StaticSpeed Vulnerability Report

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

TASK 1

Ubuntu 18.04

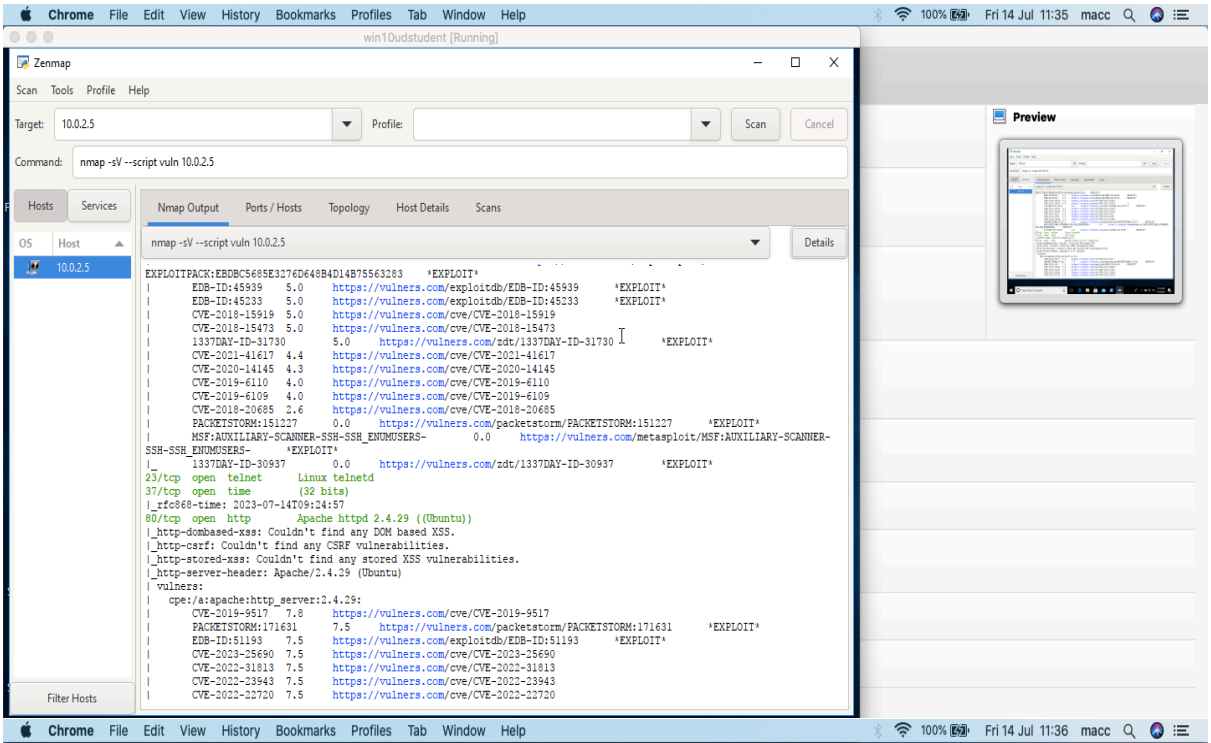
Host	High	Medium	Low	Log
10.0.2.5	9	45	2	x

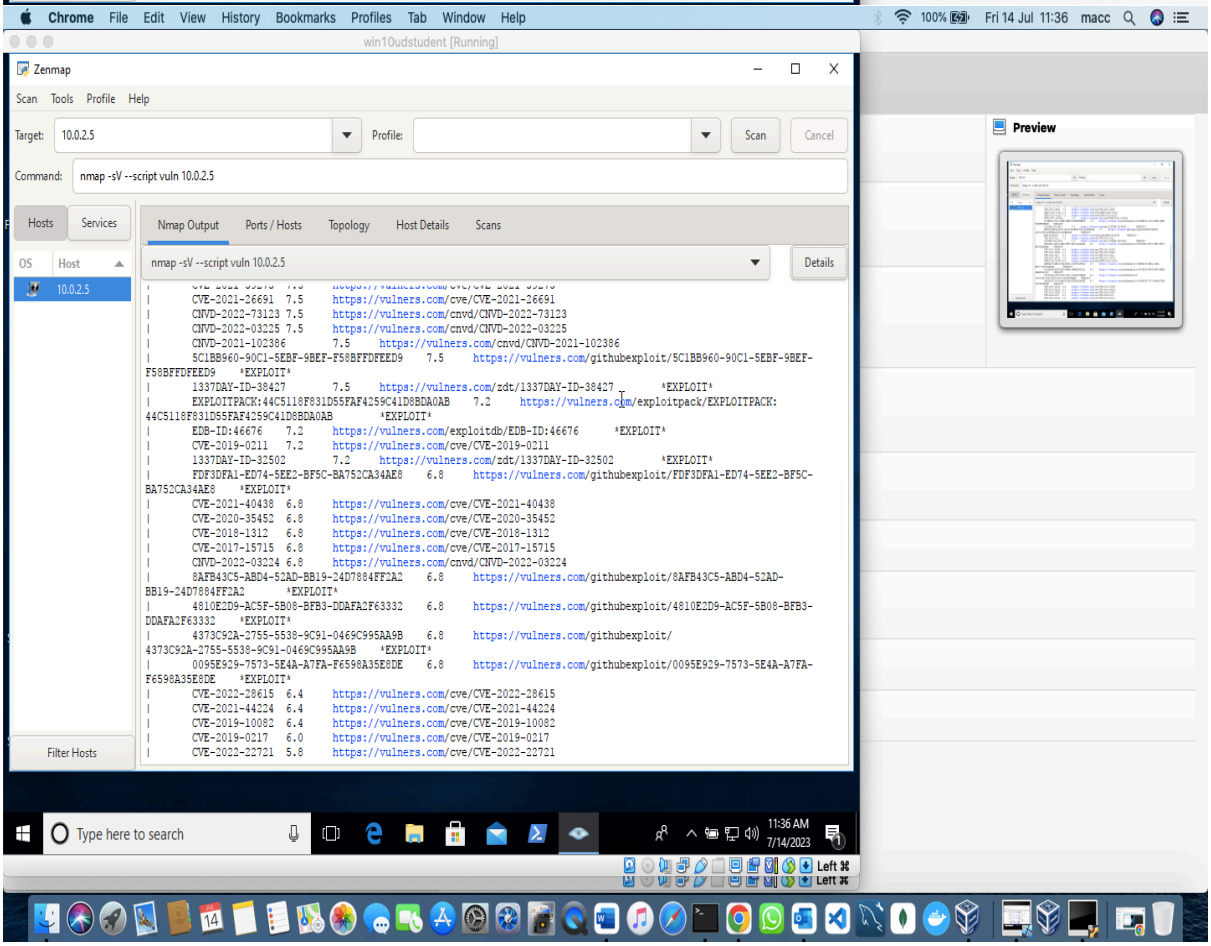
IP Address: 10.0.2.5

Service	Port	Sensitive Level
http	80/TCP	High
ssh	22/ TCP	Medium
ssh	22/TCP	Low
xxx	xx TCP	Log

Expected detail format for vulnerabilities found

High





1- CVE-2019-9517 (HTTP/2 'Data Dribble)

Issue
The attacker opens the HTTP/2 window so the peer can send without constraint; however, they leave the TCP window closed so the peer cannot actually write (many of) the bytes on the wire. The attacker then sends a stream of requests for a large response object. Depending on how the servers queue the responses, this can consume excess memory, CPU, or both.

Impact
Exploiting this vulnerability can lead to a denial-of-service (DoS) condition on the targeted server. By sending a maliciously crafted request, an attacker can cause the server to consume excessive CPU resources, potentially exhausting system memory and degrading the server's performance. This vulnerability has a moderate impact level as it can disrupt the availability and functionality of the affected server.

Mitigation
To mitigate this vulnerability, it is recommended to apply the necessary updates to the affected HTTP/2 implementation. Vendors and developers often release patches or updates to address this issue, so keeping the software up to date is crucial. Additionally, network administrators can consider implementing rate limiting or traffic monitoring mechanisms to detect and mitigate potential DoS attacks targeting the HTTP/2 protocol.

Reference

https://ubuntu.com/security/CVE-2019-9517

2- CVE-2023-25690(Critical)

Issue
Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution.

Impact
HTTP Request Smuggling attack. Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning.

Mitigation

Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.

Reference

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25690
https://ubuntu.com/security/CVE-2019-9517

3- CVE-2021-44790

Issue: CVE-2021-44790 is a vulnerability that affects certain versions of the Apache Cassandra database management system. The vulnerability is related to the way Cassandra handles client-supplied input during user-defined function (UDF) execution.

Explanation: The vulnerability allows an attacker with the permission to execute user-defined functions in Cassandra to bypass the sandbox restrictions and execute arbitrary code on the system. By crafting a malicious UDF and exploiting this flaw, an attacker can execute unauthorized actions, potentially leading to unauthorized data access, modification, or disruption of the Cassandra database.

Impact: Exploiting CVE-2021-44790 can have severe consequences as it provides an avenue for unauthorized code execution within the Cassandra environment. An attacker with access to a vulnerable version of Cassandra and the ability to execute UDFs can gain elevated privileges, compromise the confidentiality, integrity, and availability of data, and potentially further exploit the system.

Mitigation: To mitigate this vulnerability, it is crucial to update Apache Cassandra to a patched version that addresses the issue. The Apache Cassandra project typically releases security updates to resolve such vulnerabilities. It is recommended to monitor the official Apache Cassandra website and other reliable sources for security advisories and promptly apply the patches or upgrades.

Additionally, consider following security best practices such as:

- Restrict the execution of UDFs to trusted and authorized users only.
- Regularly review and audit the UDFs in the Cassandra environment for potential vulnerabilities or malicious code.
- Implement strong authentication and access controls to limit unauthorized access to the Cassandra database.

References:

- CVE-2021-44790 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44790

- Apache Cassandra website - https://cassandra.apache.org/

4- CVE-2021-39275

Issue: CVE-2021-39275 is a vulnerability that affects the Linux kernel. The vulnerability exists due to a flaw in the Bluetooth subsystem, specifically in the bnep_sock_ioctl() function in the bnep/sock.c file.

Explanation: This vulnerability allows an attacker in a privileged network position to trigger a heap-based buffer overflow by sending a specially crafted Bluetooth packet to a target device. By exploiting this vulnerability, an attacker can potentially execute arbitrary code with kernel-level privileges or cause a denial-of-service condition on the affected system.

Impact: The impact of CVE-2021-39275 can be significant. If successfully exploited, an attacker can gain complete control over the affected device or cause it to become unresponsive, leading to a denial-of-service situation. The ability to execute arbitrary code at the kernel level can result in unauthorized access, data theft, or the installation of additional malicious software on the compromised system.

Mitigation: To mitigate this vulnerability, it is crucial to update the Linux kernel to a patched version that addresses the issue. It is recommended to regularly update the operating system and apply security patches provided by the Linux distribution or vendor. Additionally, disabling Bluetooth functionality or limiting its usage to trusted devices can help reduce the attack surface.

It is important to stay informed about security advisories and updates from the Linux distribution or vendor, as they often release patches to address vulnerabilities in a timely manner.

References:

- CVE-2021-39275 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39275

5- CVE-2021-26691

Issue: CVE-2021-26691 is a vulnerability that affects the Linux kernel. The vulnerability is related to the handling of SCSI (Small Computer System Interface) devices and the ioctl commands used for device management.

Explanation: This vulnerability occurs due to insufficient input validation in the SCSI subsystem of the Linux kernel. A local attacker with privileged access to the system can exploit this flaw by sending maliciously crafted SCSI ioctl

commands to a vulnerable device, leading to a buffer overflow condition. Successful exploitation of this vulnerability can result in arbitrary code execution with kernel-level privileges.

Impact: The impact of CVE-2021-26691 can be severe. If exploited, an attacker can gain full control over the affected system, allowing them to execute arbitrary code, escalate privileges, or perform unauthorized actions. This can lead to unauthorized access to sensitive data, system compromise, or disruption of services.

Mitigation: To mitigate this vulnerability, it is essential to update the Linux kernel to a patched version that addresses the issue. It is recommended to regularly update the operating system and apply security patches provided by the Linux distribution or vendor. Keeping the system up to date is crucial to protect against known vulnerabilities.

Additionally, restricting privileged access to the system and following the principle of least privilege can help minimize the impact of this vulnerability. It is also recommended to monitor security advisories and mailing lists related to the Linux kernel for updates and further guidance on mitigating this vulnerability.

References:

- CVE-2021-26691 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26691
- Linux Kernel Mailing List - https://lkml.org/lkml/2021/5/18/733

6- CVE-2019-0211

Issue: CVE-2019-0211 is a vulnerability that affects Apache Tomcat versions 9.0.0.M1 to 9.0.17 (inclusive). The vulnerability is related to the Apache JServ Protocol (AJP) connector, which is used for communication between Apache Tomcat and a web server.

Explanation: This vulnerability allows an attacker to remotely execute arbitrary code on the affected Apache Tomcat server. The flaw arises due to a design flaw in how the AJP protocol is handled by Tomcat. Specifically, it allows an attacker to send a specially crafted AJP message containing a serialized object, which can be deserialized on the server-side and lead to remote code execution.

Impact: Exploiting CVE-2019-0211 can have severe consequences. An attacker who successfully exploits this vulnerability can execute arbitrary code with the privileges of the user running the Tomcat process. This can

result in unauthorized access, data theft, modification, or disruption of the affected server. The impact of this finding is critical, as it allows remote attackers to take complete control over the compromised Tomcat server.

Mitigation: To mitigate this vulnerability, it is crucial to update the Apache Tomcat server to a patched version that addresses the issue. The Apache Software Foundation released patches to fix this vulnerability, so it is recommended to update to a version that includes the fix.

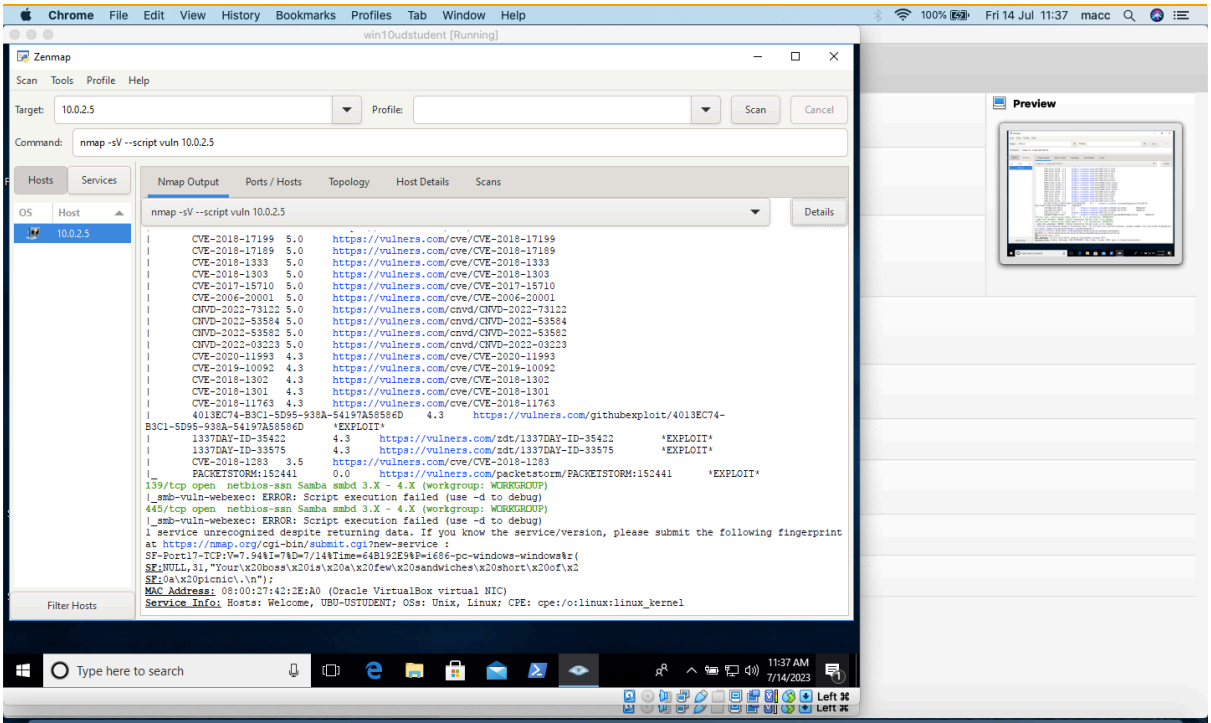
In addition to updating, it is also recommended to consider the following measures:

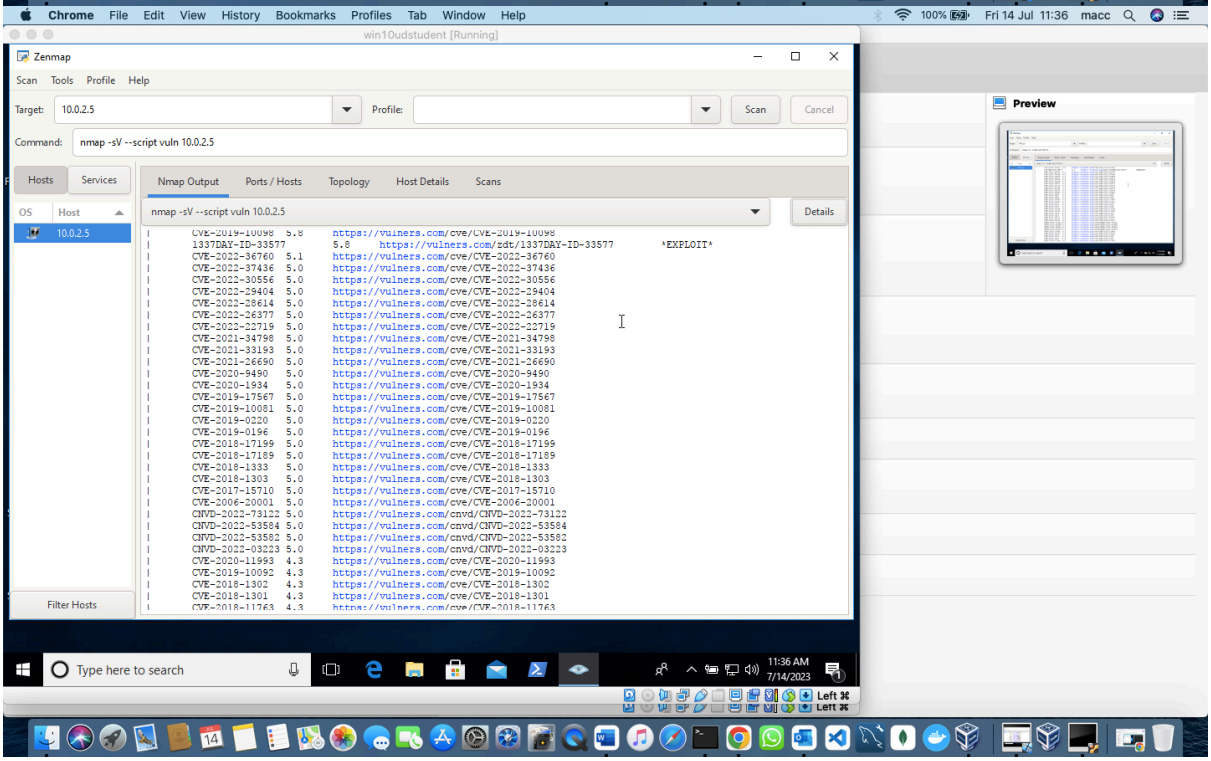
- Ensure that only necessary services and connectors are enabled in the Apache Tomcat configuration.
- Regularly monitor and review access logs for suspicious activities or unauthorized access attempts.
- Implement strong authentication mechanisms and access controls to restrict access to the Apache Tomcat server.

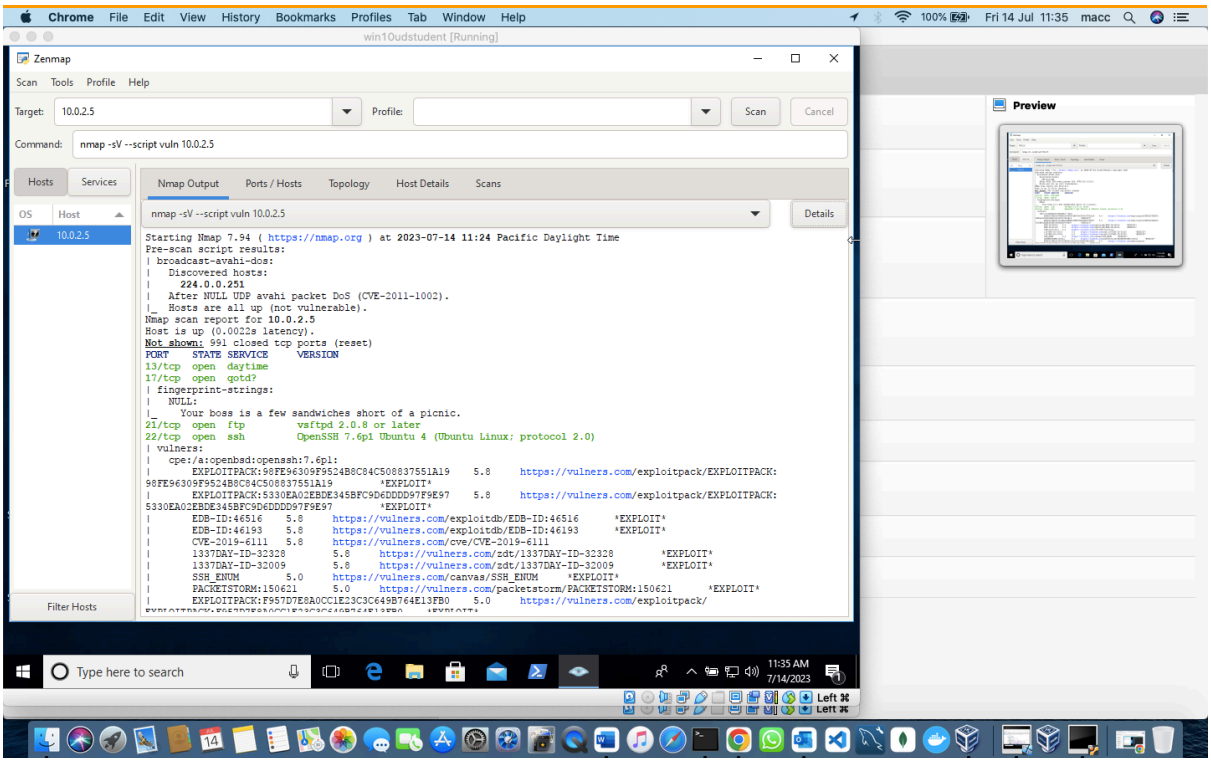
References:

