

# 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-yyyy-yyyy, 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 vulnerabilities, We found a outdated samba version raise CVE-2017-7494 vulnerability in the generate report see below screenshots:

Ans:

Nmap scan ubuntu:

```
ustudent@uba-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=653732A2XP=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
|       CVE:CVE-2017-7494
|       IDs: HIGH CVSSv3: 7.5 (HIGH) (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H)
|       Risk factor: 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.
|                   _Smb-vuln-regsvc-dos:

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@uba-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 defer
ence
|     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@uba-ustudent:~$ 

```

Nmap scan windows we can see there's CVE-2011-1002 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:

```

ubuntu1804student [執行中] - Oracle VM VirtualBox
檔案 機器 檢視 輸入 裝置 說明
File Edit View Search Terminal Help
ustudent@uba-ustudent:~$ nmap -sV --script vuln 10.0.2.4
Starting Nmap 7.60 ( https://nmap.org ) at 2023-12-06 18:45 EST
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 10.0.2.4
Host is up (0.0015s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE      VERSION
7/tcp      open  echo
9/tcp      open  discard?
13/tcp     open  daytime      Microsoft Windows USA daytime
17/tcp     open  qotd        Windows qotd (English)
19/tcp     open  chargen
80/tcp     open  http         Microsoft IIS httpd 10.0
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-server-header: Microsoft-IIS/10.0
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
3389/tcp   open  ms-wbt-server Microsoft Terminal Services
|_ssl-ccs-injection: No reply from server (TIMEOUT)

ustudent@uba-ustudent:~$ 

```

```

ubuntu1804student [正在运行] - Oracle VM VirtualBox
檔案 檔案 檢視 輸入 裝置 說明
File Edit View Search Terminal Help

7/tcp open echo
9/tcp open discard?
13/tcp open daytime Microsoft Windows USA daytime
17/tcp open qotd Windows qotd (English)
19/tcp open chargen
80/tcp open http Microsoft IIS httpd 10.0
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-server-header: Microsoft-IIS/10.0
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
445/tcp open microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
3389/tcp open ms-wbt-server Microsoft Terminal Services
|_ssl-ccs-injection: No reply from server (TIMEOUT)
|_sslv2-down:
Service Info: Host: WIN10-USTUDENT; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 312.50 seconds
ustudent@ubu-ustudent:~$
```

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

PORT	STATE	SERVICE	VERSION
22/tcp	open	ssh	OpenSSH 7.6p1 Ubuntu 4 (Ubuntu; protocol 2.0)
80/tcp	open	http	Apache httpd 2.4.29 ((Ubuntu))
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)

Zenmap

Scan Tools Profile Help

Target: fe80::5635:9f35:5f5a:1cf9 Profile: Scan Cancel

Command: nmap -sV -6 fe80::5635:9f35:5f5a:1cf9

Hosts Services

OS Host

fe80::5635:9f35:5f5a:1cf9

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -sV -6 fe80::5635:9f35:5f5a:1cf9

Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-23 18:30 Pacific Daylight Time  
Nmap scan report for fe80::5635:9f35:5f5a:1cf9  
Host is up (0.0036s latency).  
Not shown: 996 closed tcp ports (reset)  
PORT STATE SERVICE VERSION  
22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)  
80/tcp open http Apache httpd 2.4.29 ((Ubuntu))  
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)  
MAC Address: 08:00:27:45:87:FE (Oracle VirtualBox virtual NIC)  
Service Info: Host: UBU-USTUDENT; OS: Linux; CPE: cpe:/o:linux:linux\_kernel  
  
Service detection performed. Please report any incorrect results at  
<https://nmap.org/submit/>.  
Nmap done: 1 IP address (1 host up) scanned in 13.51 seconds

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

Target: 10.0.2.0 Profile: Scan Cancel

Command: nmap -sV -p 22 10.0.2.6

Hosts Services

OS Host

10.0.2.6 fe80::5635:9f35:5f5a:1cf9

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -sV -p 22 10.0.2.6

Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-23 21:31 Pacific Daylight Time  
Nmap scan report for 10.0.2.6  
Host is up (0.0010s latency).  
  
PORT STATE SERVICE VERSION  
22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)  
MAC Address: 08:00:27:45:87:FE (Oracle VirtualBox virtual NIC)  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel  
  
Service detection performed. Please report any incorrect results at  
<https://nmap.org/submit/>.  
Nmap done: 1 IP address (1 host up) scanned in 1.47 seconds

Target: 10.0.2.6

Command: nmap -sV -p 22 10.0.2.6

Hosts Services

Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

10.0.2.6 fe80::5635:9f35%5

nmap -sV -p 22 10.0.2.6

Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-23 21:31 Pacific Daylight Time

Nmap scan report for 10.0.2.6

Host is up (0.0010s latency).

PORT	STATE	SERVICE	VERSION
22/tcp	open	ssh	OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
		<u>MAC Address:</u>	08:00:27:45:87:FE (Oracle VirtualBox virtual NIC)
		<u>Service Info:</u>	OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 1.47 seconds

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:fLnA0pTUWLE3VGiuIyzXte9x1VmRePvuqlWNL1JxlUk
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:fLnA0pTUWLE3VGiuIyzXte9x1VmRePvuqlWNL1JxlUk.
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 clearly 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
```

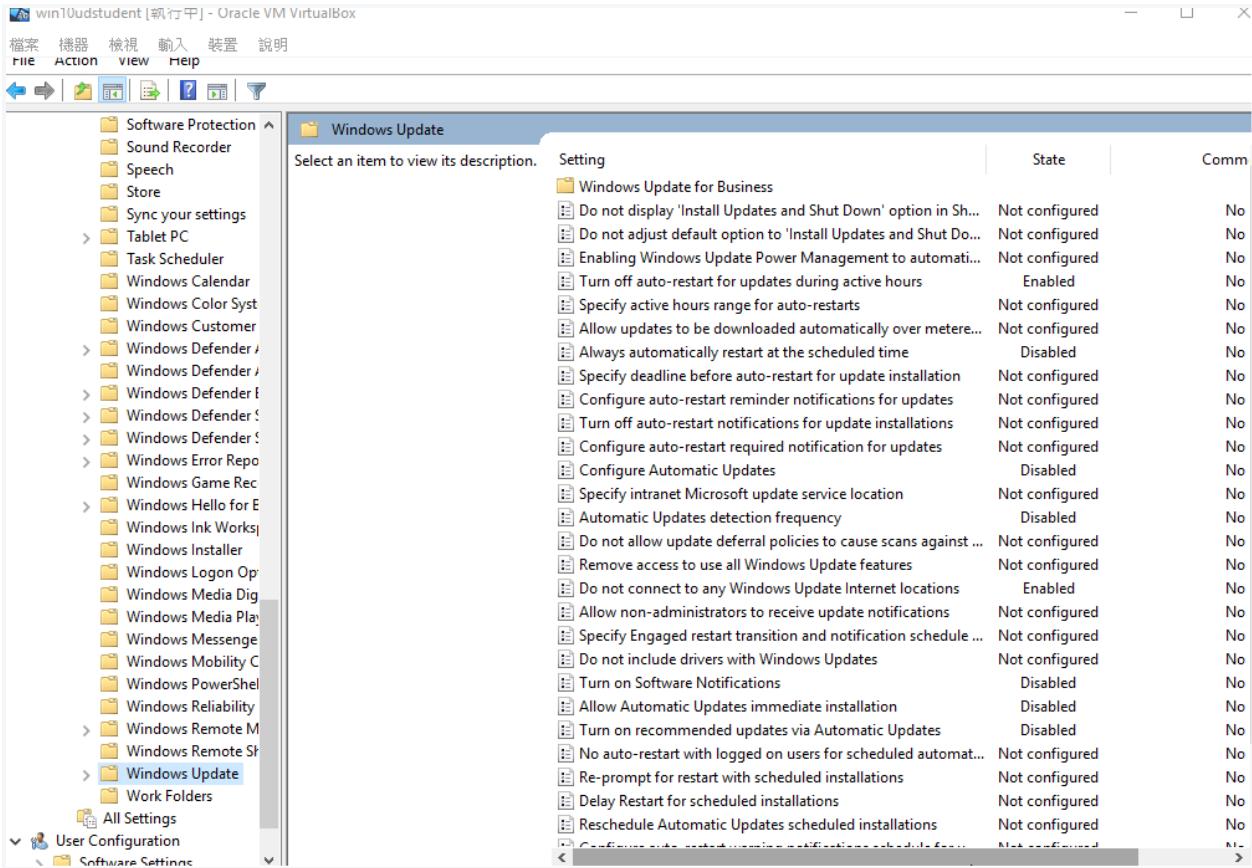
Or

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.



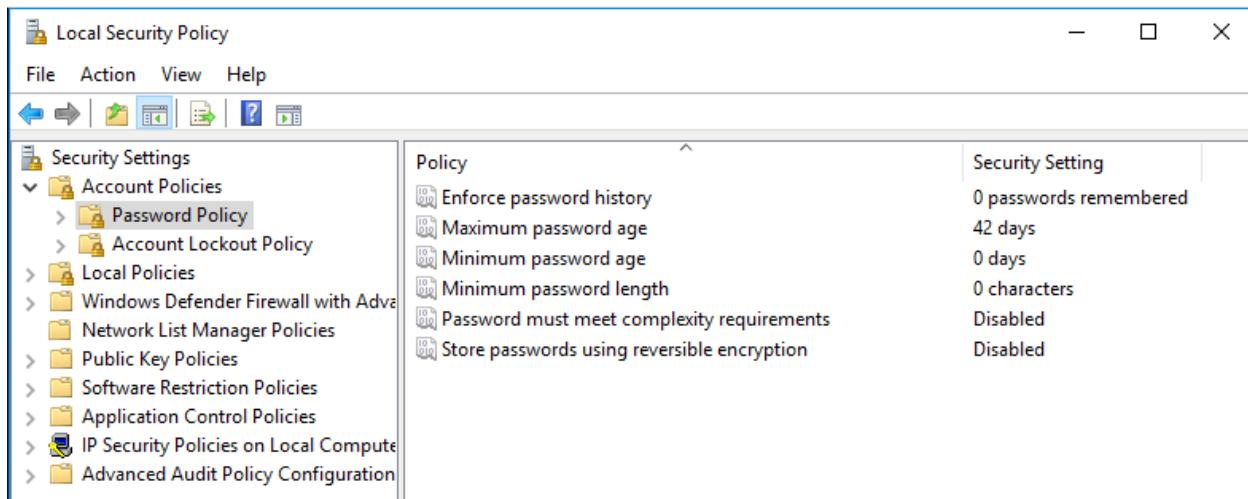
We audit StaticSpeeds systems by the following commands on Linux:

```
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.

