Task 2

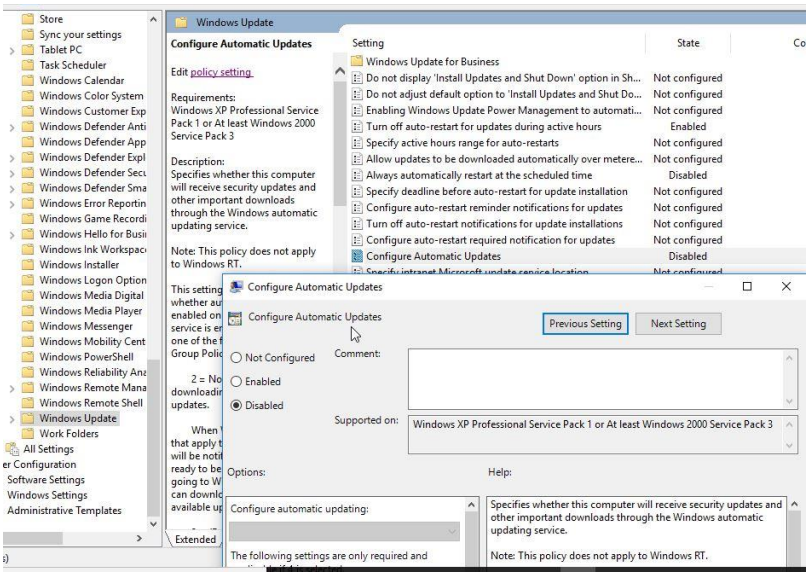
Let's get started on our assessment. We need to find out if software updates and third-party packages settings are correct. Verify in both of your hosts the following checks.
Are software updates for the systems and third parties configured correctly in these systems?
What is your assessment of StaticSpeeds 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)

Task 2

Windows CIS 18.9.102.2

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

- windows 10 Enterprise system is found to be non-compliant with the CIS benchmark for automatic updates, there are several recommended mitigations that you can consider implementing. These include:
    - Update the system: One of the most common reasons for non-compliance is outdated software. You can mitigate this by ensuring that your system is up to date with the latest security patches and updates. You can do this by running the Windows Update utility or using a third-party patch management tool.
    - Use a third-party patch management tool: If you find that the built-in Windows Update utility is not sufficient for your needs, you can consider using a third-party patch management tool that provides additional features and functionality.
    - Configure Group Policy: In addition to the "Configure Automatic Updates" setting, there are several other Windows Update-related Group Policy settings that you can configure to ensure compliance.



Ubuntu CIS 1.2.1

Ensure package manager repositories are configured correctly.

- System updates are set up to take place.
- For System & Third-Party Software Auto updates: Auto updates NOT set

```
// Automatically upgrade packages from these (origin:archive) pairs
//
// Note that in Ubuntu security updates may pull in new dependencies
// from non-security sources (e.g. chromium). By allowing the release
// pocket these get automatically pulled in.
Unattended-Upgrade::Allowed-Origins {
        "${distro_id}:${distro_codename}";
        "${distro_id}:${distro_codename}-security";
        // Extended Security Maintenance; doesn't necessarily exist for
        // every release and this system may not have it installed, but if
        // available, the policy for updates is such that unattended-upgrades
        // should also install from here by default.
        "${distro_id}ESM:${distro_codename}";
//      "${distro_id}:${distro_codename}-updates";
//      "${distro_id}:${distro_codename}-proposed";
//      "${distro_id}:${distro_codename}-backports";
};

// List of packages to not update (regexp are supported)
Unattended-Upgrade::Package-Blacklist {
//      "vim";
//      "libc6";
//      "libc6-dev";
                                [ Read 83 lines ]
```

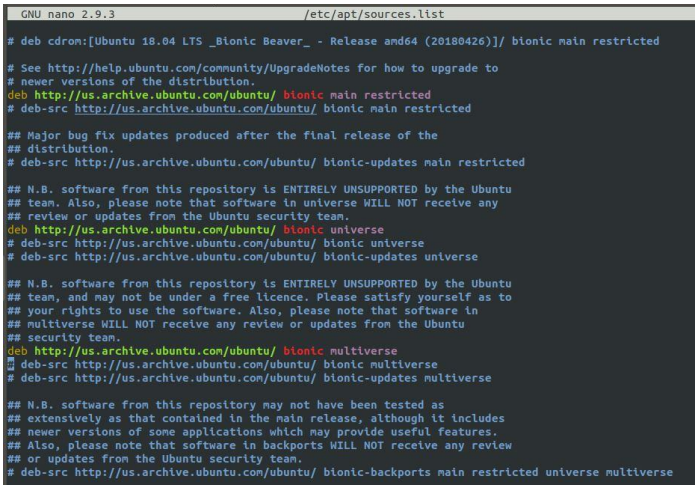
```
ustudent@ubu-ustudent:~$ apt-cache policy
Package files:
 100 /var/lib/dpkg/status
     release a=now
 500 http://us.archive.ubuntu.com/ubuntu bionic/multiverse i386 Packages
     release v=18.04,o=Ubuntu,a=bionic,n=bionic,l=Ubuntu,c=multiverse,b=i386
     origin us.archive.ubuntu.com
 500 http://us.archive.ubuntu.com/ubuntu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

```
 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
Pinned packages:
N: Ignoring file 'newfile.list.save.1' in directory '/etc/apt/sources.list.d/'
as it has an invalid filename extension
ustudent@ubu-ustudent:~$
```

```
ustudent@ubu-ustudent:~$ cat /etc/apt/sources.list
# deb cdrom:[Ubuntu 18.04 LTS _Bionic Beaver_ - Release amd64 (20180426)]/ bionic main restricted

# See http://help.ubuntu.com/community/UpgradeNotes for how to upgrade to
# newer versions of the distribution.
deb http://us.archive.ubuntu.com/ubuntu/ bionic main restricted
# deb-src http://us.archive.ubuntu.com/ubuntu/ bionic main restricted

## Major bug fix updates produced after the final release of the
## distribution.
# deb-src http://us.archive.ubuntu.com/ubuntu/ bionic-updates main restricted

## N.B. software from this repository is ENTIRELY UNSUPPORTED by the Ubuntu
## team. Also, please note that software in universe WILL NOT receive any
## review or updates from the Ubuntu security team.
deb http://us.archive.ubuntu.com/ubuntu/ bionic universe
# deb-src http://us.archive.ubuntu.com/ubuntu/ bionic universe
# deb-src http://us.archive.ubuntu.com/ubuntu/ bionic-updates universe

## N.B. software from this repository is ENTIRELY UNSUPPORTED by the Ubuntu
## team, and may not be under a free licence. Please satisfy yourself as to
## your rights to use the software. Also, please note that software in
## multiverse WILL NOT receive any review or updates from the Ubuntu
## security team.
deb http://us.archive.ubuntu.com/ubuntu/ bionic multiverse
# deb-src http://us.archive.ubuntu.com/ubuntu/ bionic multiverse
# deb-src http://us.archive.ubuntu.com/ubuntu/ bionic-updates multiverse

## N.B. software from this repository may not have been tested as
## extensively as that contained in the main release, although it includes
## newer versions of some applications which may provide useful features.
## Also, please note that software in backports WILL NOT receive any review
## or updates from the Ubuntu security team.
# deb-src http://us.archive.ubuntu.com/ubuntu/ bionic-backports main restricted universe multiverse

## Uncomment the following two lines to add software from Canonical's
## 'partner' repository.
## This software is not part of Ubuntu, but is offered by Canonical and the
```

```
ustudent@ubu-ustudent:~$ apt-cache policy
Package files:
 100 /var/lib/dpkg/status
     release a=now
 500 http://us.archive.ubuntu.com/ubuntu bionic/multiverse i386 Packages
     release v=18.04,o=Ubuntu,a=bionic,n=bionic,l=Ubuntu,c=multiverse,b=i386
     origin us.archive.ubuntu.com
 500 http://us.archive.ubuntu.com/ubuntu bionic/multiverse amd64 Packages
     release v=18.04,o=Ubuntu,a=bionic,n=bionic,l=Ubuntu,c=multiverse,b=amd64
     origin us.archive.ubuntu.com
 500 http://us.archive.ubuntu.com/ubuntu bionic/universe i386 Packages
     release v=18.04,o=Ubuntu,a=bionic,n=bionic,l=Ubuntu,c=universe,b=i386
     origin us.archive.ubuntu.com
 500 http://us.archive.ubuntu.com/ubuntu bionic/universe amd64 Packages
     release v=18.04,o=Ubuntu,a=bionic,n=bionic,l=Ubuntu,c=universe,b=amd64
     origin us.archive.ubuntu.com
 500 http://us.archive.ubuntu.com/ubuntu bionic/restricted i386 Packages
     release v=18.04,o=Ubuntu,a=bionic,n=bionic,l=Ubuntu,c=restricted,b=i386
     origin us.archive.ubuntu.com
 500 http://us.archive.ubuntu.com/ubuntu bionic/restricted amd64 Packages
     release v=18.04,o=Ubuntu,a=bionic,n=bionic,l=Ubuntu,c=restricted,b=amd64
     origin us.archive.ubuntu.com
 500 http://us.archive.ubuntu.com/ubuntu bionic/main i386 Packages
     release v=18.04,o=Ubuntu,a=bionic,n=bionic,l=Ubuntu,c=main,b=i386
     origin us.archive.ubuntu.com
 500 http://us.archive.ubuntu.com/ubuntu bionic/main amd64 Packages
     release v=18.04,o=Ubuntu,a=bionic,n=bionic,l=Ubuntu,c=main,b=amd64
     origin us.archive.ubuntu.com
Pinned packages:
N: Ignoring file 'newfile.list.save.1' in directory '/etc/apt/sources.list.d/' as it has an invalid file
name extension
```

```
## Major bug fix updates produced after the final release of the
## distribution.
# deb-src http://us.archive.ubuntu.com/ubuntu/ bionic-updates main restricted

## N.B. software from this repository is ENTIRELY UNSUPPORTED by the Ubuntu
## team. Also, please note that software in universe WILL NOT receive any
## review or updates from the Ubuntu security team.
deb http://us.archive.ubuntu.com/ubuntu/ bionic universe
# deb-src http://us.archive.ubuntu.com/ubuntu/ bionic universe
# deb-src http://us.archive.ubuntu.com/ubuntu/ bionic-updates universe

## N.B. software from this repository is ENTIRELY UNSUPPORTED by the Ubuntu
## team, and may not be under a free licence. Please satisfy yourself as to
## your rights to use the software. Also, please note that software in
## multiverse WILL NOT receive any review or updates from the Ubuntu
## security team.
deb http://us.archive.ubuntu.com/ubuntu/ bionic multiverse
# deb-src http://us.archive.ubuntu.com/ubuntu/ bionic multiverse
# deb-src http://us.archive.ubuntu.com/ubuntu/ bionic-updates multiverse

## N.B. software from this repository may not have been tested as
## extensively as that contained in the main release, although it includes
## newer versions of some applications which may provide useful features.
## Also, please note that software in backports WILL NOT receive any review
## or updates from the Ubuntu security team.
# deb-src http://us.archive.ubuntu.com/ubuntu/ bionic-backports main restricted universe multiverse

## Uncomment the following two lines to add software from Canonical's
## 'partner' repository.
## This software is not part of Ubuntu, but is offered by Canonical and the
## respective vendors as a service to Ubuntu users.
# deb http://archive.canonical.com/ubuntu bionic partner
# deb-src http://archive.canonical.com/ubuntu bionic partner

# deb-src http://security.ubuntu.com/ubuntu bionic-security main restricted
# deb-src http://security.ubuntu.com/ubuntu bionic-security universe
# deb-src http://security.ubuntu.com/ubuntu bionic-security multiverse
```

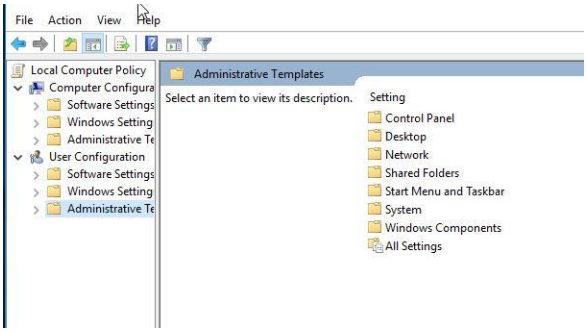


Task 3- Native Protections and Software Inventory

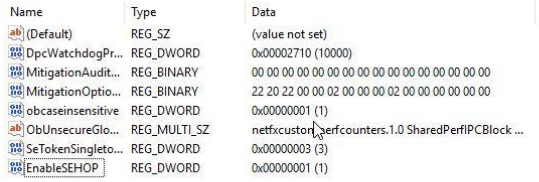
Next, verify that native protections for the operating systems are enough to protect systems from exploitation. (Hint: Think upgrades) We also need to know exactly what software is running on every machine. Also, please perform a software inventory on each computer and post your findings. The more you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

Windows CIS 18.3.4

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



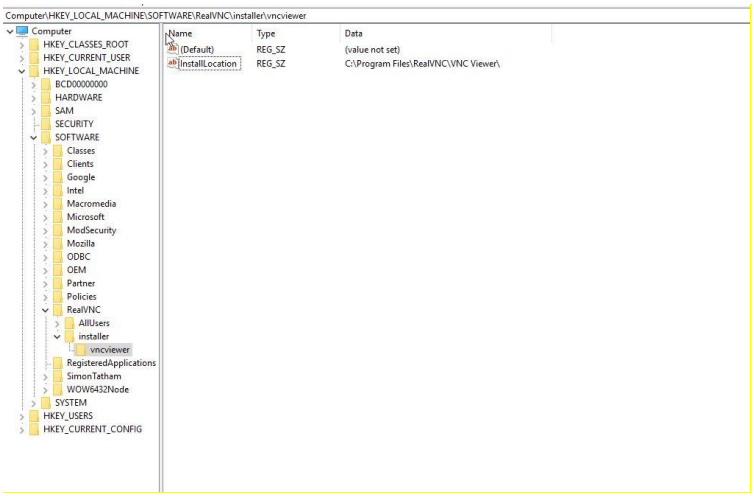
I am used the registry editor to enable SEHOP on system

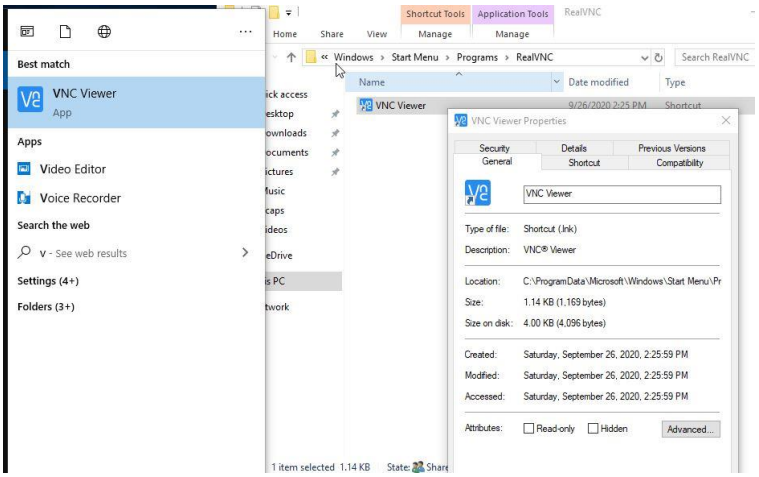


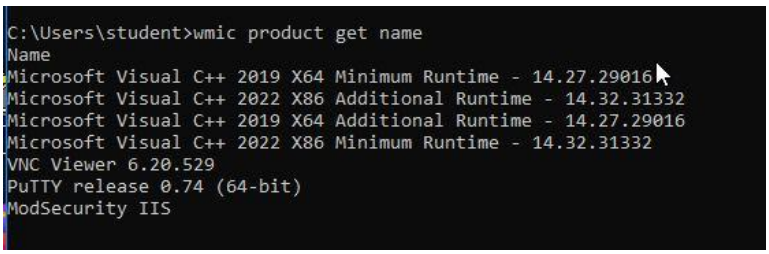
Is this system compliant? NO (Not Compliant)

- MS Security Guide is a Microsoft security baseline that provides security guidance for various Microsoft products and technologies so can not enable SEHOP but can still enable SEHOP on your system by using the registry editor This will ensure that the system is protected from malicious code that attempts to exploit Structured Exception Handling (SEH) vulnerabilities.

Provide documentation as to what applications are installed on the Windows machine.
Is VNC viewer installed in this Windows System? Yes







Ubuntu CIS 1.6.1, 1.6.2

1.6.1 Ensure XD/NX support is enabled

```
ustudent@ubu-ustudent:~$ grep -E 'flags|vmx' /proc/cpuinfo | grep -q nx && echo
"XD/NX is supported" || echo "XD/NX is not supported"
XD/NX is supported
ustudent@ubu-ustudent:~$
```

```
ustudent@ubu-ustudent:~$ dmesg | grep NX
[    0.000000] NX (Execute Disable) protection: active
[    3.573447] input: Power Button as /devices/LNXSYSTM:00/LNXPWRBN:00/input/inp
ut0
[    3.573926] input: Sleep Button as /devices/LNXSYSTM:00/LNXSLPBN:00/input/inp
ut1
[    4.059804] input: Video Bus as /devices/LNXSYSTM:00/LNXSYBUS:00/PNP0A03:00/L
NXVIDEO:00/input/input4
ustudent@ubu-ustudent:~$
```

1.6.2 Ensure address space layout randomization (ASLR) is enabled

```
ustudent@ubu-ustudent:~$ sysctl kernel.randomize_va_space
kernel.randomize_va_space = 2
ustudent@ubu-ustudent:~$ grep "kernel\.randomize va space" /etc/sysctl.conf /et
c/sysctl.d/*
ustudent@ubu-ustudent:~$
```

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

Is TightVNC installed on this Ubuntu machine? Yes (tightvncserver 1.3.10)

```
ii  ssl-cert       1.0.39       all          simple debconf wrapper for OpenSS
ii  strace         4.21-1ubuntu amd64        System call tracer
ii  sudo           1.8.21p2-3ub amd64        Provide limited super user privil
ii  syslinux       3:6.03+dfsg1 amd64        collection of bootloaders (DOS FA
ii  syslinux-commo 3:6.03+dfsg1 all          collection of bootloaders (common
ii  syslinux-legac 2:3.63+dfsg- amd64        Bootloader for Linux/i386 using M
ii  system-config- 1.5.11-1ubun all          graphical interface to configure
ii  system-config- 1.5.11-1ubun all          backend and the translation files
ii  system-config- 1.5.11-1ubun amd64        Utilities to detect and configure
ii  systemd        237-3ubuntu1 amd64        system and service manager
ii  systemd-sysv   237-3ubuntu1 amd64        system and service manager - SysV
ii  sysvinit-utils 2.88dsf-59.1 amd64        System-V-like utilities
ii  t1utils        1.41-2       amd64        Collection of simple Type 1 font
ii  tar            1.29b-2      amd64        GNU version of the tar archiving
ii  tcpd           7.6.q-27     amd64        Wietse Venema's TCP wrapper utili
ii  tcpdump        4.9.2-3      amd64        command-line network traffic anal
ii  tdb-tools      1.3.15-2     amd64        Trivial Database - bundled binari
ii  telnet         0.17-41      amd64        basic telnet client
ii  telnetd        0.17-41      amd64        basic telnet server
ii  tftp           0.17-18ubunt amd64        Trivial file transfer protocol cl
ii  tftpd-hpa      5.2+20150808 amd64        HPA's tftp server
ii  thermald       1.7.0-5ubunt amd64        Thermal monitoring and controllin
ii  thunderbird    1:68.10.0+bu amd64        Email, RSS and newsgroup client w
ii  thunderbird-gn 1:68.10.0+bu amd64        Email, RSS and newsgroup client -
ii  thunderbird-lo 1:68.10.0+bu amd64        English language pack for Thunder
ii  thunderbird-lo 1:68.10.0+bu all          Transitional English language pac
ii  tightvncserver 1.3.10-0ubun amd64        virtual network computing server
ii  time           1.7-25.1buil amd64        GNU time program for measuring CP
ii  totem          3.26.0-0ubun amd64        Simple media player for the GNOME
ii  totem-common   3.26.0-0ubun all          Data files for the Totem media pl
ii  totem-plugins  3.26.0-0ubun amd64        Plugins for the Totem media playe
ii  transmission-c 2.92-3ubuntu all          lightweight BitTorrent client (co
ii  transmission-g 2.92-3ubuntu amd64        lightweight BitTorrent client (GT
ii  tshark         2.4.5-1      amd64        network traffic analyzer - consol
ii  tzdata         2018d-1      all          time zone and daylight-saving tim
ii  ubuntu-advanta 17           all          management tools for Ubuntu Advan
ii  ubuntu-artwork 1:16.10+18.0 all          Ubuntu themes and artwork
ii  ubuntu-desktop 1.417        amd64        The Ubuntu desktop system
```

