

1: Asset identification, address update, dependencies, patches, and native protections at targeted Server/ Desktop Operating Systems

1.2 Windows CIS 18.9.102.2

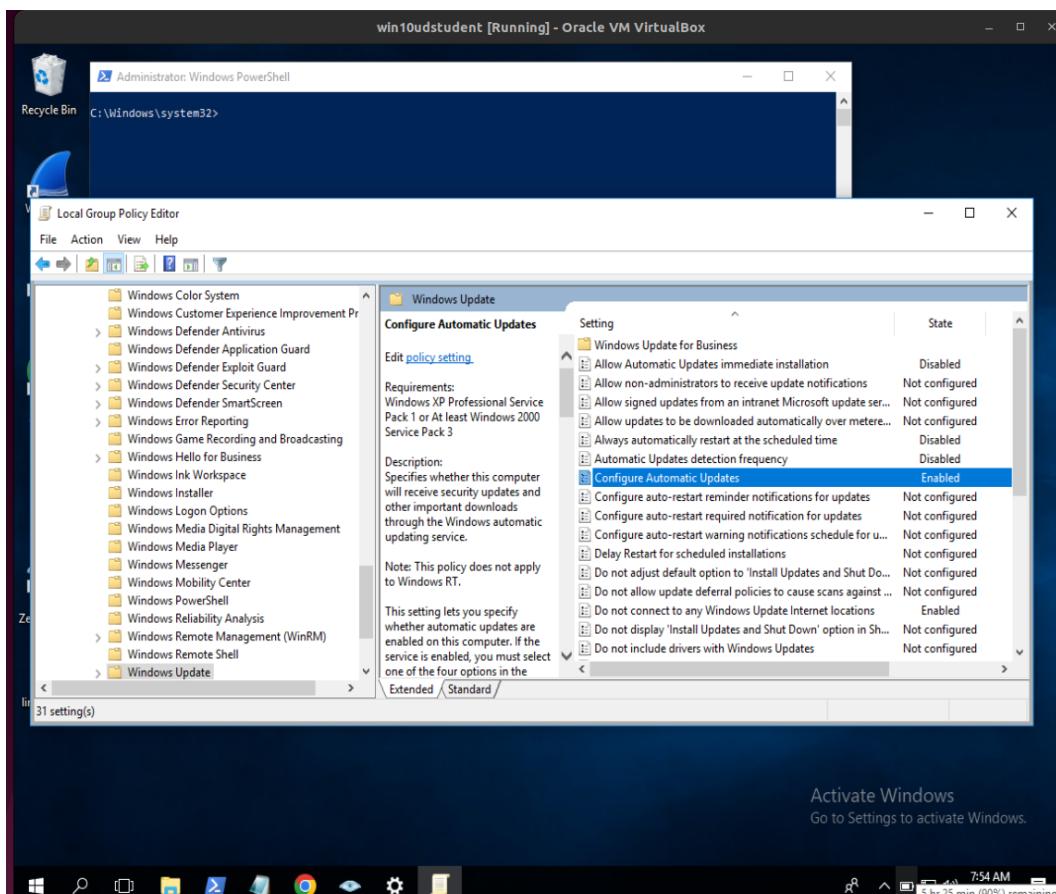
- Ensure 'configure automatic updates' is set to 'Enabled.'

Description:

The operating system will recognize when a network connection is available and then use the network connection to search Windows Update or your designated intranet site for updates that apply to them.

Remediation:

CIS benchmarks Windows 10 ENT suggest using a value of 4 - Auto download and schedule the install.



win10udstudent ova

1.2 Ubuntu CIS 1.2.1

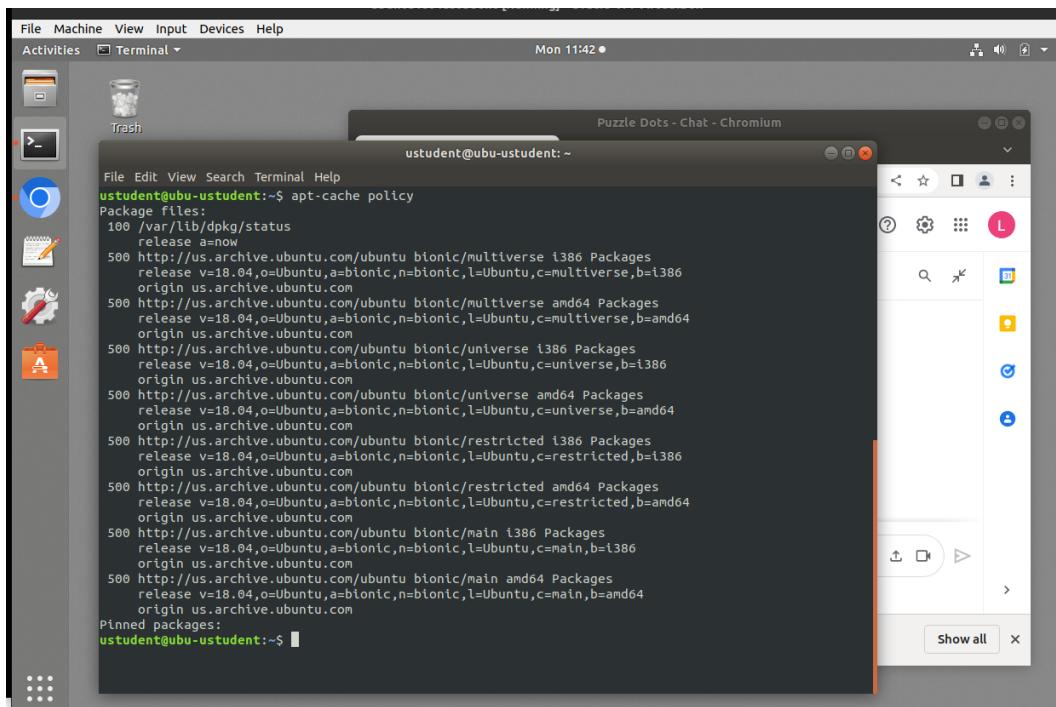
- Ensure package manager repositories are configured correctly.

Description:

Systems need to have package manager repositories configured to ensure they receive the latest patches and updates.

Remediation:

Update package manager repositories according to release.



ustudent@ubu-ustudent ova

1.3 Windows CIS 18.3.4

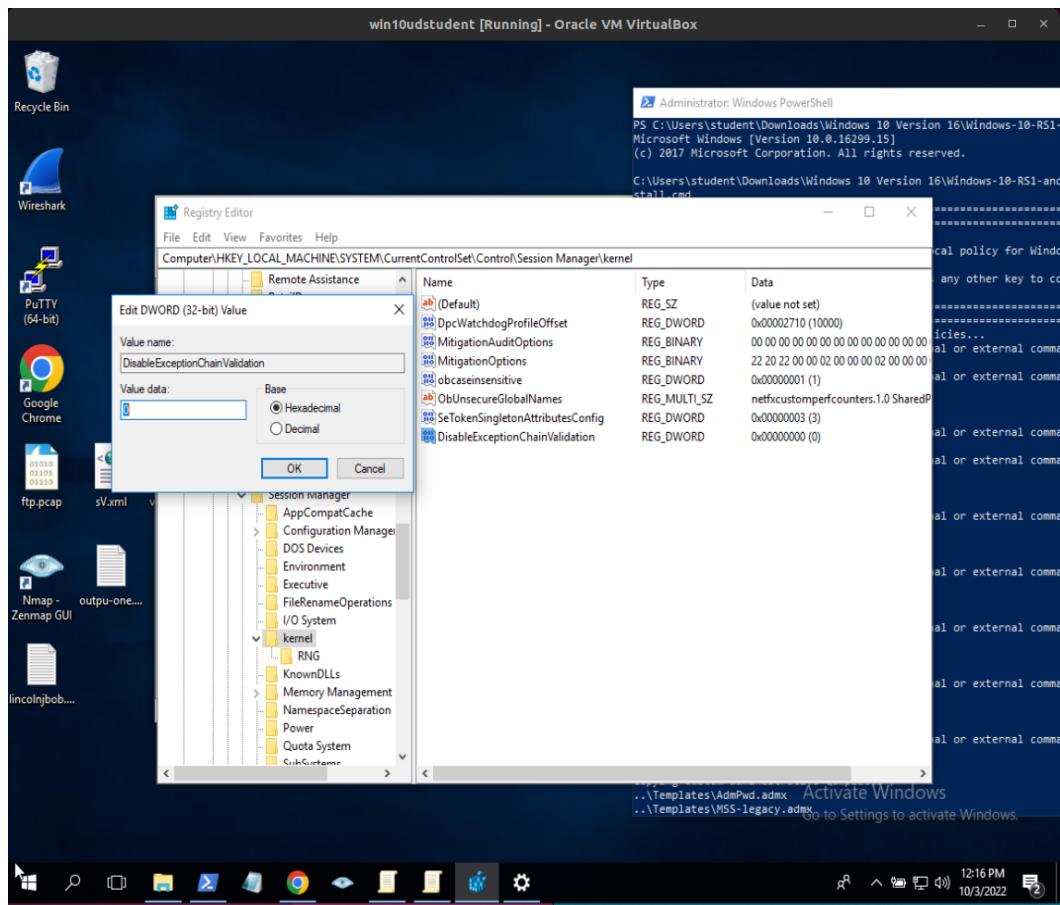
- Ensure 'Enable Structured Exception Handling Overwrite Protection (SEHOP)' is set to 'Enabled.'
- Provide documentation as to what applications are installed on the Windows machine.

Description:

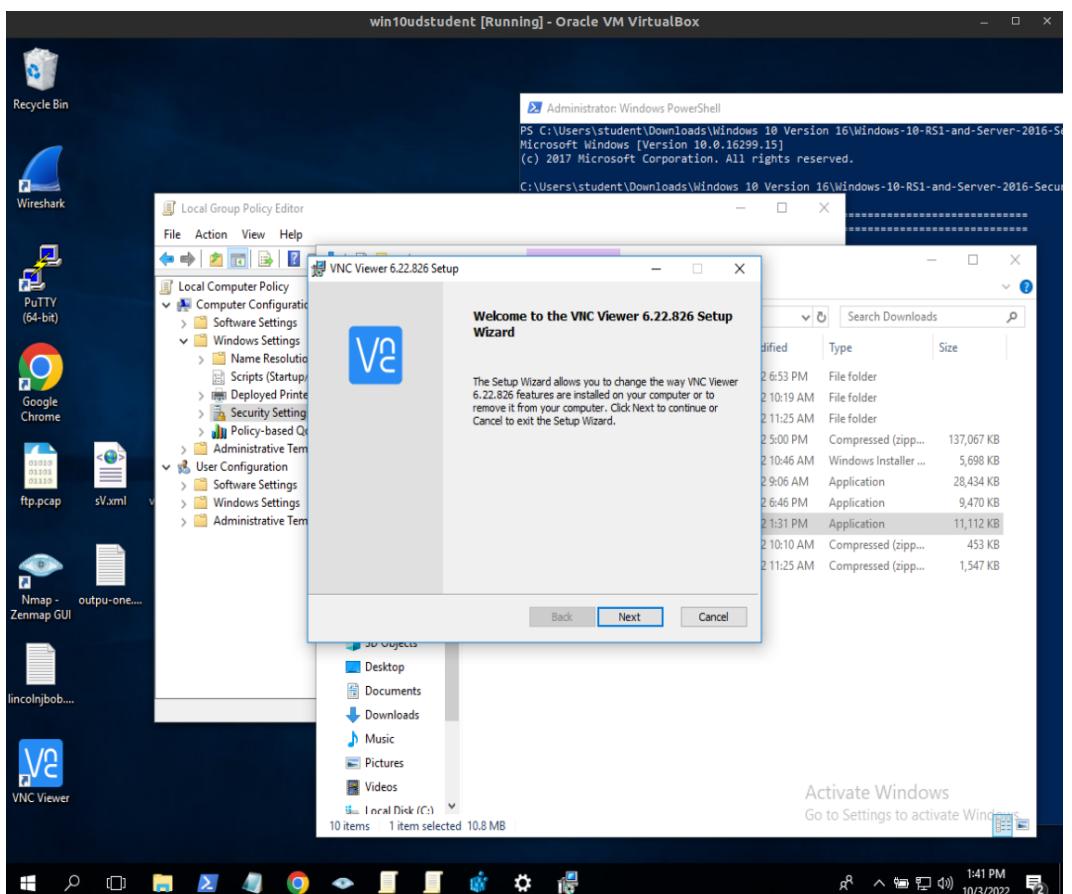
Windows includes support for Structured Exception Handling Overwrite Protection (SEHOP). CIS recommend enabling this feature to improve the security profile of the system.

Remediation:

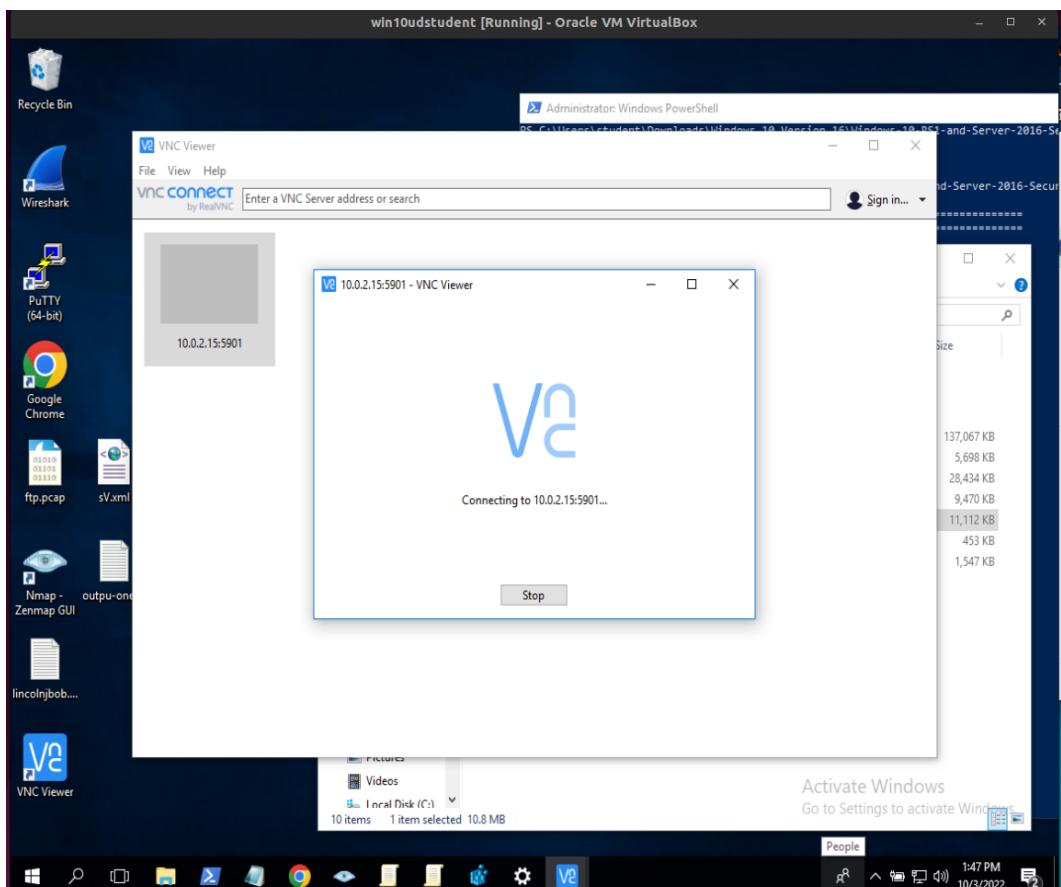
Set the value to 0 of DisableExceptionChainValidation in the Registry manually at HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\kernel\DisableExceptionChainValidation.



win10udstudent ova



win10udstudent ova - Follow default installation



win10udstudent ova - VNC installed and running

VNC installation screenshots: (next page)

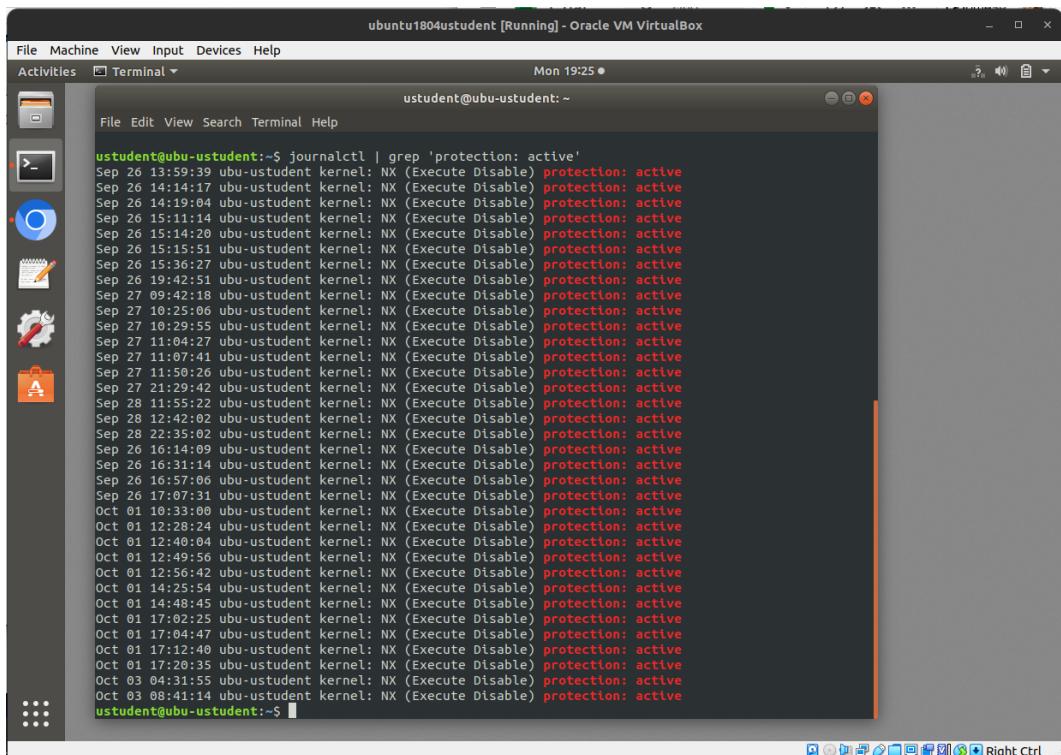
1.3 Ubuntu CIS 1.6.1, 1.6.2

- 1.6.1 Ensure XD/NX support is enabled
- 1.6.2 Ensure address space layout randomization (ASLR) is enabled

Description: 1.6.1 Ensure XD/NX support is enabled

Recent processors in the x86 family support the ability to prevent code execution on a per memory page basis. Which protect against buffer overflow attacks.

Result: Complaint, XD/NX support is enabled.



A screenshot of a terminal window titled "ubuntu1804ustudent [Running] - Oracle VM VirtualBox". The window shows a terminal session with the command "journalctl | grep 'protection: active'" being run. The output of the command is displayed in the terminal window, showing numerous log entries from the kernel indicating that NX (Execute Disable) protection is active across various dates and times. The terminal window has a dark theme and is part of the Unity desktop environment.

```
ustudent@ubu-ustudent:~$ 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 15:42:51 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
Sep 26 16:14:09 ubu-ustudent kernel: NX (Execute Disable) protection: active
Sep 26 16:31:14 ubu-ustudent kernel: NX (Execute Disable) protection: active
Sep 26 16:57:06 ubu-ustudent kernel: NX (Execute Disable) protection: active
Sep 26 17:07:31 ubu-ustudent kernel: NX (Execute Disable) protection: active
Oct 01 10:33:00 ubu-ustudent kernel: NX (Execute Disable) protection: active
Oct 01 12:28:24 ubu-ustudent kernel: NX (Execute Disable) protection: active
Oct 01 12:46:04 ubu-ustudent kernel: NX (Execute Disable) protection: active
Oct 01 12:49:56 ubu-ustudent kernel: NX (Execute Disable) protection: active
Oct 01 12:56:42 ubu-ustudent kernel: NX (Execute Disable) protection: active
Oct 01 14:25:54 ubu-ustudent kernel: NX (Execute Disable) protection: active
Oct 01 14:48:45 ubu-ustudent kernel: NX (Execute Disable) protection: active
Oct 01 17:02:25 ubu-ustudent kernel: NX (Execute Disable) protection: active
Oct 01 17:04:47 ubu-ustudent kernel: NX (Execute Disable) protection: active
Oct 01 17:12:40 ubu-ustudent kernel: NX (Execute Disable) protection: active
Oct 01 17:20:35 ubu-ustudent kernel: NX (Execute Disable) protection: active
Oct 03 04:31:55 ubu-ustudent kernel: NX (Execute Disable) protection: active
Oct 03 08:41:14 ubu-ustudent kernel: NX (Execute Disable) protection: active
ustudent@ubu-ustudent:~$
```

ustudent@ubu-ustudent ova

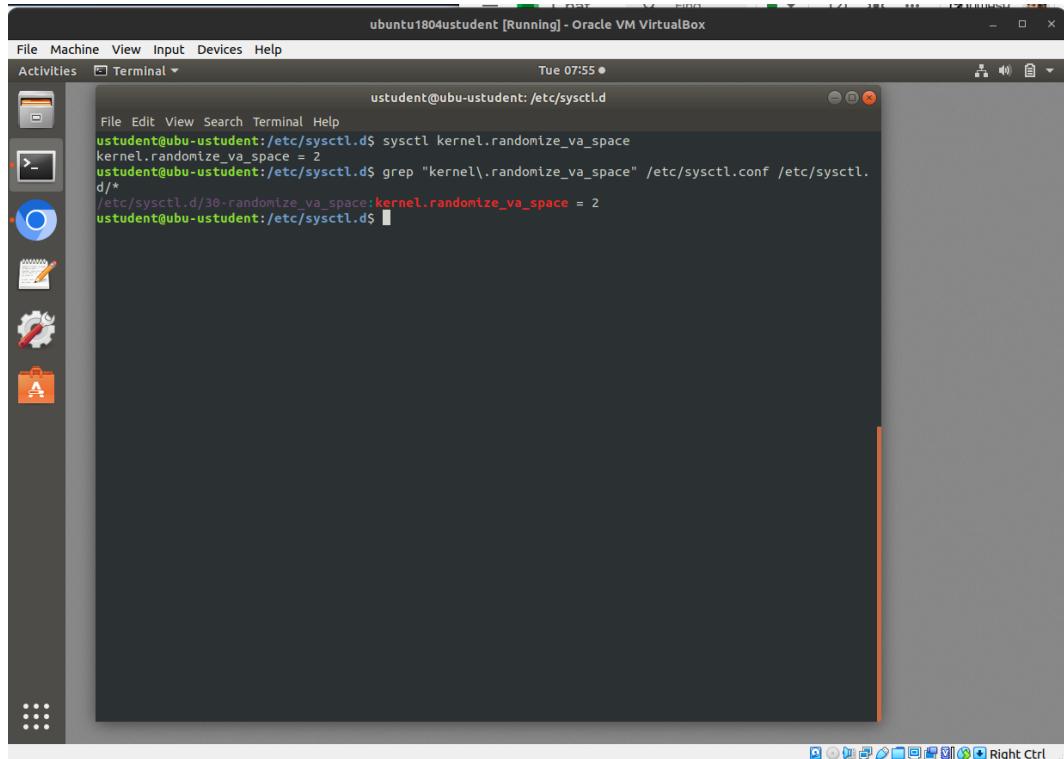
Description: 1.6.2 Ensure address space layout randomization (ASLR) is enabled

Address space layout randomization (ASLR) randomly arranges the address space of key data areas of a process. It's an exploit mitigation technique which will make it difficult to write memory page exploits as the memory placement will be consistently shifting.

Result:

Create the following file

- /etc/sysctl.d/* [range]-[file]: kernel.randomize_va_space = 2

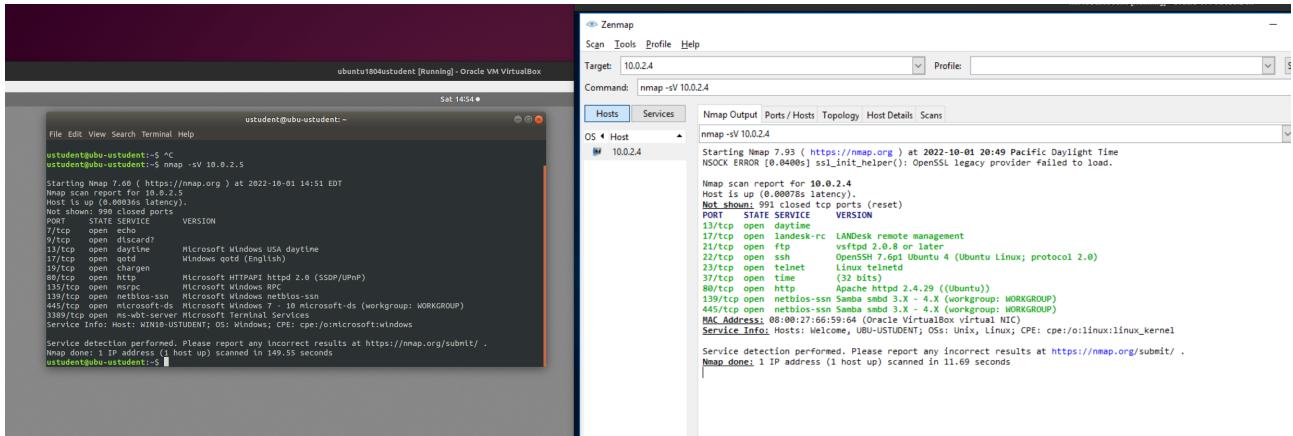


The screenshot shows a terminal window titled "ubuntu1804ustudent [Running] - Oracle VM VirtualBox". The window is running on a desktop environment with a dark theme. The terminal output is as follows:

```
File Machine View Input Devices Help
Activities Terminal Tue 07:55
ustudent@ubu-ustudent:~/etc/sysctl.d$ sysctl kernel.randomize_va_space
kernel.randomize_va_space = 2
ustudent@ubu-ustudent:~/etc/sysctl.d$ grep "kernel\.randomize_va_space" /etc/sysctl.conf /etc/sysctl.d/*
/etc/sysctl.d/30-randomize_va_space:kernel.randomize_va_space = 2
ustudent@ubu-ustudent:~/etc/sysctl.d$
```

ustudent@ubu-ustudent ova

1.4 Open ports Ubuntu / Windows



Recommendations:

Primarily, It's a must that not used ports should be disable, then those required to be open should be protected properly backed by a firewall, connection timeout and failed logon set as tries as tries by time.

Echo service on port 7 is outdated by ICMP echo. This Port just echoes whatever is sent to it and It can be used in many attacks.

Port 9 is typically used for test purposes based in UDP protocol discarding any input. It could be exploited by sending a specially malformed TCP packet.

QoTD service on port 17 is an insecure service that execute the output of a message when a connection is stablished, proven to be vulnerable, this connection when is open allows attacks as DoS, remote code execution or privilige scalation.

Chargen Detection service on port 19 simply generates characters and has no useful functionality on its own, easily used to perform Denial-of-Service attacks.

Ports based in insecure protocols as telnet (23) or ftp (21) for remote connections are outdated and vulnerable, should be replaced by SSH to keep the data transferred encrypted for remote connections if required, because even SSH port (22) is vulnerable to attacks, as DoS, arbitrary code execution or unauthorized access.

