StaticSpeed Vulnerability Report

As you start your final project, you are expected to perform the following tasks in BOTH Windows and Linux systems. We need to decide if StaticSpeeds systems should be integrated into NuttyUtility's extended network and infrastructure. In the end, your report must support your recommendation. This document is a template that NuttyUtility uses similar system reviews. Some specific information is provided in certain places after initial talks with NuttyUtility. Please follow the format of this template and answer all questions for each section. **You will need to provide either the text outputs from the command line and/or screenshots as evidence** in all sections of this template to show that you have completed the required steps of our company's template and make it easier for stakeholders to see where there might be issues.

Your report must include the findings of your CIS Benchmarks and Security control checks along with the results of Openvas and NMap scans. As a security professional, it is expected that you will relay your findings in terms of industry language (i.e., CVE-xxxx-xxxx, Mitre Technique ID Txxx where applicable). Based on NuttyUtility's security policies, are these systems ready? Your report will be used by stakeholders to decide on the integration.

The best way to find these vulnerabilities is by performing vulnerability scans using Nmap NSE Vuln scripts as shown in the course Nmap lesson and use the CIS benchmarks requested in the project.

Control checks and CIS benchmarks for Windows & Ubuntu
In this section, outline your answers from the requested checks. Please provide either the **command-line outputs in the form of text** or **screenshots** that show a CIS check and/or control check has been performed. You must also answer the questions based on your assessments.

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

Task 1

As seen in your lessons, you must have CIS Benchmarks for Ubuntu 18.04 v2.01 and Windows 10 Ent v1.9.0 to perform these checks. Use the MITRE website for the database of common vulnerabilities and exposures (CVE) https://cve.mitre.org and Mitre ATT&CK framework for referencing attack techniques, tools, and procedures attack.mitre.org.

You must download the CIS Benchmark PDFs for Ubuntu 18.04 v2.01 and Windows 10 Ent v1.9.0. In these PDFs, there will be all the information related to the CIS Benchmarks requested in the following tasks which need to be included in your final report. In order to perform the vulnerability scans via Nmap NSE scripts as shown in Lesson 6 "Use Nmap for Vulnerability Discovery" Please review the lesson if needed and use, as suggested in the Lesson NSE scripts from Vulscan and Vulners GitHub repositories. Using these NSE scripts should be enough to discover the vulnerabilities present in your virtual machines (Both Ubuntu and Windows Machines). Both machines have vulnerable services and applications, a vulnerability may include as well, a deprecated or outdated/exposed service, it is also suggested to use the highest privilege (root/administrator) when applicable to perform an audit, there might be applications not found by network scan yet present at machines that are also reportable (Please review Lesson 2 "Software Inventory and Version Tracking").

Once you discover the vulnerabilities please refer to Mitre cve.mitre.org for vulnerability classification and remediation, also Mitre ATT&CK framework attack.mitre.org (Lesson 2, "Identify Industry Frameworks for Vulnerability Reference Pt 1") to get things such as technique ids, tools, and procedures. Once you have all this information, you will need to complete the report template. Your report Must also include the CIS Benchmarks requested in the next tasks please see template examples for the report format.

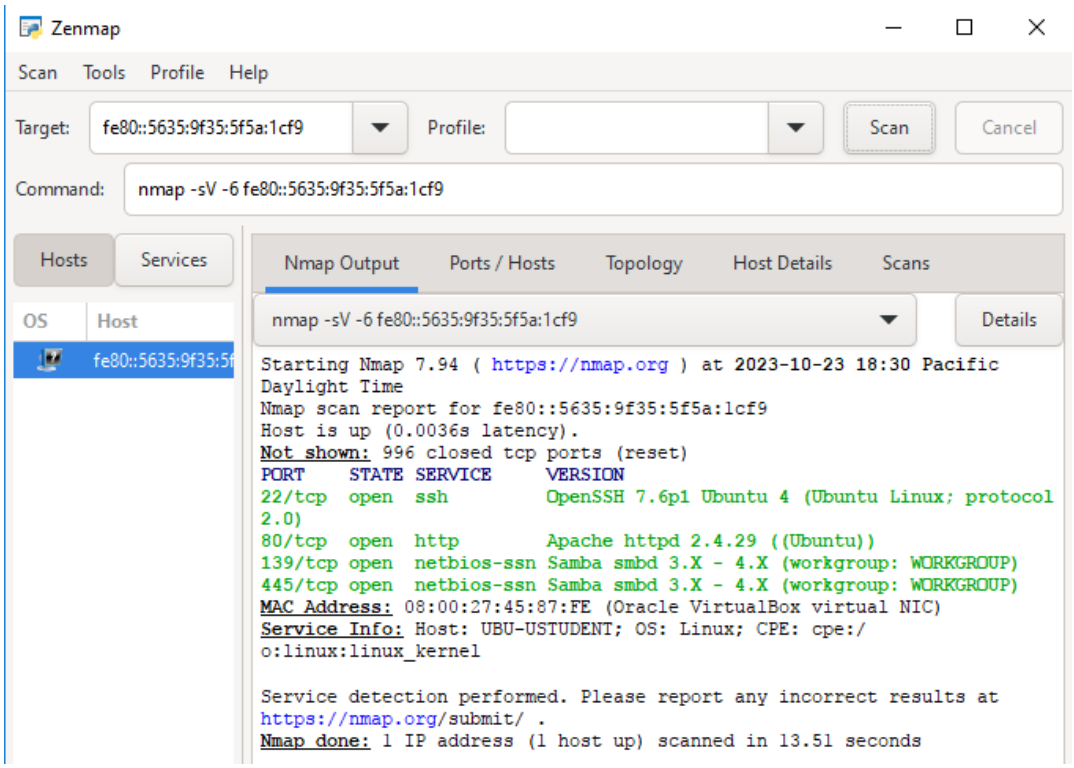
Ans: We apply nmap using the NSE script to discover the vulnerabilitie, We found a outdate samba version raise CVE-2017-7494 vulnerabilitie in the generate report see below screenshots:

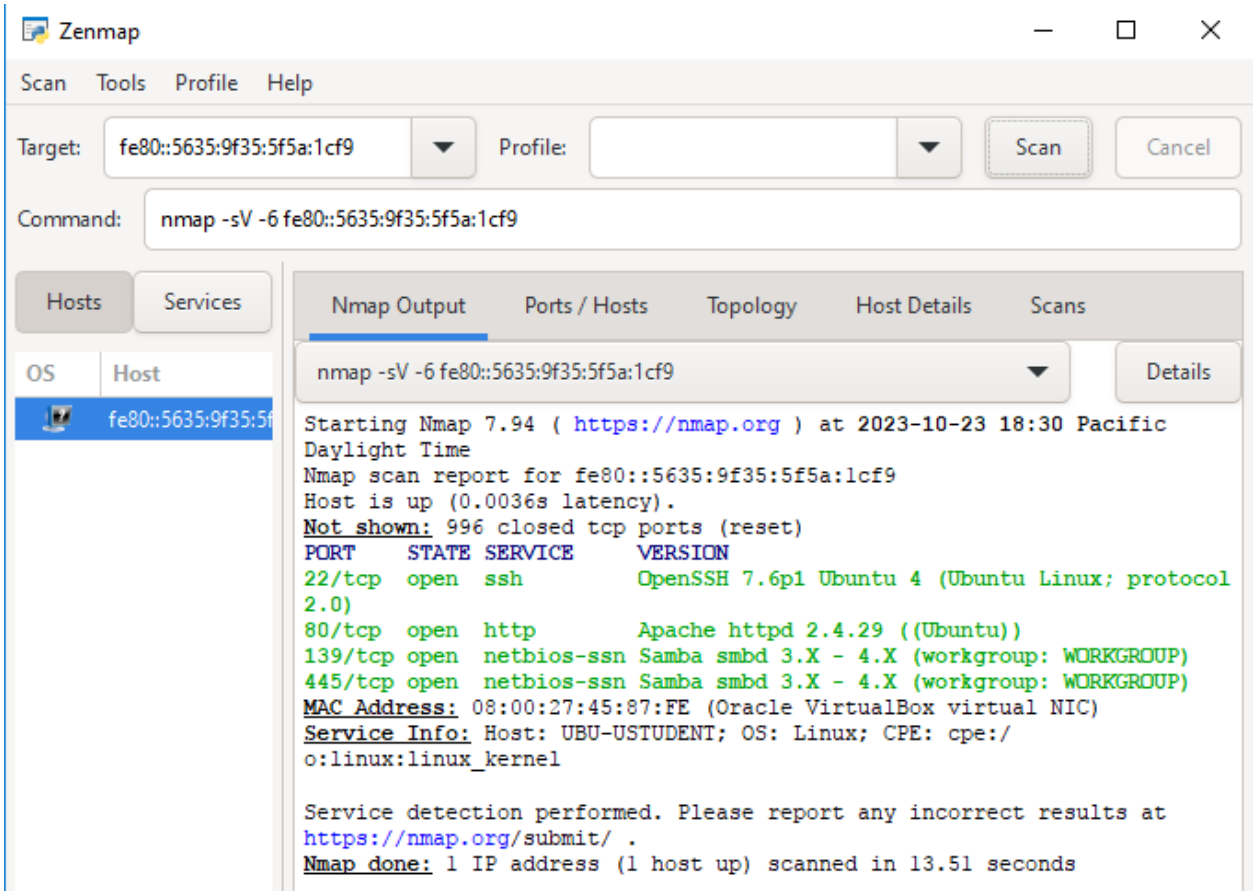
```
ustudent@ubu-ustudent:~$ nmap -sV --script vuln 10.0.2.6

Starting Nmap 7.60 ( https://nmap.org ) at 2023-10-23 22:56 EDT
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for ubu-ustudent (10.0.2.6)
Host is up (0.00017s latency).
Not shown: 991 closed ports
PORT    STATE SERVICE     VERSION
13/tcp  open  daytime
17/tcp  open  qotd?
| fingerprint-strings:
|   NULL:
|     A is for Apple.
|_    Hester Pryne
21/tcp  open  ftp         vsftpd 2.0.8 or later
|_sslv2-drown:
22/tcp  open  ssh         OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
23/tcp  open  telnet      Linux telnetd
37/tcp  open  time        (32 bits)
|_rfc868-time: 2023-10-24T02:57:52
80/tcp  open  http        Apache httpd 2.4.29 ((Ubuntu))
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint
 at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port17-TCP:V=7.60%I=7%D=10/23%Time=653732A2%P=x86_64-pc-linux-gnu%r(NUL
SF:L,22,"A\x20is\x20for\x20Apple\.\n\t\t--\x20Hester\x20Pryne\n");
Service Info: Host: Welcome; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-vuln-cve-2017-7494:
|   VULNERABLE:
|   SAMBA Remote Code Execution from Writable Share
|     State: LIKELY VULNERABLE
```

```
SF:L,22,"A\x20is\x20for\x20Apple\.\n\t\t--\x20Hester\x20Pryne\n");
Service Info: Host: Welcome; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-vuln-cve-2017-7494:
|   VULNERABLE:
|   SAMBA Remote Code Execution from Writable Share
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2017-7494
|     Risk factor: HIGH  CVSSv3: 7.5 (HIGH) (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H)
|       All versions of Samba from 3.5.0 onwards are vulnerable to a remote
|       code execution vulnerability, allowing a malicious client to upload a
|       shared library to a writable share, and then cause the server to load
|       and execute it.
|
|     Disclosure date: 2017-05-24
|     Check results:
|       Samba Version: 3.X - 4.X
|       Writable share found.
|        Name: \\10.0.2.6\data
|       File written to remote share, but unable to execute payload either due to unknown actual path, or the system ma
y be patched.
|     Extra information:
|       All writable shares:
|        Name: \\10.0.2.6\data
|     References:
|       https://www.samba.org/samba/security/CVE-2017-7494.html
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7494
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: false
| smb-vuln-regsvc-dos:
|   VULNERABLE:
|   Service regsvc in Microsoft Windows systems vulnerable to denial of service
|     State: VULNERABLE
|       The service regsvc in Microsoft Windows 2000 systems is vulnerable to denial of service caused by a null defere
nce
|       pointer. This script will crash the service if it is vulnerable. This vulnerability was discovered by Ron Bowes
|       while working on smb-enum-sessions.
|_

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 82.22 seconds
ustudent@ubu-ustudent:~$
```

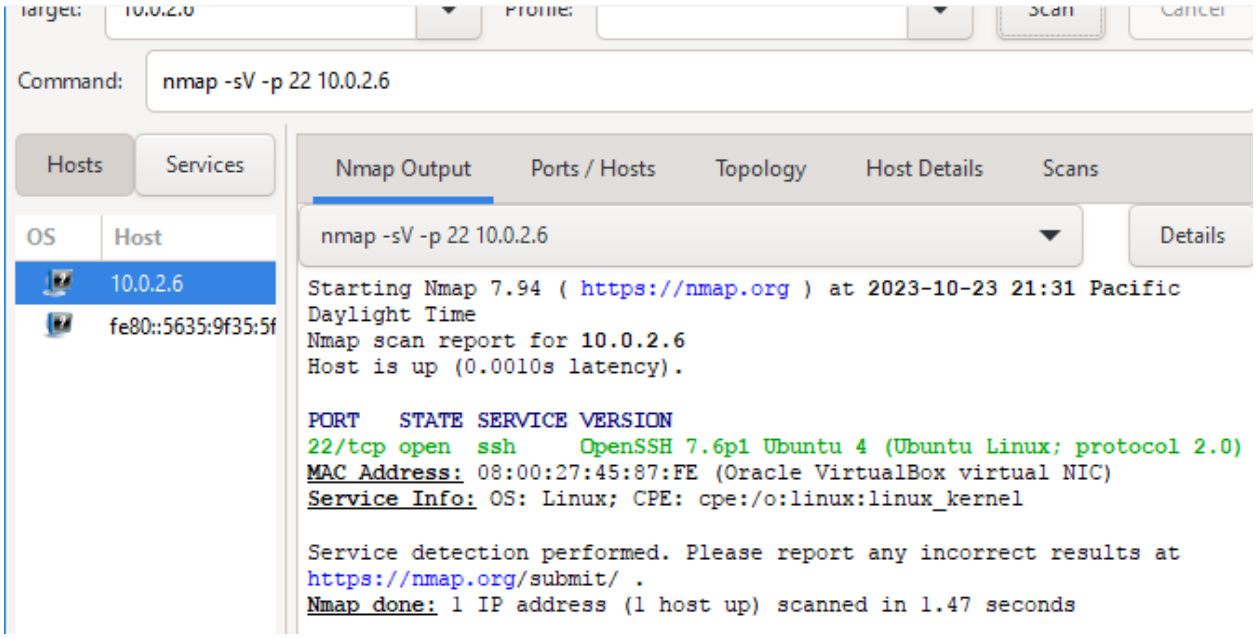
```
SF:L,22,"A\x20is\x20for\x20Apple\.\n\t\t--\x20Hester\x20Pryne\n");
Service Info: Host: Welcome; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-vuln-cve-2017-7494:
|   VULNERABLE:
|   SAMBA Remote Code Execution from Writable Share
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2017-7494
|     Risk factor: HIGH  CVSSv3: 7.5 (HIGH) (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H)
|       All versions of Samba from 3.5.0 onwards are vulnerable to a remote
|       code execution vulnerability, allowing a malicious client to upload a
|       shared library to a writable share, and then cause the server to load
|       and execute it.
|
|     Disclosure date: 2017-05-24
|     Check results:
|       Samba Version: 3.X - 4.X
|       Writable share found.
|        Name: \\10.0.2.6\data
|       File written to remote share, but unable to execute payload either due to unknown actual path, or the system ma
y be patched.
|     Extra information:
|       All writable shares:
|        Name: \\10.0.2.6\data
|     References:
|       https://www.samba.org/samba/security/CVE-2017-7494.html
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7494
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: false
| smb-vuln-regsvc-dos:
|   VULNERABLE:
|   Service regsvc in Microsoft Windows systems vulnerable to denial of service
|     State: VULNERABLE
|       The service regsvc in Microsoft Windows 2000 systems is vulnerable to denial of service caused by a null defere
nce
|       pointer. This script will crash the service if it is vulnerable. This vulnerability was discovered by Ron Bowes
|       while working on smb-enum-sessions.
|_

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 82.22 seconds
ustudent@ubu-ustudent:~$
```

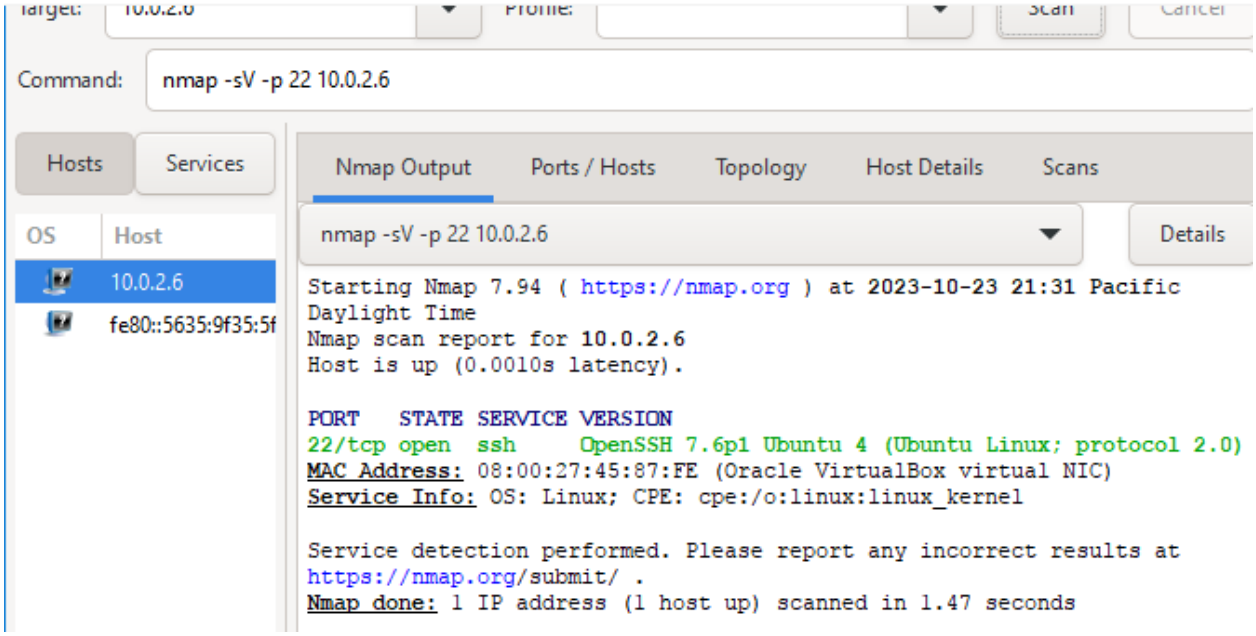
Also we use Zenmap to scan the target IPv6 address on both windows and ubuntu machine