```
ustudent@ubu-ustudent:~$ dpkg --list | grep tightvnc
ii  tightvncserver                      1.3.10-0ubuntu4                amd64        virtual
network computing server software
ii  xtightvncviewer                     1.3.10-0ubuntu4                amd64        virtual
network computing client software for X
ustudent@ubu-ustudent:~$
```

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

Answer: VNC is a technology that allows remote access and control of a computer over the network and it also used to connect to and control another PC that is running a VNC server

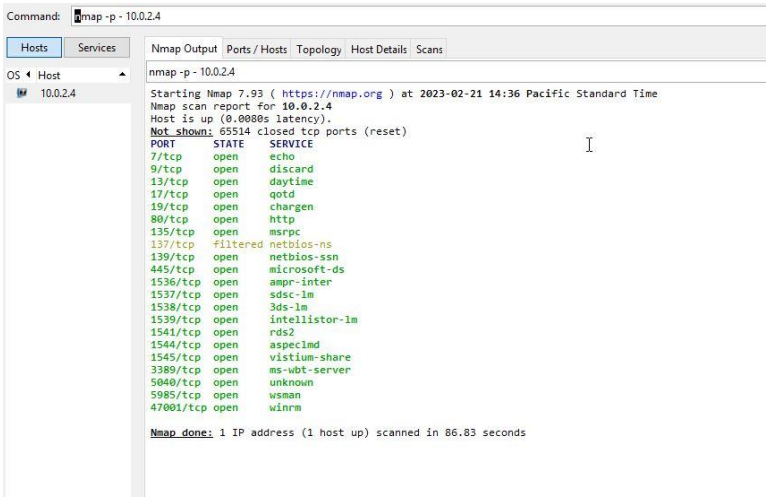
as with any remote access software, there are security risks associated with using VNC, such as data theft, malware infection and unauthorized access
But we can avoid that by following the security best practices such as:

- Use encryption: the traffic of the VNC should be encrypted to prevent interception, many of VNC applications support encryption but users should ensure that this feature is enabled
- Use strong password : the connections should be always be password protected but users should choose strong and unique password that contain characters, numbers, signs.
- Always up-to-date software: applications should be up to date with the latest security updates and patches
- Limit access: the connections should be restricted to trusted users and networks only
- Use firewall : firewalls should be configured to block all incoming VNC traffic, except for authorized connections this actions can help prevent unauthorized access to the application

Task 4

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

Windows scan



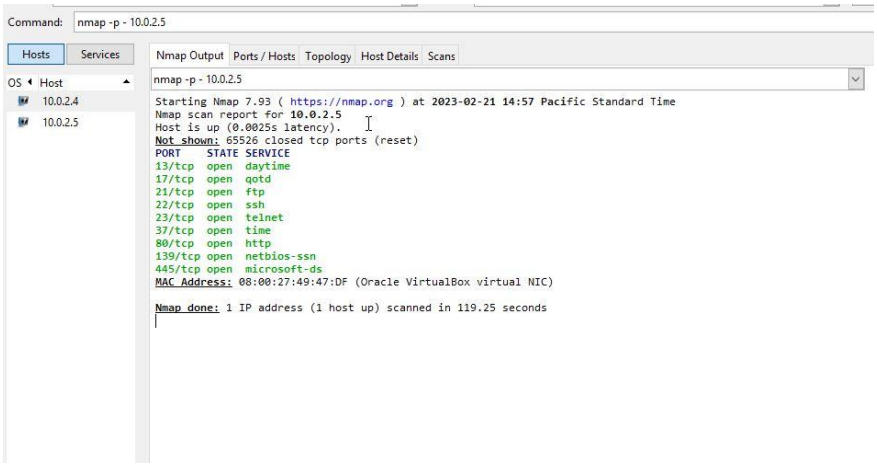
```
nmap -sV --script vuln 10.0.2.4

Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-19 14:31 Pacific Standard Time
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 10.0.2.4
NSOCK ERROR [0.2500s] ssl_init_helper(): OpenSSL legacy provider failed to load.

Host is up (0.0058s latency).
Not shown: 990 closed tcp ports (reset)
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-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-server-header: Microsoft-IIS/10.0
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
|_smb-vuln-webexec: ERROR: Script execution failed (use -d to debug)
445/tcp  open  microsoft-ds  Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
|_smb-vuln-webexec: ERROR: Script execution failed (use -d to debug)
3389/tcp open  ms-wbt-server Microsoft Terminal Services
Service Info: Host: WIN10-USTUDENT; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_smb-vuln-cve-2017-7494: ERROR: Script execution failed (use -d to debug)
|_smb-vuln-conficker: ERROR: Script execution failed (use -d to debug)
|_smb-vuln-ms17-010: ERROR: Script execution failed (use -d to debug)
|_samba-vuln-cve-2012-1182: ERROR: Script execution failed (use -d to debug)
|_smb-vuln-ms07-029: ERROR: Script execution failed (use -d to debug)
|_smb-vuln-ms06-025: ERROR: Script execution failed (use -d to debug)
|_smb-double-pulsar-backdoor: ERROR: Script execution failed (use -d to debug)
```

```
ustudent@ubu-ustudent:~$ nmap -sV --script=vuln 10.0.2.4

Starting Nmap 7.60 ( https://nmap.org ) at 2023-02-19 07:31 EST
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 10.0.2.4
Host is up (0.0063s 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
| sslv2-drown:
```

```
File  Edit  View  Search  Terminal  Help
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
|_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://nma
p.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 310.26 seconds
ustudent@ubu-ustudent:~$
```

```
ustudent@ubu-ustudent:~$ nmap -p- 10.0.2.4

Starting Nmap 7.60 ( https://nmap.org ) at 2023-02-21 08:02 EST
Nmap scan report for 10.0.2.4
Host is up (0.0043s latency).
Not shown: 65514 closed ports
PORT      STATE SERVICE
7/tcp     open  echo
9/tcp     open  discard
13/tcp    open  daytime
17/tcp    open  qotd
19/tcp    open  chargen
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1536/tcp  open  ampr-inter
1537/tcp  open  sdsc-lm
1538/tcp  open  3ds-lm
1539/tcp  open  intellistor-lm
1541/tcp  open  rds2
1544/tcp  open  aspeclmd
1545/tcp  open  vistium-share
3389/tcp  open  ms-wbt-server
5040/tcp  open  unknown
5985/tcp  open  wsman
7680/tcp  open  pando-pub
47001/tcp open  winrm

Nmap done: 1 IP address (1 host up) scanned in 27.12 seconds
ustudent@ubu-ustudent:~$
```

Ubuntu



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 VM

some recommendations to mitigate potential issues associated with these open ports:

- Apply access controls to limit access to specific services or systems. For example, limiting access to port 139 and 445 can prevent unauthorized access to file shares.
- Keep your software up-to-date to mitigate known vulnerabilities that may be exploited through open ports
- Close any ports that are not required for business operations.
    - For example, port 13 and 37 are used for network time synchronization and may not be required in some environments.

    - Ports 21 and 22 are used for file transfer protocols and remote access, respectively, and may be safely closed if not in use.
- Use firewalls to filter traffic and block unauthorized access to open ports. For example, a firewall can be configured to only allow incoming traffic to port 80 if it is intended for a specific web server.

Windows VM

some recommendations to mitigate potential issues associated with these open ports:

- Use firewalls to filter traffic and block unauthorized access to open ports.
    - For example, a firewall can be configured to only allow incoming traffic to port 80 if it is intended for a specific web server.
    - Additionally, a firewall can be configured to block all incoming traffic to ports 3389 and 5985, which are commonly used for remote desktop access and PowerShell remoting, respectively.
- Keep your software up-to-date to mitigate known vulnerabilities that may be exploited through open ports.
    - For example, updating your web server software can prevent known vulnerabilities that may be exploited through port 80.
- Close any ports that are not required for business operations.
    - For example, ports 7 and 9 are used for remote access protocols that may not be required in some environments.
    - Ports 135, 139, and 445 are commonly used by Microsoft networking services and may be safely closed if not required.

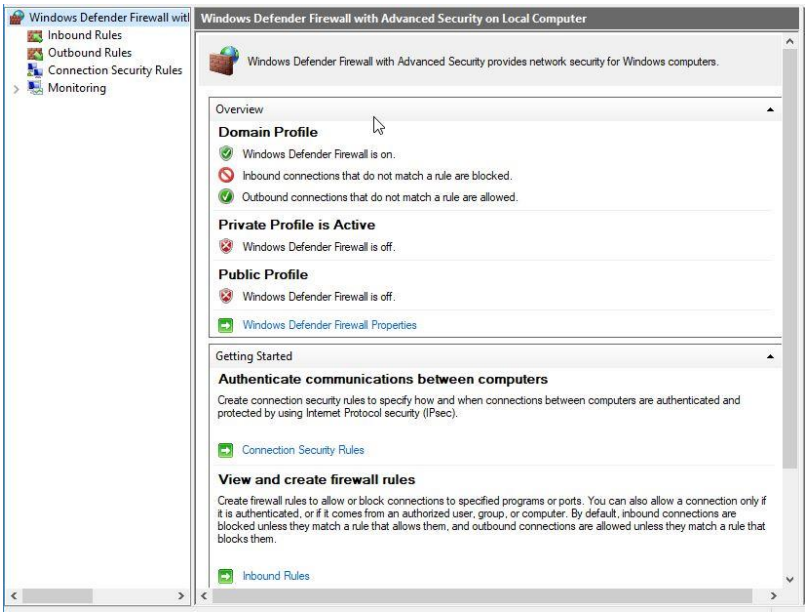
Step 2: Assess Access Management at Targeted Assets

Task 1

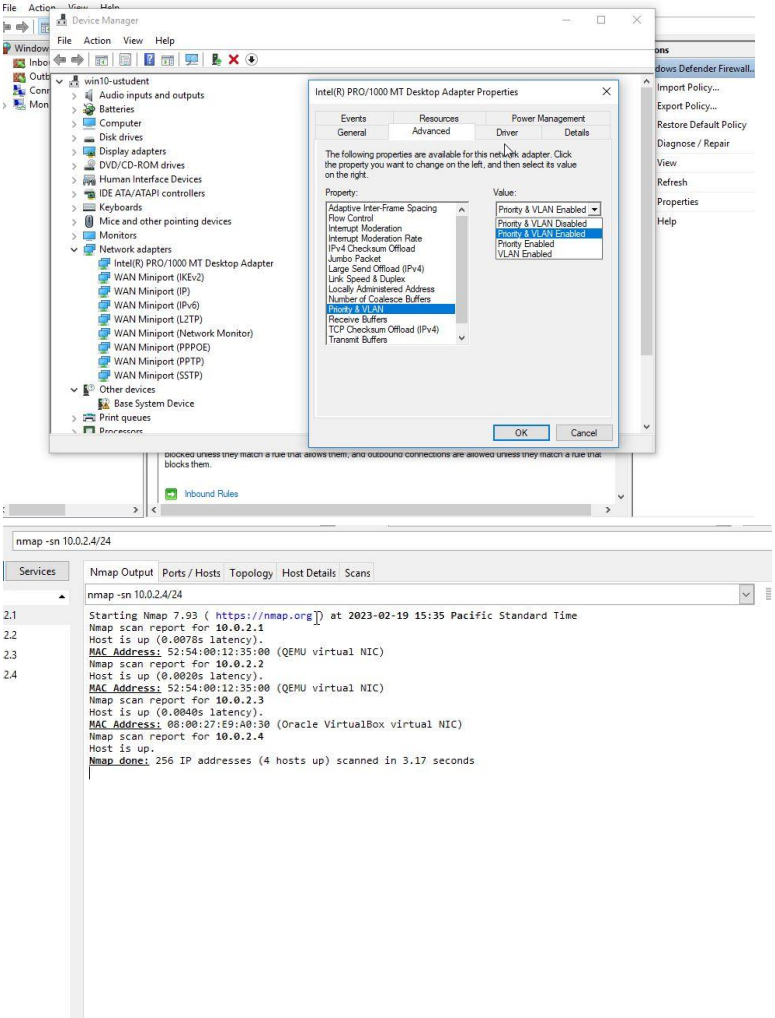
Check for current settings on Network Segmentation, VLANs, Domain Isolation, or IP Security Policies.

Windows

Network segmentation


Windows Defender Firewall with Advanced Security on Local Computer
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Windows Defender Firewall with Advanced Security provides network security for Windows computers.
Overview
Domain Profile
Windows Defender Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.
Private Profile is Active
Windows Defender Firewall is off.
Public Profile
Windows Defender Firewall is off.
Windows Defender Firewall Properties
Getting Started
Authenticate communications between computers
Create connection security rules to specify how and when connections between computers are authenticated and protected by using Internet Protocol security (IPsec).
Connection Security Rules
View and create firewall rules
Create firewall rules to allow or block connections to specified programs or ports. You can also allow a connection only if it is authenticated, or if it comes from an authorized user, group, or computer. By default, inbound connections are blocked unless they match a rule that allows them, and outbound connections are allowed unless they match a rule that blocks them.
Inbound Rules

VLANs

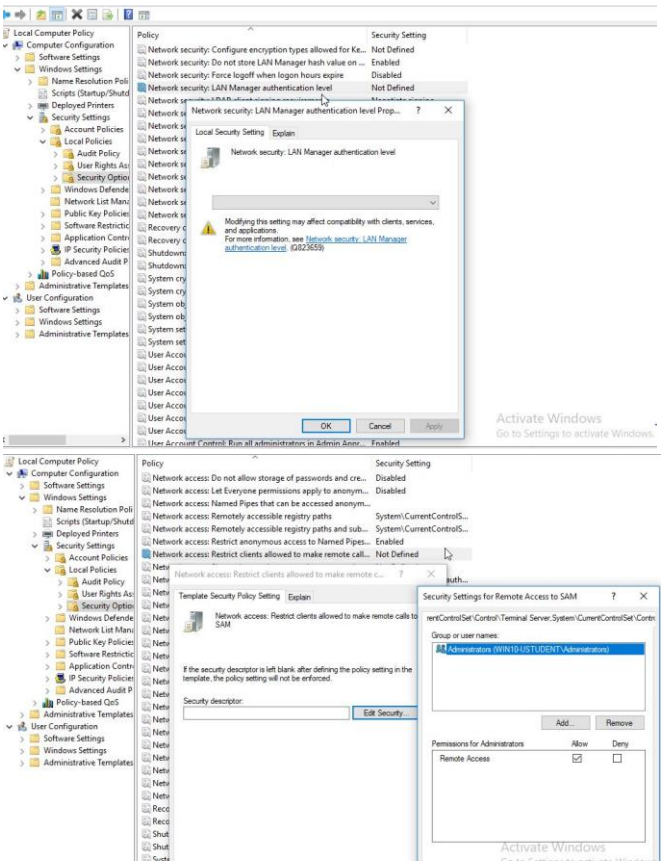

Device Manager
File Action View Help
win10-ustudent
Audio inputs and outputs
Batteries
Computer
Disk drives
Display adapters
DVD/CD-ROM drives
Human Interface Devices
IDE ATA/ATAPI controllers
Keyboards
Mice and other pointing devices
Monitors
Network adapters
Intel(R) PRO/1000 MT Desktop Adapter
WAN Miniport (IKEv2)
WAN Miniport (IP)
WAN Miniport (IPv6)
WAN Miniport (L2TP)
WAN Miniport (Network Monitor)
WAN Miniport (PPPOE)
WAN Miniport (PPTP)
WAN Miniport (SSTP)
Other devices
Base System Device
Print queues
Intel(R) PRO/1000 MT Desktop Adapter Properties
Events
Resources
Power Management
General
Advanced
Driver
Details
The following properties are available for this network adapter. Click the property you want to change on the left, and then select its value on the right.
Property:
Value:
Adaptive Inter-Frame Spacing
Flow Control
Interrupt Moderation
Interrupt Moderation Rate
IPv4 Checksum Offload
Jumbo Packet
Large Send Offload (IPv4)
Link Speed & Duplex
Locally Administered Address
Number of Coalesce Buffers
Priority & VLAN
Receive Buffers
TCP Checksum Offload (IPv4)
Transmit Buffers
Priority & VLAN Enabled
Priority & VLAN Disabled
Priority & VLAN Enabled
Priority Enabled
VLAN Enabled
OK
Cancel
Import Policy...
Export Policy...
Restore Default Policy
Diagnose / Repair
View
Refresh
Properties
Help
Inbound Rules
nmap -sn 10.0.2.4/24
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -sn 10.0.2.4/24
Starting Nmap 7.93 (https://nmap.org) at 2023-02-19 15:35 Pacific Standard Time
Nmap scan report for 10.0.2.1
Host is up (0.0070s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.2
Host is up (0.0020s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.3
Host is up (0.0040s latency).
MAC Address: 08:00:27:E9:A0:30 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.4
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 3.17 seconds

Domain Isolation

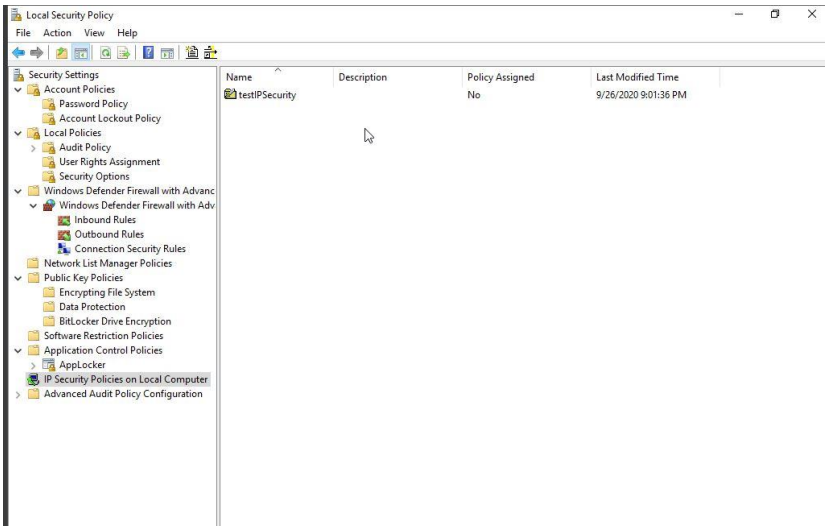
```
C:\Windows\system32>gpresult /r

Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.0
© 2017 Microsoft Corporation. All rights reserved.

