

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

Allow 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.

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

The 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

Name	Type	Data
(Default)	REG_SZ	(value not set)
BranchReadiness...	REG_SZ	CB
DeferFeatureUp...	REG_DWORD	0x00000000 (0)
DeferQualityUp...	REG_DWORD	0x00000000 (0)
FeatureUpdateP...	REG_DWORD	0x00000023 (35)
FeatureUpdates...	REG_DWORD	0x00000001 (1)
IsDeferralsActive	REG_DWORD	0x00000001 (1)
IsWUfBConfigur...	REG_DWORD	0x00000001 (1)
PauseFeatureUp...	REG_SZ	2020-10-31T19:28:18Z
PauseFeatureUp...	REG_SZ	2020-09-26T19:28:18Z
PauseQualityUp...	REG_SZ	2020-10-31T19:28:18Z
PauseQualityUp...	REG_SZ	2020-09-26T19:28:18Z
PolicySources	REG_DWORD	0x00000010 (16)
QualityUpdateP...	REG_DWORD	0x00000023 (35)
QualityUpdates...	REG_DWORD	0x00000001 (1)

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
```

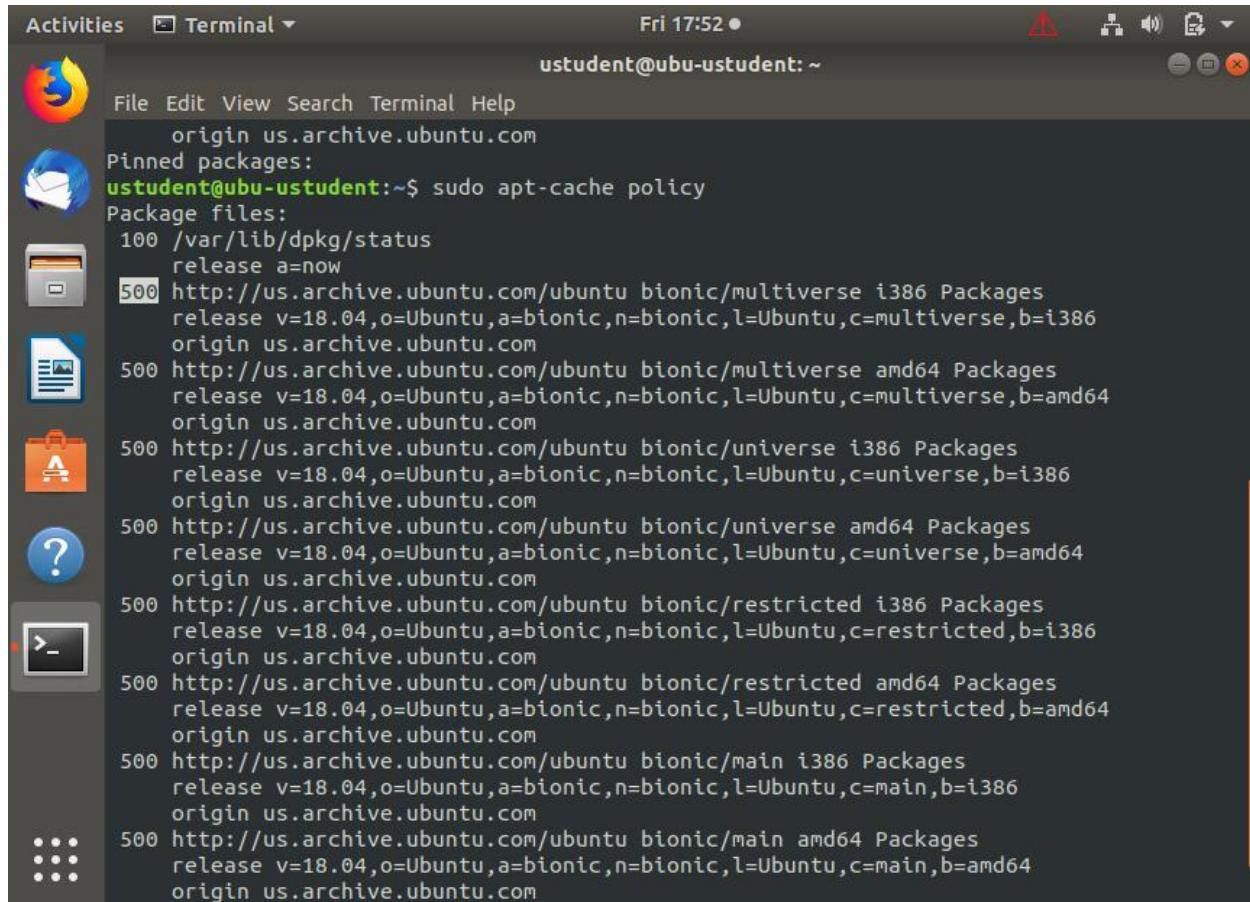
Note: This Group Policy path is provided by the Group Policy template WindowsUpdate.admx/adml that is included with all versions of the Microsoft Windows Administrative Templates.

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:



```
Activities Terminal Fri 17:52 • uststudent@ubu-ustudent: ~
File Edit View Search Terminal Help
origin us.archive.ubuntu.com
Pinned packages:
ustudent@ubu-ustudent:~$ sudo apt-cache policy
Package files:
100 /var/lib/dpkg/status
    release a=now
500 http://us.archive.ubuntu.com/ubuntu bionic/multiverse i386 Packages
    release v=18.04,o=Ubuntu,a=bionic,n=bionic,l=Ubuntu,c=multiverse,b=i386
    origin us.archive.ubuntu.com
500 http://us.archive.ubuntu.com/ubuntu bionic/multiverse amd64 Packages
    release v=18.04,o=Ubuntu,a=bionic,n=bionic,l=Ubuntu,c=multiverse,b=amd64
    origin us.archive.ubuntu.com
500 http://us.archive.ubuntu.com/ubuntu bionic/universe i386 Packages
    release v=18.04,o=Ubuntu,a=bionic,n=bionic,l=Ubuntu,c=universe,b=i386
    origin us.archive.ubuntu.com
500 http://us.archive.ubuntu.com/ubuntu bionic/universe amd64 Packages
    release v=18.04,o=Ubuntu,a=bionic,n=bionic,l=Ubuntu,c=universe,b=amd64
    origin us.archive.ubuntu.com
500 http://us.archive.ubuntu.com/ubuntu bionic/restricted i386 Packages
    release v=18.04,o=Ubuntu,a=bionic,n=bionic,l=Ubuntu,c=restricted,b=i386
    origin us.archive.ubuntu.com
500 http://us.archive.ubuntu.com/ubuntu bionic/restricted amd64 Packages
    release v=18.04,o=Ubuntu,a=bionic,n=bionic,l=Ubuntu,c=restricted,b=amd64
    origin us.archive.ubuntu.com
500 http://us.archive.ubuntu.com/ubuntu bionic/main i386 Packages
    release v=18.04,o=Ubuntu,a=bionic,n=bionic,l=Ubuntu,c=main,b=i386
    origin us.archive.ubuntu.com
500 http://us.archive.ubuntu.com/ubuntu bionic/main amd64 Packages
    release v=18.04,o=Ubuntu,a=bionic,n=bionic,l=Ubuntu,c=main,b=amd64
    origin us.archive.ubuntu.com
```

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.

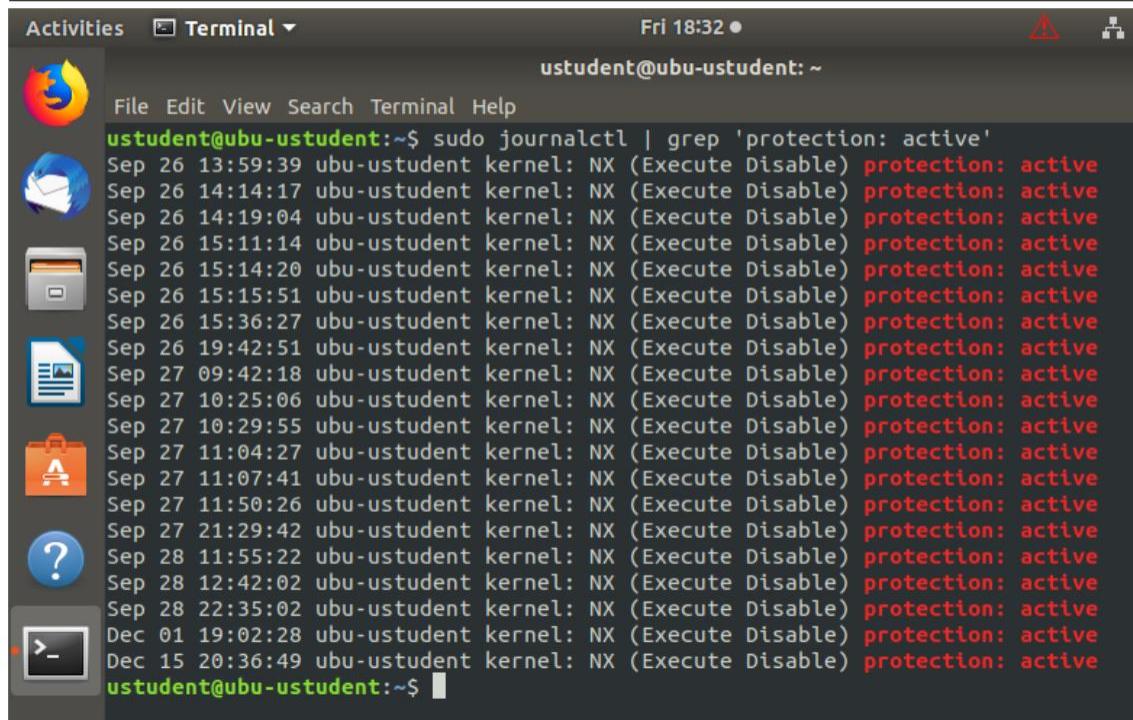
Ubuntu 18.04

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
```



A screenshot of a Linux desktop environment, specifically Ubuntu 18.04, showing a terminal window. The terminal window title is "Terminal". The terminal content shows the output of the command "sudo journalctl | grep 'protection: active'". The output lists numerous log entries from the kernel, all showing "protection: active" for the NX (Execute Disable) setting. The desktop interface includes a dock with icons for various applications like a browser, file manager, and terminal, and a system tray with icons for battery, signal, and volume.

```
ustudent@ubu-ustudent:~$ sudo journalctl | grep 'protection: active'  
Sep 26 13:59:39 ubu-ustudent kernel: NX (Execute Disable) protection: active  
Sep 26 14:14:17 ubu-ustudent kernel: NX (Execute Disable) protection: active  
Sep 26 14:19:04 ubu-ustudent kernel: NX (Execute Disable) protection: active  
Sep 26 15:11:14 ubu-ustudent kernel: NX (Execute Disable) protection: active  
Sep 26 15:14:20 ubu-ustudent kernel: NX (Execute Disable) protection: active  
Sep 26 15:15:51 ubu-ustudent kernel: NX (Execute Disable) protection: active  
Sep 26 15:36:27 ubu-ustudent kernel: NX (Execute Disable) protection: active  
Sep 26 19:42:51 ubu-ustudent kernel: NX (Execute Disable) protection: active  
Sep 27 09:42:18 ubu-ustudent kernel: NX (Execute Disable) protection: active  
Sep 27 10:25:06 ubu-ustudent kernel: NX (Execute Disable) protection: active  
Sep 27 10:29:55 ubu-ustudent kernel: NX (Execute Disable) protection: active  
Sep 27 11:04:27 ubu-ustudent kernel: NX (Execute Disable) protection: active  
Sep 27 11:07:41 ubu-ustudent kernel: NX (Execute Disable) protection: active  
Sep 27 11:50:26 ubu-ustudent kernel: NX (Execute Disable) protection: active  
Sep 27 21:29:42 ubu-ustudent kernel: NX (Execute Disable) protection: active  
Sep 28 11:55:22 ubu-ustudent kernel: NX (Execute Disable) protection: active  
Sep 28 12:42:02 ubu-ustudent kernel: NX (Execute Disable) protection: active  
Sep 28 22:35:02 ubu-ustudent kernel: NX (Execute Disable) protection: active  
Dec 01 19:02:28 ubu-ustudent kernel: NX (Execute Disable) protection: active  
Dec 15 20:36:49 ubu-ustudent kernel: NX (Execute Disable) protection: active  
ustudent@ubu-ustudent:~$
```

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

Ubuntu 18.04

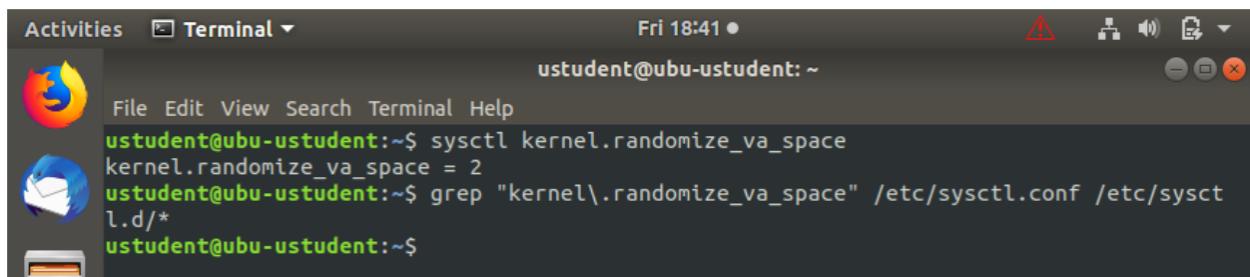
Control Check: CIS 1.6.2 Ensure address space layout randomization (ASLR) is enabled (Scored)

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
```



A screenshot of a terminal window titled "Terminal". The window shows the following command-line session:

```
File Edit View Search Terminal Help
ustudent@ubu-ustudent:~$ sysctl kernel.randomize_va_space
kernel.randomize_va_space = 2
ustudent@ubu-ustudent:~$ grep "kernel\.randomize_va_space" /etc/sysctl.conf /etc/sysct
l.d/*
ustudent@ubu-ustudent:~$
```

Remediation:

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

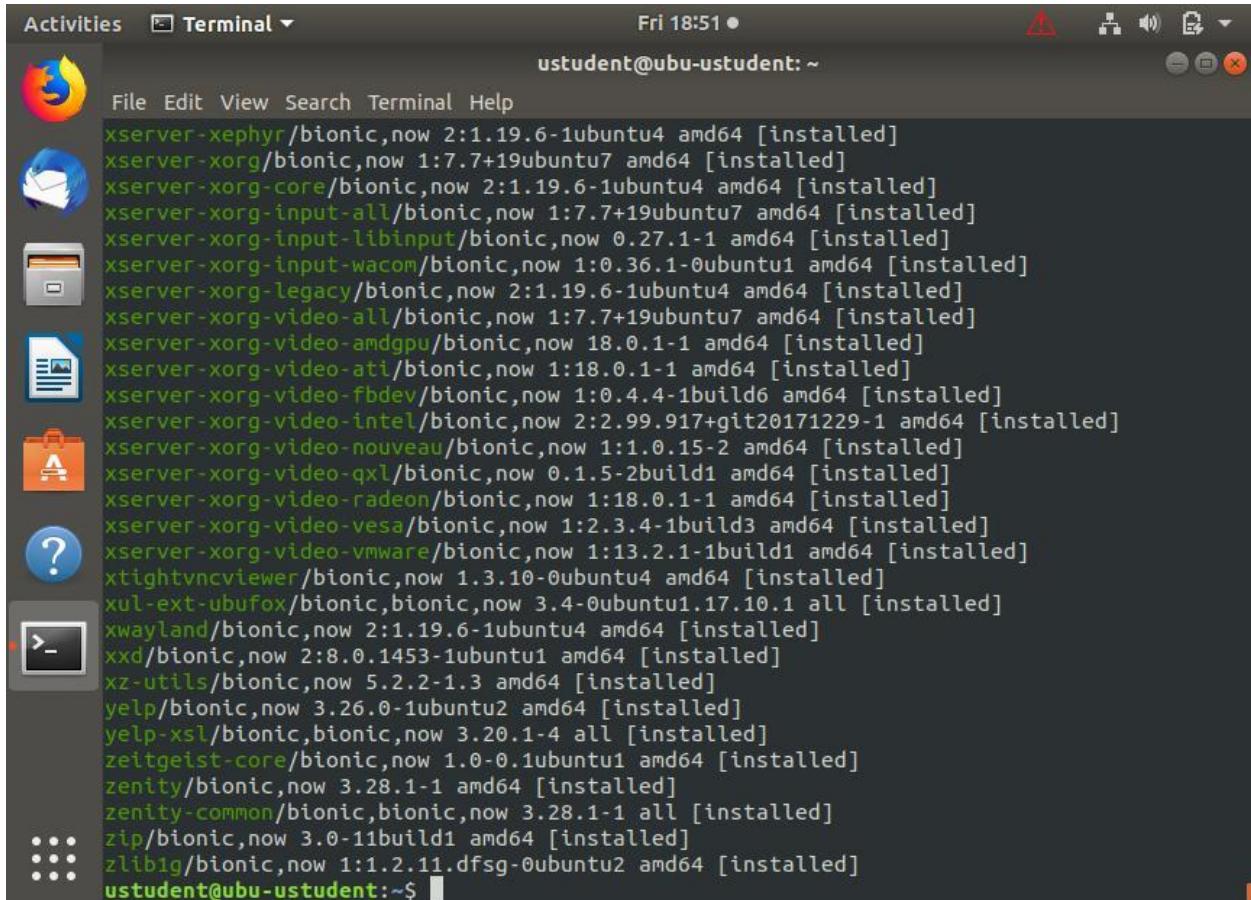
```
kernel.randomize_va_space = 2
```

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

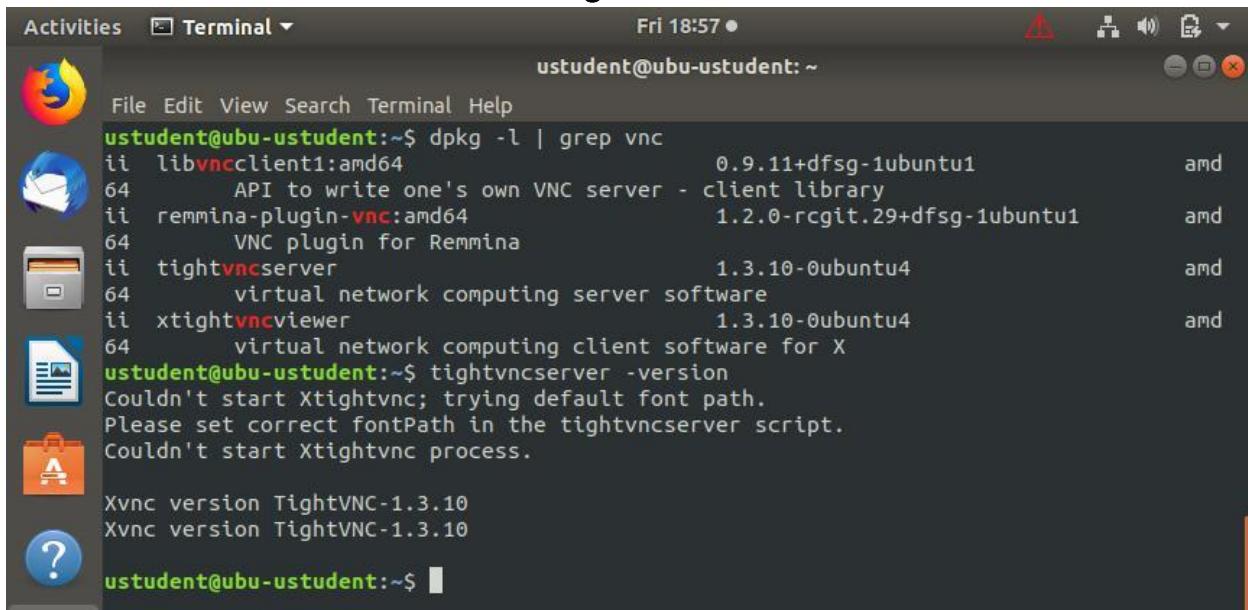


A screenshot of a Linux desktop environment, likely Ubuntu, showing a terminal window titled "Terminal". The terminal window displays a list of installed packages from the command "sudo apt list --installed". The output is as follows:

```
xserver-xephyr/bionic,now 2:1.19.6-1ubuntu4 amd64 [installed]
xserver-xorg/bionic,now 1:7.7+19ubuntu7 amd64 [installed]
xserver-xorg-core/bionic,now 2:1.19.6-1ubuntu4 amd64 [installed]
xserver-xorg-input-all/bionic,now 1:7.7+19ubuntu7 amd64 [installed]
xserver-xorg-input-libinput/bionic,now 0.27.1-1 amd64 [installed]
xserver-xorg-input-wacom/bionic,now 1:0.36.1-0ubuntu1 amd64 [installed]
xserver-xorg-legacy/bionic,now 2:1.19.6-1ubuntu4 amd64 [installed]
xserver-xorg-video-all/bionic,now 1:7.7+19ubuntu7 amd64 [installed]
xserver-xorg-video-amdgpu/bionic,now 18.0.1-1 amd64 [installed]
xserver-xorg-video-ati/bionic,now 1:18.0.1-1 amd64 [installed]
xserver-xorg-video-fbdev/bionic,now 1:0.4.4-1build6 amd64 [installed]
xserver-xorg-video-intel/bionic,now 2:2.99.917+git20171229-1 amd64 [installed]
xserver-xorg-video-nouveau/bionic,now 1:1.0.15-2 amd64 [installed]
xserver-xorg-video-qxl/bionic,now 0.1.5-2build1 amd64 [installed]
xserver-xorg-video-radeon/bionic,now 1:18.0.1-1 amd64 [installed]
xserver-xorg-video-vesa/bionic,now 1:2.3.4-1build3 amd64 [installed]
xserver-xorg-video-vmware/bionic,now 1:13.2.1-1build1 amd64 [installed]
xtightvncviewer/bionic,now 1.3.10-0ubuntu4 amd64 [installed]
xul-ext-ubufox/bionic,bionic,now 3.4-0ubuntu1.17.10.1 all [installed]
xwayland/bionic,now 2:1.19.6-1ubuntu4 amd64 [installed]
xxd/bionic,now 2:8.0.1453-1ubuntu1 amd64 [installed]
xz-utils/bionic,now 5.2.2-1.3 amd64 [installed]
yelp/bionic,now 3.26.0-1ubuntu2 amd64 [installed]
yelp-xsl/bionic,bionic,now 3.20.1-4 all [installed]
zeitgeist-core/bionic,now 1.0-0.1ubuntu1 amd64 [installed]
zenity/bionic,now 3.28.1-1 amd64 [installed]
zenity-common/bionic,bionic,now 3.28.1-1 all [installed]
zip/bionic,now 3.0-11build1 amd64 [installed]
zlib1g/bionic,now 1:1.2.11.dfsg-0ubuntu2 amd64 [installed]
```

The terminal window title bar shows "ustudent@uba-ustudent: ~". The desktop environment includes icons for the Dash, Home, and Help.

TightVNC



A screenshot of a Ubuntu desktop environment. In the top left, there's a dock with icons for the Dash, Activities, Home, and Terminal. The terminal window is open and titled "TightVNC". The title bar also shows the date and time as "Fri 18:57". The terminal window contains the following text:

```
ustudent@ubu-ustudent:~$ dpkg -l | grep vnc
ii  libvncclient1:amd64          0.9.11+dfsg-1ubuntu1      amd
64    API to write one's own VNC server - client library
ii  remmina-plugin-vnc:amd64     1.2.0-rcgit.29+dfsg-1ubuntu1  amd
64    VNC plugin for Remmina
ii  tightvncserver              1.3.10-0ubuntu4        amd
64    virtual network computing server software
ii  xtightvncviewer             1.3.10-0ubuntu4        amd
64    virtual network computing client software for X
ustudent@ubu-ustudent:~$ tightvncserver -version
Couldn't start Xtightvnc; trying default font path.
Please set correct fontPath in the tightvncserver script.
Couldn't start Xtightvnc process.

