PROJECT REPORT

On

Open Source Tools for Network Security, System Software Security, and Physical Security analysis of a System

Submitted by

Godithi Sri Lakshmi Prasanna
Registration No: 11903359
Roll.no: 41
Section: KE014
Program Name: CSE

Under the Guidance of

Nahida Nazir

School of Computer Science & Engineering
Lovely Professional University, Phagwara

(January-April, 2023)

Tables of Contents

S.No.	Title	Page.No
1	Introduction	1
2	System Description	4
3	Analysis Report	8
4	Conclusion	16
5	Bibliography	16

1. Introduction

In this project, I have performed the analysis and generated the report on Network Security, System Software Security, and Physical Security analysis of a System using open-source softwares.

I have used Four Open Source Softwares

1. Wireshark
2. Nmap
3. Lynis
4. WinAudit

Network Security protects your network and data from breaches, intrusions, and other threats. Network security is the set of measures and practices designed to protect computer networks from unauthorized access, misuse, modification, or destruction. Network security aims to ensure the confidentiality, integrity, and availability of network resources, including hardware, software, and data. Network Security involves access control, virus and antivirus software, application security, network analytics, types of network-related security (endpoint, web, wireless), firewalls, VPN encryption, and more. Network Security is vital in protecting client data and information, keeping shared data secure, and ensuring reliable access and network performance as well as protection from cyber threats.

System software security refers to the set of measures and practices designed to secure the system software that is installed on a computer or other digital device. System software includes the operating system, drivers, firmware, and other software that runs at the system level and provides a foundation for running applications. System software security is important because if the system software is compromised, it can allow an attacker to gain unauthorized access to the computer, steal data, or cause other malicious actions. The goal of system software security is to safeguard the computer system against unauthorized access, data breaches, and other malicious attacks. To achieve this, various security measures are implemented, such as regular software updates, strong authentication and access control mechanisms, encryption, antivirus and anti-malware software, firewalls, and backup and recovery mechanisms. These measures are designed to prevent, detect, and respond to security threats and to protect the integrity, confidentiality, and availability of system software and data.

Physical security of a system refers to the measures and controls put in place to protect the physical assets of a computer system, such as the hardware, facilities, and infrastructure, from unauthorized access, theft, damage, or other physical threats. Physical security of a system is an important aspect of overall security, and it refers to the measures and controls put in place to protect the physical assets of a computer system. These physical assets include the hardware, facilities, and infrastructure that support the system's operations. Physical security measures typically include access control mechanisms, environmental controls, power protection, fire suppression, and physical location. The physical security of a system is critical because a breach of physical security can result in loss of data, damage to hardware components, and disruption of business operations. Therefore, it is important to implement appropriate physical security measures based on the risk profile of the computer system and its physical assets. This includes conducting a risk assessment to identify potential threats and vulnerabilities, implementing appropriate access control mechanisms, monitoring environmental conditions, and ensuring that adequate fire suppression and power protection measures are in place. Overall, a strong physical security posture can help organizations protect their assets and ensure business continuity.

1.1 Objective of the Project

The main objective of this project is to analyze and generate a report on Network Security, System Software Security, and Physical Security analysis of a System using open-source software. The ultimate objective of this project is to improve the security of the system by identifying and addressing security vulnerabilities. This will help to reduce the risk of security breaches and protect the confidentiality, integrity, and availability of the system and its data.

1.2 Description of the Project

In this project, I have used four open-source software to generate the report on the Network Security, Software Security, and Physical Security analysis of my system.

1. Wireshark
2. Nmap
3. Lynis
4. WinAudit

1. Wireshark

Wireshark is a powerful network protocol analyzer tool that can be used for network security analysis. It allows network administrators and security professionals to capture and analyze network traffic in real time or from a saved file. With Wireshark, they can examine network packets to identify network problems, investigate security incidents, and analyze network performance. Wireshark can be used for network forensics, which involves analyzing network traffic to identify the source of a security incident or network attack. Network forensics can help organizations to understand the scope and impact of a security incident, and to take appropriate measures to prevent similar incidents in the future.

2. Nmap

Nmap (Network Mapper) is a free and open-source network exploration and security auditing tool that is widely used by network administrators and security professionals. Nmap is a tool that can be used for network security purposes, specifically to identify potential vulnerabilities in a network. By using Nmap to perform network scans, network administrators can identify open ports, services, and potential security weaknesses that could be exploited by attackers. Nmap uses various techniques, such as port scanning and OS detection, to identify hosts and services on a network, as well as potential security vulnerabilities.

3. Lynis

Lynis is a security auditing tool that can be used to improve system software security by identifying potential vulnerabilities and providing recommendations for hardening the system. One of the key areas of focus for Lynis is system software security. It performs a wide range of tests and audits to identify potential vulnerabilities in the system software, including file permissions, configuration settings, and software versions. By identifying potential vulnerabilities in the system software, Lynis can help system administrators to take corrective action to improve system security. This may involve updating software versions, modifying configuration settings, or changing file permissions to reduce the attack surface of the system.

4. WinAudit

WinAudit can be used to improve both system software security and physical security by providing detailed information about the system components and configuration. By identifying these potential vulnerabilities, system administrators can take corrective action to improve the security of the system software. WinAudit can be used to track and manage hardware components, which can be important for physical security.

1.3 Scope of the project

The scope of this project would be to use these open-source software tools to assess the network security, system software security, and physical security of the system. The project would involve installing and configuring the software tools, performing scans and audits, and generating reports. The reports would be used to identify security vulnerabilities and provide recommendations for improving the security of the system. The project could be expanded to include remediation of the identified vulnerabilities, such as applying software patches or implementing security controls. Overall, the scope of the project would be to assess the security of the system from multiple angles and generate comprehensive reports that identify potential vulnerabilities and provide recommendations for improving security. The project would require expertise in network security, system software security, and physical security, as well as proficiency in using open-source security tools to assess and analyze the system.

2. System Description

In this section, I am going to give a brief description of the open-source softwares that I have used for analyzing Network Security, Software Security, and Physical Security of my system.

2.1 Target system description

I have used four Open source softwares to analyze the Network Security, Software Security, and Physical Security of my system.

1. Wireshark
2. Nmap
3. Lynis
4. WinAudit

2.1.1 Wireshark

Wireshark is a widely-used open-source network packet analyzer tool that can help improve the network security of a system. It is designed to capture and analyze network traffic in real-time, allowing security professionals to monitor network activity and identify potential security threats. Wireshark supports a variety of network protocols, including TCP/IP, HTTP, DNS, and FTP, among others. With Wireshark, network administrators and security professionals can examine network packets to identify network problems, investigate security incidents, and analyze network performance. It enables them to see the details of each packet, such as its source and destination addresses, protocol type, packet length, and more. They can also filter packets based on various criteria, such as protocol type, IP address, port number, and more.

Features:

1. Packet capture and analysis: Wireshark can capture packets from a network interface and provide detailed information about each packet, including the source and destination addresses, protocols used, and data payloads. This information can be used to identify security threats and vulnerabilities in the network.
2. Protocol decoding: Wireshark supports a wide range of network protocols and can decode each packet to provide a detailed view of the protocol in use. This can help security professionals to identify anomalies and inconsistencies in network traffic that may indicate a security breach.
3. Filters and search: Wireshark provides powerful filtering and search capabilities that allow security professionals to quickly identify relevant packets and network traffic. Filters can be based on specific protocols, addresses, and other criteria, while search capabilities allow for more complex queries.
4. Real-time analysis: Wireshark can be used to monitor network traffic in real time, providing instant feedback on network activity and potential security threats. This can help security professionals to respond quickly to potential threats and prevent security breaches.
5. Customization: Wireshark is highly customizable and can be extended with plugins and scripts to provide additional functionality. This makes it a versatile tool that can be adapted to meet the specific needs of a security professional.

