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

Task 1

First Ubuntu machine:

```
ustudent@ubu-ustudent:~$ sudo nmap -sV --script vuln 10.0.2.7
[sudo] password for ustudent:

Starting Nmap 7.60 ( https://nmap.org ) at 2023-04-01 13:23 EDT
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
```

```
ustudent@ubu-ustudent: ~
File  Edit  View  Search  Terminal  Help

Host script results:
| smb-vuln-cve-2017-7494:
|   VULNERABLE:
|   SAMBA Remote Code Execution from Writable Share
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2017-7494
|     Risk factor: HIGH  CVSSv3: 7.5 (HIGH) (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H)
|       All versions of Samba from 3.5.0 onwards are vulnerable to a remote
|       code execution vulnerability, allowing a malicious client to upload a
|       shared library to a writable share, and then cause the server to load
|       and execute it.
|
|     Disclosure date: 2017-05-24
|     Check results:
|       Samba Version: 3.X - 4.X
|       Writable share found.
|         Name: \\10.0.2.7\data
|       File written to remote share, but unable to execute payload either due to unknown actual path, or the syste
m may be patched.
|     Extra information:
|       All writable shares:
|         Name: \\10.0.2.7\data
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7494
|_      https://www.samba.org/samba/security/CVE-2017-7494.html
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: false
| smb-vuln-regsvc-dos:
|   VULNERABLE:
|   Service regsvc in Microsoft Windows systems vulnerable to denial of service
|     State: VULNERABLE
|       The service regsvc in Microsoft Windows 2000 systems is vulnerable to denial of service caused by a null de
ference
|       pointer. This script will crash the service if it is vulnerable. This vulnerability was discovered by Ron B
owes
|       while working on smb-enum-sessions.
|_

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 77.80 seconds
ustudent@ubu-ustudent:~$
```

I Discovered a Vulnerability: avahi Packet DoS

Cve -2011-1002

Broadcast-avahi-dos

Host : 224.0.0.251

Cve classification : vulnerability is a buffer overflow vulnerability that affects the Avahi daemon, specifically in the way that the daemon handles incoming packets. It can be exploited by a remote attacker to send specially crafted packets to a vulnerable system, causing a denial of service (DoS) condition by crashing the Avahi daemon.

CVSS) score for CVE-2011-1002 is 7.8, which indicates a High severity vulnerability

Remediation : To remediate this vulnerability, it is recommended to update the affected system with the latest security patches provided by the vendor. The vulnerability was fixed in Avahi version 0.6.30, so updating to that version or a later version should resolve the issue.

Technique IDs:

- T1498.002: Network Denial of Service (DoS) - Avahi Packet Storm
- T1498.003: Network Denial of Service (DoS) - Avahi Reflection Amplification

Tools:

- Metasploit Framework: A penetration testing framework that contains modules for exploiting CVE-2011-1002.
- avahi-dos: A proof-of-concept (PoC) tool that sends specially crafted packets to trigger the DoS vulnerability.

Procedures:

- Send specially crafted packets to the Avahi daemon to trigger the vulnerability and cause the service to crash or become unresponsive.
- Use a tool like Metasploit to automate the exploitation process and launch a DoS attack against the target.
- Amplify the attack by using reflection techniques to send the packets through multiple devices on the network, increasing the volume of traffic and making it harder to trace the source of the attack.

Smb-vuln-cve-2017-7494

SAMBA Remote Code Execution from Writable Share

Classification : known as the SAMBA Remote Code Execution from Writable Share vulnerability, is a critical remote code execution vulnerability that affects the Samba file-sharing software. It allows a remote attacker to execute arbitrary code with root privileges by uploading a shared library to a writable share on a vulnerable system and then causing Samba to load and execute the library.

(CVSS) score for SMB-vuln-cve-2017-7494 is 8.8, which indicates a High severity vulnerability.

Remediation :

To remediate this vulnerability, it is recommended to update the Samba software to a patched version. The vulnerability was fixed in Samba versions 4.6.4, 4.5.10, and 4.4.14, so updating to one of these versions or a later version should resolve the issue

Technique IDs:

- T1190 - Exploit Public-Facing Application
- T1210 - Exploitation for Client Execution

- T1068 - Exploitation for Privilege Escalation
- T1059 - Command and Scripting Interpreter
- T1027 - Obfuscated Files or Information

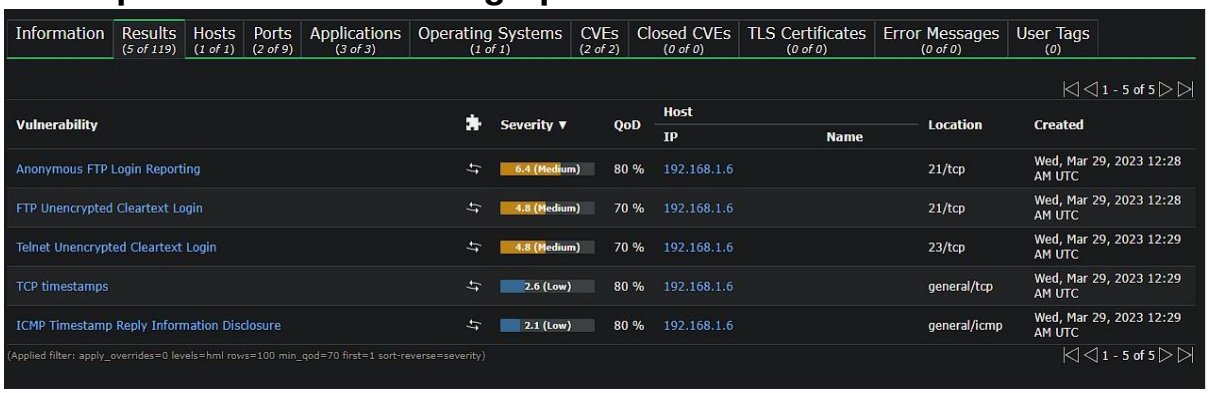
Tools:

- Samba
- Nmap

Procedures:

- Exploiting the vulnerability by uploading a shared library to a writable share on a vulnerable Samba server and causing Samba to load and execute the library
- Using Metasploit modules to exploit the vulnerability and gain remote code execution
- Using Impacket to exploit the vulnerability and gain remote code execution
- Scanning for vulnerable systems using Nmap scripts
- Leveraging the vulnerability to escalate privileges and gain higher-level access to the targeted system

Also I performed scan using openVas on ubuntu host



Information | Results (5 of 119) | Hosts (1 of 1) | Ports (2 of 9) | Applications (3 of 3) | Operating Systems (1 of 1) | CVEs (2 of 2) | Closed CVEs (0 of 0) | TLS Certificates (0 of 0) | Error Messages (0 of 0) | User Tags (0)

1 - 5 of 5

Vulnerability	Severity ▼	QoD	Host IP	Host Name	Location	Created
Anonymous FTP Login Reporting	6.4 (Medium)	80 %	192.168.1.6		21/tcp	Wed, Mar 29, 2023 12:28 AM UTC
FTP Unencrypted Cleartext Login	4.8 (Medium)	70 %	192.168.1.6		21/tcp	Wed, Mar 29, 2023 12:28 AM UTC
Telnet Unencrypted Cleartext Login	4.8 (Medium)	70 %	192.168.1.6		23/tcp	Wed, Mar 29, 2023 12:29 AM UTC
TCP timestamps	2.6 (Low)	80 %	192.168.1.6		general/tcp	Wed, Mar 29, 2023 12:29 AM UTC
ICMP Timestamp Reply Information Disclosure	2.1 (Low)	80 %	192.168.1.6		general/icmp	Wed, Mar 29, 2023 12:29 AM UTC

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

1 - 5 of 5

Medium (CVSS: 4.8) NVT: Telnet Unencrypted Cleartext Login
Summary The remote host is running a Telnet service that allows cleartext logins over unencrypted connections.
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Impact An attacker can uncover login names and passwords by sni-ng tra-c to the Telnet service.
Solution: Solution type: Mitigation Replace Telnet with a protocol like SSH which supports encrypted connections.
Vulnerability Detection Method Details: Telnet Unencrypted Cleartext Login OID:1.3.6.1.4.1.25623.1.0.108522 Version used: 2020-08-24T08:40:10Z

Summary Reports if the remote FTP Server allows anonymous logins.

Vulnerability Detection Result
It was possible to login to the remote FTP service with the following anonymous
,!account(s):
anonymous:anonymous@example.com
ftp:anonymous@example.com

Impact
Based on the les accessible via this anonymous FTP login and the permissions of this account
an attacker might be able to:
- gain access to sensitive les
- upload or delete les.

Solution:
Solution type: Mitigation

If you do not want to share les, you should disable anonymous logins.

Vulnerability Insight
A host that provides an FTP service may additionally provide Anonymous FTP access as well.
Under this arrangement, users do not strictly need an account on the host. Instead the user
typically enters 'anonymous' or 'ftp' when prompted for username. Although users are commonly
asked to send their email address as their password, little to no verication is actually performed
on the supplied data.
Remark: NIST don't see 'conguration issues' as software aws so the referenced CVE has a
severity of 0.0. The severity of this VT has been raised by Greenbone to still report a conguration
issue on the target.

Vulnerability Detection Method
Details: Anonymous FTP Login Reporting
OID:1.3.6.1.4.1.25623.1.0.900600
Version used: 2021-10-20T09:03:29Z

References
cve: CVE-1999-0497

Summary
The remote host is running a FTP service that allows cleartext logins over unencrypted connec
tions.

Vulnerability Detection Result
The remote FTP service accepts logins without a previous sent 'AUTH TLS' command
,!. Response(s):
Anonymous sessions: 331 Please specify the password.
Non-anonymous sessions: 331 Please specify the password.

Impact
An attacker can uncover login names and passwords by sni-ng tra-c to the FTP service.

Solution:
Solution type: Mitigation
Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual
of the FTP service for more information.

Vulnerability Detection Method
Tries to login to a non FTPS enabled FTP service without sending a 'AUTH TLS' command
rst and checks if the service is accepting the login without enforcing the use of the 'AUTH TLS'
command.

Details: FTP Unencrypted Cleartext Login
OID:1.3.6.1.4.1.25623.1.0.108528
Version used: 2020-08-24T08:40:10Z

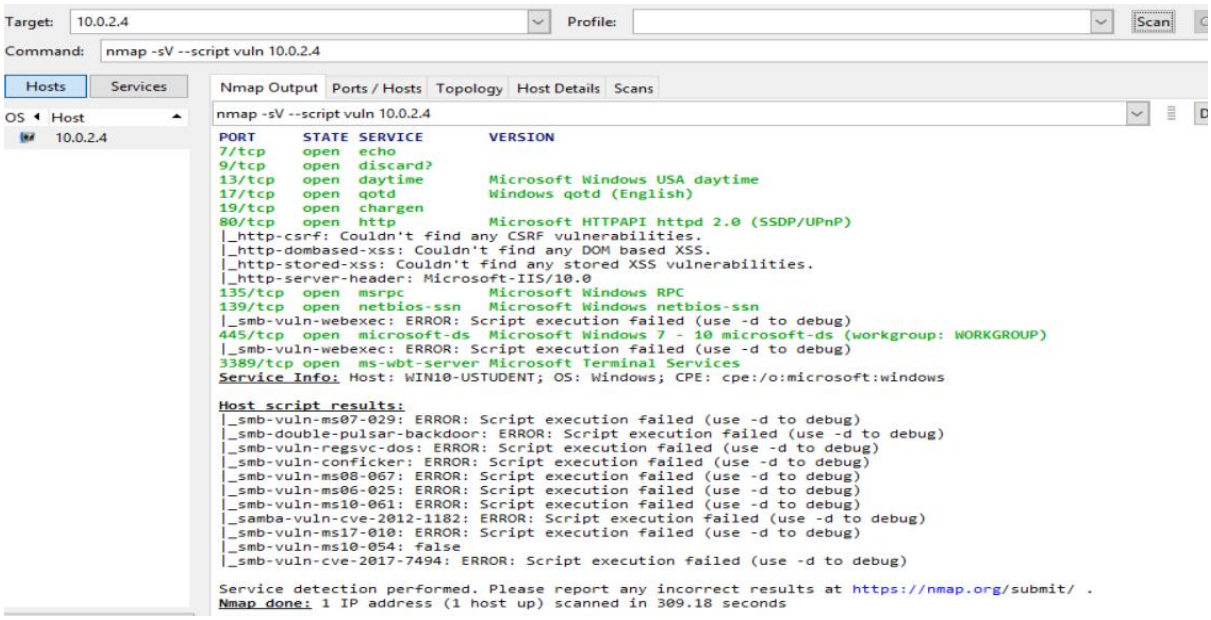
Low (CVSS: 2.1)
NVT: ICMP Timestamp Reply Information Disclosure

Summary The remote host responded to an ICMP timestamp request.
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Solution: Solution type: Mitigation Various mitigations are possible: - Disable the support for ICMP timestamp on the remote host completely - Protect the remote host by a rewall, and block ICMP packets passing through the rewall in either direction (either completely or only for untrusted networks)
Vulnerability Insight The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp. This information could theoretically be used to exploit weak time-based random number generators in other services.
Vulnerability Detection Method Details: ICMP Timestamp Reply Information Disclosure OID:1.3.6.1.4.1.25623.1.0.103190 Version used: 2022-11-18T10:11:40Z
References cve: CVE-1999-0524 url: http://www.ietf.org/rfc/rfc0792.txt cert-bund: CB-K15/1514 cert-bund: CB-K14/0632 dfn-cert: DFN-CERT-2014-0658

Low (CVSS: 2.6) NVT: TCP timestamps
Summary The remote host implements TCP timestamps and therefore allows to compute the uptime.
Vulnerability Detection Result It was detected that the host implements RFC1323/RFC7323. The following timestamps were retrieved with a delay of 1 seconds in-between: Packet 1: 3503625356 Packet 2: 3503626424
Impact A side eect of this feature is that the uptime of the remote host can sometimes be computed.
Solution: Solution type: Mitigation To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See the references for more information.
Aected Software/OS TCP implementations that implement RFC1323/RFC7323.
Vulnerability Insight The remote host implements TCP timestamps, as dened by RFC1323/RFC7323.
Vulnerability Detection Method Special IP packets are forged and sent with a little delay in between to the target IP. The

responses are searched for a timestamps. If found, the timestamps are reported. Details: TCP timestamps OID:1.3.6.1.4.1.25623.1.0.80091 Version used: 2020-08-24T08:40:10Z
References url: http://www.ietf.org/rfc/rfc1323.txt url: http://www.ietf.org/rfc/rfc7323.txt url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d ,/ownload/details.aspx?id=9152

In Windows Vuln Scan



CVE-2012-1182

Classification : vulnerability is a buffer overflow vulnerability in the Samba software that allows a remote attacker to execute arbitrary code on a vulnerable system. This vulnerability is triggered by sending a specially crafted packet to a vulnerable system, which can lead to a stack-based buffer overflow and subsequent execution of arbitrary code.

(CVSS) score for CVE-2012-1182 is 5.0, which indicates a Moderate severity vulnerability.

Remediation : To remediate this vulnerability, it is recommended to update the Samba software to a patched version. The vulnerability was fixed in Samba versions 3.6.5, 3.5.15, and 3.4.15, so updating to one of these versions or a later version should resolve the issue.

Technique IDs:

- T1190 - Exploit Public-Facing Application
- T1210 - Exploitation for Client Execution
- T1068 - Exploitation for Privilege Escalation
- T1059 - Command and Scripting Interpreter

Tools:

- Metasploit Framework

- Samba
- Nmap

Procedures:

- Exploiting the buffer overflow vulnerability by sending a specially crafted packet to a vulnerable Samba server
- Using Metasploit modules to exploit the vulnerability and gain remote code execution
- Scanning for vulnerable systems using Nmap scripts
- Leveraging the vulnerability to escalate privileges and gain higher-level access to the targeted system.

CVE-2017-7494

Classification : The SMB-vuln-cve-2017-7494 vulnerability, also known as the SAMBA Remote Code Execution from Writable Share vulnerability, is a critical remote code execution vulnerability that affects the Samba file-sharing software. It allows a remote attacker to execute arbitrary code with root privileges by uploading a shared library to a writable share on a vulnerable system and then causing Samba to load and execute the library.

(CVSS) score for CVE-2017-7494 is 8.8, which indicates a High severity vulnerability.

Remediation: To remediate this vulnerability, it is recommended to update the Samba software to a patched version. The vulnerability was fixed in Samba versions 4.6.4, 4.5.10, and 4.4.14, so updating to one of these versions or a later version should resolve the issue.

CVE-2017-7494:

Technique IDs:

- T1059.001 - Command and Scripting Interpreter: PowerShell
- T1027 - Obfuscated Files or Information
- T1024 - Custom Cryptographic Protocol
- T1210 - Exploitation for Client Execution
- T1068 - Exploitation for Privilege Escalation
- T1055 - Process Injection

Tools:

- Metasploit Framework
- Impacket

- Nmap
- Samba

Procedures:

- Exploiting the vulnerability using a specially crafted packet to execute arbitrary code on a vulnerable system
- Uploading a shared library to a writable share on a vulnerable system and causing Samba to load and execute the library
- Using Metasploit modules to exploit the vulnerability and gain remote code execution
- Using Impacket to exploit the vulnerability and gain remote code execution
- Using Nmap scripts to detect vulnerable systems

Also I performed openVas on windows machine

High (CVSS: 10.0) NVT: Check for discard Service
Summary The remote host is running a 'discard' service. This service typically sets up a listening socket and will ignore all the data which it receives. This service is unused these days, so it is advised that you disable it.
Vulnerability Detection Result The discard service was detected on the target host.
Solution: Solution type: Mitigation - Under Unix systems, comment out the 'discard' line in /etc/inetd.conf and restart the inetd process - Under Windows systems, set the following registry key to 0: HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpDiscard Then launch cmd.exe and type: net stop simptcp net start simptcp To restart the service.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Check for discard Service OID:1.3.6.1.4.1.25623.1.0.11367 Version used: 2020-10-01T11:33:30Z

High (CVSS: 10.0)
NVT: SMB Brute Force Logins With Default Credentials

Summary
A number of known default credentials are tried for the login via the SMB protocol.

Vulnerability Detection Result
It was possible to login with the following credentials via the SMB protocol to
,/the 'IPC$' share. <User>:<Password>
operator:1234

Solution:
Solution type: Mitigation
Change the password as soon as possible.

Vulnerability Detection Method
Tries to login with a number of known default credentials via the SMB protocol.
Details: SMB Brute Force Logins With Default Credentials
OID:1.3.6.1.4.1.25623.1.0.804449
Version used: 2022-04-11T14:03:55Z

References
cve: CVE-1999-0503
cve: CVE-1999-0504
cve: CVE-1999-0505
cve: CVE-1999-0506

Medium (CVSS: 5.0)
NVT: DCE/RPC and MSRPC Services Enumeration Reporting

Summary
Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC ser
vices running on the remote host can be enumerated by connecting on port 135 and doing the
appropriate queries.

Vulnerability Detection Result
Here is the list of DCE/RPC or MSRPC services running on this host via the TCP p
,/rotocol:
Port: 1536/tcp

Impact
An attacker may use this fact to gain more knowledge about the remote host.

Solution:
Solution type: Mitigation
Filter incoming tra-c to this ports.

Vulnerability Detection Method
Details: DCE/RPC and MSRPC Services Enumeration Reporting
OID:1.3.6.1.4.1.25623.1.0.10736
Version used: 2022-06-03T10:17:07Z

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

Summary
It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this
system.

Vulnerability Detection Result
In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.0 and
,/ TLSv1.1 protocols and supports one or more ciphers. Those supported ciphers c
,/an be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1
,/.25623.1.0.802067) VT.