Created on ‎2/‎21/‎2023 at 6:03:59 AM


RSOP data for WIN10-USTUDENT\student on WIN10-USTUDENT : Logging Mode
------------------------------------------------------------------------

OS Configuration:            Standalone Workstation
OS Version:                  10.0.16299
Site Name:                   N/A
Roaming Profile:             N/A
Local Profile:               C:\Users\student
Connected over a slow link?: No


COMPUTER SETTINGS
------------------

    Last time Group Policy was applied: 2/21/2023 at 1:06:07 PM
    Group Policy was applied from:      N/A
    Group Policy slow link threshold:   500 kbps
    Domain Name:                        WIN10-USTUDENT
    Domain Type:                        <Local Computer>

    Applied Group Policy Objects
    ----------------------------
        Local Group Policy

    The computer is a part of the following security groups
    -------------------------------------------------------
        System Mandatory Level
        Everyone
        BUILTIN\Users
        NT AUTHORITY\SERVICE
        CONSOLE LOGON
        NT AUTHORITY\Authenticated Users
        This Organization
        BDESVC
        BITS
        dmwappushservice
```

```
        BITS
        dmwappushservice
        DsmSvc
        Eaphost
        IKEEXT
        iphlpsvc
        LanmanServer
        lfsvc
        MSiSCSI
        NcaSvc
        NetSetupSvc
        PushToInstall
        RasAuto
        Schedule
        SENS
        SessionEnv
        SharedAccess
        ShellHWDetection
        wercplsupport
        Winmgmt
        wisvc
        wlidsvc
        WpnService
        XboxNetApiSvc
        LOCAL
        BUILTIN\Administrators


USER SETTINGS
--------------

    Last time Group Policy was applied: 2/21/2023 at 1:06:33 PM
    Group Policy was applied from:      N/A
    Group Policy slow link threshold:   500 kbps
    Domain Name:                        DESKTOP-OL2NG4U
    Domain Type:                        <Local Computer>

    Applied Group Policy Objects
    ----------------------------
        N/A

    The following GPOs were not applied because they were filtered out
    ------------------------------------------------------------------
        Local Group Policy
```

```
USER SETTINGS
--------------

    Last time Group Policy was applied: 2/21/2023 at 1:06:33 PM
    Group Policy was applied from:      N/A
    Group Policy slow link threshold:   500 kbps
    Domain Name:                        DESKTOP-OL2NG4U
    Domain Type:                        <Local Computer>

    Applied Group Policy Objects
    ----------------------------
        N/A

    The following GPOs were not applied because they were filtered out
    ------------------------------------------------------------------
        Local Group Policy
            Filtering:  Not Applied (Empty)

    The user is a part of the following security groups
    ---------------------------------------------------
        None
        Everyone
        Local account and member of Administrators group
        BUILTIN\Administrators
        BUILTIN\Users
        NT AUTHORITY\INTERACTIVE
        CONSOLE LOGON
        NT AUTHORITY\Authenticated Users
        This Organization
        Local account
        LOCAL
        NTLM Authentication
        High Mandatory Level

C:\Windows\system32>
```

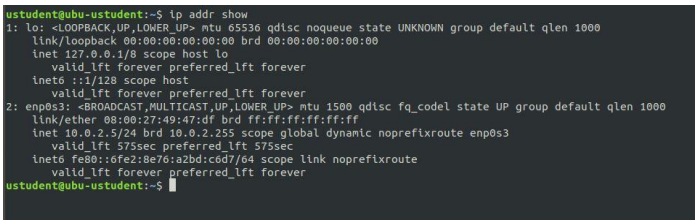


IP Security Policies

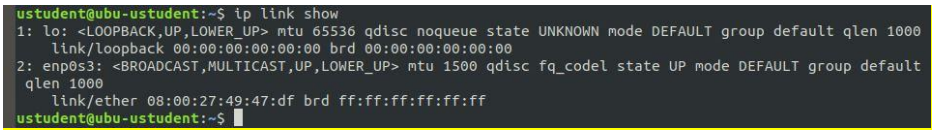


Ubuntu VM

Network Segmentation

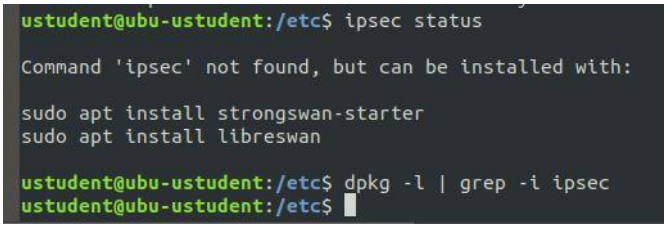


VLANs



Domain Isolation

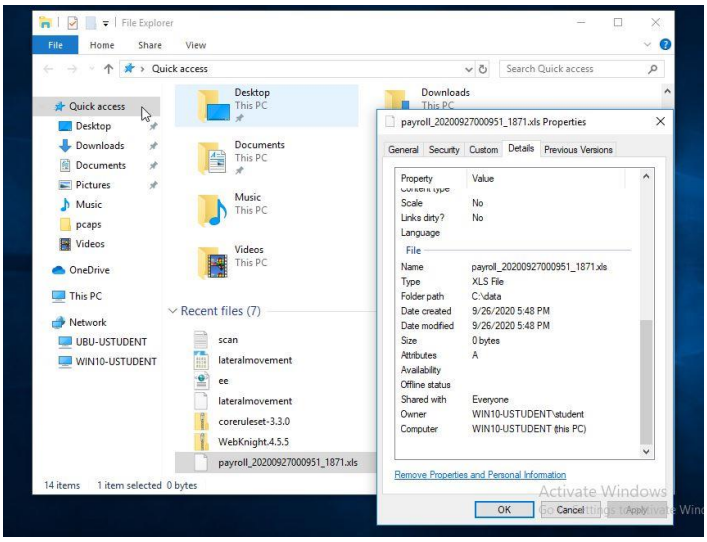
IP Security Policies



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?
    - Windows: Yes
    - Ubuntu: NO
- Are there any policies in place?
    - Windows: No
    - Ubuntu: No
    - If there are any, are they applied?
    - Windows: Yes
    - Ubuntu: No

- Is Anonymous access granted to any share?
    - Windows: Yes

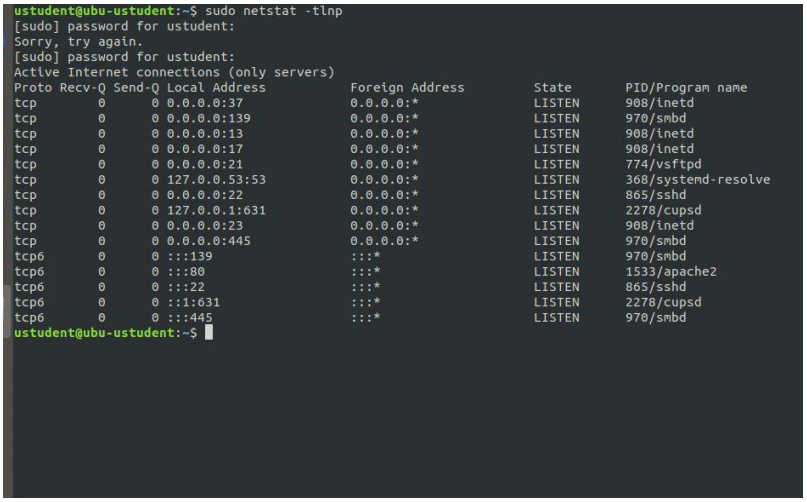


    - Ubuntu: NO

Task 2

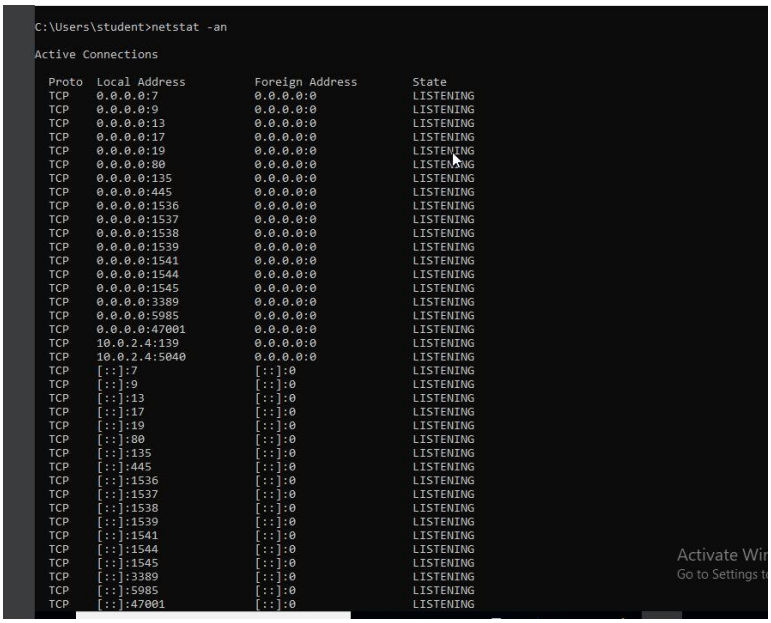
Investigate and assess the remote access services and protocols in place for StaticSpeed and determine their security level. After completing your investigation, including your assessment of how StaticSpeed is doing with remote access. Please have evidence to support your findings. Remember to consider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

Ubuntu



- Close any ports that are not required for business operations.
    - For example, port 13 and 37 are used for network time synchronization and may not be required in some environments.
    - Ports 21 and 22 are used for file transfer protocols and remote access, respectively, and may be safely closed if not in use.
- Use firewalls to filter traffic and block unauthorized access to open ports. For example, a firewall can be configured to only allow incoming traffic to port 80 if it is intended for a specific web server.

Windows



- Close any ports that are not required for business operations.

    - For example, ports 7 and 9 are used for remote access protocols that may not be required in some environments.
    - Ports 135, 139, and 445 are commonly used by Microsoft networking services and may be safely closed if not required.
- Use firewalls to filter traffic and block unauthorized access to open ports.
    - For example, a firewall can be configured to only allow incoming traffic to port 80 if it is intended for a specific web server.
    - Additionally, a firewall can be configured to block all incoming traffic to ports 3389 and 5985, which are commonly used for remote desktop access and PowerShell remoting, respectively.

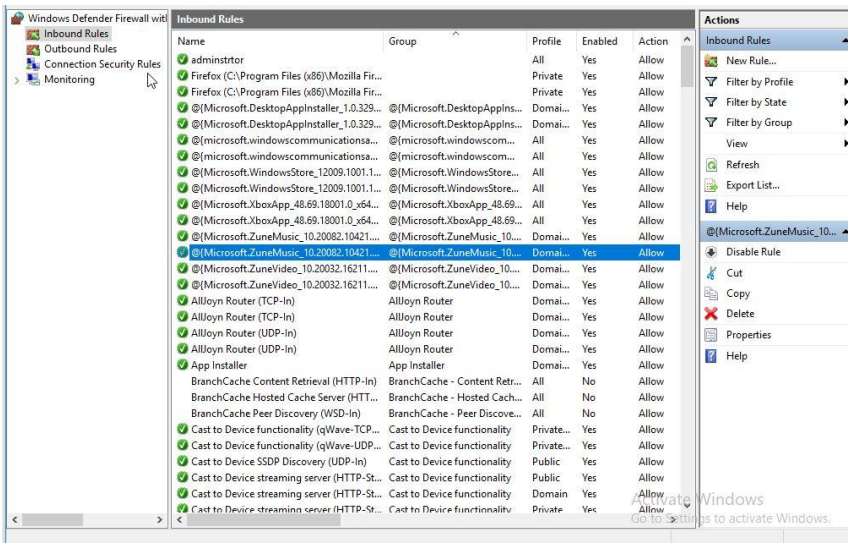
Task 3

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?

Ubuntu

```
ustudent@ubu-ustudent:~$ sudo ufw enable
[sudo] password for ustudent:
Firewall is active and enabled on system startup
ustudent@ubu-ustudent:~$ sudo ufw allow 22/tcp
Rule added
Rule added (v6)
ustudent@ubu-ustudent:~$ sudo ufw allow 3389/tcp
Rule added
Rule added (v6)
ustudent@ubu-ustudent:~$ sudo ufw allow 5900/tcp
Rule added
Rule added (v6)
ustudent@ubu-ustudent:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW       Anywhere
3389/tcp                   ALLOW       Anywhere
5900/tcp                   ALLOW       Anywhere
22/tcp (v6)                ALLOW       Anywhere (v6)
3389/tcp (v6)              ALLOW       Anywhere (v6)
5900/tcp (v6)              ALLOW       Anywhere (v6)

ustudent@ubu-ustudent:~$
```

Windows



Also, what ports would you suggest to have open and running and why?

it's a good practice to only open the ports that are necessary for the required services and to keep all other ports closed.

Here are some common ports and the services they are associated with:

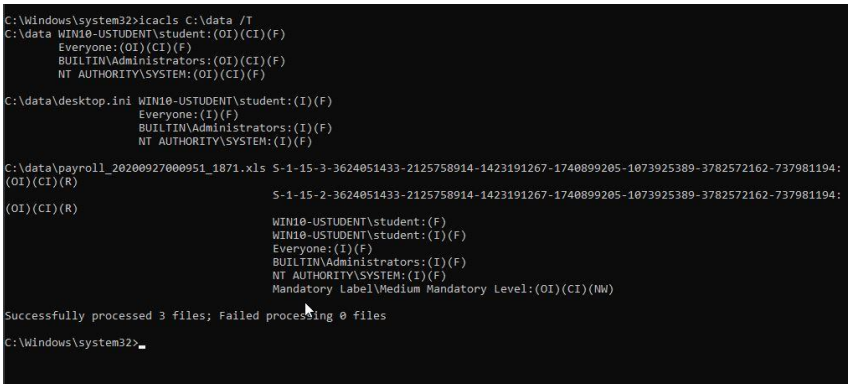
- Port 80 (HTTP): is used by web servers to serve HTTP requests.
- Port 443 (HTTPS): is used by web servers to serve HTTPS requests.
- Port 22 (SSH): is used by the SSH protocol for secure remote login and file transfer.
- Port 21 (FTP): is used by the FTP protocol for file transfer.
- Port 53 (DNS): is used by the DNS protocol for domain name resolution.

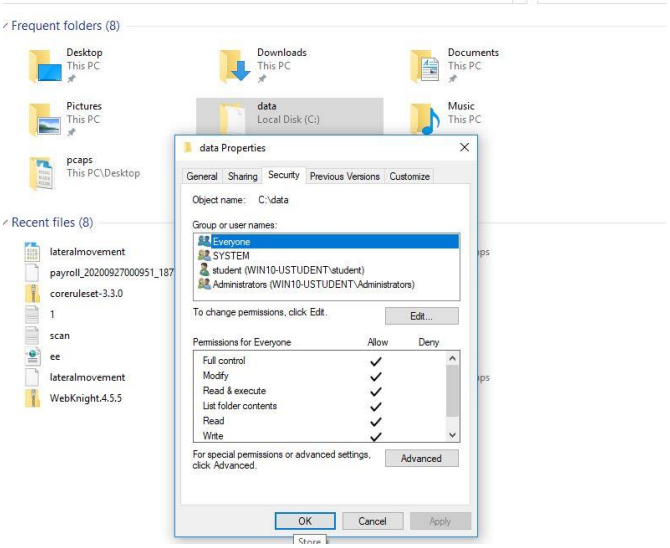
In addition to these common ports, you should also consider the specific needs of environment and applications that opening unnecessary ports can increase the attack surface of your system and make it more vulnerable to attacks.

Task 4

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

- Which users have high privileges?
    - Windows
        1. Administrators
        2. Student
    - Ubuntu
        1. Ustudent
        2. root
- Do important PII folders have the correct permissions and ownership?
    - Windows





```
C:\Windows\system32>icacls C:\Users\student\Documents /T
C:\Users\student\Documents S-1-5-21-417261718-1219827454-1960118223-1002:(OI)(CI)(RX)
                           NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)
                           BUILTIN\Administrators:(I)(OI)(CI)(F)
                           WIN10-USTUDENT\student:(I)(OI)(CI)(F)

C:\Users\student\Documents\coreruleset-3.3.0.zip S-1-15-3-3624051433-2125758914-1423191267-1740899205-1073925389-3782572162-7
37981194:(OI)(CI)(R)
                                                 S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-3782572162-7
37981194:(OI)(CI)(R)
                                                 WIN10-USTUDENT\student:(F)
                                                 S-1-5-21-417261718-1219827454-1960118223-1002:(I)(RX)
                                                 NT AUTHORITY\SYSTEM:(I)(F)
                                                 BUILTIN\Administrators:(I)(F)
                                                 WIN10-USTUDENT\student:(I)(F)
                                                 Mandatory Label\Medium Mandatory Level:(OI)(CI)(NW)

C:\Users\student\Documents\desktop.ini S-1-5-21-417261718-1219827454-1960118223-1002:(I)(RX)
                                       NT AUTHORITY\SYSTEM:(I)(F)
                                       BUILTIN\Administrators:(I)(F)
                                       WIN10-USTUDENT\student:(I)(F)

C:\Users\student\Documents\ModSecurityIIS_2.9.3-64b.msi S-1-15-3-3624051433-2125758914-1423191267-1740899205-1073925389-37825
72162-737981194:(OI)(CI)(R)
                                                        S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-37825
72162-737981194:(OI)(CI)(R)
                                                        WIN10-USTUDENT\student:(F)
                                                        S-1-5-21-417261718-1219827454-1960118223-1002:(I)(RX)
                                                        NT AUTHORITY\SYSTEM:(I)(F)
                                                        BUILTIN\Administrators:(I)(F)
                                                        WIN10-USTUDENT\student:(I)(F)
                                                        Mandatory Label\Medium Mandatory Level:(OI)(CI)(NW)

C:\Users\student\Documents\My Music Everyone:(DENY)(S,RD)
                                     S-1-5-21-417261718-1219827454-1960118223-1002:(I)(OI)(CI)(RX)
                                     NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)
                                     BUILTIN\Administrators:(I)(OI)(CI)(F)
                                     WIN10-USTUDENT\student:(I)(OI)(CI)(F)

C:\Users\student\Documents\My Pictures Everyone:(DENY)(S,RD)
                                       S-1-5-21-417261718-1219827454-1960118223-1002:(I)(OI)(CI)(RX)
                                       NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)
                                       BUILTIN\Administrators:(I)(OI)(CI)(F)
```



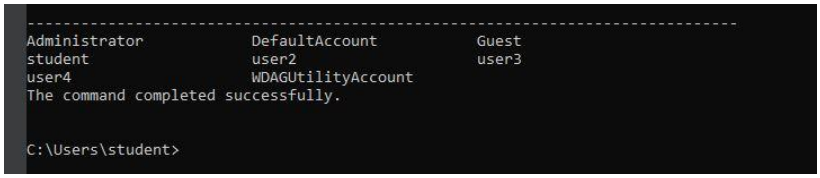
```
C:\Users\student\Documents\My Music Everyone:(DENY)(S,RD)
                                     S-1-5-21-417261718-1219827454-1960118223-1002:(I)(OI)(CI)(RX)
                                     NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)
                                     BUILTIN\Administrators:(I)(OI)(CI)(F)
                                     WIN10-USTUDENT\student:(I)(OI)(CI)(F)

C:\Users\student\Documents\My Pictures Everyone:(DENY)(S,RD)
                                       S-1-5-21-417261718-1219827454-1960118223-1002:(I)(OI)(CI)(RX)
                                       NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)
                                       BUILTIN\Administrators:(I)(OI)(CI)(F)
                                       WIN10-USTUDENT\student:(I)(OI)(CI)(F)

C:\Users\student\Documents\My Videos Everyone:(DENY)(S,RD)
                                     S-1-5-21-417261718-1219827454-1960118223-1002:(I)(OI)(CI)(RX)
                                     NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)
                                     BUILTIN\Administrators:(I)(OI)(CI)(F)
                                     WIN10-USTUDENT\student:(I)(OI)(CI)(F)

C:\Users\student\Documents\WebKnight.4.5.5.zip S-1-15-3-3624051433-2125758914-1423191267-1740899205-1073925389-3782572162-737
981194:(OI)(CI)(R)
                                               S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-3782572162-737
981194:(OI)(CI)(R)
                                               WIN10-USTUDENT\student:(F)
                                               S-1-5-21-417261718-1219827454-1960118223-1002:(I)(RX)
                                               NT AUTHORITY\SYSTEM:(I)(F)
                                               BUILTIN\Administrators:(I)(F)
                                               WIN10-USTUDENT\student:(I)(F)
                                               Mandatory Label\Medium Mandatory Level:(OI)(CI)(NW)

C:\Users\student\Documents\My Music\*: Access is denied.
Successfully processed 8 files; Failed processing 1 files

