

# 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.

## **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

The screenshot shows the Local Group Policy Editor window. The left pane displays the navigation tree under 'Computer Configuration' / 'Administrative Templates' / 'Windows Components' / 'Windows Update'. The right pane shows a list of policy settings for 'Windows Update for Business'. One setting, 'Configure Automatic Updates', is highlighted and set to 'Enabled'. Other settings listed include 'Do not display 'Install Updates and Shut Down' option in Sh...', 'Do not adjust default option to 'Install Updates and Shut Do...', 'Enabling Windows Update Power Management to automati...', 'Turn off auto-restart for updates during active hours', 'Specify active hours range for auto-restarts', 'Allow updates to be downloaded automatically over metere...', 'Always automatically restart at the scheduled time', 'Specify deadline before auto-restart for update installation', 'Configure auto-restart reminder notifications for updates', 'Turn off auto-restart notifications for update installations', 'Configure auto-restart required notification for updates', 'Configure automatic updates', 'Specify intranet Microsoft update service location', 'Automatic Updates detection frequency', 'Do not allow update deferral policies to cause scans against ...', 'Remove access to use all Windows Update features', and 'Do not connect to any Windows Update Internet locations'. The status column indicates most settings are 'Not configu'.

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

This screenshot shows the same Local Group Policy Editor window as the previous one, but with a different focus. The left pane shows the navigation tree, and the right pane is now displaying the 'Configure Automatic Updates' dialog for the 'Windows Update for Business' policy. The 'Configure Automatic Updates' button at the top of the dialog is highlighted and set to 'Enabled'. The dialog also contains descriptive text about how it specifies whether the computer will receive security updates and other important downloads through the Windows automatic updating service. A note states that this policy does not apply to Windows RT. Below this, there is a section describing how the setting lets you specify when automatic updates are enabled on the computer. The status column for this setting shows 'Enabled'.

## 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

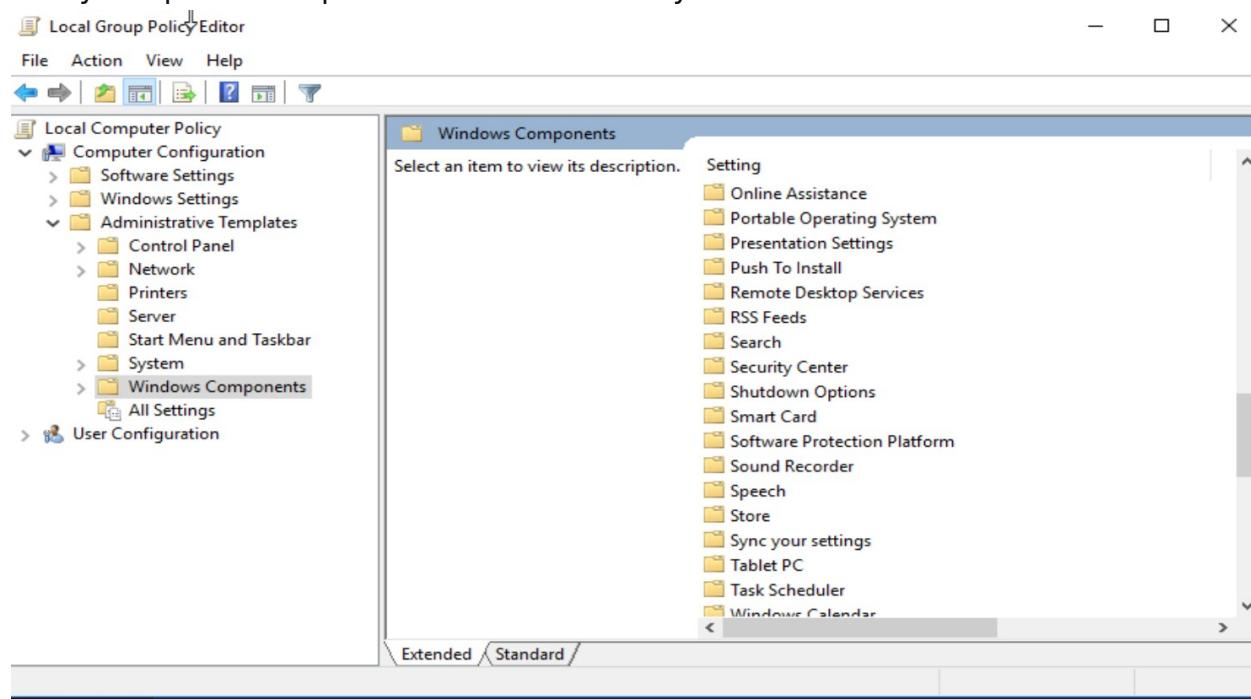
Next, verify that native protections for the operating systems are enough to protect systems from exploitation. (Hint: Think upgrades) We also need to know exactly what software is running on every machine. Also, please perform a software inventory on each computer and post your findings. The more you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

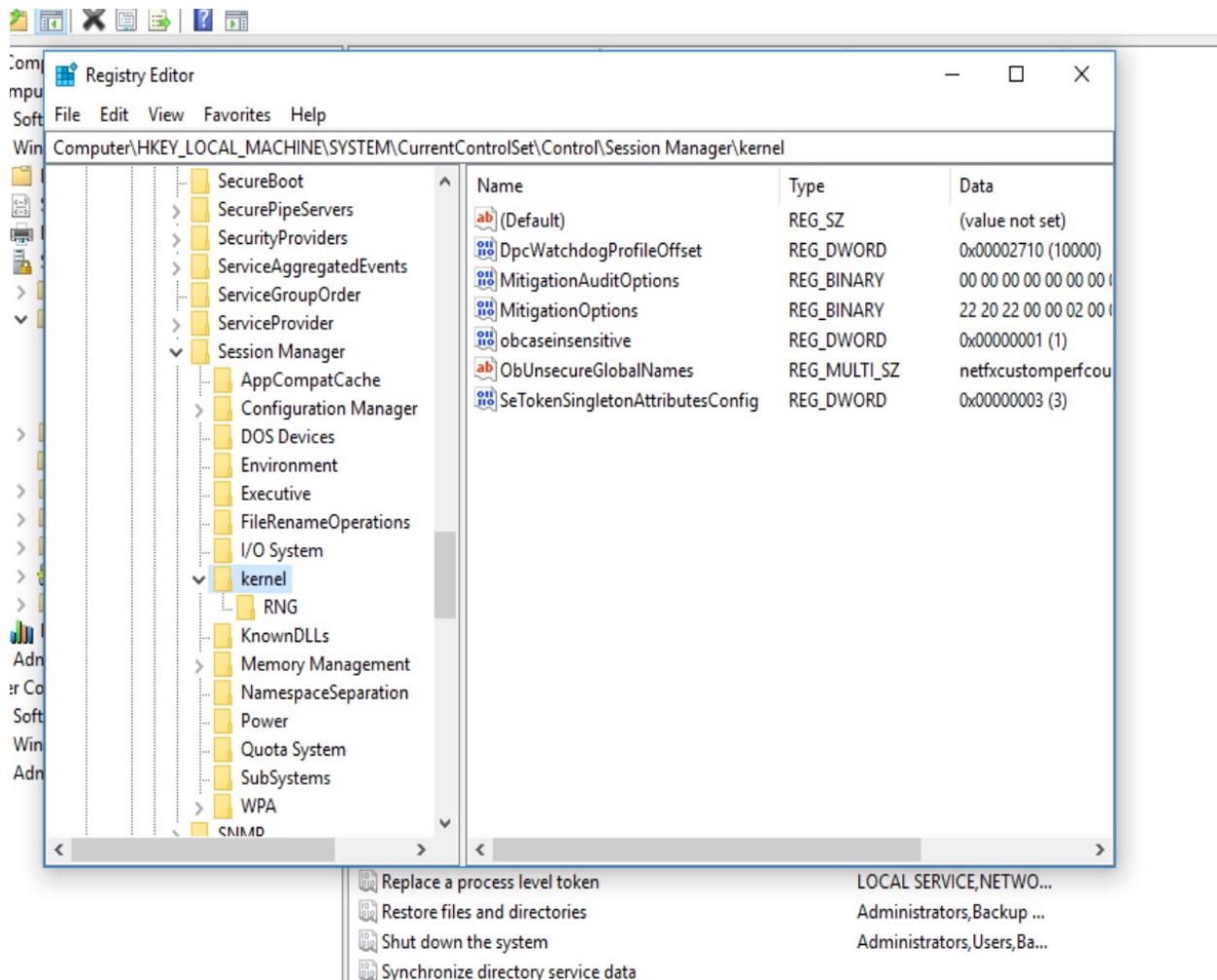
Ensure 'Enable Structured Exception Handling Overwrite Protection (SEHOP)' is set to 'Enabled.'

Is this system compliant?

It is not CIS compliant. The path from the CIS does not exist. An additional Group Policy template is required to add MS Security Guide.



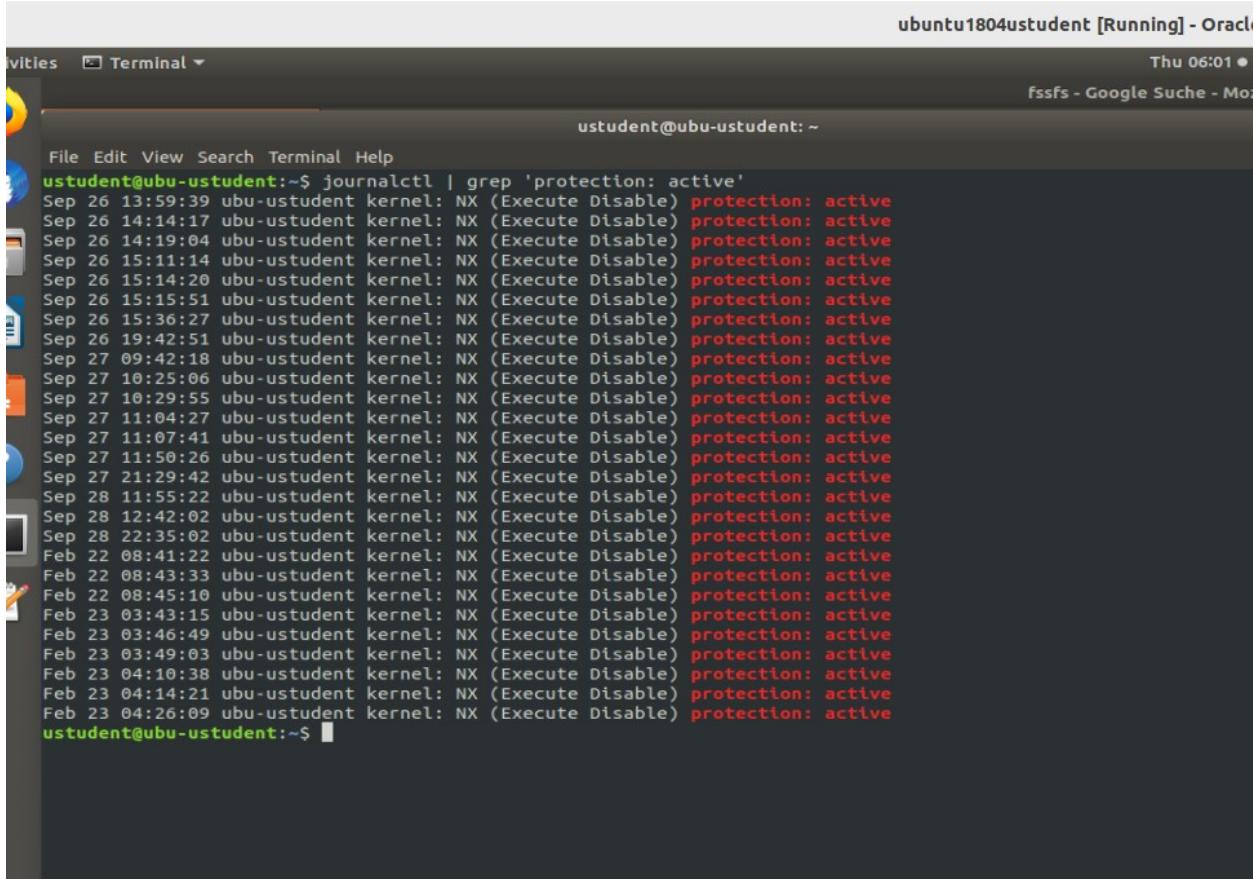
The registry entry DisableExceptionChainValidation is not available.



