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

1.2 Windows CIS 18.9.102.2

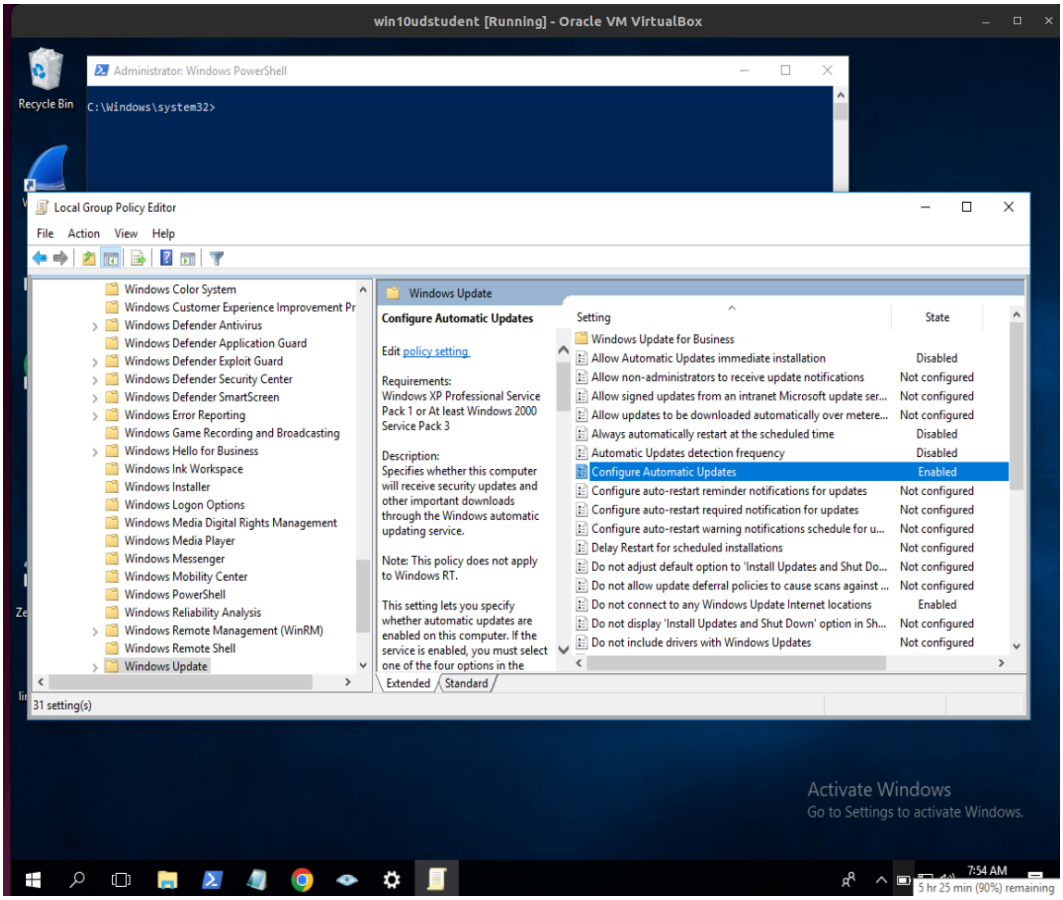
- Ensure 'configure automatic updates' is set to 'Enabled.'

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

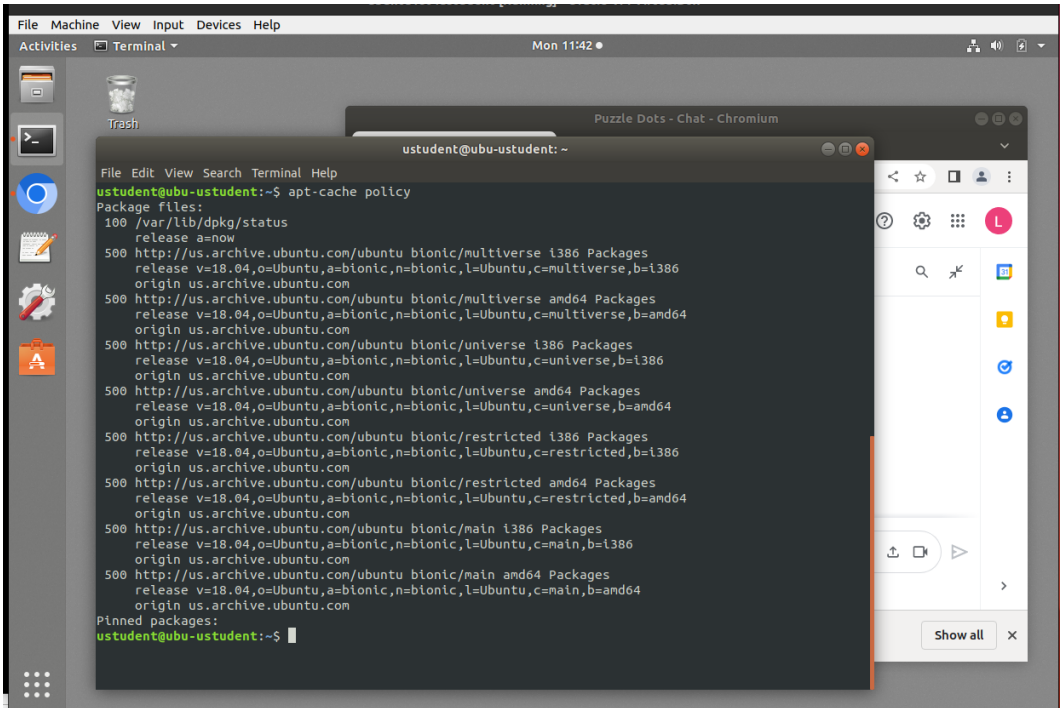
- Ensure package manager repositories are configured correctly.

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

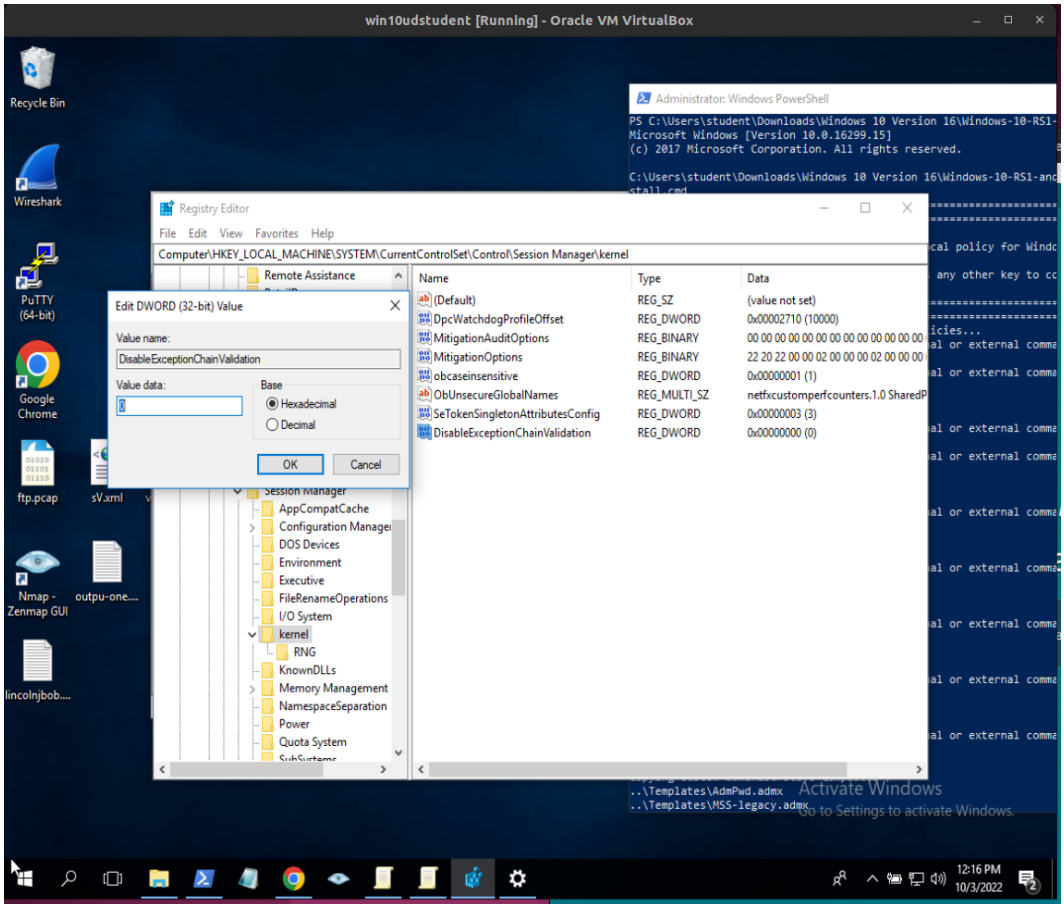
- Ensure 'Enable Structured Exception Handling Overwrite Protection (SEHOP)' is set to 'Enabled.'
- Provide documentation as to what applications are installed on the Windows machine.

Description:

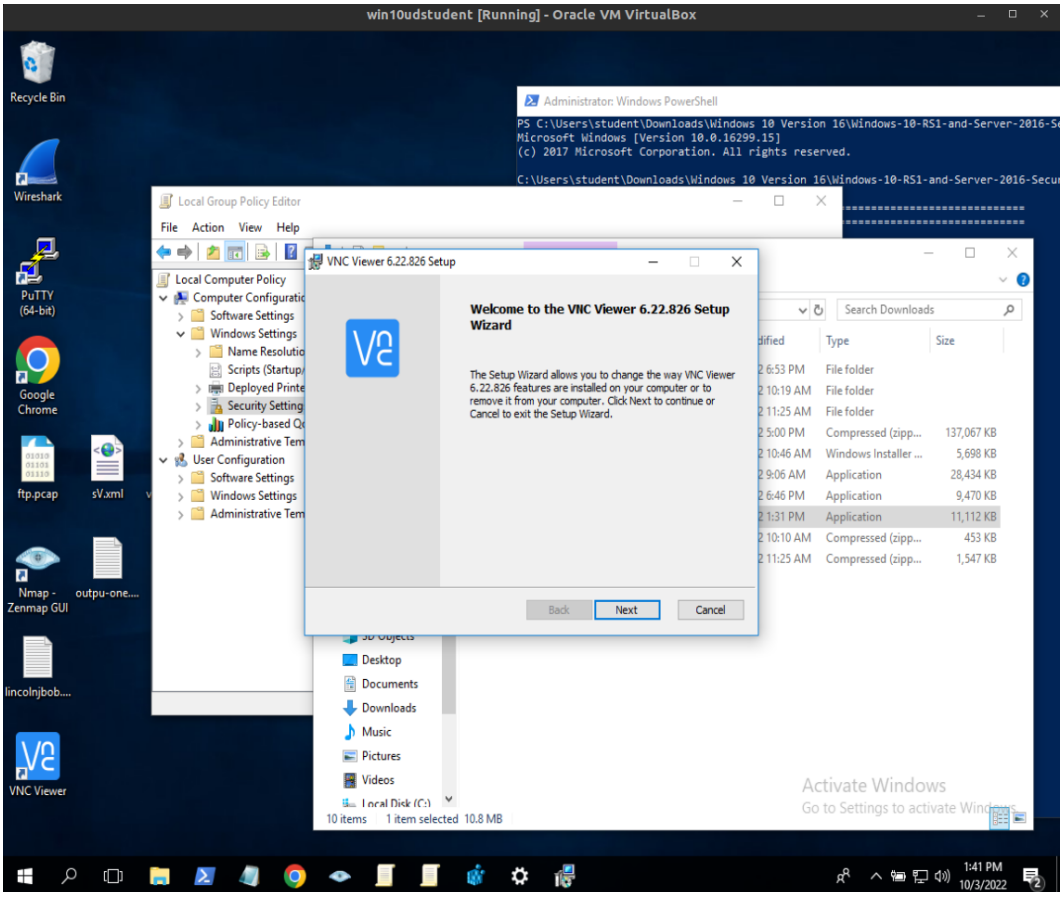
Windows includes support for Structured Exception Handling Overwrite Protection (SEHOP). CIS recommend enabling this feature to improve the security profile of the system.

Remediation:

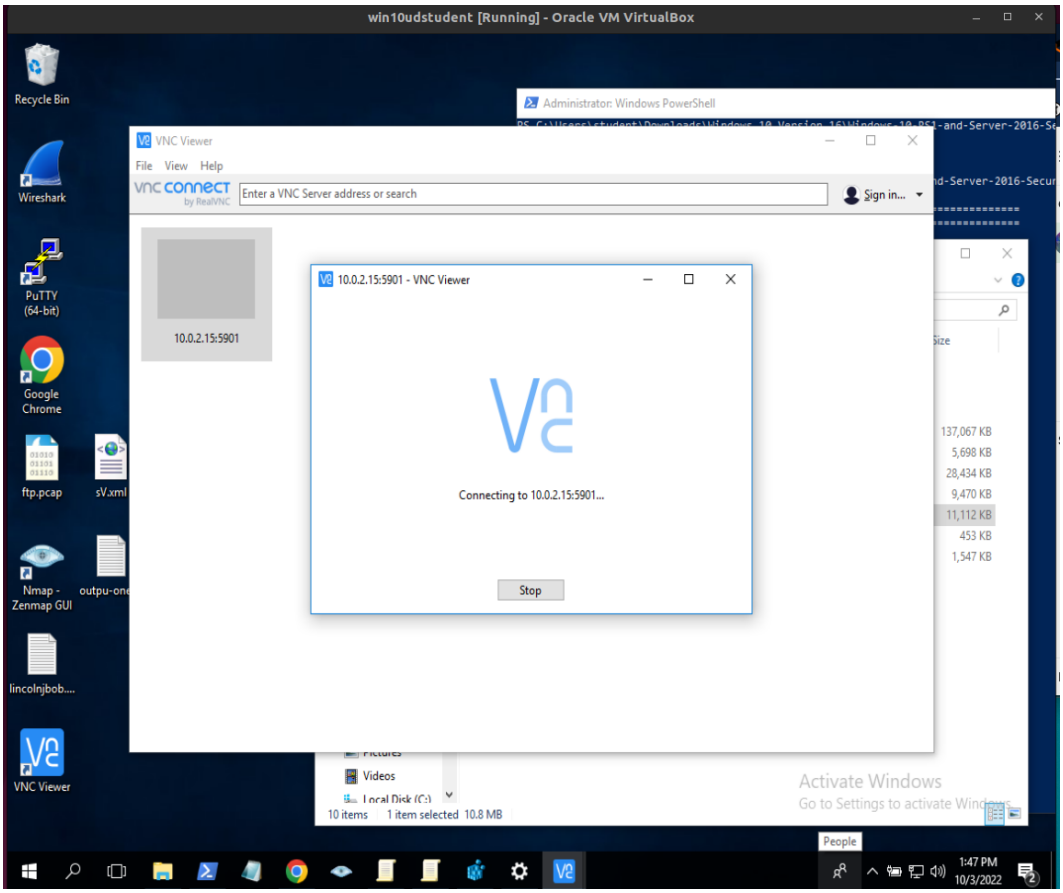
Set the value to 0 of DisableExceptionChainValidation in the Registry manually at HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\kernel\DisableExceptionChainValidation.



win10udstudent ova



win10udstudent ova - Follow default installation



win10udstudent ova - VNC installed and running

VNC installation screenshots: (next page)

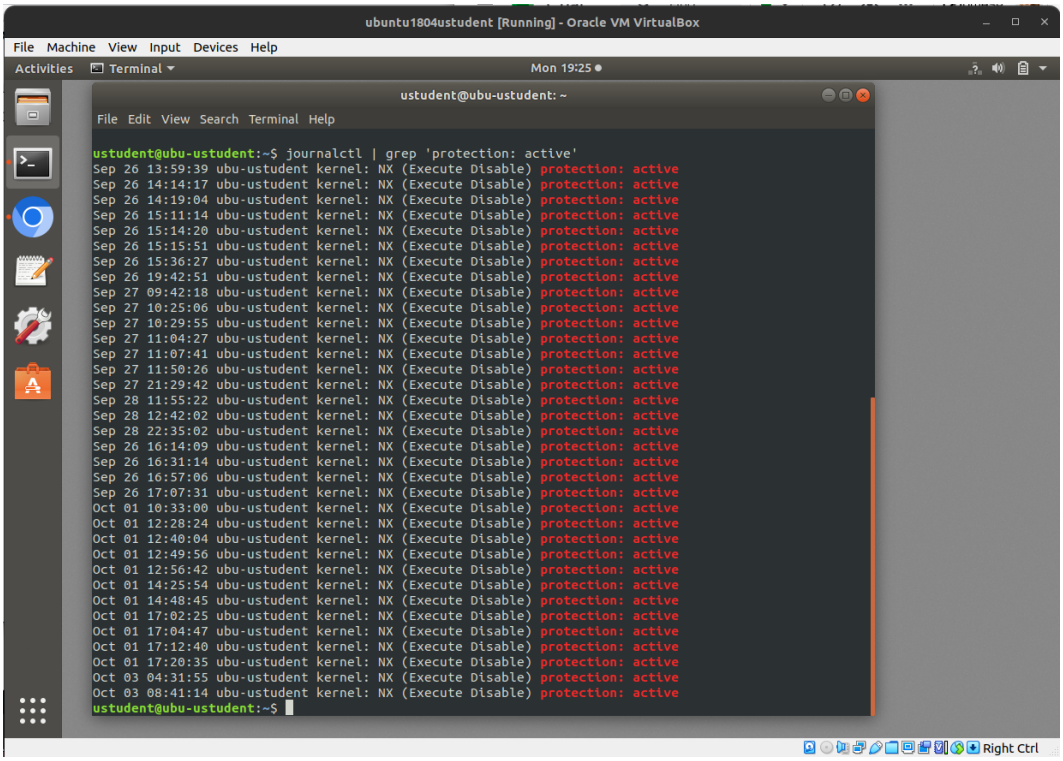
1.3 Ubuntu CIS 1.6.1, 1.6.2

- 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.



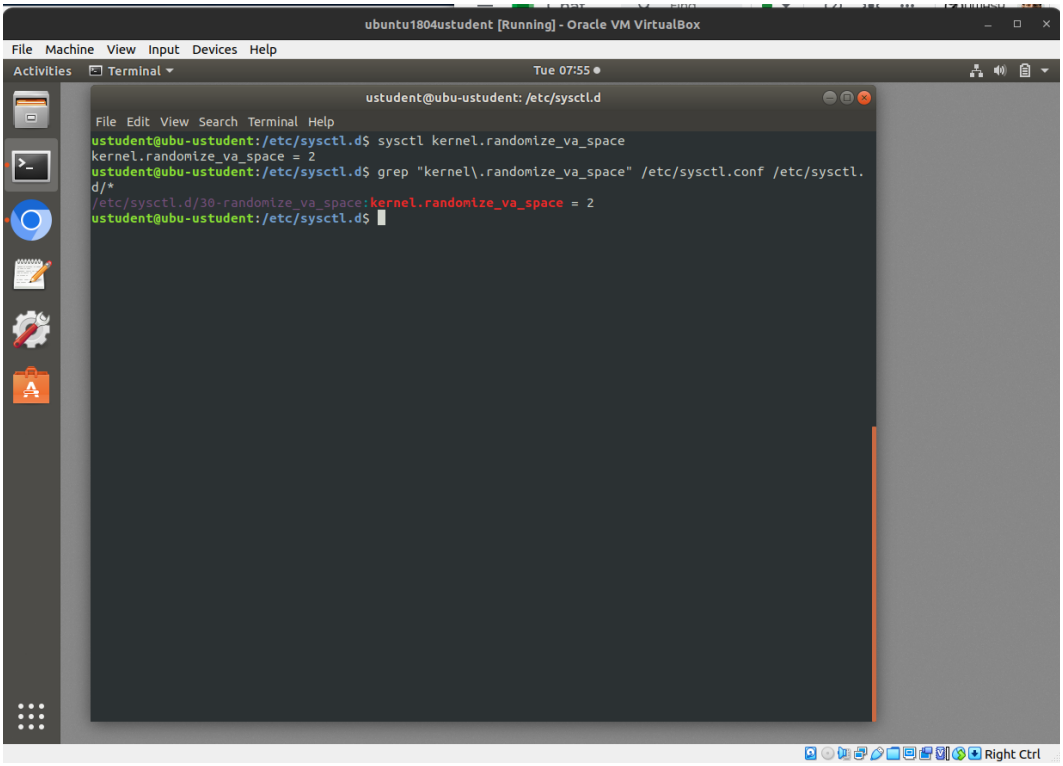
ustudent@ubu-ustudent ova

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.

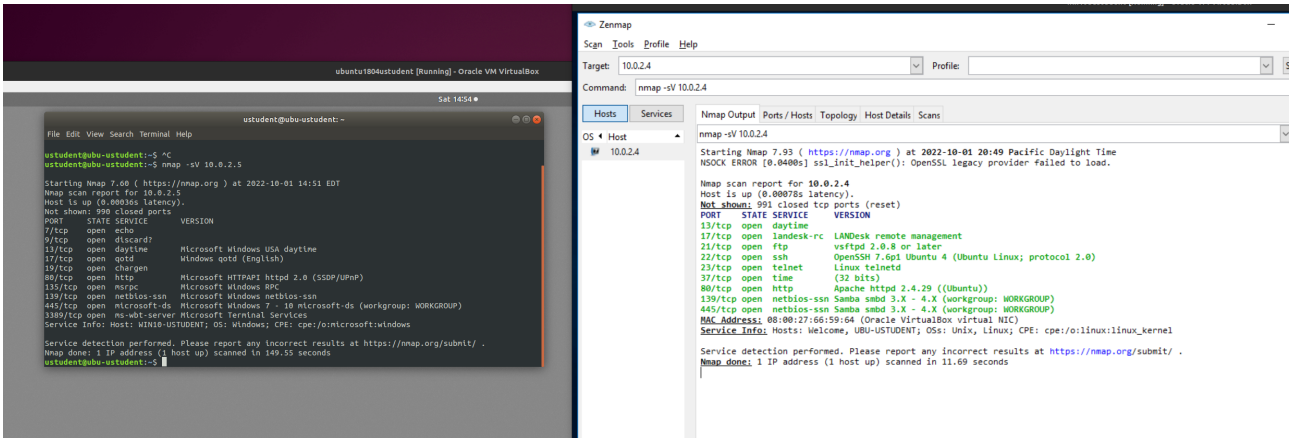
Result:

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



ustudent@ubu-ustudent ova

1.4 Open ports Ubuntu / Windows



Recommendations:
Primarly, 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 transfered 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.