C:\Windows\system32>
```

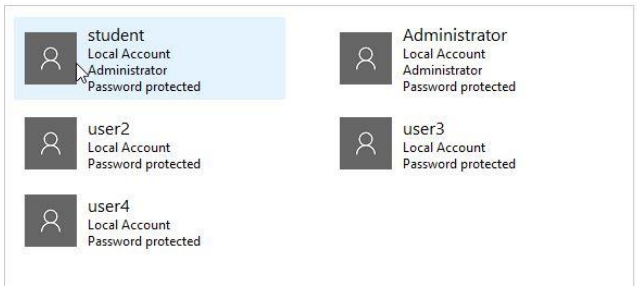
Ubuntu

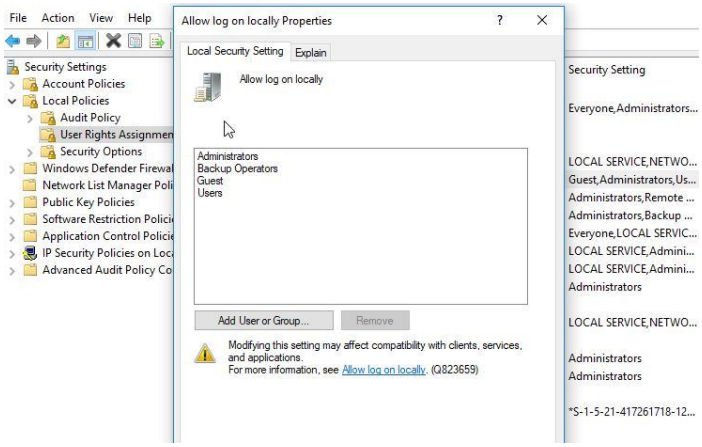
```
ustudent@ubu-ustudent:~$ ls -l
total 64
-rw-r--r-- 1 ustudent ustudent    0 Sep 27  2020 '*'
-rw-r--r-- 1 ustudent ustudent   83 Sep 26  2020  aclfile.txt
drwxr-xr-x 3 ustudent ustudent 4096 Sep 27  2020  Desktop
drwxr-xr-x 3 ustudent ustudent 4096 Sep 26  2020  Documents
drwxr-xr-x 2 ustudent ustudent 4096 Sep 26  2020  Downloads
-rw-r--r-- 1 ustudent ustudent 8980 Sep 26  2020  examples.desktop
-rw-r--r-- 1 ustudent ustudent  121 Sep 27  2020  ftpvuln.txt
drwxr-xr-x 2 ustudent ustudent 4096 Sep 26  2020  Music
-rw-r--r-- 1 ustudent ustudent 3328 Feb 18 04:40  password.txt
drwxr-xr-x 2 ustudent ustudent 4096 Sep 26  2020  Pictures
drwxr-xr-x 2 ustudent ustudent 4096 Sep 26  2020  Public
drwxr-xr-x 4 ustudent ustudent 4096 Feb 19 06:55  scipag_vulscan
drwxr-xr-x 2 ustudent ustudent 4096 Sep 26  2020  Templates
drwxr-xr-x 2 ustudent ustudent 4096 Sep 26  2020  Videos
drwxr-xr-x 9 ustudent ustudent 4096 Sep 27  2020  vsftpd-2.3.4-infected
ustudent@ubu-ustudent:~$
```

- 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? yes
- Are they allowed to use Sudo commands? No
- Are they allowed to log in to ALL workstations?. yes
    - that guest accounts should generally be disabled or restricted to minimal privileges to reduce security risks. It is recommended to only use guest accounts for temporary access

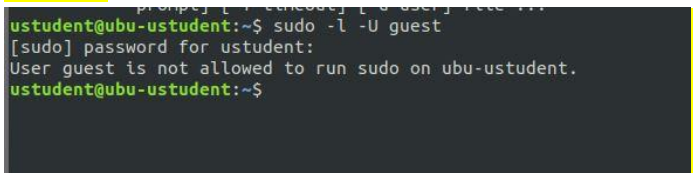
Windows







Ubuntu

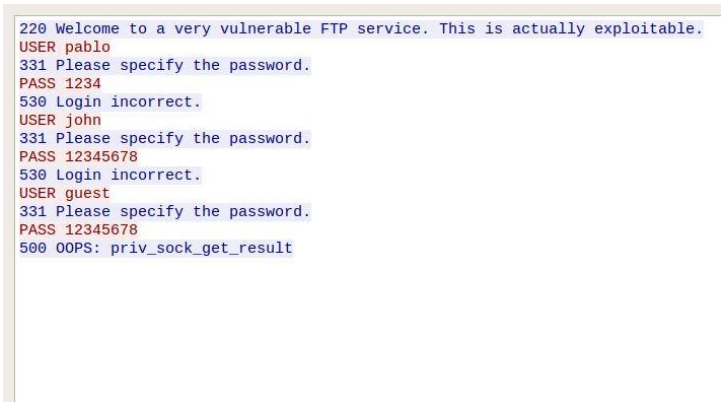


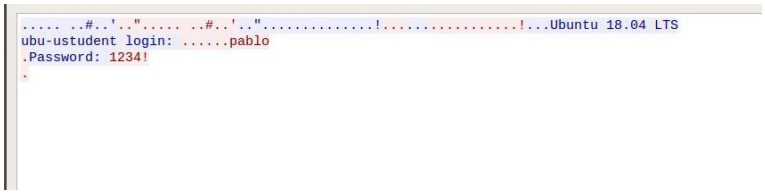
Based on your findings, what should be done to secure these accounts and permissions better? Please provide proof of your results and provide reasoning for your answer.

- Only authorized users must have high privileges
- If find any guest accounts with high privileges, it is recommended to either disable them or restrict their access to minimize the risk of unauthorized access.

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.





se the pcap file to assess and determine the following:

- What type of attack was recorded? telnet
- What is the source IP of the attack? 10.0.2.7
- What protocol was targeted? TCP
- What password was used successfully? 1234
- Which user was compromised? Pablo

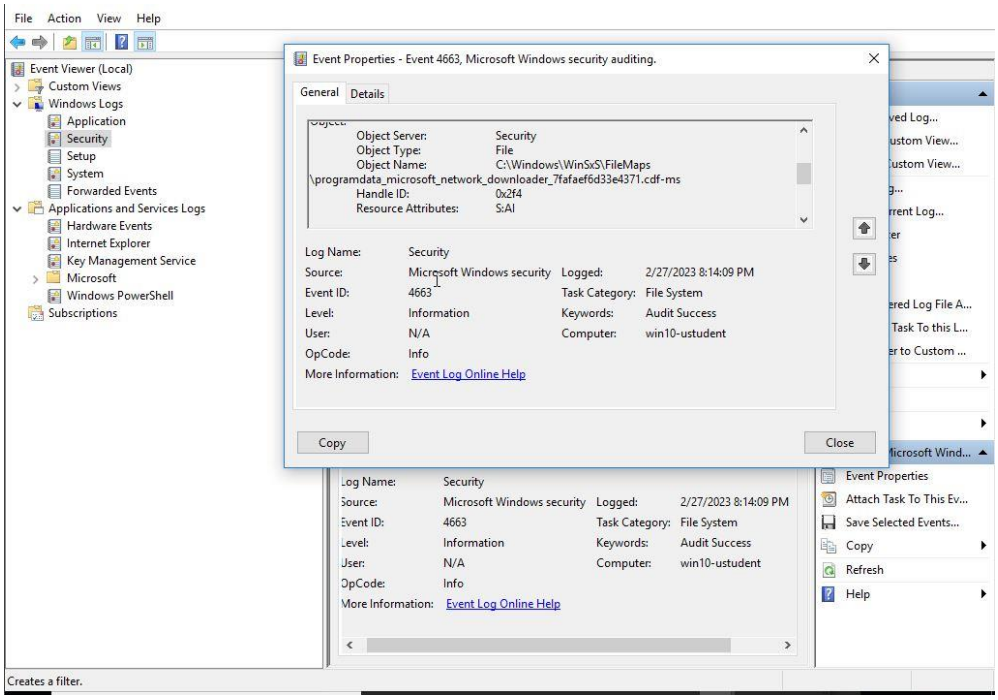
Based on your findings from above, what is your assessment of what happened? Please provide evidence to back up your results.

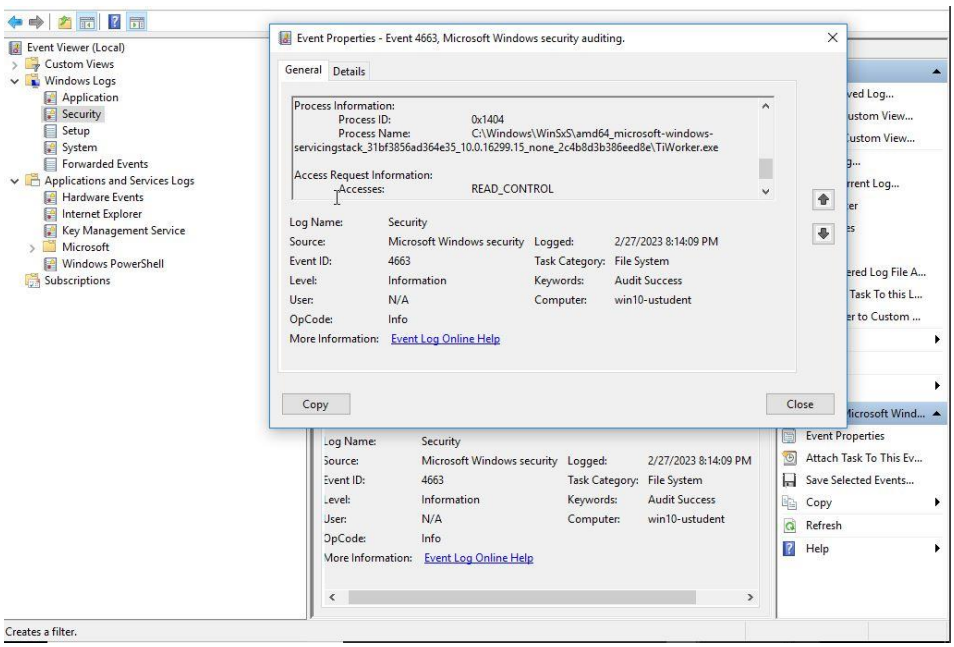
- must change the password of telnet immediately
- use firewall to prevent the attacker IP
- close the sessions if 5 min run without any action
- change the telnet password every 45 days if it possible or every 90 days
- always save a back up of the data preferred 1 production copy plus 2 additional backup copies
- copies should be in two different storage types
- preferred to save 1 copy far from the internet

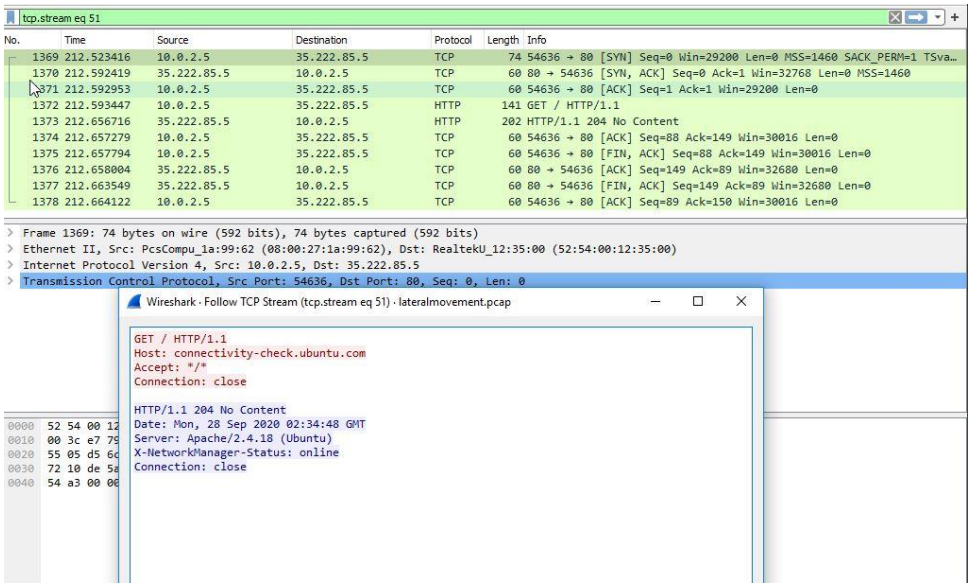
Task 2

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? 10.0.2.6
- Did the attacker try to access your machine from a compromised device - MITRE ATT&CK Technique T1021?




Event Viewer (Local)
Custom Views
Windows Logs
Application
Security
Setup
System
Forwarded Events
Applications and Services Logs
Hardware Events
Internet Explorer
Key Management Service
Microsoft
Windows PowerShell
Subscriptions
Event Properties - Event 4663, Microsoft Windows security auditing.
General
Details
Process Information:
Process ID: 0x1404
Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.16299.15_none_2c4b8d3b386eed8e\TiWorker.exe
Access Request Information:
Accesses: READ_CONTROL
Log Name: Security
Source: Microsoft Windows security
Logged: 2/27/2023 8:14:09 PM
Event ID: 4663
Task Category: File System
Level: Information
Keywords: Audit Success
User: N/A
Computer: win10-ustudent
OpCode: Info
More Information: Event Log Online Help
Copy
Close
Event Properties
Attach Task To This Ev...
Save Selected Events...
Copy
Refresh
Help
Creates a filter.

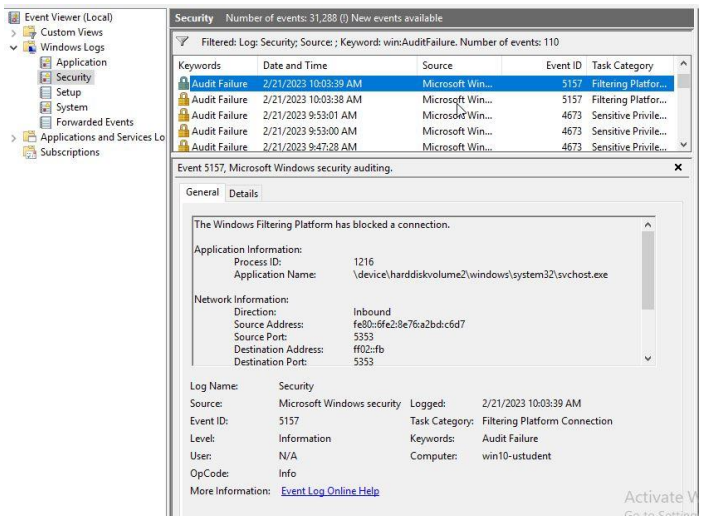

tcp.stream eq 51
No. Time Source Destination Protocol Length Info
1369 212.523416 10.0.2.5 35.222.85.5 TCP 74 54636 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSva...
1370 212.592419 35.222.85.5 10.0.2.5 TCP 60 80 → 54636 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
1371 212.592953 10.0.2.5 35.222.85.5 TCP 60 54636 → 80 [ACK] Seq=1 Ack=1 Win=29200 Len=0
1372 212.593447 10.0.2.5 35.222.85.5 HTTP 141 GET / HTTP/1.1
1373 212.656716 35.222.85.5 10.0.2.5 HTTP 202 HTTP/1.1 204 No Content
1374 212.657279 10.0.2.5 35.222.85.5 TCP 60 54636 → 80 [ACK] Seq=88 Ack=149 Win=30016 Len=0
1375 212.657794 10.0.2.5 35.222.85.5 TCP 60 54636 → 80 [FIN, ACK] Seq=88 Ack=149 Win=30016 Len=0
1376 212.658004 35.222.85.5 10.0.2.5 TCP 60 80 → 54636 [ACK] Seq=149 Ack=89 Win=32680 Len=0
1377 212.663549 35.222.85.5 10.0.2.5 TCP 60 80 → 54636 [FIN, ACK] Seq=149 Ack=89 Win=32680 Len=0
1378 212.664122 10.0.2.5 35.222.85.5 TCP 60 54636 → 80 [ACK] Seq=89 Ack=150 Win=30016 Len=0
Frame 1369: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Ethernet II, Src: PcsCompu_1a:99:62 (08:00:27:1a:99:62), Dst: RealtekU_12:35:00 (52:54:00:12:35:00)
Internet Protocol Version 4, Src: 10.0.2.5, Dst: 35.222.85.5
Transmission Control Protocol, Src Port: 54636, Dst Port: 80, Seq: 0, Len: 0
Wireshark · Follow TCP Stream (tcp.stream eq 51) · lateralmovement.pcap
GET / HTTP/1.1
Host: connectivity-check.ubuntu.com
Accept: */*
Connection: close
HTTP/1.1 204 No Content
Date: Mon, 28 Sep 2020 02:34:48 GMT
Server: Apache/2.4.18 (Ubuntu)
X-NetworkManager-Status: online
Connection: close

```
...T.SMBr......(...................V.1..LANMAN1.0..LM1.2X002..NT LANMAN 1.0..NT LM
0.12......SMBr......(...................V....2...................J...X......:.39*.d..H..f..
3..`(..+.......0...0..
+.....7....
+.....7..
.....SMBs......(...................V...............1.........T.NTLMSSP............
.......!....5CwDSxRcr06YqfxKWindows 2000 2195.Windows 2000
5.0....U.SMBs......h...................V...U.....*.NTLMSSP.........8.......o..
5.O............T..........W.I.N.1.0.-.U.S.T.U.D.E.N.T.....W.I.N.
1.0.-.U.S.T.U.D.E.N.T.....W.I.N.1.0.-.U.S.T.U.D.E.N.T.....w.i.n.
1.0.-.u.s.t.u.d.e.n.t.....w.i.n.1.0.-.u.s.t.u.d.e.n.t......0..X.......Windows 7 Professional
7601 Service Pack 1.Windows 7 Professional 6.1......SMBs......
(...................V...............:.....\...].NTLMSSP.........@.......X...................
.
.........:.......*$.<.)M.......b!..._>....w......H..v..K.............?......_>...........W.I
.N.1.0.-.U.S.T.U.D.E.N.T.....W.I.N.1.0.-.U.S.T.U.D.E.N.T.....w.i.n.
1.0.-.u.s.t.u.d.e.n.t.....w.i.n.1.0.-.u.s.t.u.d.e.n.t......0..X............
5.C.w.D.S.x.R.c.r.0.6.Y.q.f.x.K.Windows 2000 2195.Windows 2000
5.0....#.SMBsm.....h...................V......c.SMBs...... ...................V
......................@...&....Windows 2000 2195.Windows 2000 5.0....y.SMBs......
..................V...y...P.Windows 7 Professional 7601 Service Pack 1.Windows 7
Professional 6.1.WORKGROUP....B.SMBu......(...................V............\
\10.0.2.6\IPC$.?????......SMBu......(...................V.........IPC.....J.SMB%......
(...................V.....................J...J...#.....
\PIPE\....#.SMB%......h...................V......O.SMB2.........................A...........
...........B...N.......................#.SMB2.........................A....
```

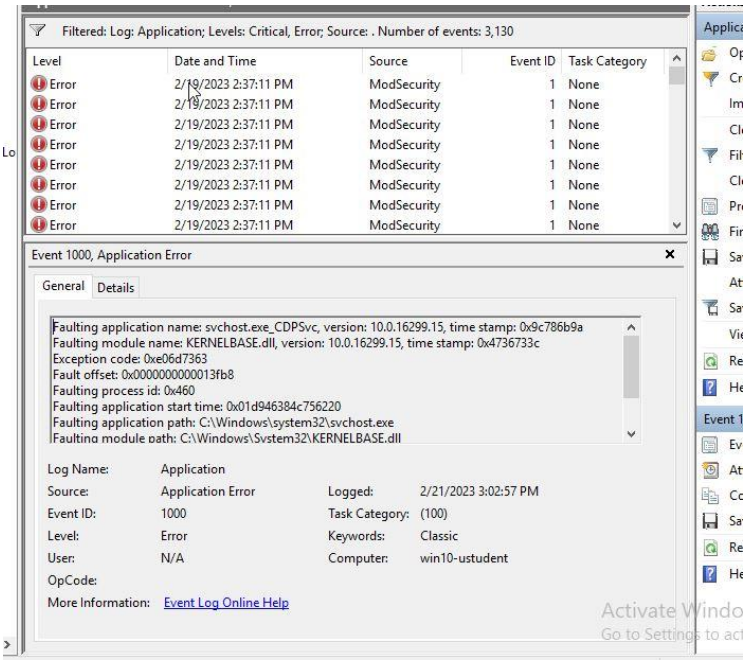
No.	Time	Source	Destination	Protocol	Length	Info
49	42.936943	10.0.2.7	10.0.2.6	SMB	149	Trans2 Request, SESSION_SETUP
50	42.937107	10.0.2.6	10.0.2.7	SMB	105	Trans2 Response, SESSION_SETUP, Error: STATUS_NOT_IMPLEMENTE
51	42.937476	10.0.2.7	10.0.2.6	TCP	66	34515 → 445 [FIN, ACK] Seq=982 Ack=769 Win=64128 Len=0 TSval
52	42.937633	10.0.2.6	10.0.2.7	TCP	66	445 → 34515 [ACK] Seq=769 Ack=983 Win=65536 Len=0 TSval=2393
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 SACK_PERM=1
55	42.939412	10.0.2.6	10.0.2.7	TCP	74	445 → 46311 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 W
56	42.939577	10.0.2.7	10.0.2.6	TCP	66	46311 → 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=37268145
57	42.941867	10.0.2.7	10.0.2.6	SMB	117	Negotiate Protocol Request
58	42.942190	10.0.2.6	10.0.2.7	SMB	197	Negotiate Protocol Response

```
> Frame 1: 208 bytes on wire (1664 bits), 208 bytes captured (1664 bits)
> Ethernet II, Src: PcsCompu_f9:6d:c9 (08:00:27:f9:6d:c9), Dst: IPv6mcast_0c (33:33:00:00:00:0c)
> Internet Protocol Version 6, Src: fe80::d07c:2340:59f:954, Dst: ff02::c
> User Datagram Protocol, Src Port: 54442, Dst Port: 1900
> Simple Service Discovery Protocol
```

```
M-SEARCH * HTTP/1.1
Host:[FF02::C]:1900
ST:urn:Microsoft Windows Peer Name Resolution Protocol: V4:IPV6:LinkLocal
Man:"ssdp:discover"
MX:3

M-SEARCH * HTTP/1.1
Host:[FF02::C]:1900
ST:urn:Microsoft Windows Peer Name Resolution Protocol: V4:IPV6:LinkLocal
Man:"ssdp:discover"
MX:3

M-SEARCH * HTTP/1.1
Host:[FF02::C]:1900
ST:urn:Microsoft Windows Peer Name Resolution Protocol: V4:IPV6:LinkLocal
Man:"ssdp:discover"
MX:3

M-SEARCH * HTTP/1.1
Host:[FF02::C]:1900
ST:urn:Microsoft Windows Peer Name Resolution Protocol: V4:IPV6:LinkLocal
Man:"ssdp:discover"
MX:3

M-SEARCH * HTTP/1.1
Host:[FF02::C]:1900
ST:urn:Microsoft Windows Peer Name Resolution Protocol: V4:IPV6:LinkLocal
Man:"ssdp:discover"
MX:3

M-SEARCH * HTTP/1.1
Host:[FF02::C]:1900
ST:urn:Microsoft Windows Peer Name Resolution Protocol: V4:IPV6:LinkLocal
Man:"ssdp:discover"
MX:3

