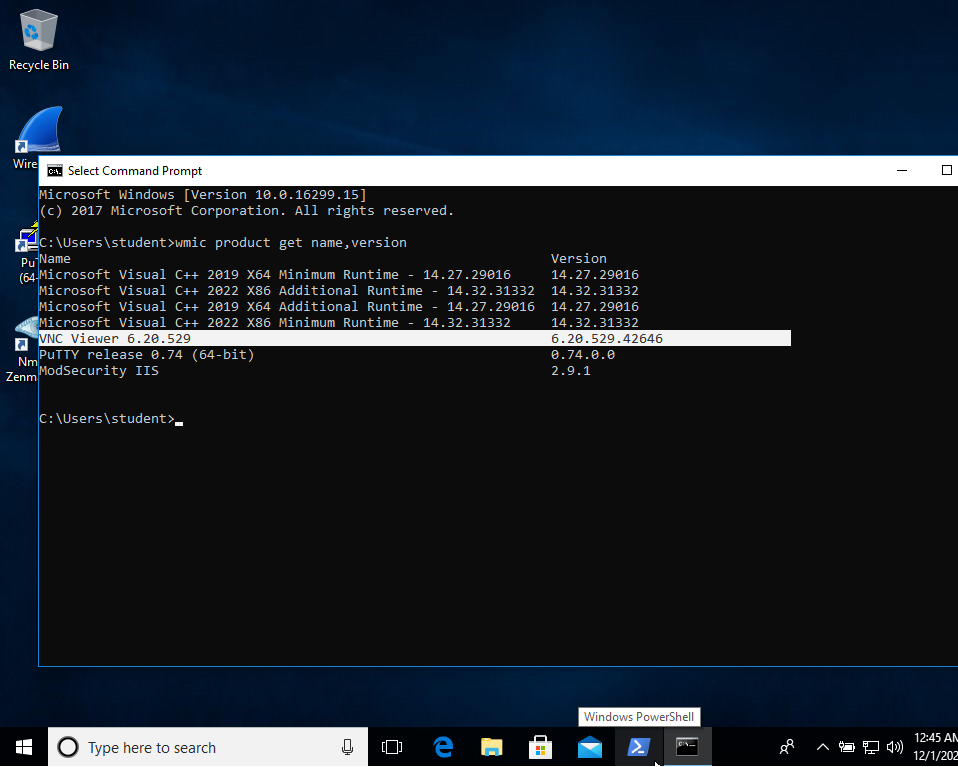
**Security Engineer : Project 3**

**Step 1 : Task 3 :Native Protections and Software Inventory in recording**

**In Windows :**

**Provide documentation as to what applications are installed on the Windows machine.**

**Is VNC viewer installed in this Windows System? screenshot**

**nmap**

We can update .

In Ubuntu :

Please provide proof of checks via command output or screenshots. According to these checks, are native protections applied to these systems? What packages are installed in this ubuntu machine?

Is TightVNC installed on this Ubuntu machine?

Text

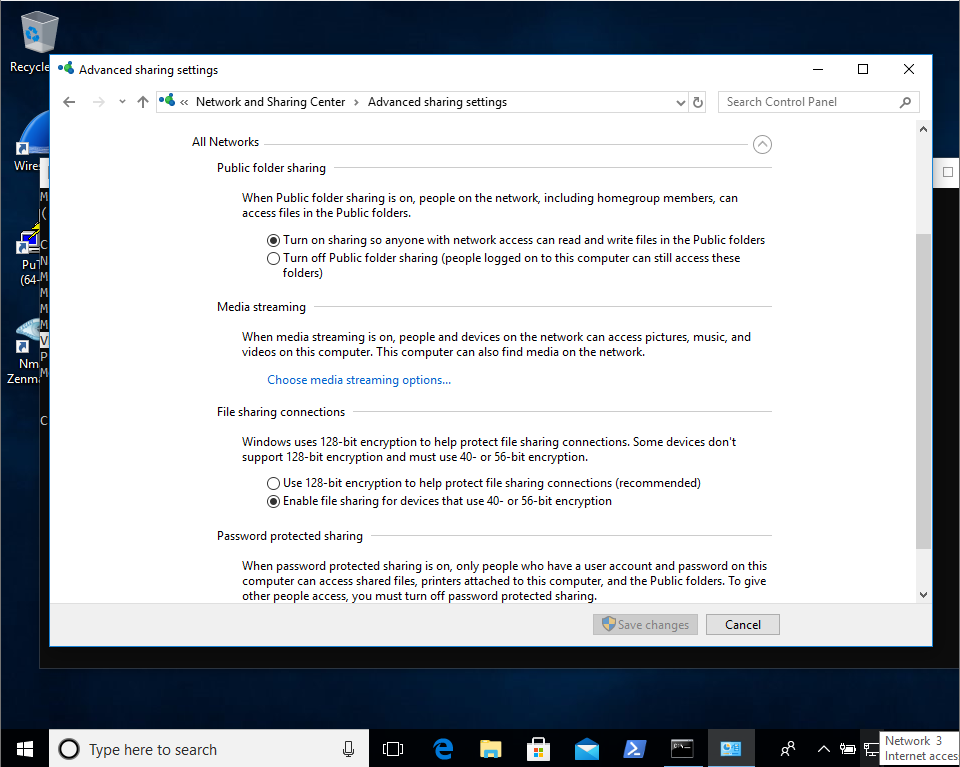
Description automatically generated

## Step 2 : Assess Access Management at Targeted Assets

**Task 1 :**

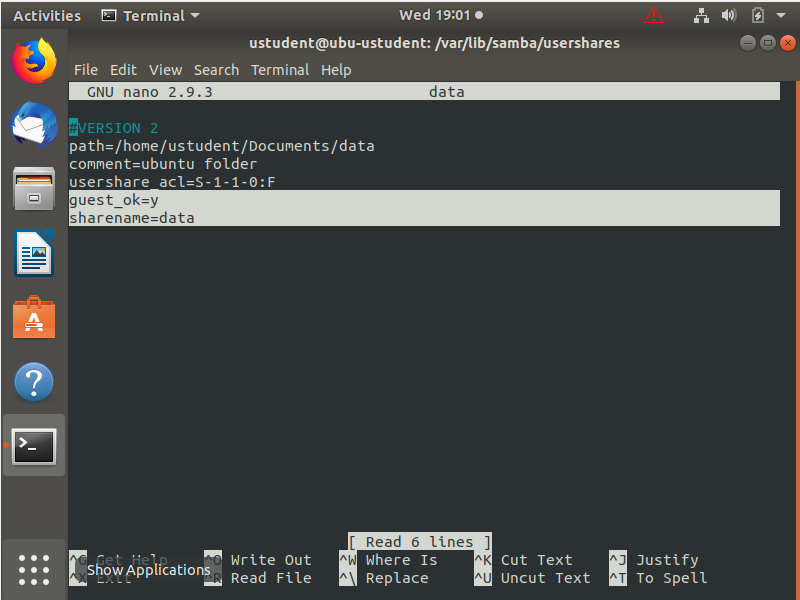
* **Is Anonymous access granted to any share?**

