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.

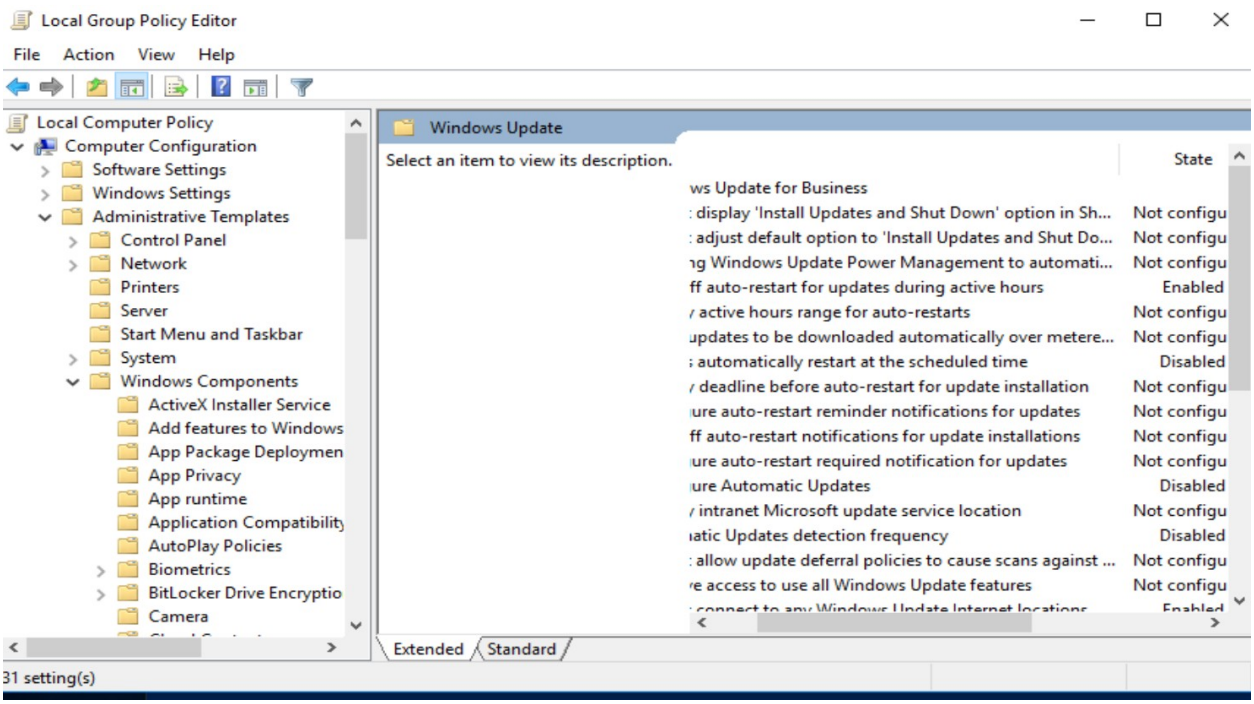
You must download the CIS Benchmark PDFs for Ubuntu 18.04 v2.01 and Windows 10 Ent v1.9.0. In these PDFs, there will be all the information related to the CIS Benchmarks requested in the following tasks which need to be included in your final report. In order to perform the vulnerability scans via Nmap 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.

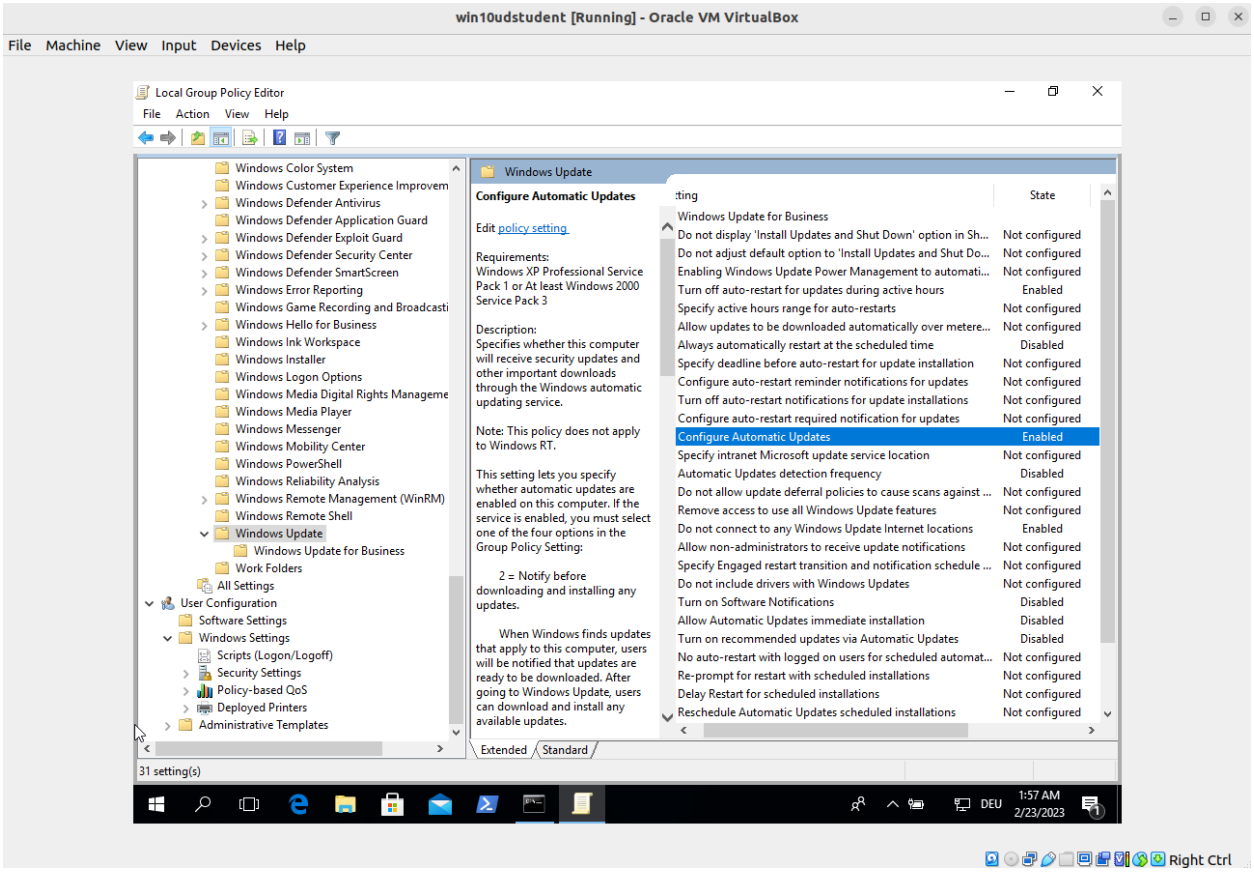
Task 2

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.'
The configuration was disabled, which is not correct.
third-party updates must be disabled or with a value of 0



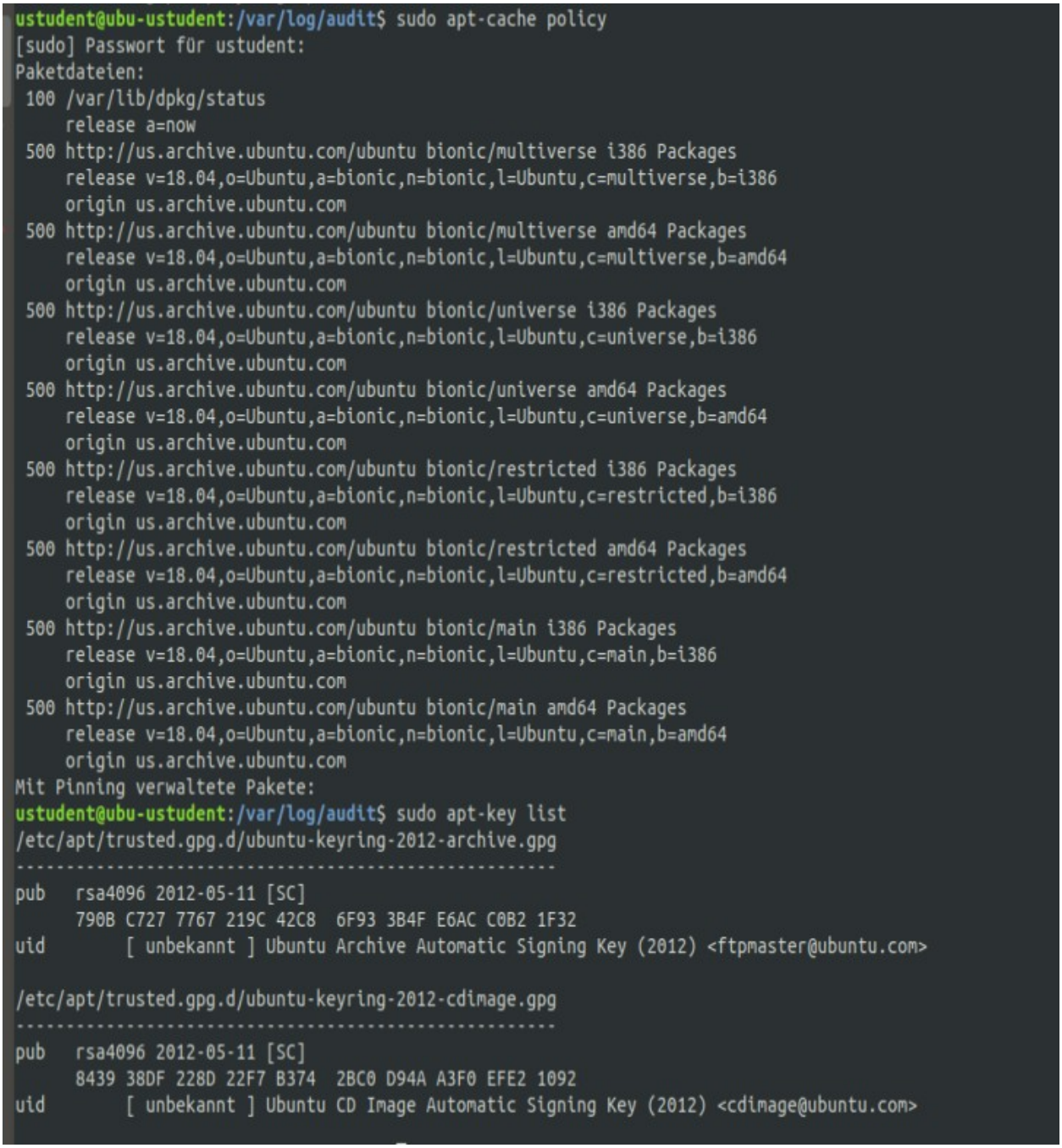
I enabled the automatic updates as can be seen in the screenshot below.



Ubuntu CIS 1.2.1

Ensure package manager repositories are configured correctly.

It can be seen that the updates in ubuntu seem to be good.



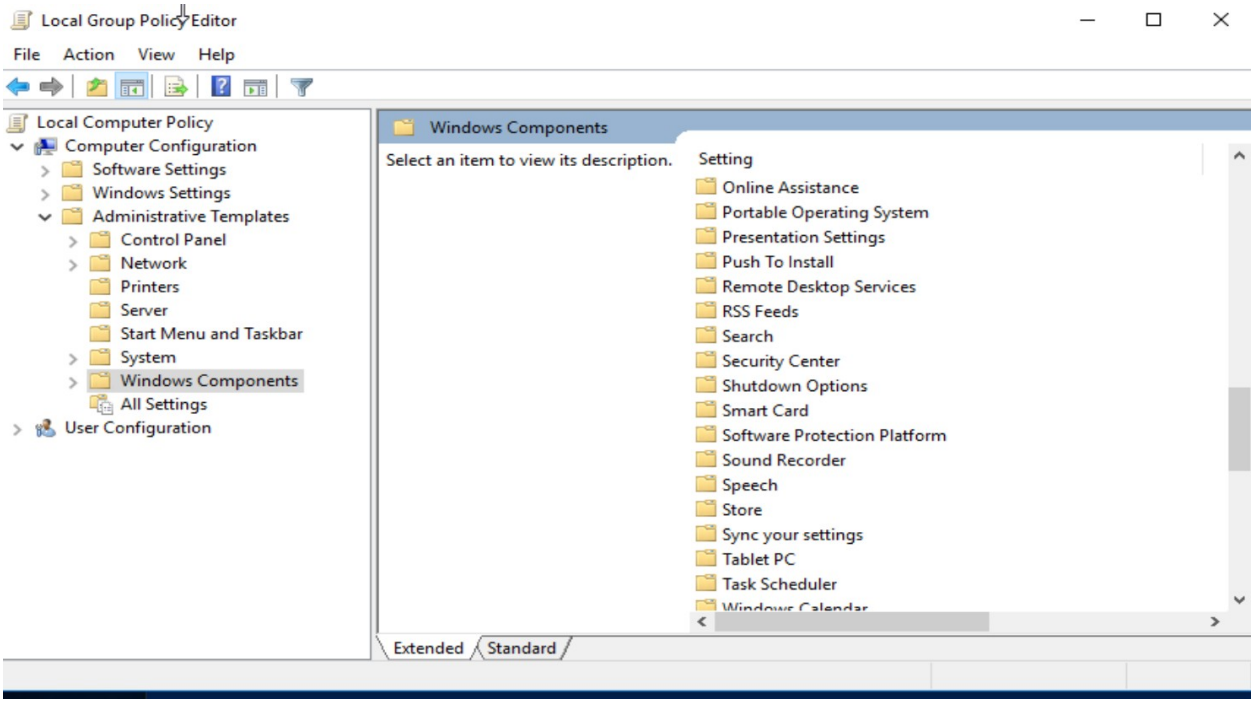
```
ustudent@ubu-ustudent:/var/log/audit$ sudo apt-cache policy
[sudo] Passwort für ustudent:
Paketdateien:
 100 /var/lib/dpkg/status
     release a=now
 500 http://us.archive.ubuntu.com/ubuntu bionic/multiverse i386 Packages
     release v=18.04,o=Ubuntu,a=bionic,n=bionic,l=Ubuntu,c=multiverse,b=i386
     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
Mit Pinning verwaltete Pakete:
ustudent@ubu-ustudent:/var/log/audit$ 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        [ unbekannt ] 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        [ unbekannt ] Ubuntu CD Image Automatic Signing Key (2012) <cdimage@ubuntu.com>
```

Task 3- Native Protections and Software Inventory

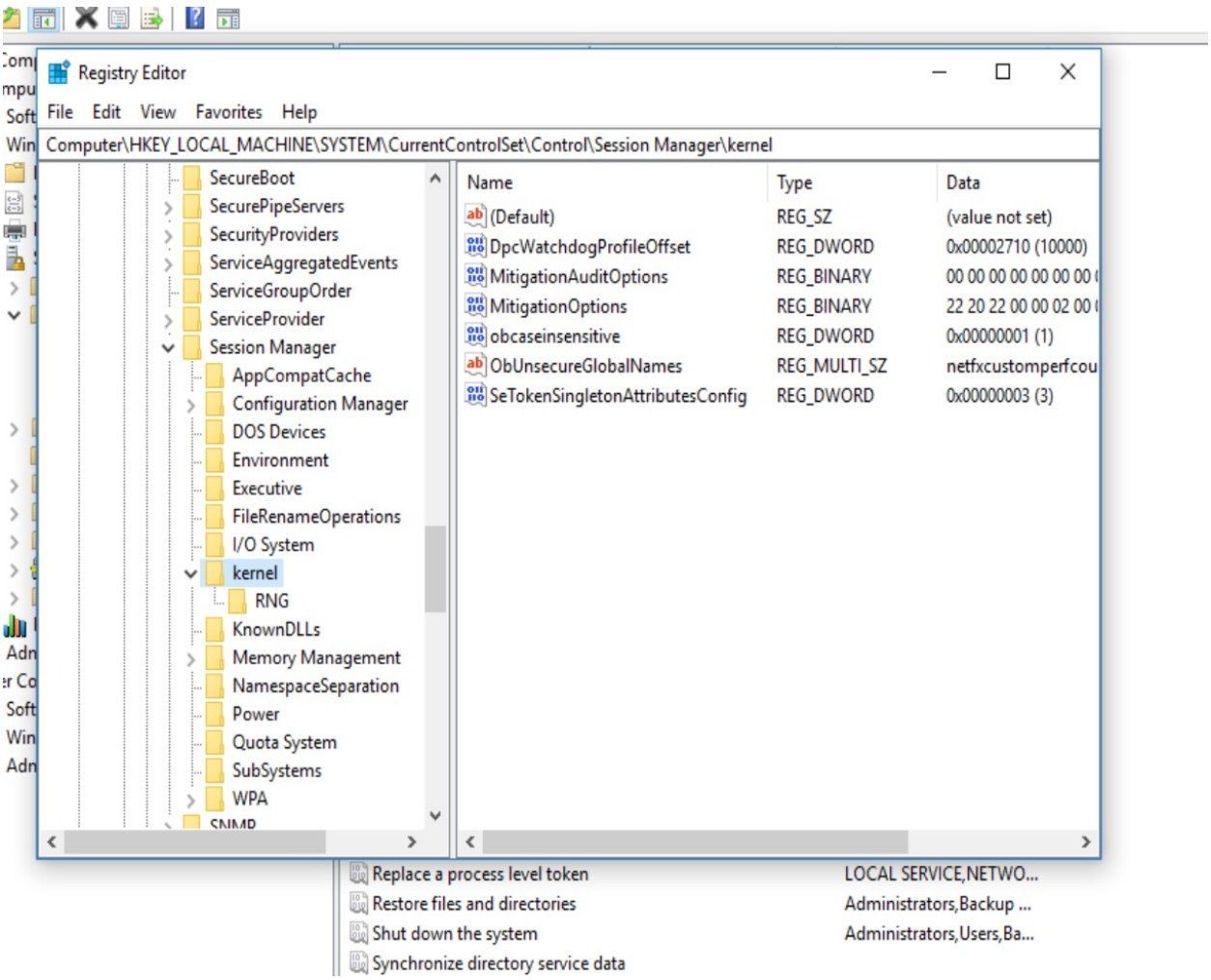
Next, verify that native protections for the operating systems are enough to protect systems from exploitation. (Hint: Think upgrades) We also need to know exactly what software is running on every machine. Also, please perform a software inventory on each computer and post your findings. The more you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

Windows CIS 18.3.4

Ensure 'Enable Structured Exception Handling Overwrite Protection (SEHOP)' is set to 'Enabled.'
Is this system compliant?
It is not CIS complement. The path from the CIS does not exist. An additional Group Policy template is required to add MS Security Guide.



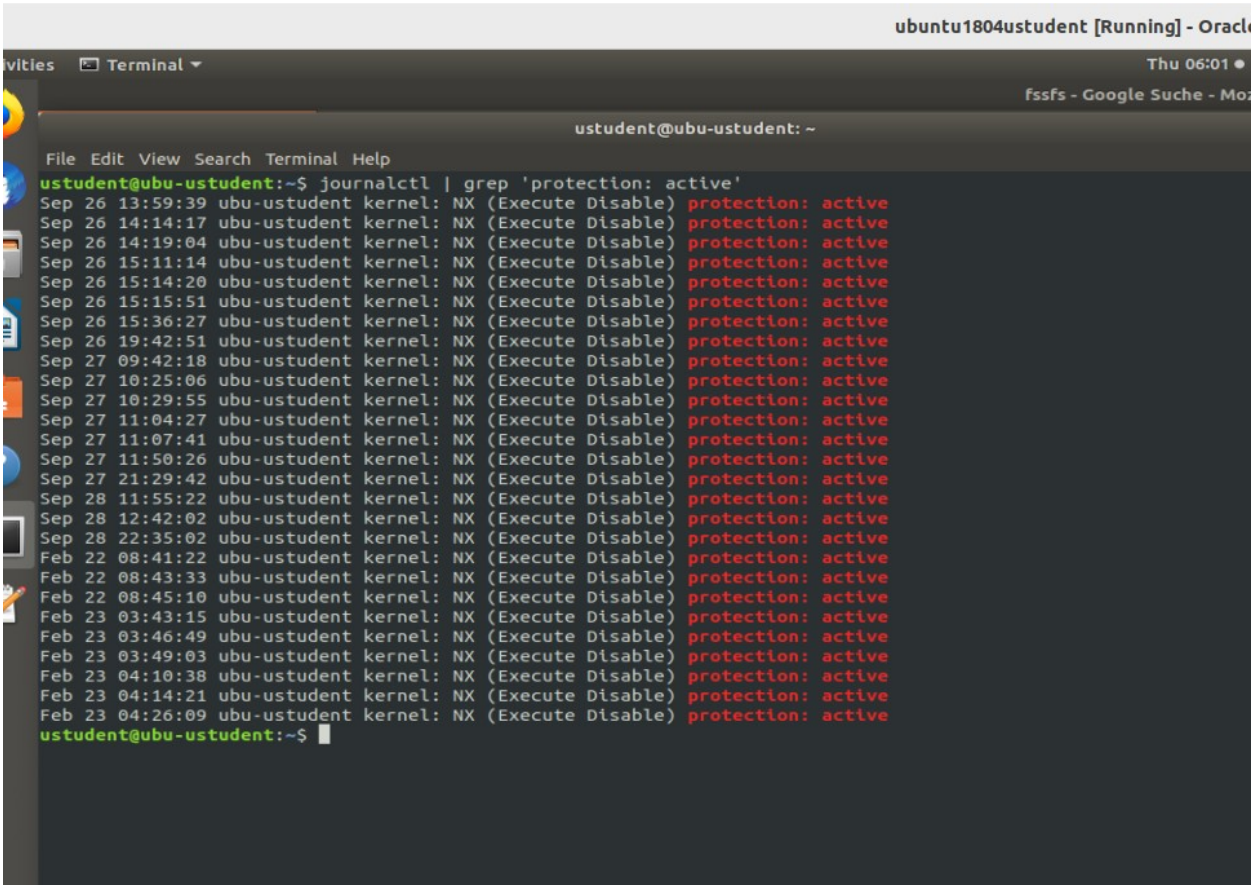
The registry entry DisableExceptionChainValidationis not available.