Xvnc version TightVNC-1.3.10
Xvnc version TightVNC-1.3.10
ustudent@ubu-ustudent:~$
```

TightVNC is installed in Ubuntu.

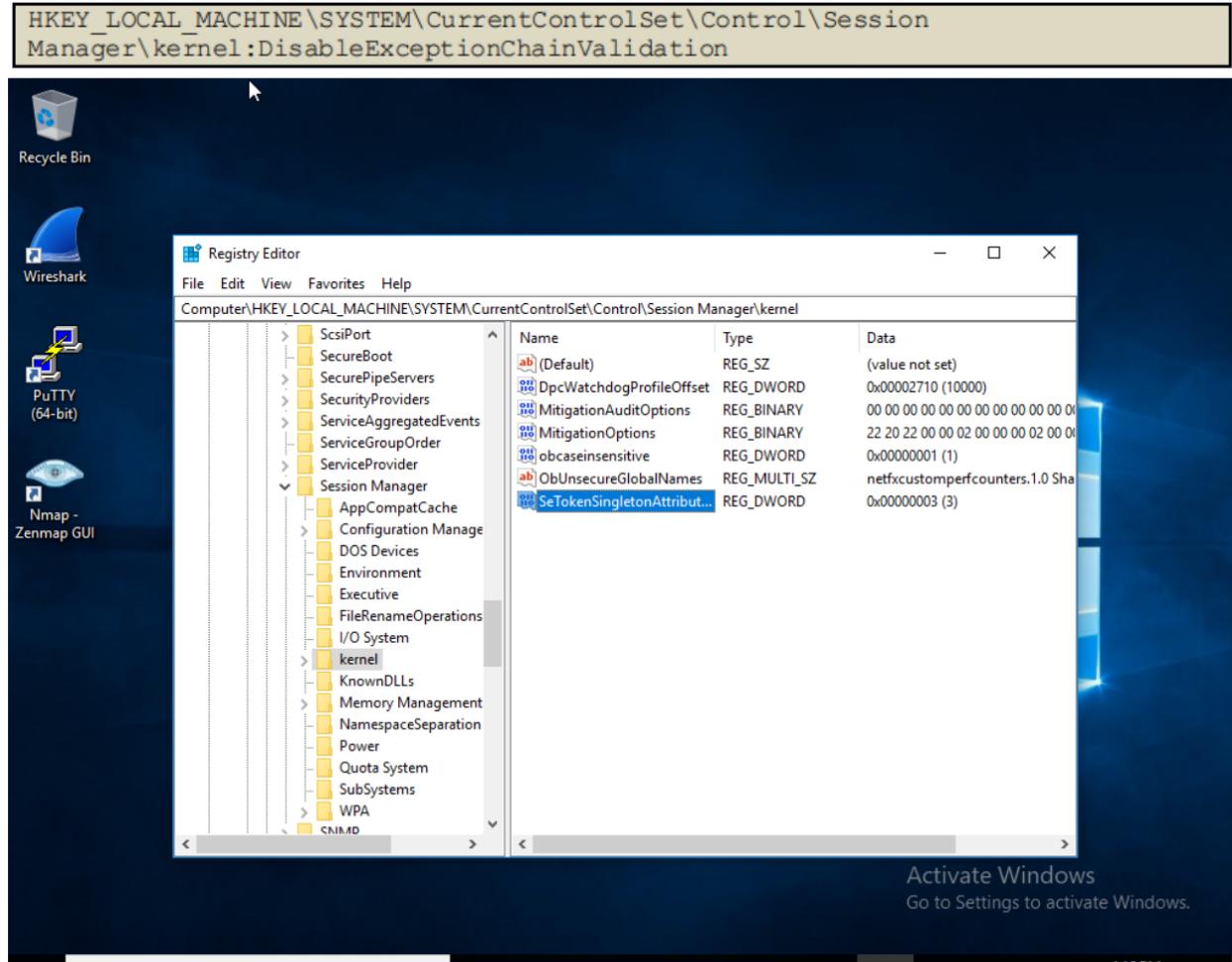
Having TightVNC brings added risk to the system. In TightVNC code version 1.3.10, there's a critical global buffer overflow ([CVE-2019-8287](#)) in HandleCoRREBBP macro function, also with a CVSS rating of 9.8 out of 10. This can also potentially result RCE, Kaspersky found.

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:



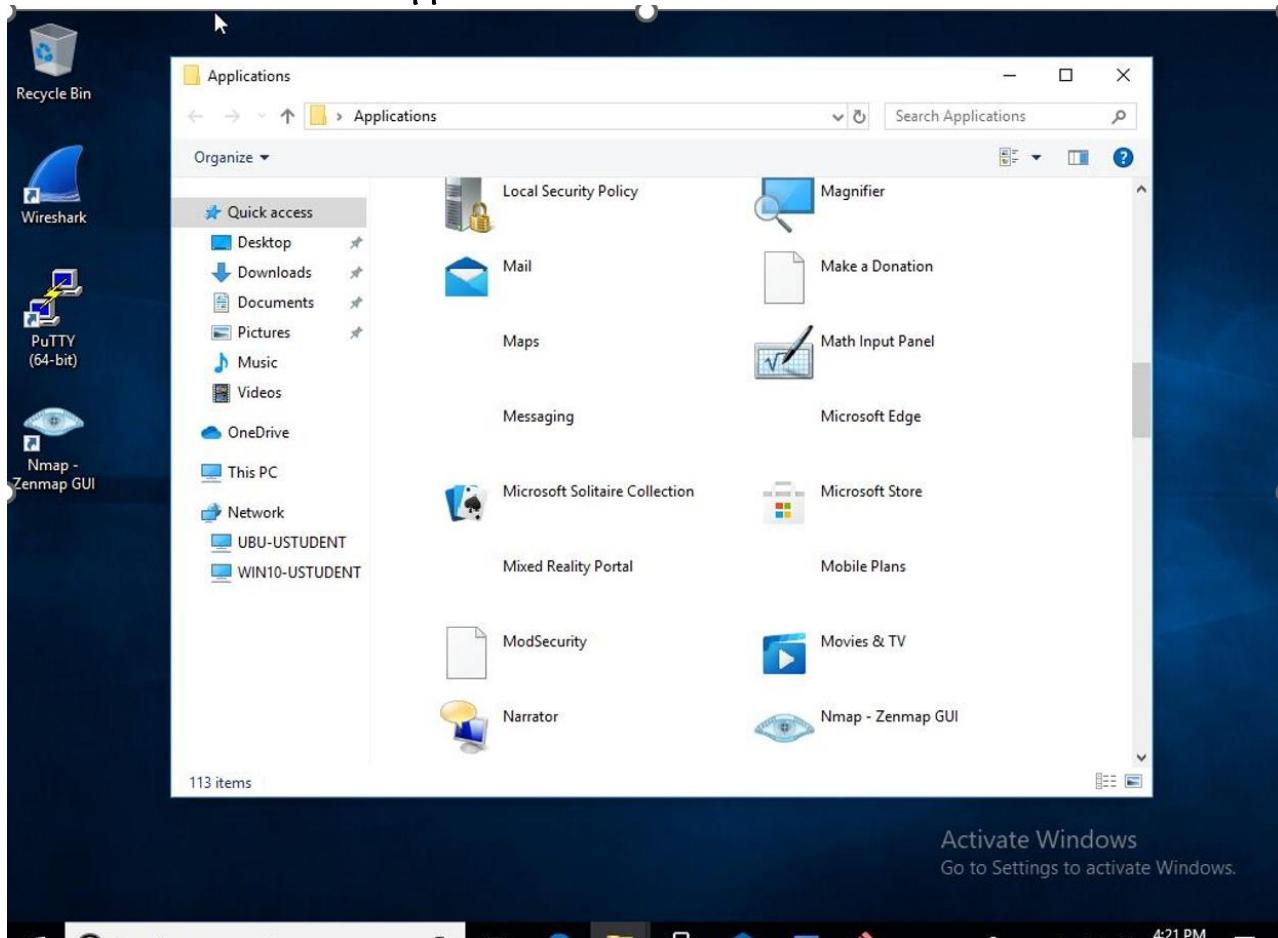
Impact: After you enable SEHOP, existing versions of Cygwin, Skype, and Armadillo-protected applications may not work correctly.

Remediation:

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

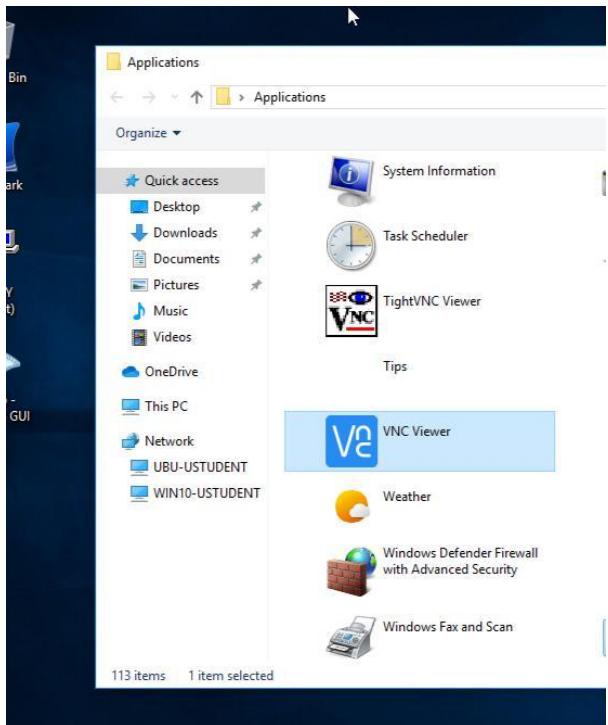
Computer Configuration\Policies\Administrative Templates\MS Security Guide\Enable Structured Exception Handling Overwrite Protection (SEHOP)

Applications installed in Windows:



113 applications are installed.

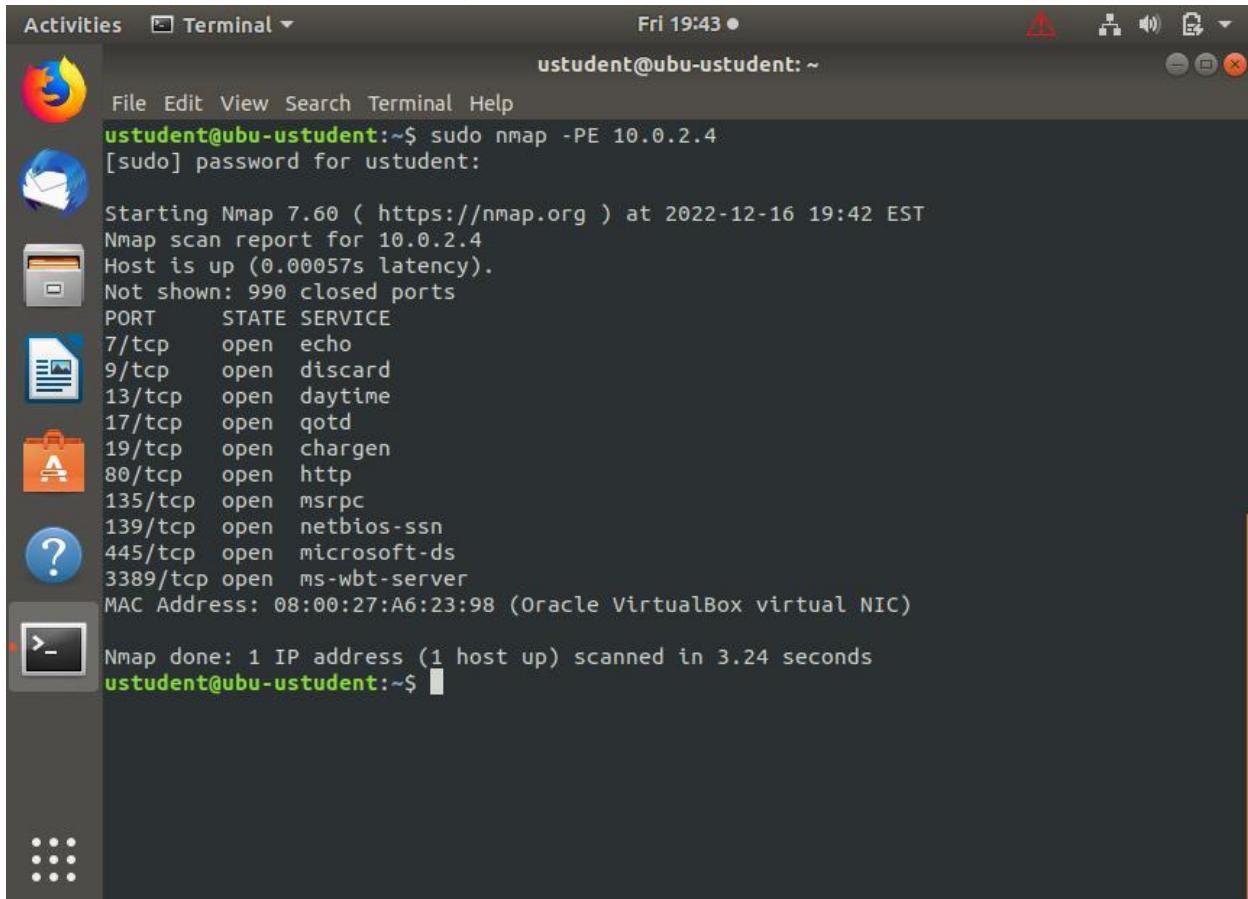
VNC Viewer:



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:



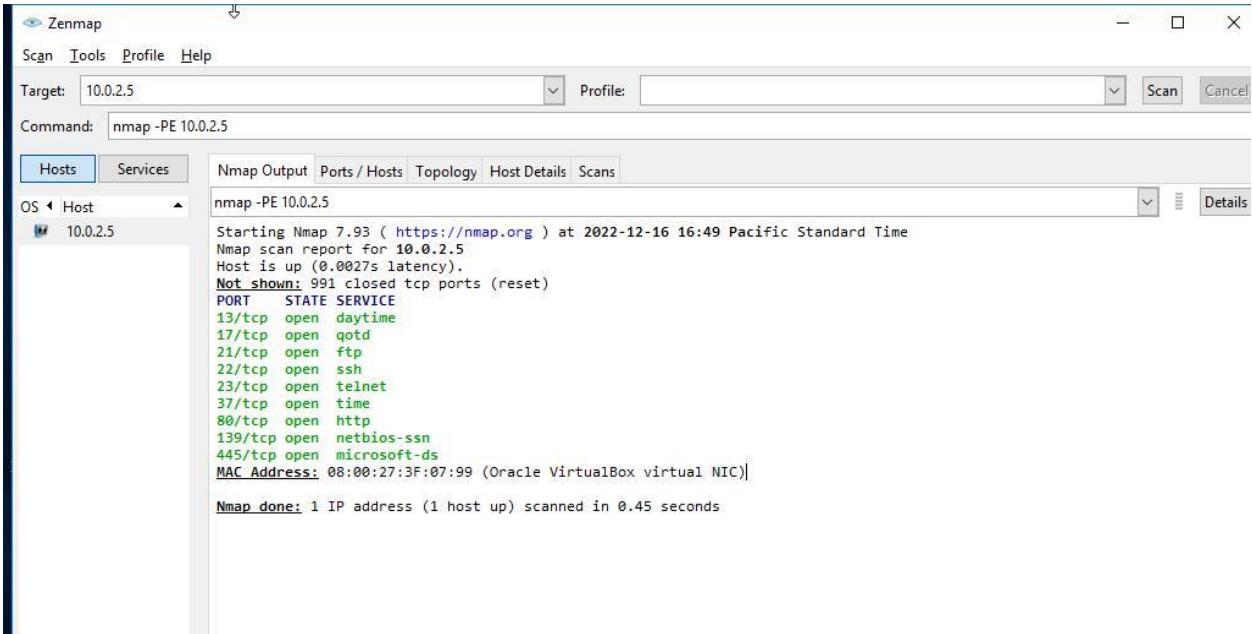
A screenshot of a Linux desktop environment, specifically Ubuntu, showing a terminal window. The terminal window title is "Terminal". The terminal content shows the output of an Nmap scan against the IP address 10.0.2.4. The output indicates that the host is up and lists various open ports, including echo, discard, daytime, qotd, chargen, http, msrpc, netbios-ssn, microsoft-ds, and ms-wbt-server. The MAC address of the interface is also listed as 08:00:27:A6:23:98 (Oracle VirtualBox virtual NIC).

```
File Edit View Search Terminal Help
ustudent@ubu-ustudent:~$ sudo nmap -PE 10.0.2.4
[sudo] password for ustudent:

Starting Nmap 7.60 ( https://nmap.org ) at 2022-12-16 19:42 EST
Nmap scan report for 10.0.2.4
Host is up (0.00057s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE
7/tcp      open  echo
9/tcp      open  discard
13/tcp     open  daytime
17/tcp     open  qotd
19/tcp     open  chargen
80/tcp     open  http
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
3389/tcp   open  ms-wbt-server
MAC Address: 08:00:27:A6:23:98 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 3.24 seconds
ustudent@ubu-ustudent:~$
```

Ports opened on Ubuntu machine:



The screenshot shows the Zenmap interface with the title "Ports opened on Ubuntu machine:". The "Targets" field contains "10.0.2.5". The "Command" field shows "nmap -PE 10.0.2.5". The "Hosts" tab is selected. The results pane displays the following Nmap output:

```
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-16 16:49 Pacific Standard Time
Nmap scan report for 10.0.2.5
Host is up (0.0027s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
13/tcp    open  daytime
17/tcp    open  qotd
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
37/tcp    open  time
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 08:00:27:3F:07:99 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.45 seconds
```

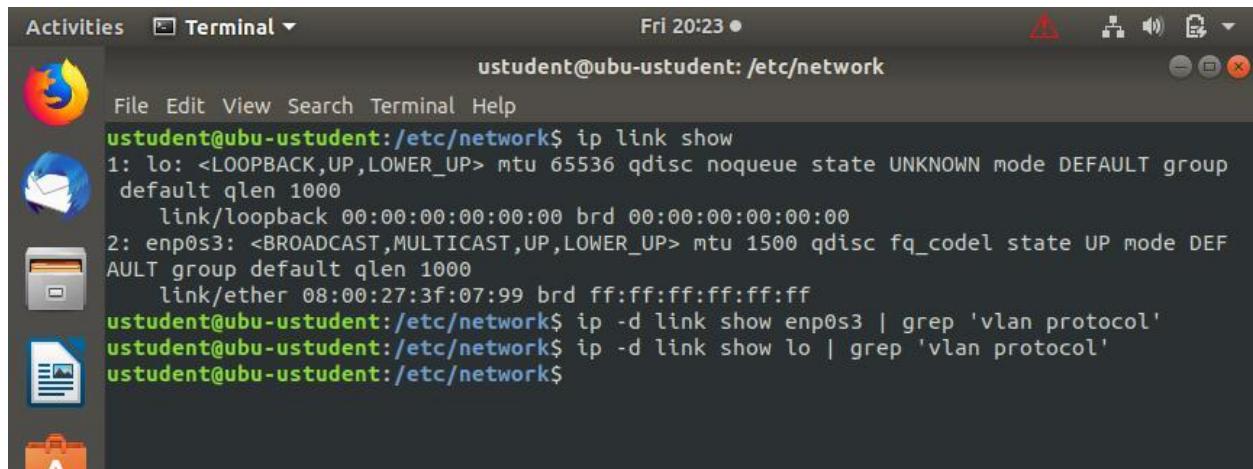
Provide recommendations to mitigate any threats related to open ports:

- 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



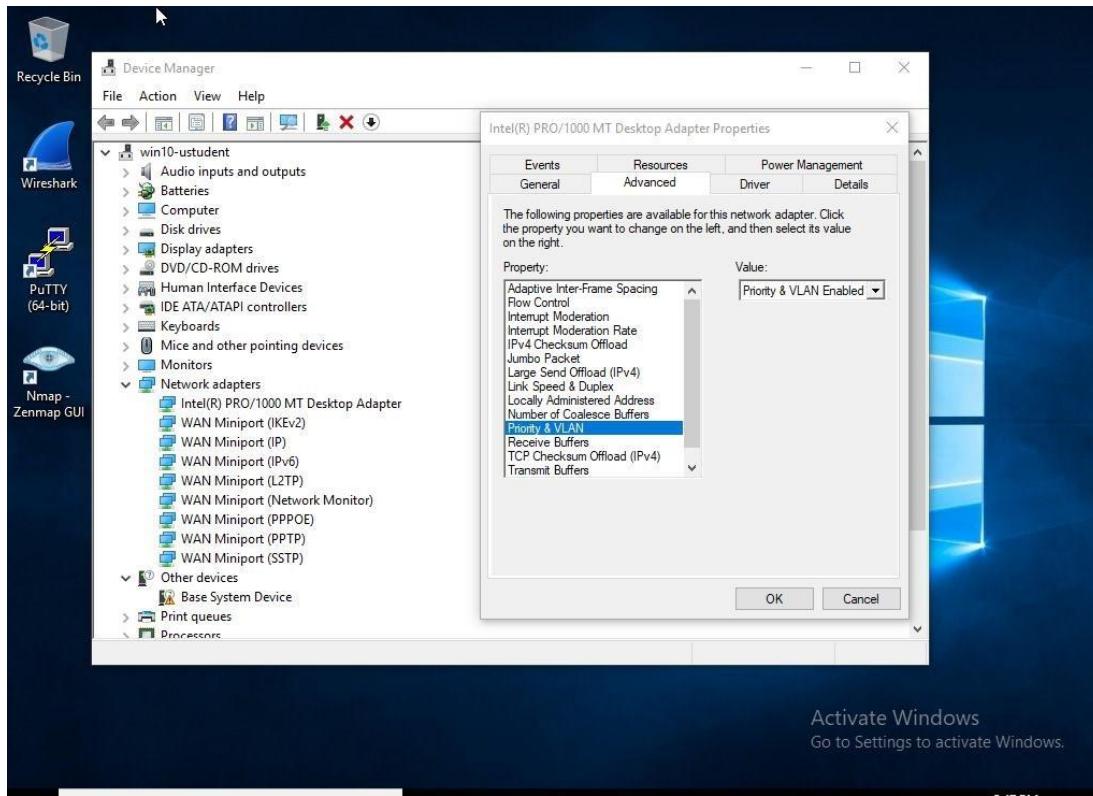
The screenshot shows a desktop environment with a terminal window open. The terminal window title is "Activities Terminal" and the command prompt is "ustudent@ubu-ustudent: /etc/network\$". The user runs the command "ip link show" which lists two interfaces: "lo" (loopback) and "enp0s3" (ethernet). Both interfaces are up and have their respective MTU values and queueing disciplines. The user then runs "ip -d link show enp0s3 | grep 'vlan protocol'" and "ip -d link show lo | grep 'vlan protocol'" to check if VLAN protocols are present on these interfaces. The output shows no VLAN configurations.

