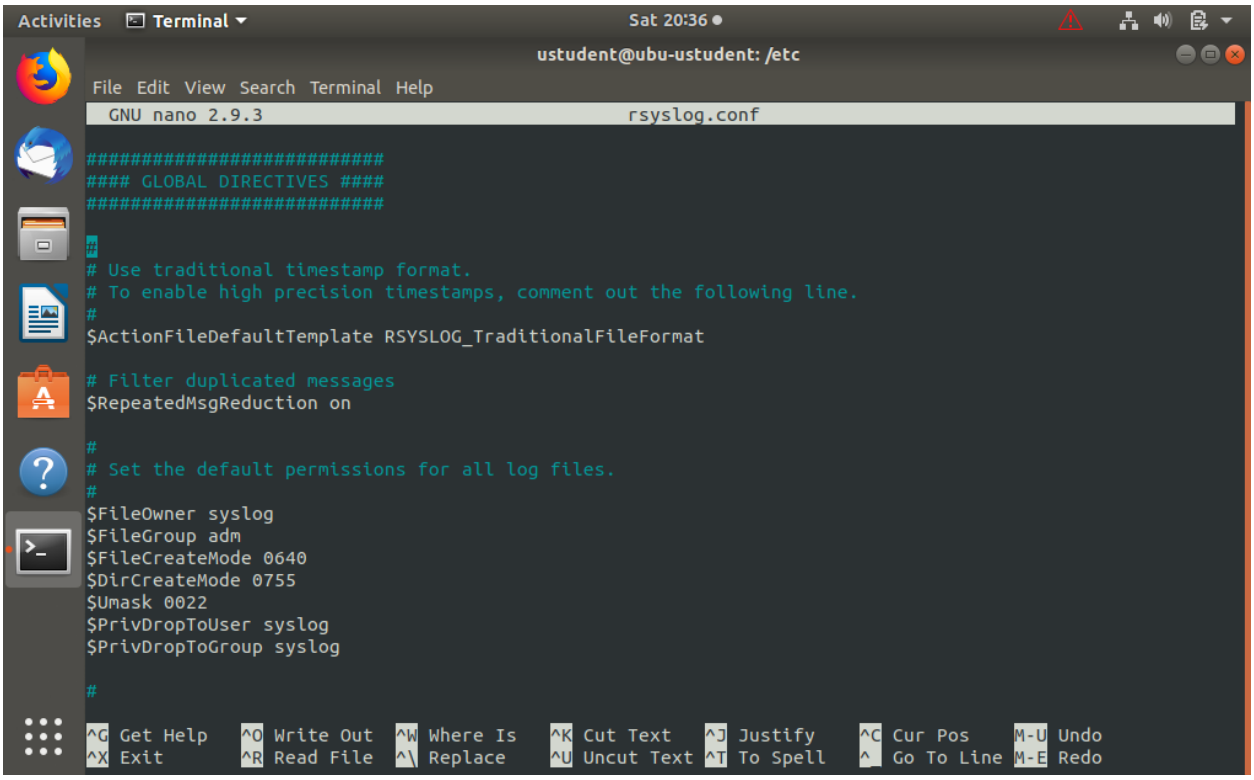
Provide mitigation recommendations:

- Use firewall to block suspicious IP addresses.
- If the service is not used its port must be disabled.
- Apply policy to lockout a user after several failed attempts.
- Services that will not be used in public must be set private to decrease the surface attack.
- Apply the principle of least privilege to reduce the impact of compromise.
- Apply policy to allow only the users that are authorized to access the service.

Verify that the systems are logging correctly.

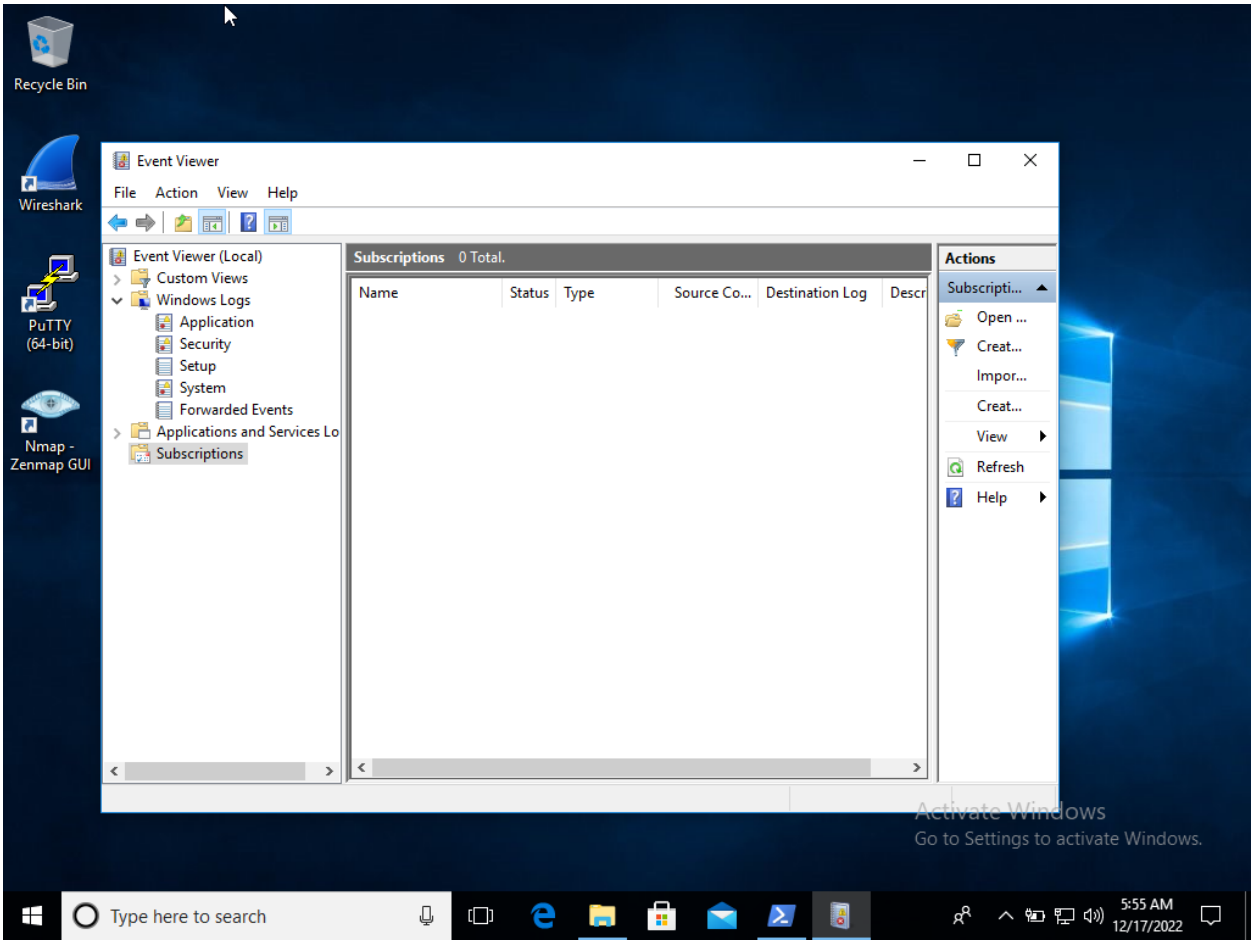
Are these machines (Ubuntu 18.04/Windows 10 ENT) currently shipping jobs to a centralized location?