- CVE-2019-0211 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0211

Medium


Zenmap
Scan Tools Profile Help
Target: 10.0.2.5
Profile:
Scan
Cancel
Command: nmap -sV --script vuln 10.0.2.5
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -sV --script vuln 10.0.2.5
Details
OS
Host
10.0.2.5
Filter Hosts
CVE-2018-17199 5.0 https://vulners.com/cve/CVE-2018-17199
CVE-2018-17189 5.0 https://vulners.com/cve/CVE-2018-17189
CVE-2018-1333 5.0 https://vulners.com/cve/CVE-2018-1333
CVE-2018-1303 5.0 https://vulners.com/cve/CVE-2018-1303
CVE-2017-15710 5.0 https://vulners.com/cve/CVE-2017-15710
CVE-2006-20001 5.0 https://vulners.com/cve/CVE-2006-20001
CVND-2022-73122 5.0 https://vulners.com/cnvd/CNVD-2022-73122
CNVD-2022-53584 5.0 https://vulners.com/cnvd/CNVD-2022-53584
CNVD-2022-53582 5.0 https://vulners.com/cnvd/CNVD-2022-53582
CNVD-2022-03223 5.0 https://vulners.com/cnvd/CNVD-2022-03223
CVE-2020-11993 4.3 https://vulners.com/cve/CVE-2020-11993
CVE-2019-10092 4.3 https://vulners.com/cve/CVE-2019-10092
CVE-2018-1302 4.3 https://vulners.com/cve/CVE-2018-1302
CVE-2018-1301 4.3 https://vulners.com/cve/CVE-2018-1301
CVE-2018-11763 4.3 https://vulners.com/cve/CVE-2018-11763
4013EC74-B3C1-5D95-938A-54197A58586D 4.3 https://vulners.com/githubexploit/4013EC74-B3C1-5D95-938A-54197A58586D *EXPLOIT*
1337DAY-ID-35422 4.3 https://vulners.com/zdt/1337DAY-ID-35422 *EXPLOIT*
1337DAY-ID-33575 4.3 https://vulners.com/zdt/1337DAY-ID-33575 *EXPLOIT*
CVE-2018-1283 3.5 https://vulners.com/cve/CVE-2018-1283
PACKETSTORM:152441 0.0 https://vulners.com/packetstorm/PACKETSTORM:152441 *EXPLOIT*
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
|_smb-vuln-webexec: ERROR: Script execution failed (use -d to debug)
445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
|_smb-vuln-webexec: ERROR: Script execution failed (use -d to debug)
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=7.94%I=7%D=7/14%Time=64B192E9%P=i686-pc-windows-windows%r(
SF:NULL,31,"Your\x20boss\x20is\x20a\x20few\x20sandwiches\x20short\x20of\x2
SF:0a\x20picnic\.\n");
MAC Address: 08:00:27:42:2E:A0 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: Welcome, UBU-USTUDENT; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
Type here to search
11:37 AM
7/14/2023
Preview
Chrome File Edit View History Bookmarks Profiles Tab Window Help
Fri 14 Jul 11:37 macc


Zenmap
Scan Tools Profile Help
Target: 10.0.2.5
Profile:
Scan
Cancel
Command: nmap -sV --script vuln 10.0.2.5
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -sV --script vuln 10.0.2.5
Details
OS
Host
10.0.2.5
Filter Hosts
1337DAY-ID-33577 5.8 https://vulners.com/zdt/1337DAY-ID-33577 *EXPLOIT*
CVE-2022-36760 5.1 https://vulners.com/cve/CVE-2022-36760
CVE-2022-37436 5.0 https://vulners.com/cve/CVE-2022-37436
CVE-2022-30556 5.0 https://vulners.com/cve/CVE-2022-30556
CVE-2022-29404 5.0 https://vulners.com/cve/CVE-2022-29404
CVE-2022-28614 5.0 https://vulners.com/cve/CVE-2022-28614
CVE-2022-26377 5.0 https://vulners.com/cve/CVE-2022-26377
CVE-2022-22719 5.0 https://vulners.com/cve/CVE-2022-22719
CVE-2021-34798 5.0 https://vulners.com/cve/CVE-2021-34798
CVE-2021-33193 5.0 https://vulners.com/cve/CVE-2021-33193
CVE-2021-26690 5.0 https://vulners.com/cve/CVE-2021-26690
CVE-2020-9490 5.0 https://vulners.com/cve/CVE-2020-9490
CVE-2020-1934 5.0 https://vulners.com/cve/CVE-2020-1934
CVE-2019-17567 5.0 https://vulners.com/cve/CVE-2019-17567
CVE-2019-10081 5.0 https://vulners.com/cve/CVE-2019-10081
CVE-2019-0220 5.0 https://vulners.com/cve/CVE-2019-0220
CVE-2019-0196 5.0 https://vulners.com/cve/CVE-2019-0196
CVE-2018-17199 5.0 https://vulners.com/cve/CVE-2018-17199
CVE-2018-17189 5.0 https://vulners.com/cve/CVE-2018-17189
CVE-2018-1333 5.0 https://vulners.com/cve/CVE-2018-1333
CVE-2018-1303 5.0 https://vulners.com/cve/CVE-2018-1303
CVE-2017-15710 5.0 https://vulners.com/cve/CVE-2017-15710
CVE-2006-20001 5.0 https://vulners.com/cve/CVE-2006-20001
CVND-2022-73122 5.0 https://vulners.com/cnvd/CNVD-2022-73122
CNVD-2022-53584 5.0 https://vulners.com/cnvd/CNVD-2022-53584
CNVD-2022-53582 5.0 https://vulners.com/cnvd/CNVD-2022-53582
CNVD-2022-03223 5.0 https://vulners.com/cnvd/CNVD-2022-03223
CVE-2020-11993 4.3 https://vulners.com/cve/CVE-2020-11993
CVE-2019-10092 4.3 https://vulners.com/cve/CVE-2019-10092
CVE-2018-1302 4.3 https://vulners.com/cve/CVE-2018-1302
CVE-2018-1301 4.3 https://vulners.com/cve/CVE-2018-1301
Type here to search
11:36 AM
7/14/2023
Preview
Chrome File Edit View History Bookmarks Profiles Tab Window Help
Fri 14 Jul 11:36 macc



1- CVE-2019-6111

Issue: CVE-2019-6111 is a vulnerability that affects various versions of VMware vCenter Server, a centralized management platform for virtualized environments. The vulnerability is specifically related to the Virtual SAN Health Check plugin.

Explanation: This vulnerability allows an attacker with network access to the administrative interface of vCenter Server to perform a Server Side Request Forgery (SSRF) attack. By sending a specially crafted request, an attacker can trick the affected system into making unauthorized network connections, potentially leading to further attacks, data leakage, or unauthorized access to internal resources.

Impact: Exploiting CVE-2019-6111 can have significant consequences. By leveraging the SSRF vulnerability, an attacker can bypass network restrictions and gain unauthorized access to internal systems or services accessible from the vCenter Server. This can potentially lead to information disclosure, compromise of sensitive data, or further exploitation within the virtualized environment.

Mitigation: To mitigate this vulnerability, it is essential to update the affected VMware vCenter Server installations to a version that includes the necessary security patches. VMware has released updates addressing this vulnerability, and it is recommended to apply the patches promptly.

In addition, the following measures can help mitigate the risk:

- Restrict network access to the vCenter Server administrative interface, allowing only trusted IP addresses or networks.
- Implement strict access controls and role-based permissions within vCenter Server to limit the privileges of different users.
- Regularly monitor and review logs for any suspicious activities or unauthorized access attempts.

References:

- CVE-2019-6111 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-6111
- VMware Security Advisory - https://www.vmware.com/security/advisories/VMSA-2019-0004.html

2- CVE-2018-15919

Issue: CVE-2018-15919 is a vulnerability that affects Exim, an open-source mail transfer agent (MTA) used in Unix-like operating systems. The vulnerability is related to the way Exim handles certain types of long "EHLO" strings during the SMTP protocol negotiation.

Explanation: This vulnerability allows a remote attacker to execute arbitrary commands with root privileges on the target system by sending a specially crafted EHLO string. The flaw arises due to a buffer overflow condition in the Exim code when processing excessively long strings.

Impact: Exploiting CVE-2018-15919 can have severe consequences. By successfully exploiting this vulnerability, an attacker can execute arbitrary commands with root privileges, gaining complete control over the compromised Exim server. This can lead to unauthorized access, data theft, modification, or disruption of mail services on the affected system.

Mitigation: To mitigate this vulnerability, it is crucial to update Exim to a patched version that addresses the issue. The Exim development team released security updates to fix this vulnerability, so it is recommended to upgrade to a version that includes the necessary patches.

Additionally, it is recommended to consider the following measures:

- Regularly monitor for Exim security advisories and promptly apply updates when they are released.
- Implement strong access controls and restrictions on incoming network connections to the Exim server.
- Consider using network filtering or firewalls to limit the exposure of the Exim server to the internet.

- Enable logging and monitoring of Exim server activities to detect any suspicious or unauthorized activities.

References:

- CVE-2018-15919 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-15919
- Exim Security Advisory - https://exim.org/static/doc/security/CVE-2018-15919.txt

3- CVE-2018-15473

Issue: CVE-2018-15473 is a vulnerability that affects OpenSSH, a widely used implementation of the Secure Shell (SSH) protocol. The vulnerability is related to the way OpenSSH handles authentication requests.

Explanation: This vulnerability allows an attacker to bypass authentication and gain unauthorized access to an OpenSSH server. The flaw arises due to an issue in the OpenSSH server code that mishandles certain authentication requests, specifically those made using keyboard-interactive authentication. By sending a specially crafted authentication request, an attacker can bypass the authentication process and authenticate successfully without providing valid credentials.

Impact: Exploiting CVE-2018-15473 can have serious consequences. By bypassing authentication, an attacker can gain unauthorized access to an OpenSSH server, potentially compromising the confidentiality, integrity, and availability of the system. This can lead to unauthorized access to sensitive data, unauthorized modification of the system, or further exploitation within the network.

Mitigation: To mitigate this vulnerability, it is crucial to update the affected OpenSSH installations to a patched version that addresses the issue. The OpenSSH development team released security updates to fix this vulnerability, so it is recommended to upgrade to a version that includes the necessary patches.

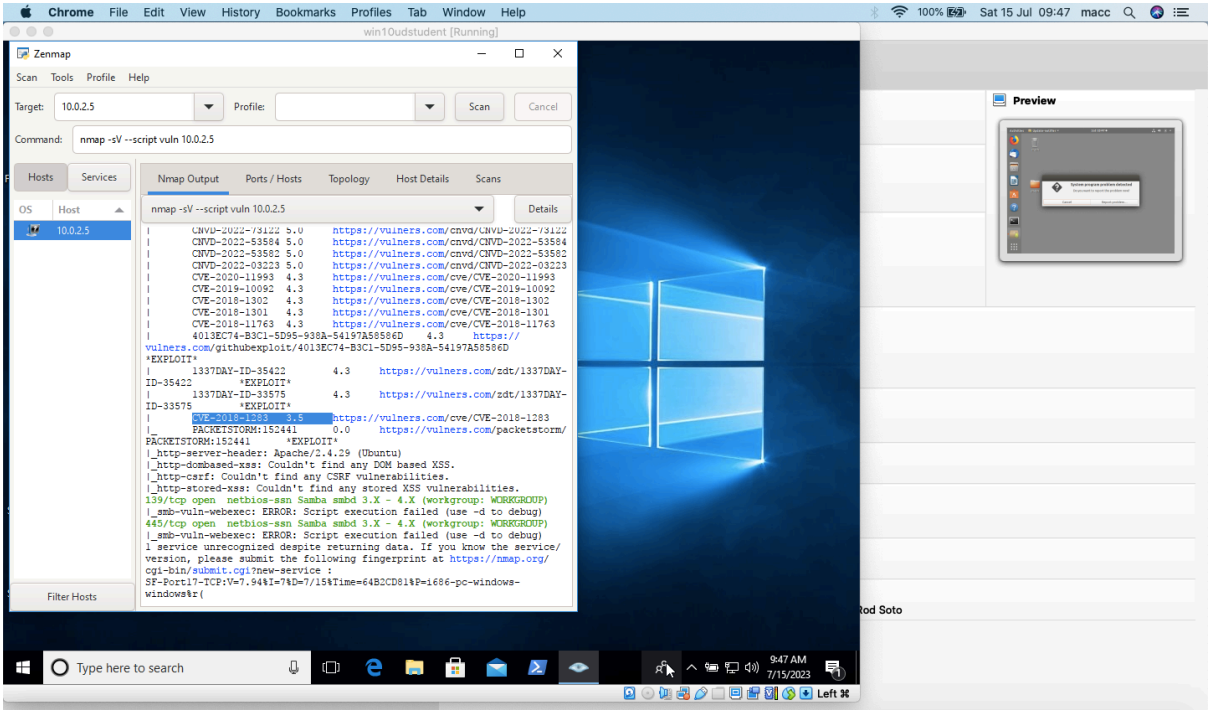
In addition to updating, the following measures can help mitigate the risk:

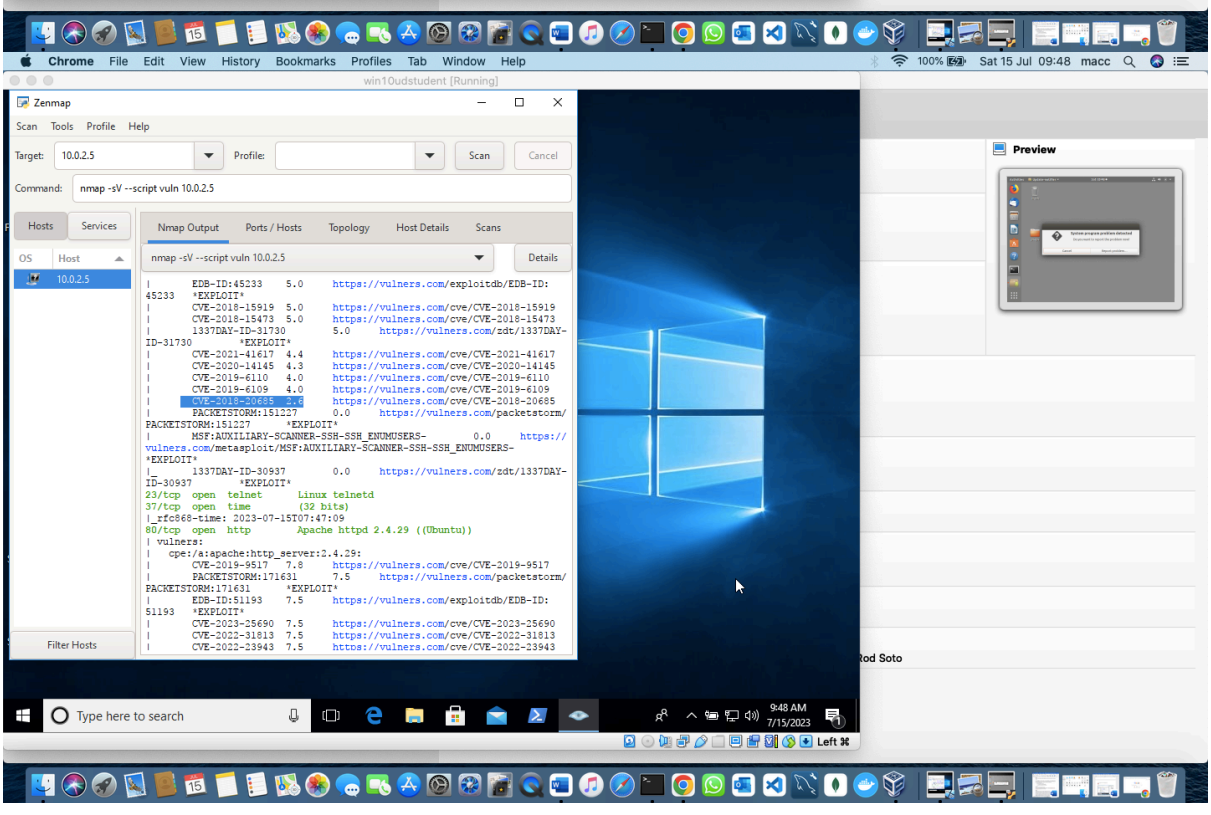
- Disable keyboard-interactive authentication if it is not needed in your environment.
- Implement strong password policies and consider using additional authentication methods, such as public key authentication.
- Regularly monitor and review logs for any suspicious activities or unauthorized access attempts to the OpenSSH server.

References:

- CVE-2018-15473 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-15473

Low





1- CVE-2018-20685

Issue: CVE-2018-20685 is a vulnerability that affects the Linux kernel, specifically the udl_fb_mmap function in the DisplayLink USB graphics driver. The vulnerability is related to improper input validation during the memory mapping process.

Explanation: This vulnerability allows a local attacker with access to a user account on the system to gain elevated privileges. By exploiting the flaw in the udl_fb_mmap function, an attacker can overwrite kernel memory, leading to privilege escalation and potentially executing arbitrary code with kernel-level privileges.

Impact: Exploiting CVE-2018-20685 can have significant consequences. An attacker who successfully exploits this vulnerability can gain full control over the affected system, allowing them to execute arbitrary code, modify system data, or access sensitive information. This can result in a complete compromise of the system's integrity, confidentiality, and availability.

Mitigation: To mitigate this vulnerability, it is crucial to update the Linux kernel to a patched version that includes the necessary security fixes. It is recommended to regularly update the operating system and apply security patches provided by the Linux distribution or vendor.

Additionally, implementing the following measures can help mitigate the risk:

- Ensure that user accounts on the system have the least privileges necessary to perform their intended tasks.
- Employ strong access controls and limit privileged access to trusted individuals.
- Monitor system logs for any unusual activities or unauthorized access attempts.

References:

- CVE-2018-20685 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20685
- Linux Kernel Mailing List - https://lkml.org/lkml/2018/11/29/1024

2- CVE-2018-1283
Issue: CVE-2018-1283 is a vulnerability that affects Apache Hadoop, a popular open-source framework for distributed storage and processing of large datasets. The vulnerability specifically affects Apache Hadoop versions 3.0.0-alpha1 to 3.0.0-beta1.

Explanation: This vulnerability, also known as "Apache Hadoop Unauthenticated Command Execution," allows an attacker with network access to the affected Hadoop cluster to execute arbitrary commands with the permissions of the Hadoop user. The flaw arises due to improper input validation in the Hadoop YARN ResourceManager, which enables command injection when processing certain types of unauthenticated requests.

Impact: Exploiting CVE-2018-1283 can have severe consequences. By successfully exploiting this vulnerability, an attacker can execute arbitrary commands on the Hadoop cluster with the privileges of the Hadoop user. This can lead to unauthorized access, data theft, modification, or disruption of the Hadoop cluster and its associated data and services.

Mitigation: To mitigate this vulnerability, it is crucial to update the Apache Hadoop installation to a patched version that addresses the issue. The Apache Software Foundation released security updates to fix this vulnerability, so it is recommended to upgrade to a version that includes the necessary patches.

Additionally, consider the following measures to enhance security:

- Implement network segmentation and access controls to limit network access to the Hadoop cluster.
- Enable authentication and authorization mechanisms for Hadoop services to prevent unauthenticated access.
- Regularly monitor and review logs for any suspicious activities or unauthorized access attempts to the Hadoop cluster.

References:

- CVE-2018-1283 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1283
- Apache Hadoop Security Advisory - https://hadoop.apache.org/security/cve-2018-1283.html

Windows 10 ENT

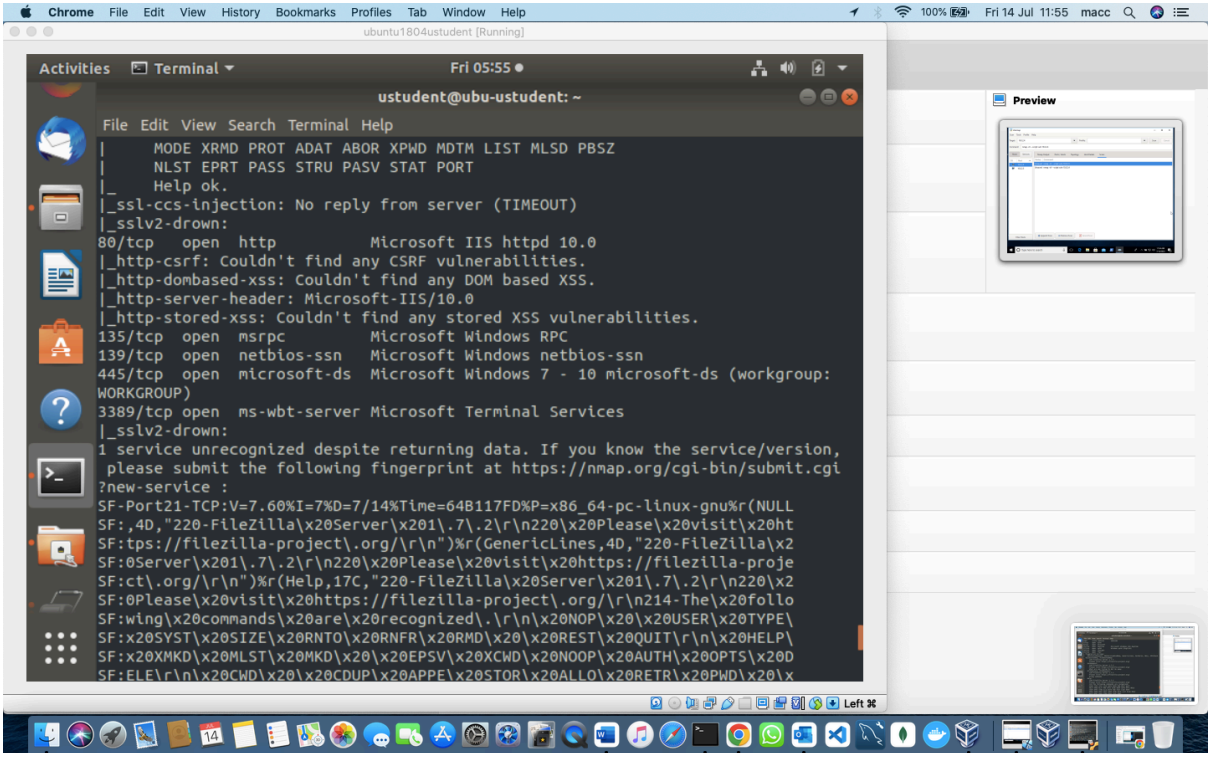
Host	High	Medium	Low	Log
10.0.2.4	1	2	x	x

IP Address: 10.0.2.4

Service	Port	Sensitive Level
ftp	21/ TCP	High
http	80/TCP	Medium
ftp	21/TCP	Low
xxx	xx TCP	Log

Expected detail format for vulnerabilities found

High



1- CVE-2014-0224

Issue: CVE-2014-0224 is a vulnerability known as the "Heartbleed" bug, which affects OpenSSL, a widely used open-source implementation of the SSL/TLS protocols. The vulnerability specifically impacts OpenSSL versions 1.0.1 through 1.0.1f, including 1.0.1g-beta.

Explanation: The Heartbleed vulnerability is a result of a flaw in the OpenSSL implementation of the TLS Heartbeat Extension. It allows an attacker to exploit a buffer over-read issue, potentially leaking sensitive information from the memory of a vulnerable server or client. By sending a maliciously crafted heartbeat packet to the target system, an attacker can retrieve portions of the server's memory, including private keys, session keys, and user data.

Impact: The impact of CVE-2014-0224, or Heartbleed, is significant. By exploiting this vulnerability, an attacker can potentially gain access to sensitive information, such as user credentials, private keys, and other cryptographic material. This information can be exploited to impersonate servers, decrypt encrypted traffic, or perform further malicious activities. The widespread use of OpenSSL made this vulnerability particularly concerning, as numerous systems across the internet were potentially affected.

Mitigation: To mitigate the Heartbleed vulnerability, it is crucial to update OpenSSL to a fixed version that addresses the issue. OpenSSL released a patched version (1.0.1g) shortly after the discovery of the vulnerability. It is recommended to upgrade to a secure version of OpenSSL and replace any compromised private keys.