Registry Editor
File Edit View Favorites Help
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\kernel
SecureBoot
SecurePipeServers
SecurityProviders
ServiceAggregatedEvents
ServiceGroupOrder
ServiceProvider
Session Manager
AppCompatCache
Configuration Manager
DOS Devices
Environment
Executive
FileRenameOperations
I/O System
kernel
RNG
KnownDLLs
Memory Management
NamespaceSeparation
Power
Quota System
SubSystems
WPA
Name
Type
Data
(Default)
REG_SZ
(value not set)
DpcWatchdogProfileOffset
REG_DWORD
0x00002710 (10000)
MitigationAuditOptions
REG_BINARY
MitigationOptions
REG_BINARY
obcaseinsensitive
REG_DWORD
0x00000001 (1)
ObUnsecureGlobalNames
REG_MULTI_SZ
netfxcustomperfcou
SeTokenSingletonAttributesConfig
REG_DWORD
0x00000003 (3)
Replace a process level token
LOCAL SERVICE,NETWO...
Restore files and directories
Administrators,Backup ...
Shut down the system
Administrators,Users,Ba...
Synchronize directory service data

Ubuntu CIS 1.6.1, 1.6.2

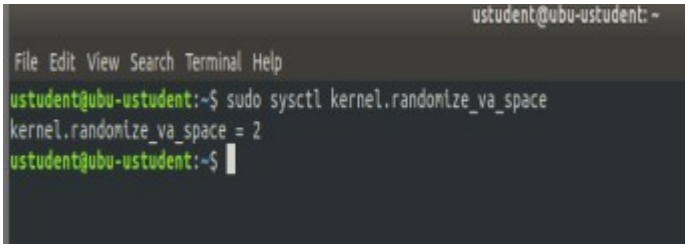
1.6.1 Ensure XD/NX support is enabled

The system is CIS conform



1.6.2 Ensure address space layout randomization (ASLR) is enabled

The system is not CIS conform. It needs to set the kernel.randomize_va_space=2 entry in the *etc*/sysctl.conf



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?

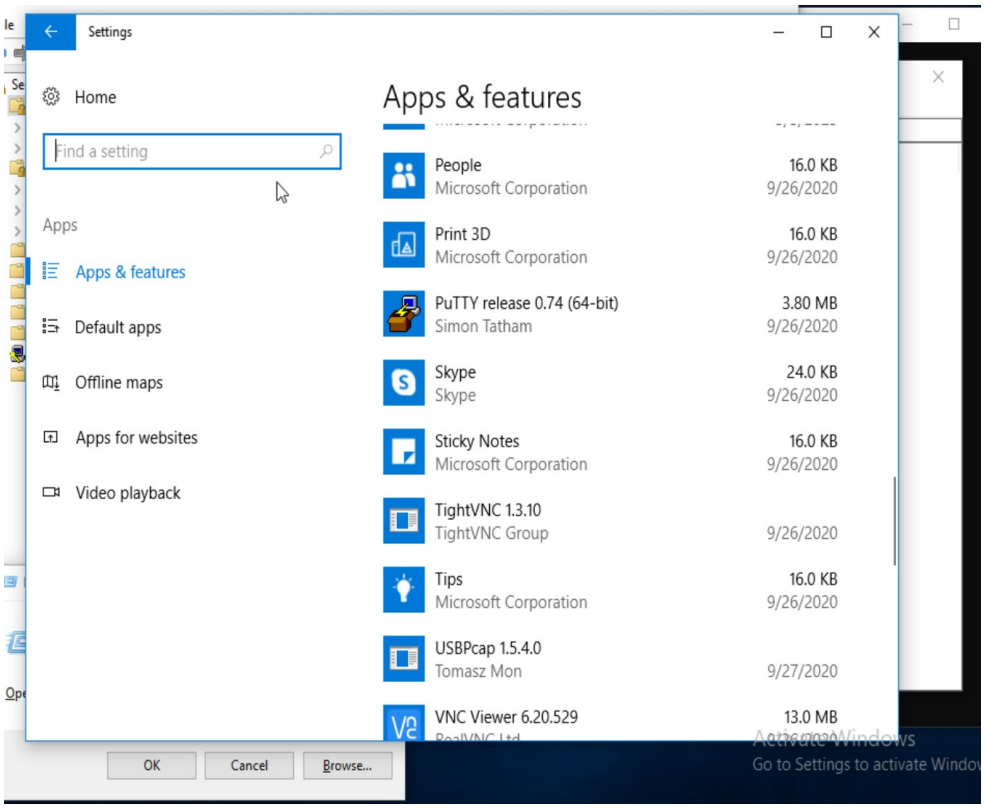
All the installed packages can be viewed in ubuntu with apt list –installed

Is TightVNC installed on this Ubuntu machine?
Yes, TightVNC is installed

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

Yes, every additional installed application increases the attack surface and thus increases the risk.
For example on ubuntu is an ftp server running which sends username/password in cleartext which can be intercepted by a man in the middle attack. This service should be deactivated. In general the number of services should be kept to a minimum.

The programs in windows can be checked by going to settings > Apps & features. It lists for example VNC Viewer, TightVNC, Putty



Task 4

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

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.

Ubuntu
Ports should be disabled:
Port 12/tcp daytime service
Port 17/tcp qotd
Port 21/tcp ftp
Port 23/telnet

Ports that are fine:
Port 22/ssh
Port 37/tcp time
Port 80/tcp http
Port 139/tcp samba
Port 445/tcp samba

```
PORT    STATE SERVICE     VERSION
13/tcp  open  daytime
17/tcp  open  qotd?
| fingerprint-strings:
|   DNSStatusRequest:
|     You see, I consider that a man's brain originally is like a little empty
|     attic, and you have to stock it with such furniture as you choose. A fool
|     takes in all the lumber of every sort he comes across, so that the knowledge
|     which might be useful to him gets crowded out, or at best is jumbled up with
|     other things, so that he has difficulty in laying his hands upon it.
|     skilful workman is very careful indeed as to what he takes into his
|     brain-attic. He will have nothing but the tools which may help him in doing
|     work, but of these he has a large assortment, and all in the most perfect
|     order. It is a mistake to think that that little room has elastic walls and
|     distend to any extent. Depend upon it there comes a time when for every
|     addition of knowledge you forget something that you knew before. It is of
|     highest importance, therefore, not to have useless facts
|   GenericLines:
|     The time is right to make new friends.
|   Help:
|     You will overcome the attacks of jealous associates.
|   Kerberos:
|     That secret you've been guarding, isn't.
|   NULL:
|     Things past redress and now with me past care.
|     William Shakespeare, "Richard II"
|   RTSPRequest:
|     You have a deep appreciation of the arts and music.
|   SSLSessionReq:
|     You will pass away very quickly.
|   TLSSessionReq:
|_    You should go home.
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: 2023-03-03T14:56:17
80/tcp  open  http        Apache httpd 2.4.29 ((Ubuntu))
```

```
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: \\10.0.2.5\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: \\10.0.2.5\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 71.34 seconds
```

Windows ip

Should be disabled
7/tcp echo
9/tcp discard
13/tcp daytime
17/tcp qotd
19/tcp chargen

Are good:
135/tcp msrpc
139/ microsoft ssn
445/tcp microsoft ds
3389/tcp ms wbt server
80/tcp http

```
Starting Nmap 7.60 ( https://nmap.org ) at 2023-03-03 10:58 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).
Stats: 0:03:03 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 100.00% done; ETC: 11:01 (0:00:00 remaining)
Nmap scan report for 10.0.2.4
Host is up (0.00029s 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)
|_sslv2-drown:
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 309.96 seconds
```

Step 2: Assess Access Management at Targeted Assets

Task 1

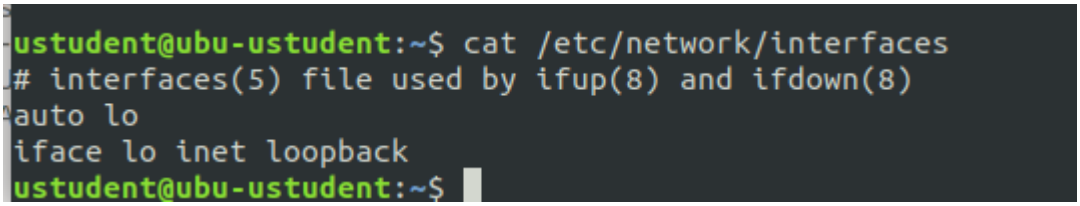
Check for current settings on Network Segmentation, VLANs, Domain Isolation, or IP Security Policies.

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:

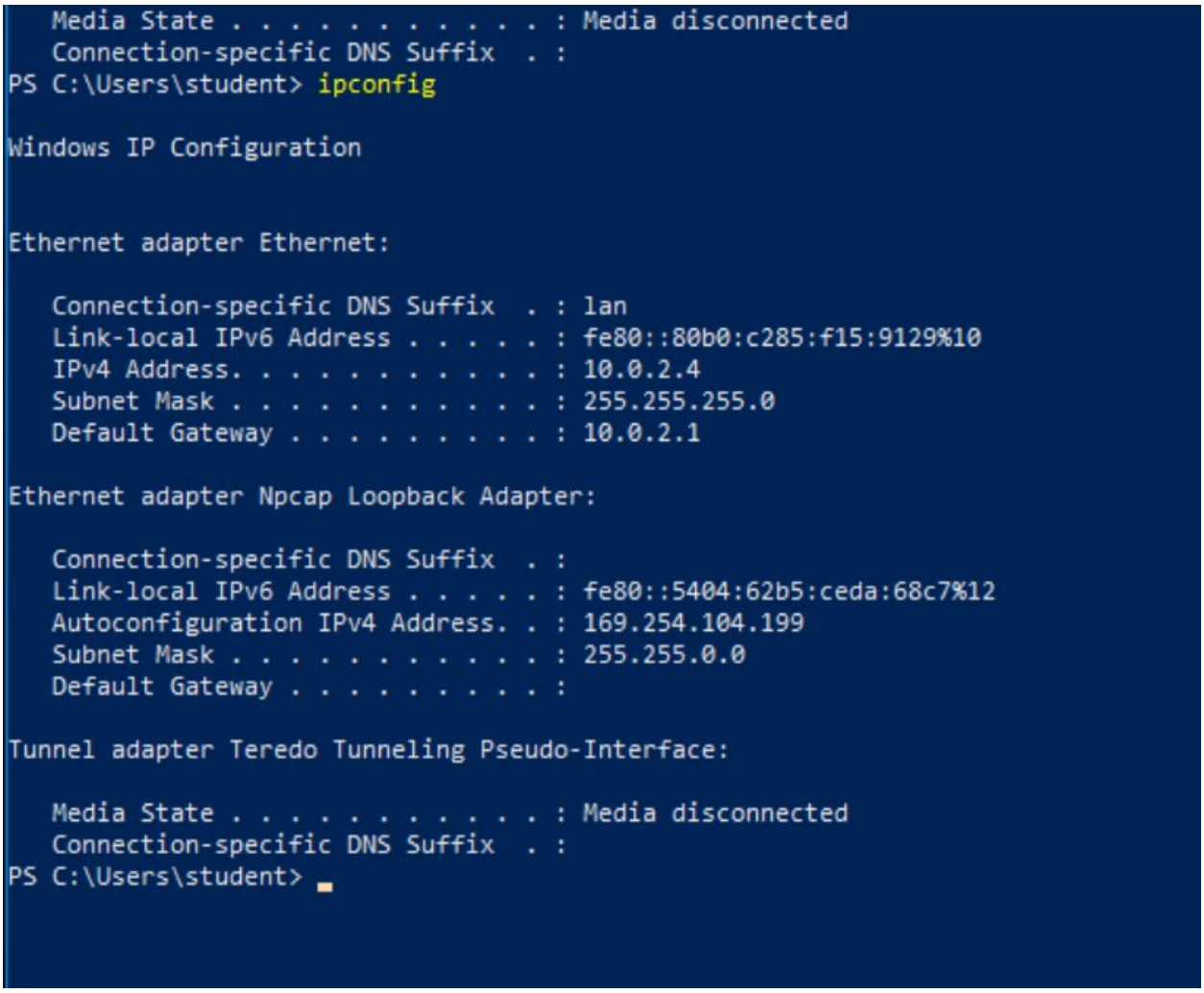
- Are there any VLANs?
- Are there any policies in place?
    - If there are any, are they applied?
- Is Anonymous access granted to any share?

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)

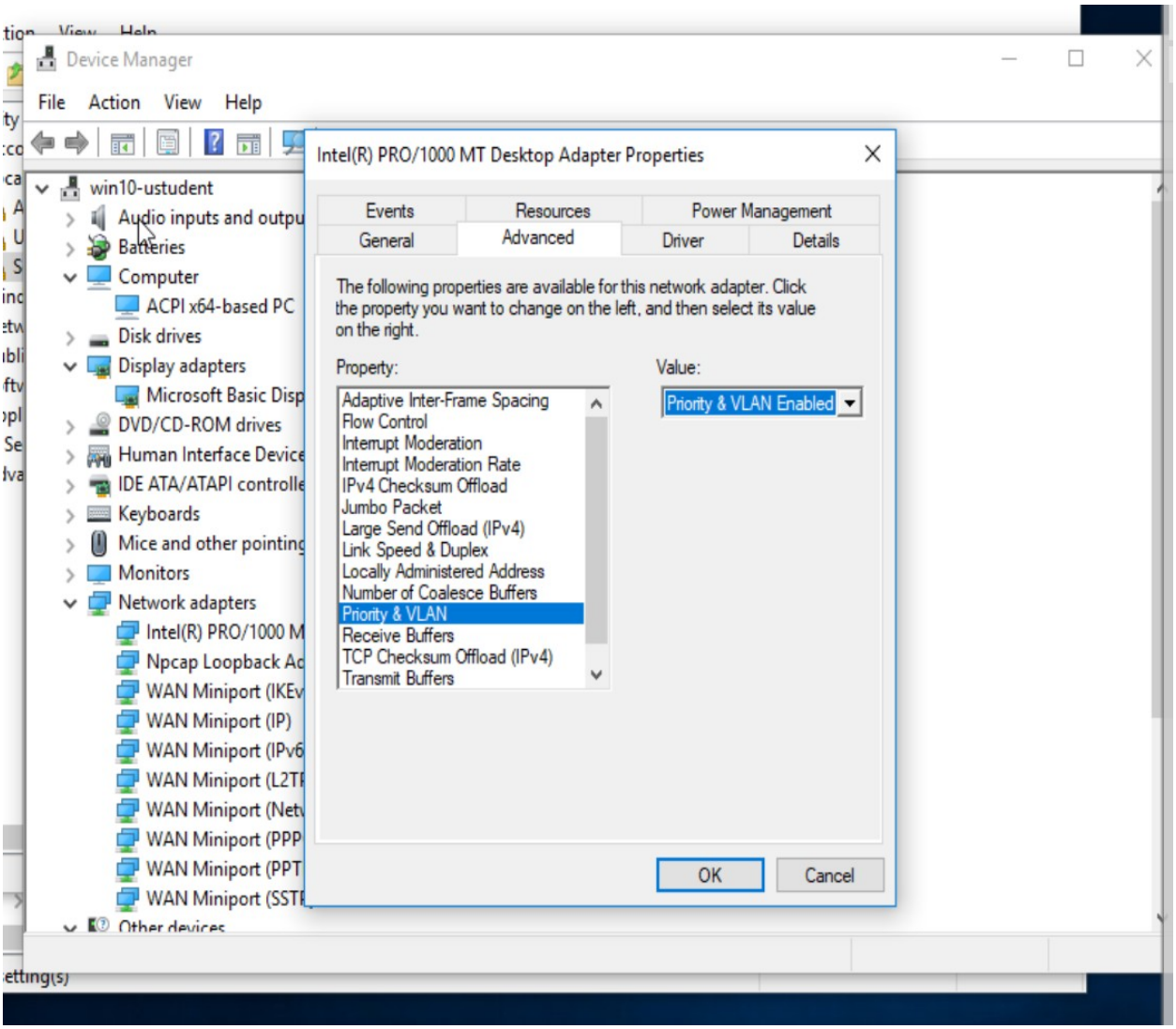
Vlans:
There are no vlans configured in ubuntu