Ports as 139/445 used for direct TCP/IP MS Networking access leaves Windows machines vulnerable to a number of trojans and worms. It should be blocked at the firewall level or disabled also.

Port 80 could propagate a number of trojans/worms/backdoors if the web service is not running, even unauthenticated remote user can upload arbitrary code and execute it with the permissions of the operating-system by sending specially crafted network packets.

Through port 3389 for Windows Remote Desktop Protocol, attackers can cause a server to reach full memory utilization causing Denial of Service. It should not be exposed unless absolutely needed, since RDP servers exposed to the Internet are prime targets for malicious actors.

The use of firewalls and anti-virus should be enforced, Users and/or Services that request for network access should connect through VPN and firewall to be allowed to access into the Network.

2: Assess Access Management at Targeted Assets

2.1 Current settings on Network Segmentation, VLANs, Domain Isolation, or IP Security Policies.

- Windows

1. VLANs

There aren't VLAN present in windows machine. VLANs are created and operated within an Ethernet network to perform isolation per network segment which is totally absent.

```
win10udstudent [Running] - Oracle VM VirtualBox
Administrator: Windows PowerShell
C:\Windows\system32>ipconfig/all

Windows IP Configuration

Host Name . . . . . : win10-udstudent
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled . . . . . : No
WINS Proxy Enabled . . . . . : No
DNS Suffix Search List . . . . . :

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . . .
Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Physical Address . . . . . : 08-00-27-F8-A2-F7
DHCP Enabled . . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::4c97:d25e:7a35:8c12%10(PREFERRED)
IPv4 Address . . . . . : 10.0.2.5(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained . . . . . : Thursday, October 6, 2022 8:53:38 AM
Lease Expires . . . . . : Thursday, October 6, 2022 12:58:38 PM
Default Gateway . . . . . : 10.0.2.1
DHCP Server . . . . . : 10.0.2.3
DHCPv6 IAID . . . . . : 50855975
DHCPv6 Client DUID . . . . . : 00-01-00-01-2A-C4-42-0E-0B-00-27-F8-A2-F7
DNS Servers . . . . . : 10.0.2.1
NetBIOS over Tcpip . . . . . : Enabled

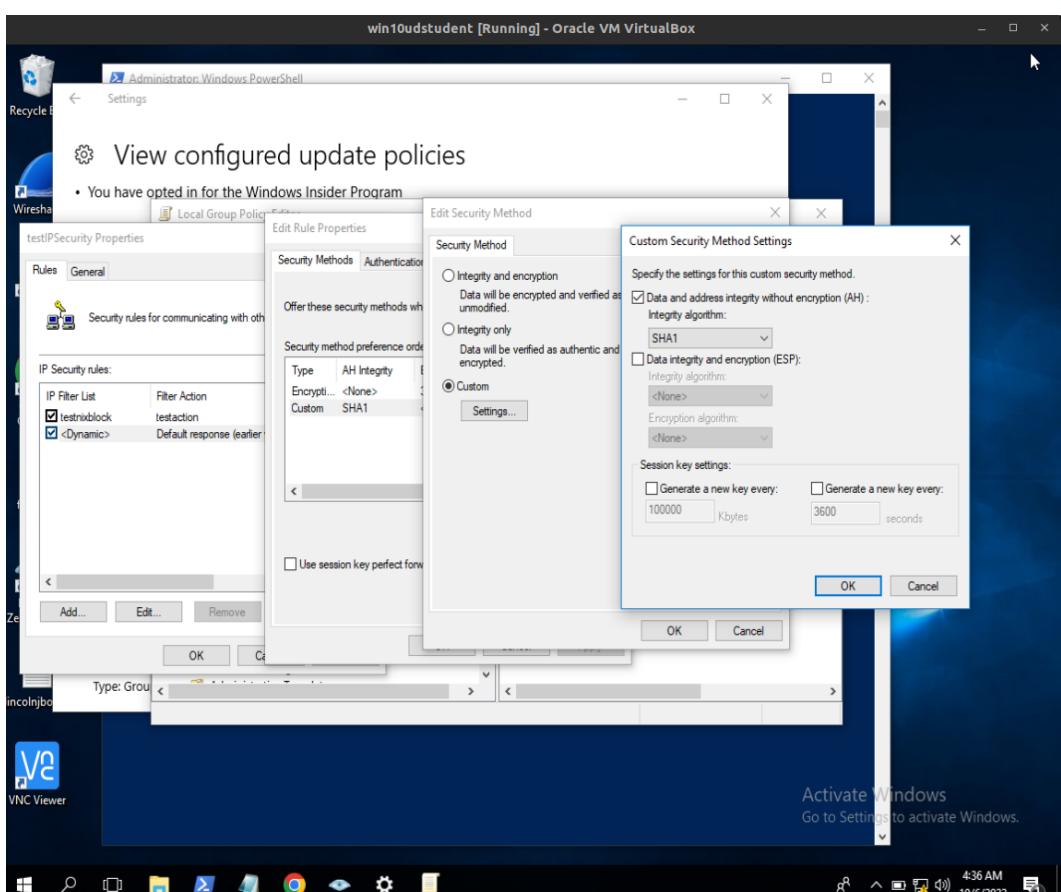
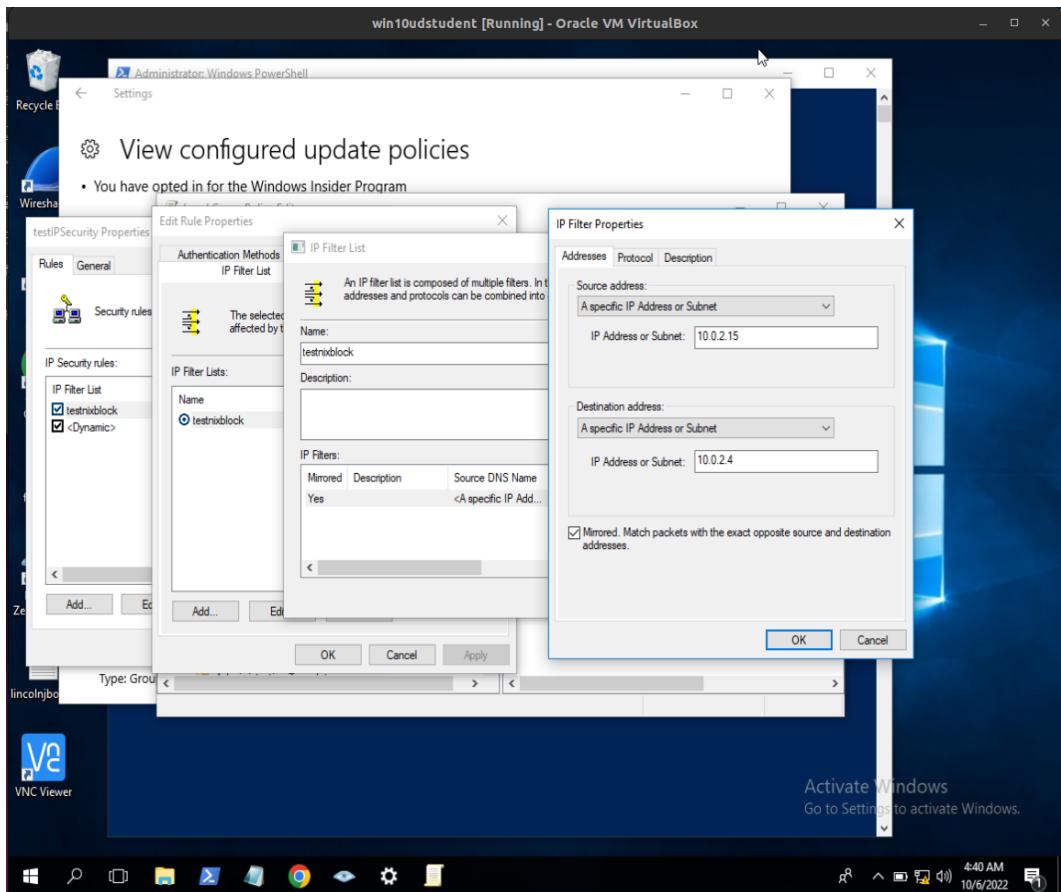
Tunnel adapter Teredo Tunneling Pseudo-Interface:

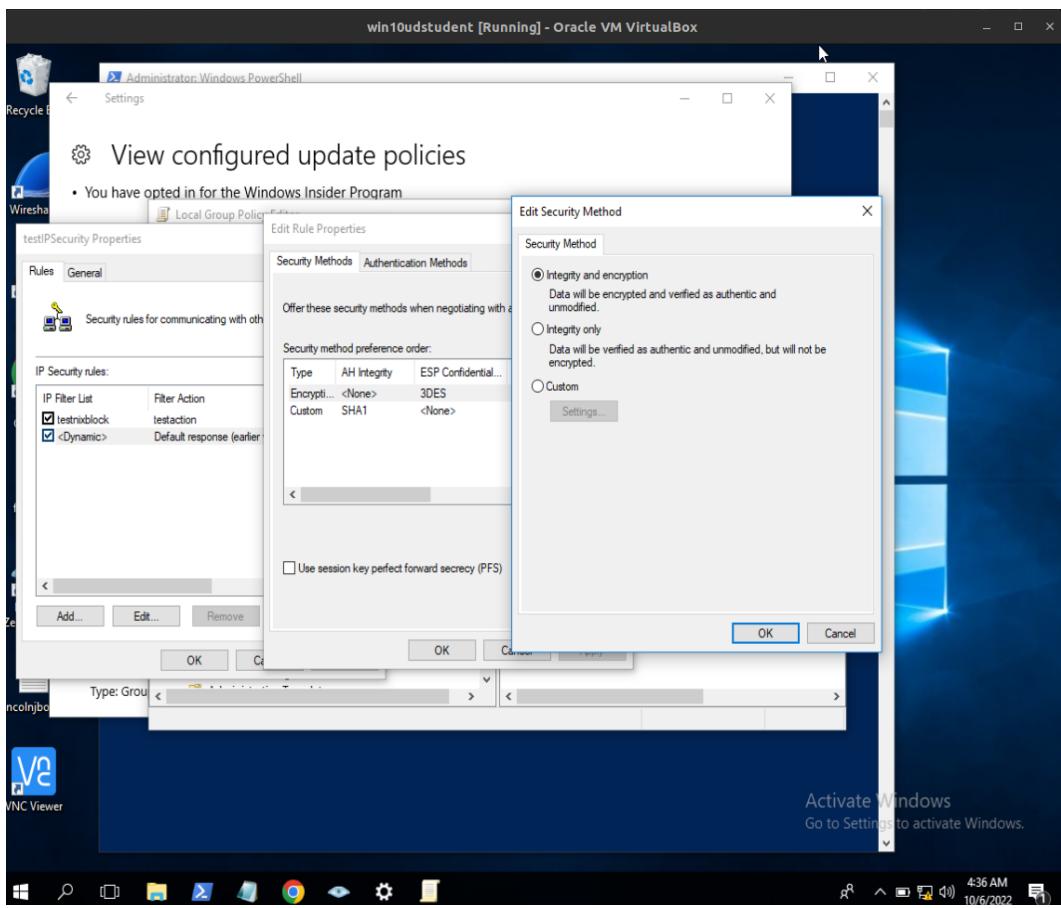
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . .
Description . . . . . : Teredo Tunneling Pseudo-Interface
Physical Address . . . . . : 00-00-00-00-00-00-E0
DHCP Enabled . . . . . : No
Autoconfiguration Enabled . . . . . : Yes

C:\Windows\system32>
```

win10udstudent ova

2. IP Security policies, Domain Isolation & Network Segmentation





win10udstudent ova

Here there is a IPSEC Policy blocking traffic from 10.0.2.15 which is an address into the range of the local network that has as destination the Ubuntu machine called ustudent@ubu-ustudent.

Besides this policy, there is an encryption specification to encrypt the communications of the dynamically assigned addresses.

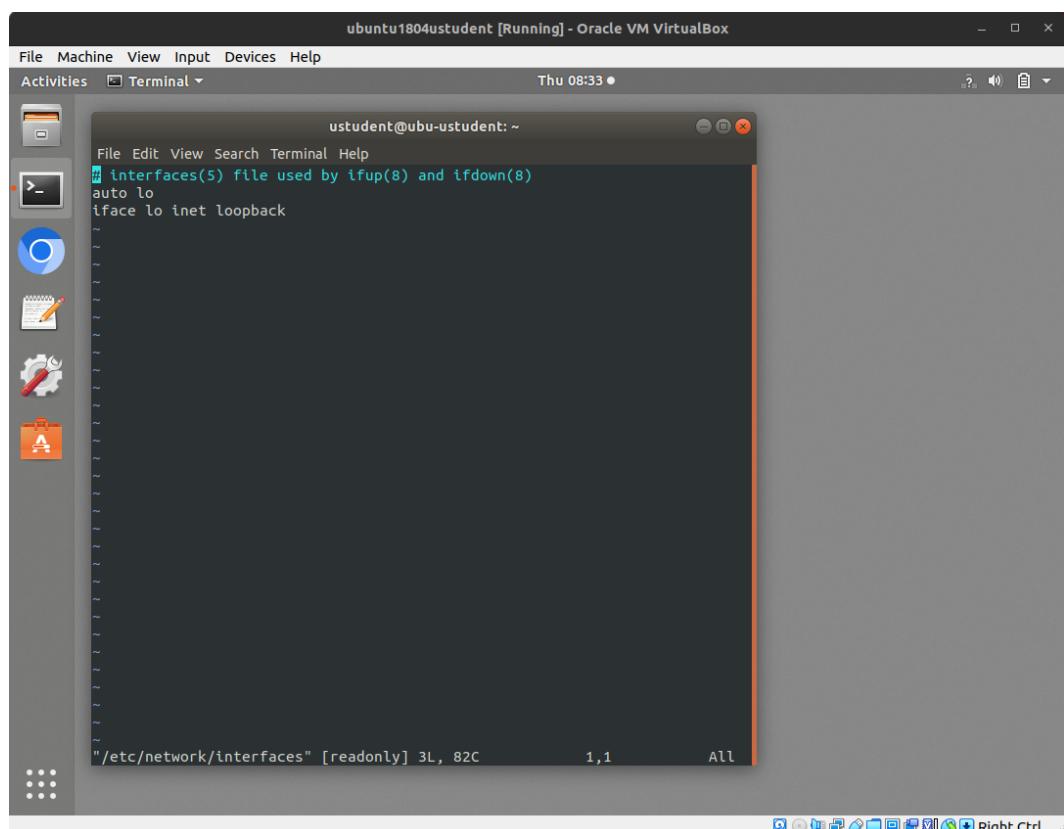
In this way, there is no Domain Isolation enforced from IPSecurity Policies since there isn't rule schemas for Group Policies besides the blocking rule mentioned.

In this scenario there are no VLANs created, no isolated hosts within a defined VLAN, hosts can directly connect with each other without segmentation and no trunks as point to point links between devices nor physical segmentation used. So, no Network Segmentation signs were found.

2.1 Current settings on Network Segmentation, VLANs, Domain Isolation, or IP Security Policies.

- Ubuntu

1. VLANs



The screenshot shows a terminal window titled "ubuntu1804ustudent [Running] - Oracle VM VirtualBox". The window is part of the Unity desktop environment. The terminal displays the following content:

```
File Edit View Search Terminal Help
# interfaces(5) file used by ifup(8) and ifdown(8)
auto lo
iface lo inet loopback
```

The terminal window has a dark background with light-colored text. The status bar at the bottom shows the file path "/etc/network/interfaces" [readonly], 3L, 82C, line 1, column 1, and the word "All".

ustudent@ubu-ustudent ova

No VLAN has been set in the Ubuntu machine, in this sense there is no isolation per network segment or networks are segmentation neither.

The screenshot shows a terminal window titled "ubuntu1804ustudent [Running] - Oracle VM VirtualBox". The window displays the output of the command "ifconfig -a". The output shows three network interfaces: enp0s3, enp0s8, and lo. The enp0s3 interface is an Ethernet interface with MAC address fe80::afbe:12e7:52cd:c70e, IP address 10.0.2.4, and subnet mask 255.255.255.0. The enp0s8 interface is another Ethernet interface with MAC address 08:00:27:66:59:64, IP address 10.0.2.1, and subnet mask 255.255.255.0. The lo interface is the loopback interface with IP address 127.0.0.1 and subnet mask 255.0.0.0.

```
ubuntu1804ustudent [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Thu 08:37 •
ustudent@ubu-ustudent:~$ ifconfig -a
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 10.0.2.4 brd 10.0.2.255 netmask 255.255.255.0
        ether fe80::afbe:12e7:52cd:c70e brd fe80::fffe:12e7:52cd:c70e
        txqueuelen 1000 (Ethernet)
        RX packets 421363 bytes 630696078 (630.6 MB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 41417 bytes 2626160 (2.6 MB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        ether 08:00:27:66:59:64 brd ff:ff:ff:ff:ff:ff
        txqueuelen 1000 (Ethernet)
        RX packets 0 bytes 0 (0.0 B)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 5340 bytes 961637 (961.6 KB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 brd 127.0.0.1 netmask 255.0.0.0
        loop txqueuelen 1000 (Local Loopback)
        RX packets 10014 bytes 650745 (650.7 KB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 10014 bytes 650745 (650.7 KB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ustudent@ubu-ustudent:~$
```

ustudent@ubu-ustudent ova

This screenshot shows the absence of any VLANs configuration in the interfaces detected by the system which matches with no configuration set related to interfaces in the file showed before.

2. IP Security policies, Domain Isolation & Network Segmentation

ubuntu1804student [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities Terminal Thu 08:36 •

? ⓘ 自

The screenshot shows a terminal window titled "ustudent@ubu-ustudent: ~". The window displays the contents of the "/etc/hosts.allow" file. The file includes comments about host access lists, examples for local and remote hosts, and a note about protecting portmapper. The terminal interface has a dark theme with orange highlights. The desktop background is visible behind the terminal window, showing icons for various applications like a browser, file manager, and system settings.

```
ustudent@ubu-ustudent: ~
File Edit View Search Terminal Help
/etc/hosts.allow: list of hosts that are allowed to access the system.
See the manual pages hosts_access(5) and hosts_options
(5).
#
# Example:    ALL: LOCAL @some_netgroup
#                  ALL: .foobar.edu EXCEPT terminalserver.foobar.edu
#
# If you're going to protect the portmapper use the name "rpcbind" for the
# daemon name. See rpcbind(8) and rpc.mountd(8) for further information.
#
~
~
```

"/etc/hosts.allow" [readonly] 10L, 411C 1,1 All

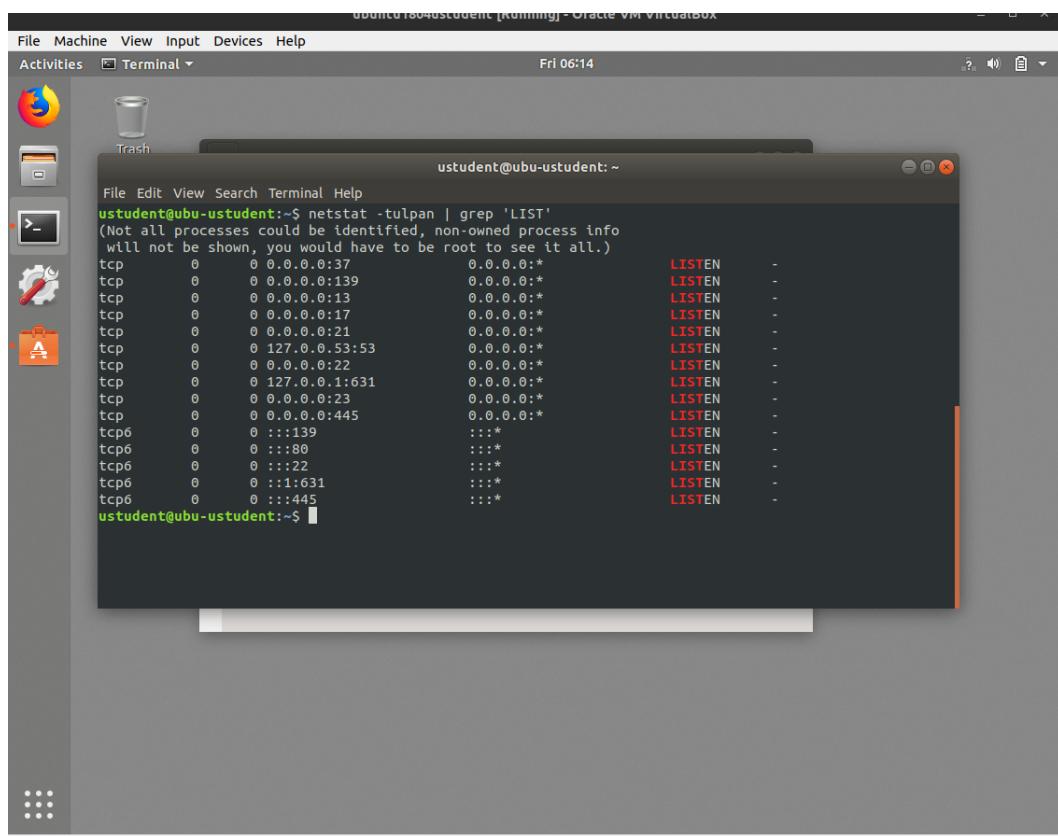
ustudent@ubu-ustudent ova

According to the files consulted, there were no IP Security policies implemented in order to block or allow ip addresses or segment the traffic in that sense. No rules related to isolate domains or prevent promiscuity in any form. In order to this, there isn't policies related to Network Segmentation or Domain Isolation in the Ubuntu machine.

2.2 Remote access services and protocols, their security level, which are running on these systems, networking features that should be disabled or hardened, and consider that in the context of IPv4 and IPv6.

Ubuntu

1. Remote access services and protocols



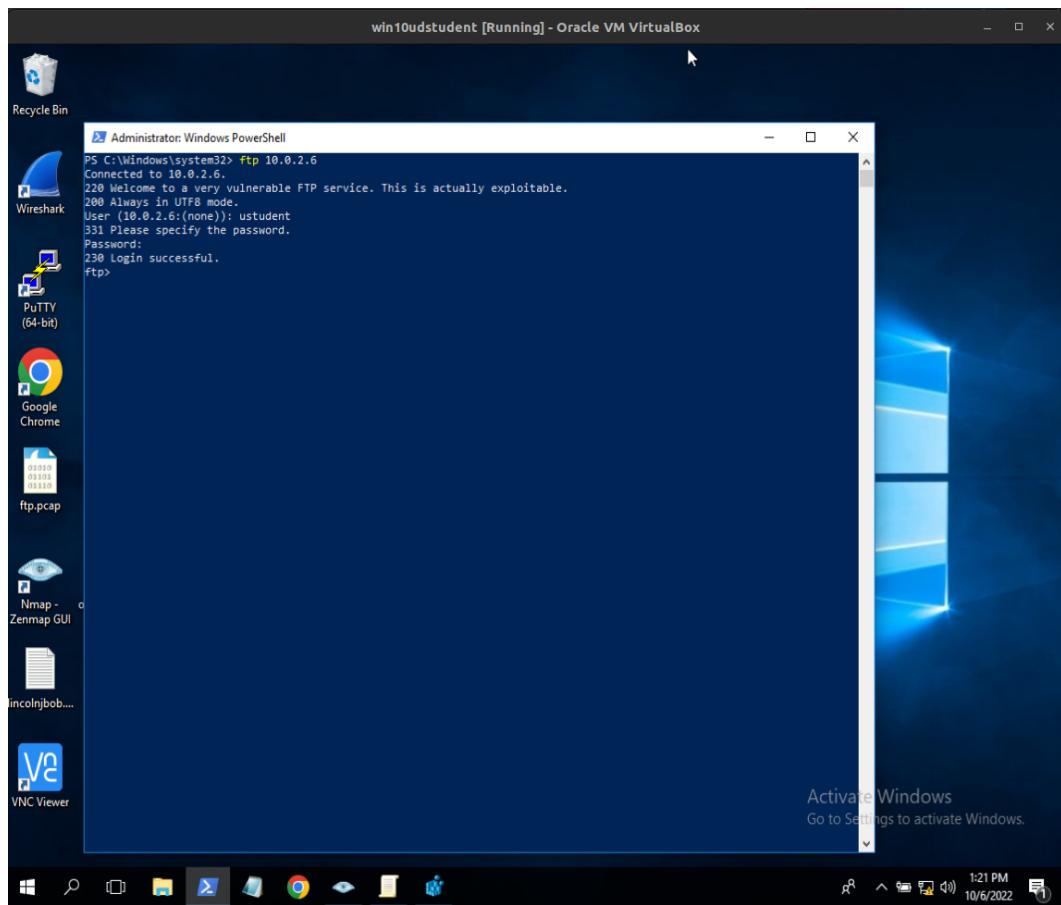
The screenshot shows a desktop environment with a terminal window open. The terminal window title is "ustudent@ubu-ustudent: ~". The terminal displays the command "netstat -tulpn | grep 'LIST'" and its output. The output lists various network ports and their states:

```
ustudent@ubu-ustudent:~$ netstat -tulpn | grep 'LIST'
(Not all processes could be identified, non-owned process info
will not be shown, you would have to be root to see it all.)
tcp        0      0 0.0.0.0:37          0.0.0.*      LISTEN
tcp        0      0 0.0.0.0:139         0.0.0.*      LISTEN
tcp        0      0 0.0.0.0:13          0.0.0.*      LISTEN
tcp        0      0 0.0.0.0:17          0.0.0.*      LISTEN
tcp        0      0 0.0.0.0:21          0.0.0.*      LISTEN
tcp        0      0 127.0.0.53:53       0.0.0.*      LISTEN
tcp        0      0 0.0.0.0:22          0.0.0.*      LISTEN
tcp        0      0 127.0.0.1:631        0.0.0.*      LISTEN
tcp        0      0 0.0.0.0:23          0.0.0.*      LISTEN
tcp        0      0 0.0.0.0:445         0.0.0.*      LISTEN
tcp6       0      0 ::1:139           ::*          LISTEN
tcp6       0      0 ::1:80            ::*          LISTEN
tcp6       0      0 ::1:22            ::*          LISTEN
tcp6       0      0 ::1:631           ::*          LISTEN
tcp6       0      0 ::1:445           ::*          LISTEN
ustudent@ubu-ustudent:~$
```

ustudent@ubu-ustudent ova

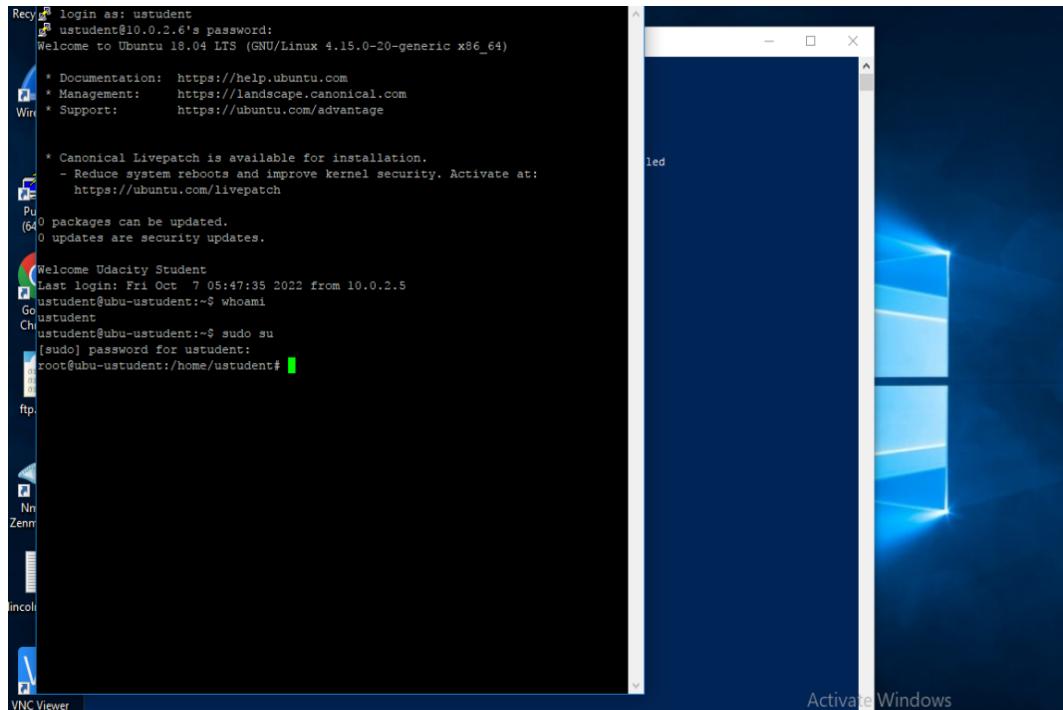
Remote access services and protocols in place allocate in port 21 (FTP), 22 (SSH) and 23 (telnet) as seen in the image above. These ports are open and ready waiting for connections, they are listening for external requests of service.