**In Windows**

****

* **Is Anonymous access granted to any share?**

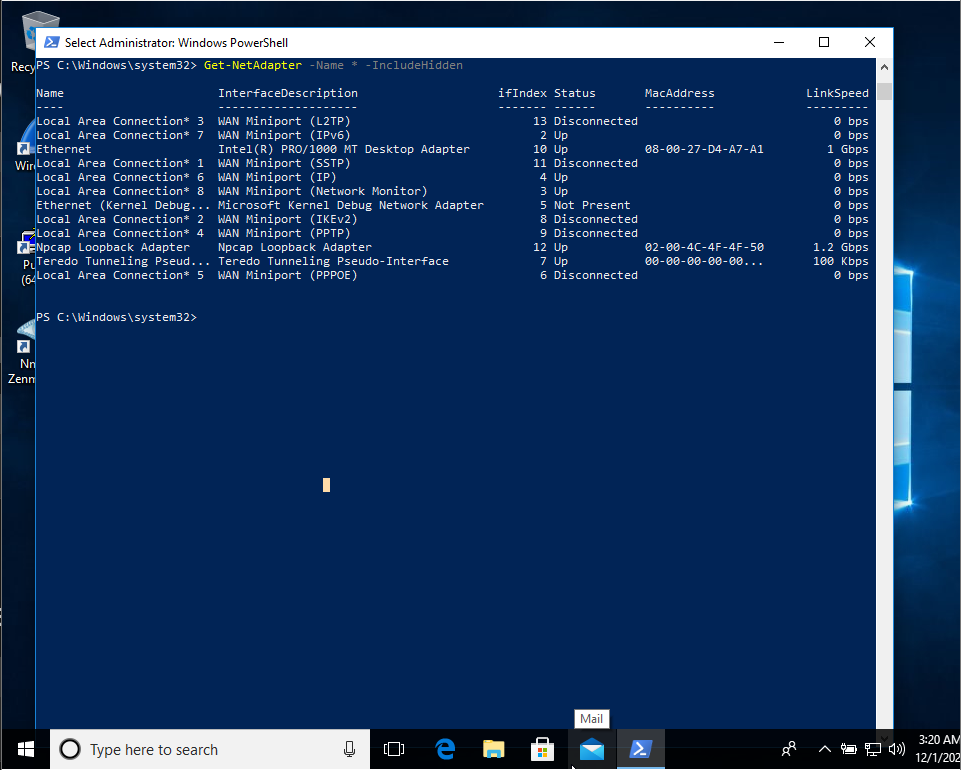
In ubuntu :



## Step 2 : Assess Access Management at Targeted Assets

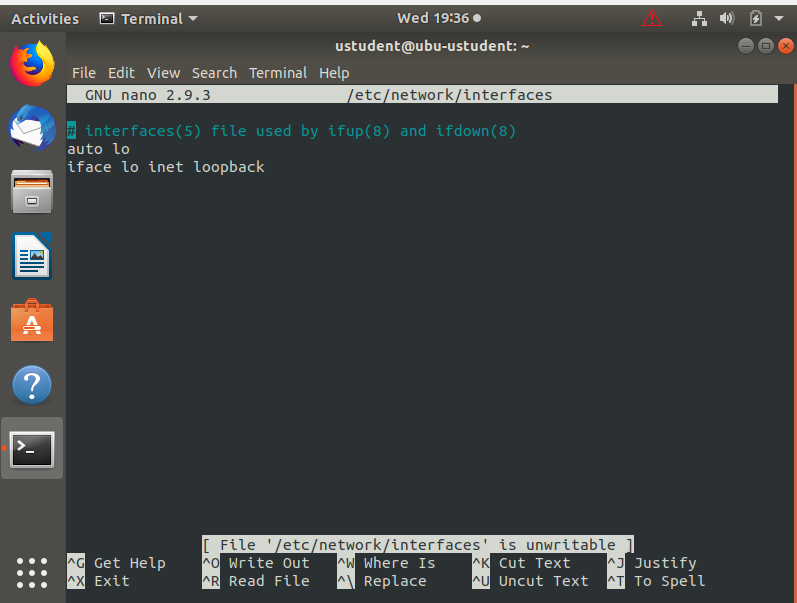
* Are there any VLANs?

In Windows :



* Are there any VLANs?

In ubuntu :



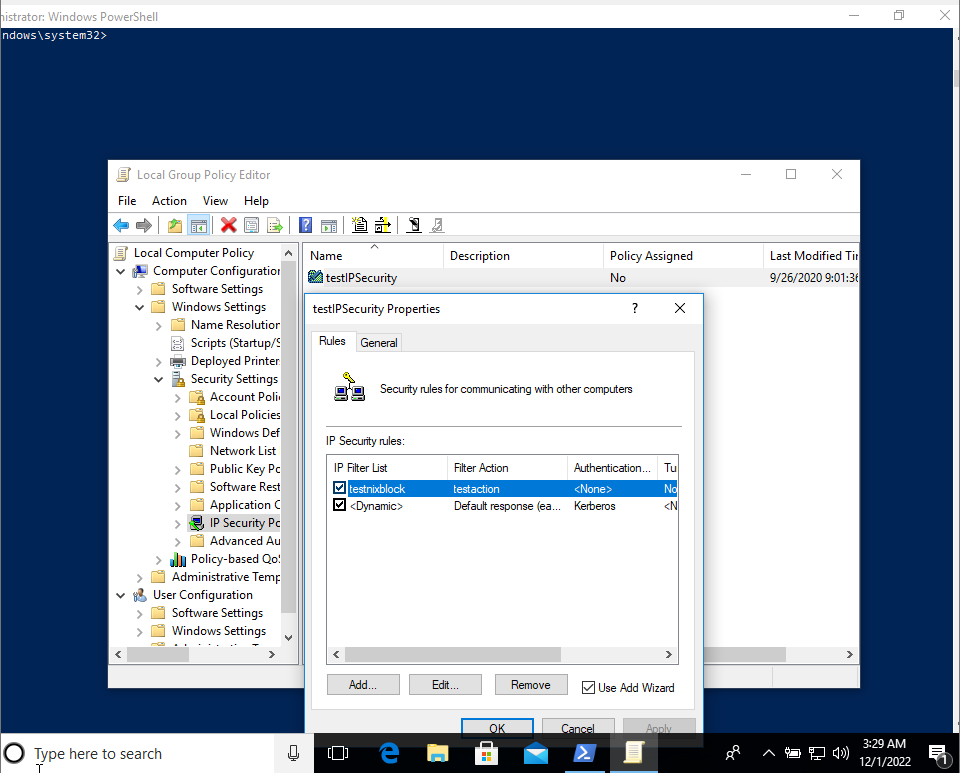
Text

Description automatically generated

## Step 2 : Assess Access Management at Targeted Assets

* Are there any policies in place? Yes there is .
  + If there are any, are they applied? No it’s not assigned

In Windows :



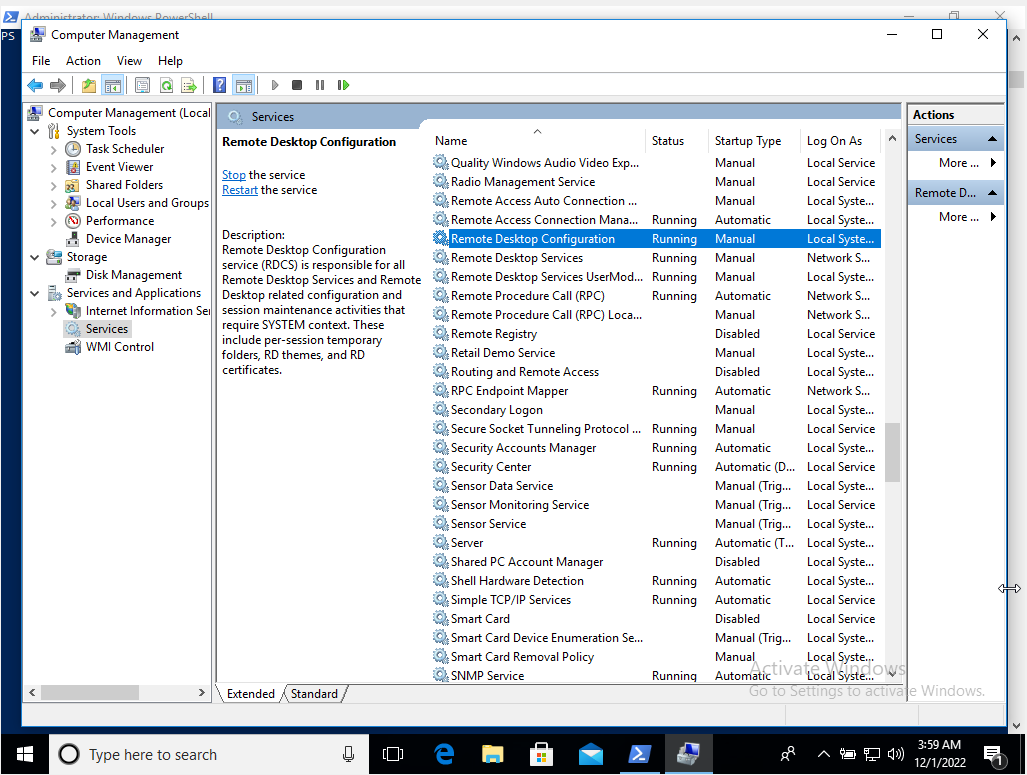
## Step 2 : Assess Access Management at Targeted Assets