Impact
An attacker might be able to use the known cryptographic aws to eavesdrop the connection

between clients and the service to get access to sensitive data transferred within the secured connection.

Solution:
Solution type: Mitigation
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

Aected Software/OS
All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

Vulnerability Insight
The TLSv1.0 and TLSv1.1 protocols contain known cryptographic aws like:
- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

Vulnerability Detection Method
Check the used TLS protocols of the services provided by this system.
Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
OID:1.3.6.1.4.1.25623.1.0.117274
Version used: 2021-07-19T08:11:48Z

References
cve: CVE-2015-0204
cve: CVE-2011-3389

Medium (CVSS: 5.0)
NVT: Check for Quote of the Day (qotd) Service (TCP)

Summary
The Quote of the Day (qotd) service is running on this host.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
An easy attack is 'pingpong' which IP spoofs a packet between two machines running qotd. This
will cause them to spew characters at each other, slowing the machines down and saturating the
network.

Solution:
Solution type: Mitigation
- Under Unix systems, comment out the 'qotd' line in /etc/inetd.conf and restart the inetd process
- Under Windows systems, set the following registry keys to 0 :
HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpQotd
HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpQotd
Then launch cmd.exe and type :
net stop simptcp
net start simptcp
To restart the service.

Vulnerability Insight
A server listens for TCP connections on TCP port 17. Once a connection is established a short message is sent out the connection (and any data received is thrown away). The service closes the connection after sending the quote.
Remark: NIST don't see 'conguration issues' as software aws so the referenced CVE has a severity of 0.0. The severity of this VT has been raised by Greenbone to still report a conguration
issue on the target.

Vulnerability Detection Method
Details: Check for Quote of the Day (qotd) Service (TCP)

OID:1.3.6.1.4.1.25623.1.0.10198 Version used: 2021-10-20T09:03:29Z
References cve: CVE-1999-0103

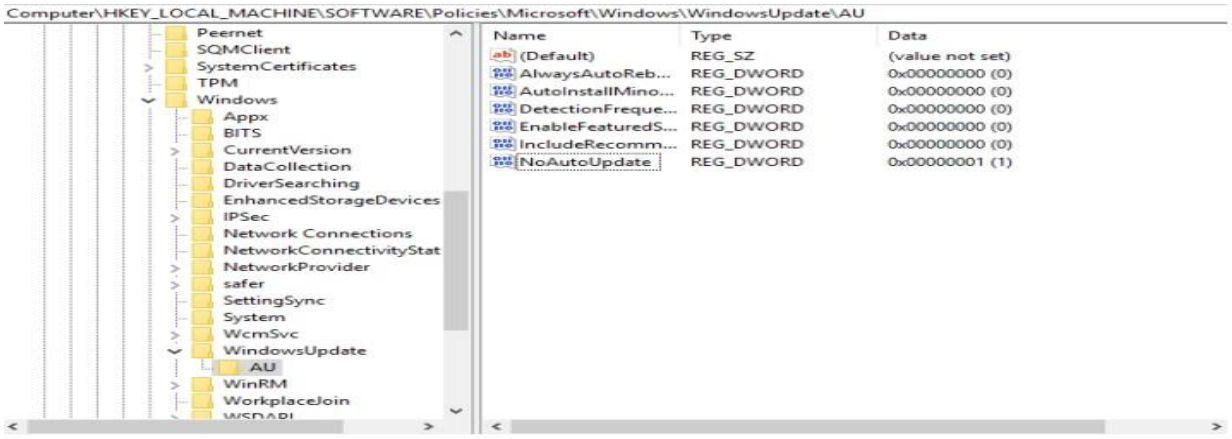
Medium (CVSS: 5.0) NVT: echo Service Reporting (TCP + UDP)
Summary An echo Service is running at this Host via TCP and/or UDP.
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Solution: Solution type: Mitigation Disable the echo Service.
Vulnerability Insight The echo service is an Internet protocol dened in RFC 862. It was originally proposed for testing and measurement of round-trip times in IP networks. While still available on most UNIX-like operating systems, testing and measurement is now performed with the Internet Control Message Protocol (ICMP), using the applications ping and traceroute. Remark: NIST don't see 'conguration issues' as software aws so the referenced CVE has a severity of 0.0. The severity of this VT has been raised by Greenbone to still report a conguration issue on the target.
Vulnerability Detection Method Details: echo Service Reporting (TCP + UDP) OID:1.3.6.1.4.1.25623.1.0.100075 Version used: 2021-10-20T09:03:29Z
References cve: CVE-1999-0635

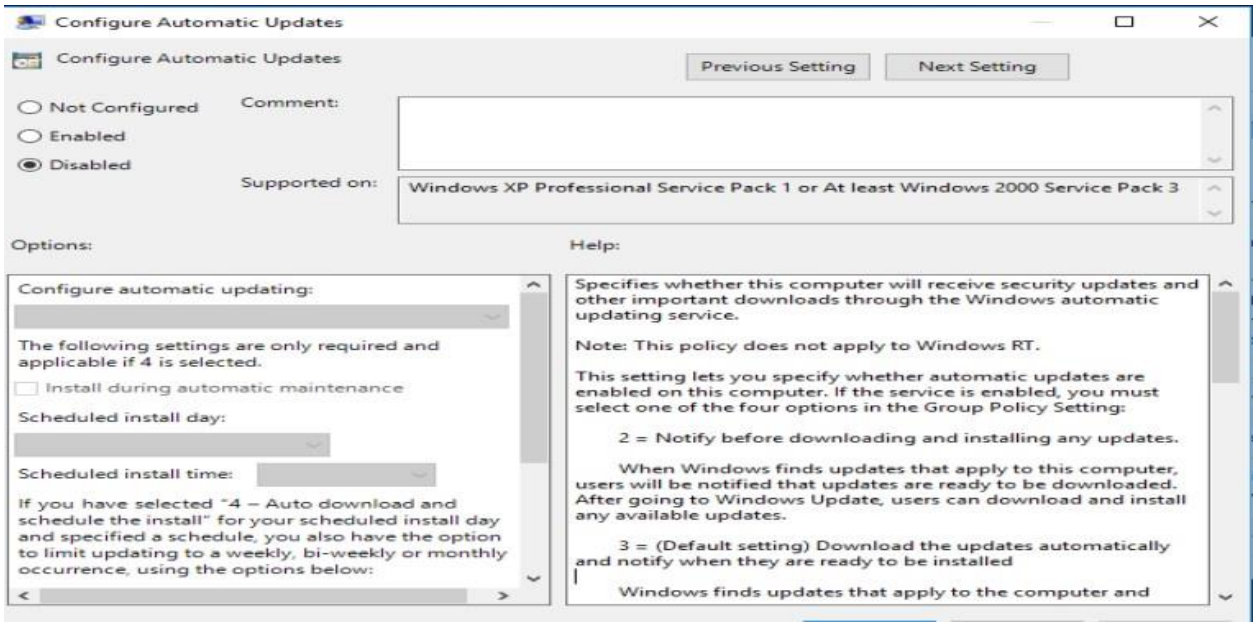
Low (CVSS: 2.1) NVT: ICMP Timestamp Reply Information Disclosure
Summary The remote host responded to an ICMP timestamp request.
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Solution: Solution type: Mitigation Various mitigations are possible: - Disable the support for ICMP timestamp on the remote host completely - Protect the remote host by a rewall, and block ICMP packets passing through the rewall in either direction (either completely or only for untrusted networks)
Vulnerability Insight The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp. This information could theoretically be used to exploit weak time-based random number generators in other services.

Vulnerability Detection Method Details: ICMP Timestamp Reply Information Disclosure OID:1.3.6.1.4.1.25623.1.0.103190 Version used: 2022-11-18T10:11:40Z
References cve: CVE-1999-0524 url: http://www.ietf.org/rfc/rfc0792.txt cert-bund: CB-K15/1514 cert-bund: CB-K14/0632 dfn-cert: DFN-CERT-2014-0658

TASK 2

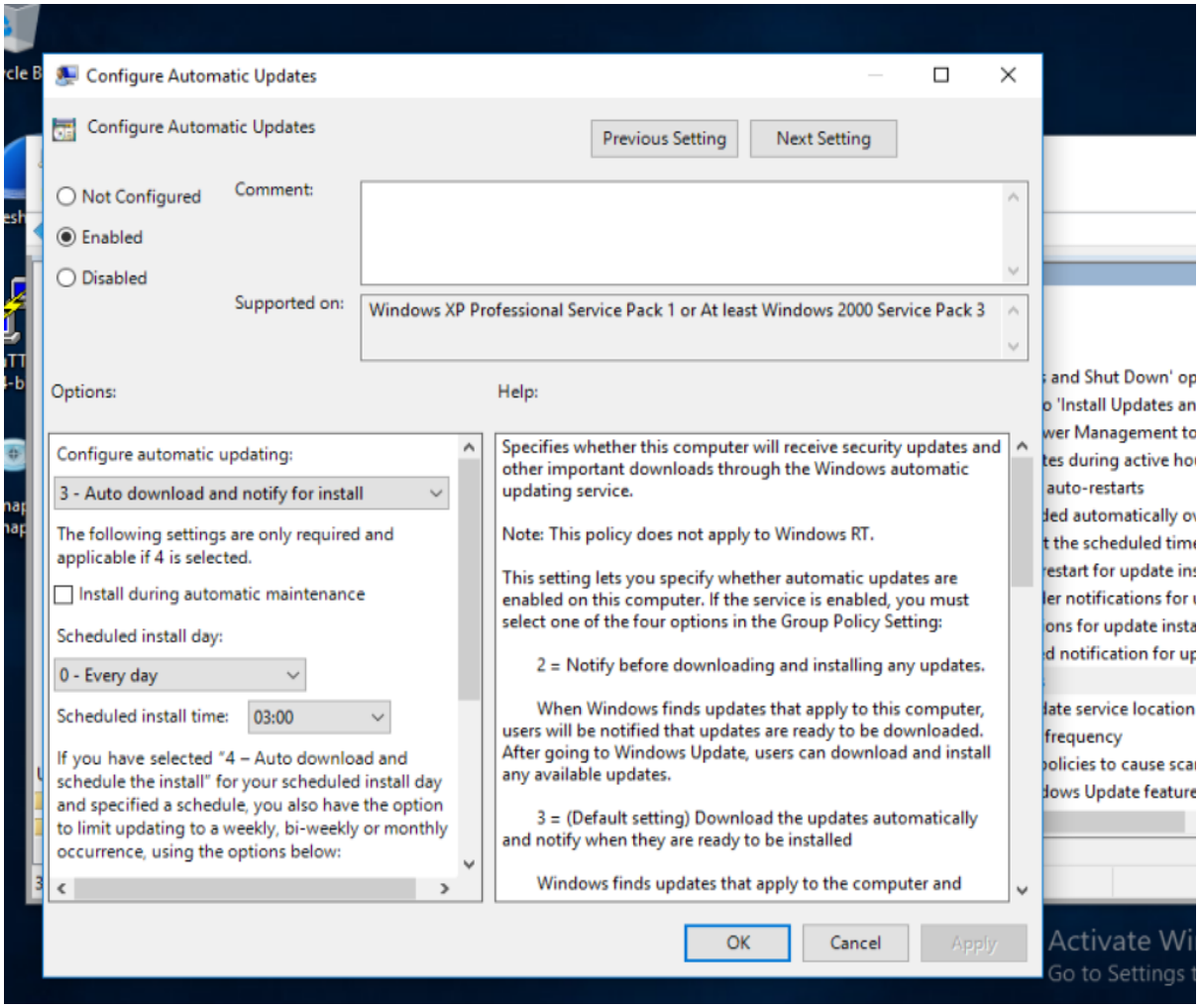
In Windows





No, Software Updates weren't configured correctly.

To remediate it



My Assessment

I would consider this a serious security risk that needs to be addressed as soon as possible.

it represents a significant security risk that requires immediate attention and remediation to minimize the risk of a security incident or breach.

In Ubuntu :

The Package manager Repositories aren’t configured correctly

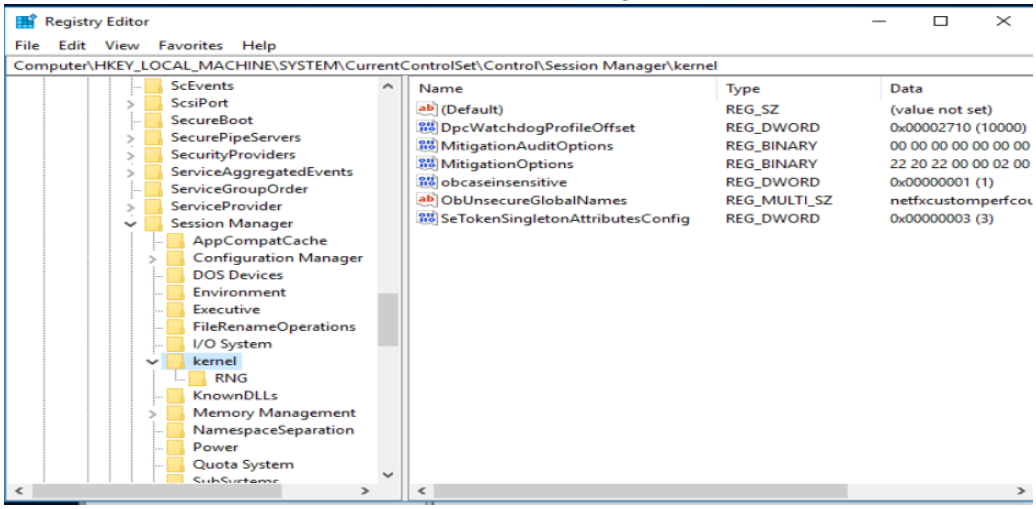
```
ustudent@ubu-ustudent:~$ apt-cache policy
Package files:
 100 /var/lib/dpkg/status
     release a=now
 500 http://us.archive.ubuntu.com/ubuntu bionic/multiverse i386 Packages
     release v=18.04,o=Ubuntu,a=bionic,n=bionic,l=Ubuntu,c=multiverse,b=i386
     origin us.archive.ubuntu.com
 500 http://us.archive.ubuntu.com/ubuntu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

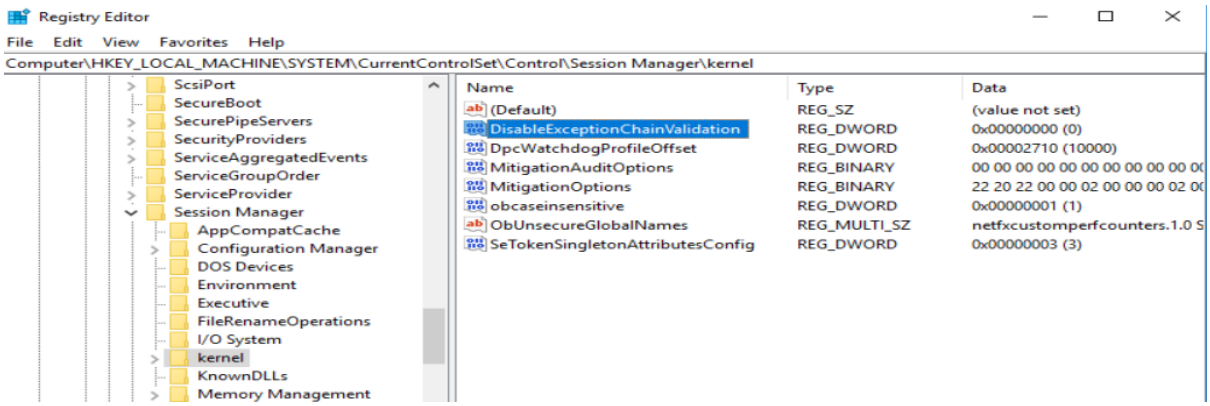
to remediate it