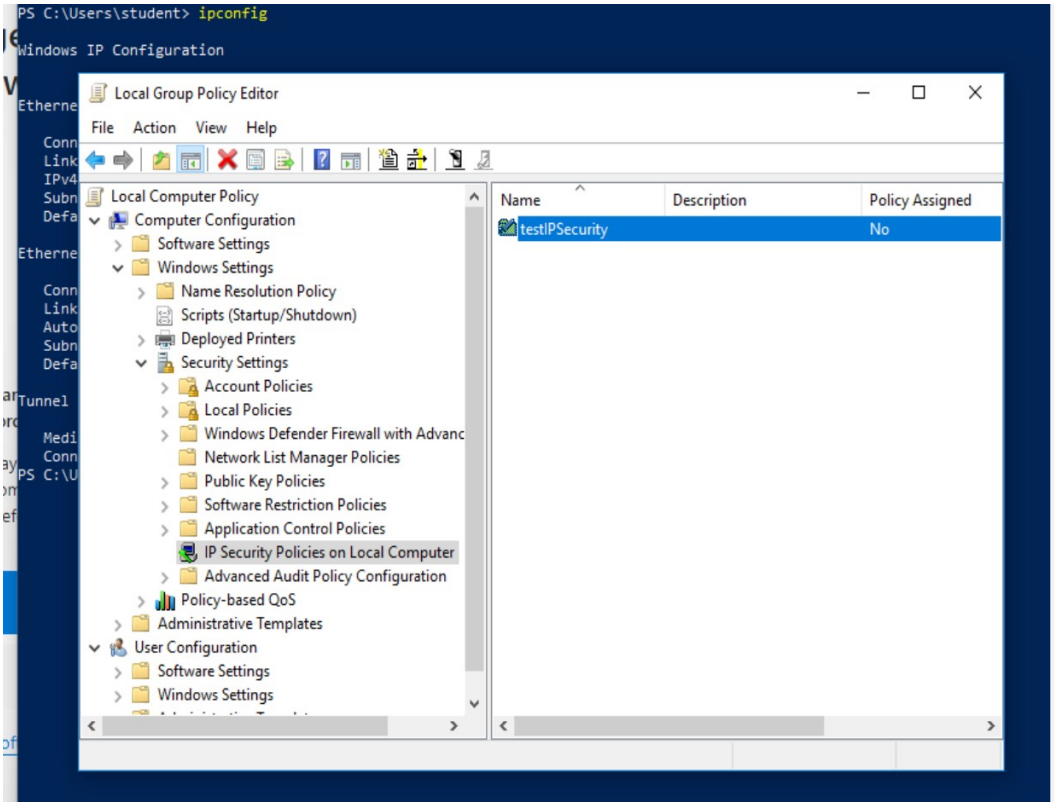
There is no vlan configured in windows



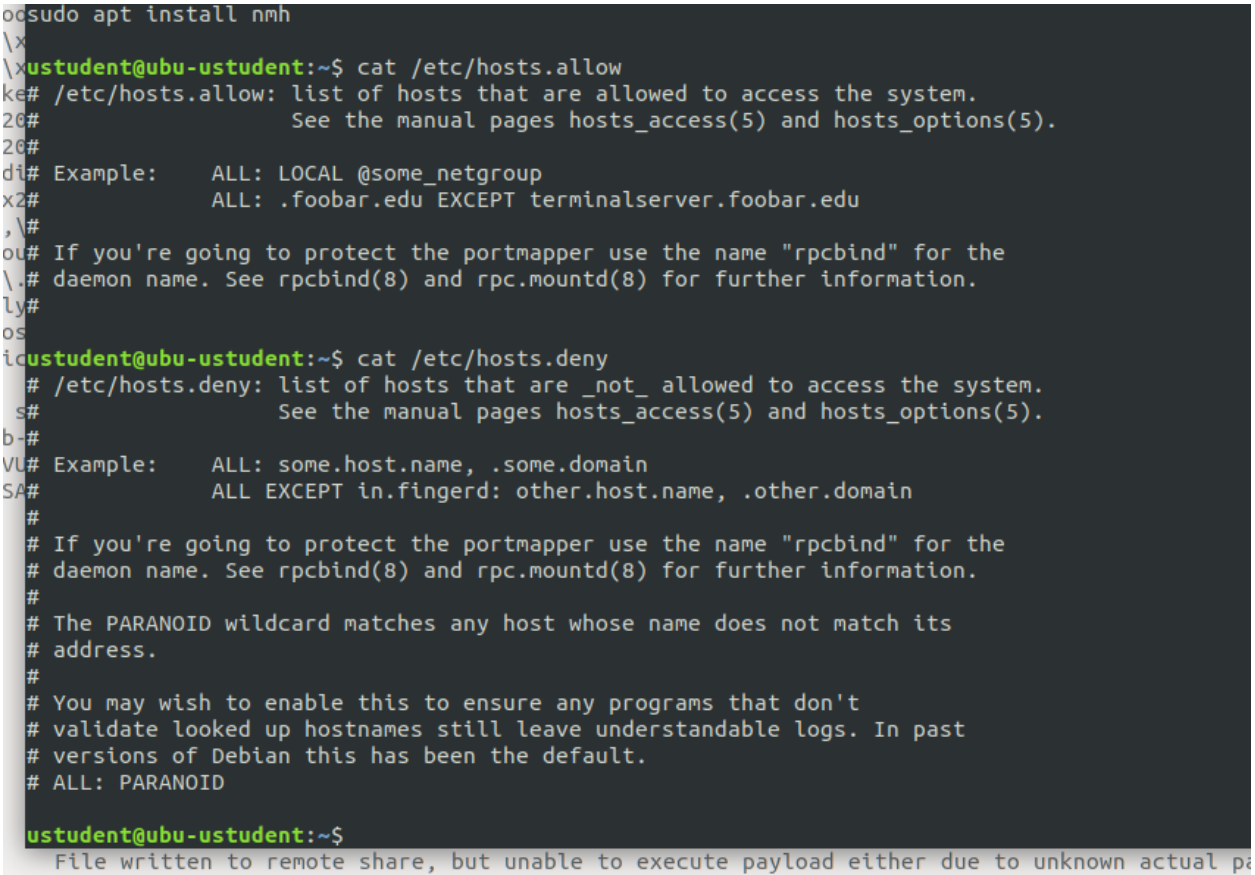
The network adapter is able to handle vlan


Device Manager
File Action View Help
win10-ustudent
Audio inputs and outpu
Batteries
Computer
ACPI x64-based PC
Disk drives
Display adapters
Microsoft Basic Disp
DVD/CD-ROM drives
Human Interface Device
IDE ATA/ATAPI controlle
Keyboards
Mice and other pointing
Monitors
Network adapters
Intel(R) PRO/1000 M
Npcap Loopback Ad
WAN Miniport (IKEv
WAN Miniport (IP)
WAN Miniport (IPv6
WAN Miniport (L2TP
WAN Miniport (Netv
WAN Miniport (PPP
WAN Miniport (PPT
WAN Miniport (SSTP
Other devices
Intel(R) PRO/1000 MT Desktop Adapter Properties
Events
Resources
Power Management
General
Advanced
Driver
Details
The following properties are available for this network adapter. Click the property you want to change on the left, and then select its value on the right.
Property:
Value:
Adaptive Inter-Frame Spacing
Flow Control
Interrupt Moderation
Interrupt Moderation Rate
IPv4 Checksum Offload
Jumbo Packet
Large Send Offload (IPv4)
Link Speed & Duplex
Locally Administered Address
Number of Coalesce Buffers
Priority & VLAN
Receive Buffers
TCP Checksum Offload (IPv4)
Transmit Buffers
Priority & VLAN Enabled
OK
Cancel

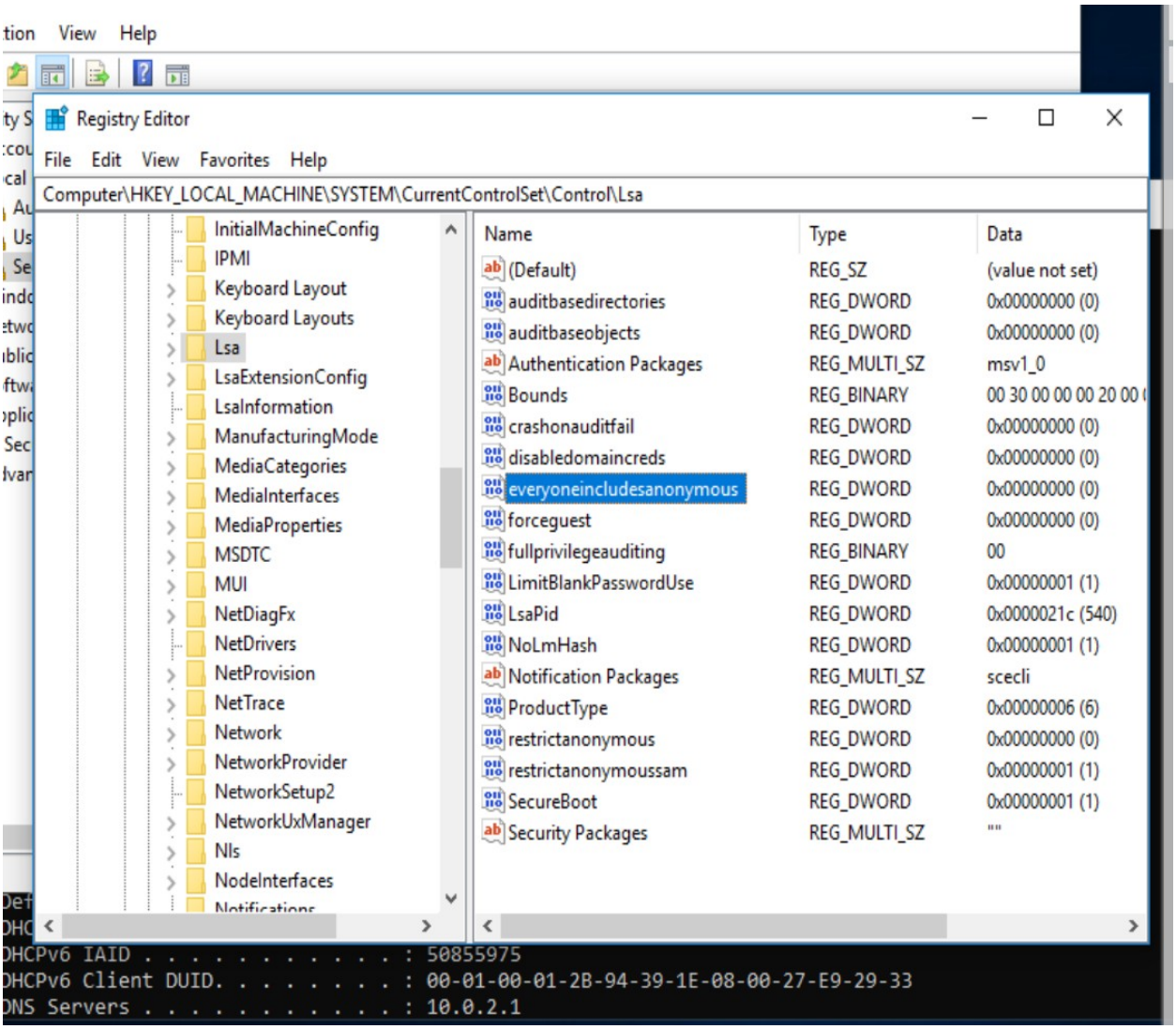
On windows there is an IPSec in place, but not applied. See screenshot below.



There are no policies configured in ubuntu



Access by anonymous users is restricted



The network should be made more secure by adding vlans to separate the networks. There could be different vlans for different departments and especially for guest access.

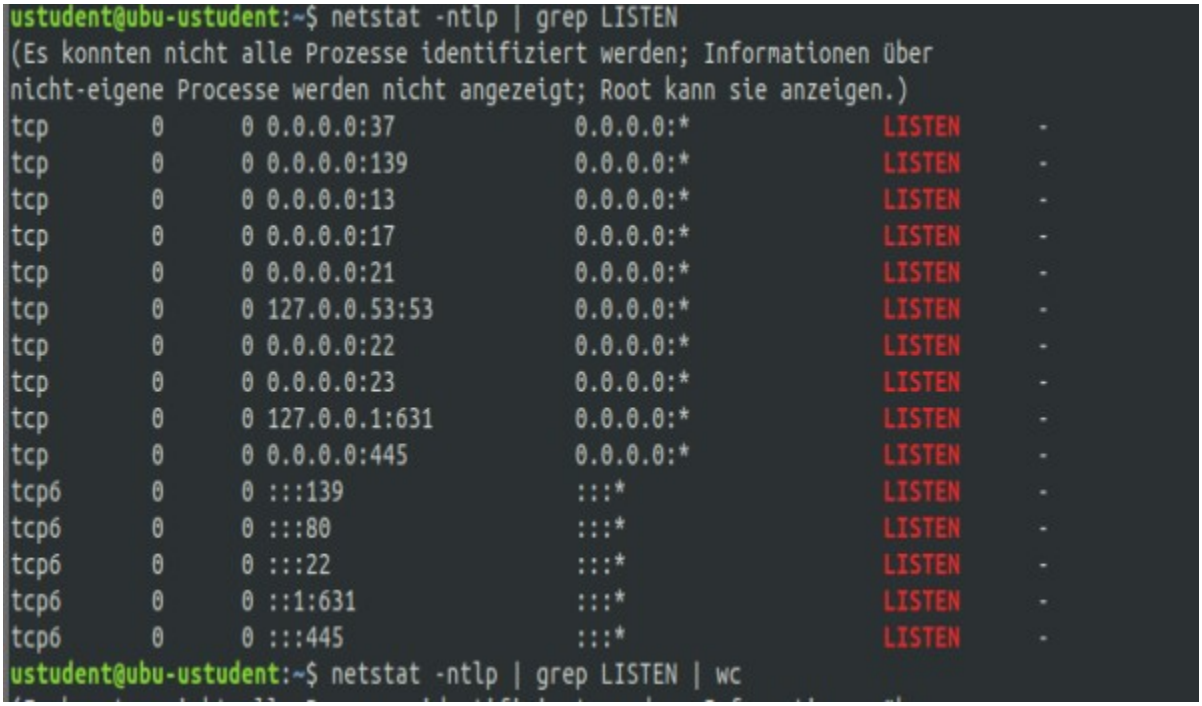
Task 2

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?

One hardening possibiltiy for ssh would be to permit root access only when an internal ip adress is used, denying access from the outside.
Services that are not used or more unsecure, like ftp should be disabled. In general it would be good to disable ipv6 as it is not necessarily used and then only ipv4 needs to be secured. This saves a lot of effort and reduces the attack surface.

The ftp service should be completely shut down as it is a unsecured protocol.



Windows ipv4

Should be disabled
7/tcp echo
9/tcp discard
13/tcp daytime
17/tcp qotd

19/tcp chargen

```
PS C:\Users\student> netstat /a | Select-String -Pattern 'LISTEN'

  TCP    0.0.0.0:7              win10-ustudent:0       LISTENING
  TCP    0.0.0.0:9              win10-ustudent:0       LISTENING
  TCP    0.0.0.0:13             win10-ustudent:0       LISTENING
  TCP    0.0.0.0:17             win10-ustudent:0       LISTENING
  TCP    0.0.0.0:19             win10-ustudent:0       LISTENING
  TCP    0.0.0.0:80             win10-ustudent:0       LISTENING
  TCP    0.0.0.0:135            win10-ustudent:0       LISTENING
  TCP    0.0.0.0:445            win10-ustudent:0       LISTENING
  TCP    0.0.0.0:3389           win10-ustudent:0       LISTENING
  TCP    0.0.0.0:5985           win10-ustudent:0       LISTENING
  TCP    0.0.0.0:47001          win10-ustudent:0       LISTENING
  TCP    0.0.0.0:49664          win10-ustudent:0       LISTENING
  TCP    0.0.0.0:49665          win10-ustudent:0       LISTENING
  TCP    0.0.0.0:49666          win10-ustudent:0       LISTENING
  TCP    0.0.0.0:49669          win10-ustudent:0       LISTENING
  TCP    0.0.0.0:49670          win10-ustudent:0       LISTENING
  TCP    0.0.0.0:49671          win10-ustudent:0       LISTENING
  TCP    0.0.0.0:49672          win10-ustudent:0       LISTENING
  TCP    10.0.2.4:139           win10-ustudent:0       LISTENING
  TCP    10.0.2.4:5040          win10-ustudent:0       LISTENING
  TCP    169.254.104.199:139    win10-ustudent:0       LISTENING
  TCP    169.254.104.199:5040   win10-ustudent:0       LISTENING
  TCP    [::]:7                 win10-ustudent:0       LISTENING
  TCP    [::]:9                 win10-ustudent:0       LISTENING
  TCP    [::]:13                win10-ustudent:0       LISTENING
  TCP    [::]:17                win10-ustudent:0       LISTENING
  TCP    [::]:19                win10-ustudent:0       LISTENING
  TCP    [::]:80                win10-ustudent:0       LISTENING
  TCP    [::]:135               win10-ustudent:0       LISTENING
  TCP    [::]:445               win10-ustudent:0       LISTENING
  TCP    [::]:3389              win10-ustudent:0       LISTENING
  TCP    [::]:5985              win10-ustudent:0       LISTENING
  TCP    [::]:47001             win10-ustudent:0       LISTENING
  TCP    [::]:49664             win10-ustudent:0       LISTENING
  TCP    [::]:49665             win10-ustudent:0       LISTENING
  TCP    [::]:49666             win10-ustudent:0       LISTENING
  TCP    [::]:49669             win10-ustudent:0       LISTENING
  TCP    [::]:49670             win10-ustudent:0       LISTENING
  TCP    [::]:49671             win10-ustudent:0       LISTENING
  TCP    [::]:49672             win10-ustudent:0       LISTENING
```

Task 3

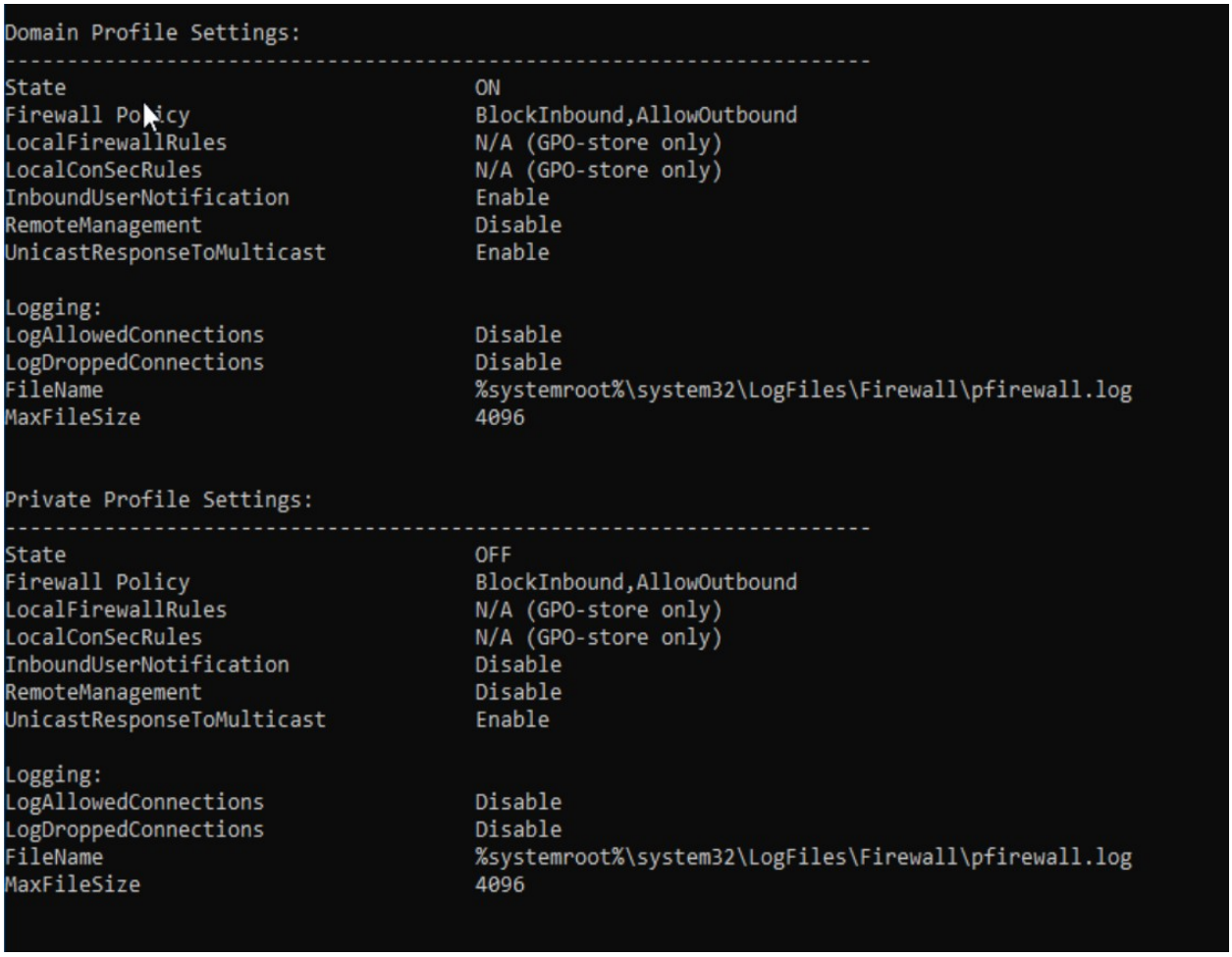
NuttyUtility only needs remote access ports for administrators on workstations. What is your assessment of the firewalls in StaticSpeed's systems? Please include evidence to support your thoughts. We need to know if the firewalls are configured correctly?
Also, what ports would you suggest to have open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

In ubuntu the firewall is inactive

```
ustudent@ubu-ustudent:~$ sudo ufw status
Status: Inaktiv
ustudent@ubu-ustudent:~$
```

I would suggest that port 22/tcp is open for the ssh service that admins can remotely log into the workstation. Additionally, I would permit access only with an internal ip adress.

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

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

Ok.