M-SEARCH * HTTP/1.1
Host:[FF02::C]:1900
```



- What service and port were targeted? svchost.exe (source 54442) (destination 1999)
- Was the attacker able to access a sensitive file at the machine you are auditing? Mitre ATT&ACK Technique - T1570 Yes



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

- The attacker try to access to the machine using initial IP 10.0.2.6
-
- Block the attacker IP and block the incoming traffic using firewall
- Change the password
- Backup the date and 1 production copy plus 2 additional backup copies

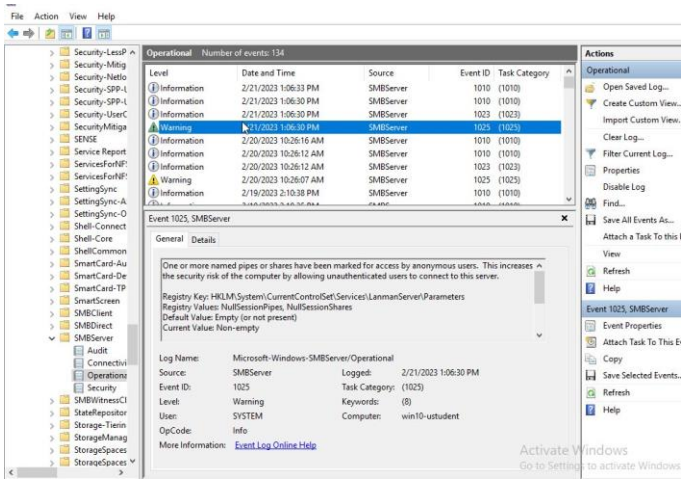
- Save the backup in unconnected device with the internet

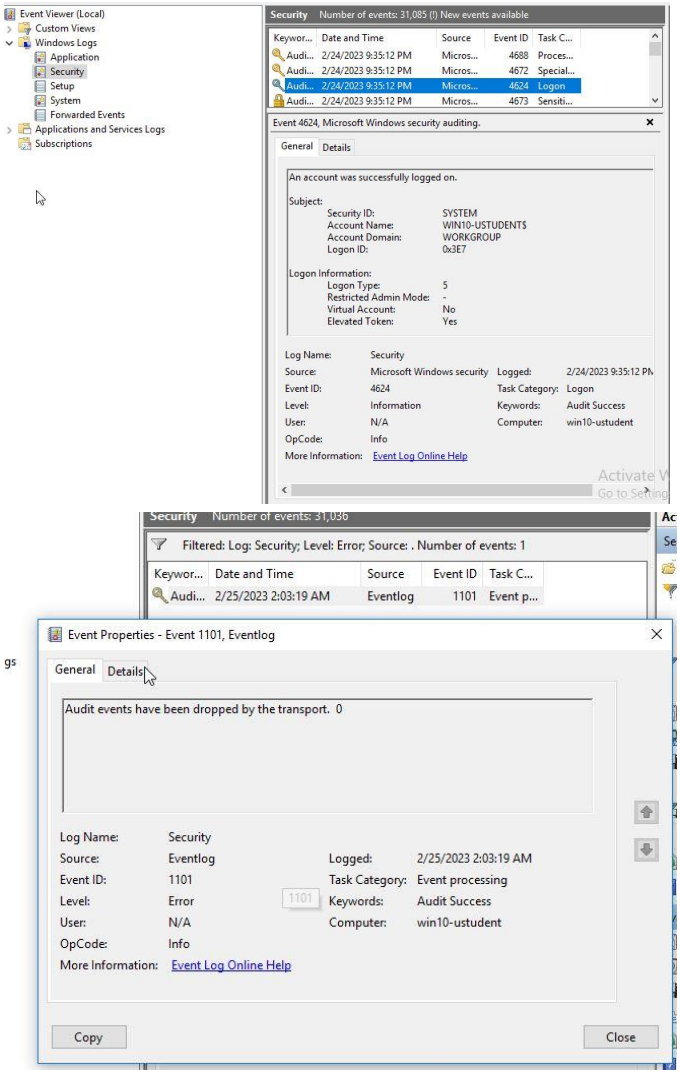
Task 3

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.
- The account name is (nobody)

```
 ses=4294967295 msg='op=PAM:setcred acct="nobody" exe="/usr/sbin/smbd" hostname
=10.0.2.15 addr=10.0.2.15 terminal=smb/4000299702 res=success'
type=USER_END msg=audit(1601325702.325:11554): pid=31868 uid=0 auid=4294967295
ses=4294967295 msg='op=PAM:session_close acct="nobody" exe="/usr/sbin/smbd" hos
tname=10.0.2.15 addr=10.0.2.15 terminal=smb/4000299702 res=success'
type=CRED_DISP msg=audit(1601325702.793:11555): pid=31869 uid=0 auid=4294967295
 ses=4294967295 msg='op=PAM:setcred acct="nobody" exe="/usr/sbin/smbd" hostname
=10.0.2.15 addr=10.0.2.15 terminal=smb/3929809160 res=success'
type=USER_END msg=audit(1601325702.809:11556): pid=31869 uid=0 auid=4294967295
ses=4294967295 msg='op=PAM:session_close acct="nobody" exe="/usr/sbin/smbd" hos
tname=10.0.2.15 addr=10.0.2.15 terminal=smb/3929809160 res=success'
type=CRED_DISP msg=audit(1601325703.313:11557): pid=31870 uid=0 auid=4294967295
 ses=4294967295 msg='op=PAM:setcred acct="nobody" exe="/usr/sbin/smbd" hostname
=10.0.2.15 addr=10.0.2.15 terminal=smb/1198747403 res=success'
type=USER_END msg=audit(1601325703.313:11558): pid=31870 uid=0 auid=4294967295
ses=4294967295 msg='op=PAM:session_close acct="nobody" exe="/usr/sbin/smbd" hos
tname=10.0.2.15 addr=10.0.2.15 terminal=smb/1198747403 res=success'
type=CRED_DISP msg=audit(1601325703.797:11559): pid=31871 uid=0 auid=4294967295
 ses=4294967295 msg='op=PAM:setcred acct="nobody" exe="/usr/sbin/smbd" hostname
=10.0.2.15 addr=10.0.2.15 terminal=smb/1450745416 res=success'
type=USER_END msg=audit(1601325703.797:11560): pid=31871 uid=0 auid=4294967295
ses=4294967295 msg='op=PAM:session_close acct="nobody" exe="/usr/sbin/smbd" hos
tname=10.0.2.15 addr=10.0.2.15 terminal=smb/1450745416 res=success'
type=CRED_DISP msg=audit(1601325704.305:11561): pid=31872 uid=0 auid=4294967295
 ses=4294967295 msg='op=PAM:setcred acct="nobody" exe="/usr/sbin/smbd" hostname
=10.0.2.15 addr=10.0.2.15 terminal=smb/423502041 res=success'
type=USER_END msg=audit(1601325704.305:11562): pid=31872 uid=0 auid=4294967295
ses=4294967295 msg='op=PAM:session_close acct="nobody" exe="/usr/sbin/smbd" hos
tname=10.0.2.15 addr=10.0.2.15 terminal=smb/423502041 res=success'
```

```
g='op=PAM:setcred acct="ustudent" exe="/usr/lib/gdm3/gdm-session-worker" hostna
me=ubu-ustudent addr=? terminal=/dev/tty1 res=success'
type=USER_AUTH msg=audit(1677393484.829:199): pid=2553 uid=0 auid=1000 ses=1 ms
g='op=PAM:authentication acct="ustudent" exe="/usr/lib/gdm3/gdm-session-worker"
 hostname=ubu-ustudent addr=? terminal=/dev/tty1 res=success'
type=USER_ACCT msg=audit(1677393484.829:200): pid=2553 uid=0 auid=1000 ses=1 ms
g='op=PAM:accounting acct="ustudent" exe="/usr/lib/gdm3/gdm-session-worker" hos
tname=ubu-ustudent addr=? terminal=/dev/tty1 res=success'
type=CRED_REFR msg=audit(1677393484.841:201): pid=2553 uid=0 auid=1000 ses=1 ms
g='op=PAM:setcred acct="ustudent" exe="/usr/lib/gdm3/gdm-session-worker" hostna
me=ubu-ustudent addr=? terminal=/dev/tty1 res=success'
type=USER_AUTH msg=audit(1677393532.689:202): pid=2569 uid=1000 auid=1000 ses=2
 msg='op=PAM:authentication acct="ustudent" exe="/usr/bin/sudo" hostname=? addr
=? terminal=/dev/pts/0 res=success'
type=USER_ACCT msg=audit(1677393532.689:203): pid=2569 uid=1000 auid=1000 ses=2
 msg='op=PAM:accounting acct="ustudent" exe="/usr/bin/sudo" hostname=? addr=? t
erminal=/dev/pts/0 res=success'
type=USER_ACCT msg=audit(1677393781.608:208): pid=2856 uid=0 auid=4294967295 se
s=4294967295 msg='op=PAM:accounting acct="root" exe="/usr/sbin/cron" hostname=?
 addr=? terminal=cron res=success'
type=CRED_ACQ msg=audit(1677393781.624:209): pid=2856 uid=0 auid=4294967295 ses
=4294967295 msg='op=PAM:setcred acct="root" exe="/usr/sbin/cron" hostname=? add
r=? terminal=cron res=success'
type=USER_START msg=audit(1677393781.668:211): pid=2856 uid=0 auid=0 ses=4 msg=
'op=PAM:session_open acct="root" exe="/usr/sbin/cron" hostname=? addr=? termina
l=cron res=success'
type=CRED_DISP msg=audit(1677393781.736:212): pid=2856 uid=0 auid=0 ses=4 msg='
op=PAM:setcred acct="root" exe="/usr/sbin/cron" hostname=? addr=? terminal=cron
 res=success'
```

```
ustudent@ubu-ustudent:~$ grep "authentication failure" /var/log/auth.log
Feb 26 18:06:39 ubu-ustudent sudo: ustudent : TTY=pts/0 ; PWD=/home/ustudent ;
USER=root ; COMMAND=/bin/grep authentication failure /var/log/auth.log
Feb 26 18:07:39 ubu-ustudent sudo: ustudent : TTY=pts/0 ; PWD=/home/ustudent ;
USER=root ; COMMAND=/bin/grep authentication failure
Feb 26 18:09:41 ubu-ustudent sudo: ustudent : TTY=pts/0 ; PWD=/home/ustudent ;
USER=root ; COMMAND=/bin/grep authentication failure /var/log/auth.log
ustudent@ubu-ustudent:~$ sudo lastb
[sudo] password for ustudent:

btmp begins Sun Feb 26 18:01:12 2023
ustudent@ubu-ustudent:~$ sudo last

wtmp begins Sun Feb 26 18:01:12 2023
```

```
ustudent@ubu-ustudent:~$ whois 10.0.2.7

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2023, American Registry for Internet Numbers, Ltd.
#


NetRange:       10.0.0.0 - 10.255.255.255
CIDR:           10.0.0.0/8
NetName:        PRIVATE-ADDRESS-ABLK-RFC1918-IANA-RESERVED
NetHandle:      NET-10-0-0-0-1
Parent:          ()
NetType:        IANA Special Use
OriginAS:
Organization:   Internet Assigned Numbers Authority (IANA)
RegDate:
Updated:        2013-08-30
Comment:        These addresses are in use by many millions of independently op
erated networks, which might be as small as a single computer connected to a ho
me gateway, and are automatically configured in hundreds of millions of devices
.  They are only intended for use within a private context  and traffic that ne
eds to cross the Internet will need to use a different, unique address.
Comment:


OrgName:        Internet Assigned Numbers Authority
OrgId:          IANA
Address:        12025 Waterfront Drive
Address:        Suite 300
City:           Los Angeles
StateProv:      CA
PostalCode:     90292
Country:        US
RegDate:
Updated:        2012-08-31
Ref:            https://rdap.arin.net/registry/entity/IANA


OrgTechHandle: IANA-IP-ARIN
OrgTechName:   ICANN
OrgTechPhone:  +1-310-301-5820
OrgTechEmail:  abuse@iana.org
OrgTechRef:    https://rdap.arin.net/registry/entity/IANA-IP-ARIN

OrgAbuseHandle: IANA-IP-ARIN
OrgAbuseName:   ICANN
OrgAbusePhone:  +1-310-301-5820
OrgAbuseEmail:  abuse@iana.org
OrgAbuseRef:    https://rdap.arin.net/registry/entity/IANA-IP-ARIN
```

```
ustudent@ubu-ustudent:/etc/ssh$ sudo grep "sshd.*Failed" /var/log/auth.log
Feb 26 18:51:46 ubu-ustudent sudo: ustudent : TTY=pts/0 ; PWD=/etc/ssh ; USER=r
oot ; COMMAND=/bin/grep sshd.*Failed /var/log/auth.log
ustudent@ubu-ustudent:/etc/ssh$
```

```
root@ubu-ustudent:/var/log# cat auth.log | grep 10.0.2.7
Sep 27 15:52:35 ubu-ustudent sshd[5356]: pam_unix(sshd:auth): authentication fa
ilure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.0.2.7  user=root
Sep 27 15:52:37 ubu-ustudent sshd[5356]: Failed password for root from 10.0.2.7
 port 49474 ssh2
Sep 27 15:52:57 ubu-ustudent sshd[5356]: Connection closed by authenticating us
er root 10.0.2.7 port 49474 [preauth]
Sep 27 15:53:06 ubu-ustudent sshd[5358]: Invalid user attacker from 10.0.2.7 po
rt 49476
Sep 27 15:53:12 ubu-ustudent sshd[5358]: pam_unix(sshd:auth): authentication fa
ilure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.0.2.7
Sep 27 15:53:15 ubu-ustudent sshd[5358]: Failed password for invalid user attac
ker from 10.0.2.7 port 49476 ssh2
Sep 27 15:53:22 ubu-ustudent sshd[5358]: Failed password for invalid user attac
ker from 10.0.2.7 port 49476 ssh2
Sep 27 15:53:33 ubu-ustudent sshd[5358]: Failed password for invalid user attac
ker from 10.0.2.7 port 49476 ssh2
Sep 27 15:53:33 ubu-ustudent sshd[5358]: Connection closed by invalid user atta
cker 10.0.2.7 port 49476 [preauth]
Sep 27 15:53:33 ubu-ustudent sshd[5358]: PAM 2 more authentication failures; lo
gname= uid=0 euid=0 tty=ssh ruser= rhost=10.0.2.7
Sep 27 15:54:40 ubu-ustudent login[5370]: pam_unix(login:auth): authentication
failure; logname= uid=0 euid=0 tty=/dev/pts/1 ruser= rhost=10.0.2.7
Sep 27 15:54:43 ubu-ustudent login[5370]: FAILED LOGIN (1) on '/dev/pts/1' from
 '10.0.2.7' FOR 'UNKNOWN', User not known to the underlying authentication modu
le
Sep 27 15:54:51 ubu-ustudent login[5370]: FAILED LOGIN (2) on '/dev/pts/1' from
 '10.0.2.7' FOR 'UNKNOWN', User not known to the underlying authentication modu
le
```

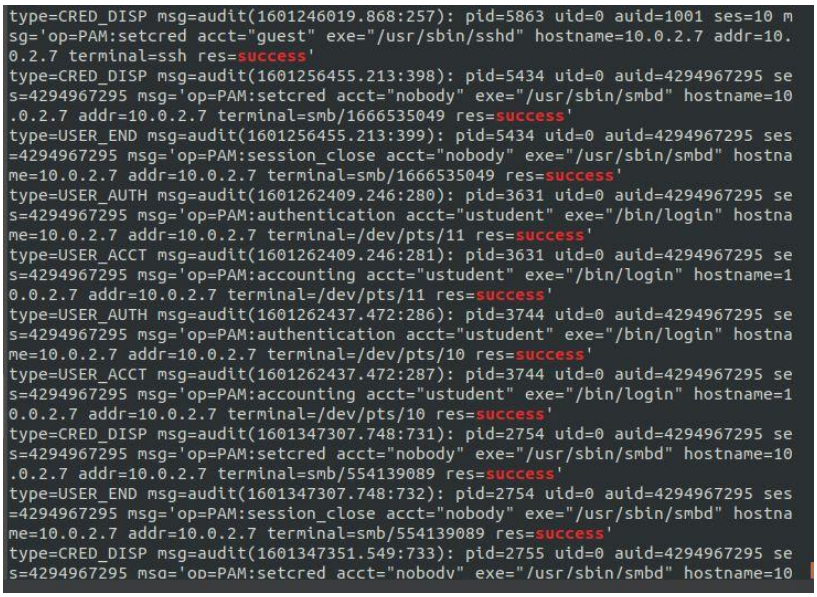
```
 '10.0.2.7' FOR 'UNKNOWN', User not known to the underlying authentication modu
le
Sep 27 15:54:54 ubu-ustudent login[5370]: pam_unix(login:auth): authentication
failure; logname= uid=0 euid=0 tty=/dev/pts/1 ruser= rhost=10.0.2.7
Sep 27 15:54:58 ubu-ustudent login[5370]: FAILED LOGIN (3) on '/dev/pts/1' from
 '10.0.2.7' FOR 'UNKNOWN', User not known to the underlying authentication modu
le
Sep 27 15:55:03 ubu-ustudent login[5370]: pam_unix(login:auth): authentication
failure; logname= uid=0 euid=0 tty=/dev/pts/1 ruser= rhost=10.0.2.7
Sep 27 15:55:06 ubu-ustudent login[5370]: FAILED LOGIN (4) on '/dev/pts/1' from
 '10.0.2.7' FOR 'UNKNOWN', User not known to the underlying authentication modu
le
Sep 27 18:22:58 ubu-ustudent sshd[5863]: pam_unix(sshd:auth): authentication fa
ilure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.0.2.7  user=guest
Sep 27 18:23:00 ubu-ustudent sshd[5863]: Failed password for guest from 10.0.2.
7 port 49510 ssh2
Sep 27 18:23:05 ubu-ustudent sshd[5863]: Accepted password for guest from 10.0.
2.7 port 49510 ssh2
Sep 27 23:06:47 ubu-ustudent login[3575]: pam_unix(login:auth): authentication
failure; logname= uid=0 euid=0 tty=/dev/pts/11 ruser= rhost=10.0.2.7
Sep 27 23:06:47 ubu-ustudent login[3577]: pam_unix(login:auth): authentication
failure; logname= uid=0 euid=0 tty=/dev/pts/14 ruser= rhost=10.0.2.7
Sep 27 23:06:47 ubu-ustudent login[3583]: pam_unix(login:auth): authentication
failure; logname= uid=0 euid=0 tty=/dev/pts/9 ruser= rhost=10.0.2.7
Sep 27 23:06:47 ubu-ustudent login[3582]: pam_unix(login:auth): authentication
failure; logname= uid=0 euid=0 tty=/dev/pts/12 ruser= rhost=10.0.2.7
Sep 27 23:06:47 ubu-ustudent login[3584]: pam_unix(login:auth): authentication
failure; logname= uid=0 euid=0 tty=/dev/pts/15 ruser= rhost=10.0.2.7
Sep 27 23:06:47 ubu-ustudent login[3586]: pam_unix(login:auth): authentication
```

```
ustudent@ubu-ustudent:~$ sudo aureport --failed -ts yesterday
[sudo] password for ustudent:

Failed Summary Report
======================
Range of time in logs: 02/26/2023 01:15:23.367 - 02/26/2023 01:20:45.340
Selected time for report: 02/25/2023 00:00:00 - 02/26/2023 01:20:45.340
Number of changes in configuration: 0
Number of changes to accounts, groups, or roles: 2
Number of logins: 0
Number of failed logins: 0
Number of authentications: 0
Number of failed authentications: 6
Number of users: 2
Number of terminals: 3
Number of host names: 2
Number of executables: 3
Number of commands: 1
Number of files: 0
Number of AVC's: 0
Number of MAC events: 0
Number of failed syscalls: 0
Number of anomaly events: 0
Number of responses to anomaly events: 0
Number of crypto events: 0
Number of integrity events: 0
Number of virt events: 0
Number of keys: 0
Number of process IDs: 5
```

```
root@ubu-ustudent:/etc/audit# cat auditd.conf
#
# This file controls the configuration of the audit daemon
#

local_events = yes
write_logs = yes
log_file = /var/log/audit/audit.log
log_group = adm
log_format = RAW
flush = INCREMENTAL_ASYNC
freq = 50
max_log_file = 8
num_logs = 5
priority_boost = 4
disp_qos = lossy
dispatcher = /sbin/audispd
name_format = NONE
##name = mydomain
max_log_file_action = ROTATE
space_left = 75
space_left_action = SYSLOG
verify_email = yes
action_mail_acct = root
admin_space_left = 50
admin_space_left_action = SUSPEND
disk_full_action = SUSPEND
disk_error_action = SUSPEND
use_libwrap = yes
```