```
File Edit View Search Terminal Help
ustudent@ubu-ustudent:/etc/network$ ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode DEF AULT group default qlen 1000
    link/ether 08:00:27:3f:07:99 brd ff:ff:ff:ff:ff:ff
ustudent@ubu-ustudent:/etc/network$ ip -d link show enp0s3 | grep 'vlan protocol'
ustudent@ubu-ustudent:/etc/network$ ip -d link show lo | grep 'vlan protocol'
ustudent@ubu-ustudent:/etc/network$
```

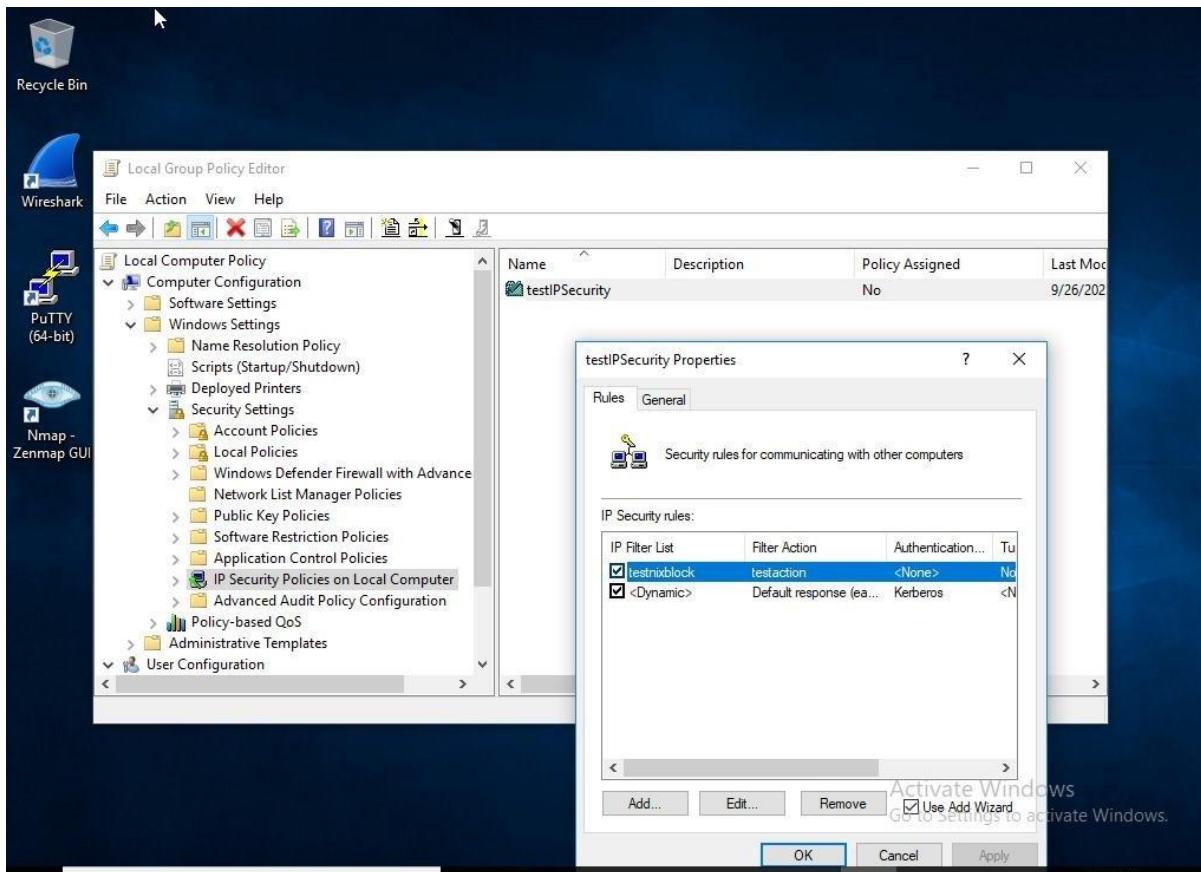
There is no VLANs configured in Ubuntu.

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.

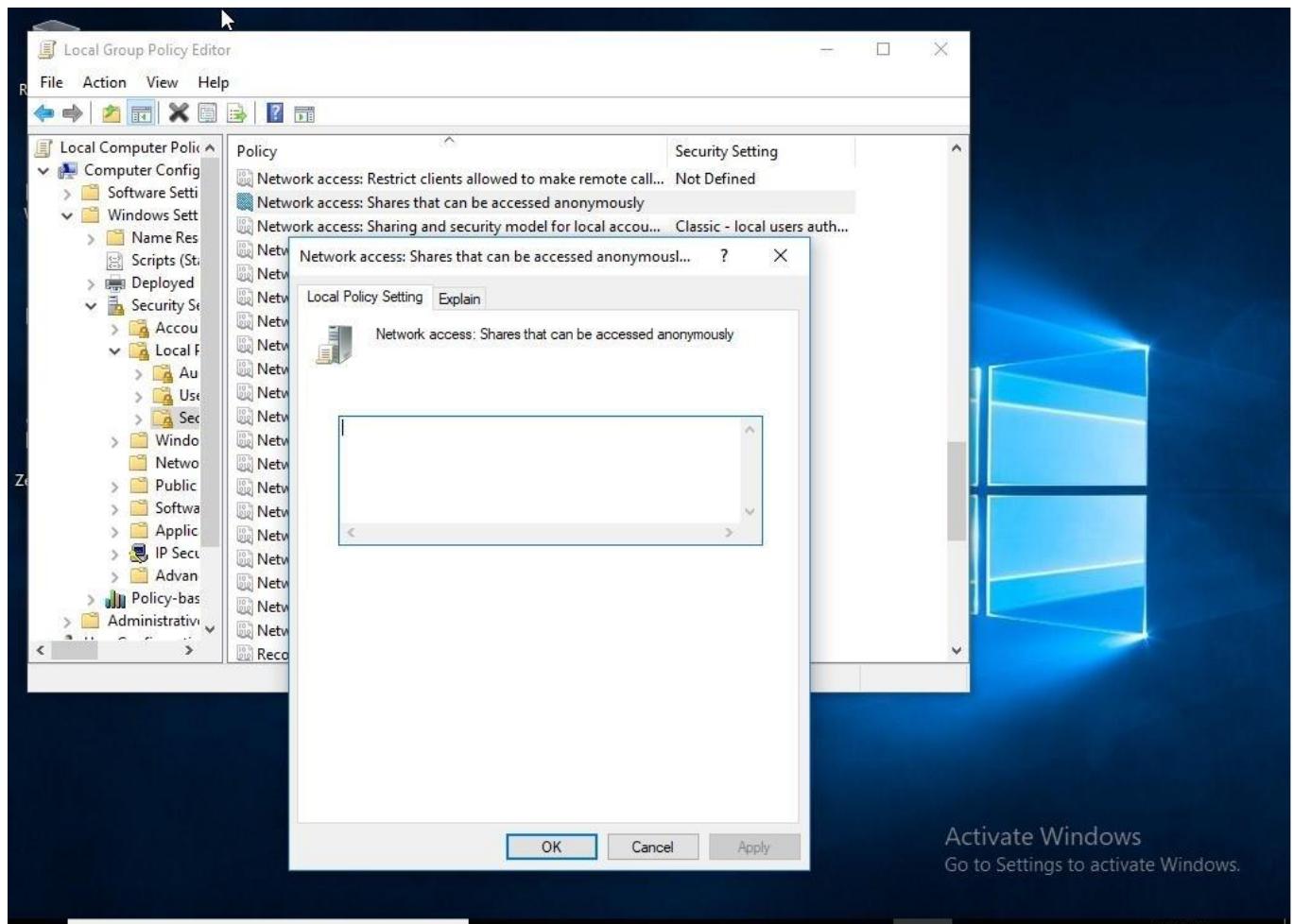
Windows 10 ENT



VLAN is Enabled in the interface.

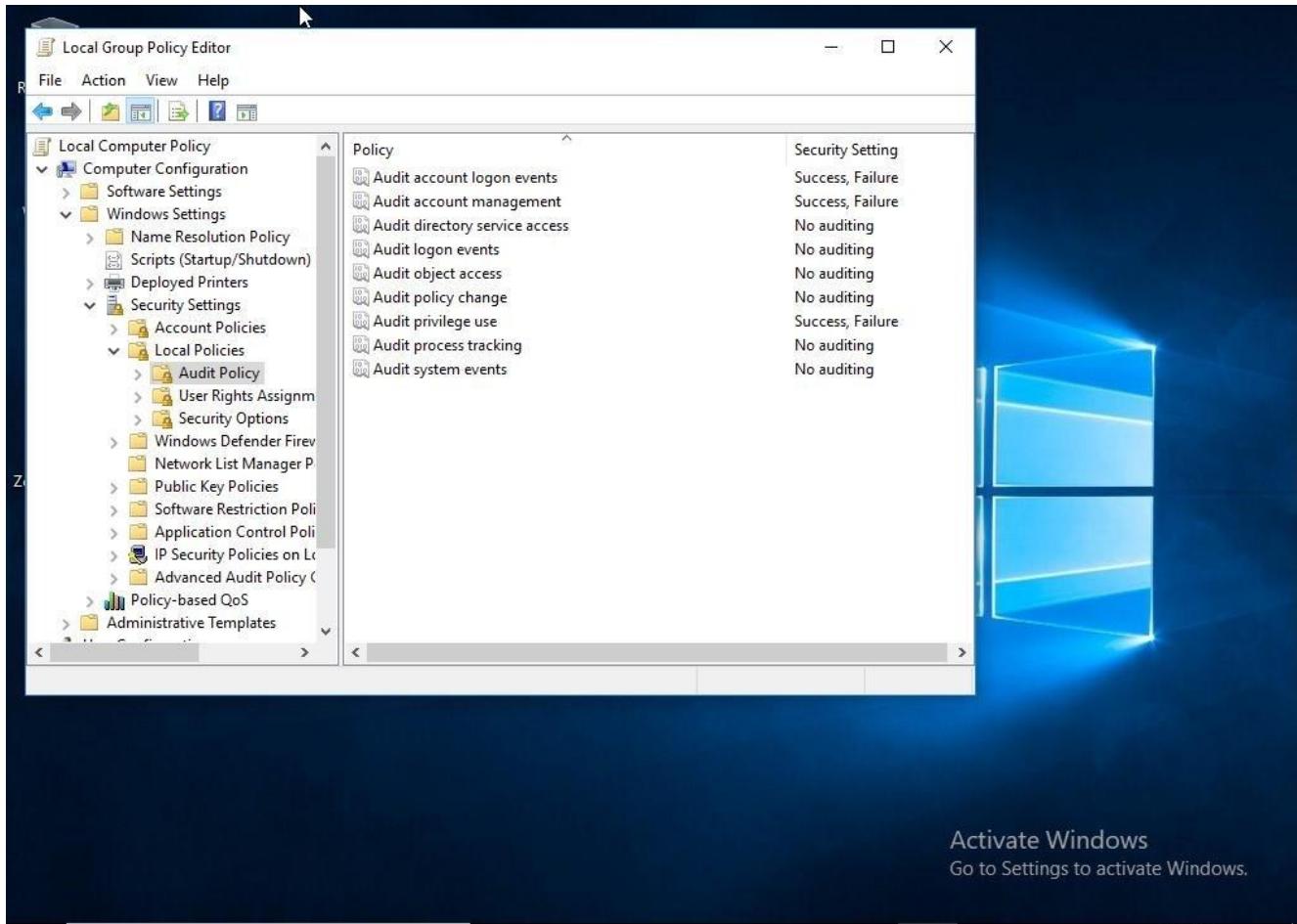


There is no Domain Isolation or IP Security Policies on Windows. Recommendation:
Domain Isolation can be achieved by using the IP Security. IP Security is important to block IP addresses of threat actors and thus mitigate the risk of getting compromised.



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 -tulpn
[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 ::::631                ::::*                LISTEN    6648/cupsd
tcp6    0      0 ::::445                ::::*                LISTEN    1308/smbd
udp     0      0 0.0.0.0:52686            0.0.0.0:*           LISTEN    919/snmpd
udp     38400   0 127.0.0.53:53            0.0.0.0:*           LISTEN    8867/systemd-resolv
udp     8704    0 0.0.0.0:68              0.0.0.0:*           LISTEN    12068/dhclient
udp     0      0 0.0.0.0:69              0.0.0.0:*           LISTEN    1260/in.tftpd
udp     0      0 0.0.0.0:631             0.0.0.0:*           LISTEN    6649/cups-browsed
udp     1536    0 10.0.2.255:137            0.0.0.0:*           LISTEN    1231/nmbd
udp     768     0 10.0.2.5:137             0.0.0.0:*           LISTEN    1231/nmbd
udp     1536    0 0.0.0.0:137             0.0.0.0:*           LISTEN    1231/nmbd
udp     41856   0 10.0.2.255:138            0.0.0.0:*           LISTEN    1231/nmbd
udp     0      0 10.0.2.5:138             0.0.0.0:*           LISTEN    1231/nmbd
udp     41856   0 0.0.0.0:138             0.0.0.0:*           LISTEN    1231/nmbd
udp     0      0 0.0.0.0:161             0.0.0.0:*           LISTEN    919/snmpd
udp     0      0 0.0.0.0:35539            0.0.0.0:*           LISTEN    676/avahi-daemon: r
udp     49856   0 0.0.0.0:5353             0.0.0.0:*           LISTEN    676/avahi-daemon: r
udp6    0      0 ::::38285               ::::*                LISTEN    676/avahi-daemon: r
udp6    0      0 ::::69                 ::::*                LISTEN    1260/in.tftpd
udp6    0      0 ::::1:161               ::::*                LISTEN    919/snmpd
udp6    36864   0 ::::5353               ::::*                LISTEN    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:

```
C:\Windows\system32>netstat -a

Active Connections

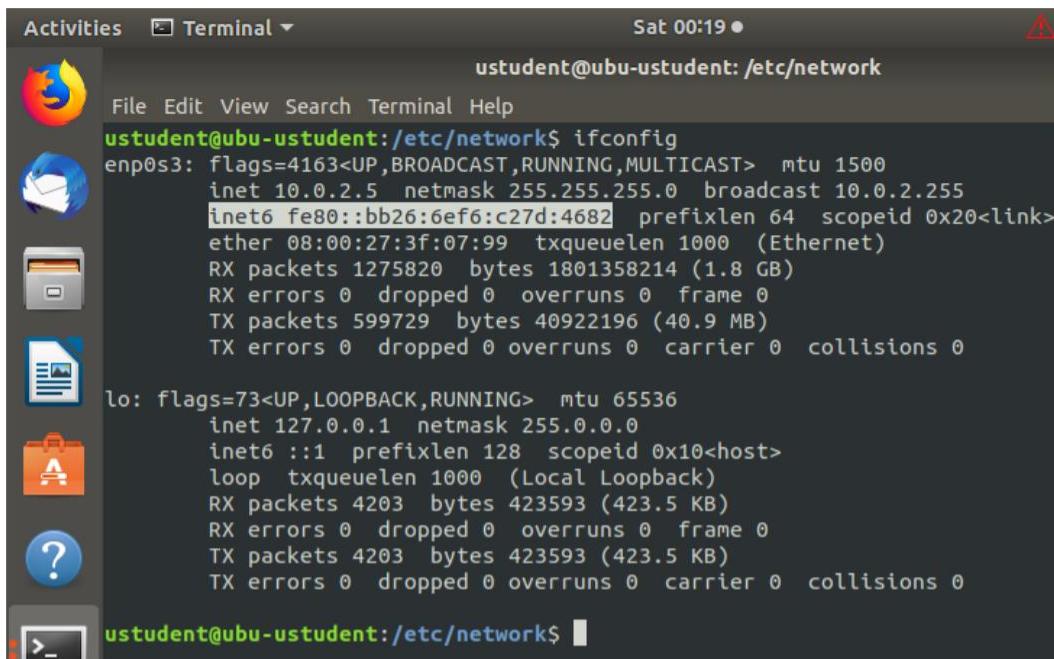
Pu (64) Proto Local Address          Foreign Address        State
(   TCP  0.0.0.0:7                win10-ustudent:0      LISTENING
(   TCP  0.0.0.0:9                win10-ustudent:0      LISTENING
(   TCP  0.0.0.0:13               win10-ustudent:0      LISTENING
(   TCP  0.0.0.0:17               win10-ustudent:0      LISTENING
(   TCP  0.0.0.0:19               win10-ustudent:0      LISTENING
(   TCP  0.0.0.0:80               win10-ustudent:0      LISTENING
Nm Zenm TCP  0.0.0.0:135              win10-ustudent:0      LISTENING
TCP  0.0.0.0:445               win10-ustudent:0      LISTENING
TCP  0.0.0.0:3389              win10-ustudent:0      LISTENING
TCP  0.0.0.0:5985              win10-ustudent:0      LISTENING
TCP  0.0.0.0:47001             win10-ustudent:0      LISTENING
TCP  0.0.0.0:49664             win10-ustudent:0      LISTENING
TCP  0.0.0.0:49665             win10-ustudent:0      LISTENING
TCP  0.0.0.0:49666             win10-ustudent:0      LISTENING
TCP  0.0.0.0:49667             win10-ustudent:0      LISTENING
TCP  0.0.0.0:49669             win10-ustudent:0      LISTENING
TCP  0.0.0.0:49670             win10-ustudent:0      LISTENING
TCP  0.0.0.0:49680             win10-ustudent:0      LISTENING
TCP  10.0.2.4:139              win10-ustudent:0      LISTENING
TCP  10.0.2.4:5040              win10-ustudent:0      LISTENING
TCP  10.0.2.4:63796             20.199.120.151:https ESTABLISHED
TCP  10.0.2.4:63797             a23-50-163-129:http TIME_WAIT
TCP  10.0.2.4:63798             204.79.197.220:https ESTABLISHED
TCP  10.0.2.4:63799             bingforbusiness:https ESTABLISHED
```

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:

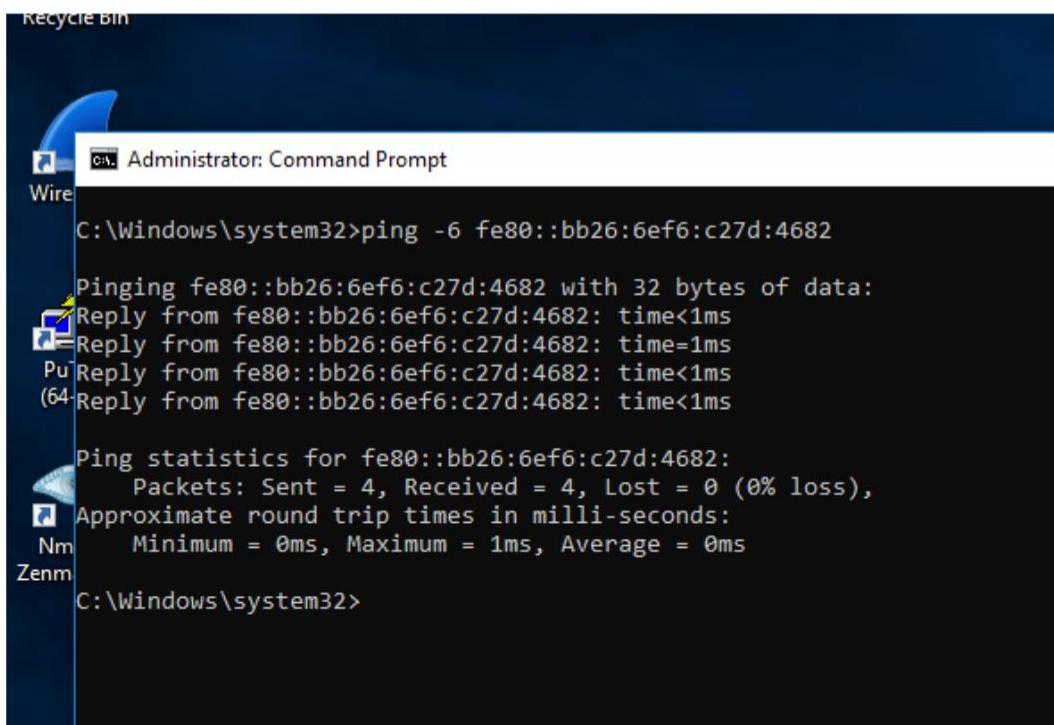


A screenshot of an Ubuntu desktop environment. A terminal window titled "ustudent@ubu-ustudent: /etc/network" is open, displaying the output of the "ifconfig" command. The output shows two network interfaces: "enp0s3" and "lo".

```
ustudent@ubu-ustudent: /etc/network$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 10.0.2.5 netmask 255.255.255.0 broadcast 10.0.2.255
        inet6 fe80::bb26:6ef6:c27d:4682 prefixlen 64 scopeid 0x20<link>
              ether 08:00:27:3f:07:99 txqueuelen 1000 (Ethernet)
              RX packets 1275820 bytes 1801358214 (1.8 GB)
              RX errors 0 dropped 0 overruns 0 frame 0
              TX packets 599729 bytes 40922196 (40.9 MB)
              TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
              loop txqueuelen 1000 (Local Loopback)
              RX packets 4203 bytes 423593 (423.5 KB)
              RX errors 0 dropped 0 overruns 0 frame 0
              TX packets 4203 bytes 423593 (423.5 KB)
              TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ustudent@ubu-ustudent: /etc/network$
```



A screenshot of a Windows desktop environment. A Command Prompt window titled "Administrator: Command Prompt" is open, showing the output of a "ping" command. The command is pinged to the IPv6 link-local address "fe80::bb26:6ef6:c27d:4682". The ping statistics show 100% loss.

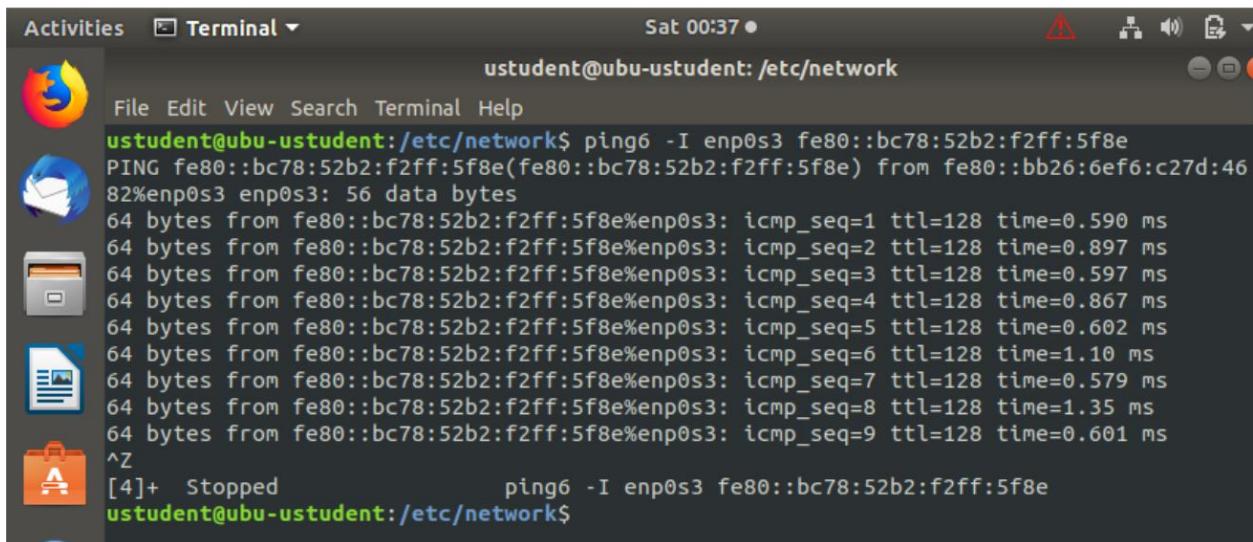
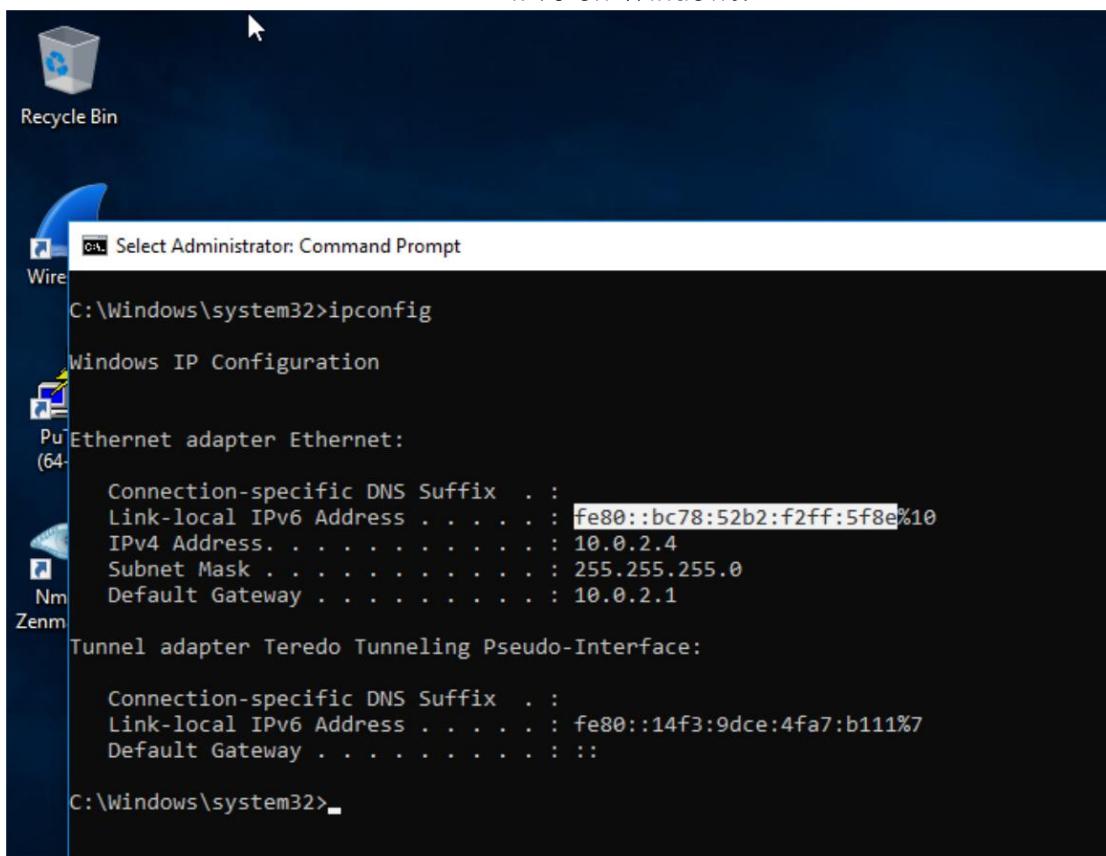
```
C:\Windows\system32>ping -6 fe80::bb26:6ef6:c27d:4682