## Ubuntu CIS 1.6.1, 1.6.2

### 1.6.1 Ensure XD/NX support is enabled

The system is CIS conform

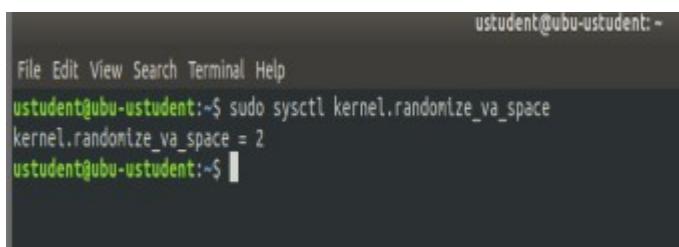


A screenshot of a Linux desktop environment showing a terminal window. The title bar says "ubuntu1804ustudent [Running] - Oracle VM VirtualBox". The terminal window shows the command "journalctl | grep 'protection: active'" being run, and its output. The output lists numerous kernel log entries from Sep 26 to Feb 23, each showing the kernel: NX (Execute Disable) protection: active. The terminal window has a dark background with light-colored text. The top right corner shows the date and time: Thu 06:01 ●. The top left corner shows the user "ustudent@ubu-ustudent: ~".

```
ustudent@ubu-ustudent:~$ journalctl | grep 'protection: active'
Sep 26 13:59:39 ubu-ustudent kernel: NX (Execute Disable) protection: active
Sep 26 14:14:17 ubu-ustudent kernel: NX (Execute Disable) protection: active
Sep 26 14:19:04 ubu-ustudent kernel: NX (Execute Disable) protection: active
Sep 26 15:11:14 ubu-ustudent kernel: NX (Execute Disable) protection: active
Sep 26 15:14:20 ubu-ustudent kernel: NX (Execute Disable) protection: active
Sep 26 15:15:51 ubu-ustudent kernel: NX (Execute Disable) protection: active
Sep 26 15:36:27 ubu-ustudent kernel: NX (Execute Disable) protection: active
Sep 26 19:42:51 ubu-ustudent kernel: NX (Execute Disable) protection: active
Sep 27 09:42:18 ubu-ustudent kernel: NX (Execute Disable) protection: active
Sep 27 10:25:06 ubu-ustudent kernel: NX (Execute Disable) protection: active
Sep 27 10:29:55 ubu-ustudent kernel: NX (Execute Disable) protection: active
Sep 27 11:04:27 ubu-ustudent kernel: NX (Execute Disable) protection: active
Sep 27 11:07:41 ubu-ustudent kernel: NX (Execute Disable) protection: active
Sep 27 11:50:26 ubu-ustudent kernel: NX (Execute Disable) protection: active
Sep 27 21:29:42 ubu-ustudent kernel: NX (Execute Disable) protection: active
Sep 28 11:55:22 ubu-ustudent kernel: NX (Execute Disable) protection: active
Sep 28 12:42:02 ubu-ustudent kernel: NX (Execute Disable) protection: active
Sep 28 22:35:02 ubu-ustudent kernel: NX (Execute Disable) protection: active
Feb 22 08:41:22 ubu-ustudent kernel: NX (Execute Disable) protection: active
Feb 22 08:43:33 ubu-ustudent kernel: NX (Execute Disable) protection: active
Feb 22 08:45:10 ubu-ustudent kernel: NX (Execute Disable) protection: active
Feb 23 03:43:15 ubu-ustudent kernel: NX (Execute Disable) protection: active
Feb 23 03:46:49 ubu-ustudent kernel: NX (Execute Disable) protection: active
Feb 23 03:49:03 ubu-ustudent kernel: NX (Execute Disable) protection: active
Feb 23 04:10:38 ubu-ustudent kernel: NX (Execute Disable) protection: active
Feb 23 04:14:21 ubu-ustudent kernel: NX (Execute Disable) protection: active
Feb 23 04:26:09 ubu-ustudent kernel: NX (Execute Disable) protection: active
ustudent@ubu-ustudent:~$
```

### 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



A screenshot of a Linux terminal window. The title bar says "ustudent@ubu-ustudent: ~". The terminal window shows the command "sudo sysctl kernel.randomize\_va\_space" being run, followed by the output "kernel.randomize\_va\_space = 2". The terminal window has a dark background with light-colored text. The top right corner shows the user "ustudent@ubu-ustudent: ~".

```
ustudent@ubu-ustudent:~$ sudo 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?

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

Is TightVNC installed on this Ubuntu machine?

Yes, TightVNC is installed

```
ustudent@uba-ustudent:~$ apt list --installed | grep vnc
WARNING: apt does not have a stable CLI interface. Use with caution in scripts.

libvncclient/bionic,now 0.9.11+dfsg-1ubuntu1 amd64 [installed]
remmina-plugin-vnc/bionic,now 1.2.0-rcgit.29+dfsg-1ubuntu1 amd64 [installed]
tightvncserver/bionic,now 1.3.10-0ubuntu4 amd64 [installed]
xtightvncviewer/bionic,now 1.3.10-0ubuntu4 amd64 [installed]
ustudent@uba-ustudent:~$
```

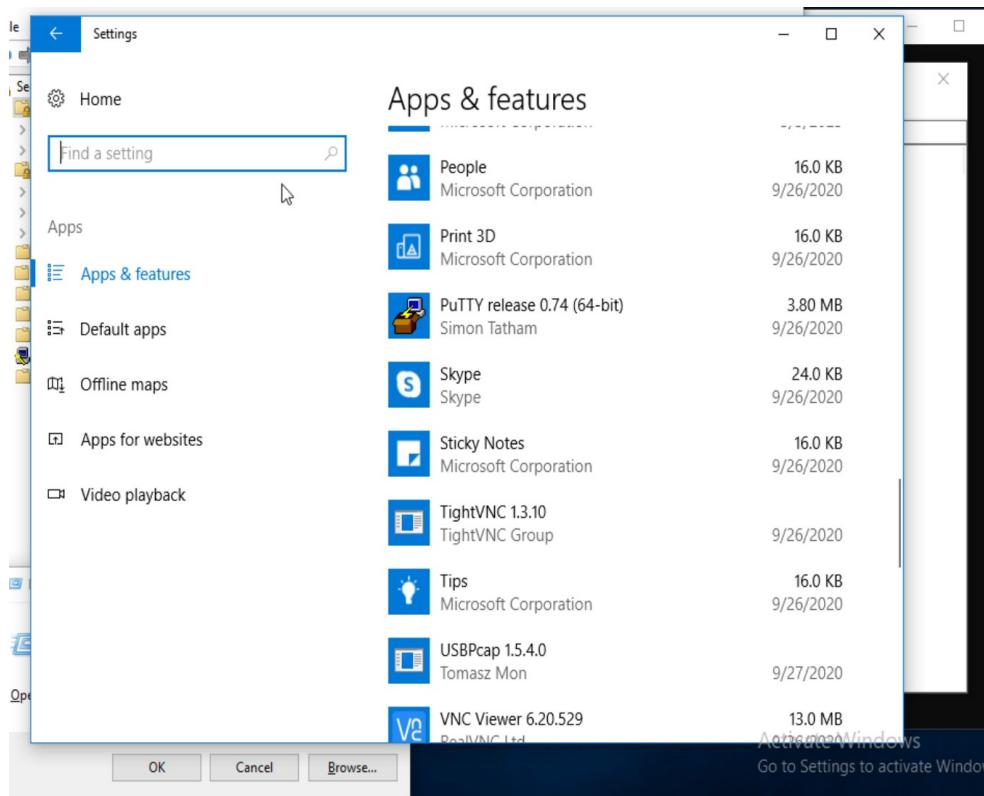
your answer.

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

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.
| TLS SessionReq:
|   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-server-header: Apache/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
```

Reiner Text ▾ Tabulatorbreite: 8 ▾

## 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

```
ustudent@ubu-ustudent:~$ cat /etc/network/interfaces
# interfaces(5) file used by ifup(8) and ifdown(8)
auto lo
iface lo inet loopback
ustudent@ubu-ustudent:~$
```

There is no vlan configured in windows

```
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
PS C:\Users\student> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . : lan
Link-local IPv6 Address . . . . . : fe80::80b0:c285:f15:9129%10
IPv4 Address. . . . . : 10.0.2.4
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.0.2.1

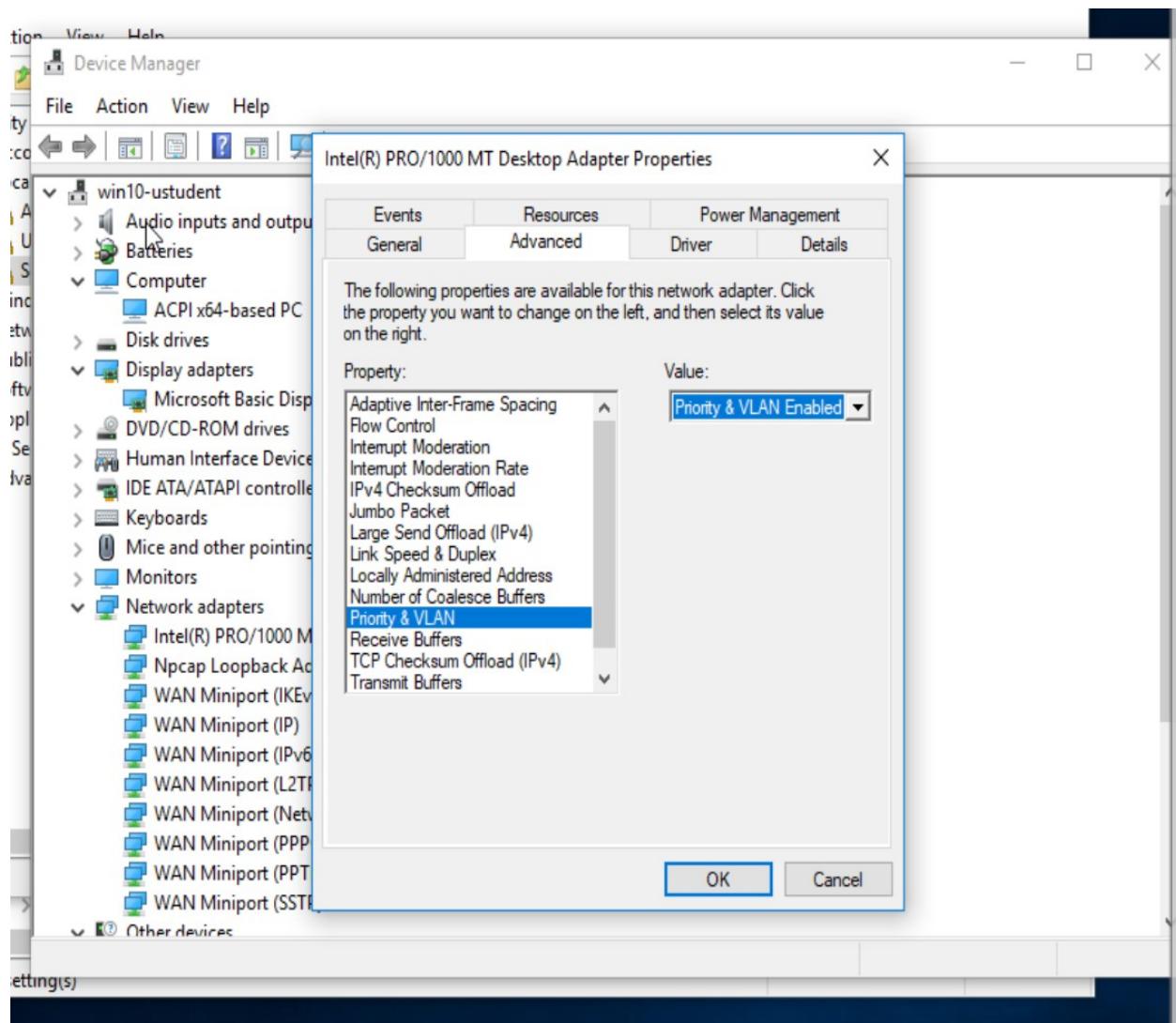
Ethernet adapter Npcap Loopback Adapter:

Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::5404:62b5:ceda:68c7%12
Autoconfiguration IPv4 Address. . . : 169.254.104.199
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . :

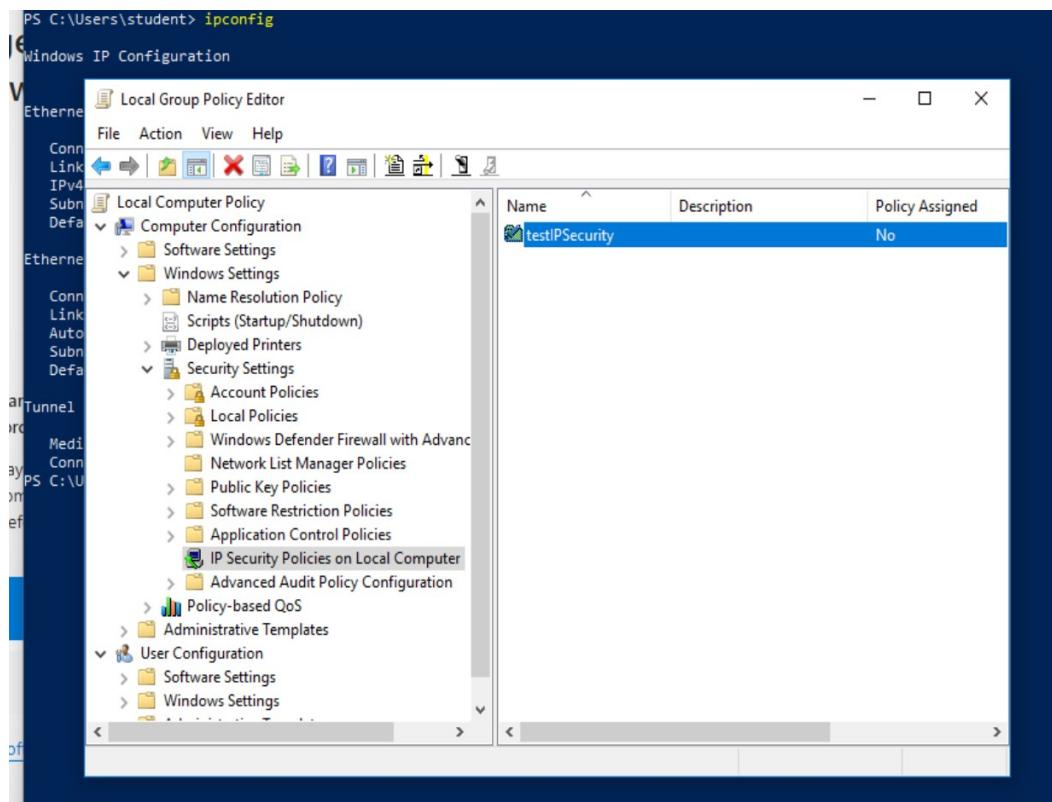
Tunnel adapter Teredo Tunneling Pseudo-Interface:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
PS C:\Users\student> ■
```