- To Discover Unpatched Services on the Linux machine, run the following commands to examine ssh and samba services:





We also able to discover unpatched services on the Linux system as well

```
ustudent@ubu-ustudent:~$ ssh -v localhost
OpenSSH_7.6p1 Ubuntu-4, OpenSSL 1.0.2n  7 Dec 2017
debug1: Reading configuration data /etc/ssh/ssh_config
debug1: /etc/ssh/ssh_config line 19: Applying options for *
debug1: Connecting to localhost [127.0.0.1] port 22.
debug1: Connection established.
debug1: key_load_public: No such file or directory
debug1: identity file /home/ustudent/.ssh/id_rsa type -1
debug1: key_load_public: No such file or directory
debug1: identity file /home/ustudent/.ssh/id_rsa-cert type -1
debug1: key_load_public: No such file or directory
debug1: identity file /home/ustudent/.ssh/id_dsa type -1
debug1: key_load_public: No such file or directory
debug1: identity file /home/ustudent/.ssh/id_dsa-cert type -1
debug1: key_load_public: No such file or directory
debug1: identity file /home/ustudent/.ssh/id_ecdsa type -1
debug1: key_load_public: No such file or directory
debug1: identity file /home/ustudent/.ssh/id_ecdsa-cert type -1
debug1: key_load_public: No such file or directory
debug1: identity file /home/ustudent/.ssh/id_ed25519 type -1
debug1: key_load_public: No such file or directory
debug1: identity file /home/ustudent/.ssh/id_ed25519-cert type -1
debug1: Local version string SSH-2.0-OpenSSH_7.6p1 Ubuntu-4
debug1: Remote protocol version 2.0, remote software version OpenSSH_7.6p1 Ubuntu-4
debug1: match: OpenSSH_7.6p1 Ubuntu-4 pat OpenSSH* compat 0x04000000
debug1: Authenticating to localhost:22 as 'ustudent'
debug1: SSH2_MSG_KEXINIT sent
debug1: SSH2_MSG_KEXINIT received
debug1: kex: algorithm: curve25519-sha256
debug1: kex: host key algorithm: ecdsa-sha2-nistp256
debug1: kex: server->client cipher: chacha20-poly1305@openssh.com MAC: <implicit> compression: none
debug1: kex: client->server cipher: chacha20-poly1305@openssh.com MAC: <implicit> compression: none
debug1: expecting SSH2_MSG_KEX_ECDH_REPLY
debug1: Server host key: ecdsa-sha2-nistp256 SHA256:flnAOpTUWlE3VGiuIyzXte9x1VmRePvuqlWNL1JxlUk
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:flnAOpTUWlE3VGiuIyzXte9x1VmRePvuqlWNL1JxlUk.
Are you sure you want to continue connecting (yes/no)? no
Host key verification failed.
ustudent@ubu-ustudent:~$ samba --version
Version 4.7.6-Ubuntu
```

- From the above procedures we can clear see they are not the most updated version of the SSH and SAMBA versions. OpenSSH 7.6 can be upgraded to OpenSSH 8 and CVE-2020-1472 is the recent security update for this SAMBA version.

Task 2

Let's get started on our assessment. We need to find out if software updates and third-party packages settings are correct. Verify in both of your hosts the following checks.
Are software updates for the systems and third parties configured correctly in these systems?
What is your assessment of StaticSpeeds systems configuration for software updates and third-party packages? Please provide evidence to support your evaluation (command line output or screenshots for each as well)

Windows CIS 18.9.102.2

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

Ubuntu CIS 1.2.1

Ensure package manager repositories are configured correctly.

On ubuntu we can check software update by the following commands:

sudo apt-cache policy

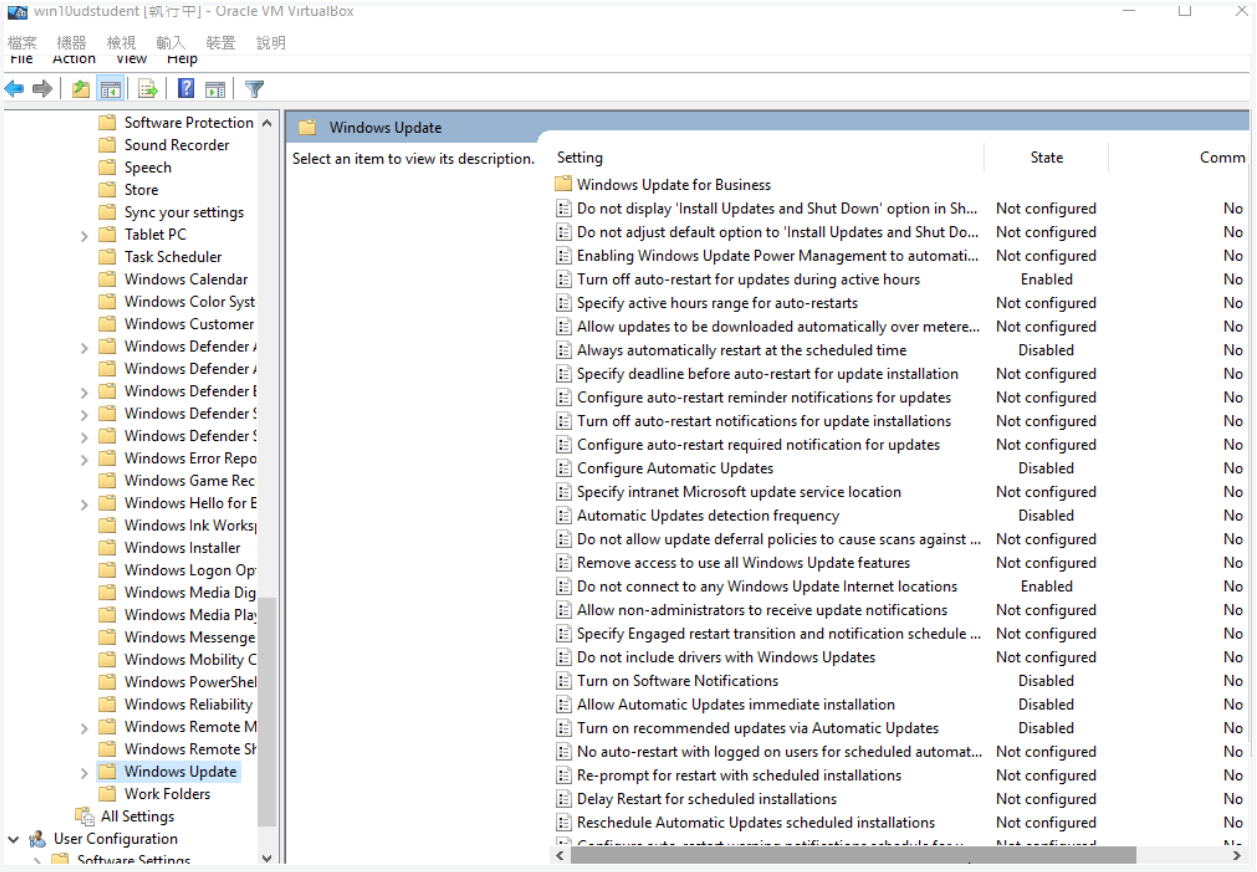
```
ustudent@ubu-ustudent:~$ sudo apt-cache policy
[sudo] password for ustudent:
Package files:
 100 /var/lib/dpkg/status
     release a=now
 500 http://us.archive.ubuntu.com/ubuntu bionic/multiverse i386 Packages
     release v=18.04,o=Ubuntu,a=bionic,n=bionic,l=Ubuntu,c=multiverse,b=i386
     origin us.archive.ubuntu.com
 500 http://us.archive.ubuntu.com/ubuntu bionic/multiverse amd64 Packages
     release v=18.04,o=Ubuntu,a=bionic,n=bionic,l=Ubuntu,c=multiverse,b=amd64
     origin us.archive.ubuntu.com
 500 http://us.archive.ubuntu.com/ubuntu bionic/universe i386 Packages
     release v=18.04,o=Ubuntu,a=bionic,n=bionic,l=Ubuntu,c=universe,b=i386
     origin us.archive.ubuntu.com
 500 http://us.archive.ubuntu.com/ubuntu bionic/universe amd64 Packages
     release v=18.04,o=Ubuntu,a=bionic,n=bionic,l=Ubuntu,c=universe,b=amd64
     origin us.archive.ubuntu.com
 500 http://us.archive.ubuntu.com/ubuntu bionic/restricted i386 Packages
     release v=18.04,o=Ubuntu,a=bionic,n=bionic,l=Ubuntu,c=restricted,b=i386
     origin us.archive.ubuntu.com
 500 http://us.archive.ubuntu.com/ubuntu bionic/restricted amd64 Packages
     release v=18.04,o=Ubuntu,a=bionic,n=bionic,l=Ubuntu,c=restricted,b=amd64
     origin us.archive.ubuntu.com
 500 http://us.archive.ubuntu.com/ubuntu bionic/main i386 Packages
     release v=18.04,o=Ubuntu,a=bionic,n=bionic,l=Ubuntu,c=main,b=i386
     origin us.archive.ubuntu.com
 500 http://us.archive.ubuntu.com/ubuntu bionic/main amd64 Packages
     release v=18.04,o=Ubuntu,a=bionic,n=bionic,l=Ubuntu,c=main,b=amd64
     origin us.archive.ubuntu.com
```

Or

sudo apt-key list

```
ustudent@ubu-ustudent:~$ sudo apt-key list
/etc/apt/trusted.gpg.d/ubuntu-keyring-2012-archive.gpg
------------------------------------------------------
pub   rsa4096 2012-05-11 [SC]
      790B C727 7767 219C 42C8  6F93 3B4F E6AC C0B2 1F32
uid           [ unknown] Ubuntu Archive Automatic Signing Key (2012) <ftpmaster
@ubuntu.com>

/etc/apt/trusted.gpg.d/ubuntu-keyring-2012-cdimage.gpg
------------------------------------------------------
pub   rsa4096 2012-05-11 [SC]
      8439 38DF 228D 22F7 B374  2BC0 D94A A3F0 EFE2 1092
uid           [ unknown] Ubuntu CD Image Automatic Signing Key (2012) <cdimage@
ubuntu.com>
```

We check the status of software updates In Group Policy Object Editor, click either of the Administrative Templates > Windows components > Windows Update.

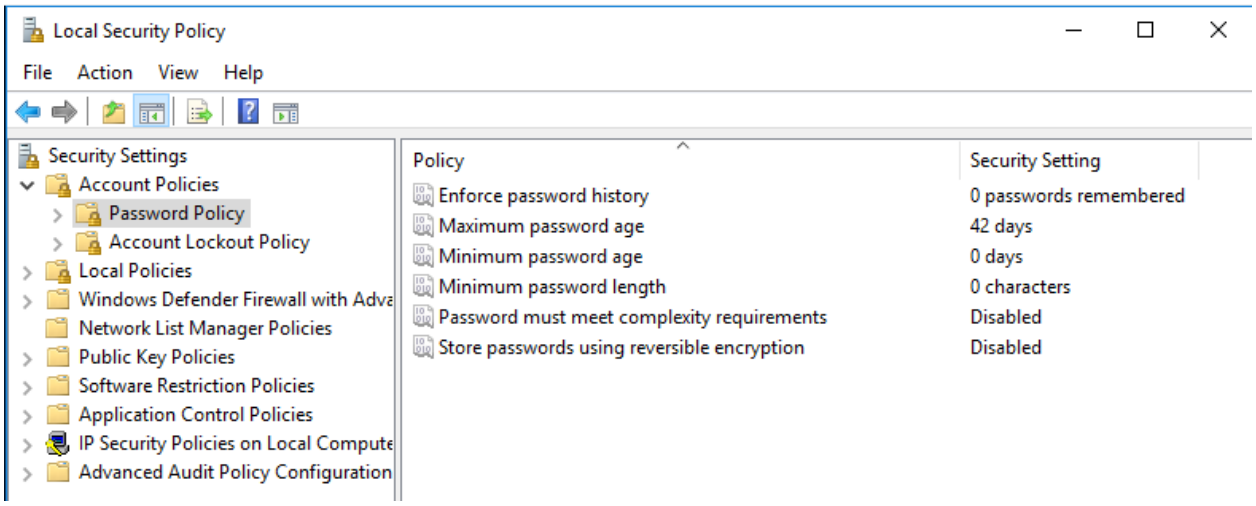


We audit StaticSpeeds systems by the following commands on Linux:

`grep 'minlen' /etc/security/pwquality.conf`

```
ustudent@ubu-ustudent:~$ grep 'minlen' /etc/security/pwquality.conf
# minlen = 8
ustudent@ubu-ustudent:~$
```

On Windows:
We can view password policies by searching for "Local Security Policy" using the windows search feature, and navigating to "Account Policy" > "Password Policy"



Task 3- Native Protections and Software Inventory

Next, verify that native protections for the operating systems are enough to protect systems from exploitation. (Hint: Think upgrades) We also need to know exactly what software is running on every machine. Also, please perform a software inventory on each computer and post your findings. The more you know about the systems you are defending, the better chance you will mitigate and harden them.

Windows CIS 18.3.4

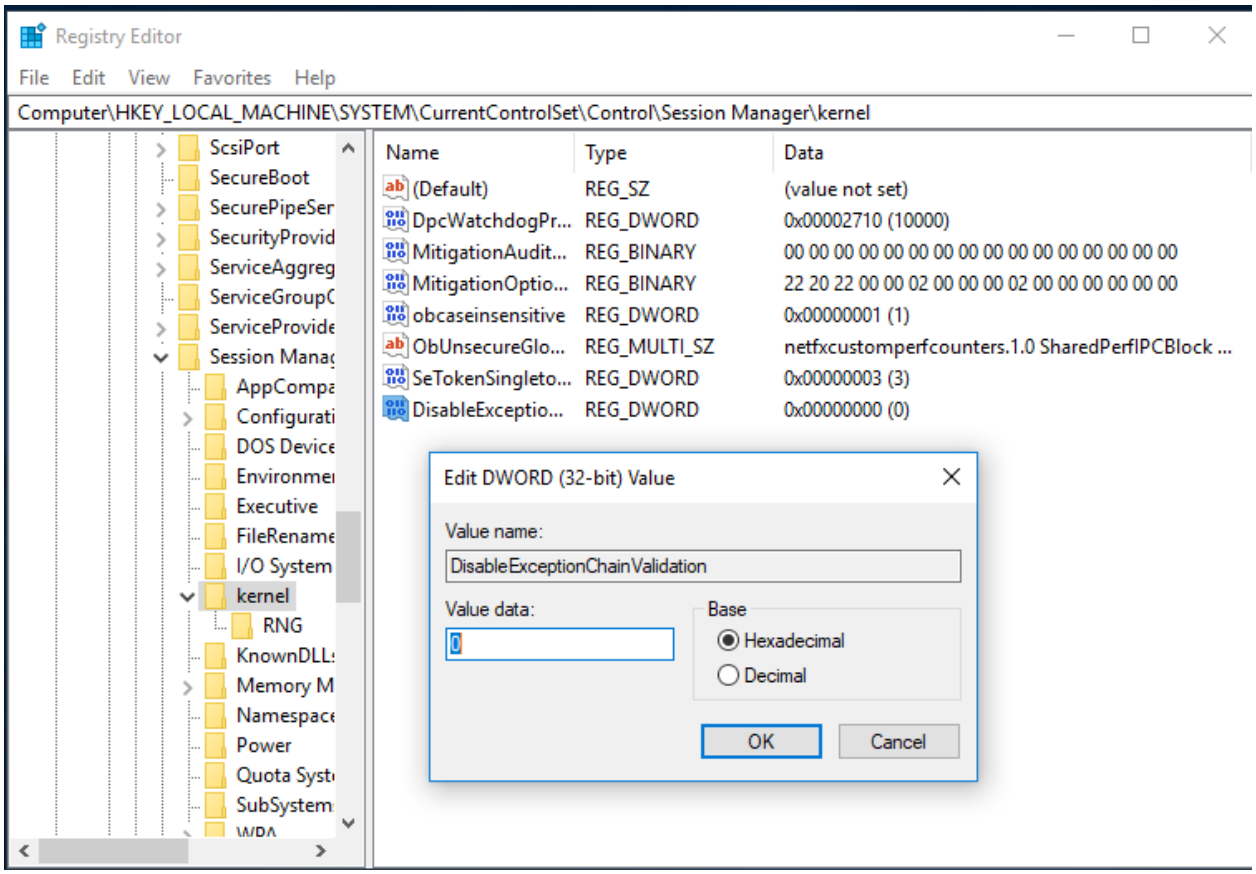
Ensure 'Enable Structured Exception Handling Overwrite Protection (SEHOP)' is set to 'Enabled.'