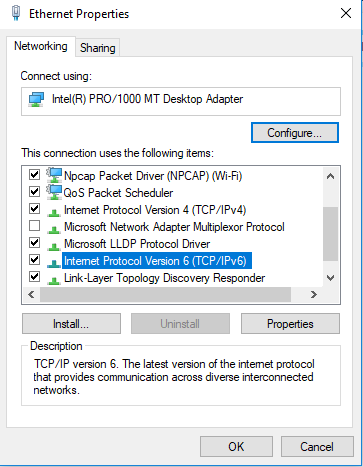
## Task 3 :

Investigate and assess the remote access services and protocols in place for StaticSpeed and determine their security level. After completing your investigation, including your assessment of how StaticSpeed is doing with remote access. Please have evidence to support your findings. Remember to consider IPv4 and IPv6. Also, include which Remote Service protocols are running on these systems (both Ubuntu and Windows)? What would you recommend to make improvements to this system? Are there protocols that should not be enabled?. Are there networking features that should be disabled or hardened?

## Investigate and assess the remote access services and protocols in place for StaticSpeed and determine their security level. After completing your investigation, including your assessment of how StaticSpeed is doing with remote access. Please have evidence to support your findings.

## In Windows :



 **consider IPv4 and IPv6**

## Investigate and assess the remote access services and protocols in place for StaticSpeed and determine their security level. After completing your investigation, including your assessment of how StaticSpeed is doing with remote access. Please have evidence to support your findings.

## In Ubuntu :

## 

## Here we can see that there is remote services such as ssh , ftp and inetd . and it’s recommended that if there is no need to use these services so it should be closed .

## Step 2 : Assess Access Management at Targeted Assets

**Task 4 :**

Next, conduct a Principles of Least Privilege assessment of StaticSpeed's system. We need to know:

* Which users have high privileges?
* Do important PII folders have the correct permissions and ownership?
* Are the default settings correct, and are there any excessive permissions?
* On our initial scan, we found "data" shared folders that need further investigation.
* Are there "guest" accounts enabled? Are they allowed to use Sudo commands? Are they allowed to log in to ALL workstations?.

Based on your findings, what should be done to secure these accounts and permissions better? Please provide proof of your results and provide reasoning for your answer.

* Which users have high privileges?

**In Windows :**

The guest user have a higher privileges that allowed to logon remotly:

Graphical user interface, application

Description automatically generated

**In Windows :**

The student user have a Higher privileges he take the administrator permissions .

Graphical user interface, application

Description automatically generated

* Which users have high privileges?

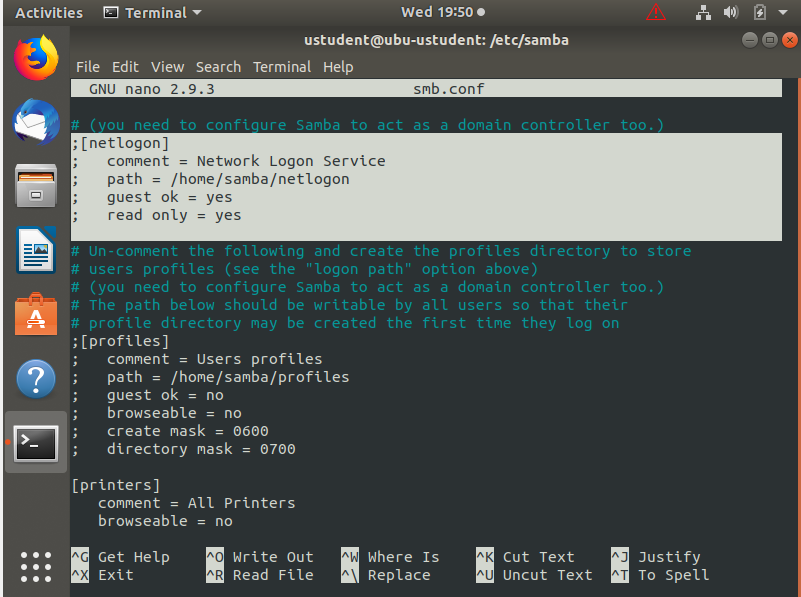
**In ubuntu**

* Are there "guest" accounts enabled? Are they allowed to use Sudo commands? Are they allowed to log in to ALL workstations?.

**In Windows**

* Are there "guest" accounts enabled? Are they allowed to use Sudo commands? Are they allowed to log in to ALL workstations?.

**In ubuntu :**

****

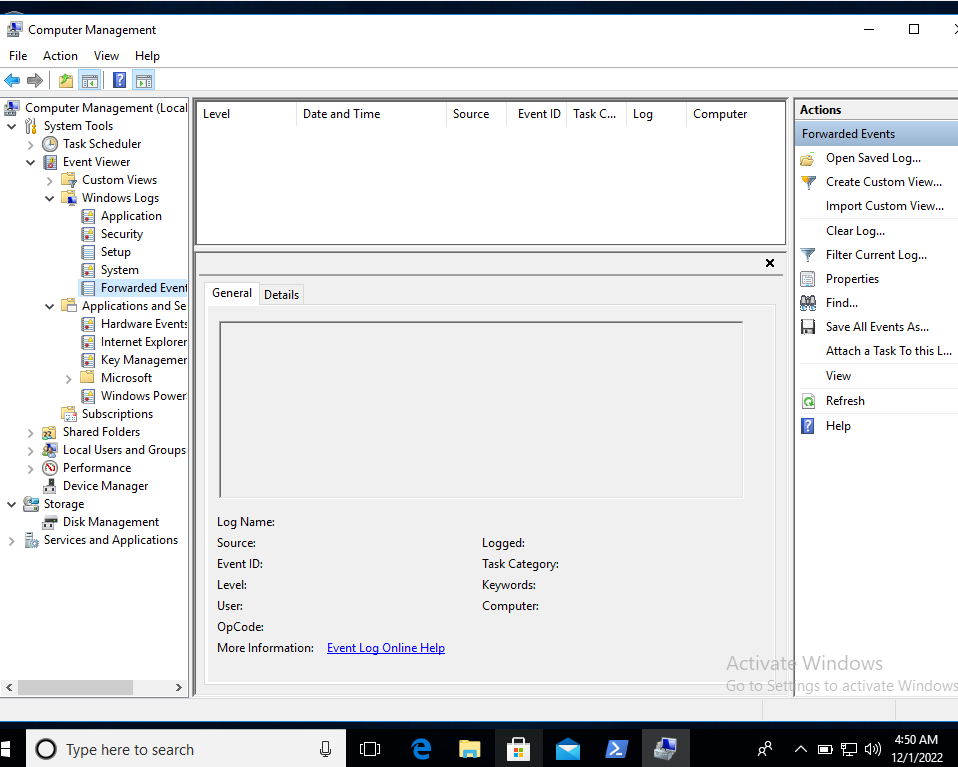
**Step 3: Log Monitoring Setup for Detection at Targeted Assets**