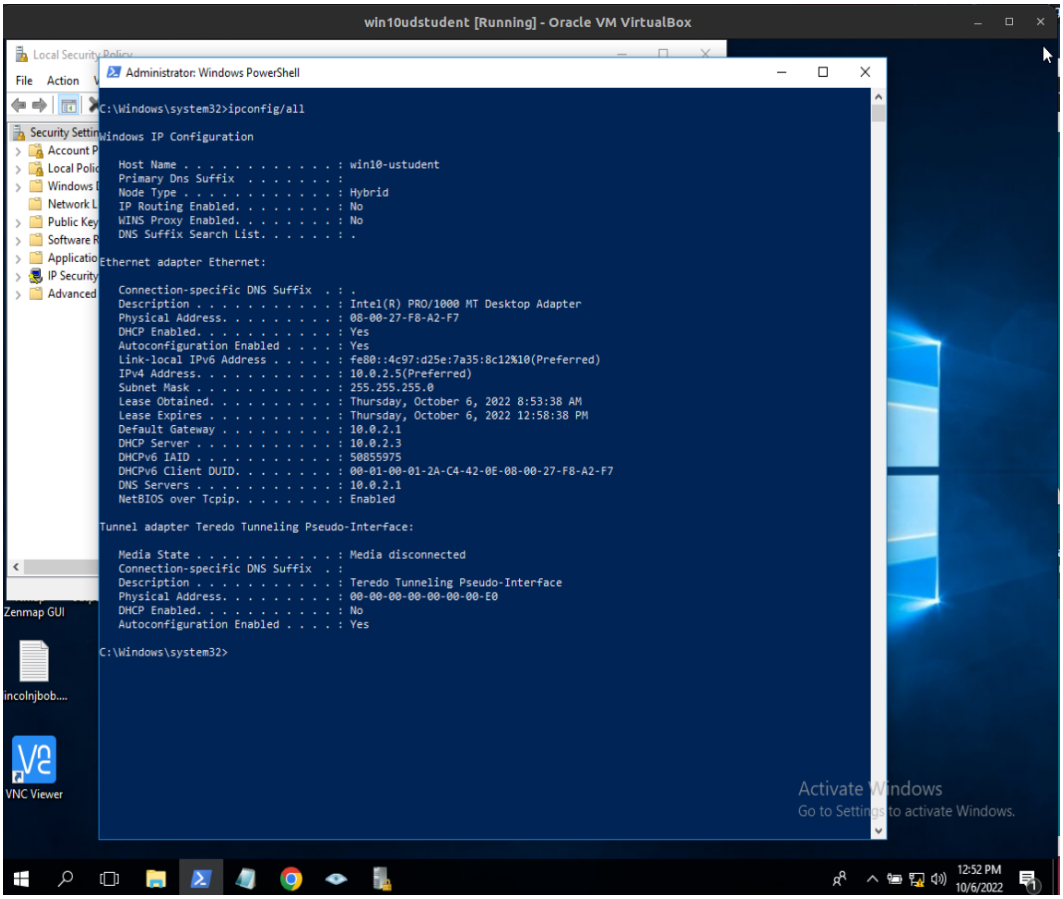
2: Assess Access Management at Targeted Assets

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

• **Windows**

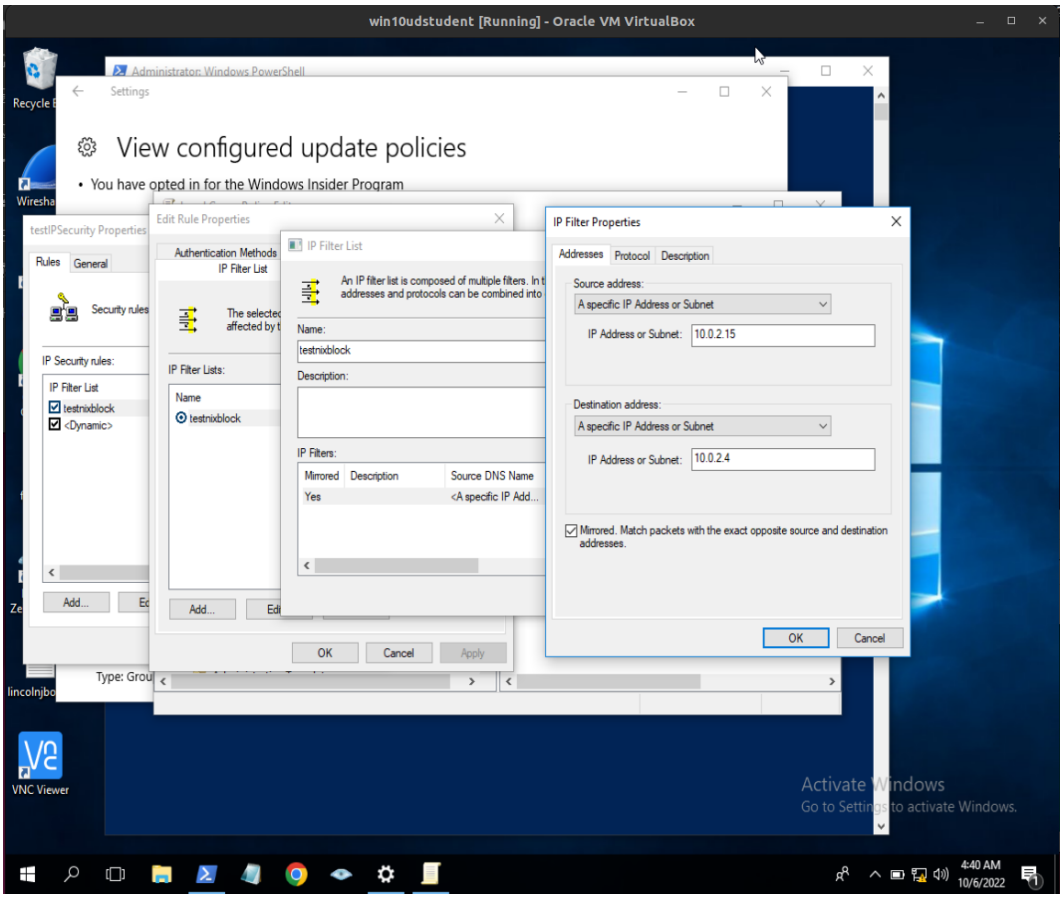
1. VLANs

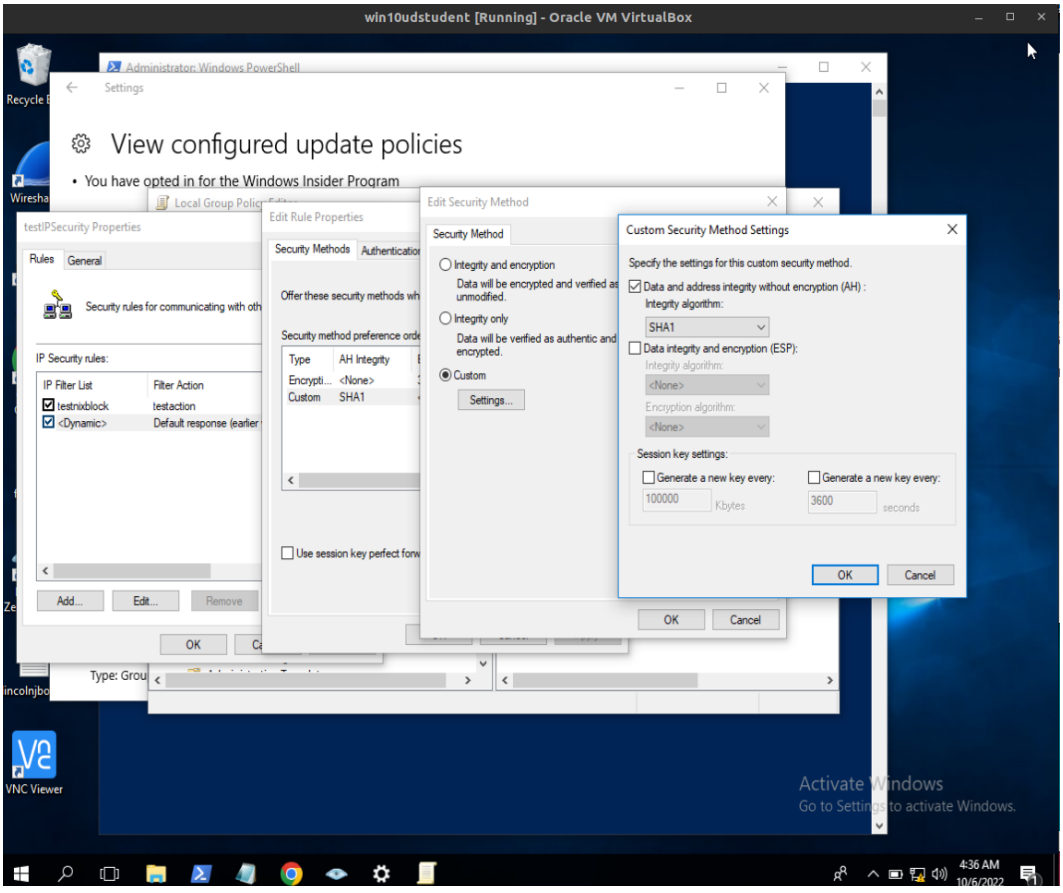
There aren't VLAN present in windows machine. VLANs are created and operated within an Ethernet network to perform isolation per network segment which is totally absent.

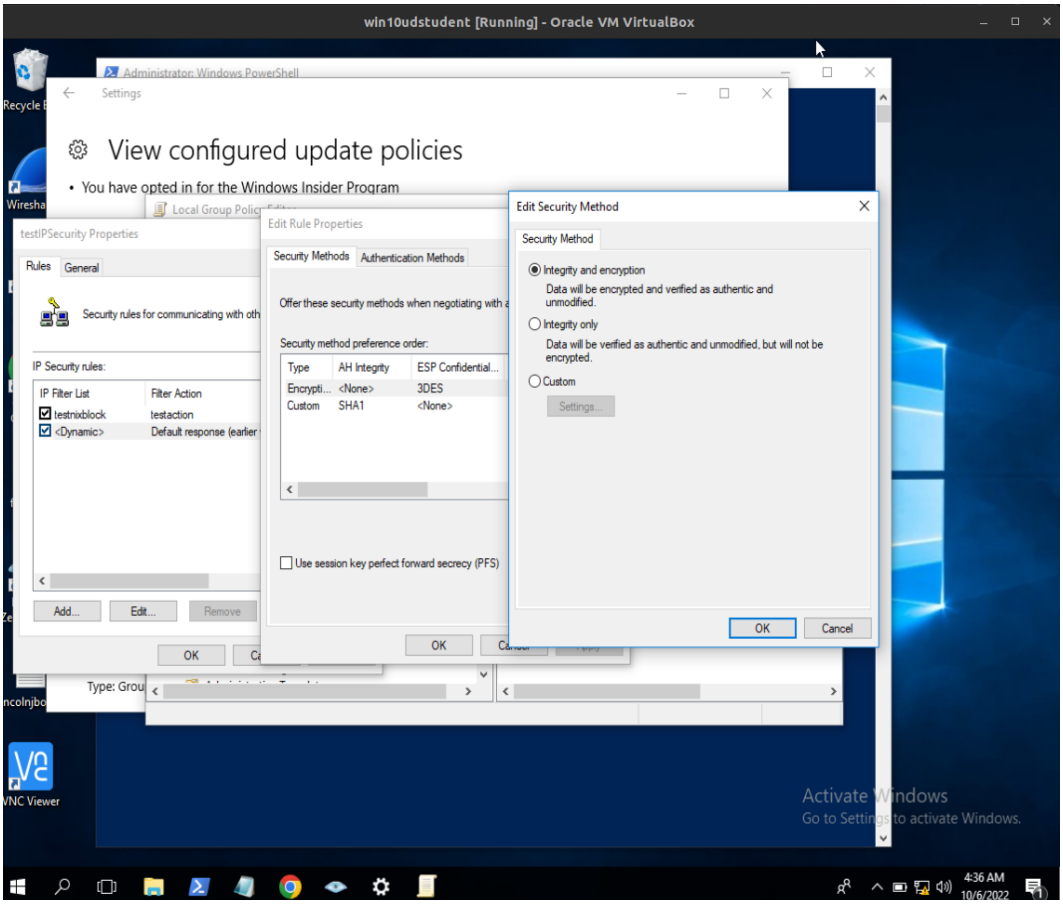


win10udstudent ova

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 destionation the Ubuntu machine called ustudent@ubu-ustudent.

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

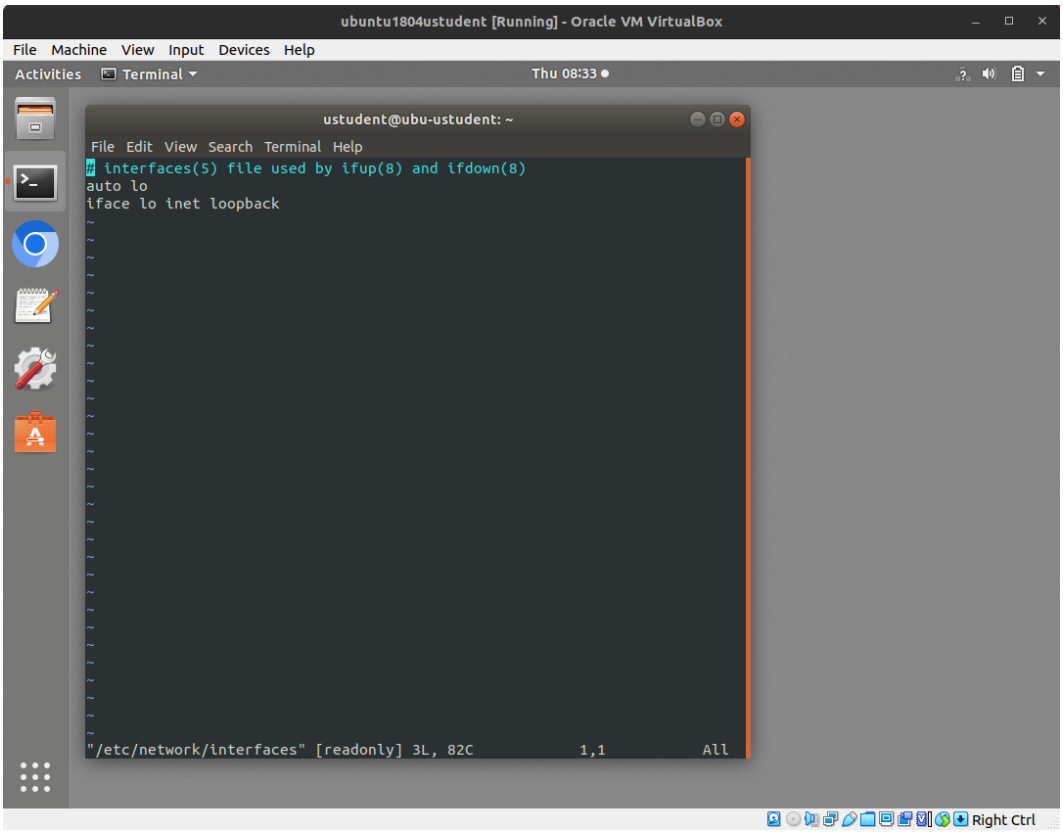
In this way, there is no Domain Isolation enforced from IPSecurity Policies since there isn't rule schemas for Group Policies besides the blocking rule mentioned.

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.

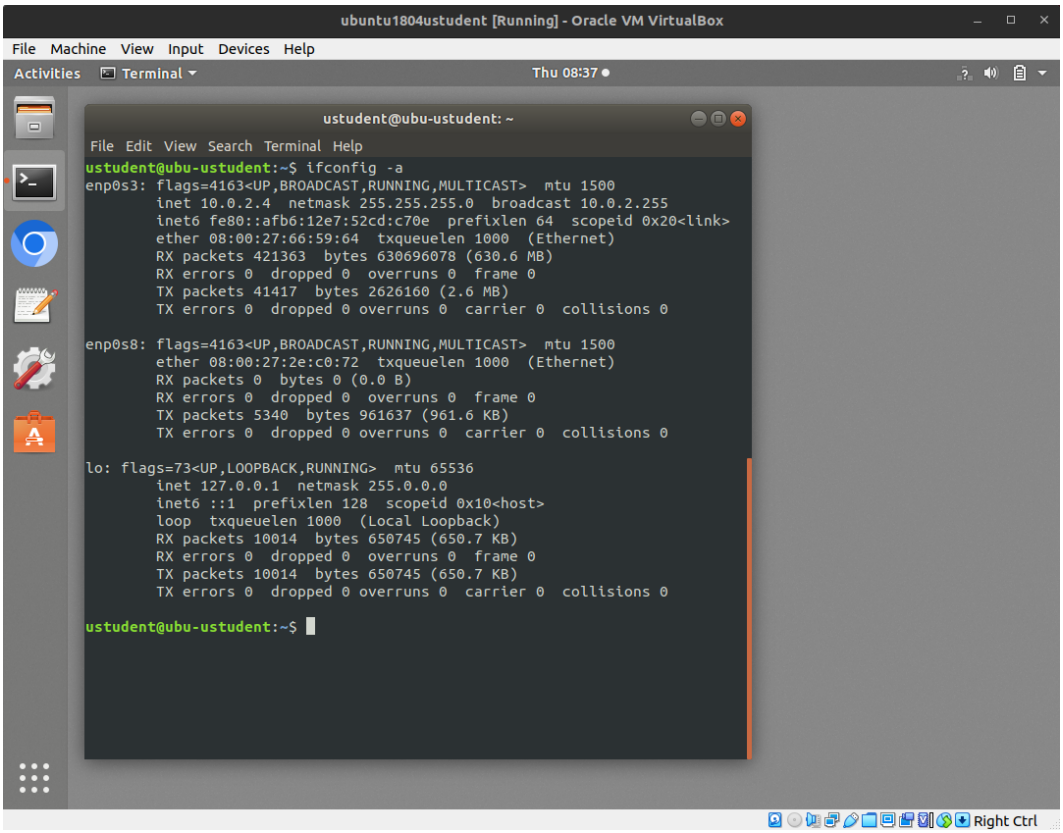
• Ubuntu

1. VLANs



ustudent@ubu-ustudent ova

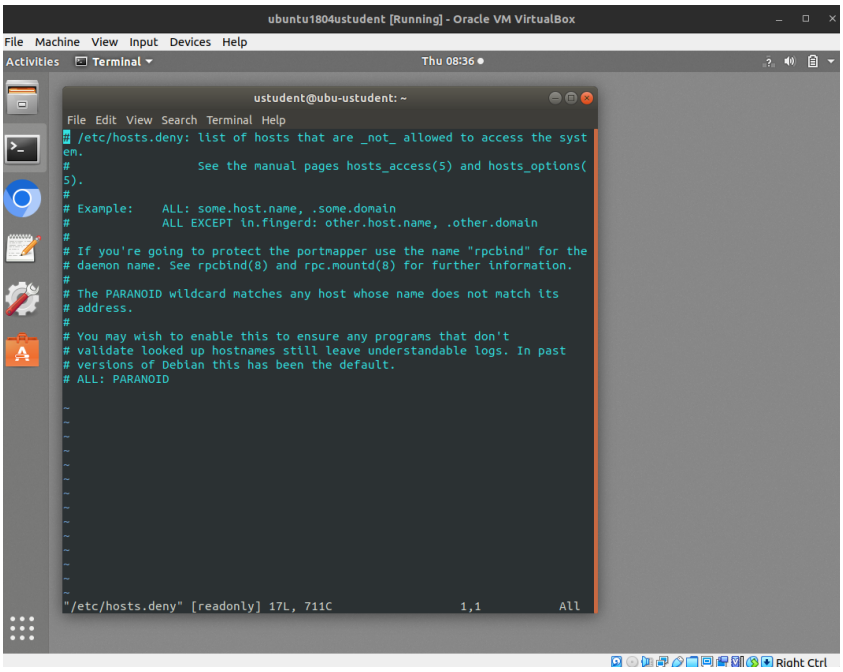
No VLAN has been set in the Ubuntu machine, in this sense there is no isolation per network segment or networks are segmentation neither.

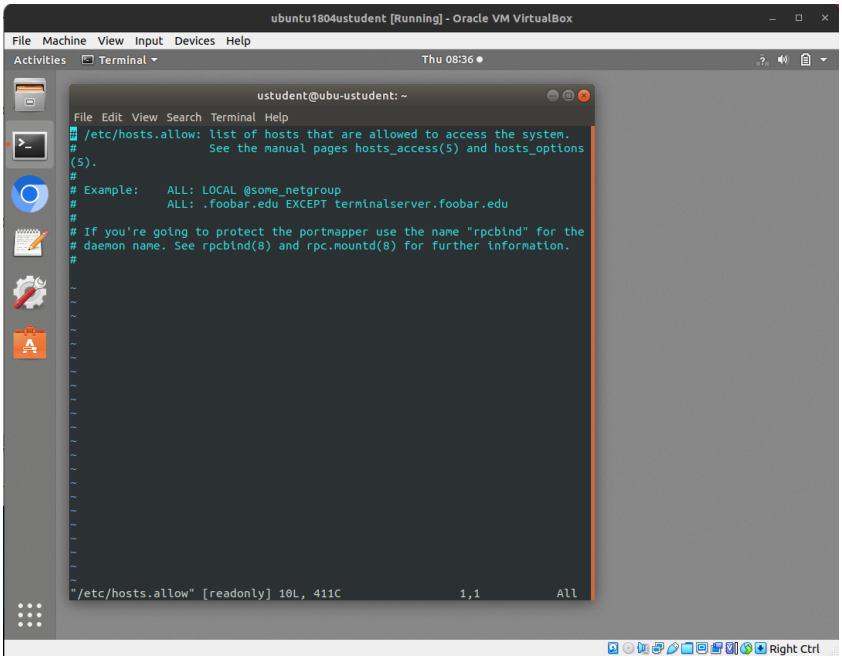


ustudent@ubu-ustudent ova

This screenshot show 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





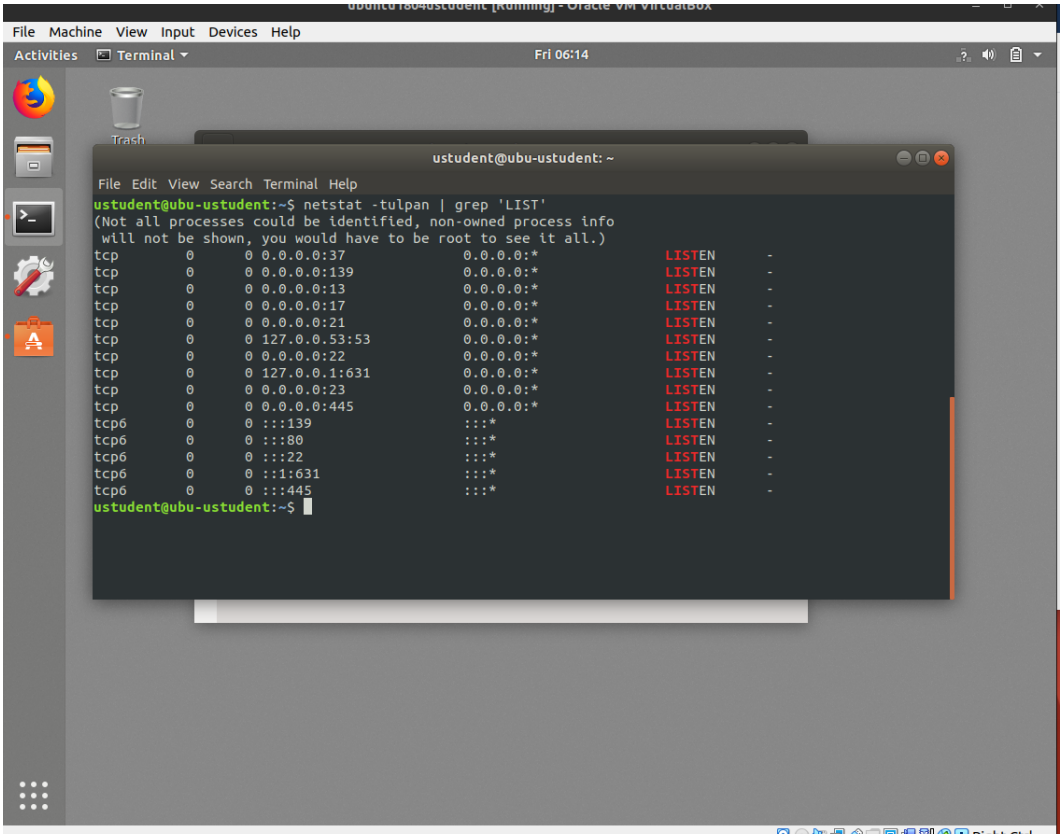
ustudent@ubu-ustudent ova

According to the files consulted, there were no IP Security policies implemented in order to block or allow ip addresses or segment the traffice 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