The network adapter is able to handle vlan



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



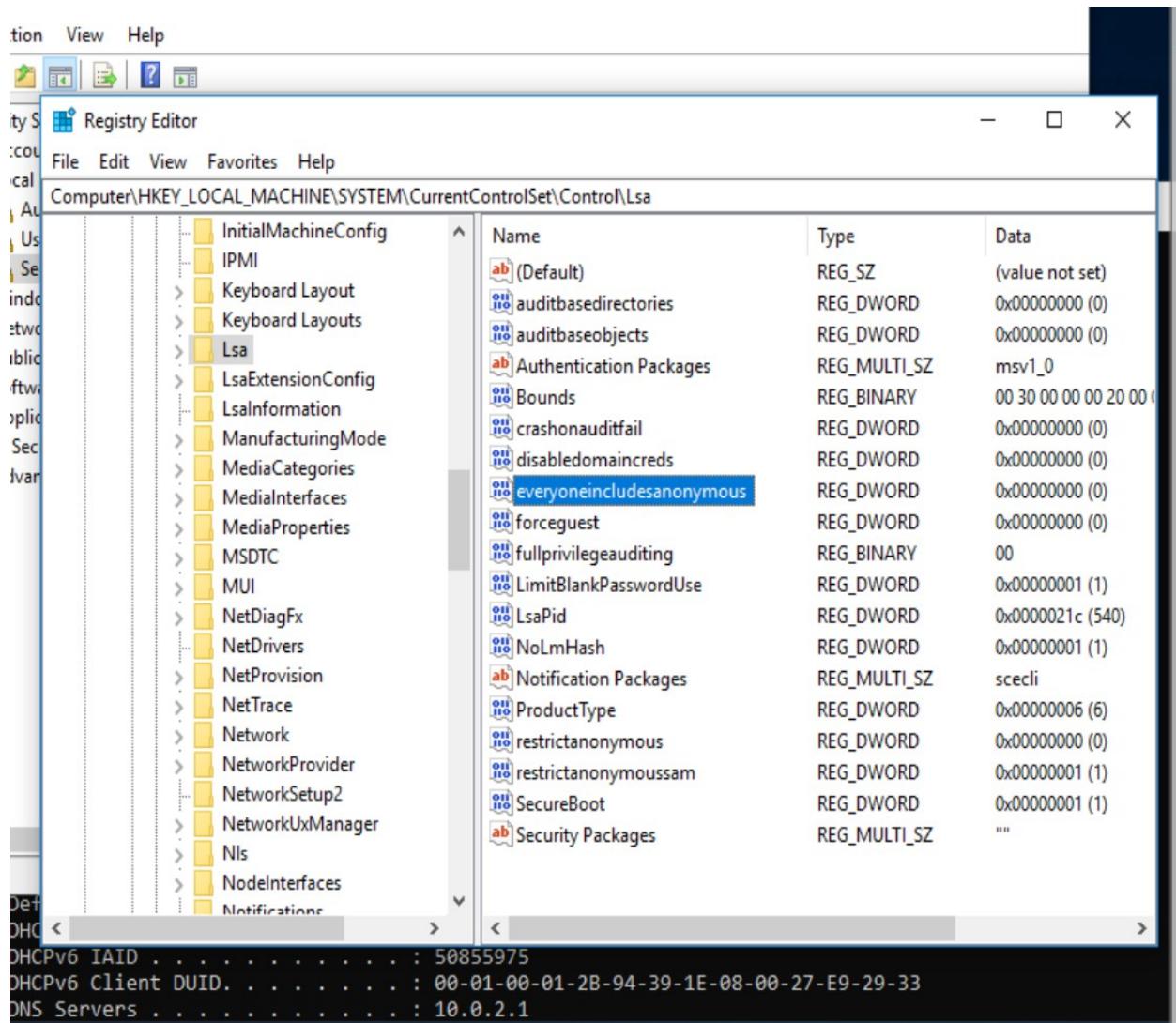
There are no policies configured in ubuntu

```
root@ubu-ustudent:~$ sudo apt install nmap
\#
\#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.
# 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.
# 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

ustudent@ubu-ustudent:~$
```

File written to remote share, but unable to execute payload either due to unknown actual pa

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 possiblitiy 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.

```
ustudent@ubu-ustudent:~$ netstat -ntlp | grep LISTEN
(Es konnten nicht alle Prozesse identifiziert werden; Informationen über
nicht-eigene Prozesse werden nicht angezeigt; Root kann sie anzeigen.)
tcp      0      0 0.0.0.0:37          0.0.0.0:*          LISTEN      -
tcp      0      0 0.0.0.0:139         0.0.0.0:*          LISTEN      -
tcp      0      0 0.0.0.0:13          0.0.0.0:*          LISTEN      -
tcp      0      0 0.0.0.0:17          0.0.0.0:*          LISTEN      -
tcp      0      0 0.0.0.0:21          0.0.0.0:*          LISTEN      -
tcp      0      0 127.0.0.53:53        0.0.0.0:*          LISTEN      -
tcp      0      0 0.0.0.0:22          0.0.0.0:*          LISTEN      -
tcp      0      0 0.0.0.0:23          0.0.0.0:*          LISTEN      -
tcp      0      0 127.0.0.1:631         0.0.0.0:*          LISTEN      -
tcp      0      0 0.0.0.0:445         0.0.0.0:*          LISTEN      -
tcp6     0      0 ::1:139            ::*:              LISTEN      -
tcp6     0      0 ::1:80             ::*:              LISTEN      -
tcp6     0      0 ::1:22             ::*:              LISTEN      -
tcp6     0      0 ::1:631            ::*:              LISTEN      -
tcp6     0      0 ::1:445            ::*:              LISTEN      -
ustudent@ubu-ustudent:~$ netstat -ntlp | grep LISTEN | wc
```

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	Local Address	Remote Address	Status
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 address.

```
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.

```
ustudent@ubu-ustudent:~/Documents$ ll
insgesamt 12
drwxr-xr-x  3 uststudent uststudent 4096 Sep 26  2020 .
drwxr-xr-x 19 uststudent uststudent 4096 Mär  5 05:24 ../
drwxrwxrwx  2 uststudent uststudent 4096 Mär  3 09:56 data/
ustudent@ubu-ustudent:~/Documents$
```

On ubuntu there are guest accounts

```
ustudent@ubu-ustudent:~$ sudo cat /etc/group | grep guest
guest:x:1001:
ustudent@ubu-ustudent:~$

ustudent@ubu-ustudent:/home$ ls
guest  user3  user4  user5  uststudent
ustudent@ubu-ustudent:/home$
```

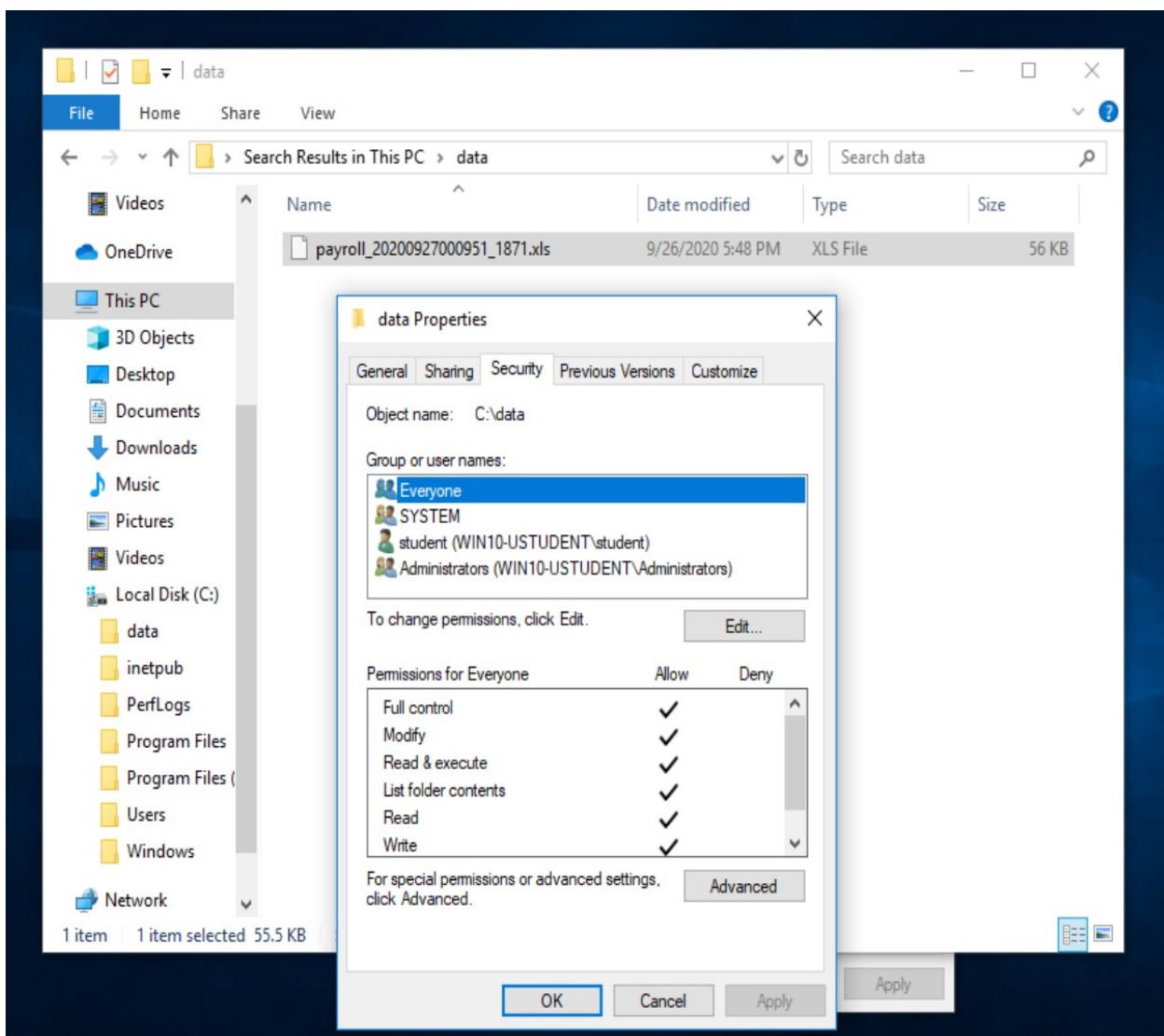
On ubuntu everyone is allowed to use sudo.