Pinging fe80::bb26:6ef6:c27d:4682 with 32 bytes of data:
Reply from fe80::bb26:6ef6:c27d:4682: time<1ms
Reply from fe80::bb26:6ef6:c27d:4682: time=1ms
Reply from fe80::bb26:6ef6:c27d:4682: time<1ms
(4) Reply from fe80::bb26:6ef6:c27d:4682: time<1ms

Ping statistics for fe80::bb26:6ef6:c27d:4682:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Windows\system32>
```

IPv6 on Windows:



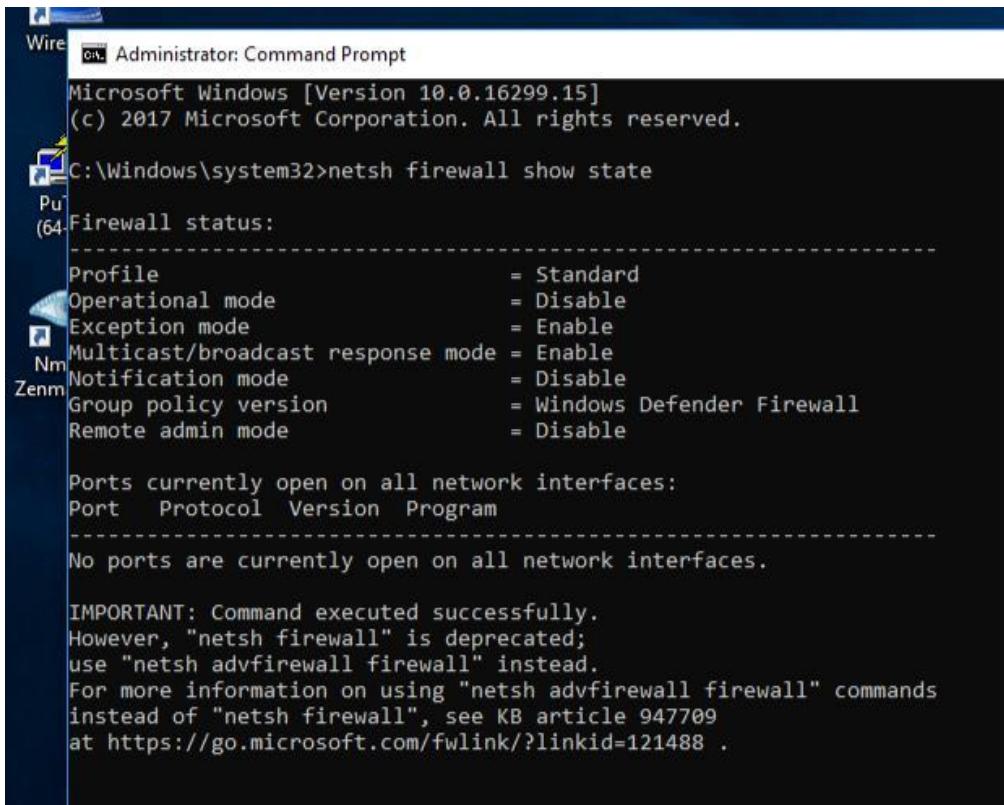
recommendation on whether IPv6 is needed?

- 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



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.16299.15]
(c) 2017 Microsoft Corporation. All rights reserved.

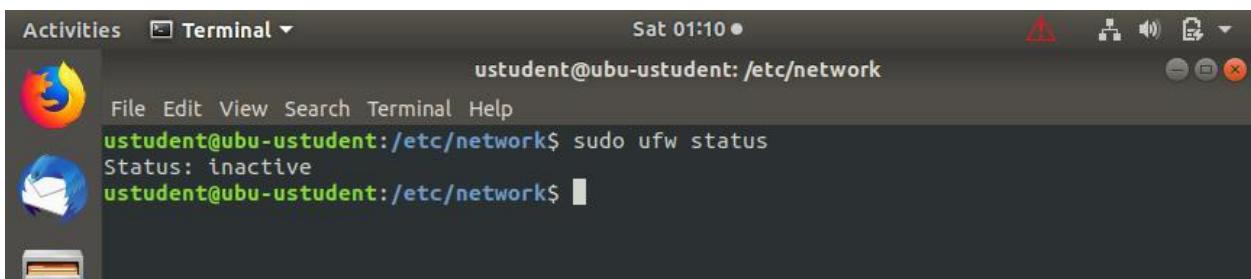
C:\Windows\system32>netsh firewall show state
Pu
(64)
Firewall status:
-----
Profile = Standard
Operational mode = Disable
Exception mode = Enable
Multicast/broadcast response mode = Enable
Notification mode = Disable
Group policy version = Windows Defender Firewall
Remote admin mode = Disable

Ports currently open on all network interfaces:
Port Protocol Version Program
-----
No ports are currently open on all network interfaces.

IMPORTANT: Command executed successfully.
However, "netsh firewall" is deprecated;
use "netsh advfirewall firewall" instead.
For more information on using "netsh advfirewall firewall" commands
instead of "netsh firewall", see KB article 947709
at https://go.microsoft.com/fwlink/?linkid=121488.
```

Firewall is Disabled on windows.

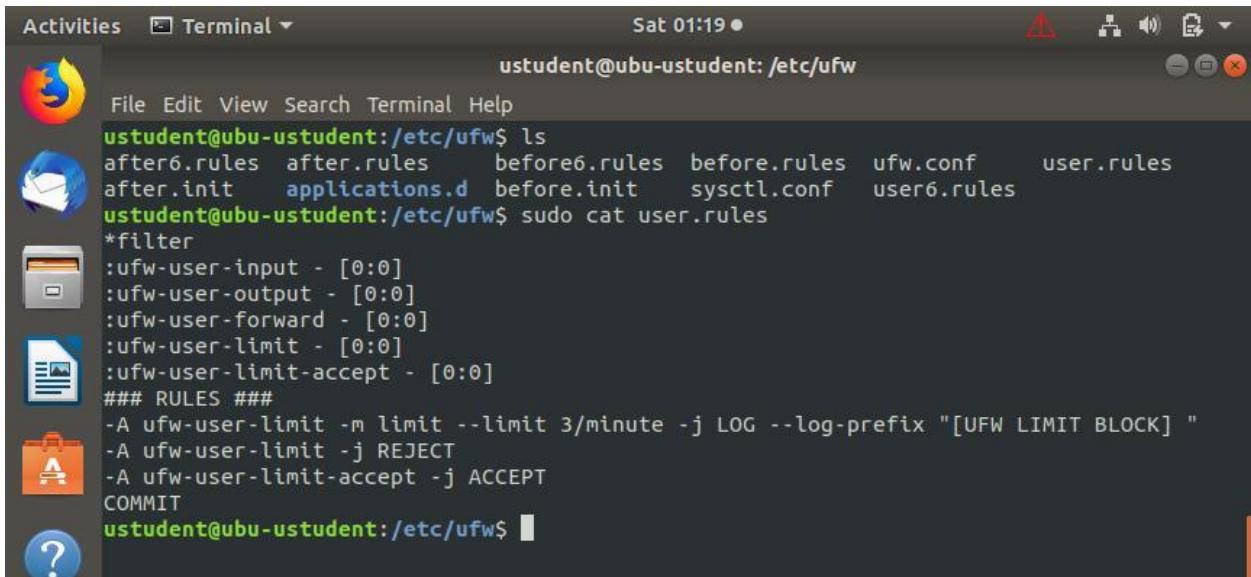
Ubuntu 18.04



A screenshot of the Ubuntu 18.04 desktop environment. At the top, there's a dock with icons for Activities, Terminal, Dash, Home, and Help. A system tray icon for a warning or error is visible. The main window is a terminal titled "Terminal" with the command "ustudent@ubu-ustudent: /etc/network". The output shows:

```
ustudent@ubu-ustudent: /etc/network$ sudo ufw status
Status: inactive
ustudent@ubu-ustudent: /etc/network$
```

UFW is inactive in Ubuntu.



A screenshot of the Ubuntu 18.04 desktop environment. The terminal window title is "Terminal" and the command is "ustudent@ubu-ustudent: /etc/ufw". The output shows the directory structure and a user-defined rules file:

```
ustudent@ubu-ustudent: /etc/ufw$ ls
after6.rules    after.rules      before6.rules   before.rules    ufw.conf      user.rules
after.init      applications.d  before.init     sysctl.conf   user6.rules
ustudent@ubu-ustudent: /etc/ufw$ sudo cat user.rules
*filter
:ufw-user-input - [0:0]
:ufw-user-output - [0:0]
:ufw-user-forward - [0:0]
:ufw-user-limit - [0:0]
:ufw-user-limit-accept - [0:0]
### RULES ###
-A ufw-user-limit -m limit --limit 3/minute -j LOG --log-prefix "[UFW LIMIT BLOCK] "
-A ufw-user-limit -j REJECT
-A ufw-user-limit-accept -j ACCEPT
COMMIT
ustudent@ubu-ustudent: /etc/ufw$
```

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.

bruteforce2.pcap

1:

```
.... .#...". .... .#...". .....!.....!...Ubuntu 18.04 LTS
ubu-ustudent login: ...uussttuuddeenntt
.
.
Password: 1234
.
Last login: Sun Sep 27 11:39:51 EDT 2020 from 10.0.2.4 on pts/1
```

2:

```
.... .#...". .... .#...". .....!.....!...Ubuntu 18.04 LTS
ubu-ustudent login: ...uussttuuddeenntt
.
.
Password: 1234
.
Last login: Sun Sep 27 23:06:49 EDT 2020 from 10.0.2.7 on pts/11
```

Based on the bruteforce2.pcap file, there are two successful connection. The TCP stream of the first one can be follow from 2455 packet, graphically the first read line. The communication starts with 10.0.2.7 IP sending a TCP SYN to 10.0.2.5. The login is confirmed in 2396 packet, when 10.0.2.5 return to 10.0.2.7 the following message: “Last login: Sun Sep 27 11:39:51 EDT 2020 from 10.0.2.4 on pts/1”. An enigmatic message to me, for the IP in the message is 10.0.2.4, and not the IP that is in communication with the server, which is 10.0.2.7. I checked throughout the file to verify if there were any packages for the condition: ip.src == 10.0.2.7 and eth.src != 08:00:27:4f:2f:6a, but there are not any. With this I would expect to find a time when 10.0.2.7 could use another MAC address to impersonate 10.0.2.4 IP, if that makes any sense.

Although there is this divergence that I cannot explain, based on the first evidence, I conclude that the source IP of the attacker is 10.0.2.7. The brute force attack was over Telnet protocol. And the credential compromised was ustudent/1234.

The TCP stream of the second one can be follow from 5285 packet, graphically the second read line. And it confirms my previous conclusion, without variation of the attacker’s IP in the server response.

It is highly recommended reset the password and use a more secure one. It is important implement password policies based on CIS 1.1 Password Policy. And it is highly recommended not use telnet protocol because it is an insecure protocol, data in transit is in plain-text, included passwords. As can be seen in the above print.

lateralmovement.pcap

Based on lateralmovement.pcap, the source IP of the attacker is 10.0.2.7. The attacker used SMB2 service through 445 port. And the attacker was able to access a sensitive file, as the following image:

..	SMB2	162 Close Response
.4	SMB2	242 Create Request File: payroll_20200927000951_1871.xls
.7	SMB2	210 Create Response File: payroll1_20200927000951_1871.xls
.4	SMB2	163 GetInfo Request FILE_INFO/SMB2_FILE_ALL_INFO File: payroll_20200927000951_1871.xls
.7	SMB2	234 GetInfo Response
.4	SMB2	146 Close Request File: payroll_20200927000951_1871.xls
.7	SMB2	182 Close Response
.4	TCP	60 39160 → 445 [ACK] Seq=3987 Ack=4868 Win=64128 Len=0
.4	SMB2	242 Create Request File: payroll1_20200927000951_1871.xls
.7	SMB2	210 Create Response File: payroll1_20200927000951_1871.xls
.4	TCP	60 39160 → 445 [ACK] Seq=4175 Ack=5024 Win=64128 Len=0
.4	SMB2	163 GetInfo Request FILE_INFO/SMB2_FILE_ALL_INFO File: payroll_20200927000951_1871.xls
.7	SMB2	234 GetInfo Response
.4	TCP	60 39160 → 445 [ACK] Seq=4284 Ack=5204 Win=64128 Len=0
.4	SMB2	146 Close Request File: payroll_20200927000951_1871.xls
.7	SMB2	182 Close Response
.4	TCP	60 39160 → 445 [ACK] Seq=4376 Ack=5332 Win=64128 Len=0
.4	SMB2	179 Create Request File:
.7	SMB2	210 Create Response File:
.4	TCP	60 39160 → 445 [ACK] Seq=4501 Ack=5488 Win=64128 Len=0
.4	SMB2	163 GetInfo Request FILE_INFO/SMB2_FILE_ALL_INFO File:
.7	SMB2	234 GetInfo Response
.4	TCP	60 39160 → 445 [ACK] Seq=4610 Ack=5668 Win=64128 Len=0
4	SMB2	146 Close Request File

My recommendation is hardening user credentials and reduce the shared folder, for with this weaker credential the attacker can access the directory tree of [C:/](#)

159 Session Setup Response
60 39160 → 445 [ACK] Seq=999 Ack=954 Win=64128 Len=0
172 Tree Connect Request Tree: \\win10-ustudent\IPC\$
138 Tree Connect Response
60 39160 → 445 [ACK] Seq=1117 Ack=1038 Win=64128 Len=0
222 Ioctl Request FSCTL_DFS_GET_REFERRALS, File: \\win10-ustudent\data
130 Ioctl Response, Error: STATUS_FS_DRIVER_REQUIRED
60 39160 → 445 [ACK] Seq=1285 Ack=1114 Win=64128 Len=0
126 Tree Disconnect Request
126 Tree Disconnect Response
60 39160 → 445 [ACK] Seq=1357 Ack=1186 Win=64128 Len=0
172 Tree Connect Request Tree: \\win10-ustudent\data
138 Tree Connect Response
60 39160 → 445 [ACK] Seq=1475 Ack=1270 Win=64128 Len=0
179 Create Request File:
210 Create Response File:
60 39160 → 445 [ACK] Seq=1600 Ack=1426 Win=64128 Len=0
163 GetInfo Request FS_INFO/FileFsAttributeInformation File:
150 GetInfo Response
60 39160 → 445 [ACK] Seq=1700 Ack=1500 Win=64128 Len=0



Windows Logs

5142 event id: Object Access: File Share

Are there any issues with Windows Share?

Security Number of events: 30,342					
Filtered: Log: Security; Source: ; Event ID: 5142, Number of events: 6					
Keywords	Date and Time	Source	Event ID	Task Category	
Audit Success	1/17/2023 12:53 AM	Microsoft Win...	5142	File Share	
Audit Success	1/17/2023 12:53 AM	Microsoft Win...	5142	File Share	
Audit Success	1/17/2023 12:53 AM	Microsoft Win...	5142	File Share	
Audit Success	1/17/2023 12:53 AM	Microsoft Win...	5142	File Share	
Audit Success	1/17/2023 12:53 AM	Microsoft Win...	5142	File Share	
Audit Success	1/17/2023 12:53 AM	Microsoft Win...	5142	File Share	

There is no entry in the event viewer related to 5140 event id. The above result is from my access in the host.

There are some event entry related to student credential, such as:

	Audit Success	9/29/2020 7:35:31 AM	Microsoft Win...	4688	Process Creation
	Audit Failure	9/29/2020 7:35:31 AM	Microsoft Win...	4673	Sensitive Privilege Use
	Audit Success	9/29/2020 7:35:31 AM	Microsoft Win...	5156	Filtering Platform Connection

Event 4673, Microsoft Windows security auditing.

General Details

A privileged service was called.

Subject:

Security ID: WIN10-USTUDENT\student
 Account Name: student
 Account Domain: WIN10-USTUDENT
 Logon ID: 0x14FA7

Service:

Server: Security
 Service Name: -

Process:

Process ID: 0x28c
 Process Name: C:\Windows\System32\svchost.exe

Service Request Information:

Privileges: SeTcbPrivilege

Log Name:	Security
Source:	Microsoft Windows security
Event ID:	4673
Level:	Information
User:	N/A
Logged:	9/29/2020 7:35:31 AM
Task Category:	Sensitive Privilege Use
Keywords:	Audit Failure
Computer:	win10-ustudent

Keywords	Date and Time	Source	Event ID	Task Category
	Audit Success	9/29/2020 7:35:31 AM	Microsoft Win...	4688 Process Creation
	Audit Failure	9/29/2020 7:35:31 AM	Microsoft Win...	4673 Sensitive Privilege Use
	Audit Success	9/29/2020 7:35:31 AM	Microsoft Win...	5156 Filtering Platform Connection

Event 4688, Microsoft Windows security auditing.

General Details

A new process has been created.

Creator Subject:

Security ID: SYSTEM
 Account Name: WIN10-USTUDENTS\$
 Account Domain: WORKGROUP
 Logon ID: 0x3E7

Target Subject:

Security ID: WIN10-USTUDENT\student
 Account Name: student
 Account Domain: WIN10-USTUDENT
 Logon ID: 0x14FA7

Process Information:

New Process ID: 0x1154
 New Process Name: C:\Windows\System32\backgroundTaskHost.exe
 Token Elevation Type: %%%1938
 Mandatory Label: Mandatory Label\Low Mandatory Level
 Creator Process ID: 0x28c
 Creator Process Name: C:\Windows\System32\svchost.exe
 Process Command Line:

Log Name:	Security
Source:	Microsoft Windows security
Event ID:	4688
Level:	Information
User:	N/A
Logged:	9/29/2020 7:35:31 AM
Task Category:	Process Creation
Keywords:	Audit Success
Computer:	win10-ustudent

Keywords	Date and Time	Source	Event ID	Task Category
Audit Failure	9/29/2020 7:35:35 AM	Microsoft Win...	4673	Sensitive Privilege Use
Audit Success	9/29/2020 7:35:34 AM	Microsoft Win...	5156	Filtering Platform Connection
Audit Success	9/29/2020 7:35:33 AM	Microsoft Win...	4689	Process Termination

Event 4673, Microsoft Windows security auditing.

General Details

A privileged service was called.

Subject:

Security ID: WIN10-USTUDENT\student
Account Name: student
Account Domain: WIN10-USTUDENT
Logon ID: 0x14FA7

Service:

Server: Security
Service Name: -

Process:

Process ID: 0xb0c
Process Name: C:\Windows\explorer.exe

Service Request Information:

Privileges: SeTcbPrivilege

Log Name: Security
Source: Microsoft Windows security Logged: 9/29/2020 7:35:35 AM
Event ID: 4673 Task Category: Sensitive Privilege Use
Level: Information Keywords: Audit Failure
User: N/A Computer: win10-ustudent

Audit Success	9/29/2020 7:35:35 AM	Microsoft Win...	4688	Process Creation
Audit Failure	9/29/2020 7:35:35 AM	Microsoft Win...	4673	Sensitive Privilege Use
Audit Success	9/29/2020 7:35:34 AM	Microsoft Win...	5156	Filtering Platform Connection

Event 4688, Microsoft Windows security auditing.

General Details

A new process has been created.

Creator Subject:

Security ID: SYSTEM
Account Name: WIN10-USTUDENTS
Account Domain: WORKGROUP
Logon ID: 0x3E7

Target Subject:

Security ID: WIN10-USTUDENT\student
Account Name: student
Account Domain: WIN10-USTUDENT
Logon ID: 0x14FA7

Process Information:

New Process ID: 0x12c0
New Process Name: C:\Windows\System32\RuntimeBroker.exe
Token Elevation Type: %&1938
Mandatory Label: Mandatory Label\Medium Mandatory Level
Creator Process ID: 0x28c
Creator Process Name: C:\Windows\System32\svchost.exe
Process Command Line:

Log Name: Security
Source: Microsoft Windows security Logged: 9/29/2020 7:35:35 AM
Event ID: 4688 Task Category: Process Creation
Level: Information Keywords: Audit Success
User: N/A Computer: win10-ustudent

The event id are 4688, 4673. 4688 logs when a program is started or a process is created.

4673 logs when the specified user exercised the user right specified in the privileges field.

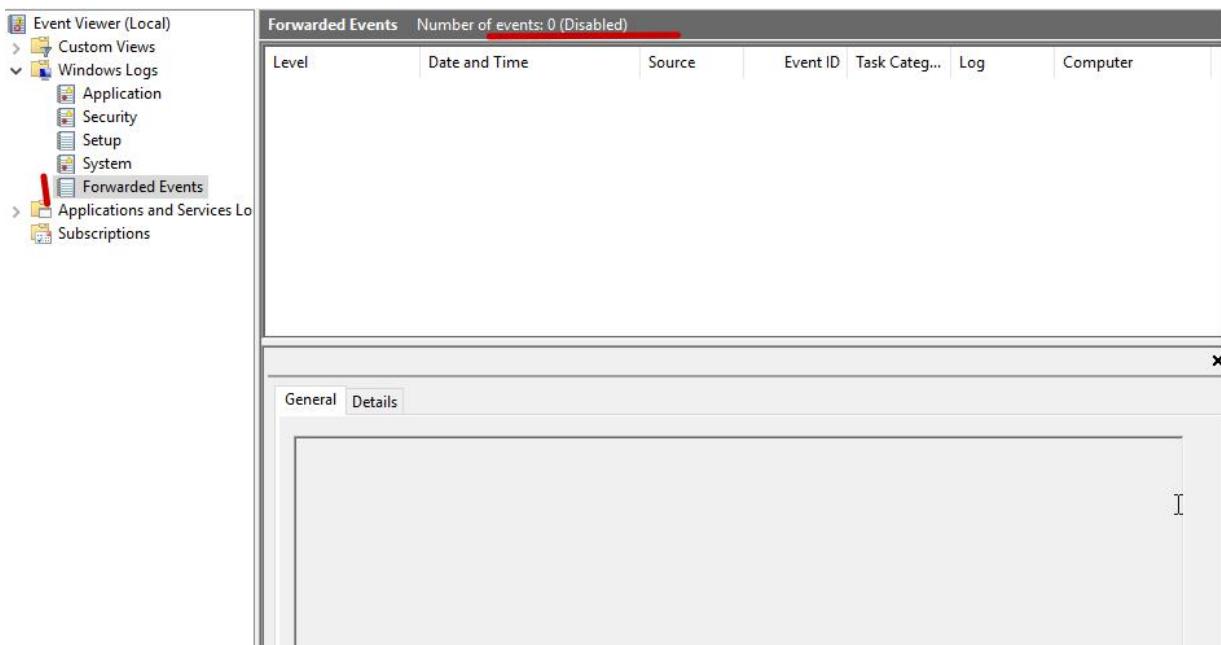
Additionally, there is a log that shows an inbound traffic from 10.0.2.15 through 3389 port, which is RDP.