2.1.2 Nmap

Nmap is a free and open-source network exploration and security auditing tool that is widely used by network administrators and security professionals. Nmap uses various techniques, such as port scanning and OS detection, to identify hosts and services on a network, as well as potential security vulnerabilities. One of the primary uses of Nmap is to identify open ports on a network, which can help network administrators to identify potential security vulnerabilities. For example, if a network device has an open port for Telnet, which is an unencrypted protocol, it may be vulnerable to a bruteforce attack. By identifying these vulnerabilities, network administrators can take steps to mitigate them and improve network security. Nmap is a powerful network exploration and security auditing tool that provides network administrators and security professionals with a range of features to identify and manage network security risks.

Features:

1. Host discovery: Nmap can be used to identify hosts that are connected to a network. It can scan the entire network to find available hosts and generate a report on the same.
2. Port scanning: Nmap can be used to scan open ports on the network. It can detect the services that are running on each port and provide information about the operating system that is being used.
3. Service and version detection: Nmap can detect the services and versions running on each host that is discovered on the network. This information can be used to identify vulnerabilities and potential security risks.
4. OS detection: Nmap can be used to identify the operating system that is running on each host. This information can be used to identify potential security risks based on known vulnerabilities associated with that particular operating system.
5. Scripting engine: Nmap's scripting engine allows users to develop custom scripts to automate security tests, and gather additional information that can be used to assess the security of the network.

2.1.3 Lynis

Lynis is an open-source security auditing tool that can be used for system hardening, vulnerability scanning, and compliance testing. It is designed to identify security weaknesses in Linux and Unix systems and provide recommendations for improving system security. Lynis works by performing a series of security tests and audits to identify potential vulnerabilities in the system. These tests cover a wide range of security areas, including system configuration, file permissions, network settings, and user accounts. One of the key features of Lynis is its ability to provide detailed security reports that can be used by system administrators to prioritize and address security issues. These reports can help system administrators to identify potential security weaknesses and take corrective action to improve system security.

Features:

1. Authentication and Authorization: Lynis can check the system for password policies, default passwords, and insecure authentication mechanisms. It can also identify unauthorized

accounts and groups and check for file and directory permissions.

2. Firewalls and Packet Filters: Lynis can check the system for configured firewalls and packet filters, their rules, and the status of the firewall.
3. File Integrity Monitoring: Lynis can perform file integrity checks by comparing hashes of
4. known good files with those of files on the system.
5. Network Services: Lynis can check for open ports and services that may pose a security risk.
6. Operating System Security: Lynis can check for vulnerabilities and misconfigurations in the operating system.
7. Software Security: Lynis can check for vulnerabilities and misconfigurations in installed software, including web servers, databases, and applications.
8. User and Group Management: Lynis can check the system for unauthorized users and groups and ensure that permissions are correctly set.
9. System Hardening: Lynis can check for security best practices, such as disabling unnecessary services and protocols, securing network services, and removing insecure software.

2.1.4 WinAudit

WinAudit is a free and open-source software utility that can be used to collect detailed information about a Windows computer system. It can be used to perform system audits, inventory management, and compliance testing. WinAudit can provide detailed information about installed software and identify potential vulnerabilities, such as outdated software versions or missing security patches. By identifying these potential vulnerabilities, system administrators can take corrective action to improve the security of the system software. WinAudit can be used to track and manage hardware components, which can be important for physical security.

Features:

1. Hardware Inventory: WinAudit can inventory the hardware components of a Windows-based system, such as the processor, RAM, hard drive, and other peripherals.
2. Software Inventory: WinAudit can inventory the software applications installed on a Windows-based system.
3. Patch Management: WinAudit can identify missing security patches and updates for the Windows operating system and installed software applications.
4. User Account Management: WinAudit can audit and report on user accounts configured on a Windows-based system.
5. Physical Inventory: WinAudit can also inventory physical components of a system, such as

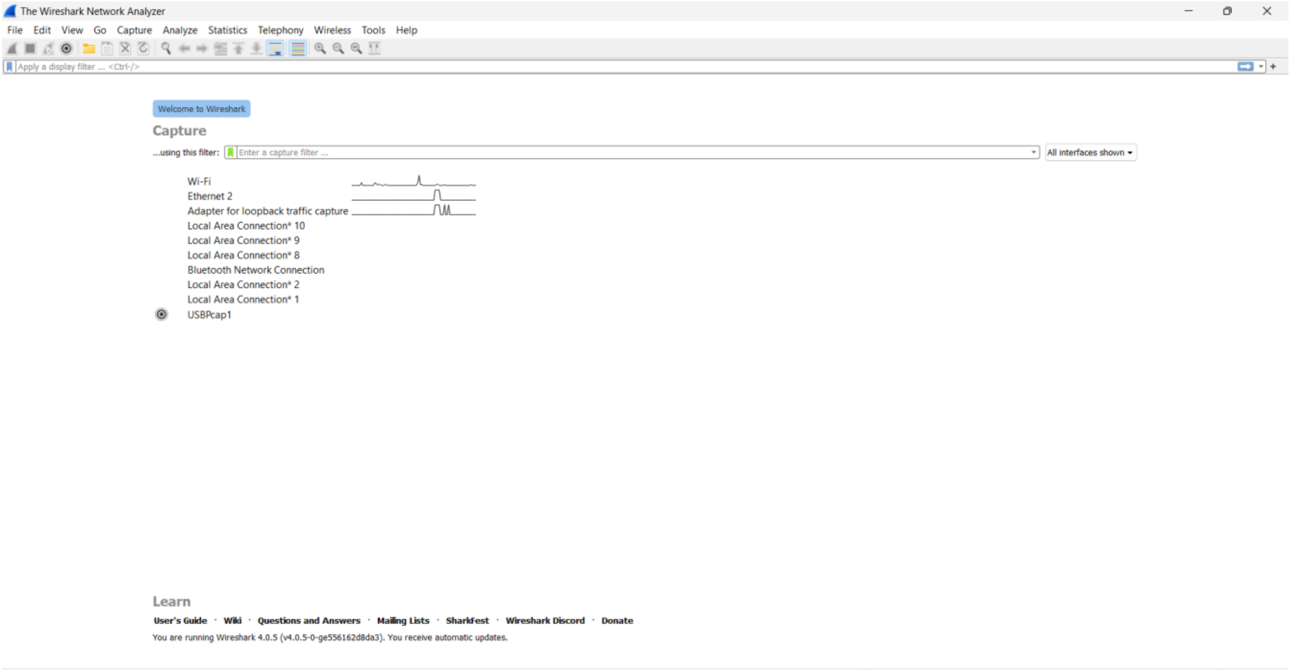
6. monitors, keyboards, and mice.
7. Reporting: WinAudit can generate customizable reports in various formats, including CSV, HTML, and PDF.
8. Command-Line Interface: WinAudit also has a command-line interface that can be used to automate system auditing tasks.
9. Remote Auditing: WinAudit can perform audits on remote systems over a network.
10. Portable: WinAudit can be run from a USB drive or other portable storage device, making it easy to use on multiple systems.