```
root@ubu-ustudent:/var/log/audit# cat audit.log | grep 10.0.2.7
type=USER_AUTH msg=audit(1601236357.783:61): pid=5356 uid=0 auid=4294967295 ses=4294967295 msg='op=PAM:a
uthentication acct="root" exe="/usr/sbin/sshd" hostname=10.0.2.7 addr=10.0.2.7 terminal=ssh res=failed'
type=USER_LOGIN msg=audit(1601236357.787:62): pid=5356 uid=0 auid=4294967295 ses=4294967295 msg='op=logi
n acct="root" exe="/usr/sbin/sshd" hostname=? addr=10.0.2.7 terminal=sshd res=failed'
type=USER_LOGIN msg=audit(1601236386.155:63): pid=5358 uid=0 auid=4294967295 ses=4294967295 msg='op=logi
n acct=28756E6B6E6F776E207573657229 exe="/usr/sbin/sshd" hostname=? addr=10.0.2.7 terminal=sshd res=fail
ed'
type=USER_LOGIN msg=audit(1601236386.155:64): pid=5358 uid=0 auid=4294967295 ses=4294967295 msg='op=logi
n acct=28696E76616C6964207573657229 exe="/usr/sbin/sshd" hostname=? addr=10.0.2.7 terminal=sshd res=fail
ed'
type=USER_AUTH msg=audit(1601236395.139:65): pid=5358 uid=0 auid=4294967295 ses=4294967295 msg='op=PAM:a
uthentication acct="attacker" exe="/usr/sbin/sshd" hostname=10.0.2.7 addr=10.0.2.7 terminal=ssh res=fail
ed'
type=USER_LOGIN msg=audit(1601236395.139:66): pid=5358 uid=0 auid=4294967295 ses=4294967295 msg='op=logi
n acct=28696E76616C6964207573657229 exe="/usr/sbin/sshd" hostname=? addr=10.0.2.7 terminal=sshd res=fail
ed'
type=USER_AUTH msg=audit(1601236402.187:67): pid=5358 uid=0 auid=4294967295 ses=4294967295 msg='op=PAM:a
uthentication acct="attacker" exe="/usr/sbin/sshd" hostname=10.0.2.7 addr=10.0.2.7 terminal=ssh res=fail
ed'
type=USER_LOGIN msg=audit(1601236402.187:68): pid=5358 uid=0 auid=4294967295 ses=4294967295 msg='op=logi
n acct=28696E76616C6964207573657229 exe="/usr/sbin/sshd" hostname=? addr=10.0.2.7 terminal=sshd res=fail
ed'
type=USER_AUTH msg=audit(1601236413.135:69): pid=5358 uid=0 auid=4294967295 ses=4294967295 msg='op=PAM:a
uthentication acct="attacker" exe="/usr/sbin/sshd" hostname=10.0.2.7 addr=10.0.2.7 terminal=ssh res=fail
ed'
type=USER_LOGIN msg=audit(1601236413.135:70): pid=5358 uid=0 auid=4294967295 ses=4294967295 msg='op=logi
n acct=28696E76616C6964207573657229 exe="/usr/sbin/sshd" hostname=? addr=10.0.2.7 terminal=sshd res=fail
ed'
type=USER_AUTH msg=audit(1601236483.131:73): pid=5370 uid=0 auid=4294967295 ses=4294967295 msg='op=PAM:a
uthentication acct="?" exe="/bin/login" hostname=10.0.2.7 addr=10.0.2.7 terminal=/dev/pts/1 res=failed'
type=USER_LOGIN msg=audit(1601236483.131:74): pid=5370 uid=0 auid=4294967295 ses=4294967295 msg='op=logi
n acct="UNKNOWN" exe="/bin/login" hostname=10.0.2.7 addr=10.0.2.7 terminal=/dev/pts/1 res=failed'
type=USER_AUTH msg=audit(1601236491.843:75): pid=5370 uid=0 auid=4294967295 ses=4294967295 msg='op=PAM:a
uthentication acct="?" exe="/bin/login" hostname=10.0.2.7 addr=10.0.2.7 terminal=/dev/pts/1 res=failed'
type=USER_LOGIN msg=audit(1601236491.843:76): pid=5370 uid=0 auid=4294967295 ses=4294967295 msg='op=logi
n acct="UNKNOWN" exe="/bin/login" hostname=10.0.2.7 addr=10.0.2.7 terminal=/dev/pts/1 res=failed'
type=USER_AUTH msg=audit(1601236497.991:77): pid=5370 uid=0 auid=4294967295 ses=4294967295 msg='op=PAM:a
```

```
root@ubu-ustudent:/var/log/audit# cat audit.log | grep 10.0.2.7 | grep success
type=USER_AUTH msg=audit(1601245384.995:204): pid=5863 uid=0 auid=4294967295 se
s=4294967295 msg='op=PAM:authentication acct="guest" exe="/usr/sbin/sshd" hostn
ame=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 se
s=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 ad
dr=10.0.2.7 terminal=ssh res=success'
type=CRED_ACQ msg=audit(1601245386.779:213): pid=5970 uid=0 auid=1001 ses=10 ms
g='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_LOGIN msg=audit(1601245386.823:214): pid=5863 uid=0 auid=1001 ses=10
msg='op=login id=1001 exe="/usr/sbin/sshd" hostname=10.0.2.7 addr=10.0.2.7 term
inal=/dev/pts/2 res=success'
type=USER_END msg=audit(1601246019.868:256): pid=5863 uid=0 auid=1001 ses=10 ms
g='op=PAM:session_close acct="guest" exe="/usr/sbin/sshd" hostname=10.0.2.7 add
r=10.0.2.7 terminal=ssh res=success'
type=CRED_DISP msg=audit(1601246019.868:257): pid=5863 uid=0 auid=1001 ses=10 m
sg='op=PAM:setcred 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(1601256455.213:398): pid=5434 uid=0 auid=4294967295 se
s=4294967295 msg='op=PAM:setcred acct="nobody" exe="/usr/sbin/smbd" hostname=10
```



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.

- Windows
  - Attacker try using svc (The Service Host (svchost.exe) is a shared-service process that Windows uses to load DLL files.)
  - Should change the password
  - Update the svc application and patch the security update
  - Prevent the attacker IP and configure the firewall
  - Give access to the authorized user only

- Ubuntu
  - Attacker try using the ssh connection to access
  - Should change the password
  - Update the ssh application and patch the security update
  - Prevent the attacker IP and configure the firewall
  - Give access to the authorized user only

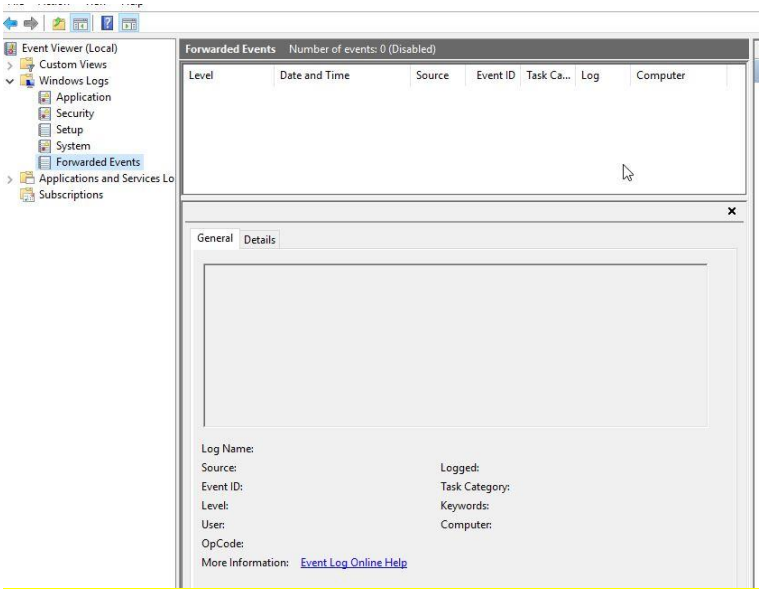
Task 4

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.

Ubuntu

```
ustudent@ubu-ustudent:~$ systemctl status rsyslog
● rsyslog.service - System Logging Service
   Loaded: loaded (/lib/systemd/system/rsyslog.service; enabled; vendor preset:
   Active: active (running) since Wed 2023-02-22 03:56:28 EST; 3min 26s ago
     Docs: man:rsyslogd(8)
           http://www.rsyslog.com/doc/
 Main PID: 684 (rsyslogd)
    Tasks: 4 (limit: 1113)
   CGroup: /system.slice/rsyslog.service
           └─684 /usr/sbin/rsyslogd -n

Feb 22 03:56:26 ubu-ustudent systemd[1]: Starting System Logging Service...
Feb 22 03:56:26 ubu-ustudent rsyslogd[684]: imuxsock: Acquired UNIX socket '/ru
Feb 22 03:56:26 ubu-ustudent rsyslogd[684]: rsyslogd's groupid changed to 106
Feb 22 03:56:26 ubu-ustudent rsyslogd[684]: rsyslogd's userid changed to 102
Feb 22 03:56:26 ubu-ustudent rsyslogd[684]:  [origin software="rsyslogd" swVers
Feb 22 03:56:28 ubu-ustudent systemd[1]: Started System Logging Service.
lines 1-16/16 (END)
```

Windows



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

Ubuntu

```
 GNU nano 2.9.3                    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")
```

```
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
```

```
# 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

#
# Include all config files in /etc/rsyslog.d/
#
$IncludeConfig /etc/rsyslog.d/*.conf
```

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.

- Identify the specific features and capabilities that the SIEM must have to meet your organization's needs.
- Set up a centralized log collection system to aggregate and store logs from all relevant systems.
- Establish monitoring protocols and alert to ensure that the SIEM can detect and respond to security incidents in a timely and effective manner.

Step 4: Assess Authentication Management at Targeted Assets

Task 1

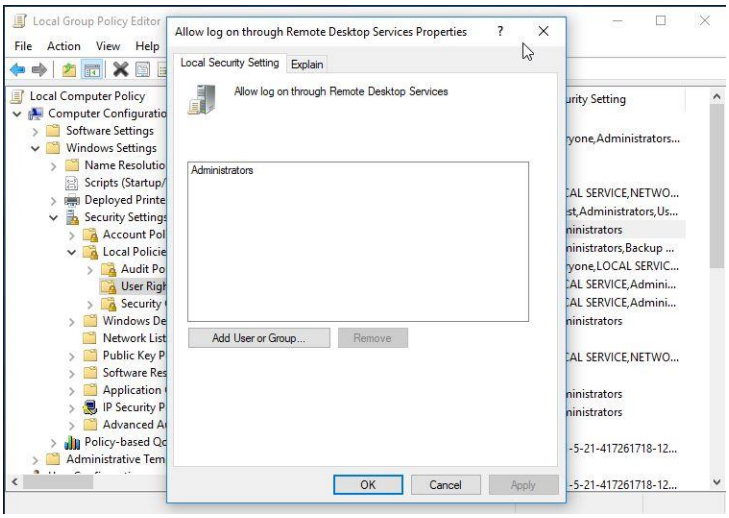
Evaluate the authentication management situation of StaticSpeed's systems. In our initial look at StaticSpeed, we discovered what is called a "FLAT" network. This means there are no either Active

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:

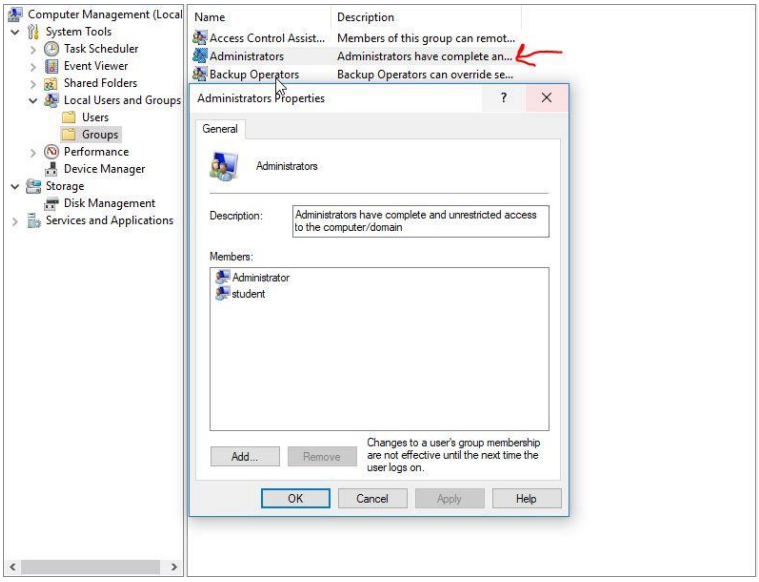
● Ensure only administrators can remotely access windows machines and verify if root access is permitted at the Linux host.




```
ustudent@ubu-ustudent:~$ grep PermitRootLogin /etc/ssh/sshd_config
#PermitRootLogin prohibit-password
# the setting of "PermitRootLogin without-password".
ustudent@ubu-ustudent:~$
```

```
# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

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

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile     .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
```

● Check for users with excessive permissions




```
ustudent@ubu-ustudent:/etc$ grep sudo /etc/group
sudo:x:27:ustudent
ustudent@ubu-ustudent:/etc$ groups ustudent
ustudent : ustudent adm cdrom sudo dip plugdev lpadmin sambashare
```

- Is root remote login allowed? No (prohibit-password)
- Are there users that should not have remote access via ssh in Linux?
    - Yes, there may be users who should not have remote access via SSH in Linux. For example, if a user does not require remote access to the system or should not have administrative privileges
- Remote Desktop Access should only be granted to administrators in Windows, are there other accounts that should not be given access?
    - In addition to non-administrative accounts, there may be other user accounts that should not be given Remote Desktop Access in Windows. These could include service accounts or accounts used for automated tasks or processes that do not require Remote Desktop

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.

- it is recommended to restrict remote access to only the accounts that require it for administration purposes. This can help reduce the attack surface of the system and improve overall security.
- In general, only accounts with administrative privileges should be allowed to log in remotely. Non-administrative accounts should be restricted from remote access to minimize the risk of unauthorized access or data breaches.

- It is also important to ensure that strong passwords are in place for all accounts that are allowed to log in remotely. Additionally, it is recommended to implement multi-factor authentication for remote access to further enhance security.

Task 2

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

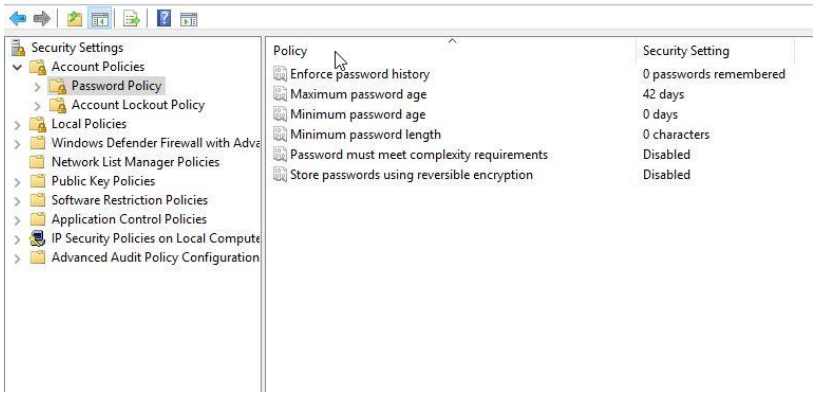
Audit the StaticSpeeds systems to verify that they comply with **CIS 5.3.1 Ubuntu**

```
ustudent@ubu-ustudent:~$ sudo grep minlen /etc/security/pwquality.conf
# minlen =14
ustudent@ubu-ustudent:~$ sudo grep minclass /etc/security/pwquality.conf
# minclass = 4
ustudent@ubu-ustudent:~$ sudo grep -E  [duol]credit /etc/security/pwquality.con
f
# dcredit = -1
# ucredit = -1
# lcredit = -1
# ocredit = -1
ustudent@ubu-ustudent:~$
```

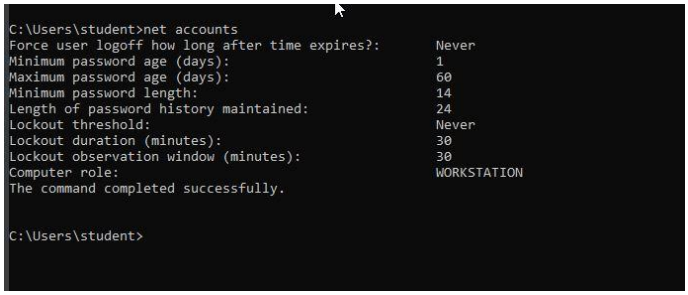
```
ustudent@ubu-ustudent:~$ sudo chage -l $(whoami)
Last password change                                    : Sep 26, 2020
Password expires                                        : never
Password inactive                                       : never
Account expires                                         : never
Minimum number of days between password change          : 0
Maximum number of days between password change          : 99999
Number of days of warning before password expires       : 7
ustudent@ubu-ustudent:~$
```

or **Windows 10 CIS benchmarks 1.1.5**?

before



After (should be like this)



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.

Windows

- password policies on the Windows system are not in compliance with best practices. Specifically, enforcing a minimum password age of 0 days and allowing passwords to be stored using reversible encryption are not recommended. Additionally, having a maximum password age of 42 days may not be sufficient for maintaining strong security.
- it is recommended to update the password policies on the Windows system to enforce a minimum password age of at least 1 day and to disable the storage of passwords using reversible encryption. Additionally, it may be beneficial to increase the maximum password age to a longer period, such as 90 or 180 days, to ensure that passwords are changed regularly.

Ubuntu

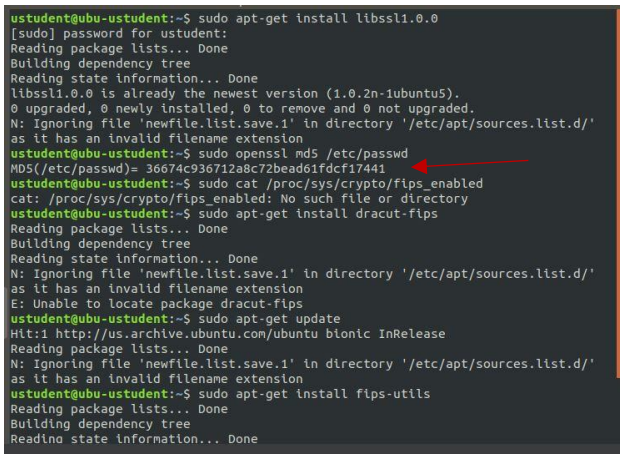
- the password policies appear to be in compliance with best practices. The password never expires, but the maximum and minimum number of days between password changes are set to reasonable values
- The warning period before password expiration is also set to a reasonable value to give users time to change their passwords before they expire.
- settings appear to be sufficient for maintaining strong security.

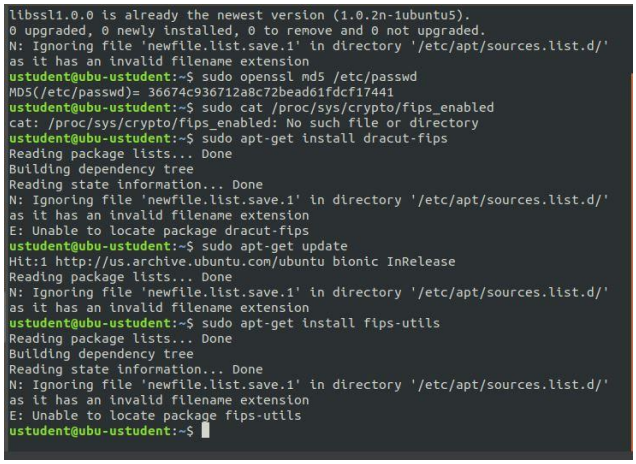
Task 3

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.

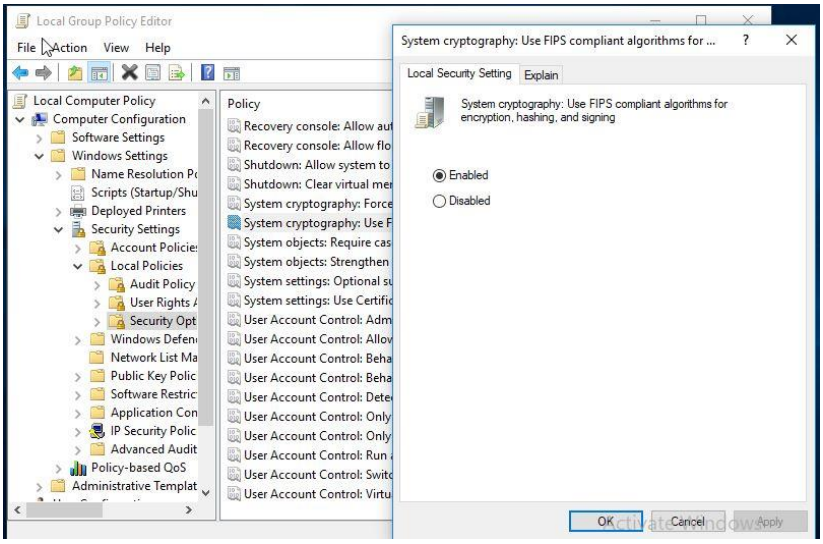
```
ustudent@ubu-ustudent:~$ sshd -T | grep ciphers
Could not load host key: /etc/ssh/ssh_host_rsa_key
Could not load host key: /etc/ssh/ssh_host_ecdsa_key
Could not load host key: /etc/ssh/ssh_host_ed25519_key
ciphers chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-g
cm@openssh.com,aes256-gcm@openssh.com
ustudent@ubu-ustudent:~$
```

- The use of "aes128-ctr", "aes192-ctr", and "aes256-ctr" encryption algorithms is compliant with FIPS 140-2 standards for cryptographic modules. Therefore, the use of these algorithms on Ubuntu 18.04 would be considered compliant with this specific requirement (CIS 5.2.13) of the CIS benchmark.





  - Ubuntu does not have native support for FIPS 140-2 but support md5 and "aes128-ctr", "aes192-ctr", and "aes256-ctr" encryption algorithms.
    - There are two options to make ubuntu18.04 v2.01 support FIPS 140-2
      - First upgrade ubuntu machine to the lasted version that support the FIPS 140-2
      - it is possible to configure FIPS 140-2 by building a custom kernel with FIPS 140-2 support and installing the necessary FIPS-compliant packages



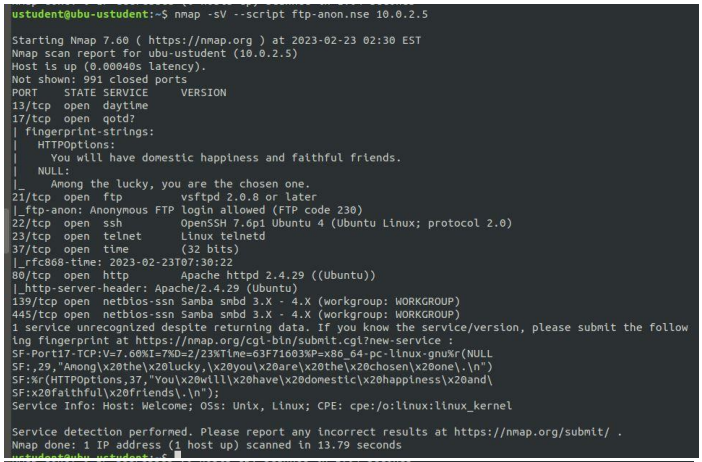
This option default value was disable but I am changed it to enable

- If the systems are found to be non-compliant, the recommendations for improvement would be to enable the FIPS compliant algorithms for encryption, hashing, and signing

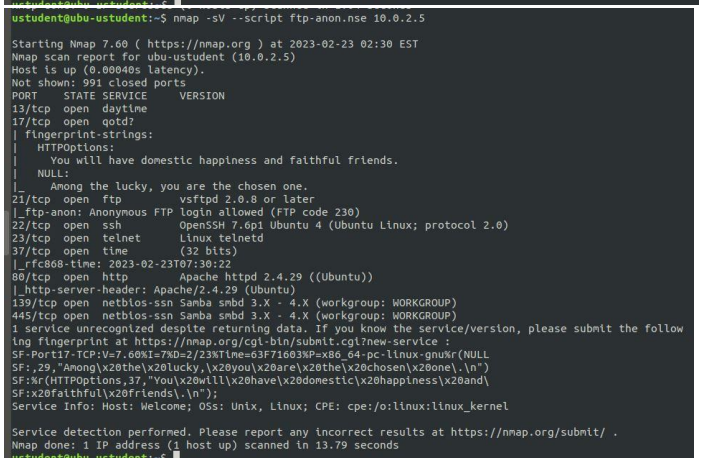
Task 4

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.

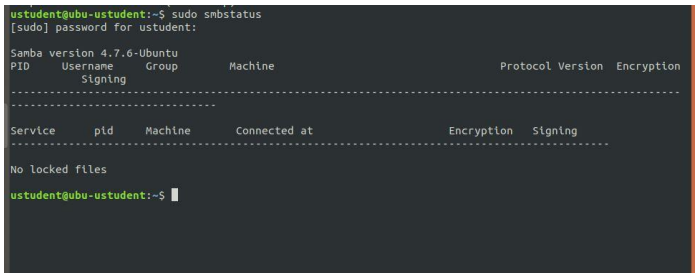
Please us an NSE Script to test Mitre ATT&CK T1110 in your Ubuntu virtual machine. Also,