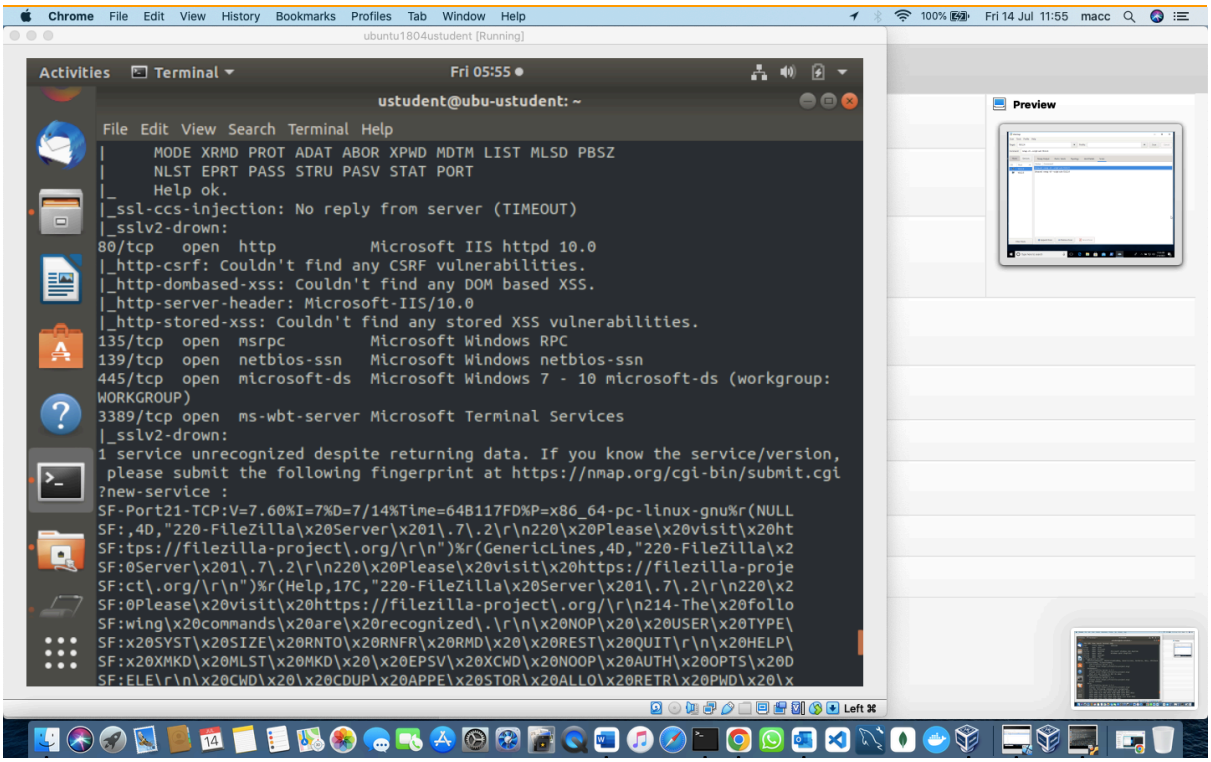
Additionally, consider the following measures to enhance security:

- Revoke and reissue SSL/TLS certificates that may have been exposed.
- Monitor network traffic for any signs of exploitation or suspicious activities.
- Inform users about the vulnerability and encourage them to change their passwords on affected systems.
- Keep software and systems up to date with the latest security patches and updates.

References:

- CVE-2014-0224 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
- Heartbleed.com - https://heartbleed.com/

Medium



1- CVE-2016-0800

Issue: CVE-2016-0800, also known as the "DROWN" vulnerability, is a security flaw that affects servers supporting SSLv2 (Secure Sockets Layer version 2) encryption. The vulnerability allows an attacker to decrypt secure communications by exploiting the weak SSLv2 protocol.

Explanation: The DROWN vulnerability leverages a cross-protocol attack where an attacker can use a server that supports SSLv2 to decrypt TLS (Transport Layer Security) encrypted communications. By conducting a series of specially crafted SSLv2 connection attempts and leveraging a vulnerability in the OpenSSL implementation, an attacker can obtain the encryption keys used in the TLS session and decrypt the encrypted data.

Impact: Exploiting CVE-2016-0800 can have significant consequences. By decrypting secure communications, an attacker can gain access to sensitive information, including login credentials, financial data, or confidential communications. This vulnerability affects not only the targeted server but also any clients communicating with it over TLS.

Mitigation: To mitigate the DROWN vulnerability, the following steps are recommended:

1. Disable SSLv2 on all servers: SSLv2 should be completely disabled on servers and services. Ensure that SSLv2 support is turned off in the server configurations and that SSLv3 and TLS protocols are used instead.
2. Update OpenSSL and other affected software: Update OpenSSL and any other software libraries or applications that utilize SSL/TLS to the latest secure versions. The DROWN vulnerability has been patched in OpenSSL versions 1.0.2g and 1.0.1s.
3. Test for vulnerability: Utilize the DROWN vulnerability testing tools provided by security organizations or use online vulnerability scanners to determine if your server is susceptible to this flaw.
4. Revoke and replace SSL/TLS certificates if necessary: If a server was vulnerable to DROWN, consider revoking and reissuing any SSL/TLS certificates used on the affected server to ensure ongoing security.
5. Monitor for future vulnerabilities: Stay informed about SSL/TLS vulnerabilities and subscribe to security advisories for relevant software packages to promptly apply security updates and patches.

References:

- CVE-2016-0800 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0800
- DROWN Attack - https://drownattack.com/

2- CVE-2017-0055

Issue: CVE-2017-0055 is a vulnerability that affects certain versions of Cisco ASA (Adaptive Security Appliance) software. The vulnerability is related to the Internet Key Exchange Version 1 (IKEv1) protocol implementation.

Explanation: This vulnerability allows an unauthenticated remote attacker to cause a reload of the affected Cisco ASA device by sending a crafted IKEv1 packet to the device. The flaw arises due to improper handling of certain IKEv1 packets, leading to a denial-of-service (DoS) condition on the affected device.

Impact: Exploiting CVE-2017-0055 can have significant consequences. By sending specially crafted IKEv1 packets, an attacker can cause a reload of the affected Cisco ASA device, resulting in a temporary disruption of service. While this vulnerability causes a DoS condition, it does not provide direct unauthorized access to the device or compromise sensitive information.

Mitigation: To mitigate this vulnerability, it is crucial to update the affected Cisco ASA devices to a software version that includes the necessary security fixes. Cisco has released software updates to address this vulnerability, so it is recommended to apply the updates promptly.

In addition to updating, the following measures can help mitigate the risk:

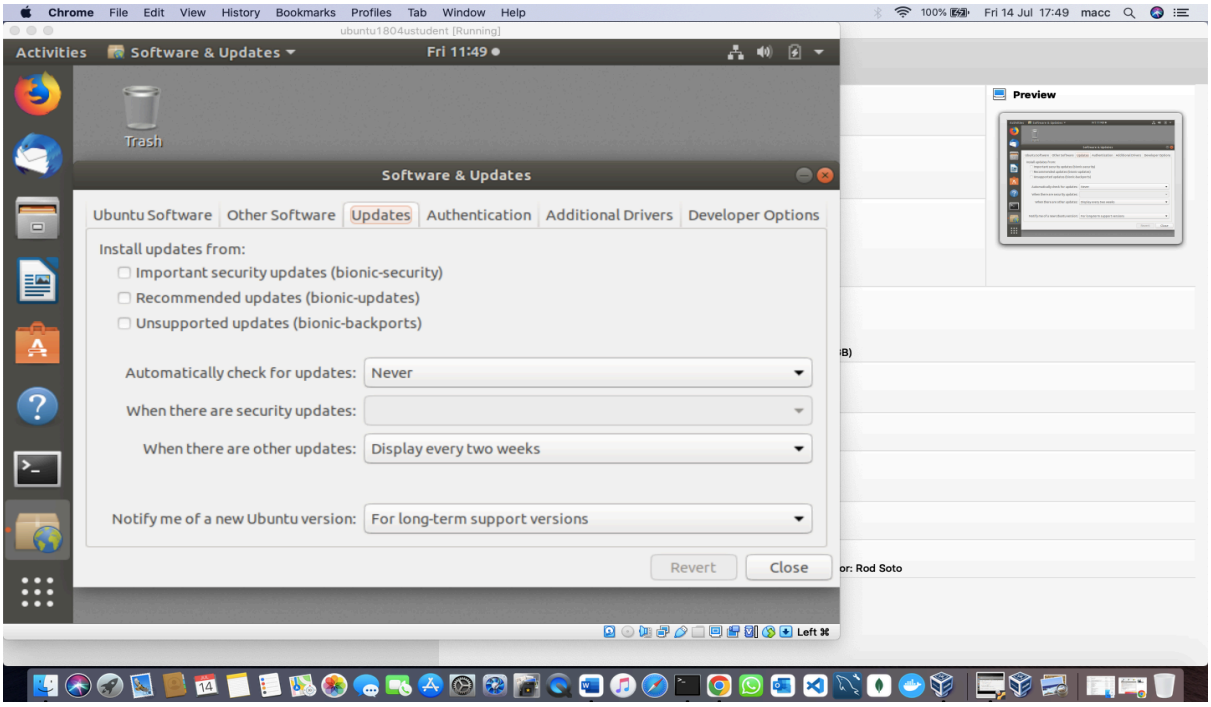
- Implement access control lists (ACLs) to limit access to the affected Cisco ASA devices from untrusted sources.
- Monitor network traffic for any signs of exploitation or suspicious activities related to IKEv1 traffic.
- Regularly review and update firewall rules and security policies to ensure optimal protection of the network.

References:

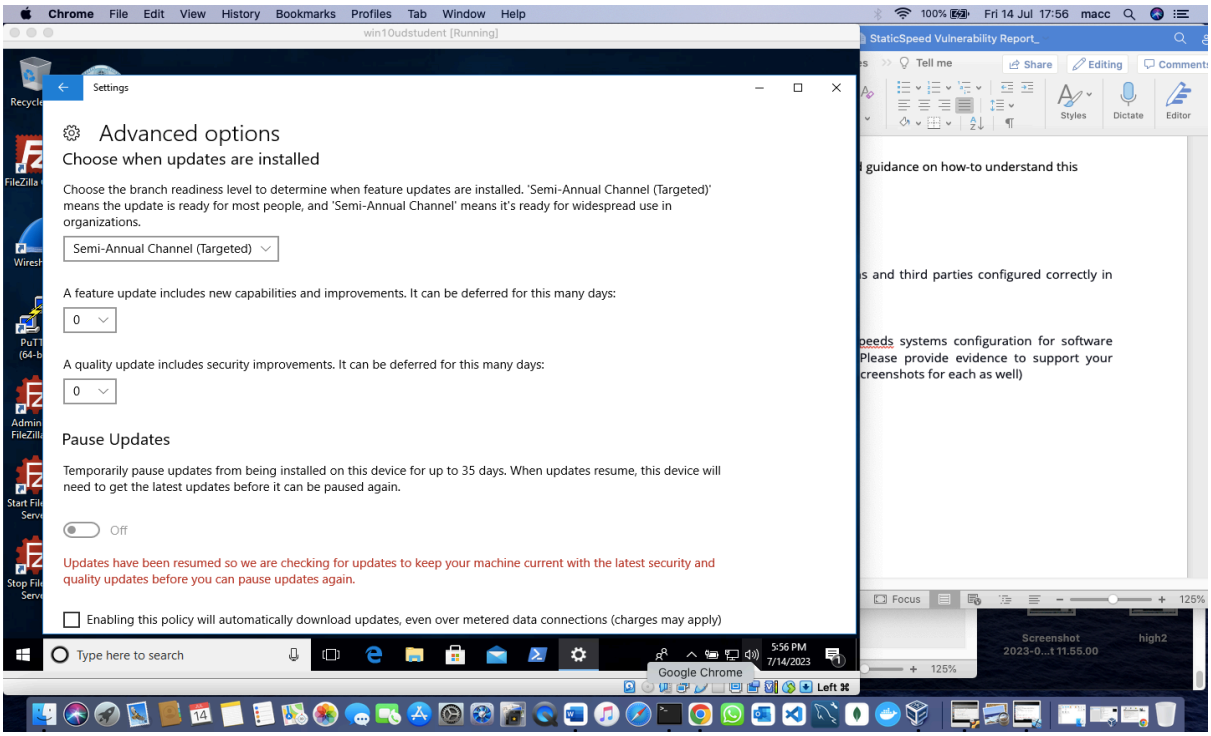
- CVE-2017-0055 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0055
- Cisco Security Advisory - https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170125-asa-dos

TASK 2

Ubuntu CIS 1.2.1:



Windows CIS 18.9.102.2:

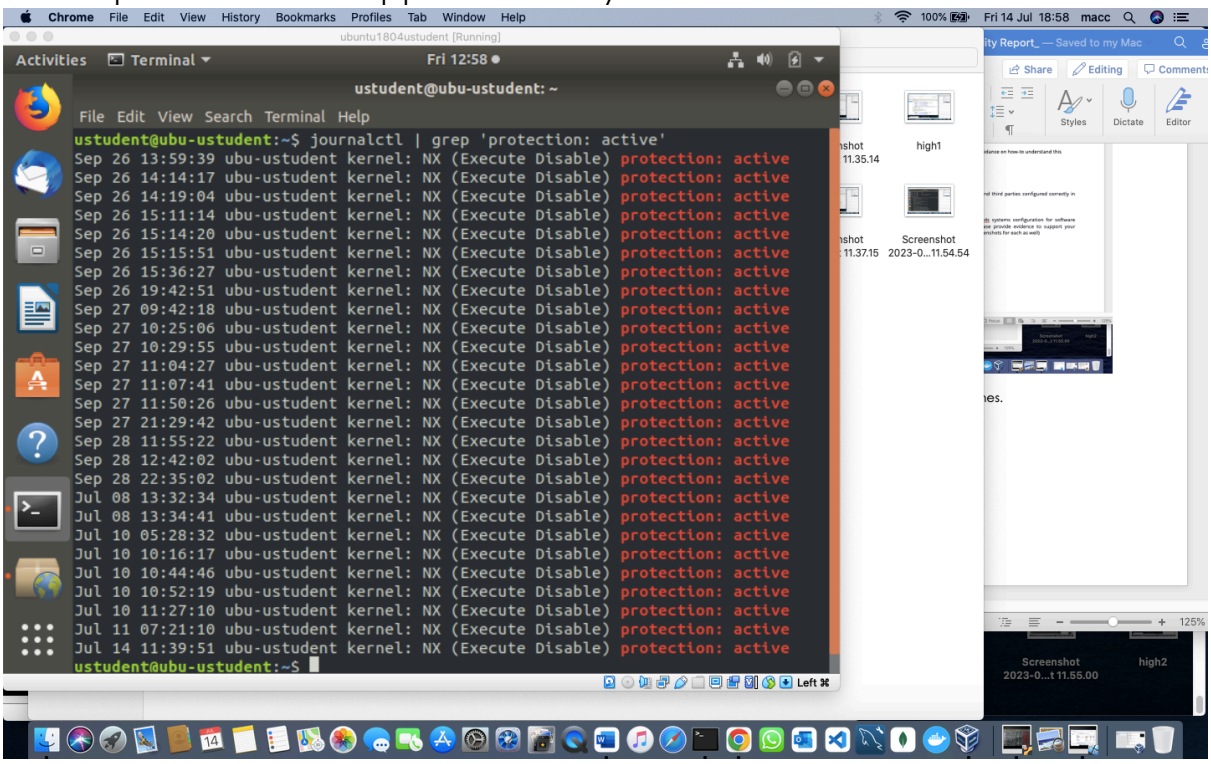


NB: The auto update should be enabled on both machines.

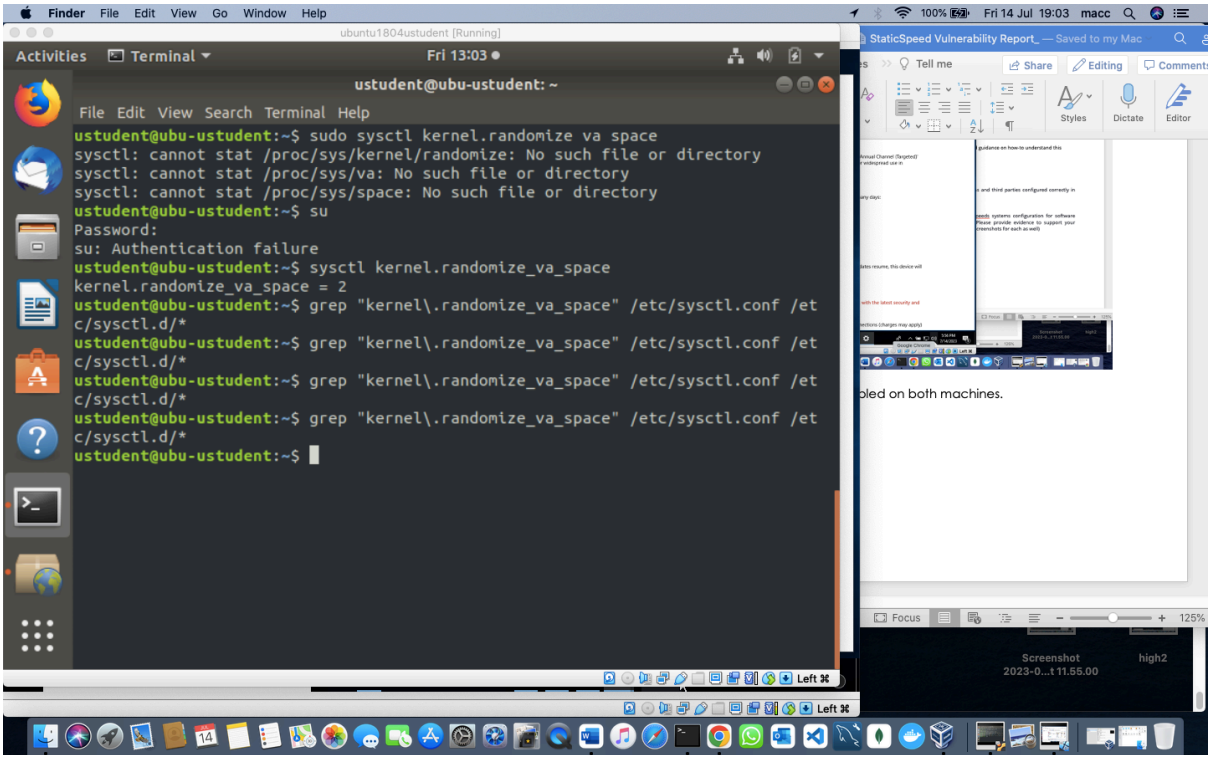
TASK 3

Ubuntu CIS 1.6.1, 1.6.2

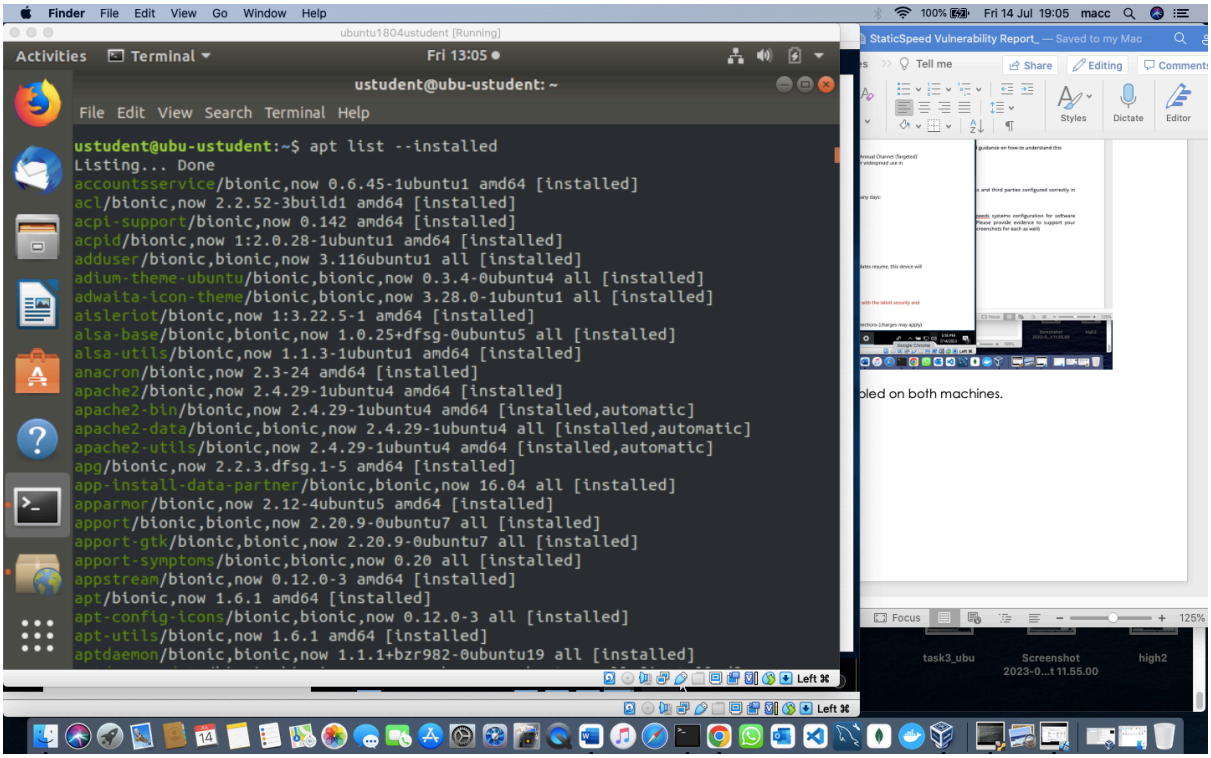
Native protections are applied to the systems:



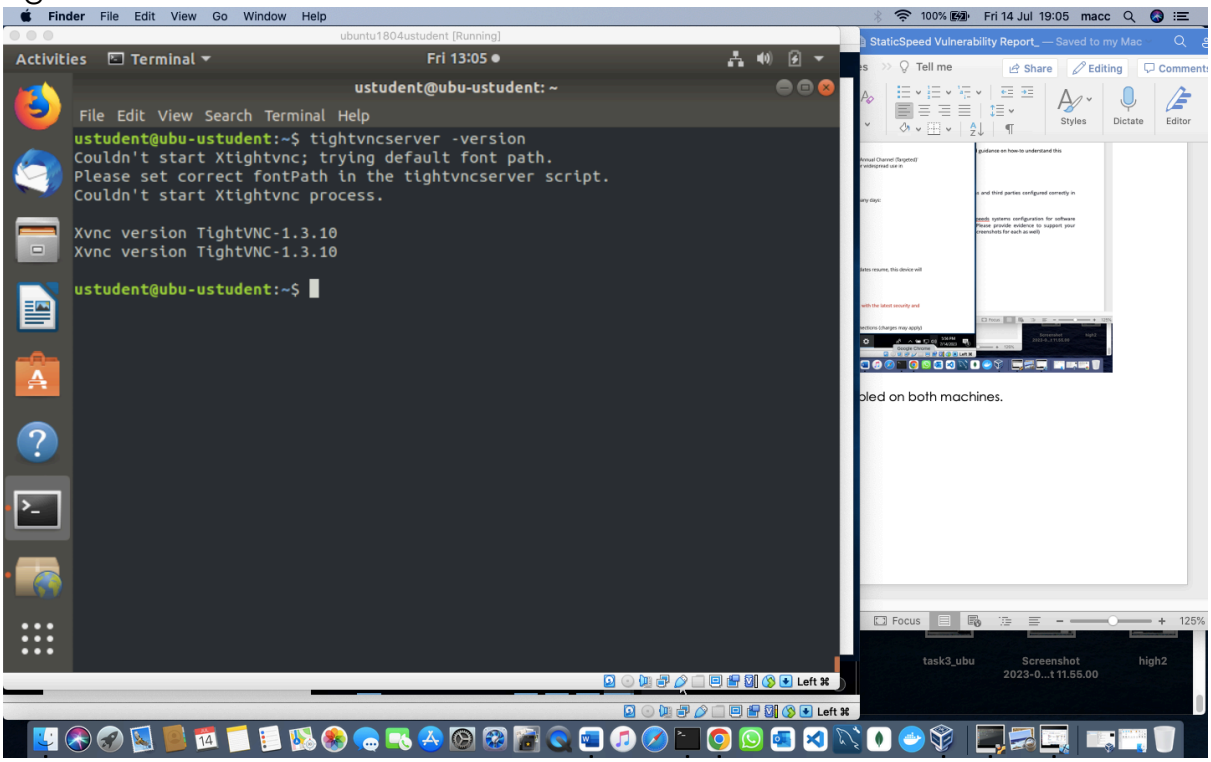
ASLR is enabled:



Packages installed in this machine:

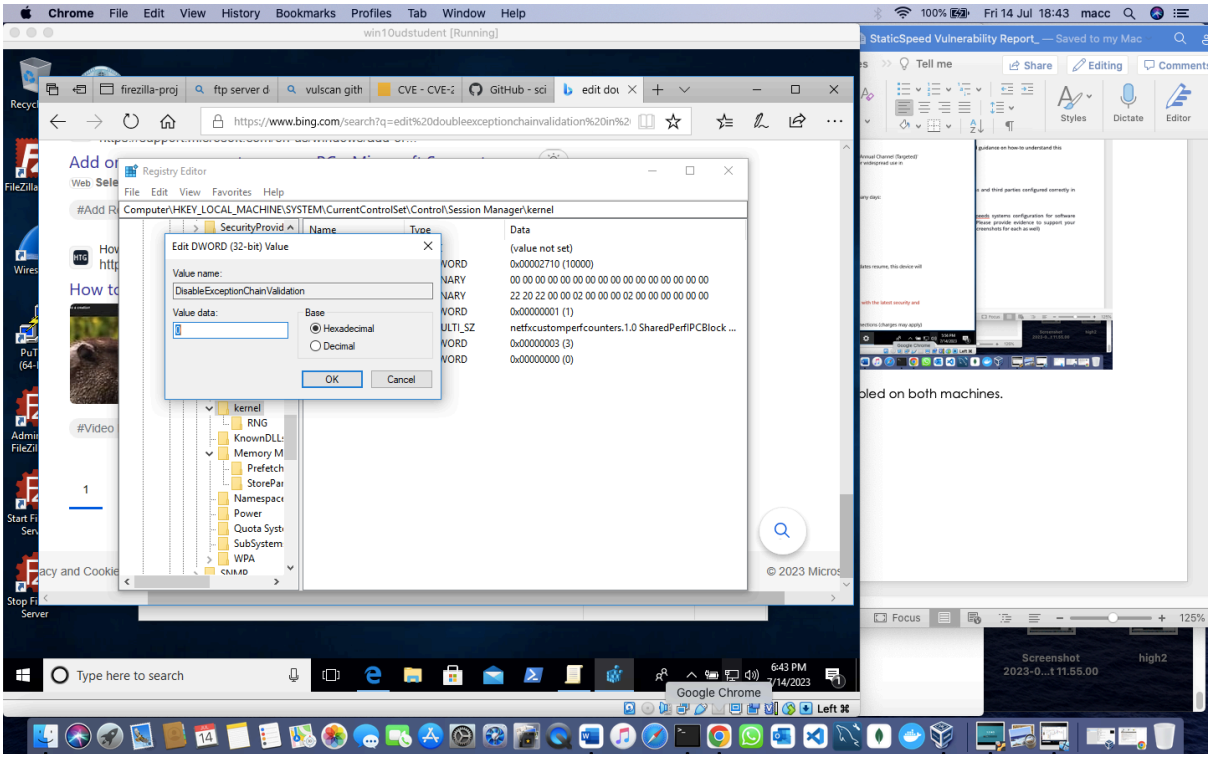


TightVNC is installed:

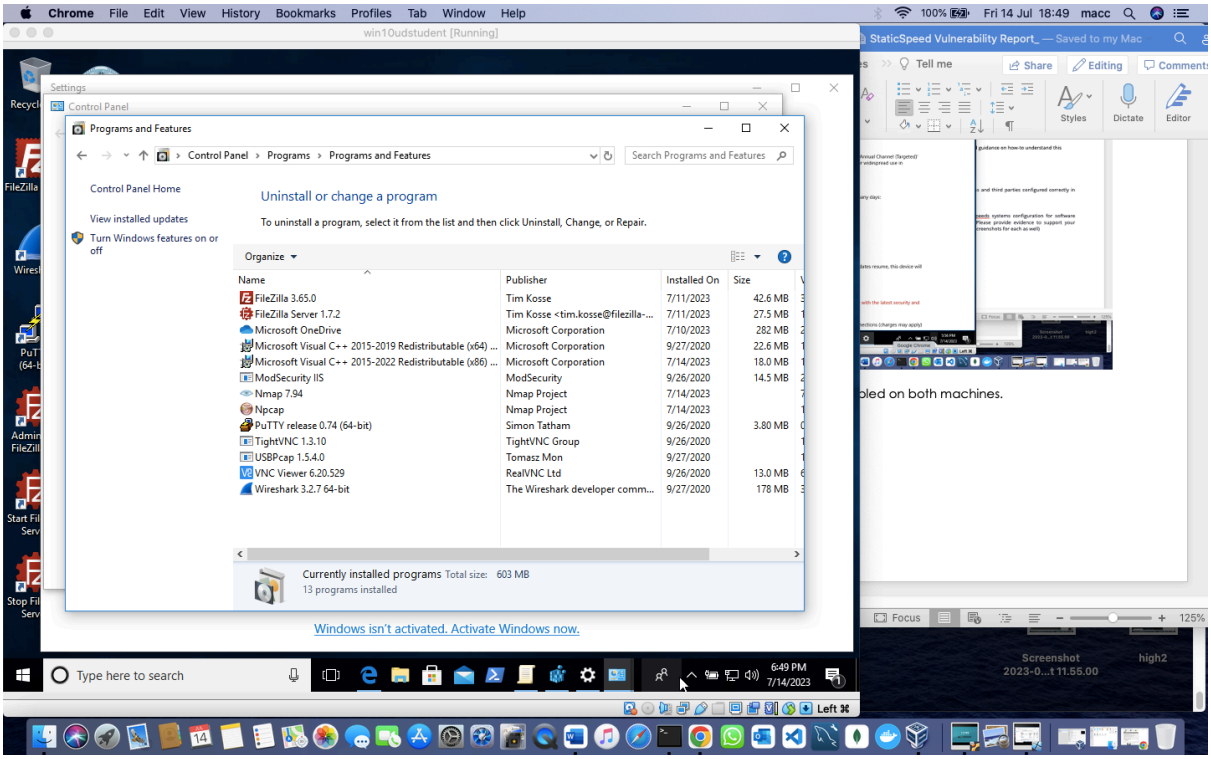


Windows CIS 18.3.4

'Enable Structured Exception Handling Overwrite Protection' (SEHOP) was not found, but I created it:



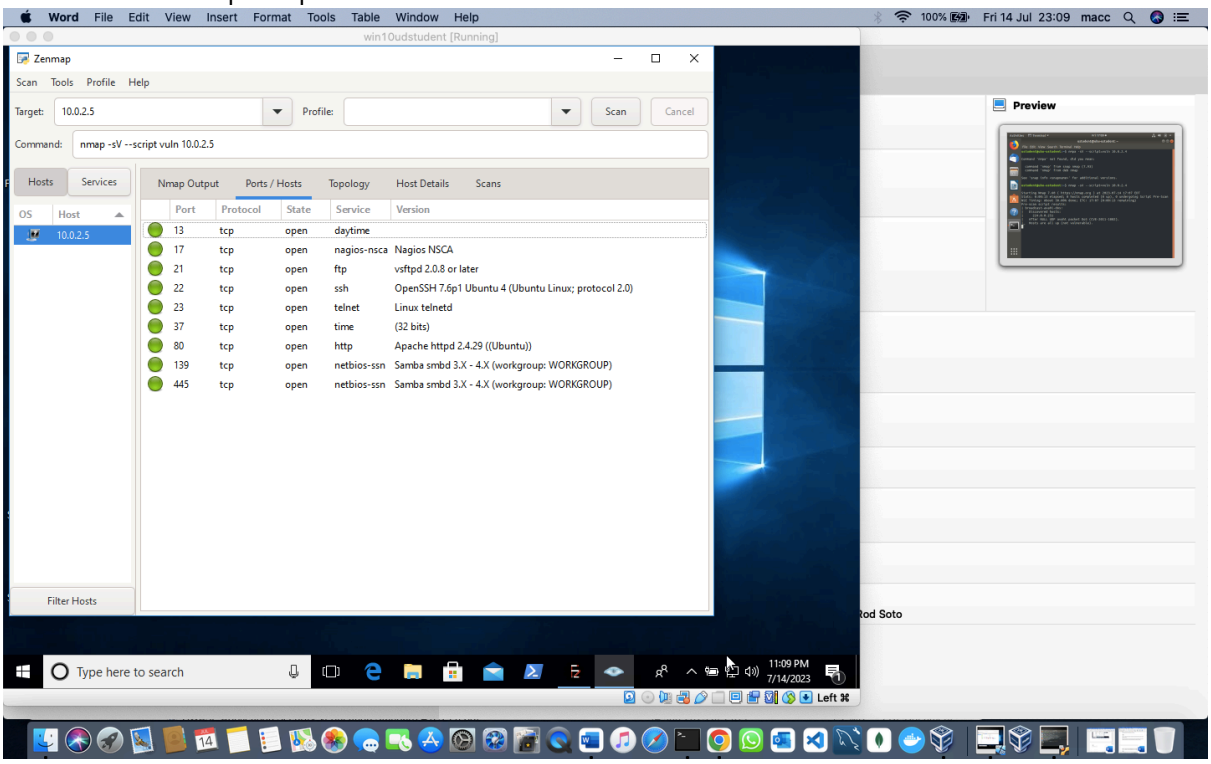
VNC viewer is installed on this machine:



TASK 4

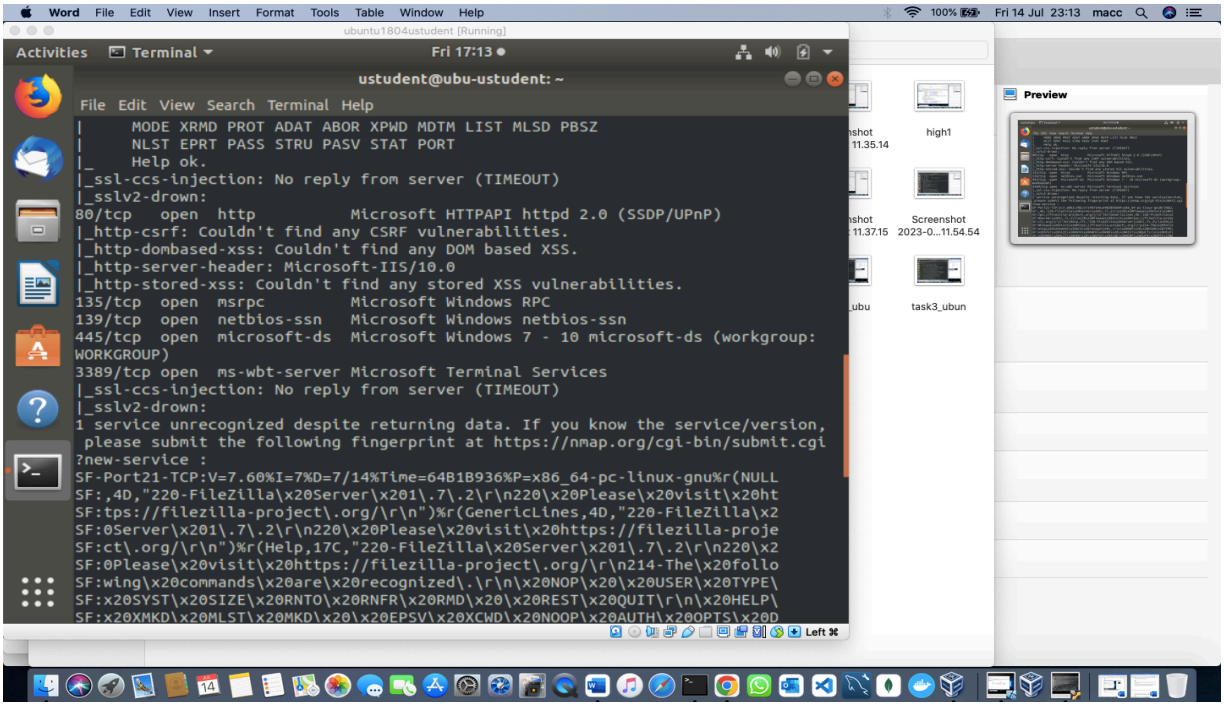
Ubuntu

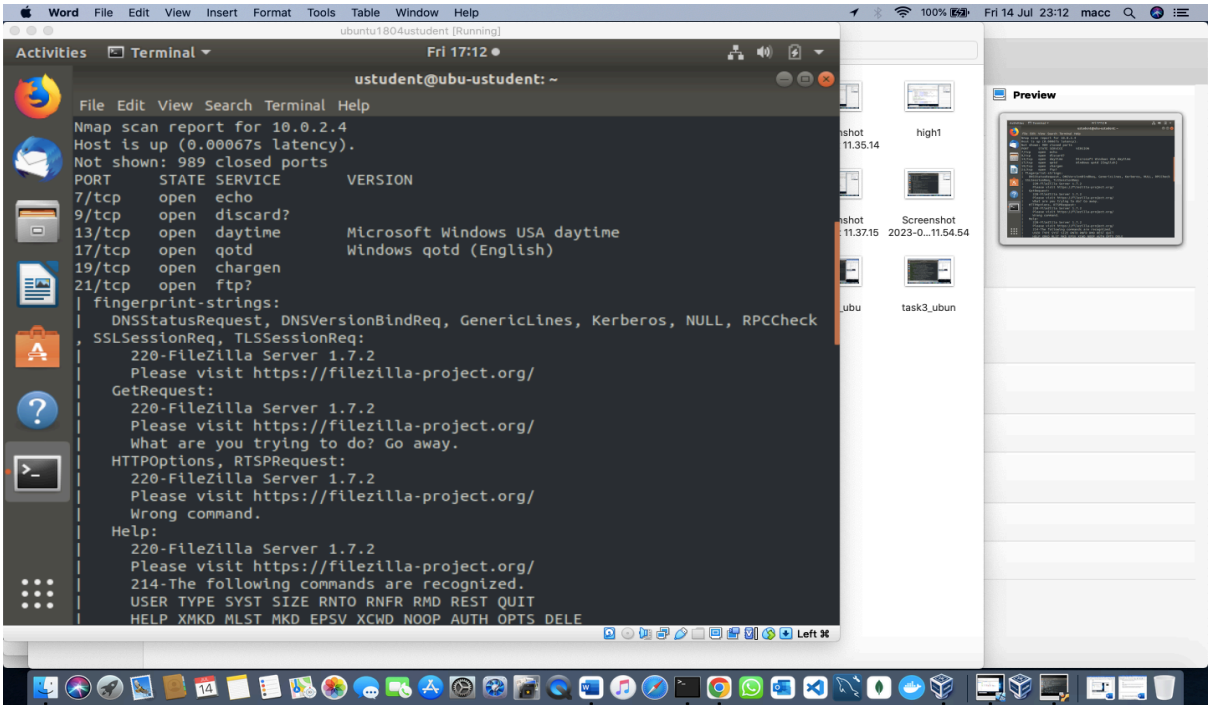
Here are the open ports on the machine:



Windows

Here are the open ports on the machine:





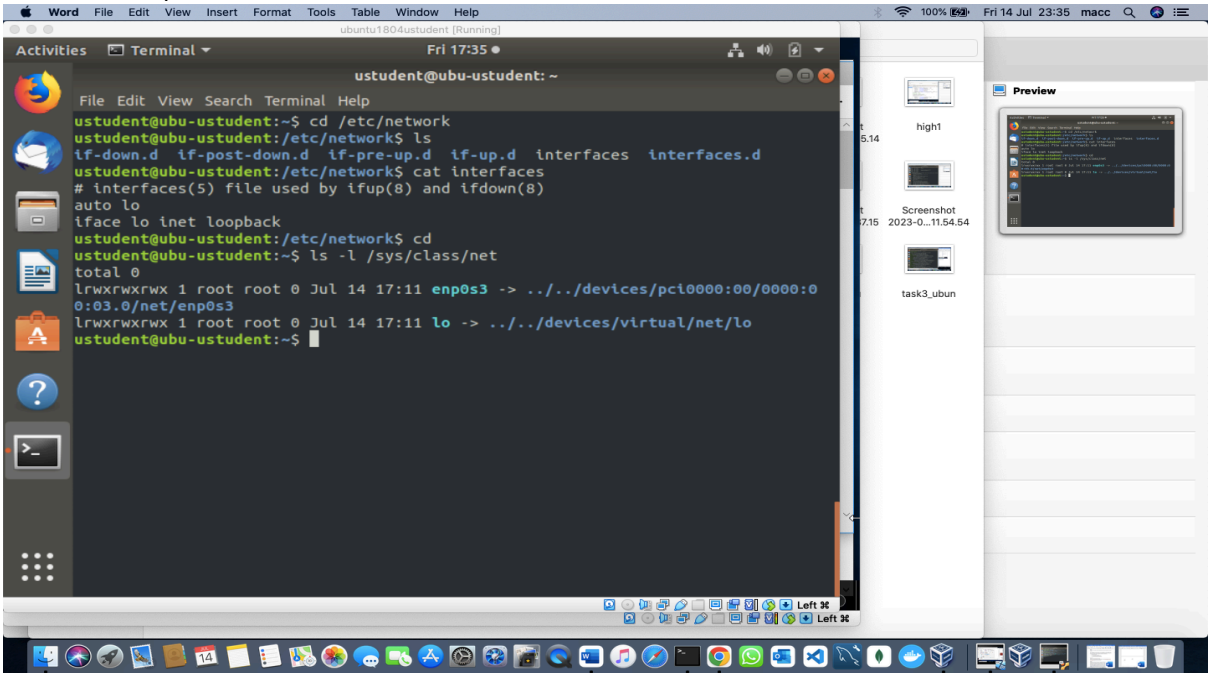
Recommendation: Close/Disable any service that is not in use.

STEP 2: Assess Access Management at Targeted Assets

TASK 1

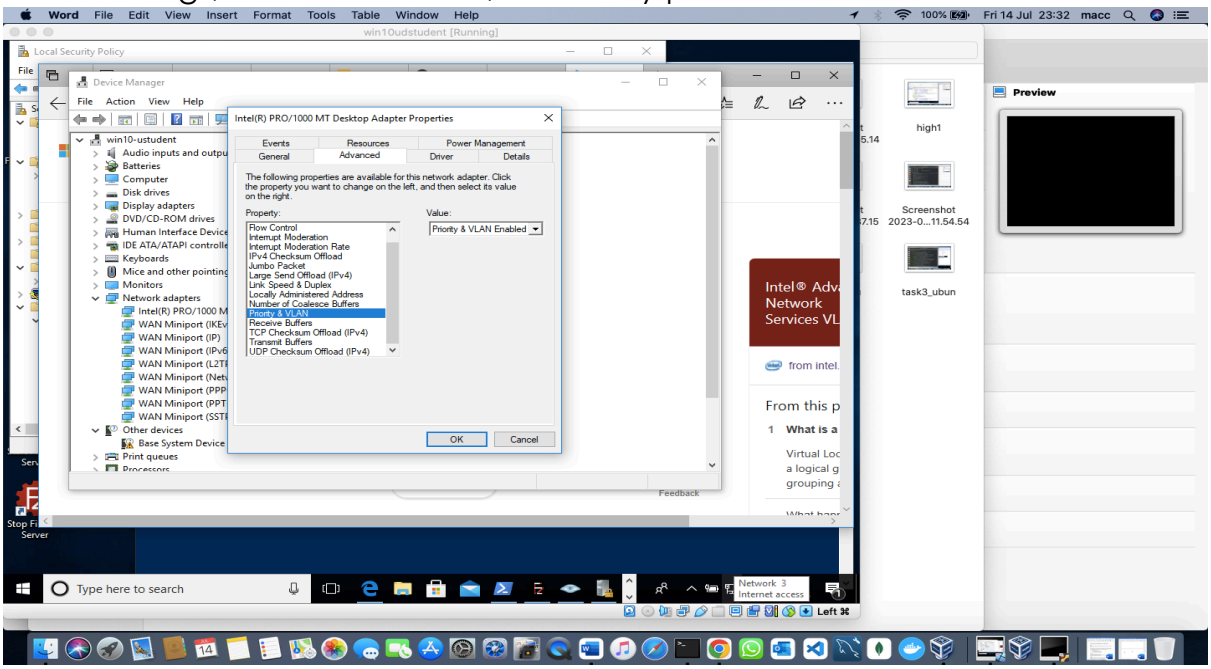
Ubuntu

No VLANs present:

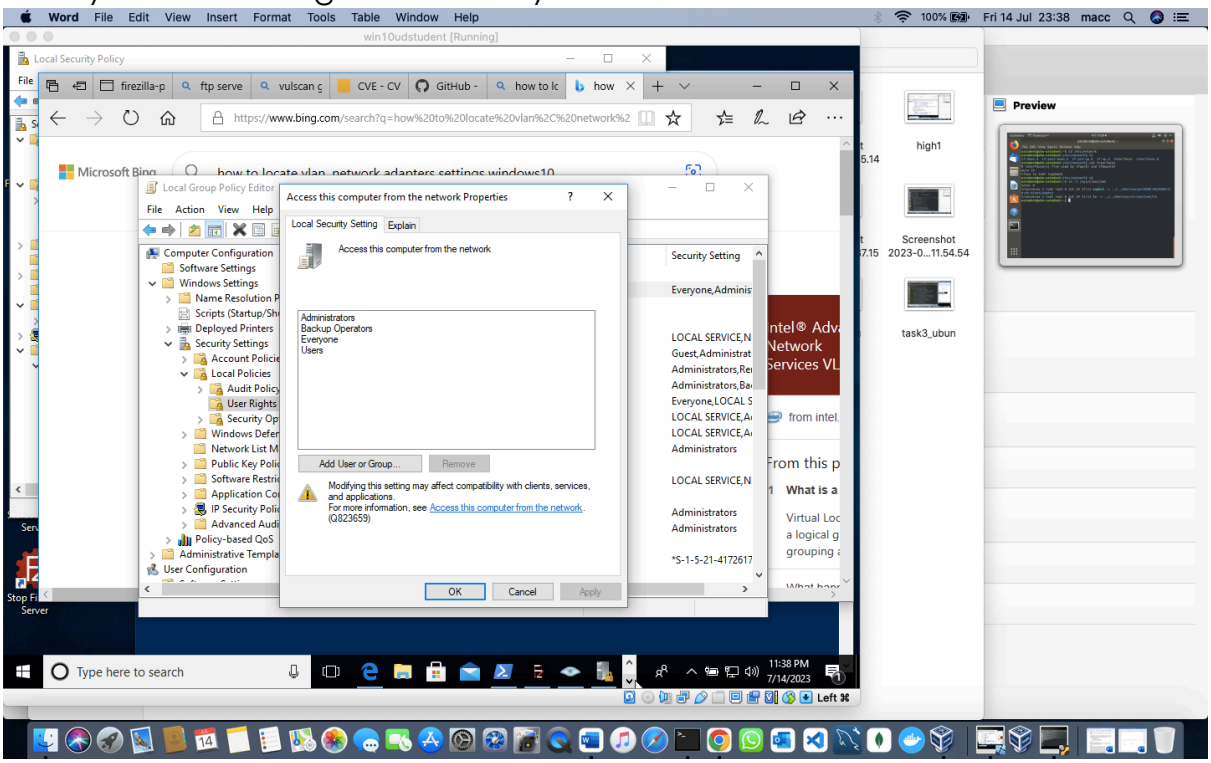


Windows

VLAN settings, Domain isolation, IP security polices:



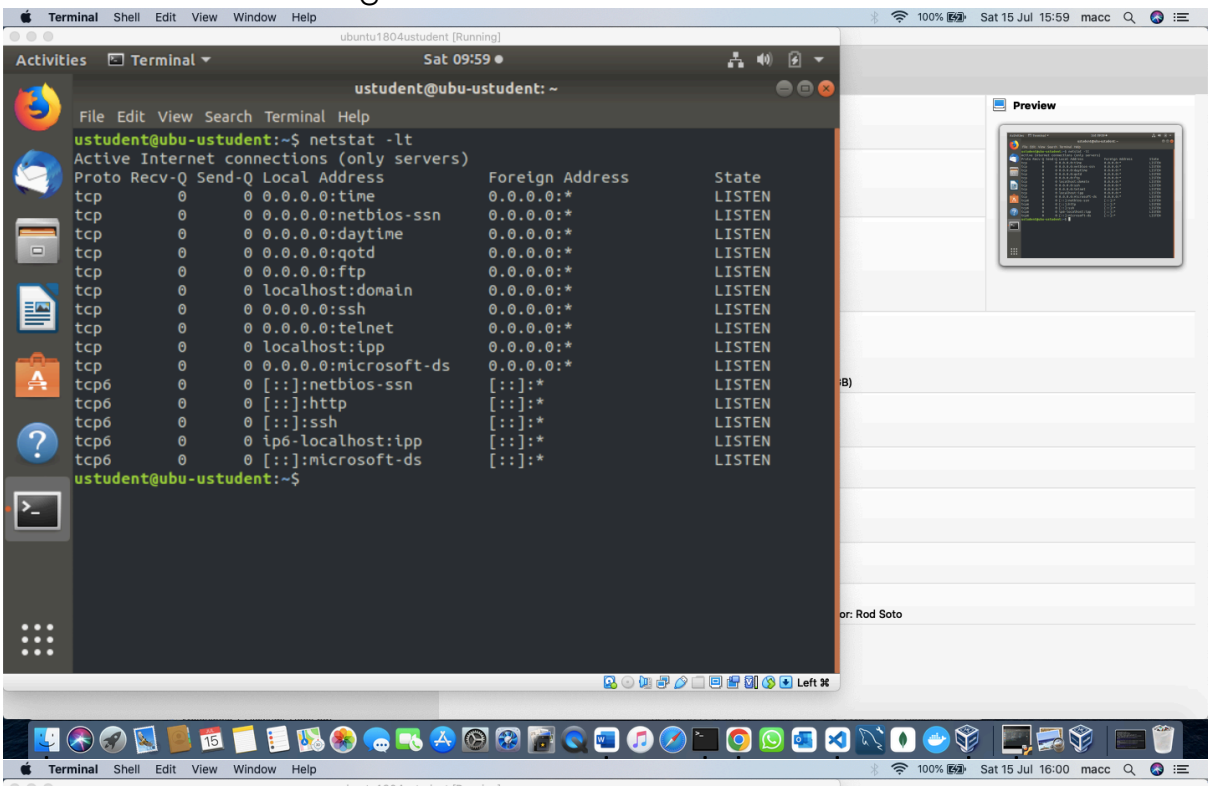
Anonymous access granted to any share:

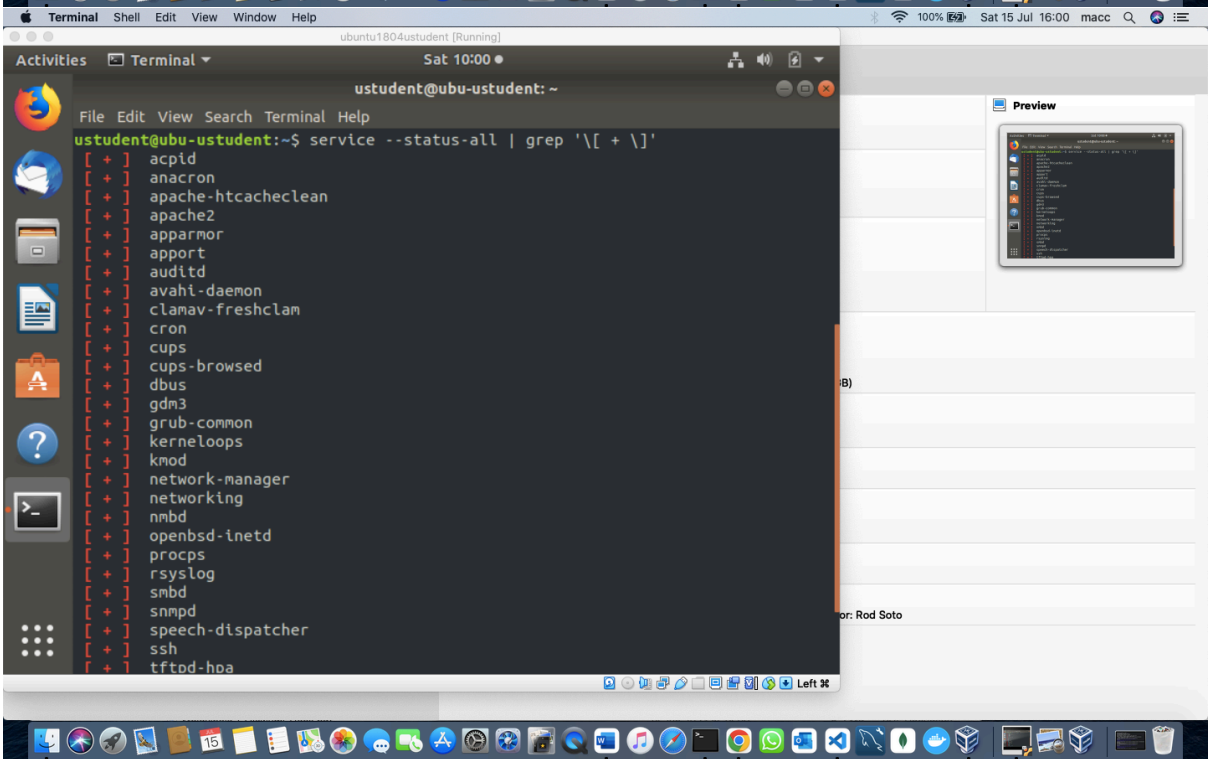


TASK 2

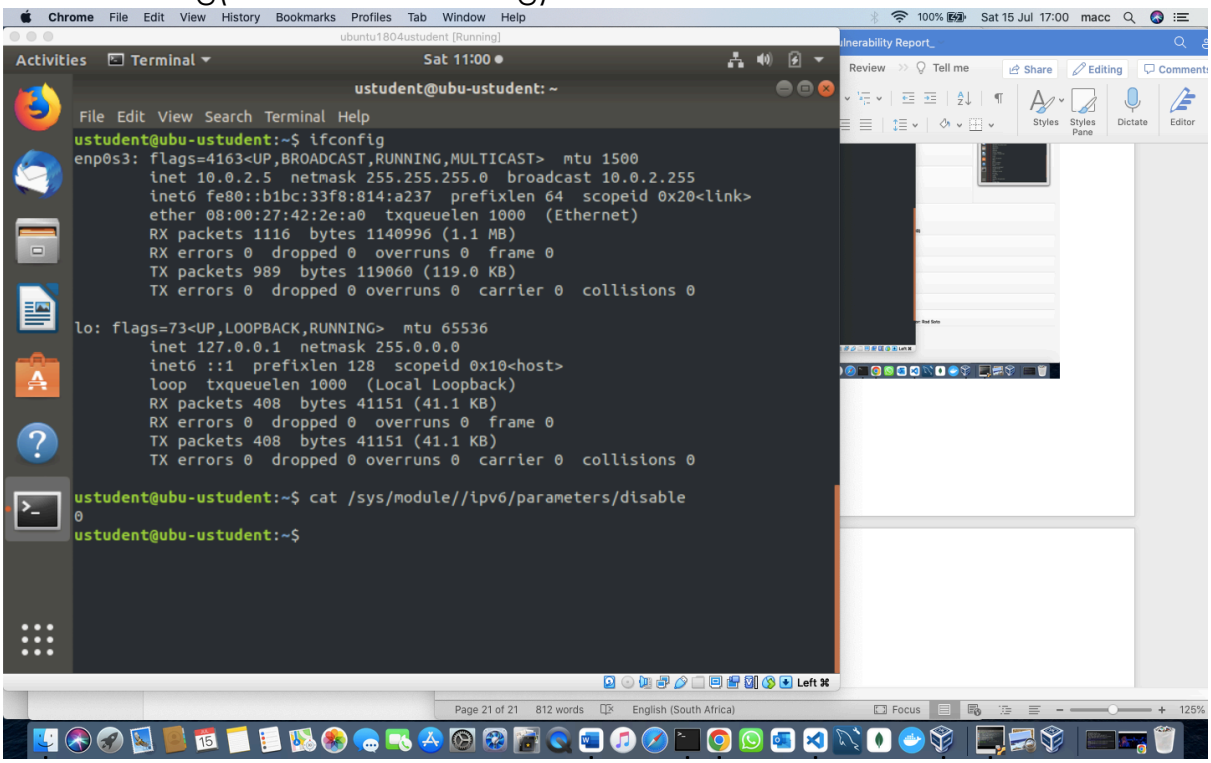
Ubuntu

Remote services running:



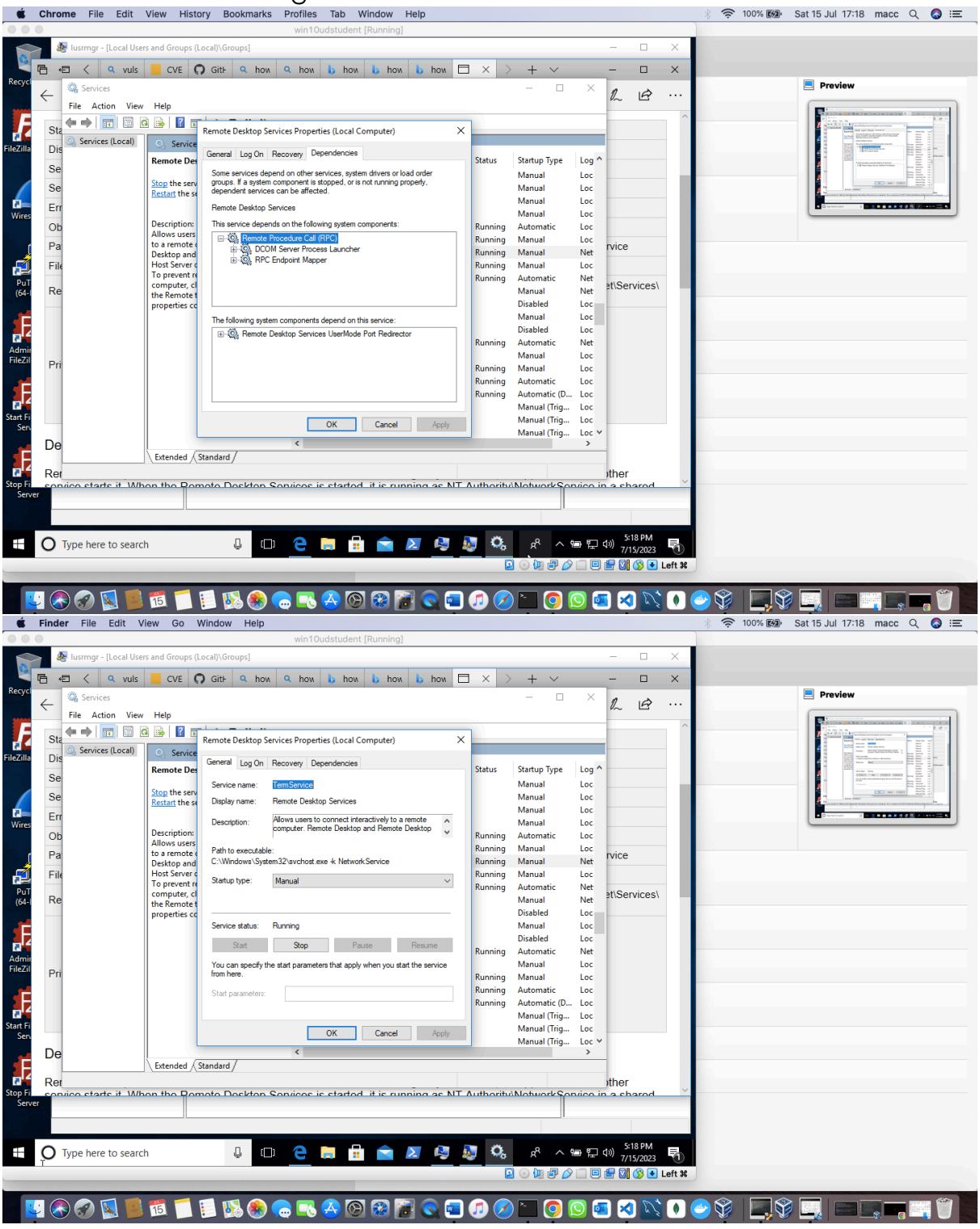


IPv6 is running(0 means it is running):

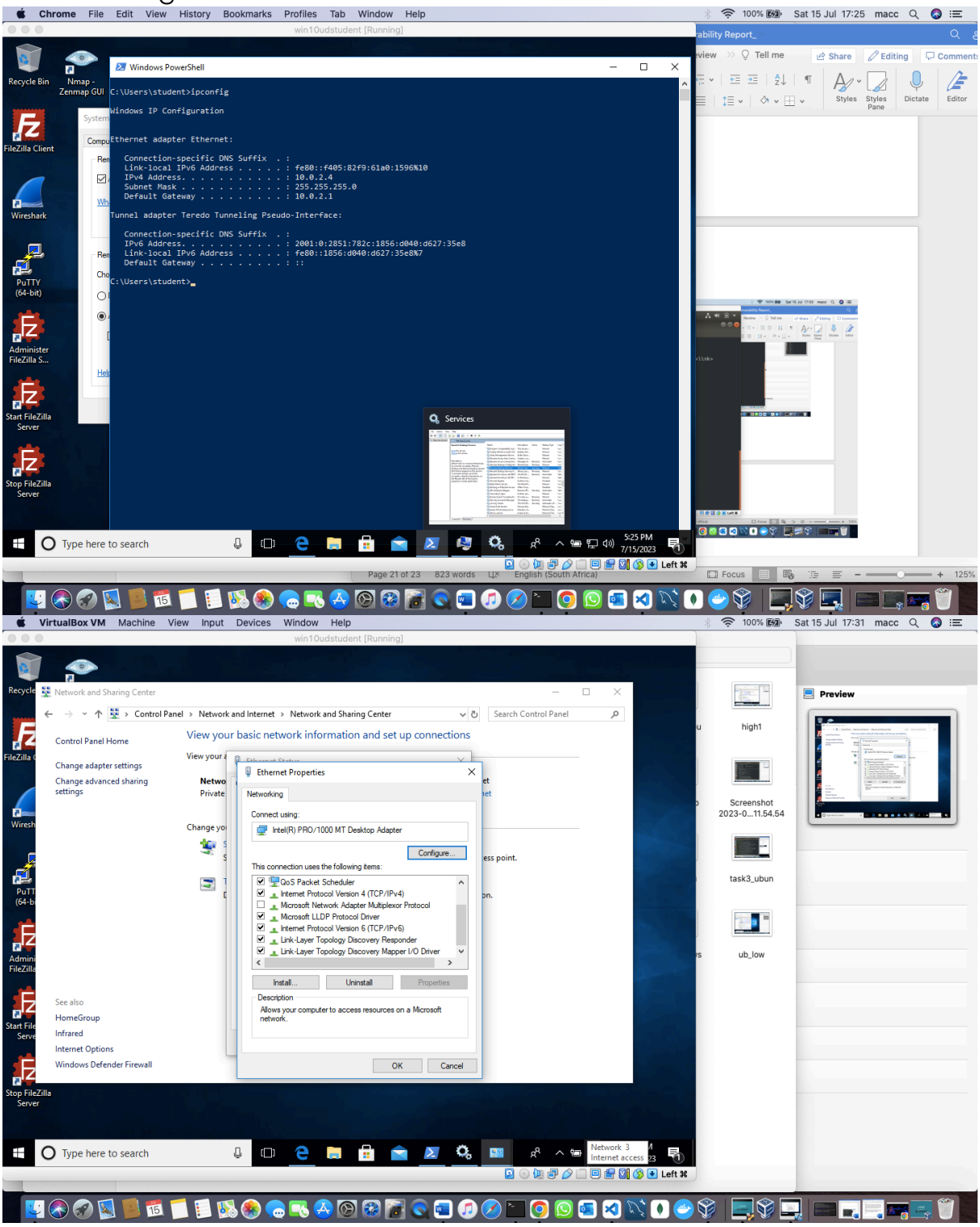


Windows

Remote services running:



IPv6 is running:

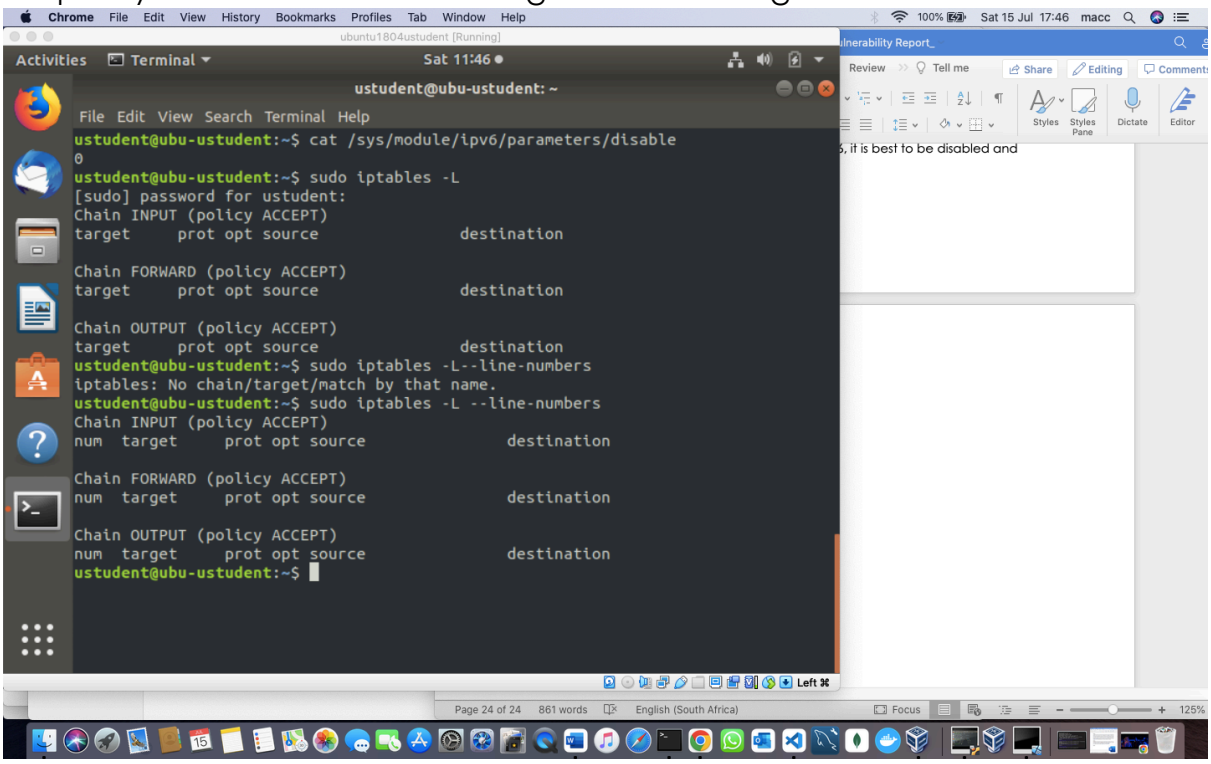


Recommendation: Since IPv6 is not widely used and the protections that apply to IPv4 do not always work with IPv6, it is best to be disabled and turned on only if needed.