**Task 4**

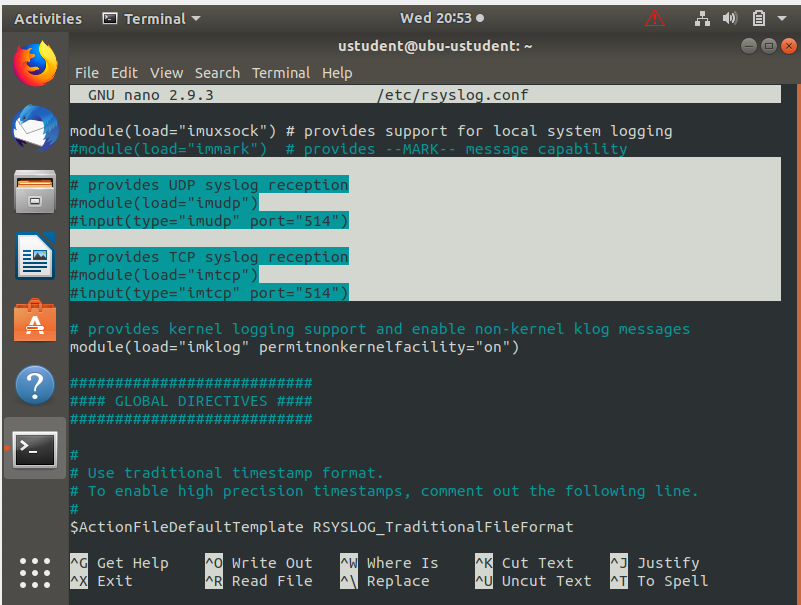
**NuttyUtility has a centralized log infrastructure using a SIEM product. You need to verify the machines you are checking from StaticSpeed have the settings enabled to use this.**

**Analyze StaticSpeeds systems and determine if these machines are currently shipping jobs to a centralized location and set up correctly for our SIEM**

**In Windows :**

****

**In Ubuntu :**

****

## **Step 4: Assess Authentication Management at Targeted Assets**

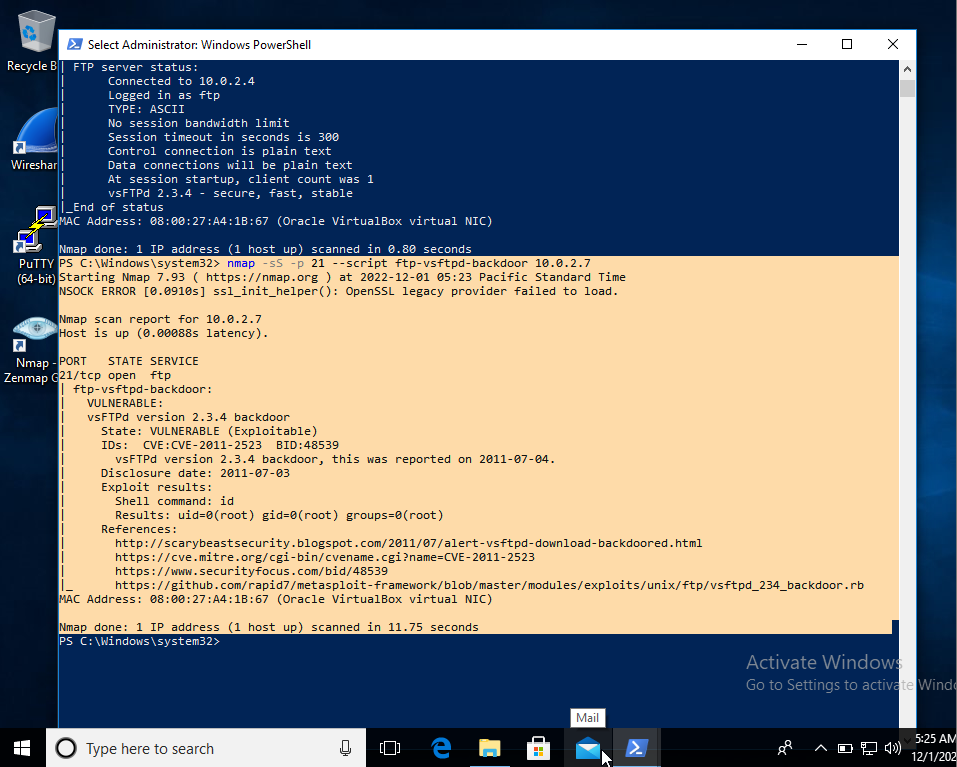
**Task 4**

**Conduct** aggressive testing for password strength. Use a Nmap NSE Script to test how easy it would be to access StaticSpeed's FTP Server and SMB Shares if an attacker probed them. We have already requested and obtained permission to perform these audits.

Please use an NSE Script to test Mitre ATT&CK T1110 in your Ubuntu virtual machine. Also, use an NSE Script to test the security mode of your SMB shares at your Windows virtual machine. What are your findings? Please provide screenshots. Remember to give an explanation of the security state of these services based on your results.