Ubuntu 18.04



No, there is no FQDN or IP address of the loghost

Windows 10 ENT

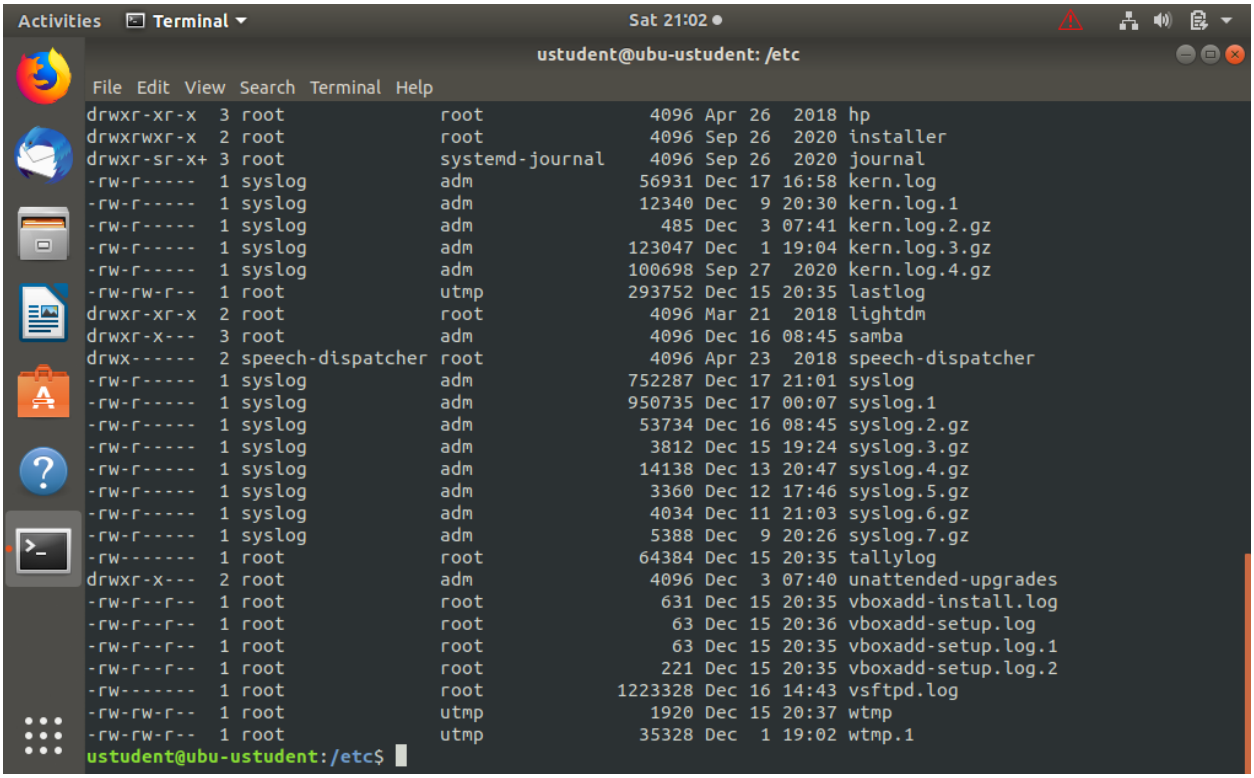


No, there is no remote subscriptions related Windows Events Forwarder

Ubuntu 18.04

Control Check: CIS 4.2.1.3 Ensure logging is configured (Not Scored)
Result: It is configured to log.
Proof of check:

```
# ls -l /var/log/
```



Impact: If the logging configuration isnt working, we will not be able to audit and investigate incidents of different events from different applications and services, and we will not be able to know the issues on the system and how it got compromised.

Recommendations on improvements to these systems.