```
File  Edit  View  Search  Terminal  Help
ustudent@ubu-ustudent:~$ sudo apt-get update
Get:1 http://archive.canonical.com/ubuntu bionic InRelease [10.2 kB]
Hit:2 http://archive.ubuntu.com/ubuntu bionic InRelease
Hit:3 http://us.archive.ubuntu.com/ubuntu bionic-updates InRelease
Get:4 http://us.archive.ubuntu.com/ubuntu bionic-backports InRelease [83.3 kB]
Get:5 http://archive.canonical.com/ubuntu bionic/partner Sources [1,280 B]
Get:6 http://archive.canonical.com/ubuntu bionic/partner i386 Packages [1,588 B]
Get:7 http://archive.canonical.com/ubuntu bionic/partner amd64 Packages [1,592 B]
Get:8 http://archive.canonical.com/ubuntu bionic/partner Translation-en [1,004 B]
Get:9 http://us.archive.ubuntu.com/ubuntu bionic-backports/universe Sources [6,600 B]
Get:10 http://us.archive.ubuntu.com/ubuntu bionic-backports/main Sources [10.5 kB]
Fetched 116 kB in 2s (67.4 kB/s)
Reading package lists... Done
ustudent@ubu-ustudent:~$ sudo apt-get upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
ustudent@ubu-ustudent:~$
```

Task 3- Native Protections and Software Inventory
In windows :

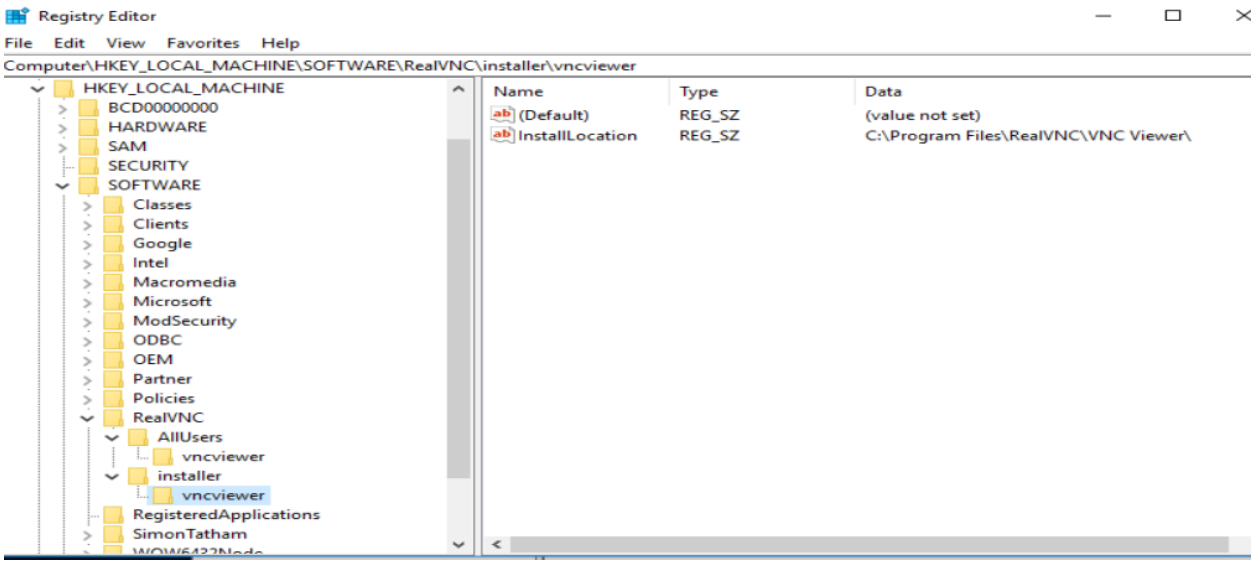
Ensure 'Enable Structured Exception Handling Overwrite Protection'





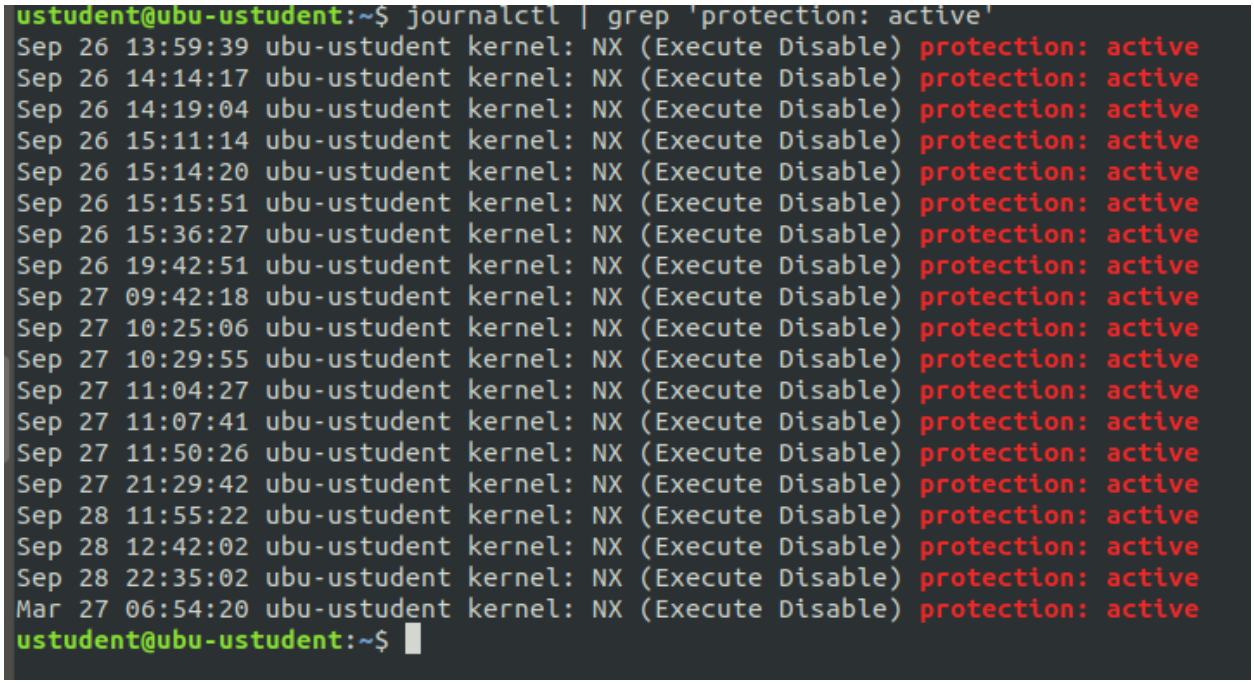
No, The System Isn’t Compliant

YES, VNC Viewer is installed

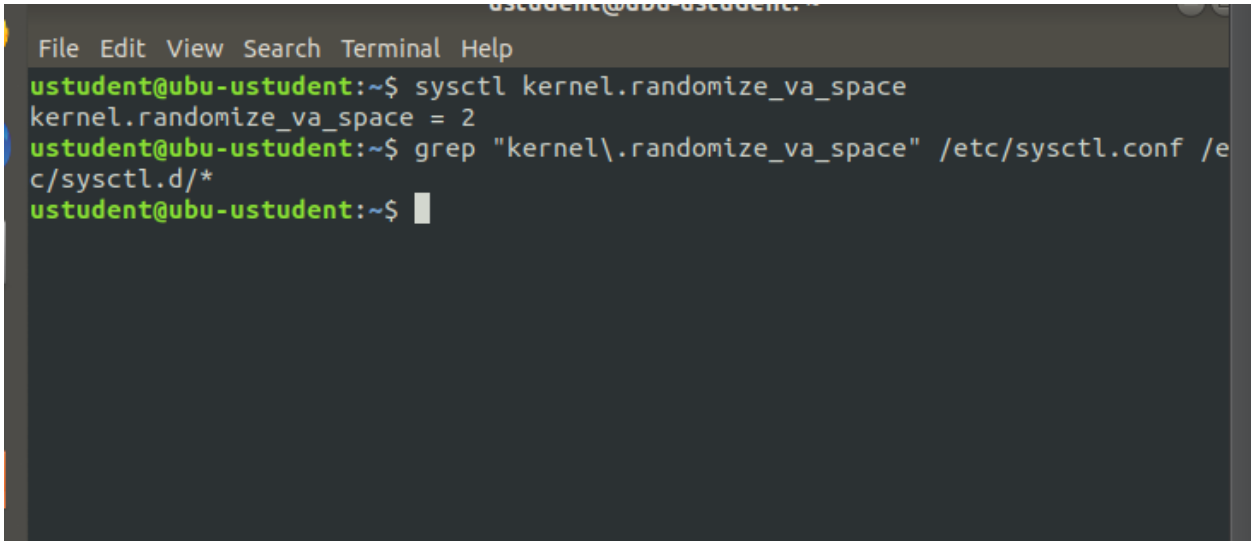


In UBUNTU :

1.6.1 Ensure XD/NX support is enabled



1.6.2 Ensure address space layout randomization (ASLR) is enabled



According to these checks the native protections is applied
We could list the package installed on ubuntu machine from this command

“dpkg –get-selections”

--

tightVNC is Installed on Ubuntu machine

```
ustudent@ubu-ustudent:~$ apt list | grep tightvnc

WARNING: apt does not have a stable CLI interface. Use with caution in scripts.

tightvnc-java/bionic,bionic 1.2.7-9 all
tightvncserver/bionic,now 1.3.10-0ubuntu4 amd64 [installed]
xtightvncviewer/bionic,now 1.3.10-0ubuntu4 amd64 [installed]
ustudent@ubu-ustudent:~$
```

While these applications can be useful for remote administration, they can also pose security risks if not properly configured.

In general, any software that enables remote access to a computer can potentially create a security vulnerability. VNC and TightVNC are no exception. If attackers are able to gain access to a computer running VNC or TightVNC, they could potentially access sensitive data, install malware, or take control of the computer.

Task 4

I Performed Network Asset Inventory From Ubuntu on the whole network :“sudo nmap -sV 10.0.2.0/24”

```
ustudent@ubu-ustudent: ~
File  Edit  View  Search  Terminal  Help
Not shown: 999 closed ports
PORT    STATE SERVICE    VERSION
53/tcp open  tcpwrapped
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 10.0.2.2
Host is up (0.0023s latency).
Not shown: 983 filtered ports
PORT      STATE  SERVICE        VERSION
135/tcp   open   msrpc          Microsoft Windows RPC
445/tcp   open   microsoft-ds?
646/tcp   closed ldp
666/tcp   closed doom
1001/tcp  open   webpush?
1024/tcp  closed kdm
1095/tcp  closed nicelink
1641/tcp  closed invision
2383/tcp  closed ms-olap4
2909/tcp  closed funk-dialout
5357/tcp  open   http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
8400/tcp  closed cvd
9110/tcp  closed unknown
10621/tcp closed unknown
24800/tcp closed unknown
34571/tcp closed unknown
54328/tcp closed unknown
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
Nmap scan report for 10.0.2.3
Host is up (0.00086s latency).
All 1000 scanned ports on 10.0.2.3 are filtered
MAC Address: 08:00:27:78:5B:35 (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.2.4
Host is up (0.0010s 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
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
MAC Address: 08:00:27:32:E0:5E (Oracle VirtualBox virtual NIC)
Service Info: Host: WIN10-USTUDENT; OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
Nmap scan report for ubu-ustudent (10.0.2.5)
Host is up (0.0000040s latency).
Not shown: 991 closed ports
PORT    STATE SERVICE     VERSION
13/tcp  open  daytime
17/tcp  open  qotd?
21/tcp  open  ftp         vsftpd 2.0.8 or later
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)
80/tcp  open  http        Apache httpd 2.4.29 ((Ubuntu))
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
1 service unrecognized despite returning data. If you know the service/version,
 please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi
?new-service :
SF-Port17-TCP:V=7.60%I=7%D=3/27%Time=6421903A%P=x86_64-pc-linux-gnu%r(NULL
SF:,13,"You'll\x20be\x20sorry\.\.\.\n");
Service Info: Host: Welcome; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nma
p.org/submit/ .
Nmap done: 256 IP addresses (5 hosts up) scanned in 388.51 seconds
ustudent@ubu-ustudent:~$
```

My Recommendation to Mitigate any Potential issues :

1. Use automated tools: Use automated network scanning tools to identify and document all the assets on the network. This can help reduce the likelihood of missing critical assets and can save time and effort.
2. Categorize assets: Categorize assets based on their criticality, location, and sensitivity. This can help prioritize security measures and make it easier to identify and manage potential risks.
3. Update asset inventory regularly: Update the asset inventory on a regular basis to ensure that it remains accurate and up-to-date. This can help identify new assets that may have been added to the network or identify assets that are no longer in use.
4. Perform vulnerability scanning: Perform vulnerability scanning on the identified assets to identify potential security risks. This can help identify vulnerabilities that can be used to exploit the assets.
5. Conduct risk assessment: Conduct a risk assessment on the identified assets to identify the potential impact and likelihood of various security risks. This can help prioritize security measures and identify areas that need additional attention.
6. Implement access controls: Implement access controls to limit access to critical assets only to authorized users. This can help prevent unauthorized access and reduce the likelihood of a successful attack.
7. Secure remote access: Ensure that remote access to assets is secure by using secure protocols like VPNs, implementing two-factor authentication, and limiting remote access to only authorized users.

Step 2: Assess Access Management at Targeted Assets

Task 1 :

In Ubuntu :

There's a NO VLANs

```
ustudent@ubu-ustudent:~$ cat /etc/network/interfaces
# interfaces(5) file used by ifup(8) and ifdown(8)
auto lo
iface lo inet loopback
ustudent@ubu-ustudent:~$ ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAUL
T group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP m
ode DEFAULT group default qlen 1000
    link/ether 08:00:27:78:d3:b5 brd ff:ff:ff:ff:ff:ff
ustudent@ubu-ustudent:~$
```

Also there's no Policies it's the default policies

```
ustudent@ubu-ustudent:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ustudent@ubu-ustudent:~$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 43 packets, 8373 bytes)
 pkts bytes target     prot opt in     out     source               destination


Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination


Chain OUTPUT (policy ACCEPT 45 packets, 6145 bytes)
 pkts bytes target     prot opt in     out     source               destination

ustudent@ubu-ustudent:~$
```

And there’s no Anonymous access

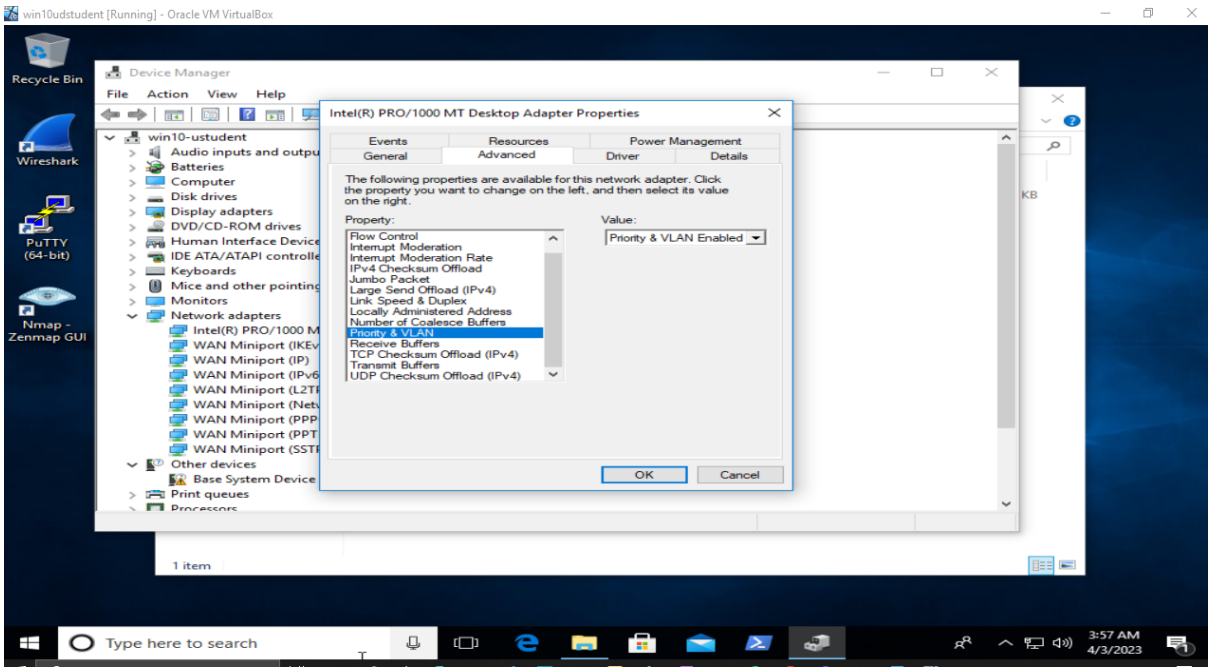
```
ustudent@ubu-ustudent:~$ sudo smbstatus