```
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:/usr/games:/usr/local/games"
# 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:
#includeincludedir /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

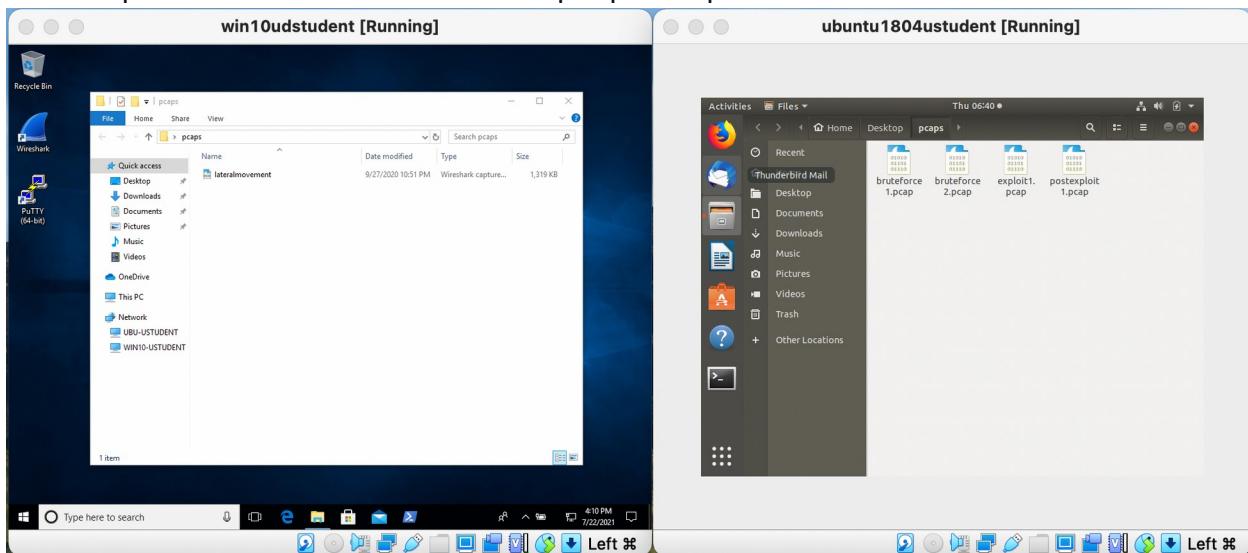
StaticSpeed has provided access to a monitoring device that has recorded some traffic marked as malicious. Please investigate and assess this further using Wireshark or tcpdump and the provided capture files (pcaps). It is also required of you to verify that appropriate logging is in place at your machines.

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.

No.	Time	Source	Destination	Protocol	Length	Info
3148	75.336938	10.0.2.7	10.0.2.5	TCP	66	32920 → 23 [ACK] Seq=37 Ack=78 Win=64256 Len=0 Tsvl=1857764048 Tscr=3538440427
3226	75.437742	10.0.2.7	10.0.2.5	TCP	66	32920 → 23 [ACK] Seq=42 Ack=83 Win=64256 Len=0 Tsvl=1857764149 Tscr=3538440508
3269	75.478596	10.0.2.7	10.0.2.5	TCP	66	32920 → 23 [ACK] Seq=42 Ack=93 Win=64256 Len=0 Tsvl=1857764189 Tscr=3538440528
3467	75.640468	10.0.2.7	10.0.2.5	TCP	66	32920 → 23 [ACK] Seq=48 Ack=95 Win=64256 Len=0 Tsvl=1857764352 Tscr=3538440715
3570	75.753561	10.0.2.7	10.0.2.5	TCP	66	32920 → 23 [ACK] Seq=49 Ack=96 Win=64256 Len=0 Tsvl=1857764465 Tscr=3538440844
3566	75.752726	10.0.2.7	10.0.2.5	TCP	66	32920 → 23 [FIN, ACK] Seq=48 Ack=95 Win=64256 Len=0 Tsvl=1857764464 Tscr=3538440715
2615	74.735629	10.0.2.7	10.0.2.5	TCP	74	32920 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1468 SACK_PERM=1 Tsvl=1857763446 Tscr=0 WS=128
Ubuntu-Software	75.0148	10.0.2.5	10.0.2.7	TELNET	78	Telnet Data ...
Ubuntu-Software	75.0166	10.0.2.7	10.0.2.5	TELNET	69	Telnet Data ...
2723	74.888451	10.0.2.5	10.0.2.7	TELNET	69	Telnet Data ...
2728	74.888530	10.0.2.7	10.0.2.5	TELNET	78	Telnet Data ...
2737	74.893453	10.0.2.5	10.0.2.7	TELNET	81	Telnet Data ...
2861	75.091404	10.0.2.7	10.0.2.5	TELNET	69	Telnet Data ...
2865	75.092111	10.0.2.5	10.0.2.7	TELNET	69	Telnet Data ...
2869	75.092938	10.0.2.7	10.0.2.5	TELNET	78	Telnet Data ...
2876	75.094210	10.0.2.5	10.0.2.7	TELNET	69	Telnet Data ...
2881	75.095139	10.0.2.5	10.0.2.7	TELNET	104	Telnet Data ...
2951	75.195623	10.0.2.7	10.0.2.5	TELNET	69	Telnet Data ...
3097	75.296371	10.0.2.7	10.0.2.5	TELNET	67	Telnet Data ...
3099	75.296542	10.0.2.5	10.0.2.7	TELNET	67	Telnet Data ...
3127	75.316394	10.0.2.7	10.0.2.5	TELNET	67	Telnet Data ...
3128	75.316453	10.0.2.5	10.0.2.7	TELNET	67	Telnet Data ...
3146	75.336533	10.0.2.7	10.0.2.5	TELNET	67	Telnet Data ...
3147	75.336612	10.0.2.5	10.0.2.7	TELNET	67	Telnet Data ...
3170	75.356594	10.0.2.7	10.0.2.5	TELNET	67	Telnet Data ...
3171	75.356724	10.0.2.5	10.0.2.7	TELNET	67	Telnet Data ...
3184	75.376869	10.0.2.7	10.0.2.5	TELNET	67	Telnet Data ...
3187	75.376975	10.0.2.5	10.0.2.7	TELNET	67	Telnet Data ...
3201	75.397276	10.0.2.7	10.0.2.5	TELNET	67	Telnet Data ...
3204	75.397573	10.0.2.5	10.0.2.7	TELNET	67	Telnet Data ...
3215	75.417381	10.0.2.7	10.0.2.5	TELNET	66	Telnet Data ...
3217	75.417941	10.0.2.5	10.0.2.7	TELNET	66	Telnet Data ...

Frame 2881: 104 bytes on wire (832 bits), 104 bytes captured (832 bits)  
Ethernet II, Src: PcsCompu\_1a:99:62 (08:00:27:1a:99:62), Dst: PcsCompu\_4f:2f:6a (08:00:27:4f:2f:6a)  
Internet Protocol Version 4, Src: 10.0.2.5, Dst: 10.0.2.7  
Transmission Control Protocol, Src Port: 23, Dst Port: 32920, Seq: 37, Ack: 31, Len: 38

▼ Telnet  
  Data: Ubuntu 18.04 LTS\r\n  Data: ubu-ustudent login:

..... .#..!".."..... .#..!'.....!....!....Ubuntu 18.04 LTS  
ubu-ustudent login: uussttuuddeenntt

.\nPassword: 12345678

.\n..... .#..!".."..... .#..!'.....!....!....Ubuntu 18.04 LTS  
ubu-ustudent login: uussttuuddeenntt

.\nPassword: password1

```
.... .#..!".."..... .#..'.....!.....!...Ubuntu 18.04 LTS
ubu-ustudent login: ...uussttuuddeenntt
.
Password: 1234
.
Last login: Sun Sep 27 23:06:49 EDT 2020 from 10.0.2.7 on pts/11
```

Bruteforce attacks can be prevented by using timeouts that slow down the attack. Furthermore, 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.

ip.addr == 10.0.2.6 and ip.addr == 10.0.2.7						
No.	Time	Source	Destination	Protocol	Length	Info
5	42.930762	10.0.2.7	10.0.2.6	SMB	136	Tree Connect AndX Request, Path: \\10.0.2.6\IPC\$
36	42.930980	10.0.2.6	10.0.2.7	SMB	116	Tree Connect AndX Response
37	42.932764	10.0.2.7	10.0.2.6	SMB Pi...	144	PeekNamedPipe Request, FID: 0x0000
38	42.932879	10.0.2.6	10.0.2.7	SMB	105	Trans Response, Error: STATUS_INSUFF_SERVER_RESOURCES
39	42.933998	10.0.2.7	10.0.2.6	TCP	74	39289 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
40	42.934200	10.0.2.6	10.0.2.7	TCP	74	135 → 39289 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0
41	42.934372	10.0.2.7	10.0.2.6	TCP	66	39289 → 135 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TS=1
42	42.934508	10.0.2.7	10.0.2.6	DCERPC	138	Bind: call_id: 0, Fragment: Single, 1 context item
43	42.934667	10.0.2.6	10.0.2.7	DCERPC	126	Bind_ack: call_id: 0, Fragment: Single, max_xmit
44	42.934830	10.0.2.7	10.0.2.6	TCP	66	39289 → 135 [ACK] Seq=73 Ack=61 Win=64256 Len=0
45	42.934830	10.0.2.7	10.0.2.6	TCP	66	39289 → 135 [FIN, ACK] Seq=73 Ack=61 Win=64256 Len=0
46	42.934936	10.0.2.6	10.0.2.7	TCP	66	135 → 39289 [ACK] Seq=61 Ack=74 Win=66560 Len=0
47	42.934936	10.0.2.6	10.0.2.7	TCP	66	135 → 39289 [FIN, ACK] Seq=61 Ack=74 Win=66560 Len=0
48	42.935098	10.0.2.7	10.0.2.6	TCP	66	39289 → 135 [ACK] Seq=74 Ack=62 Win=64256 Len=0
49	42.936943	10.0.2.7	10.0.2.6	SMB	149	Trans2 Request, SESSION_SETUP
50	42.937107	10.0.2.6	10.0.2.7	SMB	105	Trans2 Response, SESSION_SETUP, Error: STATUS_NO_SUCH_FILE_OR_DIRECTORY
51	42.937476	10.0.2.7	10.0.2.6	TCP	66	34515 → 445 [FIN, ACK] Seq=982 Ack=769 Win=64128 Len=0
52	42.937633	10.0.2.6	10.0.2.7	TCP	66	445 → 34515 [ACK] Seq=769 Ack=983 Win=65536 Len=0
53	42.937703	10.0.2.6	10.0.2.7	TCP	60	445 → 34515 [RST, ACK] Seq=769 Ack=983 Win=0 Len=0
54	42.939306	10.0.2.7	10.0.2.6	TCP	74	46311 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
55	42.939412	10.0.2.6	10.0.2.7	TCP	74	445 → 46311 [SYN, ACK] Seq=0 Ack=1 Win=6102 Len=0

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

ip.addr == 10.0.2.6 and ip.addr == 10.0.2.4						
No.	Time	Source	Destination	Protocol	Length	Info
1221	111.110195	10.0.2.4	10.0.2.6	LLMNR	160	Standard query response 0x05ed ANY win10-ustudent
1229	111.113549	10.0.2.4	10.0.2.6	LLMNR	160	Standard query response 0x6cf ANY win10-ustudent
2032	411.157355	10.0.2.4	10.0.2.6	LLMNR	160	Standard query response 0xe400 ANY win10-ustudent
2040	411.161533	10.0.2.4	10.0.2.6	LLMNR	160	Standard query response 0x56ca ANY win10-ustudent
2351	681.667224	10.0.2.6	10.0.2.4	TCP	66	49165 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
2352	681.667409	10.0.2.4	10.0.2.6	TCP	66	445 → 49165 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0
2353	681.667937	10.0.2.6	10.0.2.4	TCP	60	49165 → 445 [ACK] Seq=1 Ack=1 Win=65536 Len=0
2357	681.728690	10.0.2.6	10.0.2.4	SMB	116	Negotiate Protocol Request
2358	681.741316	10.0.2.4	10.0.2.6	SMB2	506	Negotiate Protocol Response
2364	681.810326	10.0.2.6	10.0.2.4	SMB2	224	Session Setup Request, NTLMSSP_NEGOTIATE
2365	681.819642	10.0.2.4	10.0.2.6	SMB2	390	Session Setup Response, Error: STATUS_MORE_PROCESSOR_LEVELS
2371	681.922490	10.0.2.6	10.0.2.4	SMB2	482	Session Setup Request, NTLMSSP_AUTH, User: .\Administrator
2372	681.930481	10.0.2.4	10.0.2.6	SMB2	130	Session Setup Response, Error: STATUS_LOGON_FAILURE
2378	681.989060	10.0.2.6	10.0.2.4	SMB2	160	Tree Connect Request Tree: \\10.0.2.4\IPC\$
2379	681.989361	10.0.2.4	10.0.2.6	TCP	54	445 → 49165 [RST, ACK] Seq=865 Ack=767 Win=0 Len=0
2413	711.209439	10.0.2.4	10.0.2.6	LLMNR	160	Standard query response 0x6450 ANY win10-ustudent
2421	711.212670	10.0.2.4	10.0.2.6	LLMNR	160	Standard query response 0x33d3 ANY win10-ustudent
2531	753.374783	10.0.2.6	10.0.2.4	TCP	66	49166 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
2532	753.374849	10.0.2.4	10.0.2.6	TCP	66	445 → 49166 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0
2533	753.375187	10.0.2.6	10.0.2.4	TCP	60	49166 → 445 [ACK] Seq=1 Ack=1 Win=65536 Len=0
2537	753.466561	10.0.2.4	10.0.2.4	SMB	116	Negotiate Protocol Request

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.