1. Click **Start**, click **Run**, type regedit, and then press ENTER.
2. Locate the following registry subkey:
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\kernel\DisableExceptionChainValidation Note If you cannot find the **DisableExceptionChainValidation** registry entry under the **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\kernel** subkey, follow these steps to create it:

   1. Right-click **kernel**, point to
      New, and then click **DWORD Value**.

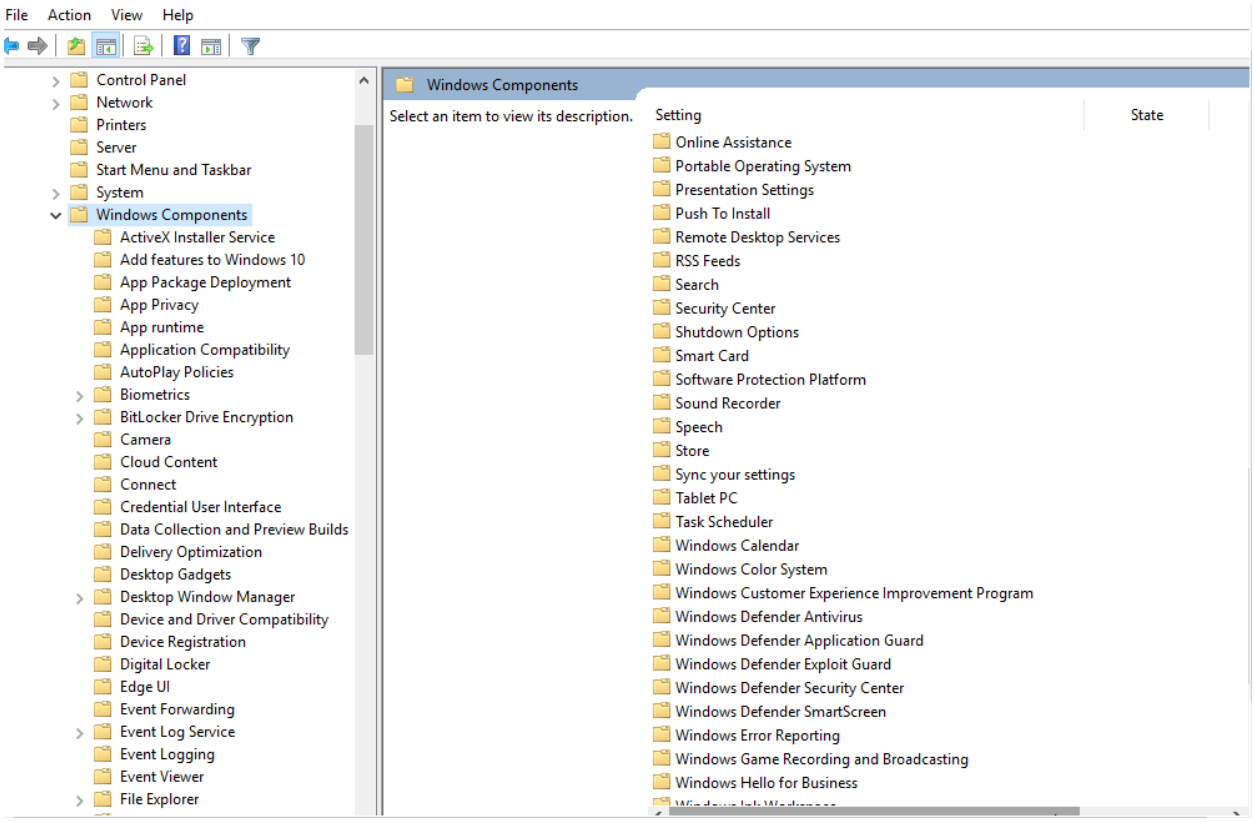
2. Type
   DisableExceptionChainValidation, and then press ENTER.
3. Double-click
   DisableExceptionChainValidation.
4. Change the value of the **DisableExceptionChainValidation** registry entry to 0 to enable it, and then click **OK**.

   Note A value of 1 disables the registry entry. A value of 0 enables it.
5. Exit Registry Editor.



Is this system compliant?

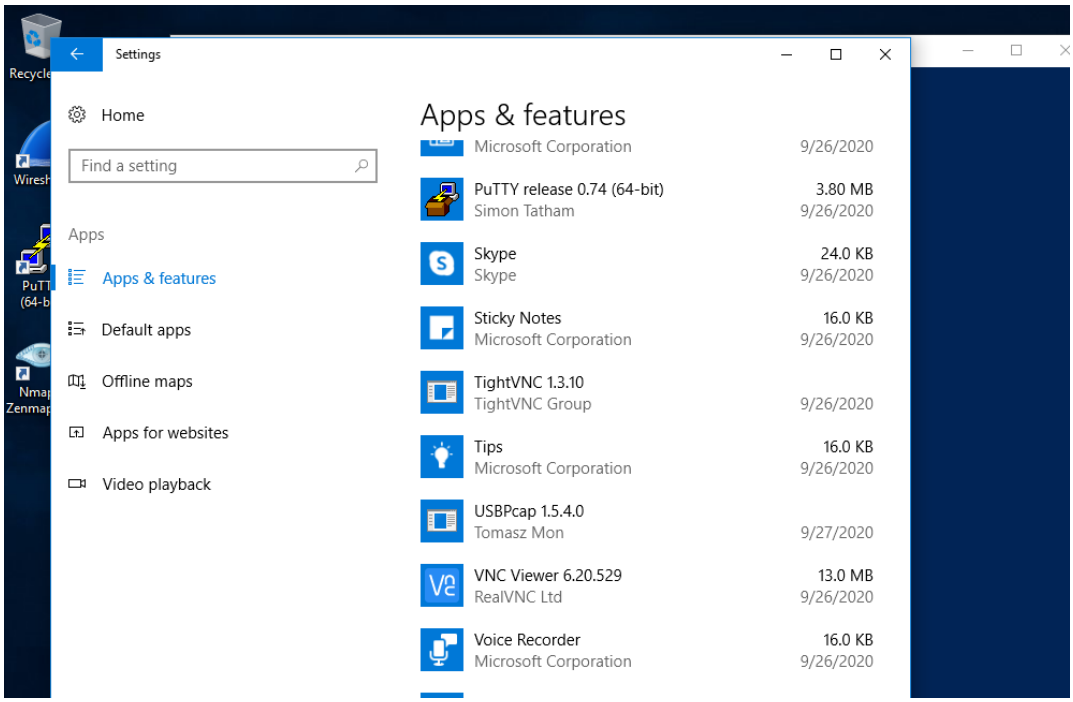
Ans: No, The path from CIS is not exsist. An additional group policy template is required to add MS security group. The registry entry “DisableExceptionChainValidation” is not available.



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

Is VNC viewer installed in this Windows System?

Yes.



Ubuntu CIS 1.6.1, 1.6.2

1.6.1 Ensure XD/NX support is enabled

journalctl | grep 'protection: active'

```
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 19:42:51 ubu-ustudent kernel: NX (Execute Disable) protection: active
Sep 27 09:42:18 ubu-ustudent kernel: NX (Execute Disable) protection: active
Sep 27 10:25:06 ubu-ustudent kernel: NX (Execute Disable) protection: active
Sep 27 10:29:55 ubu-ustudent kernel: NX (Execute Disable) protection: active
Sep 27 11:04:27 ubu-ustudent kernel: NX (Execute Disable) protection: active
Sep 27 11:07:41 ubu-ustudent kernel: NX (Execute Disable) protection: active
Sep 27 11:50:26 ubu-ustudent kernel: NX (Execute Disable) protection: active
Sep 27 21:29:42 ubu-ustudent kernel: NX (Execute Disable) protection: active
Sep 28 11:55:22 ubu-ustudent kernel: NX (Execute Disable) protection: active
Sep 28 12:42:02 ubu-ustudent kernel: NX (Execute Disable) protection: active
Sep 28 22:35:02 ubu-ustudent kernel: NX (Execute Disable) protection: active
Oct 19 23:13:45 ubu-ustudent kernel: NX (Execute Disable) protection: active
Oct 21 01:36:43 ubu-ustudent kernel: NX (Execute Disable) protection: active
Oct 21 01:38:55 ubu-ustudent kernel: NX (Execute Disable) protection: active
Oct 21 22:51:47 ubu-ustudent kernel: NX (Execute Disable) protection: active
Oct 21 22:58:19 ubu-ustudent kernel: NX (Execute Disable) protection: active
Oct 23 20:44:23 ubu-ustudent kernel: NX (Execute Disable) protection: active
Oct 23 21:18:48 ubu-ustudent kernel: NX (Execute Disable) protection: active
Nov 02 09:20:28 ubu-ustudent kernel: NX (Execute Disable) protection: active
Nov 03 06:28:08 ubu-ustudent kernel: NX (Execute Disable) protection: active
Nov 04 05:08:31 ubu-ustudent kernel: NX (Execute Disable) protection: active
```

1.6.2 Ensure address space layout randomization (ASLR) is enabled

Run the following command:

kernel.randomize_va_space = 2

```
ustudent@ubu-ustudent:~$ sysctl kernel.randomize_va_space
kernel.randomize_va_space = 2
ustudent@ubu-ustudent:~$
```

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?

Yes.

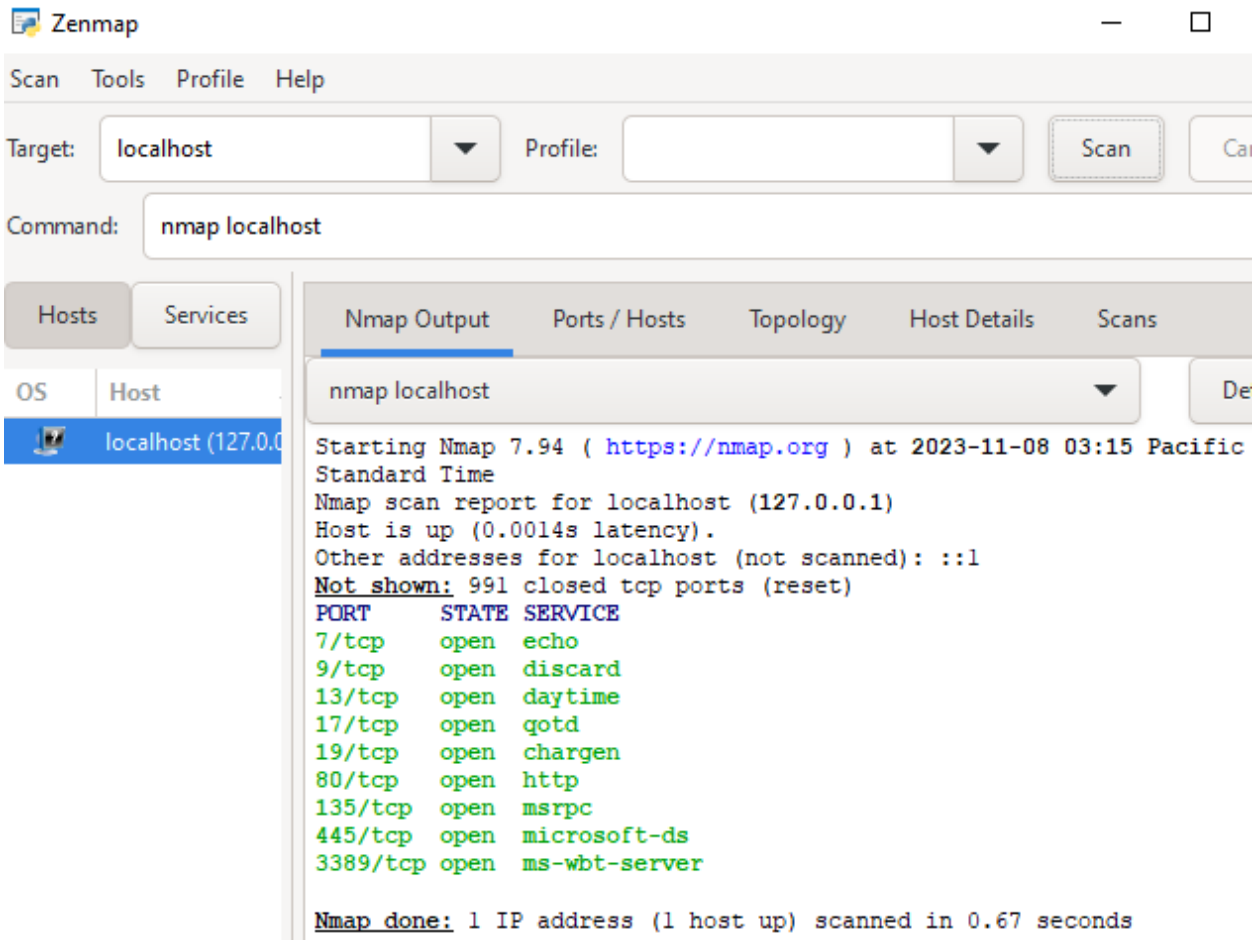
```
ustudent@ubu-ustudent:~$ dpkg -l | grep vnc
ii  libvncclient1:amd64                          0.9.11+dfsg-1ubuntu1
    amd64        API to write one's own VNC server - client library
ii  remmina-plugin-vnc:amd64                     1.2.0-rcgit.29+dfsg-1ubuntu1
    amd64        VNC plugin for Remmina
ii  tightvncserver                               1.3.10-0ubuntu4
    amd64        virtual network computing server software
ii  xtightvncviewer                              1.3.10-0ubuntu4
    amd64        virtual network computing client software for X
ustudent@ubu-ustudent:~$
```

Do these applications, both for Windows and Ubuntu, bring added risks to these systems? Please provide proof and reasoning for your answer.

Task 4

Perform a network asset inventory using Nmap to identify VMs with open ports on both Windows and Linux

```
ustudent@ubu-ustudent:~$ nmap -sV --script vuln 10.0.2.6

Starting Nmap 7.60 ( https://nmap.org ) at 2023-10-23 22:56 EDT
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for ubu-ustudent (10.0.2.6)
Host is up (0.00017s latency).
Not shown: 991 closed ports
PORT    STATE SERVICE     VERSION
13/tcp  open  daytime
17/tcp  open  qotd?
| fingerprint-strings:
|   NULL:
|     A is for Apple.
|_    Hester Pryne
21/tcp  open  ftp         vsftpd 2.0.8 or later
|_sslv2-drown:
22/tcp  open  ssh         OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
23/tcp  open  telnet      Linux telnetd
37/tcp  open  time        (32 bits)
|_rfc868-time: 2023-10-24T02:57:52
80/tcp  open  http        Apache httpd 2.4.29 ((Ubuntu))
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint
 at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port17-TCP:V=7.60%I=7%D=10/23%Time=653732A2%P=x86_64-pc-linux-gnu%r(NUL
SF:L,22,"A\x20is\x20for\x20Apple\.\n\t\t--\x20Hester\x20Pryne\n");
Service Info: Host: Welcome; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-vuln-cve-2017-7494:
|   VULNERABLE:
|   SAMBA Remote Code Execution from Writable Share
|     State: LIKELY VULNERABLE
```



What is your assessment of the Asset Inventory and what recommendations do you have to mitigate any potential issues. Please provide evidence to support your findings.

Step 2: Assess Access Management at Targeted Assets

Task 1

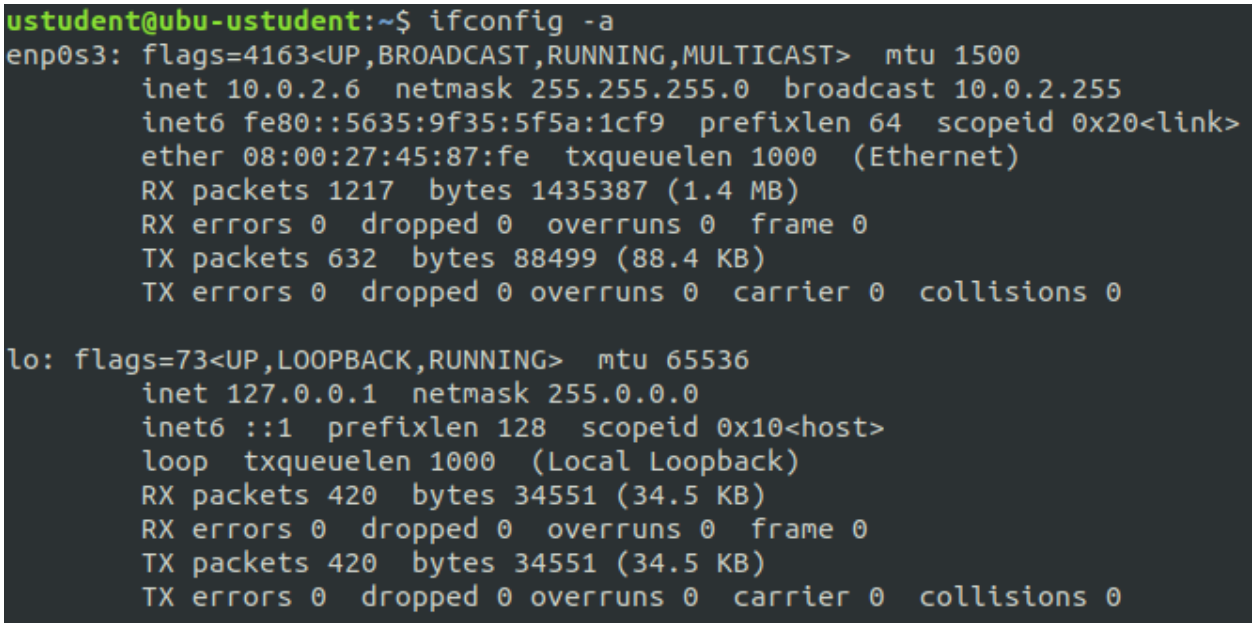
Check for current settings on Network Segmentation, VLANs, Domain Isolation, or IP Security Policies.

After completing your checks, what is your assessment of these settings? What recommendations do you have to improve the settings? Remember to provide evidence to back up your thoughts. Things to consider on both Ubuntu and Windows:

- Are there any VLANs?
- Are there any policies in place?
    - If there are any, are they applied?
- Is Anonymous access granted to any share?