Task 3

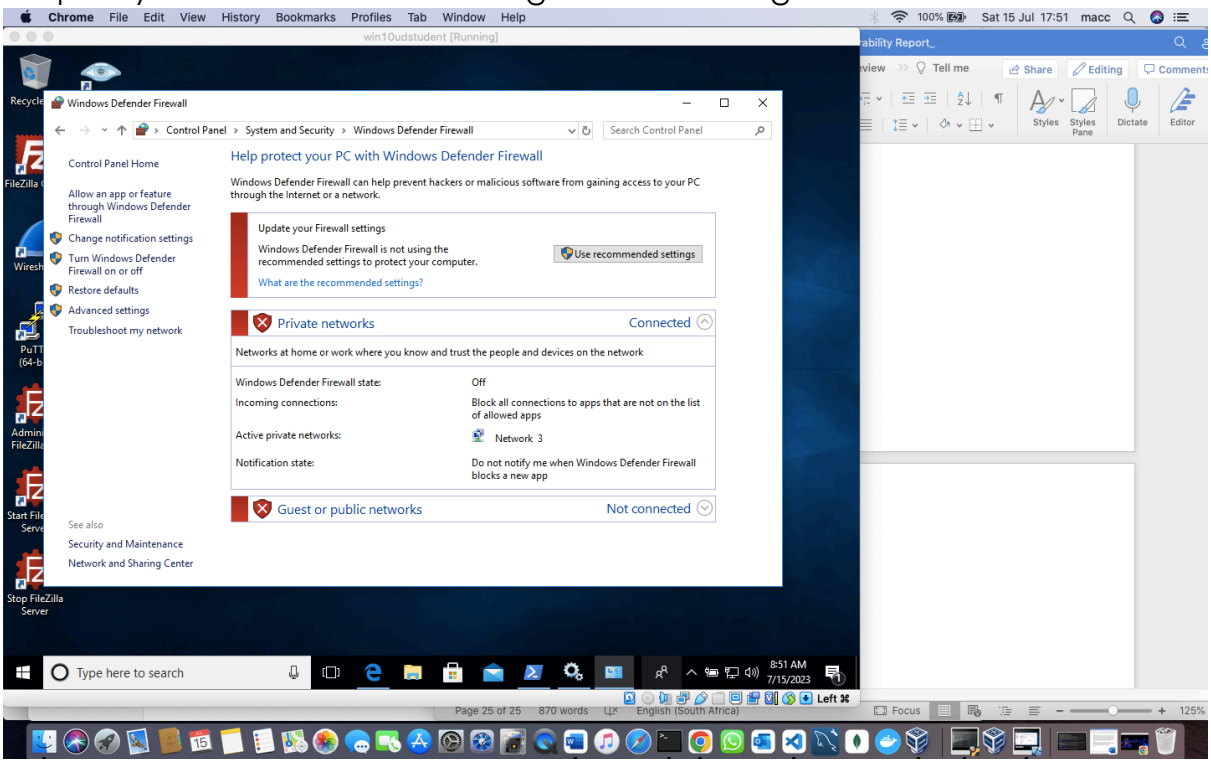
Ubuntu

No policy for correct firewall configuration is configured:



Windows

No policy for correct firewall configuration is configured:

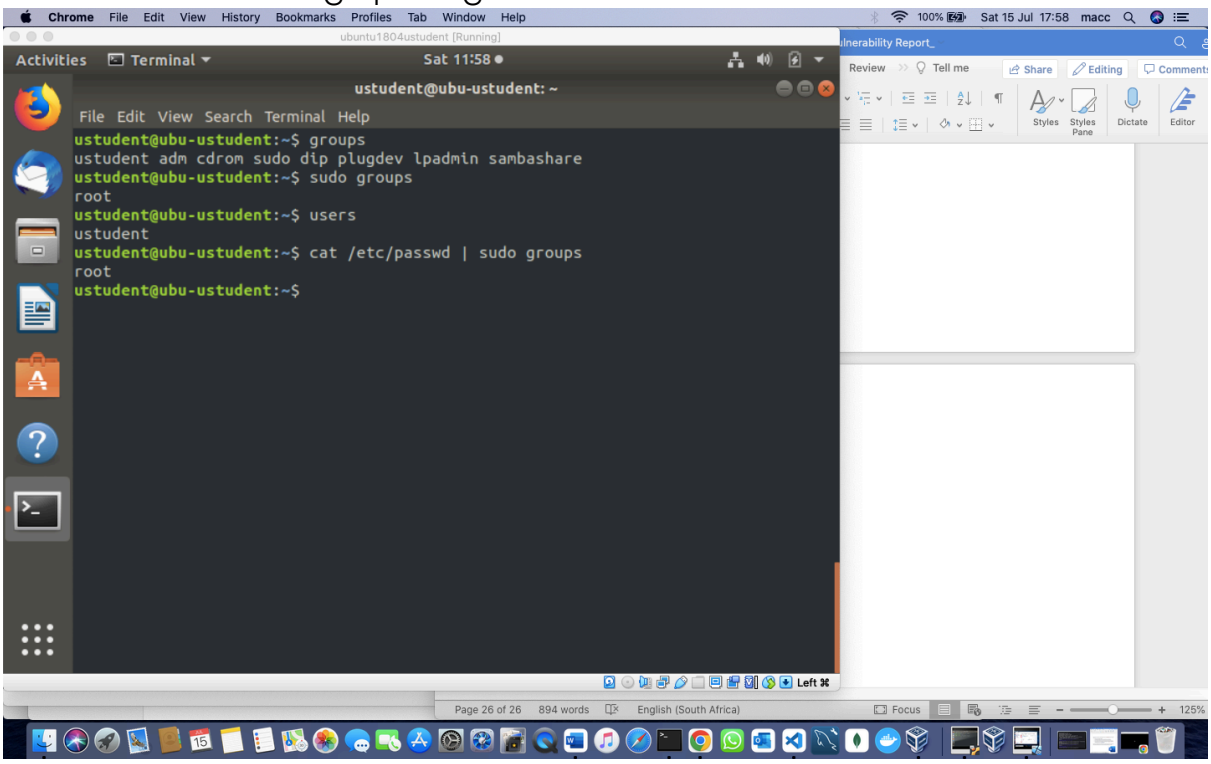


Recommendation: I would suggest to have port 22 open because it is encrypted.

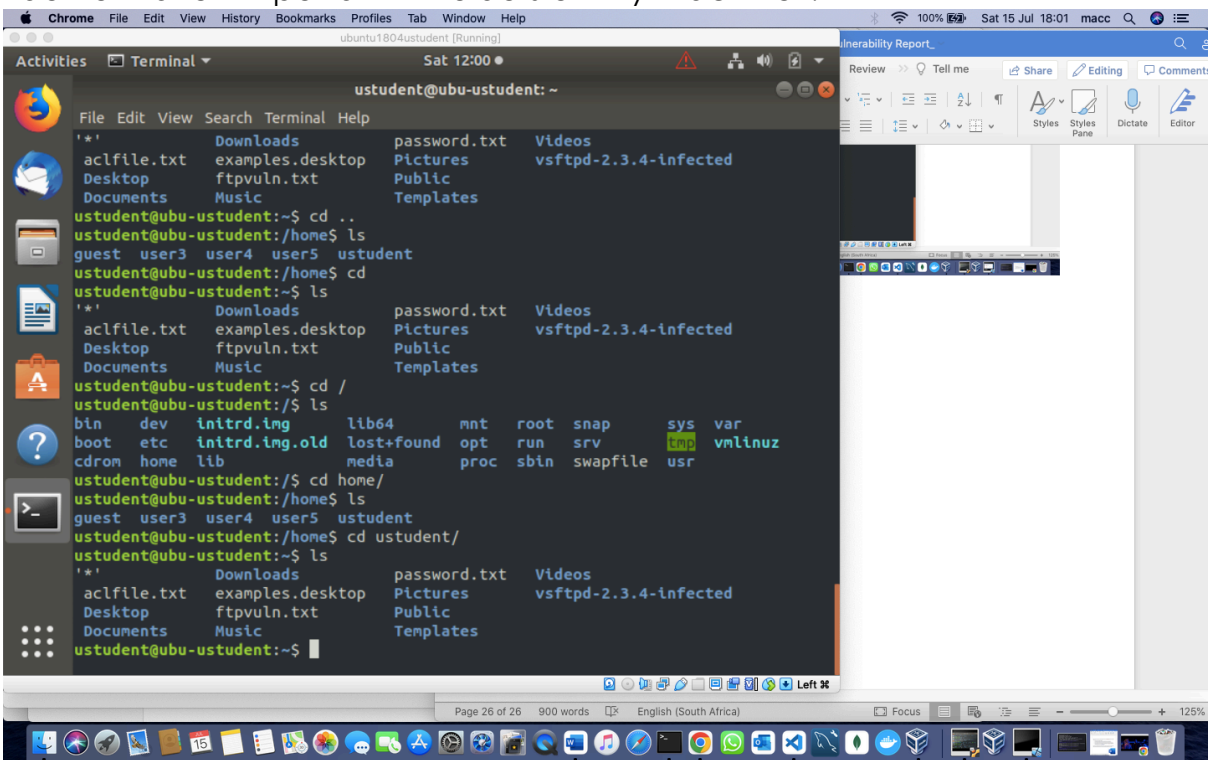
Task 4

Ubuntu

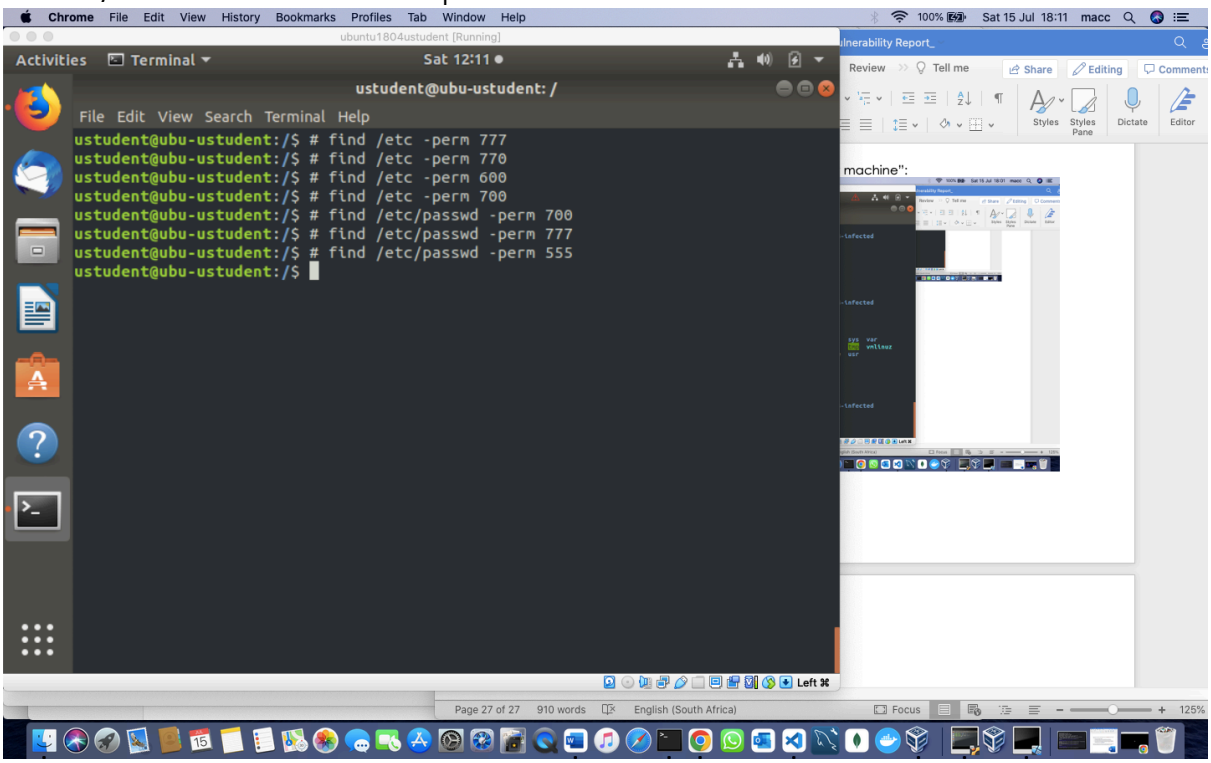
The root user have high privileges:



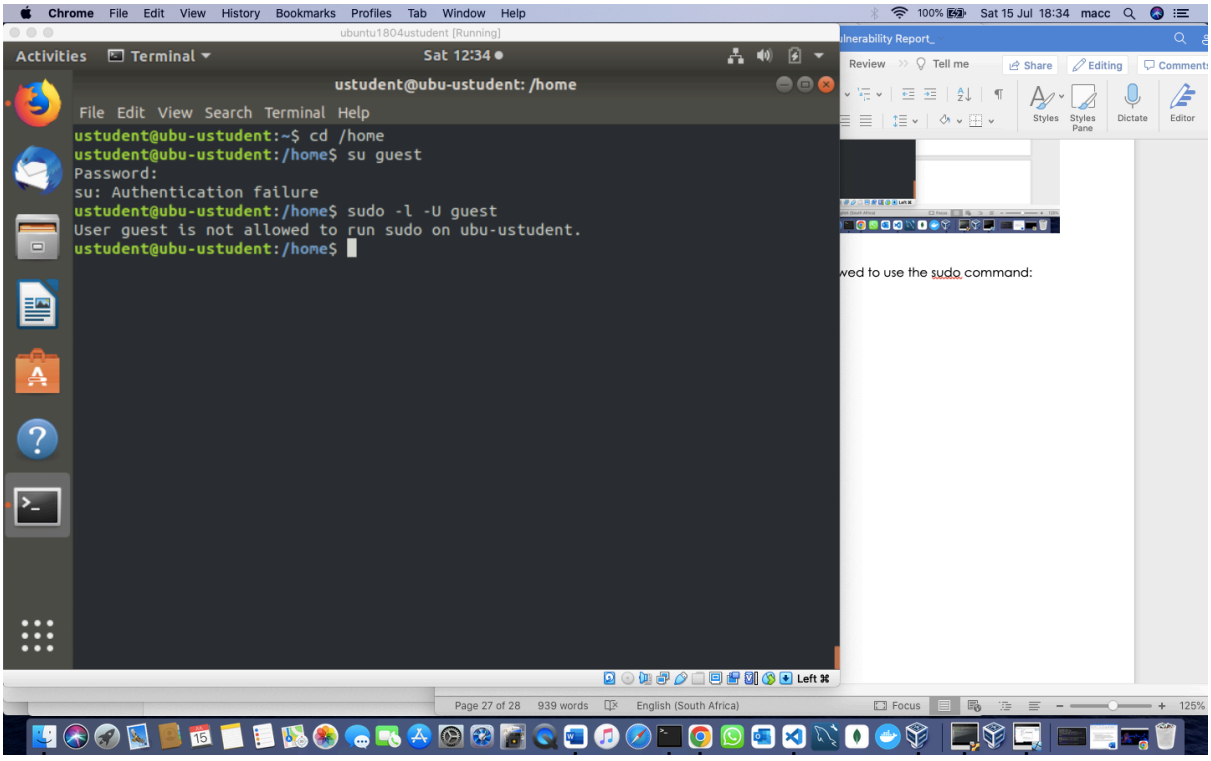
I do not have "important PII folders on my machine":



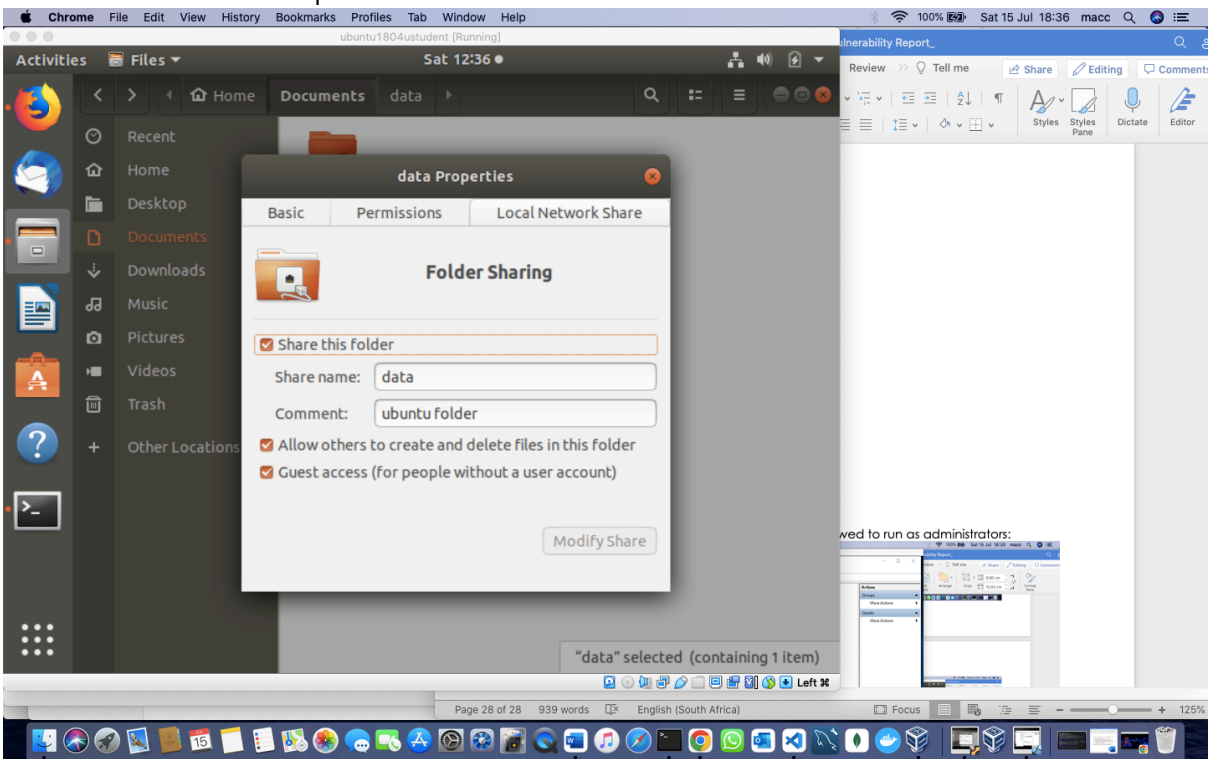
No file/folder with excessive permissions:



Guest accounts are enabled but not allowed to use the sudo command:

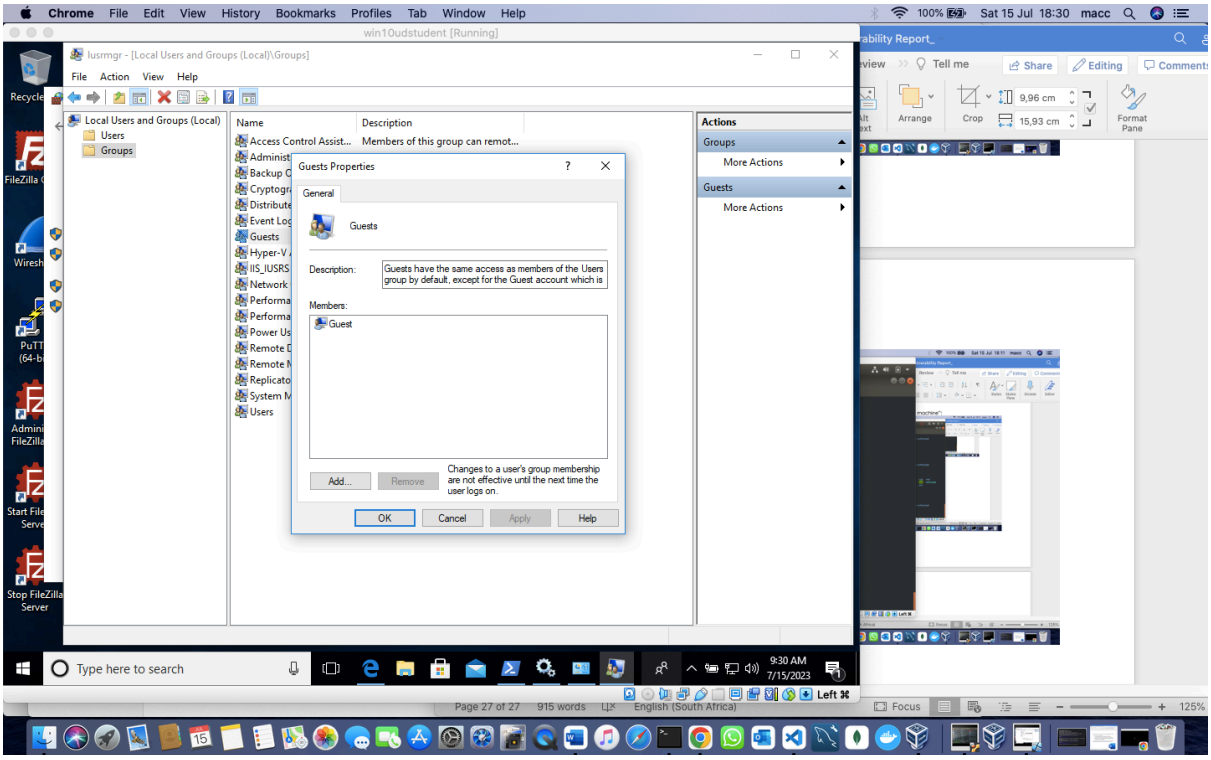


There are excessive permissions on the data folder:

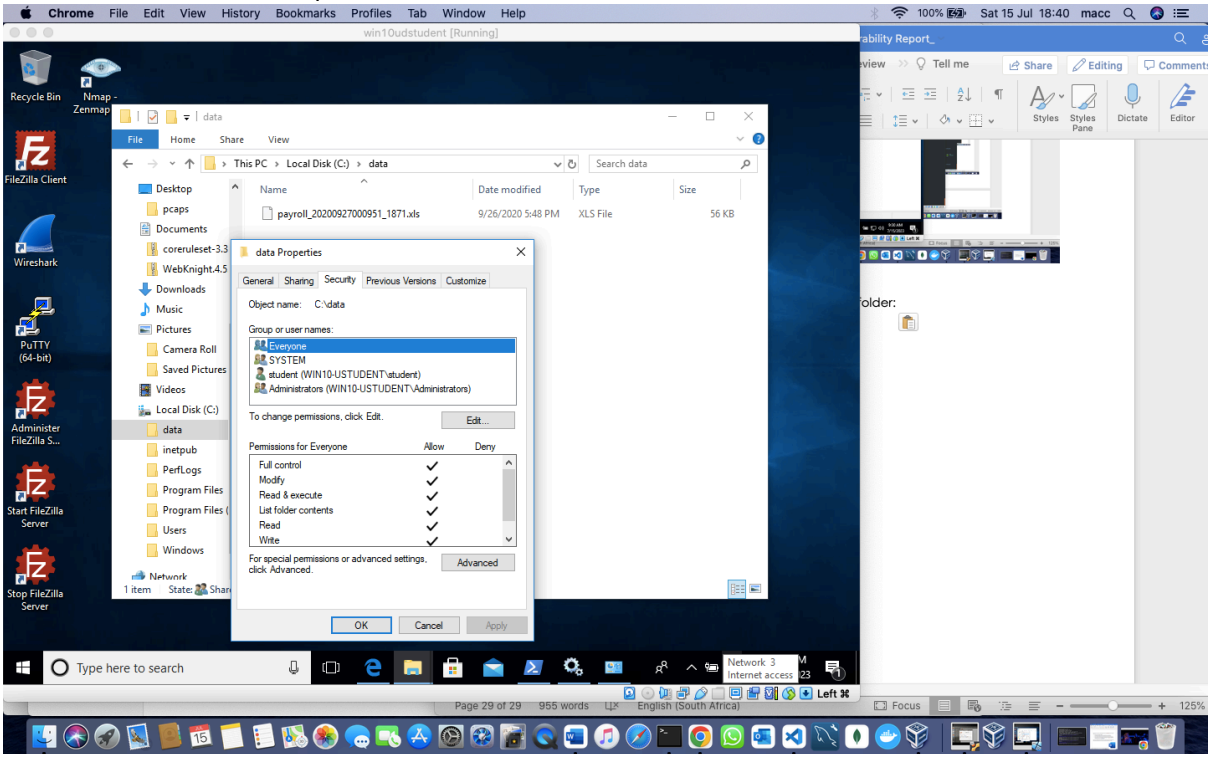


Windows

Guest accounts are enabled but not allowed to run as administrators:



There are excessive permissions on the data folder:

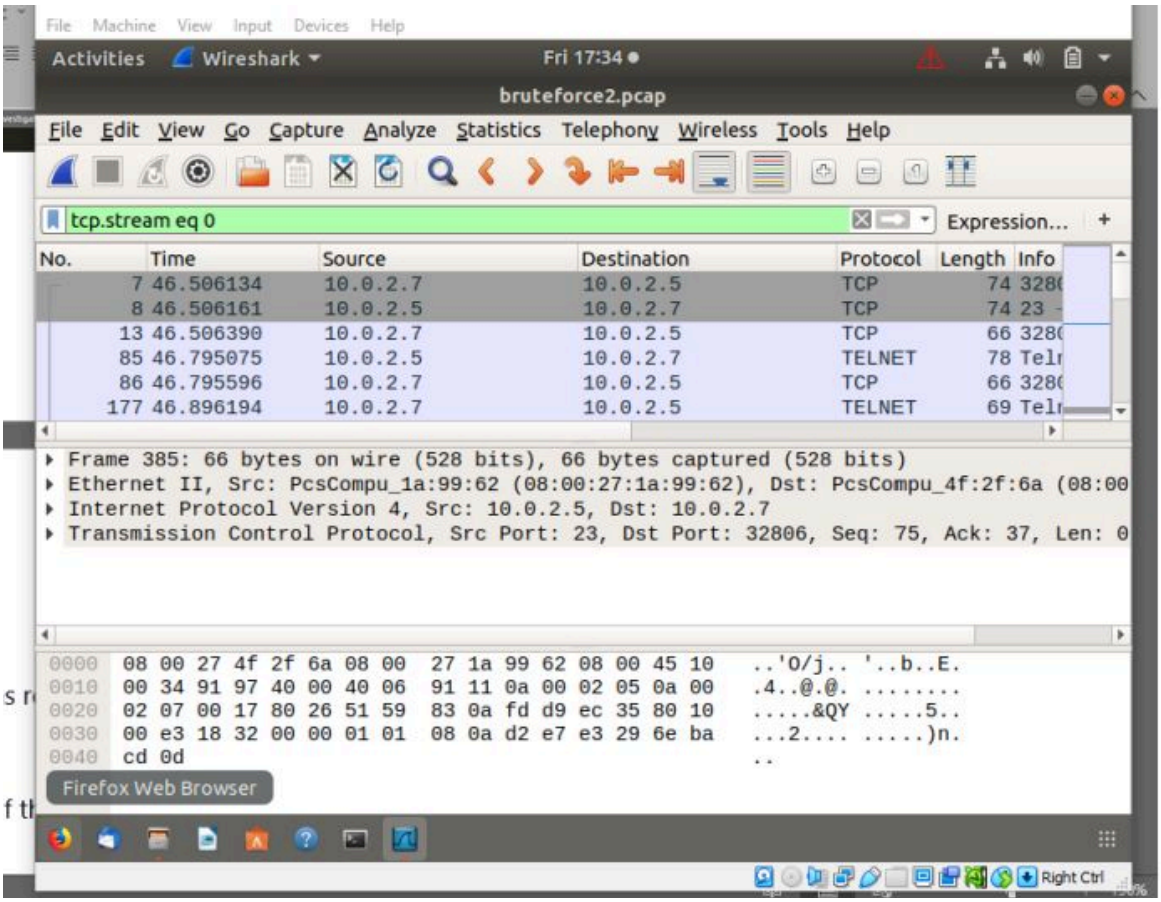


Recommendation: Accounts and permissions should be restricted to users who must have access for their work on both machines.