Linux Log

```
ustudent@ubu-ustudent:/var/log/audit$ grep attacker audit.log
type=USER_AUTH msg=audit(1601236395.139:65): pid=5358 uid=0 auid=4294967295 ses=4294967295 msg='
op=PAM:authentication acct="attacker" exe="/usr/sbin/sshd" hostname=10.0.2.7 addr=10.0.2.7 termi
nal=ssh res=failed'
type=USER_AUTH msg=audit(1601236402.187:67): pid=5358 uid=0 auid=4294967295 ses=4294967295 msg='
op=PAM:authentication acct="attacker" exe="/usr/sbin/sshd" hostname=10.0.2.7 addr=10.0.2.7 termi
nal=ssh res=failed'
type=USER_AUTH msg=audit(1601236413.135:69): pid=5358 uid=0 auid=4294967295 ses=4294967295 msg='
op=PAM:authentication acct="attacker" exe="/usr/sbin/sshd" hostname=10.0.2.7 addr=10.0.2.7 termi
nal=ssh res=failed'
ustudent@ubu-ustudent:/var/log/audit$
```

SIEM LOGS

In Windows host there is no evidence that the logs are sending to a centralized location.



In the Linux host there is no evidence that the logs are sending to a centralized location.

```
ustudent@ubu-ustudent:/var/log/audit$ cat /etc/rsyslog.conf
# /etc/rsyslog.conf      Configuration file for rsyslog.
#
#                                     For more information see
#                                     /usr/share/doc/rsyslog-doc/html/rsyslog_conf.html
#
# Default logging rules can be found in /etc/rsyslog.d/50-default.conf

#####
#### MODULES #####
#####

module(load="imuxsock") # provides support for local system logging
#module(load="immark")  # provides --MARK-- message capability

# provides UDP syslog reception
#module(load="imudp")
#input(type="imudp" port="514")

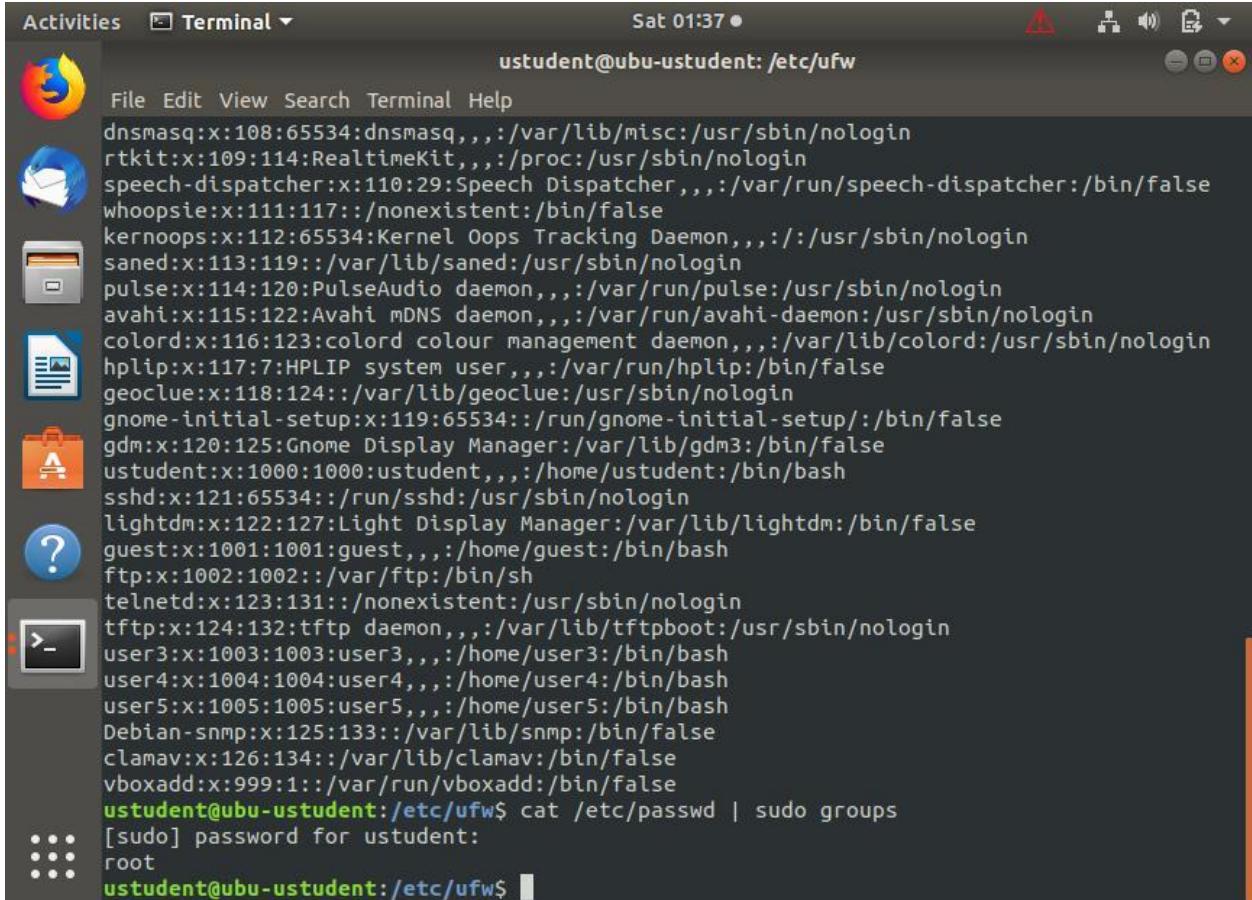
# provides TCP syslog reception
#module(load="imtcp")
#input(type="imtcp" port="514")

# provides kernel logging support and enable non-kernel klog messages
module(load="imklog" permitnonkernelfacility="on")
```

Identify and mitigate user privilege Issues.

Which users have high privileges:

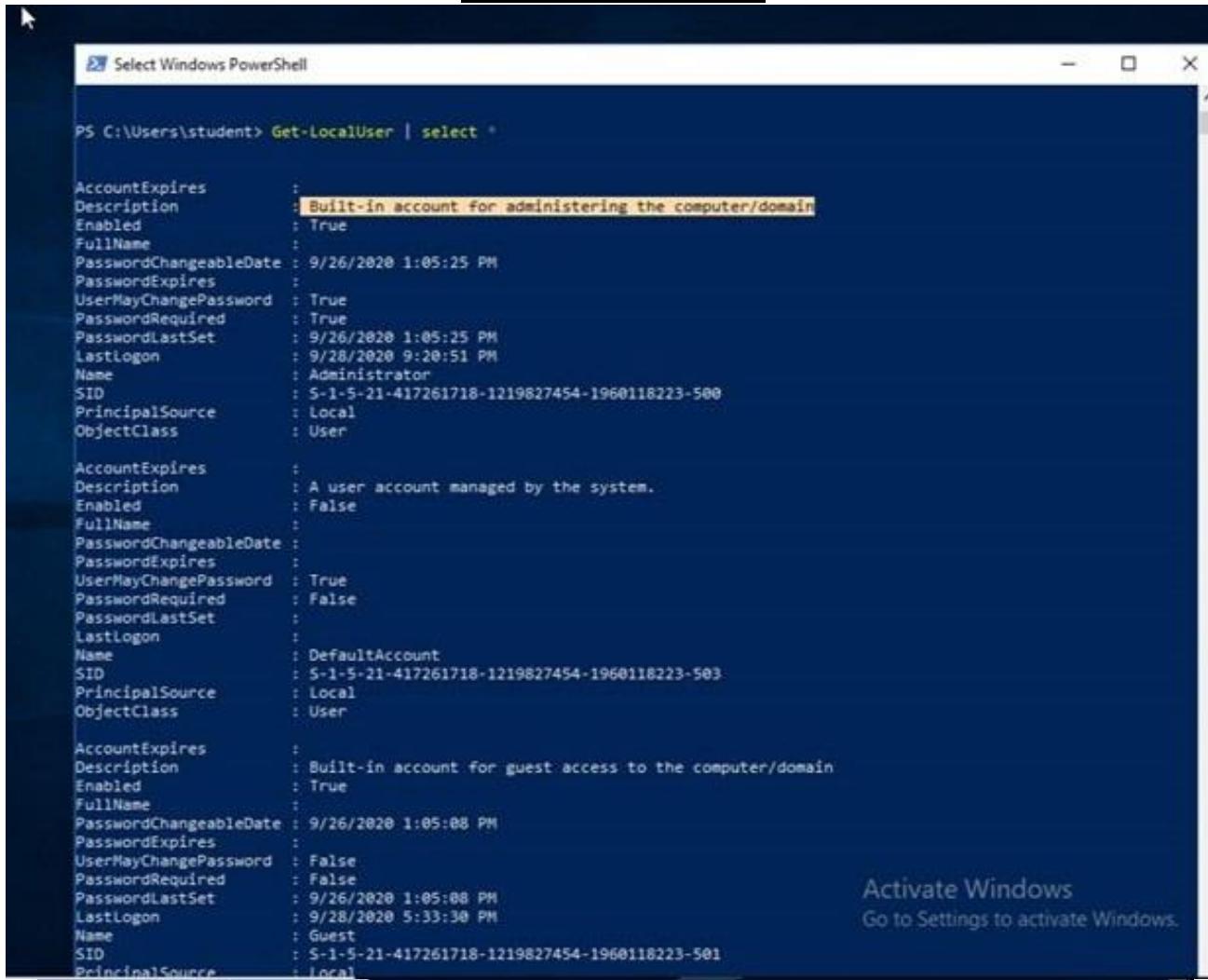
Ubuntu 18.04



```
Activities Terminal Sat 01:37 ● uststudent@ubu-ustudent: /etc/ufw
File Edit View Search Terminal Help
dnsmasq:x:108:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
rtkit:x:109:114:RealtimeKit,,,:/proc:/usr/sbin/nologin
speech-dispatcher:x:110:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
whoopsie:x:111:117::/nonexistent:/bin/false
kernoops:x:112:65534:Kernel Oops Tracking Daemon,,,:/usr/sbin/nologin
saned:x:113:119::/var/lib/saned:/usr/sbin/nologin
pulse:x:114:120:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
avahi:x:115:122:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
colord:x:116:123:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
hplip:x:117:7:HPLIP system user,,,:/var/run/hplip:/bin/false
geoclue:x:118:124::/var/lib/geoclue:/usr/sbin/nologin
gnome-initial-setup:x:119:65534::/run/gnome-initial-setup:/bin/false
gdm:x:120:125:Gnome Display Manager:/var/lib/gdm3:/bin/false
ustudent:x:1000:1000:ustudent,,,:/home/ustudent:/bin/bash
sshd:x:121:65534::/run/sshd:/usr/sbin/nologin
lightdm:x:122:127:Light Display Manager:/var/lib/lightdm:/bin/false
guest:x:1001:1001:guest,,,:/home/guest:/bin/bash
ftp:x:1002:1002::/var/ftp:/bin/sh
telnetd:x:123:131::/nonexistent:/usr/sbin/nologin
tftp:x:124:132:tftp daemon,,,:/var/lib/tftpboot:/usr/sbin/nologin
user3:x:1003:1003:user3,,,:/home/user3:/bin/bash
user4:x:1004:1004:user4,,,:/home/user4:/bin/bash
user5:x:1005:1005:user5,,,:/home/user5:/bin/bash
Debian-snmp:x:125:133::/var/lib/snmp:/bin/false
clamav:x:126:134::/var/lib/clamav:/bin/false
vboxadd:x:999:1::/var/run/vboxadd:/bin/false
ustudent@ubu-ustudent:/etc/ufw$ cat /etc/passwd | sudo groups
[sudo] password for uststudent:
root
ustudent@ubu-ustudent:/etc/ufw$
```

user: root, has the highest privilege.

Windows 10 ENT



The screenshot shows a Windows PowerShell window titled "Select Windows PowerShell" running on a Windows 10 Enterprise (ENT) system. The command "Get-LocalUser | select *" is run, displaying the properties of local users. The output shows three users: "Administrator" (Enabled: True, Description: "Built-in account for administering the computer/domain"), "SYSTEM" (Enabled: False, Description: "A user account managed by the system."), and "Guest" (Enabled: True, Description: "Built-in account for guest access to the computer/domain"). The "Administrator" account has a LastLogon of 9/28/2020 9:20:51 PM and a SID of S-1-5-21-417261718-1219827454-1960118223-500. The "SYSTEM" account has a LastLogon of 9/26/2020 1:05:25 PM and a SID of S-1-5-21-417261718-1219827454-1960118223-503. The "Guest" account has a LastLogon of 9/26/2020 1:05:08 PM and a SID of S-1-5-21-417261718-1219827454-1960118223-501. A watermark for "Activate Windows" and "Go to Settings to activate Windows." is visible in the bottom right corner of the window.

```
PS C:\Users\student> Get-LocalUser | select *

AccountExpires      :
Description         : Built-in account for administering the computer/domain
Enabled             : True
FullName            :
PasswordChangeableDate : 9/26/2020 1:05:25 PM
PasswordExpires     :
UserMayChangePassword : True
PasswordRequired    : True
PasswordLastSet     : 9/26/2020 1:05:25 PM
LastLogon           : 9/28/2020 9:20:51 PM
Name                : Administrator
SID                 : S-1-5-21-417261718-1219827454-1960118223-500
PrincipalSource     : Local
ObjectClass         : User

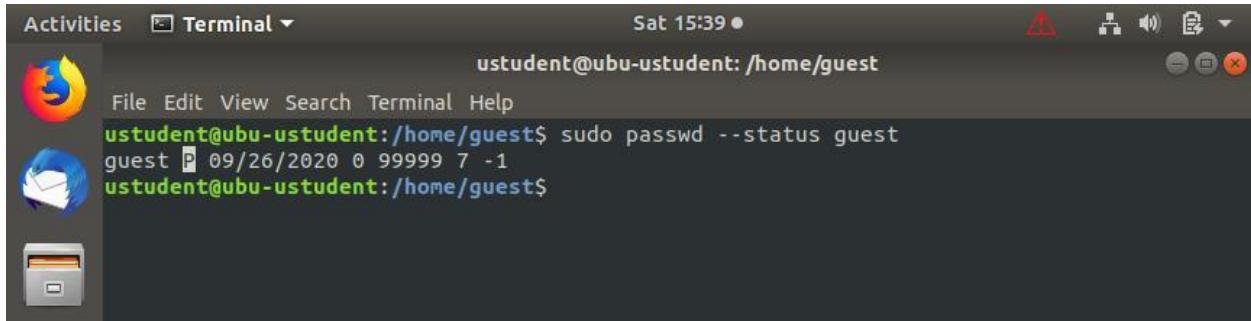
AccountExpires      :
Description         : A user account managed by the system.
Enabled             : False
FullName            :
PasswordChangeableDate :
PasswordExpires     :
UserMayChangePassword : True
PasswordRequired    : False
PasswordLastSet     :
LastLogon           :
Name                : SYSTEM
SID                 : S-1-5-21-417261718-1219827454-1960118223-503
PrincipalSource     : Local
ObjectClass         : User

AccountExpires      :
Description         : Built-in account for guest access to the computer/domain
Enabled             : True
FullName            :
PasswordChangeableDate : 9/26/2020 1:05:08 PM
PasswordExpires     :
UserMayChangePassword : False
PasswordRequired    : False
PasswordLastSet     : 9/26/2020 1:05:08 PM
LastLogon           : 9/28/2020 5:33:30 PM
Name                : Guest
SID                 : S-1-5-21-417261718-1219827454-1960118223-501
PrincipalSource     : Local
```

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

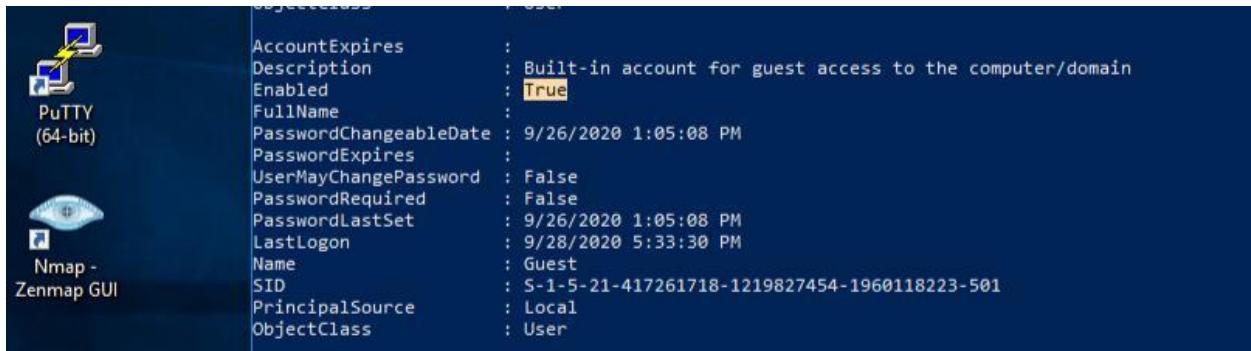


A screenshot of an Ubuntu 18.04 desktop environment. The terminal window shows the command `sudo passwd --status guest` being run, with the output indicating the guest account is enabled (status P) and not locked (status 0).

```
ustudent@ubu-ustudent: /home/guest
ustudent@ubu-ubtudent:/home/guest$ sudo passwd --status guest
guest P 09/26/2020 0 99999 7 -1
ustudent@ubu-ubtudent:/home/guest$
```

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



A screenshot of a Windows 10 desktop environment showing a Windows PowerShell window. The command `Get-LocalUser -Name Guest | Format-List` is run, displaying the properties of the Guest account. The Enabled property is shown as True, indicating the account is enabled.

```
ObjectClass : User
AccountExpires : 
Description : Built-in account for guest access to the computer/domain
Enabled : True
FullName : 
PasswordChangeableDate : 9/26/2020 1:05:08 PM
PasswordExpires : 
UserMayChangePassword : False
PasswordRequired : False
PasswordLastSet : 9/26/2020 1:05:08 PM
LastLogon : 9/28/2020 5:33:30 PM
Name : Guest
SID : S-1-5-21-417261718-1219827454-1960118223-501
PrincipalSource : Local
ObjectClass : User
```

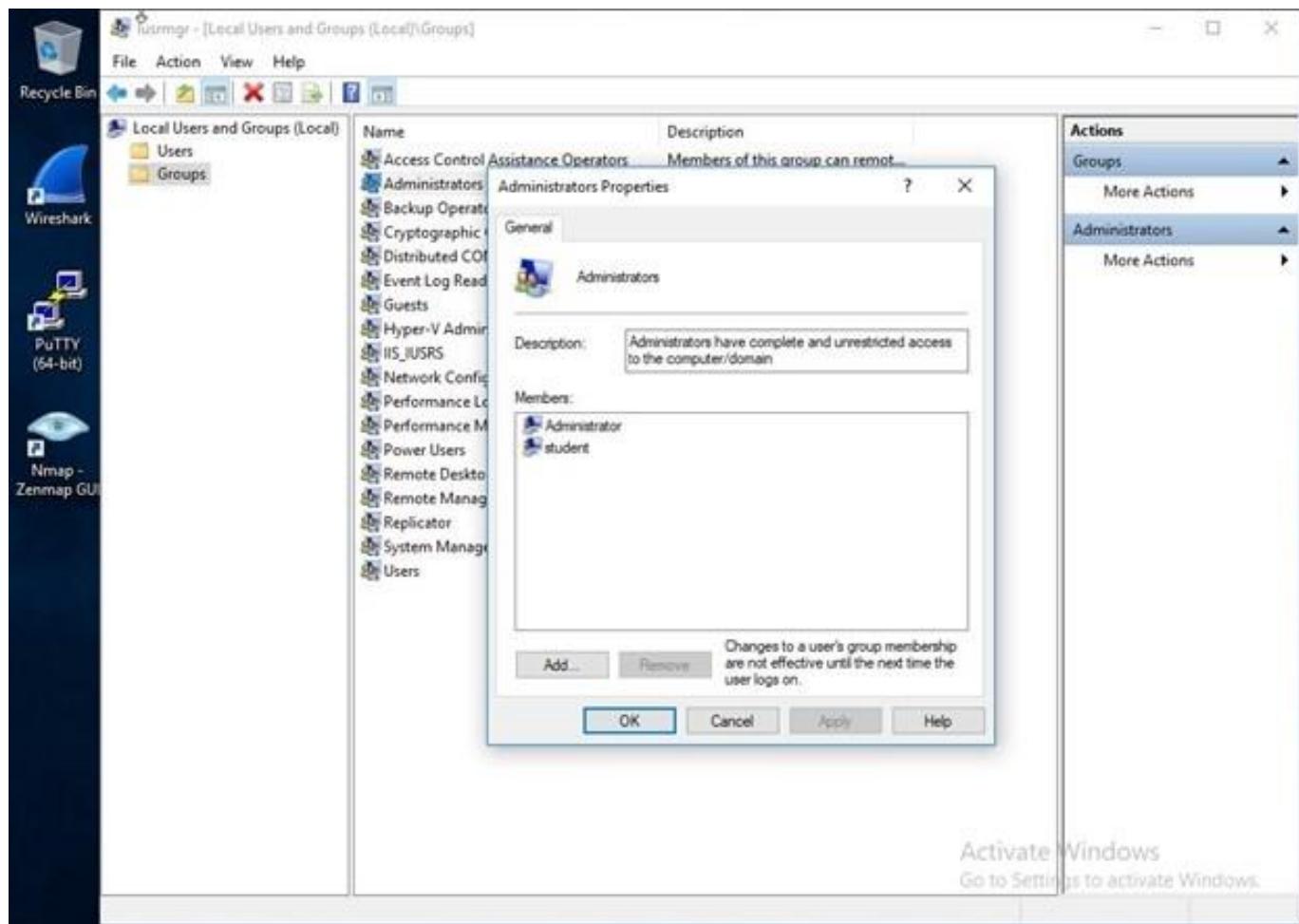
The guest account is enabled in Windows.

Is the guest account allowed to sudo in Linux?

```
Activities Terminal Sat 15:43 ●
ustudent@ubu-ustudent: /home/guest
File Edit View Search Terminal Help
ustudent@ubu-ustudent:/home/guest$ sudo -l -U guest
User guest is not allowed to run sudo on ubu-ustudent.
ustudent@ubu-ustudent:/home/guest$
```

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

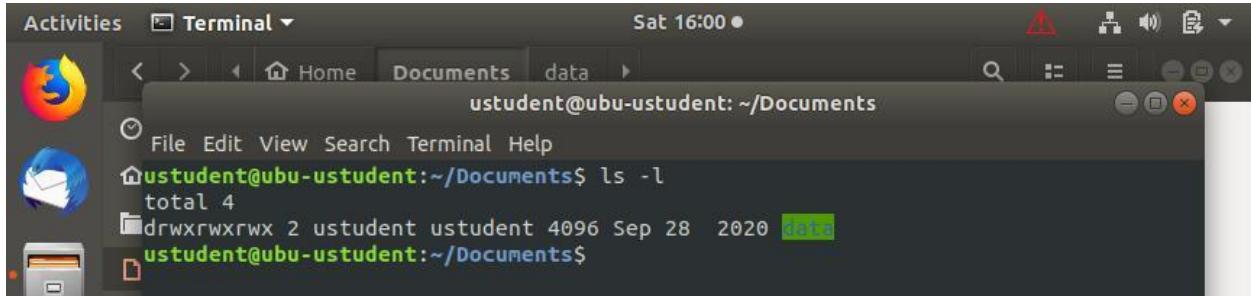
Is the guest account allowed to run as administrator in Windows?