3. Analysis Report

3.1 System snapshots and full analysis report

3.1.1 Wireshark

I have used Wireshark to analyze the network traffic of all the networks which are connected to my system.


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Enter a capture filter ...
All interfaces shown

Capture

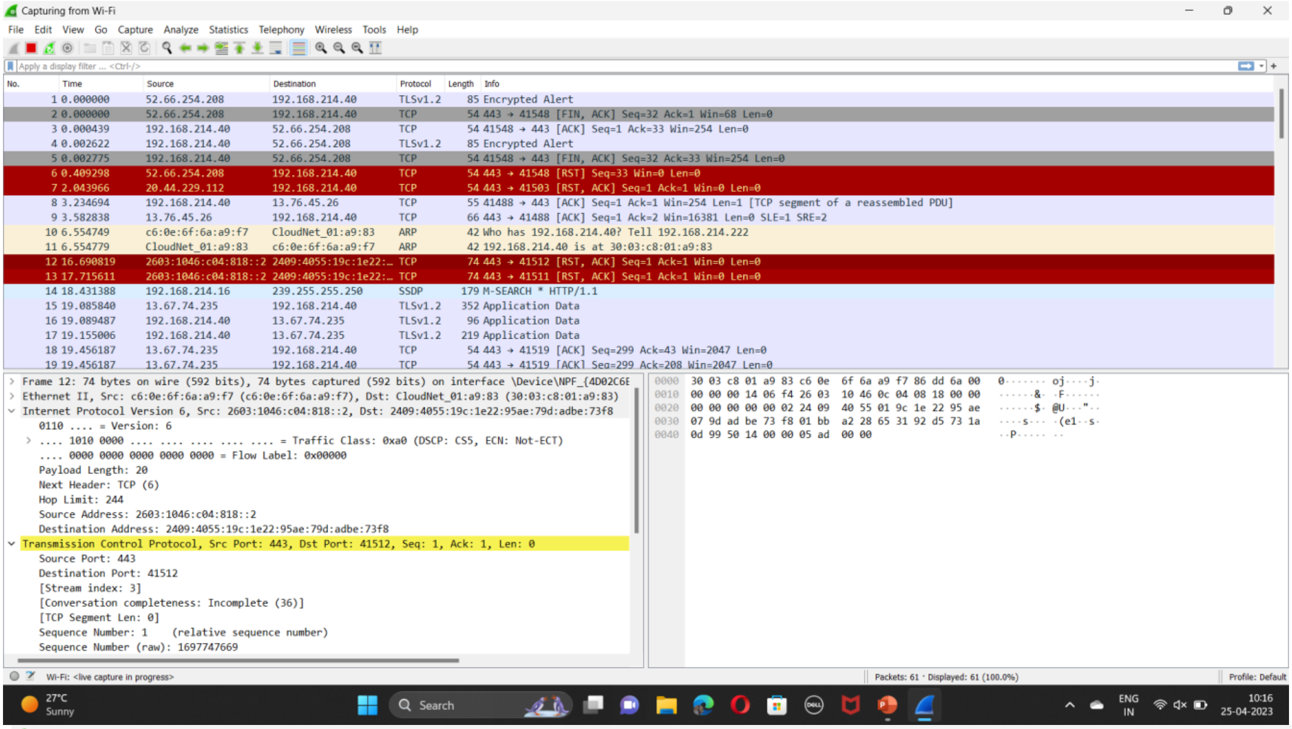
...using this filter:

Wi-Fi
Ethernet 2
Adapter for loopback traffic capture
Local Area Connection* 10
Local Area Connection* 9
Local Area Connection* 8
Bluetooth Network Connection
Local Area Connection* 2
Local Area Connection* 1
USBPcap1

Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

You are running Wireshark 4.0.5 (v4.0.5-0-ge556162d8da3). You receive automatic updates.



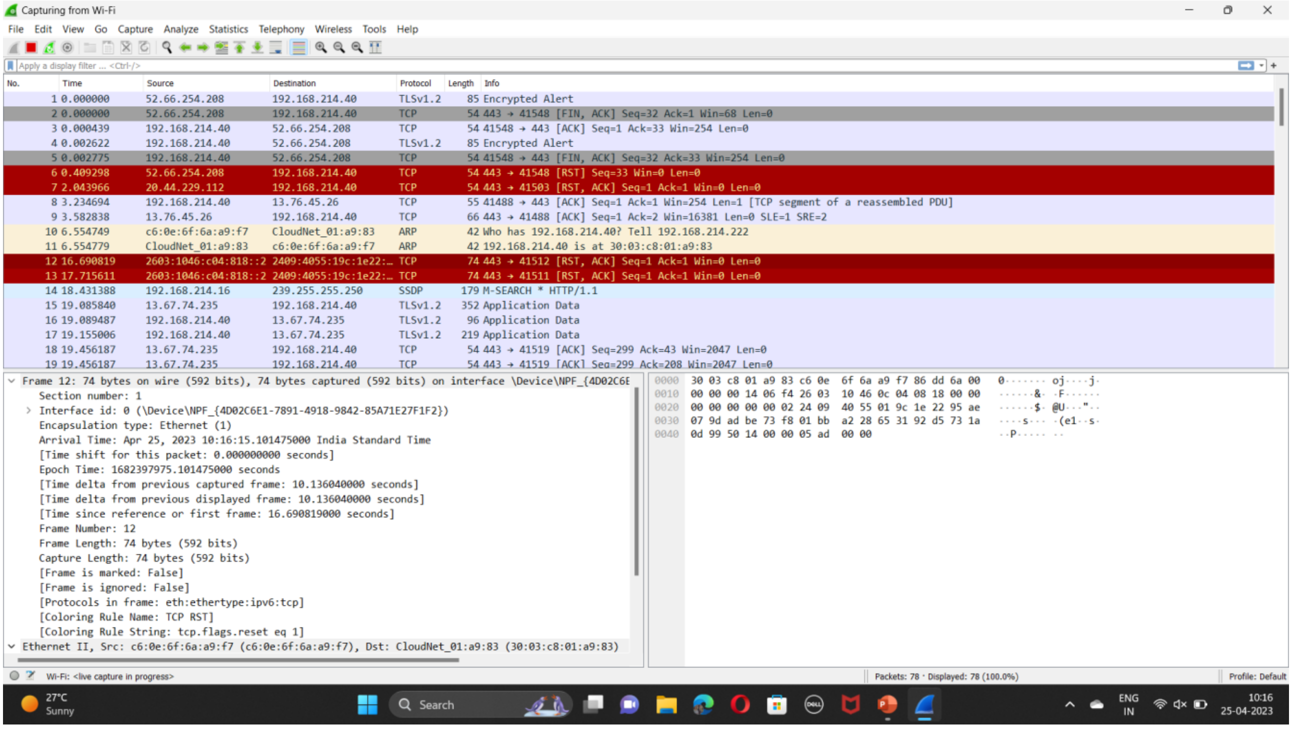
Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time        Source              Destination           Protocol  Length Info
   1 0.000000    52.66.254.208       192.168.214.40        TLSv1.2   85 Encrypted Alert
   2 0.000000    52.66.254.208       192.168.214.40        TCP       54 443 → 41548 [FIN, ACK] Seq=32 Ack=1 Win=68 Len=0
   3 0.000439    192.168.214.40      52.66.254.208         TCP       54 41548 → 443 [ACK] Seq=1 Ack=33 Win=254 Len=0
   4 0.002622    192.168.214.40      52.66.254.208         TLSv1.2   85 Encrypted Alert
   5 0.002775    192.168.214.40      52.66.254.208         TCP       54 41548 → 443 [FIN, ACK] Seq=32 Ack=33 Win=254 Len=0
   6 0.409298    52.66.254.208       192.168.214.40        TCP       54 443 → 41548 [RST] Seq=33 Win=0 Len=0
   7 2.043966    20.44.229.112       192.168.214.40        TCP       54 443 → 41503 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
   8 3.234694    192.168.214.40      13.76.45.26           TCP       55 41488 → 443 [ACK] Seq=1 Ack=1 Win=254 Len=1 [TCP segment of a reassembled PDU]
   9 3.582838    13.76.45.26         192.168.214.40        TCP       66 443 → 41488 [ACK] Seq=1 Ack=2 Win=16381 Len=0 SLE=1 SRE=2
  10 6.554749    c6:0e:6f:6a:a9:f7   CloudNet_01:a9:83     ARP       42 Who has 192.168.214.40? Tell 192.168.214.222
  11 6.554779    CloudNet_01:a9:83   c6:0e:6f:6a:a9:f7     ARP       42 192.168.214.40 is at 30:03:c8:01:a9:83
  12 16.690819   2603:1046:c04:818::2 2409:4055:19c:1e22:… TCP       74 443 → 41512 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  13 17.715611   2603:1046:c04:818::2 2409:4055:19c:1e22:… TCP       74 443 → 41511 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  14 18.431388   192.168.214.16      239.255.255.250       SSDP      179 M-SEARCH * HTTP/1.1
  15 19.085840   13.67.74.235        192.168.214.40        TLSv1.2   352 Application Data
  16 19.089487   192.168.214.40      13.67.74.235          TLSv1.2   96 Application Data
  17 19.155006   192.168.214.40      13.67.74.235          TLSv1.2   219 Application Data
  18 19.456187   13.67.74.235        192.168.214.40        TCP       54 443 → 41519 [ACK] Seq=299 Ack=43 Win=2047 Len=0
  19 19.456187   13.67.74.235        192.168.214.40        TCP       54 443 → 41519 [ACK] Seq=299 Ack=208 Win=2047 Len=0
```