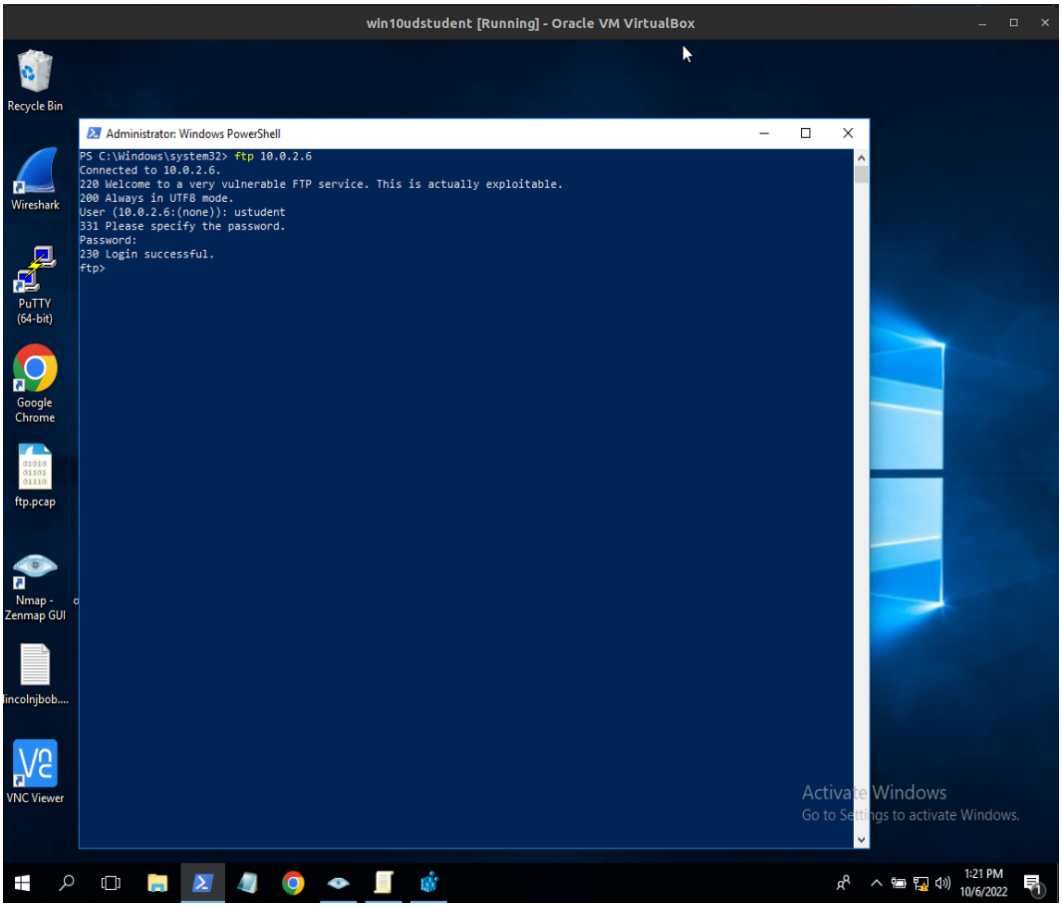
1. Remote access services and protocols



ustudent@ubu-ustudent ova

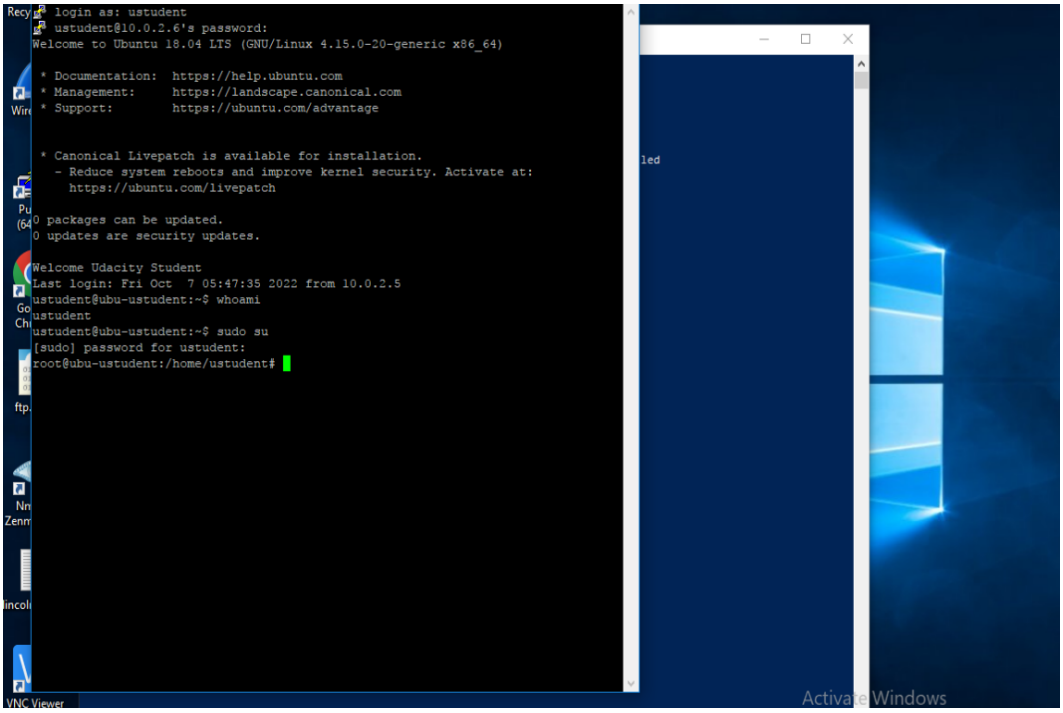
Remote access services and protocols in place allocate in port 21 (FTP), 22 (SSH) and 23 (telnet) as seen in the image above. This ports are open and ready waiting for connections, they are listen for external request of service.

- **FTP (21)**



win10udstudent ova

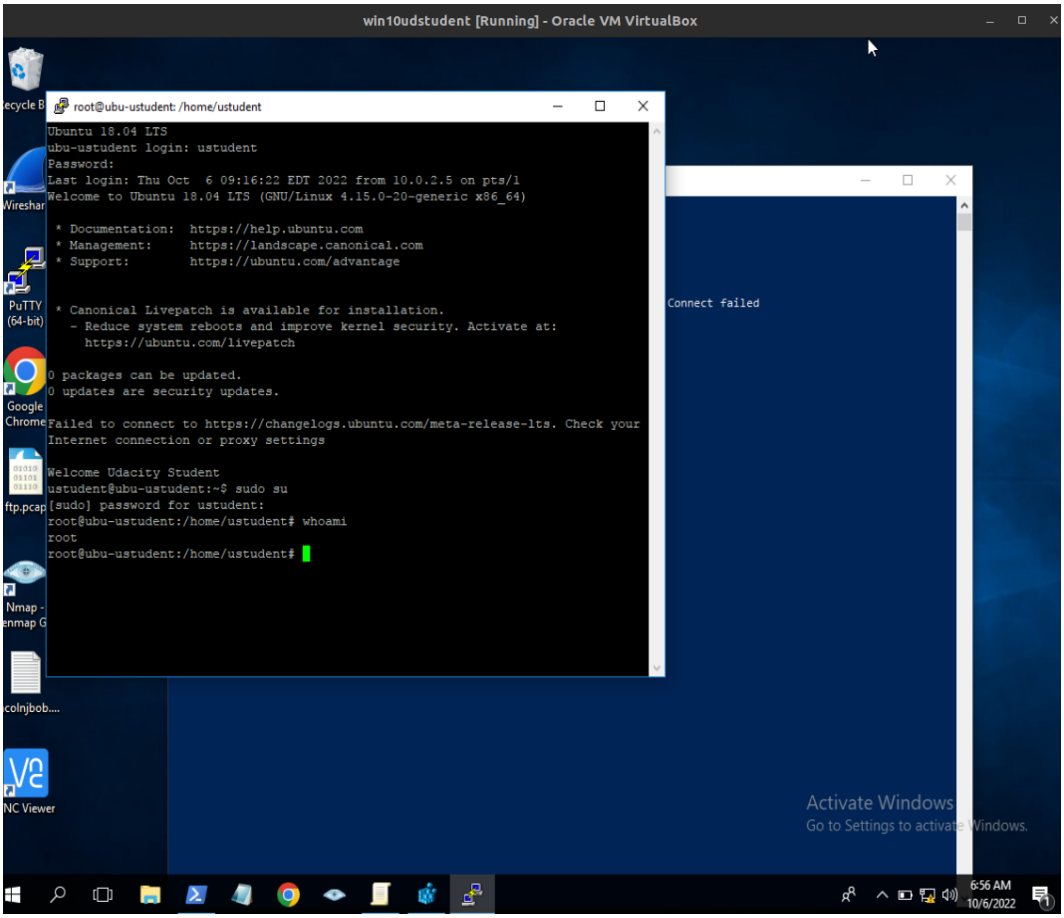
- **SSH (22)**



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.

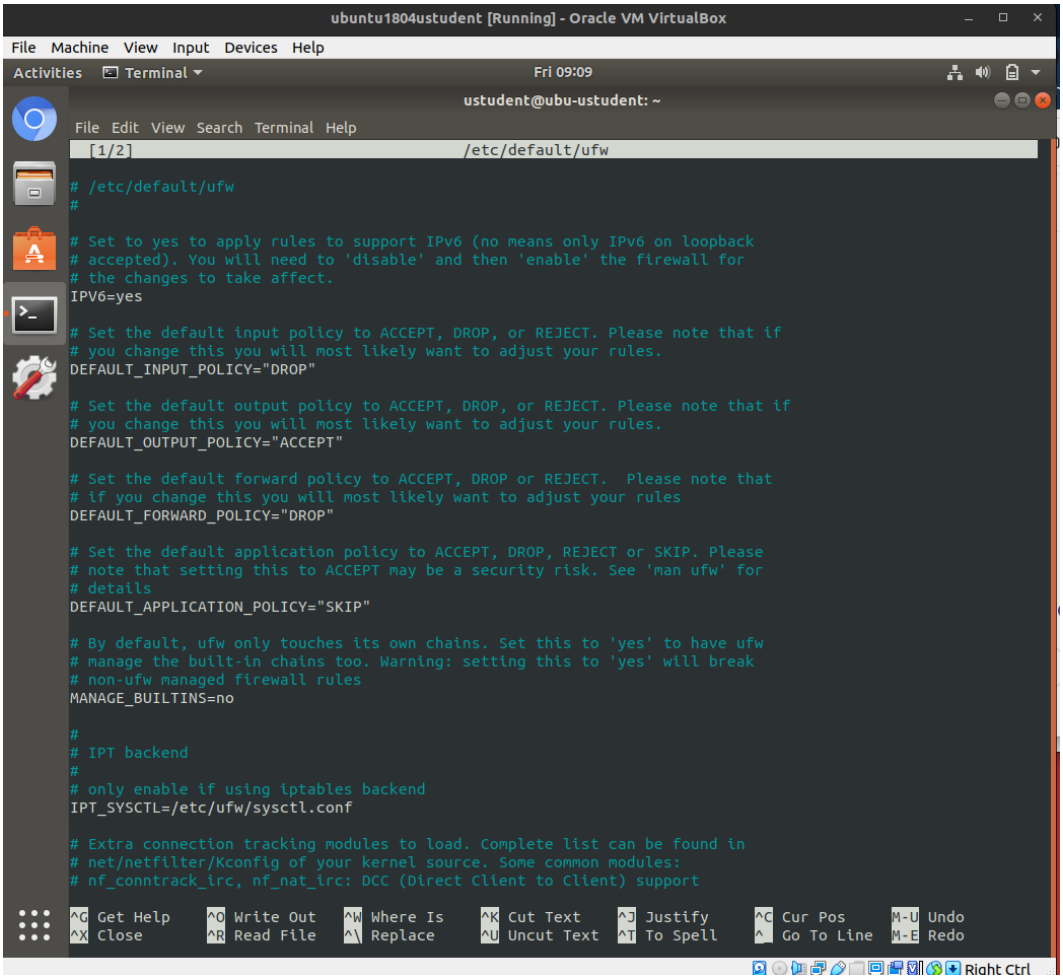
There is no constraints in order to filter inbound connections as seen in the previous topics nor firewalls (images in next topic - 2.3) rules that apply any layer of protection more than the user & password of the system (which is not a 100% secure protection).

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 potencial 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 pictore above.

- **IPv6**

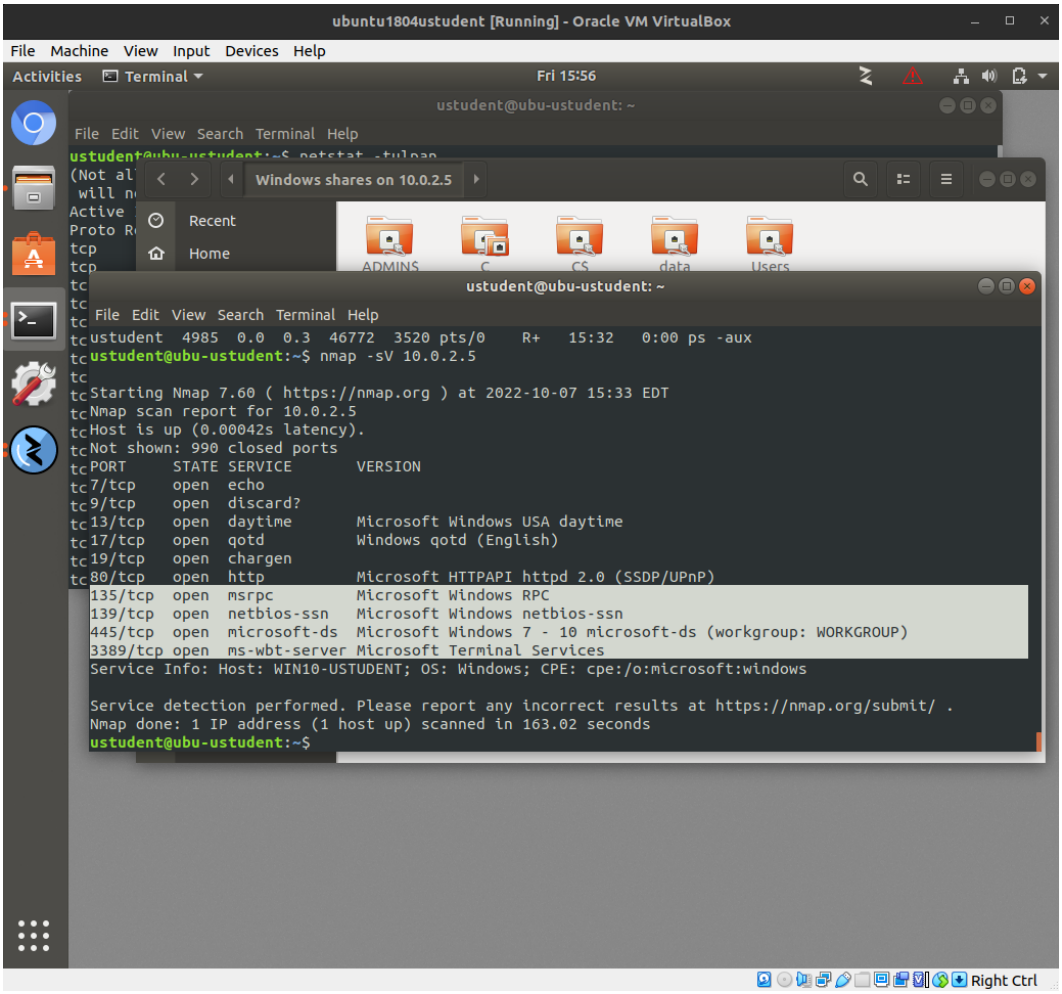


ustudent@ubu-ustudent ova

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

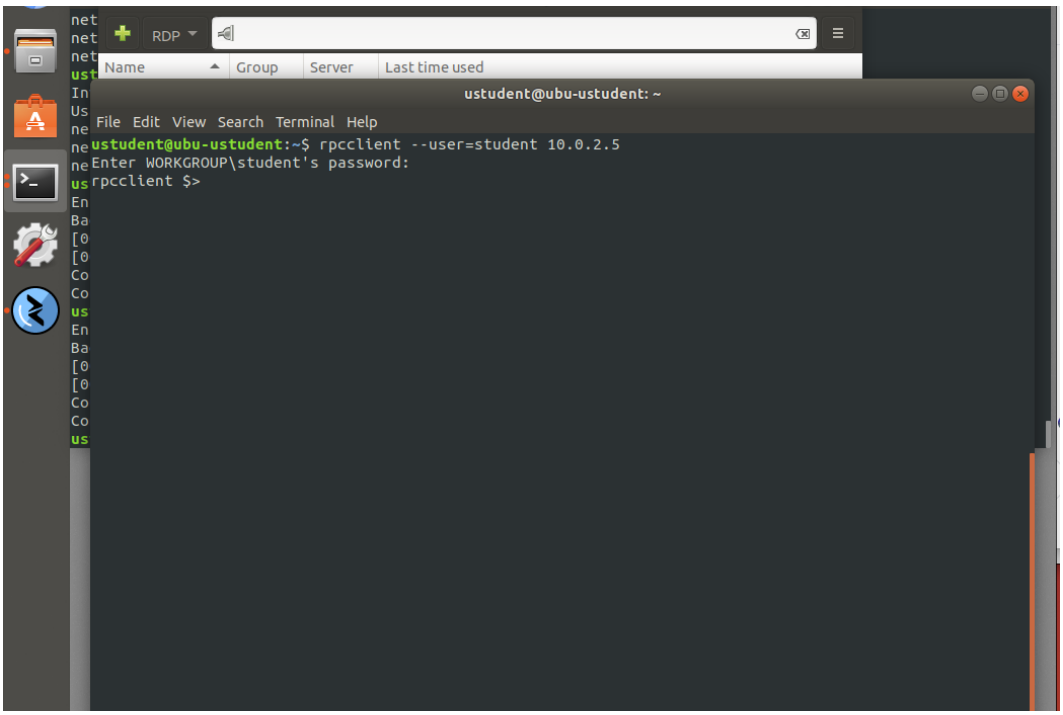
1. Remote access services and protocols



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. This ports are open and ready waiting for connections, listen for external request of service without more security than username & password.

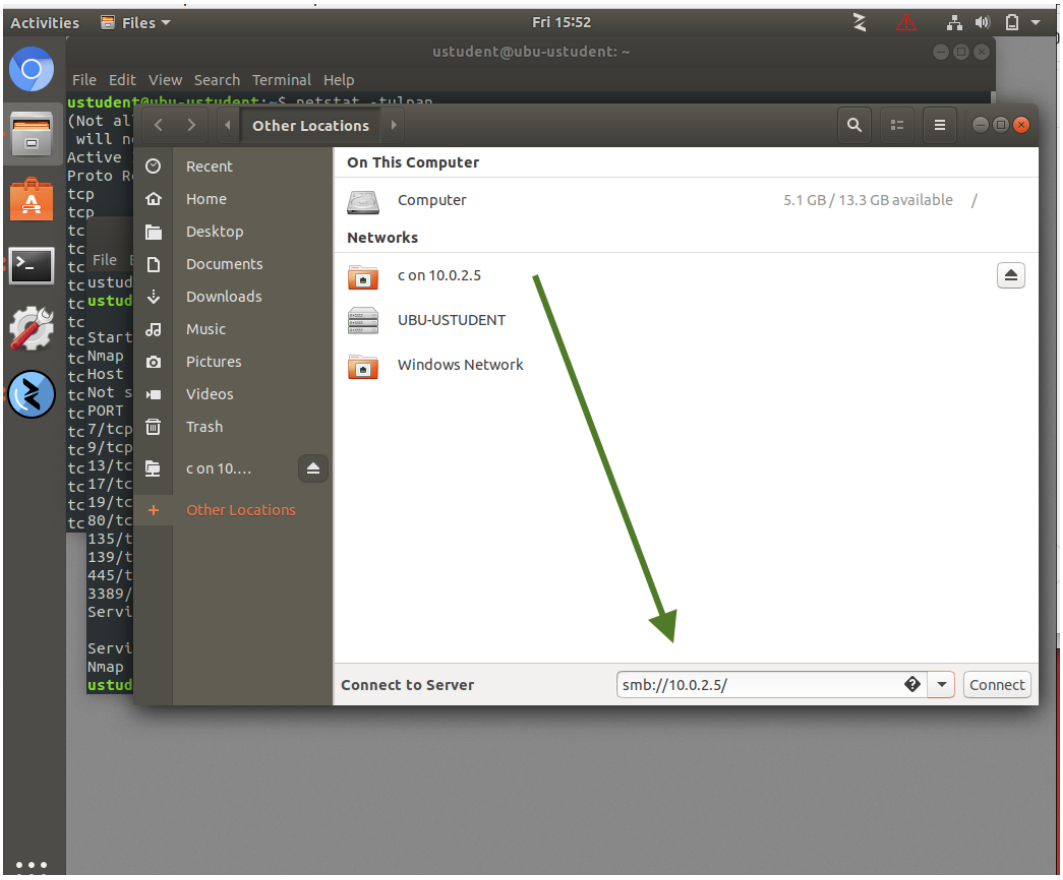
- **135 (RPC)**



win10udstudent ova

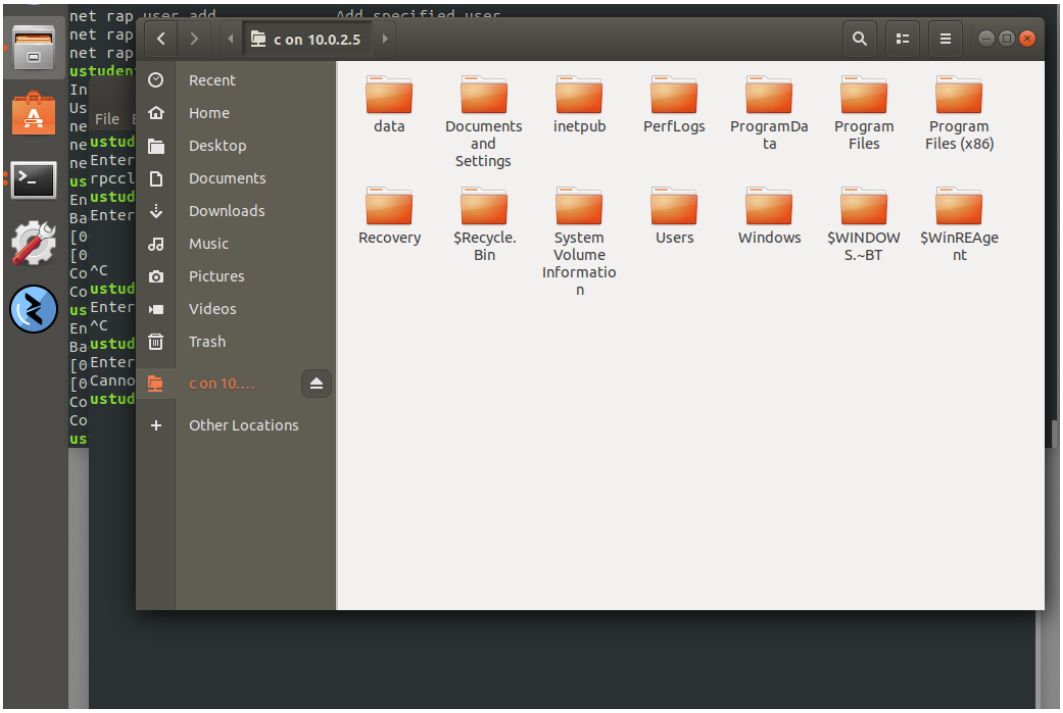
Remote Procedure Call (RPC) port 135 is used in client/server applications such as Exchange clients (e.g messenger service) as well as other Windows NT/2K/XP software, in order to allow one program to request service from a program on another computer.