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

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

No locked files
```

My Assessment : This may pose a security risk as it can allow unauthorized access or attacks on the system.
To improve the settings, it is recommended to implement VLANs and IP security policies. VLANs can help segregate network traffic and limit access to specific resources

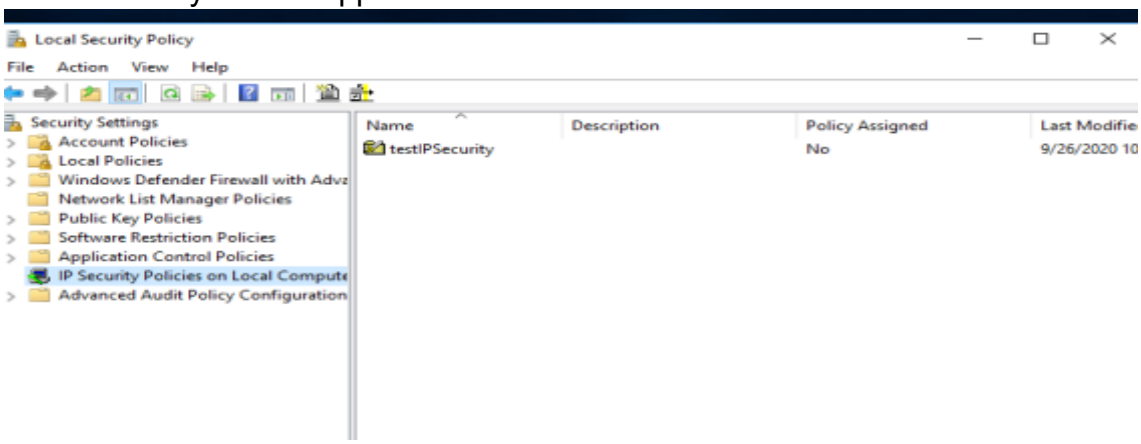
---

In Windows Machine

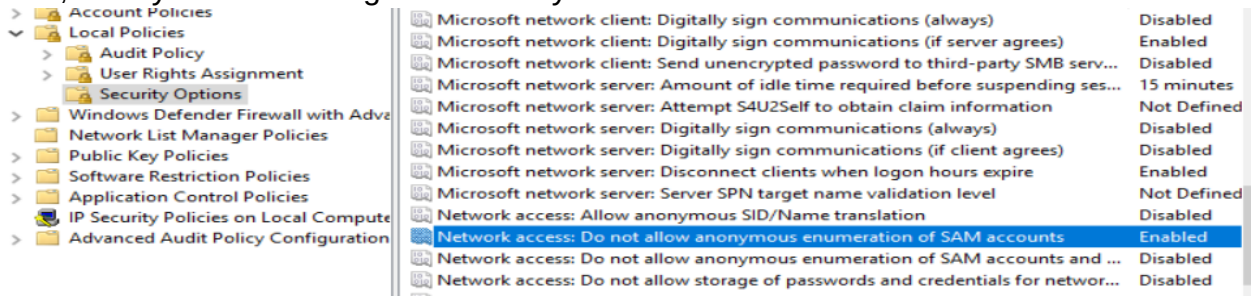
Yes There’s VLAN on Windows



There’s Policy but not applied



Yes, Anonymous access granted to any shares

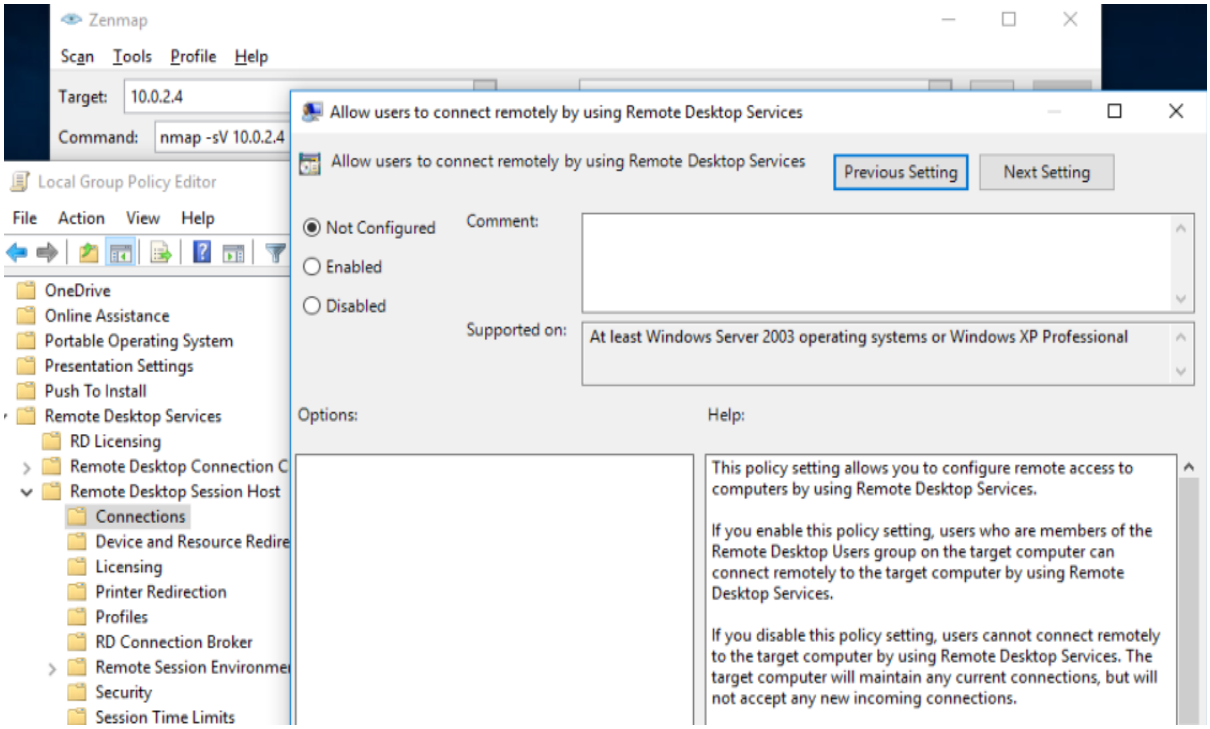


My Assessment and recommendation:

1- recommended to use VLANs to segment network traffic and improve security. VLANs help to separate different types of network traffic and reduce the risk of unauthorized access or data leakage.
2- recommended to implement IPsec policies to encrypt network traffic and protect against network-based attacks. IPsec provides a way to secure communications between hosts and can be used to enforce security policies such as authentication, integrity, and confidentiality.
3- Anonymous access to shares can pose a security risk as it allows anyone to access shared resources without authentication. It is recommended to disable anonymous access and enforce authentication to improve security.

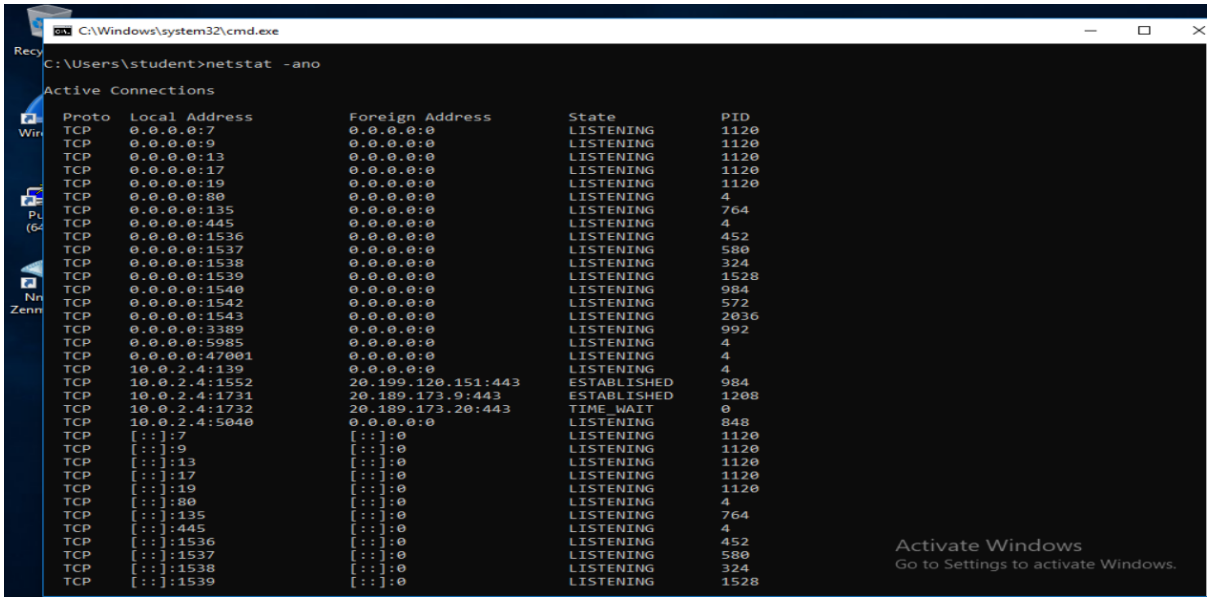
TASK 2

In Windows:



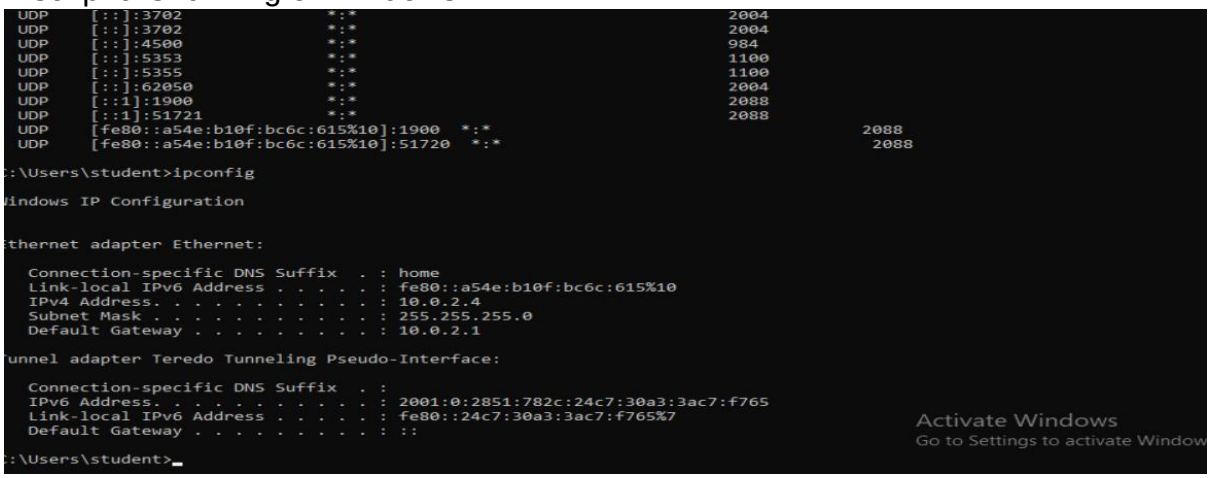
The Remote Services and protocols policy is not configured.

The remote Service protocols are running on the windows Machine:



HTTP, MSRPC, NETBIOS-SSN, MICROSOFT-DS

Also ipv6 is running on windows



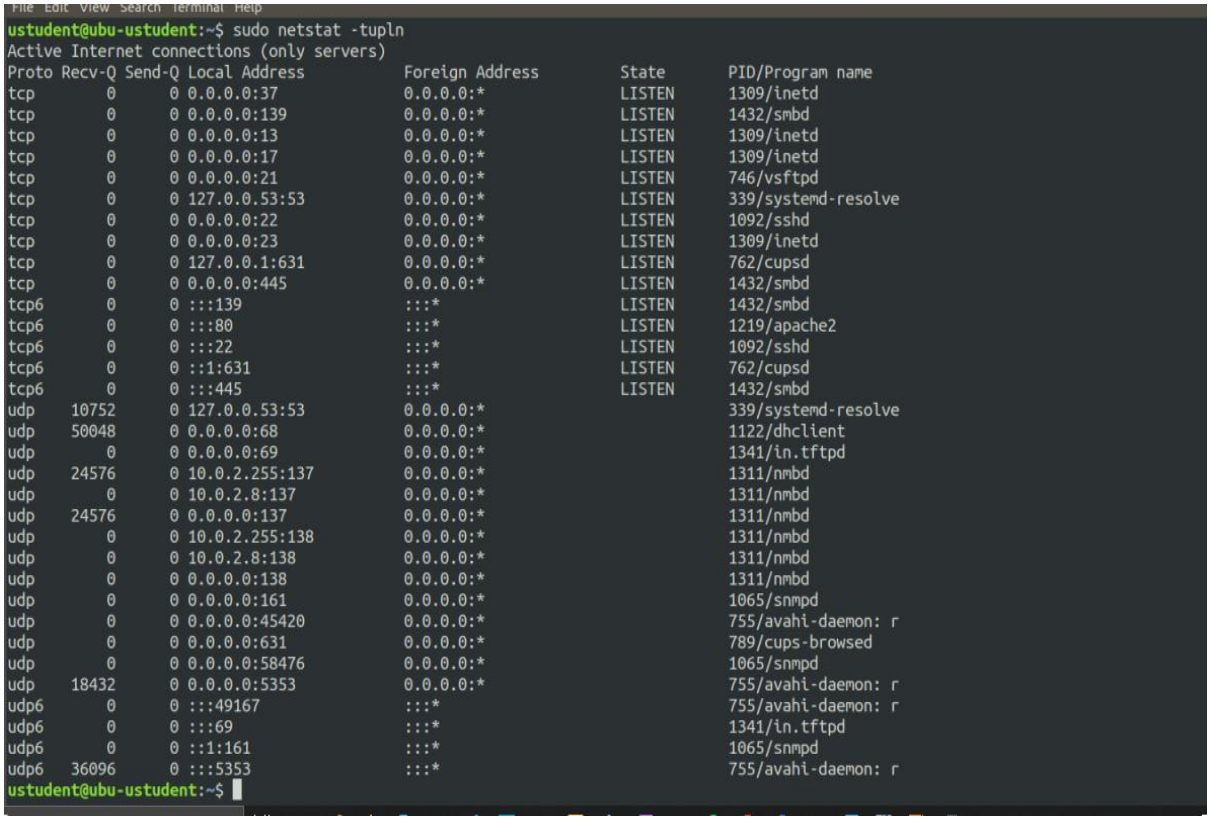
1. Disable unnecessary services: Echo, Discard, Daytime, Quote of the Day (QOTD), and Character Generator (CHARGEN) services are rarely used and can be disabled. Disabling these services will reduce the attack surface of your system.
2. Disable insecure protocols: The NetBIOS-SSN protocol (port 138/tcp) is often used by attackers to conduct reconnaissance and launch attacks. You should consider disabling this protocol if it is not required in your environment.
3. Harden the HTTP service: If the HTTP service (port 80/tcp) is required, it should be hardened by applying security patches, using secure configurations, and implementing HTTPS encryption.

In Ubuntu:

remote access service Policy not configured on ubuntu machine because the uwf not active

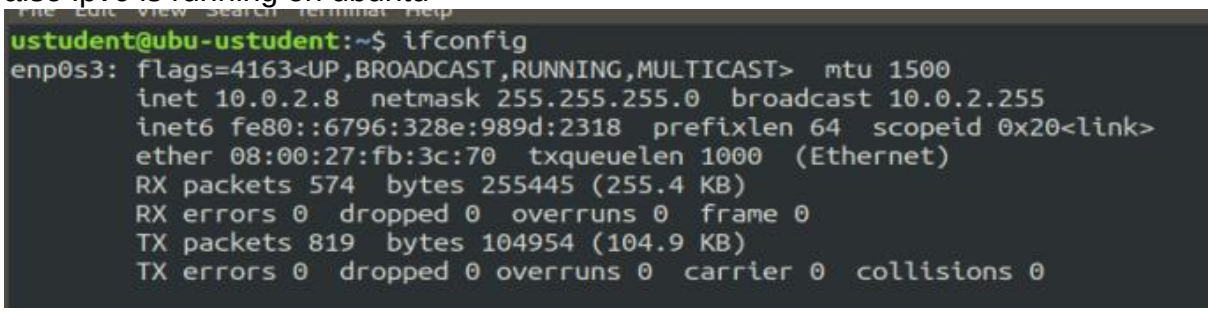
To list the remote service protocols, we could use “netstat -tuplan”

The Remote Service Protocols are Running on Ubuntu Machine:



```
File  Edit  View  Search  Terminal  Help
ustudent@ubu-ustudent:~$ sudo netstat -tupln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:37              0.0.0.0:*               LISTEN      1309/inetd
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN      1432/smbd
tcp        0      0 0.0.0.0:13              0.0.0.0:*               LISTEN      1309/inetd
tcp        0      0 0.0.0.0:17              0.0.0.0:*               LISTEN      1309/inetd
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN      746/vsftpd
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      339/systemd-resolve
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1092/sshd
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN      1309/inetd
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      762/cupsd
tcp        0      0 0.0.0.0:445             0.0.0.0:*               LISTEN      1432/smbd
tcp6       0      0 :::139                  :::*                    LISTEN      1432/smbd
tcp6       0      0 :::80                   :::*                    LISTEN      1219/apache2
tcp6       0      0 :::22                   :::*                    LISTEN      1092/sshd
tcp6       0      0 ::1:631                 :::*                    LISTEN      762/cupsd
tcp6       0      0 :::445                  :::*                    LISTEN      1432/smbd
udp    10752      0 127.0.0.53:53           0.0.0.0:*                           339/systemd-resolve
udp    50048      0 0.0.0.0:68              0.0.0.0:*                           1122/dhclient
udp        0      0 0.0.0.0:69              0.0.0.0:*                           1341/in.tftpd
udp    24576      0 10.0.2.255:137          0.0.0.0:*                           1311/nmbd
udp        0      0 10.0.2.8:137            0.0.0.0:*                           1311/nmbd
udp    24576      0 0.0.0.0:137             0.0.0.0:*                           1311/nmbd
udp        0      0 10.0.2.255:138          0.0.0.0:*                           1311/nmbd
udp        0      0 10.0.2.8:138            0.0.0.0:*                           1311/nmbd
udp        0      0 0.0.0.0:138             0.0.0.0:*                           1311/nmbd
udp        0      0 0.0.0.0:161             0.0.0.0:*                           1065/snmpd
udp        0      0 0.0.0.0:45420           0.0.0.0:*                           755/avahi-daemon: r
udp        0      0 0.0.0.0:631             0.0.0.0:*                           789/cups-browsed
udp        0      0 0.0.0.0:58476           0.0.0.0:*                           1065/snmpd
udp    18432      0 0.0.0.0:5353            0.0.0.0:*                           755/avahi-daemon: r
udp6       0      0 :::49167                :::*                                755/avahi-daemon: r
udp6       0      0 :::69                   :::*                                1341/in.tftpd
udp6       0      0 ::1:161                 :::*                                1065/snmpd
udp6   36096      0 :::5353                 :::*                                755/avahi-daemon: r
ustudent@ubu-ustudent:~$
```

also ipv6 is running on ubuntu



```
ustudent@ubu-ustudent:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.8  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::6796:328e:989d:2318  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:fb:3c:70  txqueuelen 1000  (Ethernet)
        RX packets 574  bytes 255445 (255.4 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 819  bytes 104954 (104.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

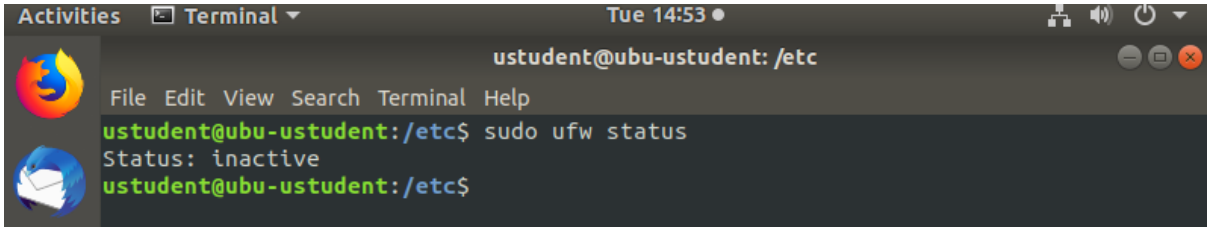
My Recommendation:

1. Only allowing necessary remote access services and protocols, and disabling or blocking all others.
2. Configuring the remote access services and protocols to use secure authentication and encryption methods, such as SSH with key-based authentication and encryption.

3. Monitoring and logging all remote access activity, and regularly reviewing the logs for any signs of unauthorized access or other security incidents.

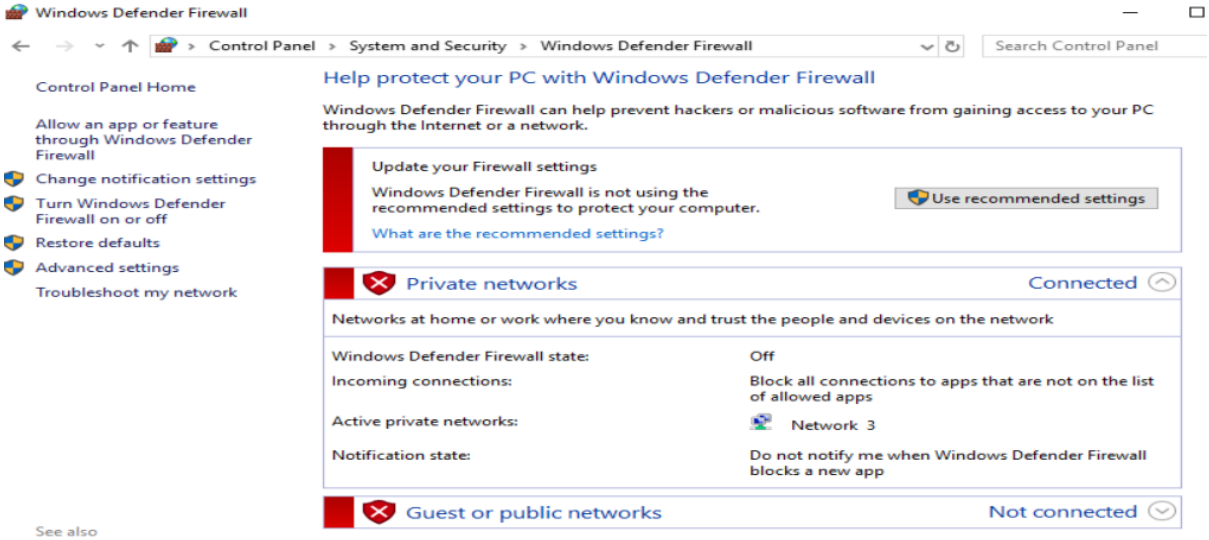
TASK 3

On Ubuntu Machine:



The firewall: inactive

On Windows Machine:



Also not Configured

this means that both machines are currently not protected by a firewall. This could potentially leave them vulnerable to unauthorized access and attacks from malicious actors.

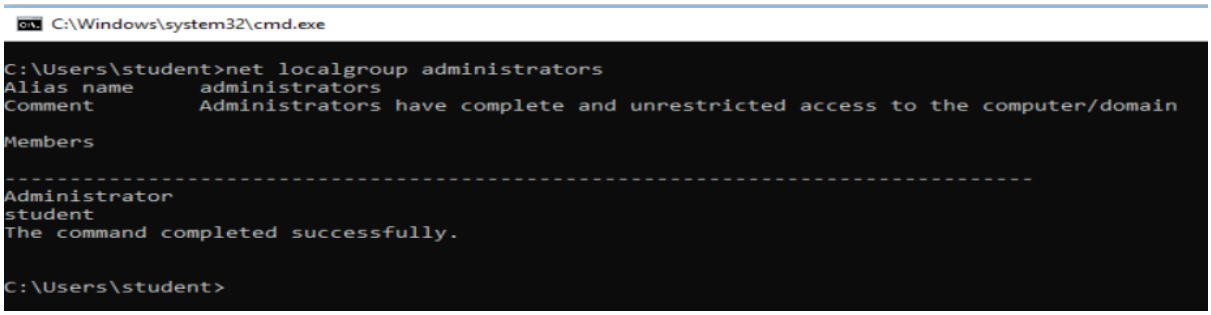
The ports that I suggest being open.

- Port 80 (HTTP): This is the standard port used for web traffic, and is required if you want to host a website on your server.
- Port 443 (HTTPS): This port is used for secure web traffic (encrypted with SSL/TLS) and is required if you want to host a website with HTTPS enabled.
- Port 22 (SSH): This port is used for secure shell (SSH) access, and is required if you want to remotely access your server or computer via SSH.
- Port 53 (DNS): This port is used for DNS traffic, and is required if you want to run a DNS server.