```
> Frame 12: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{4D02C6E
> Ethernet II, Src: c6:0e:6f:6a:a9:f7 (c6:0e:6f:6a:a9:f7), Dst: CloudNet_01:a9:83 (30:03:c8:01:a9:83)
v Internet Protocol Version 6, Src: 2603:1046:c04:818::2, Dst: 2409:4055:19c:1e22:95ae:79d:adbe:73f8
    0110 .... = Version: 6
  > .... 1010 0000 .... .... .... .... .... = Traffic Class: 0xa0 (DSCP: CS5, ECN: Not-ECT)
    .... 0000 0000 0000 0000 0000 = Flow Label: 0x00000
    Payload Length: 20
    Next Header: TCP (6)
    Hop Limit: 244
    Source Address: 2603:1046:c04:818::2
    Destination Address: 2409:4055:19c:1e22:95ae:79d:adbe:73f8
v Transmission Control Protocol, Src Port: 443, Dst Port: 41512, Seq: 1, Ack: 1, Len: 0
    Source Port: 443
    Destination Port: 41512
    [Stream index: 3]
    [Conversation completeness: Incomplete (36)]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 1697747669
```

```
0000  30 03 c8 01 a9 83 c6 0e  6f 6a a9 f7 86 dd 6a 00   0······· oj····j·
0010  00 00 00 14 06 f4 26 03  10 46 0c 04 08 18 00 00   ······&· ·F······
0020  00 00 00 00 00 02 24 09  40 55 01 9c 1e 22 95 ae   ······$· @U···"··
0030  07 9d ad be 73 f8 01 bb  a2 28 65 31 92 d5 73 1a   ····s··· ·(e1··s·
0040  0d 99 50 14 00 00 05 ad  00 00                     ··P····· ··
```

Wi-Fi: <live capture in progress>
Packets: 61 · Displayed: 61 (100.0%)
Profile: Default
27°C
Sunny
Search
ENG
IN
10:16
25-04-2023



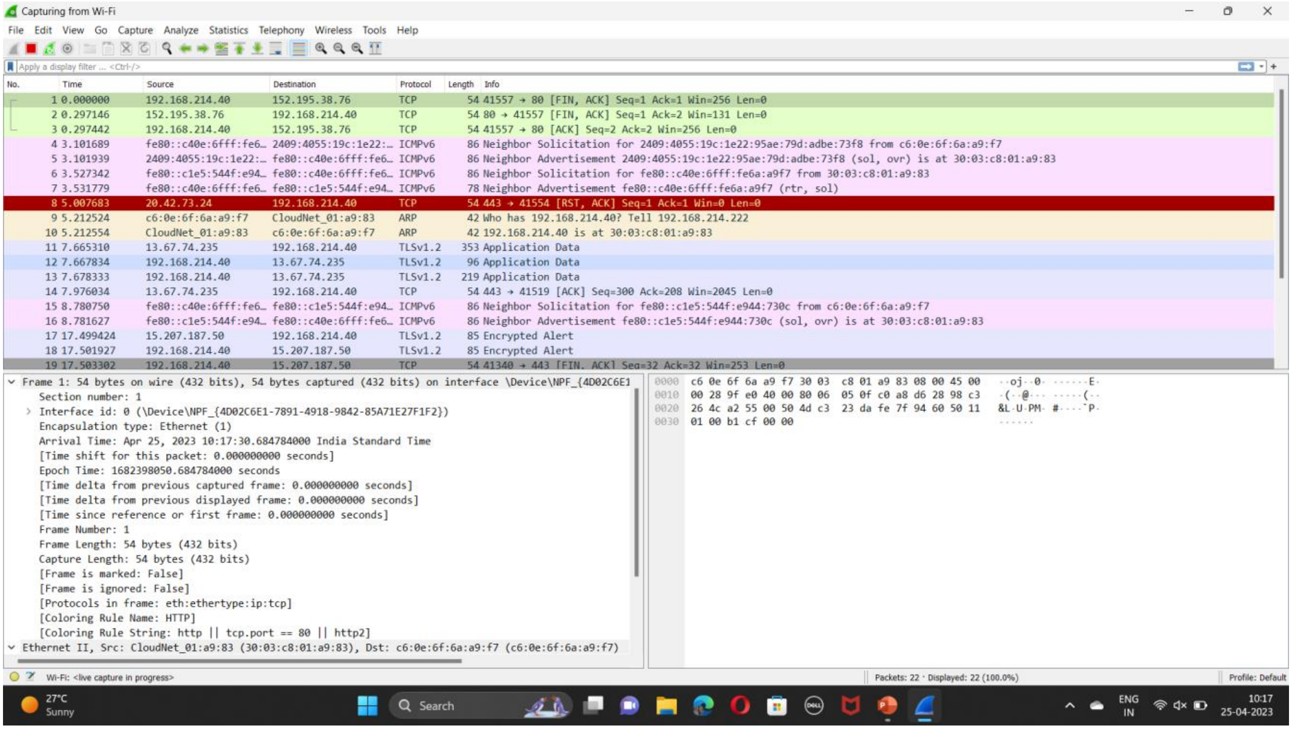
Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time        Source              Destination           Protocol  Length Info
   1 0.000000    52.66.254.208       192.168.214.40        TLSv1.2   85 Encrypted Alert
   2 0.000000    52.66.254.208       192.168.214.40        TCP       54 443 → 41548 [FIN, ACK] Seq=32 Ack=1 Win=68 Len=0
   3 0.000439    192.168.214.40      52.66.254.208         TCP       54 41548 → 443 [ACK] Seq=1 Ack=33 Win=254 Len=0
   4 0.002622    192.168.214.40      52.66.254.208         TLSv1.2   85 Encrypted Alert
   5 0.002775    192.168.214.40      52.66.254.208         TCP       54 41548 → 443 [FIN, ACK] Seq=32 Ack=33 Win=254 Len=0
   6 0.409298    52.66.254.208       192.168.214.40        TCP       54 443 → 41548 [RST] Seq=33 Win=0 Len=0
   7 2.043966    20.44.229.112       192.168.214.40        TCP       54 443 → 41503 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
   8 3.234694    192.168.214.40      13.76.45.26           TCP       55 41488 → 443 [ACK] Seq=1 Ack=1 Win=254 Len=1 [TCP segment of a reassembled PDU]
   9 3.582838    13.76.45.26         192.168.214.40        TCP       66 443 → 41488 [ACK] Seq=1 Ack=2 Win=16381 Len=0 SLE=1 SRE=2
  10 6.554749    c6:0e:6f:6a:a9:f7   CloudNet_01:a9:83     ARP       42 Who has 192.168.214.40? Tell 192.168.214.222
  11 6.554779    CloudNet_01:a9:83   c6:0e:6f:6a:a9:f7     ARP       42 192.168.214.40 is at 30:03:c8:01:a9:83
  12 16.690819   2603:1046:c04:818::2 2409:4055:19c:1e22:… TCP       74 443 → 41512 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  13 17.715611   2603:1046:c04:818::2 2409:4055:19c:1e22:… TCP       74 443 → 41511 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  14 18.431388   192.168.214.16      239.255.255.250       SSDP      179 M-SEARCH * HTTP/1.1
  15 19.085840   13.67.74.235        192.168.214.40        TLSv1.2   352 Application Data
  16 19.089487   192.168.214.40      13.67.74.235          TLSv1.2   96 Application Data
  17 19.155006   192.168.214.40      13.67.74.235          TLSv1.2   219 Application Data
  18 19.456187   13.67.74.235        192.168.214.40        TCP       54 443 → 41519 [ACK] Seq=299 Ack=43 Win=2047 Len=0
  19 19.456187   13.67.74.235        192.168.214.40        TCP       54 443 → 41519 [ACK] Seq=299 Ack=208 Win=2047 Len=0
```

```
v Frame 12: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{4D02C6E
    Section number: 1
  > Interface id: 0 (\Device\NPF_{4D02C6E1-7891-4918-9842-85A71E27F1F2})
    Encapsulation type: Ethernet (1)
    Arrival Time: Apr 25, 2023 10:16:15.101475000 India Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1682397975.101475000 seconds
    [Time delta from previous captured frame: 10.136040000 seconds]
    [Time delta from previous displayed frame: 10.136040000 seconds]
    [Time since reference or first frame: 16.690819000 seconds]
    Frame Number: 12
    Frame Length: 74 bytes (592 bits)
    Capture Length: 74 bytes (592 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ipv6:tcp]
    [Coloring Rule Name: TCP RST]
    [Coloring Rule String: tcp.flags.reset eq 1]
v Ethernet II, Src: c6:0e:6f:6a:a9:f7 (c6:0e:6f:6a:a9:f7), Dst: CloudNet_01:a9:83 (30:03:c8:01:a9:83)
```

```
0000  30 03 c8 01 a9 83 c6 0e  6f 6a a9 f7 86 dd 6a 00   0······· oj····j·
0010  00 00 00 14 06 f4 26 03  10 46 0c 04 08 18 00 00   ······&· ·F······
0020  00 00 00 00 00 02 24 09  40 55 01 9c 1e 22 95 ae   ······$· @U···"··
0030  07 9d ad be 73 f8 01 bb  a2 28 65 31 92 d5 73 1a   ····s··· ·(e1··s·
0040  0d 99 50 14 00 00 05 ad  00 00                     ··P····· ··
```

Wi-Fi: <live capture in progress>
Packets: 78 · Displayed: 78 (100.0%)
Profile: Default
27°C
Sunny
Search
ENG
IN
10:16
25-04-2023


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Wi-Fi: <live capture in progress>
Packets: 22 · Displayed: 22 (100.0%)
Profile: Default
27°C
Sunny
Search
ENG
IN
10:17
25-04-2023