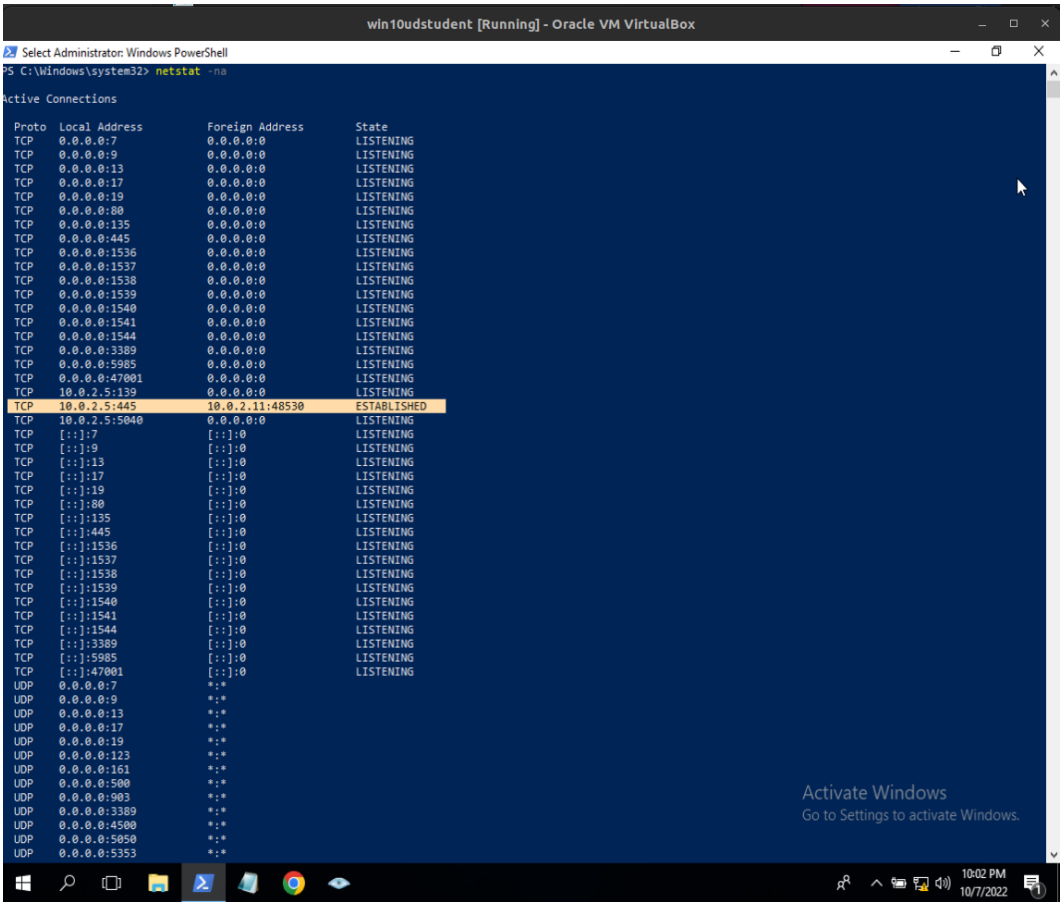
- **445 (files & print sharing - SMB after Windows 2000)**



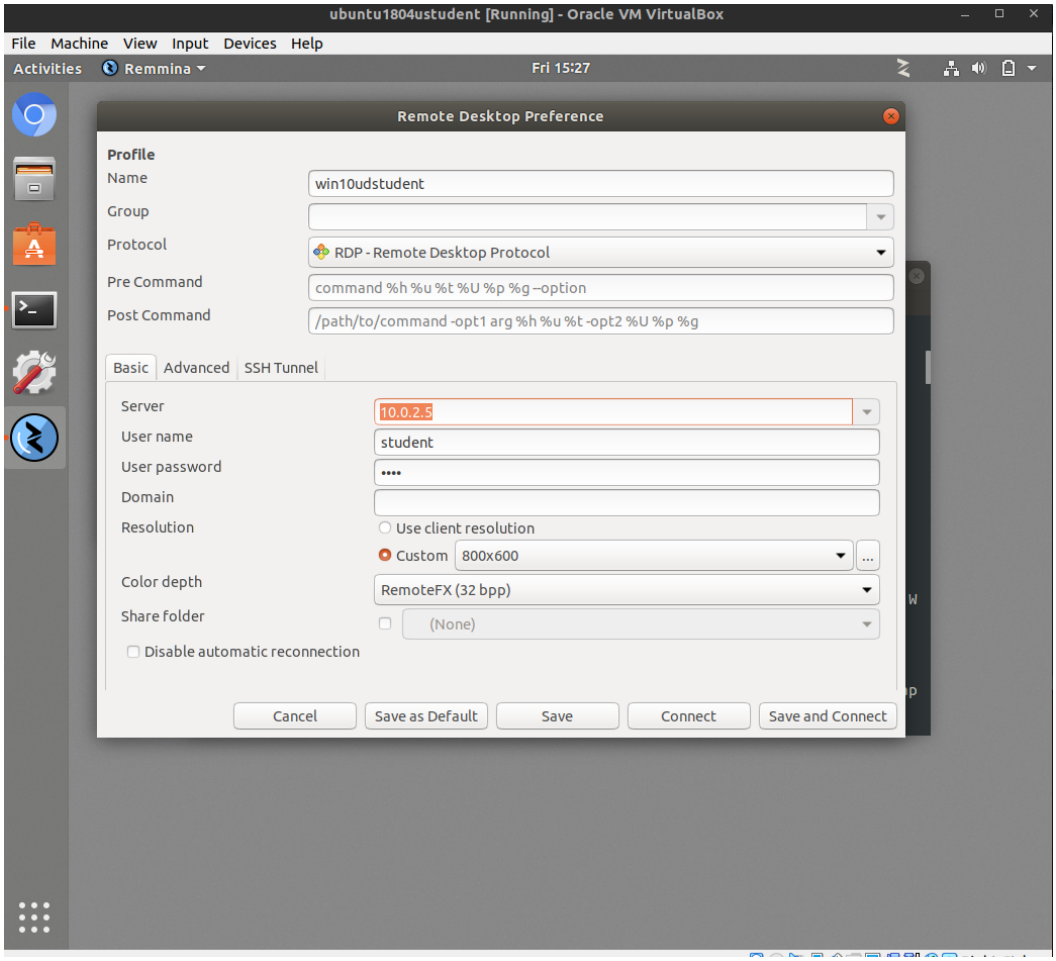
SMB Protocol (Server Message Block Protocol) is a client-server communication protocol used for sharing access to files, printers.

(following in the next page)


c on 10.0.2.5
Recent
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Trash
c on 10....
Other Locations
data
Documents and Settings
inetpub
PerfLogs
ProgramData
Program Files
Program Files (x86)
Recovery
$Recycle.Bin
System Volume Information
Users
Windows
$WINDOWS.~BT
$WinREAgent

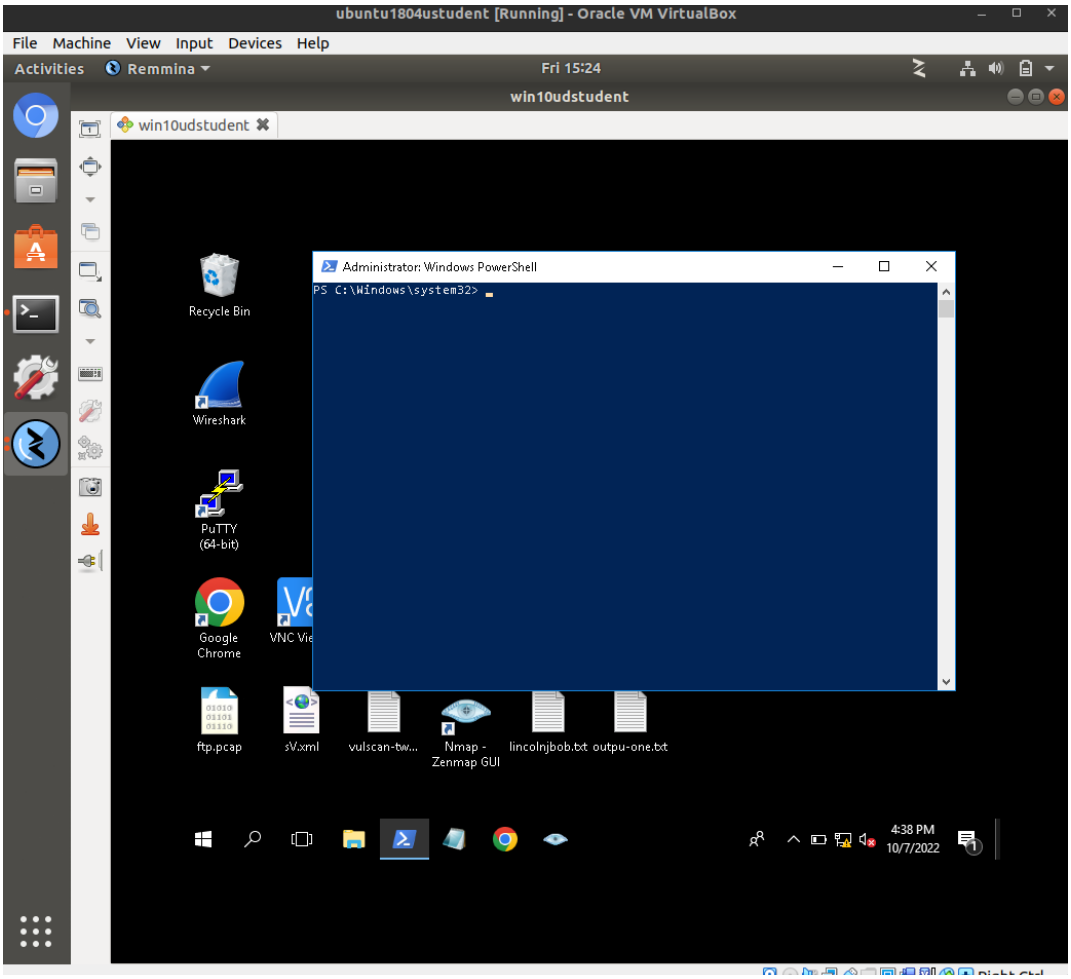

win10udstudent [Running] - Oracle VM VirtualBox
Select Administrator: Windows PowerShell
PS C:\Windows\system32> netstat -na
Active Connections
Proto Local Address Foreign Address State
TCP 0.0.0.0:7 0.0.0.0:0 LISTENING
TCP 0.0.0.0:9 0.0.0.0:0 LISTENING
TCP 0.0.0.0:13 0.0.0.0:0 LISTENING
TCP 0.0.0.0:17 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 [::]:445 [::]: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 0.0.0.0:500 *:*
UDP 0.0.0.0:903 *:*
UDP 0.0.0.0:3389 *:*
UDP 0.0.0.0:4500 *:*
UDP 0.0.0.0:5050 *:*
UDP 0.0.0.0:5353 *:*
Activate Windows
Go to Settings to activate Windows.
10:02 PM
10/7/2022

- **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.

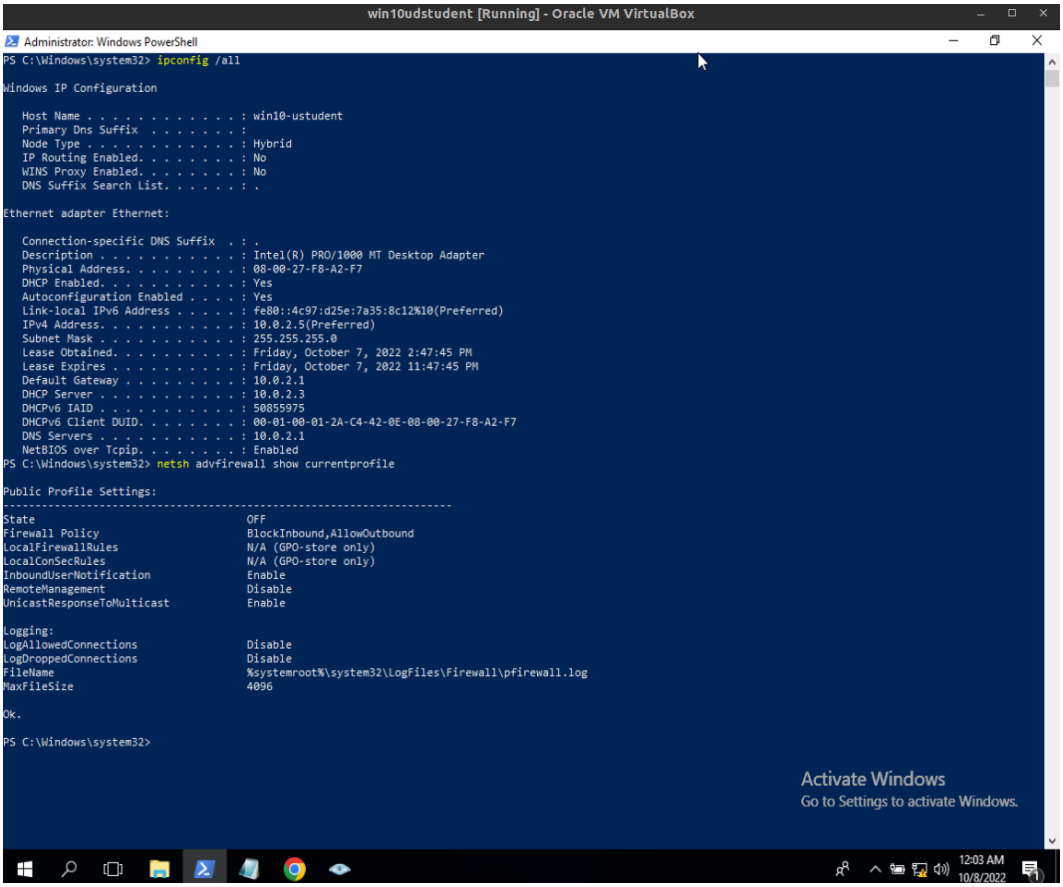
As seen before, since there is no security policies regarding inbound traffic that target those services, any connection that match a user & password access the system.

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.

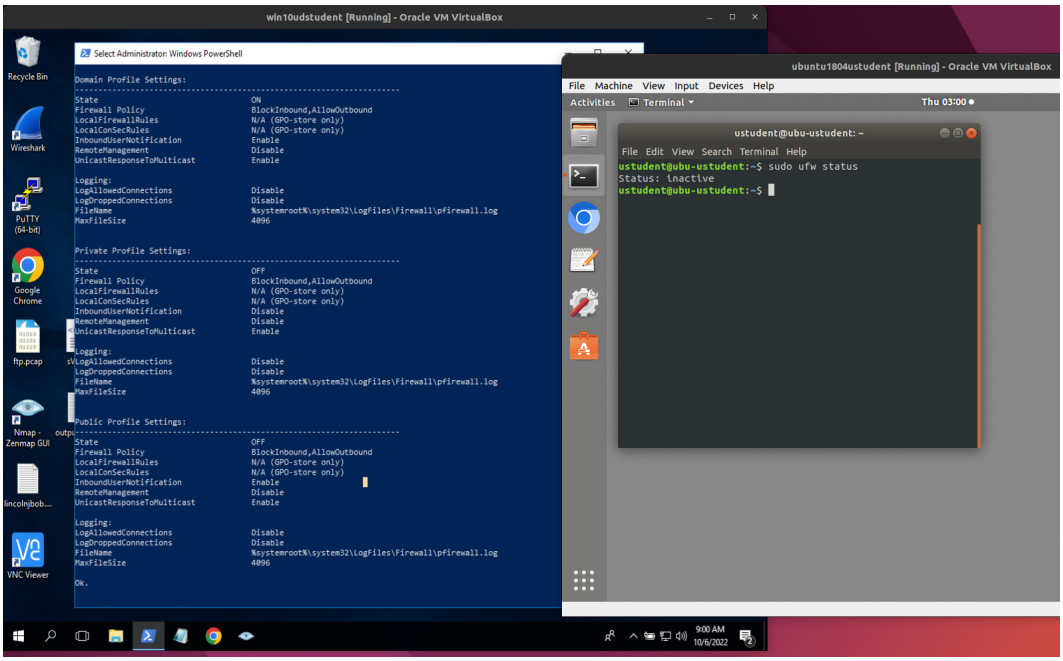
This services and protocols shares insecure characteristics that makes them vulnerable. Once the credentials are correctly provided, the connection is authenticated and authorized as system user. It's allowed to access to all the information as group member, execute allowed commands for the group.

- **IPv6**



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



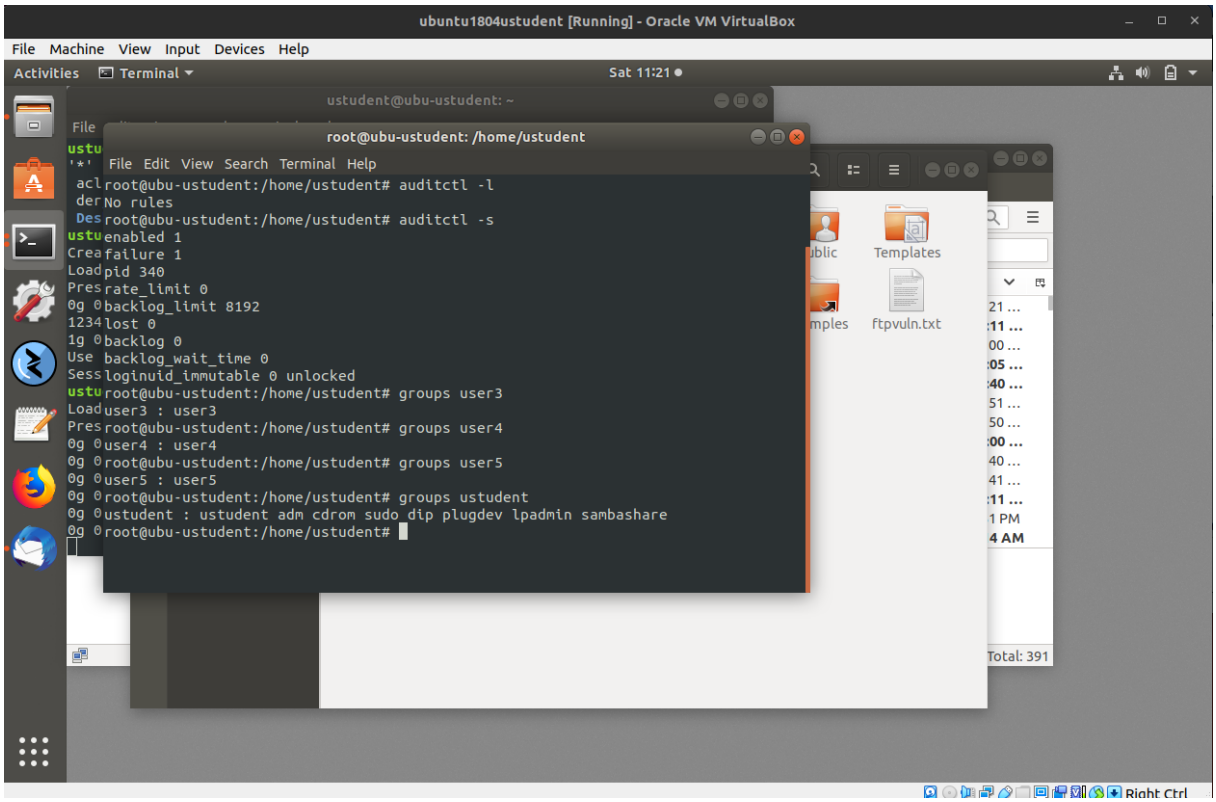
Windows / Ubuntu

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**

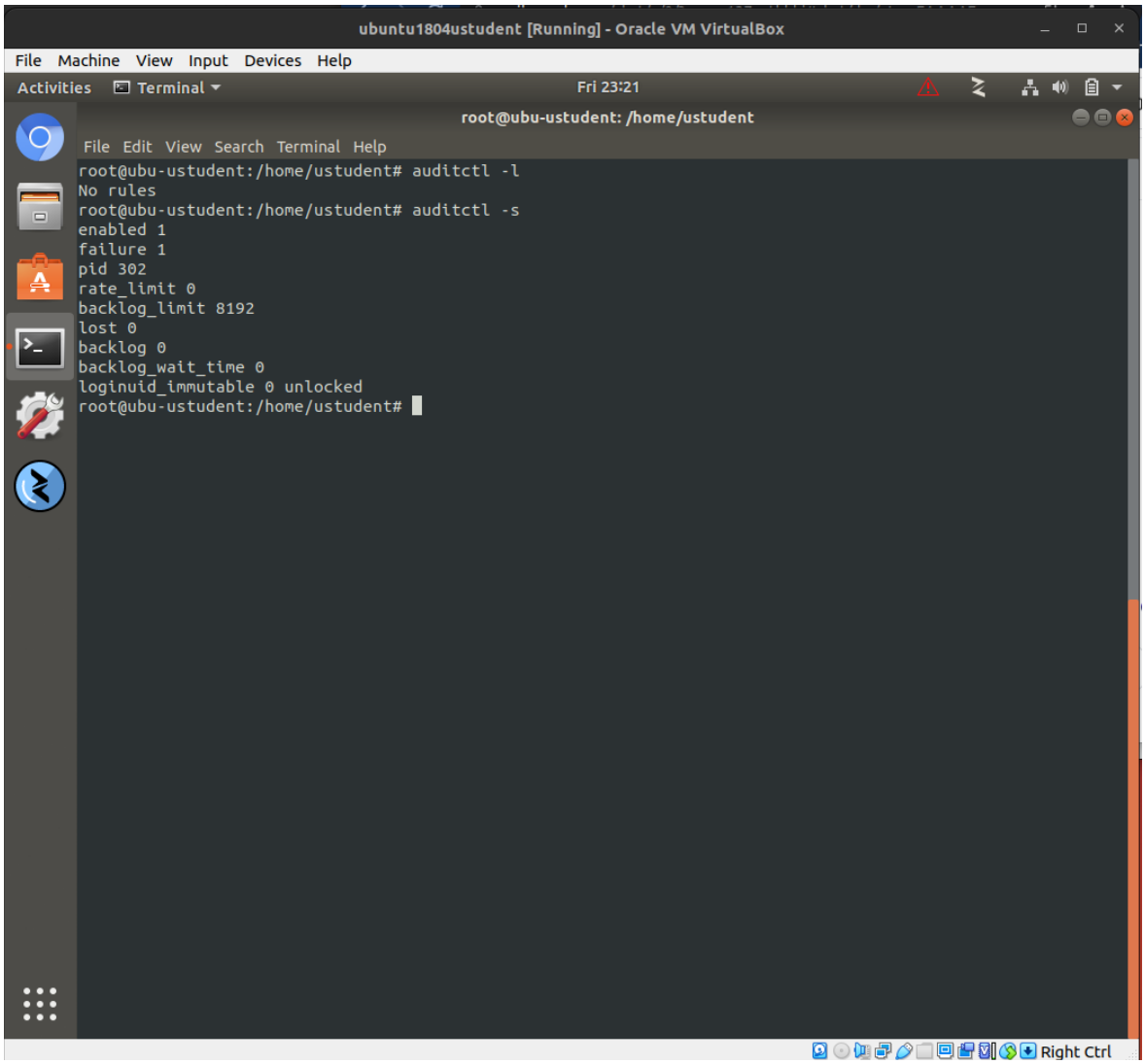
1. Which users have high privileges? ustudent



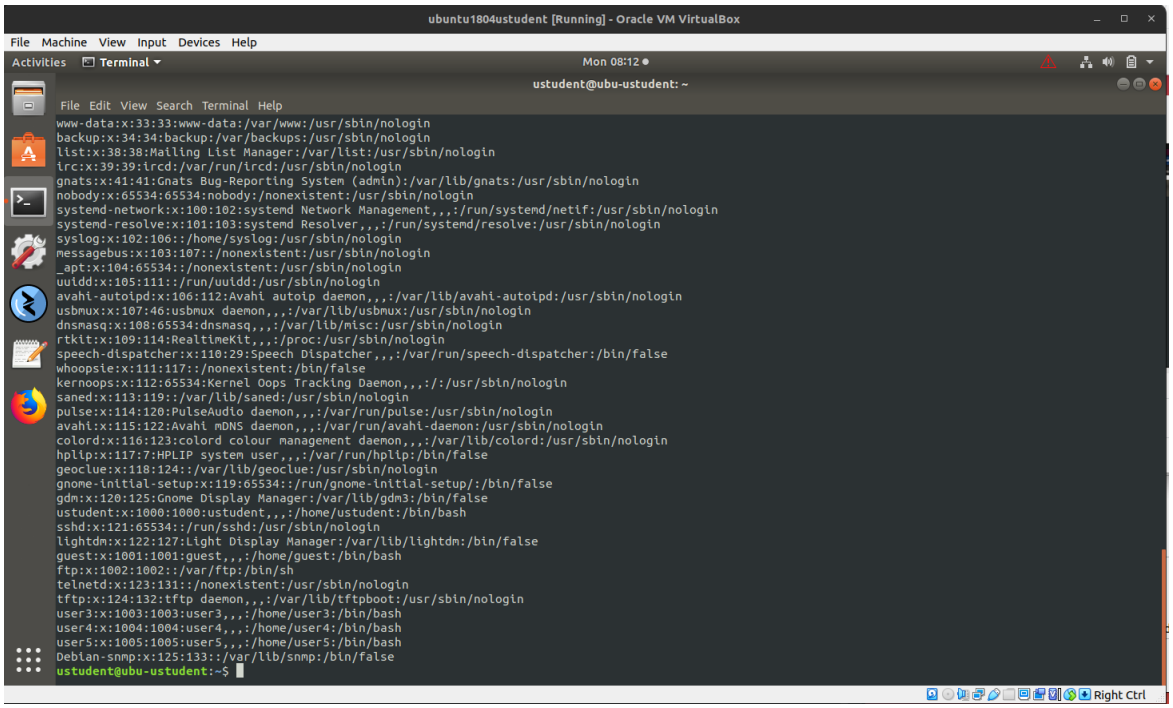
"ustudent" belongs to sudo group (between others) which allow it to use sudo commands and execute high level operations.
Numbered users and guest user belongs to their own groups without been related to sudo group or command.

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.