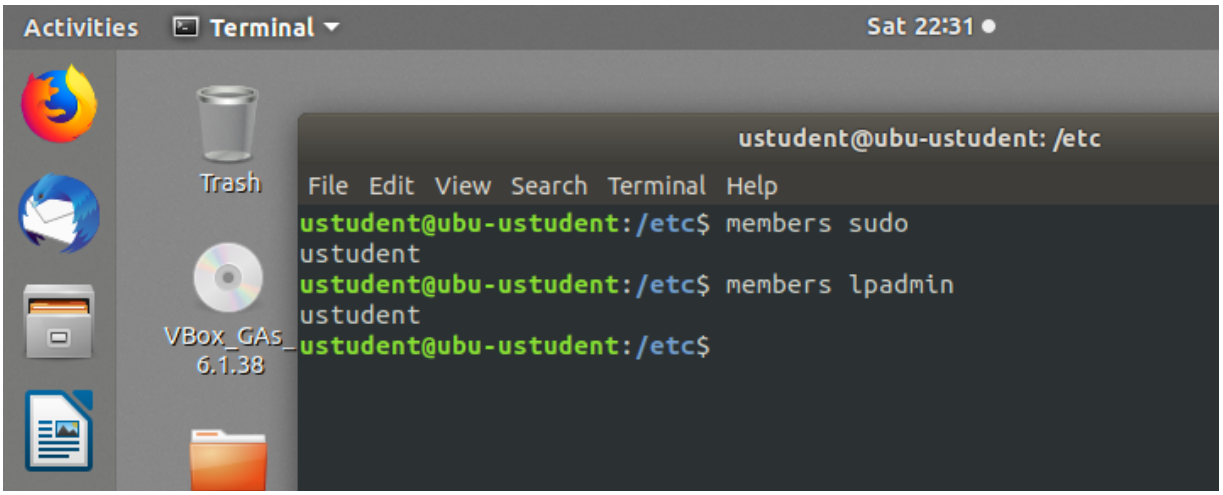
- Edit the /etc/rsyslog.conf and /etc/rsyslog.d/*.conf files and add the following line: **.* @@<FQDN or ip of loghost>*
- **Configure a remote subscription related to Windows Events Forwarder.**

Assess Authentication Management

Verify what type of authentication and access controls are in place for privileged and unprivileged users.

Are there users with excessive permissions?

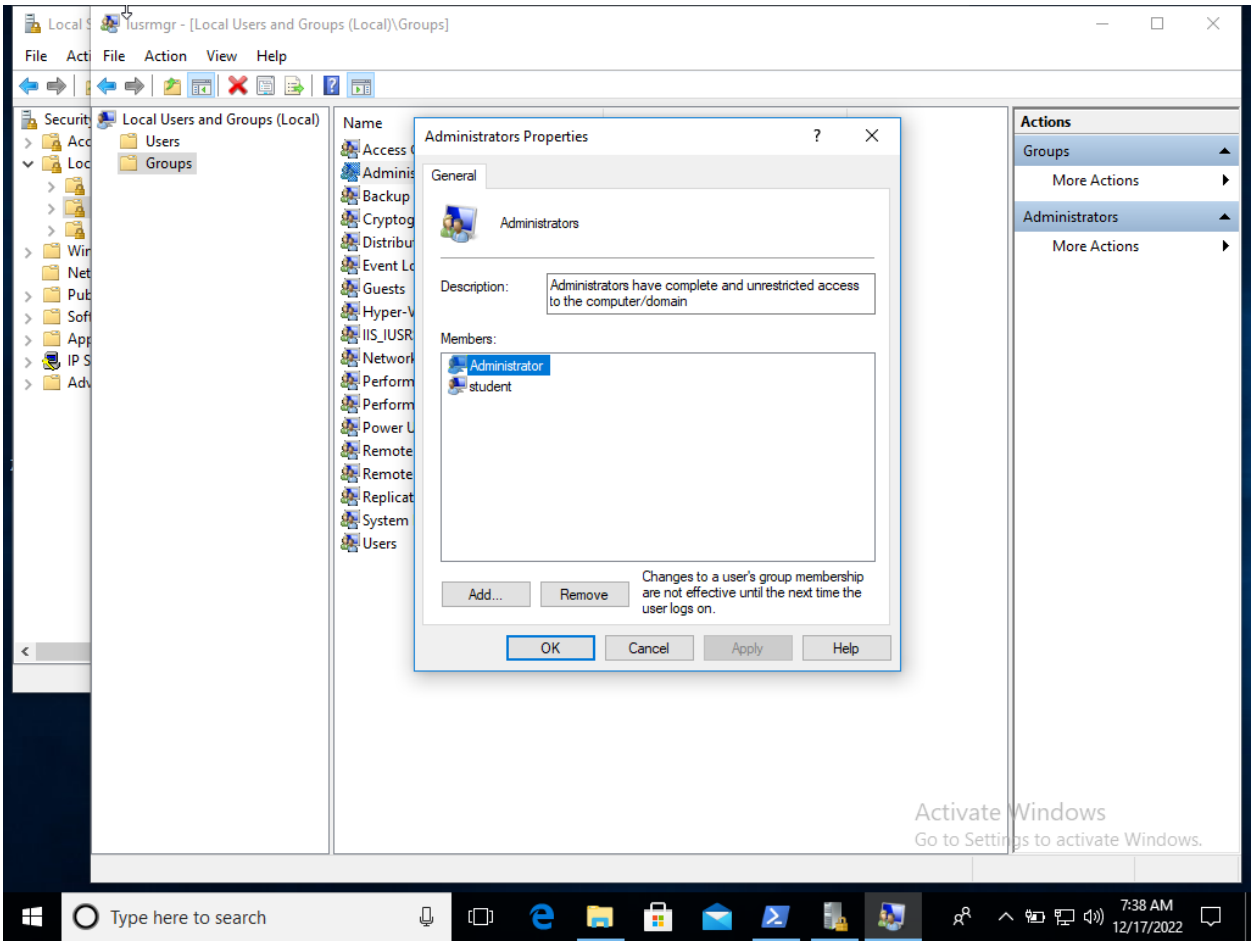
Ubuntu 18.04



Only the ustudent user is a member in the sudo and the lpadmin groups, therefore he has the same privilege as the root user and can run any command.

Yes, ustudent.