```
ustudent@ubu-ustudent:~$ nmap -sV --script ftp-anon.nse 10.0.2.5

Starting Nmap 7.60 ( https://nmap.org ) at 2023-02-23 02:30 EST
Nmap scan report for ubu-ustudent (10.0.2.5)
Host is up (0.00040s latency).
Not shown: 991 closed ports
PORT    STATE SERVICE     VERSION
13/tcp  open  daytime
17/tcp  open  qotd?
| fingerprint-strings:
|   HTTPOptions:
|     You will have domestic happiness and faithful friends.
|   NULL:
|_    Among the lucky, you are the chosen one.
21/tcp  open  ftp         vsftpd 2.0.8 or later
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
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: 2023-02-23T07:30:22
80/tcp  open  http        Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
1 service unrecognized despite returning data. If you know the service/version, please submit the follow
ing fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port17-TCP:V=7.60%I=7%D=2/23%Time=63F71603%P=x86_64-pc-linux-gnu%r(NULL
SF:,29,"Among\x20the\x20lucky,\x20you\x20are\x20the\x20chosen\x20one\.\n")
SF:%r(HTTPOptions,37,"You\x20will\x20have\x20domestic\x20happiness\x20and\
SF:x20faithful\x20friends\.\n");
Service Info: Host: Welcome; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.79 seconds
```

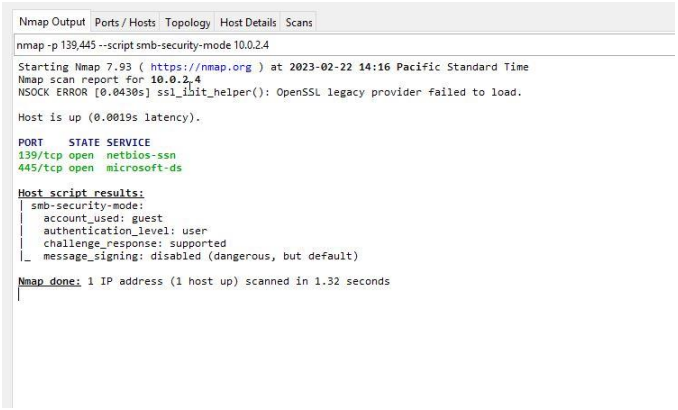


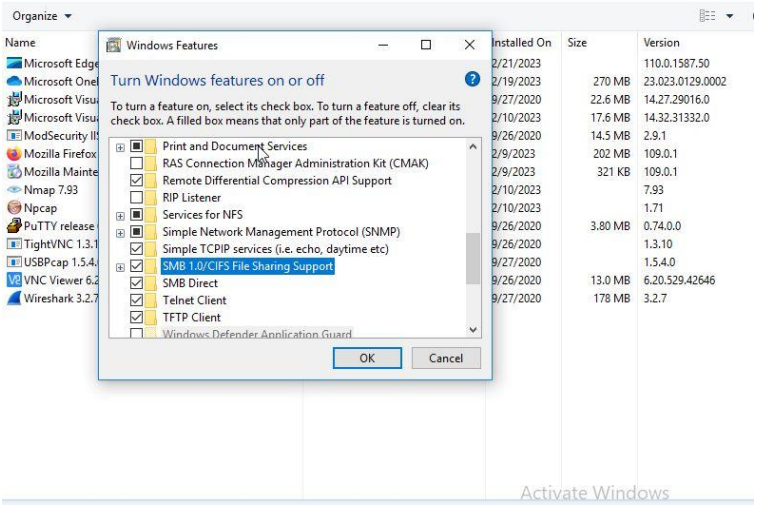
```
ustudent@ubu-ustudent:~$ nmap -sV --script ftp-anon.nse 10.0.2.5

Starting Nmap 7.60 ( https://nmap.org ) at 2023-02-23 02:30 EST
Nmap scan report for ubu-ustudent (10.0.2.5)
Host is up (0.00040s latency).
Not shown: 991 closed ports
PORT    STATE SERVICE     VERSION
13/tcp  open  daytime
17/tcp  open  qotd?
| fingerprint-strings:
|   HTTPOptions:
|     You will have domestic happiness and faithful friends.
|   NULL:
|_    Among the lucky, you are the chosen one.
21/tcp  open  ftp         vsftpd 2.0.8 or later
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
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: 2023-02-23T07:30:22
80/tcp  open  http        Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
1 service unrecognized despite returning data. If you know the service/version, please submit the follow
ing fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port17-TCP:V=7.60%I=7%D=2/23%Time=63F71603%P=x86_64-pc-linux-gnu%r(NULL
SF:,29,"Among\x20the\x20lucky,\x20you\x20are\x20the\x20chosen\x20one\.\n")
SF:%r(HTTPOptions,37,"You\x20will\x20have\x20domestic\x20happiness\x20and\
SF:x20faithful\x20friends\.\n");
Service Info: Host: Welcome; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.79 seconds
```



```
ustudent@ubu-ustudent:~$ sudo smbstatus
[sudo] password for ustudent:

Samba version 4.7.6-Ubuntu
PID     Username     Group        Machine                                   Protocol Version  Encryption
          Signing
----------------------------------------------------------------------------------------------------
--------------------------------

Service      pid     Machine       Connected at                     Encryption   Signing
---------------------------------------------------------------------------------------------

No locked files

ustudent@ubu-ustudent:~$
```

use an NSE Script to test the security mode of your SMB shares at your Windows virtual machine.





What are your findings?

- SMBv1

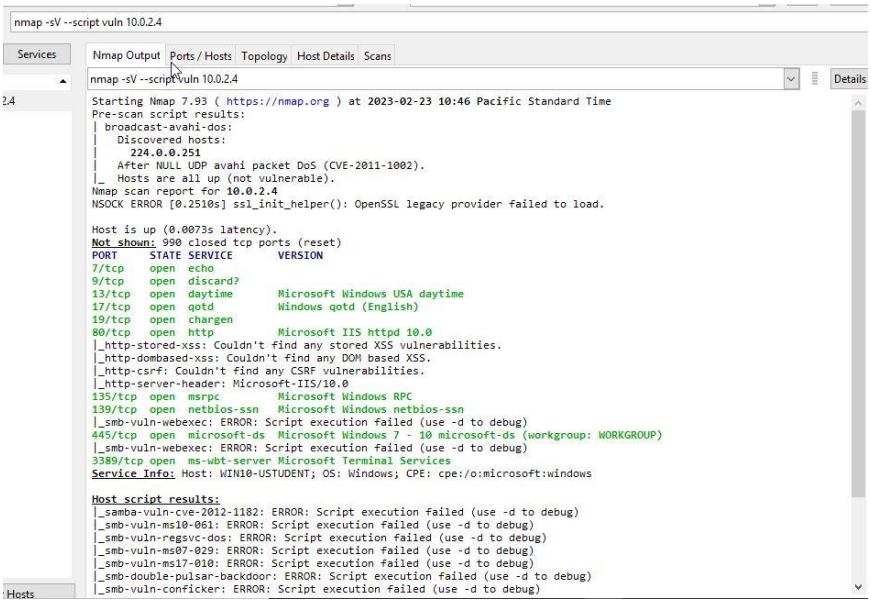
Please provide screenshots. Remember to give an explanation of the security state of these services based on your results.

- SMBv1: that is considered deprecated and insecure, and should be disabled if possible.

Ubuntu

- there are several known vulnerabilities and errors associated with the vsftpd version 2.0.8. Some of the known vulnerabilities include
  - The vsftpd version 2.0.8 was found to have a backdoor vulnerability in 2011, which allowed attackers to gain unauthorized access to the system. This vulnerability was fixed in later versions of vsftpd.
  - Vsftpd version 2.0.8 uses weak encryption algorithms, such as DES and MD5, which can be easily compromised by attackers.

Windows 10 ENT



Ex

Host	High	Medium	Low	Log
10.0.2.4	CVE 2011-1002	x	x	x

IP Address: 10.0.2.4

Service	Port	Sensitive Level
FTP (vsftpd)	21 TCP	High
xxx	xxx TCP	Medium
xxx	TCP	Low
xxx	xx TCP	Log

Expected detail format for vulnerabilities found

High

1- CVE-2011-1002 and or finding (7.5 out of 10)

Issue

The vulnerability is caused by a flaw in the way vsftpd handles certain FTP commands. An attacker can exploit this flaw by sending a specially crafted FTP command to the server, which can trigger a buffer overflow and allow the attacker to execute arbitrary code with the privileges of the vsftpd process.

Impact

An attacker can gain complete control of the vulnerable system by exploiting this vulnerability, which can lead to unauthorized access to sensitive data, disruption of services, and other malicious activities.

Mitigation

The vulnerability can be mitigated by upgrading to the latest version of vsftpd, which includes a patch for the vulnerability. Additionally, it is recommended to follow security best practices such as:

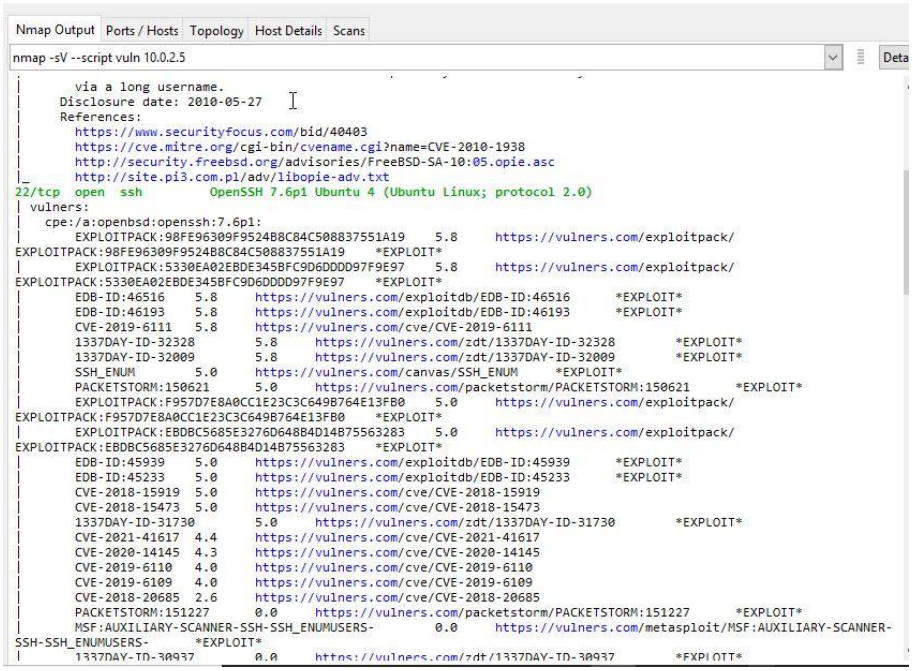
- Use strong passwords and authentication mechanisms.
- Use a firewall to restrict access to the FTP server.

Reference

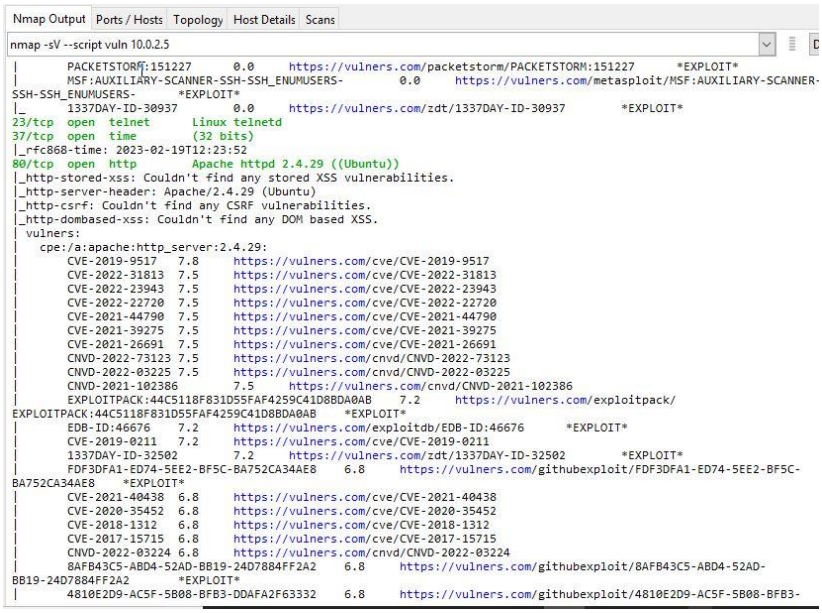
- https://nvd.nist.gov/vuln/detail/CVE-2011-1002
- https://www.exploit-db.com/exploits/17391
- https://securitytracker.com/id/1025117

Ubuntu 18.04

```
nmap -sV --script vuln 10.0.2.5

Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-19 14:22 Pacific Standard Time
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).
NSOCK ERROR [0.3460s] ssl_init_helper(): OpenSSL legacy provider failed to load.

Nmap scan report for 10.0.2.5
Host is up (0.011s latency).
Not shown: 991 closed tcp ports (reset)
PORT    STATE SERVICE     VERSION
13/tcp  open  daytime
17/tcp  open  nagios-nsca Nagios NSCA
21/tcp  open  ftp         vsftpd 2.0.8 or later
| ftp-libopie:
|   VULNERABLE:
|   OPIE off-by-one stack overflow
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2010-1938  BID:40403
|     Risk factor: High  CVSSv2: 9.3 (HIGH) (AV:N/AC:M/Au:N/C:C/I:C/A:C)
|       An off-by-one error in OPIE library 2.4.1-test1 and earlier, allows remote
|       attackers to cause a denial of service or possibly execute arbitrary code
|       via a long username.
|     Disclosure date: 2010-05-27
|     References:
|       https://www.securityfocus.com/bid/40403
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1938
|       http://security.freebsd.org/advisories/FreeBSD-SA-10:05.opie.asc
|_      http://site.pi3.com.pl/adv/libopie-adv.txt
22/tcp  open  ssh         OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:7.6p1:
|       EXPLOITPACK:98FE96309F9524B8C84C508837551A19    5.8     https://vulners.com/exploitpack/
EXPLOITPACK:98FE96309F9524B8C84C508837551A19    *EXPLOIT*
|       EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97    5.8     https://vulners.com/exploitpack/
EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97    *EXPLOIT*
|       EDB-ID:46516    5.8     https://vulners.com/exploitdb/EDB-ID:46516      *EXPLOIT*
```



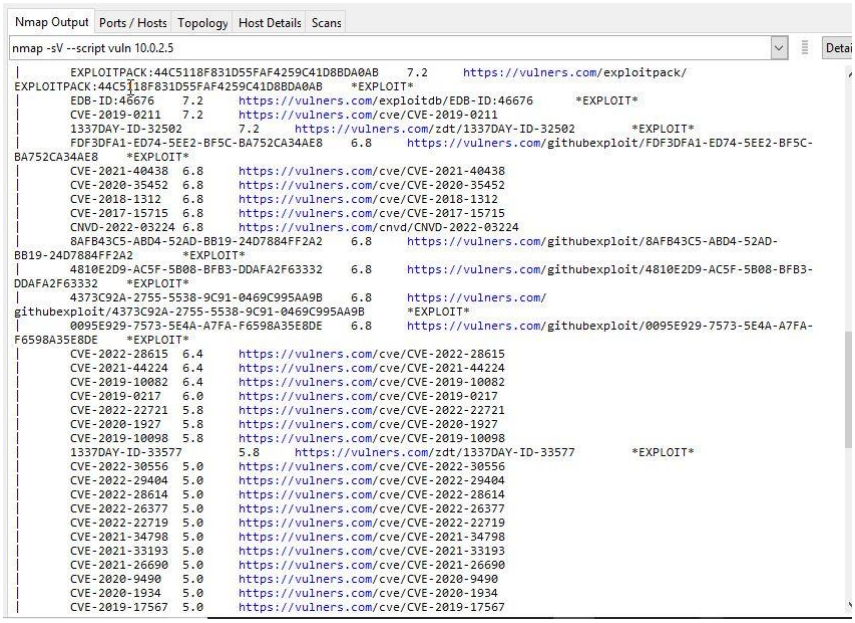
```
Nmap Output | Ports / Hosts | Topology | Host Details | Scans