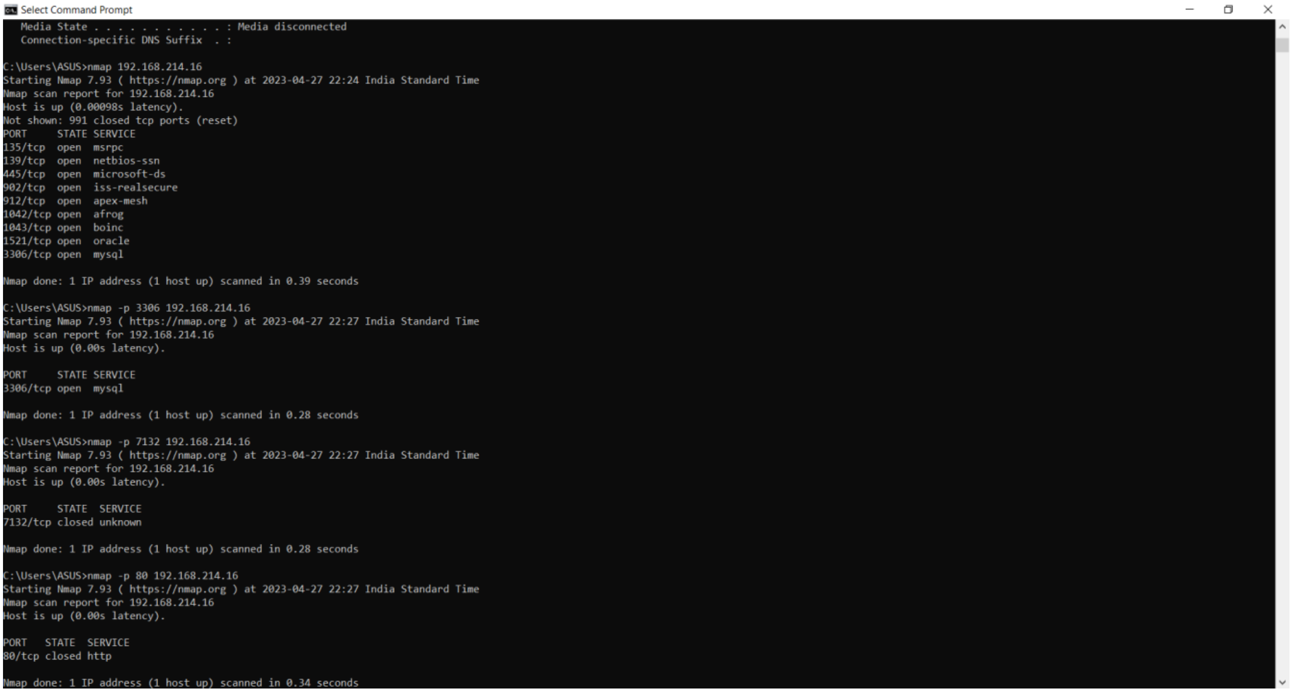
```
No.   Time       Source              Destination         Protocol  Length Info
    1 0.000000   192.168.214.40      152.195.38.76       TCP        54 41557 → 80 [FIN, ACK] Seq=1 Ack=1 Win=256 Len=0
    2 0.297146   152.195.38.76       192.168.214.40      TCP        54 80 → 41557 [FIN, ACK] Seq=1 Ack=2 Win=131 Len=0
    3 0.297442   192.168.214.40      152.195.38.76       TCP        54 41557 → 80 [ACK] Seq=2 Ack=2 Win=256 Len=0
    4 3.101689   fe80::c40e:6fff:fe6… 2409:4055:19c:1e22:… ICMPv6   86 Neighbor Solicitation for 2409:4055:19c:1e22:95ae:79d:adbe:73f8 from c6:0e:6f:6a:a9:f7
    5 3.101939   2409:4055:19c:1e22:… fe80::c40e:6fff:fe6… ICMPv6   86 Neighbor Advertisement 2409:4055:19c:1e22:95ae:79d:adbe:73f8 (sol, ovr) is at 30:03:c8:01:a9:83
    6 3.527342   fe80::c1e5:544f:e94… fe80::c40e:6fff:fe6… ICMPv6   86 Neighbor Solicitation for fe80::c40e:6fff:fe6a:a9f7 from 30:03:c8:01:a9:83
    7 3.531779   fe80::c40e:6fff:fe6… fe80::c1e5:544f:e94… ICMPv6   78 Neighbor Advertisement fe80::c40e:6fff:fe6a:a9f7 (rtr, sol)
    8 5.007683   20.42.73.24         192.168.214.40      TCP        54 443 → 41554 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
    9 5.212524   c6:0e:6f:6a:a9:f7   CloudNet_01:a9:83   ARP        42 Who has 192.168.214.40? Tell 192.168.214.222
   10 5.212554   CloudNet_01:a9:83   c6:0e:6f:6a:a9:f7   ARP        42 192.168.214.40 is at 30:03:c8:01:a9:83
   11 7.665310   13.67.74.235        192.168.214.40      TLSv1.2   353 Application Data
   12 7.667834   192.168.214.40      13.67.74.235        TLSv1.2    96 Application Data
   13 7.678333   192.168.214.40      13.67.74.235        TLSv1.2   219 Application Data