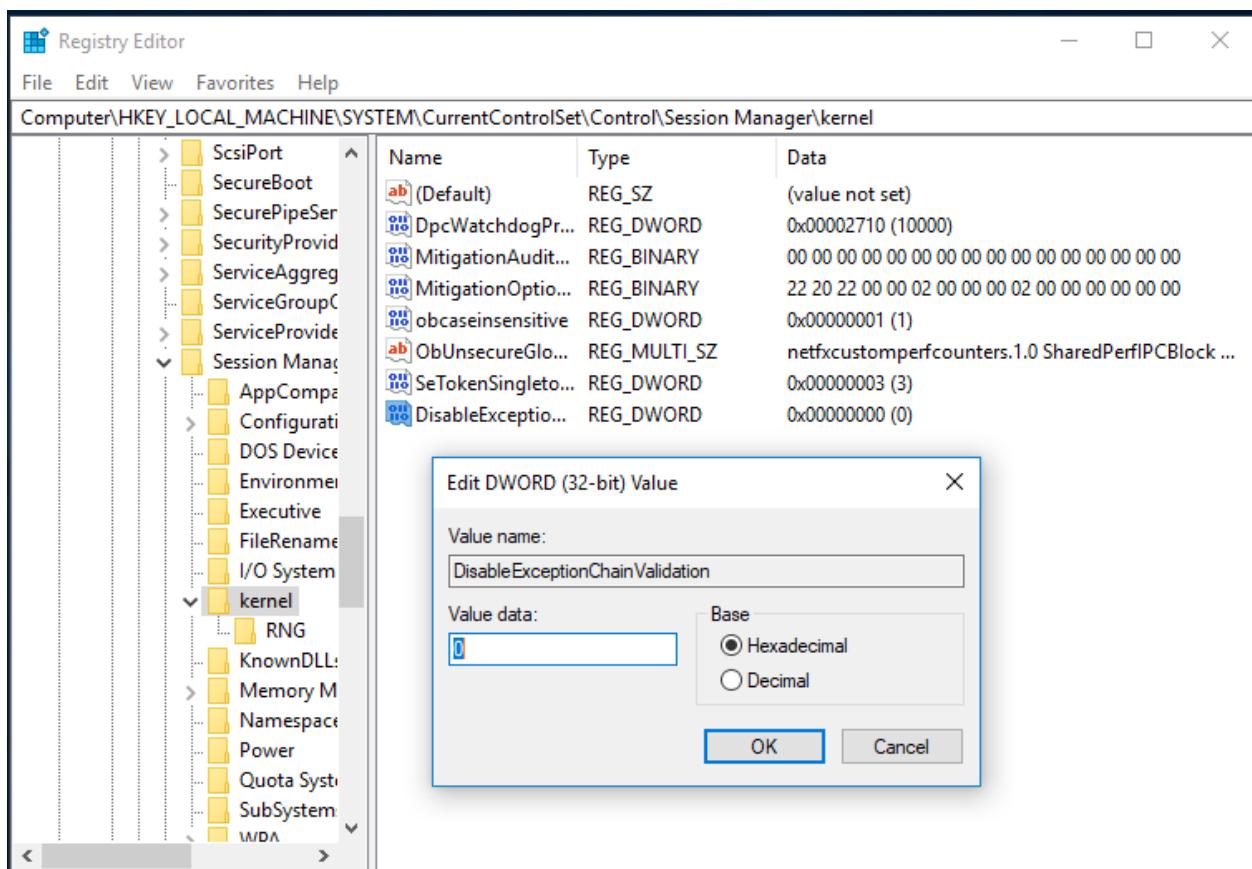
3. Double-click

**DisableExceptionChainValidation.**

4. Change the value of the **DisableExceptionChainValidation** registry entry to 0 to enable it, and then click **OK**.

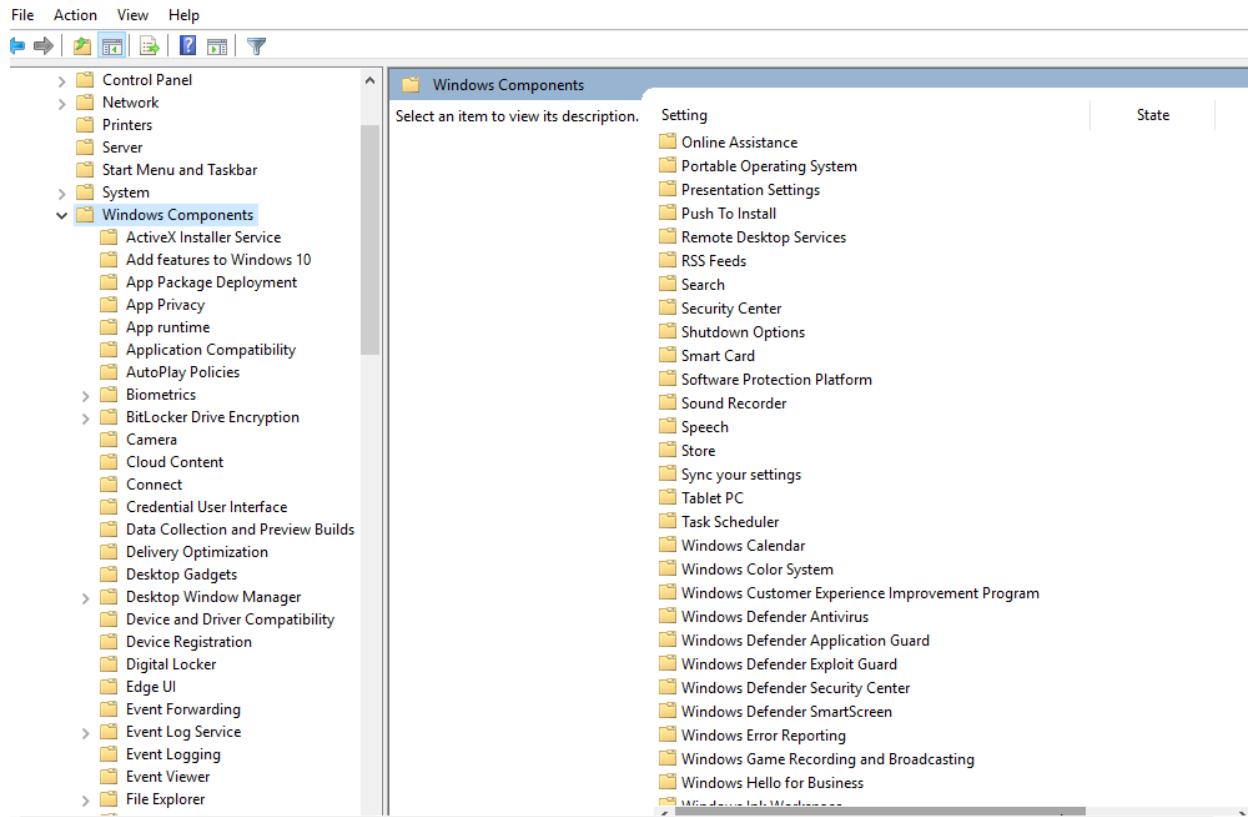
Note A value of 1 disables the registry entry. A value of 0 enables it.

5. Exit Registry Editor.



Is this system compliant?

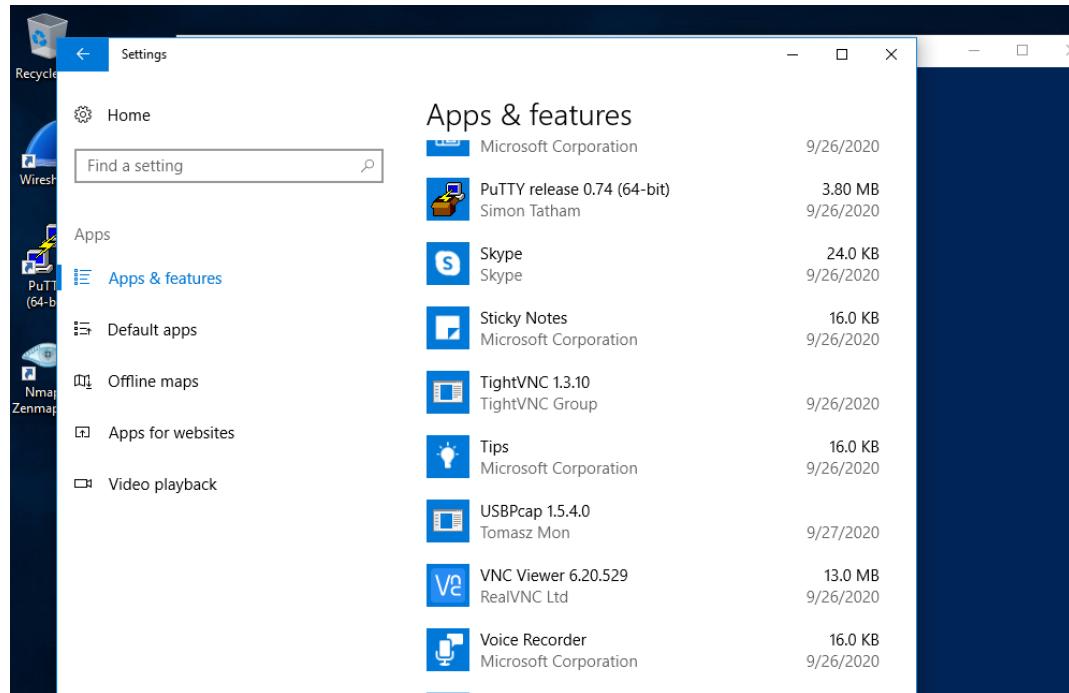
Ans: No, The path from CIS is not exist. An additional group policy template is required to add MS security group. The registry entry "DisableExceptionChainValidation" is not available.



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

```
journctl | grep 'protection: active'
```

```
ustudent@ubu-ustudent:~$ journctl | 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@uba-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@uba-ustudent:~$
```

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

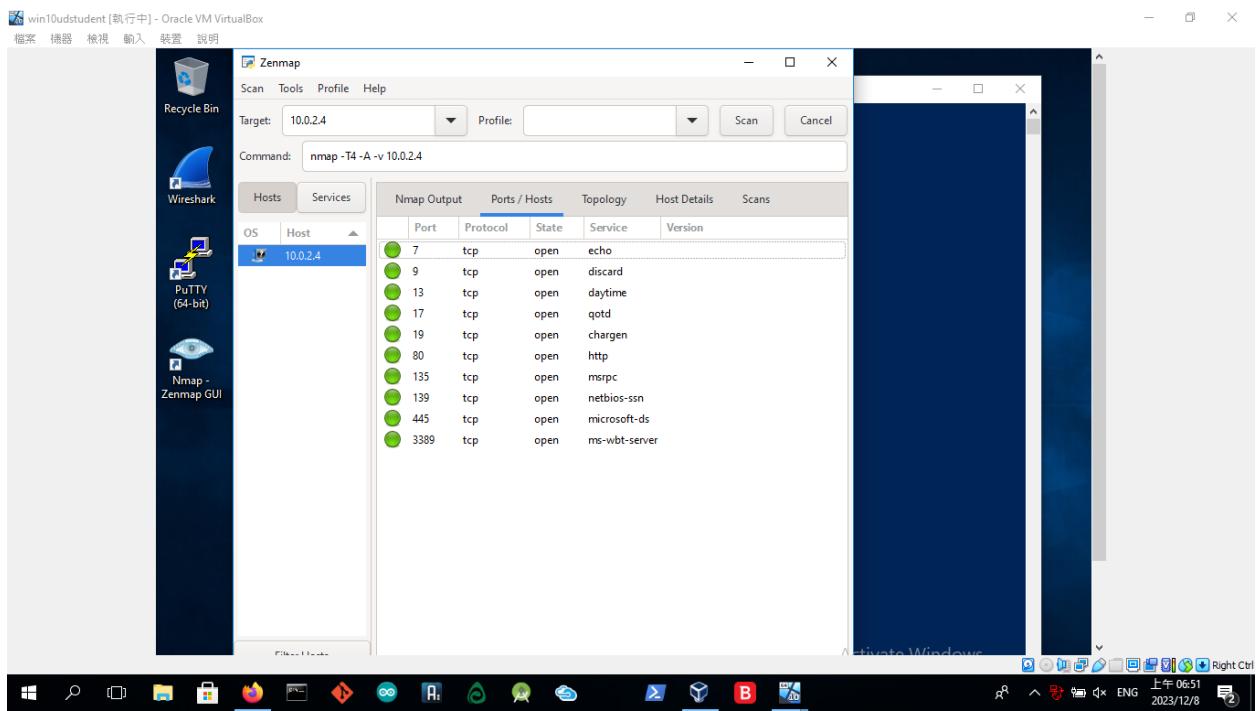
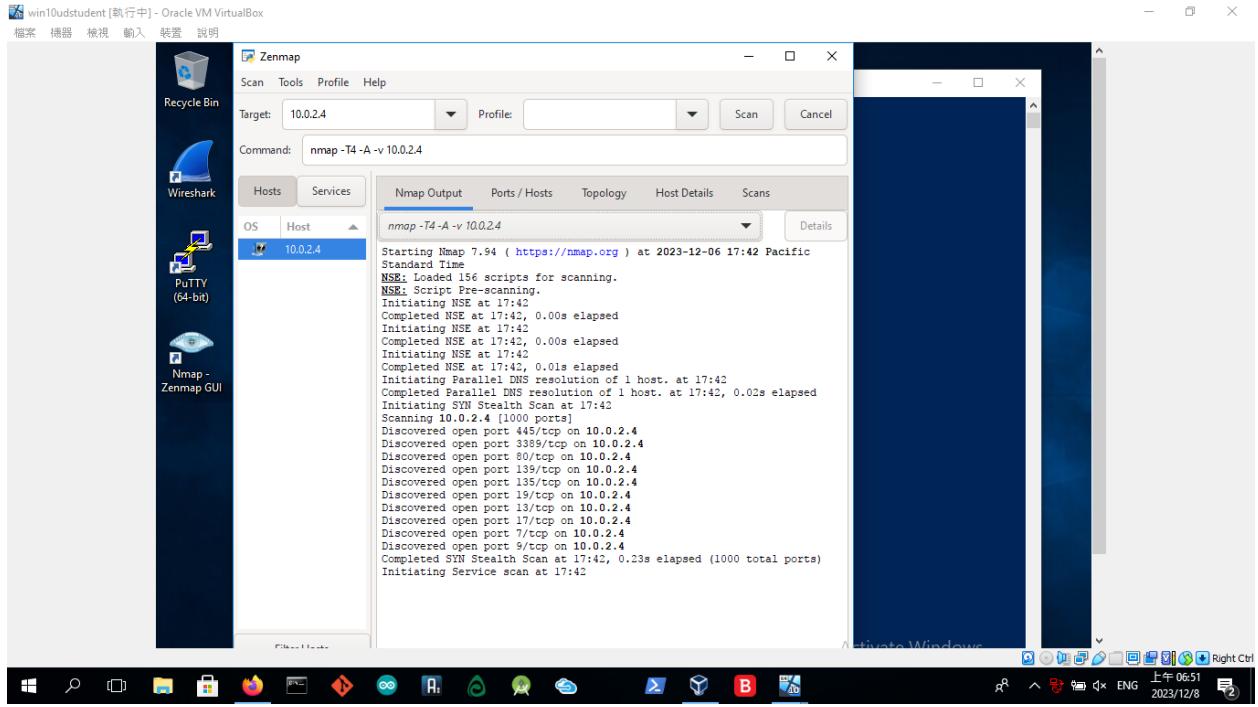
## Task 4

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

```
ustudent@uba-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%T=ee653732A2KP=x86_64-pc-linux-gnu%R(NUL
SF:L,22,"A\x20is\x20for\x20apple.\n\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
```

Open ports on **Windows** systems using **ZenMap**:



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.

Mitigating the risks associated with open ports we can:

- Apply the principle of least privilege and zero trust to reduce compromise impact.
- Blocking inbound traffic coming from unidentified sources with firewalls.

- Limiting the number of open ports by only permitting connections from reliable sources.
- Closing unnecessary ports.
- To restrict the amount of MAC addresses that can connect to a port, enable port security.

## 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

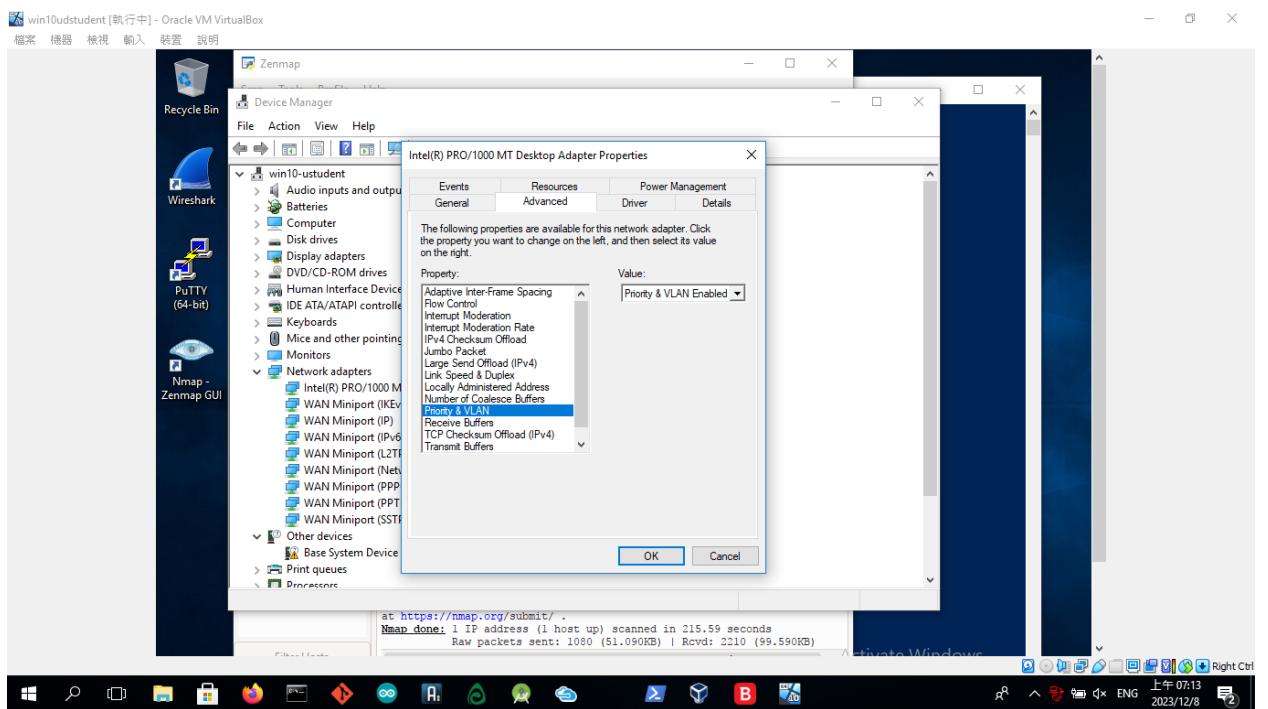
ifconfig -a

```
ustudent@ubu-ustudent:~$ ifconfig -a
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 10.0.2.6 netmask 255.255.255.0 broadcast 10.0.2.255
        inet6 fe80::5635:5f5a:1cf9 prefixlen 64 scopeid 0x20<link>
          ether 08:00:27:45:87:fe txqueuelen 1000 (Ethernet)
            RX packets 1217 bytes 1435387 (1.4 MB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 632 bytes 88499 (88.4 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
          loop txqueuelen 1000 (Local Loopback)
            RX packets 420 bytes 34551 (34.5 KB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 420 bytes 34551 (34.5 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

## Windows

1. Run the Device Manager ([devmgmt.msc](#));
2. Expand the **Network adapters** section and open the properties of your network adapter;
3. Go to the **Advanced** tab we can see the VLAN setting:



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
```

The screenshot shows the Windows Local Security Policy snap-in. The title bar reads "win10udstudent [執行中] - Oracle VM VirtualBox". The menu bar includes 檔案, 機器, 檢視, 輸入, 裝置, 說明, and LOCAL SECURITY POLICY. The main window has a toolbar with icons for Back, Forward, Refresh, and Search. On the left is a navigation pane with "Security Settings" expanded, showing "Account Policies", "Local Policies" (which is expanded to show "Audit Policy", "User Rights Assignment", "Security Options", "Windows Defender Firewall with Adv...", "Network List Manager Policies", "Public Key Policies", "Software Restriction Policies", "Application Control Policies", "IP Security Policies on Local Computer" (which is selected), and "Advanced Audit Policy Configuration"). On the right is a table with columns: Name, Description, Policy Assigned, and Last Modified. One row is visible: "testIPSecurity" with "No" under "Policy Assigned" and "9/26/2020 9:0" under "Last Modified".