nmap -sV --script vuln 10.0.2.5

|       via a long username.
|     Disclosure date: 2010-05-27
|     References:
|       https://www.securityfocus.com/bid/40403
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1938
|       http://security.freebsd.org/advisories/FreeBSD-SA-10:05.opie.asc
|_      http://site.pi3.com.pl/adv/libopie-adv.txt
22/tcp  open  ssh         OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:7.6p1:
|       EXPLOITPACK:98FE96309F9524B8C84C508837551A19    5.8     https://vulners.com/exploitpack/
EXPLOITPACK:98FE96309F9524B8C84C508837551A19    *EXPLOIT*
|       EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97    5.8     https://vulners.com/exploitpack/
EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97    *EXPLOIT*
|       EDB-ID:46516    5.8     https://vulners.com/exploitdb/EDB-ID:46516      *EXPLOIT*
|       EDB-ID:46193    5.8     https://vulners.com/exploitdb/EDB-ID:46193      *EXPLOIT*
|       CVE-2019-6111   5.8     https://vulners.com/cve/CVE-2019-6111
|       1337DAY-ID-32328        5.8     https://vulners.com/zdt/1337DAY-ID-32328        *EXPLOIT*
|       1337DAY-ID-32009        5.8     https://vulners.com/zdt/1337DAY-ID-32009        *EXPLOIT*
|       SSH_ENUM        5.0     https://vulners.com/canvas/SSH_ENUM     *EXPLOIT*
|       PACKETSTORM:150621      5.0     https://vulners.com/packetstorm/PACKETSTORM:150621      *EXPLOIT*
|       EXPLOITPACK:F957D7E8A0CC1E23C3C649B764E13FB0    5.0     https://vulners.com/exploitpack/
EXPLOITPACK:F957D7E8A0CC1E23C3C649B764E13FB0    *EXPLOIT*
|       EXPLOITPACK:EBDBC5685E3276D648B4D14B75563283    5.0     https://vulners.com/exploitpack/
EXPLOITPACK:EBDBC5685E3276D648B4D14B75563283    *EXPLOIT*
|       EDB-ID:45939    5.0     https://vulners.com/exploitdb/EDB-ID:45939      *EXPLOIT*
|       EDB-ID:45233    5.0     https://vulners.com/exploitdb/EDB-ID:45233      *EXPLOIT*
|       CVE-2018-15919  5.0     https://vulners.com/cve/CVE-2018-15919
|       CVE-2018-15473  5.0     https://vulners.com/cve/CVE-2018-15473
|       1337DAY-ID-31730        5.0     https://vulners.com/zdt/1337DAY-ID-31730        *EXPLOIT*
|       CVE-2021-41617  4.4     https://vulners.com/cve/CVE-2021-41617
|       CVE-2020-14145  4.3     https://vulners.com/cve/CVE-2020-14145
|       CVE-2019-6110   4.0     https://vulners.com/cve/CVE-2019-6110
|       CVE-2019-6109   4.0     https://vulners.com/cve/CVE-2019-6109
|       CVE-2018-20685  2.6     https://vulners.com/cve/CVE-2018-20685
|       PACKETSTORM:151227      0.0     https://vulners.com/packetstorm/PACKETSTORM:151227      *EXPLOIT*
|       MSF:AUXILIARY-SCANNER-SSH-SSH_ENUMUSERS-        0.0     https://vulners.com/metasploit/MSF:AUXILIARY-SCANNER-
SSH-SSH_ENUMUSERS-      *EXPLOIT*
|       1337DAY-ID-30937        0.0     https://vulners.com/zdt/1337DAY-ID-30937        *EXPLOIT*
```



Nmap Output | Ports / Hosts | Topology | Host Details | Scans

nmap -sV --script vuln 10.0.2.5

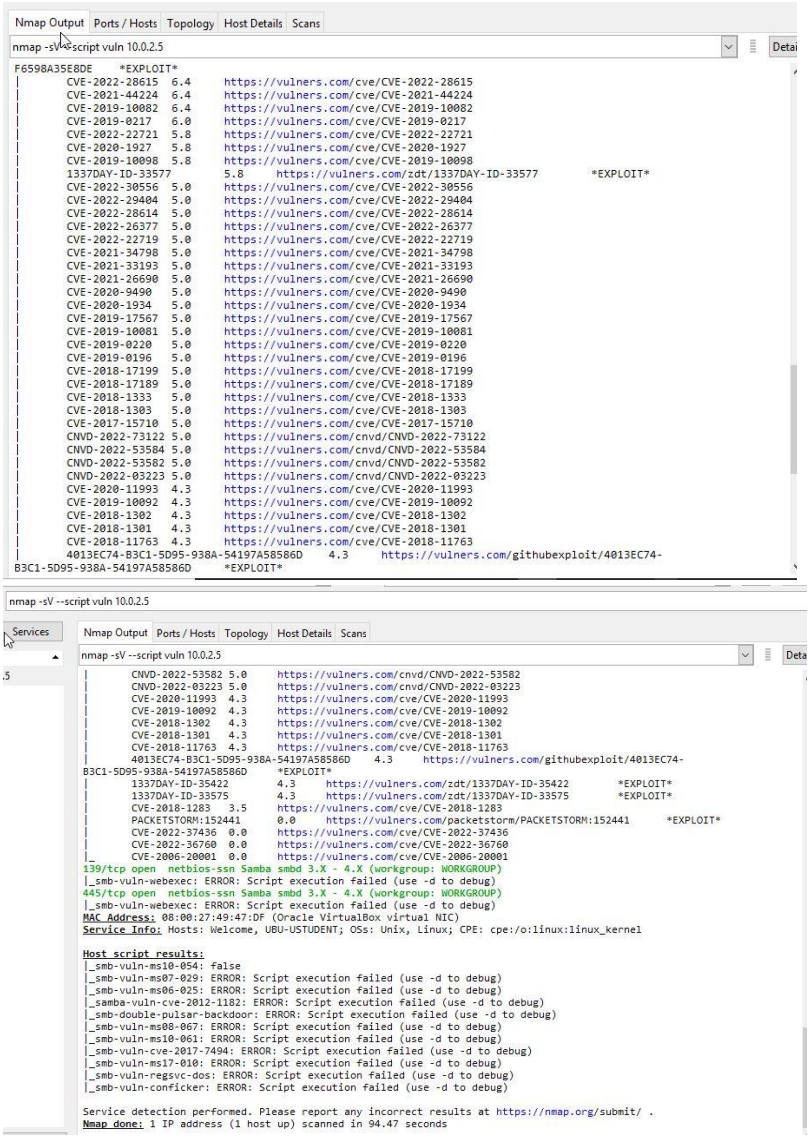
```
|       PACKETSTORM:151227      0.0     https://vulners.com/packetstorm/PACKETSTORM:151227      *EXPLOIT*
|       MSF:AUXILIARY-SCANNER-SSH-SSH_ENUMUSERS-       0.0     https://vulners.com/metasploit/MSF:AUXILIARY-SCANNER-
SSH-SSH_ENUMUSERS-      *EXPLOIT*
|_      1337DAY-ID-30937        0.0     https://vulners.com/zdt/1337DAY-ID-30937        *EXPLOIT*
23/tcp  open  telnet      Linux telnetd
37/tcp  open  time        (32 bits)
|_rfc868-time: 2023-02-19T12:23:52
80/tcp  open  http        Apache httpd 2.4.29 ((Ubuntu))
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| vulners:
|   cpe:/a:apache:http_server:2.4.29:
|       CVE-2019-9517   7.8     https://vulners.com/cve/CVE-2019-9517
|       CVE-2022-31813  7.5     https://vulners.com/cve/CVE-2022-31813
|       CVE-2022-23943  7.5     https://vulners.com/cve/CVE-2022-23943
|       CVE-2022-22720  7.5     https://vulners.com/cve/CVE-2022-22720
|       CVE-2021-44790  7.5     https://vulners.com/cve/CVE-2021-44790
|       CVE-2021-39275  7.5     https://vulners.com/cve/CVE-2021-39275
|       CVE-2021-26691  7.5     https://vulners.com/cve/CVE-2021-26691
|       CNVD-2022-73123 7.5     https://vulners.com/cnvd/CNVD-2022-73123
|       CNVD-2022-03225 7.5     https://vulners.com/cnvd/CNVD-2022-03225
|       CNVD-2021-102386        7.5     https://vulners.com/cnvd/CNVD-2021-102386
|       EXPLOITPACK:44C5118F831D55FAF4259C41D8BDA0AB    7.2     https://vulners.com/exploitpack/
EXPLOITPACK:44C5118F831D55FAF4259C41D8BDA0AB    *EXPLOIT*
|       EDB-ID:46676    7.2     https://vulners.com/exploitdb/EDB-ID:46676      *EXPLOIT*
|       CVE-2019-0211   7.2     https://vulners.com/cve/CVE-2019-0211
|       1337DAY-ID-32502        7.2     https://vulners.com/zdt/1337DAY-ID-32502        *EXPLOIT*
|       FDF3DFA1-ED74-5EE2-BF5C-BA752CA34AE8    6.8     https://vulners.com/githubexploit/FDF3DFA1-ED74-5EE2-BF5C-
BA752CA34AE8    *EXPLOIT*
|       CVE-2021-40438  6.8     https://vulners.com/cve/CVE-2021-40438
|       CVE-2020-35452  6.8     https://vulners.com/cve/CVE-2020-35452
|       CVE-2018-1312   6.8     https://vulners.com/cve/CVE-2018-1312
|       CVE-2017-15715  6.8     https://vulners.com/cve/CVE-2017-15715
|       CNVD-2022-03224 6.8     https://vulners.com/cnvd/CNVD-2022-03224
|       8AFB43C5-ABD4-52AD-BB19-24D7884FF2A2    6.8     https://vulners.com/githubexploit/8AFB43C5-ABD4-52AD-
BB19-24D7884FF2A2       *EXPLOIT*
|       4810E2D9-AC5F-5B08-BFB3-DDAFA2F63332    6.8     https://vulners.com/githubexploit/4810E2D9-AC5F-5B08-BFB3-
```



Nmap Output | Ports / Hosts | Topology | Host Details | Scans

nmap -sV --script vuln 10.0.2.5

```
|       EXPLOITPACK:44C5118F831D55FAF4259C41D8BDA0AB    7.2     https://vulners.com/exploitpack/
EXPLOITPACK:44C5118F831D55FAF4259C41D8BDA0AB    *EXPLOIT*
|       EDB-ID:46676    7.2     https://vulners.com/exploitdb/EDB-ID:46676      *EXPLOIT*
|       CVE-2019-0211   7.2     https://vulners.com/cve/CVE-2019-0211
|       1337DAY-ID-32502        7.2     https://vulners.com/zdt/1337DAY-ID-32502        *EXPLOIT*
|       FDF3DFA1-ED74-5EE2-BF5C-BA752CA34AE8    6.8     https://vulners.com/githubexploit/FDF3DFA1-ED74-5EE2-BF5C-
BA752CA34AE8    *EXPLOIT*
|       CVE-2021-40438  6.8     https://vulners.com/cve/CVE-2021-40438
|       CVE-2020-35452  6.8     https://vulners.com/cve/CVE-2020-35452
|       CVE-2018-1312   6.8     https://vulners.com/cve/CVE-2018-1312
|       CVE-2017-15715  6.8     https://vulners.com/cve/CVE-2017-15715
|       CNVD-2022-03224 6.8     https://vulners.com/cnvd/CNVD-2022-03224
|       8AFB43C5-ABD4-52AD-BB19-24D7884FF2A2    6.8     https://vulners.com/githubexploit/8AFB43C5-ABD4-52AD-
BB19-24D7884FF2A2       *EXPLOIT*
|       4810E2D9-AC5F-5B08-BFB3-DDAFA2F63332    6.8     https://vulners.com/githubexploit/4810E2D9-AC5F-5B08-BFB3-
DDAFA2F63332    *EXPLOIT*
|       4373C92A-2755-5538-9C91-0469C995AA9B    6.8     https://vulners.com/
githubexploit/4373C92A-2755-5538-9C91-0469C995AA9B      *EXPLOIT*
|       0095E929-7573-5E4A-A7FA-F6598A35E8DE    6.8     https://vulners.com/githubexploit/0095E929-7573-5E4A-A7FA-
F6598A35E8DE    *EXPLOIT*
|       CVE-2022-28615  6.4     https://vulners.com/cve/CVE-2022-28615
|       CVE-2021-44224  6.4     https://vulners.com/cve/CVE-2021-44224
|       CVE-2019-10082  6.4     https://vulners.com/cve/CVE-2019-10082
|       CVE-2019-0217   6.0     https://vulners.com/cve/CVE-2019-0217
|       CVE-2022-22721  5.8     https://vulners.com/cve/CVE-2022-22721
|       CVE-2020-1927   5.8     https://vulners.com/cve/CVE-2020-1927
|       CVE-2019-10098  5.8     https://vulners.com/cve/CVE-2019-10098
|       1337DAY-ID-33577        5.8     https://vulners.com/zdt/1337DAY-ID-33577        *EXPLOIT*
|       CVE-2022-30556  5.0     https://vulners.com/cve/CVE-2022-30556
|       CVE-2022-29404  5.0     https://vulners.com/cve/CVE-2022-29404
|       CVE-2022-28614  5.0     https://vulners.com/cve/CVE-2022-28614
|       CVE-2022-26377  5.0     https://vulners.com/cve/CVE-2022-26377
|       CVE-2022-22719  5.0     https://vulners.com/cve/CVE-2022-22719
|       CVE-2021-34798  5.0     https://vulners.com/cve/CVE-2021-34798
|       CVE-2021-33193  5.0     https://vulners.com/cve/CVE-2021-33193
|       CVE-2021-26690  5.0     https://vulners.com/cve/CVE-2021-26690
|       CVE-2020-9490   5.0     https://vulners.com/cve/CVE-2020-9490
|       CVE-2020-1934   5.0     https://vulners.com/cve/CVE-2020-1934
|       CVE-2019-17567  5.0     https://vulners.com/cve/CVE-2019-17567
```



Ex

Host	High	Medium	Low	Log
10.0.2.5	CVE 2010-1938	CVE 2020-1927		x

IP Address: 10.0.2.5

Service	Port	Sensitive Level
the Apache web server	80 or 443 (HTTP/HTTPS) TCP	High

Apache Tomcat AJP protocol	8009 TCP	Medium
xxx	TCP	Low
xxx	xx TCP	Log

Expected detail format for vulnerabilities found

High

1- CVE-2010-1938 **and or finding (**9.3 (out of 10)**)**

Issue

The vulnerability is caused by a buffer overflow in the Apache mod_isapi module when handling specially crafted ISAPI extension requests. An attacker can exploit this vulnerability by sending a specially crafted HTTP request to a vulnerable server running Apache with mod_isapi enabled.

Impact

An attacker can gain complete control of the vulnerable system by exploiting this vulnerability, which can lead to unauthorized access to sensitive data, disruption of services, and other malicious activities.

Mitigation

The vulnerability can be mitigated by disabling the mod_isapi module or upgrading to a non-vulnerable version of Apache. Additionally, it is recommended to follow security best practices such as:

- Restrict access to the web server and implement strong authentication mechanisms.
- Use a web application firewall to monitor and filter incoming HTTP requests.

Reference

- https://httpd.apache.org/docs/2.2/mod/mod_isapi.html
- https://www.exploit-db.com/exploits/14737
- https://nvd.nist.gov/vuln/detail/CVE-2010-1938

Medium

1- CVE-2020-1927**and or finding** (6.5 (out of 10))

Issue

The vulnerability is caused by a flaw in the Apache Tomcat server that allows attackers to perform a Denial of Service (DoS) attack by exploiting a bug in the Tomcat AJP protocol. The vulnerability occurs due to a mismatch in the maximum size of AJP packets that are sent between the Apache Tomcat server and the Apache web server.

Impact
An attacker who successfully exploits this vulnerability can cause the Apache Tomcat server to crash, resulting in a denial of service condition that can lead to disruption of services.

Mitigation
The vulnerability can be mitigated by upgrading to a non-vulnerable version of Apache Tomcat. It is also recommended to follow security best practices such as :

- Using a web application firewall to monitor and filter incoming AJP requests.
- Regularly updating software and applying security patches as soon as they become available
- Implementing network segmentation and access controls to limit the exposure of vulnerable systems.

Reference

- https://nvd.nist.gov/vuln/detail/CVE-2020-1927
- https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.31

Critical

CVE-2019-0211 (service is the Apache HTTP Server) (port 80 or 443 (HTTP/HTTPS))

CVSS Score: 9.8 (out of 10)

Sensitive level: Critical

Issue: The vulnerability is caused by a flaw in the Apache HTTP Server that allows attackers to perform a Remote Code Execution (RCE) attack by exploiting a bug in the way the server handles certain requests.

Impact: An attacker who successfully exploits this vulnerability can execute arbitrary code on the vulnerable system with the privileges of the user running the web server, which can lead to unauthorized access to sensitive data, disruption of services, and other malicious activities.

Mitigation: The vulnerability can be mitigated by upgrading to a non-vulnerable version of Apache HTTP Server. It is also recommended to follow security best practices such as:

- **updating software and applying security patches as soon as they become available.**
- **Implementing network segmentation and access controls to limit the exposure of vulnerable systems**

Reference:

- **https://httpd.apache.org/security/vulnerabilities_24.html**
- **https://nvd.nist.gov/vuln/detail/CVE-2019-0211**

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

There are critical vuln on the Ubuntu machine

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?

  - Yes, based on the vulnerabilities that have been examined, there is a possibility of risk. There are some open and not updated ports that may lead to the possibility of remote access because they are not updated and sufficiently protected.
  - Opent port on Windows
    - Port 80: the default port used for HTTP traffic. If the system is hosting a web server, then there is a risk of attacks like remote code execution, cross-site scripting (XSS), and SQL injection.
    - Port 7: used for the Echo protocol, which is primarily used for debugging and troubleshooting purposes. It is generally considered safe to leave open.
    - Port 9: used for the Wake-On-LAN (WoL) protocol, which allows a device to be turned on remotely. If enabled, an attacker with network access can potentially wake up the device without authorization.
    - Port 13: used for the Daytime protocol, which returns the current date and time. It is generally considered safe to leave open.
    - Port 17: used for the Quote of the Day (QOTD) protocol, which returns a random quote or message. It is generally considered safe to leave open.
    - Port 19: used for the Character Generator protocol, which generates random characters. It is generally considered safe to leave open.
    - Port 135: used for the Remote Procedure Call (RPC) protocol, which is commonly used for interprocess communication. It has been known to be vulnerable to exploits like DCOM, which could result in remote code execution.

- Port 139: used for the NetBIOS protocol, which allows Windows systems to share files and printers. It has been known to be vulnerable to attacks like the EternalBlue exploit, which could result in remote code execution.
- Port 445: used for the SMB protocol, which is used for file sharing, printer sharing, and remote administration. It has been known to be vulnerable to exploits like EternalBlue, which could result in remote code execution.
- Port 3389: used for the Remote Desktop Protocol (RDP), which allows remote access to a Windows system. If RDP is enabled and poorly configured, attackers can use brute-force attacks to gain access to the system.

If the port it is not important it's better to close it but if it's important must secure it especially if this port is connect to remote access and the admin and authorized user

So before implementing the integration should close and secure this open ports and close unimportant ports and must check and solve all the vulnerability.

On Ubuntu

- Port 13: the daytime protocol, which is used to provide the current date and time to connected clients. It is not typically considered a high-risk port.

- Port 17: the quote of the day (QOTD) protocol, which provides a random quote to connected clients. Like port 13, it is not typically considered a high-risk port.

- Port 21: the FTP (File Transfer Protocol) port. If the server is running an outdated version of vsftpd (such as the vulnerable version 2.0.8), it could be susceptible to various security issues, including remote code execution and information disclosure.

- Port 22: the SSH (Secure Shell) port, which is used for secure remote shell access. If SSH is not properly configured, it could be vulnerable to various attacks such as brute force attacks, password cracking, and remote code execution.

- Port 23: the Telnet port, which is an unencrypted remote shell access protocol. Telnet is not typically used on modern systems as it is considered insecure and easily susceptible to eavesdropping attacks.

- Port 37: the Time protocol, which provides the current time to connected clients. It is not typically considered a high-risk port.

- Port 80: the default HTTP (Hypertext Transfer Protocol) port used for serving web pages. If the web server is not properly configured, it could be vulnerable to various attacks such as cross-site scripting, SQL injection, and remote code execution.

- Port 445: the SMB (Server Message Block) port, which is used for file and printer sharing. If the SMB service is not properly configured, it could be vulnerable to various attacks such as remote code execution, denial of service, and information disclosure.

- There are an attacker used the ssh service so first we need to kill this process to prevent him to access the ubuntu machine kill -9 UID that should be done before integrating this network into the extended network of our company

- If it would be a risk to NuttyUtility, what recommendations would you make to mitigate these risks before implementing the integration, and why?

  - Disable unnecessary services and ports: Ports 13, 17, 37, and 135 are not commonly used and can be disabled if not required by the system or application. Similarly, if the services running on ports 21, 22, 23, and 80 are not needed, they should also be disabled.
  - Regularly update and patch the system: The identified CVEs have known vulnerabilities that can be exploited by attackers. Regularly updating and patching the system can mitigate the risks associated with CVEs.
  - Monitor and log system activities: Monitoring and logging system activities can help detect any suspicious activities or potential security breaches, allowing for timely response and mitigation.
  - Implementing firewall rules can be implemented to restrict incoming and outgoing traffic on the identified ports, especially for those services that are not required for the system or application.Regularly updating software and applying security patches as soon as they become available
  - Implement strong authentication mechanisms: If NuttyUtility requires remote access, it is essential to implement strong authentication mechanisms, such as multi-factor authentication and encryption, to prevent unauthorized access to the system.
  - Implementing network segmentation and access controls to limit the exposure of vulnerable systems.
  - Restrict access to the web server and implement strong authentication mechanisms.

- Please provide reasoning based on the proof obtained throughout your assessment.

  - there are several risks associated with the integration of NuttyUtility. The open ports on both Windows and Ubuntu systems pose a significant risk, especially if they are not secured properly. For example, ports 13 and 17 are often used for testing purposes and can be used by attackers to launch DoS attacks or gain unauthorized access to a system. Ports 135, 139, and 445 are commonly used by SMB (Server

Message Block) protocol, which has been the target of many high-profile cyber attacks, including WannaCry ransomware attack.

- The CVEs also pose significant risks to the security of the systems. These vulnerabilities range from buffer overflow to code execution and can be used to gain unauthorized access, elevate privileges, or launch DoS attacks.
- To mitigate these risks, it is recommended to implement a few security measures before integrating NuttyUtility. These measures include:
    - Implement intrusion detection and prevention systems to detect and block any attempts to exploit the identified vulnerabilities.
    - Configure the system to use secure protocols like SSH instead of Telnet for remote access.
    - Apply patches and updates to address any identified vulnerabilities.
    - Perform a vulnerability assessment and penetration testing to identify vulnerabilities in the system and assess the overall security posture.

The End

On Ubuntu

- The FTP server vsftpd version 2.0.8 not updated and secure so this may be give An attacker can gain complete control of the vulnerable system by exploiting this vulnerability, which can lead to unauthorized access to sensitive data, disruption of services, and other malicious activities.

On windows

- SMBv1: is a protocol used for file sharing and other network operations in Windows operating systems. It has been known to have several security vulnerabilities, which can result in serious issues and impact, such as:
  - SMBv1 vulnerabilities can be exploited to cause a DoS attack on systems, leading to system crashes or unavailability.
  - SMBv1 has been used as a vector for ransomware attacks, where attackers exploit vulnerabilities in the protocol to gain access to systems and encrypt files for ransom.