   14 7.976034   13.67.74.235        192.168.214.40      TCP        54 443 → 41519 [ACK] Seq=300 Ack=208 Win=2045 Len=0
   15 8.780750   fe80::c40e:6fff:fe6… fe80::c1e5:544f:e94… ICMPv6   86 Neighbor Solicitation for fe80::c1e5:544f:e944:730c from c6:0e:6f:6a:a9:f7
   16 8.781627   fe80::c1e5:544f:e94… fe80::c40e:6fff:fe6… ICMPv6   86 Neighbor Advertisement fe80::c1e5:544f:e944:730c (sol, ovr) is at 30:03:c8:01:a9:83
   17 17.499424  15.207.187.50       192.168.214.40      TLSv1.2    85 Encrypted Alert
   18 17.501927  192.168.214.40      15.207.187.50       TLSv1.2    85 Encrypted Alert
   19 17.503302  192.168.214.40      15.207.187.50       TCP        54 41340 → 443 [FIN, ACK] Seq=32 Ack=32 Win=253 Len=0
```

```
v Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{4D02C6E1
    Section number: 1
  > Interface id: 0 (\Device\NPF_{4D02C6E1-7891-4918-9842-85A71E27F1F2})
    Encapsulation type: Ethernet (1)
    Arrival Time: Apr 25, 2023 10:17:30.684784000 India Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1682398050.684784000 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 54 bytes (432 bits)
    Capture Length: 54 bytes (432 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
v Ethernet II, Src: CloudNet_01:a9:83 (30:03:c8:01:a9:83), Dst: c6:0e:6f:6a:a9:f7 (c6:0e:6f:6a:a9:f7)
```

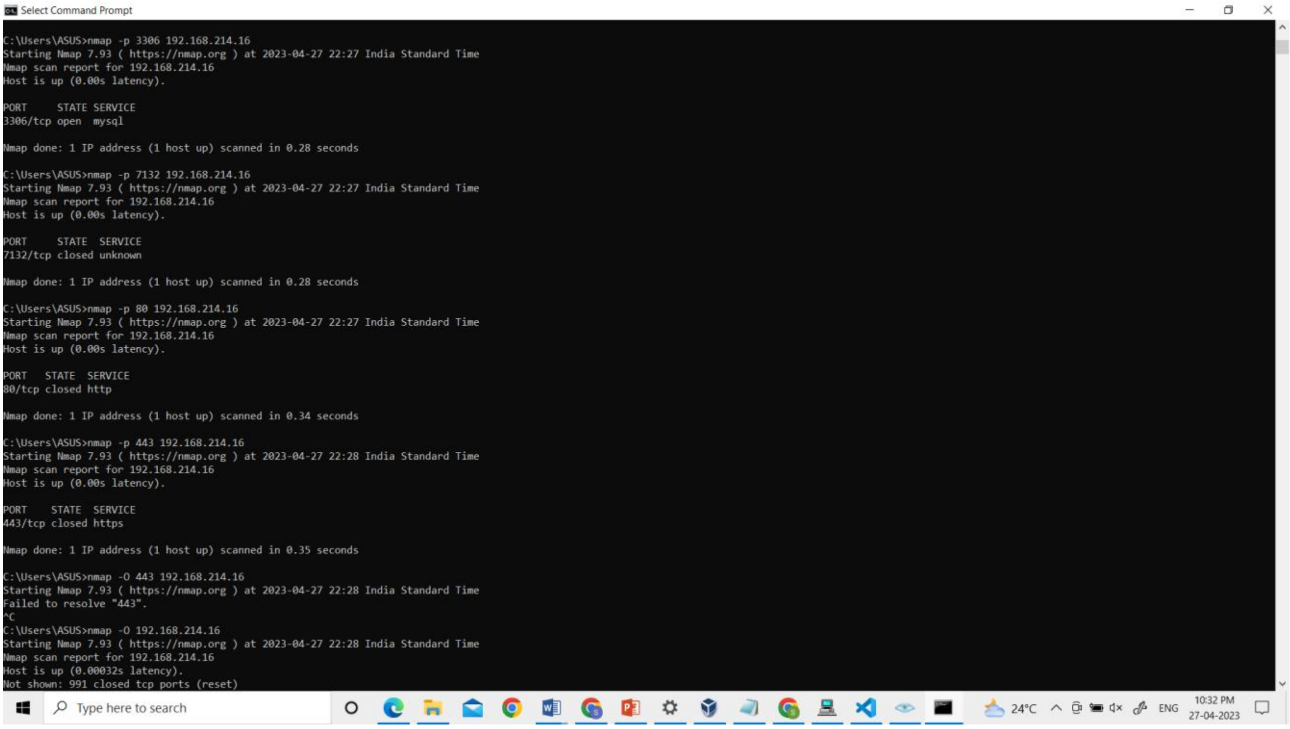
```
0000  c6 0e 6f 6a a9 f7 30 03  c8 01 a9 83 08 00 45 00   ··oj··0· ······E·
0010  00 28 9f e0 40 00 80 06  05 0f c0 a8 d6 28 98 c3   ·(··@··· ·····(··
0020  26 4c a2 55 00 50 4d c3  23 da fe 7f 94 60 50 11   &L·U·PM· #····`P·
0030  01 00 b1 cf 00 00                                  ······
```