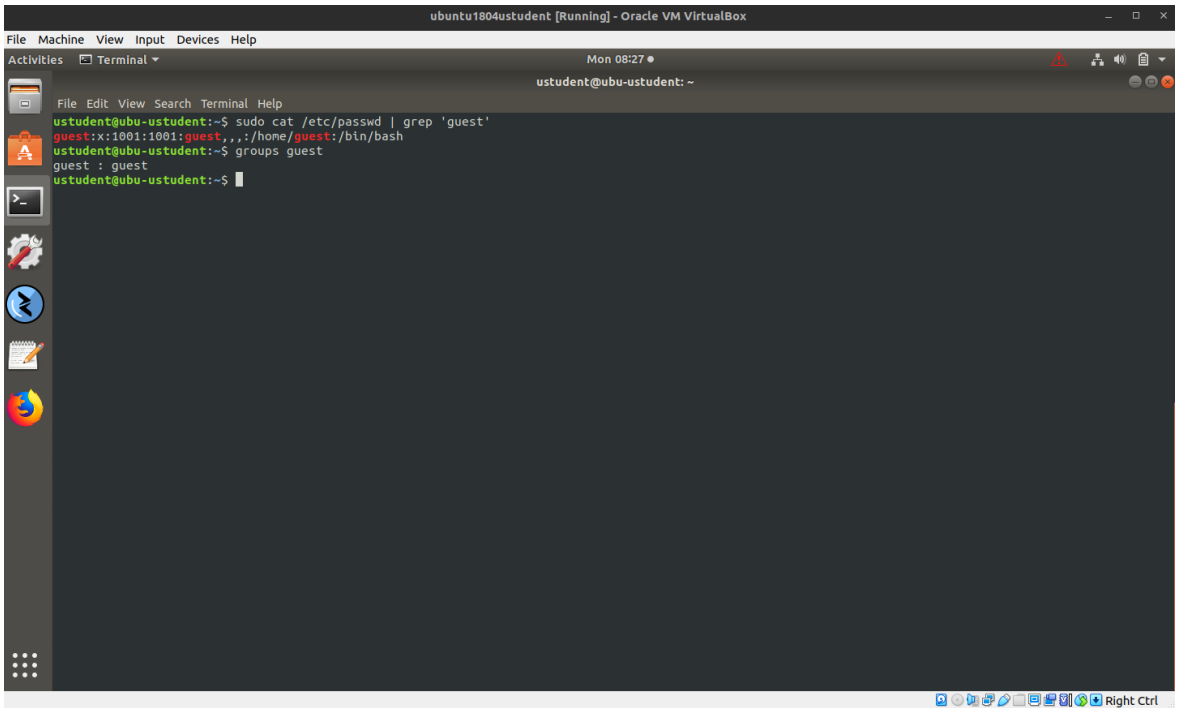


3. Are the default settings correct, and are there any excessive permissions? Permissions for numbered users (as user3, etc...) and "guest" are barely defined, they can access system folders and prompt out system files. They does not have permissions to modify or install programs in the system. Each 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.



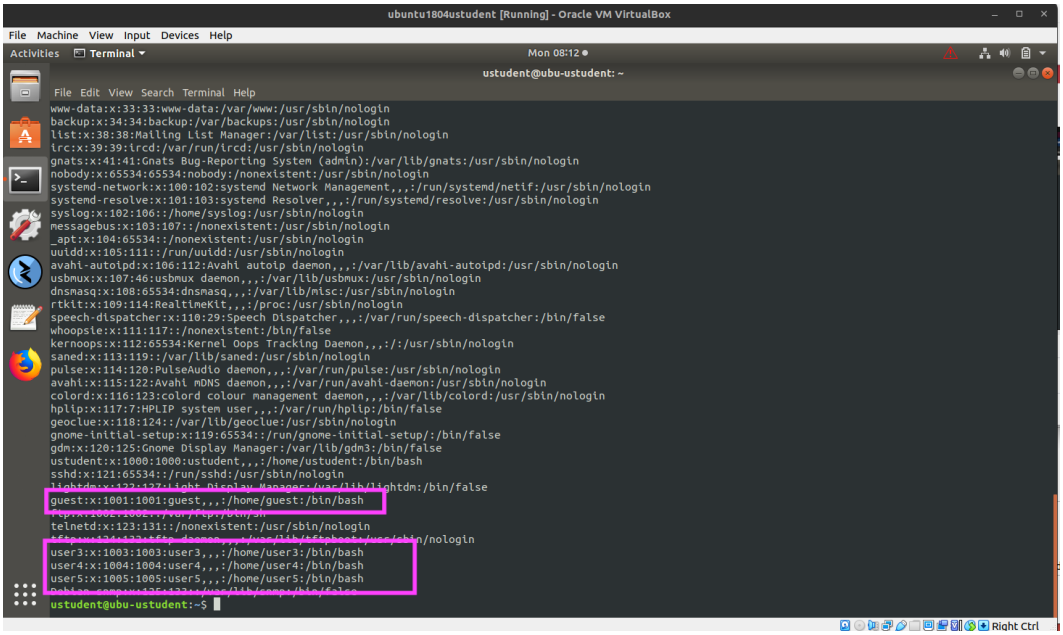
As it's shown in the image above, the absolute path of their shell (/bin/bash) is the system shell there is no replacement shell for the user accounts. The shell environment lacks of restrictions which increases the vulnerability of the system.

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 grat permissions according to this. If it's needed according to their needs, more users and groups could be created following that basic criteria.

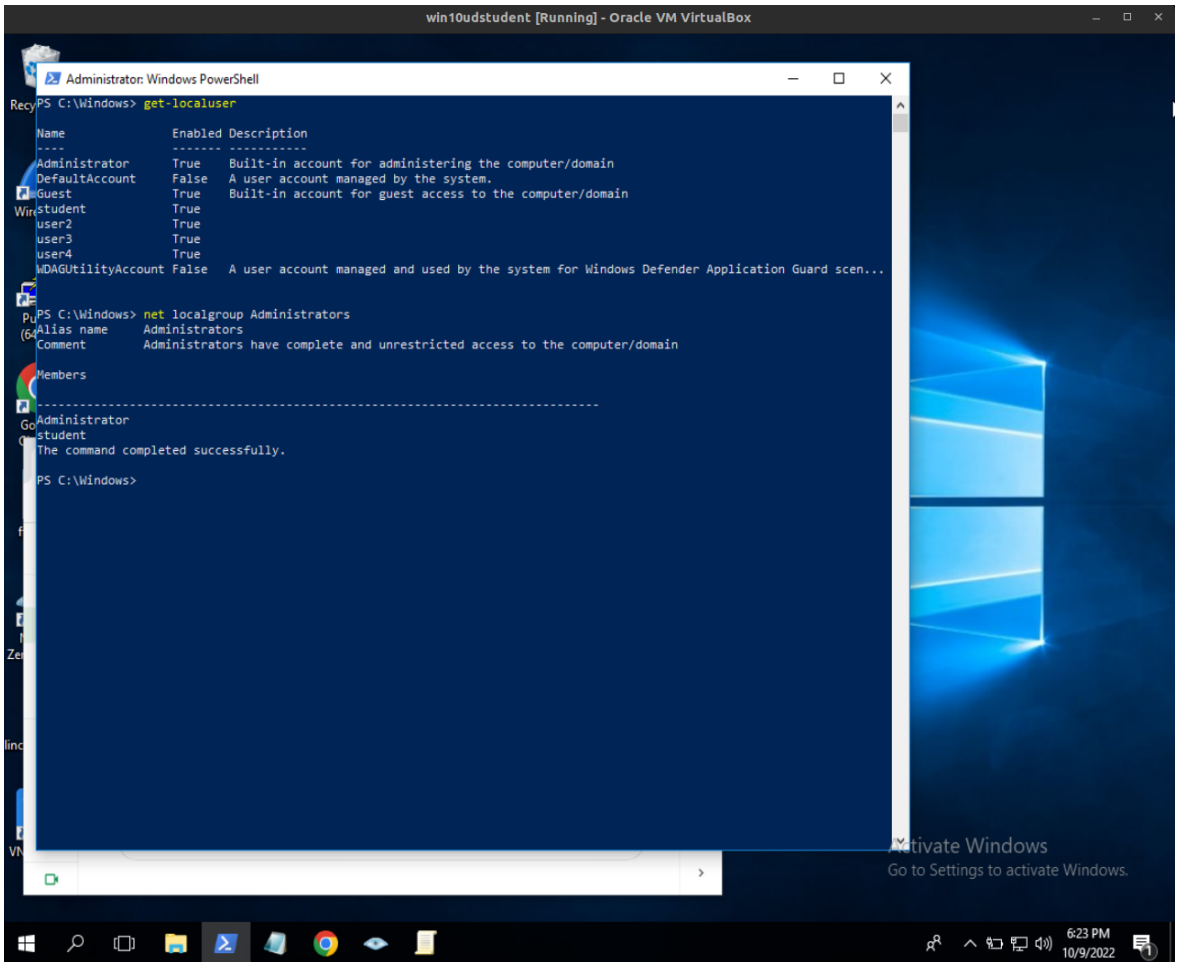


It's possible to see how the "numbered users" are replicated, there is no specifications that differentiates one from the other more than the name choosen for them. From that perspective, a deeper detailed requirements for the assignation of users identity should be done in order to avoid insecure access.

2.4 Principles of Least Privilege

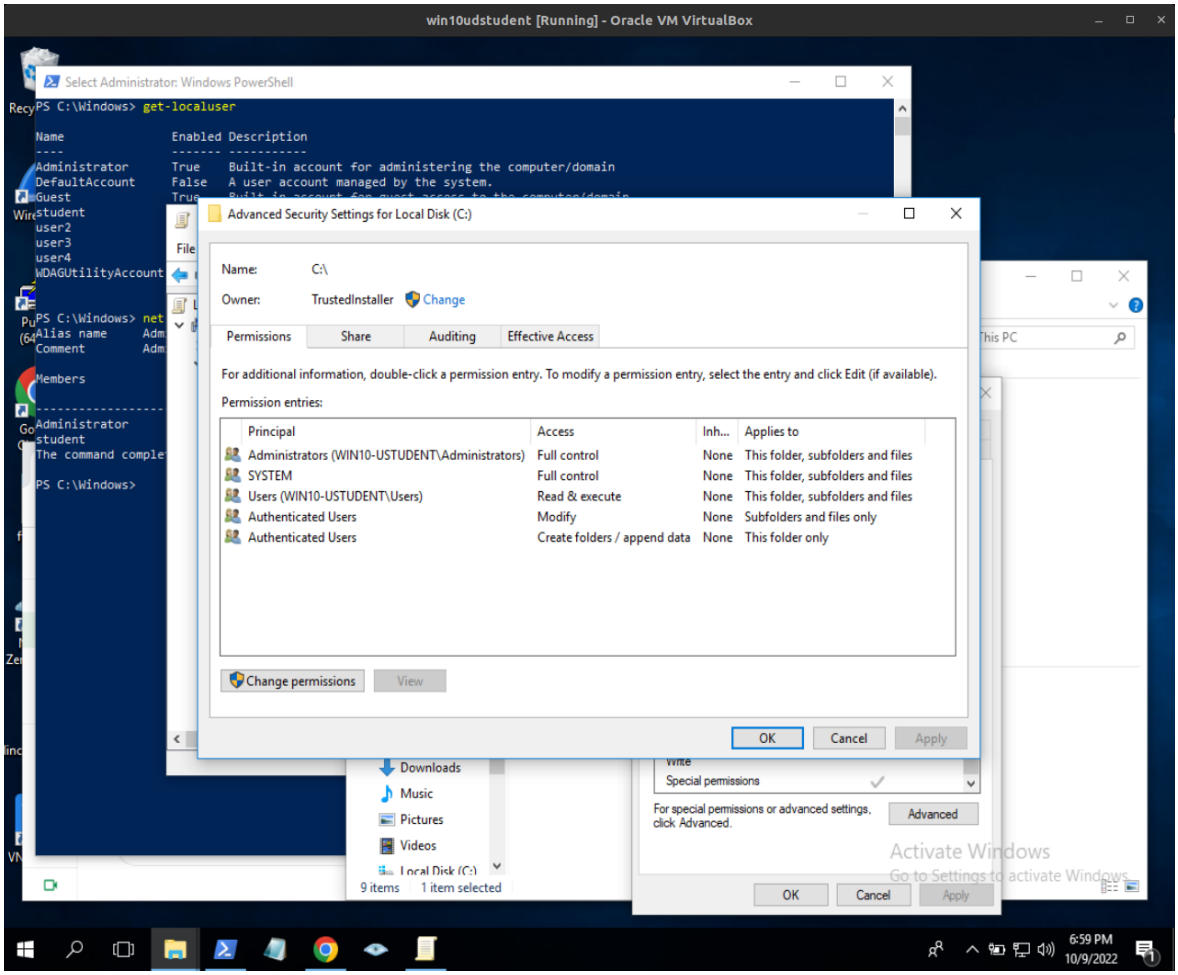
- **Windows**

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



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

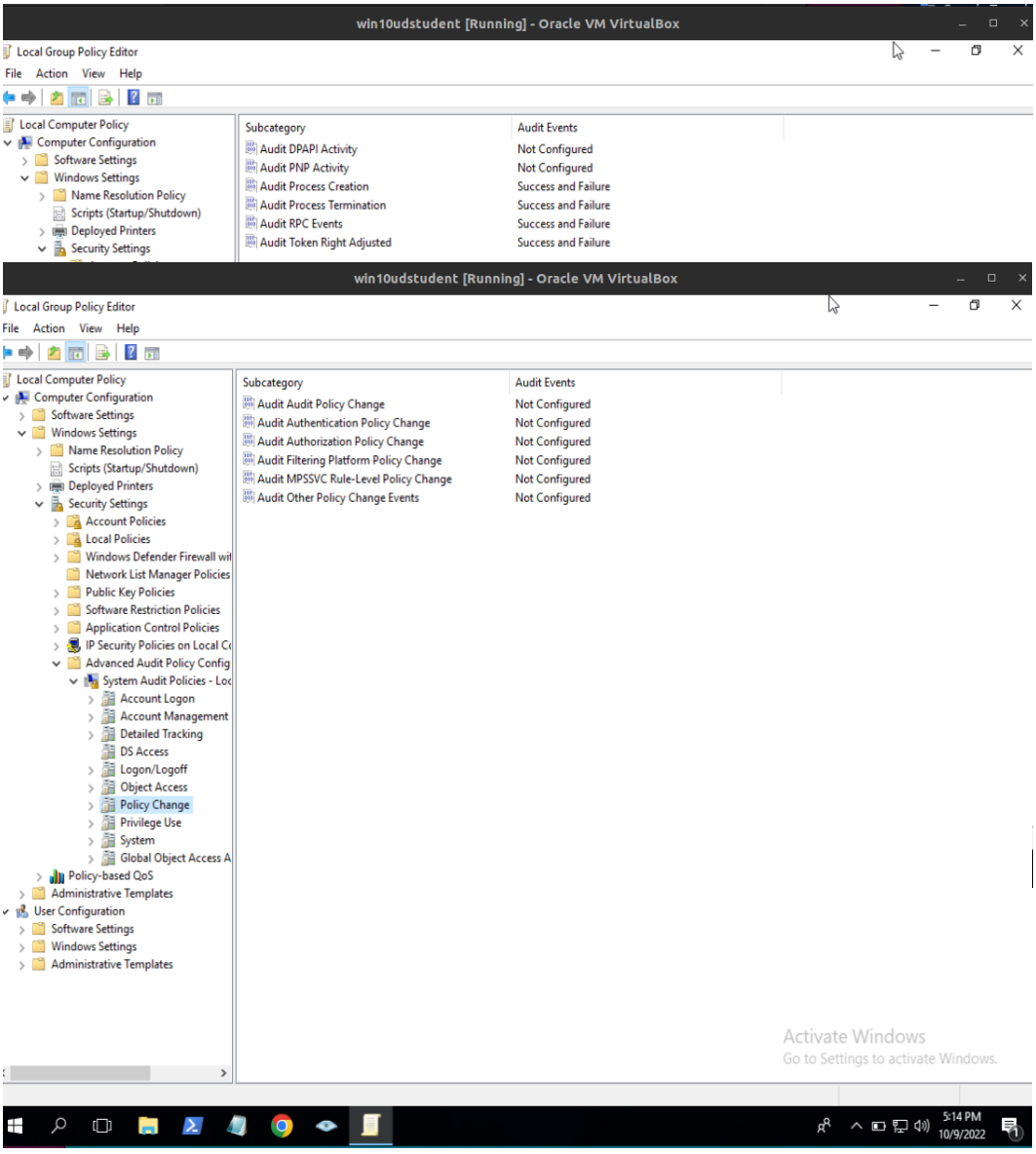
- Audit Account Lockout: Success, Failure

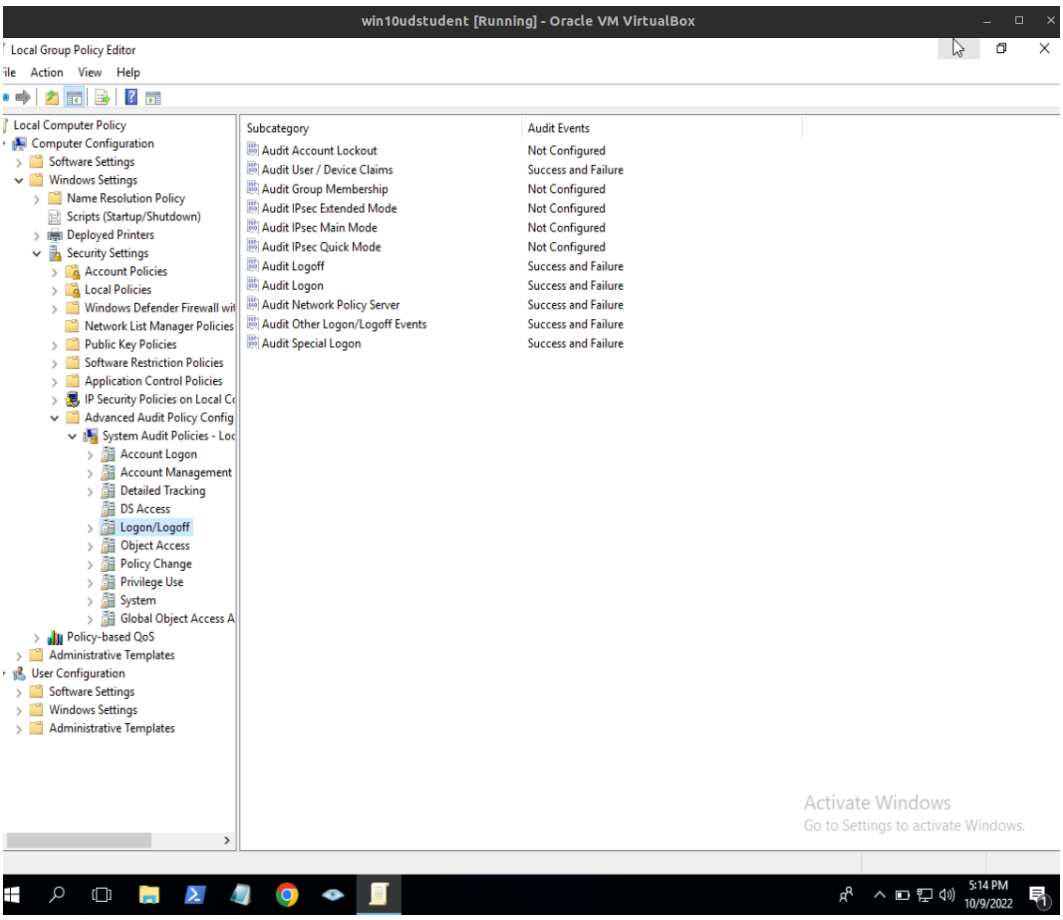
Policy Change

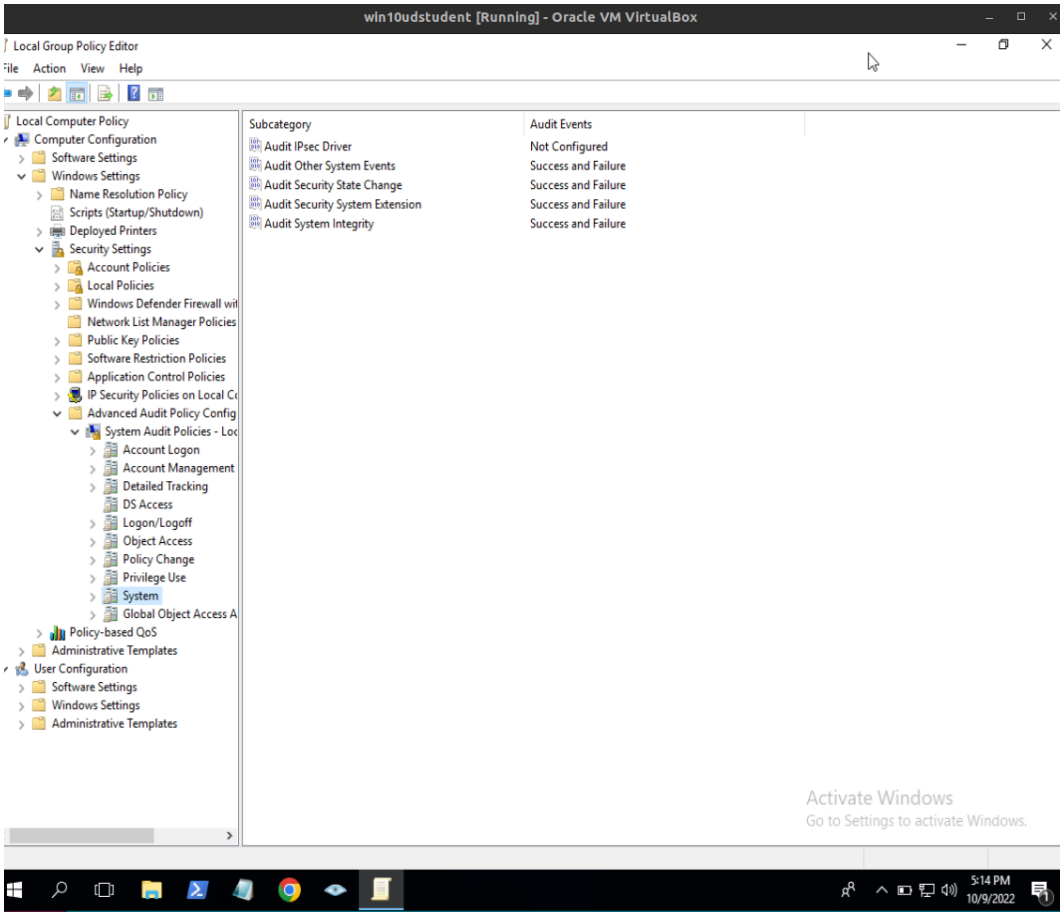
- Audit Policy Change: Success, Failure
- Audit Authentication Policy Change: Success, Failure
- Audit MPSSVC Rule-Level Policy Change: Success, Failure.