- **FTP (21)**



win10udstudent ova

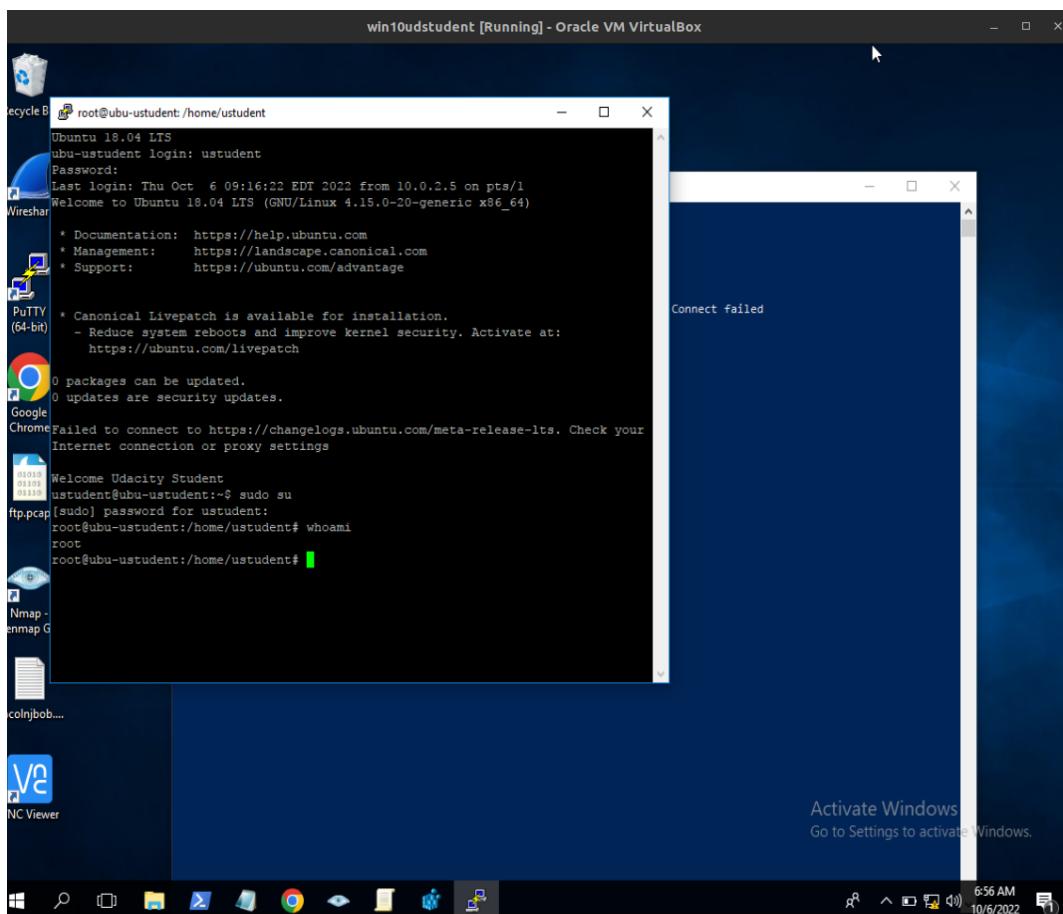
- **SSH (22)**



win10udstudent ova

- SSH provide system information after the user has been authenticated (line 3).

- Telnet (23)



win10udstudent ova

- Telnet provide system information before the user has been authenticated (line 1).

Each of the three remote services and protocols shares a bundle of insecure characteristics.

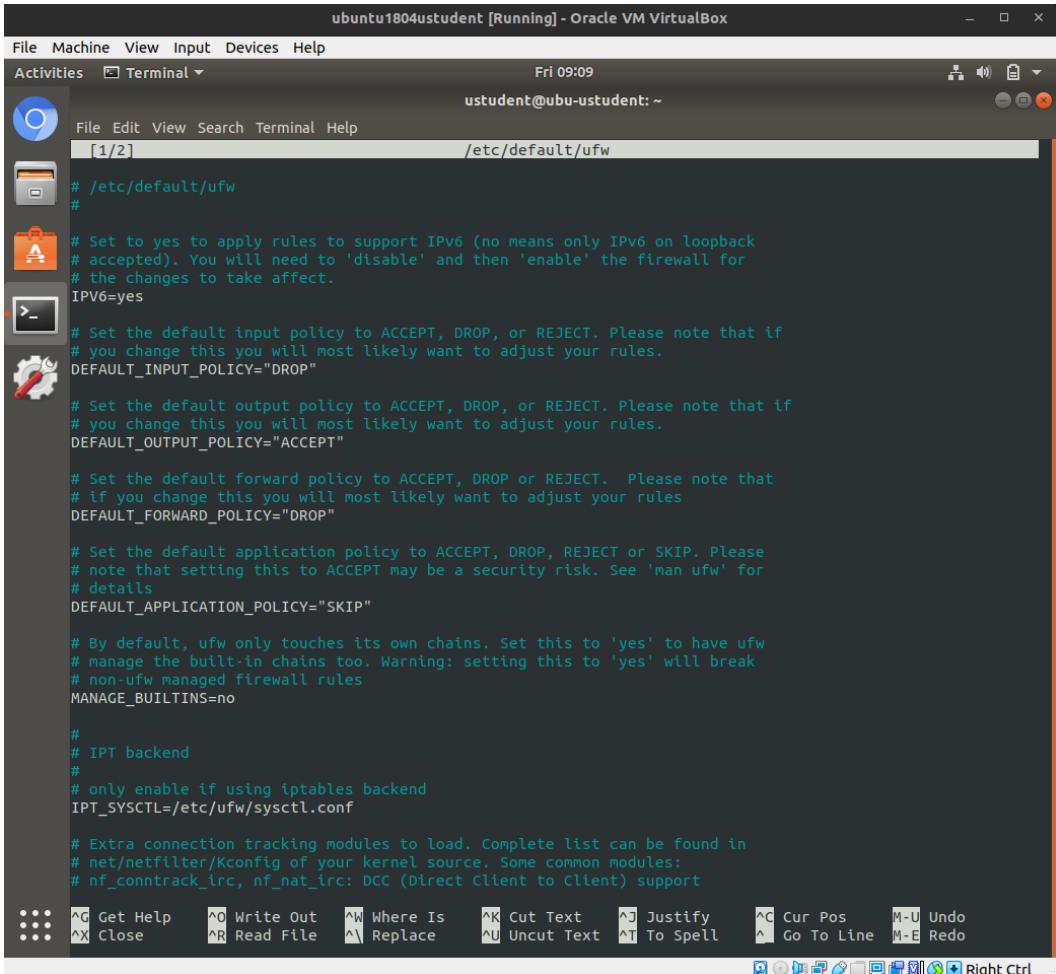
There is no constraints in order to filter inbound connections as seen in the previous topics nor firewalls (images in next topic - 2.3) rules that apply any layer of protection more than the user & password of the system (which is not a 100% secure protection).

It is possible to see how any connection that provides the correct user & password can get into the system unregardless its location (ip geolocation), ip address or any IP Security policy nor any kind of network segmentation or domain isolation.

Telnet connections provides information of the system as well, even before a connection has been established (just by request for service) giving to potential attackers one more piece of the information to break into the system. SSH provide it after the user has been authenticated.

Once the credentials are correctly provided, the connection is authenticated and authorized as system user. It's allowed to access to all the information as group member, execute allowed commands for the group, execute sudo commands and even become root user as seen in the picture above.

- IPv6



The screenshot shows a terminal window titled "ubuntu1804ustudent [Running] - Oracle VM VirtualBox". The window is running on a dark-themed desktop environment. The terminal title bar includes the session name, host name, and date ("Fri 09:09"). The terminal window itself has a dark background and light-colored text. It displays the contents of the file "/etc/default/ufw". The configuration includes several policy settings:

```
# /etc/default/ufw
#
# Set to yes to apply rules to support IPv6 (no means only IPv4 on loopback
# accepted). You will need to 'disable' and then 'enable' the firewall for
# the changes to take affect.
IPV6=yes

# Set the default input policy to ACCEPT, DROP, or REJECT. Please note that if
# you change this you will most likely want to adjust your rules.
DEFAULT_INPUT_POLICY="DROP"

# Set the default output policy to ACCEPT, DROP, or REJECT. Please note that if
# you change this you will most likely want to adjust your rules.
DEFAULT_OUTPUT_POLICY="ACCEPT"

# Set the default forward policy to ACCEPT, DROP or REJECT. Please note that
# if you change this you will most likely want to adjust your rules
DEFAULT_FORWARD_POLICY="DROP"

# Set the default application policy to ACCEPT, DROP, REJECT or SKIP. Please
# note that setting this to ACCEPT may be a security risk. See 'man ufw' for
# details
DEFAULT_APPLICATION_POLICY="SKIP"

# By default, ufw only touches its own chains. Set this to 'yes' to have ufw
# manage the built-in chains too. Warning: setting this to 'yes' will break
# non-ufw managed firewall rules
MANAGE_BUILTINS=no

#
# IPT backend
#
# only enable if using iptables backend
IPT_SYSCTL=/etc/ufw/sysctl.conf

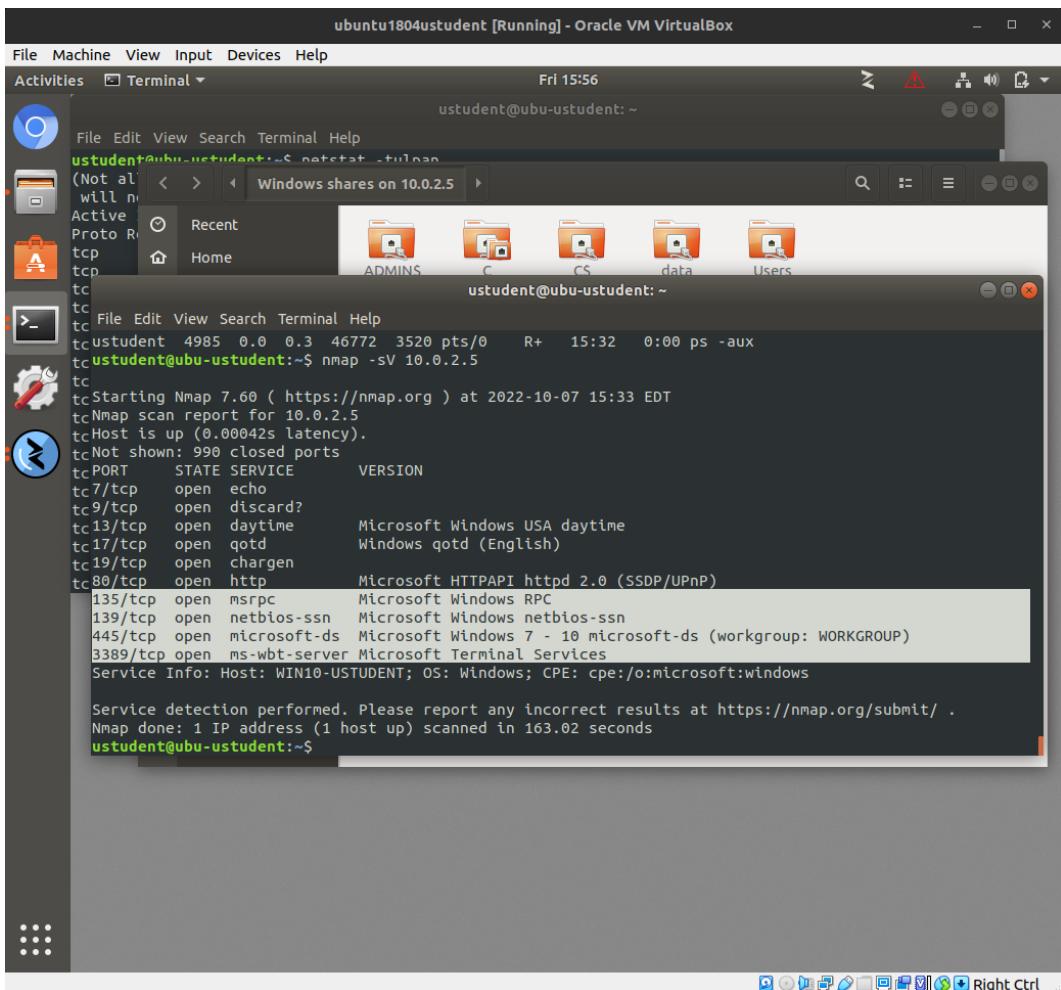
# Extra connection tracking modules to load. Complete list can be found in
# net/netfilter/Kconfig of your kernel source. Some common modules:
# nf_conntrack_lrc, nf_nat_lrc: DCC (Direct Client to Client) support
```

ustudent@ubu-ustudent ova

Settings concerning IPv6 are covered by the default policies for an Ubuntu system. As showed in the image, the configurations are to drop input, allow output and skip the traffic defined by applications.

Windows

1. Remote access services and protocols



The screenshot shows a terminal window titled "ubuntu1804student [Running] - Oracle VM VirtualBox". The terminal displays the output of an nmap scan against a Windows host at 10.0.2.5. The output shows several open ports:

```
ustudent@ubu-ustudent:~$ nmap -sV 10.0.2.5
Starting Nmap 7.60 ( https://nmap.org ) at 2022-10-07 15:33 EDT
Nmap scan report for 10.0.2.5
Host is up (0.00042s latency).

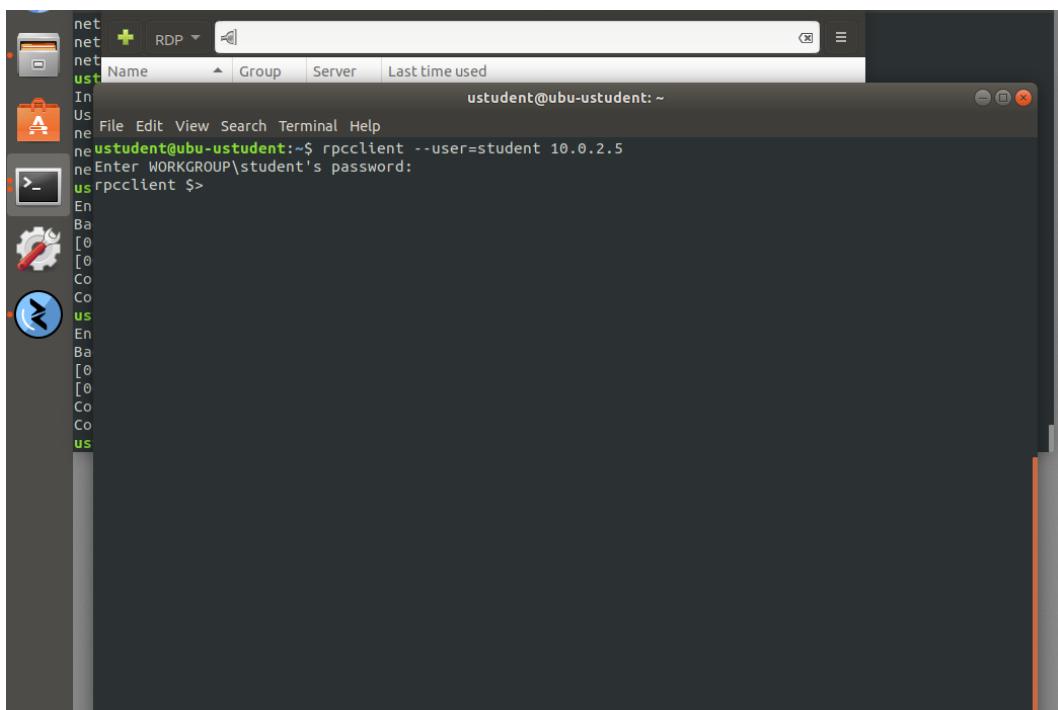
PORT      STATE SERVICE      VERSION
7/tcp      open  echo
9/tcp      open  discard?
13/tcp     open  daytime      Microsoft Windows USA daytime
17/tcp     open  qotd         Windows qotd (English)
19/tcp     open  chargen
80/tcp     open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
3389/tcp   open  ms-wbt-server Microsoft Terminal Services
Service Info: Host: WIN10-USTUDENT; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 163.02 seconds
ustudent@ubu-ustudent:~$
```

ustudent@ubu-ustudent ova

Remote access services and protocols in place allocate in port 135 (RPC), 139 (files & print sharing - SMB before Windows 2000), 445 (files & print sharing - SMB after Windows 2000) and 3389 (RDP) as seen in the image above. These ports are open and ready waiting for connections, listen for external request of service without more security than username & password.

- 135 (RPC)

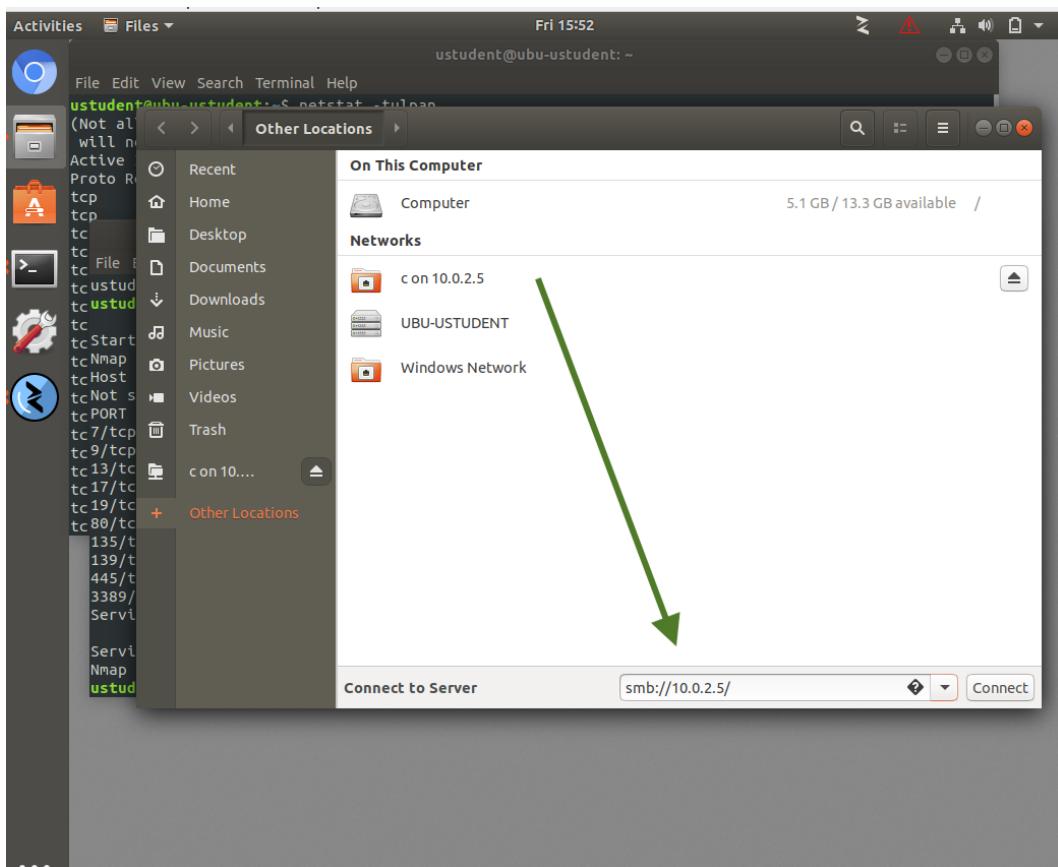


A screenshot of a terminal window titled "net" with the tab "RDP" selected. The window shows a file browser sidebar on the left. The terminal prompt is "ustudent@ubu-ustudent:~". The user has run the command "rpcclient --user=student 10.0.2.5" and is prompted to enter the password for the WORKGROUP\student account. The password is partially visible as "En [0 [0 Co Co us".

win10udstudent ova

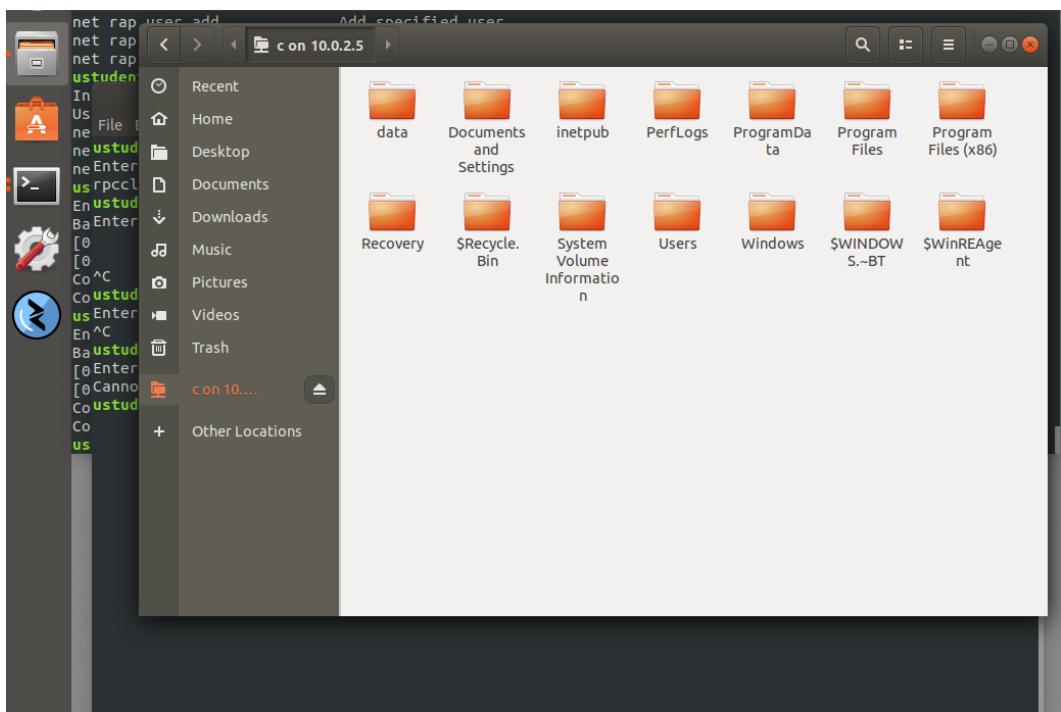
Remote Procedure Call (RPC) port 135 is used in client/server applications such as Exchange clients (e.g messenger service) as well as other Windows NT/2K/XP software, in order to allow one program to request service from a program on another computer.

- 445 (files & print sharing - SMB after Windows 2000)



SMB Protocol (Server Message Block Protocol) is a client-server communication protocol used for sharing access to files, printers.