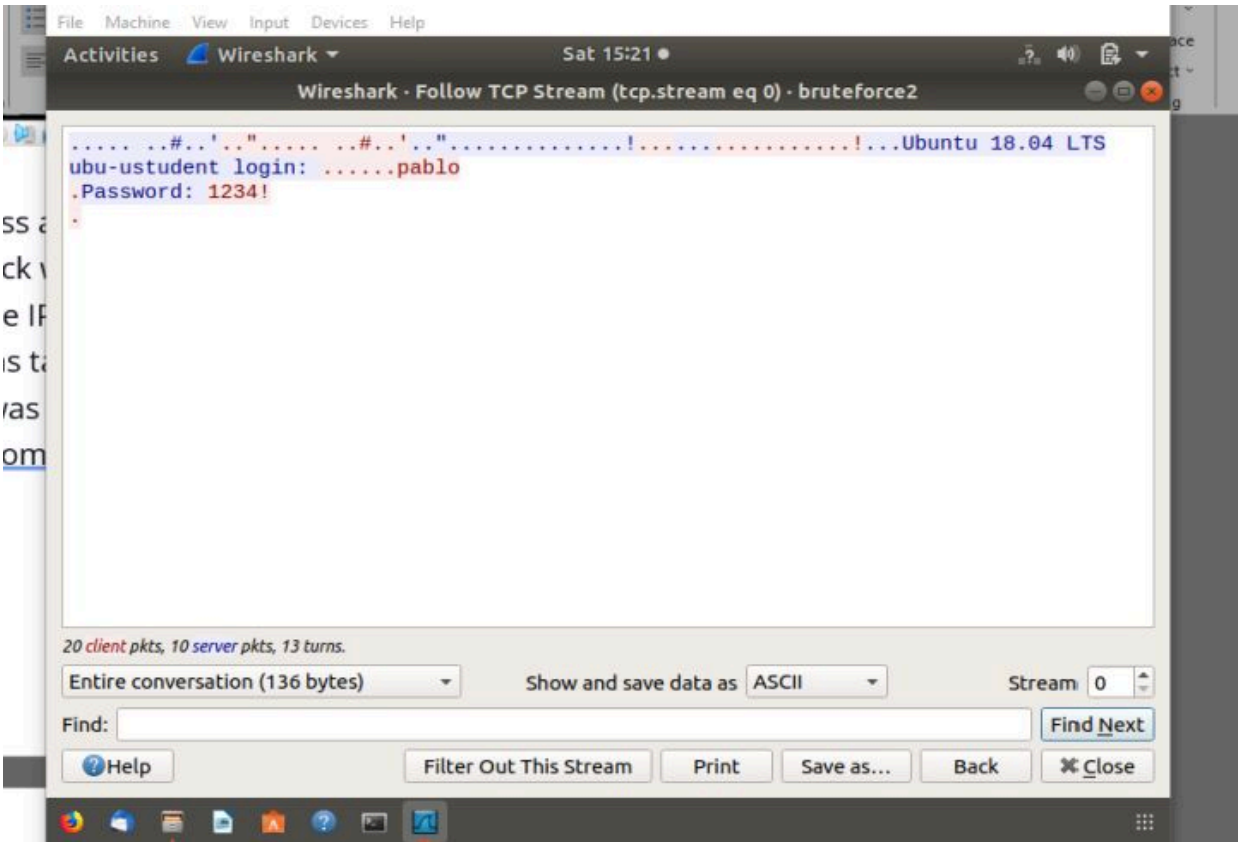
STEP 3: Log Monitoring Setup for Detection at Targeted Assets

TASK 1

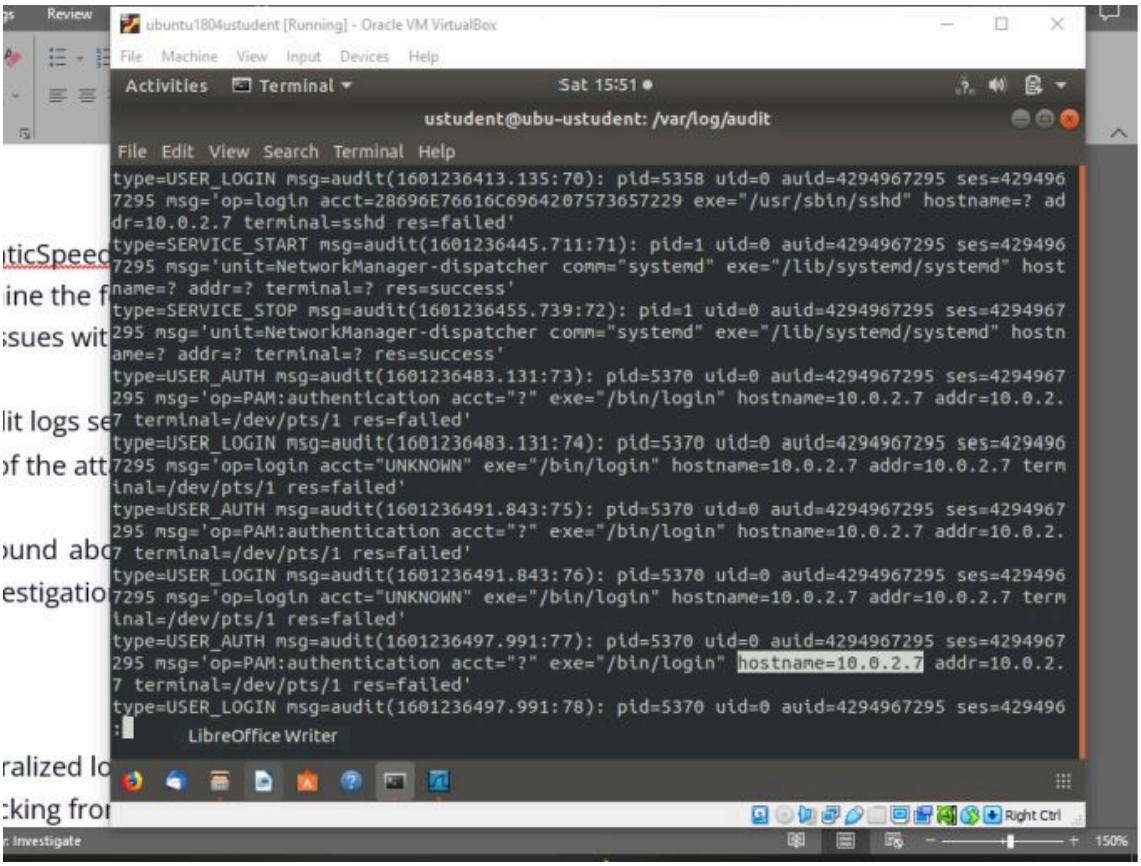
A brute force attack was recorded,
The source of the attack was 10.0.2.7:



The TCP protocol was targeted,
‘1234’ was the successful password used,
“pablo” user was compromised:



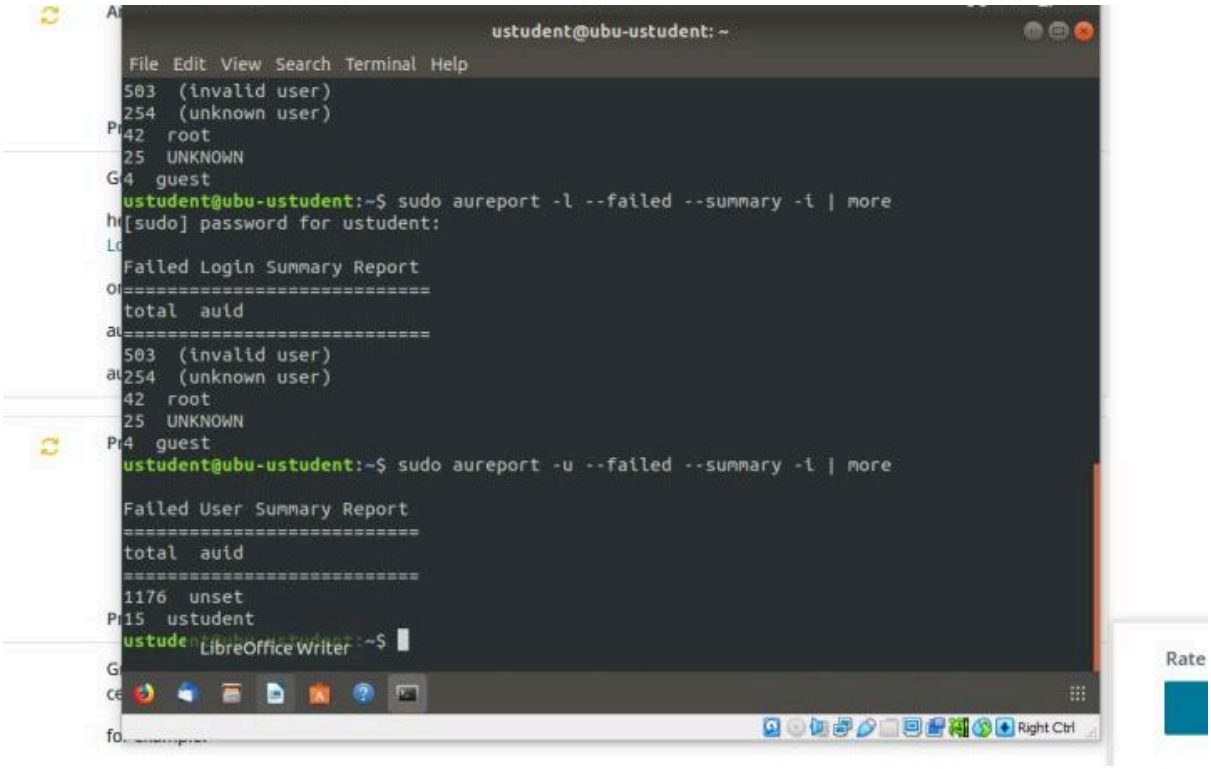
Task 2


ubuntu1804ustudent [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Sat 15:51
ustudent@ubu-ustudent: /var/log/audit
File Edit View Search Terminal Help
type=USER_LOGIN msg=audit(1601236413.135:70): pid=5358 uid=0 auid=4294967295 ses=4294967295 msg='op=login acct=28696E76616C6964207573657229 exe="/usr/sbin/sshd" hostname=? addr=10.0.2.7 terminal=sshd res=failed'
type=SERVICE_START msg=audit(1601236445.711:71): pid=1 uid=0 auid=4294967295 ses=4294967295 msg='unit=NetworkManager-dispatcher comm="systemd" exe="/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'
type=SERVICE_STOP msg=audit(1601236455.739:72): pid=1 uid=0 auid=4294967295 ses=4294967295 msg='unit=NetworkManager-dispatcher comm="systemd" exe="/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'
type=USER_AUTH msg=audit(1601236483.131:73): pid=5370 uid=0 auid=4294967295 ses=4294967295 msg='op=PAM:authentication acct="?" exe="/bin/login" hostname=10.0.2.7 addr=10.0.2.7 terminal=/dev/pts/1 res=failed'
type=USER_LOGIN msg=audit(1601236483.131:74): pid=5370 uid=0 auid=4294967295 ses=4294967295 msg='op=login acct="UNKNOWN" exe="/bin/login" hostname=10.0.2.7 addr=10.0.2.7 terminal=/dev/pts/1 res=failed'
type=USER_AUTH msg=audit(1601236491.843:75): pid=5370 uid=0 auid=4294967295 ses=4294967295 msg='op=PAM:authentication acct="?" exe="/bin/login" hostname=10.0.2.7 addr=10.0.2.7 terminal=/dev/pts/1 res=failed'
type=USER_LOGIN msg=audit(1601236491.843:76): pid=5370 uid=0 auid=4294967295 ses=4294967295 msg='op=login acct="UNKNOWN" exe="/bin/login" hostname=10.0.2.7 addr=10.0.2.7 terminal=/dev/pts/1 res=failed'
type=USER_AUTH msg=audit(1601236497.991:77): pid=5370 uid=0 auid=4294967295 ses=4294967295 msg='op=PAM:authentication acct="?" exe="/bin/login" hostname=10.0.2.7 addr=10.0.2.7 terminal=/dev/pts/1 res=failed'
type=USER_LOGIN msg=audit(1601236497.991:78): pid=5370 uid=0 auid=4294967295 ses=4294967295
LibreOffice Writer
Right Ctrl
150%

Task 3

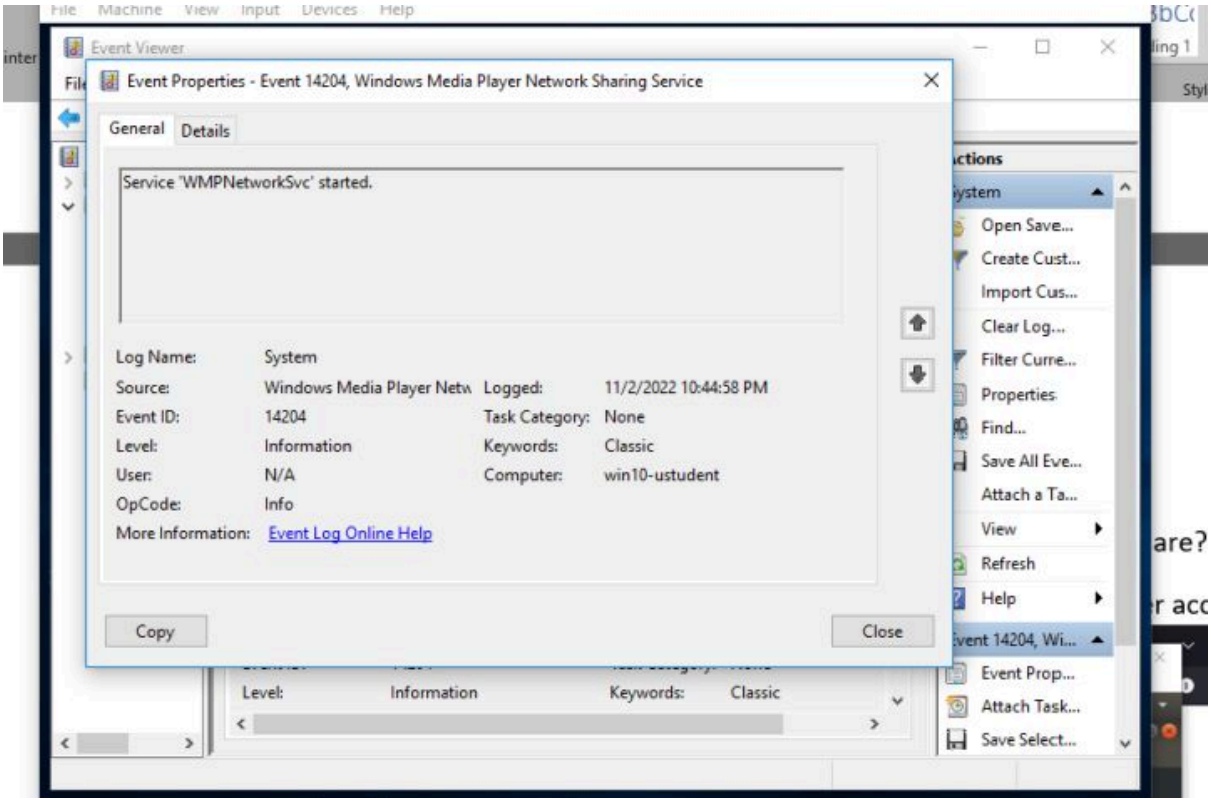
Ubuntu

Attacker's account name is unset:

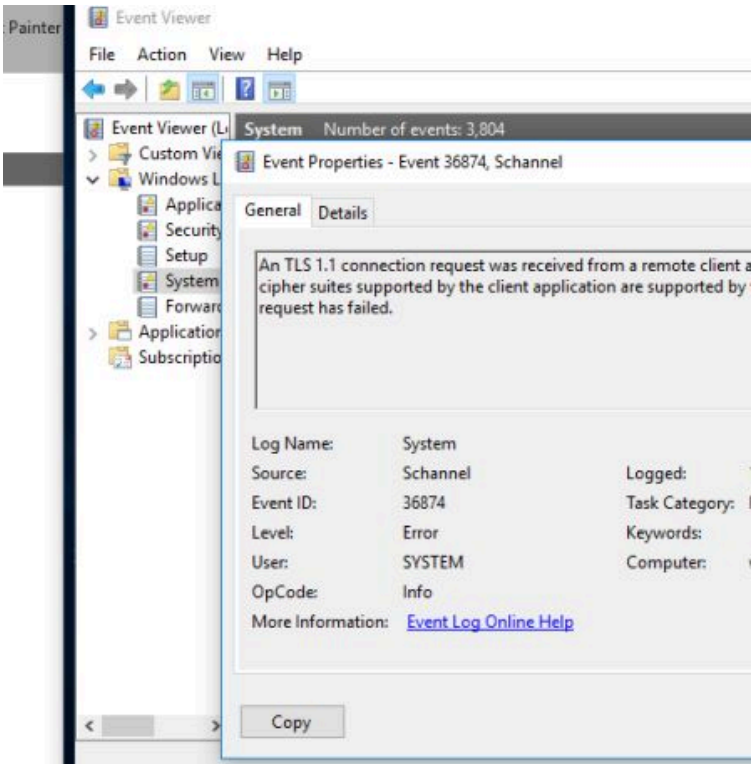


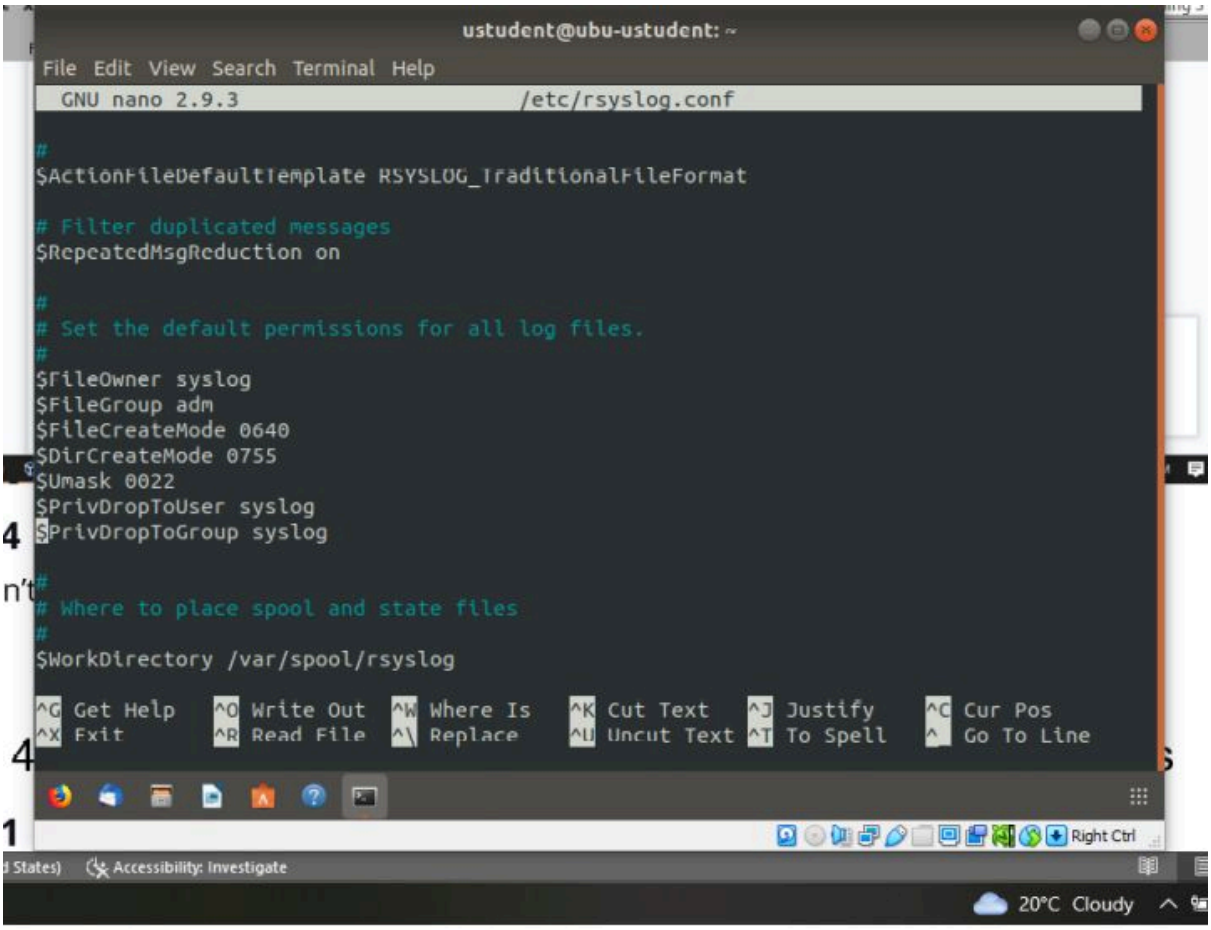
Windows

There was an account uncharacteristic of Windows trying to access the Windows share:



Task 4


Event Viewer
File Action View Help
Event Viewer (L
System Number of events: 3,804
Event Properties - Event 36874, Schannel
General Details
An TLS 1.1 connection request was received from a remote client a
cipher suites supported by the client application are supported by
request has failed.
Log Name: System
Source: Schannel
Logged:
Event ID: 36874
Task Category:
Level: Error
Keywords:
User: SYSTEM
Computer:
OpCode: Info
More Information: Event Log Online Help
Copy