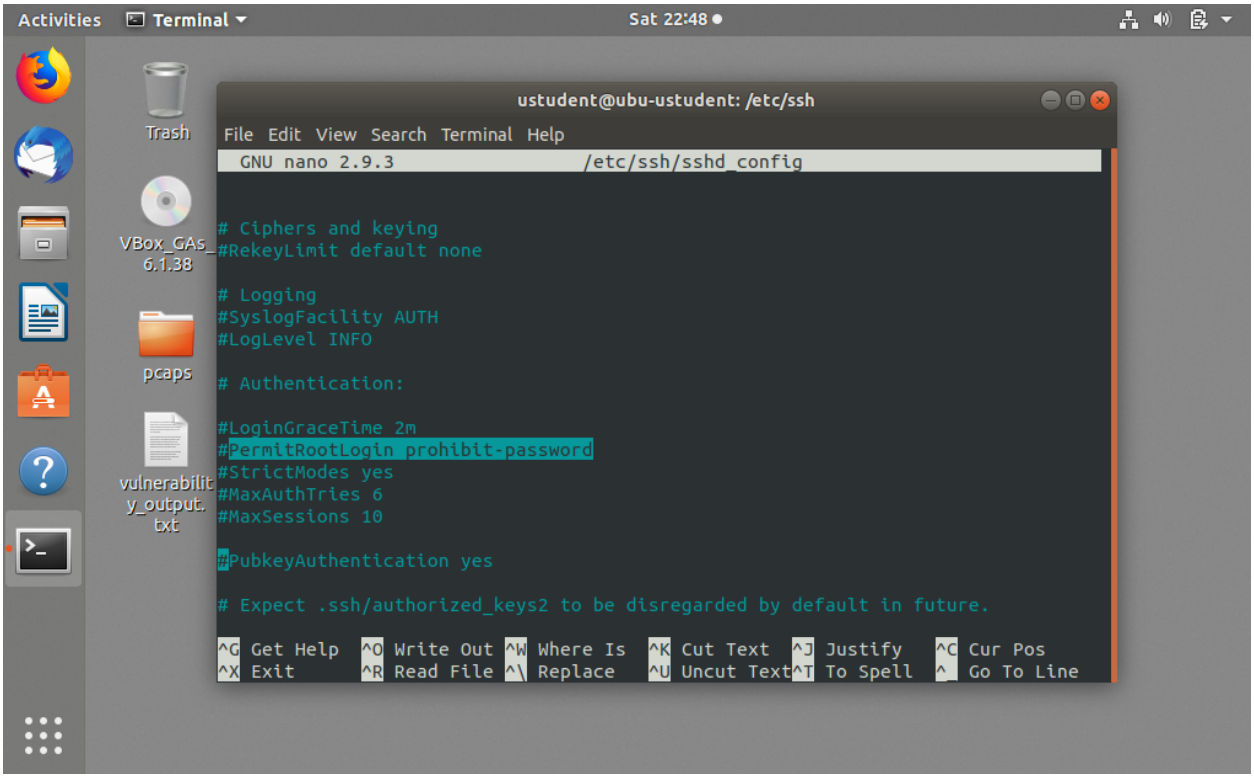
Windows 10 ENT



The student user is in the Administrators group, therefore he has the same privilege as the administrator.

Yes, student.

Is root remote login permitted?



Yes, because the line is commented.

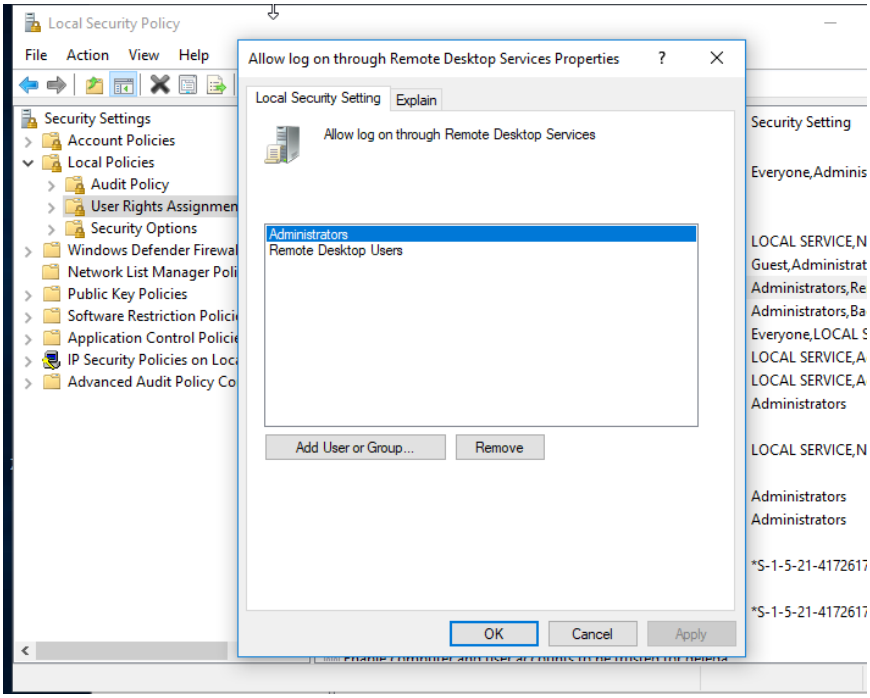
Are there other users allowed to SSH that shouldn't?

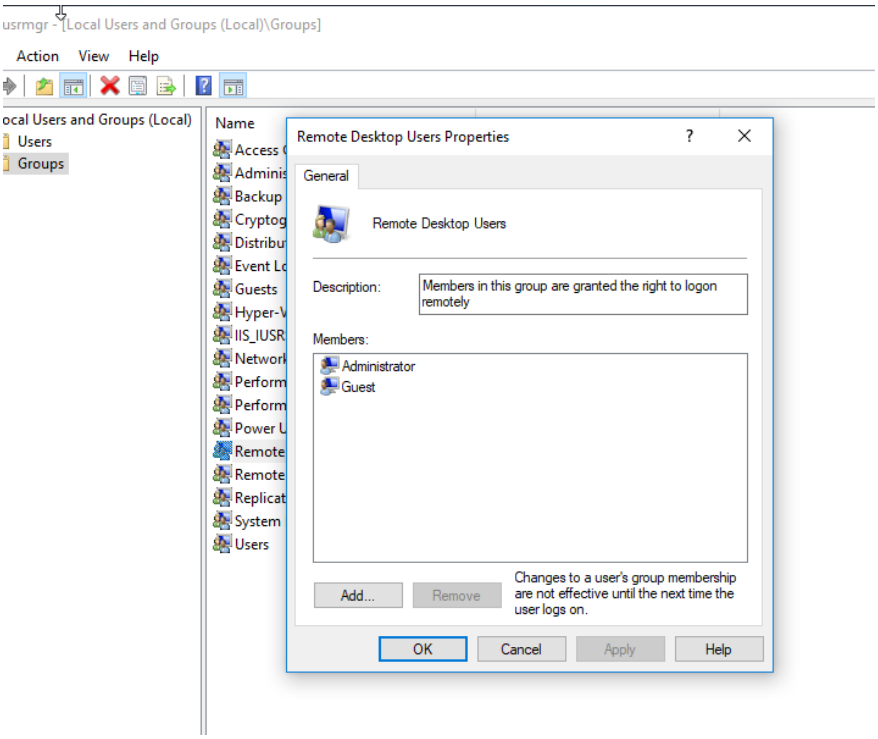
without the AllowUsers directive, there are no restrictions on which users can log in via ssh.