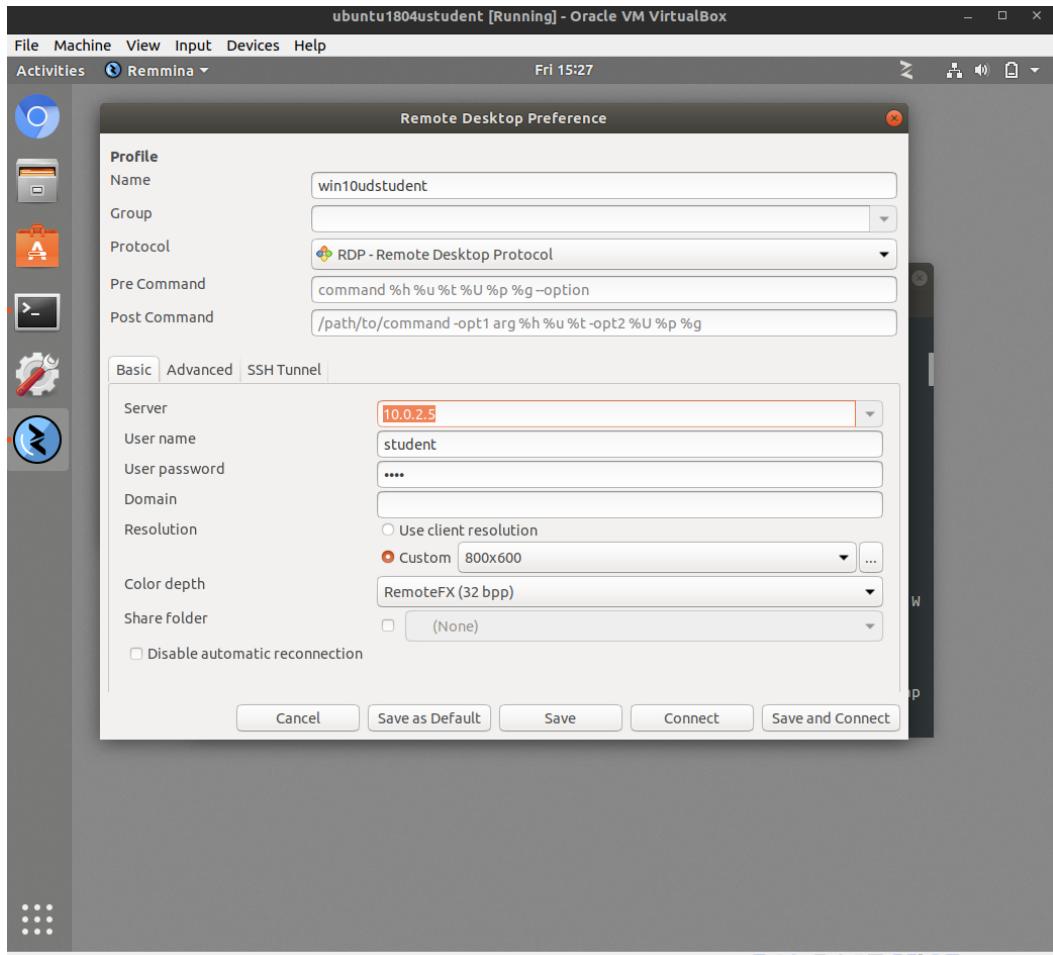
(following in the next page)



```
win10student [Running] - Oracle VM VirtualBox
PS C:\Windows\system32> netstat -na
Active Connections

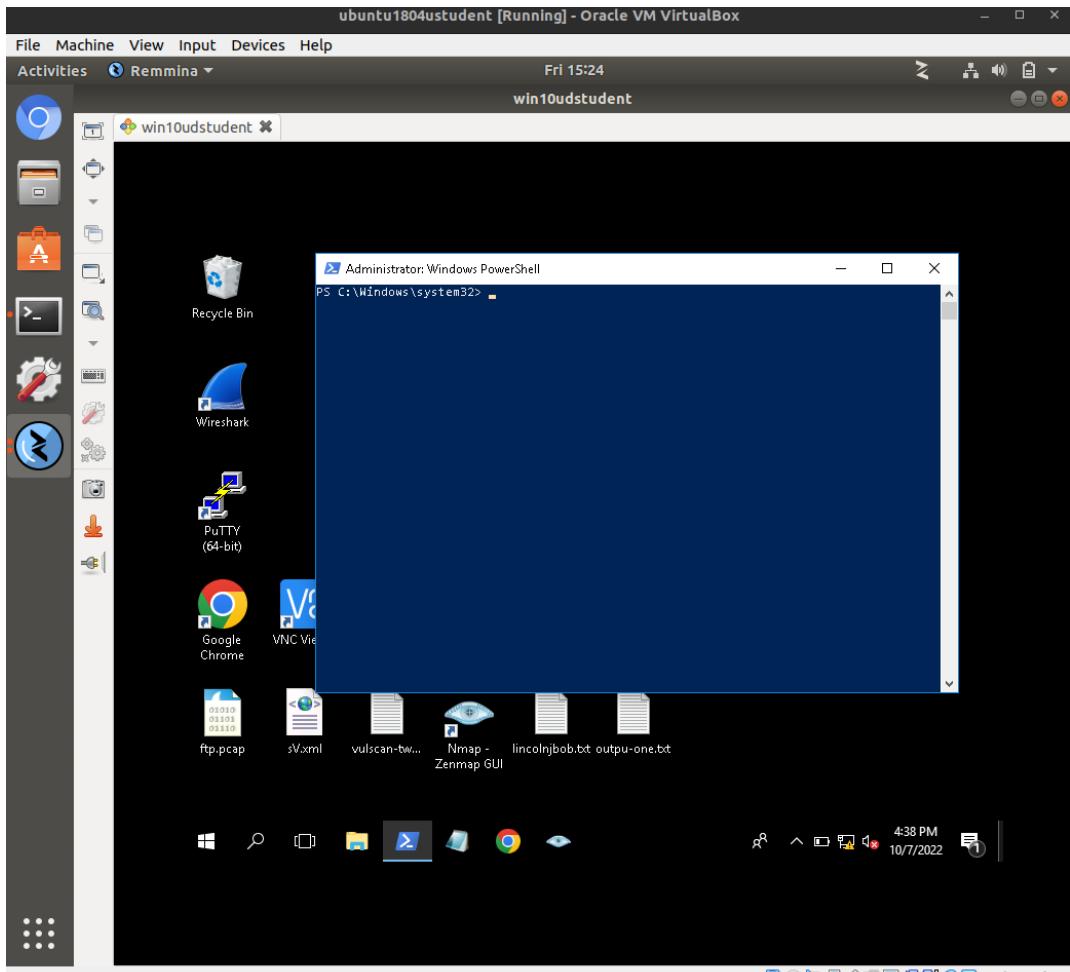
Proto Local Address          Foreign Address        State
TCP   0.0.0.0:7              0.0.0.0:0             LISTENING
TCP   0.0.0.0:9              0.0.0.0:0             LISTENING
TCP   0.0.0.0:13             0.0.0.0:0             LISTENING
TCP   0.0.0.0:17             0.0.0.0:0             LISTENING
TCP   0.0.0.0:19             0.0.0.0:0             LISTENING
TCP   0.0.0.0:80             0.0.0.0:0             LISTENING
TCP   0.0.0.0:135            0.0.0.0:0             LISTENING
TCP   0.0.0.0:445            0.0.0.0:0             LISTENING
TCP   0.0.0.0:1536            0.0.0.0:0             LISTENING
TCP   0.0.0.0:1537            0.0.0.0:0             LISTENING
TCP   0.0.0.0:1538            0.0.0.0:0             LISTENING
TCP   0.0.0.0:1539            0.0.0.0:0             LISTENING
TCP   0.0.0.0:1540            0.0.0.0:0             LISTENING
TCP   0.0.0.0:1541            0.0.0.0:0             LISTENING
TCP   0.0.0.0:1544            0.0.0.0:0             LISTENING
TCP   0.0.0.0:3389            0.0.0.0:0             LISTENING
TCP   0.0.0.0:5985            0.0.0.0:0             LISTENING
TCP   0.0.0.0:47001           0.0.0.0:0             LISTENING
TCP   10.0.2.5:139            0.0.0.0:0             LISTENING
TCP   10.0.2.5:445            10.0.2.11:48530      ESTABLISHED
TCP   10.0.2.5:5040            0.0.0.0:0             LISTENING
TCP   [::]:7                  [::]:0               LISTENING
TCP   [::]:9                  [::]:0               LISTENING
TCP   [::]:13                 [::]:0               LISTENING
TCP   [::]:17                 [::]:0               LISTENING
TCP   [::]:19                 [::]:0               LISTENING
TCP   [::]:80                 [::]:0               LISTENING
TCP   [::]:135                [::]:0               LISTENING
TCP   [::]:1445               [::]:0               LISTENING
TCP   [::]:1536                [::]:0               LISTENING
TCP   [::]:1537                [::]:0               LISTENING
TCP   [::]:1538                [::]:0               LISTENING
TCP   [::]:1539                [::]:0               LISTENING
TCP   [::]:1540                [::]:0               LISTENING
TCP   [::]:1541                [::]:0               LISTENING
TCP   [::]:1544                [::]:0               LISTENING
TCP   [::]:3389               [::]:0               LISTENING
TCP   [::]:5985               [::]:0               LISTENING
TCP   [::]:47001               [::]:0               LISTENING
UDP  0.0.0.0:7              :::*
UDP  0.0.0.0:9              :::*
UDP  0.0.0.0:13             :::*
UDP  0.0.0.0:17             :::*
UDP  0.0.0.0:19             :::*
UDP  0.0.0.0:123            :::*
UDP  0.0.0.0:161            :::*
UDP  0.0.0.0:506             :::*
UDP  0.0.0.0:983            :::*
UDP  0.0.0.0:3389            :::*
UDP  0.0.0.0:4500            :::*
UDP  0.0.0.0:5050            :::*
UDP  0.0.0.0:5353            :::*
```

- 3389 (RDP)



This test was used Rammina (image above), a remote desktop client app that supports RDP (Remote Desktop Protocol) used by Windows operating systems for remote connections.

(following in the next page)



Once the IP address, username and password, the Remote Desktop Client establish a connection that opens a window running a remote Windows desktop.

The Windows system provides about 4 insecure services and protocols, all of them are open and listen waiting to establish connections.

As seen before, since there is no security policies regarding inbound traffic that target those services, any connection that match a user & password access the system.

No ip address, IP Security policy nor any kind of network segmentation or domain isolation prevents from accessing.

No firewalls (images in next topic - 2.3) rules applies extra layers of protection.

This services and protocols shares insecure characteristics that makes them vulnerable. Once the credentials are correctly provided, the connection is authenticated and authorized as system user. It's allowed to access to all the information as group member, execute allowed commands for the group.

- IPv6

The screenshot shows a Windows PowerShell window titled "win10udstudent [Running] - Oracle VM VirtualBox". The command `ipconfig /all` is run, displaying network configuration details for the "Ethernet adapter Ethernet". The output includes host name, primary DNS suffix (win10-ustudent), node type (Hybrid), and various IP and DNS settings. Below this, the command `netsh advfirewall show currentprofile` is run, showing public profile settings like state (OFF), logging options, and file paths. The status bar at the bottom right indicates the date and time (10/3/2022, 12:03 AM).

```
Administrator: Windows PowerShell
PS C:\Windows\system32> ipconfig /all
Windows IP Configuration

Host Name . . . . . : win10-ustudent
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled . . . . . : No
WINS Proxy Enabled . . . . . : No
DNS Suffix Search List . . . . . :

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . . . . . :
Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Physical Address . . . . . : 08-00-27-F8-A2-F7
DHCP Enabled . . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::4c97:d25e:7a35:8c12%10(PREFERRED)
IPv4 Address . . . . . : 10.0.2.5(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained . . . . . : Friday, October 7, 2022 2:47:45 PM
Lease Expires . . . . . : Friday, October 7, 2022 11:47:45 PM
Default Gateway . . . . . : 10.0.2.1
DHCP Server . . . . . : 10.0.2.3
DHCPv6 T1ID . . . . . : 50855975
DHCPv6 Client DUID . . . . . : 00-01-00-01-2A-C4-42-0E-0B-00-27-F8-A2-F7
DNS Servers . . . . . : 10.0.2.1
NetBIOS over Tcpip . . . . . : Enabled

PS C:\Windows\system32> netsh advfirewall show currentprofile

Public Profile Settings:
-----
State OFF
Firewall Policy BlockInbound,AllowOutbound
LocalFirewallRules N/A (GPO-store only)
LocalConSecRules N/A (GPO-store only)
InboundUserNotification Enable
RemoteManagement Disable
UnicastResponseToMulticast Enable

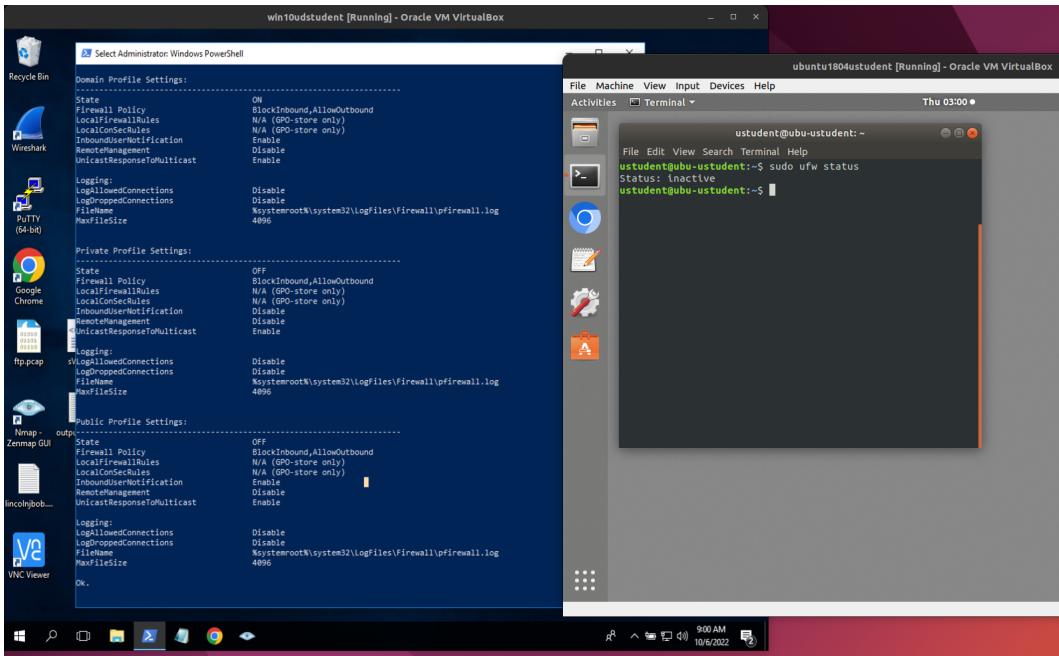
Logging:
LogAllowedConnections Disable
LogDroppedConnections Disable
FileName %systemroot%\system32\LogFiles\Firewall\pfirewall.log
MaxFileSize 4096

Ok.

PS C:\Windows\system32>
```

It's possible to see in the image above that the Windows system has a IPv6 assigned to the Ethernet interface for the local network but no policies has been given to protect this endpoint.

2.3 Firewalls



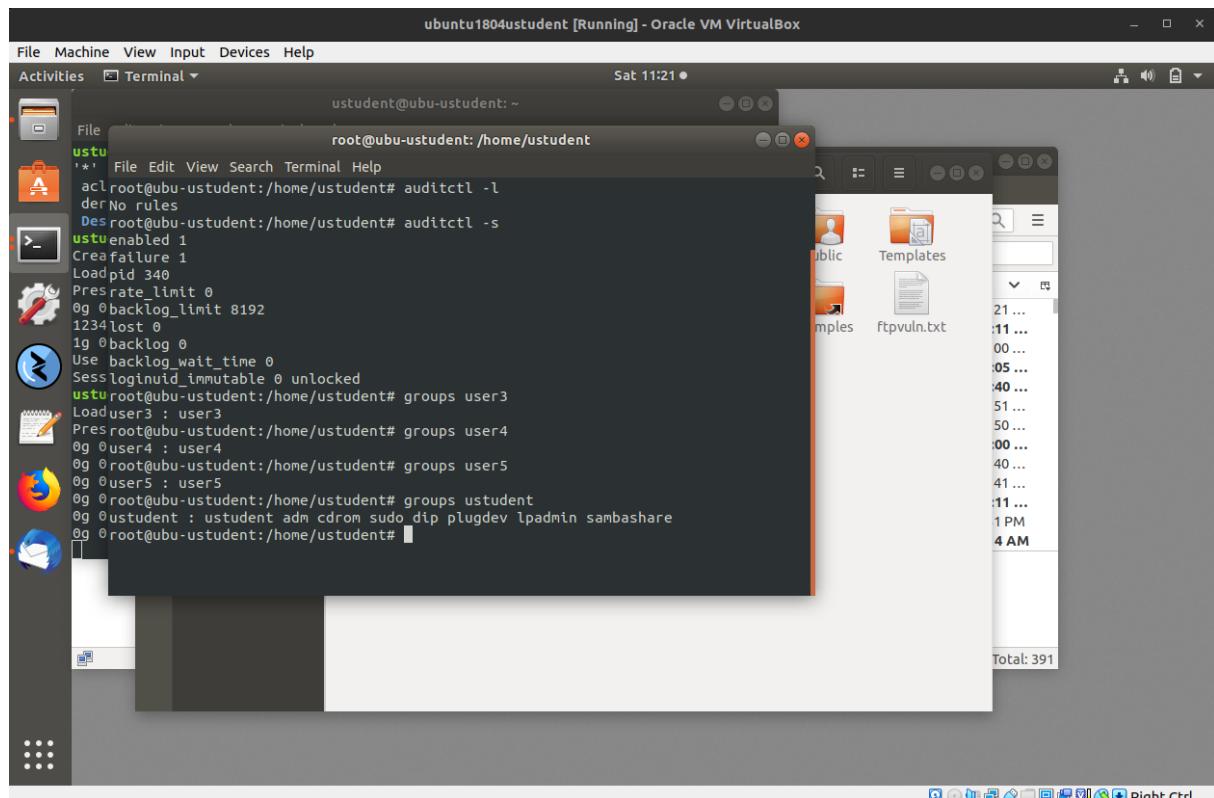
Windows / Ubuntu

Currently, the firewall is not active in the Ubuntu machine which means that there is no monitoring or control about the inbound and outbound traffic. In this scenario, If the internal network may be compromised, a malicious actor could move laterally inside the network without mayor difficulties.

2.4 Principles of Least Privilege

- Ubuntu

1. Which users have high privileges? uststudent

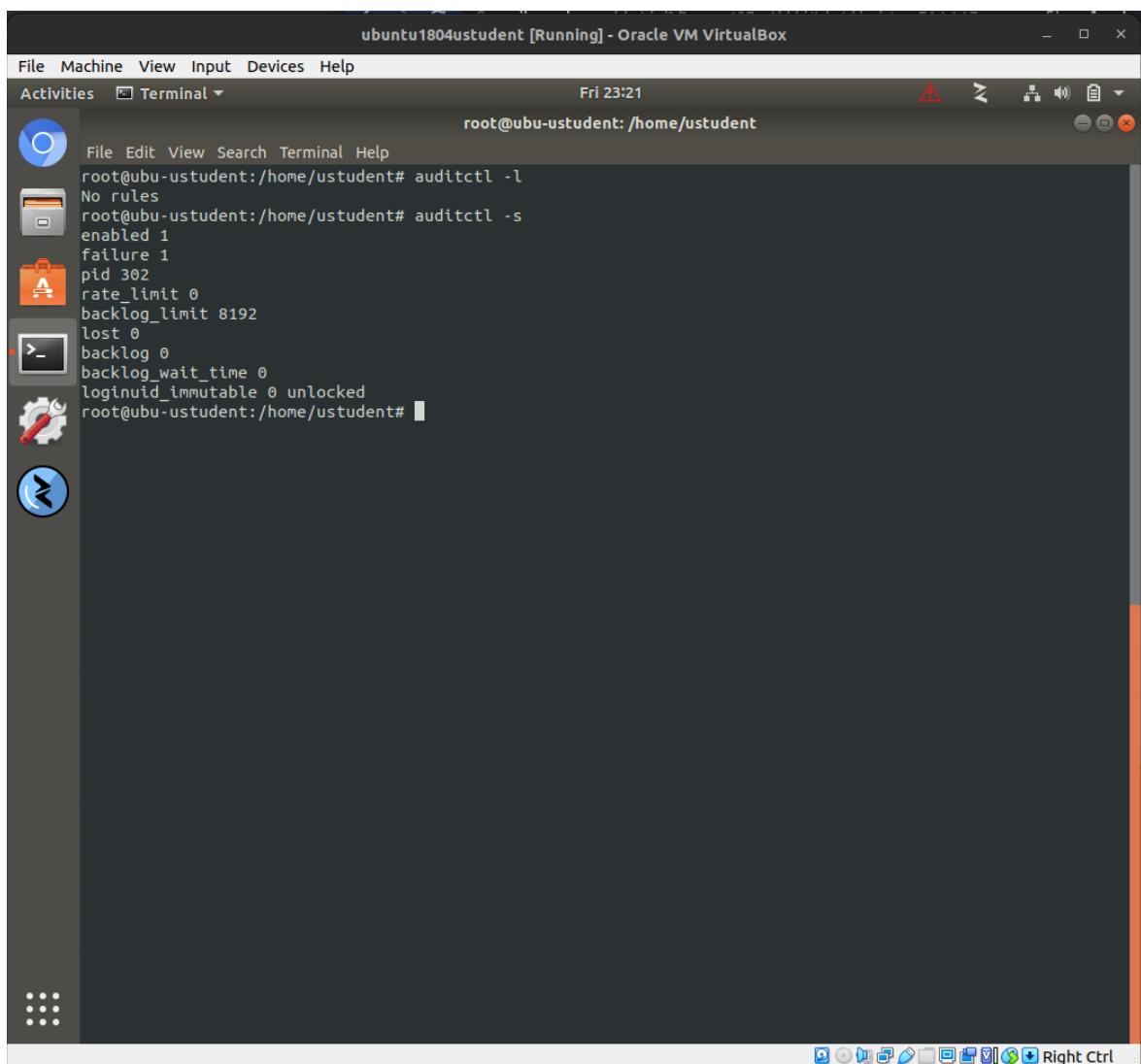


"ustudent" belongs to sudo group (between others) which allow it to use sudo commands and execute high level operations.

Numbered users and guest user belongs to their own groups without been related to sudo group or command.

2. Do important PII folders have the correct permissions and ownership? No policy has been set in relation with system commands, all the commands under sudo are available for user "ustudent". Users as "guest", "user3", "user4" or "user5" are out of sudo group but commands as stat or file are still available which provides metadata that belongs to the creator since there is no specific command restrictions.

No policy has been set in relation with identifiers provided by devices, applications, tools or protocols, such as internet protocol addresses, cookie identifiers or other identifiers. Any traces combined with unique identifiers and other information received by the servers, could be used to identify the persons who belong to.



The screenshot shows a Linux desktop environment with a dark theme. A terminal window titled "ubuntu1804ustudent [Running] - Oracle VM VirtualBox" is open, showing the following command-line session:

```
root@ubu-ustudent:/home/ustudent# auditctl -l
No rules
root@ubu-ustudent:/home/ustudent# auditctl -s
enabled 1
failure 1
pid 302
rate_limit 0
backlog_limit 8192
lost 0
backlog 0
backlog_wait_time 0
loginuid_immutable 0 unlocked
root@ubu-ustudent:/home/ustudent#
```

The desktop interface includes a docked panel on the left containing icons for Home, Applications, Activities, Dash, and Help. The top bar shows the window title, menu options (File, Machine, View, Input, Devices, Help), the date and time (Fri 23:21), and system status indicators. The bottom dock contains various application icons.

3. Are the default settings correct, and are there any excessive permissions? Permissions for numbered users (as user3, etc...) and "guest" are barely defined, they can access system folders and prompt out system files. They does not have permissions to modify or install programs in the system. Each of them has their own local folder and bash defined but without any isolation or jail which prevent from freely navigate across the system at the point of having each other access to a local folder that it doesn't belong.

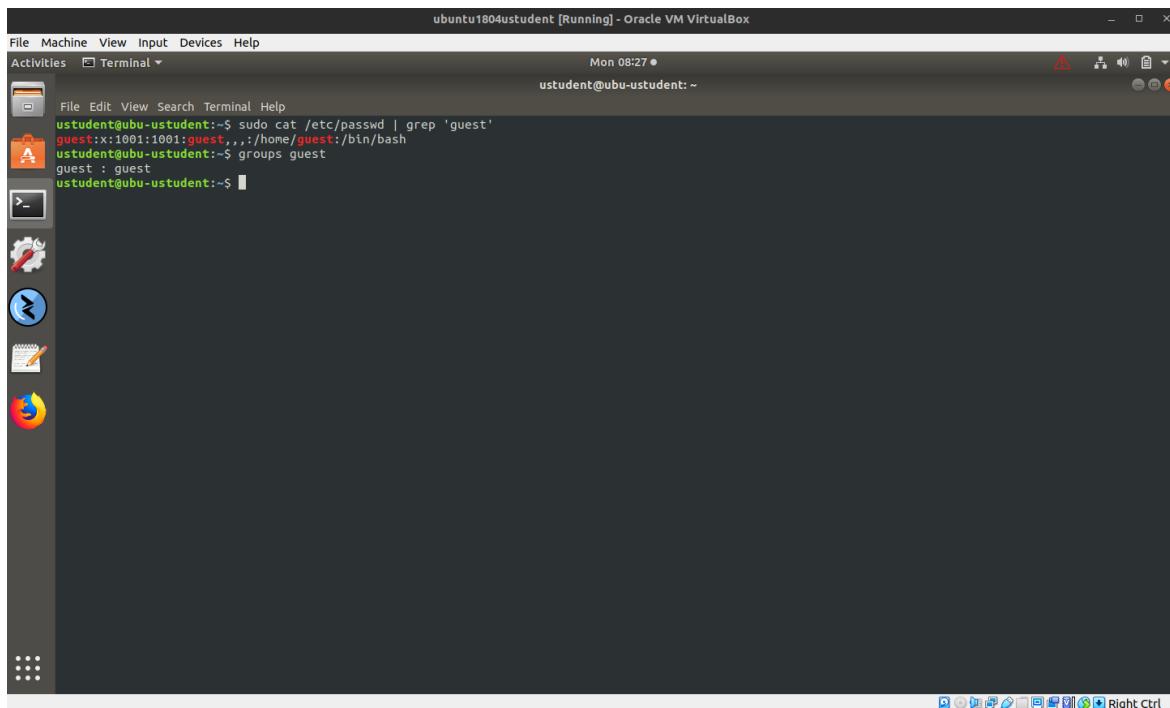
```

ubuntu1804ustudent [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Mon 08:12 •
ustudent@uba-ustudent: ~
File Edit View Search Terminal Help
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:system Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolved:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106:/home/syslog:/usr/sbin/nologin
messagebus:x:103:107:/nonexistent:/usr/sbin/nologin
apt:x:104:65534:/nonexistent:/usr/sbin/nologin
uuldd:x:105:111:/run/uuldd:/usr/sbin/nologin
avahi-autoipd:x:106:12:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
usbmux:x:107:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
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 Ooops 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/users5:/bin/bash
Debian-snmp:x:125:133::/var/lib/snmp:/bin/false
ustudent@uba-ustudent:~$ 

```

As it's shown in the image above, the absolute path of their shell (`/bin/bash`) is the system shell there is no replacement shell for the user accounts. The shell environment lacks of restrictions which increases the vulnerability of the system.

4. Are there "guest" accounts enabled? Are they allowed to use Sudo commands? Guest account are enabled but not allowed to use sudo commands.



Guest is allowed to log in and is also available, as it's shown, It doesn't belongs to sudo group.

5. Based on your findings, what should be done to secure these accounts and permissions better? There is too many accounts, guest, user3, user4, user5, they should be all condensed based in horizontal and vertical requirements, this is based in the needs of the target user and the scope of access that its group could have to system. This multiplicity of generic accounts shown the absence of defined user prospect in relation to their tasks, It's needed to be know what the user will do into the system, what tasks need to do, what are the systems, domains, services or resources the user need to access and grant permissions according to this. If it's needed according to their needs, more users and groups could be created following that basic criteria.

```

ubuntu1804student [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Mon 08:12 ~
ustudent@ubu-ustudent: ~

File Edit View Search Terminal Help
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
llist:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:IRCd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106:/home/syslog:/usr/sbin/nologin
messagebus:x:103:107:/nonexistent:/usr/sbin/nologin
messagebus:x:104:108:/nonexistent:/usr/sbin/nologin
apki:x:105:111:/run/apki:/usr/sbin/nologin
vdd:x:106:112:Vdd daemon,,,:/var/lib/vdd:/usr/sbin/nologin
avahi-autopid:x:106:112:Avahi autopid daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
usbmux:x:107:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
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
kerneloops:x:112:65534:Kernel Ooops 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:color colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
hplip:x:117:7:HP-LP system user,,,:/var/run/hplip:/bin/false
geoclue:x:118:124:/var/lib/geoclue:/usr/sbin/nologin
gmonit:x:119:125:Gmonit initial setup,,,:/var/lib/gmonit:/bin/false
gdm:x:120:125:Gnome Display Manager:/var/lib/gdm:/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
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
telnetd:x:123:131:/nonexistent:/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/users5:/bin/bash
ustudent@ubu-ustudent: ~

```

It's possible to see how the "numbered users" are replicated, there is no specifications that differentiates one from the other more than the name chosen for them. From that perspective, a deeper detailed requirements for the assignation of users identity should be done in order to avoid insecure access.

2.4 Principles of Least Privilege

- Windows

1. Which users have high privileges? student user is included in the Administrators group receiving high privileges, in contrast with numbered users out of this group preventing them of it.