3.1.2 Nmap

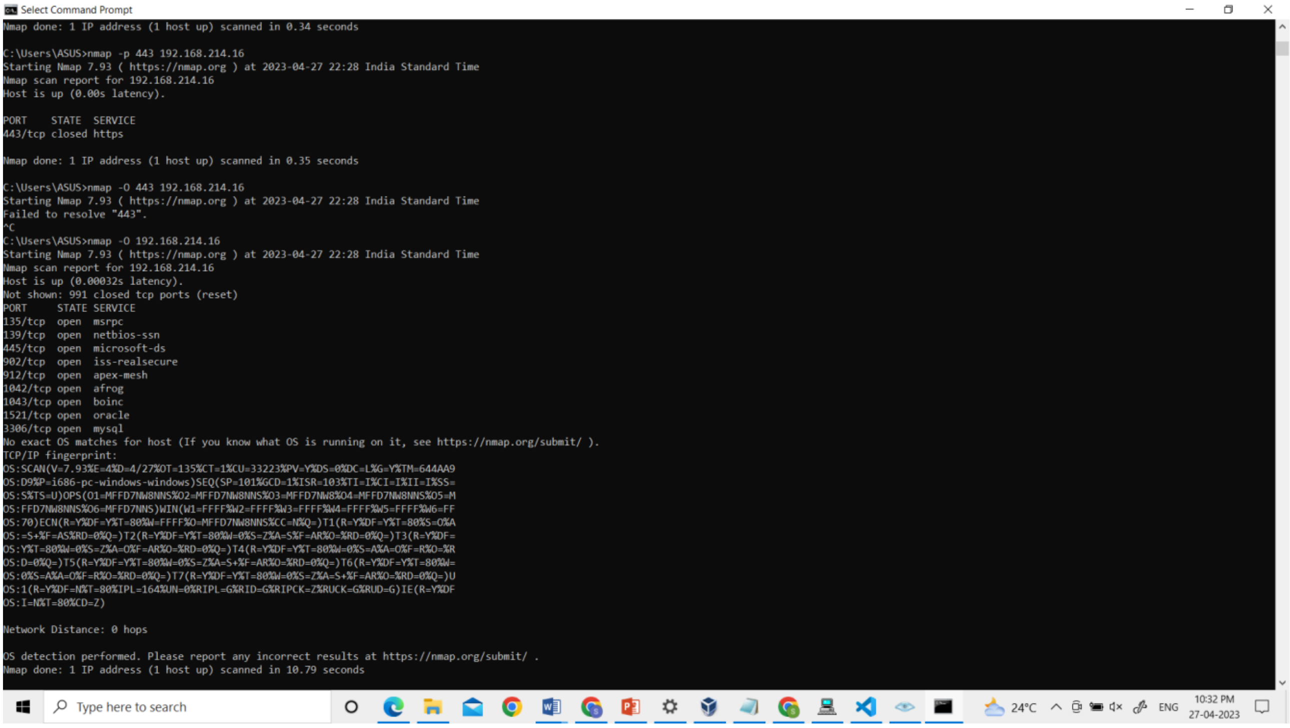
I have used Nmap for analyzing the System Software Security of my system such as scanning the ports, ip for checking the vulnerabilities of my system.



```
   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\ASUS>nmap 192.168.214.16
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-27 22:24 India Standard Time
Nmap scan report for 192.168.214.16
Host is up (0.00098s latency).
Not shown: 991 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
1042/tcp open  afrog
1043/tcp open  boinc
1521/tcp open  oracle
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds

C:\Users\ASUS>nmap -p 3306 192.168.214.16
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-27 22:27 India Standard Time
Nmap scan report for 192.168.214.16
Host is up (0.00s latency).

PORT     STATE SERVICE
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds

C:\Users\ASUS>nmap -p 7132 192.168.214.16
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-27 22:27 India Standard Time
Nmap scan report for 192.168.214.16
Host is up (0.00s latency).

PORT     STATE  SERVICE
7132/tcp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds

C:\Users\ASUS>nmap -p 80 192.168.214.16
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-27 22:27 India Standard Time
Nmap scan report for 192.168.214.16
Host is up (0.00s latency).

PORT   STATE  SERVICE
80/tcp closed http

Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds
```



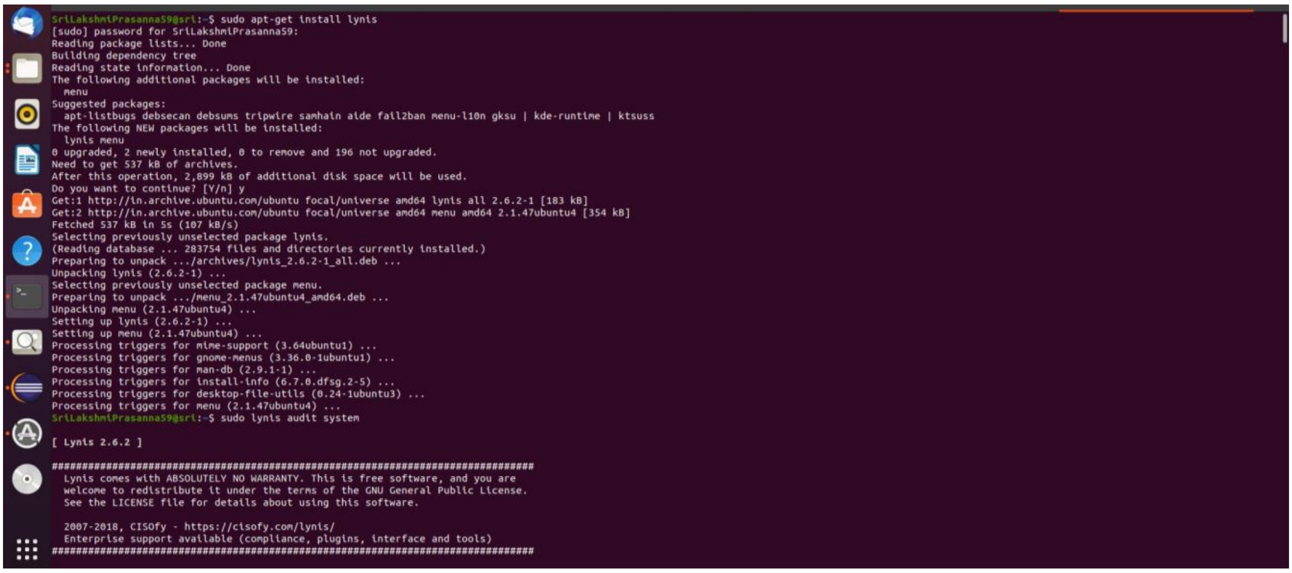
```
C:\Users\ASUS>nmap -p 3306 192.168.214.16
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-27 22:27 India Standard Time
Nmap scan report for 192.168.214.16
Host is up (0.00s latency).

PORT     STATE SERVICE
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds

C:\Users\ASUS>nmap -p 7132 192.168.214.16
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-27 22:27 India Standard Time
Nmap scan report for 192.168.214.16
Host is up (0.00s latency).

PORT     STATE  SERVICE
7132/tcp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds

C:\Users\ASUS>nmap -p 80 192.168.214.16
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-27 22:27 India Standard Time
Nmap scan report for 192.168.214.16
Host is up (0.00s latency).

PORT   STATE  SERVICE
80/tcp closed http

Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds

C:\Users\ASUS>nmap -p 443 192.168.214.16
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-27 22:28 India Standard Time
Nmap scan report for 192.168.214.16
Host is up (0.00s latency).

PORT    STATE  SERVICE
443/tcp closed https

Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds

C:\Users\ASUS>nmap -O 443 192.168.214.16
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-27 22:28 India Standard Time
Failed to resolve "443".
^C
C:\Users\ASUS>nmap -O 192.168.214.16
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-27 22:28 India Standard Time
Nmap scan report for 192.168.214.16
Host is up (0.00032s latency).
Not shown: 991 closed tcp ports (reset)
```