9037450	10.0.2.4	10.0.2.7	SMB2	102 Close Response
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

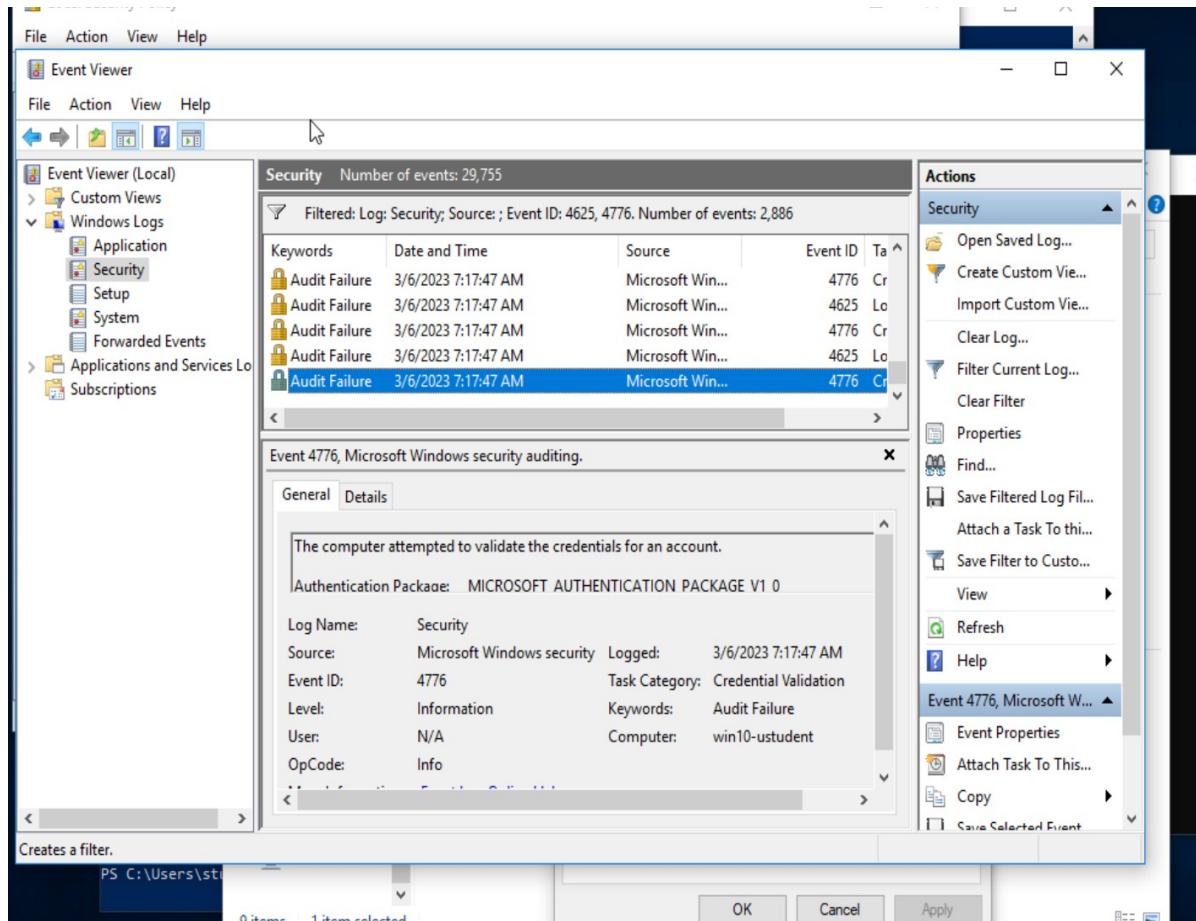
Look at logs on the StaticSpeed Windows machine.

Using the logs, determine the following:

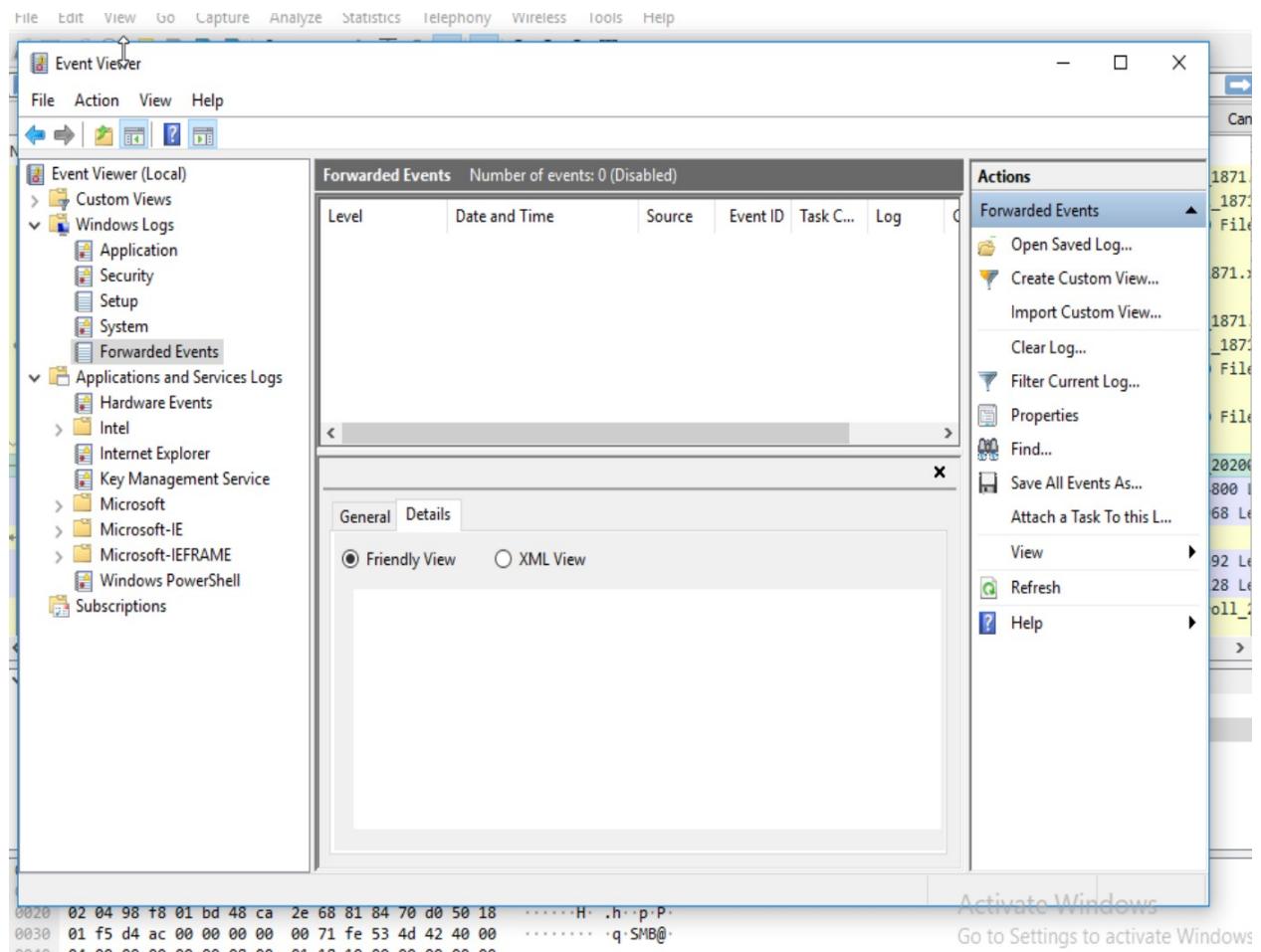
- Are there any issues with Windows Share? Please provide screenshots of your findings.
- Look at the audit logs setup at your Linux machine and find the audit.log file. What was the name of the attacker's account? Please provide screenshots.

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.

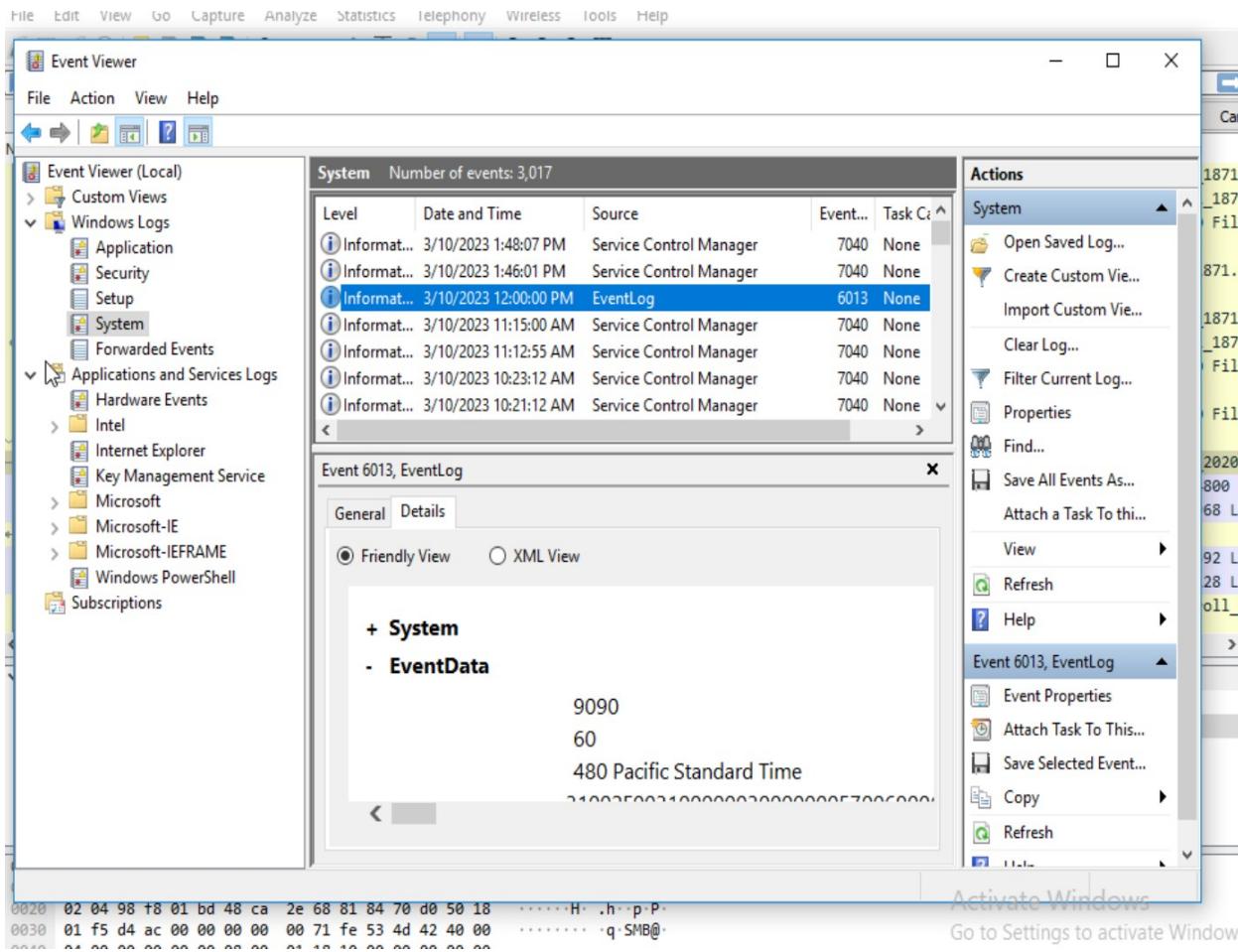
I don't see anything suspicious in the windows event viewer in security tab.



## Nothing interesting in forwarding events



## Nothing interesting in system



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

The screenshot shows the Windows Event Viewer interface. The title bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The main pane displays a table for the 'SMBClient' log source. The table has columns: Name, Type, Number of Events, and Size. The data is as follows:

Name	Type	Number of Events	Size
Audit	Operational	0	68 KB
Connectivity	Operational	9,055	4.07 MB
Diagnostic	Analytic	N/A	0 Bytes
HelperClassDiagnostic	Analytic	N/A	0 Bytes
ObjectStateDiagnostic	Debug	N/A	0 Bytes
Operational	Operational	1	68 KB
Security	Operational	0	68 KB
XPerfAnalytic	Analytic	N/A	0 Bytes

The Actions pane on the right shows options for 'SMBClient' and 'Audit'. Under 'SMBClient', 'Open Saved Log...' is selected. Under 'Audit', 'Properties' is selected. The status bar at the bottom right shows 'Activate Windows' and 'Go to Settings to activate Windows'.