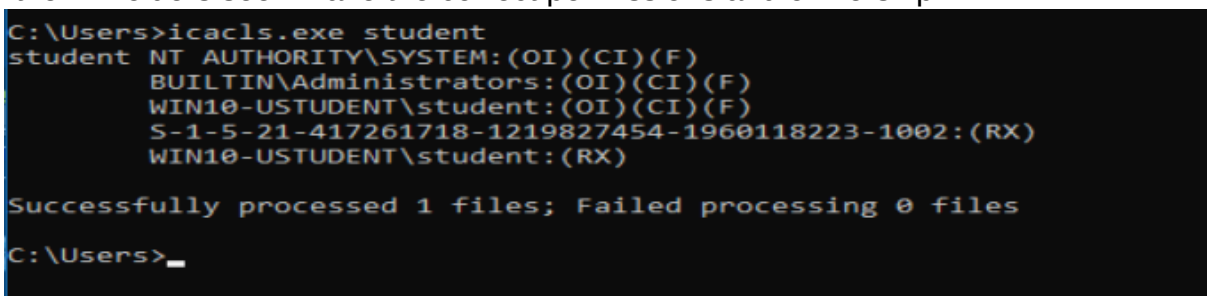
Task 4

On Windows

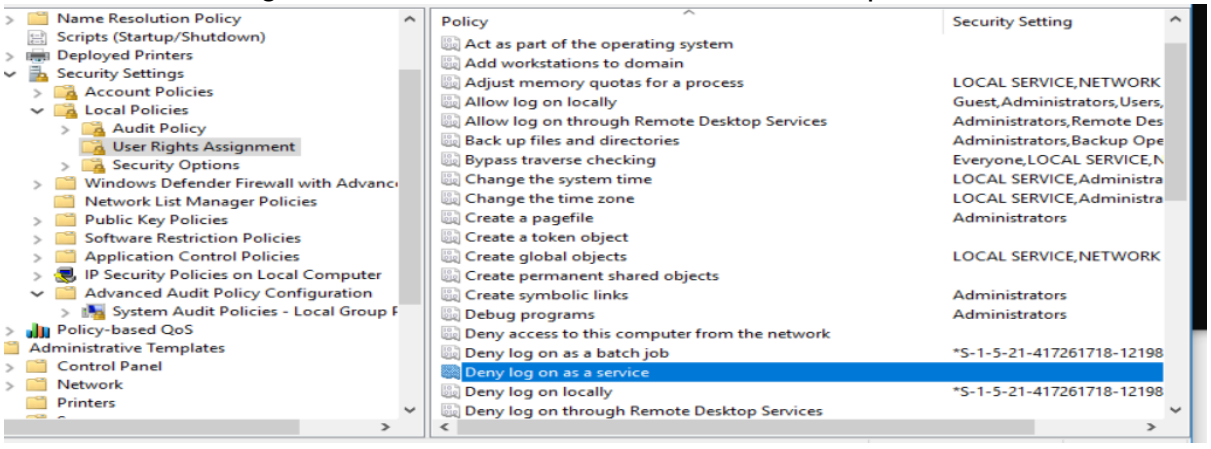
-The users with highest privileges
administrator, student



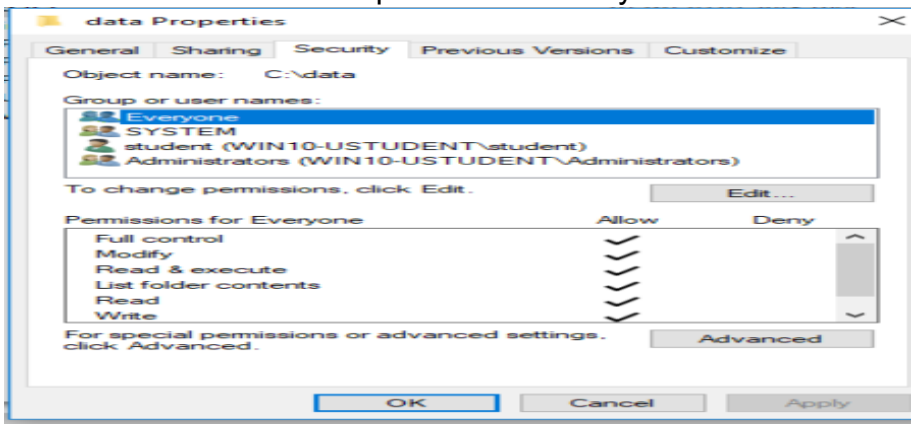
-the PII folders seem have the correct permissions and ownership



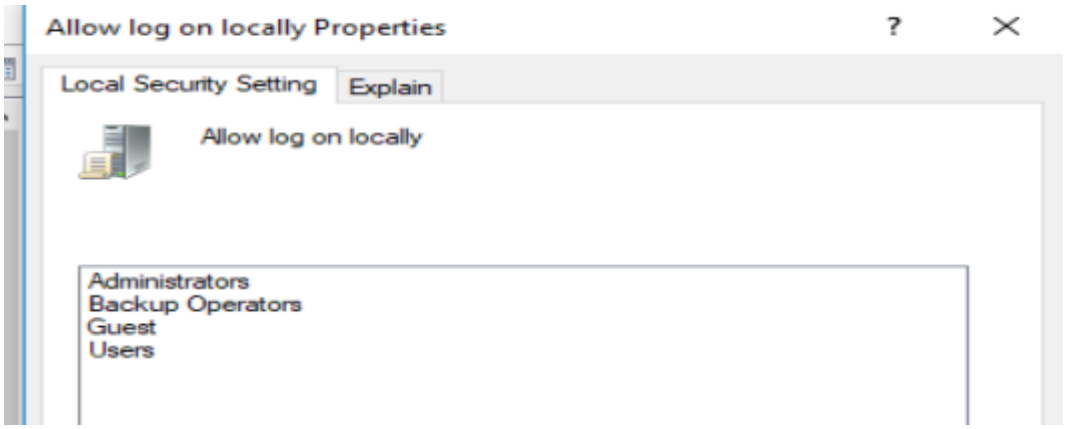
-The default settings seem correct and there's not excessive permissions



-The "data" Folder has no permissions everyone could access the folder.



-Guest Account Are enables, but Not have the administrator privilege, the guest user allowed only to log in locally



ON UBUNTU:

-The user who has the highest privileges : is the root

```
File  Edit  View  Search  Terminal  Help
ustudent@ubu-ustudent:/etc$ groups ustudent
ustudent : ustudent adm cdrom sudo dip plugdev lpadmin sambashare
ustudent@ubu-ustudent:/etc$ groups
ustudent adm cdrom sudo dip plugdev lpadmin sambashare
ustudent@ubu-ustudent:/etc$ users
ustudent
ustudent@ubu-ustudent:/etc$
```

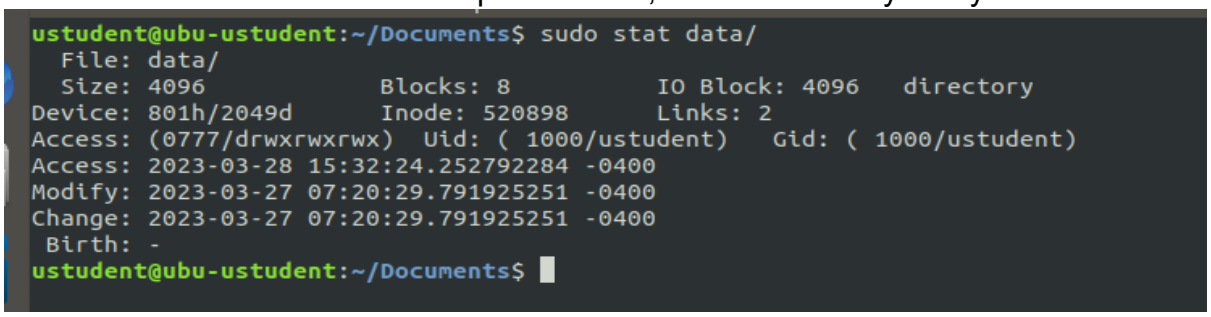
Also the members in the root group has the privilege so ustudent has high privilege

```
# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL
```

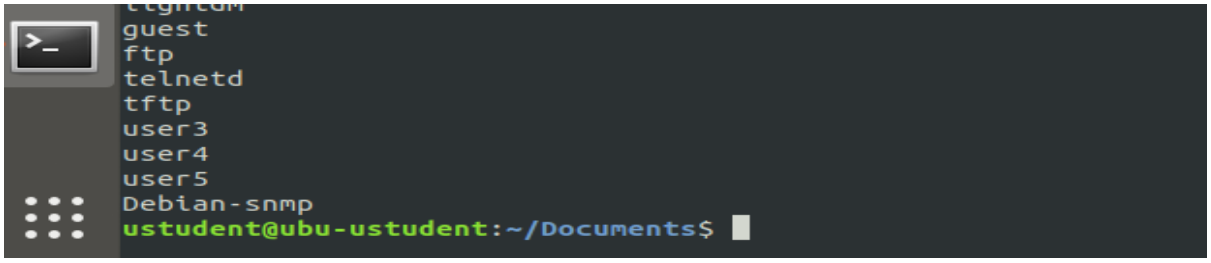
-the PII Folders don’t have the correct permissions ownership it should be 700 or 500

```
ustudent@ubu-ustudent:~$ sudo stat /home/ustudent/
[sudo] password for ustudent:
  File: /home/ustudent/
  Size: 4096            Blocks: 8          IO Block: 4096   directory
Device: 801h/2049d      Inode: 683954      Links: 20
Access: (0755/drwxr-xr-x)  Uid: ( 1000/ustudent)   Gid: ( 1000/ustudent)
Access: 2023-03-28 07:20:20.360779584 -0400
Modify: 2023-03-28 07:20:12.604779584 -0400
Change: 2023-03-28 07:20:12.604779584 -0400
 Birth: -
ustudent@ubu-ustudent:~$
```

-The “data” Shared folder has no permissions, its accessible by everyone



-There’s Guest user on , but aren’t allowed to use ‘sudo’ commands



Based on the findings:

1. Remove the guest account or limit its privileges: Since the guest account has no administrative privileges, it can be used by an attacker to gain access to your system. To prevent this, you can either remove the guest account entirely or limit its privileges by configuring Group Policy settings.
2. Review the permissions of the "DATA" folder: If the "DATA" folder is shared with no permissions, it means that anyone can access it without any restrictions. This could potentially lead to a data breach. To secure this folder, you should review the permissions and ensure that only authorized users have access to it.
3. Limit the number of accounts with administrative privileges: The more accounts that have administrative privileges, the more vulnerable your system is to attacks. You should limit the number of accounts with administrative privileges to only those who require them.

Step 3: Log Monitoring Setup for Detection at Targeted Assets

Task 1

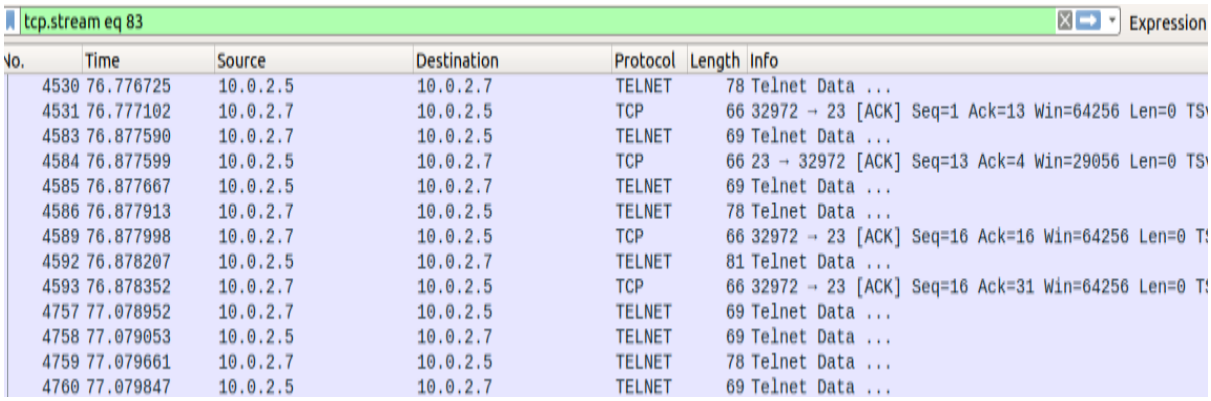
The attack type: Bruteforce

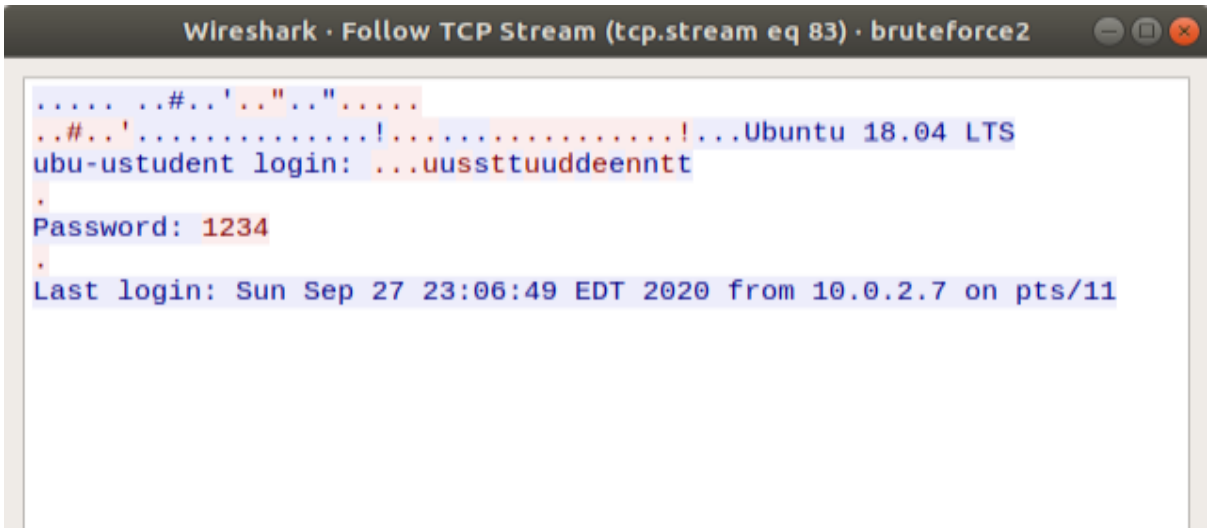
The source IP of attack is: 10.0.2.7

The Targeted protocol: telnet

The password used successfully: 1234

The user was compromised: ustudent





There was a bruteforce attack that targeted the telnet protocol

From ipaddress 10.0.2.7

And that attack able to compromised ustudent user on the machine

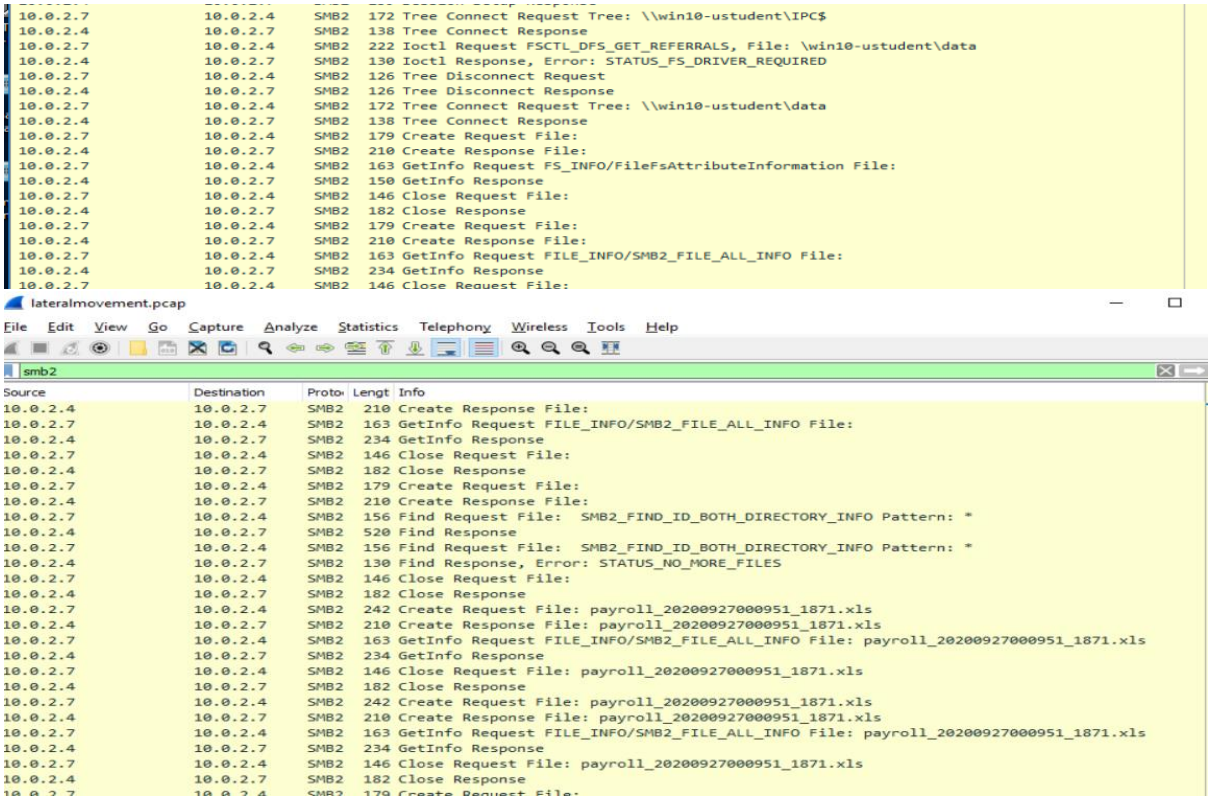
Task 2

The source of the initial attack: 10.0.2.7

Yes, the attacker tried to access the Machine from Compromised device

The service: NETBIOS ,SMB2 Protocol on port: 445

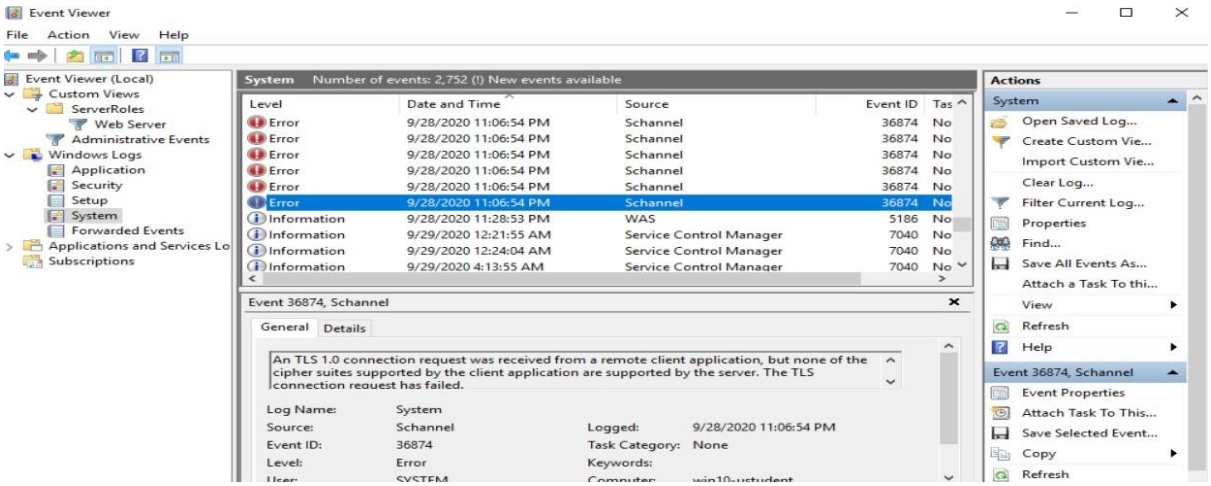
Yes, the attacker able to access a sensitive file at the machine using Mitre ATT&ACK Technique - T1570

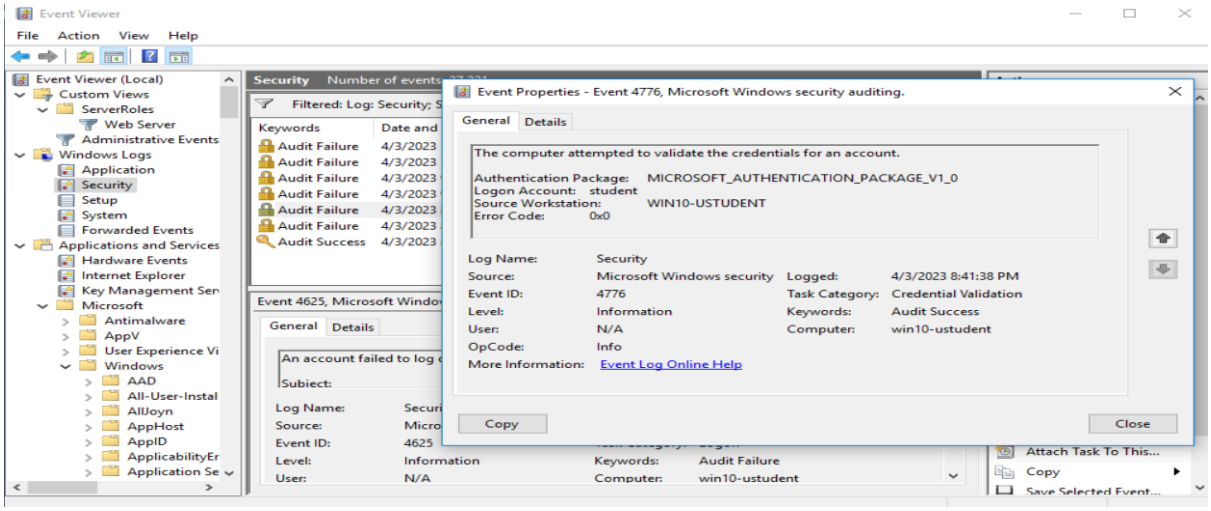


Based on the analysis of the pcap file, it appears that the attacker targeted the SMB2 protocol to gain access to the victim's machine. The attacker attempted to establish a session using the user account "./student" and was successful in gaining access to the victim's machine.