Are there users that should not have remote access?

Yes, all the users except the root should not have remote access.

Are there users with Remote Desktop Access that should not have it?





Yes, the Guest user.

Provide recommendations on how to improve security in these areas.

- **Allow only root/Administrator to log remotely by configuring the sshd_config file in Linux, and updating the user rights and group policy in Windows to make only the admin with the remote access right.**
- **Make only the privileged users have remote access.**
- **Normal users like student/ustudent should not have excessive permissions.**

Audit password policies in Windows & Linux.

Ubuntu 18.04

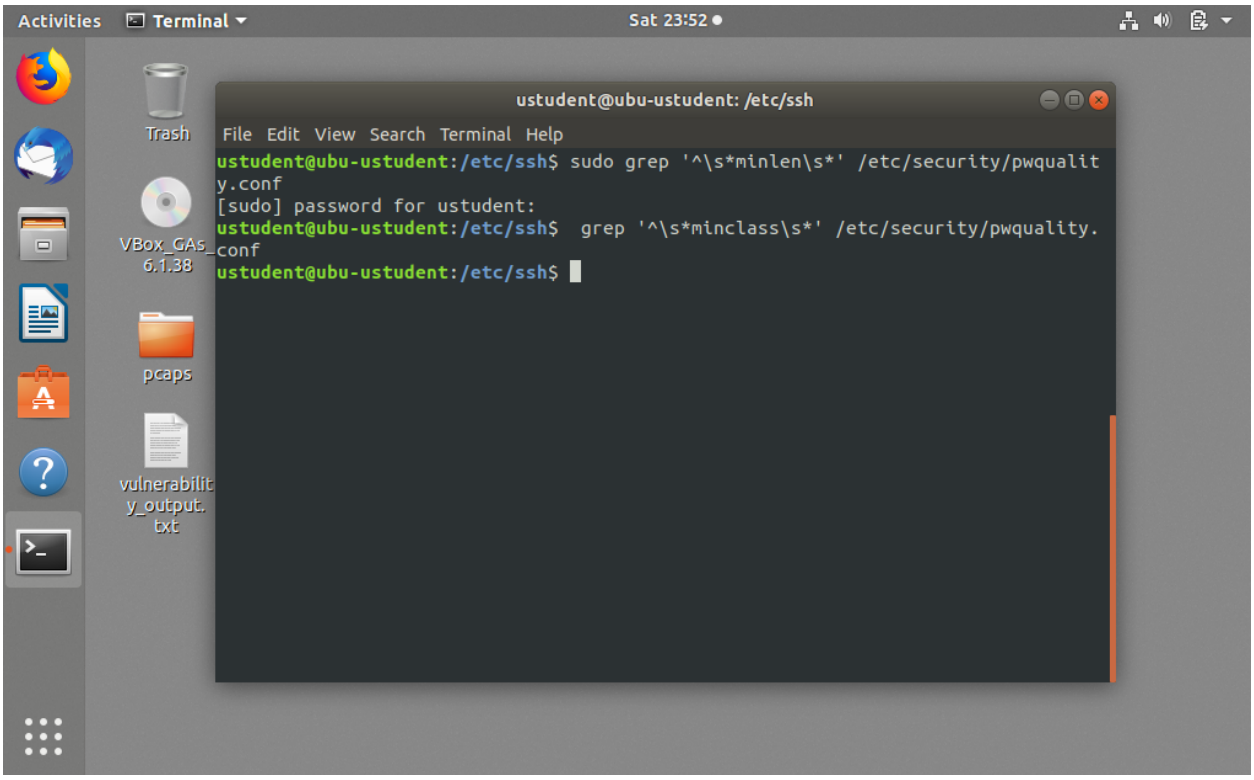
Control Check: CIS 5.3.1 Ensure password creation requirements are configured (Scored)
Result: Password creation requirements are not configured.
Proof of check:

```
# grep '^\s*minlen\s*' /etc/security/pwquality.conf

minlen = 14
```

```
# grep '^\s*minclass\s*' /etc/security/pwquality.conf

minclass = 4
```



Impact: Strong passwords protect systems from being hacked through brute force methods.

Remediation:

Run the following command to install the pam_pwquality module:

```
apt install libpam-pwquality
```

Edit the file `/etc/security/pwquality.conf` and add or modify the following line for password length to conform to site policy

```
minlen = 14
```

Edit the file /etc/security/pwquality.conf and add or modify the following line for password complexity to conform to site policy

```
minclass = 4
```

OR

```
dcredit = -1
ucredit = -1
ocredit = -1
lcredit = -1
```

Edit the `/etc/pam.d/common-password` file to include the appropriate options for `pam_pwquality.so` and to conform to site policy:

```
password requisite pam_pwquality.so retry=3
```