Name	Description	Policy Assigned	Last Modified
testIPSecurity		No	9/26/2020 9:0

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

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control			
	Name	Type	Data
Computer	(Default)	REG_SZ	(value not set)
HKEY_CLASSES_ROOT	BootDriverFlags	REG_DWORD	0x0000001c (28)
HKEY_CURRENT_USER	CurrentUser	REG_SZ	USERNAME
HKEY_LOCAL_MACHINE	DirtyShutdownC...	REG_DWORD	0x0000000a (10)
BCD00000000	EarlyStartServices	REG_MULTI_SZ	RpcSs Power BrokerInfrastructure SystemEventsBr...
HARDWARE	FirmwareBootD...	REG_SZ	multi(0)disk(0)rdisk(0)partition(1)
SAM	LastBootShutdo...	REG_DWORD	0x00000000 (0)
SECURITY	LastBootSuccee...	REG_DWORD	0x00000001 (1)
SOFTWARE	PresutdownOr...	REG_MULTI_SZ	Usosvc DeviceInstall gpsvc trustedinstaller
SYSTEM	SvcHostSplitThr...	REG_DWORD	0x00380000 (3670016)
ActivationBroker	SystemBootDevi...	REG_SZ	multi(0)disk(0)rdisk(0)partition(2)
ControlSet001	SystemStartOpti...	REG_SZ	NOEXECUTE=OPTIN
CurrentControlSet	WaitToKillServic...	REG_SZ	5000
Control	{7746D80F-97E...		
ACPI			
AppID			
AppReadiness			
Arbiters			
BackupRestore			
BGFX			
BitLocker			
BitlockerStatus			
CI			

## 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?

Ans:

We should allow only the services and protocols required for remote access, and restricting or disabling any others. By default, IPv6 is used, which means that logging settings and monitoring devices could ignore it. This gives attackers a possible point of entry. See the following screenshot for proof that **IPv6** and remote access is operational in the corresponding virtual machines.

```
ustudent@ubu-ustudent:~$ ifconfig -a
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 10.0.2.6 netmask 255.255.255.0 broadcast 10.0.2.255
        inet6 fe80::5635:9f35:5f5a:1cf9 prefixlen 64 scopeid 0x20<link>
          ether 08:00:27:45:87:fe txqueuelen 1000 (Ethernet)
            RX packets 1217 bytes 1435387 (1.4 MB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 632 bytes 88499 (88.4 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
          loop txqueuelen 1000 (Local Loopback)
            RX packets 420 bytes 34551 (34.5 KB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 420 bytes 34551 (34.5 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

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

Windows IP Configuration

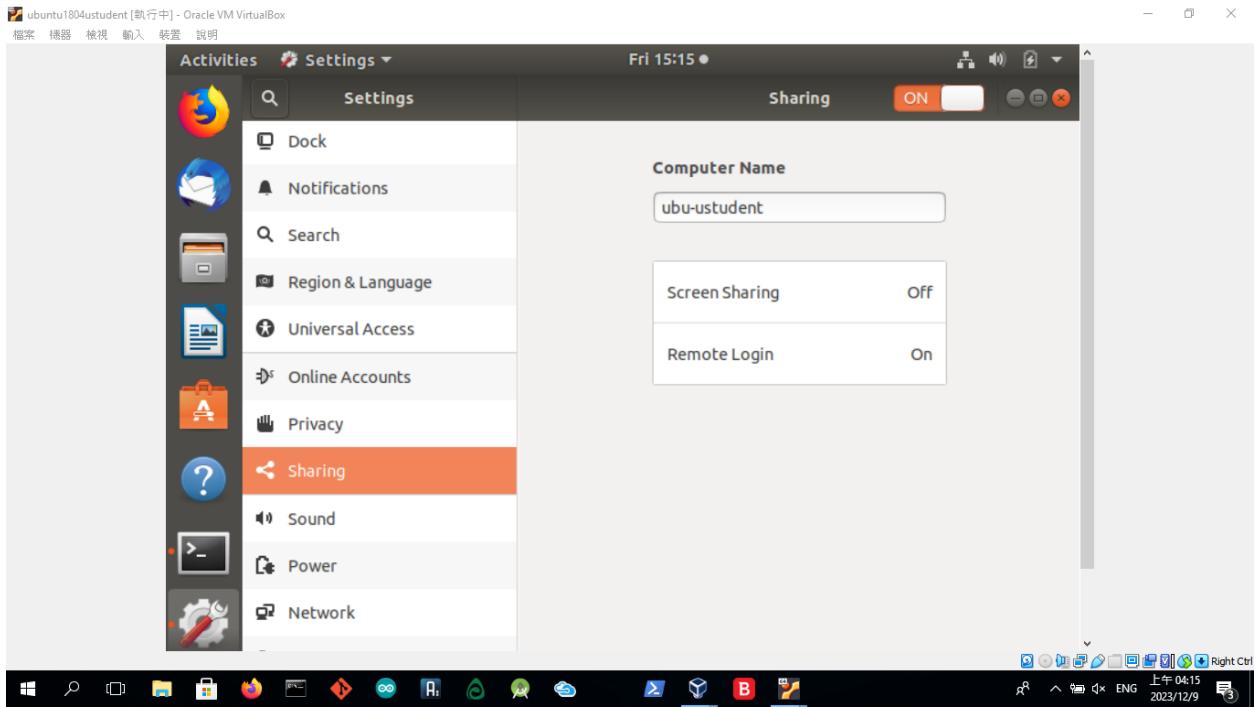
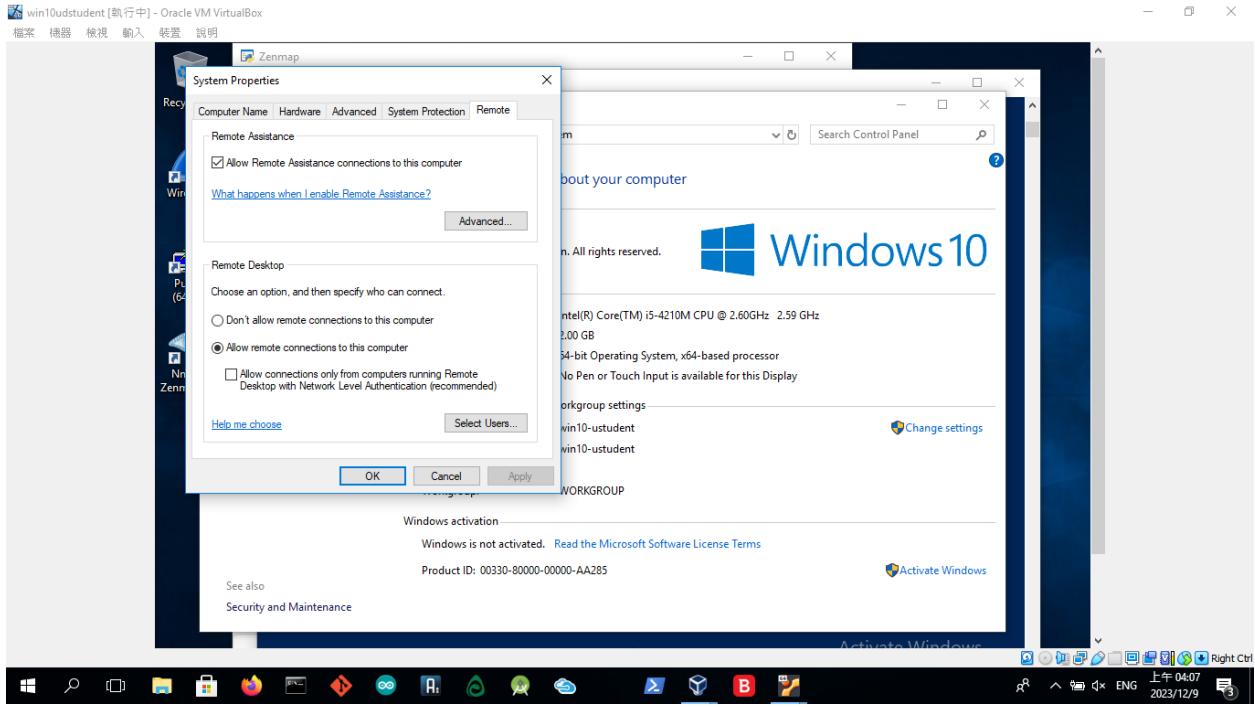
Host Name . . . . . : win10-ustudent
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : home

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-E0
  DHCP Enabled. . . . . : No
  Autoconfiguration Enabled . . . . . : Yes
```



## 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
```

The screenshot shows a Windows Command Prompt window titled "win10udstudent [執行中] - Oracle VM VirtualBox". The window displays network configuration details and the output of the "netsh advfirewall show allprofiles state" command. The network configuration includes IPv4 settings like address, subnet mask, lease obtained, lease expires, default gateway, DHCP server, and DNS servers. The firewall status section shows Domain Profile Settings (State: ON), Private Profile Settings (State: OFF), and Public Profile Settings (State: OFF). A watermark for "Activate Windows Go to Settings to activate Windows" is visible in the background.

```
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-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes

C:\Windows\system32>netsh advfirewall show allprofiles state

Domain Profile Settings:
-----
State          ON

Private Profile Settings:
-----
State          OFF

Public Profile Settings:
-----
State          OFF

Ok.

Activate Windows
Go to Settings to activate Windows.

C:\Windows\system32>
```

On Ubuntu we use the following command:

```
ufw status
```

The screenshot shows a terminal window on Ubuntu. The user runs the "ufw status" command, which outputs an error message: "ERROR: You need to be root to run this script". The user then runs "sudo ufw status" and is prompted for a password. The output shows the status as "inactive".

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

## Task 4

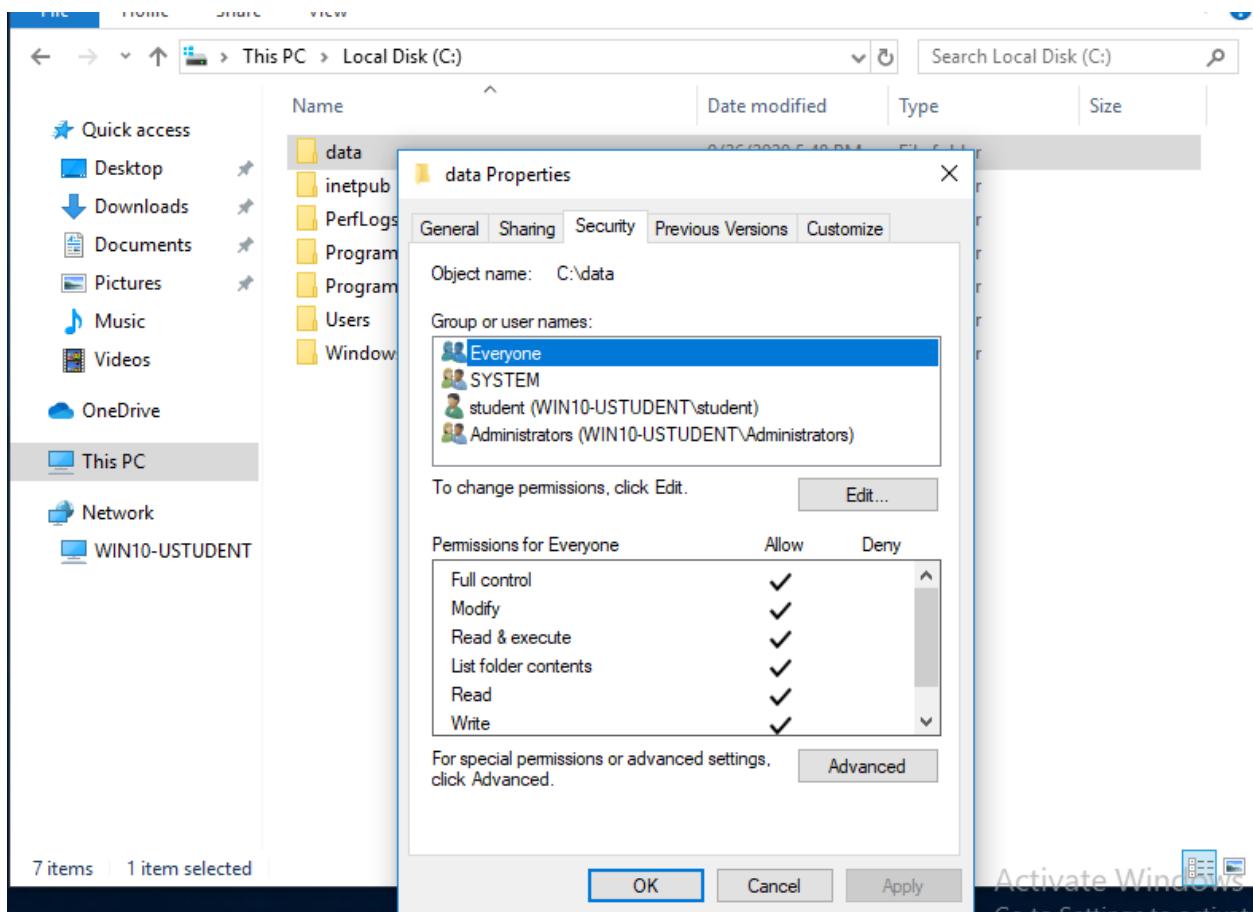
Next, conduct a Principles of Least Privilege assessment of StaticSpeed's system. We need to know:

- 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 locate "data" folder under "This PC" and see the properties and permissions it has.



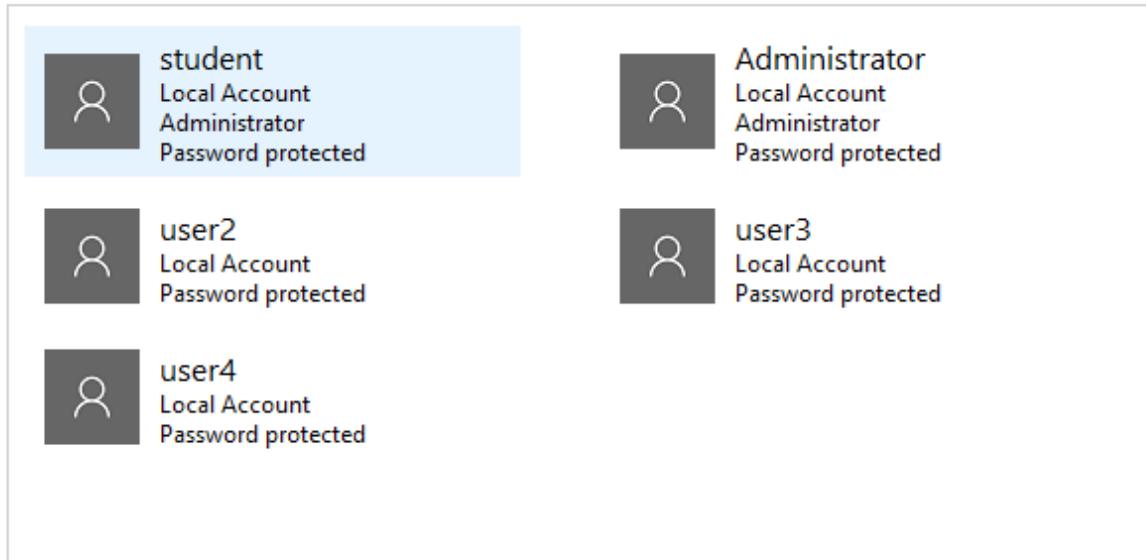
We can find this folder "data" in documents in linux.