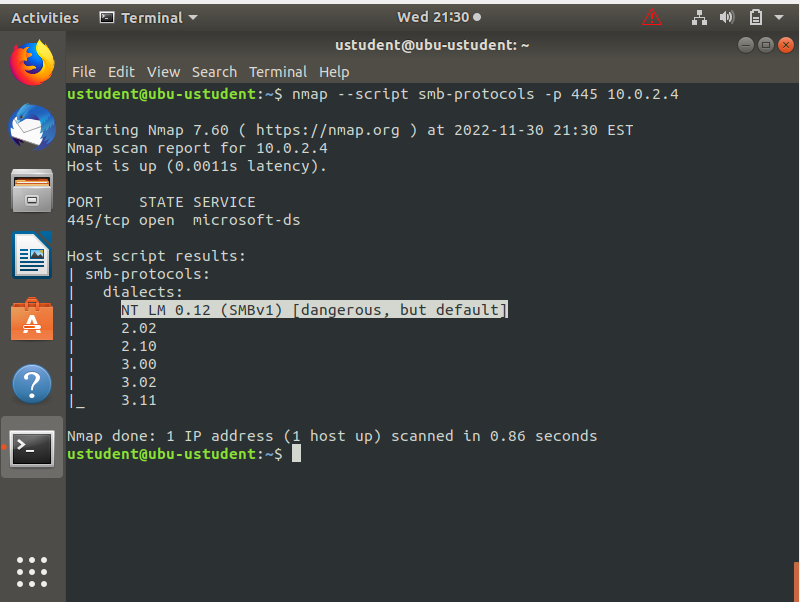
**In Windows**

**Nmap for the ftp service in ubuntu machine :**

****

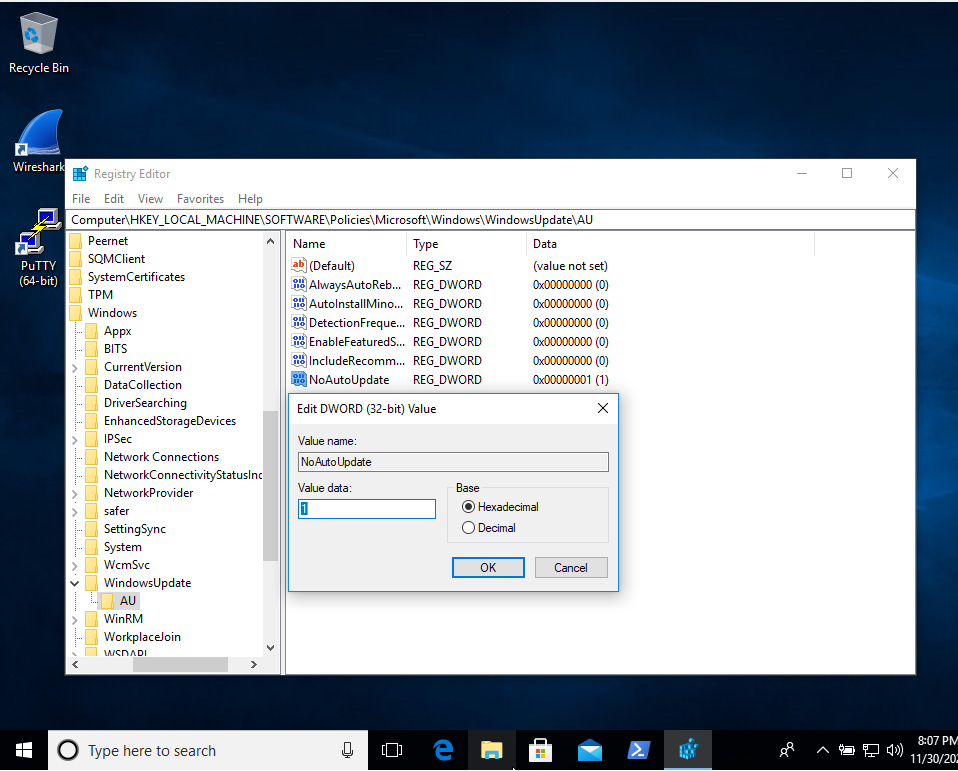
**In Ubuntu :**

**Nmap for the smb service in windows machine :**

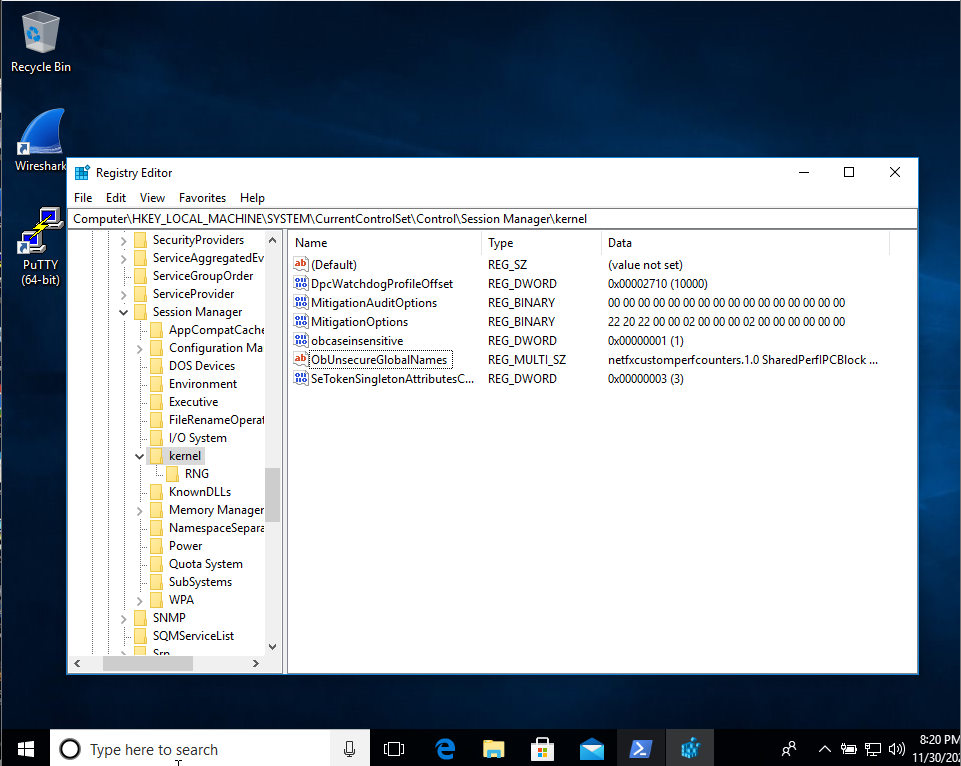
****

**CIS for Windows Ent v1.9.0. :**

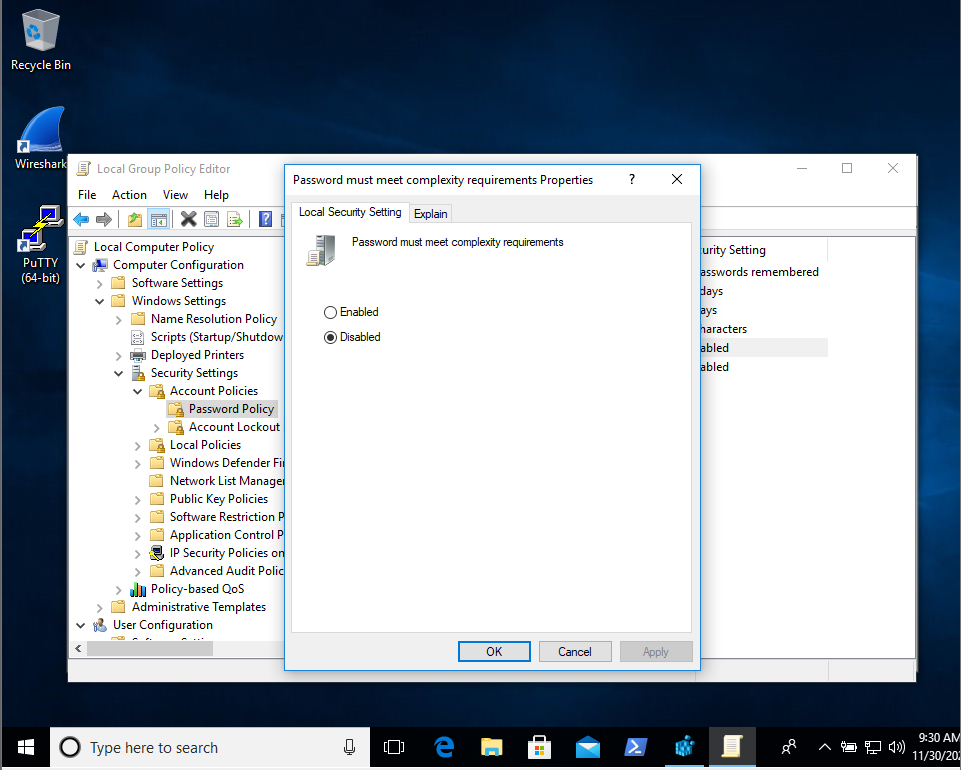
18.9.102.2 (L1) Ensure 'Configure Automatic Updates' is set to 'Enabled' (Automated)



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

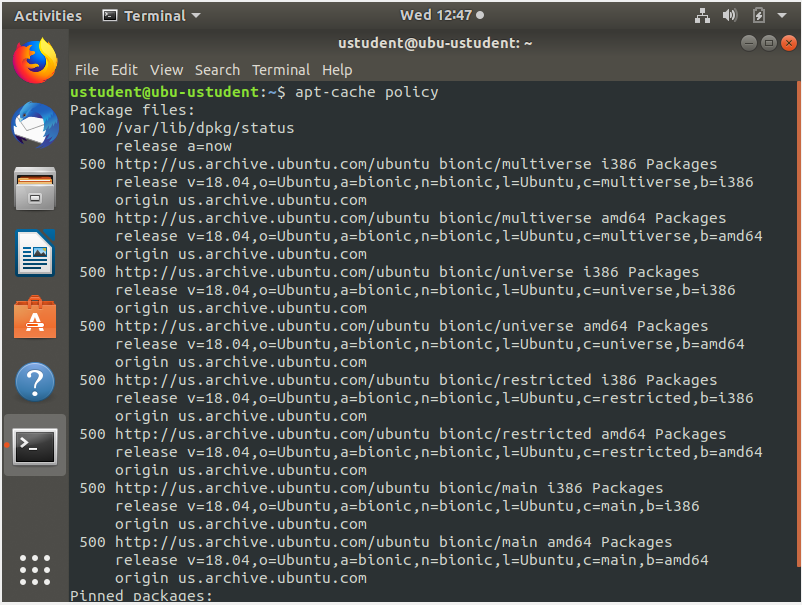


1.1.5 (L1) Ensure 'Password must meet complexity requirements' is set to 'Enabled' (Automated) .