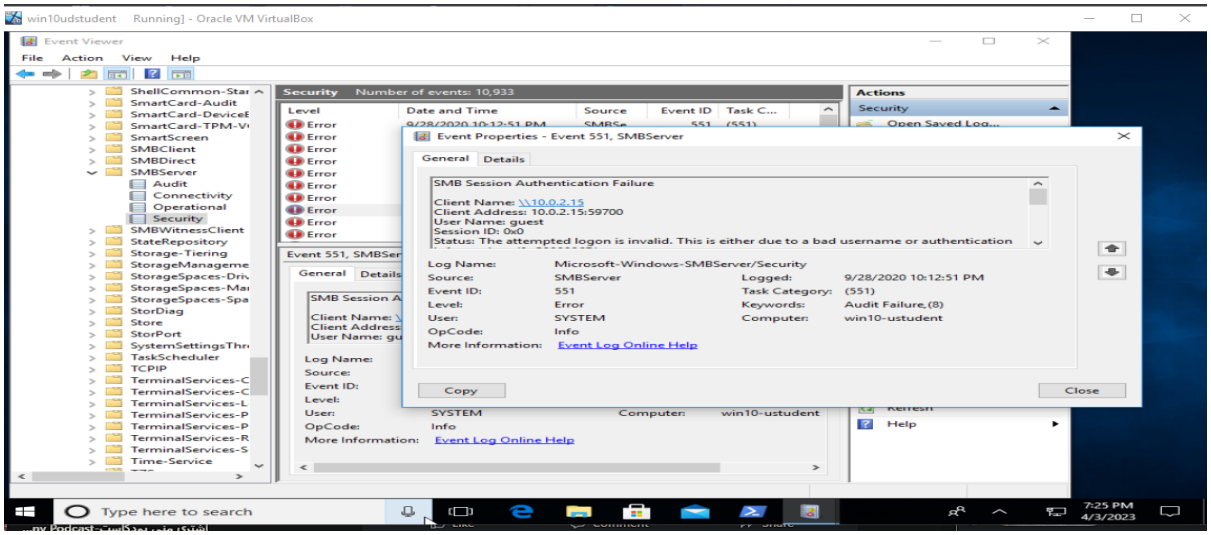
The attacker then attempted to access the user's data directory, but was denied access. The attacker then turned their attention to the workgroup of the user and was able to gain access to shared data.

Task 3


Event Viewer
File Action View Help
Event Viewer (Local)
Custom Views
ServerRoles
Web Server
Administrative Events
Windows Logs
Application
Security
Setup
System
Forwarded Events
Applications and Services Lo
Subscriptions
System Number of events: 2,752 (!) New events available
Level Date and Time Source Event ID Tas
Error 9/28/2020 11:06:54 PM Schannel 36874 No
Information 9/28/2020 11:28:53 PM WAS 5186 No
Information 9/29/2020 12:21:55 AM Service Control Manager 7040 No
Information 9/29/2020 12:24:04 AM Service Control Manager 7040 No
Information 9/29/2020 4:13:55 AM Service Control Manager 7040 No
Event 36874, Schannel
General Details
An TLS 1.0 connection request was received from a remote client application, but none of the cipher suites supported by the client application are supported by the server. The TLS connection request has failed.
Log Name: System
Source: Schannel
Logged: 9/28/2020 11:06:54 PM
Event ID: 36874
Task Category: None
Level: Error
Keywords:
Actions
System
Open Saved Log...
Create Custom Vie...
Import Custom Vie...
Clear Log...
Filter Current Log...
Properties
Find...
Save All Events As...
Attach a Task To thi...
View
Refresh
Help
Event 36874, Schannel
Event Properties
Attach Task To This...
Save Selected Event...
Copy
Refresh


Event Viewer
File Action View Help
Event Viewer (Local)
Custom Views
ServerRoles
Web Server
Administrative Events
Windows Logs
Application
Security
Setup
System
Forwarded Events
Applications and Services
Hardware Events
Internet Explorer
Key Management Ser
Microsoft
Antimalware
AppV
User Experience Vi
Windows
AAD
All-User-Instal
AllJoyn
AppHost
AppID
ApplicabilityEr
Application Se
Security Number of events
Filtered: Log: Security;
Keywords Date and
Audit Failure 4/3/2023
Audit Failure 4/3/2023
Audit Failure 4/3/2023
Audit Failure 4/3/2023
Audit Failure 4/3/2023
Audit Failure 4/3/2023
Audit Success 4/3/2023
Event 4625, Microsoft Windo
General Details
An account failed to log
Subject:
Log Name: Secur
Source: Micro
Event ID: 4625
Level: Information
User: N/A
Keywords: Audit Failure
Computer: win10-ustudent
Event Properties - Event 4776, Microsoft Windows security auditing.
General Details
The computer attempted to validate the credentials for an account.
Authentication Package: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Logon Account: student
Source Workstation: WIN10-USTUDENT
Error Code: 0x0
Log Name: Security
Source: Microsoft Windows security
Logged: 4/3/2023 8:41:38 PM
Event ID: 4776
Task Category: Credential Validation
Level: Information
Keywords: Audit Success
User: N/A
Computer: win10-ustudent
OpCode: Info
More Information: Event Log Online Help
Copy
Close
Attach Task To This...
Copy

Also there’s authentication failure with smb server



There is an issue with windows share.

On ubuntu:

I used “aureport” to filter all logs

The Name of The Attacker’s Account is: UNKNOWN

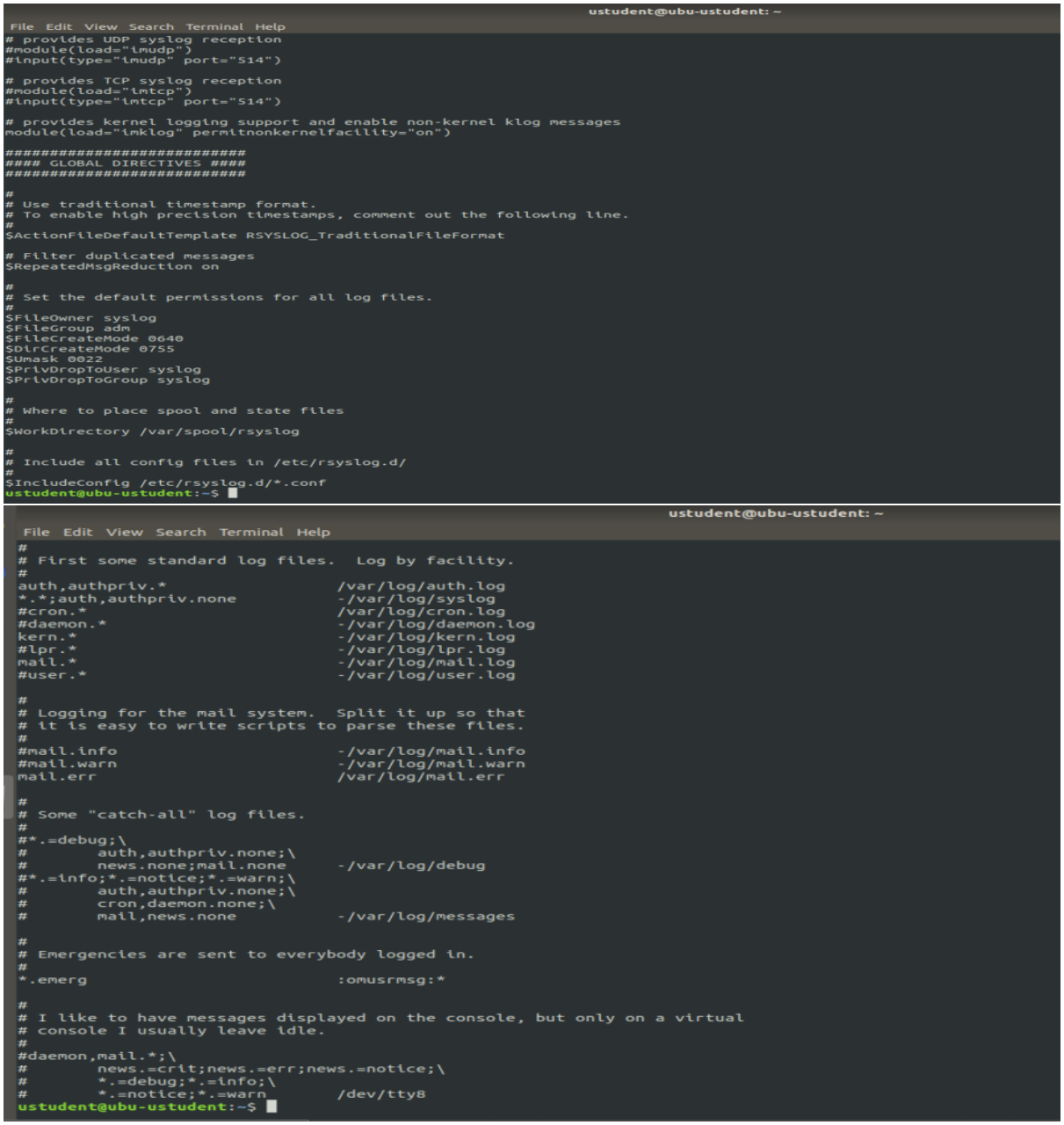
My assessment
Yes, these events are definitely enough to start an investigation, as they indicate a potential security breach or unauthorized access to the systems.

Task 4

In Ubuntu: Reviewing the contents of rsyslog.conf and rsyslog.d/*.conf files to ensure appropriate logging is set In addition, run the following command and verify that the

log
files are logging information:

```
# ls -l /var/log/
```



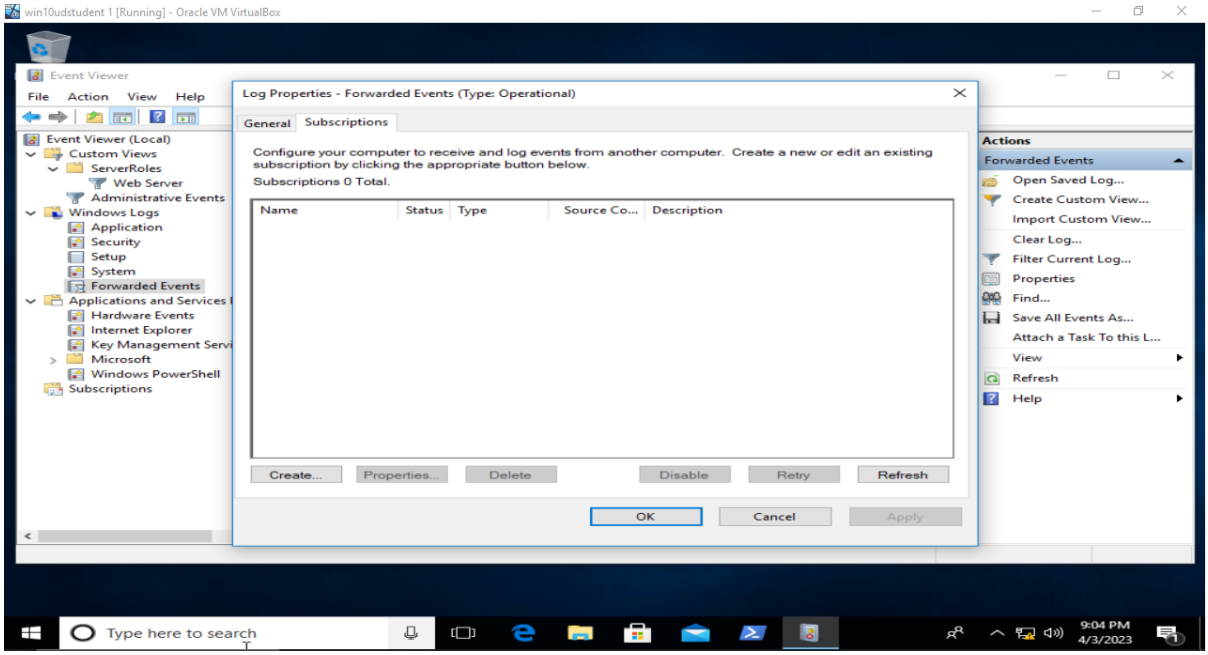
```
ustudent@ubu-ustudent: ~
File  Edit  View  Search  Terminal  Help
# provides UDP syslog reception
#module(load="imudp")
#input(type="imudp" port="514")

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

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

###########################
#### GLOBAL DIRECTIVES ####
###########################

#
# Use traditional timestamp format.
# To enable high precision timestamps, comment out the following line.
#
$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat

# Filter duplicated messages
$RepeatedMsgReduction on

#
# Set the default permissions for all log files.
#
$FileOwner syslog
$FileGroup adm
$FileCreateMode 0640
$DirCreateMode 0755
$Umask 0022
$PrivDropToUser syslog
$PrivDropToGroup syslog

#
# Where to place spool and state files
#
$WorkDirectory /var/spool/rsyslog

#
# Include all config files in /etc/rsyslog.d/
#
$IncludeConfig /etc/rsyslog.d/*.conf
ustudent@ubu-ustudent:~$
```



```
ustudent@ubu-ustudent: ~
File  Edit  View  Search  Terminal  Help
#
# First some standard log files.  Log by facility.
#
auth,authpriv.*                 /var/log/auth.log
*.*;auth,authpriv.none          -/var/log/syslog
#cron.*                         /var/log/cron.log
#daemon.*                       -/var/log/daemon.log
kern.*                          -/var/log/kern.log
#lpr.*                          -/var/log/lpr.log
mail.*                          -/var/log/mail.log
#user.*                         -/var/log/user.log

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

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

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

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

the machine is not currently configured to forward events to a centralized location In this case, you may need to configure the machine by editing the rsyslog.conf and rsyslog.d/*.conf files to set it up correctly for your SIEM.

IN Windows:



There’s no subscriptions.
after checking the event viewer I found that, the machine is not currently configured to forward events to a centralized location using the Windows Event Forwarder. In this case, you may need to configure the machine to use the Windows Event Forwarder and set it up correctly for your SIEM.

Step 4: Assess Authentication Management at Targeted Assets

Task 1

Administrator and remote Desktop users which is “guest” user can remotely access windows machine.

Root access permitted at Linux host

```
ustudent@ubu-ustudent:~$ sudo su -
root@ubu-ustudent:~#
```

The users with executive permissions on Linux: ustudent

```
ustudent@ubu-ustudent:~$ sudo -l
[sudo] password for ustudent:
Matching Defaults entries for ustudent on ubu-ustudent:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bi
n\:/snap/bin

User ustudent may run the following commands on ubu-ustudent:
    (ALL : ALL) ALL
ustudent@ubu-ustudent:~$
```

On windows there’s no users with executive permissions

root remote login not allowed after checking /etc/ssh/sshd_config

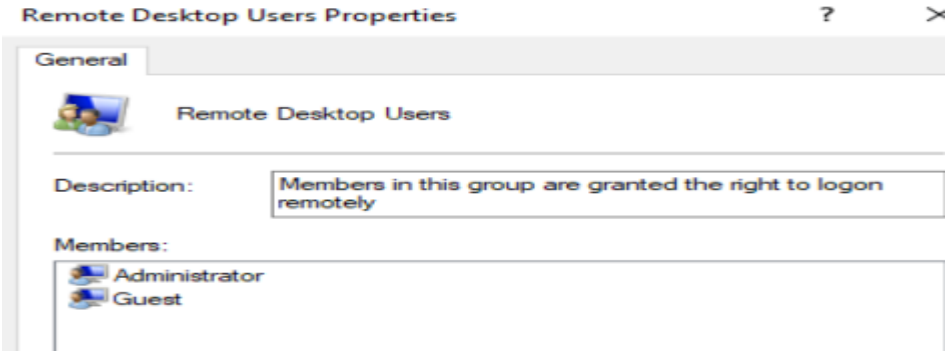
```
#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

```
root@ubu-ustudent:~# ssh 10.0.2.7
root@10.0.2.7's password:
Permission denied, please try again.
root@10.0.2.7's password:
Permission denied, please try again.
root@10.0.2.7's password:
root@10.0.2.7: Permission denied (publickey,password).
root@ubu-ustudent:~#
```

there is users that should not have remote access via ssh in Linux
because ustudent has sudo privileges

```
ustudent@ubu-ustudent:/etc/ssh$ ssh ustudent@10.0.2.7
ustudent@10.0.2.7's password:
Welcome to Ubuntu 18.04 LTS (GNU/Linux 4.15.0-20-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

0 packages can be updated.
0 updates are security updates.

Welcome Udacity Student
Last login: Sun Sep 27 23:07:17 2020 from 10.0.2.7
```

In Windows:



there is other account that has been given remote desktop access

Summary:

- On the Windows machine, both the **Administrator** and **Remote Desktop Users** group, which includes the **Guest** user, have remote access to the machine. No users have excessive permissions.
- On the Ubuntu machine, the **ustudent** user has executive permissions and root access is permitted. However, remote login as root is not allowed. There are users that should not have remote access via ssh, including **ustudent** who has sudo privileges.

In order to improve the security of both machines, the following recommendations can be made:

- On the Windows machine, it is recommended to remove the Guest user from the Remote Desktop Users group to limit access to only administrators. Other non-administrative accounts should not be granted remote access.
- On the Ubuntu machine, it is recommended to disable root login entirely and ensure that only necessary users have ssh access. The ustudent account, which has sudo privileges, should not be granted remote access via ssh. Instead, a separate administrative account with limited permissions should be created for remote access.

Task 2

audit the password policies in Ubuntu according to CIS Benchmarks 5.3.1

Audit:

Verify password creation requirements conform to organization policy.
Run the following command to verify the minimum password length is 14 or more characters.

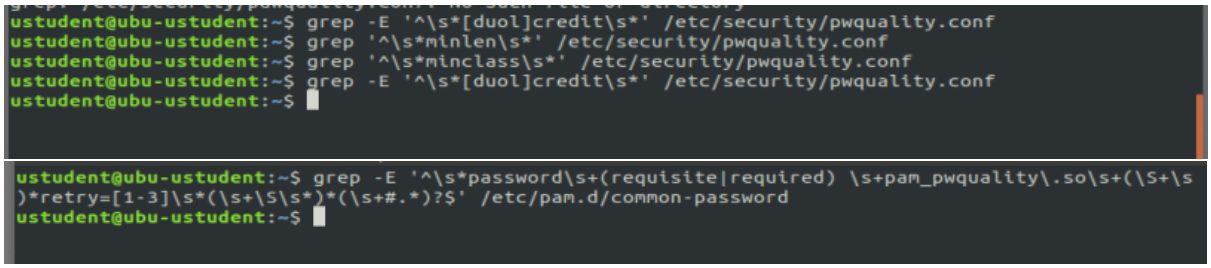
```
# grep '^\s*minlen\s*' /etc/security/pwquality.conf

minlen = 14
```

Run one of the following commands to verify the required password complexity:

```
# grep '^\s*minclass\s*' /etc/security/pwquality.conf

minclass = 4
```

OR

```
# grep -E '^\s*[duol]credit\s*' /etc/security/pwquality.conf

dcredit = -1
ucredit = -1
lcredit = -1
ocredit = -1
```



The commands don’t return any output which mean it’s not applicable After checking the system isn’t comply.