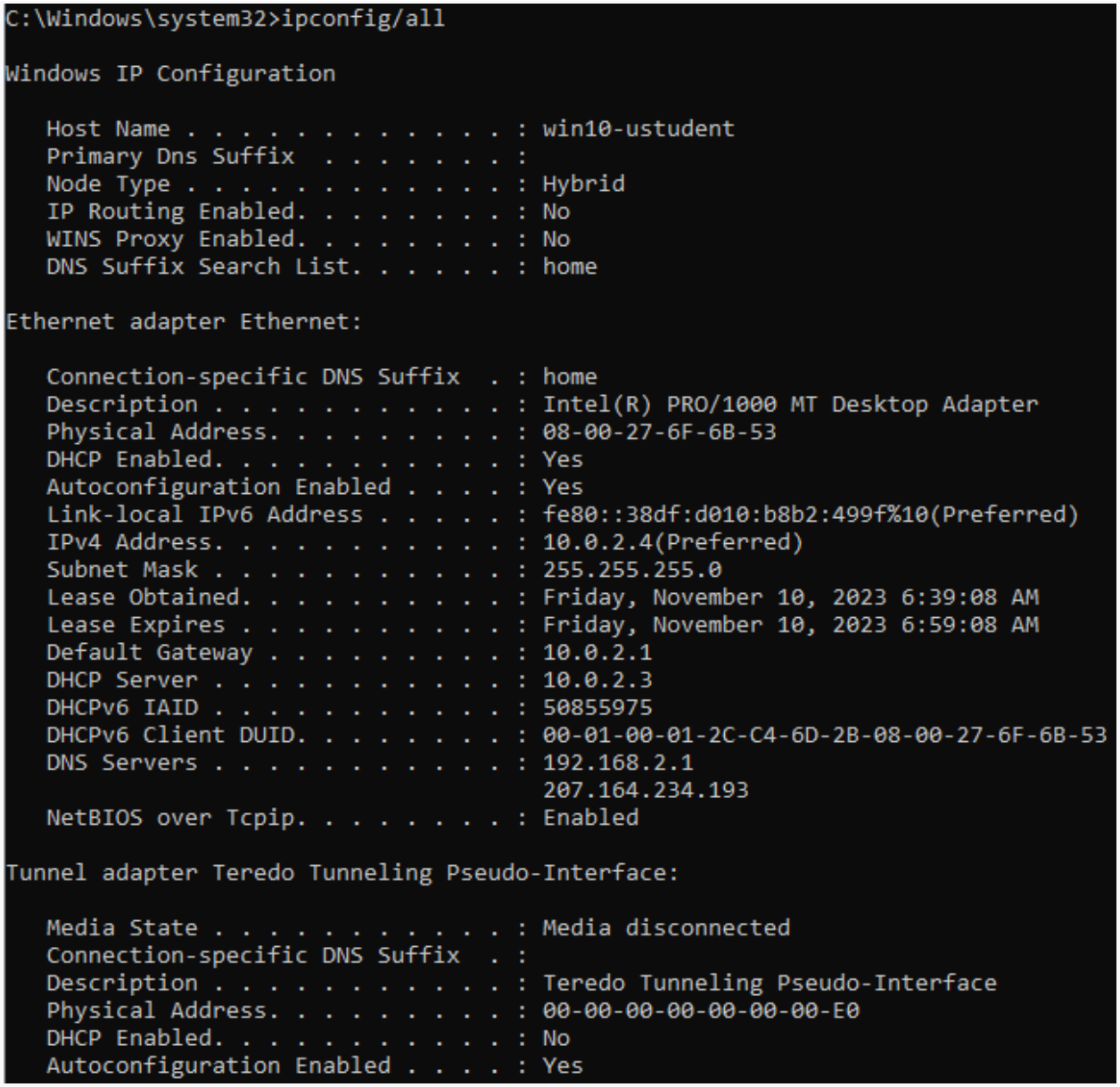
VLAN hints:
Ubuntu: look under /etc/network/interfaces
Windows: Look under properties of network adapter or Cmdlet
Get-NetAdapter|Format-List*, secpol.msc (please provide screenshots)

I don't see any VLANs in the following screenshots.
Linux
ifconfig -a



Windows

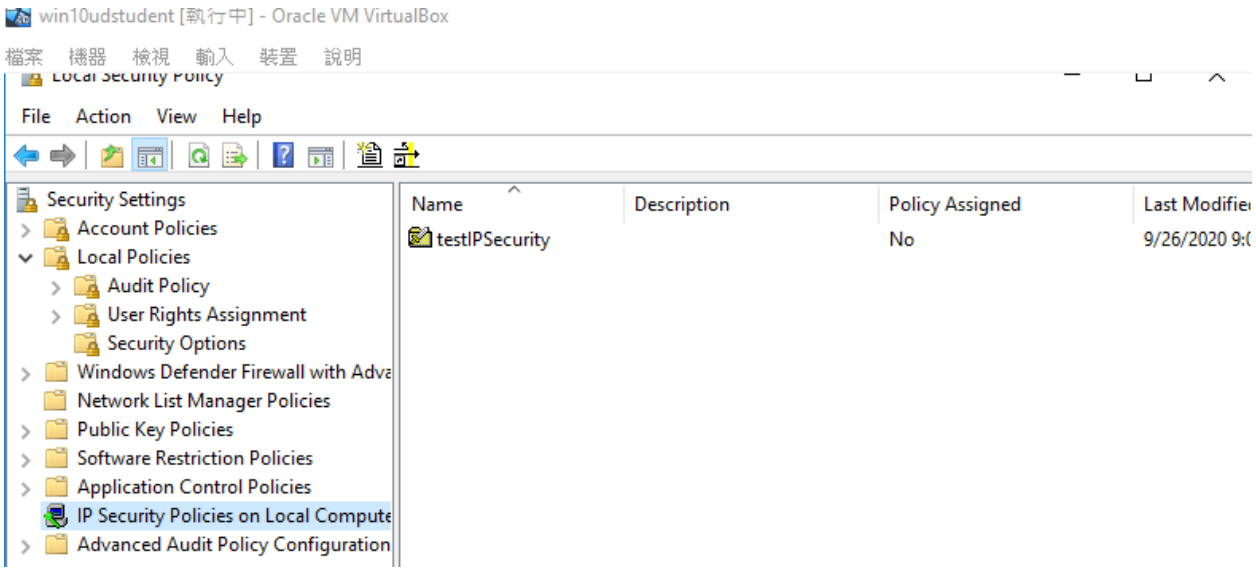
ipconfig /all



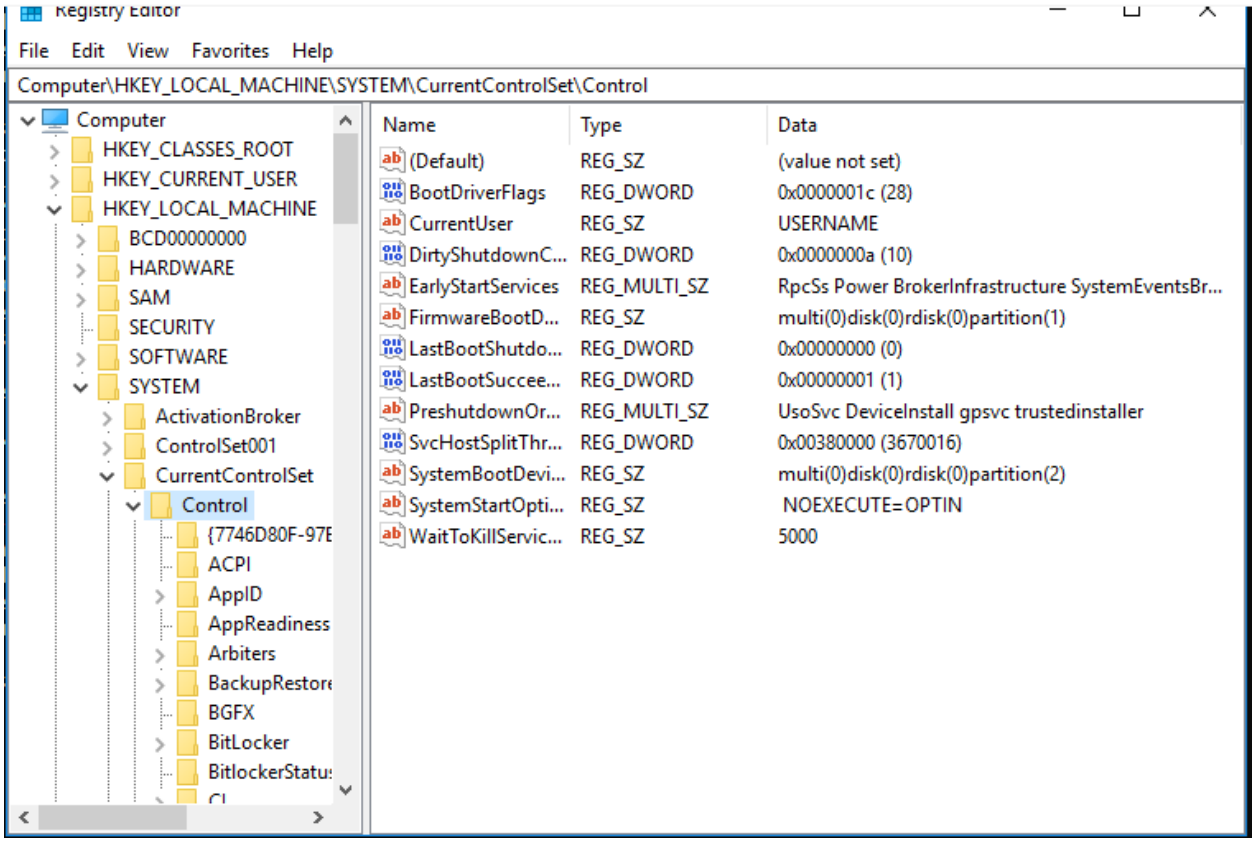
```
C:\Windows\system32>ipconfig/all

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. . . . . . : home

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : home
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
   Physical Address. . . . . . . . . : 08-00-27-6F-6B-53
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::38df:d010:b8b2:499f%10(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.0.2.4(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Friday, November 10, 2023 6:39:08 AM
   Lease Expires . . . . . . . . . . : Friday, November 10, 2023 6:59:08 AM
   Default Gateway . . . . . . . . . : 10.0.2.1
   DHCP Server . . . . . . . . . . . : 10.0.2.3
   DHCPv6 IAID . . . . . . . . . . . : 50855975
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2C-C4-6D-2B-08-00-27-6F-6B-53
   DNS Servers . . . . . . . . . . . : 192.168.2.1
                                       207.164.234.193
   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. . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
```

There’s no any policy in the following screenshots:

```
ustudent@ubu-ustudent:~$ cat /etc/hosts.allow
# /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.
#

ustudent@ubu-ustudent:~$ cat /etc/hosts.deny
# /etc/hosts.deny: list of hosts that are _not_ allowed to access the system.
#                  See the manual pages hosts_access(5) and hosts_options(5).
#
# Example:    ALL: some.host.name, .some.domain
#             ALL EXCEPT in.fingerd: other.host.name, .other.domain
#
# 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.
#
# The PARANOID wildcard matches any host whose name does not match its
# address.
#
# You may wish to enable this to ensure any programs that don't
# validate looked up hostnames still leave understandable logs. In past
# versions of Debian this has been the default.
# ALL: PARANOID
```



From the following screenshots we can see the anonymous access has not been granted.



Task 2

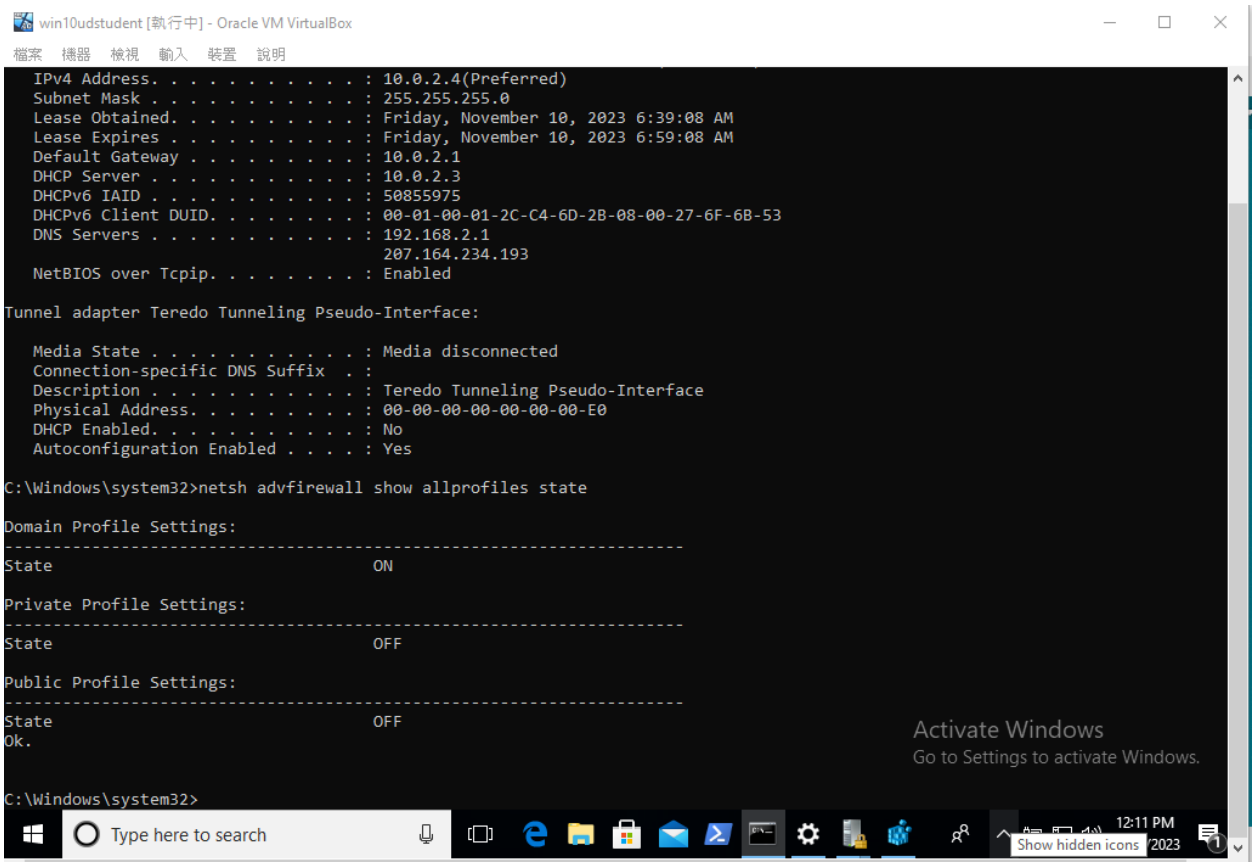
Investigate and assess the remote access services and protocols in place for StaticSpeed and determine their security level. After completing your investigation, including your assessment of how StaticSpeed is doing with remote access. Please have evidence to support your findings. Remember to consider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

Task 3

NuttyUtility only needs remote access ports for administrators on workstations. What is your assessment of the firewalls in StaticSpeed's systems? Please include evidence to support your thoughts. We need to know if the firewalls are configured correctly?
Also, what ports would you suggest to have open and running and why?

On windows we check firewall status by the following command:

`netsh advfirewall show allprofiles state`



On Ubuntu we use the following command:

`ufw status`

```
ustudent@ubu-ustudent:~$ ufw status
ERROR: You need to be root to run this script
ustudent@ubu-ustudent:~$ sudo ufw status
[sudo] password for ustudent:
Status: inactive
ustudent@ubu-ustudent:~$
```

Task 4

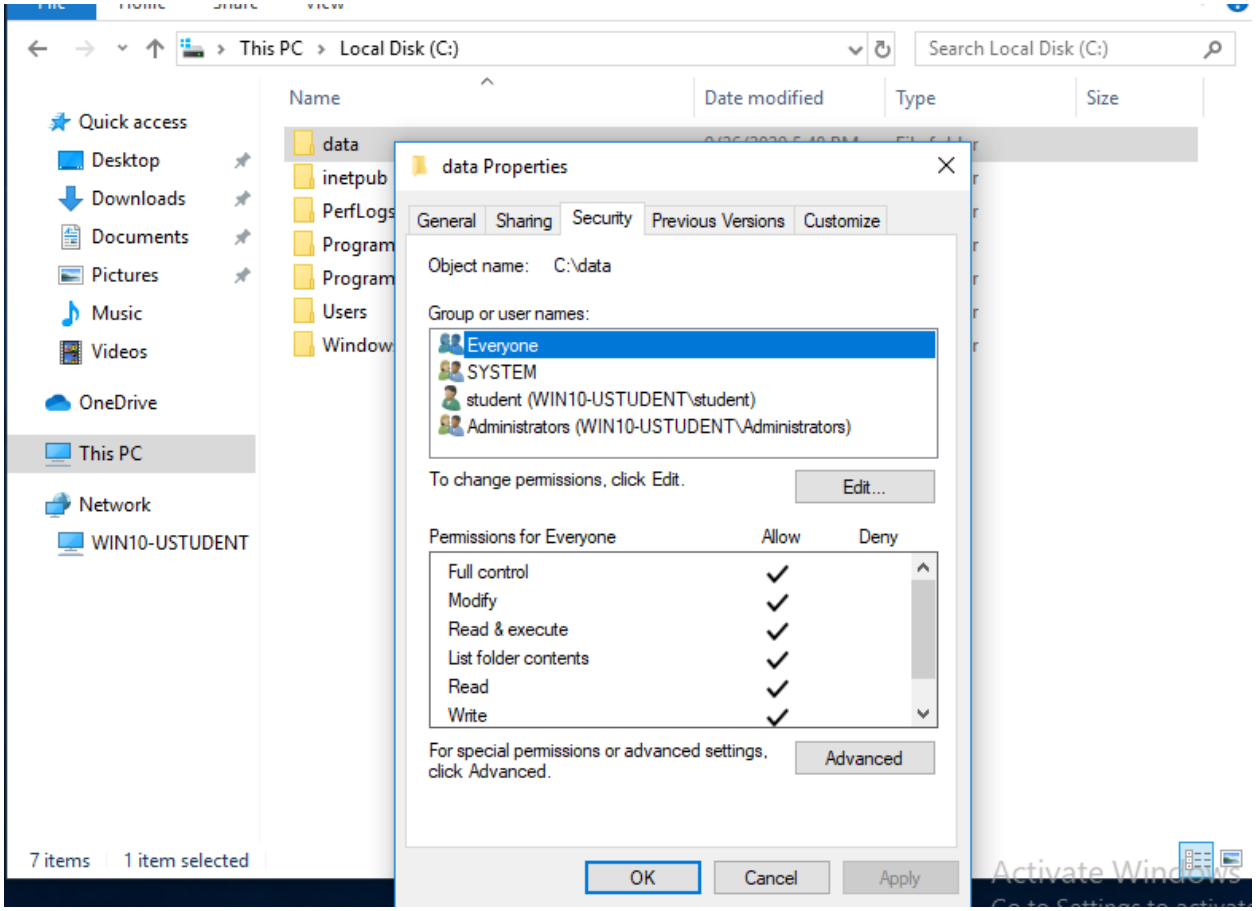
Next, conduct a Principles of Least Privilege assessment of StaticSpeed's system. We need to know:

- 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.

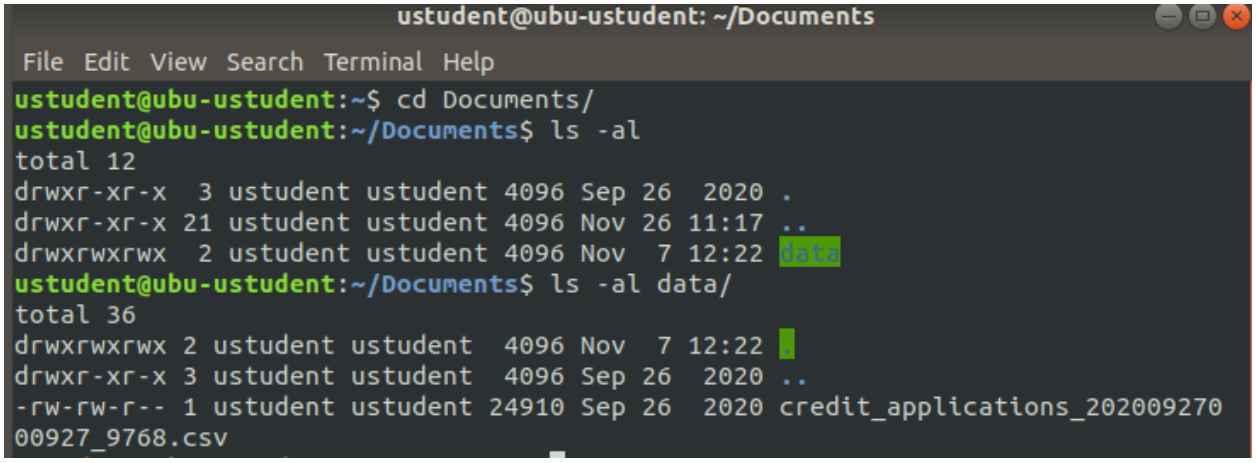
- Are there "guest" accounts enabled? Are they allowed to use Sudo commands? Are they allowed to log in to ALL workstations?.