```
ustudent@ubu-ustudent: ~/Documents
File Edit View Search Terminal Help
ustudent@ubu-ustudent:~$ cd Documents/
ustudent@ubu-ustudent:~/Documents$ ls -al
total 12
drwxr-xr-x 3 uststudent uststudent 4096 Sep 26 2020 .
drwxr-xr-x 21 uststudent uststudent 4096 Nov 26 11:17 ..
drwxrwxrwx 2 uststudent uststudent 4096 Nov 7 12:22 data
ustudent@ubu-ustudent:~/Documents$ ls -al data/
total 36
drwxrwxrwx 2 uststudent uststudent 4096 Nov 7 12:22 .
drwxr-xr-x 3 uststudent uststudent 4096 Sep 26 2020 ..
-rw-rw-r-- 1 uststudent uststudent 24910 Sep 26 2020 credit_applications_202009270
00927_9768.csv
```

```
ustudent@ubu-ustudent: ~/Documents
File Edit View Search Terminal Help
usbmux:x:107:46:usbmux daemon,,,,:/var/lib/usbmux:/usr/sbin/nologin
dnsmasq:x:108:65534:dnsmasq,,,,:/var/lib/misc:/usr/sbin/nologin
rtkit:x:109:114:RealtimeKit,,,,:/proc:/usr/sbin/nologin
speech-dispatcher:x:110:29:Speech Dispatcher,,,,:/var/run/speech-dispatcher:/bin/false
whoopsie:x:111:117::/nonexistent:/bin/false
kernoops:x:112:65534:Kernel Oops Tracking Daemon,,,,:/usr/sbin/nologin
saned:x:113:119::/var/lib/saned:/usr/sbin/nologin
pulse:x:114:120:PulseAudio daemon,,,,:/var/run/pulse:/usr/sbin/nologin
avahi:x:115:122:Avahi mDNS daemon,,,,:/var/run/avahi-daemon:/usr/sbin/nologin
colord:x:116:123:colord colour management daemon,,,,:/var/lib/colord:/usr/sbin/nologin
hplip:x:117:7:HPLIP system user,,,,:/var/run/hplip:/bin/false
geoclue:x:118:124::/var/lib/geoclue:/usr/sbin/nologin
gnome-initial-setup:x:119:65534::/run/gnome-initial-setup/:/bin/false
gdm:x:120:125:Gnome Display Manager:/var/lib/gdm3:/bin/false
ustudent:x:1000:1000:ustudent,,,,:/home/ustudent:/bin/bash
sshd:x:121:65534::/run/sshd:/usr/sbin/nologin
lightdm:x:122:127:Light Display Manager:/var/lib/lightdm:/bin/false
guest:x:1001:1001:guest,,,,:/home/guest:/bin/bash
ftp:x:1002:1002::/var/ftp:/bin/sh
telnetd:x:123:131::/nonexistent:/usr/sbin/nologin
tftp:x:124:132:tftp daemon,,,,:/var/lib/tftpboot:/usr/sbin/nologin
user3:x:1003:1003:user3,,,,:/home/user3:/bin/bash
user4:x:1004:1004:user4,,,,:/home/user4:/bin/bash
user5:x:1005:1005:user5,,,,:/home/user5:/bin/bash
Debian-snmp:x:125:133::/var/lib/snmp:/bin/false
ustudent@ubu-ustudent:~/Documents$ \|\|
```

From the above screenshots we can see uststudent 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.

Choose the user you would like to change



[Add a new user in PC settings](#)

```
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

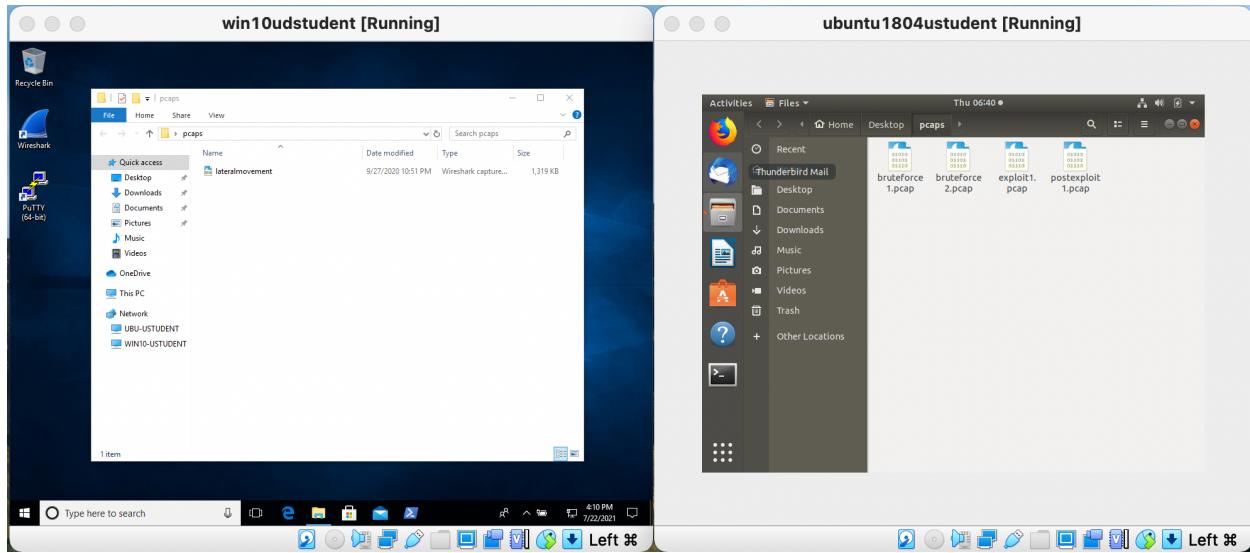
StaticSpeed has provided access to a monitoring device that has recorded some traffic marked as malicious. Please investigate and assess this further using Wireshark or tcpdump and the provided capture files (pcaps). It is also required of you to verify that appropriate logging is in place at your machines.

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:

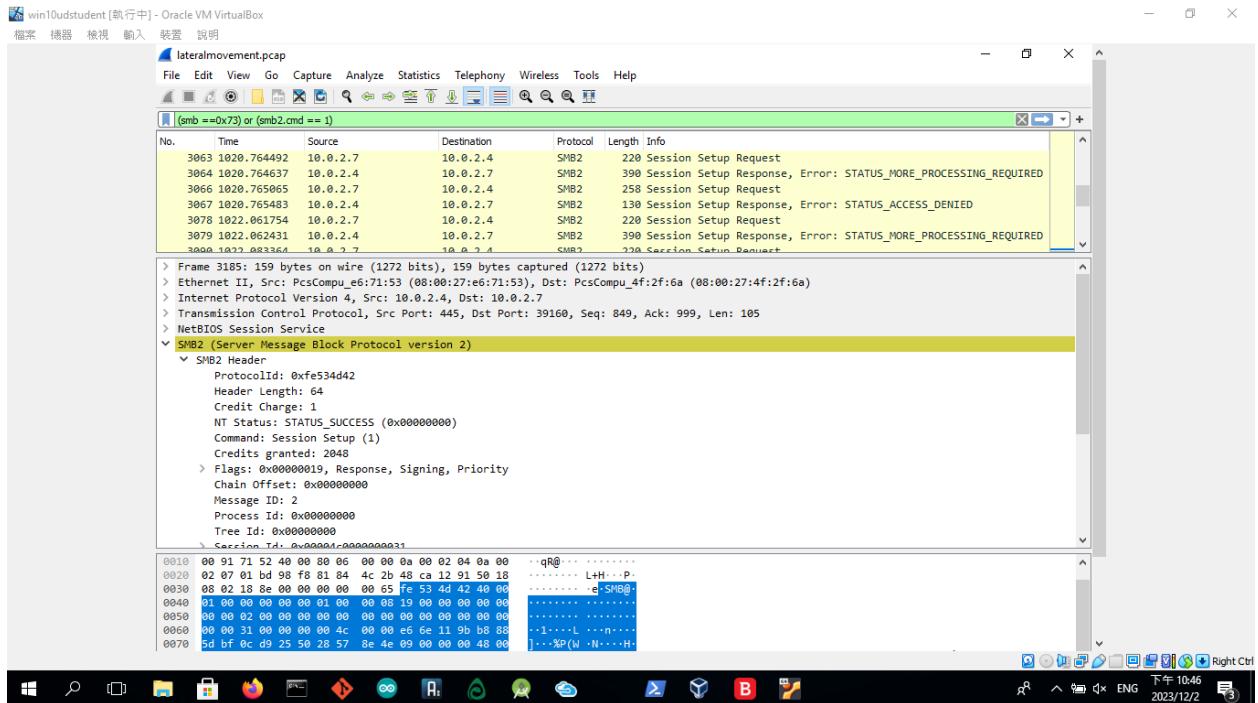
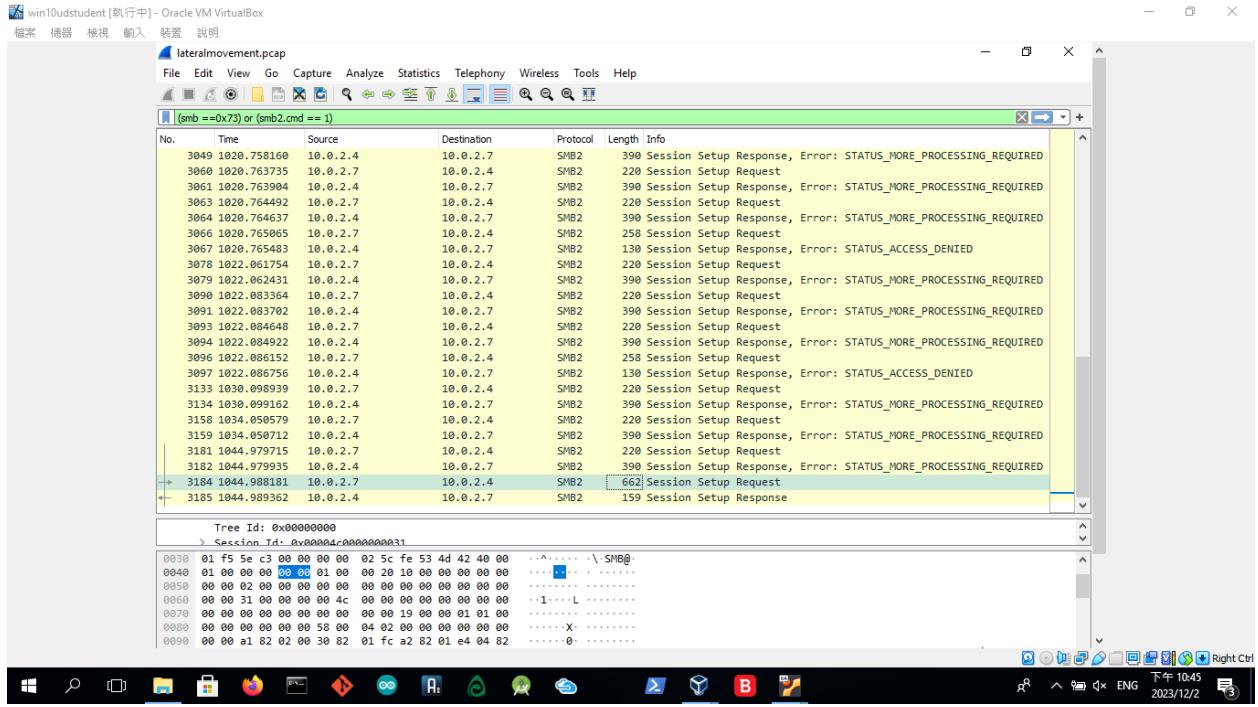
- What type of attack was recorded?
- What is the source IP of the attack?
- What protocol was targeted?
- What password was used successfully?
- Which user was compromised?

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

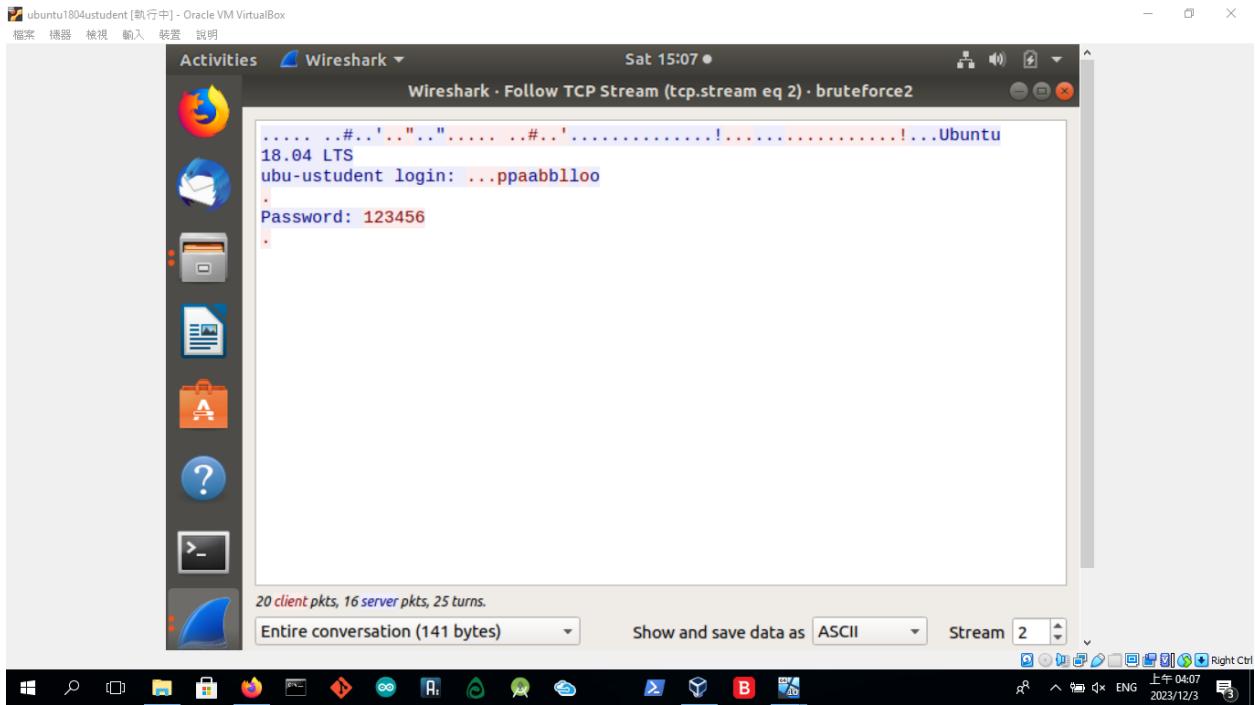
Ans:

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.