To remediate it

Run the following command to install the pam_pwquality module:

```
apt install libpam-pwquality
```

Edit the file `/etc/security/pwquality.conf` and add or modify the following line for password length to conform to site policy

```
minlen = 14
```

Edit the file /etc/security/pwquality.conf and add or modify the following line for password complexity to conform to site policy

```
minclass = 4
```

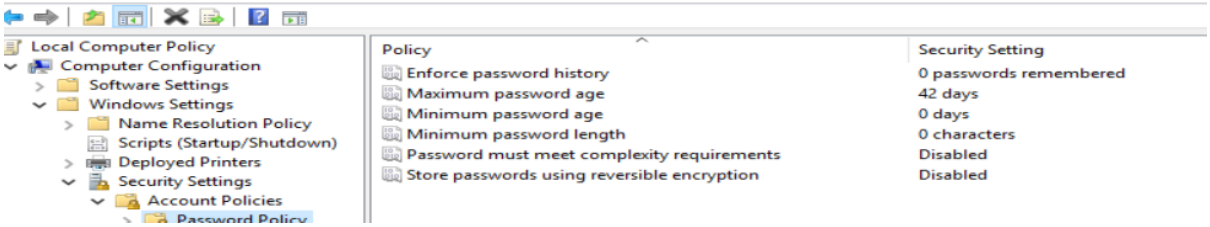
OR

```
dcredit = -1
ucredit = -1
ocredit = -1
lcredit = -1
```

Edit the `/etc/pam.d/common-password` file to include the appropriate options for `pam_pwquality.so` and to conform to site policy:

```
password requisite pam_pwquality.so retry=3
```

In Windows: we need to *Ensure 'Password must meet complexity requirements'*



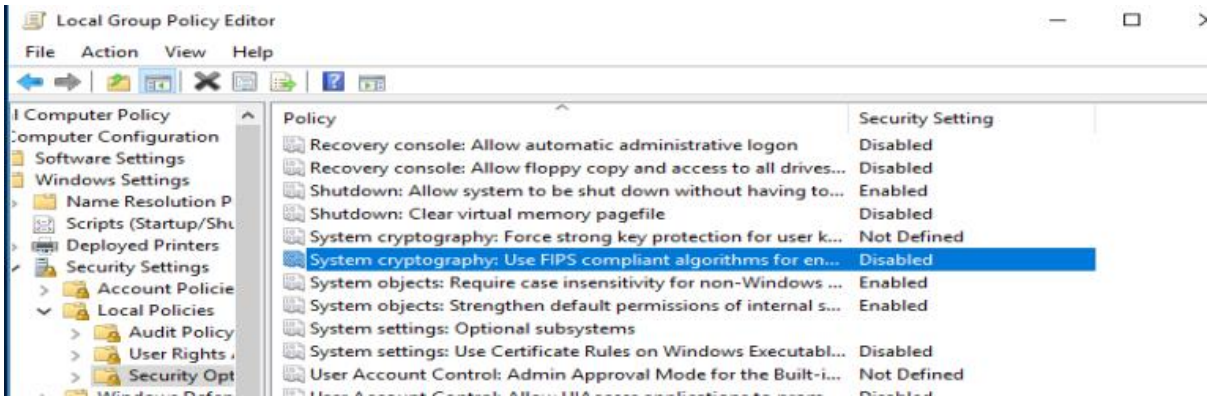
The current setting doesn't comply with the windows 10 CIS benchmarks 1.1.5

Overview:

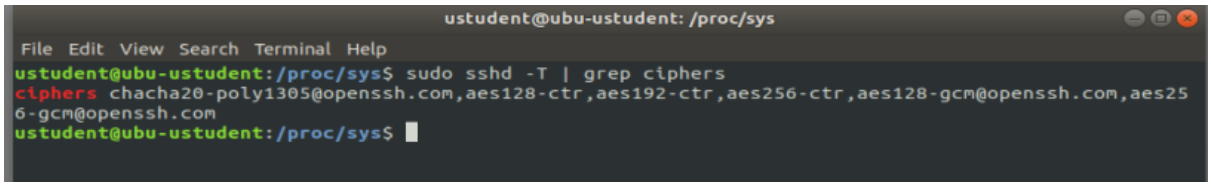
1. Password creation requirements: The password creation requirements should be set to ensure that passwords are strong and difficult to guess. This includes setting a minimum password length, requiring a combination of uppercase and lowercase letters, numbers, and special characters. The specific settings may vary depending on the organization's policy, but typically a minimum length of 8-12 characters is recommended.
2. Password complexity: The password complexity requirements should also be set to ensure that passwords are difficult to guess. This includes requiring a combination of uppercase and lowercase letters, numbers, and special characters. Additionally, common words, phrases, or patterns should be prohibited.
3. Failed login attempts: The number of failed login attempts allowed before sending back a failure should be set to a value that is in line with the organization's policy. Typically, a value of 5-10 failed attempts is recommended, depending on the organization's risk tolerance.

Task 3

Windows Machine doesn't comply with the (FIPS 140-2) policy



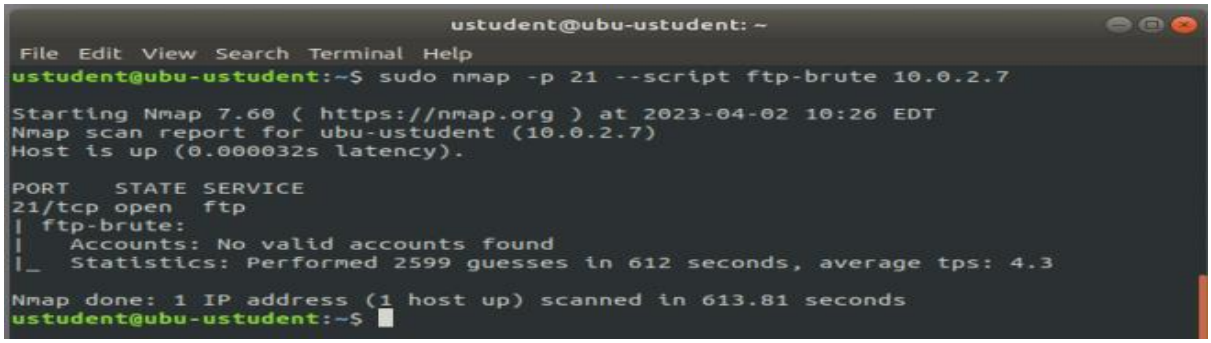
In Ubuntu



The systems aren't compliant, we need to configure the system to use FIPS 140-2 compliant cryptographic algorithms and modules. This can typically be done through the system's security policy settings. For Windows, you can use the Local Security Policy editor or Group Policy Editor to configure the system to use FIPS-compliant cryptography.
For Ubuntu, you can modify the system-wide OpenSSL configuration file located at /etc/ssl/openssl.cnf.

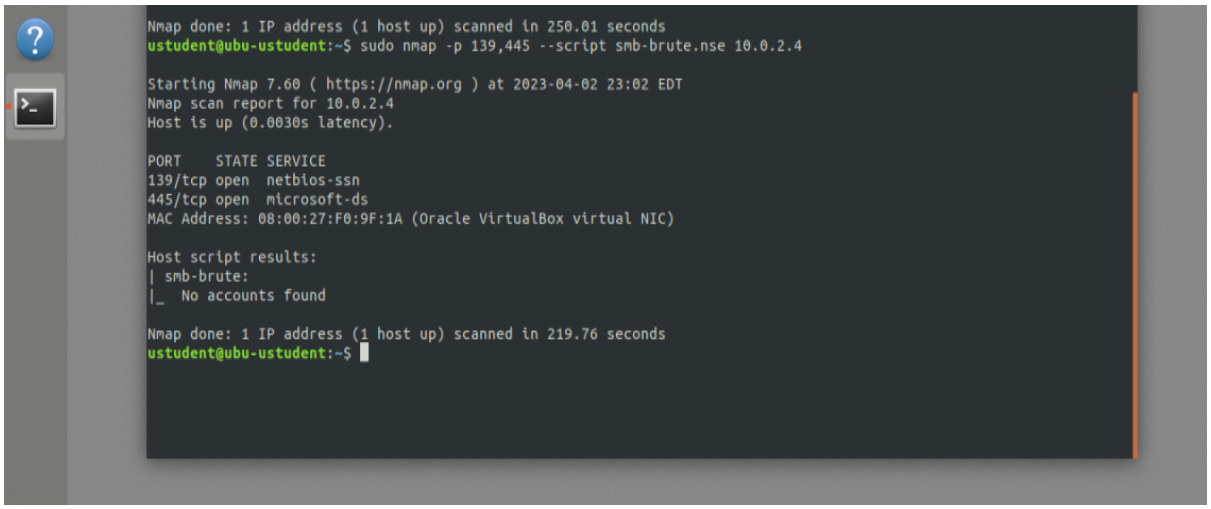
Task 4

On Ubuntu Machine:



- The result of the ftp-brute script indicates that no valid accounts were found on the target FTP server after attempting 2599 guesses. This suggests that the FTP server has strong password protection and the default or common usernames and passwords have not been used.
- The security state of the FTP server seems to be in good condition as the script was unable to successfully authenticate any valid accounts.

On Window Machine:



The results of the smb-brute script indicate that no accounts were found during the scan, which means that the script was not able to brute force or guess any valid login credentials for the SMB service on your Windows machine.

From a security perspective, this is a good result because it suggests that your SMB service is not vulnerable to brute force attacks.

The security state of these services can be improved. For example, you can secure the FTP server by enforcing secure authentication methods such as publickey and disabling the use of weak passwords. For the Windows SMB share, you can disable anonymous access and enable message signing to provide better protection against unauthorized access and tampering.

Step 5: Final Report

Windows 10 ENT

Ex

Host	High	Medium	Low	Log
10.0.2.4	3	3	1	1

IP Address: 10.0.2.4

Service	Port	Sensitive Level
discard	9 TCP	High
SMB protocol	445 TCP	High
echo	7 TCP	Medium
SMB	445 TCP	Medium
ICMP	general TCP	Low
HTTP HEADERS	TCP	Log

Expected detail format for vulnerabilities found.

High

1- CVE-1999-0636

Issue

The remote host is running a 'discard' service.
This service is unused these days, so it is advised that you disable it.

Impact

This service typically sets up a listening socket
and will ignore all the data which it receives.

Mitigation

Under Windows systems, set the following registry key to 0:
HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpDiscard
Then launch cmd.exe and type:
net stop simptcp
net start simptcp
To restart the service.

Reference

Details: Check for discard Service
OID:1.3.6.1.4.1.25623.1.0.11367
Version used: 2020-10-01T11:33:30Z

High

1- CVE-1999-0503

Issue

A number of known default credentials are tried for the login via the SMB protocol.

Impact

It was possible to login with the following credentials via the SMB protocol to
,!the 'IPC$' share. <User>:<Password>
operator:1234

Mitigation

Enforce strong password policies: This involves requiring complex passwords that are difficult to guess and ensuring that users change their passwords regularly.

Reference

cve: CVE-1999-0503
cve: CVE-1999-0504
cve: CVE-1999-0505
cve: CVE-1999-0506

High

1- CVE-2017-7494

Issue

known as the SAMBA Remote Code Execution from Writable Share vulnerability

Impact

It allows a remote attacker to execute arbitrary code with root privileges by uploading a shared library to a writable share on a vulnerable system and then causing Samba to load and execute the library.

Mitigation

To remediate this vulnerability, it is recommended to update the Samba software to a patched version.
Reference

Medium

1- CVE-1999-0635

Issue

An echo Service is running at this Host via TCP and/or UDP.

Impact

The echo service is an Internet protocol de ned in RFC 862. It was originally proposed for testing

and measurement of round-trip times in IP networks. While still available on most UNIX-like
operating systems, testing and measurement is now performed with the Internet Control Message

Mitigation

Solution type: Mitigation
Disable the echo Service.

Reference

cve: CVE-1999-0635

Medium

1- CVE-1999-0635

Issue

It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this
system.

Impact

An attacker might be able to use the known cryptographic aws to eavesdrop the connection
between clients and the service to get access to sensitive data transferred within the secured
connection.

Mitigation

It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the
TLSv1.2+ protocols. Please see the references for more information.

Reference

cve: CVE-2015-0204
cve: CVE-2011-3389

Low

1- CVE-1999-0524

Issue

The impact of this vulnerability is that it can allow an attacker to bypass certain security checks and access files or resources that they would not otherwise be able to access.

Impact

The remote host responded to an ICMP timestamp request.

Mitigation

- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks).

Reference
cve: CVE-1999-0524

url: http://www.ietf.org/rfc/rfc0792.txt

cert-bund: CB-K15/1514

cert-bund: CB-K14/0632

dfn-cert: DFN-CERT-2014-0658

Log

8- HTTP Security Headers Detection

Issue

Known security headers are being checked on the host.

Impact

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

References

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

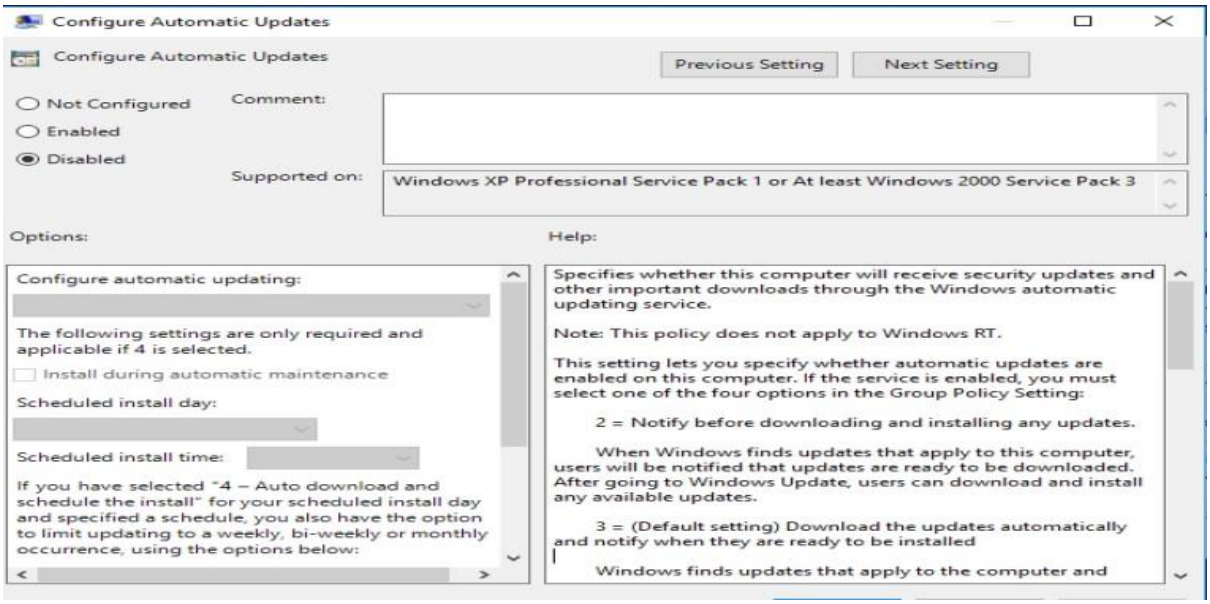
https://owasp.org/www-project-secure-headers/#div-headers

https://securityheaders.io

Example of control checks & CIS benchmarks Windows 10 ENT

18.9.102.2 (L1) Ensure 'Configure Automatic Updates' is set to 'Enabled'
(Automated)

Result: not compliant, the policy is Disabled



Impact: Critical operating system updates and service packs will be installed as necessary.

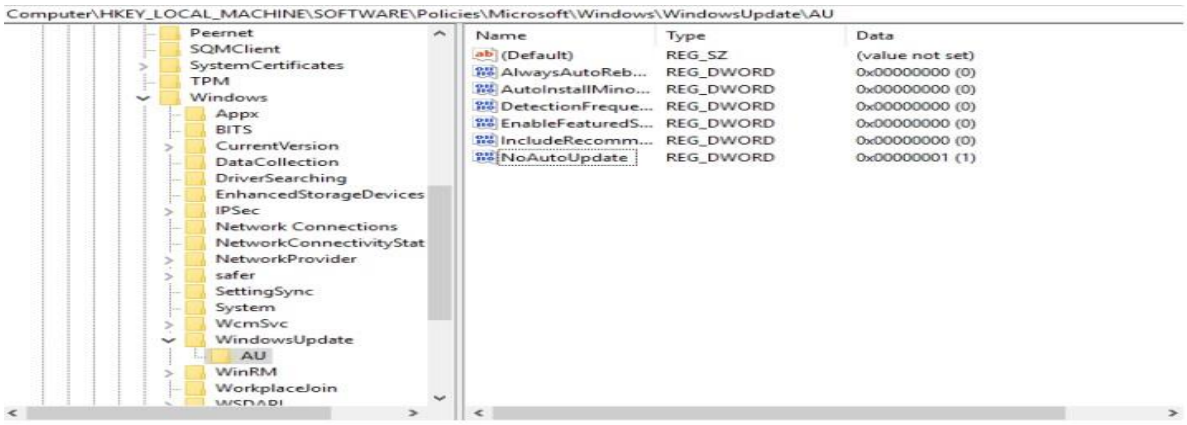
CIS Controls:
Version 7
3.4 Deploy Automated Operating System Patch Management Tools
Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.
3.5 Deploy Automated Software Patch Management Tools
Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.