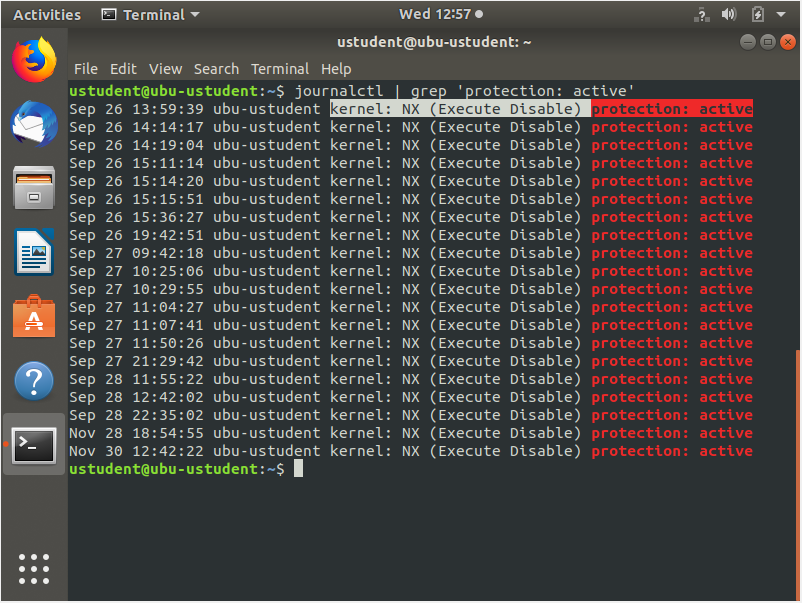


**CIS for Ubuntu 18.04 v2.01**

1.2.1 Ensure package manager repositories are configured (Not Scored)



1.6.1 Ensure XD/NX support is enabled (Scored)



1.6.2 Ensure address space layout randomization (ASLR) is enabled (Scored(

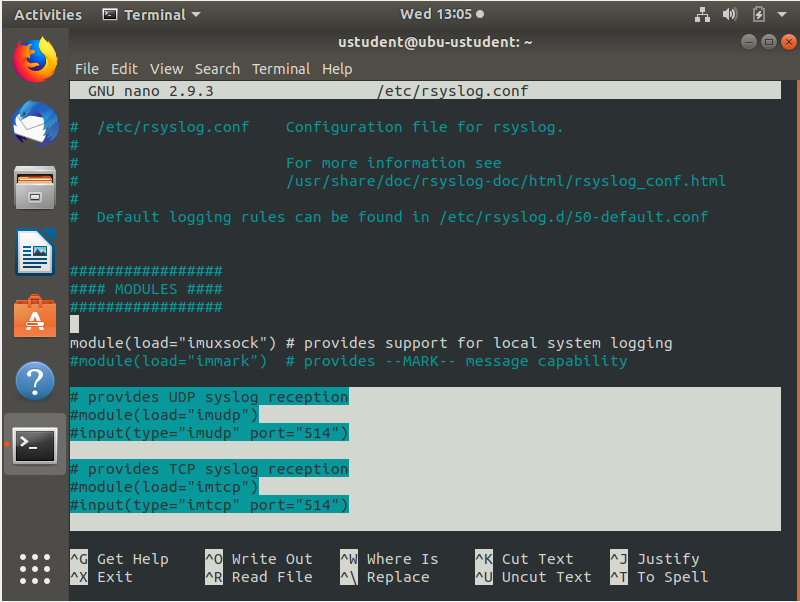
Text

Description automatically generated

Set the following parameter in /etc/sysctl.conf or a /etc/sysctl.d/\* file: kernel.randomize\_va\_space = 2

Run the following command to set the active kernel parameter: # sysctl -w kernel.randomize\_va\_space=2

4.2.1.3 Ensure logging is configured (Not Scored)



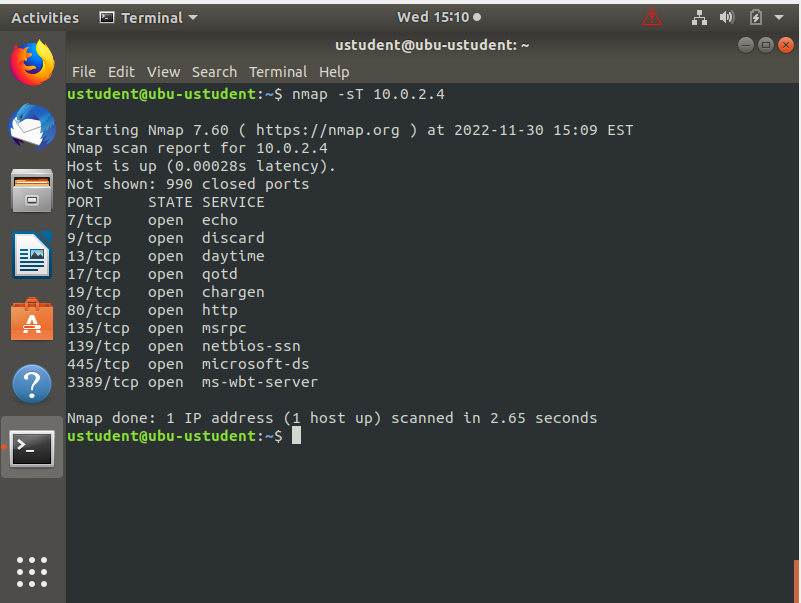
5.3.1 Ensure password creation requirements are configured (Scored)

Text

Description automatically generated

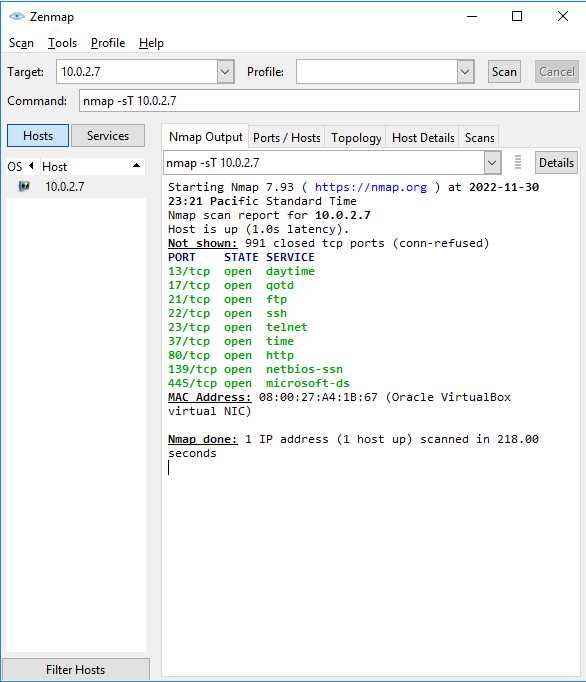
**Nmap : about the open ports in the two machines**