C:\Users\student>
```


Domain Profile Settings:
State ON
Firewall Policy BlockInbound,AllowOutbound
LocalFirewallRules N/A (GPO-store only)
LocalConSecRules N/A (GPO-store only)
InboundUserNotification Enable
RemoteManagement Disable
UnicastResponseToMulticast Enable
Logging:
LogAllowedConnections Disable
LogDroppedConnections Disable
FileName %systemroot%\system32\LogFiles\Firewall\pfirewall.log
MaxFileSize 4096
Private Profile Settings:
State OFF
Firewall Policy BlockInbound,AllowOutbound
LocalFirewallRules N/A (GPO-store only)
LocalConSecRules N/A (GPO-store only)
InboundUserNotification Disable
RemoteManagement Disable
UnicastResponseToMulticast Enable
Logging:
LogAllowedConnections Disable
LogDroppedConnections Disable
FileName %systemroot%\system32\LogFiles\Firewall\pfirewall.log
MaxFileSize 4096

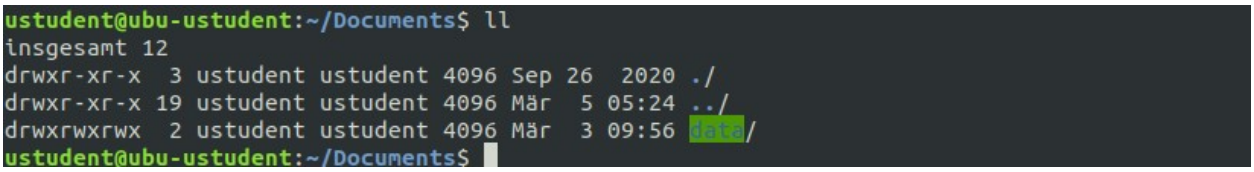
Task 4

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

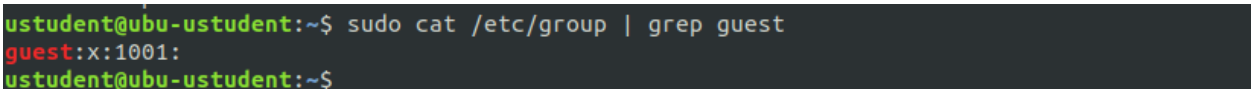
- Which users have high privileges?
- Do important PII folders have the correct permissions and ownership?
- Are the default settings correct, and are there any excessive permissions?
- On our initial scan, we found "data" shared folders that need further investigation.
- Are there "guest" accounts enabled? 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 ubutu the folder permissions are not set correctly as everyone has read, write and execute permission to the data folder for example.



On ubuntu there are guest accounts



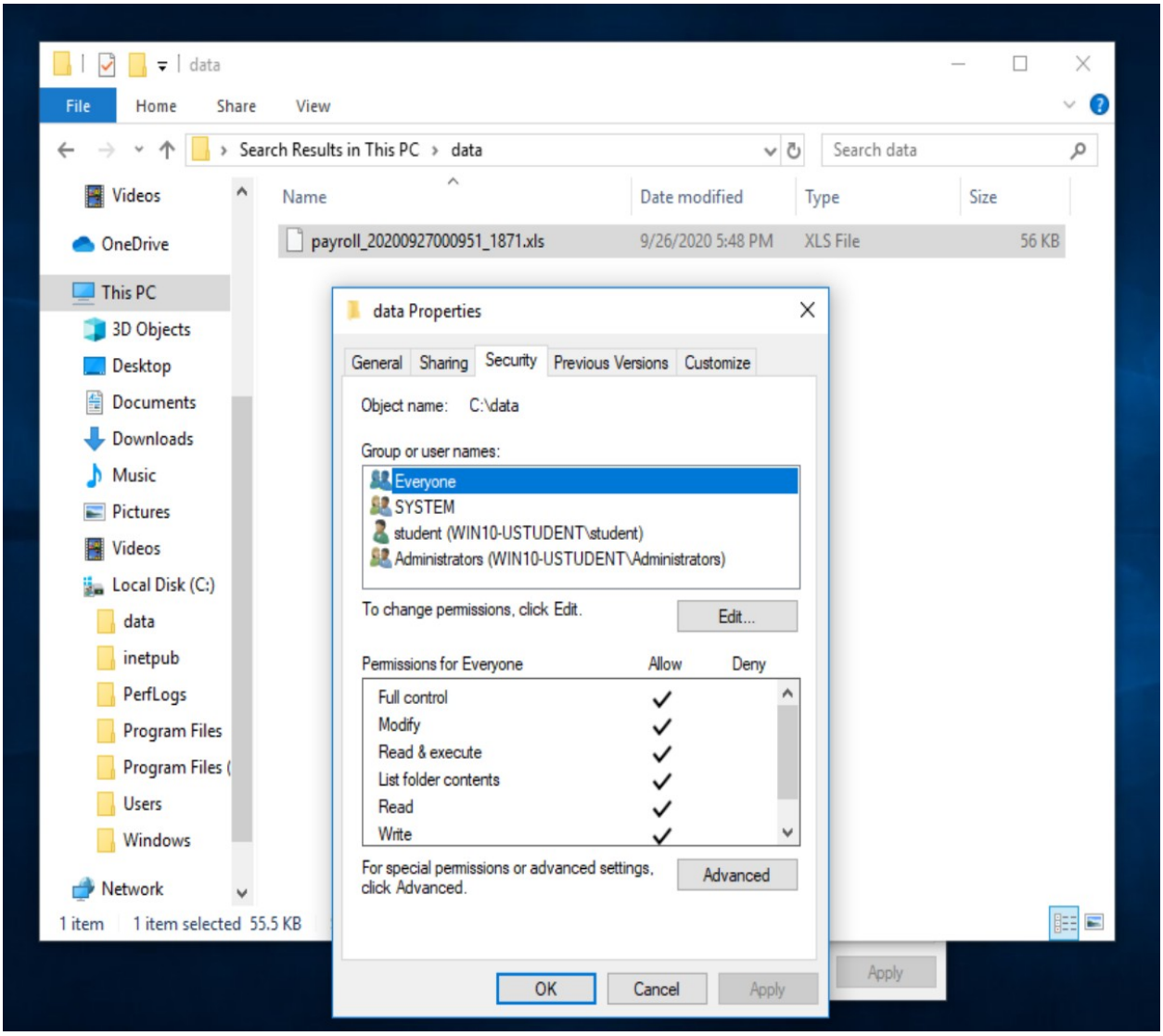
On ubuntu everyone is allowed to use sudo.

```
ustudent@ubu-ustudent:~$ sudo cat /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# 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:/s