Administrator: Windows PowerShell

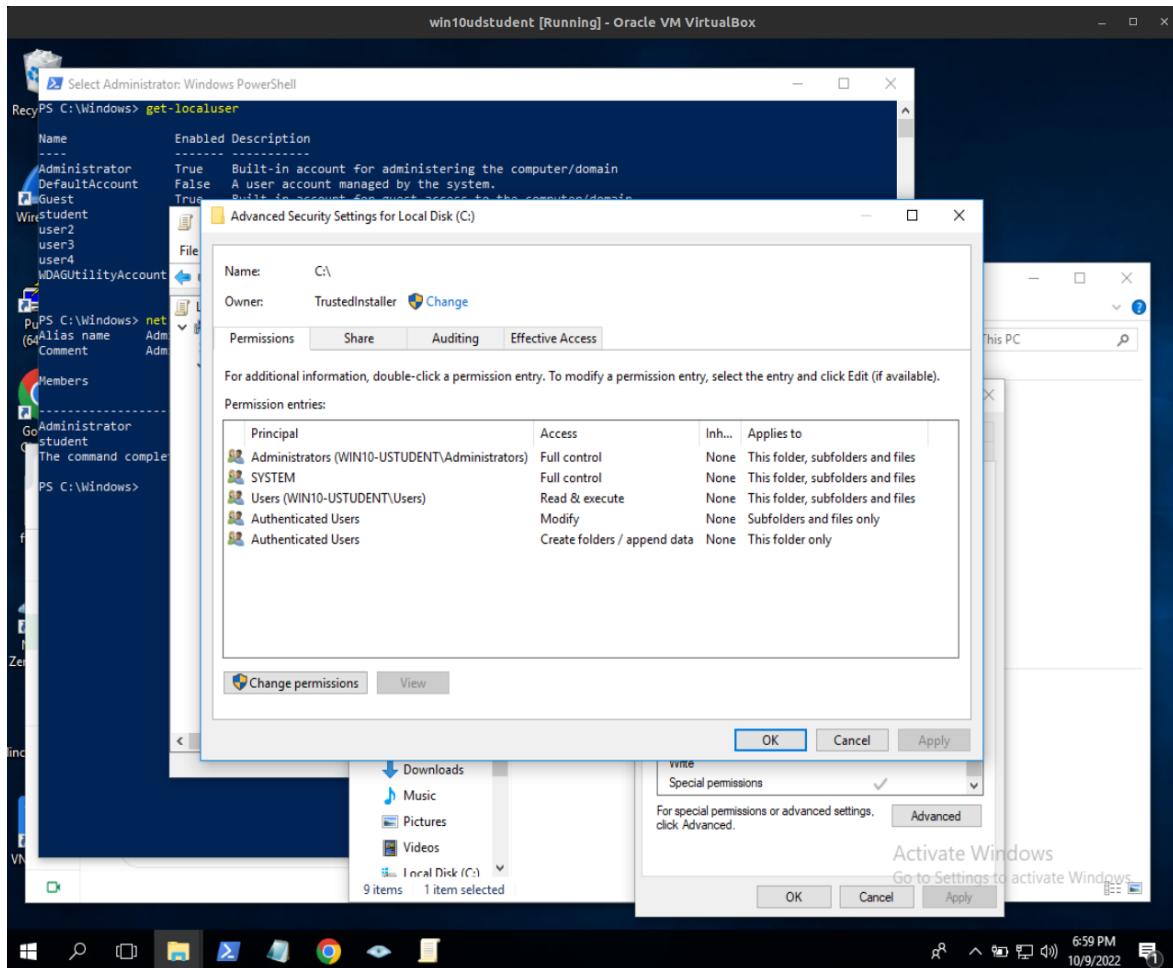
```
PS C:\Windows> get-localuser
Name          Enabled Description
----          --     -----
Administrator True   Built-in account for administering the computer/domain
DefaultAccount False  A user account managed by the system.
Guest          True   Built-in account for guest access to the computer/domain
Winstudent     True
user2          True
user3          True
user4          True
MDAGUtilityAccount False  A user account managed and used by the system for Windows Defender Application Guard scen...
PS C:\Windows> net localgroup Administrators
(64) Alias name      Administrators
Comment        Administrators have complete and unrestricted access to the computer/domain
Members
Administrator
Go student
The command completed successfully.

PS C:\Windows>
```

Activate Windows
Go to Settings to activate Windows.

2. Do important PII folders have the correct permissions and ownership?

No, Users has not full control over the system files and folders but they are allowed to modify subfolders from the C:\ directory, create, append, read and execute.



3. Are the default settings correct, and are there any excessive permissions? In order to best practices for windows, there is a lack of settings in the Local Group Policy:

Audit Detailed Tracking

- Audit DPAPI Activity: Success, Failure

Audit Logon/Logoff

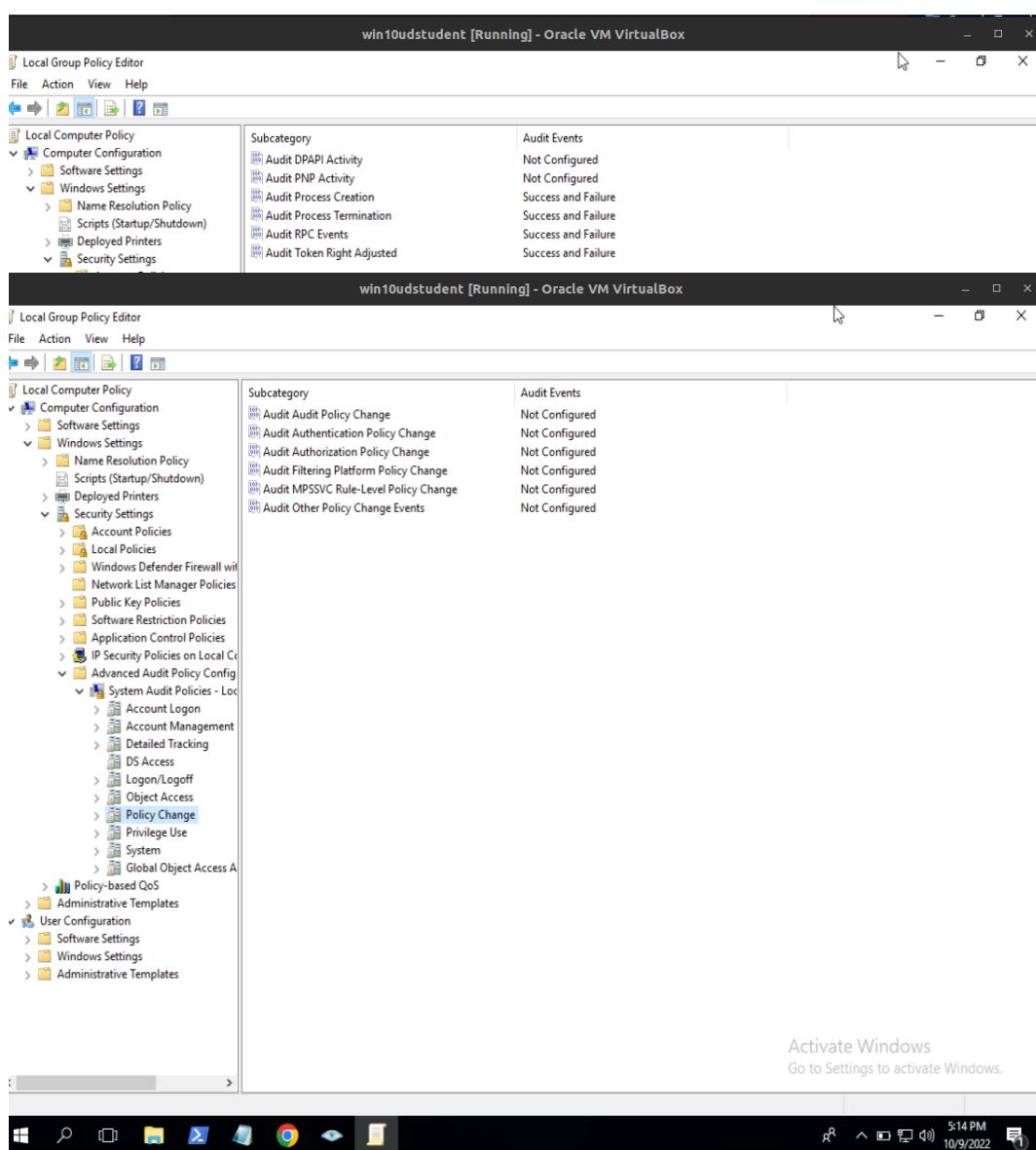
- Audit Account Lockout: Success, Failure

Policy Change

- Audit Policy Change: Success, Failure
- Audit Authentication Policy Change: Success, Failure
- Audit MPSSVC Rule-Level Policy Change: Success, Failure.

System

- Audit IPSec Driver: Success, Failure



Local Group Policy Editor [Running] - Oracle VM VirtualBox

File Action View Help

Local Computer Policy

Computer Configuration

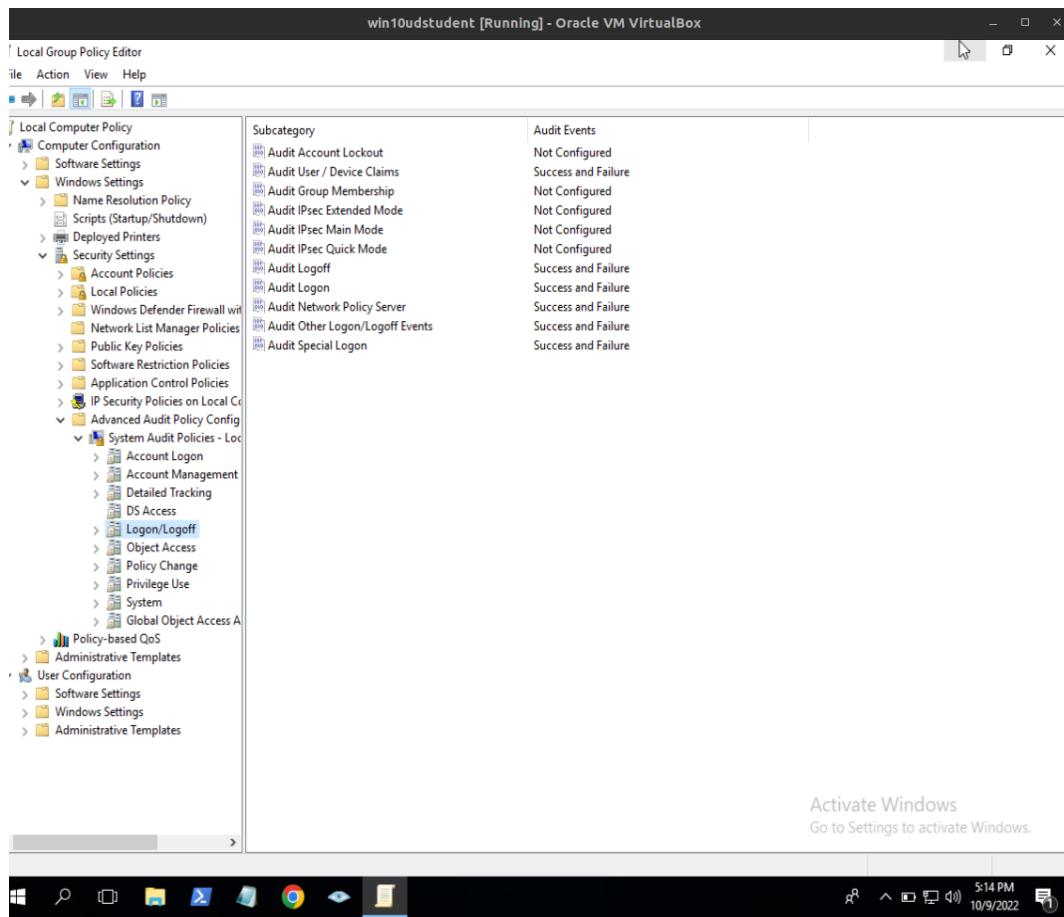
- Software Settings
- Windows Settings
 - Name Resolution Policy
 - Scripts (Startup/Shutdown)
 - Deployed Printers
 - Security Settings
 - Account Policies
 - Local Policies
 - Windows Defender Firewall with Advanced Security
 - Network List Manager Policies
 - Public Key Policies
 - Software Restriction Policies
 - Application Control Policies
 - IP Security Policies on Local Computer
 - Advanced Audit Policy Configuration
 - System Audit Policies - Local
 - Account Logon
 - Account Management
 - Detailed Tracking
 - DS Access
 - Logon/Logoff
 - Logon/Logoff
 - Object Access
 - Policy Change
 - Privilege Use
 - System
 - Global Object Access
- User Configuration
- Software Settings
- Windows Settings
- Administrative Templates

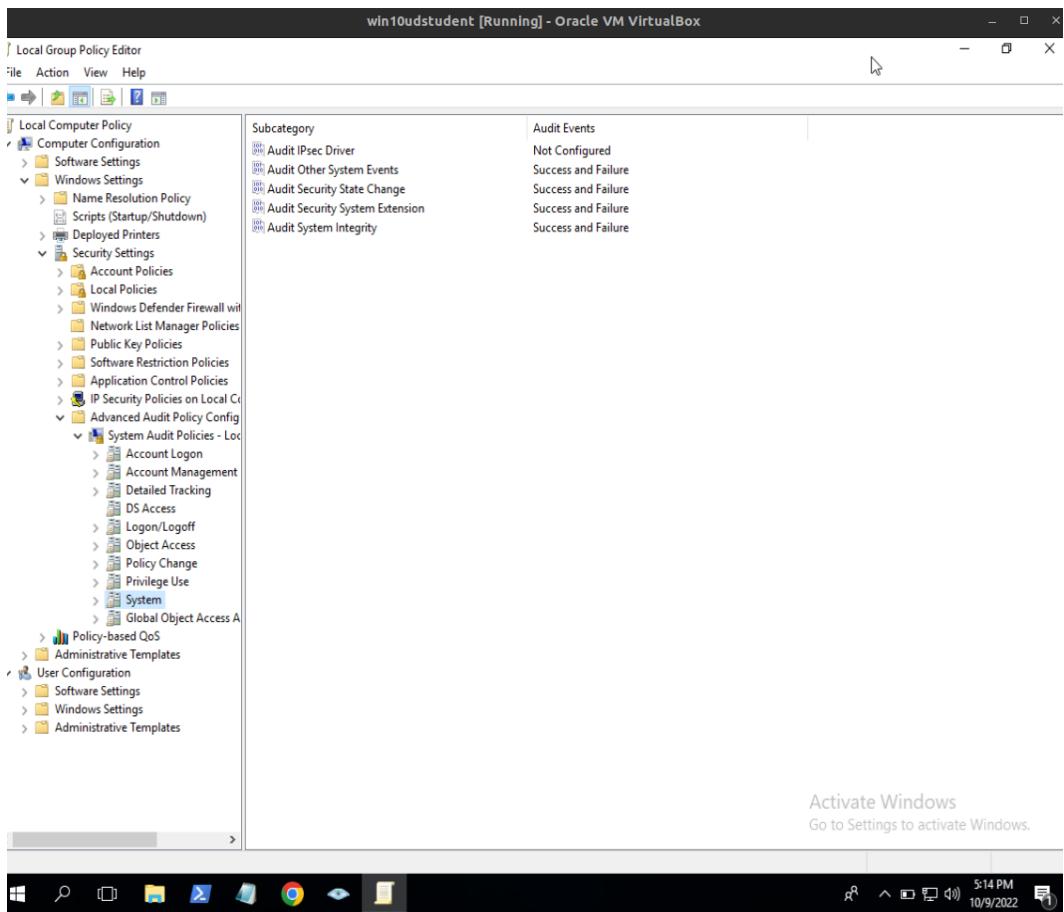
Subcategory

Subcategory	Audit Events
Audit Account Lockout	Not Configured
Audit User / Device Claims	Success and Failure
Audit Group Membership	Not Configured
Audit IPsec Extended Mode	Not Configured
Audit IPsec Main Mode	Not Configured
Audit IPsec Quick Mode	Not Configured
Audit Logoff	Success and Failure
Audit Logon	Success and Failure
Audit Network Policy Server	Success and Failure
Audit Other Logon/Logoff Events	Success and Failure
Audit Special Logon	Success and Failure

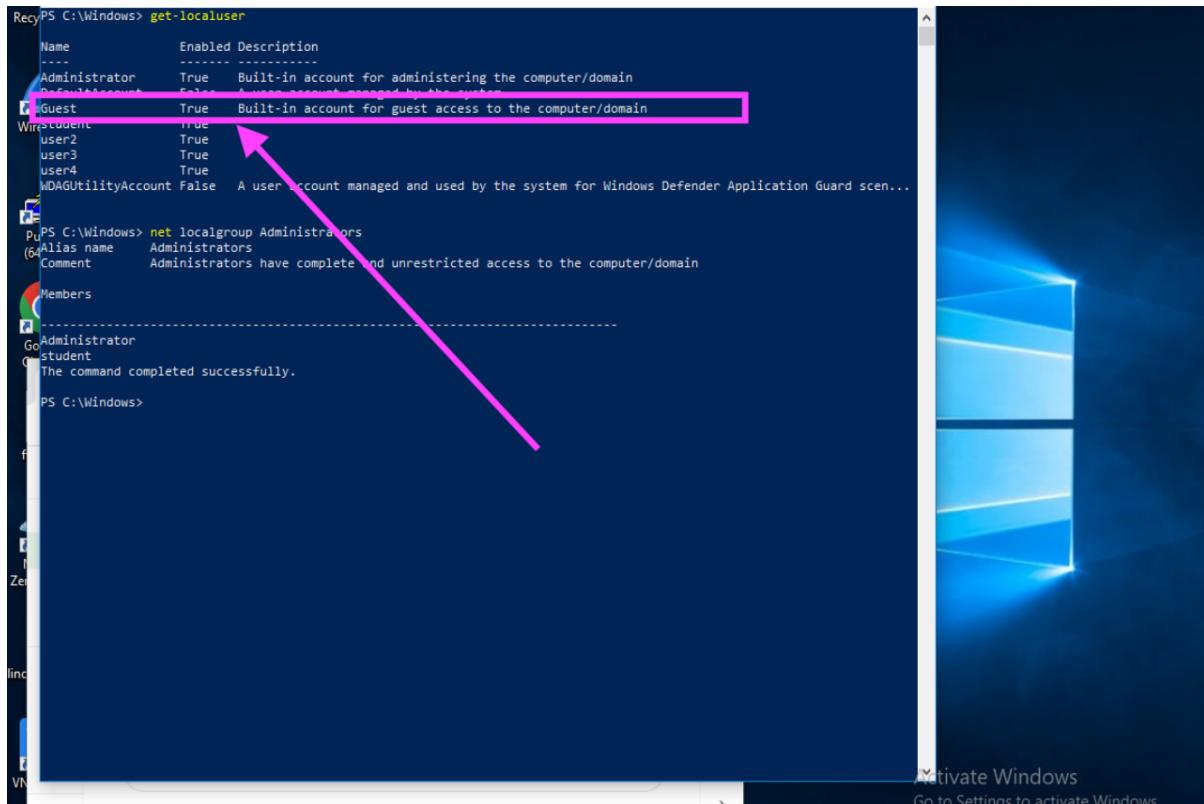
Activate Windows
Go to Settings to activate Windows.

5:14 PM 10/9/2022



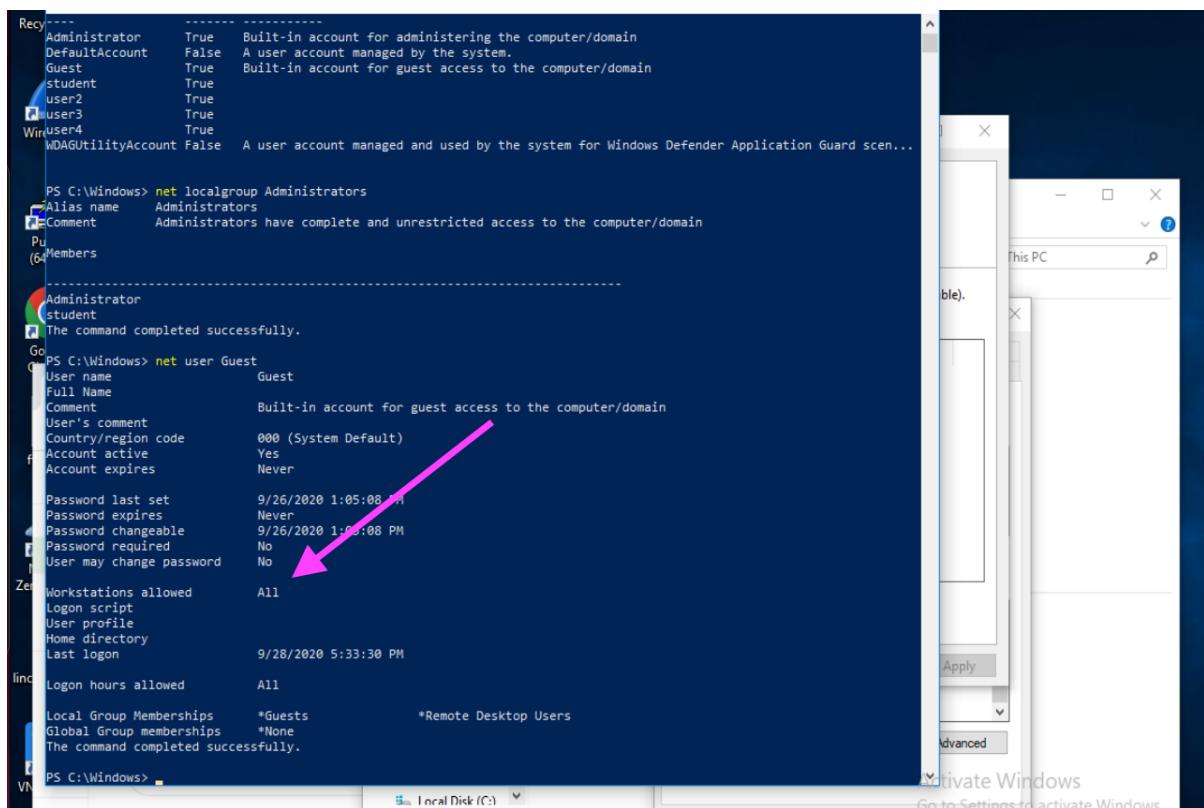


4. Are there "guest" accounts enabled? Yes.
- Is Guest allowed to log in to ALL workstations? Yes



```
PS C:\Windows> get-localuser
Name          Enabled Description
----          --     -----
Administrator True   Built-in account for administering the computer/domain
DefaultAccount False  A user account managed by the system
Guest         True   Built-in account for guest access to the computer/domain
WirelessUser  True
user1         True
user2         True
user3         True
user4         True
WDAGUtilityAccount False  A user account managed and used by the system for Windows Defender Application Guard scen...
PS C:\Windows> net localgroup Administrators
Alias name    Administrators
Comment       Administrators have complete and unrestricted access to the computer/domain
Members
Administrator
student
The command completed successfully.

PS C:\Windows>
```



```
PS C:\Windows> get-localuser
Name          Enabled Description
----          --     -----
Administrator True   Built-in account for administering the computer/domain
DefaultAccount False  A user account managed by the system
Guest         True   Built-in account for guest access to the computer/domain
student
user1
user2
user3
user4
WDAGUtilityAccount False  A user account managed and used by the system for Windows Defender Application Guard scen...
PS C:\Windows> net localgroup Administrators
Alias name    Administrators
Comment       Administrators have complete and unrestricted access to the computer/domain
Members
Administrator
student
The command completed successfully.

PS C:\Windows> net user Guest
User name        Guest
Full Name
Comment          Built-in account for guest access to the computer/domain
User's comment
Country/region code 000 (System Default)
Account active   Yes
Account expires  Never
Password last set 9/26/2020 1:05:08 PM
Password expires Never
Password changeable 9/26/2020 1:05:08 PM
Password required No
User may change password No
Workstations allowed All
Logon script
User profile
Home directory
Last logon      9/28/2020 5:33:30 PM
Logon hours allowed All
Local Group Memberships *Guests           *Remote Desktop Users
Global Group memberships *None
The command completed successfully.

PS C:\Windows>
```

5. Based on your findings, what should be done to secure these accounts and permissions better?

There is too many accounts, Guest, user2, user3, user4, they should be all condensed based in horizontal and vertical requirements, this should be based in the target user needs and requirements, its access scope and actions over services, software and execution.

This generic accounts shown the absence of defined user prospect in relation to their tasks, It's needed to be know what the user will do into the system, what tasks need to do, what are the systems, domains, services or resources the user need to access and must know if it's a real need that a user would have access and rights over the system core files and folder

From that perspective, a deeper detailed requirements for the assignation of users identity should be done in order to avoid insecure access.