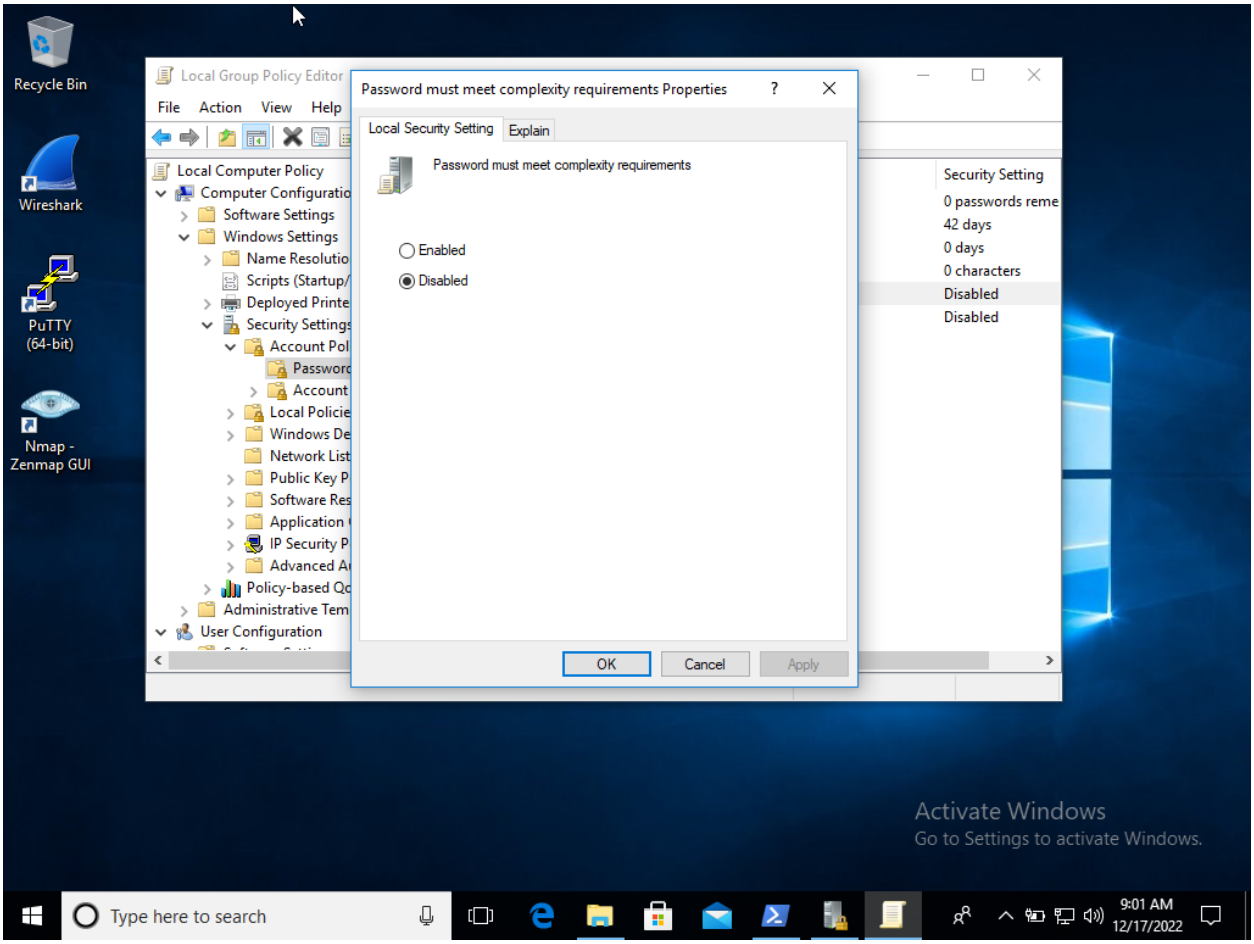
Windows 10 ENT

Control check - 1.1.5 (L1) Ensure 'Password must meet complexity requirements' is set to 'Enabled' (Automated)

Result: Password did not meet complexity requirement.

Proof of check:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Account
Policies\Password Policy\Password must meet complexity requirements
```



Impact: Passwords that contain only alphanumeric characters are extremely easy to discover with several publicly available tools.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

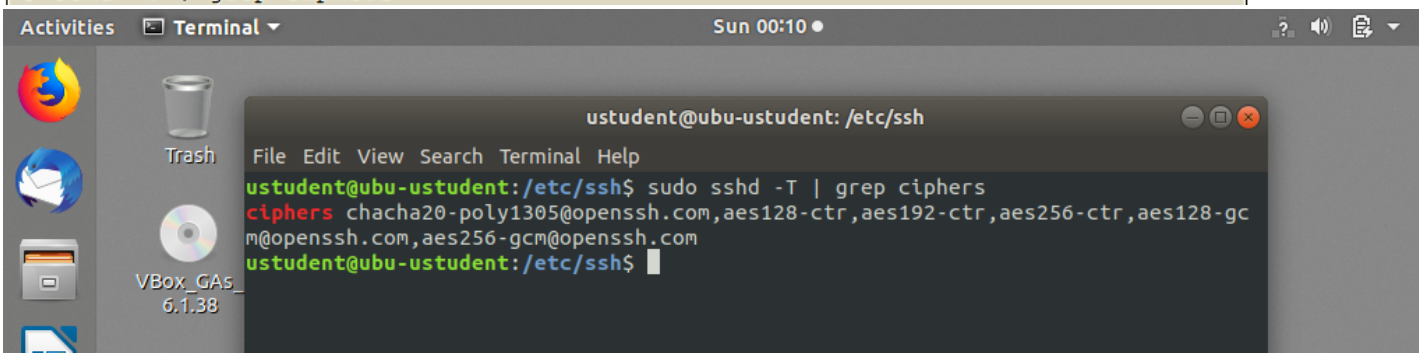
```
Computer Configuration\Policies\Windows Settings\Security Settings\Account
Policies\Password Policy\Password must meet complexity requirements
```

Verify the use of strong encryption in audited systems.

Ubuntu 18.04

Control Check: CIS 5.2.13 Ensure only strong Ciphers are used (Scored)
Result: The system is not compliant with FIPS 140-2
Proof of check:

```
# sshd -T | grep ciphers
```

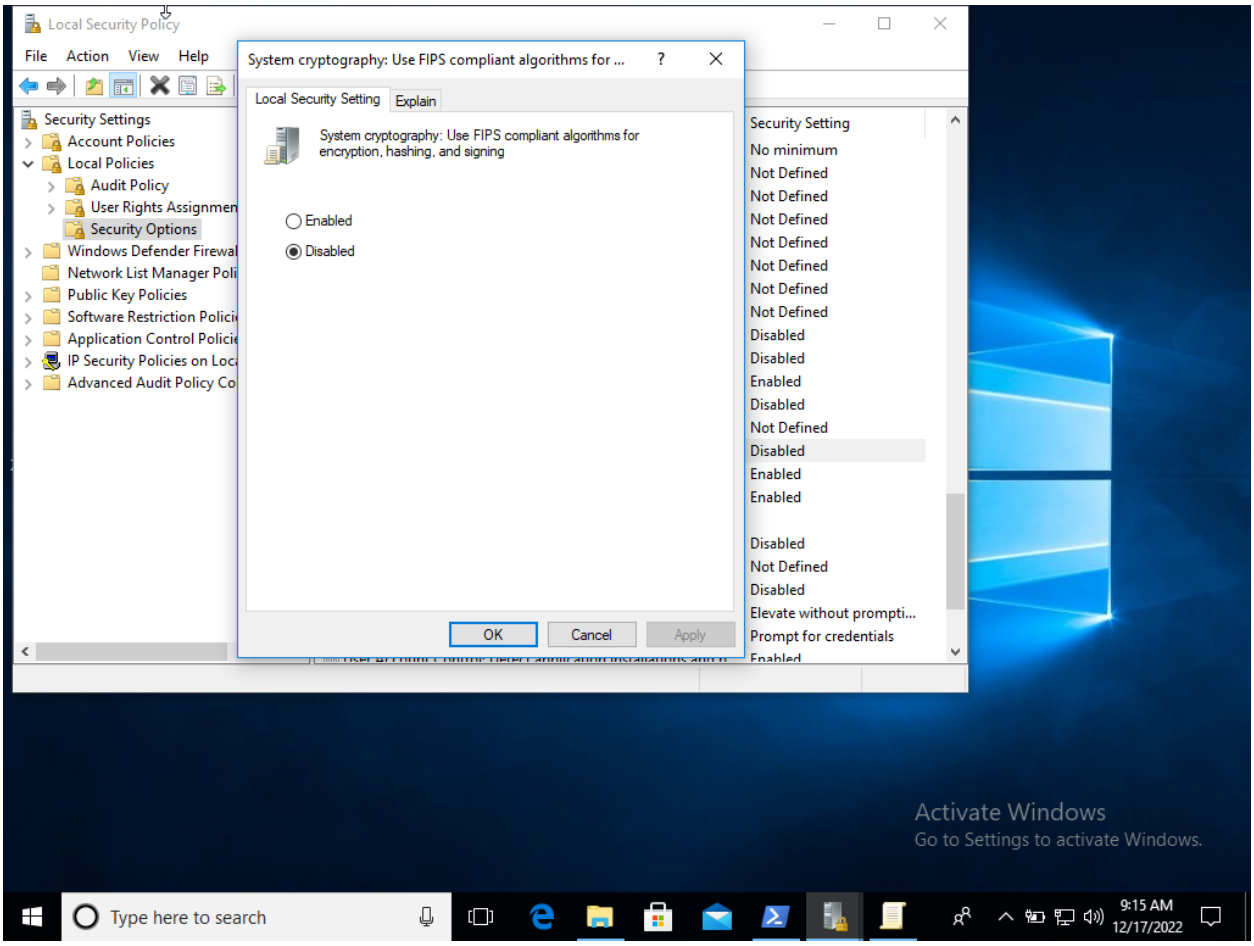


Impact: The system does not comply with the security policy of the infrastructure, therefore the security posture will be affected.

Remediation:

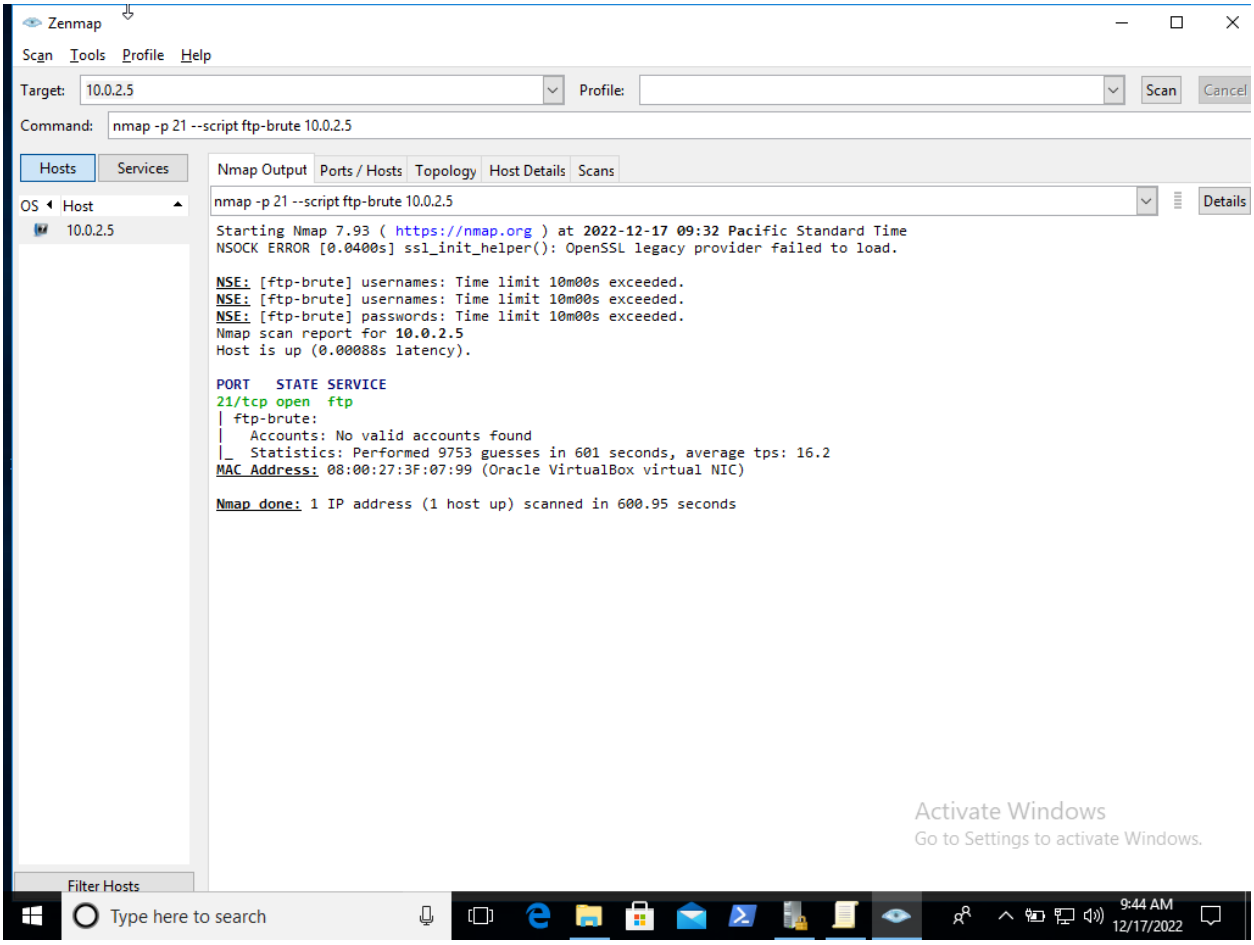
Edit the `/etc/ssh/sshd_config` file add/modify the `Ciphers` line to contain a comma separated list of the site approved ciphers

Windows 10 ENT

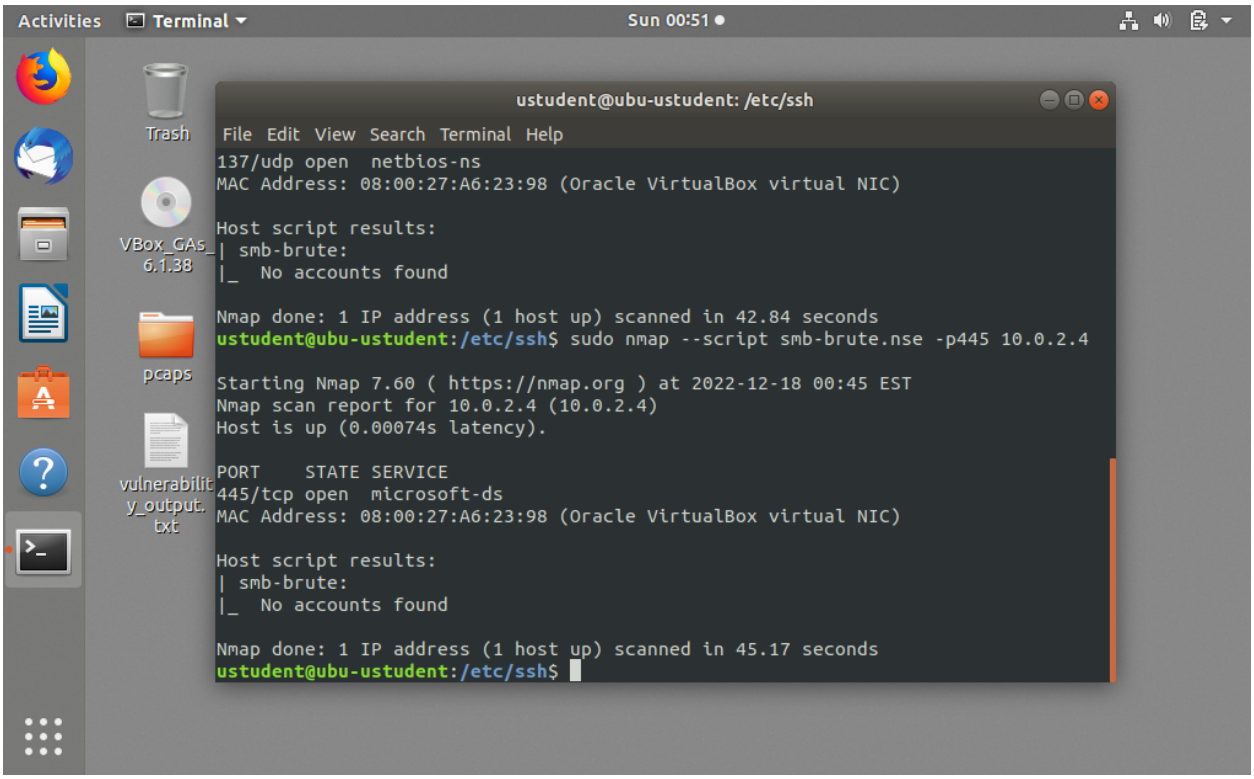


Windows is not compliant with the infrastructure security policy.
Recommendation: Enable the system cryptography: Use FIPS.

Audit network services passwords using NMAP NSE scripts.



With the NSE script used, the FTP brute-force here did not succeed.



No accounts was found when brute forcing smb.

Final Assessment and Recommendations Based on Your Scans and Checks

- Would integrating this network into the extended network of our company bring new risks and exposures?
Yes, it definitely would bring numerous amount of risks.

- If it would be a risk to NuttyUtility, what recommendations would you make to mitigate these risks before implementing the integration, and why?

- Follow through the remediation steps presented in this report.
- Comply with the security policy for encryption so that the system can maintain a good security posture.
- upgrade services and patch vulnerabilities to reduce the surface attack.
- Avoid using VNC as it is easily exploitable by threat actors.
- Disable unused ports and services to reduce the surface attack.
- Apply domain isolation through IP Security and firewalls to harden the system further and reduce the impact incase of a compromise.
- Avoid using IPv6 unless necessary because not all security controls are configured to work with it.
- Apply the Principle of least privilege and zero trust on users.
- Allow only admins and roots to have remote access, so that threat actors cannot compromise easy low security users accounts like guests to remote access the system.
- Ensure the system is logged correctly and to a centralized SIEM to monitor and manage the logs.
- Ensure strong password complexity is complied to avoid brute-force attacks.

Should this happen immediately? Why or why not?

Yes, the remediation should happen immediately and when done, another assessment should be made to make sure all the issues are solved and that its ready to be extended safely to the infrastructure.