# 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

# 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@ubu-ustudent:~$
```

On windows

There are guest accounts

The permissions are not set correctly as everyone has full control over the data folder.



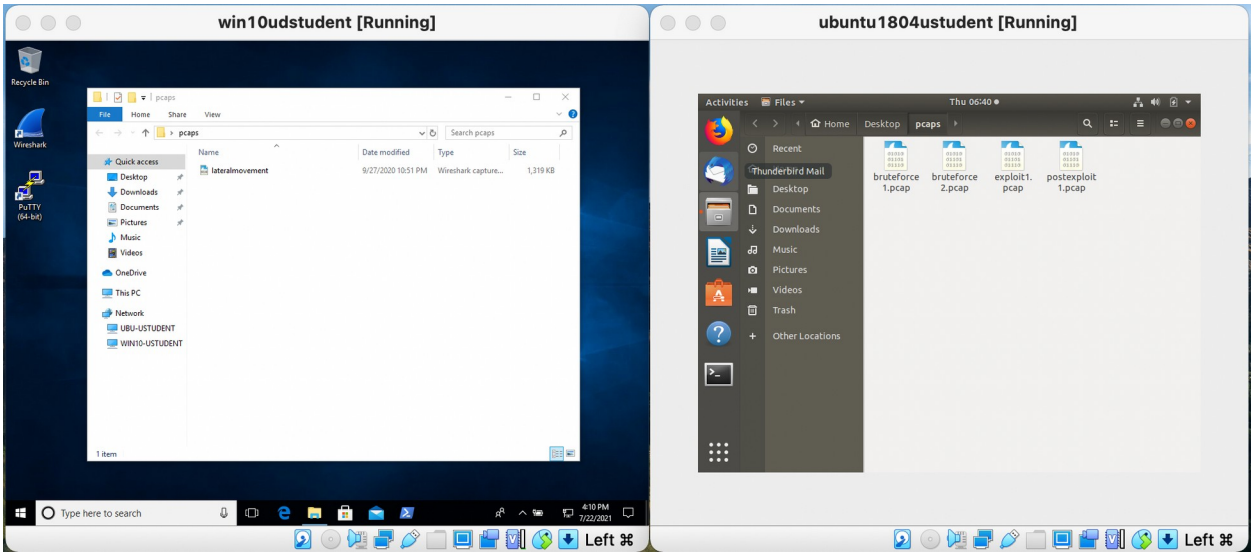
Step 3: Log Monitoring Setup for Detection at Targeted Assets

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.

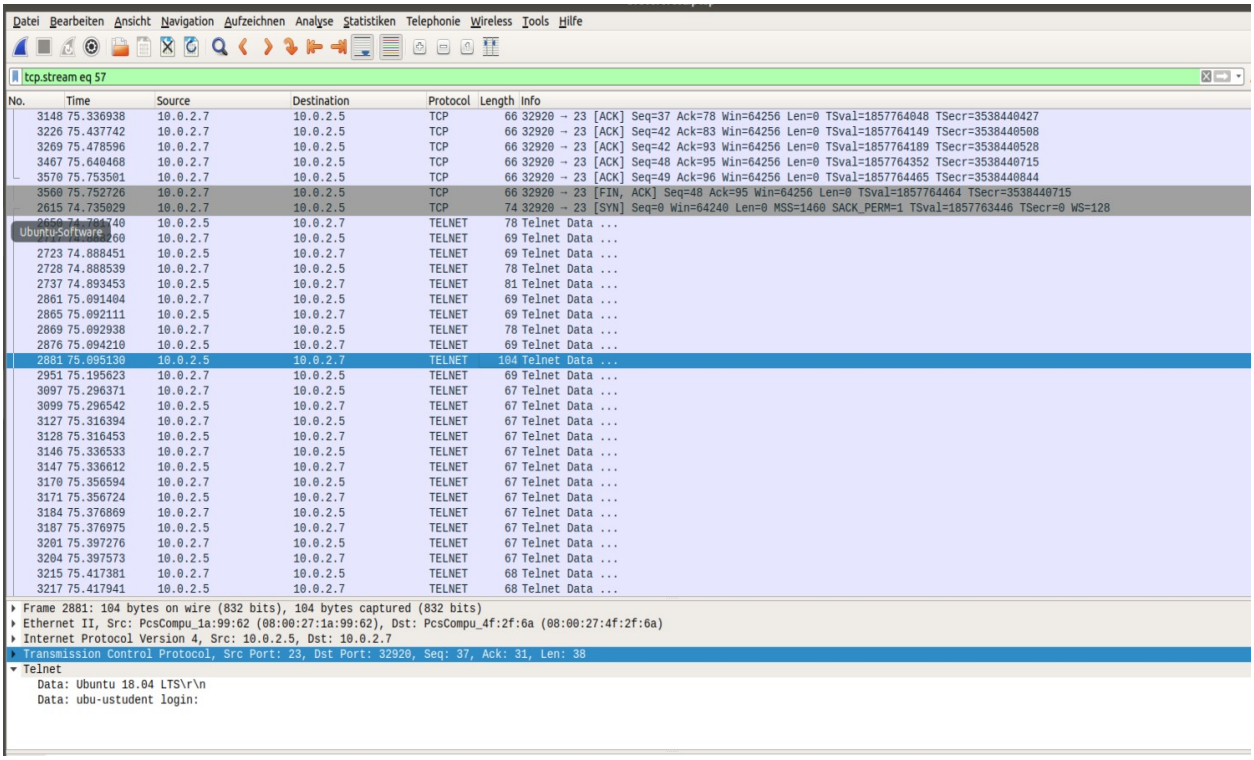


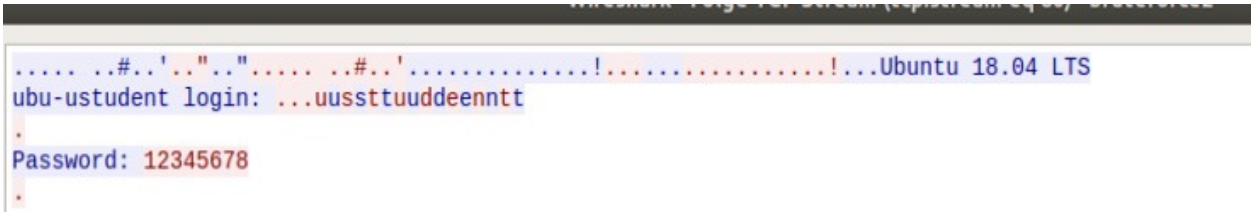
Use the pcap file to assess and determine the following:

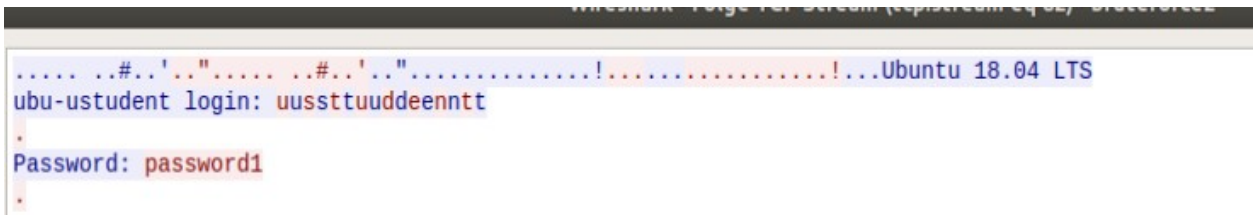
- What type of attack was recorded?
- What is the source IP of the attack?
- What protocol was targeted?
- What password was used successfully?
- Which user was compromised?

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

There was a bruteforce attack from the host 10.0.2.7. This can be seen that request with different username/password combinations are recorded.
The telnet protocol was targeted.
The successful credentials are: ustudent/1234 as seen in the last screenshot.







Bruteforce attacks can be prevented by using timeouts that slow down the attack. Futhermore, the quality of the password should be extended. It should be longer and have small and big letters as well as special characters.

Task 2

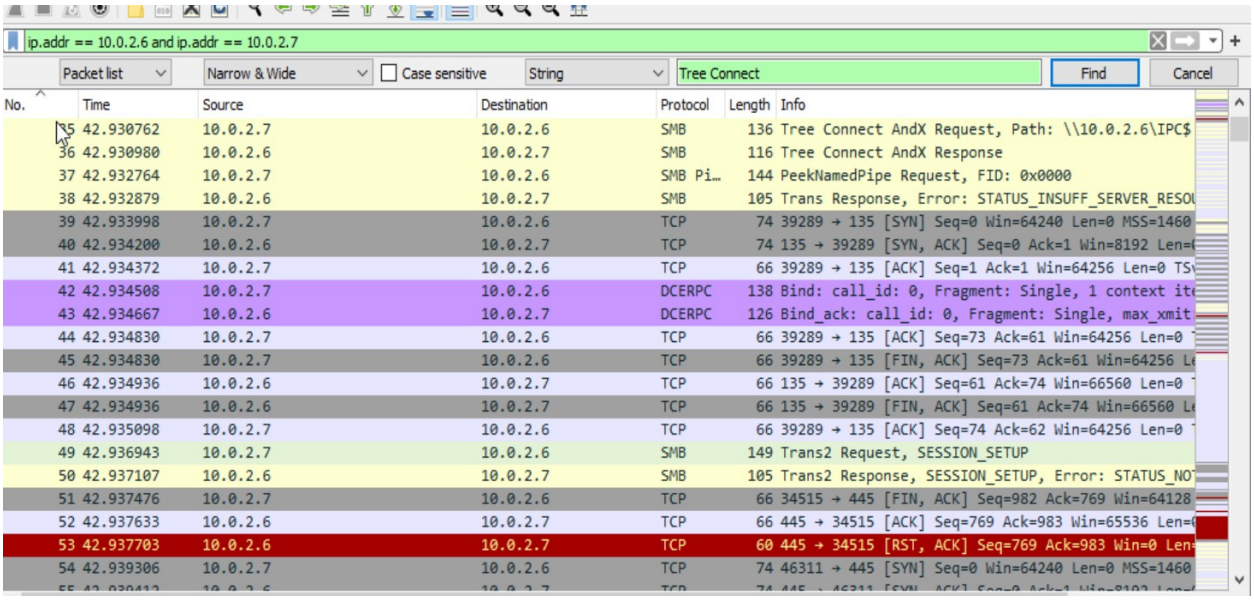
We suspect that an internal user may have compromised another machine inside StaticSpeed's network and pivoted to one of the devices you are auditing. Please use lateralmovement.pcap and determine the following:

- 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

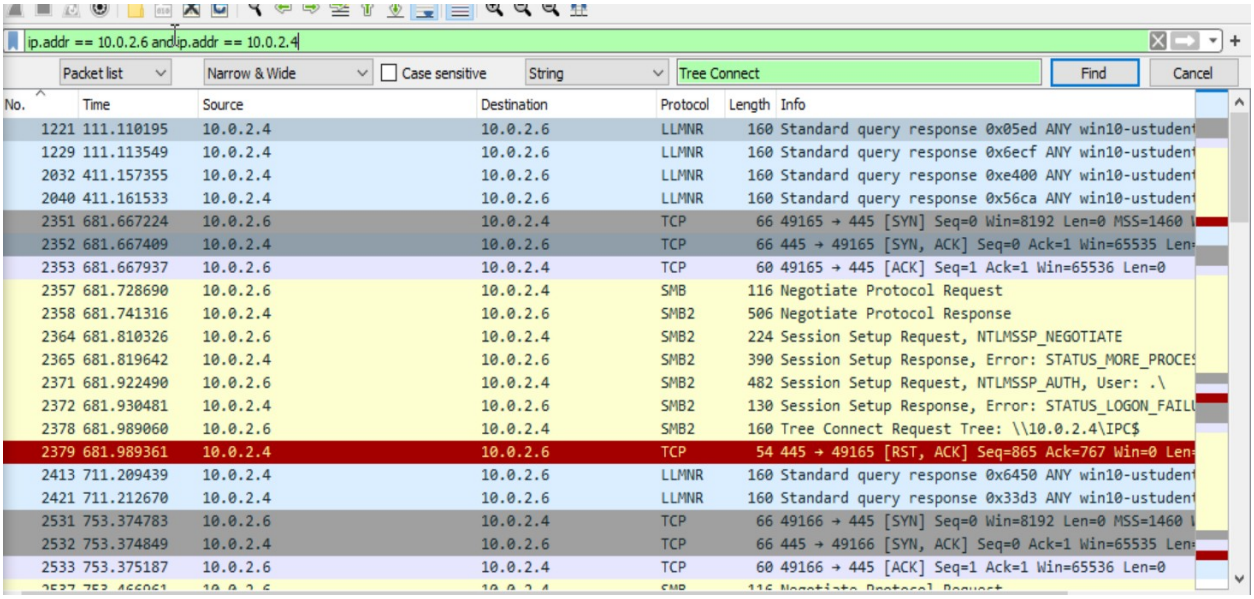
Please provide a narrative of what happened based on your findings. Justify your report based on the answers.

The source ip of the initial attack is 10.0.2.7.

It seems the attacker also attacked the machine 10.0.2.6.

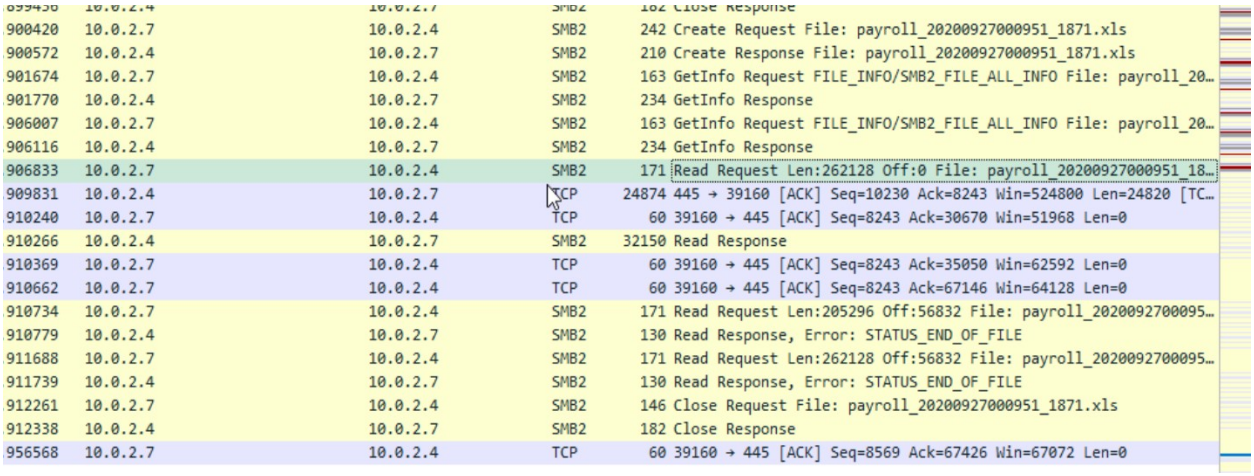


The attacker tried to access my machine 10.0.2.4 from a compromised machine with ip 10.0.2.6.



The smb2 protocol on port 445 of 10.0.2.4 is the target.

The attacker 10.0.2.7 was able to read sensitive information. He got access to the payroll_xxxxx.xls file.



900420	10.0.2.7	10.0.2.4	SMB2	242	Create Request File: payroll_20200927000951_1871.xls
900572	10.0.2.4	10.0.2.7	SMB2	210	Create Response File: payroll_20200927000951_1871.xls
901674	10.0.2.7	10.0.2.4	SMB2	163	GetInfo Request FILE_INFO/SMB2_FILE_ALL_INFO File: payroll_20…
901770	10.0.2.4	10.0.2.7	SMB2	234	GetInfo Response
906007	10.0.2.7	10.0.2.4	SMB2	163	GetInfo Request FILE_INFO/SMB2_FILE_ALL_INFO File: payroll_20…
906116	10.0.2.4	10.0.2.7	SMB2	234	GetInfo Response
906833	10.0.2.7	10.0.2.4	SMB2	171	Read Request Len:262128 Off:0 File: payroll_20200927000951_18…
909831	10.0.2.4	10.0.2.7	TCP	24874	445 → 39160 [ACK] Seq=10230 Ack=8243 Win=524800 Len=24820 [TC…
910240	10.0.2.7	10.0.2.4	TCP	60	39160 → 445 [ACK] Seq=8243 Ack=30670 Win=51968 Len=0
910266	10.0.2.4	10.0.2.7	SMB2	32150	Read Response
910369	10.0.2.7	10.0.2.4	TCP	60	39160 → 445 [ACK] Seq=8243 Ack=35050 Win=62592 Len=0
910662	10.0.2.7	10.0.2.4	TCP	60	39160 → 445 [ACK] Seq=8243 Ack=67146 Win=64128 Len=0
910734	10.0.2.7	10.0.2.4	SMB2	171	Read Request Len:205296 Off:56832 File: payroll_2020092700095…
910779	10.0.2.4	10.0.2.7	SMB2	130	Read Response, Error: STATUS_END_OF_FILE
911688	10.0.2.7	10.0.2.4	SMB2	171	Read Request Len:262128 Off:56832 File: payroll_2020092700095…
911739	10.0.2.4	10.0.2.7	SMB2	130	Read Response, Error: STATUS_END_OF_FILE
912261	10.0.2.7	10.0.2.4	SMB2	146	Close Request File: payroll_20200927000951_1871.xls
912338	10.0.2.4	10.0.2.7	SMB2	182	Close Response
956568	10.0.2.7	10.0.2.4	TCP	60	39160 → 445 [ACK] Seq=8569 Ack=67426 Win=67072 Len=0

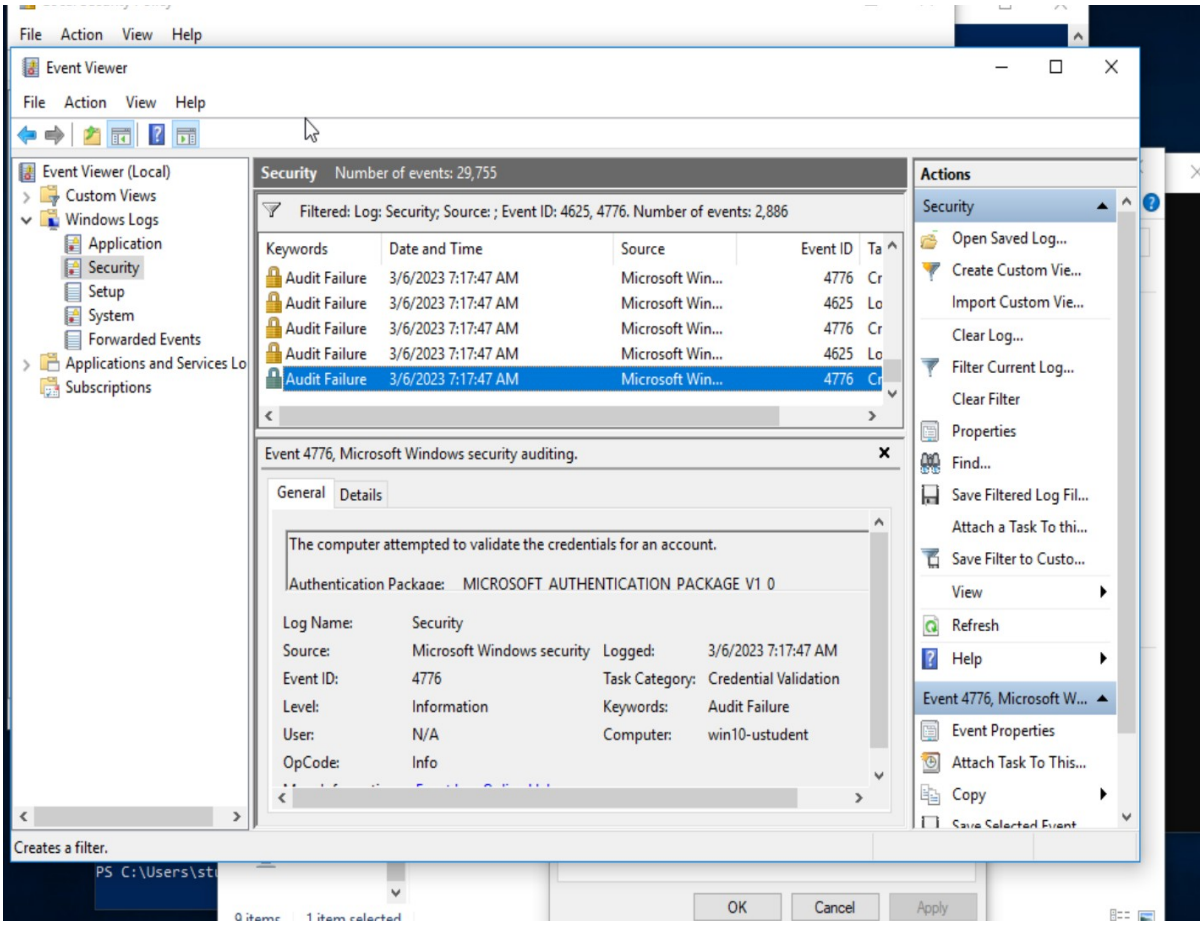
Task 3

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

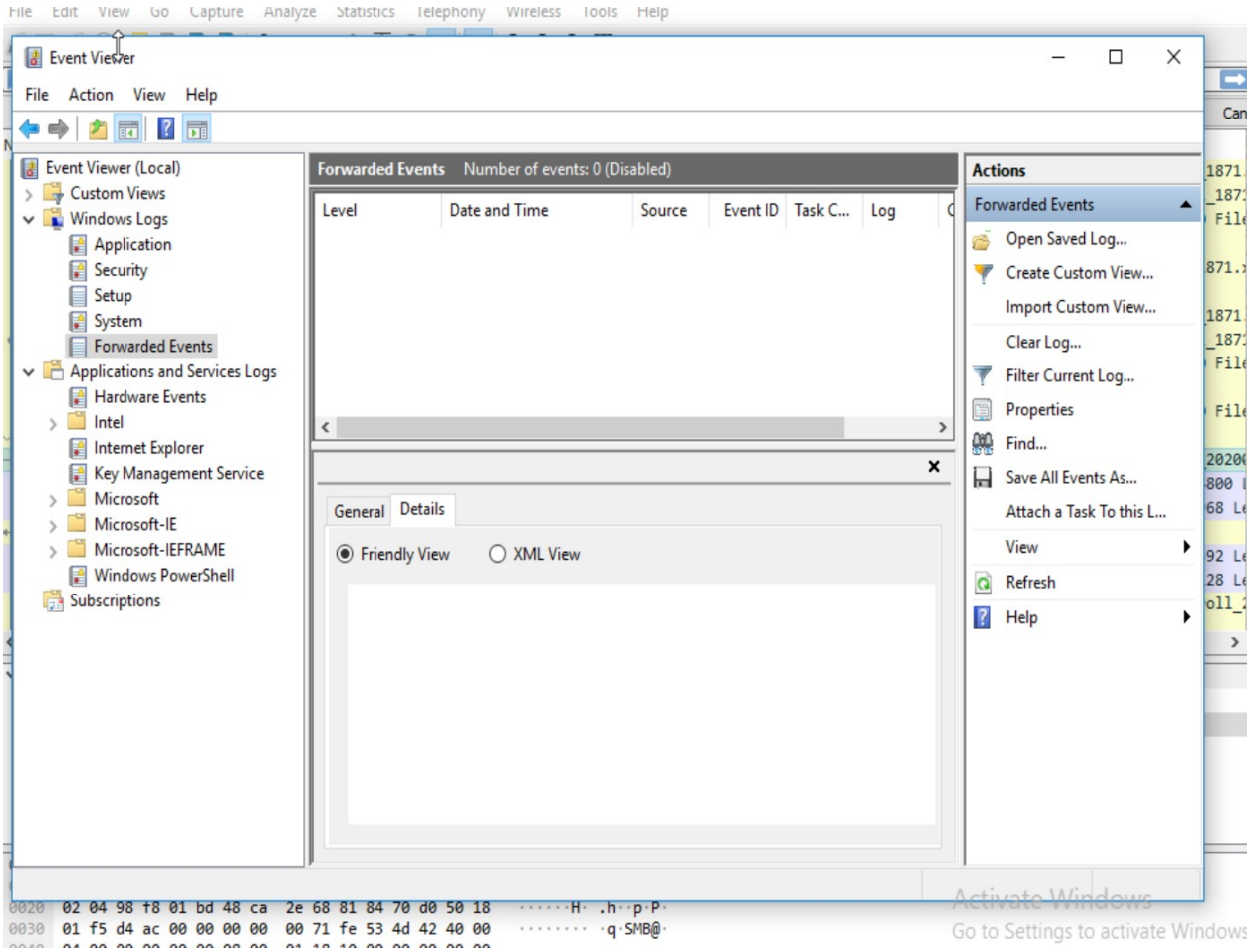
- Are there any issues with Windows Share? Please provide screenshots of your findings.
- Look at the audit logs setup at your Linux machine and find the audit.log file. What was the name of the attacker’s account? Please provide screenshots.

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.

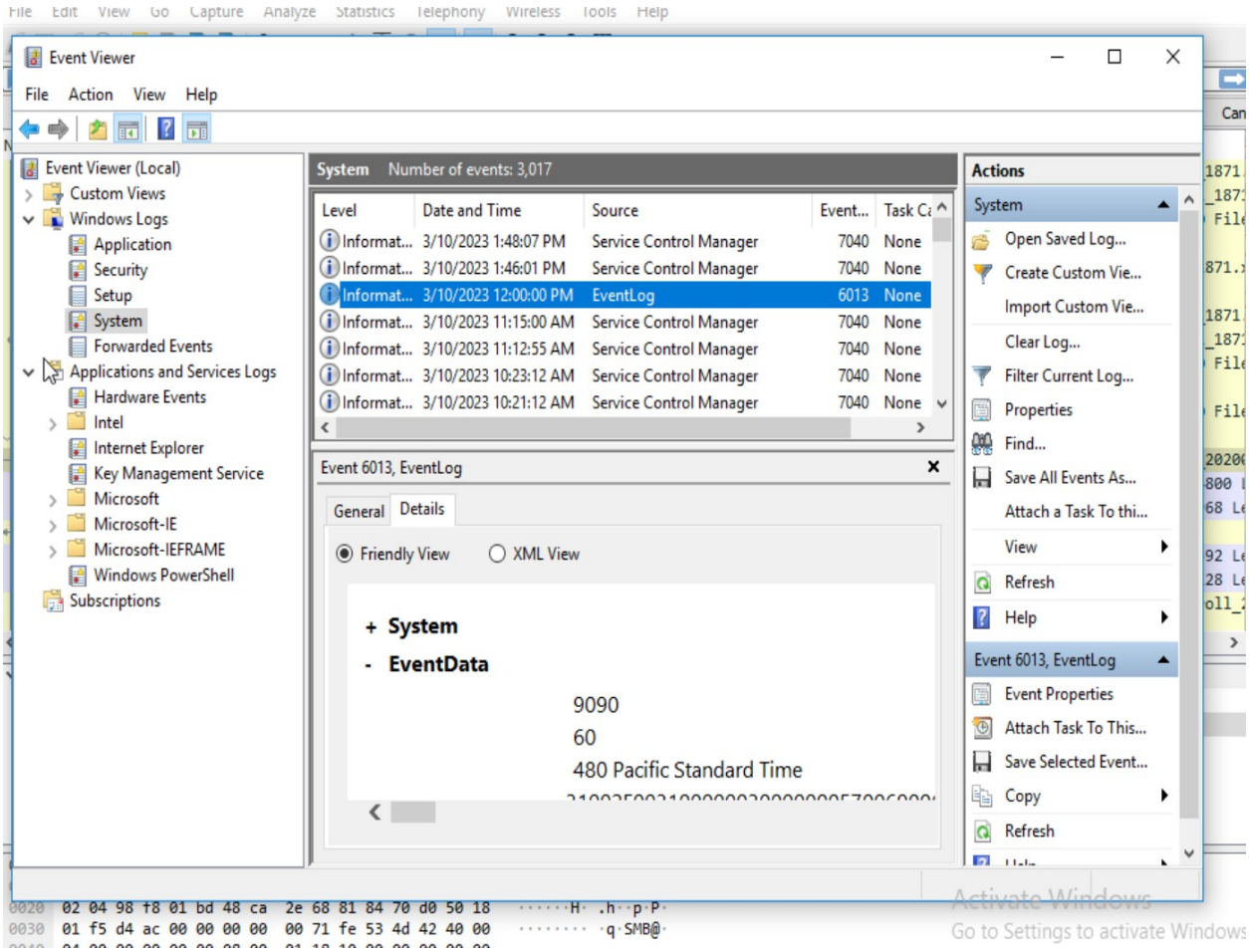
I don’t see anything suspicious in the windows event viewer in security tab.



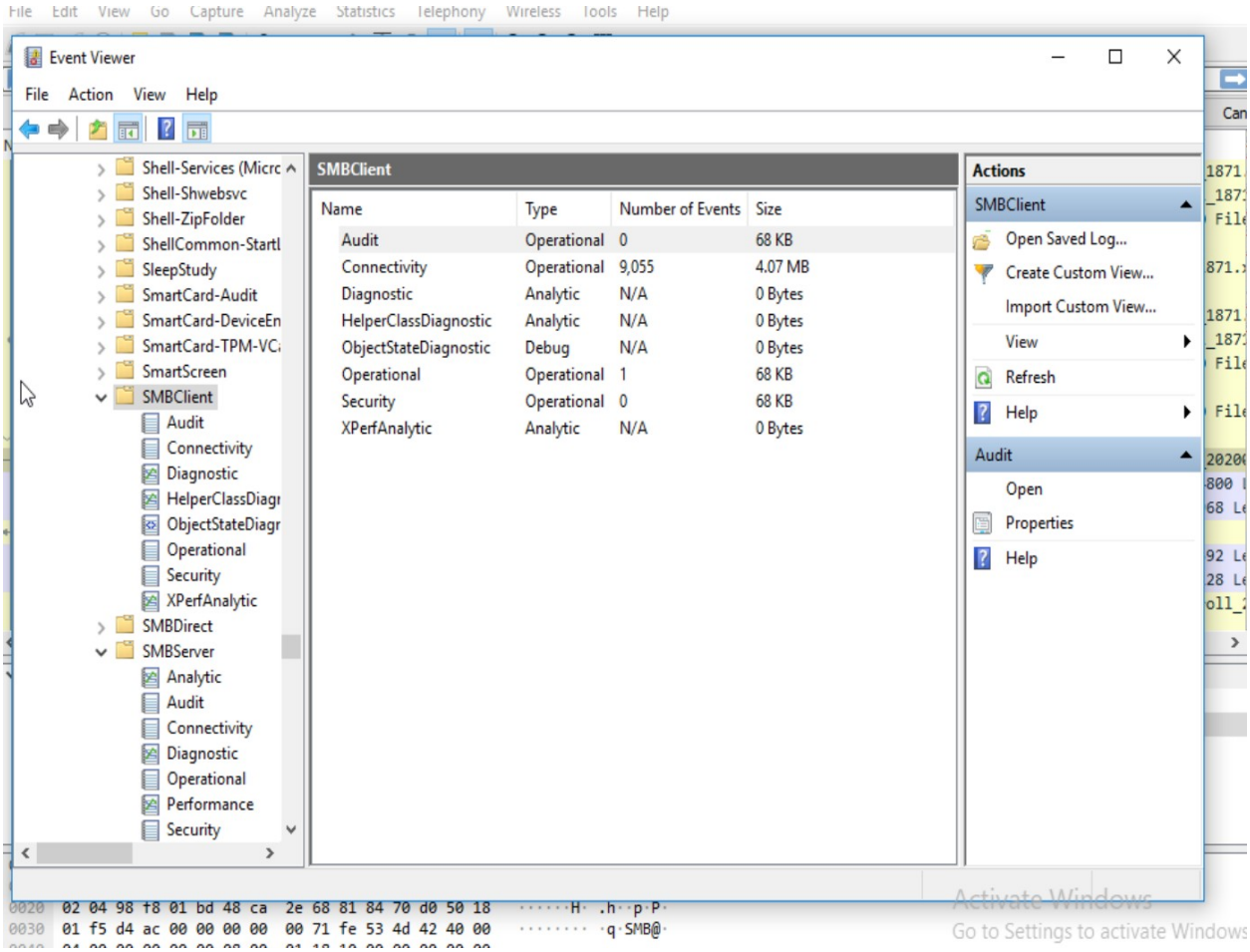
Nothing interesting in forwarding events



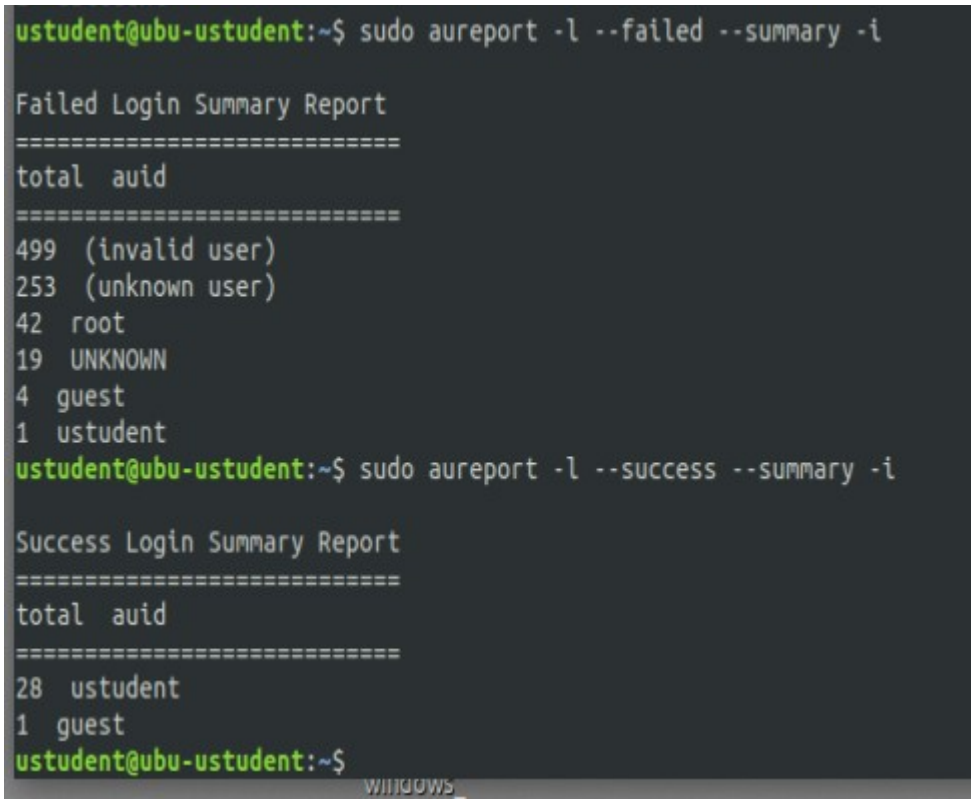
Nothing intersting in system

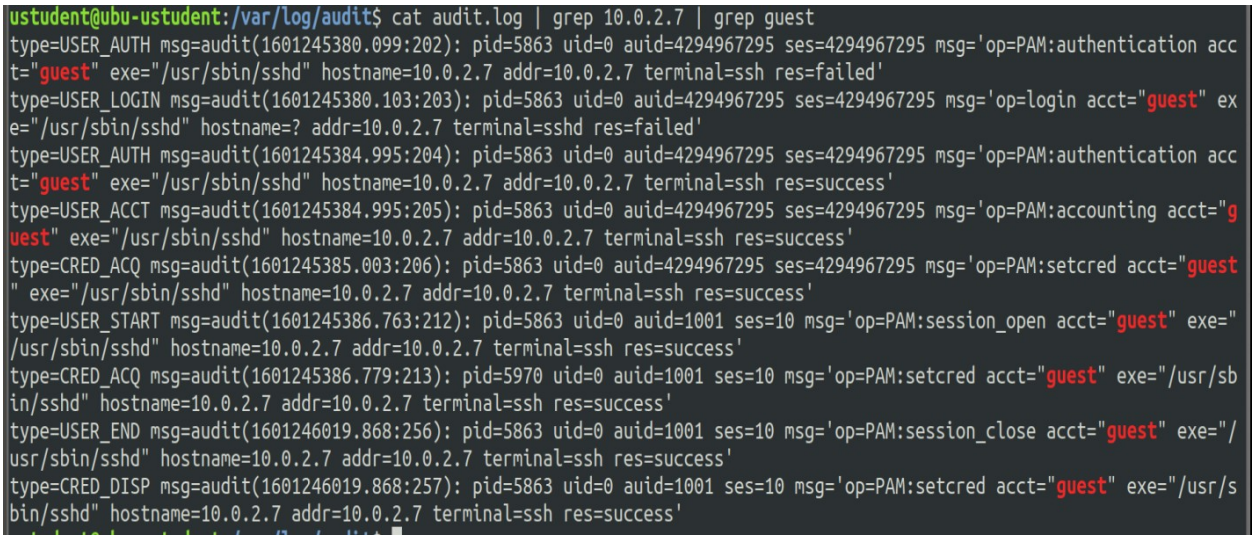


I also don’t see anything strange in SMB Client and SMB Server

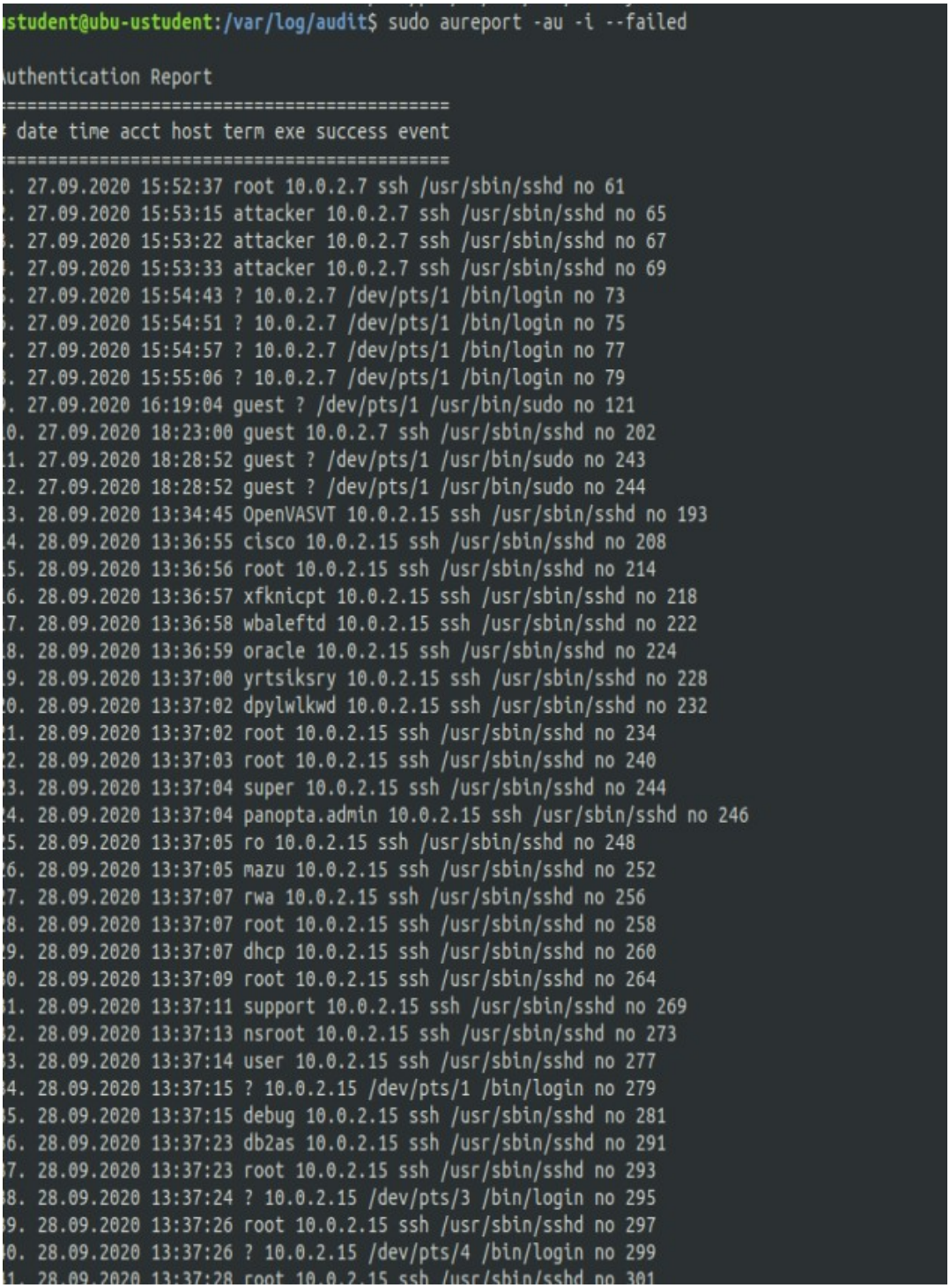


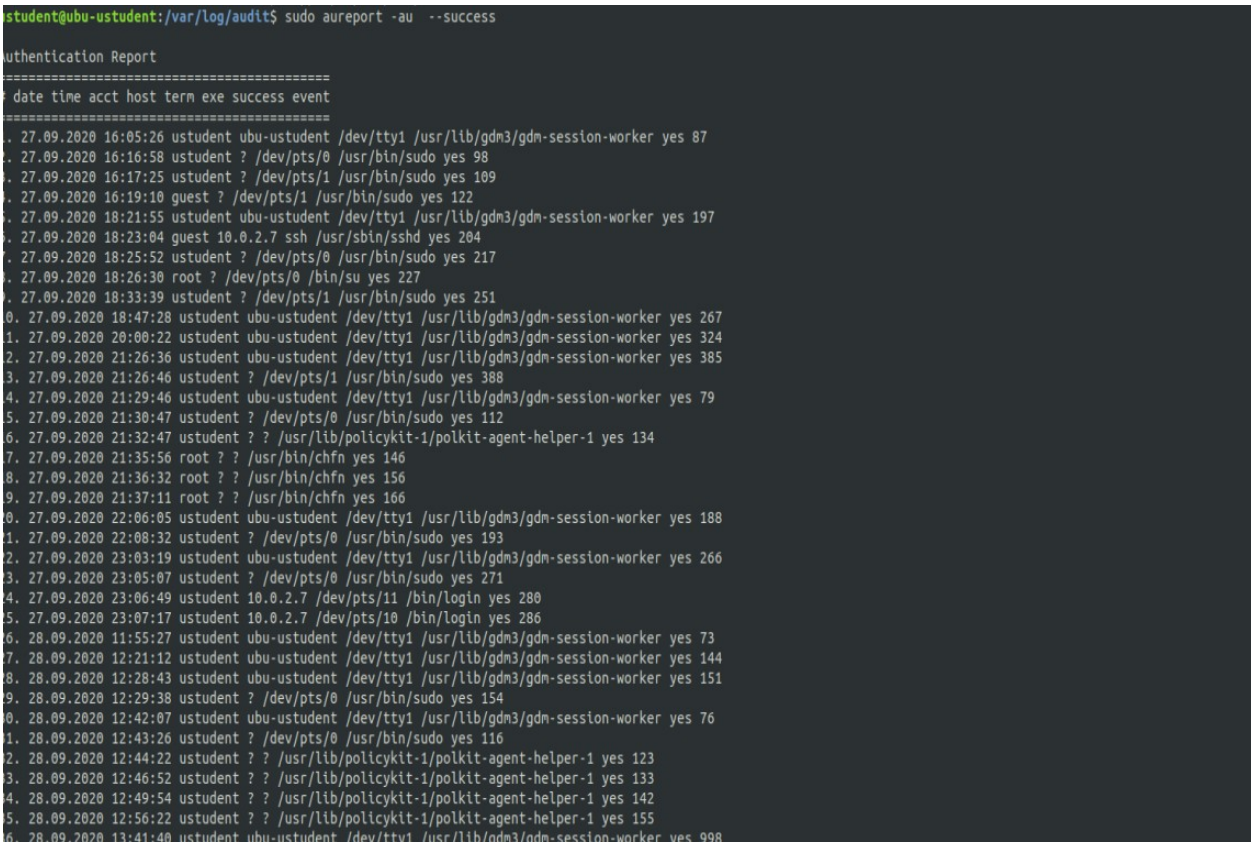
The aureport shows that there are a lot of login attempts with unknown/invalid user names. That could be a possible bruteforce attack. We will check this later. The only ones that were abel to login successfully were ustudent and guest. They only have 4 and 1 failed wrong password attempts. Thus they are not part of any brute force attack. Therefore, the assumption is that nothing special happened here.





It looks like a bruteforce attack from host 10.0.2.7 as by checking the timeline of the failed attempts we see that there are many attempts with different usernames in a short period of time.





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.

Ubuntu:
Ubuntu CIS 4.2.1.3 is satisfied.

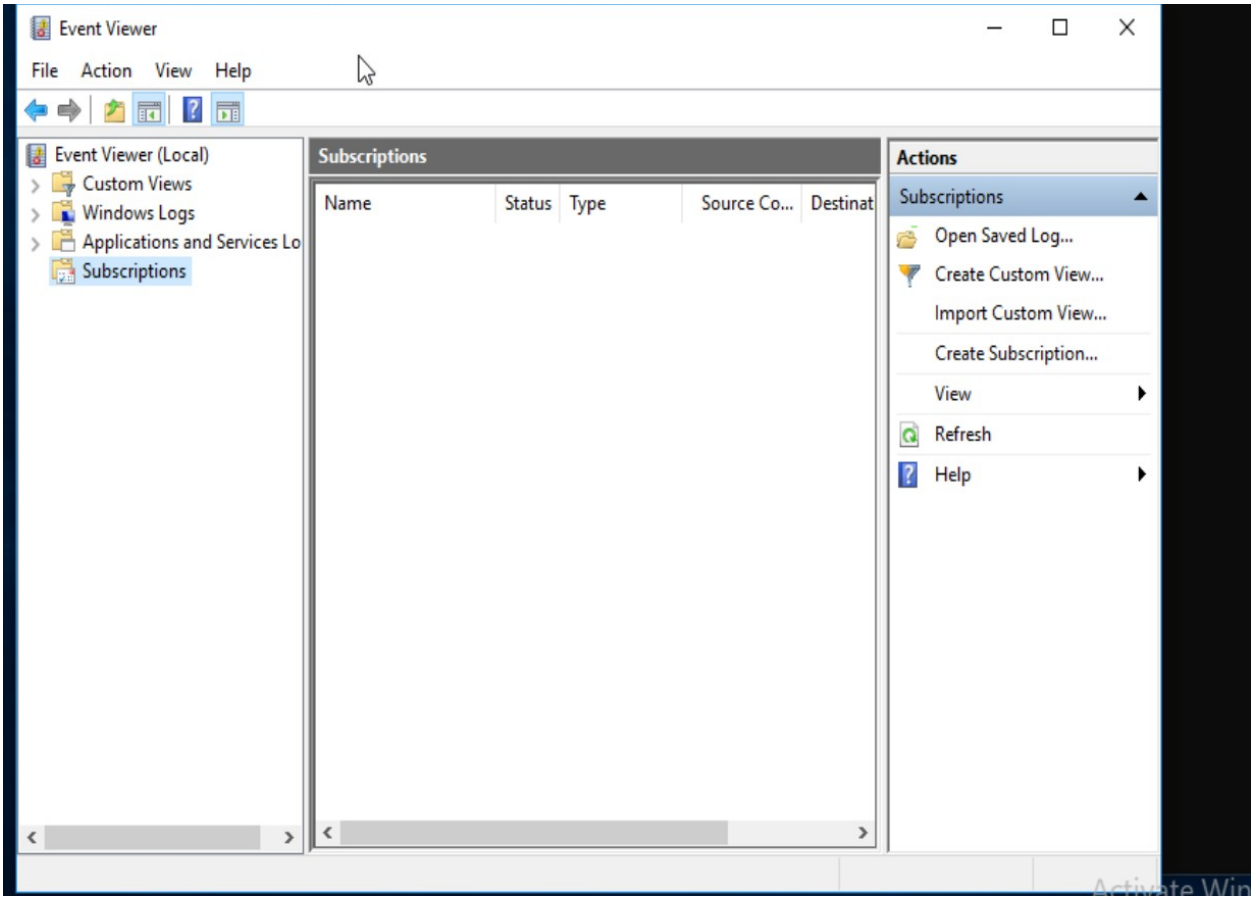
```
ustudent@ubu-ustudent:/etc$ cat rsyslog.conf
#  /etc/rsyslog.conf    Configuration file for rsyslog.
#
#                       For more information see
#                       /usr/share/doc/rsyslog-doc/html/rsyslog_conf.html
#
#  Default logging rules can be found in /etc/rsyslog.d/50-default.conf