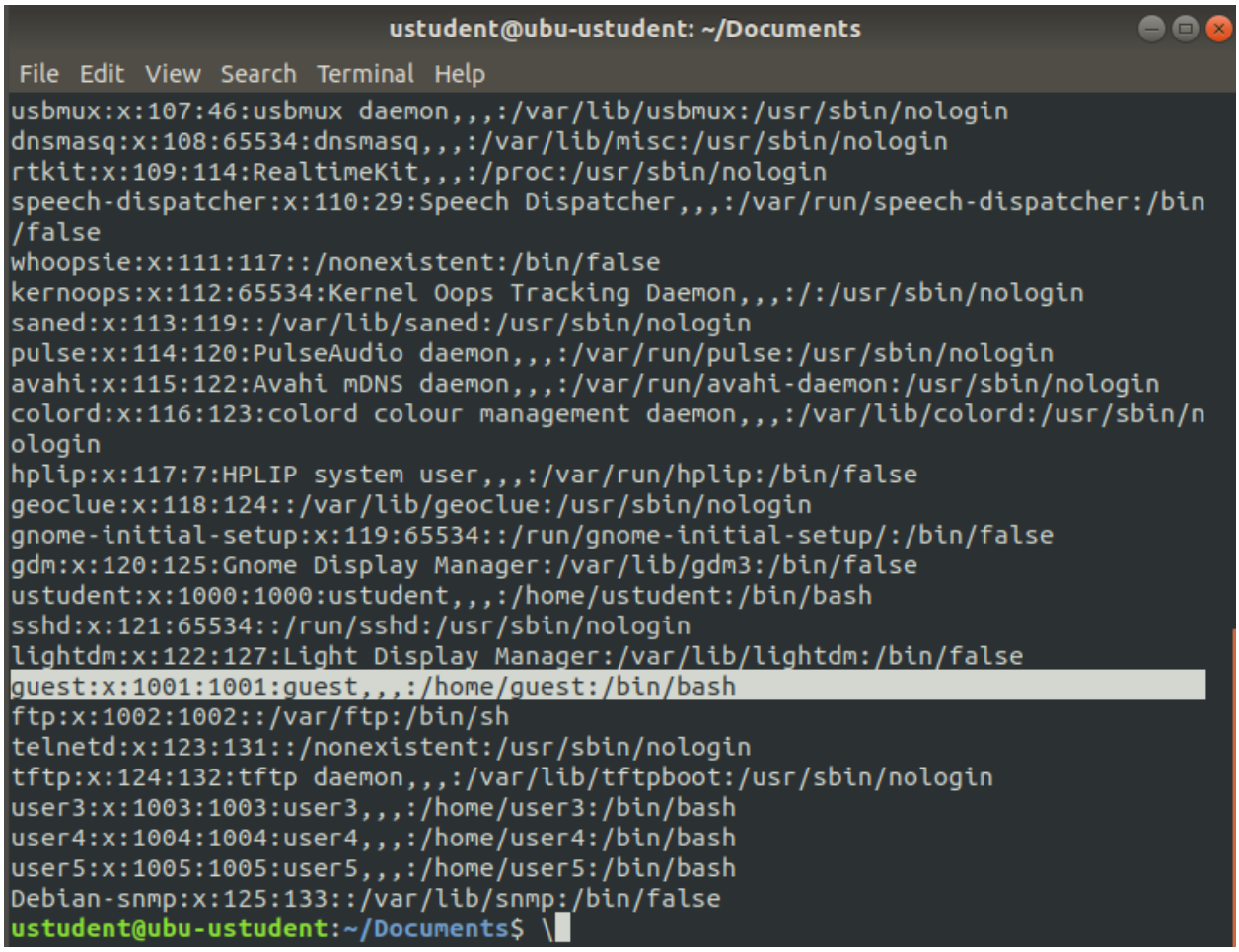
Based on your findings, what should be done to secure these accounts and permissions better? Please provide proof of your results and provide reasoning for your answer.

In windows, In windows locat “data” folder under "This PC" and see the properties and permissions it has.

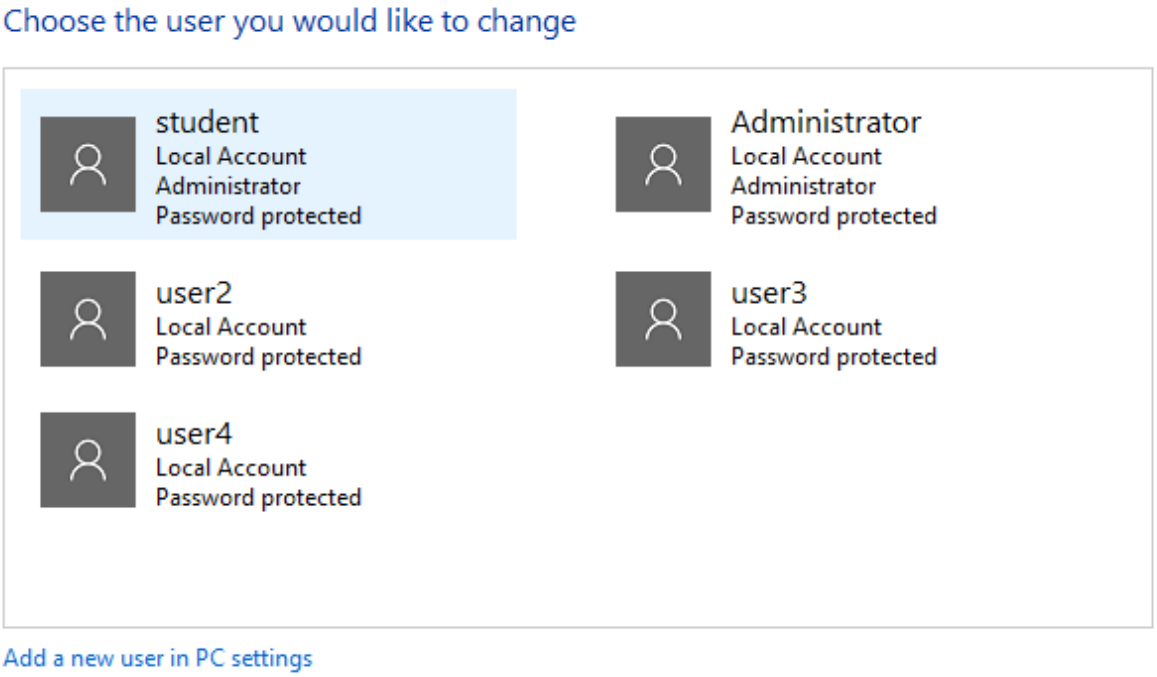


We can find this folder "data" in documents in linux.





From the above screenshots we can see ustudent have the high privileges for both windows and ubuntu machine. There's "guest" accounts enabled you can see it from the above ubuntu screenshots. There's no guest account in windows machine from below screenshots.




```
ustudent@ubu-ustudent:~$ getent group |grep admin
lpadmin:x:116:ustudent
ustudent@ubu-ustudent:~$ getent group |grep sudo
sudo:x:27:ustudent
ustudent@ubu-ustudent:~$
```

From above screenshot we can see ubuntu guest doesn't has administrator privileges.

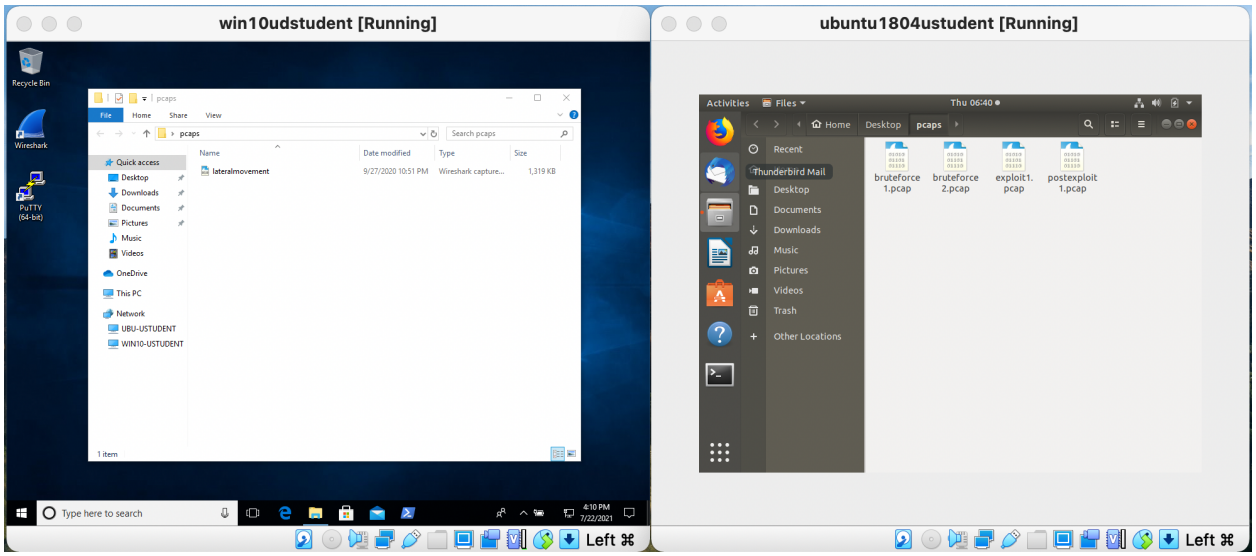
Step 3: Log Monitoring Setup for Detection at Targeted Assets

StaticSpeed has provided access to a monitoring device that has recorded some traffic marked as malicious. Please investigate and assess this further using Wireshark or tcpdump and the provided capture files (pcaps). It is also required of you to verify that appropriate logging is in place at your machines.
Complete your assessment of this traffic. Then, add your suggestions on any issues and improvements by following the steps below. Remember to provide evidence to support your work and recommendations.

Task 1

In this audit, use the pcaps named bruteforce2.pcap and lateralmovement.pcap, along with the other pcaps that may provide more insight into StaticSpeed's network. We recommend focusing on bruteforce2.pcap.

The snapshot below shows the list of pcap files present in both machines.

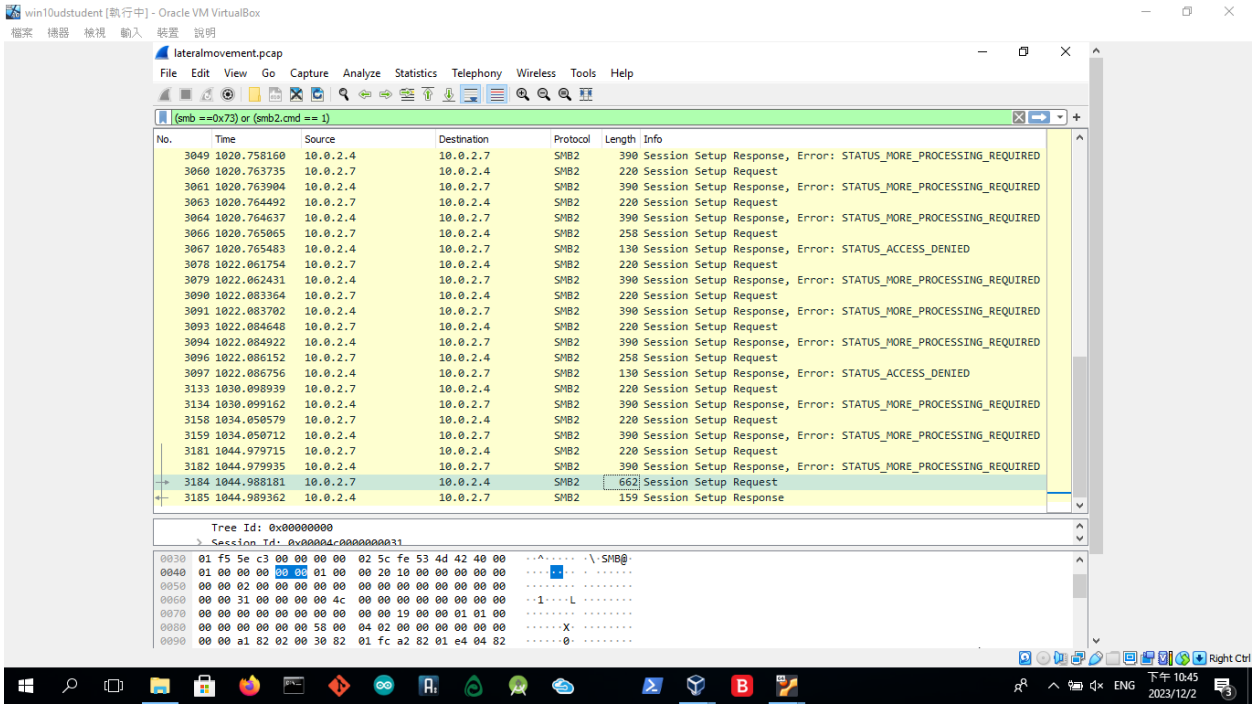


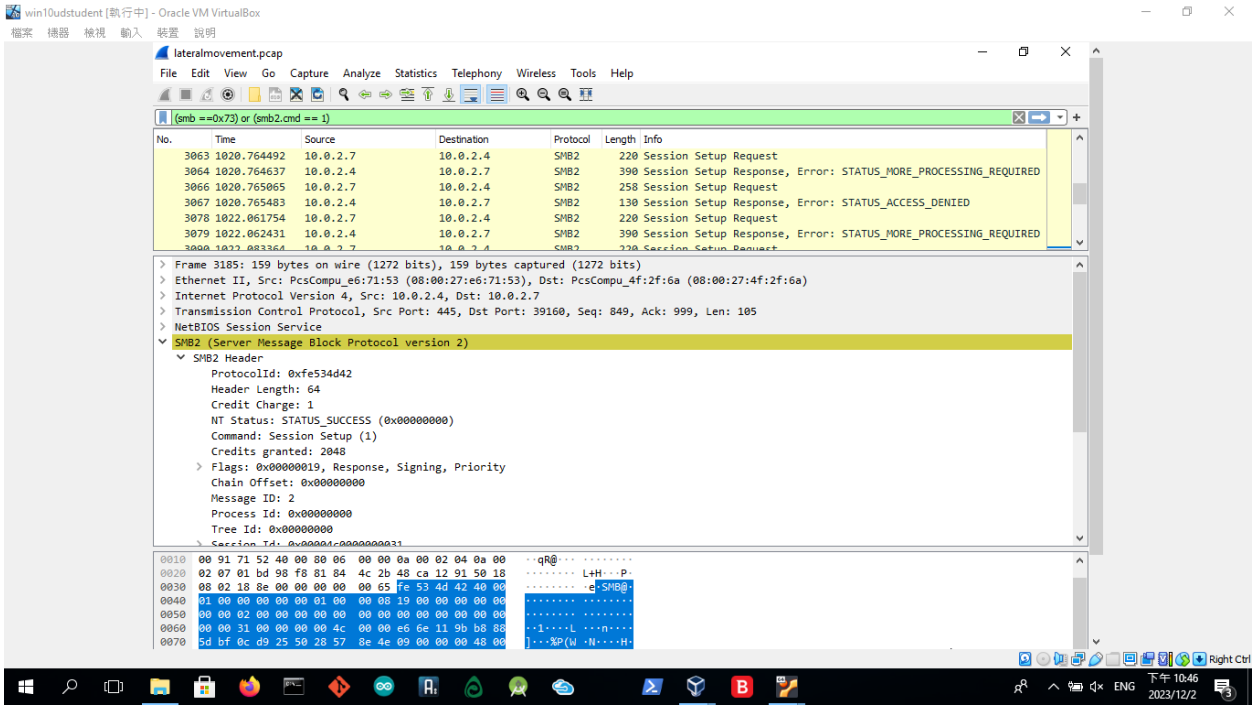
Use the pcap file to assess and determine the following:

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

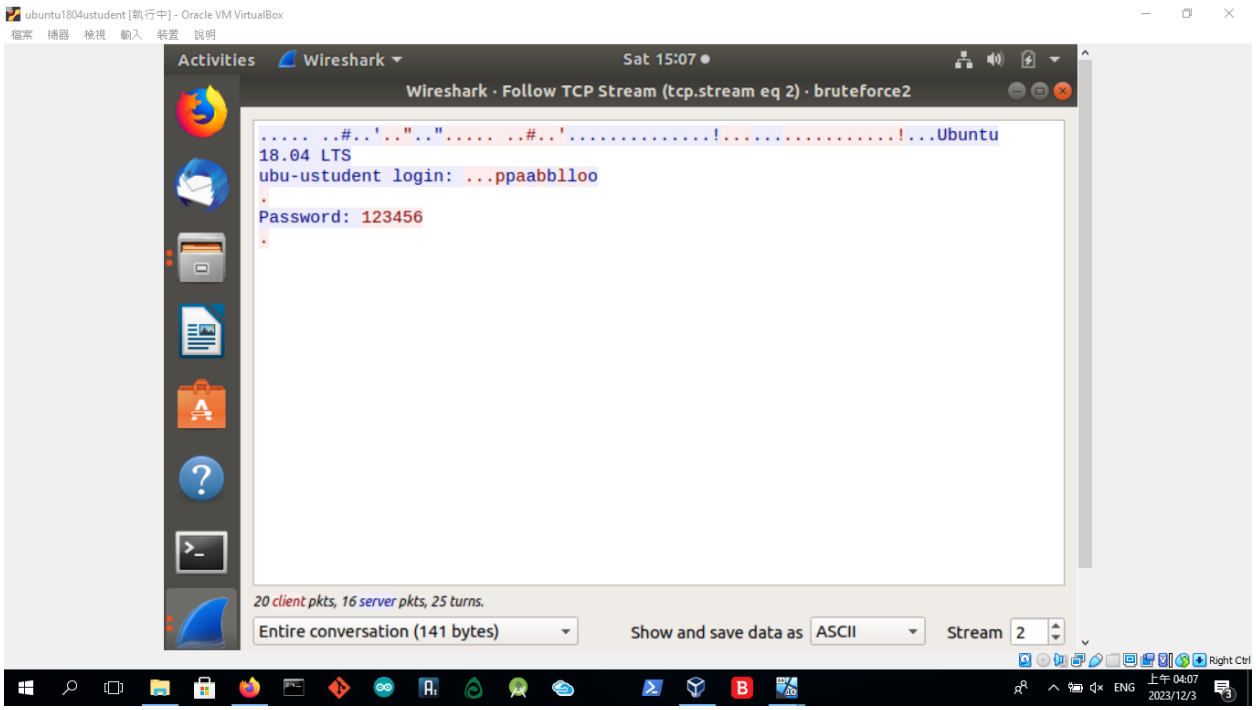
Based on your findings from above, what is your assessment of what happened? Please provide evidence to back up your results.