The aureport shows that there are a lot of login attempts with unknown/invalid user names. That could be a possible brute force attack. We will check this later. The only ones that were able 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.

```
ustudent@ubu-ustudent:~$ sudo aureport -l --failed --summary -i

Failed Login Summary Report
=====
total  auid
=====
499  (invalid user)
253  (unknown user)
42  root
19  UNKNOWN
4  guest
1  ustudent
ustudent@ubu-ustudent:~$ sudo aureport -l --success --summary -i

Success Login Summary Report
=====
total  auid
=====
28  ustudent
1  guest
ustudent@ubu-ustudent:~$
```

```
ustudent@ubu-ustudent:/var/log/audit$ cat audit.log | grep 10.0.2.7 | grep guest
type=USER_AUTH msg=audit(1601245380.099:20): pid=5863 uid=0 auid=4294967295 ses=4294967295 msg='op=PAM:authentication acct="guest" exe="/usr/sbin/sshd" hostname=10.0.2.7 addr=10.0.2.7 terminal=ssh res=failed'
type=USER_LOGIN msg=audit(1601245380.103:203): pid=5863 uid=0 auid=4294967295 ses=4294967295 msg='op=login acct="guest" exe="/usr/sbin/sshd" hostname=? addr=10.0.2.7 terminal=ssh res=failed'
type=USER_AUTH msg=audit(1601245384.995:204): pid=5863 uid=0 auid=4294967295 ses=4294967295 msg='op=PAM:authentication acct="guest" exe="/usr/sbin/sshd" hostname=10.0.2.7 addr=10.0.2.7 terminal=ssh res=success'
type=USER_ACCT msg=audit(1601245384.995:205): pid=5863 uid=0 auid=4294967295 ses=4294967295 msg='op=PAM:accounting acct="guest" exe="/usr/sbin/sshd" hostname=10.0.2.7 addr=10.0.2.7 terminal=ssh res=success'
type=CRED_ACQ msg=audit(1601245385.003:206): pid=5863 uid=0 auid=4294967295 ses=4294967295 msg='op=PAM:setcred acct="guest" exe="/usr/sbin/sshd" hostname=10.0.2.7 addr=10.0.2.7 terminal=ssh res=success'
type=USER_START msg=audit(1601245386.763:212): pid=5863 uid=0 auid=1001 ses=10 msg='op=PAM:session_open acct="guest" exe="/usr/sbin/sshd" hostname=10.0.2.7 addr=10.0.2.7 terminal=ssh res=success'
type=CRED_ACQ msg=audit(1601245386.779:213): pid=5970 uid=0 auid=1001 ses=10 msg='op=PAM:setcred acct="guest" exe="/usr/sbin/sshd" hostname=10.0.2.7 addr=10.0.2.7 terminal=ssh res=success'
type=USER_END msg=audit(1601246019.868:256): pid=5863 uid=0 auid=1001 ses=10 msg='op=PAM:session_close acct="guest" exe="/usr/sbin/sshd" hostname=10.0.2.7 addr=10.0.2.7 terminal=ssh res=success'
type=CRED_DISP msg=audit(1601246019.868:257): pid=5863 uid=0 auid=1001 ses=10 msg='op=PAM:setcred acct="guest" exe="/usr/sbin/sshd" hostname=10.0.2.7 addr=10.0.2.7 terminal=ssh res=success'
```

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.

```
student@ubu-ustudent:/var/log/audit$ sudo aureport -au -i --failed

Authentication Report
=====
# date time acct host term exe success event
=====
.. 27.09.2020 15:52:37 root 10.0.2.7 ssh /usr/sbin/sshd no 61
.. 27.09.2020 15:53:15 attacker 10.0.2.7 ssh /usr/sbin/sshd no 65
.. 27.09.2020 15:53:22 attacker 10.0.2.7 ssh /usr/sbin/sshd no 67
.. 27.09.2020 15:53:33 attacker 10.0.2.7 ssh /usr/sbin/sshd no 69
.. 27.09.2020 15:54:43 ? 10.0.2.7 /dev/pts/1 /bin/login no 73
.. 27.09.2020 15:54:51 ? 10.0.2.7 /dev/pts/1 /bin/login no 75
.. 27.09.2020 15:54:57 ? 10.0.2.7 /dev/pts/1 /bin/login no 77
.. 27.09.2020 15:55:06 ? 10.0.2.7 /dev/pts/1 /bin/login no 79
.. 27.09.2020 16:19:04 guest ? /dev/pts/1 /usr/bin/sudo no 121
.. 27.09.2020 18:23:00 guest 10.0.2.7 ssh /usr/sbin/sshd no 202
.. 27.09.2020 18:28:52 guest ? /dev/pts/1 /usr/bin/sudo no 243
.. 27.09.2020 18:28:52 guest ? /dev/pts/1 /usr/bin/sudo no 244
.. 28.09.2020 13:34:45 OpenVASVT 10.0.2.15 ssh /usr/sbin/sshd no 193
.. 28.09.2020 13:36:55 cisco 10.0.2.15 ssh /usr/sbin/sshd no 208
.. 28.09.2020 13:36:56 root 10.0.2.15 ssh /usr/sbin/sshd no 214
.. 28.09.2020 13:36:57 xfknicpt 10.0.2.15 ssh /usr/sbin/sshd no 218
.. 28.09.2020 13:36:58 wbaleftd 10.0.2.15 ssh /usr/sbin/sshd no 222
.. 28.09.2020 13:36:59 oracle 10.0.2.15 ssh /usr/sbin/sshd no 224
.. 28.09.2020 13:37:00 yrtsiksry 10.0.2.15 ssh /usr/sbin/sshd no 228
.. 28.09.2020 13:37:02 dpylwlwd 10.0.2.15 ssh /usr/sbin/sshd no 232
.. 28.09.2020 13:37:02 root 10.0.2.15 ssh /usr/sbin/sshd no 234
.. 28.09.2020 13:37:03 root 10.0.2.15 ssh /usr/sbin/sshd no 240
.. 28.09.2020 13:37:04 super 10.0.2.15 ssh /usr/sbin/sshd no 244
.. 28.09.2020 13:37:04 panopta.admin 10.0.2.15 ssh /usr/sbin/sshd no 246
.. 28.09.2020 13:37:05 ro 10.0.2.15 ssh /usr/sbin/sshd no 248
.. 28.09.2020 13:37:05 mazu 10.0.2.15 ssh /usr/sbin/sshd no 252
.. 28.09.2020 13:37:07 rwa 10.0.2.15 ssh /usr/sbin/sshd no 256
.. 28.09.2020 13:37:07 root 10.0.2.15 ssh /usr/sbin/sshd no 258
.. 28.09.2020 13:37:07 dhcp 10.0.2.15 ssh /usr/sbin/sshd no 260
.. 28.09.2020 13:37:09 root 10.0.2.15 ssh /usr/sbin/sshd no 264
.. 28.09.2020 13:37:11 support 10.0.2.15 ssh /usr/sbin/sshd no 269
.. 28.09.2020 13:37:13 nsroot 10.0.2.15 ssh /usr/sbin/sshd no 273
.. 28.09.2020 13:37:14 user 10.0.2.15 ssh /usr/sbin/sshd no 277
.. 28.09.2020 13:37:15 ? 10.0.2.15 /dev/pts/1 /bin/login no 279
.. 28.09.2020 13:37:15 debug 10.0.2.15 ssh /usr/sbin/sshd no 281
.. 28.09.2020 13:37:23 db2as 10.0.2.15 ssh /usr/sbin/sshd no 291
.. 28.09.2020 13:37:23 root 10.0.2.15 ssh /usr/sbin/sshd no 293
.. 28.09.2020 13:37:24 ? 10.0.2.15 /dev/pts/3 /bin/login no 295
.. 28.09.2020 13:37:26 root 10.0.2.15 ssh /usr/sbin/sshd no 297
.. 28.09.2020 13:37:26 ? 10.0.2.15 /dev/pts/4 /bin/login no 299
.. 28.09.2020 13:37:28 root 10.0.2.15 ssh /usr/sbin/sshd no 301
```

```

student@ubu-ustudent:/var/log/audit$ sudo aureport -au --success
authentication Report
=====
# date time acct host term exe success event
=====
.. 27.09.2020 16:05:26 ustUDENT ubu-ustUDENT /dev/tty1 /usr/lib/gdm3/gdm-session-worker yes 87
.. 27.09.2020 16:16:58 ustUDENT ? /dev/pts/0 /usr/bin/sudo yes 98
.. 27.09.2020 16:17:25 ustUDENT ? /dev/pts/1 /usr/bin/sudo yes 109
.. 27.09.2020 16:19:10 guest ? /dev/pts/1 /usr/bin/sudo yes 122
.. 27.09.2020 18:21:55 ustUDENT ubu-ustUDENT /dev/tty1 /usr/lib/gdm3/gdm-session-worker yes 197
.. 27.09.2020 18:23:04 guest 10.0.2.7 ssh /usr/sbin/sshd yes 204
.. 27.09.2020 18:25:52 ustUDENT ? /dev/pts/0 /usr/bin/sudo yes 217
.. 27.09.2020 18:26:30 root ? /dev/pts/0 /bin/su yes 227
.. 27.09.2020 18:33:39 ustUDENT ? /dev/pts/1 /usr/bin/sudo yes 251
.. 27.09.2020 18:47:28 ustUDENT ubu-ustUDENT /dev/tty1 /usr/lib/gdm3/gdm-session-worker yes 267
.. 27.09.2020 20:00:22 ustUDENT ubu-ustUDENT /dev/tty1 /usr/lib/gdm3/gdm-session-worker yes 324
.. 27.09.2020 21:26:36 ustUDENT ubu-ustUDENT /dev/tty1 /usr/lib/gdm3/gdm-session-worker yes 385
.. 27.09.2020 21:26:46 ustUDENT ? /dev/pts/1 /usr/bin/sudo yes 388
.. 27.09.2020 21:29:46 ustUDENT ubu-ustUDENT /dev/tty1 /usr/lib/gdm3/gdm-session-worker yes 79
.. 27.09.2020 21:30:47 ustUDENT ? /dev/pts/0 /usr/bin/sudo yes 112
.. 27.09.2020 21:32:47 ustUDENT ? /usr/lib/policykit-1/polkit-agent-helper-1 yes 134
.. 27.09.2020 21:35:56 root ? /usr/bin/chfn yes 146
.. 27.09.2020 21:36:32 root ? /usr/bin/chfn yes 156
.. 27.09.2020 21:37:11 root ? /usr/bin/chfn yes 166
.. 27.09.2020 22:06:05 ustUDENT ubu-ustUDENT /dev/tty1 /usr/lib/gdm3/gdm-session-worker yes 188
.. 27.09.2020 22:08:32 ustUDENT ? /dev/pts/0 /usr/bin/sudo yes 193
.. 27.09.2020 23:03:19 ustUDENT ubu-ustUDENT /dev/tty1 /usr/lib/gdm3/gdm-session-worker yes 266
.. 27.09.2020 23:05:07 ustUDENT ? /dev/pts/0 /usr/bin/sudo yes 271
.. 27.09.2020 23:06:49 ustUDENT 10.0.2.7 /dev/pts/11 /bin/login yes 280
.. 27.09.2020 23:07:17 ustUDENT 10.0.2.7 /dev/pts/10 /bin/login yes 286
.. 28.09.2020 11:55:27 ustUDENT ubu-ustUDENT /dev/tty1 /usr/lib/gdm3/gdm-session-worker yes 73
.. 28.09.2020 12:21:12 ustUDENT ubu-ustUDENT /dev/tty1 /usr/lib/gdm3/gdm-session-worker yes 144
.. 28.09.2020 12:28:43 ustUDENT ubu-ustUDENT /dev/tty1 /usr/lib/gdm3/gdm-session-worker yes 151
.. 28.09.2020 12:29:38 ustUDENT ? /dev/pts/0 /usr/bin/sudo yes 154
.. 28.09.2020 12:42:07 ustUDENT ubu-ustUDENT /dev/tty1 /usr/lib/gdm3/gdm-session-worker yes 76
.. 28.09.2020 12:43:26 ustUDENT ? /dev/pts/0 /usr/bin/sudo yes 116
.. 28.09.2020 12:44:22 ustUDENT ? /usr/lib/policykit-1/polkit-agent-helper-1 yes 123
.. 28.09.2020 12:46:52 ustUDENT ? /usr/lib/policykit-1/polkit-agent-helper-1 yes 133
.. 28.09.2020 12:49:54 ustUDENT ? /usr/lib/policykit-1/polkit-agent-helper-1 yes 142
.. 28.09.2020 12:56:22 ustUDENT ? /usr/lib/policykit-1/polkit-agent-helper-1 yes 155
.. 28.09.2020 13:41:40 ustUDENT ubu-ustUDENT /dev/tty1 /usr/lib/ndm3/ndm-session-worker yes 998

```

## 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.

Ubuntu:

Ubuntu CIS 4.2.1.3 is satisfied.

```
ustudent@uba-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
```

```

Datei Bearbeiten Ansicht Suchen Terminal Hilfe
#      *.=notice;*.=warn      /dev/tty8
ustudent@uba-ustudent:/etc/rsyslog.d$ cat *
# Log kernel generated UFW log messages to file
:msg,contains,"[UFW" /var/log/ufw.log

# Uncomment the following to stop logging anything that matches the last rule.
# Doing this will stop logging kernel generated UFW log messages to the file
# normally containing kern.* messages (eg, /var/log/kern.log)
#& stop
# Default rules for rsyslog.
#
#               For more information see rsyslog.conf(5) and /etc/rsyslog.conf

#
# First some standard log files.  Log by facility.
#
auth,authpriv.*          /var/log/auth.log
*.*;auth,authpriv.none    -/var/log/syslog
#cron.*                  /var/log/cron.log
#daemon.*                -/var/log/daemon.log
kern.*                   -/var/log/kern.log
#lpr.*                   -/var/log/lpr.log
mail.*                   -/var/log/mail.log
#user.*                  -/var/log/user.log

#
# Logging for the mail system.  Split it up so that
# it is easy to write scripts to parse these files.
#
#mail.info              -/var/log/mail.info
#mail.warn              -/var/log/mail.warn
mail.err                 /var/log/mail.err

#
# Some "catch-all" log files.
#
#*=debug;\*
#      auth,authpriv.none;\*
#      news.none;mail.none    -/var/log/debug
#*=info;*.=notice;*.=warn;\*
#      auth,authpriv.none;\*
#      cron,daemon.none;\*
#      mail,news.none        -/var/log/messages

#
# Emergencies are sent to everybody logged in.
#
*.emerg                 :omusrmsg:*

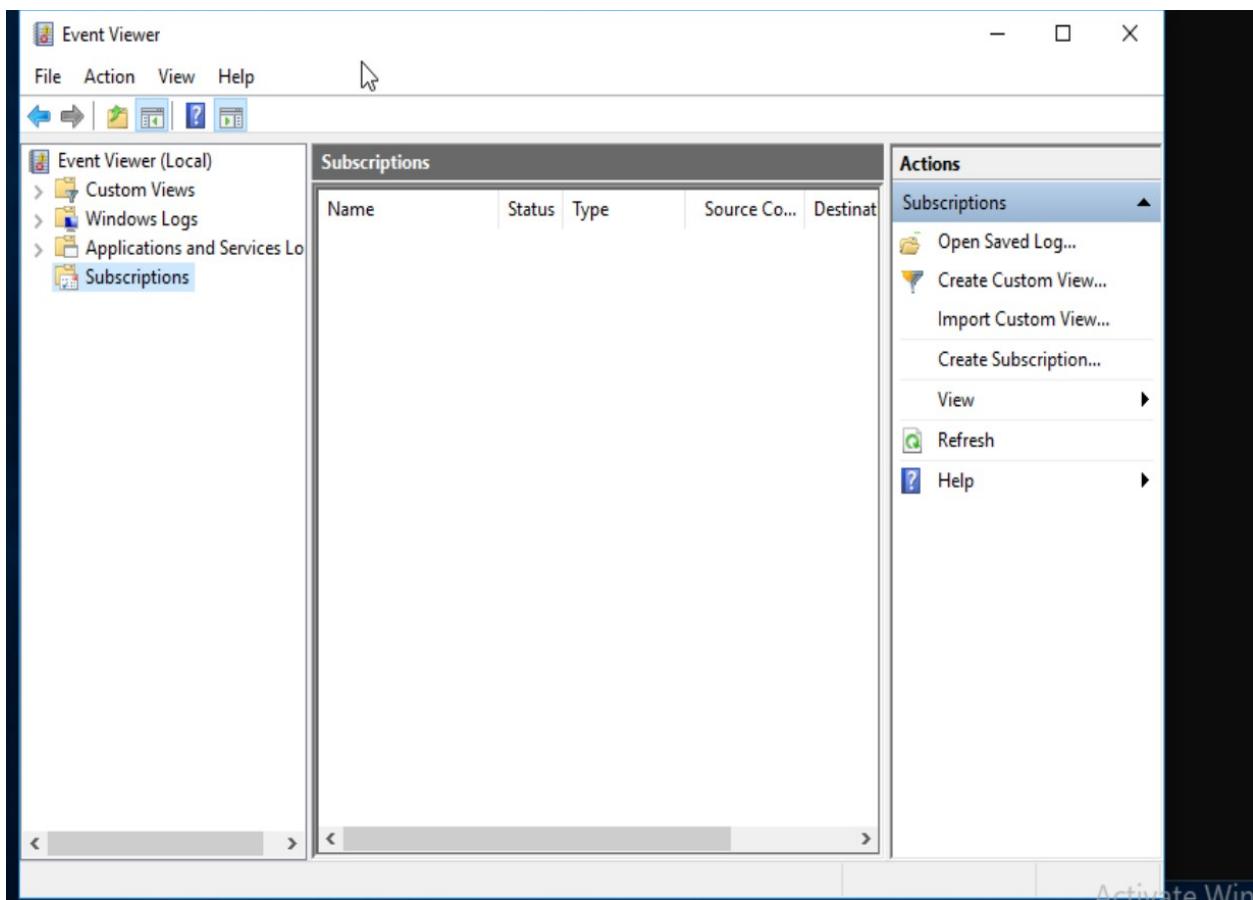
#
# I like to have messages displayed on the console, but only on a virtual
# console I usually leave idle.
#
#daemon,mail.*;\*
#      news.=crit;news.=err;news.=notice;\*
#      *.=debug;*.=info;\*
#      *.=notice;*.=warn      /dev/tty8
ustudent@uba-ustudent:/etc/rsyslog.d$ 
```

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 address where to send the logs to.

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

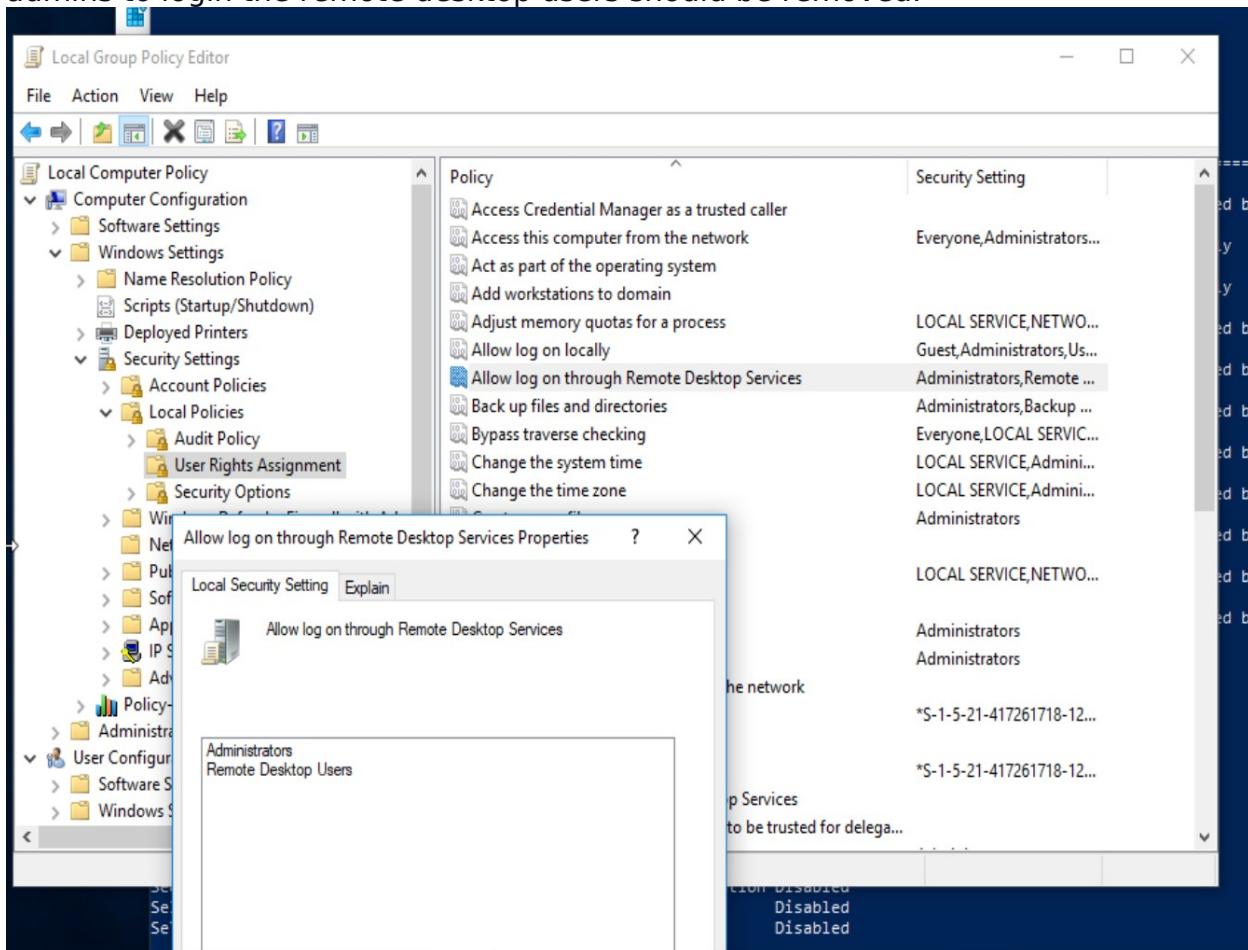
In ubuntu all users have excessive permissions as discussed earlier. That's because all are allowed to switch to the superuser(sudo).

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 local ip addresses 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.

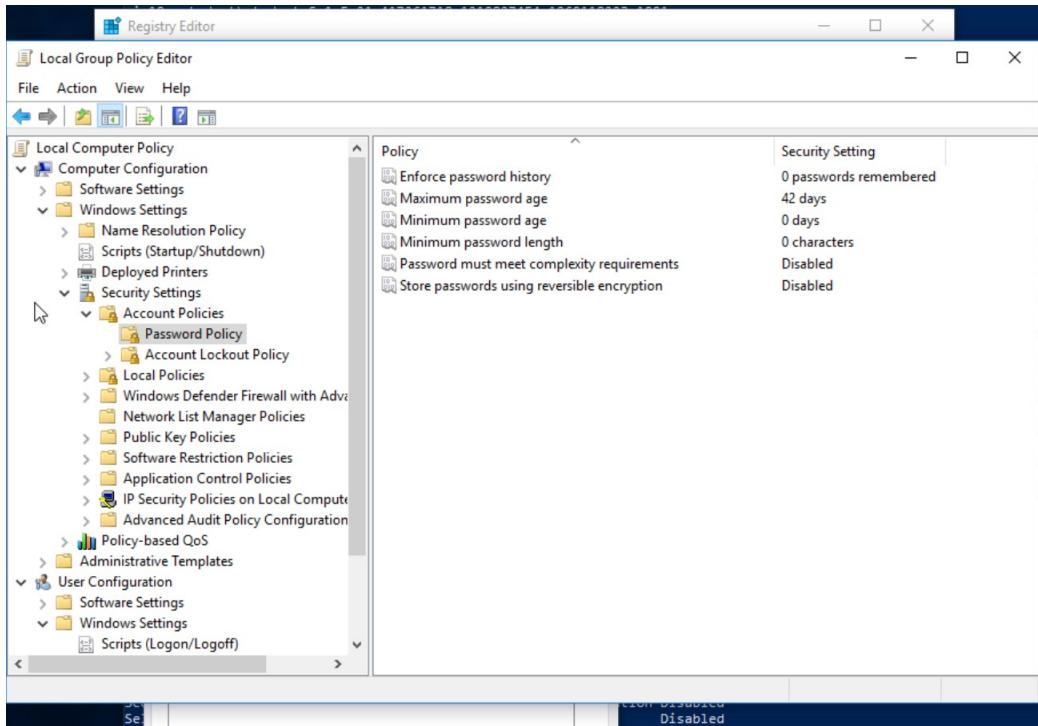
### **CIS 5.3.1 Ubuntu -Ensure password creation requirements are configured**