3: Log Monitoring Setup for Detection at Targeted Assets

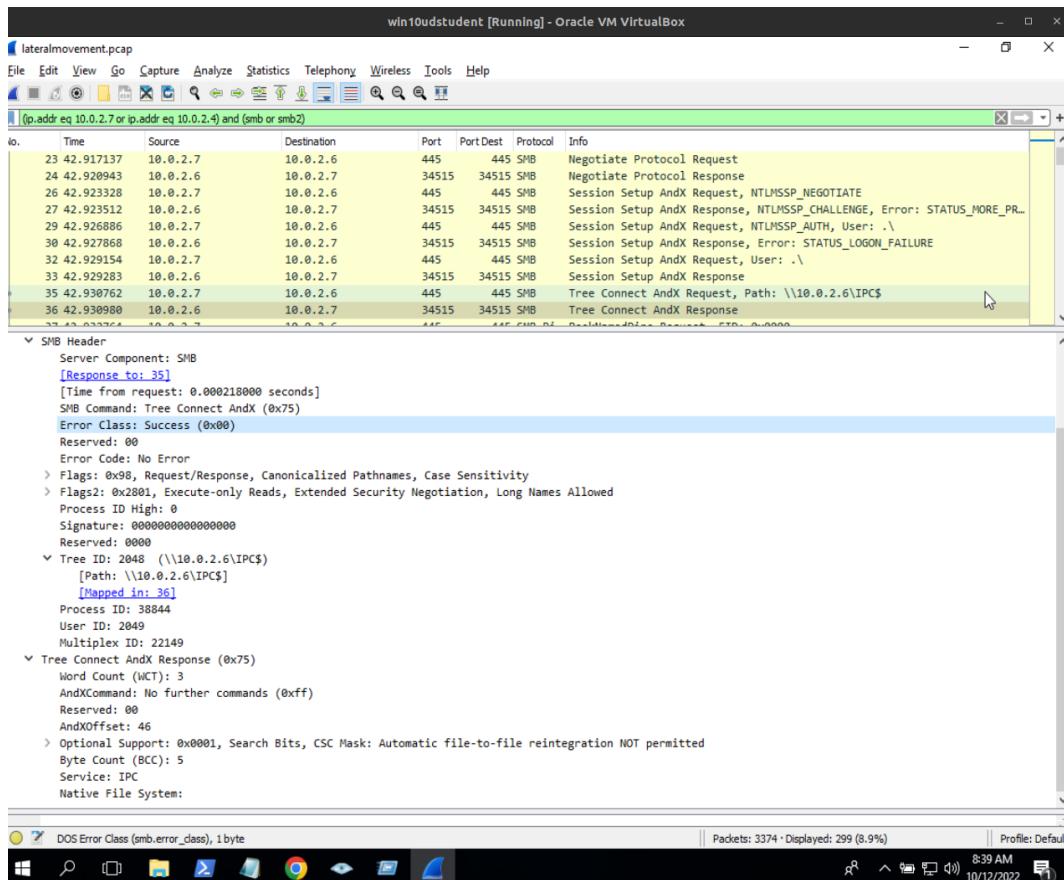
• Windows

3.1 Use the pcap file to assess and determine the following

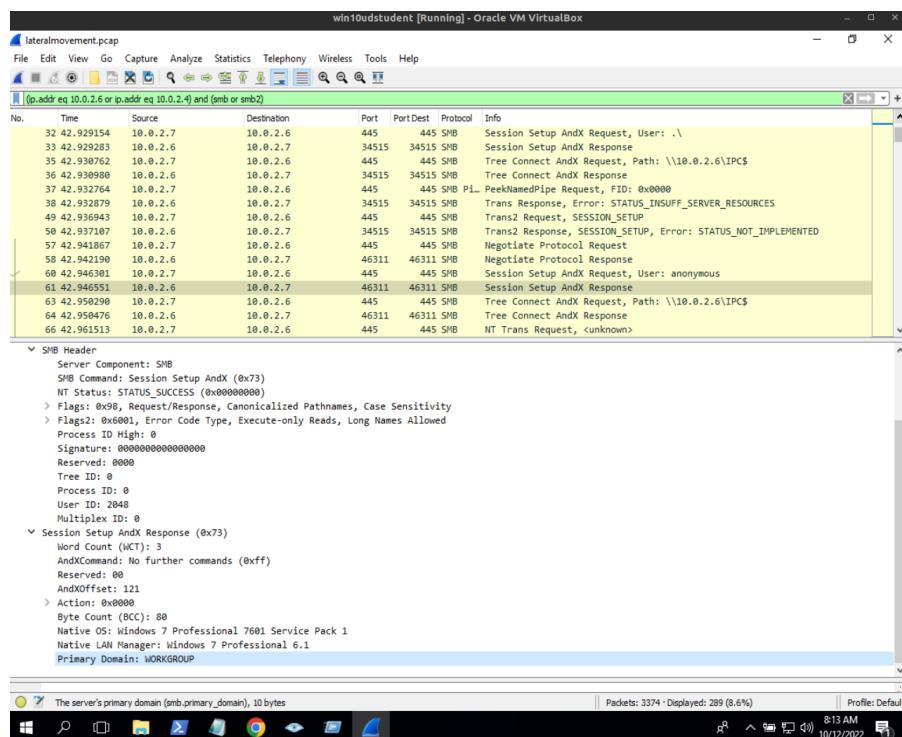
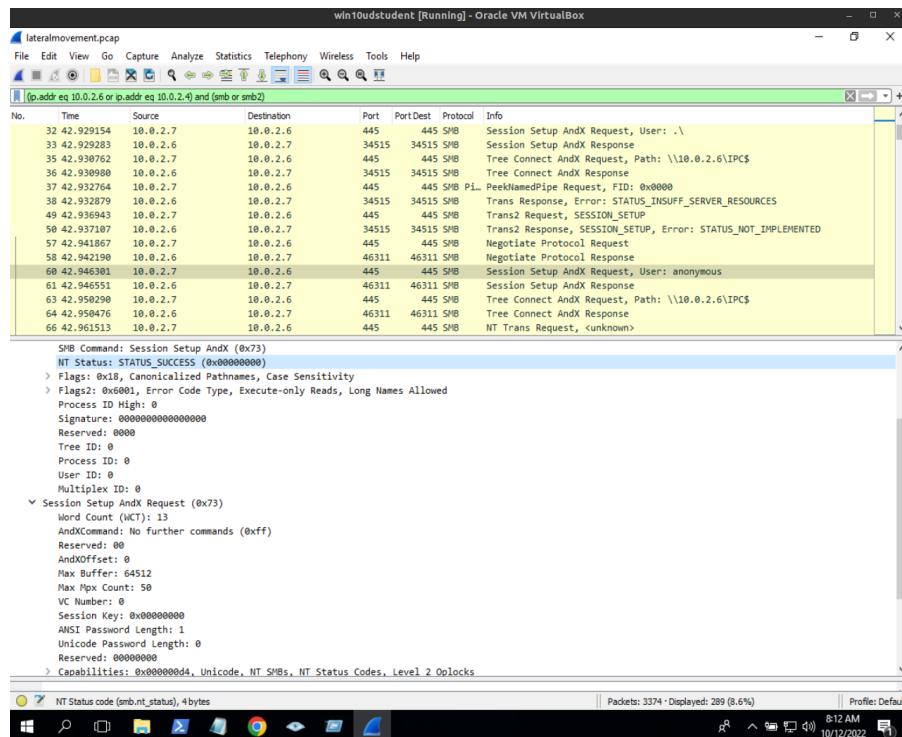
- 3.1.1 What type of attack was recorded?
- 3.1.2 What is the source IP of the attack?
- 3.1.3 What protocol was targeted?
- 3.1.4 What password was used successfully?
- 3.1.5 Which user was compromised?

The attacker ip address is 10.0.2.7 the protocol targeted was SMB, the Server Message Block which allow to share files and printers in a network.

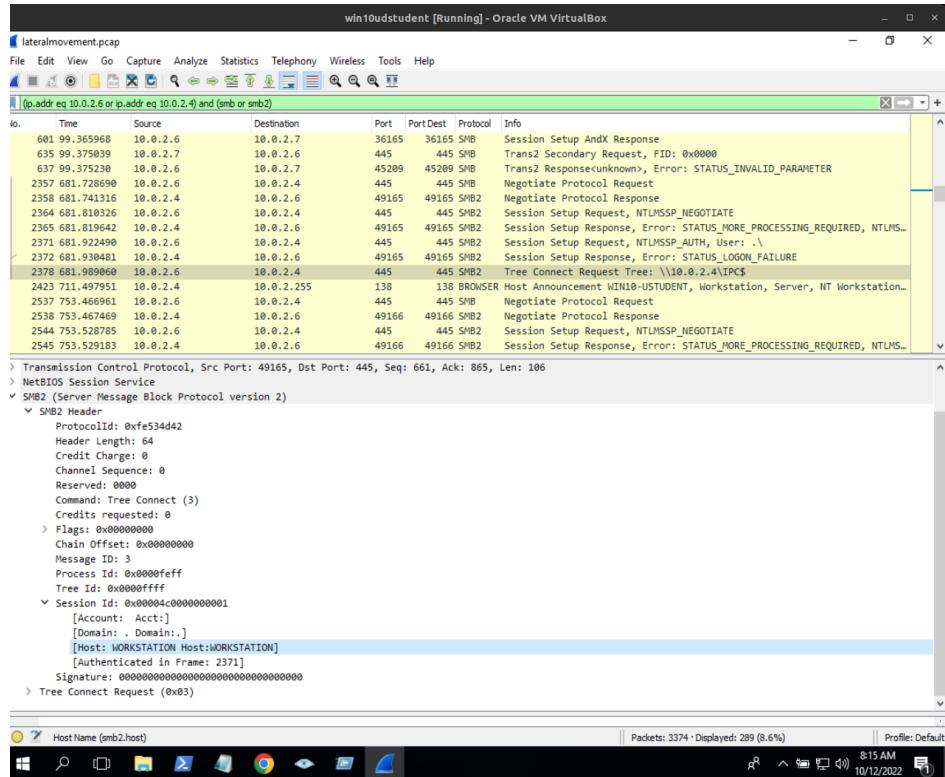
The attack started with a security hole for anonymous connections, the "IPC\$ share" allows anonymous users to perform a "null session connection" for system access and other activities, such as enumerating the names of domain accounts and network shares. No user and password is required for this type of connections.



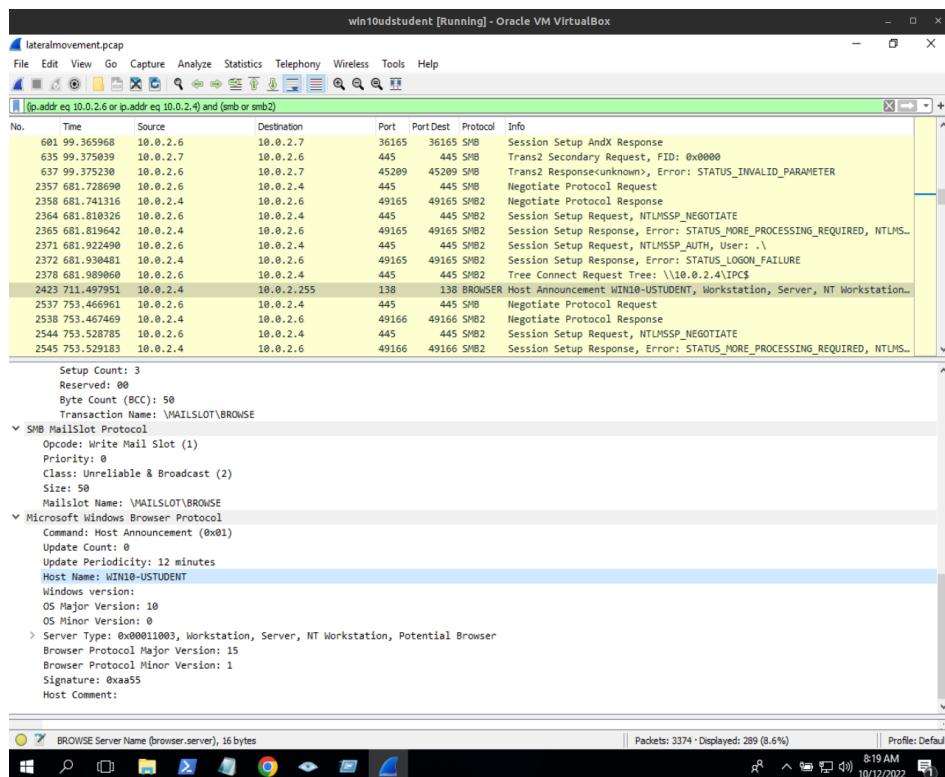
Using anonymous access the attacker is authenticated in the network without any password getting access to the Workgroup.



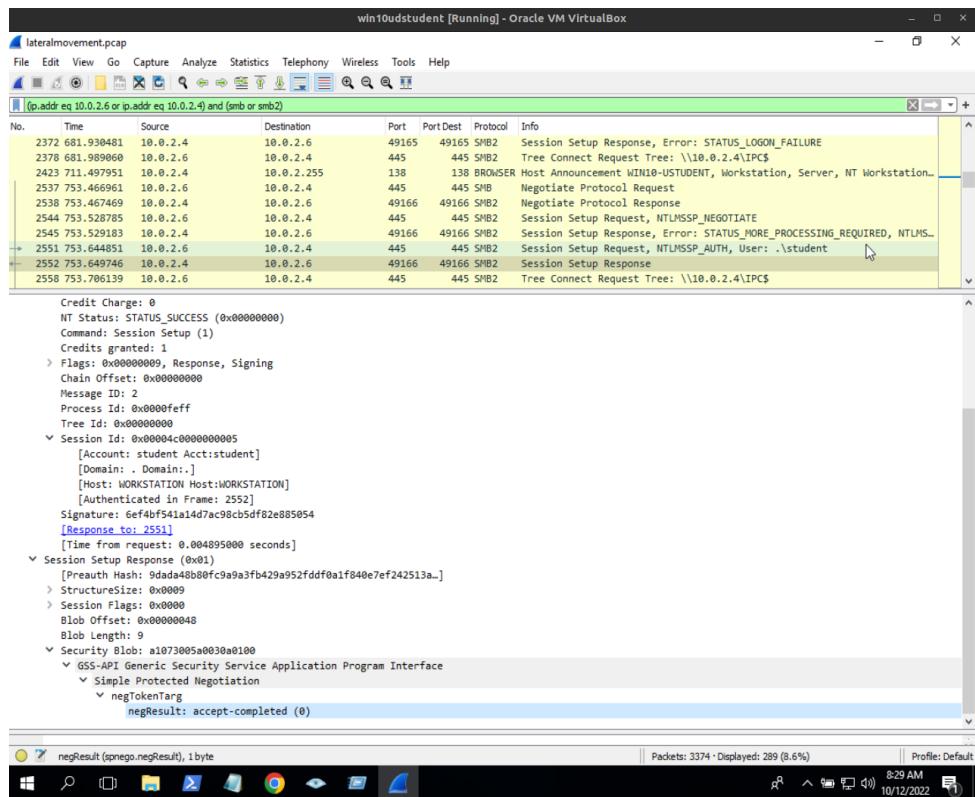
The final phase of the attack is about to gain access horizontally, moving from 10.0.2.6 to 10.0.2.4 using the same technique as an authenticated host.



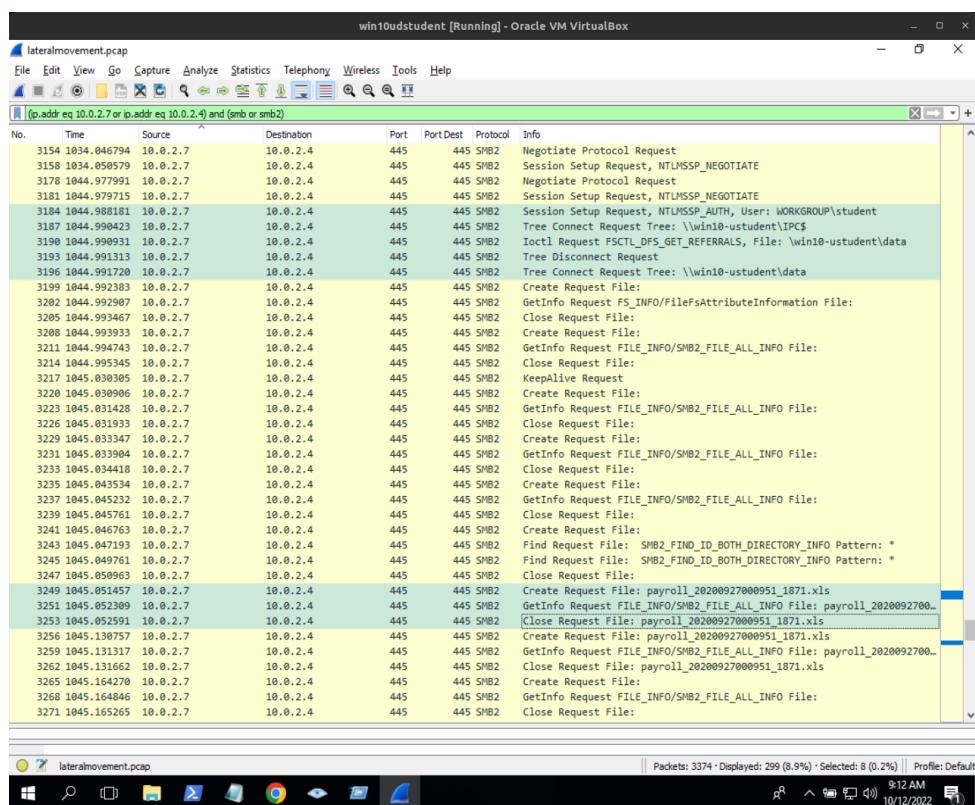
The attacker uses the BROWSER protocol which operates on top of SMB and is used to discover machines and resources on the network.



The "student" account is discovered and accessed.



Finally, gathering all this information together the attacker access to the system navigates through the system tree and extracts information.

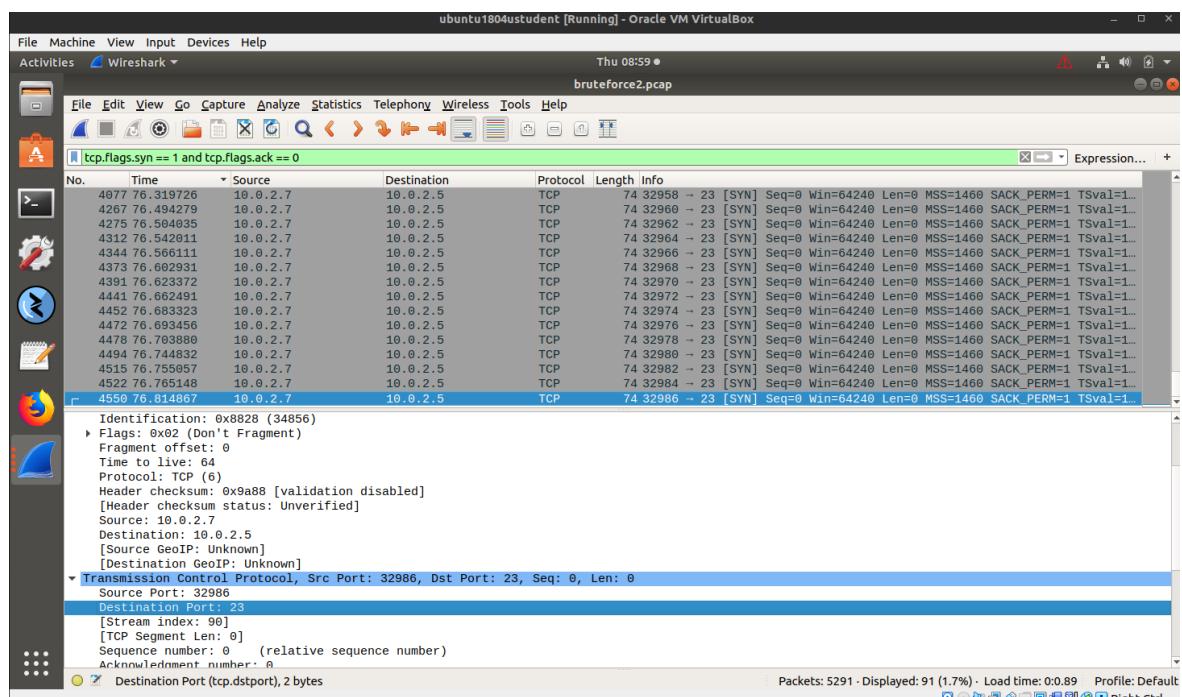


• Ubuntu

3.1 Use the pcap file to assess and determine the following

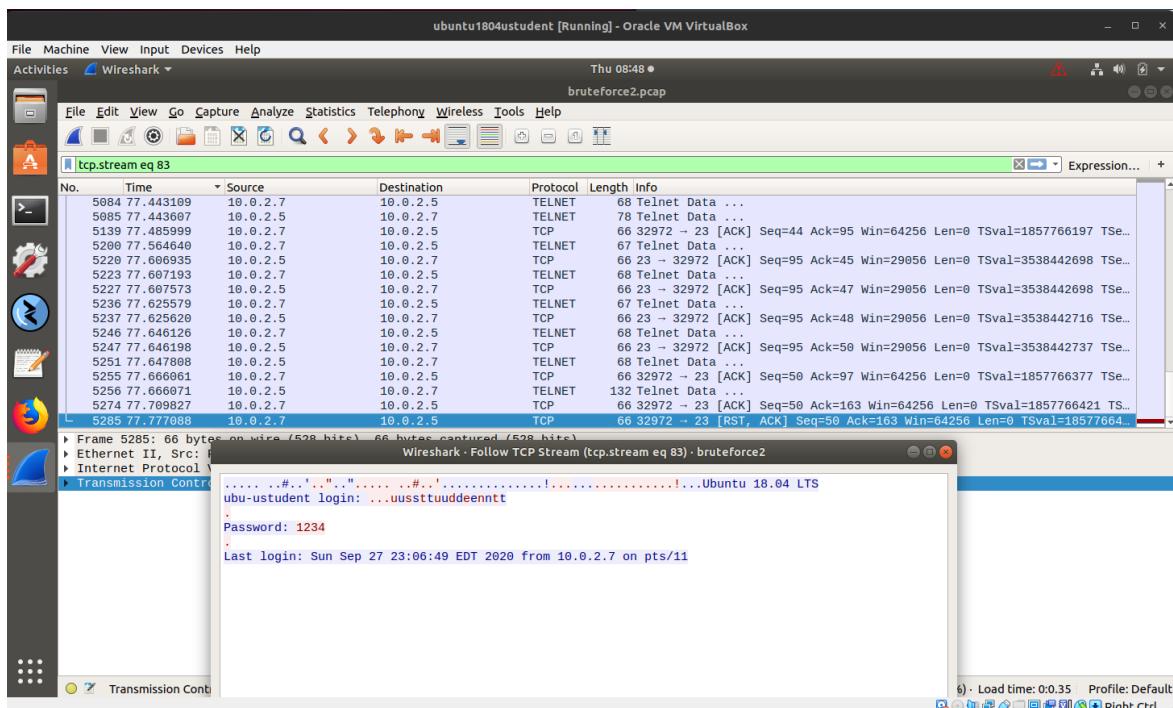
- **3.1.1** What type of attack was recorded?
- **3.1.2** What is the source IP of the attack?
- **3.1.3** What protocol was targeted?
- **3.1.4** What password was used successfully?
- **3.1.5** Which user was compromised?

The attack is brute force, a method that uses trial and error to crack password. in the first stage the attacker does a port scan recognition. In the final phase sent repeatedly characters till the user and password is discovered.



port scan

The ip address of the attacker is 10.0.2.7. The protocol used for the attack was Telnet compromising the user "ustudent" with password "1234".



3.2 An internal user may have compromised another machine, use lateralmovement.pcap and determine the following:

- 3.2.1 What was the source IP of the "initial" attack?
- 3.2.2 Did the attacker try to access your machine from a compromised device - MITRE ATT&CK Technique T1021?
- 3.2.3 What service and port were targeted?
- 3.2.4 Was the attacker able to access a sensitive file at the machine you are auditing? Mitre ATT&ACK Technique - T1570

The initial attack ip address source was 10.0.2.7. The attacker uses the MITRE ATT&CK Technique T1021, concretely the variation T1021.002 : SMB/Windows Admin Shares.

The protocol targeted was SMB, the Server Message Block which allow to share files and printers in a network over the port 445.

The attacker was able to access a sensitive file at the machine using the Mitre ATT&ACK Technique - T1570 through file sharing protocols such as file sharing over SMB/Windows Admin Shares.

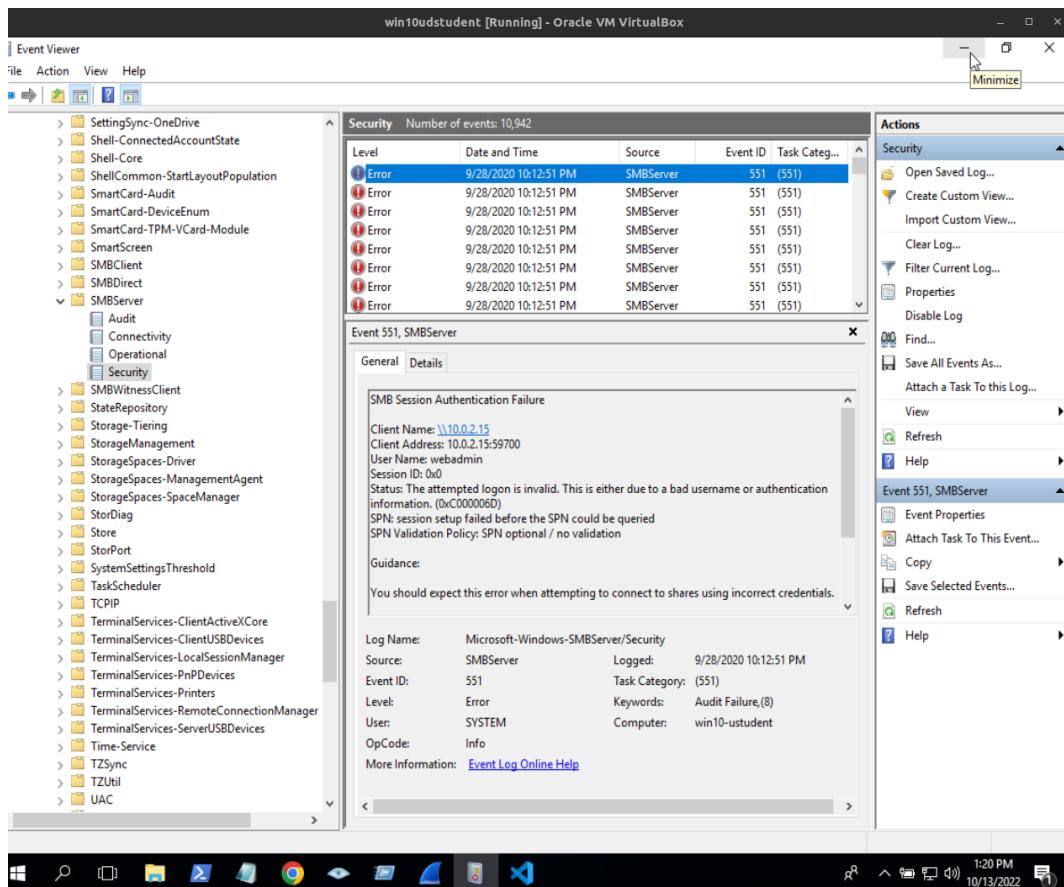
No.	Time	Source	Destination	Port	PortDest	Protocol	Info
3154	1034.046794	10.0.2.7	10.0.2.4	445	445	SMB2	Negotiate Protocol Request
3158	1034.050579	10.0.2.7	10.0.2.4	445	445	SMB2	Session Setup Request, NTLMSSP_NEGOTIATE
3178	1044.977991	10.0.2.7	10.0.2.4	445	445	SMB2	Negotiate Protocol Request
3181	1044.979715	10.0.2.7	10.0.2.4	445	445	SMB2	Session Setup Request, NTLMSSP_NEGOTIATE
3184	1044.998181	10.0.2.7	10.0.2.4	445	445	SMB2	Session Setup Request, NTLMSSP_AUTH, User: WORKGROUP\student
3187	1044.990423	10.0.2.7	10.0.2.4	445	445	SMB2	Tree Connect Request Tree: \\win10-ustudent\IPC\$
3190	1044.990931	10.0.2.7	10.0.2.4	445	445	SMB2	Ioctl Request FSCTL_DFS_GET_REFERRALS, File: \\win10-ustudent\data
3193	1044.991313	10.0.2.7	10.0.2.4	445	445	SMB2	Tree Disconnect Request
3196	1044.991724	10.0.2.7	10.0.2.4	445	445	SMB2	Tree Connect Request Tree: \\win10-ustudent\data
3199	1044.992383	10.0.2.7	10.0.2.4	445	445	SMB2	Create Request File:
3202	1044.992907	10.0.2.7	10.0.2.4	445	445	SMB2	GetInfo Request FS_INFO/FileFsAttributeInformation File:
3205	1044.993467	10.0.2.7	10.0.2.4	445	445	SMB2	Close Request File:
3208	1044.993933	10.0.2.7	10.0.2.4	445	445	SMB2	Create Request File:
3211	1044.994743	10.0.2.7	10.0.2.4	445	445	SMB2	GetInfo Request FILE_INFO/SMB2_FILE_ALL_INFO File:
3214	1044.995345	10.0.2.7	10.0.2.4	445	445	SMB2	Close Request File:
3217	1045.030395	10.0.2.7	10.0.2.4	445	445	SMB2	KeepAlive Request
3220	1045.030996	10.0.2.7	10.0.2.4	445	445	SMB2	Create Request File:
3223	1045.031428	10.0.2.7	10.0.2.4	445	445	SMB2	GetInfo Request FILE_INFO/SMB2_FILE_ALL_INFO File:
3226	1045.031933	10.0.2.7	10.0.2.4	445	445	SMB2	Close Request File:
3229	1045.033347	10.0.2.7	10.0.2.4	445	445	SMB2	Create Request File:
3231	1045.033980	10.0.2.7	10.0.2.4	445	445	SMB2	GetInfo Request FILE_INFO/SMB2_FILE_ALL_INFO File:
3233	1045.034418	10.0.2.7	10.0.2.4	445	445	SMB2	Close Request File:
3235	1045.043534	10.0.2.7	10.0.2.4	445	445	SMB2	Create Request File:
3237	1045.045232	10.0.2.7	10.0.2.4	445	445	SMB2	GetInfo Request FILE_INFO/SMB2_FILE_ALL_INFO File:
3239	1045.045761	10.0.2.7	10.0.2.4	445	445	SMB2	Close Request File:
3241	1045.046763	10.0.2.7	10.0.2.4	445	445	SMB2	Create Request File:
3243	1045.047193	10.0.2.7	10.0.2.4	445	445	SMB2	Find Request File: SMB2_FIND_ID_BOTH_DIRECTORY_INFO Pattern: *
3245	1045.049761	10.0.2.7	10.0.2.4	445	445	SMB2	Find Request File: SMB2_FIND_ID_BOTH_DIRECTORY_INFO Pattern: *
3247	1045.050963	10.0.2.7	10.0.2.4	445	445	SMB2	Close Request File:
3249	1045.051457	10.0.2.7	10.0.2.4	445	445	SMB2	Create Request File: payroll_20200927000951_1871.xls
3251	1045.052399	10.0.2.7	10.0.2.4	445	445	SMB2	GetInfo Request FILE_INFO/SMB2_FILE_ALL_INFO File: payroll_20200927000951_1871.xls
3253	1045.052591	10.0.2.7	10.0.2.4	445	445	SMB2	Close Request File: payroll_20200927000951_1871.xls
3256	1045.130757	10.0.2.7	10.0.2.4	445	445	SMB2	Create Request File: payroll_20200927000951_1871.xls
3259	1045.131317	10.0.2.7	10.0.2.4	445	445	SMB2	GetInfo Request FILE_INFO/SMB2_FILE_ALL_INFO File: payroll_20200927000951_1871.xls
3262	1045.131662	10.0.2.7	10.0.2.4	445	445	SMB2	Close Request File: payroll_20200927000951_1871.xls
3265	1045.164270	10.0.2.7	10.0.2.4	445	445	SMB2	Create Request File:
3268	1045.164846	10.0.2.7	10.0.2.4	445	445	SMB2	GetInfo Request FILE_INFO/SMB2_FILE_ALL_INFO File:
3271	1045.165265	10.0.2.7	10.0.2.4	445	445	SMB2	Close Request File:

3.3 Using the logs, determine the following:

- 3.3.1 Are there any issues with Windows Share? Please provide screenshots of your findings.
- 3.3.2 Look at the audit logs setup at your Linux machine and find the audit.log file. What was the name of the attacker's account? Please provide screenshots.