The nmap result show the open ports in Windows machine



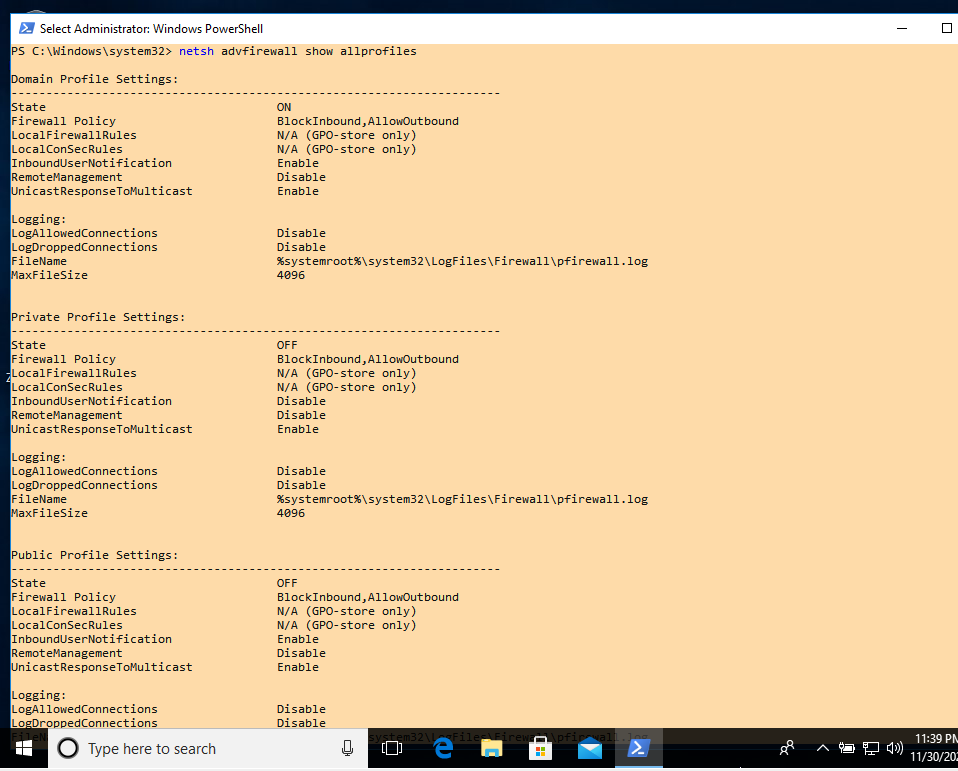
Also check the result from openvas scan .

The nmap result to show the open ports for ubuntu machine .



**Firewall status for two machines :**

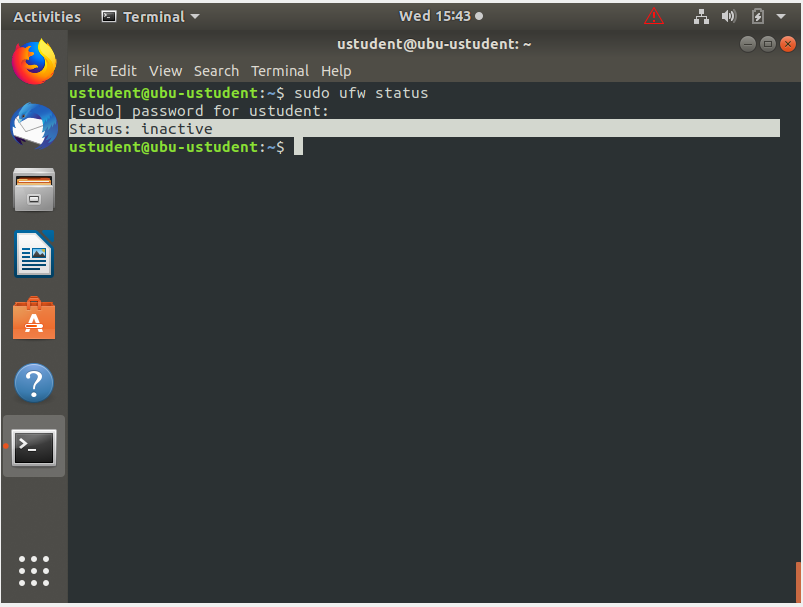
In Windows machine :



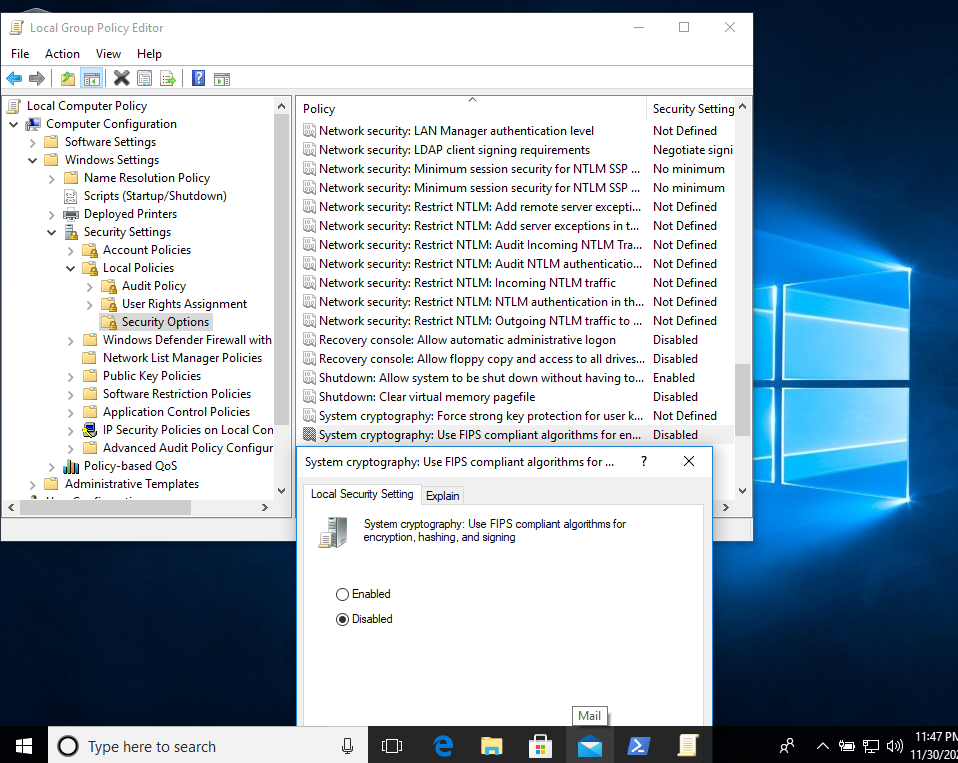
Graphical user interface

Description automatically generated

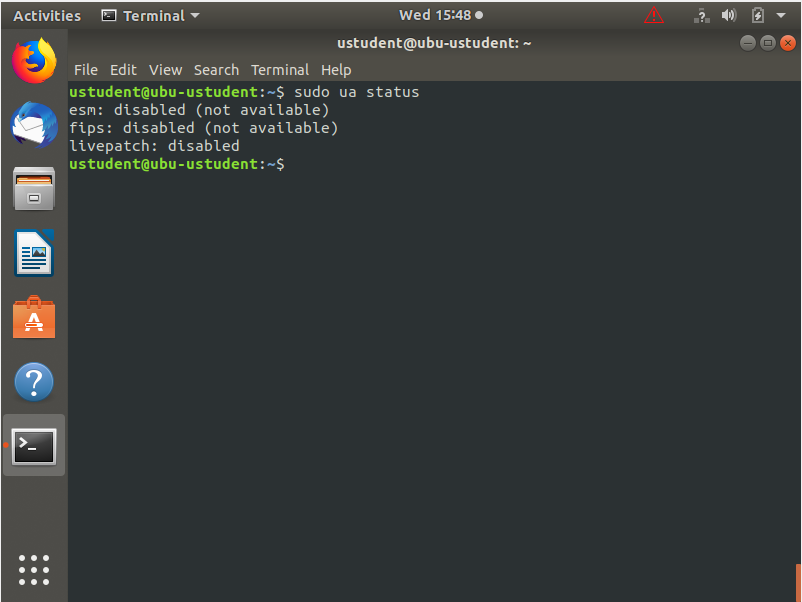
The firewall status in ubuntu machine :



Using FIPS policy in windows :



Using FIPS policy in ubuntu :



Step 5: Final Report

After performing the project's tasks, you must produce a report that will include an overview of your findings using the best practices industry format. You are expected to include ALL high, medium, low vulnerabilities, and informational findings (Things that are not necessarily scored but are relevant). Make sure to use and include the scanner switches and vulnerability scripts as they may provide conclusions that are not found in the default scanner settings.