################
#### MODULES ####
################

module(load="imuxsock") # provides support for local system logging
#module(load="immark")  # provides --MARK-- message capability

# provides UDP syslog reception
#module(load="imudp")
#input(type="imudp" port="514")

# provides TCP syslog reception
#module(load="imtcp")
#input(type="imtcp" port="514")

# provides kernel logging support and enable non-kernel klog messages
module(load="imklog" permitnonkernelfacility="on")

###########################
#### 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
```

But Ubuntu CIS 4.2.1.5 which checks if rsyslog is configured to send logs to a remote host is not fulfilled. There is no target ip adress where to send the logs to.

```
ustudent@ubu-ustudent:/etc$ cat /etc/rsyslog.conf /etc/rsyslog.d/*.conf | grep target
ustudent@ubu-ustudent:/etc$
```

Windows:

I can’t see any subscription in Windows. So it’s not correctly set up.



In summary the system is not prepared for using a SIEM. The sending of the logs needs to be configured to be able to use it with a SIM.

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?

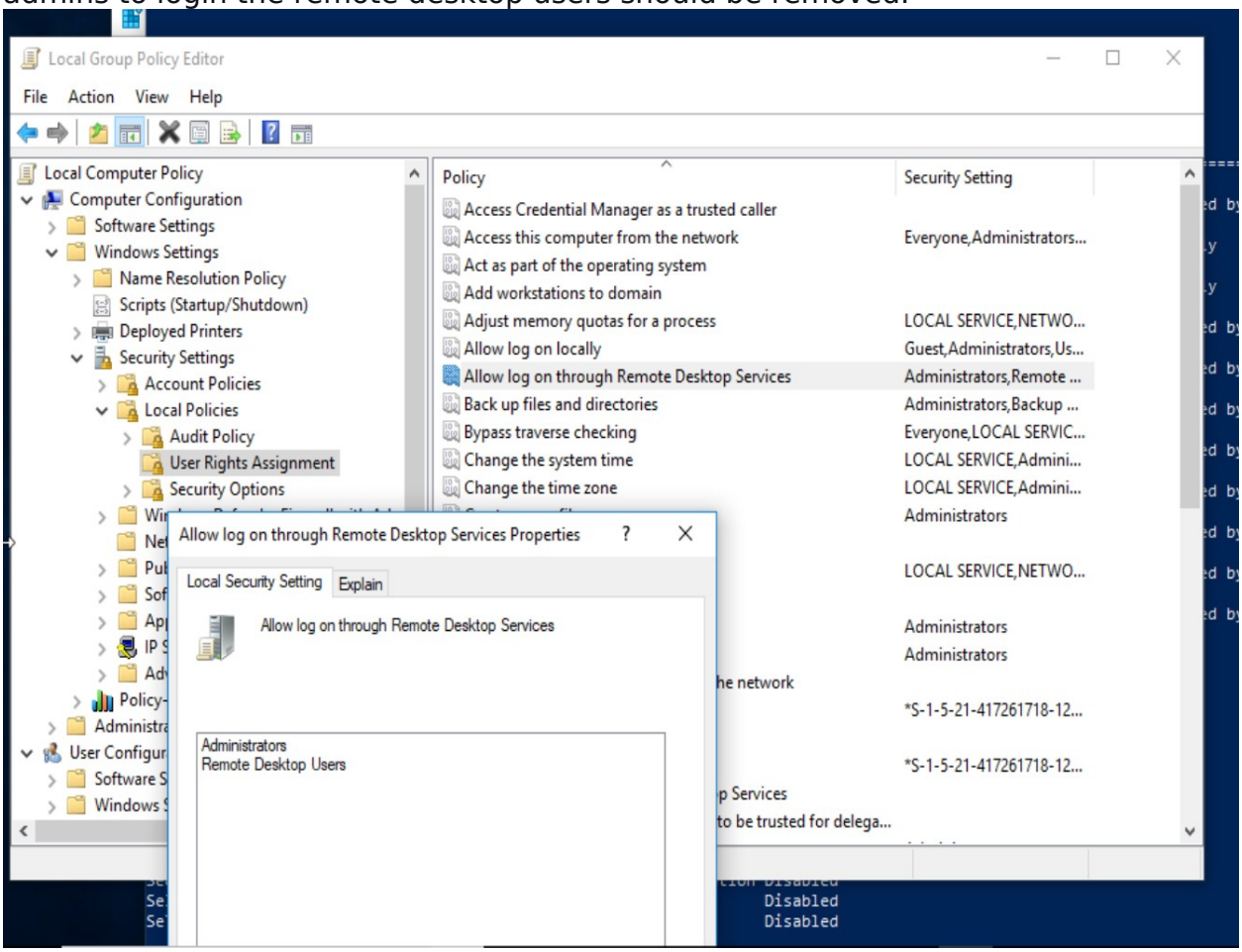
Knowing that your company only wants administrators to log remotely, provide a summary of the current situation for StaticSpeed. Then, suggest what accounts should be allowed to log remotely and why. Include your recommendations on whether StaticSpeeds authentication is acceptable and how you would improve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

In ubuntu all users have excessive permissions as discussed earlier. That’s because all are allowed to switch to the superuser(sudo).

In ubuntu ssh root login is disabled by default as a security feature. I don’t see a PermitRootLogin yes in the configuration file. Thus root login is not allowed.
There should be not root access in linux from the outside. It should be restricted to to local ip adresses for root login. Normal users can login. To improve security all users can be denied the access. The only exception is root if they are in the local network.