Based on what you found above, provide your assessment on whether these events are enough to start an investigation? Please explain your answer based on what you saw in the logs.

3.3.1 There is many issues in the log of the targeted share.



3.3.2 The name of the attacker's account was "guest".

The user "nobody" also perform an attack but the sessions is never opened as It does "guest".

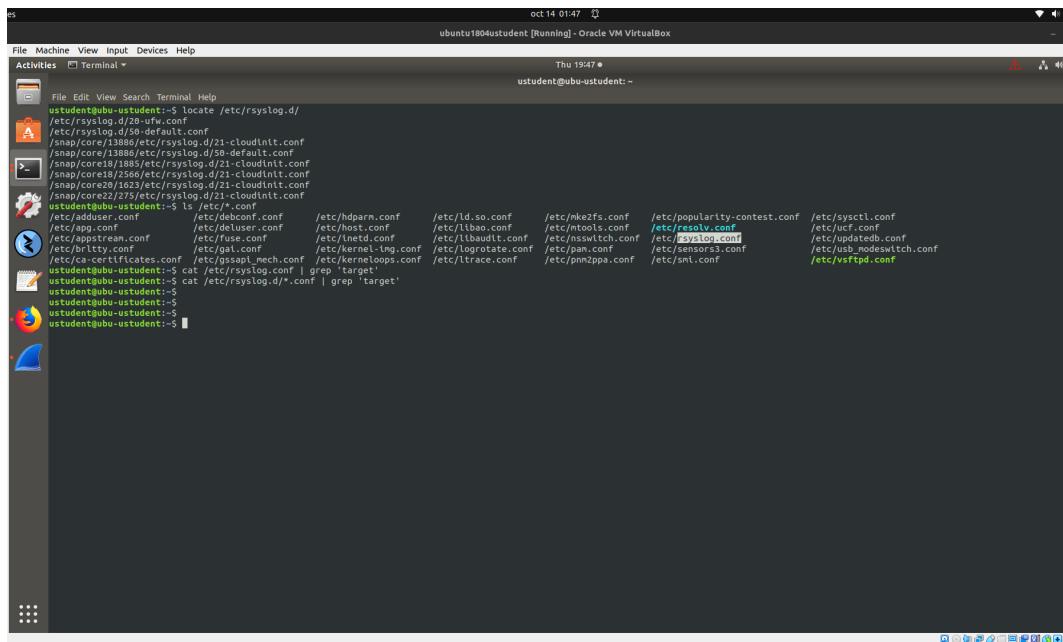
```
oct 14 01:05 /ubuntu1804student [Running] - Oracle VM VirtualBox
ine View Input Devices Help
Terminal Thu 19:05 ~
ustudent@ubu-ustudent: ~
ile Edit View Search Terminal Help
351883 res-success'
|>peCRED DISP msg=audit(1601347048.836:692): pid=2737 uid=0 auid=4294967295 ses=4294967295 msg='op=PAM:setcred acct="nobody" exe="/usr/sbin/smbd" hostname=10.0.2.15 addr=10.0.2.15
37583 res-success'
|>peCRED DISP msg=audit(1601347048.836:694): pid=2725 uid=0 auid=4294967295 ses=4294967295 msg='op=PAM:setcred acct="nobody" exe="/usr/sbin/smbd" hostname=10.0.2.15 addr=10.0.2.15
467164 res-success'
|>peCRED DISP msg=audit(1601347048.836:696): pid=2729 uid=0 auid=4294967295 ses=4294967295 msg='op=PAM:setcred acct="nobody" exe="/usr/sbin/smbd" hostname=10.0.2.15 addr=10.0.2.15
293201 res-success'
|>peCRED DISP msg=audit(1601347048.836:697): pid=2722 uid=0 auid=4294967295 ses=4294967295 msg='op=PAM:setcred acct="nobody" exe="/usr/sbin/smbd" hostname=10.0.2.15 addr=10.0.2.15
54195 res-success'
|>peCRED DISP msg=audit(1601347048.836:699): pid=2727 uid=0 auid=4294967295 ses=4294967295 msg='op=PAM:setcred acct="nobody" exe="/usr/sbin/smbd" hostname=10.0.2.15 addr=10.0.2.15
236378 res-success'
|>peCRED DISP msg=audit(1601347048.836:700): pid=2731 uid=0 auid=4294967295 ses=4294967295 msg='op=PAM:setcred acct="nobody" exe="/usr/sbin/smbd" hostname=10.0.2.15 addr=10.0.2.15
326979 res-success'
|>peCRED DISP msg=audit(1601347048.836:702): pid=2736 uid=0 auid=4294967295 ses=4294967295 msg='op=PAM:setcred acct="nobody" exe="/usr/sbin/smbd" hostname=10.0.2.15 addr=10.0.2.15
82094 res-success'
|>peCRED DISP msg=audit(1601347048.836:703): pid=2735 uid=0 auid=4294967295 ses=4294967295 msg='op=PAM:setcred acct="nobody" exe="/usr/sbin/smbd" hostname=10.0.2.15 addr=10.0.2.15
7385 res-success'
|>peCRED DISP msg=audit(1601347048.836:704): pid=2733 uid=0 auid=4294967295 ses=4294967295 msg='op=PAM:setcred acct="nobody" exe="/usr/sbin/smbd" hostname=10.0.2.15 addr=10.0.2.15
218804 res-success'
|>peCRED DISP msg=audit(1601347048.836:705): pid=2721 uid=0 auid=4294967295 ses=4294967295 msg='op=PAM:setcred acct="nobody" exe="/usr/sbin/smbd" hostname=10.0.2.15 addr=10.0.2.15
543910 res-success'
|>peCRED DISP msg=audit(1601347048.836:706): pid=2723 uid=0 auid=4294967295 ses=4294967295 msg='op=PAM:setcred acct="nobody" exe="/usr/sbin/smbd" hostname=10.0.2.15 addr=10.0.2.15
706439 res-success'
|>peCRED DISP msg=audit(1601347048.836:708): pid=2724 uid=0 auid=4294967295 ses=4294967295 msg='op=PAM:setcred acct="nobody" exe="/usr/sbin/smbd" hostname=10.0.2.15 addr=10.0.2.15
16086 res-success'
|>peCRED DISP msg=audit(1601347048.836:709): pid=2726 uid=0 auid=4294967295 ses=4294967295 msg='op=PAM:setcred acct="nobody" exe="/usr/sbin/smbd" hostname=10.0.2.15 addr=10.0.2.15
422924 res-success'
|>peCRED DISP msg=audit(1601347048.836:711): pid=2728 uid=0 auid=4294967295 ses=4294967295 msg='op=PAM:setcred acct="nobody" exe="/usr/sbin/smbd" hostname=10.0.2.15 addr=10.0.2.15
840734 res-success'
|>peCRED DISP msg=audit(1601347048.836:714): pid=2732 uid=0 auid=4294967295 ses=4294967295 msg='op=PAM:setcred acct="nobody" exe="/usr/sbin/smbd" hostname=10.0.2.15 addr=10.0.2.15
9194861 res-success'
|>peCRED DISP msg=audit(1601347048.836:715): pid=2738 uid=0 auid=4294967295 ses=4294967295 msg='op=PAM:setcred acct="nobody" exe="/usr/sbin/smbd" hostname=10.0.2.15 addr=10.0.2.15
47244 res-success'
|>peCRED DISP msg=audit(1601347048.836:716): pid=2730 uid=0 auid=4294967295 ses=4294967295 msg='op=PAM:setcred acct="nobody" exe="/usr/sbin/smbd" hostname=10.0.2.15 addr=10.0.2.15
9536000 res-success'
|>peCRED DISP msg=audit(1601347048.852:726): pid=2739 uid=0 auid=4294967295 ses=4294967295 msg='op=PAM:setcred acct="nobody" exe="/usr/sbin/smbd" hostname=10.0.2.15 addr=10.0.2.15
3638051 res-success'
|>peCRED DISP msg=audit(1601347307.748:731): pid=2754 uid=0 auid=4294967295 ses=4294967295 msg='op=PAM:setcred acct="nobody" exe="/usr/sbin/smbd" hostname=10.0.2.7 add=10.0.2.7 te
78222 res-success'
|>peCRED DISP msg=audit(1605147079.704:101): pid=1612 uid=0 auid=4294967295 ses=4294967295 msg='op=PAM:setcred acct="nobody" exe="/usr/sbin/smbd" hostname=127.0.0.1 add=127.0.0.1
5164893 res-success'
|>peCRED DISP msg=audit(1665147184.080:134): pid=1984 uid=0 auid=4294967295 ses=4294967295 msg='op=PAM:setcred acct="nobody" exe="/usr/sbin/smbd" hostname=127.0.0.1 add=127.0.0.1
3741414 res-success'
|>peCRED DISP msg=audit(1605147374.586:99): pid=1591 uid=0 auid=4294967295 ses=4294967295 msg='op=PAM:setcred acct="nobody" exe="/usr/sbin/smbd" hostname=127.0.0.1 add=127.0.0.1 t
550236 res-success'
student@ubu-ustudent: ~ cat /var/log/audit/audit.log | grep 'acct=="' | grep 'res-success' | grep -v 'acct="guest"' | grep -v 'acct="root"' | grep -v 'acct="ustudent"' | grep -v 'acct="root"' | grep -v 'session_close' |
```

Based on these events, attacks using protocols for remote connections with default shares configurations and settings, all this evidence is enough to start an investigation.

3.4

- **3.4.1** NuttyUtility has a centralized log infrastructure using a SIEM (Security Information and Event Management) product. You need to verify the machines you are checking from StaticSpeed have the settings enabled to use this.
- **3.4.2** Analyze StaticSpeeds systems and determine if these machines are currently shipping jobs to a centralized location and set up correctly for our SIEM.

The rsyslog utility supports the ability to send logs to a remote log host, to verify if it's shipping jobs to a centralized SIEM, the /etc/rsyslog.conf and /etc/rsyslog.d/*.conf files has been audited and to verify that logs output include target=<FQDN or IP of remote loghost>.

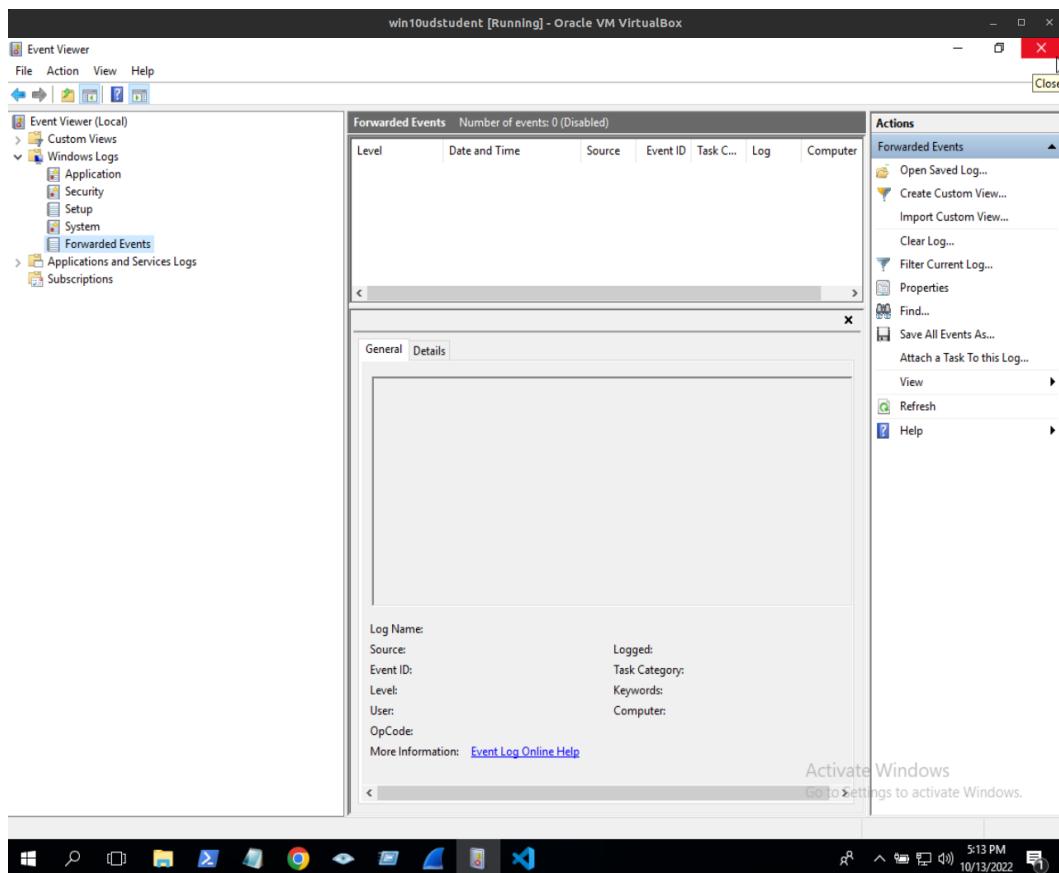


A screenshot of a Linux desktop environment showing a terminal window. The terminal window title is "ubuntu1804student [Running] - Oracle VM VirtualBox". The terminal content shows the user navigating through configuration files:

```
ustudent@ubu-ustudent:~$ locate /etc/rsyslog.d/
/etc/rsyslog.d/20-ufw.conf
/etc/rsyslog.d/30-syslog.conf
/snap/core13886/etc/rsyslog.d/21-cloudinit.conf
/snap/core18/1885/etc/rsyslog.d/50-default.conf
/snap/core18/17805/etc/rsyslog.d/21-cloudinit.conf
/snap/core18/275/etc/rsyslog.d/21-cloudinit.conf
/snap/core22/275/etc/rsyslog.d/21-cloudinit.conf
ustudent@ubu-ustudent:~$ ls /etc/*/.conf
/etc/adbuser.com          /etc/debcconf.conf      /etc/hdbarn.conf      /etc/lid.so.conf      /etc/mke2fs.conf      /etc/popularity-contest.conf /etc/ysvcctl.conf
/etc/addrule.conf         /etc/distro.conf       /etc/host.conf       /etc/lib�.conf       /etc/nfsck.conf       /etc/rsyslog.conf      /etc/xef.conf
/etc/appstream.conf        /etc/fuse.conf        /etc/lnetd.conf       /etc/libaudit.conf    /etc/nsswitch.conf    /etc/rsyslog.conf      /etc/updatedb.conf
/etc/bratty.conf          /etc/gal.conf         /etc/kernel-lng.conf /etc/logrotate.conf   /etc/pam.conf        /etc/sensors3.conf   /etc/usb-modeswitch.conf
/etc/certificates.conf    /etc/gssapi_nech.conf /etc/kernelloops.conf /etc/ltrace.conf     /etc/pnm2ppa.conf    /etc/sml.conf        /etc/vsftpd.conf
/etc/cron.d               /etc/hosts           /etc/hostname        /etc/mkisofs.conf    /etc/rsyslog.conf    /etc/syslog.conf
ustudent@ubu-ustudent:~$ cat /etc/rsyslog.conf | grep "target"
ustudent@ubu-ustudent:~$ cat /etc/rsyslog.d/*.*.conf | grep "target"
ustudent@ubu-ustudent:~$ 
ustudent@ubu-ustudent:~$ 
ustudent@ubu-ustudent:~$ 
```

After execute the "cat [file] | grep [criteria]" command to filter the files to extract the "target" there is no output. This means the settings aren't enabled and there aren't log shipping jobs to a centralized SIEM.

In Windows, verification in the event viewer of configurations or jobs running for subscriptions in Windows Event Forwarder related to a remote SIEM shows that there is none.



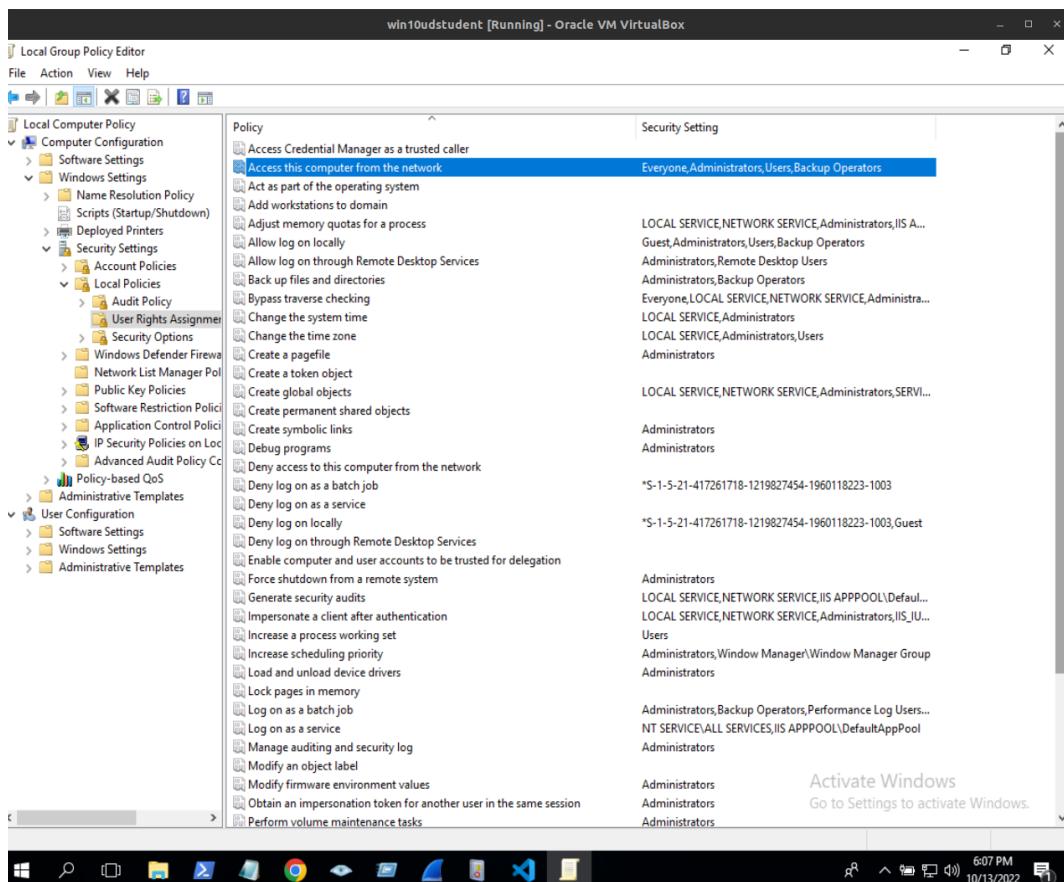
Based in this findings, the suggested course of action to ensure StaticSpeed meets the need of use a SIEM is configure Windows Event Forwarding and rsyslog to collect as many data as possible, this includes Perimeter device logs, Windows event logs, Application logs and Endpoint logs.

4: Assess Authentication Management at Targeted Assets

- 4.1.1 Ensure only administrators can remotely access windows machines and verify if root access is permitted at the Linux host.
- 4.1.2 Check for users with excessive permissions
- 4.1.3 Is root remote login allowed?
- 4.1.4 Are there users that should not have remote access via ssh in Linux?
- 4.1.5 Remote Desktop Access should only be granted to administrators in Windows, are there other accounts that should not be given access?

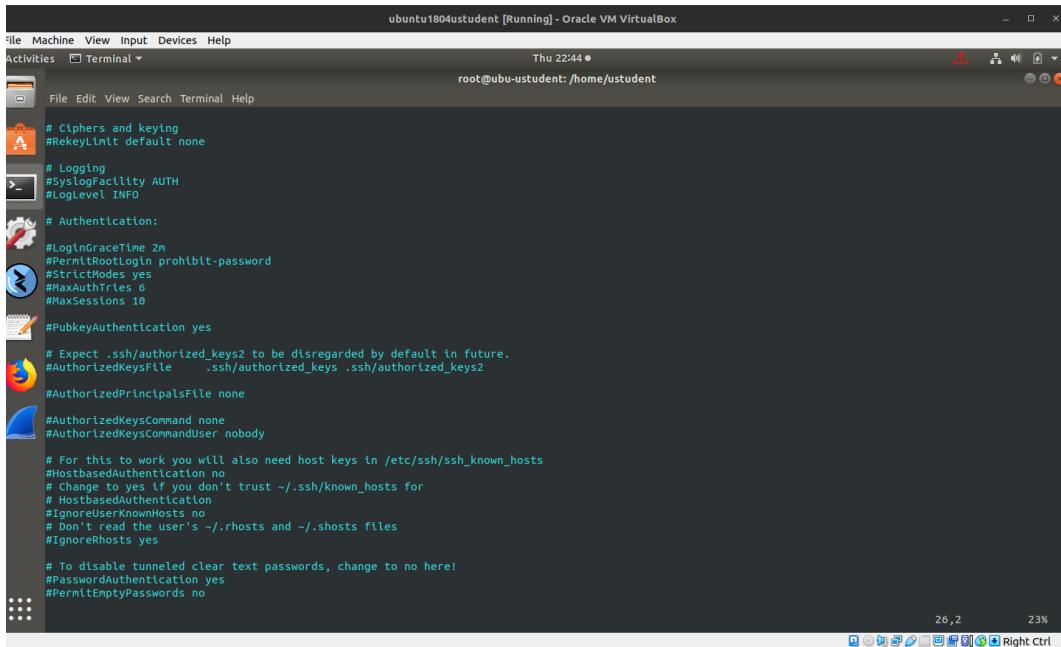
• Windows

- 1. Administrators are not the only group allowed to access remotely access windows machines.
- 2. Users with excessive permissions are match with some default values, e.g users as Everyone, Guest and Users for rules like "Bypass traverse checking", "Allow log on locally", etc...
- 3. Remote root login is allowed as Administrator.
- 5. Remote Desktop Access is also granted to Everyone and Users.



- **Ubuntu**

- 1. root access is not allowed at the Linux host.
- 2. Users has not excessive permissions since they are isolated into their own groups out of the scope of sudo command.
- 3. Remote root login is not enabled.
- 4. As There is no users restrictions set for access via ssh



This screenshot shows a terminal window titled "ubuntu1804student [Running] - Oracle VM VirtualBox". The window displays the contents of the `/etc/ssh/sshd_config` file. The configuration includes various SSH settings such as ciphers, logging, authentication methods (including RSA keys), and host-based authentication. It also specifies the use of known hosts and the disabling of password authentication for tunneled connections.

```
# Ciphers and keying
#RekeyLimit default none

# Logging
#LogLevel AUTH
#LogLevel INFO

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

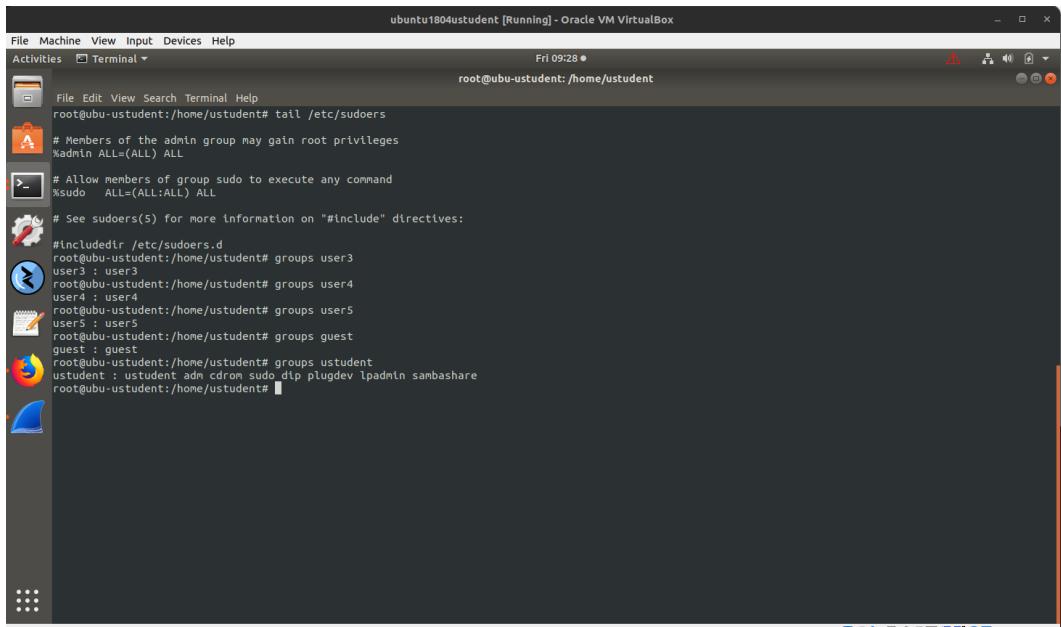
#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile      .ssh/authorized_keys .ssh/authorized_keys2
#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
#PermitEmptyPasswords no
```



This screenshot shows a terminal window titled "ubuntu1804student [Running] - Oracle VM VirtualBox". The window displays the contents of the `/etc/sudoers` file. The configuration includes rules for the "admin" group to gain root privileges and specific entries for users like "user3", "user4", "user5", and "guest". It also shows the inclusion of the `/etc/sudoers.d` directory.