System

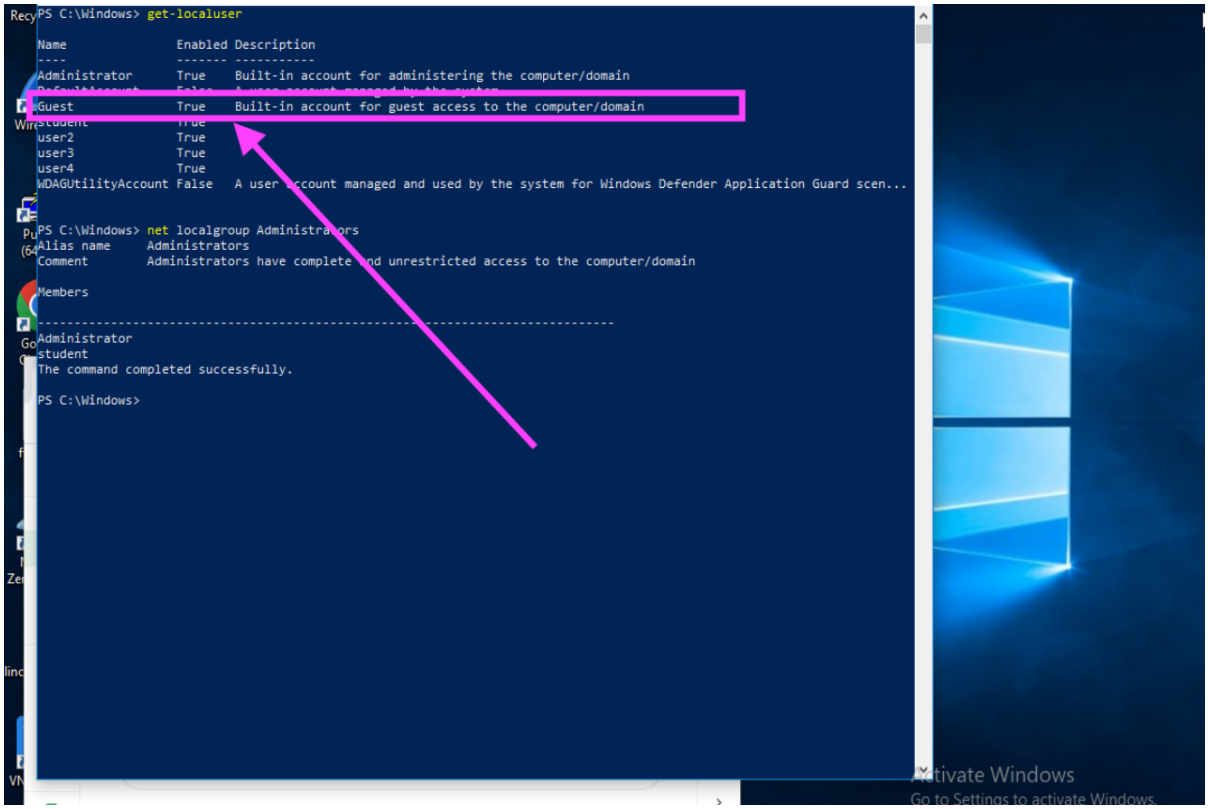
- Audit IPSec Driver: Success, Failure

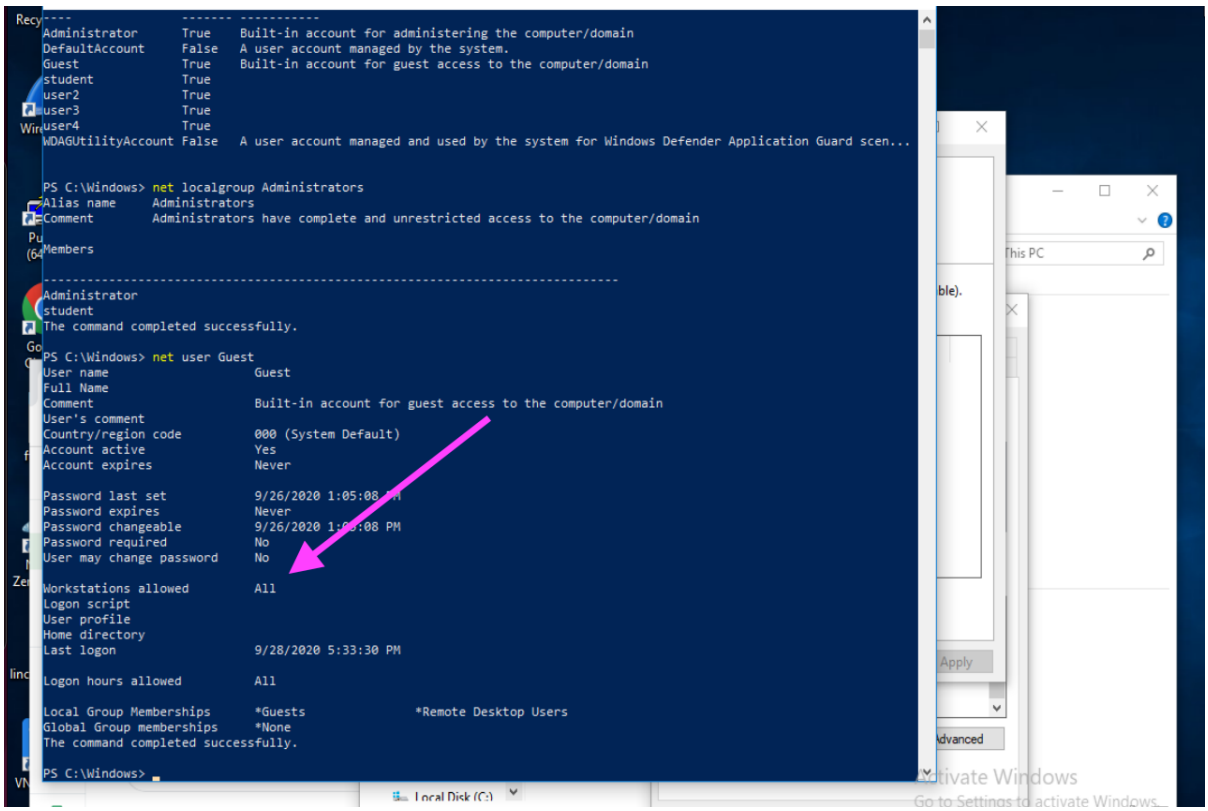



win10udstudent [Running] - Oracle VM VirtualBox
Local Group Policy Editor
File Action View Help
Local Computer Policy
Computer Configuration
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Windows Defender Firewall wit
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local C
Advanced Audit Policy Config
System Audit Policies - Loc
Account Logon
Account Management
Detailed Tracking
DS Access
Logon/Logoff
Object Access
Policy Change
Privilege Use
System
Global Object Access A
Policy-based QoS
Administrative Templates
User Configuration
Software Settings
Windows Settings
Administrative Templates
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


win10udstudent [Running] - Oracle VM VirtualBox
Local Group Policy Editor
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 wit
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local C
Advanced Audit Policy Config
System Audit Policies - Loc
Account Logon
Account Management
Detailed Tracking
DS Access
Logon/Logoff
Object Access
Policy Change
Privilege Use
System
Global Object Access A
Policy-based QoS
Administrative Templates
User Configuration
Software Settings
Windows Settings
Administrative Templates
Subcategory
Audit Events
Audit IPsec Driver
Not Configured
Audit Other System Events
Success and Failure
Audit Security State Change
Success and Failure
Audit Security System Extension
Success and Failure
Audit System Integrity
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





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

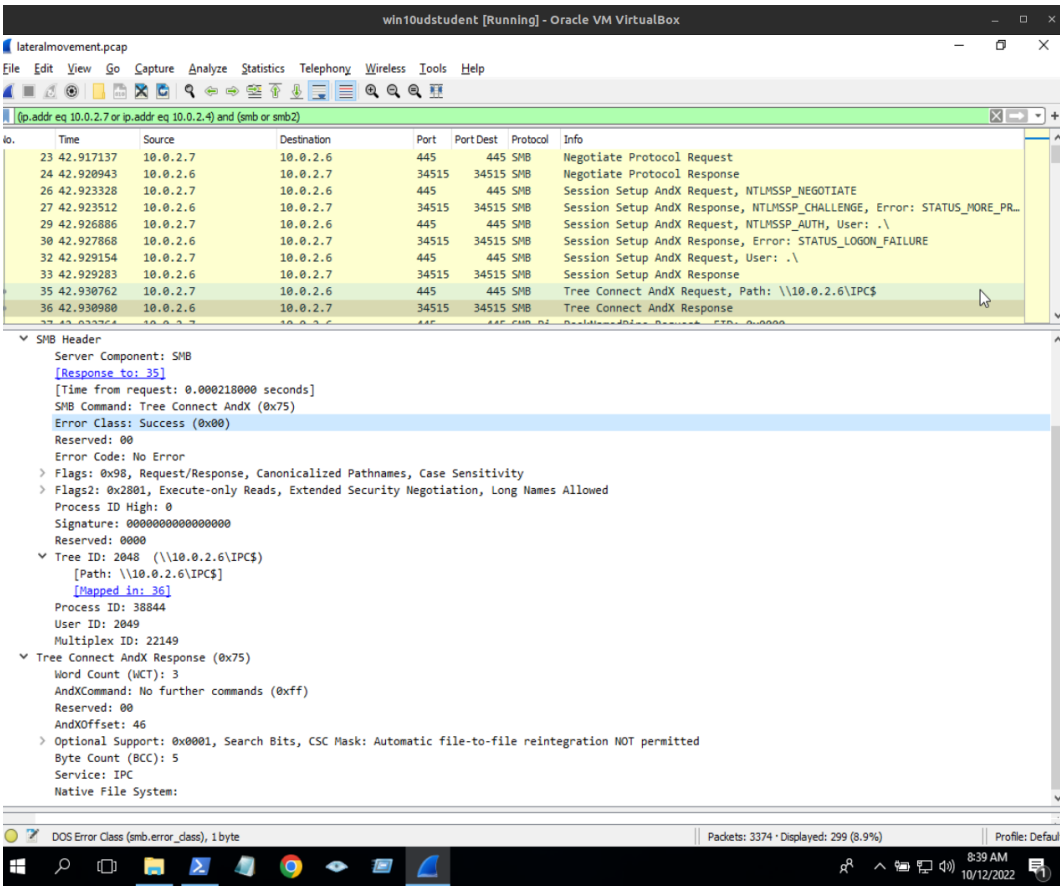
- **Windows**

3.1 Use the pcap file to assess and determine the following

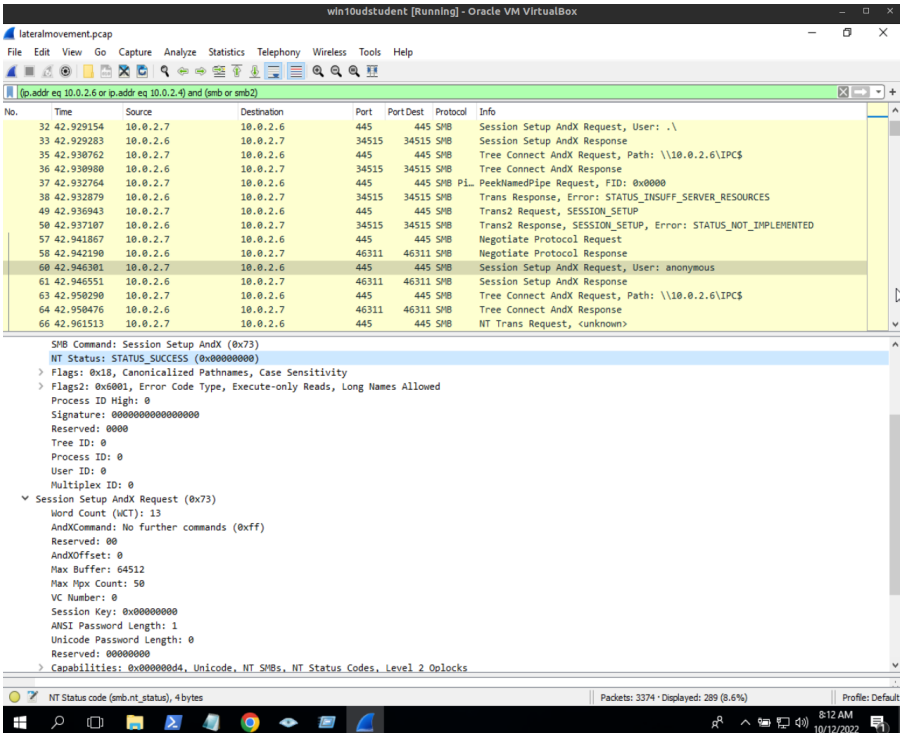
- **3.1.1** What type of attack was recorded?
- **3.1.2** What is the source IP of the attack?
- **3.1.3** What protocol was targeted?
- **3.1.4** What password was used successfully?
- **3.1.5** Which user was compromised?

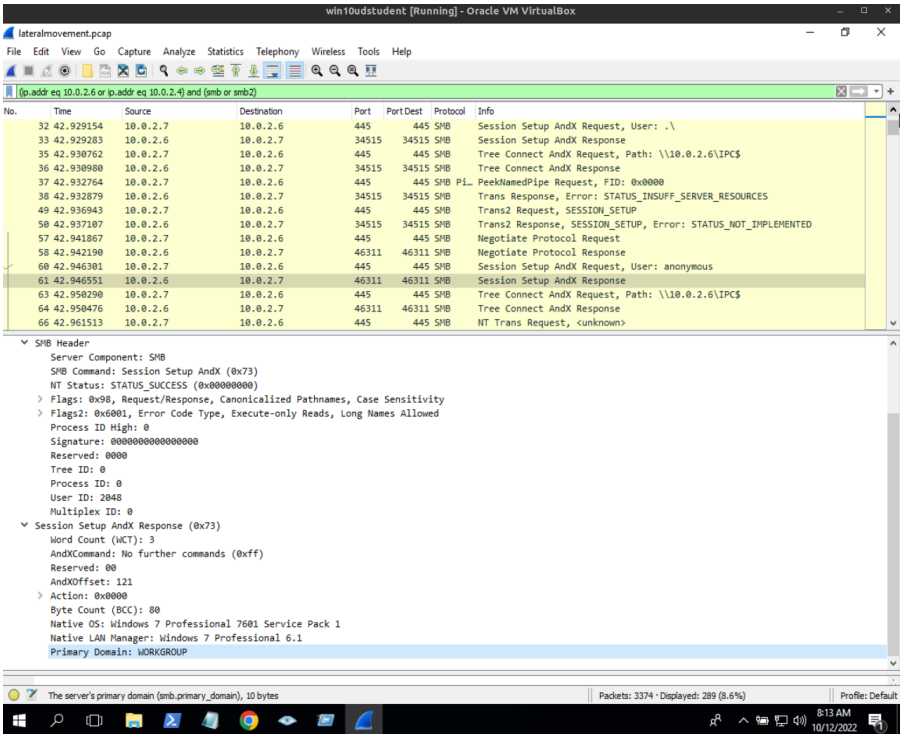
The attacker ip address is 10.0.2.7 the protocol targeted was SMB, the Server Message Block which allow to share files and printers in a network.

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.

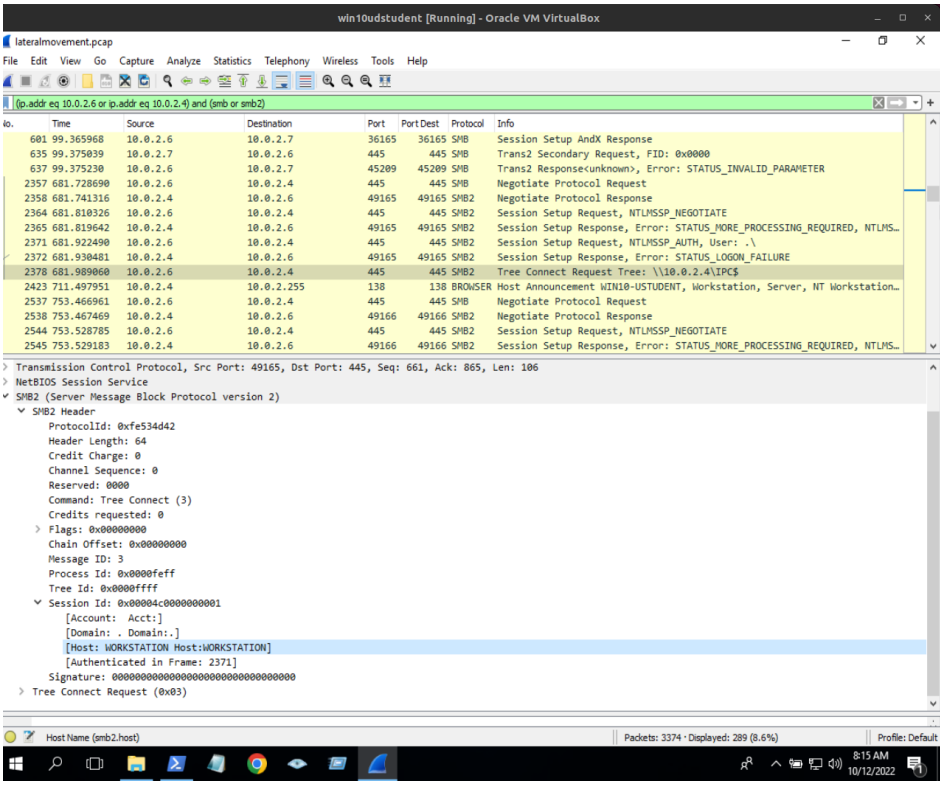


Using anonymous access the attacker is authenticated in the network without any password getting access to the Workgroup.

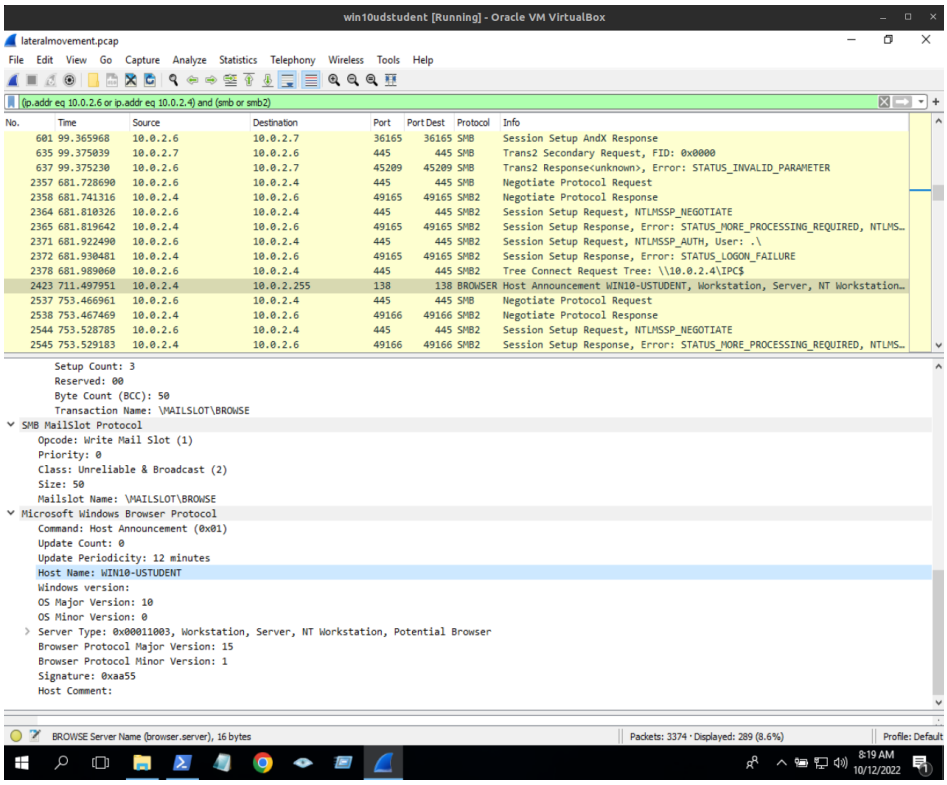




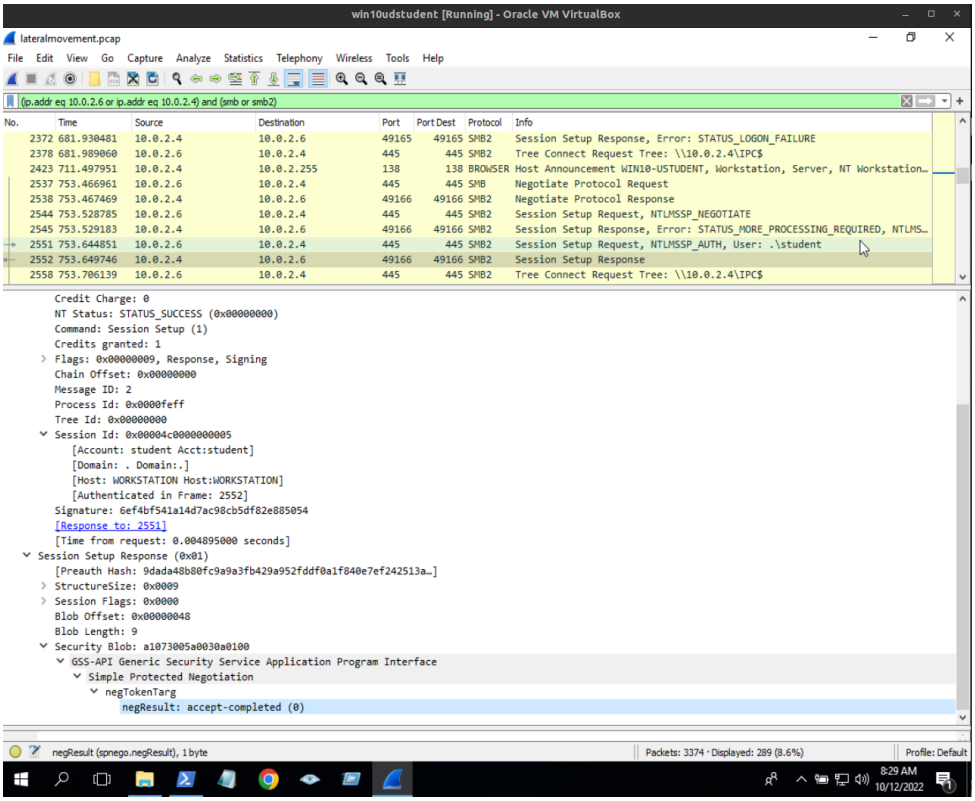
The final phase of the attack is about to gain access horizontally, moving from 10.0.2.6 to 10.0.2.4 using the same technique as an authenticated host.



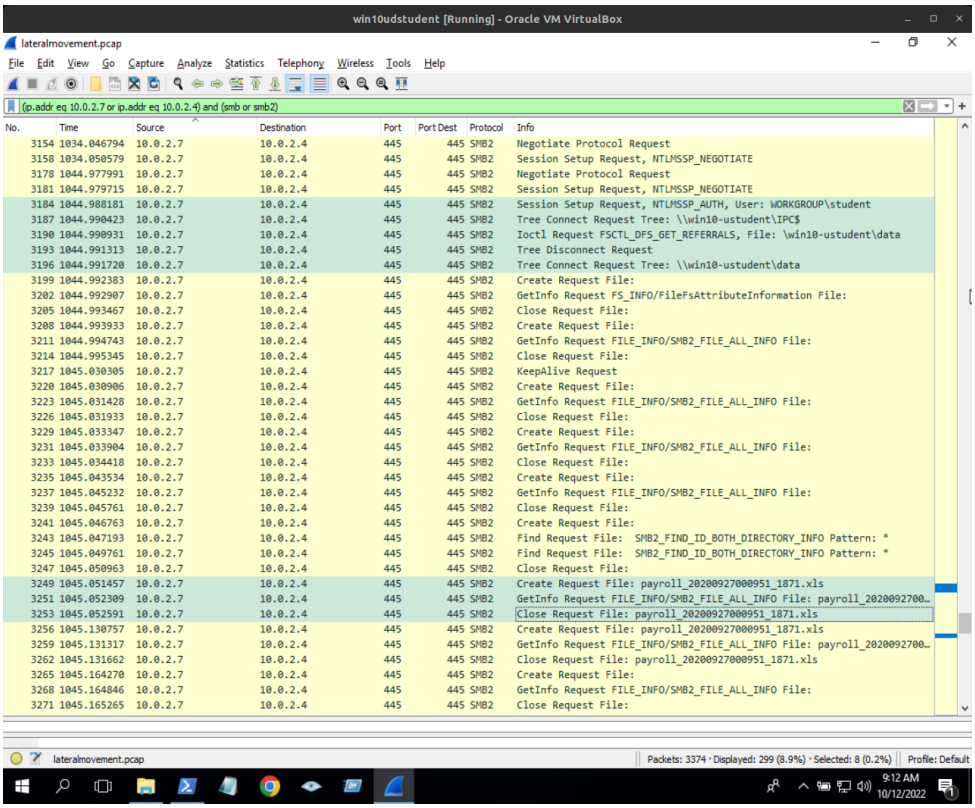
The attacker us the The BROWSER protocol which operates on top of SMB and is used to discover machines and resources on the network.



The "student" account is discovered and accessed.