The CIS is not fulfilled as can be seen in the screenshot below. The password should be set to minlen = 14 and minclass = 4 or dccredit = -1 uccredit = -1 ocredit = -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.
# dccredit = 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.
# uccredit = 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: disabled (not available)
livepatch: disabled
ustudent@ubu-ustudent:/etc$ sshd -T | grep ciphers
Could not load host key: /etc/ssh/ssh_host_rsa_key
Could not load host key: /etc/ssh/ssh_host_ecdsa_key
Could not load host key: /etc/ssh/ssh_host_ed25519_key
ciphers chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com
ustudent@ubu-ustudent:/etc$
```

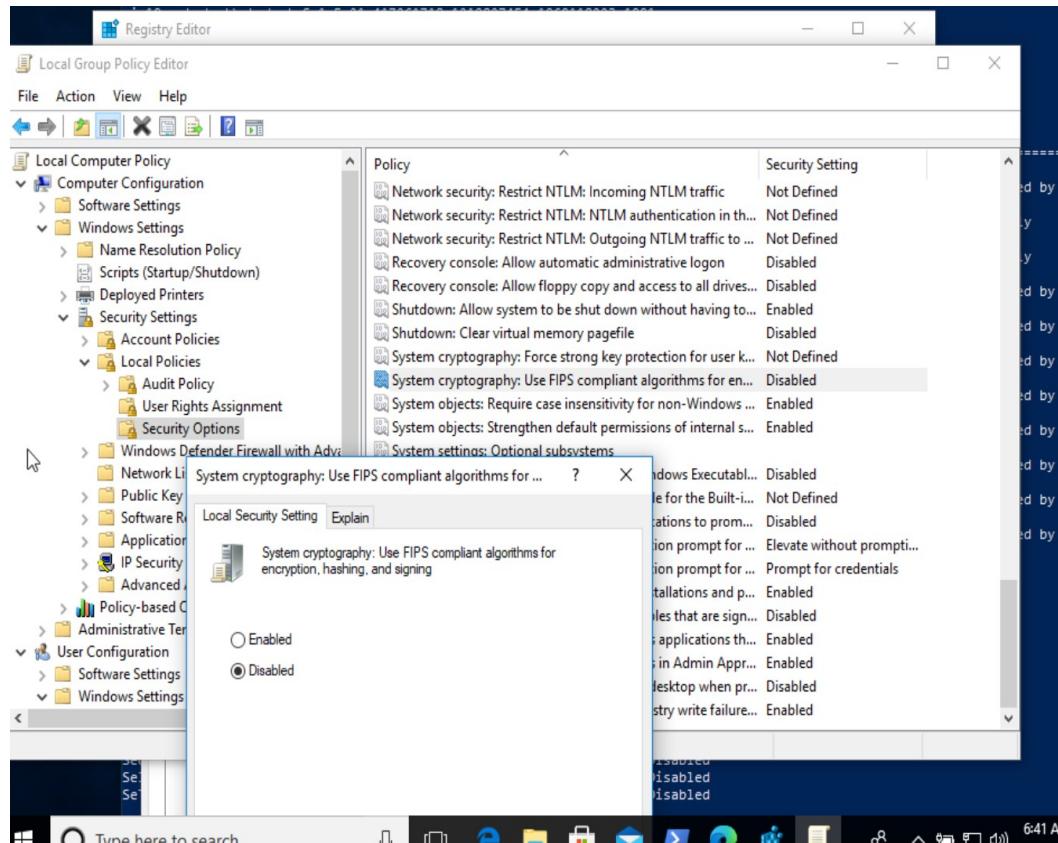
FIPS 140-2 is not installed in ubuntu.

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

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 security as the bruteforce attack didn't return any valid credentials:

```
ustudent@ubu-ustudent:~$ sudo nmap --script=ftp-brute -p 21 10.0.2.5

Starting Nmap 7.60 ( https://nmap.org ) at 2023-03-06 09:56 EST
Stats: 0:00:13 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 0.00% done
Stats: 0:00:13 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 0.00% done
Stats: 0:00:42 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 0.00% done
Stats: 0:03:21 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 0.00% done
Stats: 0:03:22 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 0.00% done
Stats: 0:05:19 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 0.00% done
Stats: 0:05:19 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 0.00% done
Stats: 0:08:31 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 0.00% done
Nmap scan report for ubu-ustudent (10.0.2.5)
Host is up (0.000028s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
|_ ftp-brute:
|| Accounts: No valid accounts found
||_ Statistics: Performed 7263 guesses in 601 seconds, average tps: 11.8

Nmap done: 1 IP address (1 host up) scanned in 601.56 seconds
ustudent@ubu-ustudent:~$
```

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

```
Nmap done. 1 IP address (1 host up) scanned in 559.70 seconds
ustudent@ubu-ustudent:~$ sudo nmap -sU -sS --script=smb-brute.nse -p 445 10.0.2.4
[sudo] Passwort für ustudent:

Starting Nmap 7.60 ( https://nmap.org ) at 2023-03-06 10:16 EST
Nmap scan report for 10.0.2.4
Host is up (0.00042s latency).

PORT      STATE    SERVICE
445/tcp    open     microsoft-ds
445/udp    closed   microsoft-ds
MAC Address: 08:00:27:E9:29:33 (Oracle VirtualBox virtual NIC)

Host script results:
| smb-brute:
|_ No accounts found

Nmap done: 1 IP address (1 host up) scanned in 75.74 seconds
ustudent@ubu-ustudent:~$
```

## 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

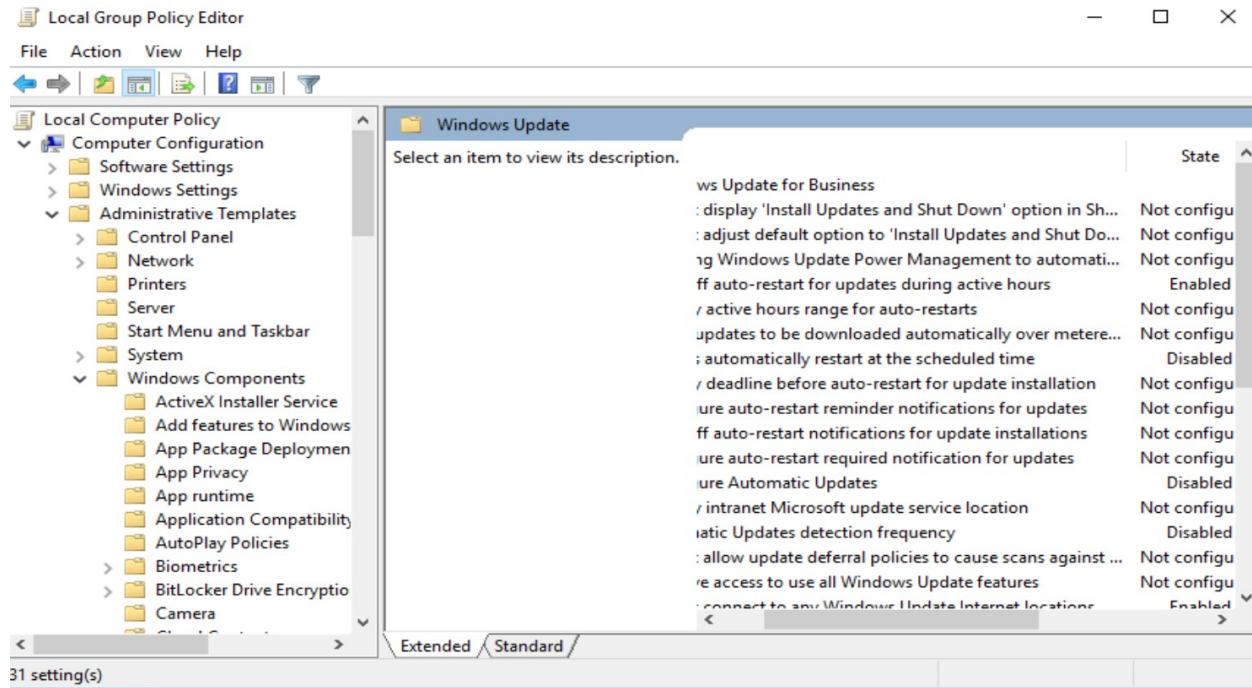
Host script results:
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED

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

Registry Editor			Reference
File	Edit	View	<a href="#">Favorites</a>
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager			<b>Medium - Enable</b>

**Issue**  
At a high-level, the SEH

**Table 1: Registry Editor showing Session Manager keys**

Name	Type	Data
(Default)	REG_SZ	(value not set)
AutoChkSkipSys...	REG_DWORD	0x00000000 (0)
AutoChkTimeout	REG_DWORD	0x00000008 (8)
BootExecute	REG_MULTI_SZ	autocheck autochk *
BootShell	REG_EXPAND_SZ	%SystemRoot%\system32\bootim.exe
CriticalSectionTi...	REG_DWORD	0x00278d00 (2592000)
ExcludeFromKn...	REG_MULTI_SZ	
GlobalFlag	REG_DWORD	0x00000000 (0)
HeapDeCommit...	REG_DWORD	0x00000000 (0)
HeapDeCommit...	REG_DWORD	0x00000000 (0)
HeapSegmentC...	REG_DWORD	0x00000000 (0)
HeapSegmentR...	REG_DWORD	0x00000000 (0)
InitConsoleFlags	REG_DWORD	0x00000000 (0)
NumberOfInitial...	REG_DWORD	0x00000002 (2)
ObjectDirectories	REG_MULTI_SZ	\Windows \RPC Control
ProcessorControl	REG_DWORD	0x00000002 (2)
ProtectionMode	REG_DWORD	0x00000001 (1)
ResourceTimeo...	REG_DWORD	0x0009e340 (648000)
RunLevelExecute	REG_MULTI_SZ	WinInit ServiceControlManager
RunLevelValidate	REG_MULTI_SZ	ServiceControlManager
SETUPEXECUTE	REG_MULTI_SZ	

## **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

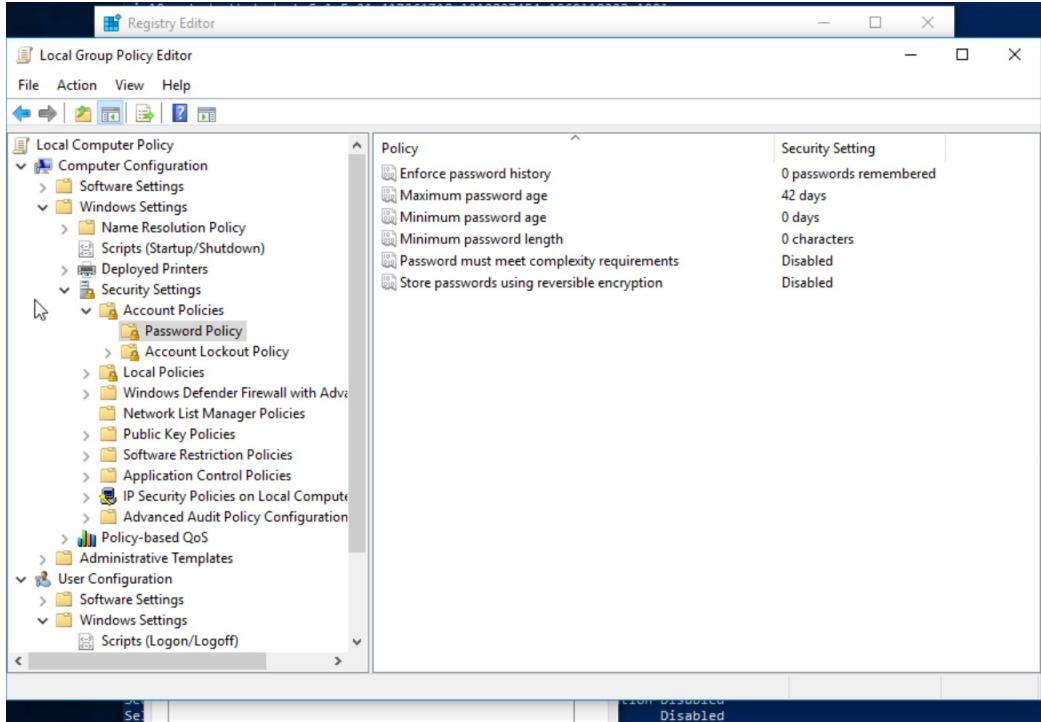
## **Reference**

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 brute-force 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 (0.0003s 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-down:  
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)  
|_fc868-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:&#xA0;<RE>\x20d\x20l\x20t\x20e\x20d\x20m\x20p\x20t\x20c,\x20d\x20u\x20y\x20u\x20n\x20d\x20e\x20l\x20o\x20
SF:stock\x20lt\x20with\x20such\x20furniture\x20as\x20you\x20choose).\x20\x
SF:20A\x20fool\x20takes\x20n\x20all\x20th\x20umber\x20of\x20every\x20sort
SF:\x20he\x20comes\x20across,\x20so\x20that\x20the\x20knowledge\whitch\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\x20skillful\x20workman\x20is\x20ver
SF:y\x20careful\x20indeed\x20as\x20to\x20what\x20he\x20takes\x20into\x20hi
SF:s\nbrain-attic.\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\x20thinx\x20that\x20hat\x20little\x20room\x20has\x20elastic\x
SF:x20walls\x20and\x20can\x20distend\x20to\x20any\x20extent.\x20\x20Depend\
SF:x20upon\x20it\x20there\x20comes\x20a\x20time\x20when\x20for\x20every\na
SF:dition\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.

```
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) Gruppen=0(root)
    References:
      http://osvdb.org/73573
      http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
      https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_back
rb
|_sslv2-drown:
```

## 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

23/tcp open telnet

### **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.

```
87/tcp open  time      (32 bits)
80/tcp open  http      Apache httpd 2.4.29 ((Ubuntu))
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGR
45/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGR
```

### **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 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.