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

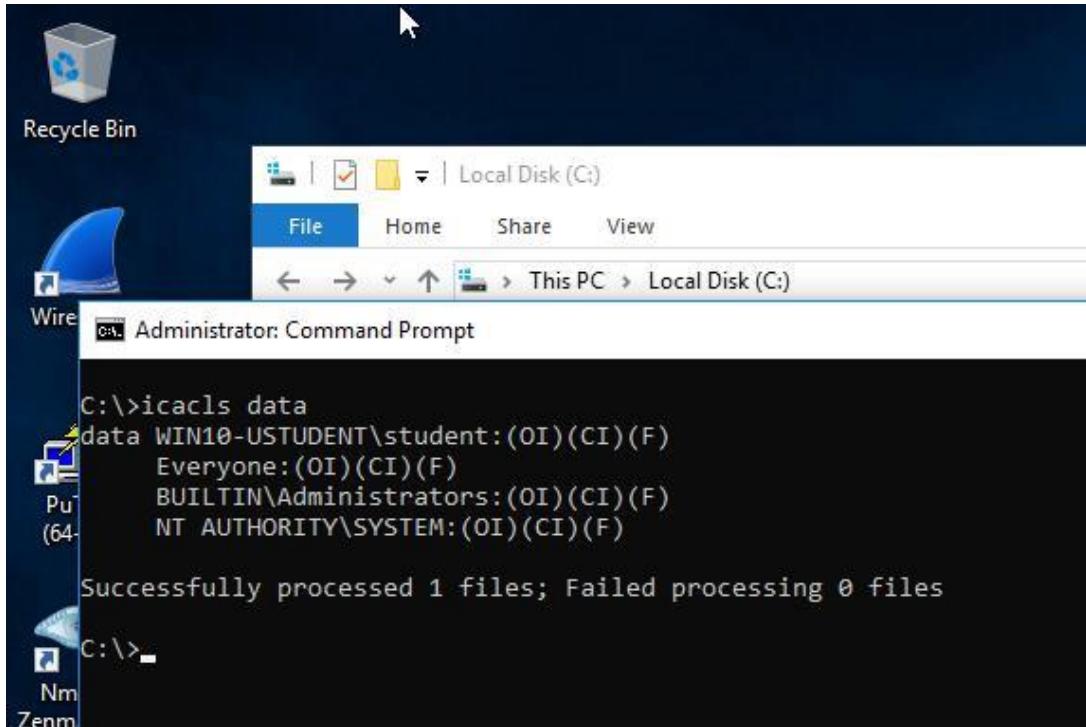


A screenshot of an Ubuntu 18.04 desktop environment. The terminal window shows the command `ls -l` being run in the directory `~/Documents`. The output shows a folder named "data" with permissions `drwxrwxrwx`, which is considered excessive as it allows all users to modify it.

```
ustudent@ubu-ustudent: ~/Documents$ ls -l
total 4
drwxrwxrwx 2 ustudent ustudent 4096 Sep 28 2020 data
ustudent@ubu-ustudent: ~/Documents$
```

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

Windows 10 ENT



A screenshot of a Windows 10 desktop environment. A Command Prompt window titled "Administrator: Command Prompt" is open, showing the output of the `icacls data` command. The output lists several users with full control (F) permissions on the "data" folder, including "Everyone", "BUILTIN\Administrators", and "NT AUTHORITY\SYSTEM".

```
C:\>icacls data
data WIN10-USSTUDENT\student:(OI)(CI)(F)
      Everyone:(OI)(CI)(F)
      BUILTIN\Administrators:(OI)(CI)(F)
      NT AUTHORITY\SYSTEM:(OI)(CI)(F)

      Successfully processed 1 files; Failed processing 0 files

C:\>
```

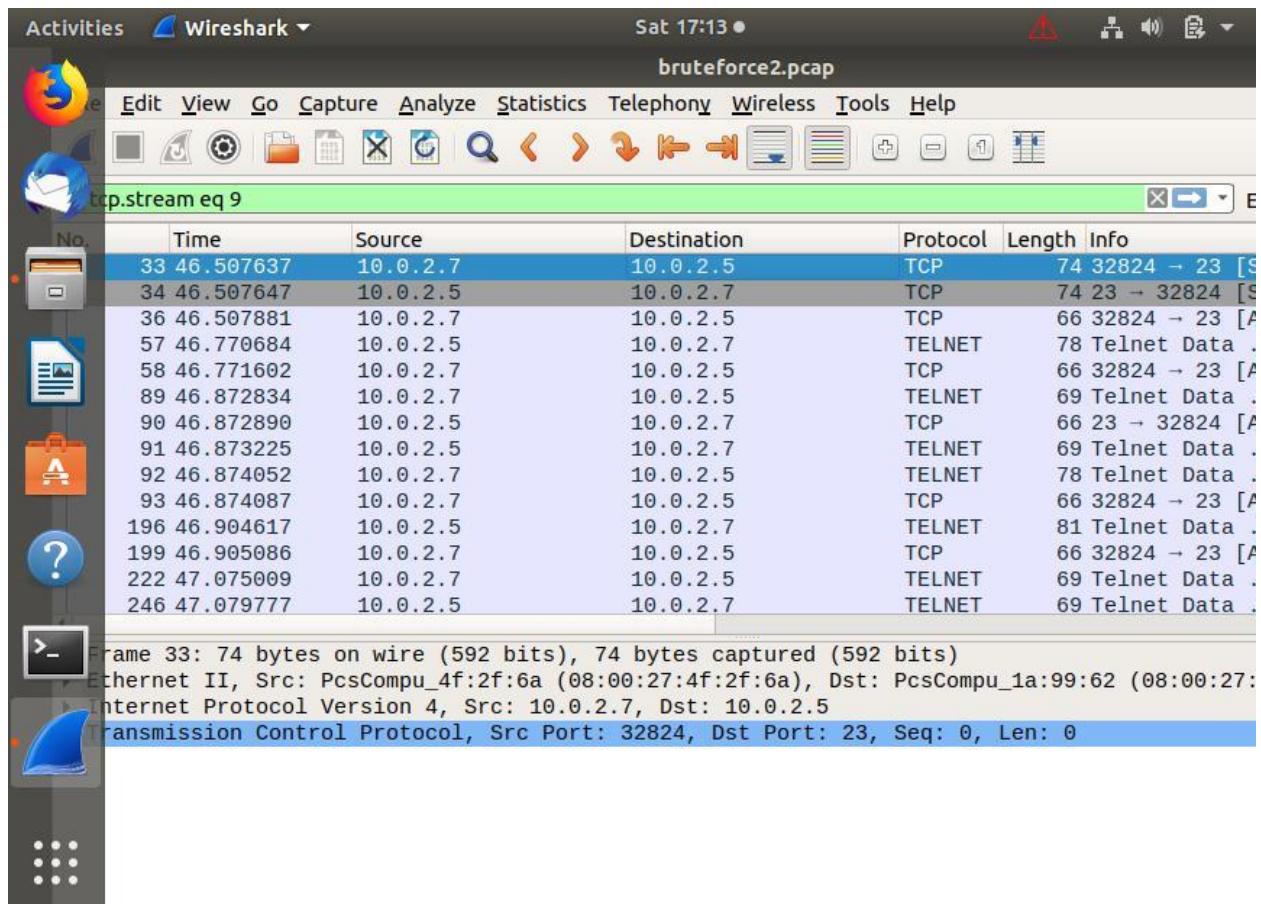
Yes, there are excessive permission on the data folder in Windows.

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

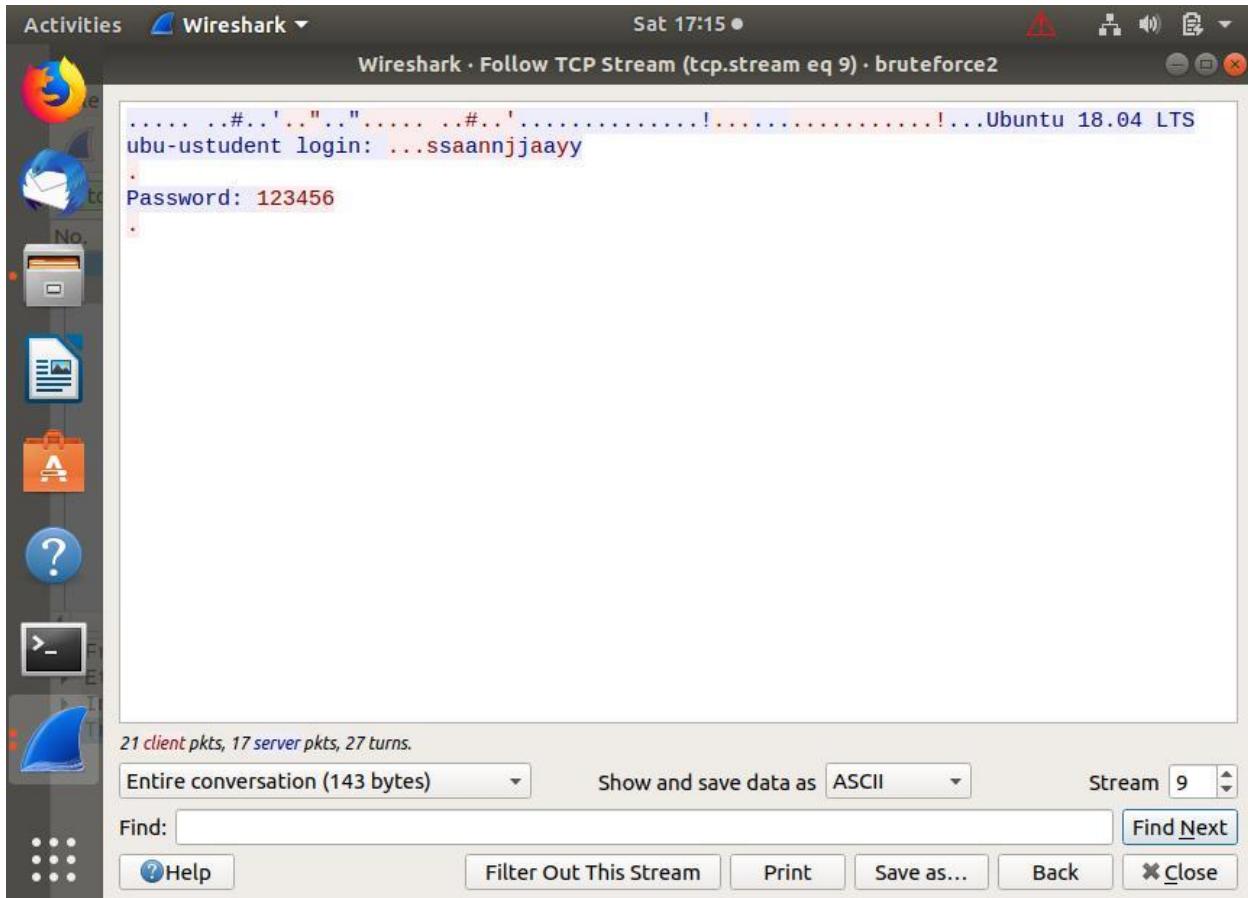
Use Wireshark or tcpdump to perform traffic inspection and investigation.

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)?

The screenshot shows the Wireshark interface with a capture file named "lateralmovement.pcap". The packet list pane displays SMB traffic between two hosts:

No.	Time	Source	Destination	Protocol	Length	Info
23	42.917137	10.0.2.7	10.0.2.6	SMB	154	Negotiate Protocol Request
24	42.920943	10.0.2.6	10.0.2.7	SMB	197	Negotiate Protocol Response
26	42.923328	10.0.2.7	10.0.2.6	SMB	213	Session Setup AndX Request, NTLMSSP_NEGOTIATE
27	42.923512	10.0.2.6	10.0.2.7	SMB	411	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_LOGON_FAILURE
29	42.926886	10.0.2.7	10.0.2.6	SMB	478	Session Setup AndX Request, NTLMSSP_AUTH, User: .\Administrator, Domain: .\, Workstation: .\PcsCompu_f9:6d:c9
30	42.927868	10.0.2.6	10.0.2.7	SMB	105	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
32	42.929154	10.0.2.7	10.0.2.6	SMB	169	Session Setup AndX Request, User: .\Administrator, Domain: .\, Workstation: .\PcsCompu_f9:6d:c9
33	42.929283	10.0.2.6	10.0.2.7	SMB	191	Session Setup AndX Response
35	42.930762	10.0.2.7	10.0.2.6	SMB	136	Tree Connect AndX Request, Path: \\10.0.2.6\IPC\$

The details pane shows the following analysis for the selected SMB request (Frame 23):

```
> Frame 23: 116 bytes on wire (928 bits), 116 bytes captured (928 bits)
> Ethernet II, Src: PcsCompu_f9:6d:c9 (08:00:27:f9:6d:c9), Dst: PcsCompu_e6:71:53 (08:00:27:e6:71:53)
> Internet Protocol Version 4, Src: 10.0.2.6, Dst: 10.0.2.4
> Transmission Control Protocol, Src Port: 49165, Dst Port: 445, Seq: 1, Ack: 1, Len: 62
> NetBIOS Session Service
> SMB (Server Message Block Protocol)
```

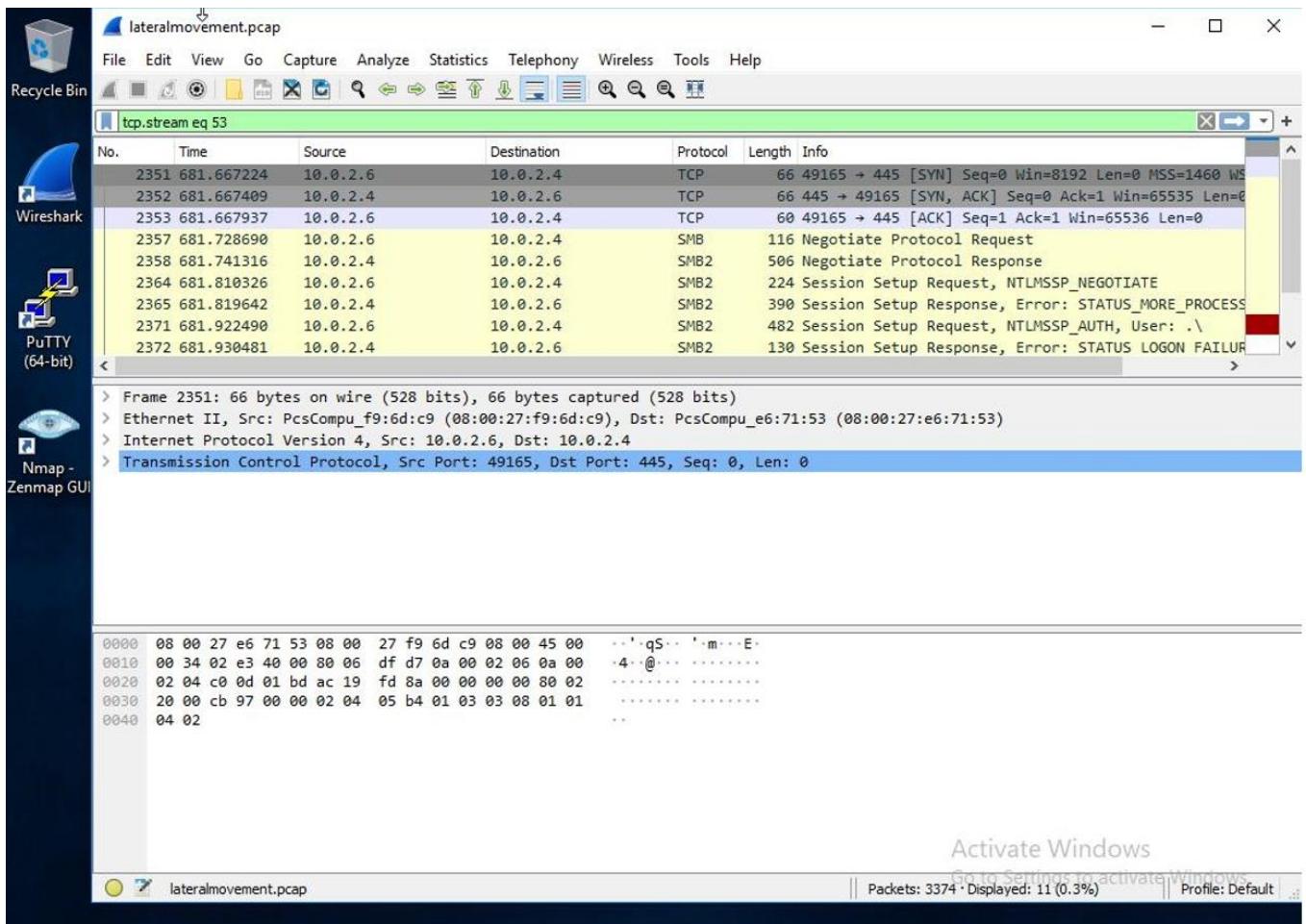
The bytes pane shows the raw hex and ASCII data for the selected SMB request:

Hex	ASCII
0000 08 00 27 e6 71 53 08 00 27 f9 6d c9 08 00 45 00	..'qs.. 'm...E.
0010 00 66 02 e6 40 00 80 06 df a2 0a 00 02 06 0a 00	f-@.....
0020 02 04 c0 0d 01 bd ac 19 fd 8b 4c 6f 28 cd 50 18Lo(.P-
0030 01 00 ae 7f 00 00 00 00 00 3a ff 53 4d 42 72 00:SMBr..
0040 00 00 00 18 01 68 00 00 00 00 00 00 00 00 00 00h.....
0050 00 00 00 00 00 00 00 00 00 00 17 00 02 4e 54NT
0060 20 4c 4d 20 30 2e 31 32 00 02 53 4d 42 20 32 2e	LM 0.12 ..SMB 2.
0070 30 30 32 00	002.

At the bottom, the status bar indicates: "SMB (Server Message Block Protocol): Protocol", "Packets: 3374 · Displayed: 101 (3.0%)", and "Profile: Default".

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

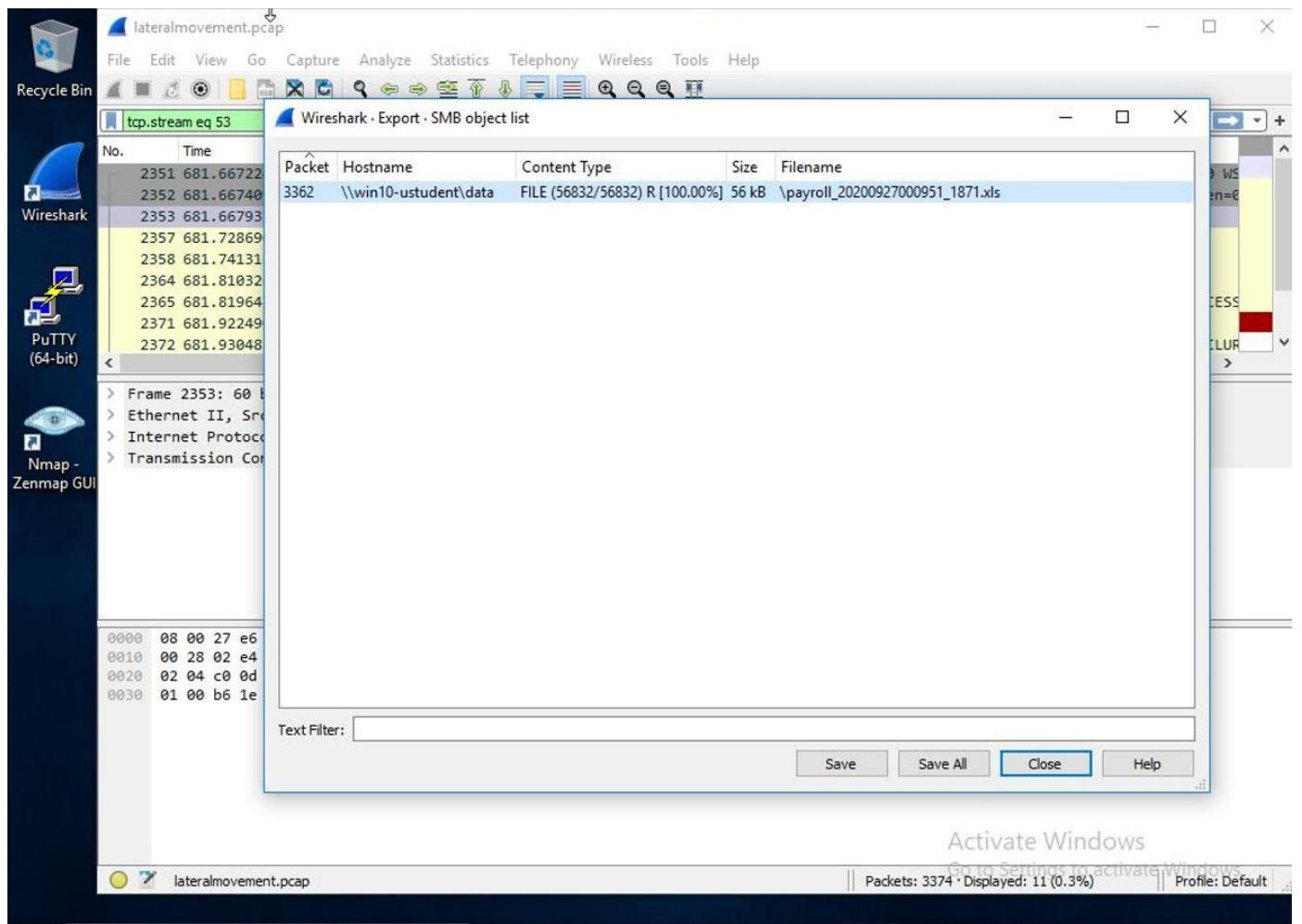
Then he used the compromised machine and pivoted to my machine:



What service and port were targeted?

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
 - 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?

The screenshot shows the Windows Event Viewer interface. The left pane displays a tree view of logs: Event Viewer (Local), Custom Views, Windows Logs (selected), Application, Security (selected), Setup, System, Forwarded Events, Applications and Services Log, and Subscriptions. The right pane shows the Security log with 31,223 events. A filter is applied: Log: Security; Source: ; Event ID: 4776,4625. Number of events: 2. Two entries are listed:

Keywords	Date and Ti...	Source	Event ID	Task Category
Audit Failure	12/16/2022 ...	Microsoft Windows security auditing.	4625	Logon
Audit Failure	12/16/2022 ...	Microsoft Windows security auditing.	4625	Logon

A detailed view of the first event (Event ID 4625) is shown in a modal window. The General tab is selected, displaying the following details:

Security ID:	SYSTEM
Account Name:	WIN10-USSTUDENTS
Account Domain:	WORKGROUP
Logon ID:	0x3E7

General tab details:

Log Name:	Security
Source:	Microsoft Windows security
Event ID:	4625
Level:	Information
User:	N/A
OpCode:	Info

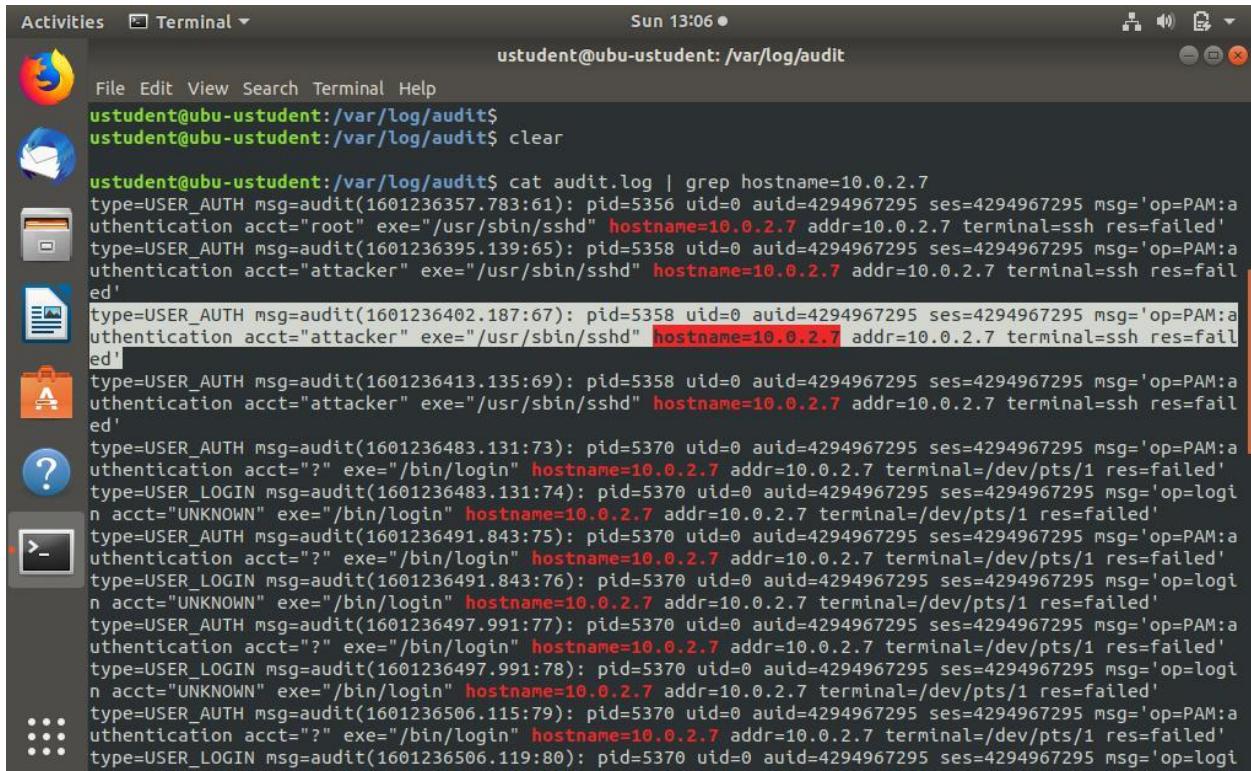
Task Category: Logon
Keywords: Audit Failure
Computer: win10-ustudent
Logged: 12/16/2022 9:48:00 PM
More Information: [Event Log Online Help](#)

The Actions pane on the right lists various options: Open..., Create..., Import..., Clear..., Filter..., Clear..., Prop..., Find..., Save F..., Attach..., Save F..., View, Refresh, Help, Event 4625..., Event..., Attach..., Save S..., Copy, Refresh, Help.