**The format expected for both virtual machine results is below. Please divide by Operating System**

**- Linux Ubuntu 18.04**

- **Windows 10**

Windows 10 ENT

Ex

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Host | High | Medium | Low | Log |
| 192.168.1.27 | 32 | 5 | 0 | 0 |

**IP Address: 192.168.1.27**

|  |  |  |
| --- | --- | --- |
| Service | Port | Sensitive Level |
| tcp | 445 | High |
| tcp | General | High |
| tcp | 9 | High |
| tcp | 135 | Medium |
| tcp | 19 | Medium |
| tcp | 7 | Medium |
| tcp | 3389 | Medium |
| tcp | 17 | Medium |

Expected detail format for vulnerabilities found

**High 445/TCP CVSS:10.0**

**1- NVT: SMB Brute Force Logins With Default Credentials**

**Issue**

A number of known default credentials are tried for the login via the SMB protocol.

**Impact**

It was possible to login with the following credentials via the SMB protocol to

,the 'IPC$' share. <User>:<Password>

User:1234

**Mitigation**

Change the password as soon as possible.

**Reference**

cve: CVE-1999-0503 : <https://exchange.xforce.ibmcloud.com/vulnerabilities/1297>

cve: CVE-1999-0504 : <https://exchange.xforce.ibmcloud.com/vulnerabilities/21151>

cve: CVE-1999-0505 : <https://nvd.nist.gov/vuln/detail/CVE-1999-0505>

**Medium 3389/TCP - CVSS:4.3**

**1- NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection**

**Issue**

It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

**Impact**

An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.

Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

**Mitigation**

It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

**Reference**

Please add URLs that give context and guidance on how-to understand this finding and fix it.

cve: CVE-2011-3389 : <https://www.cisa.gov/uscert/ics/advisories/ICSMA-18-058-02>

cve: CVE-2015-0204 : <https://access.redhat.com/errata/RHSA-2015:0066.html>

url: <https://ssl-config.mozilla.org/>

url: <https://bettercrypto.org/>

url: <https://datatracker.ietf.org/doc/rfc8996/>

url: <https://vnhacker.blogspot.com/2011/09/beast.html>

**Medium 17/TCP - CVSS:5.0**

**1- NVT: Check for Quote of the Day (qotd) Service (TCP)**

**Issue**

The Quote of the Day (qotd) service is running on this host.

**Impact**

An easy attack is 'pingpong' which IP spoofs a packet between two machines running qotd. This will cause them to spew characters at each other, slowing the machines down and saturating the

network.

**Mitigation**

- Under Unix systems, comment out the 'qotd' line in /etc/inetd.conf and restart the inetd

process

- Under Windows systems, set the following registry keys to 0 :

HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpQotd

HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpQotd

Then launch cmd.exe and type :

net stop simptcp

net start simptcp

To restart the service.

**Reference**

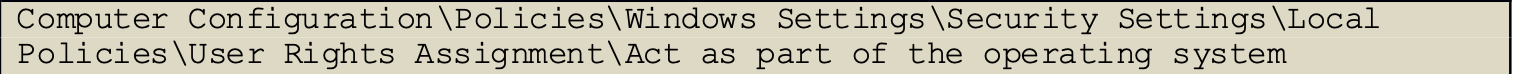
cve: CVE-1999-0103 : <https://www.cisa.gov/uscert/ics/advisories/ICSMA-18-233-01>

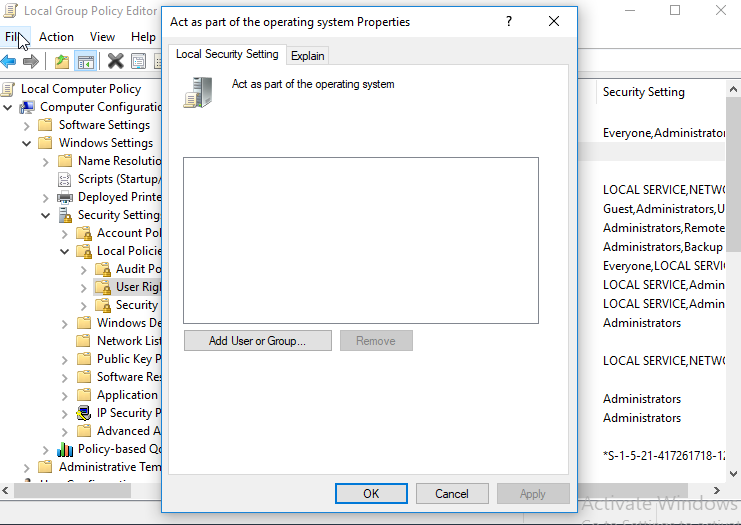
Example of control checks & CIS benchmarks Windows 10 ENT

**Control check - 2.2.3 Ensure ‘Act as part of the operating system’ is set to ‘No One’**

**Result:** Compliant, no user or group found in the setting

**Proof of check:**

****

****

**Impact:** The Act as part of the operating system user right is extremely powerful. Anyone with this user right can take complete control of the computer and erase evidence of their activities.This system is compliant with corporate policy CIS 2.2.3 for Windows 10 ENT.

Ubuntu 18.04

Ex

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Host | High | Medium | Low | Log |
| 192.168.1.28 | 36 | 38 | 3 | 0 |

**IP Address : 192.168.1.28**

Host scan start Thu Dec 1 05:49:55 2022 UTC

Host scan end Thu Dec 1 06:07:36 2022 UTC

|  |  |  |
| --- | --- | --- |
| Service | Port | Sensitive Level |
| TCP | 80 | High |
| TCP | 22 | High |
| TCP | 445 | High |
| TCP | 23 | Medium |
| TCP | 80 | Medium |
| TCP | 22 | Medium |
| TCP | 21 | Medium |
| TCP | 445 | Medium |
| TCP | GERNERAL | Low |
| TCP | 445 | Low |

Expected detail format for vulnerabilities found

**High 80/TCP – CVSS:9.8**

**1-NVT: Apache HTTP Server 2.4.0 - 2.4.46 Multiple Vulnerabilities - Linux**

**Issue**

Apache HTTP Server is prone to multiple vulnerabilities.

**Impact**

CVE-2020-35452: A specially crafted Digest nonce can cause a stack overow in

mod\_auth\_digest.

- CVE-2021-26690: A specially crafted Cookie header handled by mod\_session can cause a NULL

pointer dereference and crash, leading to a possible Denial Of Service.

- CVE-2021-26691: A specially crafted SessionHeader sent by an origin server could cause a heap overflow.

**Mitigation**

Update to version 2.4.48 or later.

**Reference**

cve: CVE-2020-35452

cve: CVE-2021-26690

cve: CVE-2021-26691

url: <https://httpd.apache.org/security/vulnerabilities_24.html>

**Medium 80/TCP – CVSS:5:9**

**1- NVT: Apache HTTP Server HTTP/2 'SETTINGS' Data Processing DoS Vulnerability (Linux)**

**Issue**

Apache HTTP Server is prone to a denial-of-service vulnerability.

**Impact**

Successful exploitation will allow remote attackers to cause a denial of service (DoS) condition on a targeted system.

**Mitigation**

Update to Apache HTTP Server 2.4.35 or later.

**Reference**

cve: CVE-2018-11763

url:<https://access.redhat.com/errata/RHSA-2018:3558>

url: <https://httpd.apache.org/security/vulnerabilities_24.html>

Low GENERAL/TCP – CVSS:2.6

**1- NVT: TCP timestamps**

**Issue**

The remote host implements TCP timestamps and therefore allows to compute the uptime.

**Impact**

A side effect of this feature is that the uptime of the remote host can sometimes be computed.

**Mitigation**

To disable TCP timestamps on linux add the line 'net.ipv4.tcp\_timestamps = 0' to

/etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.

To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'

Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.

The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.

**Reference**

**url:** [**http://www.ietf.org/rfc/rfc1323.txt**](http://www.ietf.org/rfc/rfc1323.txt)

**url:** [**http://www.ietf.org/rfc/rfc7323.txt**](http://www.ietf.org/rfc/rfc7323.txt)