Ans:
We found that IP 10.0.2.7, which performs a port scan and a brute force assault against SMB 445, is the source of the attack.
It appears that the password was compromised and the telnet on port 21 was open to brute force attacks.





The following are the password was used successfully and username was compromised.



Task 2

We suspect that an internal user may have compromised another machine inside StaticSpeed's network and pivoted to one of the devices you are auditing. Please use lateralmovement.pcap and determine the following:

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

Please provide a narrative of what happened based on your findings. Justify your report based on the answers.

Ans:

We found that IP 10.0.2.7, which performs a port scan and a brute force assault against SMB 445, is the source of the attack. Yes attacker try to access our machine from a compromised device - MITRE ATT&CK Technique T1021. FTP on port 21 was open to brute force attacks. Yes as you can see the screenshots from previous task the attacker use built-in file sharing protocols, such as file sharing across SMB/Windows Admin Shares to

linked network shares or with authenticated connections via Remote Desktop Protocol, to create, copy files between inside victim systems to enable lateral movement.

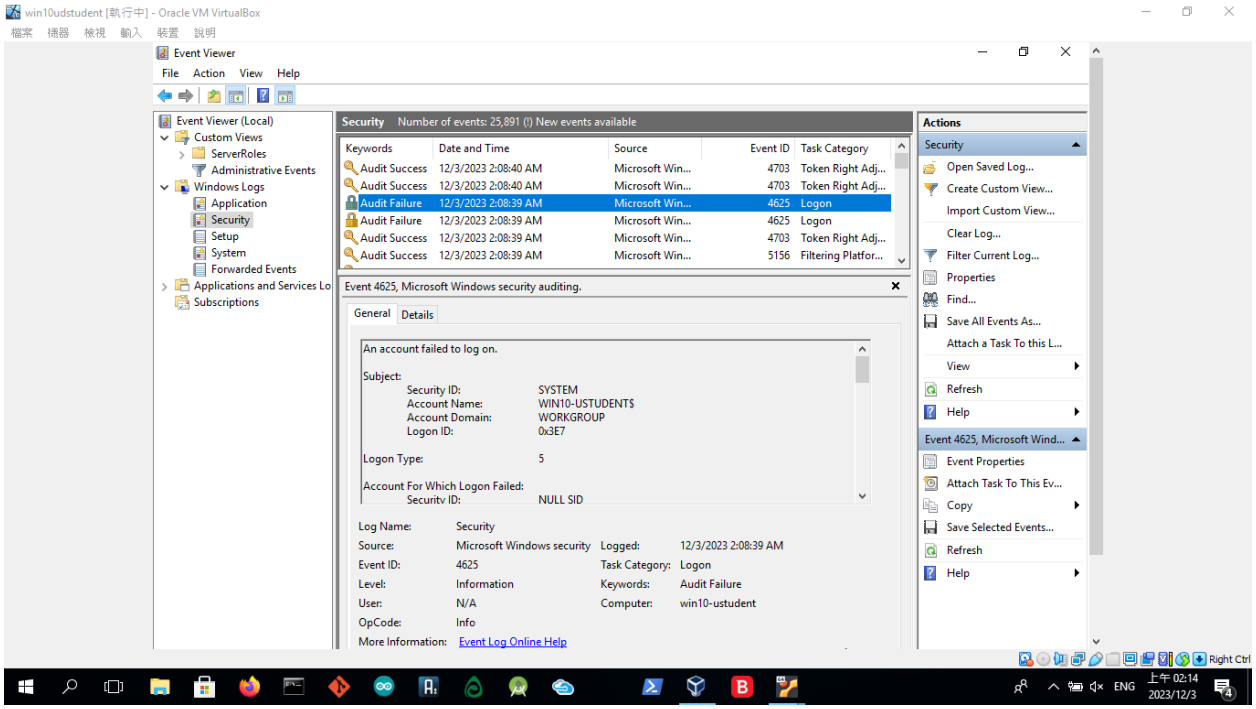
Task 3

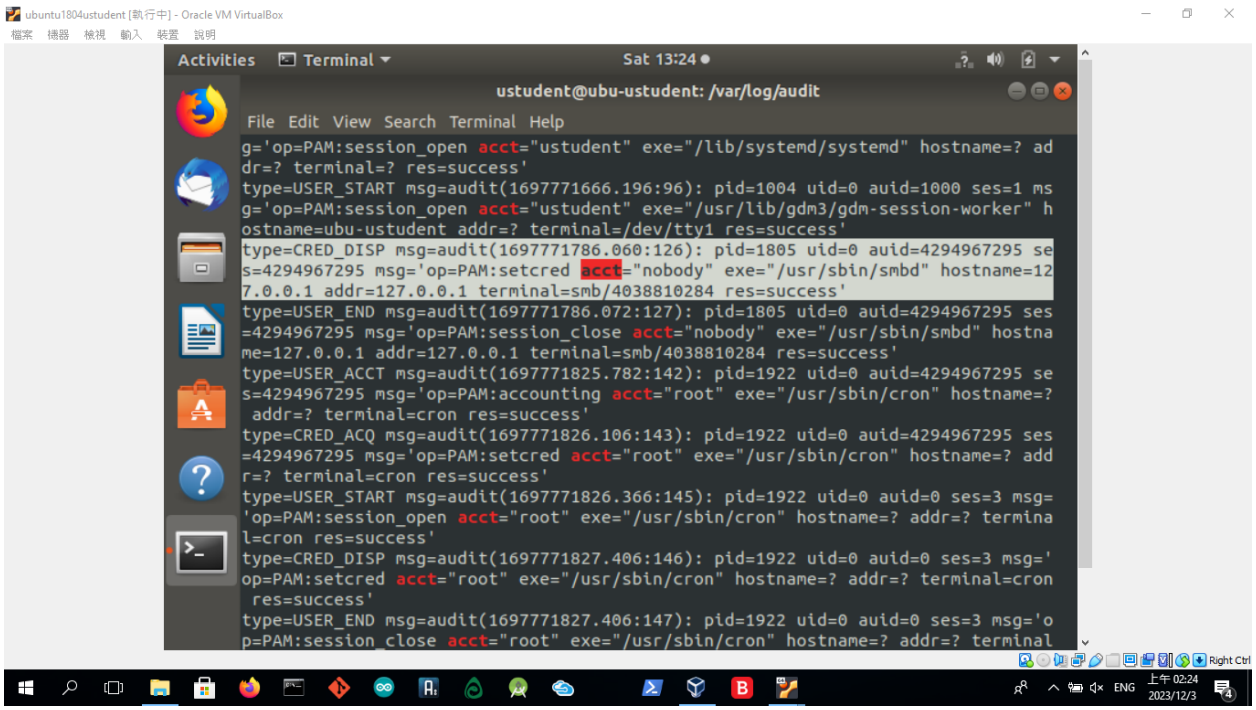
Look at logs on the StaticSpeed Windows machine.
Using the logs, determine the following:

- Are there any issues with Windows Share? Please provide screenshots of your findings.
- 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.

Ans:
We can spot EventID 4625 in our windows log ans in linux we can see username "nobody" is trying to access the certain things





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.

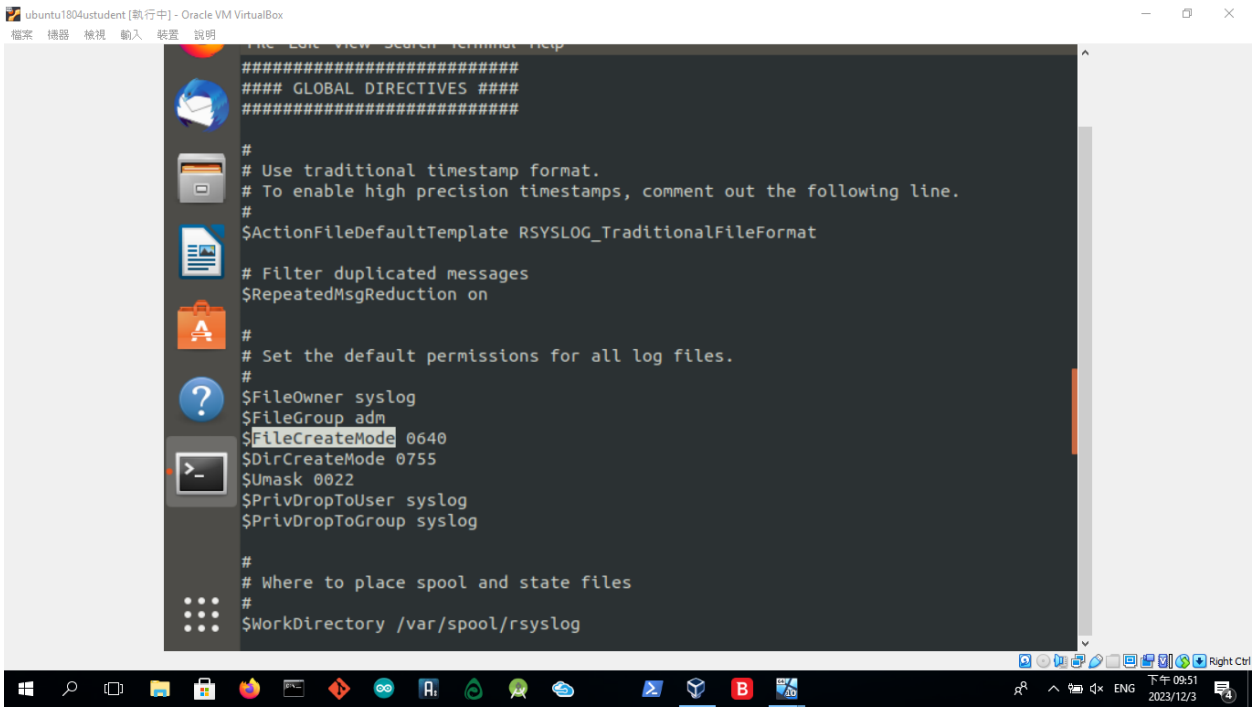
Analyze StaticSpeeds systems and determine if these machines are currently shipping jobs to a centralized location and set up correctly for our SIEM.

Hint: Perform **Ubuntu CIS 4.2.1.3** and verify if remote Syslog is configured for sending logs. In **Windows,** verify in the event viewer if there are any remote subscriptions related to Windows Event Forwarder.

Based on your answers, suggest a course of action to ensure StaticSpeed meets our needs to use a SIEM.

Ans:
To make sure that the right logging is enabled, check the contents of the /etc/rsyslog.conf by running the following command:
cat /etc/rsyslog.conf

We can see the /etc/rsyslog.conf and set $FileCreateMode to 0640.



Step 4: Assess Authentication Management at Targeted Assets

Task 1

Evaluate the authentication management situation of StaticSpeed's systems. In our initial look at StaticSpeed, we discovered what is called a "FLAT" network. This means there are no either Active Directory servers or OpenLDAP servers for Linux. We need these to provide us with tools to administer the network and enforce access control models. Specifically, when it comes to separate departments, supervisors, end-users, administrators, contractors, visitors, etc.

We also suspected that anyone that accesses this network could pretty much access everything. Determine if the current authentication scheme at StaticSpeed is unacceptable. Make sure to include the following:

- Ensure only administrators can remotely access windows machines and verify if root access is permitted at the Linux host.
- Check for users with excessive permissions

- Is root remote login allowed?
- Are there users that should not have remote access via ssh in Linux?
- Remote Desktop Access should only be granted to administrators in Windows, are there other accounts that should not be given access?

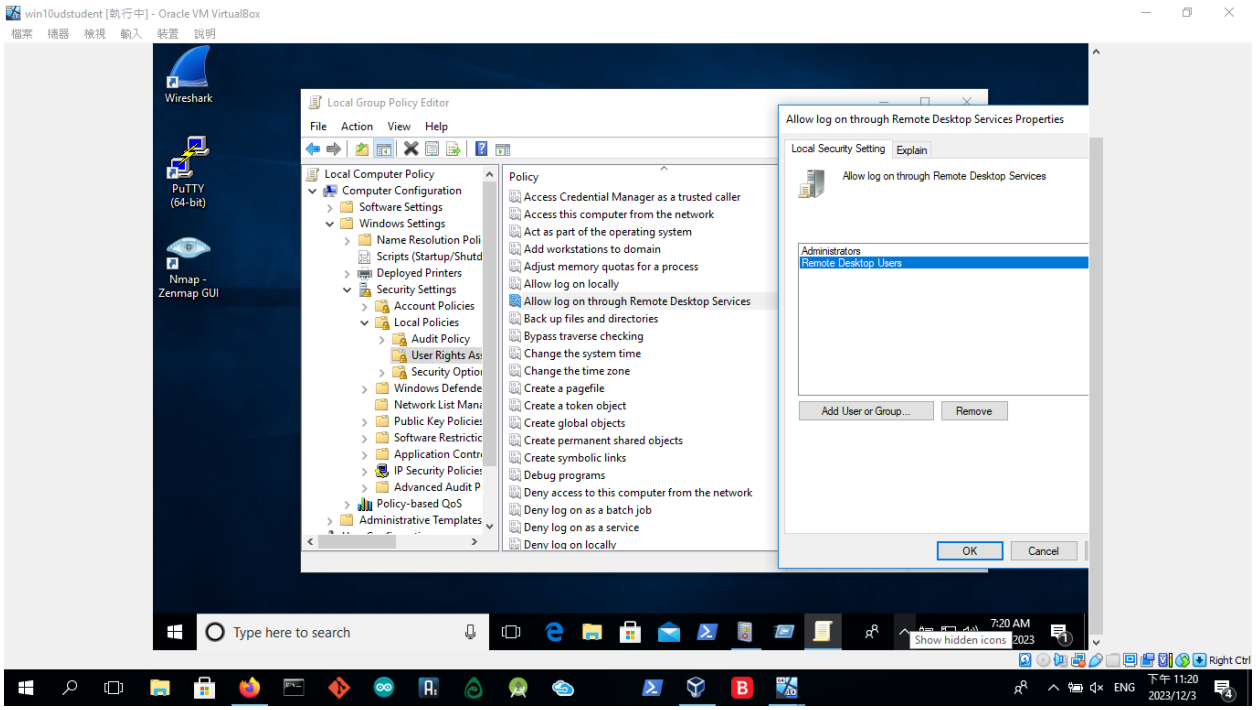
Knowing that your company only wants administrators to log remotely, provide a summary of the current situation for StaticSpeed. Then, suggest what accounts should be allowed to log remotely and why. Include your recommendations on whether StaticSpeeds authentication is acceptable and how you would improve it if it is not. Don't forget to include evidence to back up your recommendations.

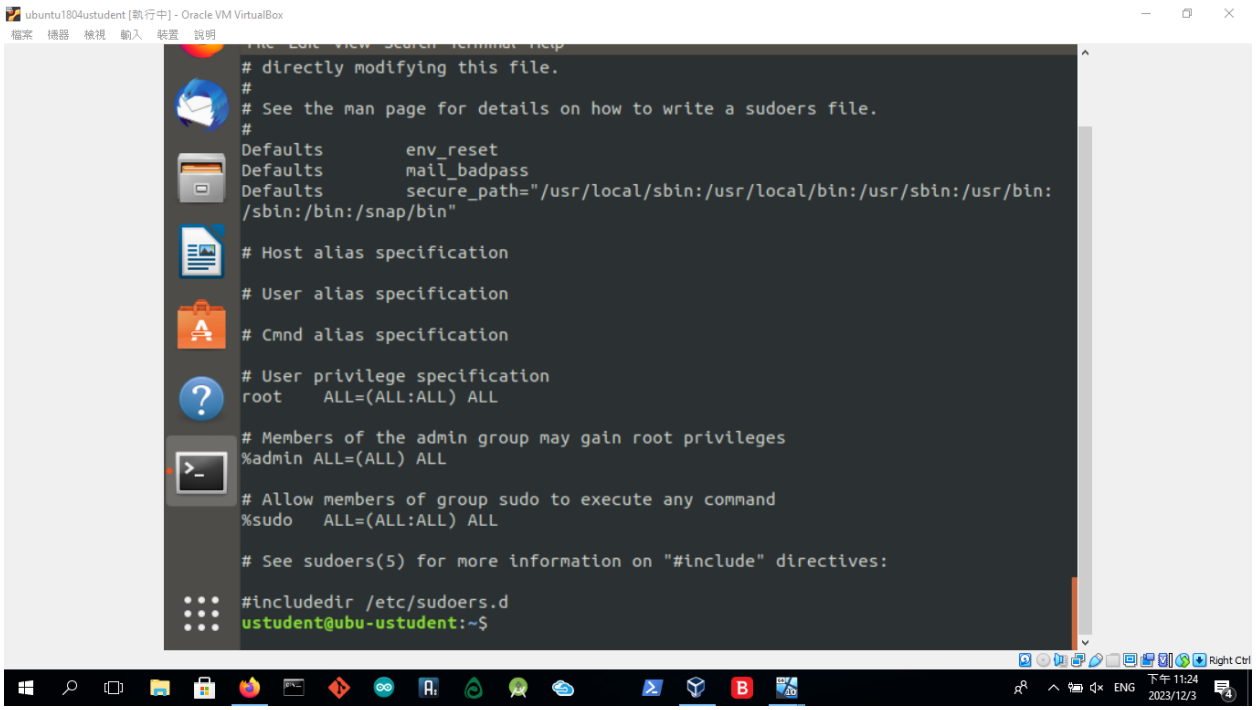
Ans:

By Start > Run > gpedit.msc.