Activate Windows
Go to Settings to activate Windows.

Creates a filter.

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



```
ustudent@ubu-ustudent: /var/log/audit$ cat audit.log | grep hostname=10.0.2.7
ustudent@ubu-ustudent: /var/log/audit$ uststudent@ubu-ustudent: /var/log/audit$ clear
ustudent@ubu-ustudent: /var/log/audit$ cat audit.log | grep hostname=10.0.2.7
type=USER_AUTH msg=audit(1601236357.783:61): pid=5356 uid=0 auid=4294967295 ses=4294967295 msg='op=PAM:authentication acct="root" exe="/usr/sbin/sshd" hostname=10.0.2.7 addr=10.0.2.7 terminal=ssh res=failed'
type=USER_AUTH msg=audit(1601236395.139:65): pid=5358 uid=0 auid=4294967295 ses=4294967295 msg='op=PAM:authentication acct="attacker" exe="/usr/sbin/sshd" hostname=10.0.2.7 addr=10.0.2.7 terminal=ssh res=failed'
type=USER_AUTH msg=audit(1601236402.187:67): pid=5358 uid=0 auid=4294967295 ses=4294967295 msg='op=PAM:authentication acct="attacker" exe="/usr/sbin/sshd" hostname=10.0.2.7 addr=10.0.2.7 terminal=ssh res=failed'
type=USER_AUTH msg=audit(1601236413.135:69): pid=5358 uid=0 auid=4294967295 ses=4294967295 msg='op=PAM:authentication acct="attacker" exe="/usr/sbin/sshd" hostname=10.0.2.7 addr=10.0.2.7 terminal=ssh res=failed'
type=USER_AUTH msg=audit(1601236483.131:73): pid=5370 uid=0 auid=4294967295 ses=4294967295 msg='op=PAM:authentication acct="?" exe="/bin/login" hostname=10.0.2.7 addr=10.0.2.7 terminal=/dev/pts/1 res=failed'
type=USER_LOGIN msg=audit(1601236483.131:74): pid=5370 uid=0 auid=4294967295 ses=4294967295 msg='op=login acct="UNKNOWN" exe="/bin/login" hostname=10.0.2.7 addr=10.0.2.7 terminal=/dev/pts/1 res=failed'
type=USER_AUTH msg=audit(1601236491.843:75): pid=5370 uid=0 auid=4294967295 ses=4294967295 msg='op=PAM:authentication acct="?" exe="/bin/login" hostname=10.0.2.7 addr=10.0.2.7 terminal=/dev/pts/1 res=failed'
type=USER_LOGIN msg=audit(1601236491.843:76): pid=5370 uid=0 auid=4294967295 ses=4294967295 msg='op=login acct="UNKNOWN" exe="/bin/login" hostname=10.0.2.7 addr=10.0.2.7 terminal=/dev/pts/1 res=failed'
type=USER_AUTH msg=audit(1601236497.991:77): pid=5370 uid=0 auid=4294967295 ses=4294967295 msg='op=PAM:authentication acct="?" exe="/bin/login" hostname=10.0.2.7 addr=10.0.2.7 terminal=/dev/pts/1 res=failed'
type=USER_LOGIN msg=audit(1601236497.991:78): pid=5370 uid=0 auid=4294967295 ses=4294967295 msg='op=login acct="UNKNOWN" exe="/bin/login" hostname=10.0.2.7 addr=10.0.2.7 terminal=/dev/pts/1 res=failed'
type=USER_AUTH msg=audit(1601236506.115:79): pid=5370 uid=0 auid=4294967295 ses=4294967295 msg='op=PAM:authentication acct="?" exe="/bin/login" hostname=10.0.2.7 addr=10.0.2.7 terminal=/dev/pts/1 res=failed'
type=USER_LOGIN msg=audit(1601236506.119:80): pid=5370 uid=0 auid=4294967295 ses=4294967295 msg='op=login
```

Name of the attacker account: **attacker**

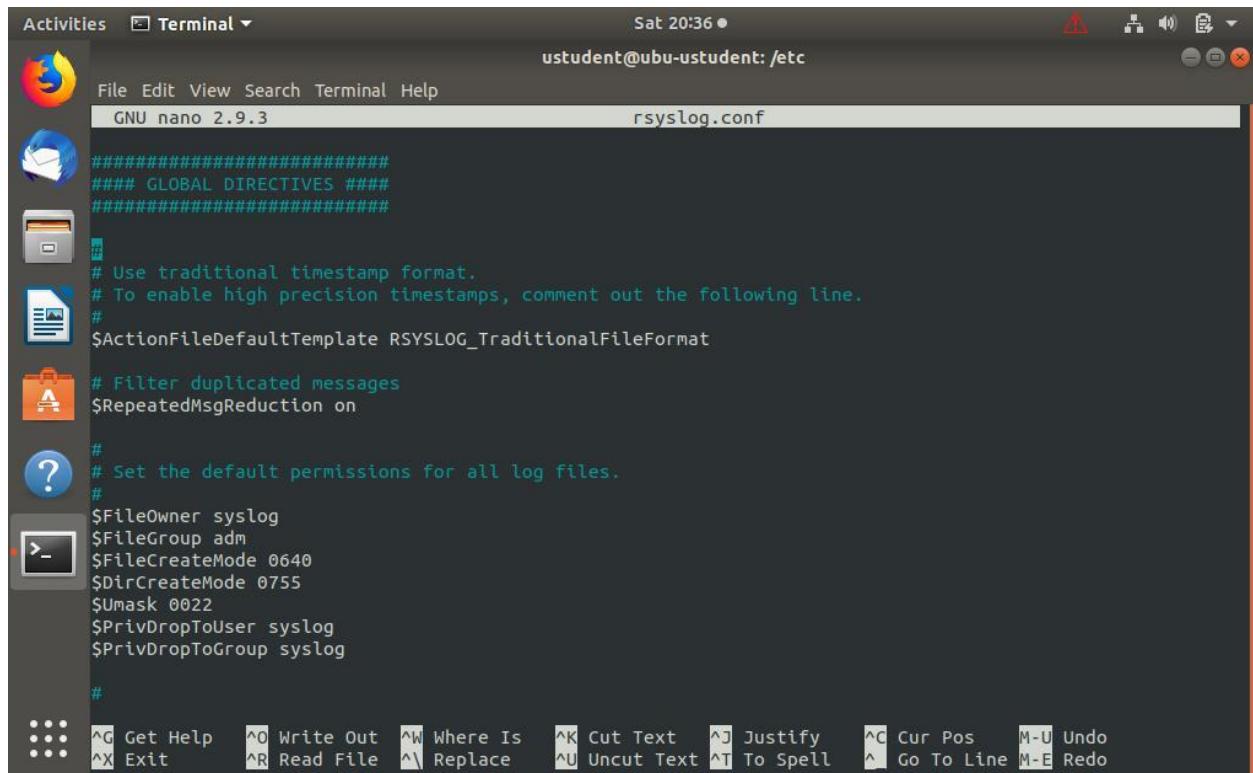
Provide mitigation recommendations:

- 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



The screenshot shows a Linux desktop environment with a terminal window open in the Activities overview. The terminal window title is "rsyslog.conf" and it displays the configuration file for rsyslog. The file contains various directives for log handling, including global directives, file permissions, and log file rotation. The terminal window is part of the Unity interface, with other application icons visible in the dock.

```
#####
#### GLOBAL DIRECTIVES #####
#####

# Use traditional timestamp format.
# To enable high precision timestamps, comment out the following line.
#
$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat

# Filter duplicated messages
$RepeatedMsgReduction on

#
# Set the default permissions for all log files.
#
$FileOwner syslog
$FileGroup adm
$FileCreateMode 0640
$DirCreateMode 0755
$Umask 0022
$PrivDropToUser syslog
$PrivDropToGroup syslog

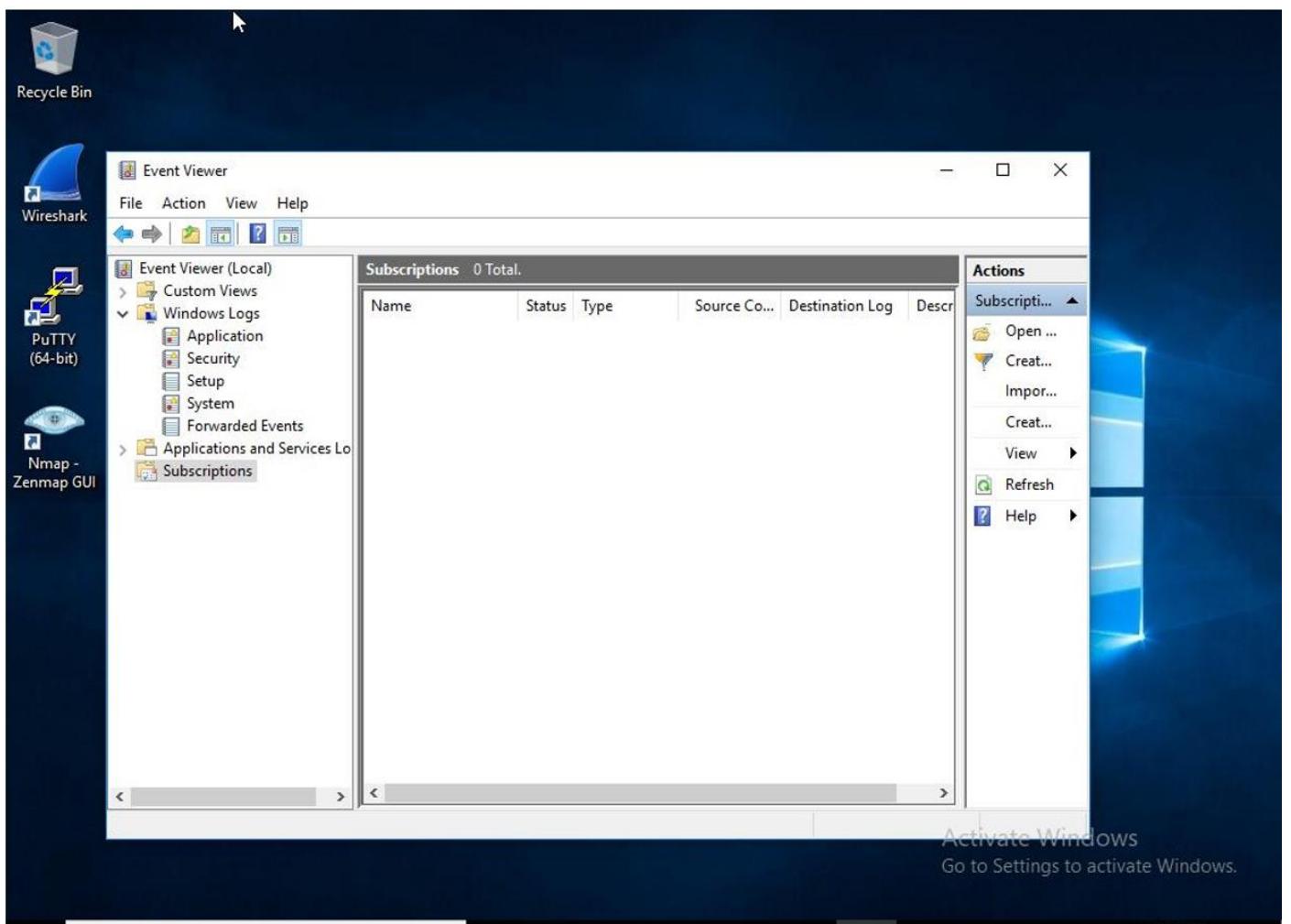
#
```

At the bottom of the terminal window, there is a menu bar with standard nano editor commands:

- Get Help (Alt+G)
- Write Out (Alt+O)
- Where Is (Alt+W)
- Cut Text (Alt+K)
- Justify (Alt+J)
- Cur Pos (Alt+C)
- Undo (M-U)
- Exit (Alt+X)
- Read File (Alt+R)
- Replace (Alt+A)
- Uncut Text (Alt+U)
- To Spell (Alt+T)
- Go To Line (Alt+L)
- Redo (M-E)

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/
```

File	Permissions	User	Date	Size	Description
hp	drwxr-xr-x	root	Apr 26 2018	4096	hp
installer	drwxrwxr-x	root	Sep 26 2020	4096	installer
journal	drwxr-sr-x+	root	Sep 26 2020	4096	journal
kern.log	-rw-r-----	1 syslog	Dec 17 16:58	56931	kern.log
kern.log.1	-rw-r-----	1 syslog	Dec 9 20:30	12340	kern.log.1
kern.log.2.gz	-rw-r-----	1 syslog	Dec 3 07:41	485	kern.log.2.gz
kern.log.3.gz	-rw-r-----	1 syslog	Dec 1 19:04	123047	kern.log.3.gz
kern.log.4.gz	-rw-r-----	1 syslog	Sep 27 2020	100698	kern.log.4.gz
lastlog	-rw-rw-r--	1 root	Dec 15 20:35	293752	lastlog
lightdm	drwxr-xr-x	2 root	Mar 21 2018	4096	lightdm
samba	drwxr-x---	3 root	Dec 16 08:45	4096	samba
speech-dispatcher	drwxr----	2 speech-dispatcher	Apr 23 2018	4096	speech-dispatcher
syslog	-rw-r-----	1 syslog	Dec 17 21:01	752287	syslog
syslog.1	-rw-r-----	1 syslog	Dec 17 00:07	950735	syslog.1
syslog.2.gz	-rw-r-----	1 syslog	Dec 16 08:45	53734	syslog.2.gz
syslog.3.gz	-rw-r-----	1 syslog	Dec 15 19:24	3812	syslog.3.gz
syslog.4.gz	-rw-r-----	1 syslog	Dec 13 20:47	14138	syslog.4.gz
syslog.5.gz	-rw-r-----	1 syslog	Dec 12 17:46	3360	syslog.5.gz
syslog.6.gz	-rw-r-----	1 syslog	Dec 11 21:03	4034	syslog.6.gz
syslog.7.gz	-rw-r-----	1 syslog	Dec 9 20:26	5388	syslog.7.gz
tallylog	-rw-----	1 root	Dec 15 20:35	64384	tallylog
unattended-upgrades	drwxr-x-	2 root	Dec 3 07:40	4096	unattended-upgrades
vboxadd-install.log	-rw-r--r--	1 root	Dec 15 20:35	631	vboxadd-install.log
vboxadd-setup.log	-rw-r--r--	1 root	Dec 15 20:36	63	vboxadd-setup.log
vboxadd-setup.log.1	-rw-r--r--	1 root	Dec 15 20:35	63	vboxadd-setup.log.1
vboxadd-setup.log.2	-rw-r--r--	1 root	Dec 15 20:35	221	vboxadd-setup.log.2
vsftpd.log	-rw-r--r--	1 root	Dec 16 14:43	1223328	vsftpd.log
wtmp	-rw-rw-r--	1 root	Dec 15 20:37	1920	wtmp
wtmp.1	-rw-rw-r--	1 root	Dec 1 19:02	35328	wtmp.1

```
ustudent@ubuntu-ustudent:/etc$
```

Impact: If the logging configuration isn't 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.

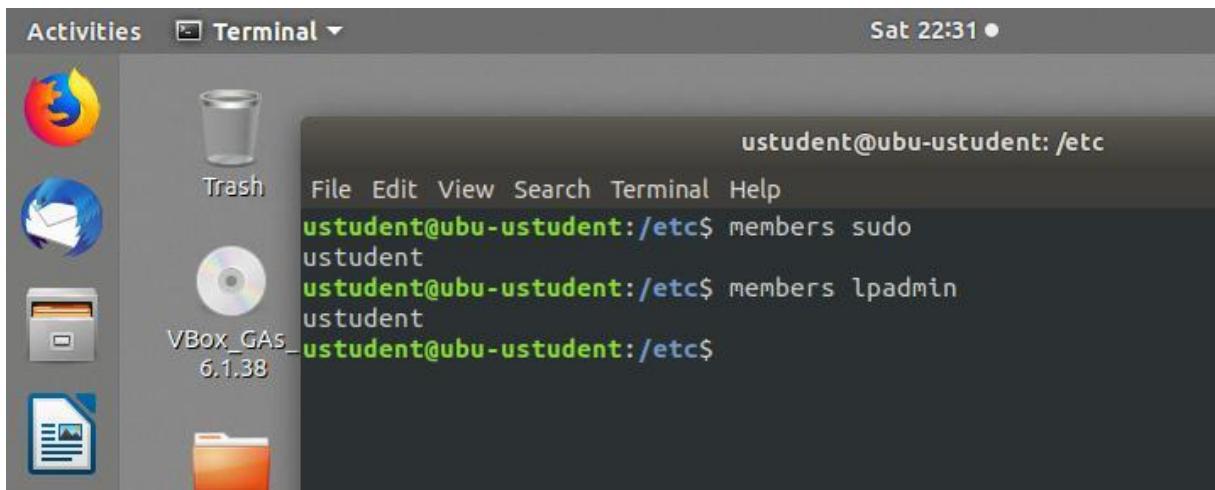
- Edit the /etc/rsyslog.conf and /etc/rsyslog.d/*.conf files and add the following line: `*.* @@<FQDN or ip of loghost>`
 - Configure a remote subscription related to Windows Events Forwarder.

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?

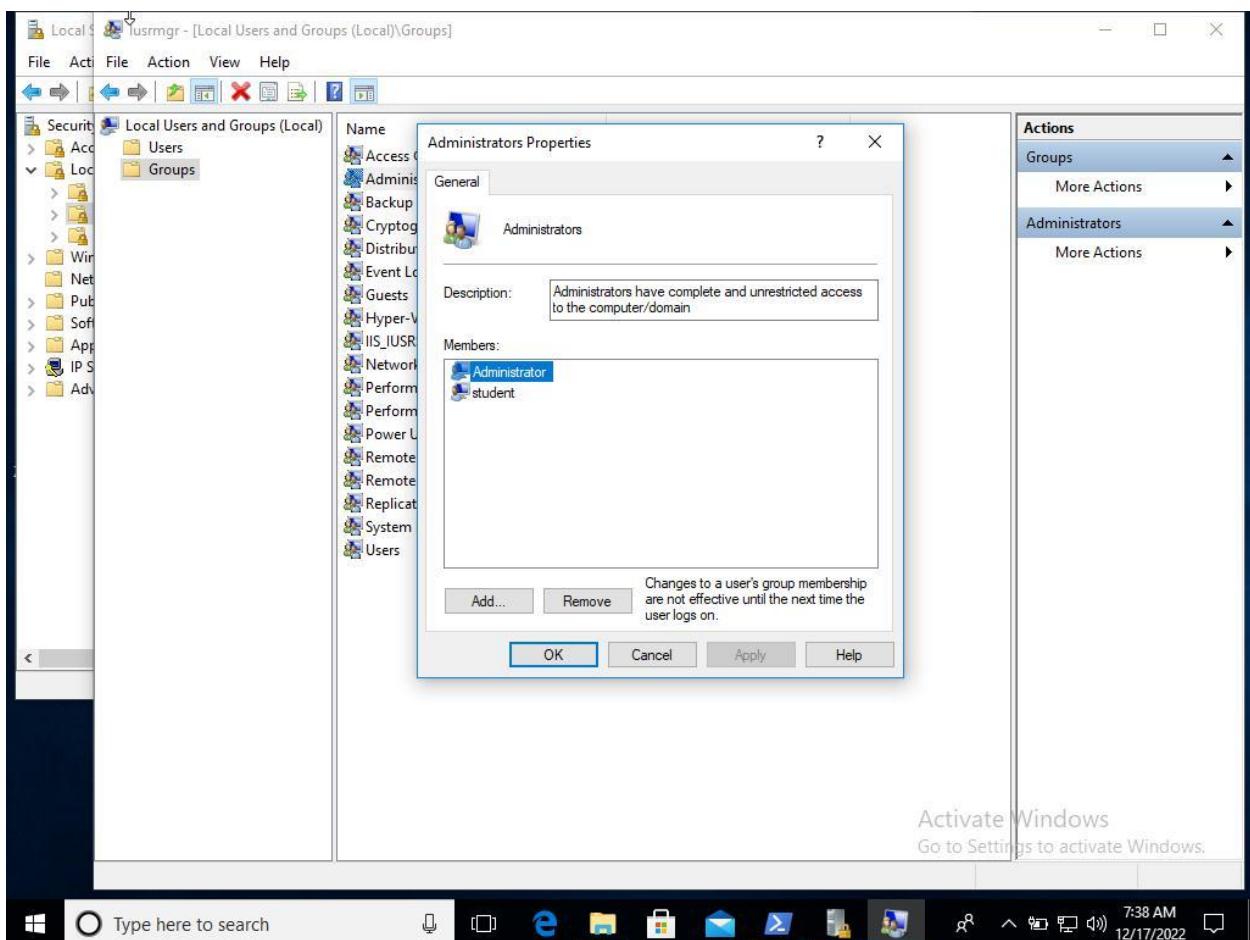
Ubuntu 18.04



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**.

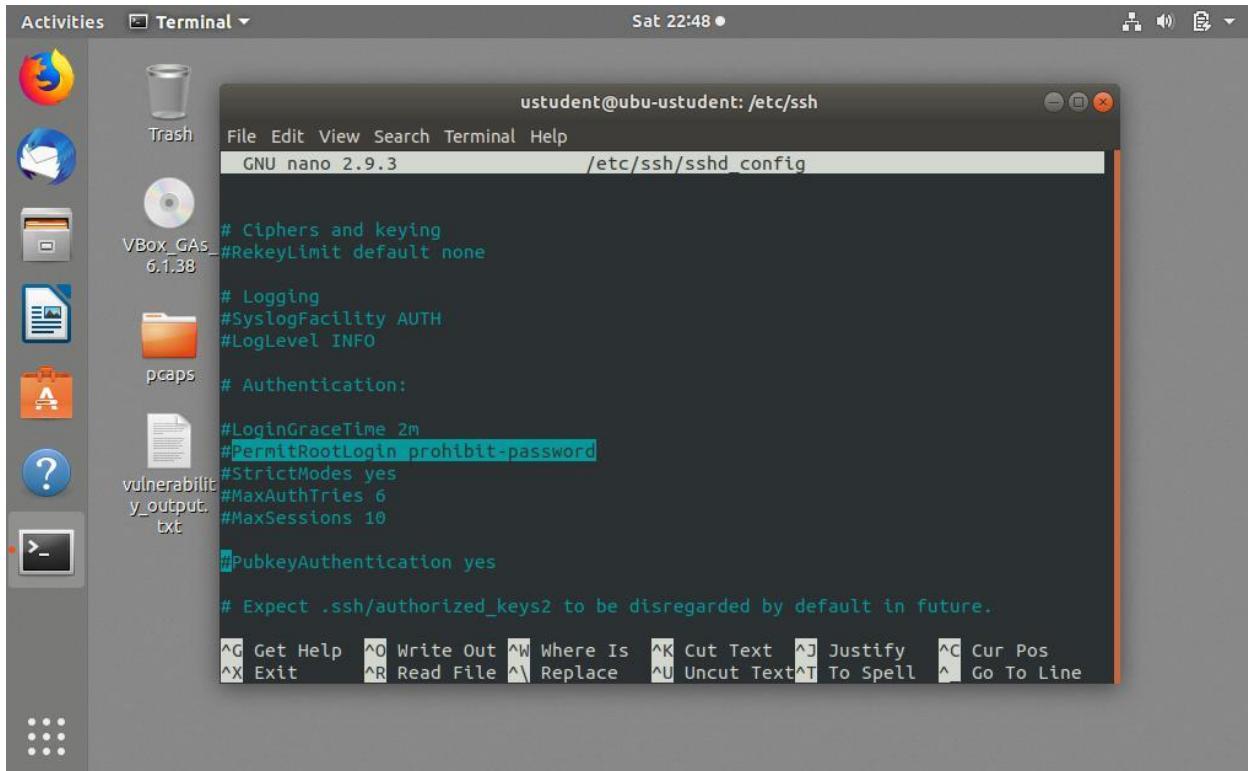
Windows 10 ENT



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

Yes, student.

Is root remote login permitted?