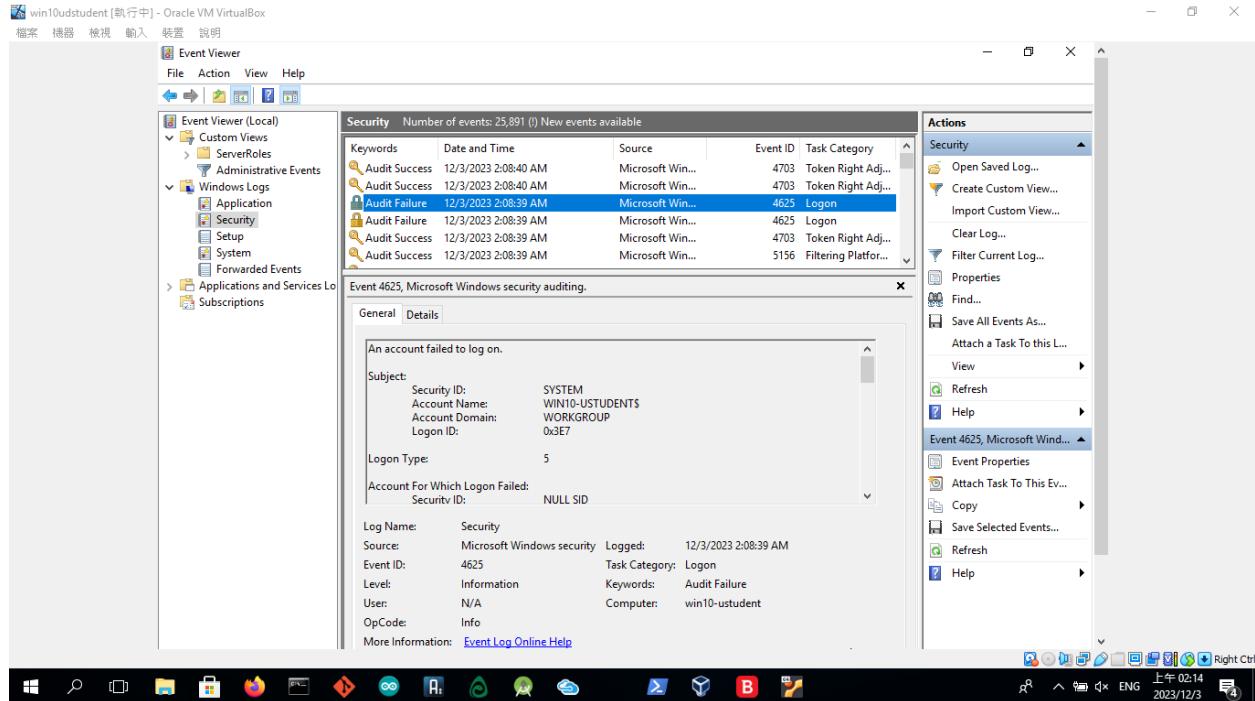
Using the logs, determine the following:

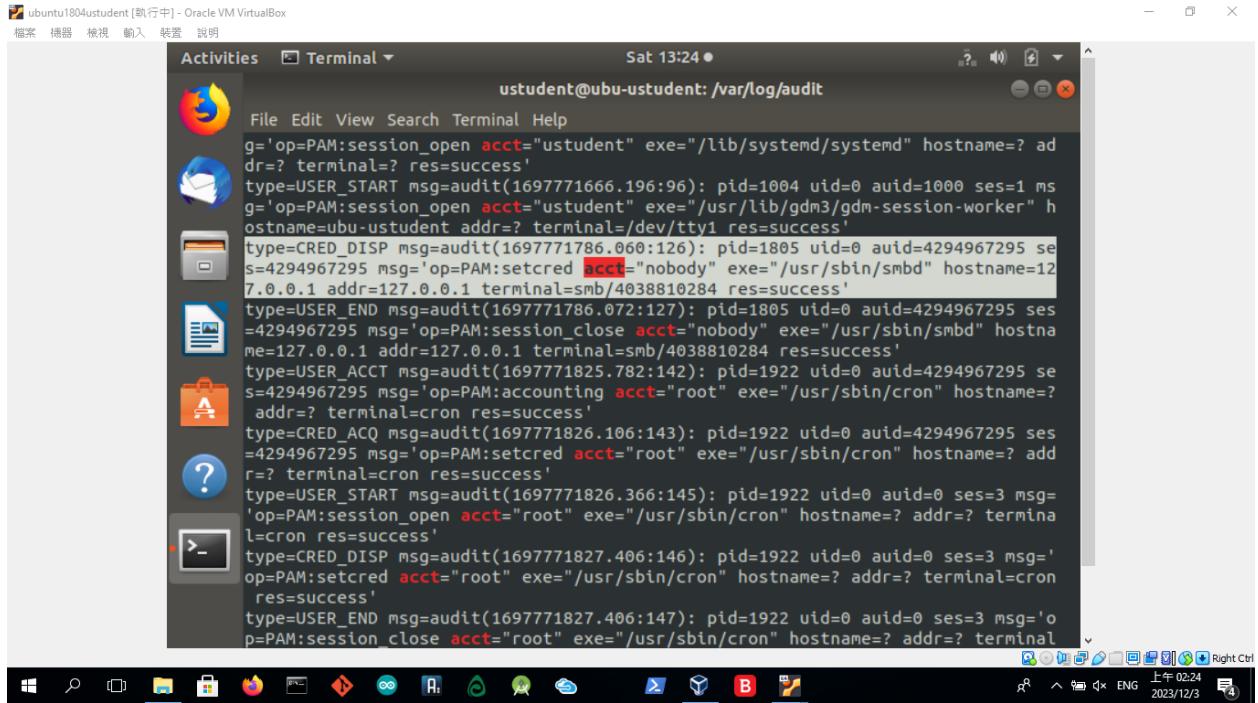
- Are there any issues with Windows Share? Please provide screenshots of your findings.
- Look at the audit logs setup at your Linux machine and find the audit.log file. What was the name of the attacker's account? Please provide screenshots.

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 and 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 StaticSpeed 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.

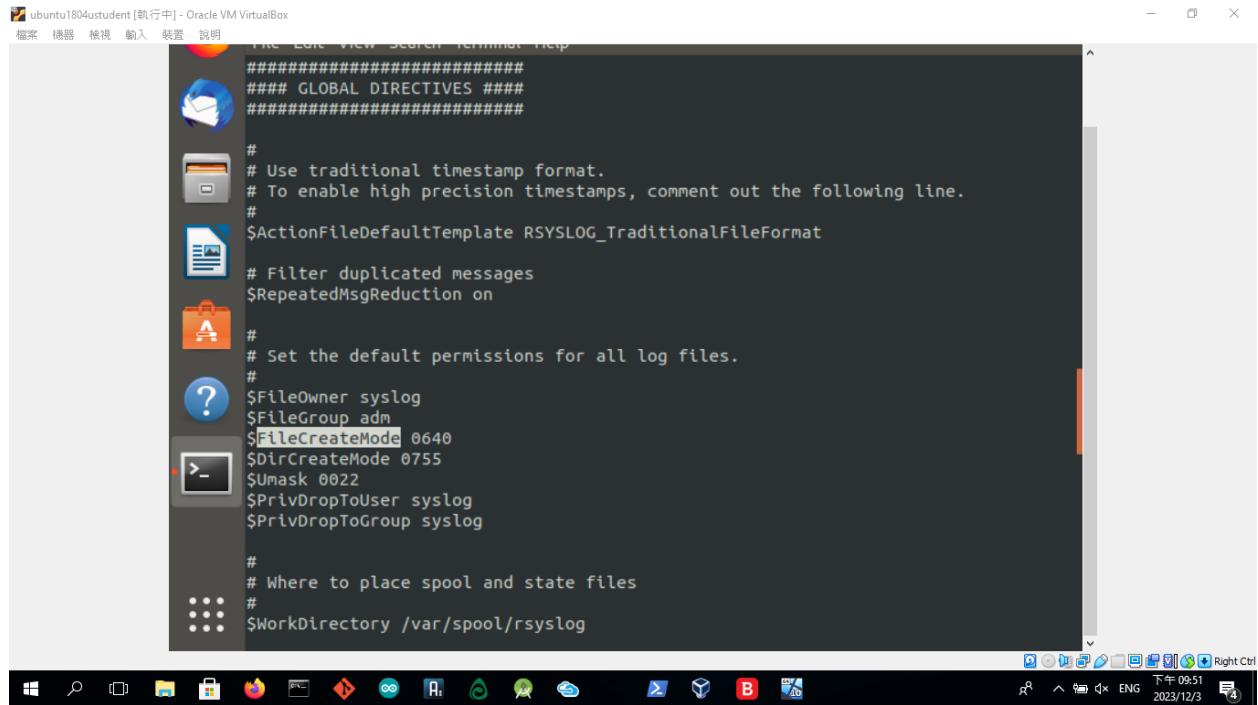
Based on your answers, suggest a course of action to ensure StaticSpeed meets our needs to use a SIEM.

Ans:

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

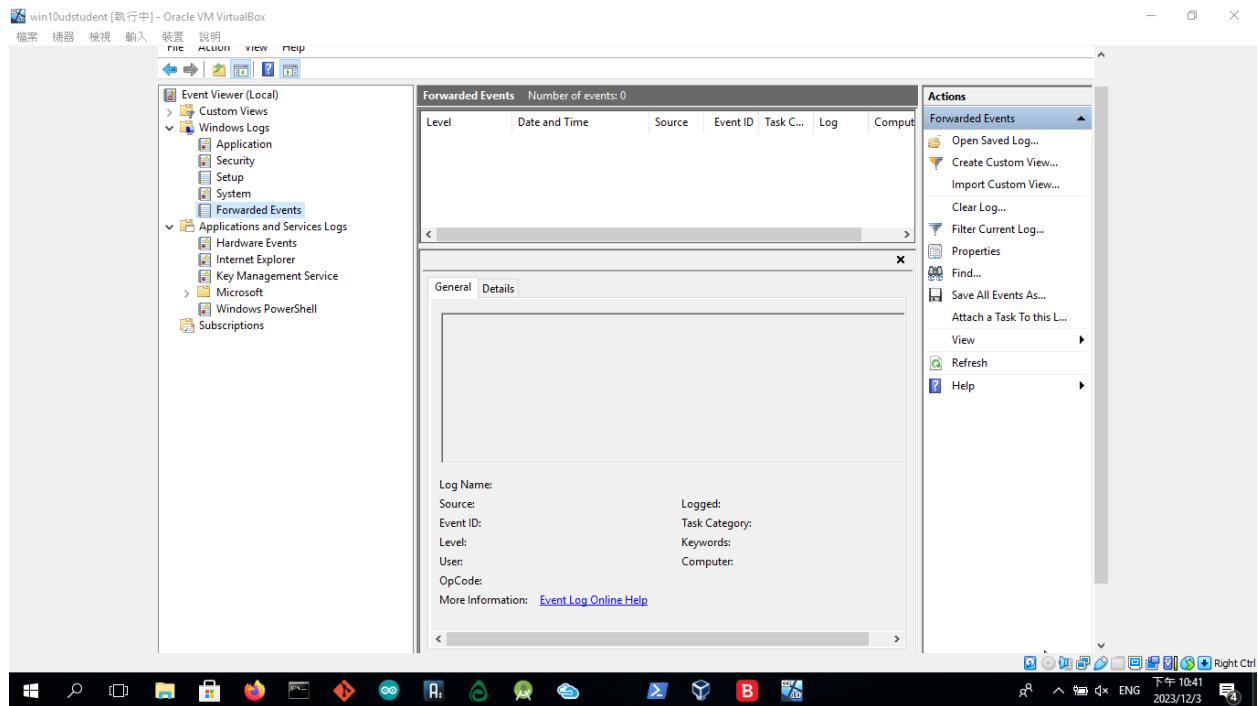
```
cat /etc/rsyslog.conf
```

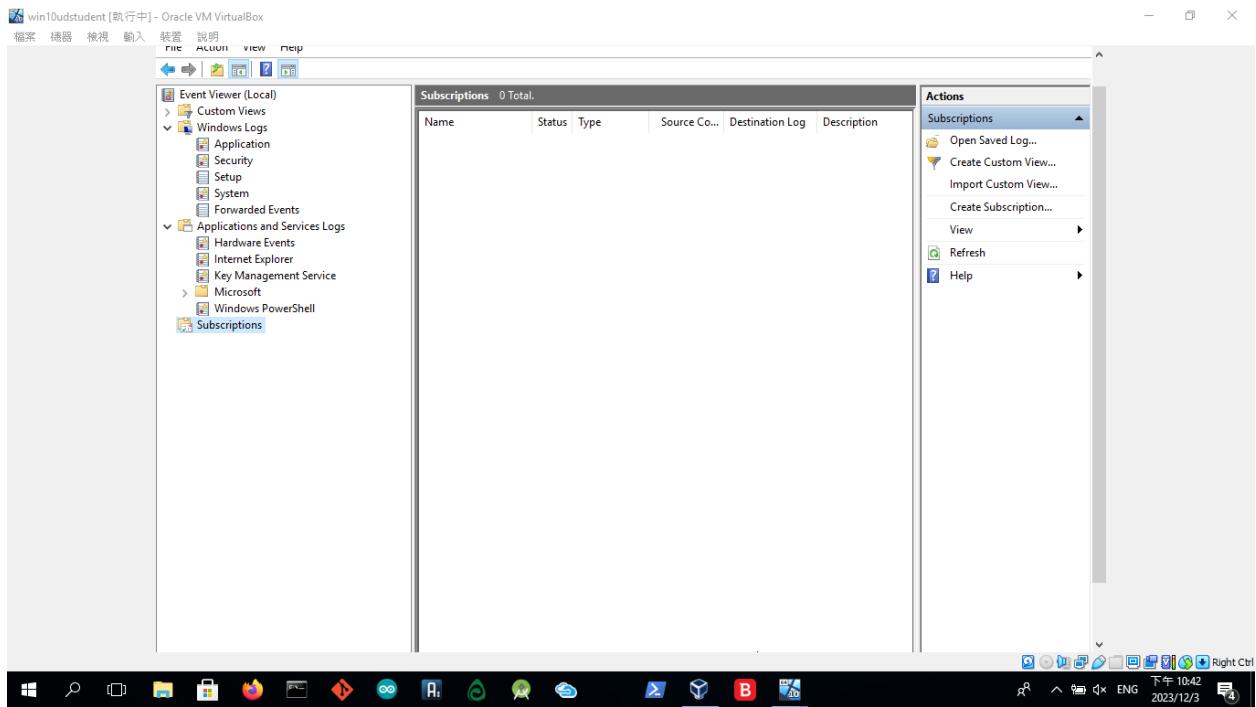
We can see the /etc/rsyslog.conf and set \$FileCreateMode to 0640.



```
ubuntu1804student [執行中] - Oracle VM VirtualBox
檔案 檔案 檢視 輸入 裝置 說明
File Edit View Search Terminal Help
#####
#### GLOBAL DIRECTIVES #####
#####
#
# Use traditional timestamp format.
# To enable high precision timestamps, comment out the following line.
#
$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat
#
# Filter duplicated messages
$RepeatedMsgReduction on
#
# Set the default permissions for all log files.
#
$FileOwner syslog
$FileGroup adm
$FileCreateMode 0640
$DirCreateMode 0755
$Umask 0022
$PrivDropToUser syslog
$PrivDropToGroup syslog
#
# Where to place spool and state files
#
$WorkDirectory /var/spool/rsyslog
```

On windows we see event viewer and subscriptions are empty which means remote subscriptions related Windows Events Forwarder is not being used.