Ensure 'Enable Structured Exception Handling Overwrite Protection (SEHOP)'

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session
Manager\kernel:DisableExceptionChainValidation
```

Result: not compliant, there's no registry for it

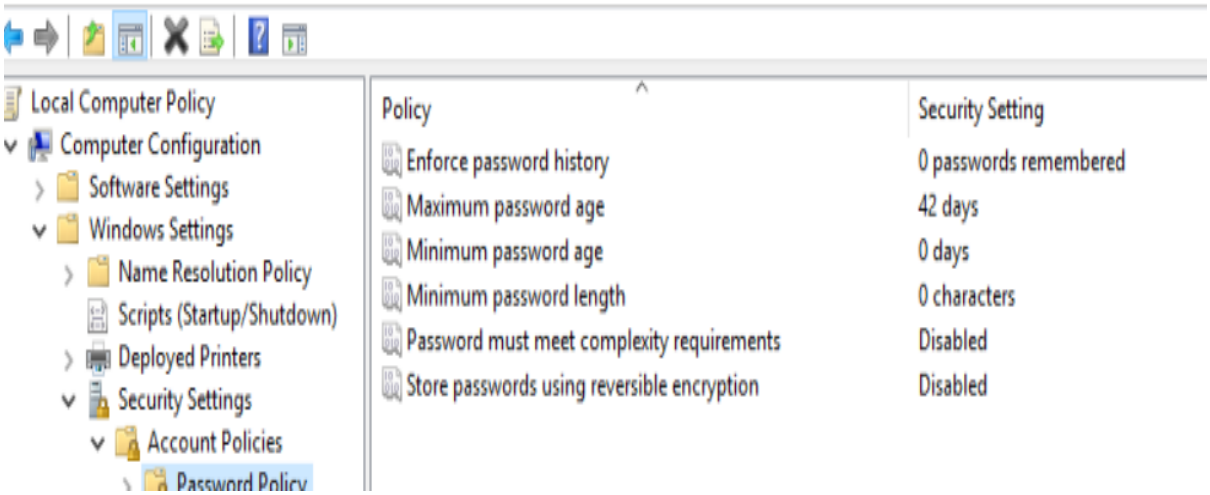


Impact: After you enable SEHOP, existing versions of Cygwin, Skype, and Armadillo-protected
applications may not work correctly.

CIS Controls:
Version 7
8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies
Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.
9.3 Perform Regular Automated Port Scans
Perform automated port scans on a regular basis against all systems and alert if unauthorized ports are detected on a system.

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

Result: not compliant.



Impact: If the default password complexity configuration is retained, additional help desk calls for
locked-out accounts could occur because users might not be accustomed to passwords that
contain non-alphabetic characters. However, all users should be able to comply with the complexity requirement with minimal difficulty

CIS Controls:
Version 7
10.4 Ensure Protection of Backups
Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.
13.6 Encrypt the Hard Drive of All Mobile Devices.
Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.

Ubuntu 18.04

Ex

Host	High	Medium	Low	Log
10.0.2.7	2	2	2	1

IP Address: xxx.xxx.xxx.xxx

Service	Port	Sensitive Level
NETBIOS-SSN SAMBA	445 TCP	High
broadcast-avahi-dos	UDP	High
Anonymous FTP Login	21 TCP	Medium
Telnet	23 TCP	Medium
TCP timestamps	General/TCP	Low
ICMP timestamps	General/ICMP	Low

Expected detail format for vulnerabilities found

High

1- cve-2017-7494

Issue
known as the SAMBA Remote Code Execution from Writable Share vulnerability, is a critical remote code execution vulnerability that affects the Samba file-sharing software
Impact
It allows a remote attacker to execute arbitrary code with root privileges by uploading a shared library to a writable share on a vulnerable system and then causing Samba to load and execute the library.
Mitigation
To remediate this vulnerability, it is recommended to update the Samba software to a patched version. The vulnerability was fixed in Samba versions 4.6.4, 4.5.10, and 4.4.14, so updating to one of these versions or a later version should resolve the issue

High

1- Cve-2011-1002

Issue
vulnerability is a buffer overflow vulnerability that affects the Avahi daemon,
Impact
It can be exploited by a remote attacker to send specially crafted packets to a vulnerable system, causing a denial of service (DoS)
Mitigation
To remediate this vulnerability, it is recommended to update the affected system with the latest security patches provided by the vendor.
Reference
NVD (National Vulnerability Database) entry: https://nvd.nist.gov/vuln/detail/CVE-2011-1002
Red Hat Security Advisory: https://access.redhat.com/security/cve/cve-2011-1002
Apache HTTP Server 2.2.18 release notes: https://www.apache.org/dist/httpd/Announcement2.2.html#2.2.18

Medium

1- CVE-2017-1000030

Issue
a remote attacker can bypass authentication and access sensitive data on an FTP server
Impact
Based on the files accessible via this anonymous FTP login and the permissions of this account
an attacker might be able to:
- gain access to sensitive files
- upload or delete files
Mitigation
you should disable anonymous logins.
Reference
NVD (National Vulnerability Database) entry: https://nvd.nist.gov/vuln/detail/CVE-2017-1000030
Red Hat Security Advisory: https://access.redhat.com/security/cve/cve-2017-1000030
Debian Security Advisory: https://www.debian.org/security/2017/dsa-3889

Medium

1- CVE-2018-7640

Issue

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

Impact

An attacker can uncover login names and passwords by sni-ng tra-c to the Telnet service.

Mitigation

Replace Telnet with a protocol like SSH which supports encrypted connections.

Reference

NVD (National Vulnerability Database) entry: https://nvd.nist.gov/vuln/detail/CVE-2018-7640
Red Hat Security Advisory: https://access.redhat.com/security/cve/cve-2018-7640
Debian Security Tracker: https://security-tracker.debian.org/tracker/CVE-2018-7640

Low

1- CVE-2018-7750

Issue

The remote host implements TCP timestamps and therefore allows to compute the uptime.

Impact

A side effect of this feature is that the uptime of the remote host can sometimes be computed

Mitigation

To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.
To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'

Reference

url: http://www.ietf.org/rfc/rfc1323.txt
url: http://www.ietf.org/rfc/rfc7323.txt
url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d,download/details.aspx?id=9152

Low

1- CVE-2018-7750

Issue

The remote host responded to an ICMP timestamp request.

Impact

it allows an attacker to send specially crafted ICMP packets with malicious timestamp values to a target system. This can result in a denial-of-service (DoS) condition or remote code execution on the affected system

Mitigation

Various mitigations are possible:
- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

Reference

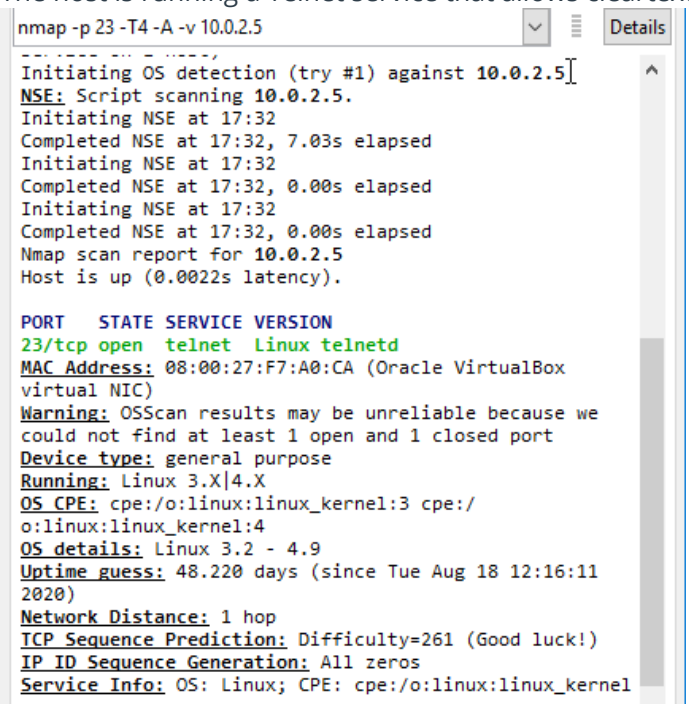
cve: CVE-1999-0524
url: http://www.ietf.org/rfc/rfc0792.txt
cert-bund: CB-K15/1514
cert-bund: CB-K14/0632
dfn-cert: DFN-CERT-2014-0658

Example of Log

Log

3 - Telnet Unencrypted Cleartext Login

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



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

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

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

Example of control checks & CIS benchmarks Ubuntu 18.04

Ensure package manager repositories are configured

Result:

```
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:
```

Impact: Systems need to have package manager repositories configured to ensure they receive the
latest patches and updates

Ensure XD/NX support is enabled

Result: XD/NX support is enabled

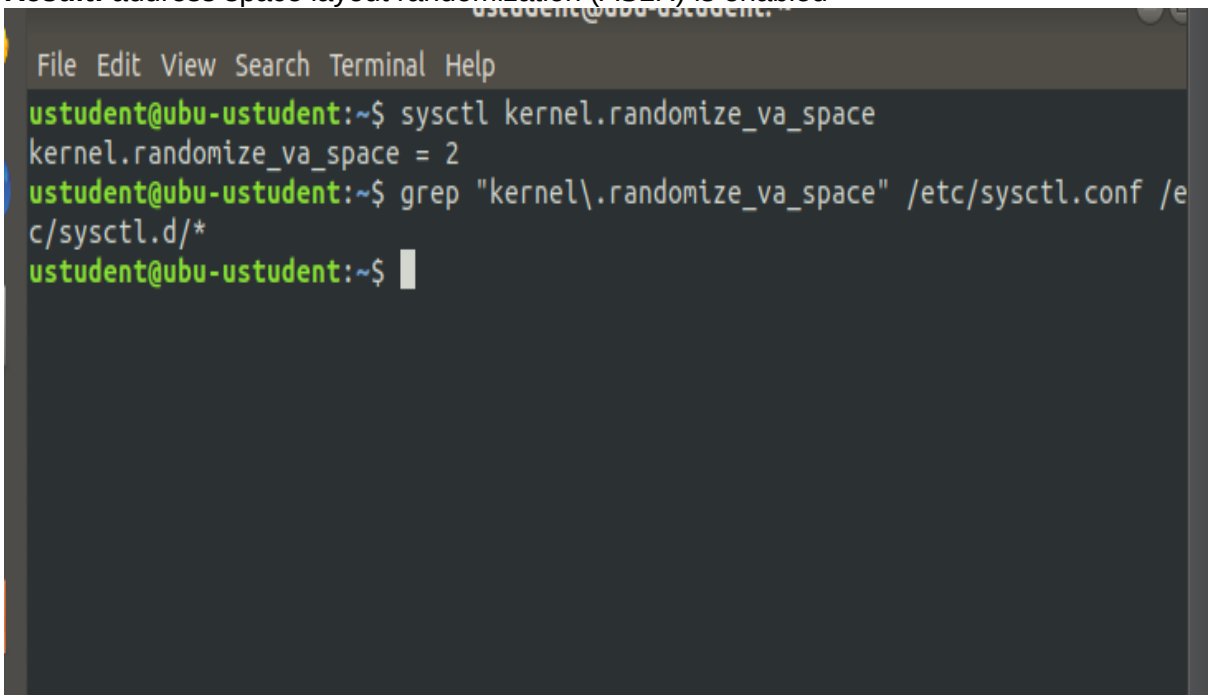
```
ustudent@ubu-ustudent:~$ journalctl | grep 'protection: active'
Sep 26 13:59:39 ubu-ustudent kernel: NX (Execute Disable) protection: active
Sep 26 14:14:17 ubu-ustudent kernel: NX (Execute Disable) protection: active
Sep 26 14:19:04 ubu-ustudent kernel: NX (Execute Disable) protection: active
Sep 26 15:11:14 ubu-ustudent kernel: NX (Execute Disable) protection: active
Sep 26 15:14:20 ubu-ustudent kernel: NX (Execute Disable) protection: active
Sep 26 15:15:51 ubu-ustudent kernel: NX (Execute Disable) protection: active
Sep 26 15:36:27 ubu-ustudent kernel: NX (Execute Disable) protection: active
Sep 26 19:42:51 ubu-ustudent kernel: NX (Execute Disable) protection: active
Sep 27 09:42:18 ubu-ustudent kernel: NX (Execute Disable) protection: active
Sep 27 10:25:06 ubu-ustudent kernel: NX (Execute Disable) protection: active
Sep 27 10:29:55 ubu-ustudent kernel: NX (Execute Disable) protection: active
Sep 27 11:04:27 ubu-ustudent kernel: NX (Execute Disable) protection: active
Sep 27 11:07:41 ubu-ustudent kernel: NX (Execute Disable) protection: active
Sep 27 11:50:26 ubu-ustudent kernel: NX (Execute Disable) protection: active
Sep 27 21:29:42 ubu-ustudent kernel: NX (Execute Disable) protection: active
Sep 28 11:55:22 ubu-ustudent kernel: NX (Execute Disable) protection: active
Sep 28 12:42:02 ubu-ustudent kernel: NX (Execute Disable) protection: active
Sep 28 22:35:02 ubu-ustudent kernel: NX (Execute Disable) protection: active
Mar 27 06:54:20 ubu-ustudent kernel: NX (Execute Disable) protection: active
ustudent@ubu-ustudent:~$
```

CIS Controls:
Version 7
8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit

Technologies
Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.

Ensure address space layout randomization (ASLR) is enabled

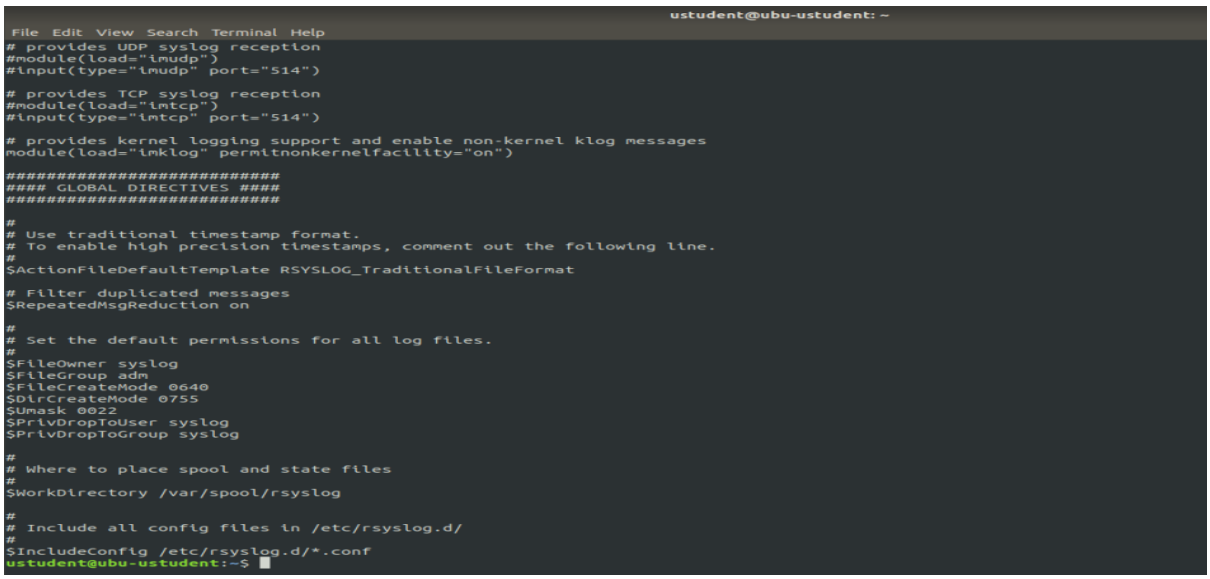
Result: address space layout randomization (ASLR) is enabled

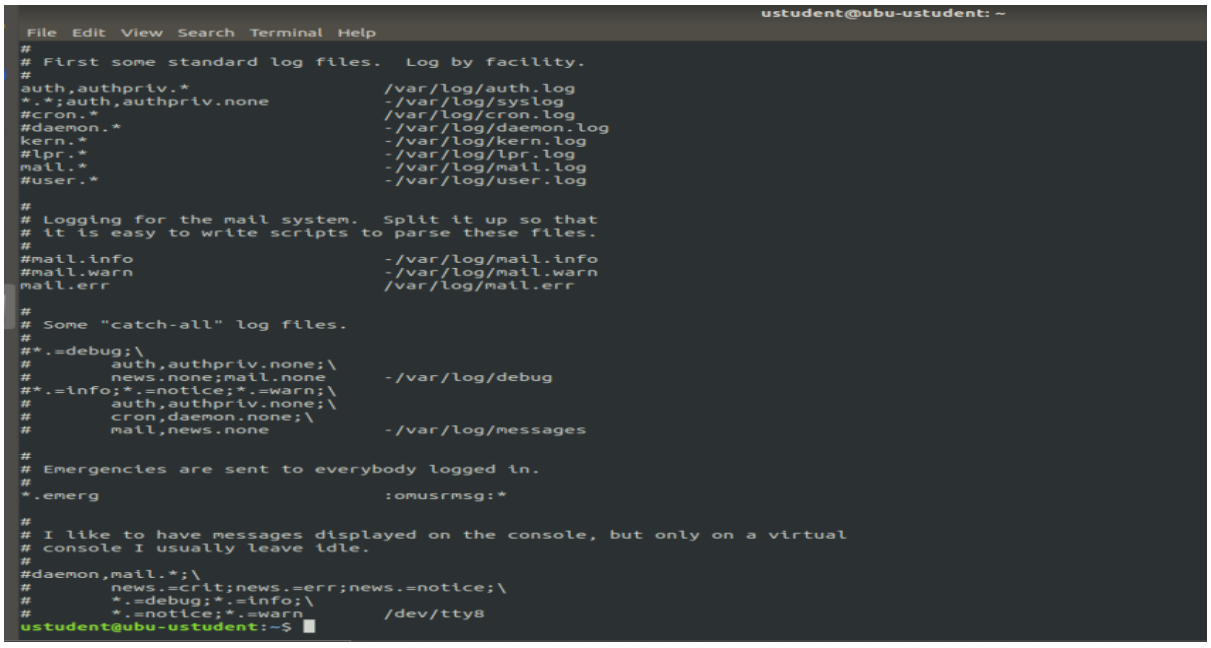


CIS Controls:
Version 7
8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies
Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables

Ensure logging is configured

Result:





Rationale:

A great deal of important security-related information is sent via `rsyslog` (e.g., successful
and failed su attempts, failed login attempts, root login attempts, etc.).

CIS Controls:

Version 7

6.2 Activate audit logging

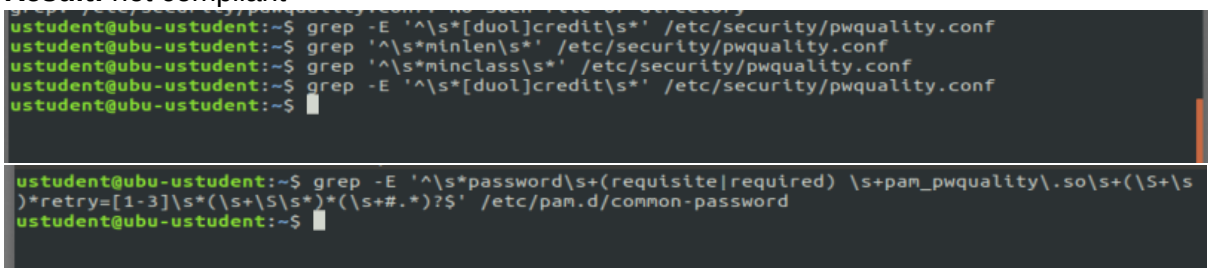
Ensure that local logging has been enabled on all systems and networking devices.

6.3 Enable Detailed Logging

Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

Ensure password creation requirements are configured

Result: not compliant



Impact:it can have a significant impact on the security of the system or platform that the password is protecting. Password requirements are put in place to ensure that passwords are strong, complex, and difficult for hackers to guess or crack.

CIS Controls:

Version 7

4.4 Use Unique Passwords

Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.

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

1. Vulnerabilities: Both machines have vulnerabilities that can be exploited by attackers, such as the NETBIOS-SSN samba vulnerability in Ubuntu and the SMB logon vulnerability in Windows. These vulnerabilities could be used to gain unauthorized access to the network and sensitive information.
2. Misconfigurations: There are several misconfigurations in both machines, such as the lack of software updates, incorrect permissions on PII folders, and anonymous access to shared folders. These misconfigurations could be used by attackers to gain unauthorized access and exfiltrate sensitive data.
3. Non-compliance: Both machines do not comply with certain policies, such as the FIPS 140-2 policy. Non-compliance could result in legal and financial liabilities for NuttyUtility in case of a security breach.
4. Lack of centralization: Both machines are not configured to forward events to a centralized location, making it difficult to monitor and detect security incidents in real-time.

Considering these risks, it is recommended that NuttyUtility implements the following measures before integrating these machines into its network:

1. Vulnerability scanning and patching: Both machines should undergo a thorough vulnerability scan to identify and remediate any vulnerabilities.

2. Configuration hardening: Both machines should be configured to comply with security policies, such as disabling unnecessary services, applying appropriate permissions on PII folders, and disabling anonymous access to shared folders.
3. Compliance auditing: Both machines should be audited for compliance with relevant security policies, such as FIPS 140-2.
4. Centralized logging: Both machines should be configured to forward events to a centralized location to enable real-time monitoring and detection of security incidents.
5. Privileged access management: NuttyUtility should implement a privileged access management (PAM) solution to control and monitor access to privileged accounts on both machines.

By implementing these measures, NuttyUtility can reduce the risk of security breaches and compliance violations associated with integrating these machines into its network.

In conclusion, while integrating these machines into NuttyUtility's network can provide some benefits, it also comes with significant risks that need to be addressed. It is recommended that NuttyUtility implements the measures outlined above before integrating these machines into its network to mitigate these risks. Ultimately, the decision to integrate these machines into the network should be made by the stakeholders based on a careful consideration of the risks and benefits.