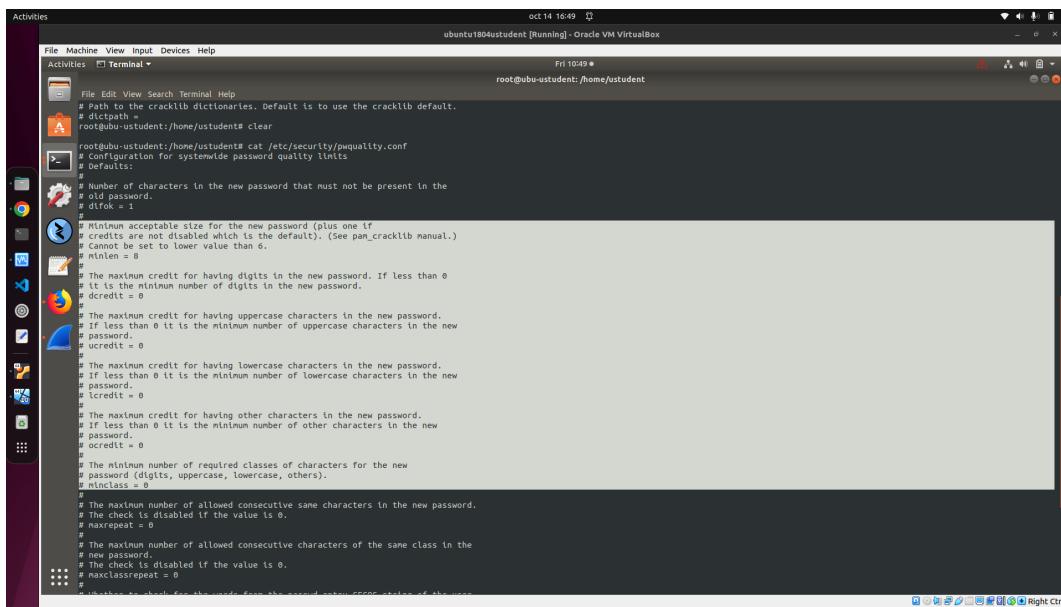
```
# Members of the admin group may gain root privileges
%admin  ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

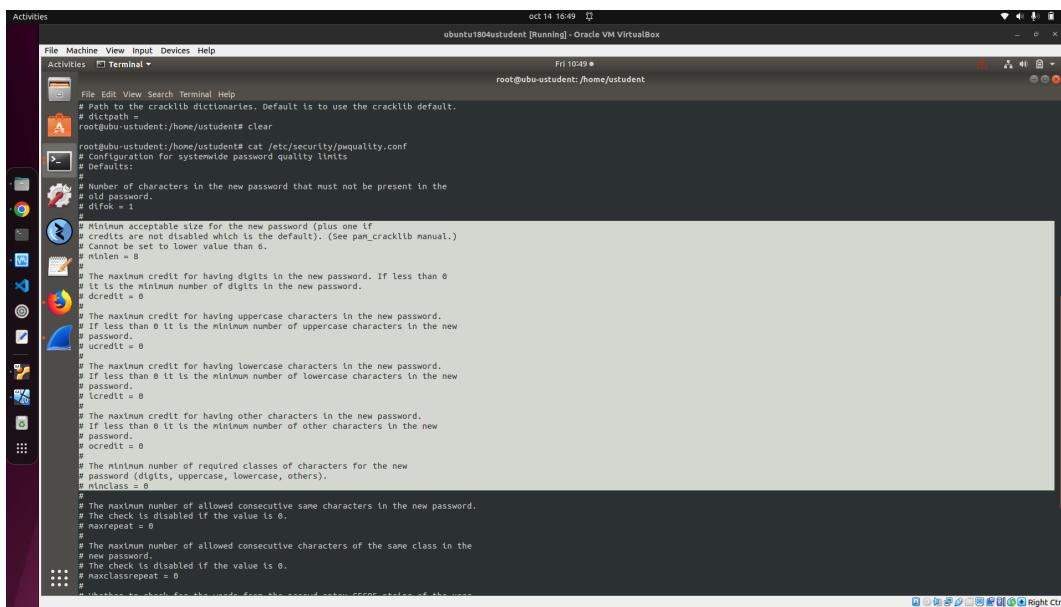
# See sudoers(5) for more information on "#include" directives:
#includedir /etc/sudoers.d
root@ubu-ustudent:/home/ustudent# groups user3
user3 : user3
root@ubu-ustudent:/home/ustudent# groups user4
user4 : user4
root@ubu-ustudent:/home/ustudent# groups user5
user5 : user5
root@ubu-ustudent:/home/ustudent# groups guest
guest : guest
root@ubu-ustudent:/home/ustudent# groups uststudent
uststudent : uststudent adm cdrom sudo dip plugdev lpadmin sambashare
root@ubu-ustudent:/home/ustudent#
```

4.2 Verify that Ubuntu and Windows comply with

- CIS Benchmarks 5.3.1 (Ubuntu)
- CIS Benchmarks 1.1.5 (Windows)



```
# Path to the cracklib dictionaries. Default is to use the cracklib default.
# dictpath =
root@ubu-ustudent:~# cat /etc/security/pwquality.conf
# Configuration for systemwide password quality limits
#
# Defaults:
#
# Number of characters in the new password that must not be present in the
# old password.
# difok = 1
#
# Minimum acceptable size for the new password (plus one if
# checks are not disabled which is the default). (See pam_cracklib manual.)
# minlen = 8
#
# The maximum credit for having digits in the new password. If less than 0
# it is the minimum number of digits in the new password.
# dcredit = 0
#
# The maximum credit for having uppercase characters in the new password.
# If less than 0 it is the minimum number of uppercase characters in the new
# password.
# ucredit = 0
#
# The maximum credit for having lowercase characters in the new password.
# If less than 0 it is the minimum number of lowercase characters in the new
# password.
# lcredit = 0
#
# The maximum credit for having other characters in the new password.
# If less than 0 it is the minimum number of other characters in the new
# password.
# ocredit = 0
#
# The minimum number of required classes of characters for the new
# password (digits, uppercase, lowercase, others).
# minclass = 3
#
# The maximum number of allowed consecutive same characters in the new password.
# If the check is disabled if the value is 0.
# maxrepeat = 0
#
# The maximum number of allowed consecutive characters of the same class in the
# new password.
# The check is disabled if the value is 0.
# maxclassrepeat = 0
#
# Whether to check for lowercase characters in the new password.
# checklower = 1
```

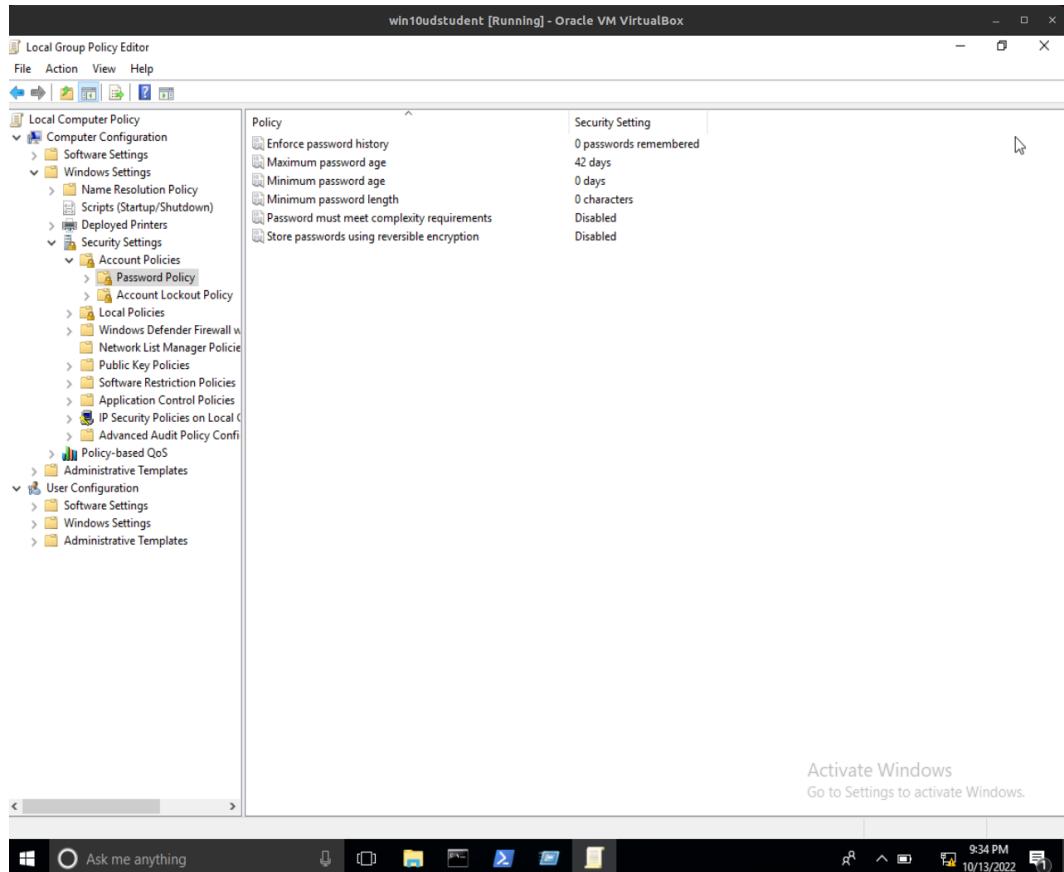


```
# Path to the cracklib dictionaries. Default is to use the cracklib default.
# dictpath =
root@ubu-ustudent:~# cat /etc/security/pwquality.conf
# Configuration for systemwide password quality limits
#
# Defaults:
#
# Number of characters in the new password that must not be present in the
# old password.
# difok = 1
#
# Minimum acceptable size for the new password (plus one if
# checks are not disabled which is the default). (See pam_cracklib manual.)
# minlen = 8
#
# The maximum credit for having digits in the new password. If less than 0
# it is the minimum number of digits in the new password.
# dcredit = 0
#
# The maximum credit for having uppercase characters in the new password.
# If less than 0 it is the minimum number of uppercase characters in the new
# password.
# ucredit = 0
#
# The maximum credit for having lowercase characters in the new password.
# If less than 0 it is the minimum number of lowercase characters in the new
# password.
# lcredit = 0
#
# The maximum credit for having other characters in the new password.
# If less than 0 it is the minimum number of other characters in the new
# password.
# ocredit = 0
#
# The minimum number of required classes of characters for the new
# password (digits, uppercase, lowercase, others).
# minclass = 3
#
# The maximum number of allowed consecutive same characters in the new password.
# If the check is disabled if the value is 0.
# maxrepeat = 0
#
# The maximum number of allowed consecutive characters of the same class in the
# new password.
# The check is disabled if the value is 0.
# maxclassrepeat = 0
#
# Whether to check for lowercase characters in the new password.
# checklower = 1
```

Verify password creation requirements conform to organization policy.

To approve the Benchmark audit the minimum password length should be 14 or more characters, password complexity minclass equal to 4 or dcredit equal to -1, ucredit equal to -1, lcredit equal to -1, ocredit equal to -1, he number of attempts allowed before sending back a failure shouldn't be more than 3, all of which as It's shown **does not compliant**.

To establish the recommended configuration Password must meet complexity requirements as use Unique Passwords Configure centralized point of Authentication, encrypt transmittal of Username and Authentication Credentials, all of which as It's shown **does not compliant**.



4.3 Verify If comply with this strong encryption ciphers policy (FIPS 140-2)

Windows (Disable) and Ubuntu (outdated OpenSSL version) not complain.

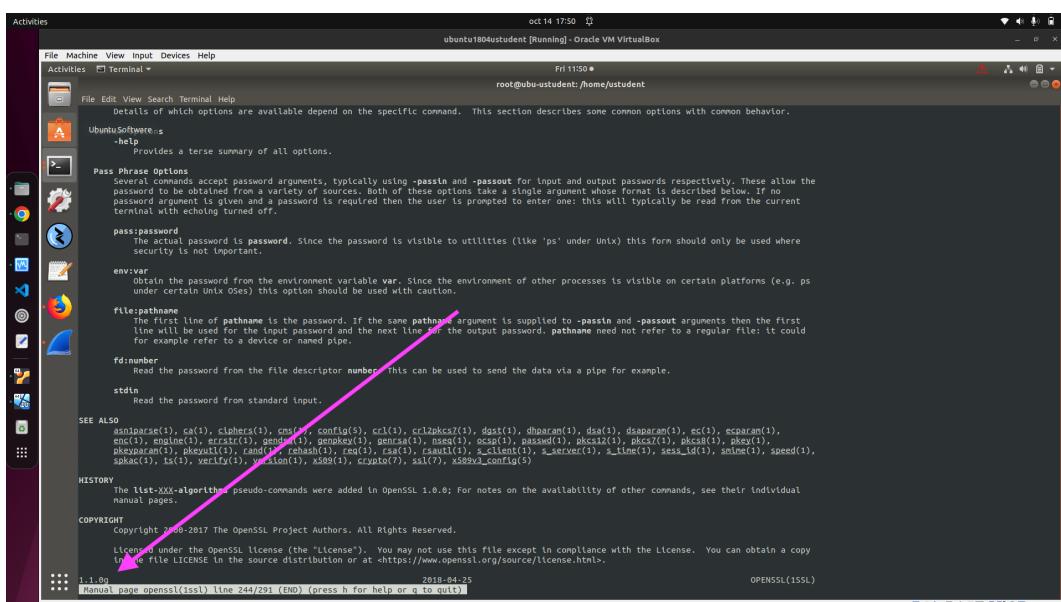
Maintaining FIPS Certified modules security

To keep your FIPS Certified Ubuntu secure we will re-certify all modules every year.

Today, Ubuntu 18.04 LTS and 16.04 LTS has certifications for 5 distinct modules:

Ubuntu 18.04 LTS

Component	Description	Version	CMVP Certificate
Linux kernel (generic)	The Linux kernel cryptographic library	4.15.0	3647
OpenSSL	General purpose cryptographic library that includes TLS implementation	1.1.1	3622
OpenSSH client	SSH server application for operating systems	7.9p1	3633
OpenSSH server	SSH client application for operating systems	7.9p1	3632
StrongSWAN	IPSec based VPN solution library	5.6.2	3648



```
Activities          oct 14 17:50 ⓘ
ubuntu@ubu-ustudent [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Fri 11:50 ⓘ
root@ubu-ustudent: /home/ustudent
UbuntuSoftware.s -help
Provides a terse summary of all options.

Pass Phrase Options:
  Several commands accept password arguments, typically using -passin and -passout for input and output passwords respectively. These allow the password to be obtained from a variety of sources. Both of these options take a single argument whose format is described below. If no password argument is given and a password is required then the user is prompted to enter one: this will typically be read from the current terminal with echoing turned off.

  pass:password
    The actual password is password. Since the password is visible to utilities (like 'ps' under Unix) this form should only be used where security is not important.

  env:var
    Obtain the password from the environment variable var. Since the environment of other processes is visible on certain platforms (e.g. ps under certain Unix OSes) this option should be used with caution.

  file:pipeline
    The first line of pipeline is the password. If the same pipeline argument is supplied to -passin and -passout arguments then the first line will be used for the input password and the next line for the output password. pipeline need not refer to a regular file: it could for example refer to a device or named pipe.

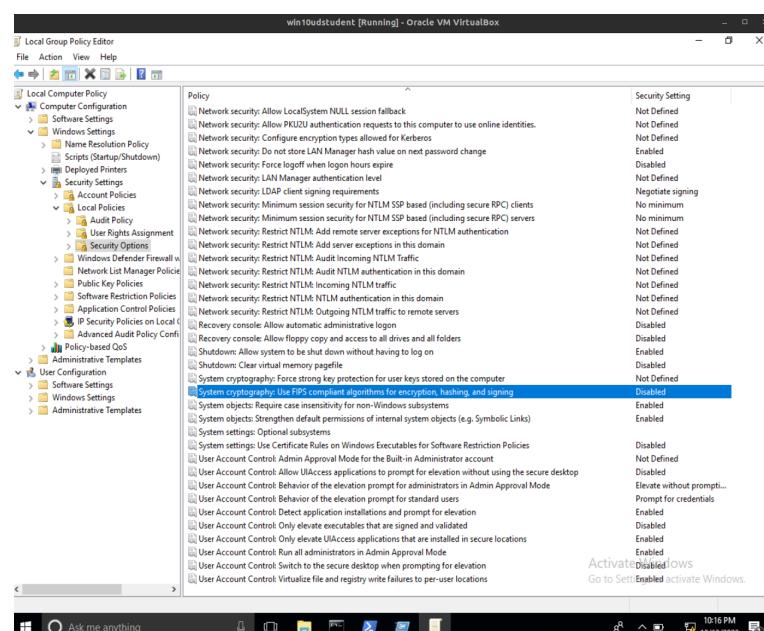
  fd:number
    Read the password from the file descriptor number, this can be used to send the data via a pipe for example.

  stdn
    Read the password from standard input.

SEE ALSO
asn1parse(1), ca(1), ciphers(1), cnf(1), config(5), crl(1), dgst(1), dhparam(1), dsa(1), disparam(1), ec(1), ecpair(1),
enc(1), engine(1), errstr(1), gen(1), genkey(1), gencat(1), nsecd(1), oscar(1), passwd(1), pkcs12(1), pkcs7(1), pkey(1),
pkcs15(1), pkcs12(1), rand(1), rehash(1), ren(1), rsautl(1), sclient(1), s_server(1), s_time(1), sess_id(1), snime(1), speed(1),
srandom(1), tms(1), verify(1), vnc(1), x509(1), crypto(7), ssl(7), x509v3(5)
HISTORY
The llet-XXX-algorithm pseudo-commands were added in OpenSSL 1.0.0; For notes on the availability of other commands, see their individual manual pages.

COPYRIGHT
Copyright 2000-2017 The OpenSSL Project Authors. All Rights Reserved.

License under the OpenSSL license (the "License"). You may not use this file except in compliance with the License. You can obtain a copy of the file LICENSE in the source distribution or at https://www.openssl.org/source/license.html.
```



win10ustudent [Running] - Oracle VM VirtualBox

File Action View Help

Local Computer Policy

Policy

Network security: Allow LocalSystem NULL session fallback
Network security: Allow PKI2U authentication requests to this computer to use online identities
Network security: Configure encryption types allowed for Kerberos
Network security: Do not store LAN Manager hash value on net password change
Network security: Force logoff when logon hours expire
Network security: LAN Manager authentication level
Network security: LDAP client signing requirements
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers
Network security: Restrict NTLM: Add remote server exceptions for NTLM authentication
Network security: Restrict NTLM: Add server exceptions in this domain
Network security: Restrict NTLM: Audit incoming NTLM Traffic
Network security: Restrict NTLM: Audit NTLM authentication in this domain
Network security: Restrict NTLM: Incoming NTLM traffic
Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers
Recovery console: Allow automatic administrative logon
Shutdown: Allow system to be shut down without having to log on
Shutdown: Clear virtual memory pagefile
System objects: Force strong key protection for user keys stored on the computer
System objects: Force strong key protection for user keys stored on the computer (disabled)
System objects: Require case insensitivity for non-Windows subsystems
System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)
System settings: Optional subsystems
System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies
User Account Control: Admin Approval Mode for the Built-in Administrator account
User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop
User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode
User Account Control: Behavior of the elevation prompt for standard users
User Account Control: Detect application installations and prompt for elevation
User Account Control: Only elevate executables that are signed and validated
User Account Control: Only elevate UIAccess applications that are installed in secure locations
User Account Control: Run all administrators in Admin Approval Mode
User Account Control: Switch to the secure desktop when prompting for elevation
User Account Control: Virtualize file and registry write failures for per-user locations

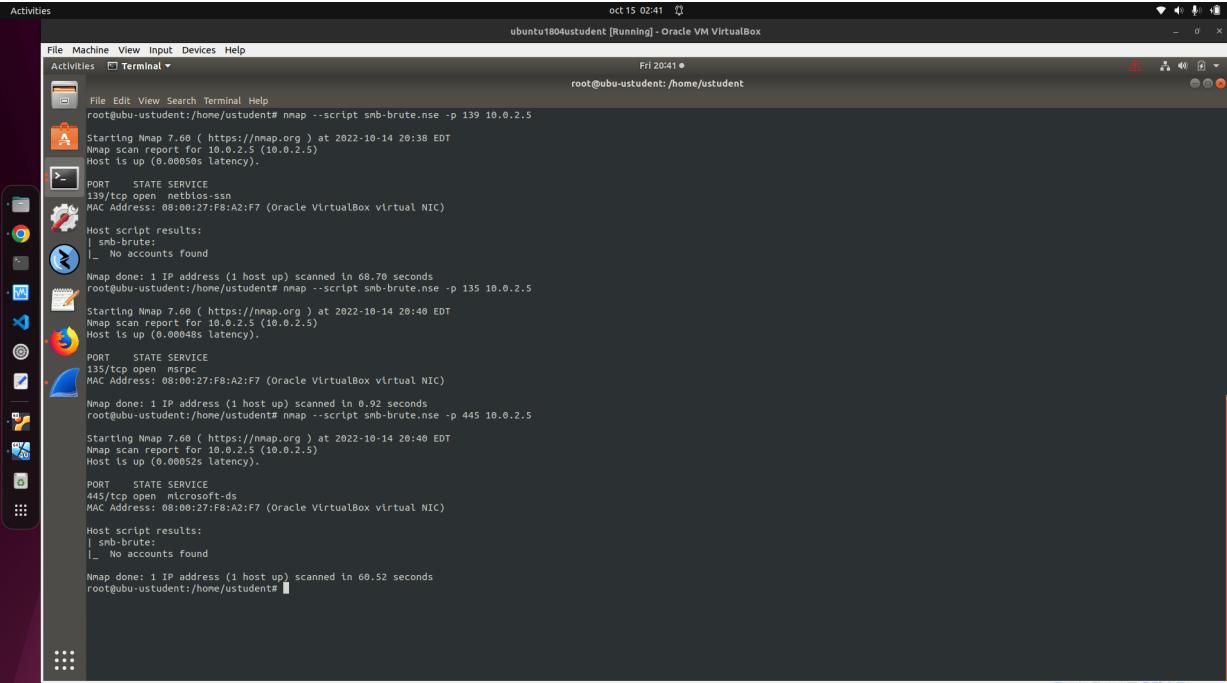
Activated: Disabled (Windows Go to Settings)

10:16 PM 10/15/2022

4.4 Conduct aggressive testing for password strength Mitre ATT&CK T1110

- **4.4.1** SMB shares at Windows virtual machine
- **4.4.2** FTP Server at Ubuntu virtual machine

• Windows



Activities oct 15 02:41 ubuntu1804student [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help Activities Terminal Fri 20:41 root@ubu-ustudent: /home/ustudent

```
root@ubu-ustudent:~/home/ustudent# nmap --script smb-brute.nse -p 139 10.0.2.5
Starting Nmap 7.60 ( https://nmap.org ) at 2022-10-14 20:38 EDT
Nmap scan report for 10.0.2.5 (10.0.2.5)
Host is up (0.00050s latency).

PORT      STATE SERVICE
139/tcp    open  netbios-ssn
MAC Address: 08:00:27:F8:A2:F7 (Oracle VirtualBox virtual NIC)

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

Nmap done: 1 IP address (1 host up) scanned in 68.70 seconds
root@ubu-ustudent:~/home/ustudent# nmap --script smb-brute.nse -p 135 10.0.2.5
Starting Nmap 7.60 ( https://nmap.org ) at 2022-10-14 20:40 EDT
Nmap scan report for 10.0.2.5 (10.0.2.5)
Host is up (0.00048s latency).

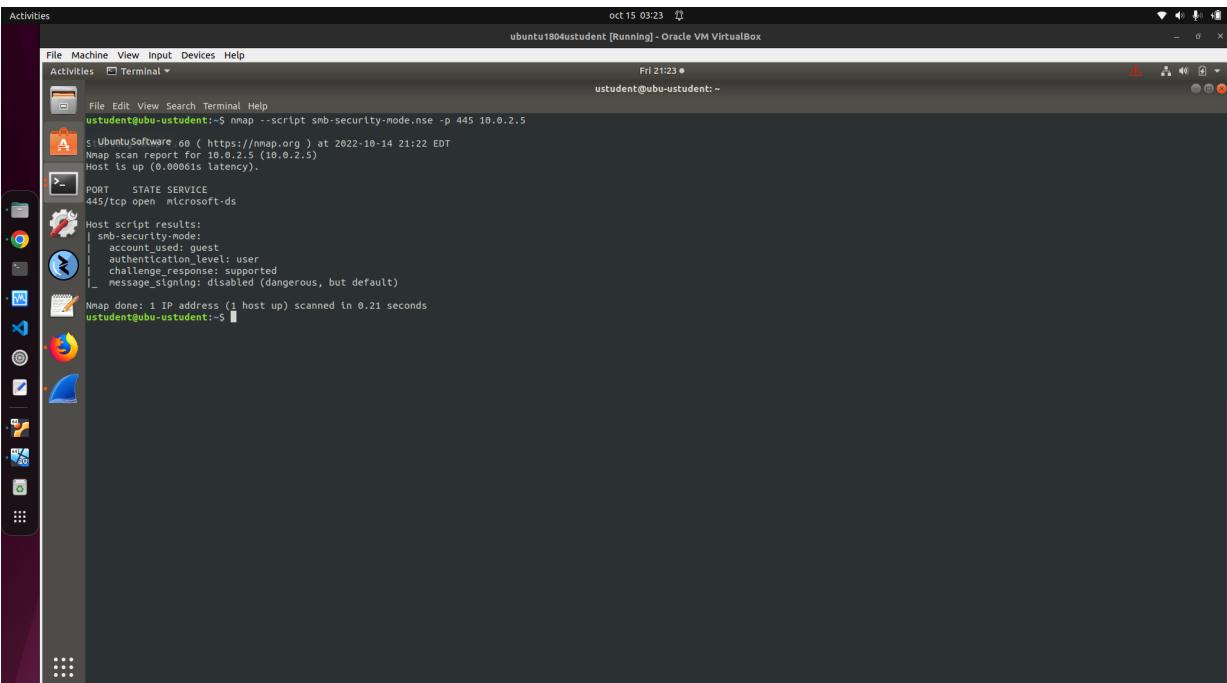
PORT      STATE SERVICE
135/tcp   open  msrpc
MAC Address: 08:00:27:F8:A2:F7 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.92 seconds
root@ubu-ustudent:~/home/ustudent# nmap --script smb-brute.nse -p 445 10.0.2.5
Starting Nmap 7.60 ( https://nmap.org ) at 2022-10-14 20:40 EDT
Nmap scan report for 10.0.2.5 (10.0.2.5)
Host is up (0.00052s latency).

PORT      STATE SERVICE
445/tcp   open  microsoft-ds
MAC Address: 08:00:27:F8:A2:F7 (Oracle VirtualBox virtual NIC)

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

Nmap done: 1 IP address (1 host up) scanned in 60.52 seconds
root@ubu-ustudent:~/home/ustudent#
```



Activities oct 15 03:23 ubuntu1804student [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help Activities Terminal Fri 21:23 root@ubu-ustudent: ~

```
ustudent@ubu-ustudent:~$ nmap -s-script smb-security-mode.nse -p 445 10.0.2.5
Starting Nmap 7.60 ( https://nmap.org ) at 2022-10-14 21:22 EDT
Nmap scan report for 10.0.2.5 (10.0.2.5)
Host is up (0.00061s latency).

PORT      STATE SERVICE
445/tcp   open  microsoft-ds

Host script results:
| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
| message_signing: disabled (dangerous, but default)
|_ No accounts found

Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
ustudent@ubu-ustudent:~$
```

- Ubuntu