## 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?

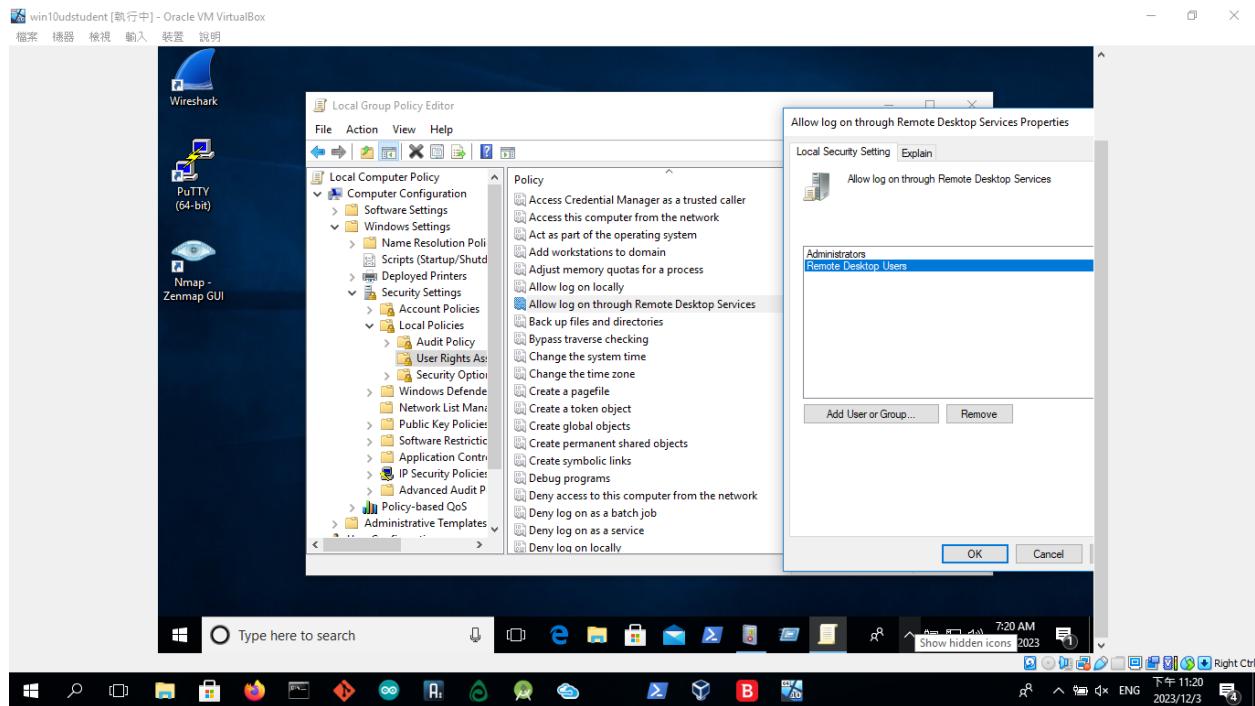
Knowing that your company only wants administrators to log remotely, provide a summary of the current situation for StaticSpeed. Then, suggest what accounts should be allowed to log remotely and why. Include your recommendations on whether StaticSpeed's authentication is acceptable and how you would 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.



```
# directly modifying this file.  
#  
# See the man page for details on how to write a sudoers file.  
#  
Defaults env_reset  
Defaults mail_badpass  
Defaults secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"  
# Host alias specification  
# User alias specification  
# Cmnd alias specification  
# User privilege specification  
root    ALL=(ALL:ALL) ALL  
# Members of the admin group may gain root privileges  
%admin  ALL=(ALL:ALL) ALL  
# Allow members of group sudo to execute any command  
%sudo   ALL=(ALL:ALL) ALL  
# See sudoers(5) for more information on "#include" directives:  
#includedir /etc/sudoers.d  
ustudent@uba-ustudent:~$
```

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

```
#HostKey /etc/ssh/ssh_host_rsa_key  
#HostKey /etc/ssh/ssh_host_ecdsa_key  
#HostKey /etc/ssh/ssh_host_ed25519_key  
# Ciphers and keying  
#RekeyLimit default none  
# Logging  
#SyslogFacility AUTH  
#LogLevel INFO  
# Authentication:  
#LoginGraceTime 2m  
#PermitRootLogin prohibit-password  
#StrictModes yes  
#MaxAuthTries 6  
#MaxSessions 10  
#PubkeyAuthentication yes  
# Expect .ssh/authorized_keys2 to be disregarded by default in future.  
#AuthorizedKeysFile    .ssh/authorized_keys .ssh/authorized_keys2  
#AuthorizedPrincipalsFile none  
#AuthorizedKeysCommand none  
#AuthorizedKeysCommandUser nobody
```

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:

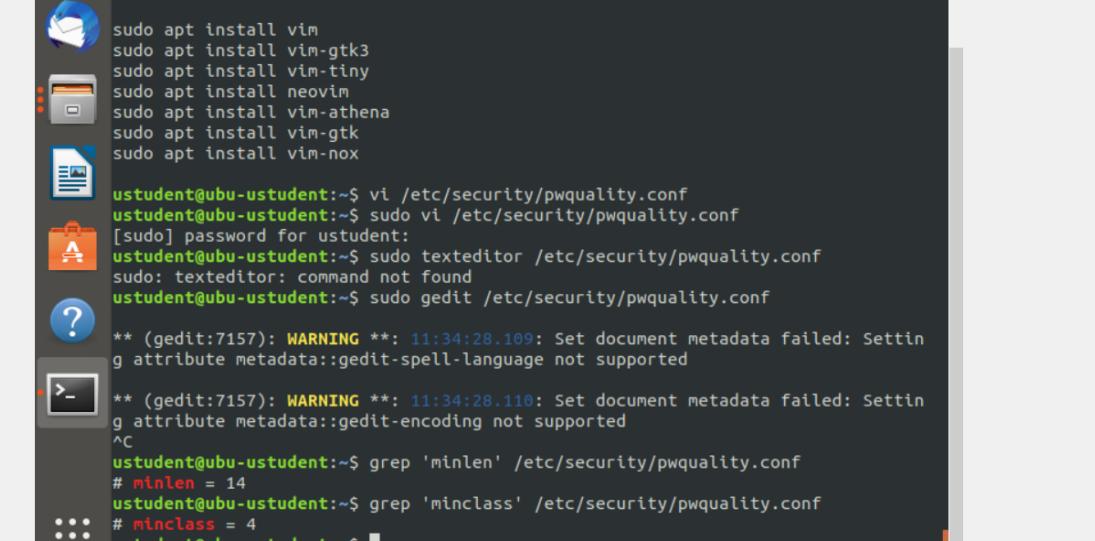
On Linux use the following command:

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)



The screenshot shows a Linux desktop environment with a terminal window open. The terminal window has a dark background and displays the following text:

```
FIRE LOG VIEW Search Terminal Help
Command 'vim' not found, but can be installed with:
sudo apt install vim
sudo apt install vim-gtk3
sudo apt install vim-tiny
sudo apt install neovim
sudo apt install vim-athena
sudo apt install vim-gtk
sudo apt install vim-nox

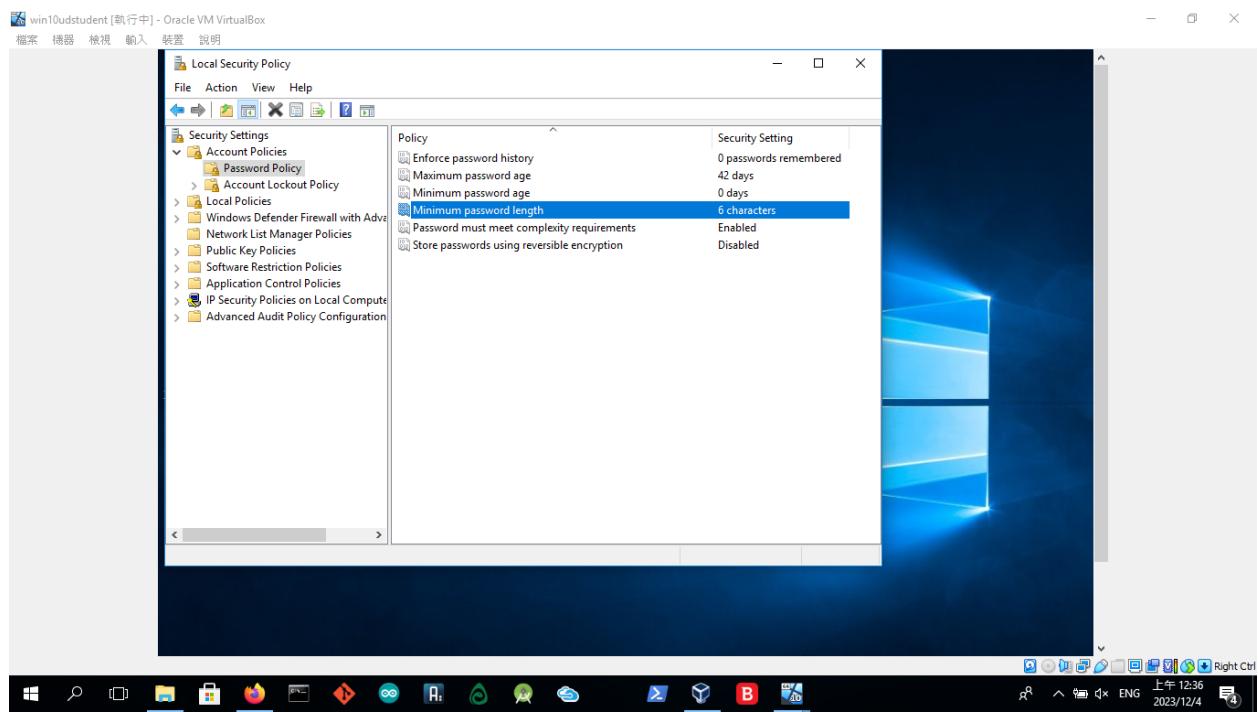
ustudent@ubu-ustudent:~$ vi /etc/security/pwquality.conf
ustudent@ubu-ustudent:~$ sudo vi /etc/security/pwquality.conf
[sudo] password for uststudent:
ustudent@ubu-ustudent:~$ sudo texteditor /etc/security/pwquality.conf
sudo: texteditor: command not found
ustudent@ubu-ustudent:~$ sudo gedit /etc/security/pwquality.conf

** (gedit:7157): WARNING **: 11:34:28.109: Set document metadata failed: Setting attribute metadata::gedit-spell-language not supported

** (gedit:7157): WARNING **: 11:34:28.110: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported
^C
ustudent@ubu-ustudent:~$ grep 'minlen' /etc/security/pwquality.conf
# minlen = 14
ustudent@ubu-ustudent:~$ grep 'minclass' /etc/security/pwquality.conf
# minclass = 4
ustudent@ubu-ustudent:~$
```

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.

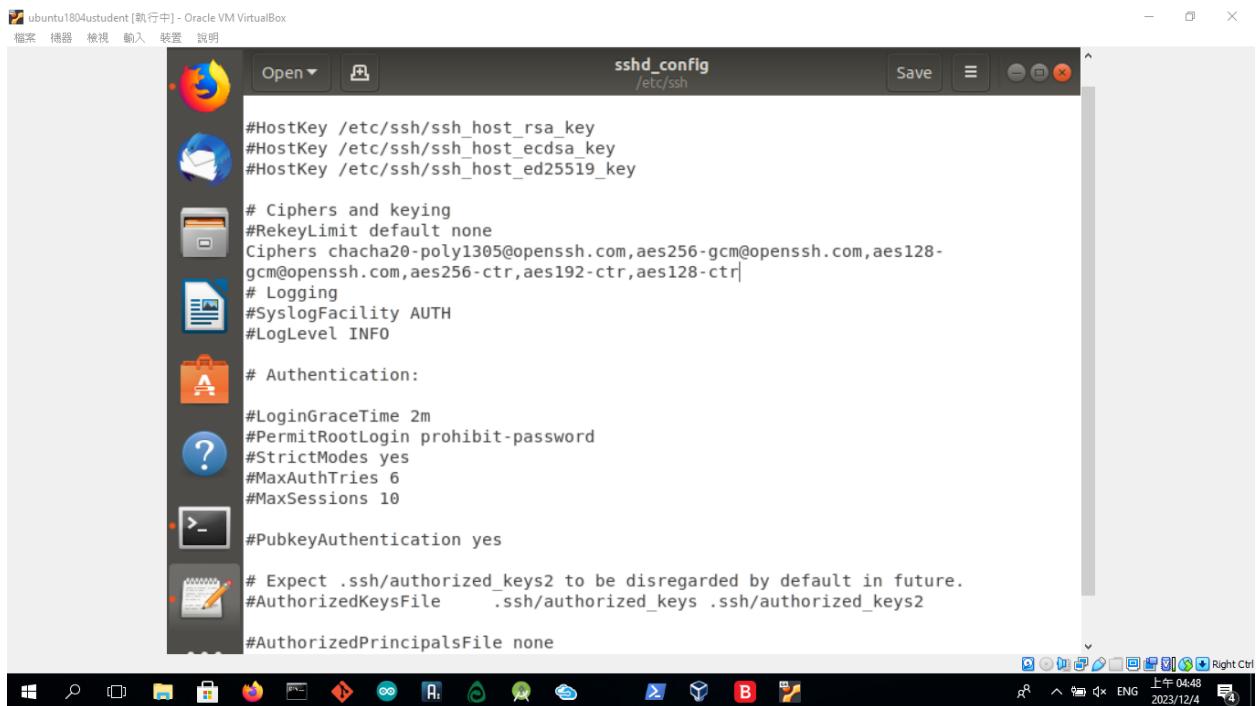


## Task 3

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.