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

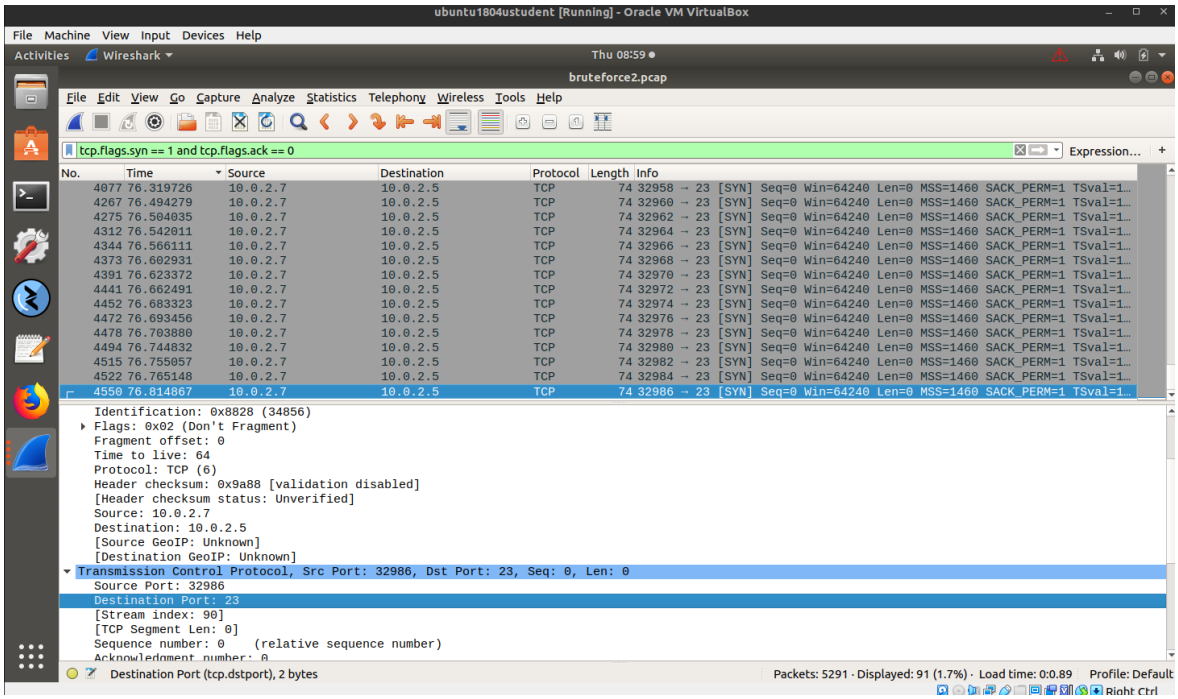


• **Ubuntu**

3.1 Use the pcap file to assess and determine the following

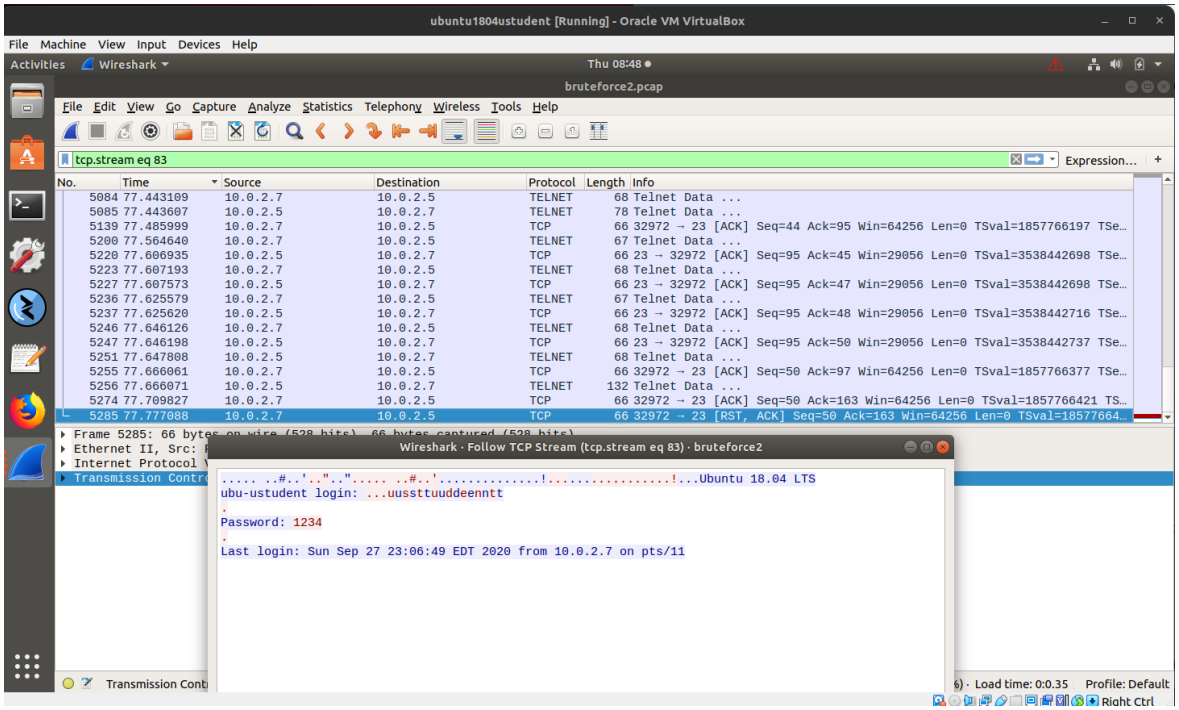
- **3.1.1** What type of attack was recorded?
- **3.1.2** What is the source IP of the attack?
- **3.1.3** What protocol was targeted?
- **3.1.4** What password was used successfully?
- **3.1.5** Which user was compromised?

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".



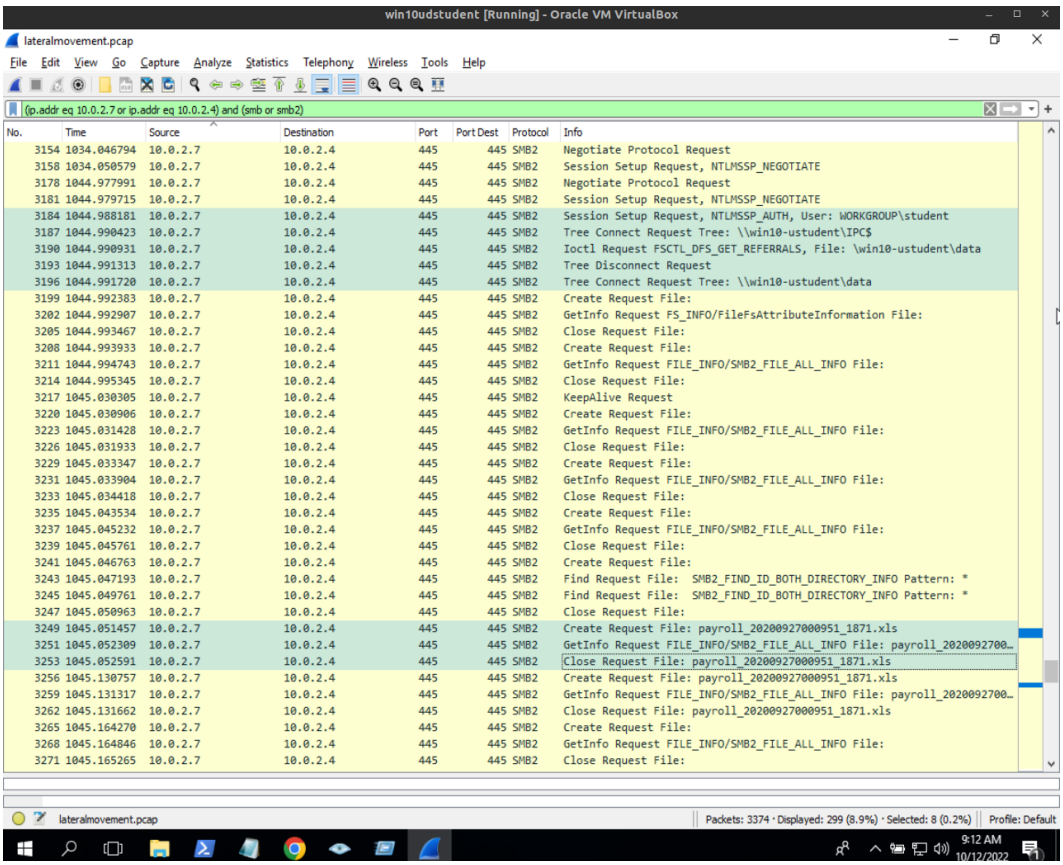
3.2 An internal user may have compromised another machine, use lateralmovement.pcap and determine the following:

- **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.

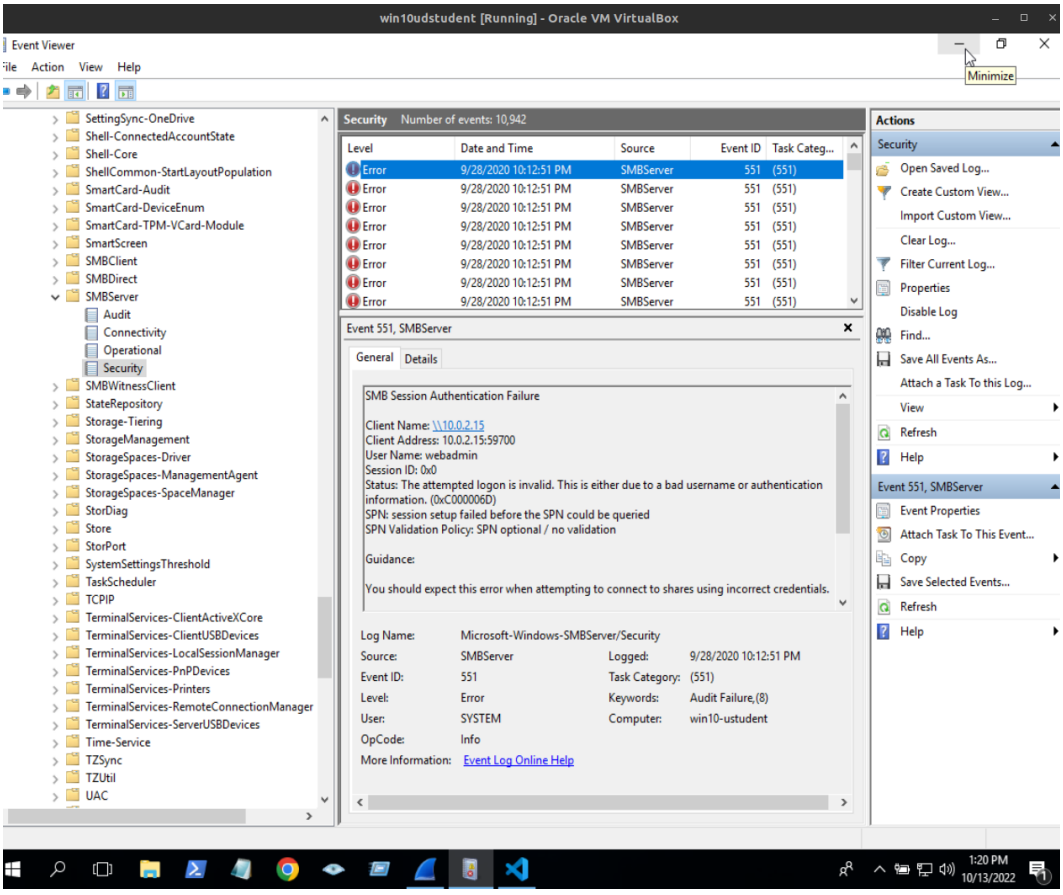


3.3 Using the logs, determine the following:

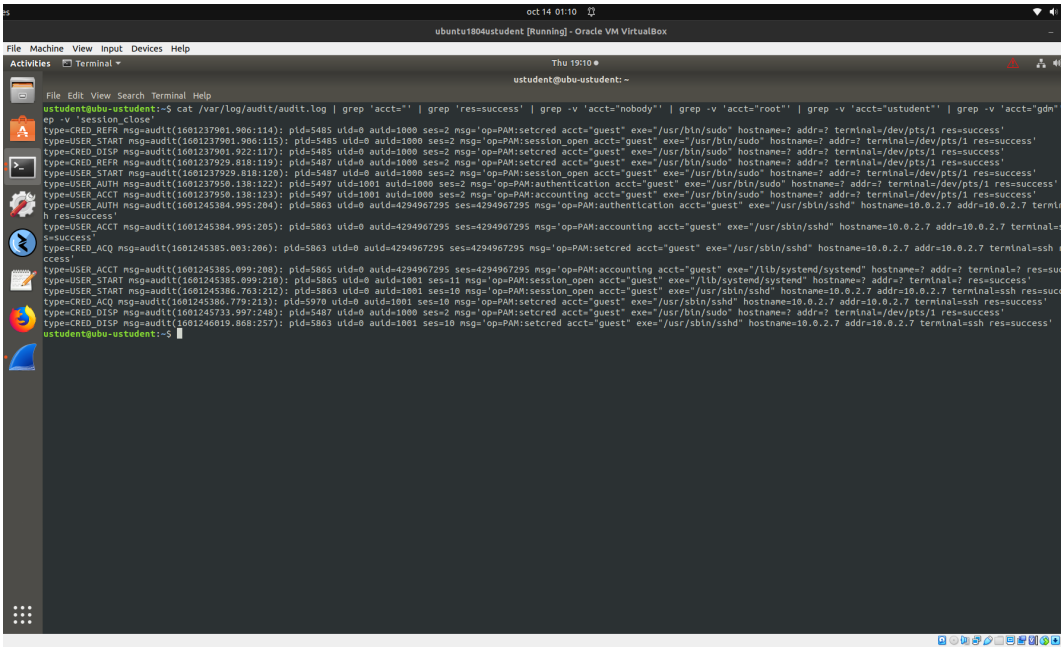
- **3.3.1** Are there any issues with Windows Share? Please provide screenshots of your findings.
- **3.3.2** Look at the audit logs setup at your Linux machine and find the audit.log file. What was the name of the attacker's account? Please provide screenshots.

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.

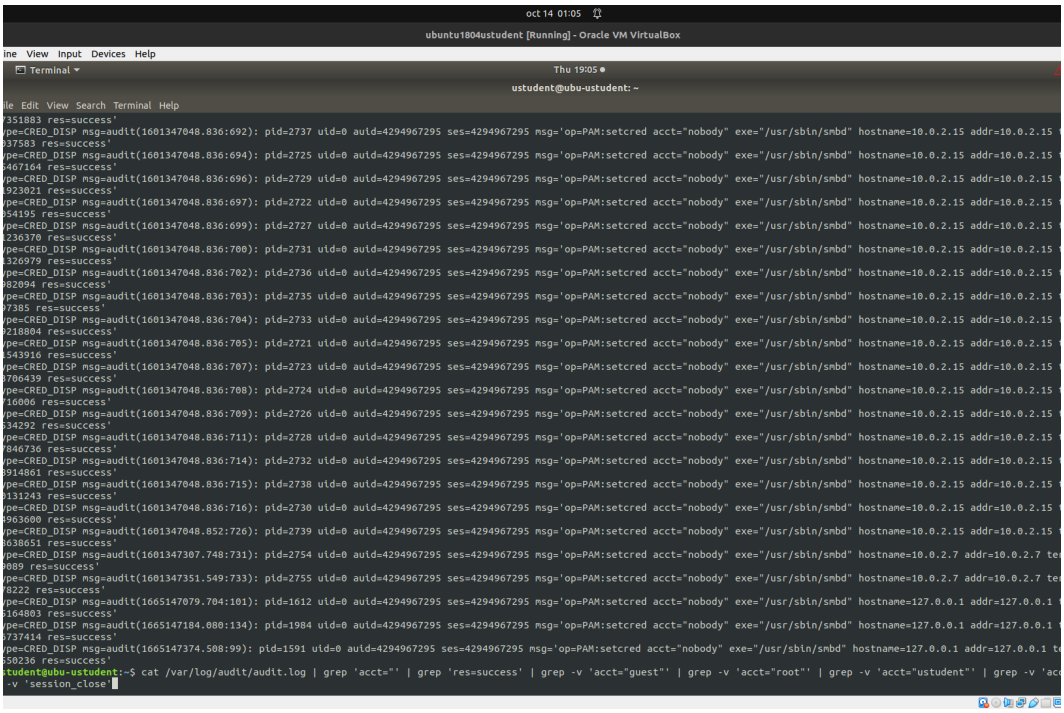
3.3.1 There is many issues in the log of the targeted share.



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".

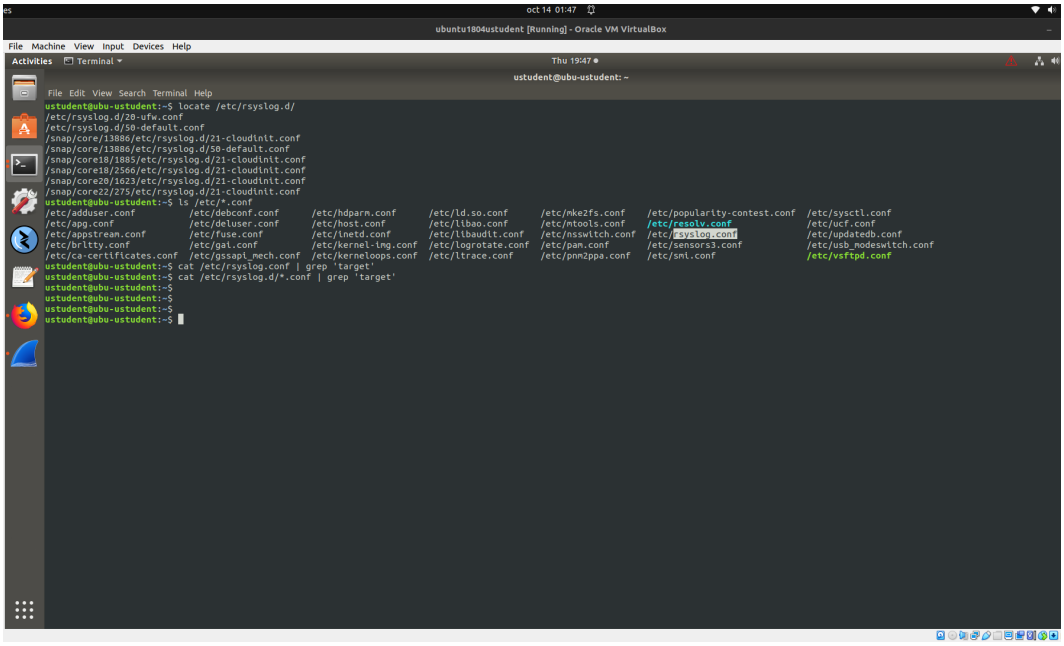


Based on these events, attacks using protocols for remote connections with default shares configurations and settings, all this evidence is enough to start an investigation.

3.4

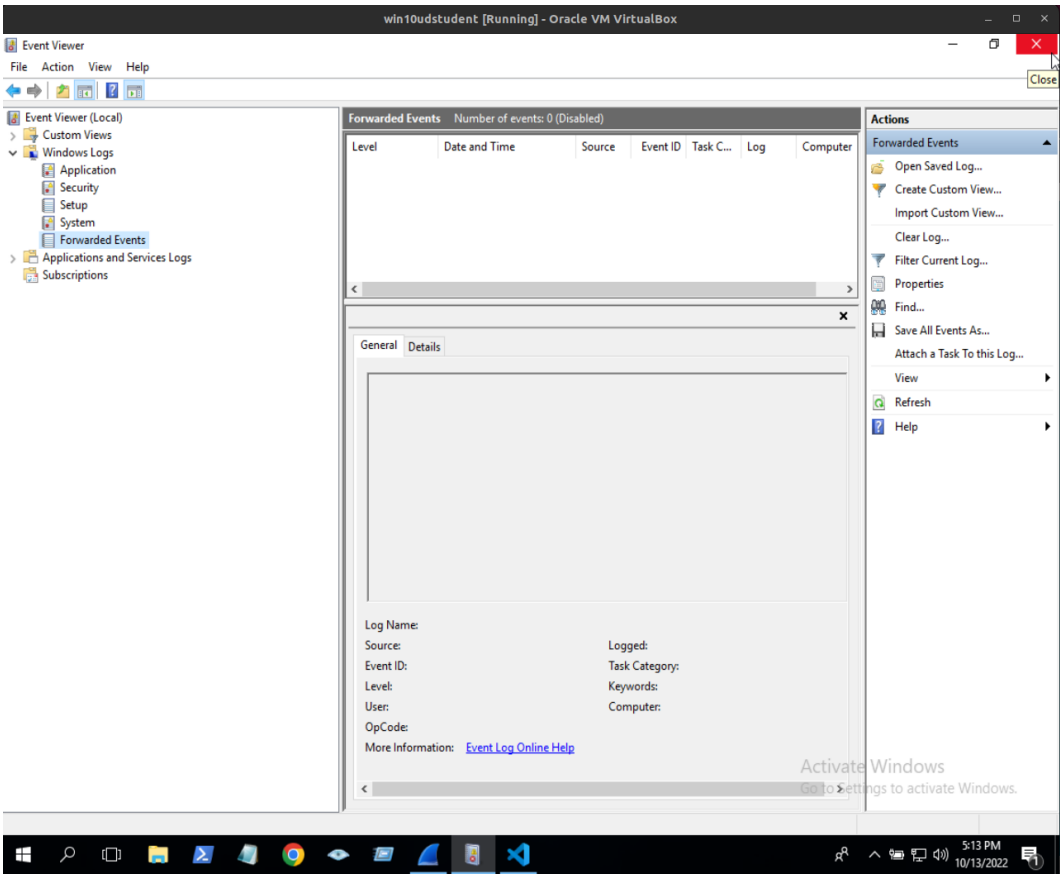
- **3.4.1** NuttyUtility has a centralized log infrastructure using a SIEM (Security Information and Event Management) product. You need to verify the machines you are checking from StaticSpeed have the settings enabled to use this.
- **3.4.2** Analyze StaticSpeeds systems and determine if these machines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



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 thre 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.



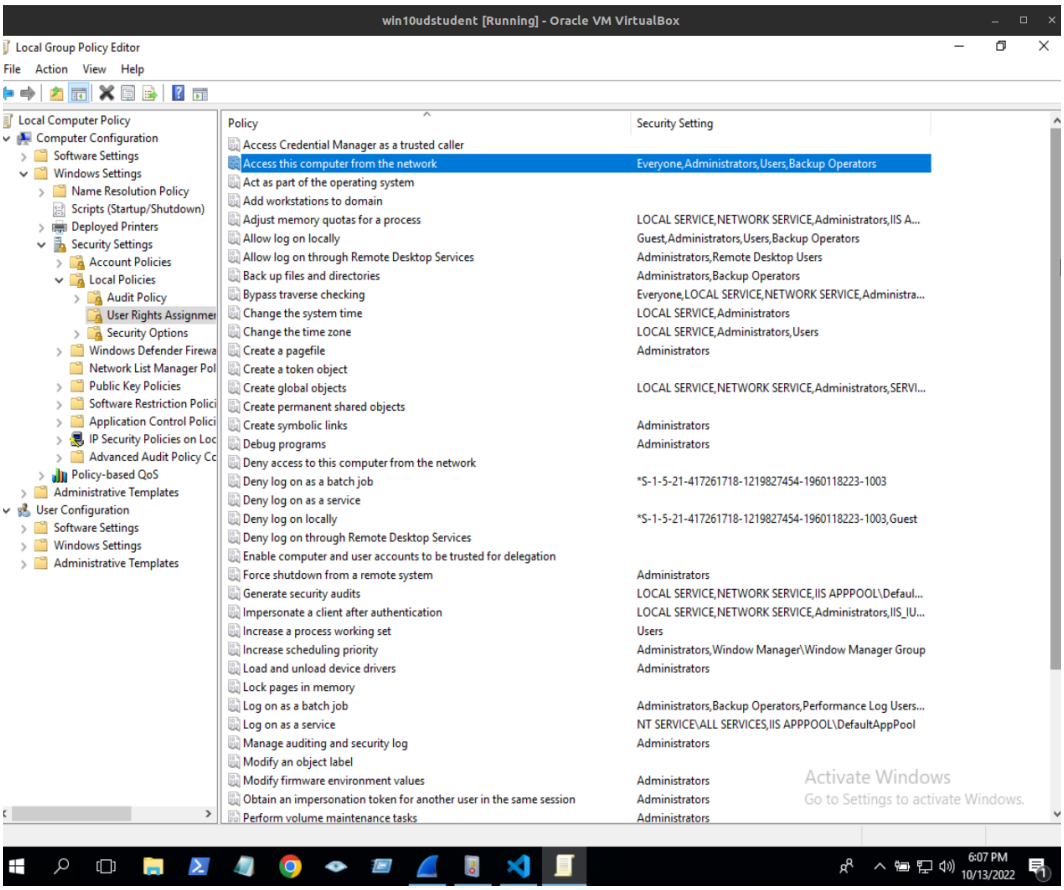
Based in this findings, the suggested course of action to ensure StaticSpeed meets the need of use a SIEM is configure Windows Event Forwarding and rsyslog to collect as many data as possible, this includes Perimeter device logs, Windows event logs, Application logs and Endpoint logs.