```
File Edit View Search Terminal Help
GNU nano 2.9.3          /etc/ssh/sshd_config

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.

^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos
^X Exit      ^R Read File  ^\ Replace   ^U Uncut Text ^T To Spell  ^L Go To Line
```

Yes, because the line is commented.

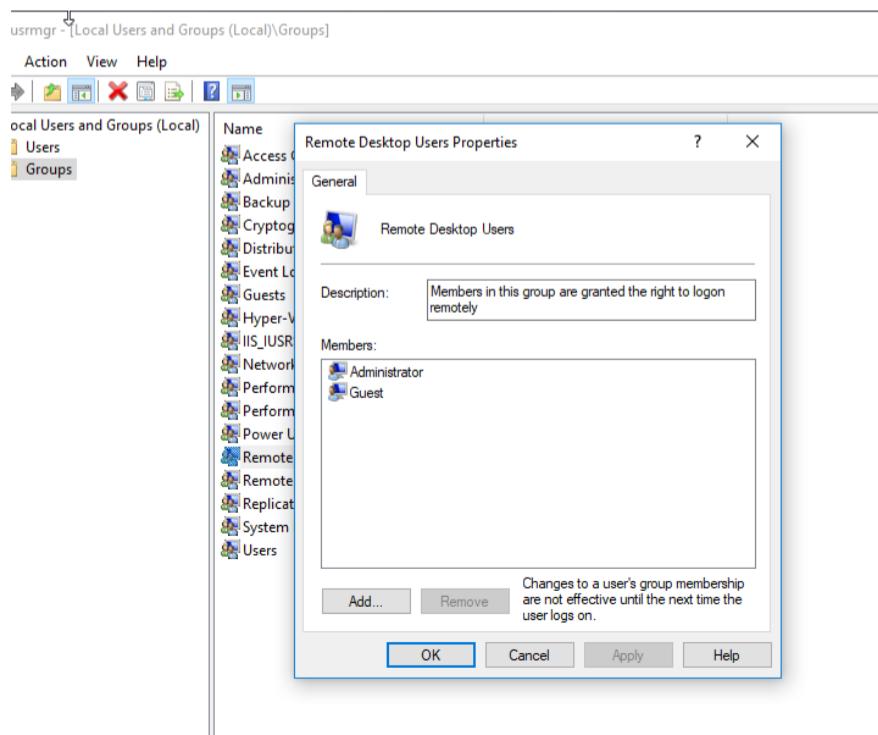
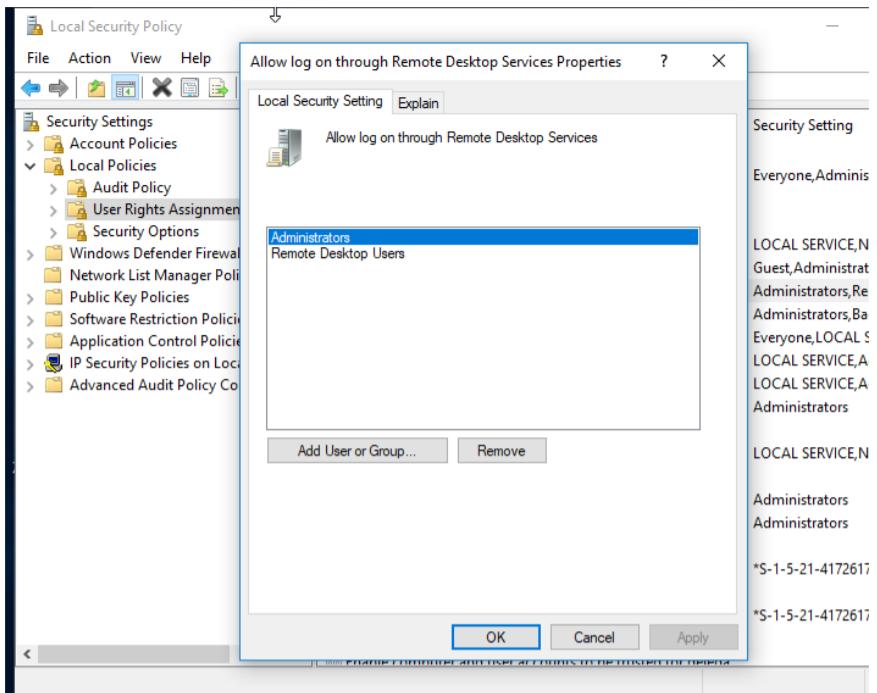
Are there other users allowed to SSH that shouldn't?

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.

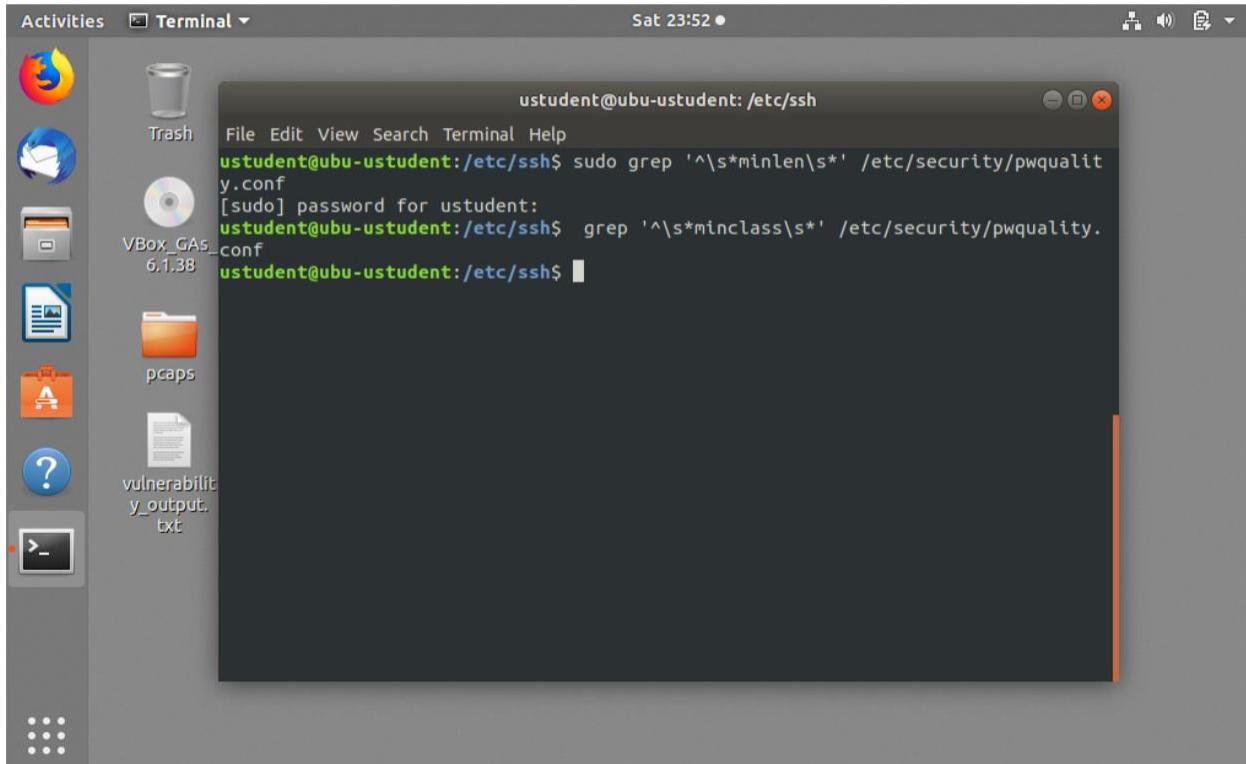
Proof of check:

```
# 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
```

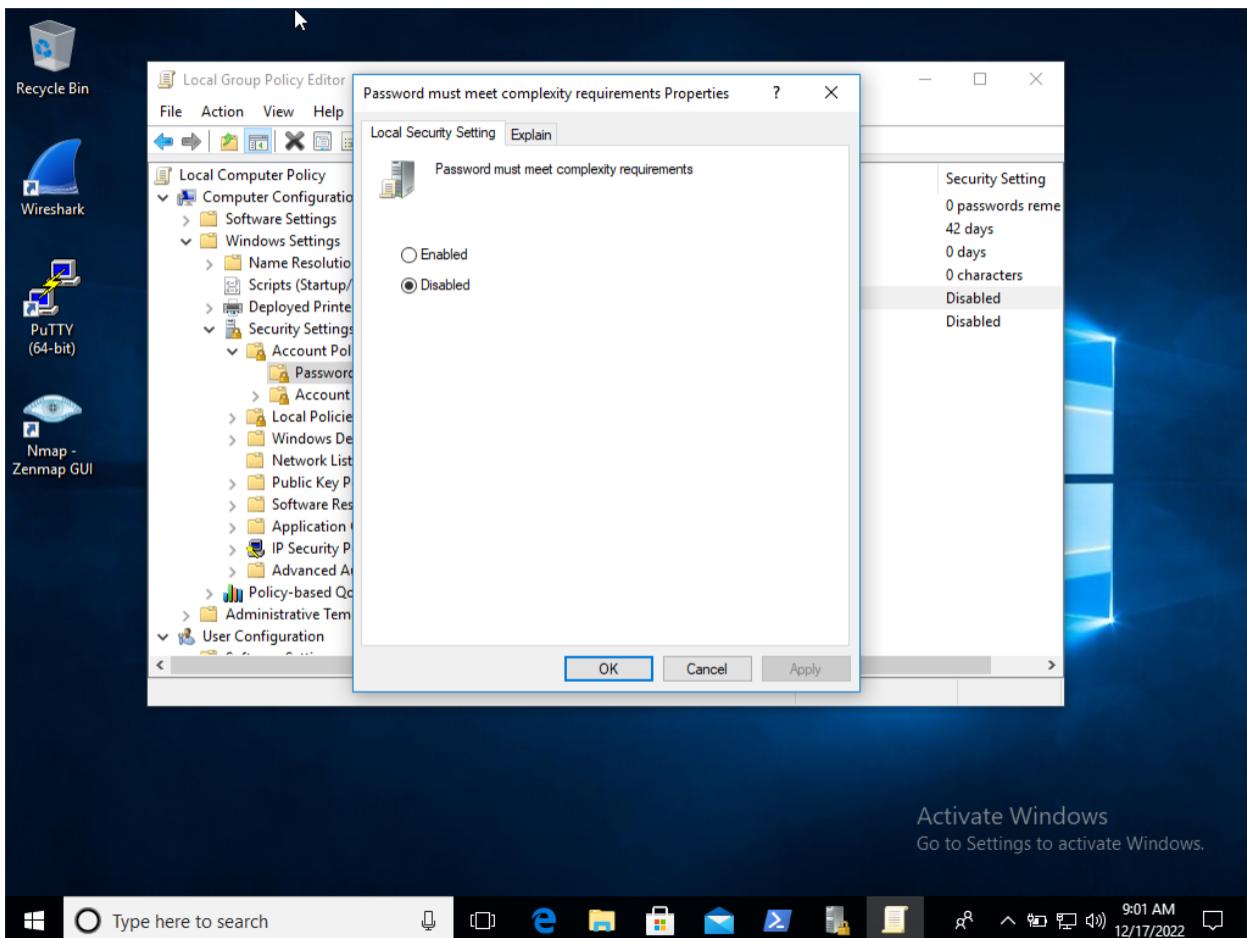
Windows 10 ENT

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

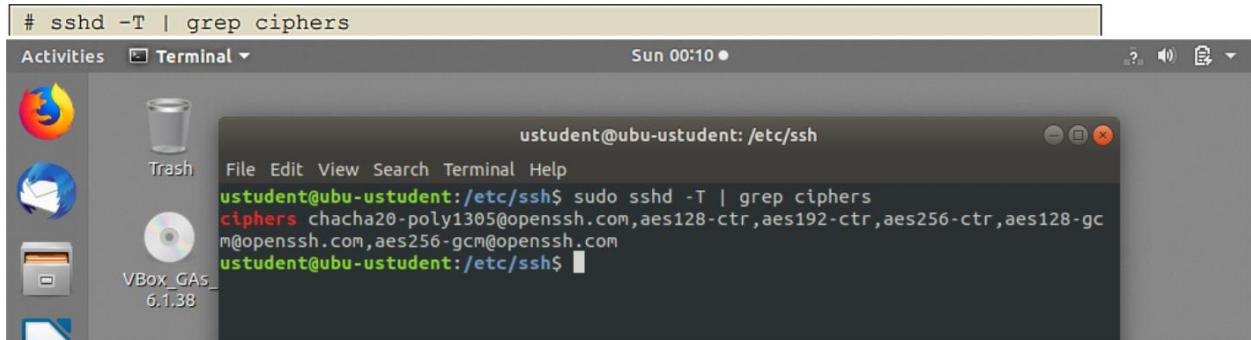
Verify the use of strong encryption in audited systems.

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:



A screenshot of an Ubuntu 18.04 desktop environment. On the left is a dock with icons for the Dash, Home, Activities, Terminal, and Dash. A trash can icon is also visible. The main area shows a terminal window titled 'ustudent@ubu-ustudent: /etc/ssh'. The terminal displays the command 'sudo sshd -T | grep ciphers' followed by its output, which includes 'chacha20-poly1305@openssh.com, aes128-ctr, aes192-ctr, aes256-ctr, aes128-gcm@openssh.com, aes256-gcm@openssh.com'. The terminal prompt 'ustudent@ubu-ustudent: /etc/ssh\$' is at the bottom. The desktop background is a dark grey gradient.

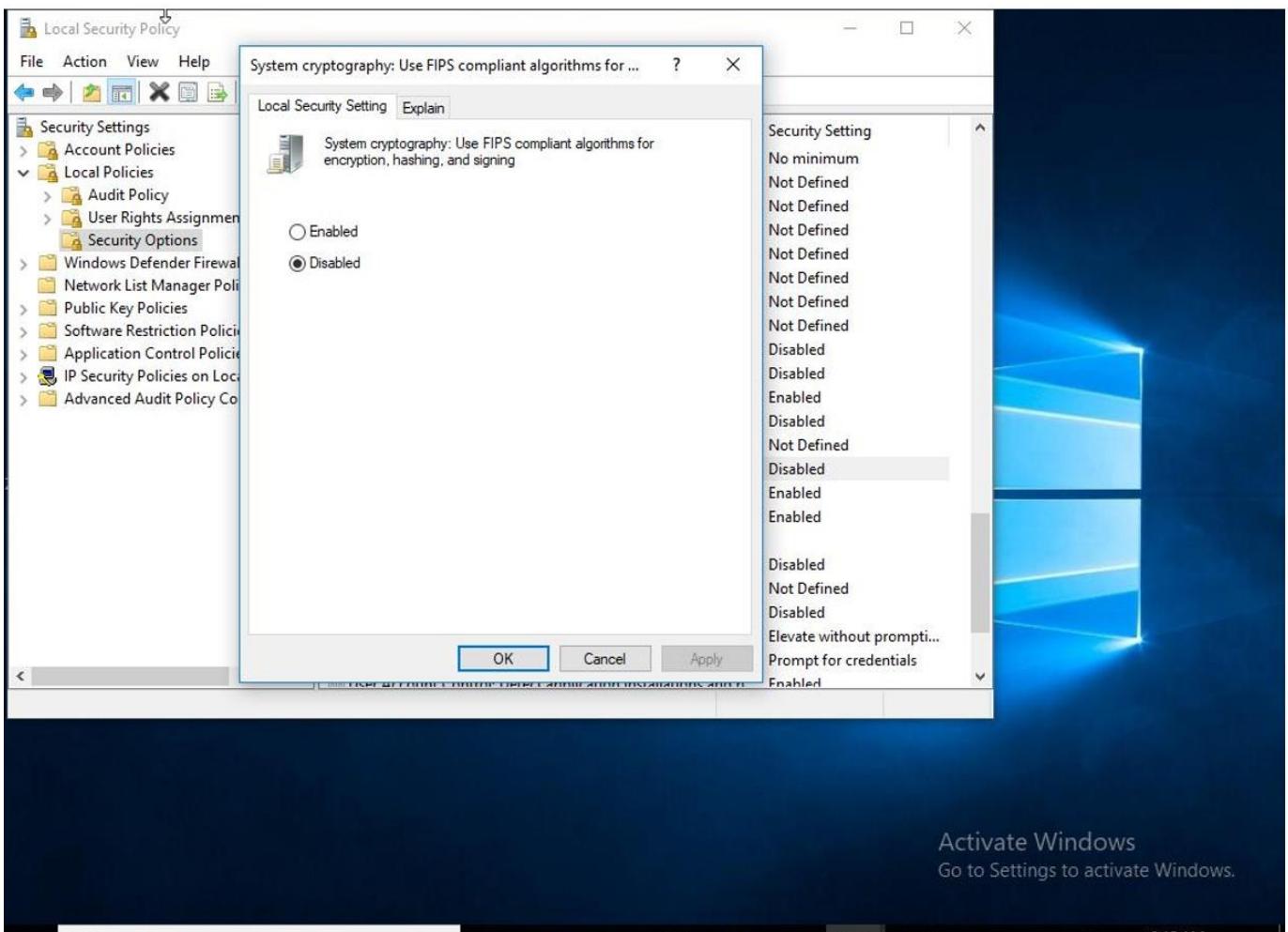
```
# sshd -T | grep ciphers
ustudent@ubu-ustudent: /etc/ssh$ sudo sshd -T | grep ciphers
ciphers chacha20-poly1305@openssh.com, aes128-ctr, aes192-ctr, aes256-ctr, aes128-gcm@openssh.com, aes256-gcm@openssh.com
ustudent@ubu-ustudent: /etc/ssh$
```

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.

Zenmap

Scan Tools Profile Help

Target: 10.0.2.5 Profile:

Command: nmap -p 21 --script ftp-brute 10.0.2.5

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host 10.0.2.5

nmap -p 21 --script ftp-brute 10.0.2.5

Starting Nmap 7.93 (https://nmap.org) at 2022-12-17 09:32 Pacific Standard Time
N SOCK ERROR [0.0400s] ssl_init_helper(): OpenSSL legacy provider failed to load.

NSE: [ftp-brute] usernames: Time limit 10m00s exceeded.
NSE: [ftp-brute] usernames: Time limit 10m00s exceeded.
NSE: [ftp-brute] passwords: Time limit 10m00s exceeded.
Nmap scan report for 10.0.2.5
Host is up (0.00088s latency).

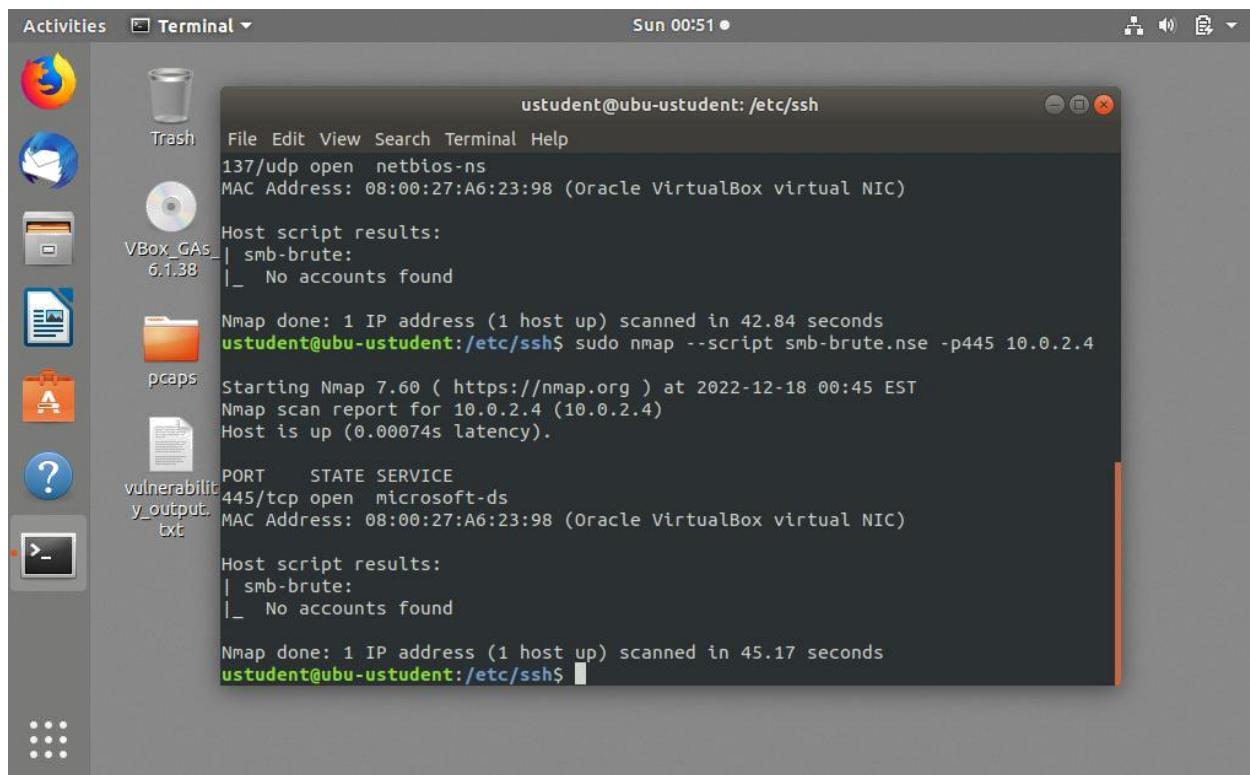
PORt	STATE	SERVICE
21/tcp	open	ftp
		ftp-brute:
		Accounts: No valid accounts found
	_	Statistics: Performed 9753 guesses in 601 seconds, average tps: 16.2
		MAC Address: 08:00:27:3F:07:99 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 600.95 seconds

Activate Windows
Go to Settings to activate Windows.

Filter Hosts

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



A screenshot of an Ubuntu desktop environment. The terminal window title is "ustudent@ubu-ustudent: /etc/ssh". The terminal output shows the following:

```
File Edit View Search Terminal Help
137/udp open netbios-ns
MAC Address: 08:00:27:A6:23:98 (Oracle VirtualBox virtual NIC)

Host script results:
| smb-brute:
|_ No accounts found

Nmap done: 1 IP address (1 host up) scanned in 42.84 seconds
ustudent@ubu-ustudent:/etc/ssh$ sudo nmap --script smb-brute.nse -p445 10.0.2.4

Starting Nmap 7.60 ( https://nmap.org ) at 2022-12-18 00:45 EST
Nmap scan report for 10.0.2.4 (10.0.2.4)
Host is up (0.00074s latency).

PORT      STATE SERVICE
445/tcp    open  microsoft-ds
MAC Address: 08:00:27:A6:23:98 (Oracle VirtualBox virtual NIC)

Host script results:
| smb-brute:
|_ No accounts found

Nmap done: 1 IP address (1 host up) scanned in 45.17 seconds
ustudent@ubu-ustudent:/etc/ssh$
```

No accounts was found when brute forcing smb.

Final Assessment and Recommendations Based on Your Scans and Checks

After this analyses, it is highly recommended not add these system to our current infrastructure. Before that, it is important imposes safety constraints such as those related to rules for passwords. “1234” it is a extremely weak password, broken in just over 170 seconds. Additionally, it is necessary to review the user groups and permissions, as presented before, because we are facing a permissions overload situation. After that, it is highly recommended update the operation system to a version that have still support. The next step is block ports (TCP/UDP) or services that will no used.

- Would integrating this network into the extended network of our company bring new risks and exposures?

Yes, it defnitely 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.

Doing those recommendations, the host can be added to the infrastructure.