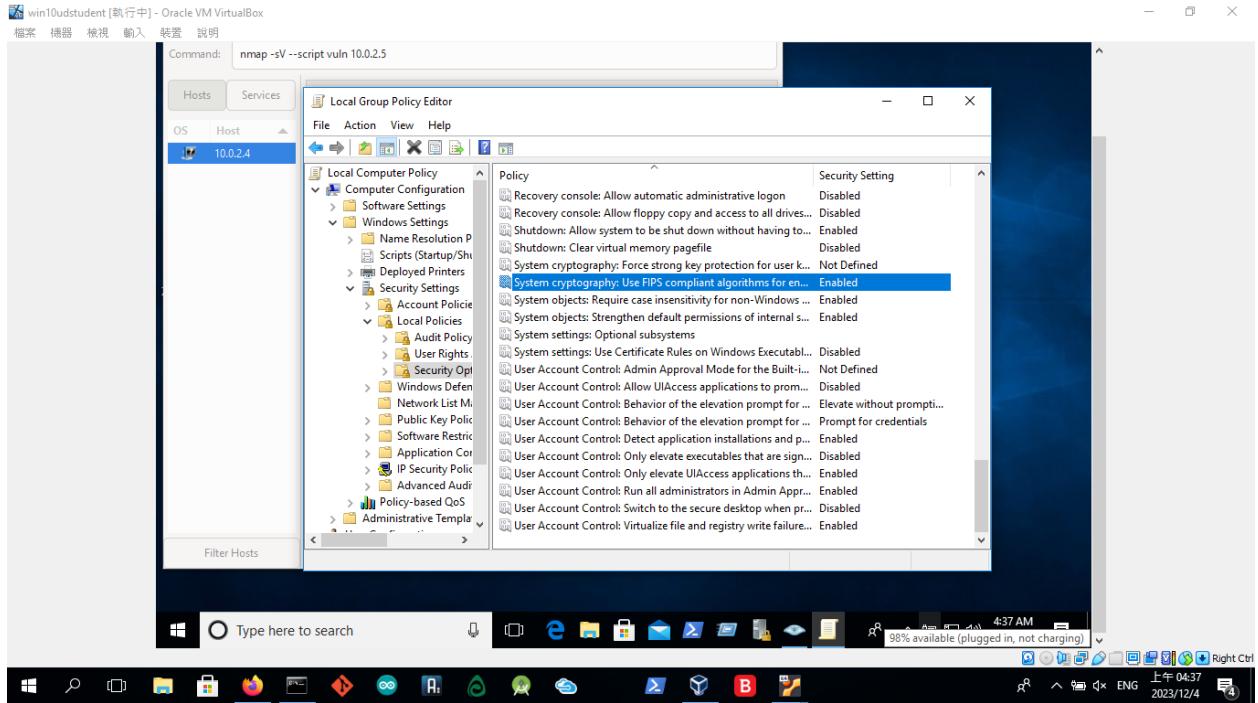
```
#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none
Ciphers chacha20-poly1305@openssh.com,aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr
# Logging
#SyslogFacility AUTH
#LogLevel INFO

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

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

On Windows we enable FIPS configuration.

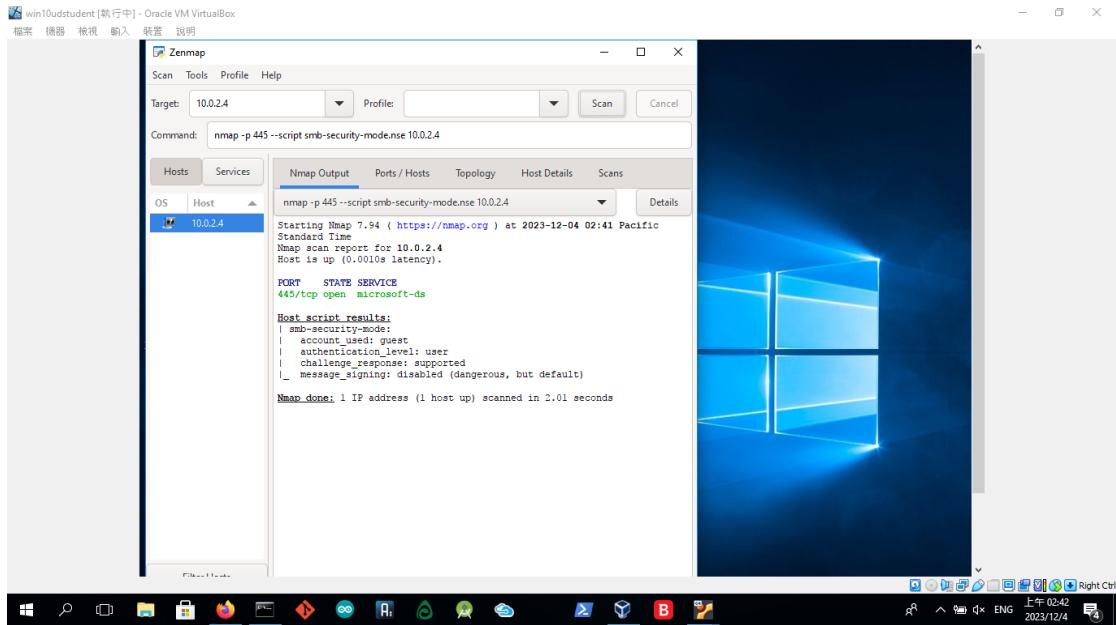


## Task 4

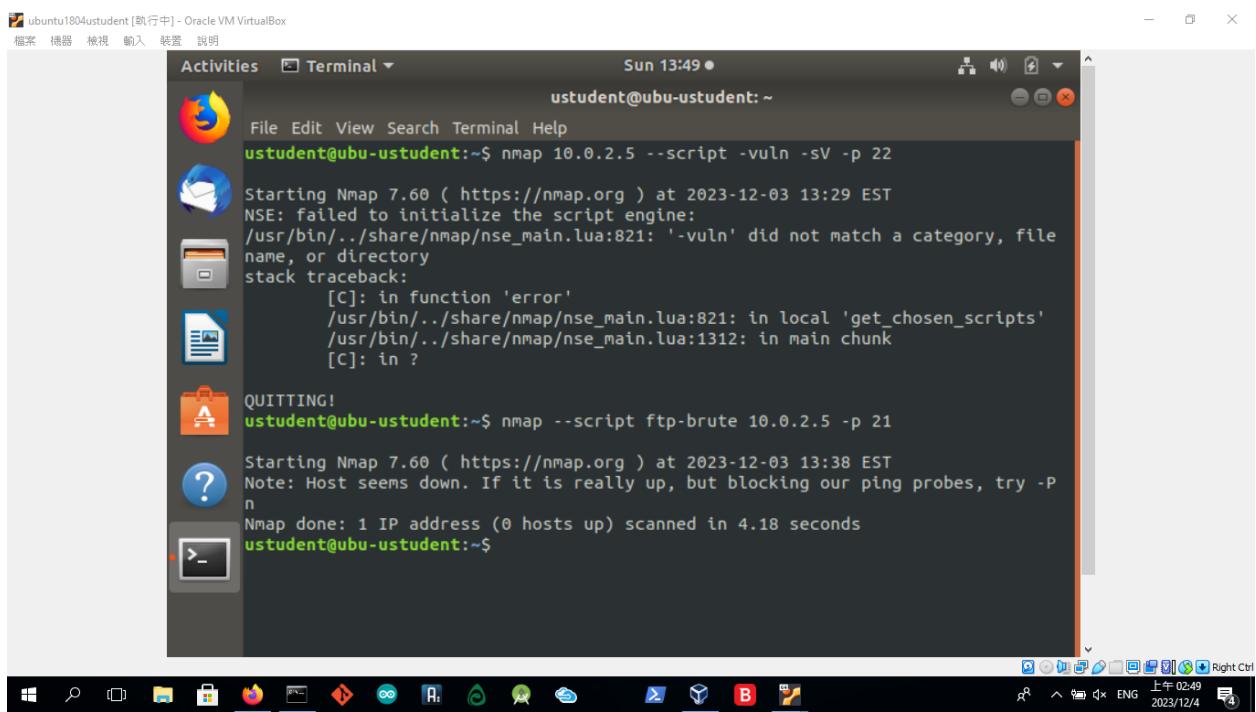
**Conduct** aggressive testing for password strength. Use a Nmap NSE Script to test how easy it would be to access StaticSpeed's FTP Server and SMB Shares if an attacker probed them. We have already requested and obtained permission to perform these audits.

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	CVE-2009-1133	CVE-2002-1141	CVE-2011-1002	x

**IP Address: 10.0.2.4**

Service	Port	Sensitive Level
microsoft-ds	445 TCP	High
msrpc	135 TCP	Medium
xxx	TCP	Low
xxx	xx TCP	Log

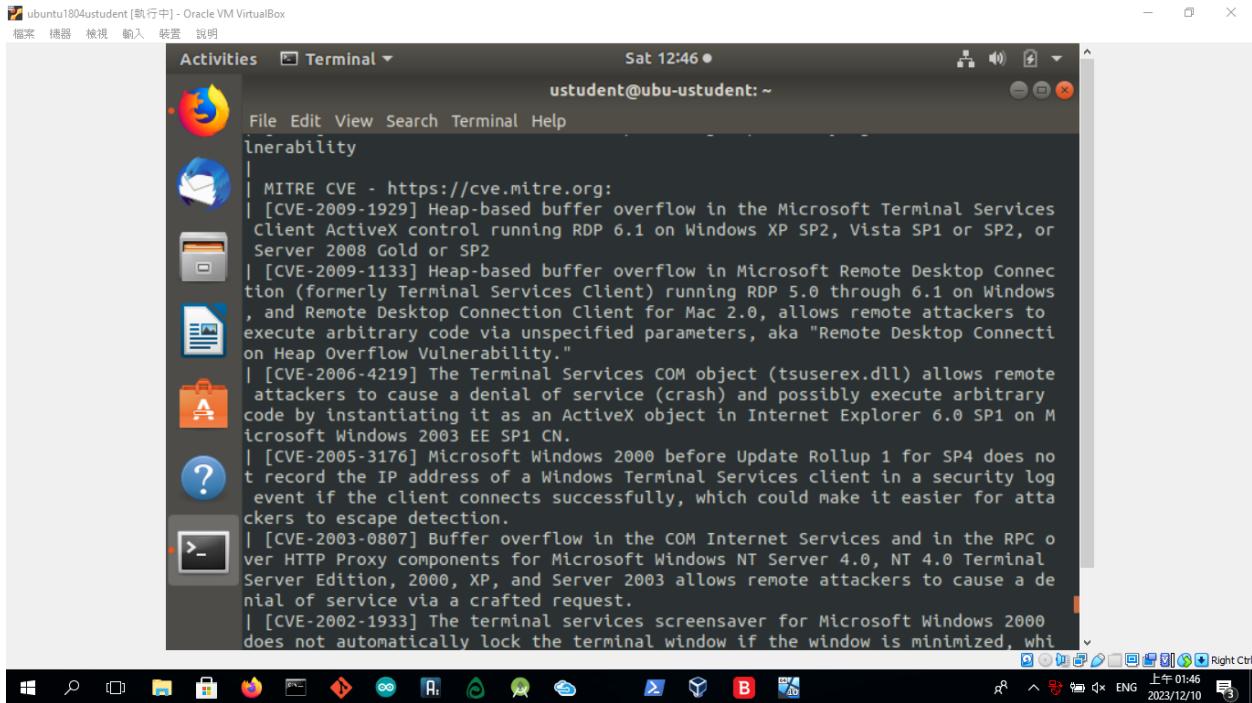
Expected detail format for vulnerabilities found

**High**

**1- CVE-2009-1133**

**Issue**

Heap-based buffer overflow in Microsoft Remote Desktop Connection (formerly Terminal Services Client) running RDP 5.0 through 6.1 on Windows.



The screenshot shows a terminal window titled "Terminal" with the command "inherability" entered. The output lists several CVE entries:

- | MITRE CVE - <https://cve.mitre.org>:
- | [CVE-2009-1929] Heap-based buffer overflow in the Microsoft Terminal Services Client ActiveX control running RDP 6.1 on Windows XP SP2, Vista SP1 or SP2, or Server 2008 Gold or SP2
- | [CVE-2009-1133] Heap-based buffer overflow in Microsoft Remote Desktop Connection (formerly Terminal Services Client) running RDP 5.0 through 6.1 on Windows, and Remote Desktop Connection Client for Mac 2.0, allows remote attackers to execute arbitrary code via unspecified parameters, aka "Remote Desktop Connection Heap Overflow Vulnerability."
- | [CVE-2006-4219] The Terminal Services COM object (tsuserex.dll) allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code by instantiating it as an ActiveX object in Internet Explorer 6.0 SP1 on Microsoft Windows 2003 EE SP1 CN.
- | [CVE-2005-3176] Microsoft Windows 2000 before Update Rollup 1 for SP4 does not record the IP address of a Windows Terminal Services client in a security log event if the client connects successfully, which could make it easier for attackers to escape detection.
- | [CVE-2003-0807] Buffer overflow in the COM Internet Services and in the RPC over HTTP Proxy components for Microsoft Windows NT Server 4.0, NT 4.0 Terminal Server Edition, 2000, XP, and Server 2003 allows remote attackers to cause a denial of service via a crafted request.
- | [CVE-2002-1933] The terminal services screensaver for Microsoft Windows 2000 does not automatically lock the terminal window if the window is minimized, whi

The terminal window is part of a desktop environment with a taskbar at the bottom showing various application icons.

## Impact

Allows remote attackers to execute arbitrary code via unspecified parameters, aka "Remote Desktop Connection Heap Overflow Vulnerability."

## Mitigation

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

## Reference

<https://www.cvedetails.com/cve/CVE-2009-1133/?q=CVE-2009-1133>

## Medium

### 1- CVE-2002-1141

#### Issue

An input validation error in the Sun Microsystems RPC library Services for Unix 3.0 Interix SD, as implemented on Microsoft Windows NT4, 2000, and XP

The screenshot shows a terminal window titled "Terminal" with the command "ustudent@ubu-ustudent: ~" at the top. The window displays a list of security vulnerabilities:

- | [CVE-2002-1141] An input validation error in the Sun Microsystems RPC library Services for Unix 3.0 Interix SD, as implemented on Microsoft Windows NT4, 2000, and XP, allows remote attackers to cause a denial of service via malformed fragmented RPC client packets, aka "Denial of service by sending an invalid RPC request."
- | [CVE-2002-1140] The Sun Microsystems RPC library Services for Unix 3.0 Interix SD, as implemented on Microsoft Windows NT4, 2000, and XP, allows remote attackers to cause a denial of service (service hang) via malformed packet fragments, aka "Improper parameter size check leading to denial of service."
- | [CVE-2002-0719] SQL injection vulnerability in the function that services for Microsoft Content Management Server (MCMS) 2001 allows remote attackers to execute arbitrary commands via an MCMS resource request for image files or other files.
- | [CVE-2002-0697] Microsoft Metadirectory Services (MMS) 2.2 allows remote attackers to bypass authentication and modify sensitive data by using an LDAP client to directly connect to MMS and bypass the checks for MMS credentials.
- | [CVE-2002-0694] The HTML Help facility in Microsoft Windows 98, 98 Second Edition, Millennium Edition, NT 4.0, NT 4.0 Terminal Server Edition, Windows 2000, and Windows XP uses the Local Computer Security Zone when opening .chm files from the Temporary Internet Files folder, which allows remote attackers to execute arbitrary code via HTML mail that references or inserts a malicious .chm file containing shortcuts that can be executed, aka "Code Execution via Compiled HTML Help File."
- | [CVE-2002-0693] Buffer overflow in the HTML Help ActiveX Control (hhctrl.ocx) in Microsoft Windows 98, 98 Second Edition, Millennium Edition, NT 4.0, NT 4.0

The terminal window has a dark theme and includes a dock with various application icons at the bottom.

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

## Impact

Allows remote attackers to cause a denial of service via malformed fragmented RPC client packets, aka "Denial of service by sending an invalid RPC request."

## Mitigation

Applying the patch MS02-057 is able to eliminate this problem.

## Reference

<https://www.cvedetails.com/cve/CVE-2002-1141/>

Low

## 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