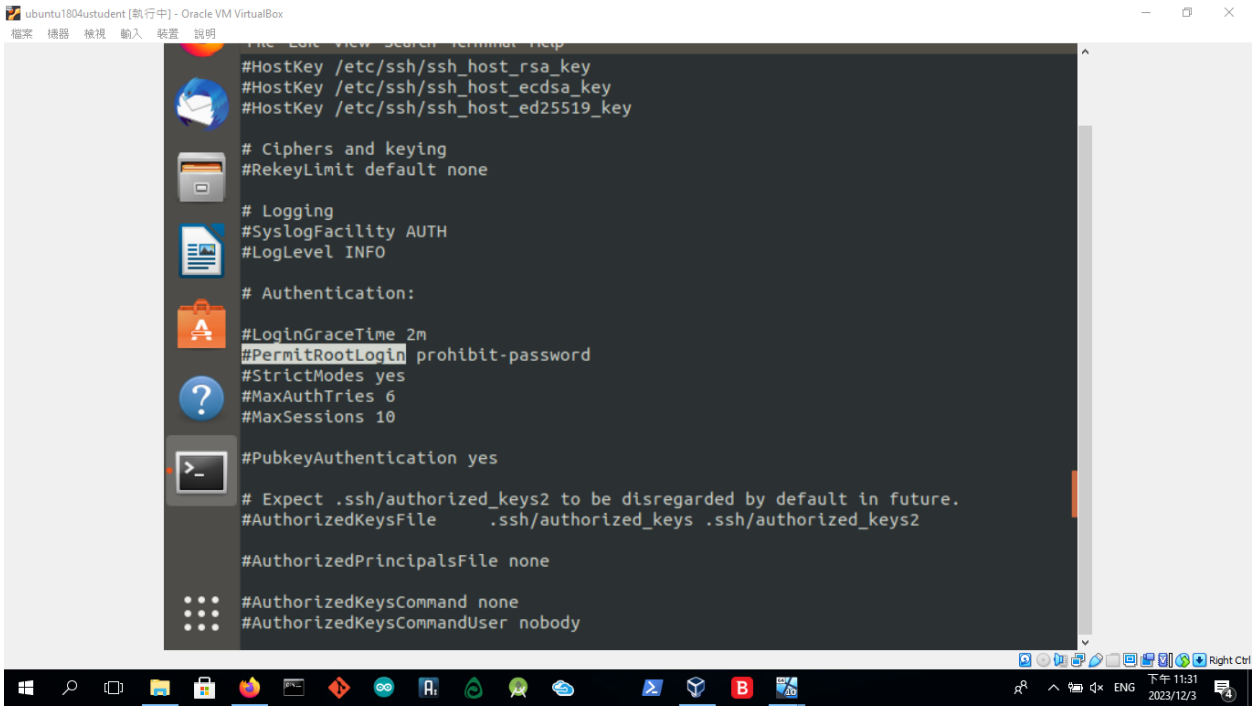
Expand: Computer Configuration > Windows Settings > Security Settings > Local Policies > User Rights Management.

Select: Allow log on through Remote Desktop Services. And sudo cat /etc/sudoers we can see administrators can remotely access windows machines and root access is permitted at the Linux host.





From the `/etc/ssh/sshd_config` file, we can see it doesn't permit root login via ssh.



There's no users with excessive permissions and root remote login isn't allowed
There's no any users that should not have remote access via ssh in Linux.

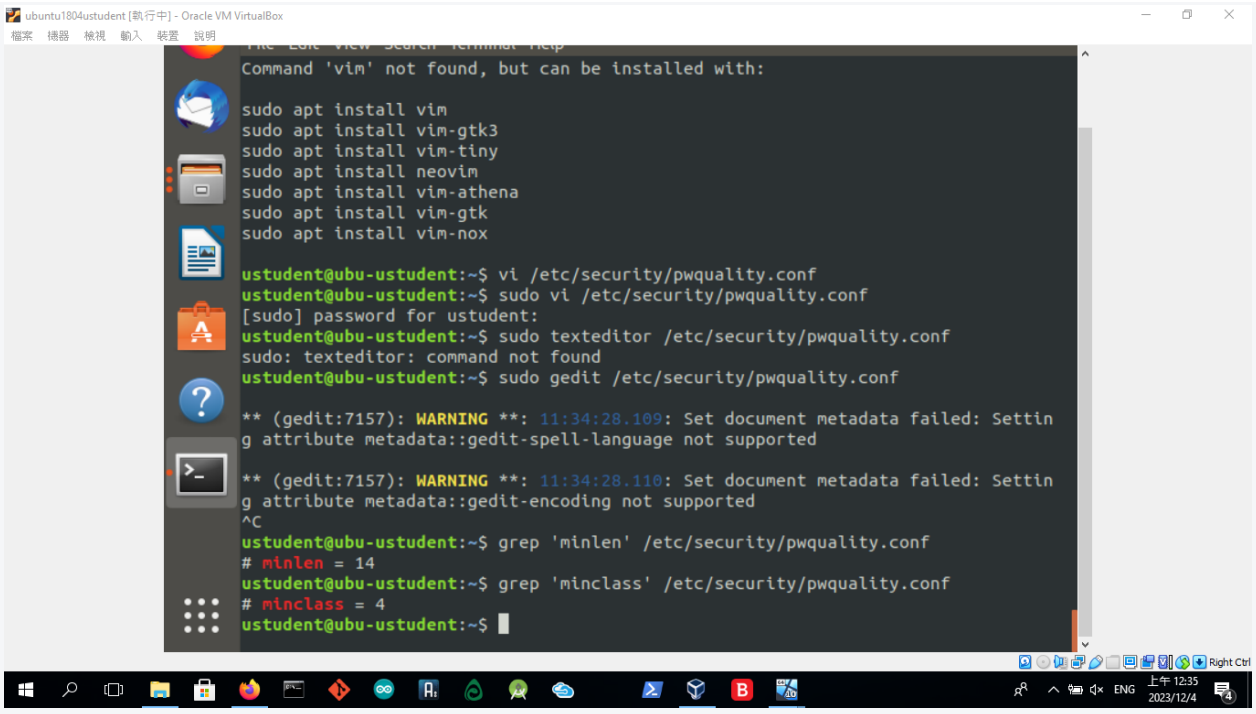
Remote Desktop Access should only be granted to administrators in Windows there are other accounts “Remote Desktop User” given access.

Task 2

NuttyUtility follows CIS Benchmarks. Therefore, we need to audit the password policies of StaticSpeed to see if they comply.
Audit the StaticSpeeds systems to verify that they comply with **CIS 5.3.1 Ubuntu** or **Windows 10 CIS benchmarks 1.1.5**? Please provide screenshots of current settings in both systems.

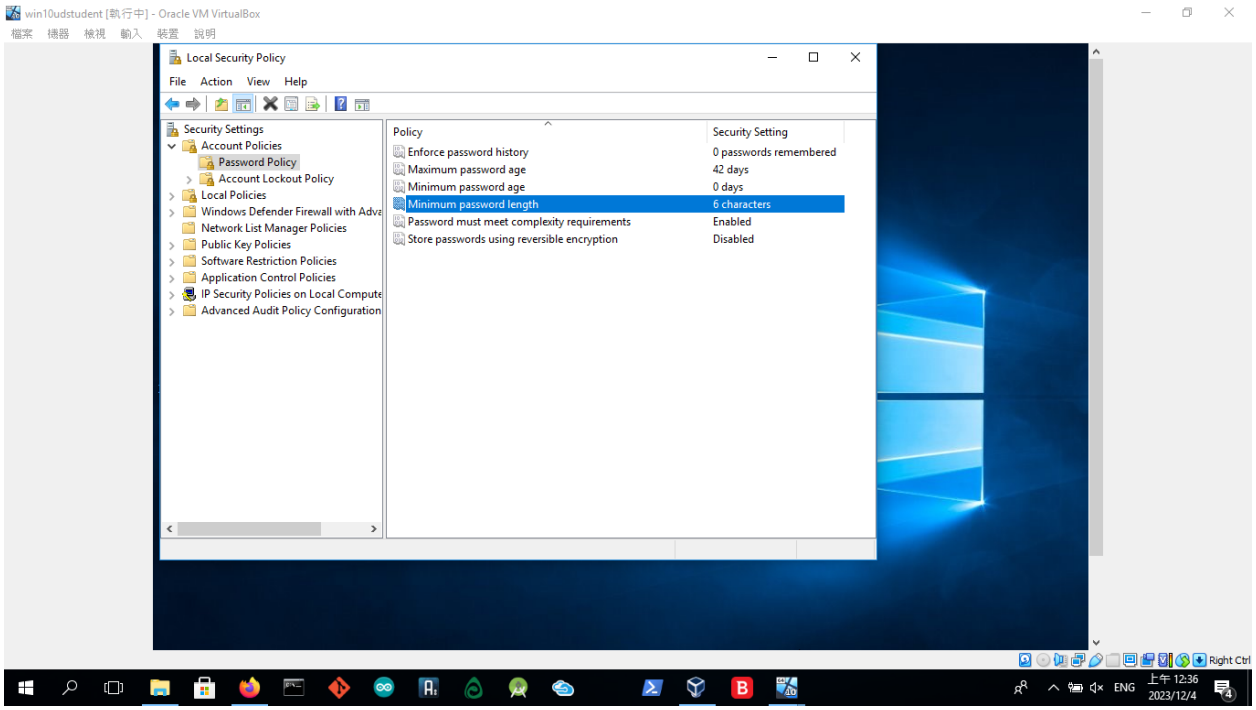
After you perform the checks, please provide an overview of your findings with the specific settings that should be in place and any other changes that should be made. Remember to justify your answer.

Ans:
On Linux use the following command:
We modified Password Length:
minlen = 14 - password must be 14 characters or more
Password complexity:
minclass = 4 - The minimum number of required classes of characters for the new password (digits, uppercase, lowercase, others)



On windows:

Searching for "Local Security Policy" using the windows search feature, and navigating to "Account Policy" > "Password Policy". We set at least six characters in length and enable password must meet complex requirements.

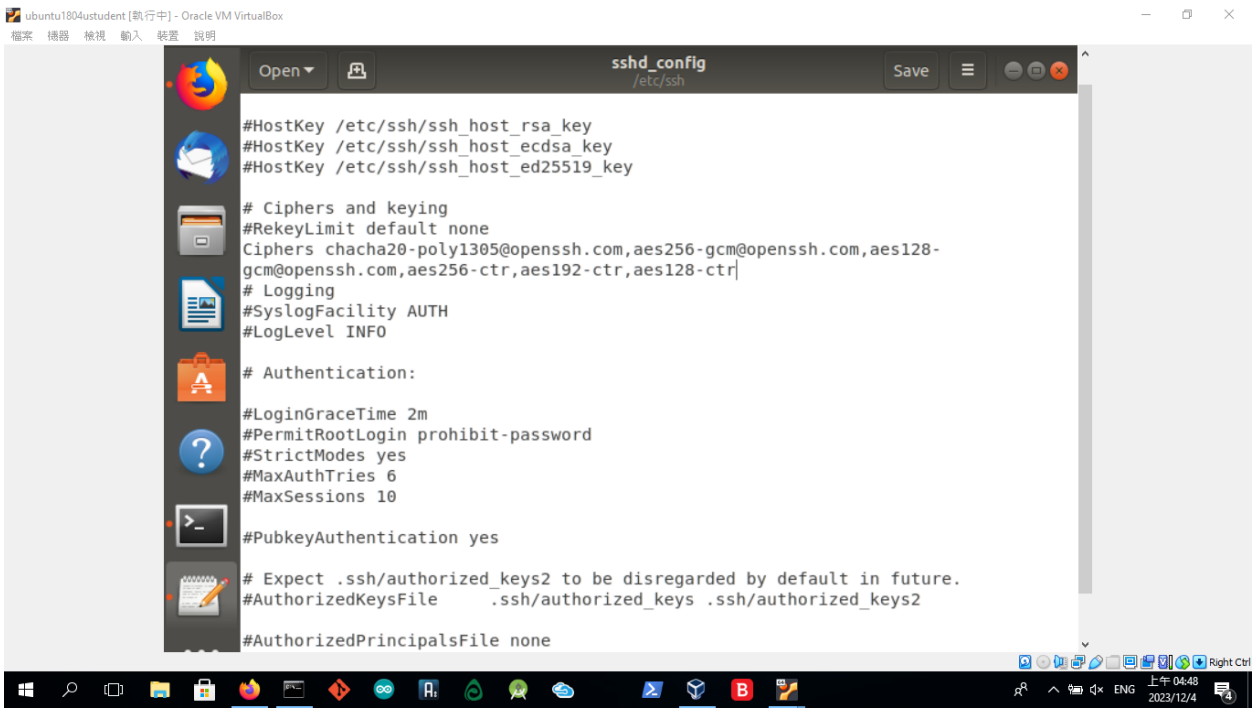


Task 3

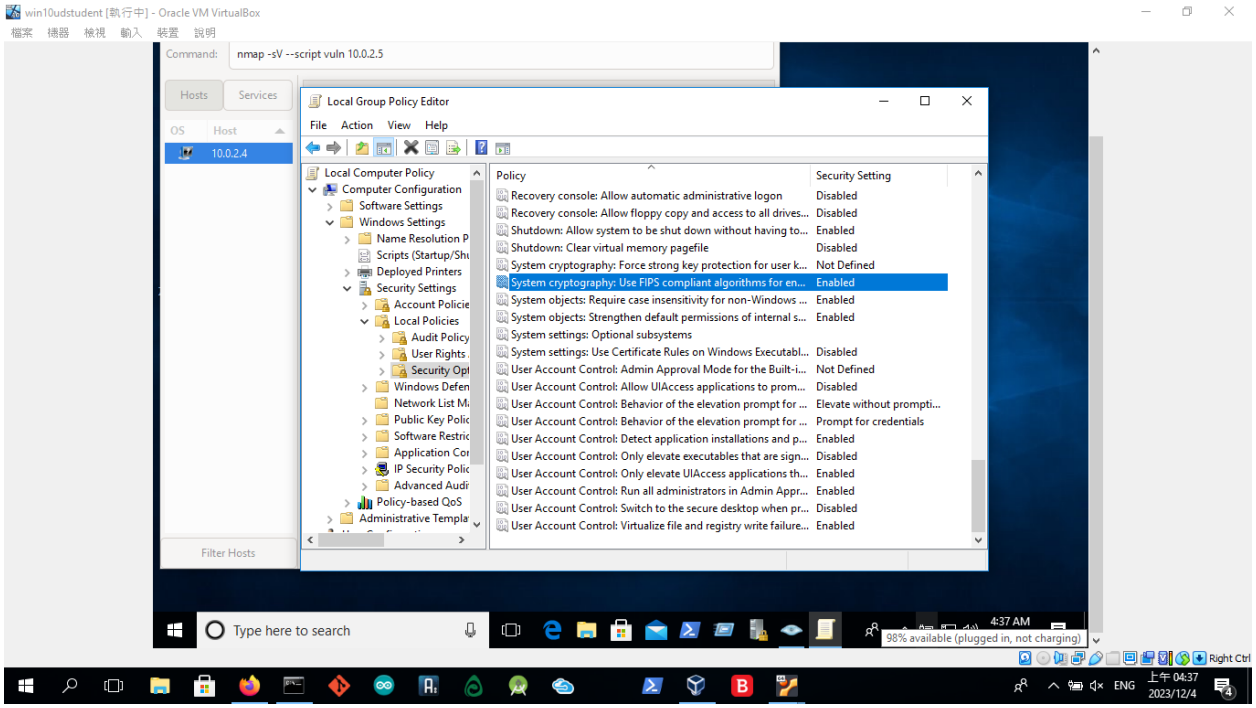
NuttyUtility uses a strong encryption ciphers policy (FIPS 140-2). Verify that your target assets comply with this policy. Check that these systems are compliant?. Please provide proof of the checks and give specifics on what to do next to get these systems compliant.

Ans:

From the following screenshots, these systems are compliant with FIPS 140-2 within the infrastructure. On ubuntu we edit the /etc/ssh/sshd_config file add/modify the Ciphers line to contain a comma separated list of the site approved ciphers follow Ubuntu 18.04 CIS 5.2.13.



On Windows we enable FIPS configuration.