```
ustudent@ubu-ustudent:~$ cat /etc/ssh/sshd_config | grep Permit
#PermitRootLogin prohibit-password
#PermitEmptyPasswords no
# the setting of "PermitRootLogin without-password".
#PermitTTY yes
#PermitUserEnvironment no
#PermitTunnel no
#       PermitTTY no
ustudent@ubu-ustudent:~$
```

In Windows Admins as well as normal users can remotely login. To only allow admins to login the remote desktop users should be removed.



Task 2

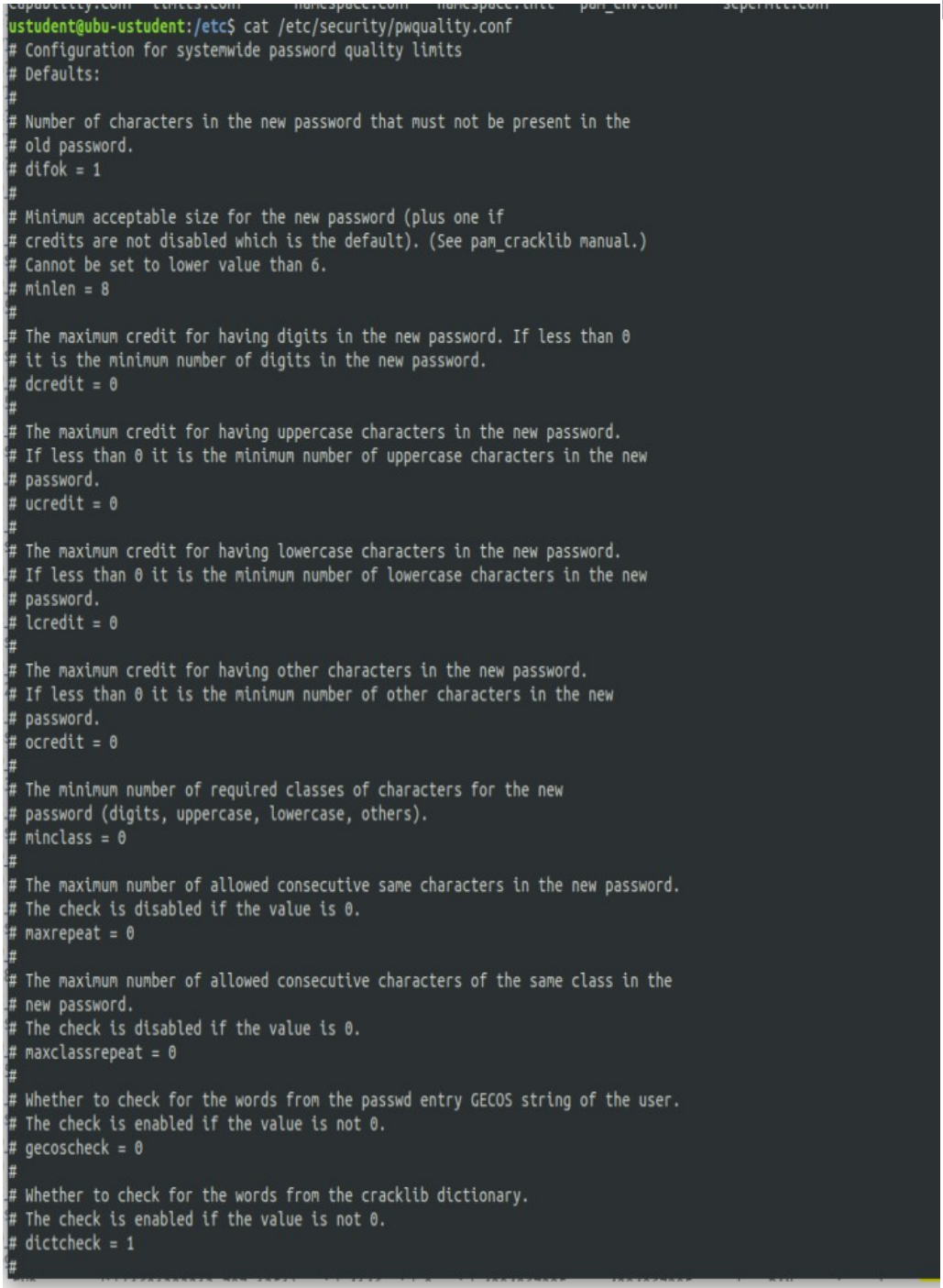
NuttyUtility follows CIS Benchmarks. Therefore, we need to audit the password policies of StaticSpeed to see if they comply.

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.

CIS 5.3.1 Ubuntu –Ensure password creation requirements are configured

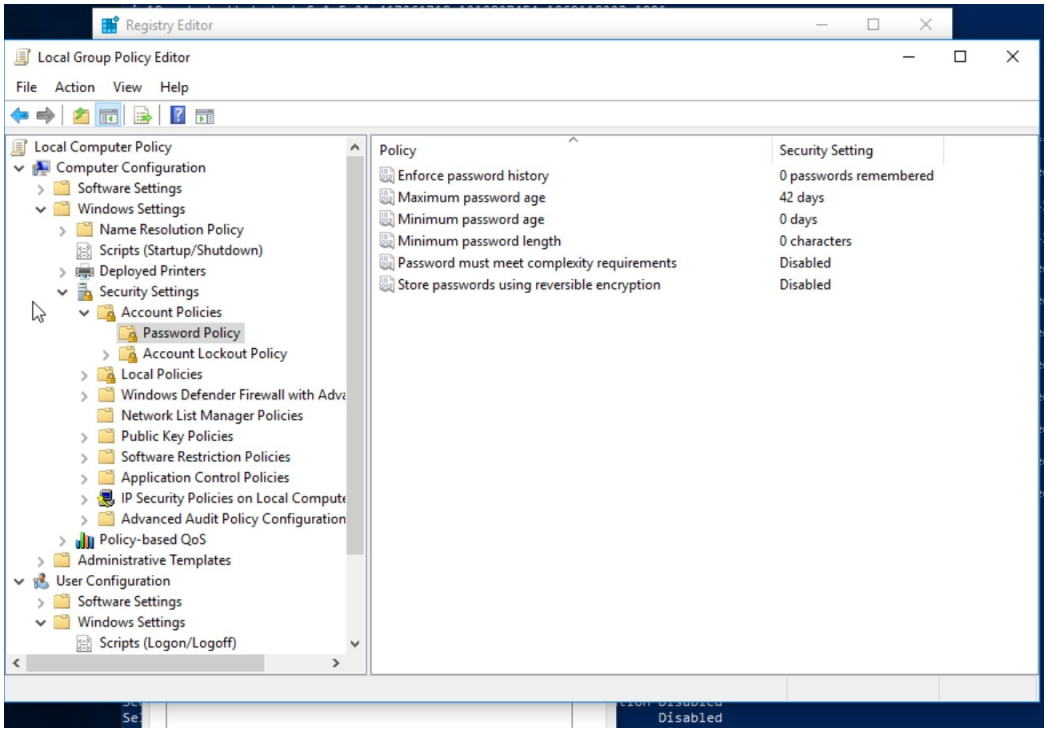
The CIS is not fullfilled as can be seen in the screenshot below. The password should be set to minlen = 14 and minclass = 4 or dcredit = -1 ucredit = -1 ocredit = -1 lcredit = -1



```
ustudent@ubu-ustudent:/etc$ cat /etc/security/pwquality.conf
# Configuration for systemwide password quality limits
# Defaults:
#
# Number of characters in the new password that must not be present in the
# old password.
# difok = 1
#
# Minimum acceptable size for the new password (plus one if
# credits are not disabled which is the default). (See pam_cracklib manual.)
# Cannot be set to lower value than 6.
# minlen = 8
#
# The maximum credit for having digits in the new password. If less than 0
# it is the minimum number of digits in the new password.
# dcredit = 0
#
# The maximum credit for having uppercase characters in the new password.
# If less than 0 it is the minimum number of uppercase characters in the new
# password.
# ucredit = 0
#
# The maximum credit for having lowercase characters in the new password.
# If less than 0 it is the minimum number of lowercase characters in the new
# password.
# lcredit = 0
#
# The maximum credit for having other characters in the new password.
# If less than 0 it is the minimum number of other characters in the new
# password.
# ocredit = 0
#
# The minimum number of required classes of characters for the new
# password (digits, uppercase, lowercase, others).
# minclass = 0
#
# The maximum number of allowed consecutive same characters in the new password.
# The check is disabled if the value is 0.
# maxrepeat = 0
#
# The maximum number of allowed consecutive characters of the same class in the
# new password.
# The check is disabled if the value is 0.
# maxclassrepeat = 0
#
# Whether to check for the words from the passwd entry GECOS string of the user.
# The check is enabled if the value is not 0.
# gecoscheck = 0
#
# Whether to check for the words from the cracklib dictionary.
# The check is enabled if the value is not 0.
# dictcheck = 1
#
```

Windows 10 CIS benchmarks 1.1.5 – Ensure 'Password must meet complexity requirements' is set to 'Enabled'

The setting is disabled. It should be enabled to ensure that passwords are secure.

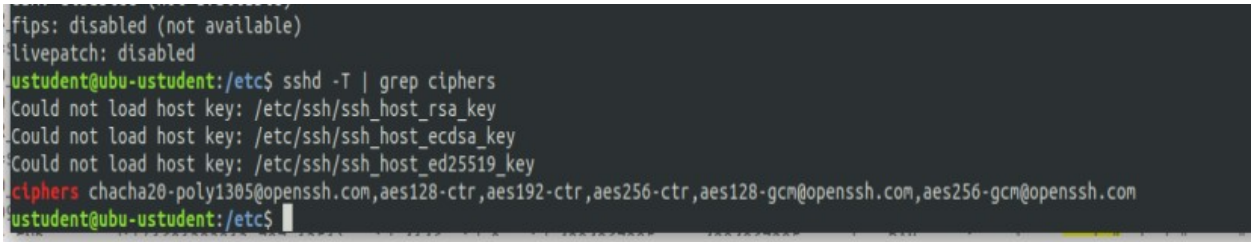


Task 3

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.

Ubuntu 18.04 CIS 5.2.13 -Ensure only strong Ciphers are used

This CIS is fulfilled by the linux machine



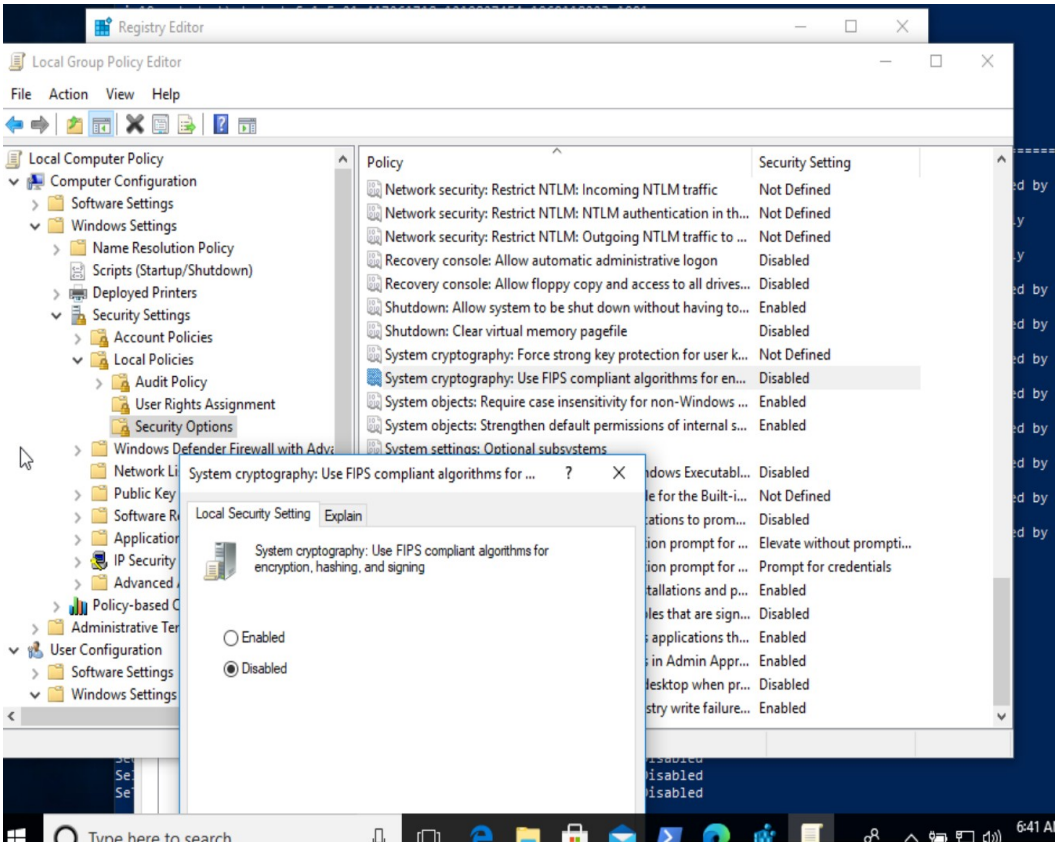
FIPS 140-2 is not installed in ubuntu.

```
Datei  Bearbeiten  Ansicht  Suchen  Terminal  Hilfe
ustudent@ubu-ustudent:~$ dpkg -l | grep fips
ustudent@ubu-ustudent:~$ cat /proc/sys/crypto/fips_enabled
cat: /proc/sys/crypto/fips_enabled: Datei oder Verzeichnis nicht gefunden
ustudent@ubu-ustudent:~$
```

This link describes how to enable FIPS 140-2: https://ubuntu.com/security/certifications/docs/fips-faq

```
# dictpath =
ustudent@ubu-ustudent:/etc$ ^C
ustudent@ubu-ustudent:/etc$ sudo ua status
[sudo] Passwort für ustudent:
esm: disabled (not available)
fips: disabled (not available)
livepatch: disabled
ustudent@ubu-ustudent:/etc$
```

FIPS is disable in windows. It should be set to enabled

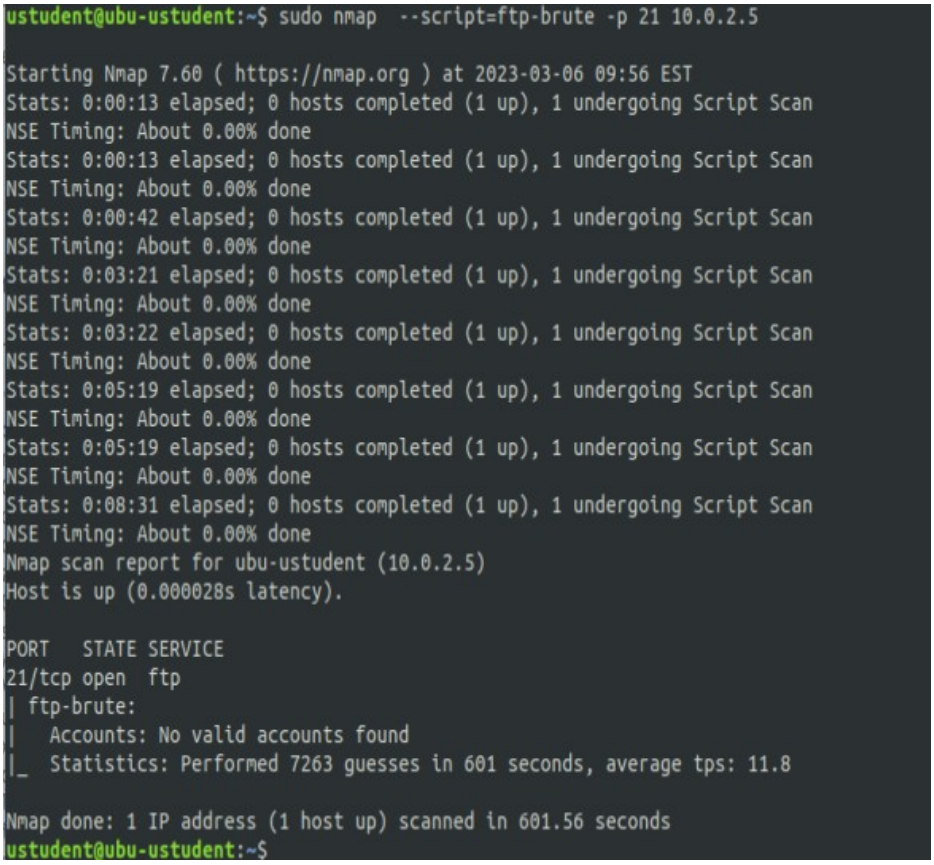


Task 4

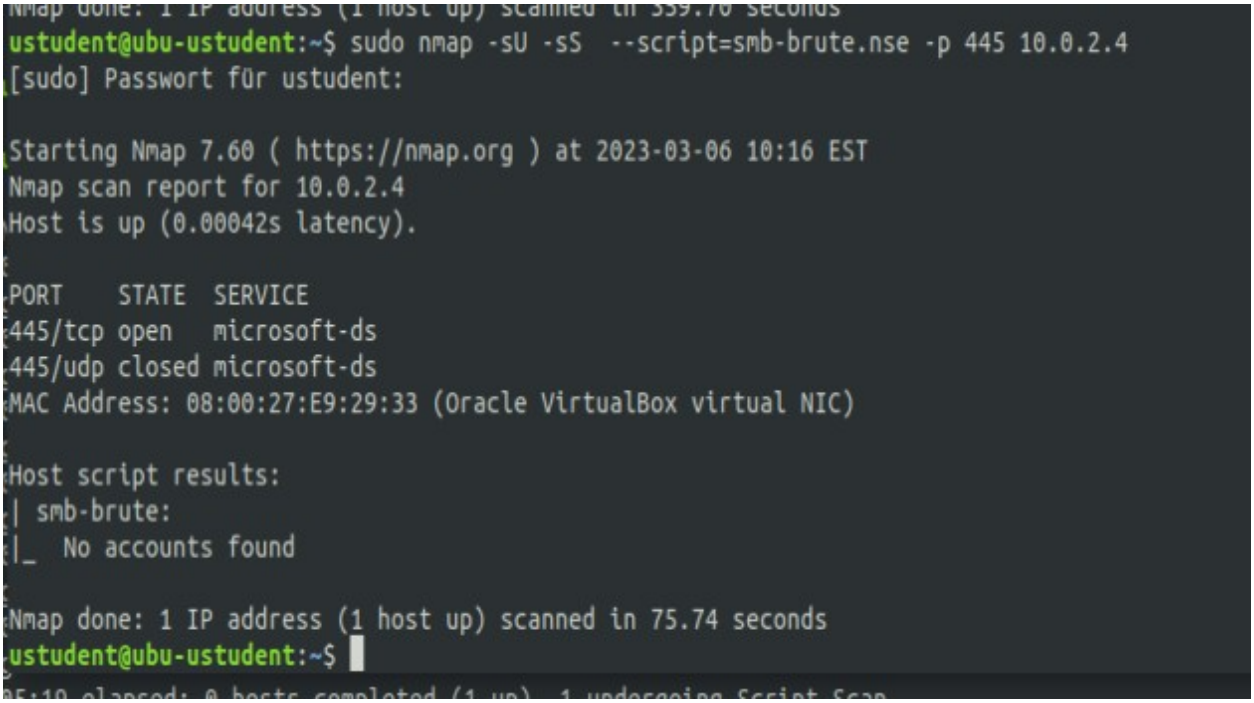
Conduct aggressive testing for password strength. Use a Nmap NSE Script to test how easy it would be to access StaticSpeed's FTP Server and SMB Shares if an attacker probed them. We have already requested and obtained permission to perform these audits.

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.

The ftp server in ubuntu seems to be at least at basic securtiy as the bruteforce attack didn’t return any valid credentials:



No valid credentials found for smb. Thus it seems at least to be not easily attacked.



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	5	6	1	0

IP Address: 10.0.2.4

Service	Port	Sensitive Level
Auto Update		High
Discard Service	9 tcp	High
msrpc	135 tcp	
netbios-ssn	139 tcp	
Microsoft ds	445 tcp	
SEHOP Password Complexity	TCP	Medium
Password Quality		Medium
chargen	19 tcp	Medium
echo	7 tcp	Medium
qotd	17 tcp	Medium
Ms-wbt server	3389 tcp	
Daytime	13 tcp	Low
xxx	xx TCP	Log

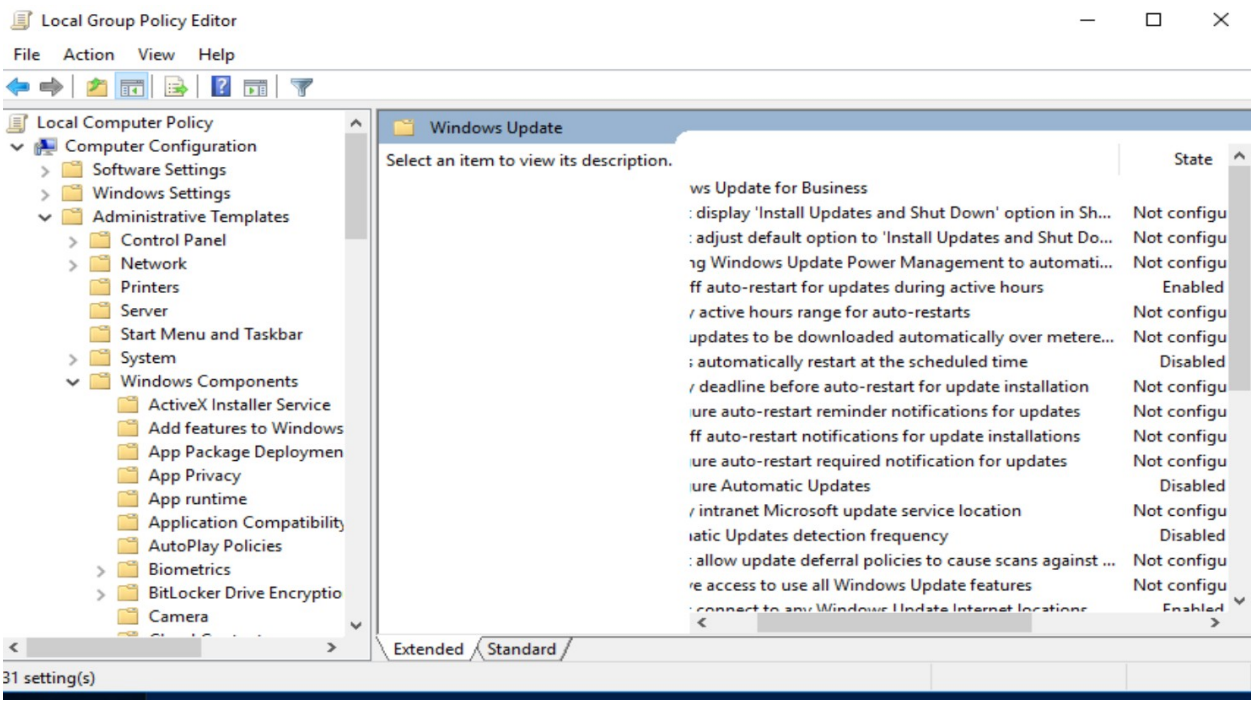
Expected detail format for vulnerabilities found

The scan shows multiple open ports:

```
Starting Nmap 7.60 ( https://nmap.org ) at 2023-03-03 10:58 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).
Stats: 0:03:03 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 100.00% done; ETC: 11:01 (0:00:00 remaining)
Nmap scan report for 10.0.2.4
Host is up (0.00029s 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)
|_sslv2-drown:
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 309.96 seconds
```

High - Windows Auto Update is disabled

Issue
Windows is not getting the latest security patches, which makes the system vulnerable



Impact
Attackers can exploit the knowledge about known security problems.

Mitigation
Windows Auto Update should be enabled

Reference
Windows CIS 18.9.102.2

High - CVE-1999-0636 – Discard Service Running

Issue
The discard service is running

Impact
Using a weakness in discard service users can elevate privileges. The attack is described in Das MITRE ATT&CK Projekt deklariert die Angriffstechnik als T1068.

Mitigation
Disable the discard service

Reference
https://www.cvedetails.com/cve/CVE-1999-0636/
https://vuldb.com/de/?id.14400

High - CVE-CVE-2022-26809 – msrpc Service

Issue
An integer overflow in MSRPC that, if exploited, allows for arbitrary code execution over the network without requiring authentication or user interaction.

Impact
The attacker can perform code execution which is very critical

Mitigation
According to Microsoft “The known attack that was presented to Microsoft does not use TCP Port 135 to initiate an exploit but, as the vulnerability is in RPC, blocking TCP port 135 at the enterprise perimeter firewall is a recommended best practice that would reduce the likelihood of other potential attacks against this vulnerability.”

Otherwise service should be patched

Reference
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26809

High - CVE-CVE-2022-26809 – netbios-ssn

Issue
Ports 139 and 445 are used for ‘NetBIOS’ communication between two Windows 2000 hosts. In the case of port 445 an attacker may use this to perform NetBIOS attacks as it would on port 139.

Impact
The attacker can perform code execution which is very critical

Mitigation
The ports should be disabled

Reference
https://support.microsoft.com/en-us/topic/preventing-smb-traffic-from-lateral-connections-and-entering-or-leaving-the-network-c0541db7-2244-0dce-18fd-14a3ddeb282a

High - CVE-CVE-2022-26809 – Microsoft Ds

Issue
Ports 139 and 445 are used for ‘NetBIOS’ communication between two Windows 2000 hosts. In the case of port 445 an attacker may use this to perform NetBIOS attacks as it would on port 139.

Impact
The attacker can perform code execution which is very critical

Mitigation
The ports should be disabled

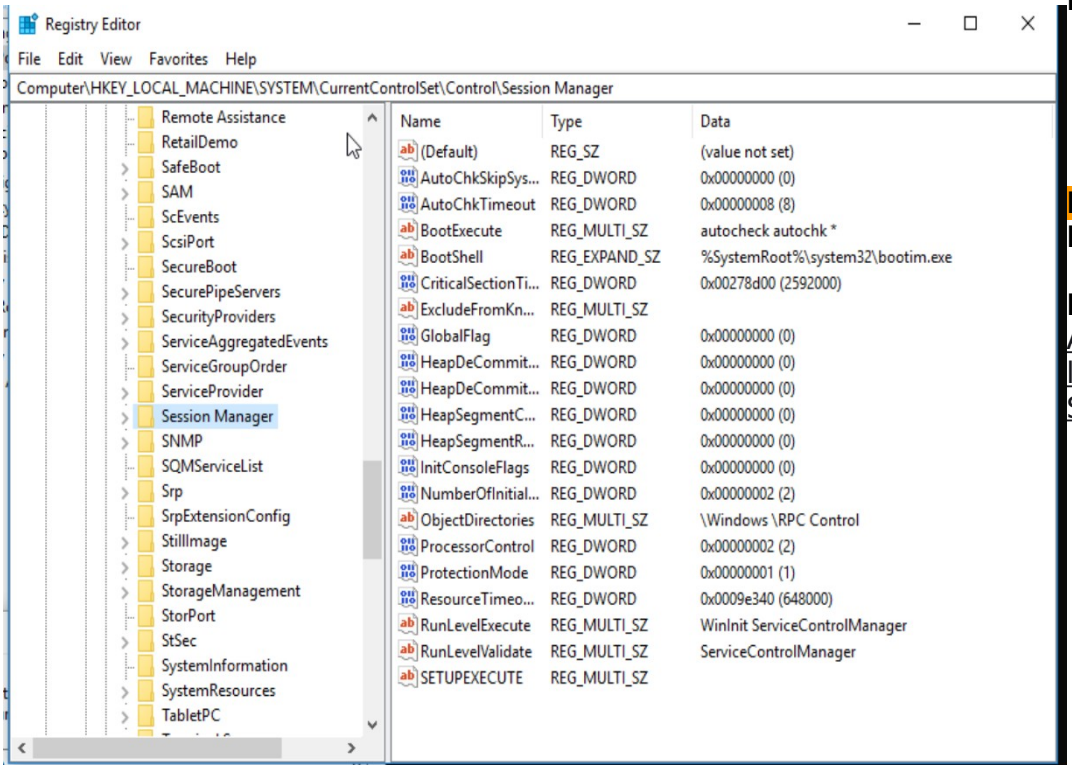
Reference
https://support.microsoft.com/en-us/topic/preventing-smb-traffic-from-lateral-connections-and-entering-or-leaving-the-network-c0541db7-2244-0dce-18fd-14a3ddeb282a

High - CVE-CVE-2022-26809 – msrpc Service

Issue

Impact

Mitigation



Reference

Medium - Enable

Issue
At a high-level, the SEH

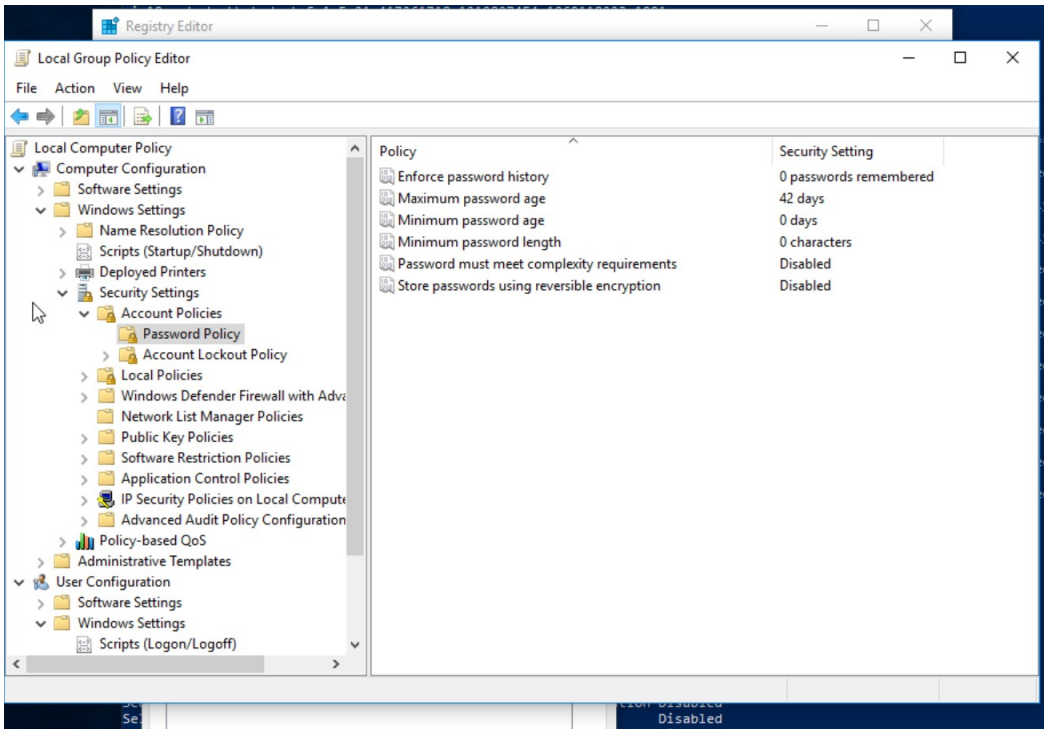
Impact
This feature is designed to block exploits that use the Structured Exception Handler (SEH) overwrite technique.

Mitigation
Set it to enabled. Just follow CIS 18.3.4

Reference
Windows CIS 18.3.4.

Medium - Ensure 'Password must meet complexity requirements' is set to 'Enabled'

Issue
There is no check that passwords contain a minimum complexity. If a weak password is chosen the attacker has an easy game.



Impact
An attacker can easily brutefore the password.

Mitigation
Follow the instructions of Windows 10 CIS benchmarks 1.1.5 and set the flag to enabled.

Reference
Windows 10 CIS benchmarks 1.1.5

Medium - CVE-1999-0103 - Chargen Service can be exploited

Issue
The chargen service can be used for denial of service attacks.

Impact
The attacker can flood the server and make it unavailable. It furthermore can be used as an intermediate server for causing the attack.

Mitigation
The chargen service should be disabled

Reference
https://www.cvedetails.com/cve/CVE-1999-0103/
https://www.incibe-cert.es/en/blog/chargen-cyberattacks-based-chargen-protocol

Medium - CVE-1999-0103 - Echo Service can be exploited

Issue
The echo service can be used for denial of service attacks.

Impact
The attacker can flood the server and make it unavailable. It furthermore can be used as an intermediate server for causing the attack.

Mitigation
The echo service should be disabled

Reference
https://www.cvedetails.com/cve/CVE-1999-0103/
https://www.incibe-cert.es/en/blog/chargen-cyberattacks-based-chargen-protocol

Medium- CVE-1999-0103 – QOTD Service Running

Issue
Remote Code Execution Vulnerability

Impact
A remote code execution vulnerability exists in Remote Desktop Services formerly known as Terminal Services when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests, aka 'Remote Desktop Services Remote Code Execution Vulnerability'.

Mitigation
Disable the service

Reference
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0708

Medium- CVE-2019-0708 - MS Terminal Services Running

Issue
The qotd service is running.

Impact
The qotd service can be used to flood the server with a bomb or packet storm.

Mitigation
Disable the service

Reference
https://www.cvedetails.com/cve/CVE-1999-0103/

Low- CVE-1999-0638 – Daytime Service Running

Issue
The daytime service is running.

Impact
The daytime service is an unsecured and obsolete protocol and it should be disabled.

Mitigation
Should be disabled

Reference
https://nvd.nist.gov/vuln/detail/CVE-1999-0638

Ubuntu 18.04

Ex

Host	High	Medium	Low	Log
10.0.2.5	3	3	2	1

IP Address: 10.0.2.5

Service	Port	Sensitive Level
ftp	21 tcp	High
ssh	22 tcp	High
telnet	23 tcp	High
netbios-ssn	139 tcp	HIgh
netbios-ssn	445 tcp	High
http	80 tcp	Medium
http	80 tcp	Medium
qotd	17/tcp	Medium
Daytime	13/tcp	Low
ASLR		Low

Scan Results of Ubuntu:

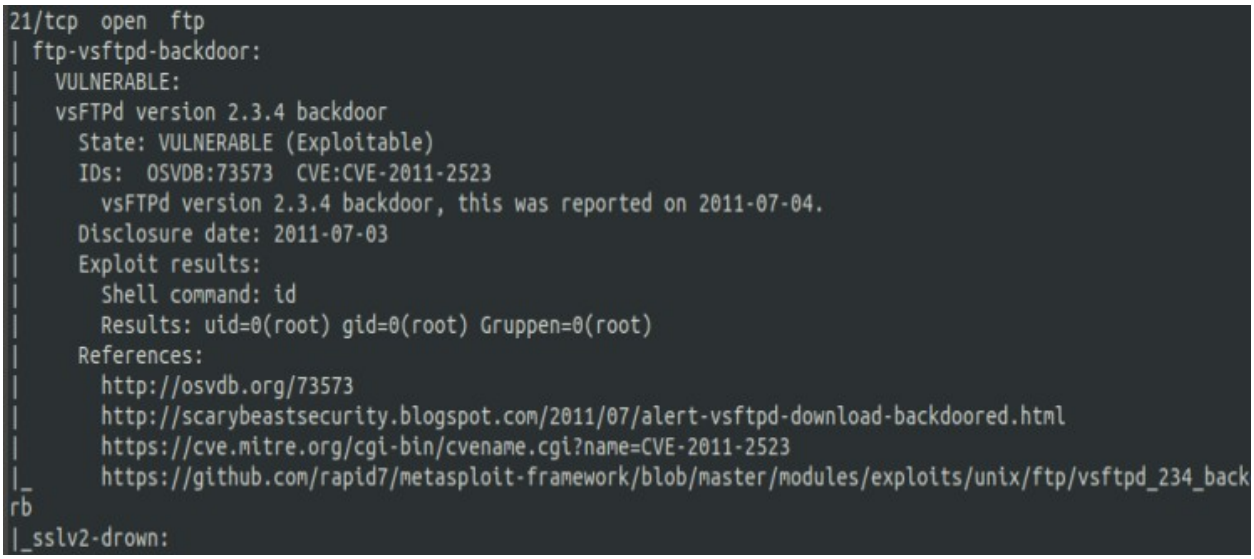
```
Nmap scan report for ubu-ustudent (10.0.2.5)
Host is up (0.00033s latency).
Not shown: 991 closed ports
PORT    STATE SERVICE     VERSION
13/tcp  open  daytime
17/tcp  open  qotd?
| fingerprint-strings:
|   DNSStatusRequest:
|     You see, I consider that a man's brain originally is like a little empty
|     attic, and you have to stock it with such furniture as you choose. A fool
|     takes in all the lumber of every sort he comes across, so that the knowledge
|     which might be useful to him gets crowded out, or at best is jumbled up with
|     other things, so that he has difficulty in laying his hands upon it.
|     skilful workman is very careful indeed as to what he takes into his
|     brain-attic. He will have nothing but the tools which may help him in doing
|     work, but of these he has a large assortment, and all in the most perfect
|     order. It is a mistake to think that that little room has elastic walls and
|     distend to any extent. Depend upon it there comes a time when for every
|     addition of knowledge you forget something that you knew before. It is of
|     highest importance, therefore, not to have useless facts
|   GenericLines:
|     The time is right to make new friends.
|   Help:
|     You will overcome the attacks of jealous associates.
|   Kerberos:
|     That secret you've been guarding, isn't.
|   NULL:
|     Things past redress and now with me past care.
|     William Shakespeare, "Richard II"
|   RTSPRequest:
|     You have a deep appreciation of the arts and music.
|   SSLSessionReq:
|     You will pass away very quickly.
|   TLSSessionReq:
|_    You should go home.
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: 2023-03-03T14:56:17
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)
```

```
SF:stock\x20it\x20with\x20such\x20furniture\x20as\x20you\x20choose\.\x20\x
SF:20A\x20fool\ntakes\x20in\x20all\x20the\x20lumber\x20of\x20every\x20sort
SF:\x20he\x20comes\x20across,\x20so\x20that\x20the\x20knowledge\nwhich\x20
SF:might\x20be\x20useful\x20to\x20him\x20gets\x20crowded\x20out,\x20or\x20
SF:at\x20best\x20is\x20jumbled\x20up\x20with\na\x20lot\x20of\x20other\x20t
SF:hings,\x20so\x20that\x20he\x20has\x20difficulty\x20in\x20laying\x20his\
SF:x20hands\x20upon\x20it\.\nNow\x20the\x20skilful\x20workman\x20is\x20ver
SF:y\x20careful\x20indeed\x20as\x20to\x20what\x20he\x20takes\x20into\x20hi
SF:s\nbrain-attic\.\x20\x20He\x20will\x20have\x20nothing\x20but\x20the\x20
SF:tools\x20which\x20may\x20help\x20him\x20in\x20doing\nhis\x20work,\x20bu
SF:t\x20of\x20these\x20he\x20has\x20a\x20large\x20assortment,\x20and\x20al
SF:l\x20in\x20the\x20most\x20perfect\norder\.\x20\x20It\x20is\x20a\x20mist
SF:ake\x20to\x20think\x20that\x20that\x20little\x20room\x20has\x20elastic\
SF:x20walls\x20and\ncan\x20distend\x20to\x20any\x20extent\.\x20\x20Depend\
SF:x20upon\x20it\x20there\x20comes\x20a\x20time\x20when\x20for\x20every\na
SF:ddition\x20of\x20knowledge\x20you\x20forget\x20something\x20that\x20you
SF:\x20knew\x20before\.\x20\x20It\x20is\x20of\nthe\x20highest\x20importanc
SF:e,\x20therefore,\x20not\x20to\x20have\x20useless\x20facts")%r(Help,35,"
SF:You\x20will\x20overcome\x20the\x20attacks\x20of\x20jealous\x20associate
SF:s\.\n")%r(SSLSessionReq,21,"You\x20will\x20pass\x20away\x20very\x20quic
SF:kly\.\n")%r(TLSSessionReq,14,"You\x20should\x20go\x20home\.\n")%r(Kerbe
SF:ros,29,"That\x20secret\x20you've\x20been\x20guarding,\x20isn't\.\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: \\10.0.2.5\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: \\10.0.2.5\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 71.34 seconds
```

High - ftp - CVE-2011-2523

Issue

vsFTPd contains a backdoor which opens a shell on port 6200/tcp.



Impact
The attacker can open a shell and then is able to takeover full control

Mitigation
In general ftp should be disabled due to this and other problems. It should be replaced by a more secure service.

Reference

https://nvd.nist.gov/vuln/detail/CVE-2011-2523

High - ssh - CVE-2021-41617

Issue
ssh runs in an old version OpenSSH 7.6

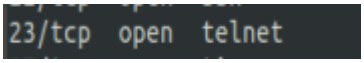
Impact
sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

Mitigation
Update to the newest version of OpenSSH

Reference
https://nvd.nist.gov/vuln/detail/CVE-2021-41617

High - 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/

High - CVE-2017-7494 – netbios-ssn

Issue
Ports 139 and 445 are used for 'NetBIOS' communication between hosts. In the case of port 445 an attacker may use this to perform NetBIOS attacks as it would on port 139.

Impact
The attacker can perform code execution which is very critical

Mitigation
The ports should be disabled

Reference
https://support.microsoft.com/en-us/topic/preventing-smb-traffic-from-lateral-connections-and-entering-or-leaving-the-network-c0541db7-2244-0dce-18fd-14a3ddeb282a

High - CVE-2017-7494 – netbios-ssn

Issue
Ports 139 and 445 are used for 'NetBIOS' communication between hosts. In the case of port 445 an attacker may use this to perform NetBIOS attacks as it would on port 139.

Impact
The attacker can perform code execution which is very critical

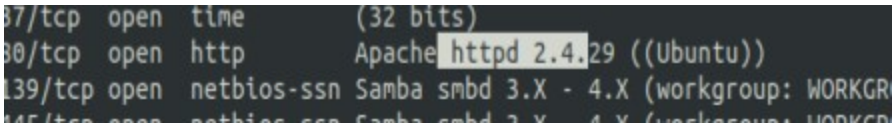
Mitigation

The ports should be disabled

Reference
https://support.microsoft.com/en-us/topic/preventing-smb-traffic-from-lateral-connections-and-entering-or-leaving-the-network-c0541db7-2244-0dce-18fd-14a3ddeb282a

Med - http - CVE-2018-17189

Issue
In Apache HTTP server versions 2.4.37 and prior, by sending request bodies in a slow loris way to plain resources, the h2 stream for that request unnecessarily occupied a server thread cleaning up that incoming data.



Impact
The server resources are lowered

Mitigation
The version of apache should be upgraded

Reference
https://www.cvedetails.com/cve/CVE-2018-17189/

Med - http - CVE-2018-1312

Issue
In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed.

Impact
In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.

Mitigation
upgrade the versioin of apache

Reference
https://www.cvedetails.com/cve/CVE-2018-1312/

Med- CVE-1999-0103 – QOTD Service Running

Issue
The qotd service is running.

Impact
The qotd service can be used to flood the server with a bomb or packet storm.

Mitigation
Disable the service

Reference
https://www.cvedetails.com/cve/CVE-1999-0103/

Low- CVE-1999-0638 – Daytime Service Running

Issue
The daytime service is running.

Impact
The daytime service is an unsecured and obsolete protocol and it should be disabled.

Mitigation
Should be disabled

Reference
https://nvd.nist.gov/vuln/detail/CVE-1999-0638

Low Ensure address space layout randomization (ASLR) is enabled

Issue
An attacker can examine the layout of an program and thus can use memory exploits

Impact
In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.

Mitigation
Follow the steps of CIS 1.6.2 and activate ASLR. Randomly placing virtual memory regions will make it difficult to write memory page exploits as the memory placement will be consistently shifting

Reference
Ubuntu CIS 1.6.2

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.

The final recommendation is not to include the StaticSpeed System

The table above shows that there are multiple vulnerabilities with a high criticality are found. In general it can be seen that the current system does not fulfill the the security standards that are needed to include it.

There were only a few CIS checked that failed the audition. Thus, it is recommend to go through the whole list of CIS and for each disabled one check if that’s really what we want.

The next steps would be to fix all the issues mention in this report. Afterwards a new scan should be made to check if there are other findings that are not already mentioned yet due to the high number of issues.