```
ubuntu1804student [正在运行] - Oracle VM VirtualBox
File Edit View Search Terminal Help
ustudent@ubu-ustudent:~$ nmap -sV --script vuln 10.0.2.4
Starting Nmap 7.60 ( https://nmap.org ) at 2023-12-06 18:45 EST
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.251
|       After NULL UDP avahi packet DoS (CVE-2011-1002).
|       Hosts are all up (not vulnerable).
Nmap scan report for 10.0.2.4
Host is up (0.0015s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE      VERSION
7/tcp      open  echo
9/tcp      open  discard?
13/tcp     open  daytime      Microsoft Windows USA daytime
17/tcp     open  qotd        Windows qotd (English)
19/tcp     open  chargen
80/tcp     open  http         Microsoft IIS httpd 10.0
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-server-header: Microsoft-IIS/10.0
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
3389/tcp   open  ms-wbt-server Microsoft Terminal Services
| ssl-ccs-injection: No reply from server (TIMEOUT)
```

## 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

Upgrading to version 0.6.11 eliminates this vulnerability. Applying a patch is able to eliminate this problem.

## Reference

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

## 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 →/#content-security-policy	<a href="https://owasp.org/www-project-secure-headers">https://owasp.org/www-project-secure-headers</a>
Feature-Policy →/#feature-policy	<a href="https://owasp.org/www-project-secure-headers">https://owasp.org/www-project-secure-headers</a>
Referrer-Policy →/#referrer-policy	<a href="https://owasp.org/www-project-secure-headers">https://owasp.org/www-project-secure-headers</a>
X-Content-Type-Options →/#x-content-type-options	<a href="https://owasp.org/www-project-secure-headers">https://owasp.org/www-project-secure-headers</a>
X-Frame-Options →/#x-frame-options	<a href="https://owasp.org/www-project-secure-headers">https://owasp.org/www-project-secure-headers</a>
X-Permitted-Cross-Domain-Policies →/#x-permitted-cross-domain-policies	<a href="https://owasp.org/www-project-secure-headers">https://owasp.org/www-project-secure-headers</a>
X-XSS-Protection →/#x-xss-protection	<a href="https://owasp.org/www-project-secure-headers">https://owasp.org/www-project-secure-headers</a>

## References

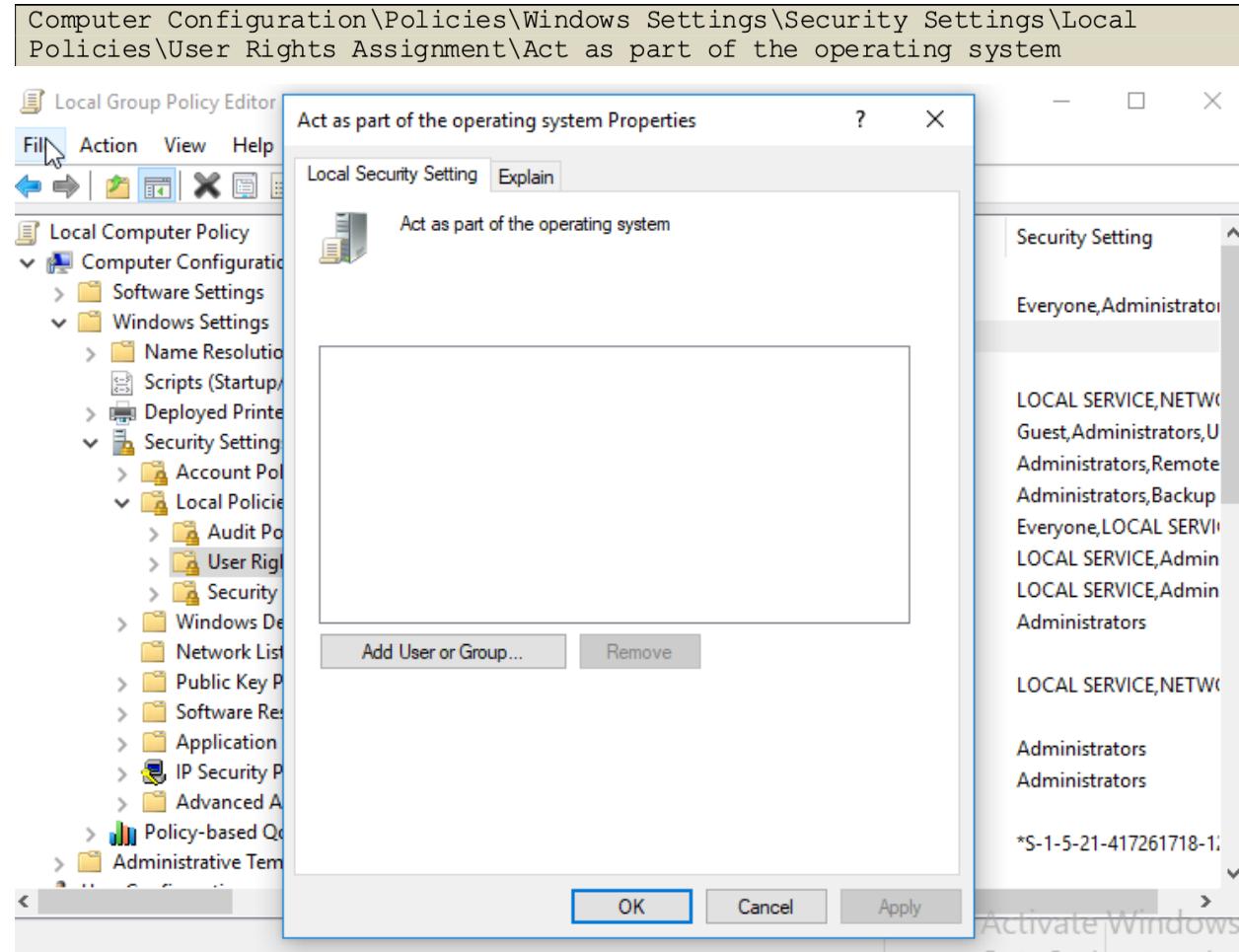
- <https://owasp.org/www-project-secure-headers/>
- <https://owasp.org/www-project-secure-headers/#div-headers>
- <https://securityheaders.io>

## 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:



**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	<b>CVE-2017-7494</b>	<b>CVE-2011-2523</b>	<b>CVE-2011-1002</b>	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.

```

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 may 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 deference
|     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@uba-ustudent:~$ █

```

## 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>

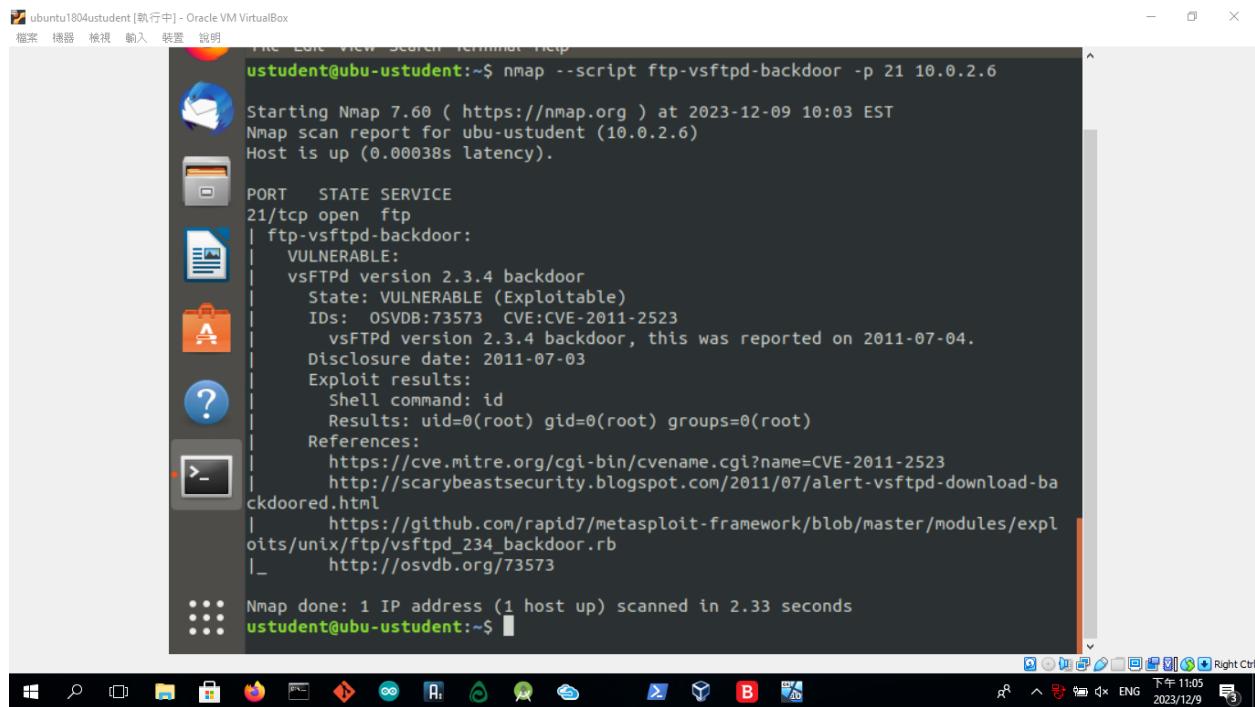
<https://access.redhat.com/security/cve/cve-2017-7494>

**Medium**

**1- CVE-2011-2523**

## Issue

This version of FTP is vulnerable to Backdoor.



```
ubuntu1804student [執行中] - Oracle VM VirtualBox
File Edit View Search Terminal Help
ustudent@ubu-ustudent:~$ nmap --script ftp-vsftpd-backdoor -p 21 10.0.2.6
Starting Nmap 7.60 ( https://nmap.org ) at 2023-12-09 10:03 EST
Nmap scan report for ubu-ustudent (10.0.2.6)
Host is up (0.00038s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
|  ftp-vsftpd-backdoor:
|    VULNERABLE:
|      vsFTPD version 2.3.4 backdoor
|        State: VULNERABLE (Exploitable)
|        IDs: OSVDB:73573 CVE: CVE-2011-2523
|          vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|          Disclosure date: 2011-07-03
|          Exploit results:
|            Shell command: id
|              Results: uid=0(root) gid=0(root) groups=0(root)
|              References:
|                https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|                http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-ba
|                  ckdoored.html
|                  https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|_
|__ http://osvdb.org/73573

Nmap done: 1 IP address (1 host up) scanned in 2.33 seconds
ustudent@ubu-ustudent:~$
```

## Impact

Trigger the malicious `vsf_sysutil_extra()` function by sending a sequence of specific bytes on port 21, which, on successful execution, results in opening the backdoor on port 6200 of the system.

## Mitigation

Upgrade vsftpd version.

## Reference

- <https://www.hackingdna.com/2020/09/exploit-vsftpd-208.html>
- <https://nvd.nist.gov/vuln/detail/CVE-2011-2523>
- <https://access.redhat.com/security/cve/cve-2011-2523>

Low

## 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@uba-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=653732A2XP=x86_64-pc-linux-gnu%R(NUL
SF:L,22,"A\x20is\x20for\x20Apple.\.\n\tt--\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

Upgrading to version 0.6.11 eliminates this vulnerability. Applying a patch is able to eliminate this problem.

## Reference

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1022>

<https://access.redhat.com/security/cve/cve-2011-1002>

# Example of Log

## Log

### 3 - Telnet Unencrypted Cleartext Login

#### Issue

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

```
nmap -p 23 -T4 -A -v 10.0.2.5
Initiating OS detection (try #1) against 10.0.2.5
NSE: Script scanning 10.0.2.5.
Initiating NSE at 17:32
Completed NSE at 17:32, 7.03s elapsed
Initiating NSE at 17:32
Completed NSE at 17:32, 0.00s elapsed
Initiating NSE at 17:32
Completed NSE at 17:32, 0.00s elapsed
Nmap scan report for 10.0.2.5
Host is up (0.0022s latency).

PORT      STATE SERVICE VERSION
23/tcp    open  telnet  Linux telnetd
MAC Address: 08:00:27:F7:A0:CA (Oracle VirtualBox
virtual NIC)
Warning: OSScan results may be unreliable because we
could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 3.X|4.X
OS_CPE: cpe:/o:linux:linux_kernel:3 cpe://
o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Uptime guess: 48.220 days (since Tue Aug 18 12:16:11
2020)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

#### 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
<b>18.9.102.2</b>	<b>1.2.1</b>
<b>18.3.4</b>	<b>1.6.1, 1.6.2</b>
<b>1.1.5</b>	<b>4.2.1.3</b>
	<b>5.3.1</b>

## 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.

Ans:

- Integrating this network into the extended network of our company will bring many new risks and exposures as you can see there are many high risk CVE discovered in the final report.
- Third-party risk is the possibility that your company will suffer a negative outcome if you decide to use software developed by a third party or outsource specific services to complete specific tasks.
- Software upgrade for the system: Replacing an old product with a newer model of the same product is called upgrading.
- A collection of internationally acknowledged and consensus-driven best practices, CIS Benchmarks are provided by the Center for Internet Security (CIS) to assist security practitioners in setting up and maintaining their cybersecurity defenses.
- Reduce the impact of compromise by implementing the least privilege and zero trust principles.
- By using VLANs, the network can be segmented to prevent collisions.
- Blocking threat actors' IP addresses with IP security helps reduce the likelihood of a compromise.
- Allowing only the services and protocols required for remote access, and restricting or disabling any others.
- By default, IPv6 is used, which means that logging settings and monitoring devices might overlook it. This gives attackers a possible point of entry.
- Systems that have an inactive firewall may be more susceptible to malicious actors' attacks and illegal access.
- Depending on the type of network, firewall policies can be configured with security rules that either allow or prohibit access to prevent potential hacker or virus attacks.
- Since this folder may contain important company data, only the authorized user should be able to access it.
- The simplest method of preventing brute-force assaults is to simply lock users out of their accounts after a certain amount of unsuccessful password tries.
- A standard risk assessment entails determining which information assets—such as targeted ports, services, and protocols, as well as source and destination IP hardware—may be impacted by a cyberattack.
- The technique of recording activities within the software platforms utilized by your entire firm is called audit logging.

- When an update is installed and files are moved around the Windows directory, this is known as configuring Windows updates.
- Remote Desktop Protocol (RDP) is a secure network communication protocol that necessitates user authentication prior to the establishment of a server connection.
- A collection of compliance best practices for various IT products and systems is provided by the Center for Internet Security (CIS) benchmarks. These standards offer the foundational setups necessary to guarantee CIS compliance as well as adherence to industry-agreed.