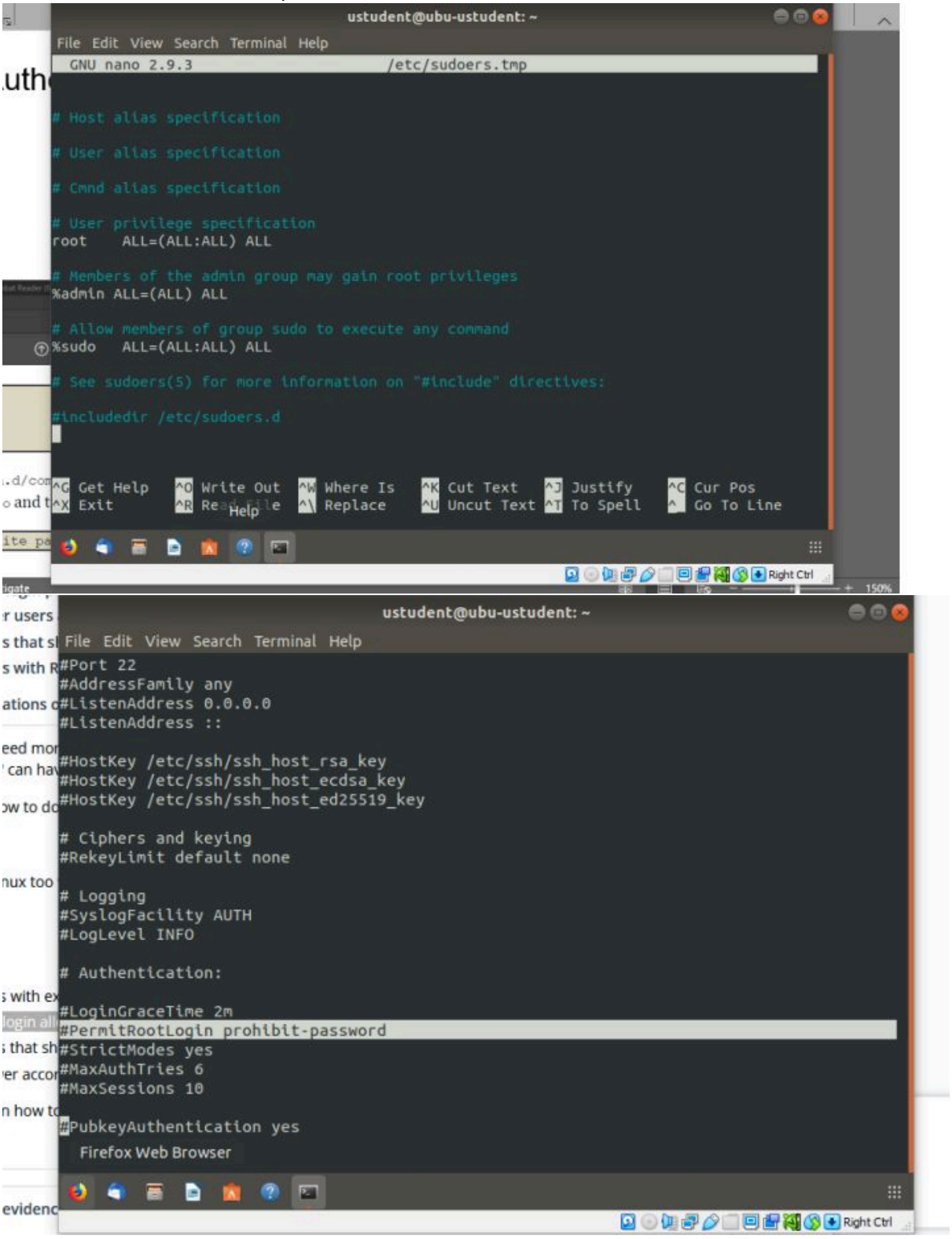

ustudent@ubu-ustudent: ~
File Edit View Search Terminal Help
GNU nano 2.9.3 /etc/rsyslog.conf
$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat
Filter duplicated messages
$RepeatedMsgReduction on
Set the default permissions for all log files.
$FileOwner syslog
$FileGroup adm
$FileCreateMode 0640
$DirCreateMode 0755
$Umask 0022
$PrivDropToUser syslog
$PrivDropToGroup syslog
Where to place spool and state files
$WorkDirectory /var/spool/rsyslog
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line
Right Ctrl
Accessibility: Investigate
20°C Cloudy

STEP 4: Assess Authentication Management at Targeted Assets

TASK 1

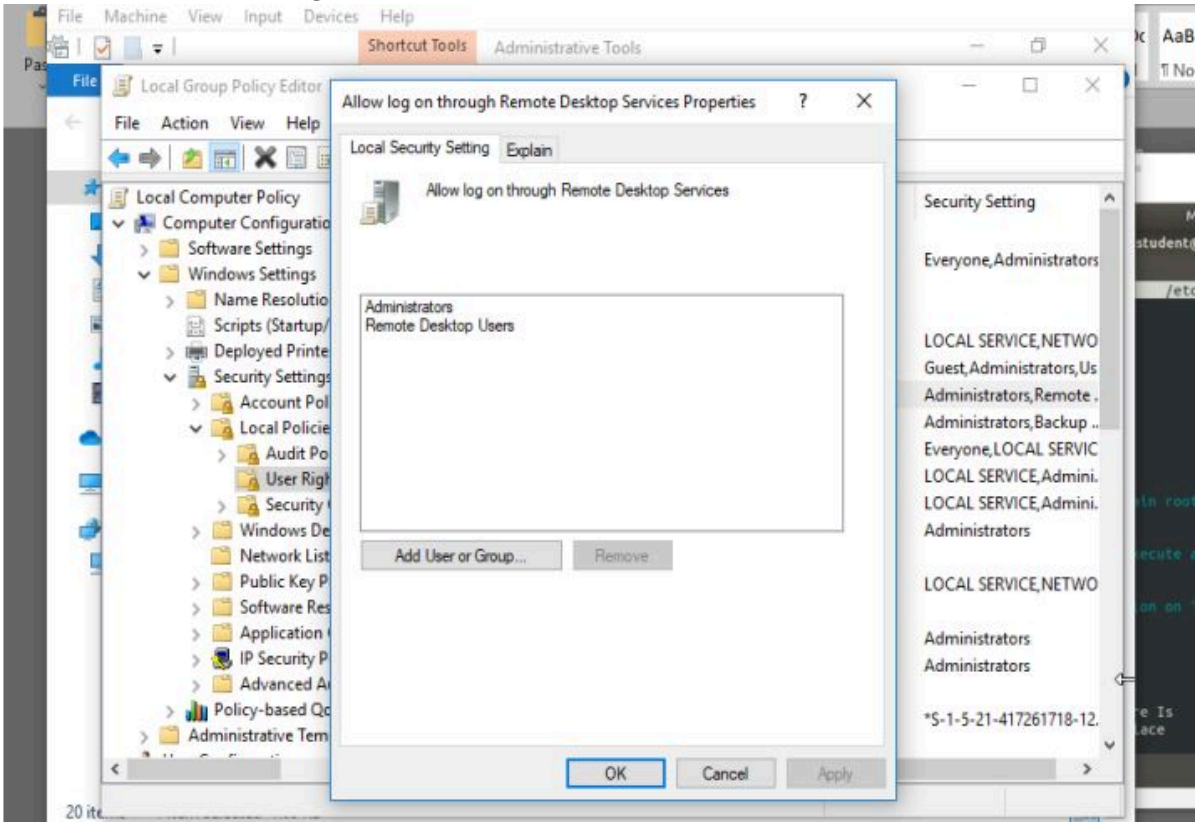
Ubuntu

No user with excessive permissions:

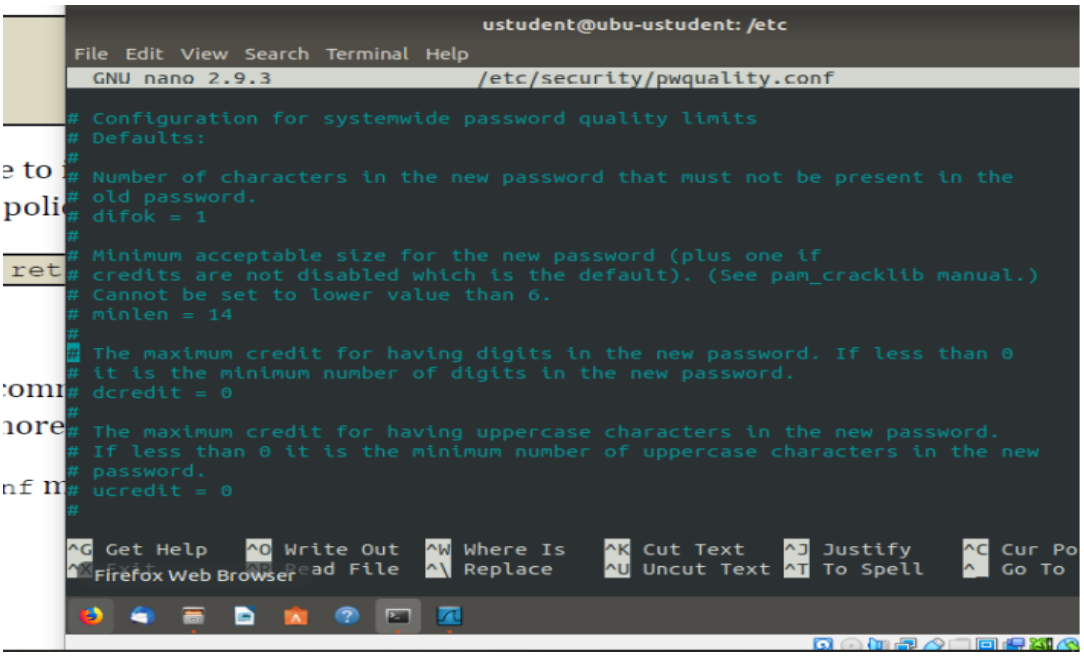


Windows

No user with excessive permissions, only the administrator and remote desktop users can login remotely:



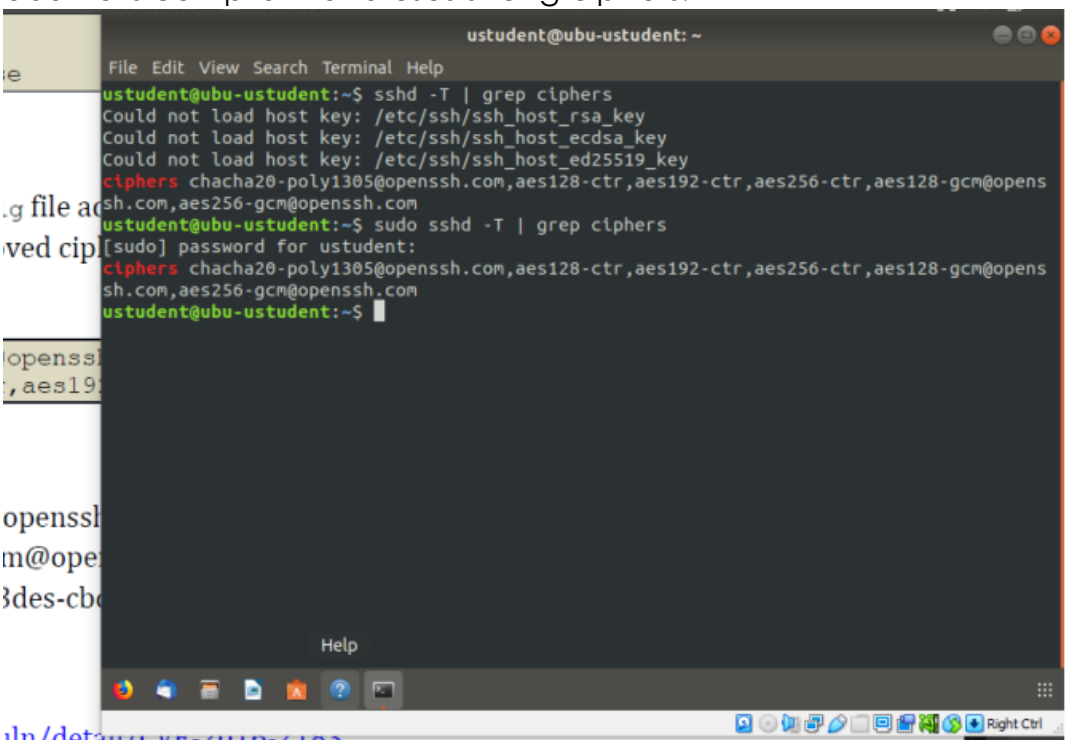
TASK 2



TASK 3

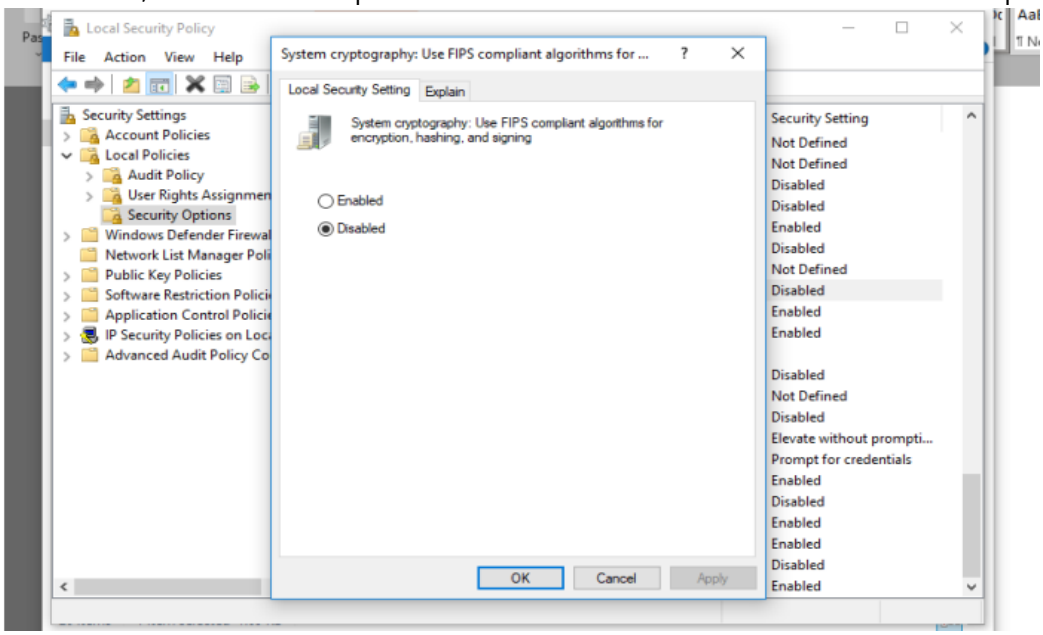
Ubuntu

Ubuntu is compliant and uses strong ciphers:

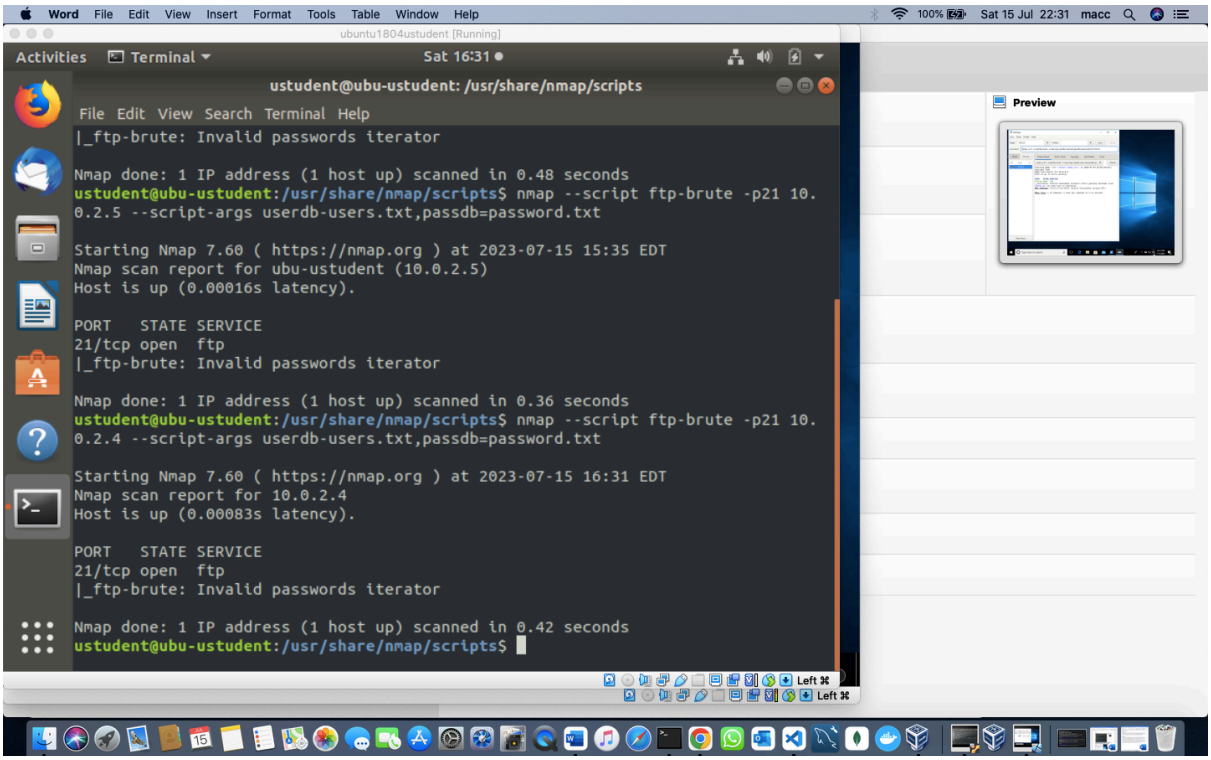


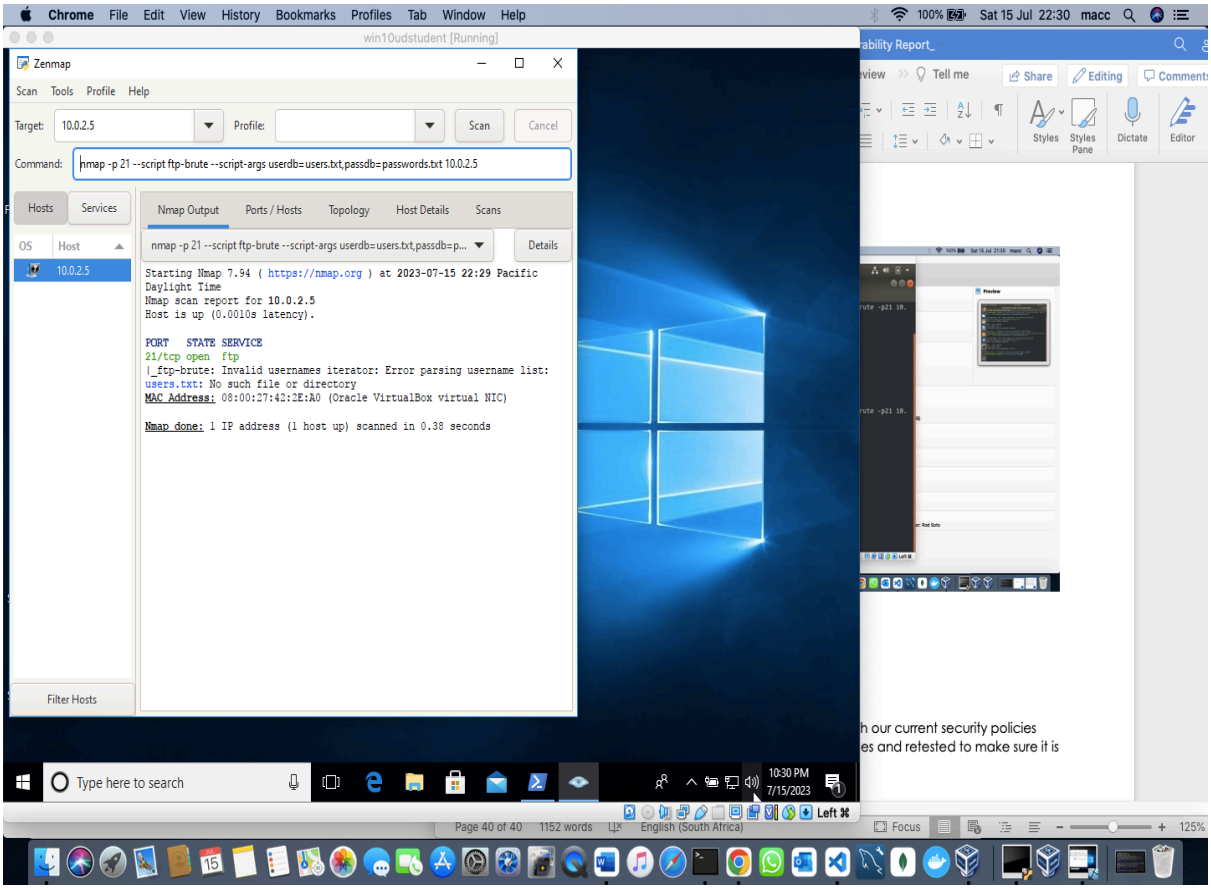
Windows

In windows, it is non-compliant but it should be enabled to be compliant:



TASK 4


Word File Edit View Insert Format Tools Table Window Help
ubuntu1804ustudent [Running]
Activities Terminal Sat 16:31
ustudent@ubu-ustudent: /usr/share/nmap/scripts
File Edit View Search Terminal Help
|_ftp-brute: Invalid passwords iterator
Nmap done: 1 IP address (1 host up) scanned in 0.48 seconds
ustudent@ubu-ustudent:/usr/share/nmap/scripts$ nmap --script ftp-brute -p21 10.0.2.5 --script-args userdb-users.txt,passdb=password.txt
Starting Nmap 7.60 (https://nmap.org) at 2023-07-15 15:35 EDT
Nmap scan report for ubu-ustudent (10.0.2.5)
Host is up (0.00016s latency).
PORT STATE SERVICE
21/tcp open ftp
|_ftp-brute: Invalid passwords iterator
Nmap done: 1 IP address (1 host up) scanned in 0.36 seconds
ustudent@ubu-ustudent:/usr/share/nmap/scripts$ nmap --script ftp-brute -p21 10.0.2.4 --script-args userdb-users.txt,passdb=password.txt
Starting Nmap 7.60 (https://nmap.org) at 2023-07-15 16:31 EDT
Nmap scan report for 10.0.2.4
Host is up (0.00083s latency).
PORT STATE SERVICE
21/tcp open ftp
|_ftp-brute: Invalid passwords iterator
Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
ustudent@ubu-ustudent:/usr/share/nmap/scripts$
Preview


Chrome File Edit View History Bookmarks Profiles Tab Window Help
win10udstudent [Running]
Zenmap
Scan Tools Profile Help
Target: 10.0.2.5
Profile:
Scan
Cancel
Command: nmap -p 21 --script ftp-brute --script-args userdb=users.txt,passdb=passwords.txt 10.0.2.5
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Details
Starting Nmap 7.94 (https://nmap.org) at 2023-07-15 22:29 Pacific Daylight Time
Nmap scan report for 10.0.2.5
Host is up (0.0010s latency).
PORT STATE SERVICE
21/tcp open ftp
|_ftp-brute: Invalid usernames iterator: Error parsing username list: users.txt: No such file or directory
MAC Address: 08:00:27:42:2E:A0 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.38 seconds
Filter Hosts
Type here to search
10:30 PM
7/15/2023
Page 40 of 40
1152 words
English (South Africa)
Focus
125%

Final Recommendation:

Before these systems would be compliant with our current security policies and added, we must resolve all the listed issues and retest to make sure it is safe enough to do so.