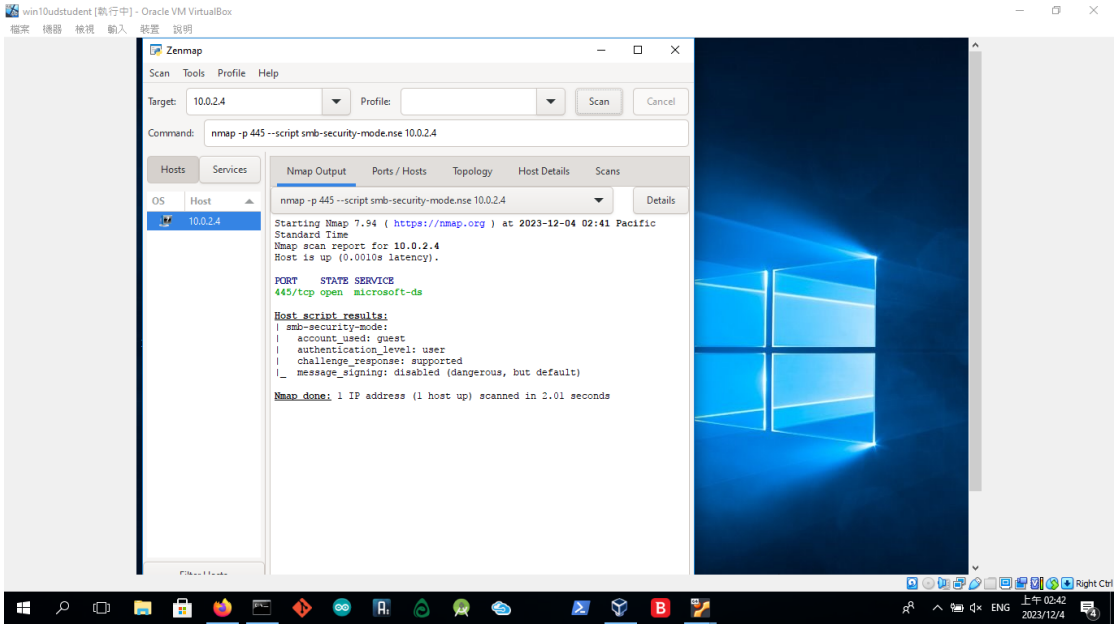


Task 4

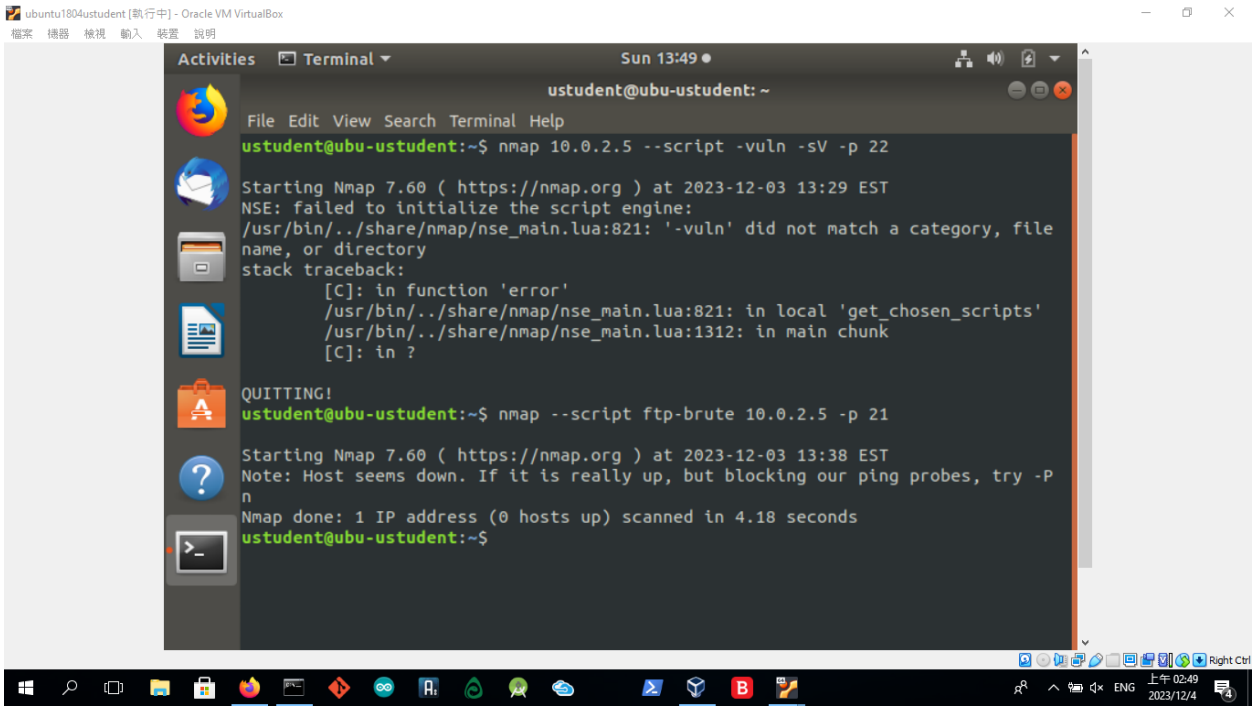
Conduct aggressive testing for password strength. Use a Nmap NSE Script to test how easy it would be to access StaticSpeed's FTP Server and SMB Shares if an attacker probed them. We have already requested and obtained permission to perform these audits.

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.

On windows machine we can clear see there is a vulnerability on port 445 with the command `nmap -p 445 --script smb-security-mode.nse 10.0.2.4`



On ubuntu we run nmap –script ftp-brute 10.0.2.5 -p 21 to check ftp service



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
10.0.2.4	xx	x	x	x

IP Address: 10.0.2.4

Service	Port	Sensitive Level
xxx	Xxx TCP	High
xxx	xxx TCP	Medium
xxx	TCP	Low
xxx	xx TCP	Log

Expected detail format for vulnerabilities found

High

1- CVE-XXXX-XXXX and or finding

Issue

Explain the vulnerability and add screenshots for proof of concept if applicable

Impact
Explain the impact of this finding and sensitivity level. I.E “Attacker can take over the system”

Mitigation
Add your suggestions and industry-accepted recommendations to mitigate this vulnerability.

Reference

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

Medium

1- CVE-XXXX-XXXX and or finding

Issue
Explain the vulnerability and add screenshots for proof of concept if applicable

Impact
Explain the impact of this finding and sensitivity level. I.E “Attacker can take over the system”

Mitigation
Add your suggestions and industry-accepted recommendations to mitigate this vulnerability.

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

Low

1- CVE-XXXX-XXXX and or finding

Issue
Explain the vulnerability and add screenshots for proof of concept if applicable

Impact

Explain the impact of this finding and sensitivity level. I.E “Attacker can take over the system”

Mitigation
Add your suggestions and industry-accepted recommendations to mitigate this vulnerability.

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

Example

Log

8- HTTP Security Headers Detection

Issue
Known security headers are being checked on the host.

Impact

```
Missing Headers                    | More Information
-----------------------------------------------------------------------------
↪-----------------------------------
Content-Security-Policy            | https://owasp.org/www-project-secure-headers
↪/#content-security-policy
Feature-Policy                     | https://owasp.org/www-project-secure-headers
↪/#feature-policy
Referrer-Policy                    | https://owasp.org/www-project-secure-headers
↪/#referrer-policy
X-Content-Type-Options             | https://owasp.org/www-project-secure-headers
↪/#x-content-type-options
X-Frame-Options                    | https://owasp.org/www-project-secure-headers
↪/#x-frame-options
X-Permitted-Cross-Domain-Policies | https://owasp.org/www-project-secure-headers
↪/#x-permitted-cross-domain-policies
X-XSS-Protection                   | https://owasp.org/www-project-secure-headers
↪/#x-xss-protection
```

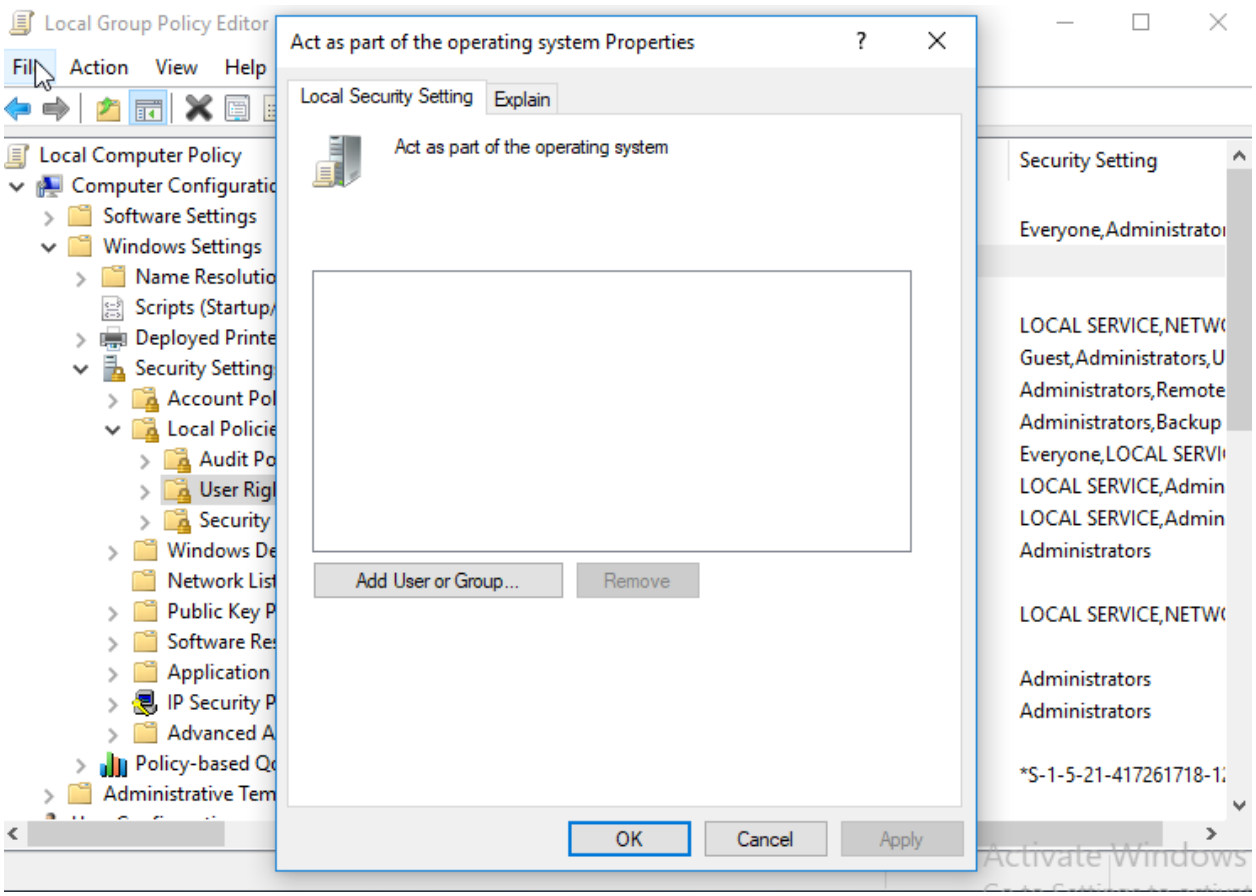
References
https://owasp.org/www-project-secure-headers/

https://owasp.org/www-project-secure-headers/#div-headers
https://securityheaders.io

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:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Act as part of the operating system
```



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
10.0.2.6	xx	x	x	x

IP Address: 10.0.2.6

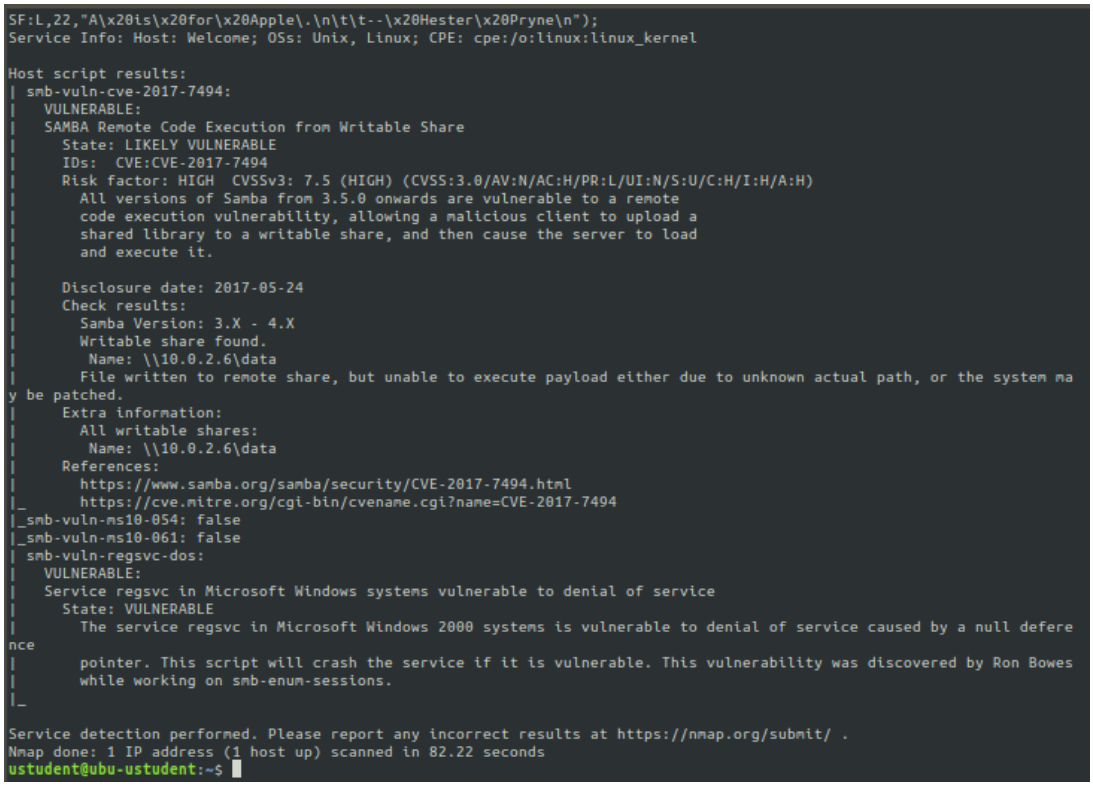
Service	Port	Sensitive Level
smb	445 TCP	High
ftp	21 TCP	Medium
xxx	TCP	Low
xxx	xx TCP	Log

Expected detail format for vulnerabilities found

High

1- CVE-2017-7494

Issue
A remote code execution vulnerability exists in Samba since version 3.5.0 and before 4.6.4, 4.5.10, and 4.4.14.



Impact
This vulnerability enables a malevolent client to upload a shared library to a writable share, which in turn causes the server to load and execute it.

Mitigation
1. Use the "noexec" option to mount the filesystem that Samba uses for its writable share.

2. Include the following parameter:
nt pipe support = no
Add your smb.conf's [global] section, then restart smbd. Clients are unable to reach any named pipe endpoints as a result. Be aware that this may prevent Windows clients from using some expected features.

Reference
https://www.exploit-db.com/exploits/42060
https://www.cvedetails.com/cve/CVE-2017-7494/?q=CVE-2017-7494
https://access.redhat.com/security/cve/cve-2017-7494

Medium

1- CVE-2011-1002

Issue

Before Avahi 0.6.29, the avahi-core/socket.c in avahi-daemon allowed remote attackers to generate an infinite loop or denial of service by sending an empty mDNS (1) IPv4 or (2) IPv6 UDP packet to port 5353

```
ustudent@ubu-ustudent:~$ nmap -sV --script vuln 10.0.2.6

Starting Nmap 7.60 ( https://nmap.org ) at 2023-10-23 22:56 EDT
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for ubu-ustudent (10.0.2.6)
Host is up (0.00017s latency).
Not shown: 991 closed ports
PORT    STATE SERVICE     VERSION
13/tcp  open  daytime
17/tcp  open  qotd?
| fingerprint-strings:
|   NULL:
|     A is for Apple.
|_    Hester Pryne
21/tcp  open  ftp         vsftpd 2.0.8 or later
|_sslv2-drown:
22/tcp  open  ssh         OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
23/tcp  open  telnet      Linux telnetd
37/tcp  open  time        (32 bits)
|_rfc868-time: 2023-10-24T02:57:52
80/tcp  open  http        Apache httpd 2.4.29 ((Ubuntu))
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint
 at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port17-TCP:V=7.60%I=7%D=10/23%Time=653732A2%P=x86_64-pc-linux-gnu%r(NUL
SF:L,22,"A\x20is\x20for\x20Apple\.\n\t\t--\x20Hester\x20Pryne\n");
Service Info: Host: Welcome; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-vuln-cve-2017-7494:
|   VULNERABLE:
|   SAMBA Remote Code Execution from Writable Share
|     State: LIKELY VULNERABLE
```

Impact

Prior to Avahi 0.6.29, by sending an empty mDNS (1) IPv4 or (2) IPv6 UDP packet to port 5353, remote attackers could create an infinite loop or denial of service via the avahi-core/socket.c in the avahi-daemon.

Mitigation

Add your suggestions and industry-accepted recommendations to mitigate this vulnerability.

Reference

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1022
https://access.redhat.com/security/cve/cve-2011-1002

Low

1- CVE-2011-1002

Issue

Impact

Mitigation
Add your suggestions and industry-accepted recommendations to mitigate this vulnerability.

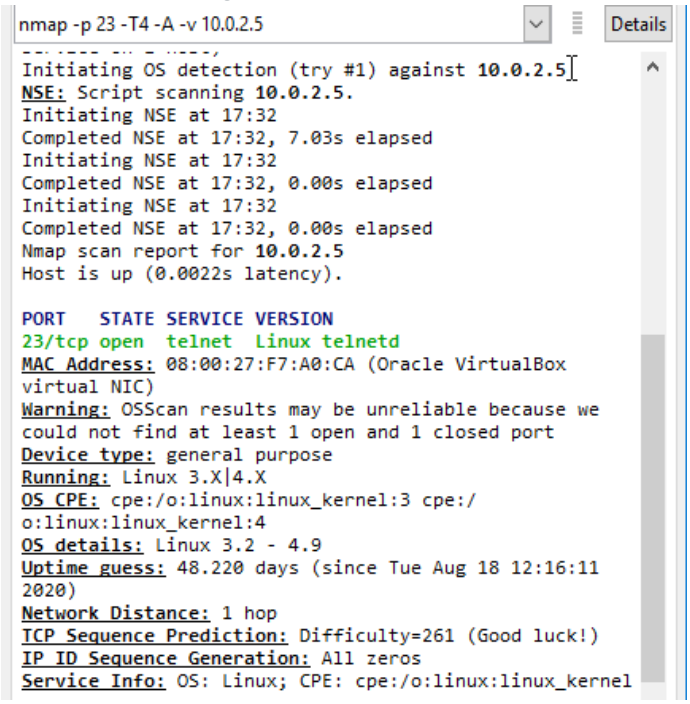
Reference

Example of Log

Log

3 - Telnet Unencrypted Cleartext Login

Issue
The host is running a Telnet service that allows cleartext logins over unencrypted connections



Impact
Attackers can uncover login names and passwords by sniffing traffic to the Telnet service.

Mitigation
Replace Telnet with remote access protocols that support encryption such as SSH.

Reference
https://attack.mitre.org/techniques/T1021/

Example of control checks & CIS benchmarks Ubuntu 18.04

Control Check: CIS 1.1.21 Ensure sticky bit is set on all world-writable directories
Result: Compliant. Not output from the audit command.

```
ustudent@ubu-ustudent:~$ df --local -P |awk '{if (NR!=1) print $6}' | xargs -I
'{}' -xdev -type d \( -perm -002 -a ! -perm -1000 \) 2>/dev/null
ustudent@ubu-ustudent:~$
```

Impact: This feature prevents the ability to delete or rename files in world-writable directories (such as /tmp) that are owned by another user. This system is compliant with corporate policy CIS 1.1.21 for Linux Ubuntu 18.04 machines.

Note: The CIS benchmarks that need to be checked are listed in all the previous steps.

CIS for Windows Ent v1.9.0.	CIS for Ubuntu 18.04 v2.01
18.9.102.2	**1.2.1**
18.3.4	**1.6.1, 1.6.2**
1.1.5	**4.2.1.3**
	5.3.1

Step 6: Final Assessment and Recommendations Based on Your Scans and Checks

In this section, provide a final recommendation, supported by the information above, on whether NuttyUtility should extend its network and integrate the StaticSpeed system into its current infrastructure.
Include the following in your assessment:
- Would integrating this network into the extended network of our company bring new risks and exposures?
- If it would be a risk to NuttyUtility, what recommendations would you make to mitigate these risks before implementing the integration, and why?
- Please provide reasoning based on the proof obtained throughout your assessment.

- Remember, the Stakeholders need to decide as to whether or not to complete this integration now.