4: Assess Authentication Management at Targeted Assets

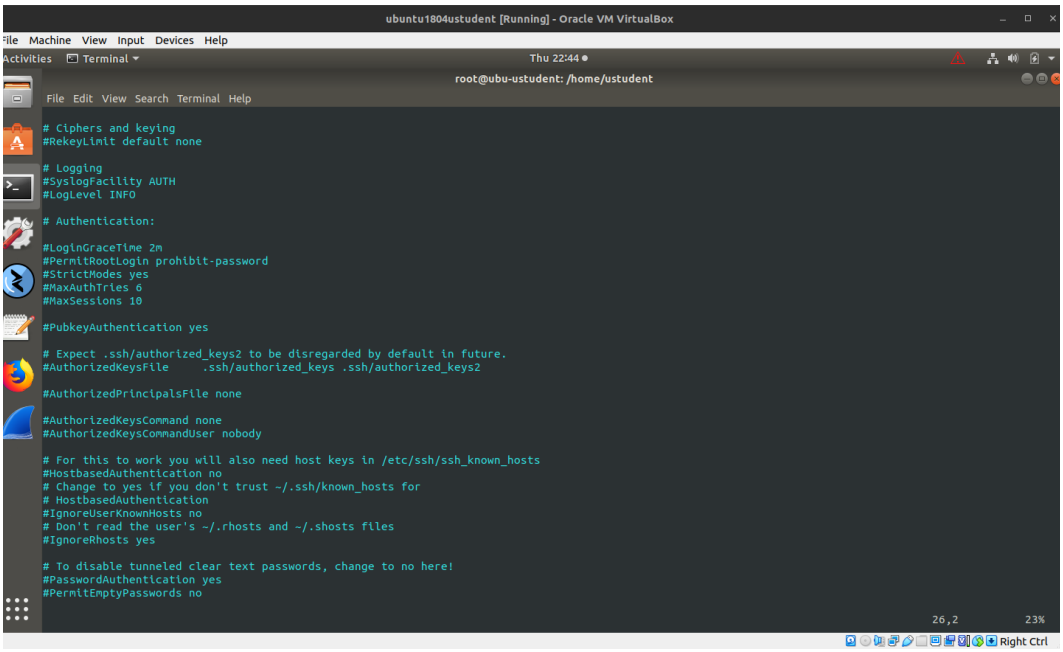
- **4.1.1** Ensure only administrators can remotely access windows machines and verify if root access is permitted at the Linux host.
- **4.1.2** Check for users with excessive permissions
- **4.1.3** Is root remote login allowed?
- **4.1.4** Are there users that should not have remote access via ssh 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?

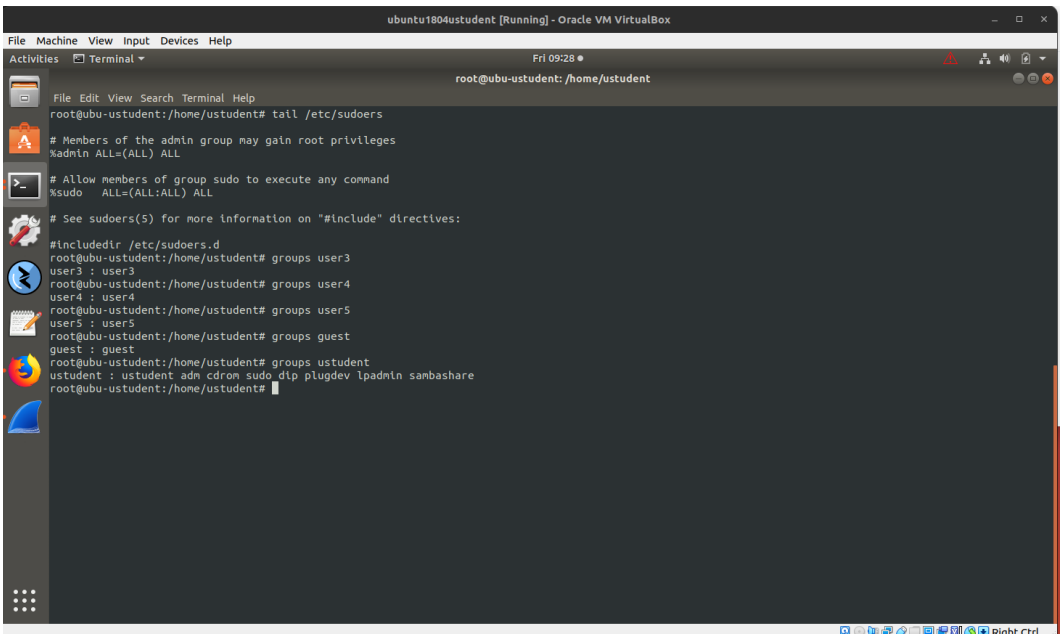
• **Windows**

- **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.



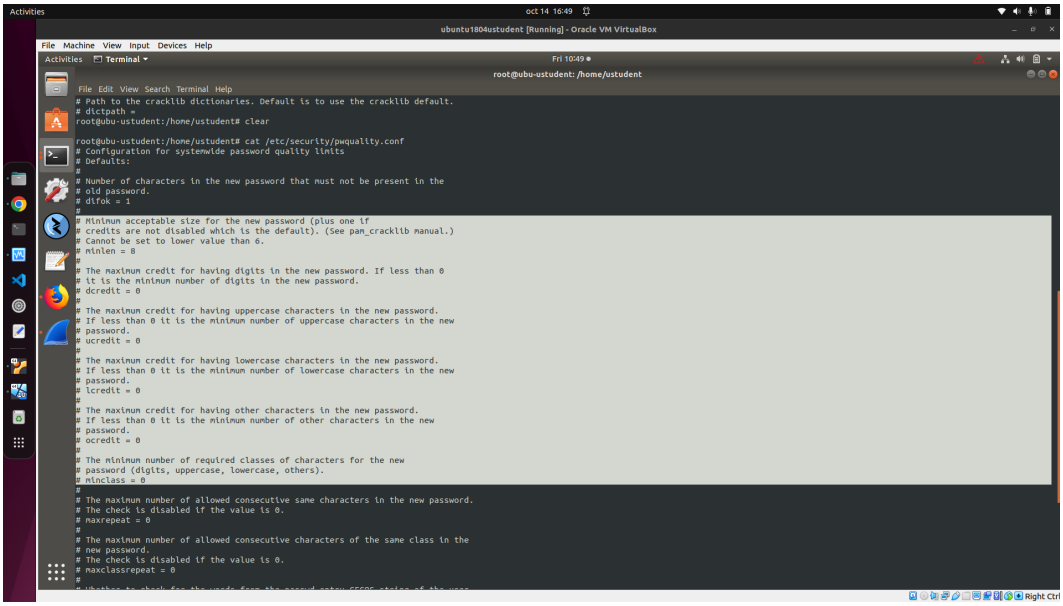
- **Ubuntu**
  - **1.** root access is not allowed at the Linux host.
  - **2.** Users has not excessive permissions since they are isolated into their own groups out of the scope of sudo command.
  - **3.** Remote root login is not enabled.
  - **4.** As There is no users restrictions set for access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

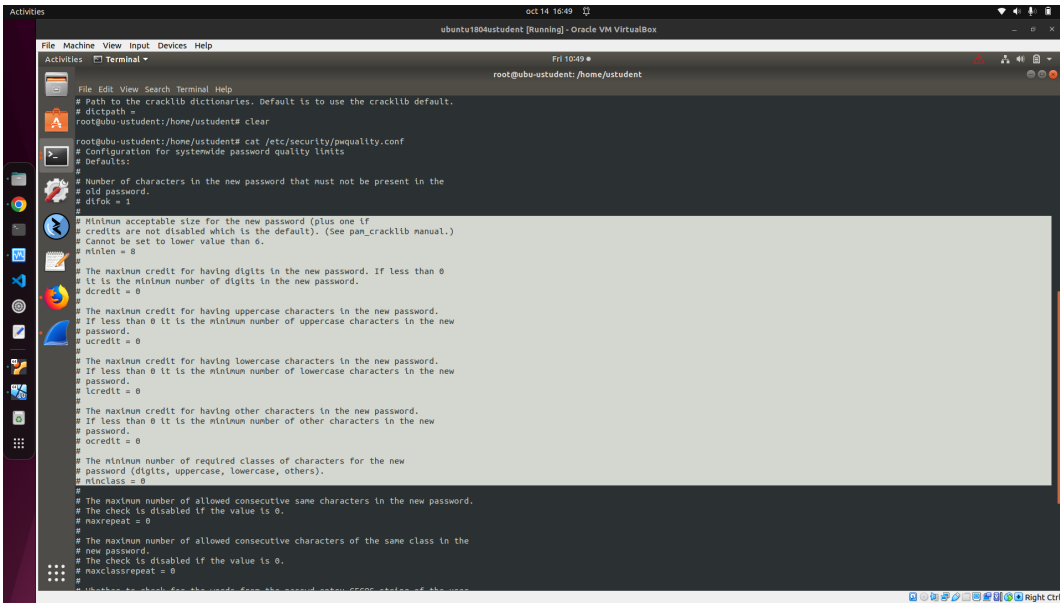




4.2 Verify that Ubuntu and Windows comply with

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

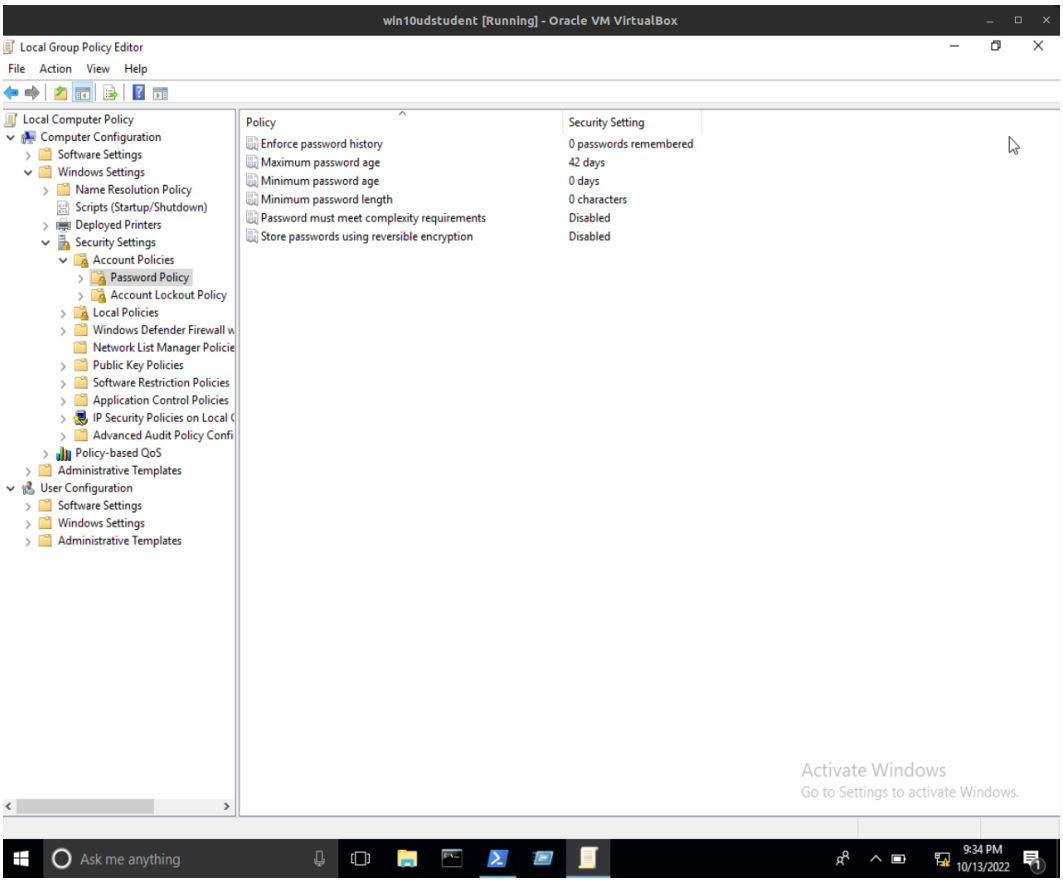




Verify password creation requirements conform to organization policy.

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.

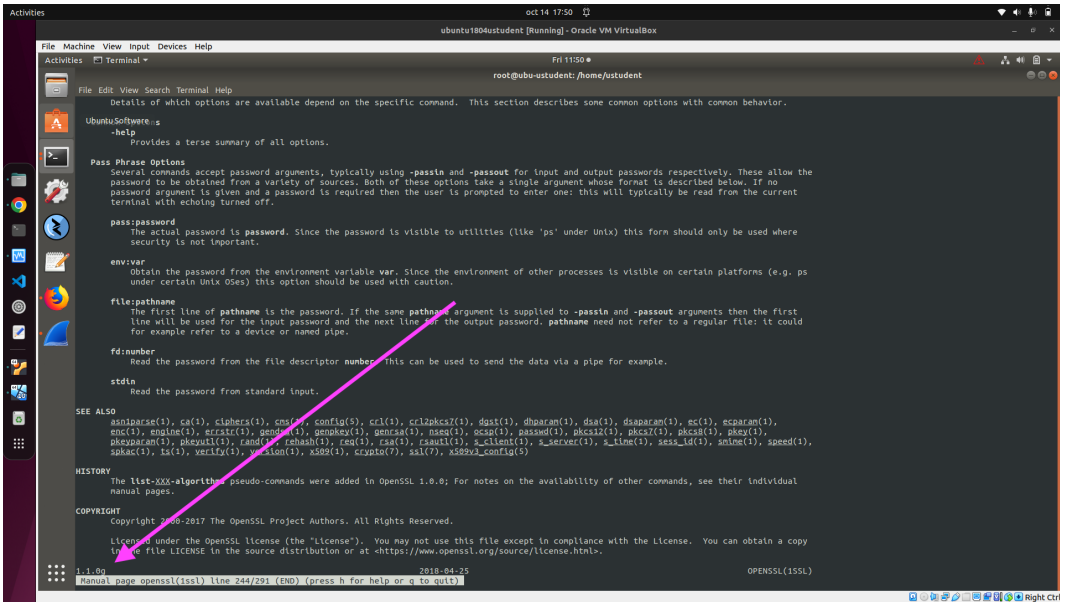
Maintaining FIPS Certified modules security

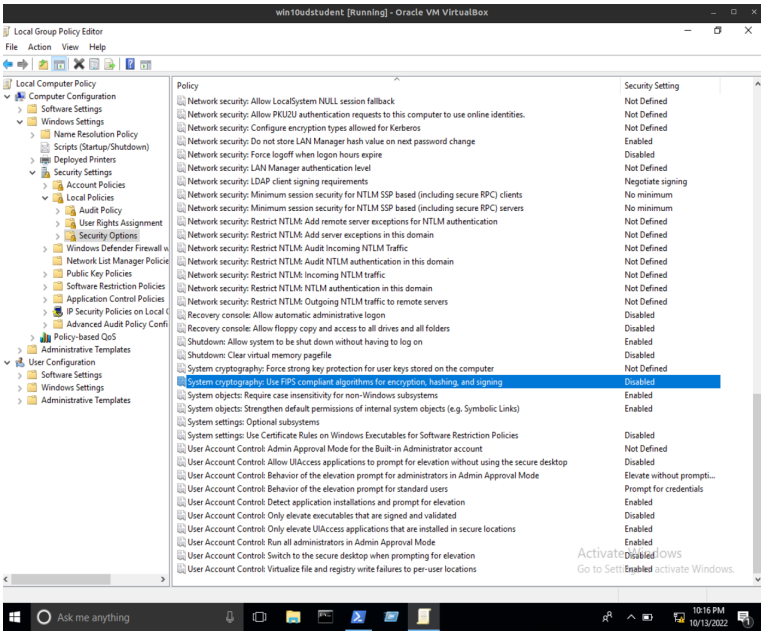
To keep your FIPS Certified Ubuntu secure we will re-certify all modules every year.

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

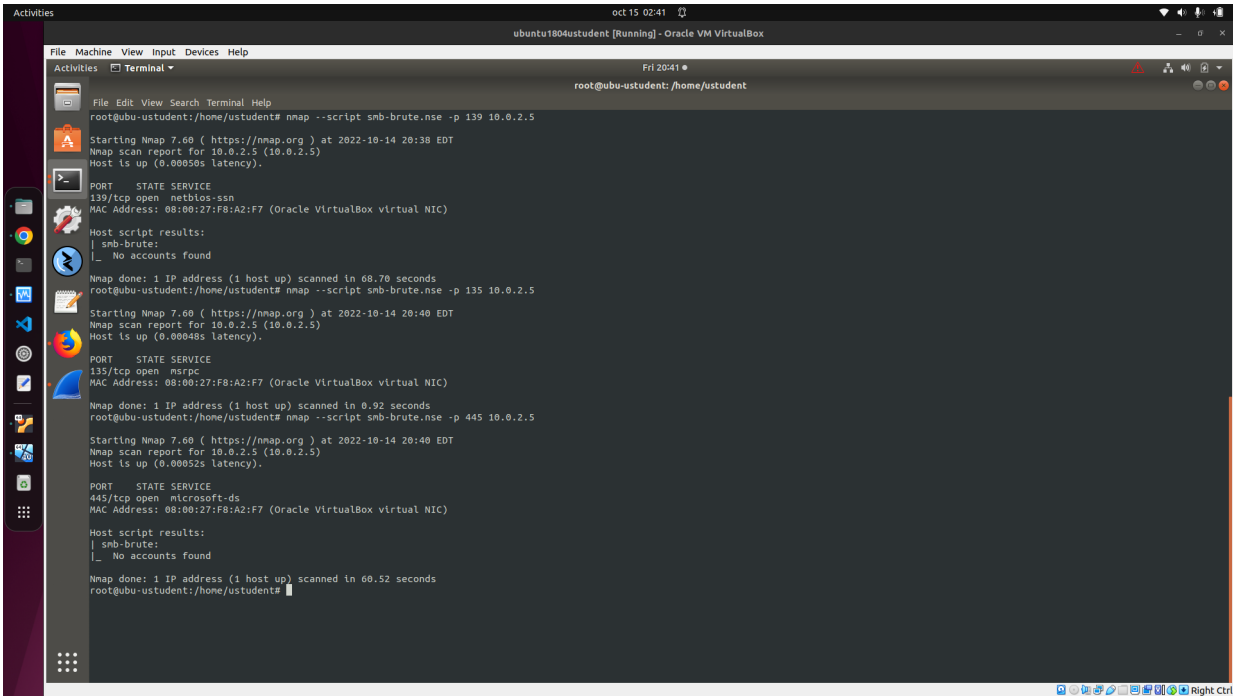


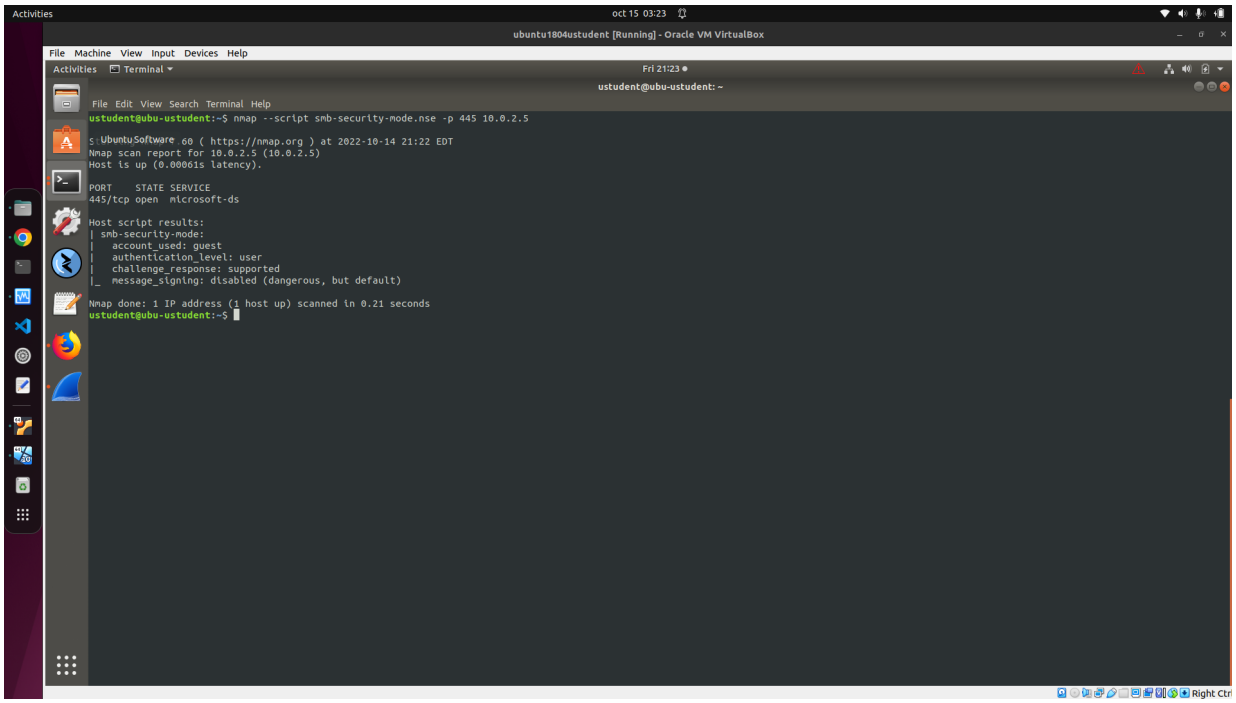


4.4 Conduct aggressive testing for password strength Mitre ATT&CK T1110

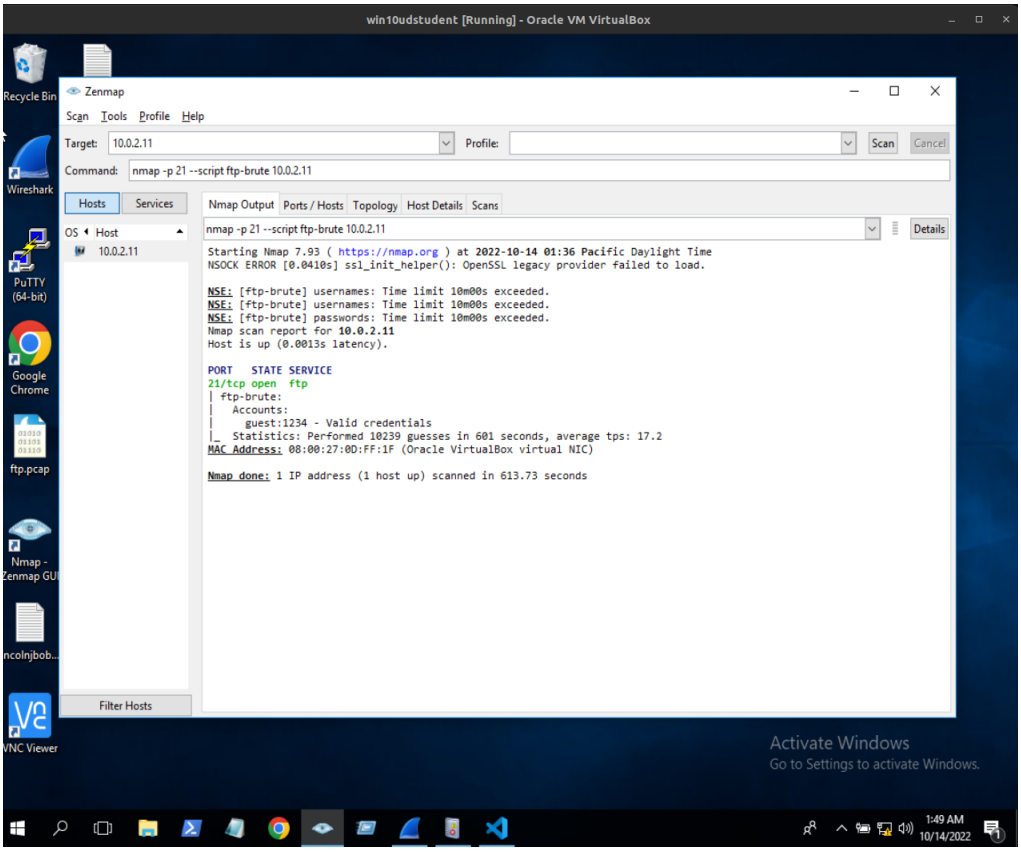
- **4.4.1** SMB shares at Windows virtual machine
- **4.4.2** FTP Server at Ubuntu virtual machine

- **Windows**





- **Ubuntu**


win10udstudent [Running] - Oracle VM VirtualBox
Recycle Bin
Wireshark
PuTTY (64-bit)
Google Chrome
ftp.pcap
Nmap - Zenmap GUI
VNC Viewer
Zenmap
Scan Tools Profile Help
Target: 10.0.2.11
Profile:
Scan
Cancel
Command: nmap -p 21 --script ftp-brute 10.0.2.11
Hosts
Services
OS Host
10.0.2.11
Filter Hosts
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -p 21 --script ftp-brute 10.0.2.11
Details
Starting Nmap 7.93 (https://nmap.org) at 2022-10-14 01:36 Pacific Daylight Time
NSOCK ERROR [0.0410s] 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 10.0.2.11
Host is up (0.0013s latency).
PORT STATE SERVICE
21/tcp open ftp
| ftp-brute:
| Accounts:
| guest:1234 - Valid credentials
|_ Statistics: Performed 10239 guesses in 601 seconds, average tps: 17.2
MAC Address: 08:00:27:0D:FF:1F (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 613.73 seconds
Activate Windows
Go to Settings to activate Windows.
1:49 AM
10/14/2022