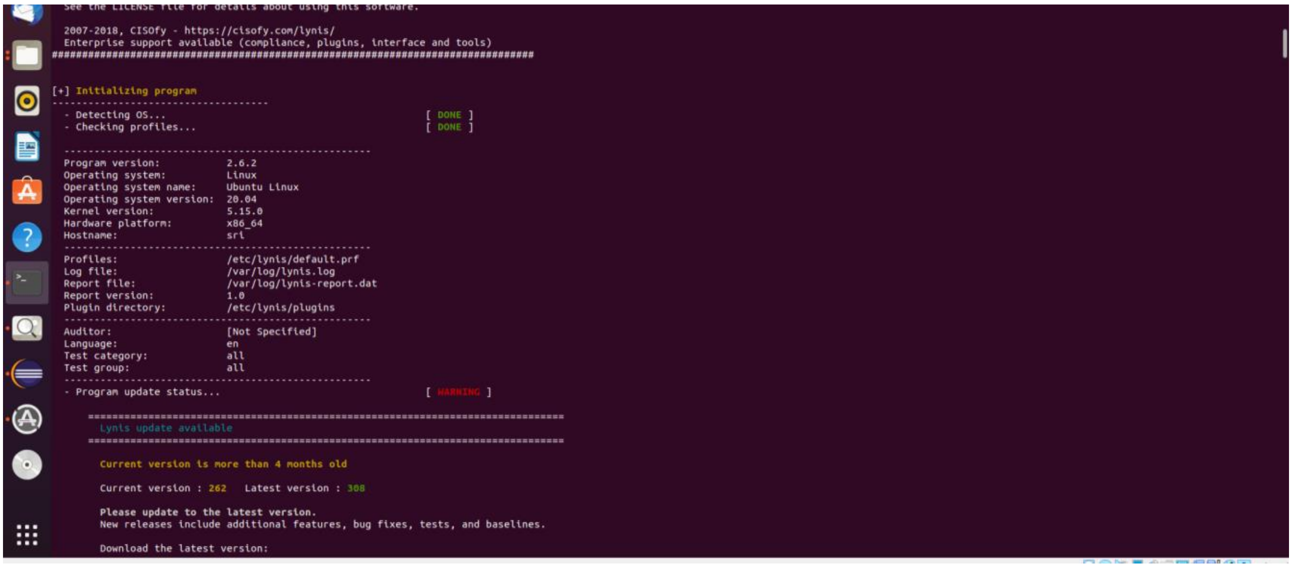
```
Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds

C:\Users\ASUS>nmap -p 443 192.168.214.16
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-27 22:28 India Standard Time
Nmap scan report for 192.168.214.16
Host is up (0.00s latency).

PORT    STATE  SERVICE
443/tcp closed https

Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds

C:\Users\ASUS>nmap -O 443 192.168.214.16
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-27 22:28 India Standard Time
Failed to resolve "443".
^C
C:\Users\ASUS>nmap -O 192.168.214.16
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-27 22:28 India Standard Time
Nmap scan report for 192.168.214.16
Host is up (0.00032s latency).
Not shown: 991 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
1042/tcp open  afrog
1043/tcp open  boinc
1521/tcp open  oracle
3306/tcp open  mysql
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.93%E=4%D=4/27%OT=135%CT=1%CU=33223%PV=Y%DS=0%DC=L%G=Y%TM=644AA9
OS:D9%P=i686-pc-windows-windows)SEQ(SP=101%GCD=1%ISR=103%TI=I%CI=I%II=I%SS=
OS:S%TS=U)OPS(O1=MFFD7NW8NNS%O2=MFFD7NW8NNS%O3=MFFD7NW8%O4=MFFD7NW8NNS%O5=M
OS:FFD7NW8NNS%O6=MFFD7NNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF
OS:70)ECN(R=Y%DF=Y%T=80%W=FFFF%O=MFFD7NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%A
OS:=S+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=
OS:Y%T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%R
OS:D=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=
OS:0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U
OS:1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=Z%RUCK=G%RUD=G)IE(R=Y%DF
OS:I=N%T=80%CD=Z)

Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.79 seconds
```

3.1.3 Lynis

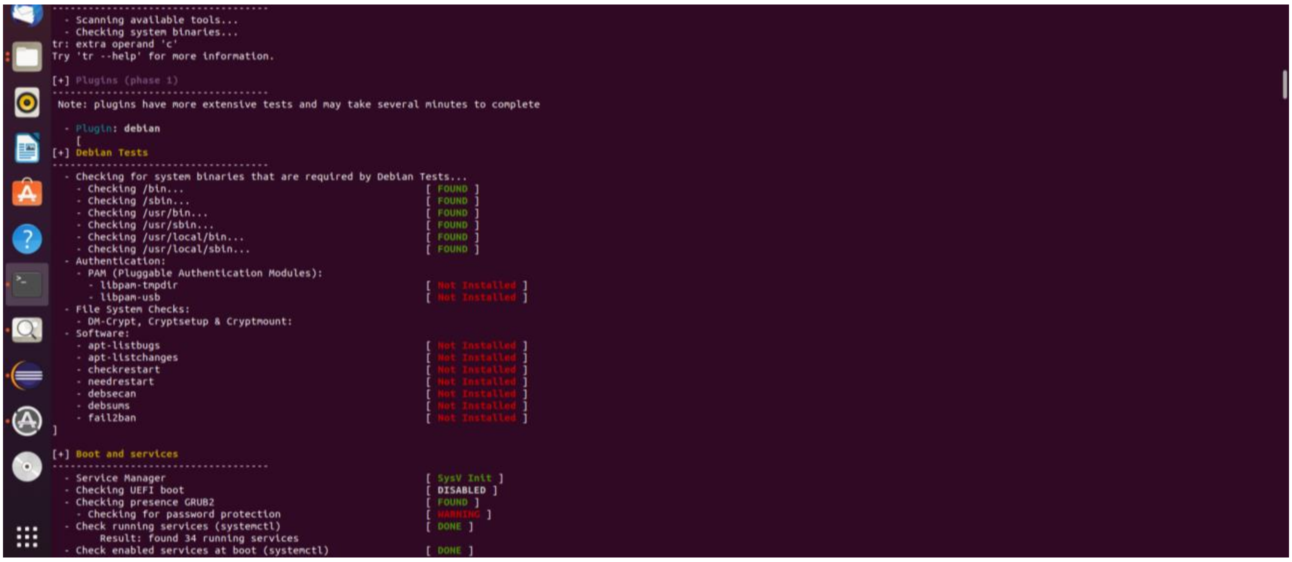
I have used the Lynis for checking System Software security of my system.



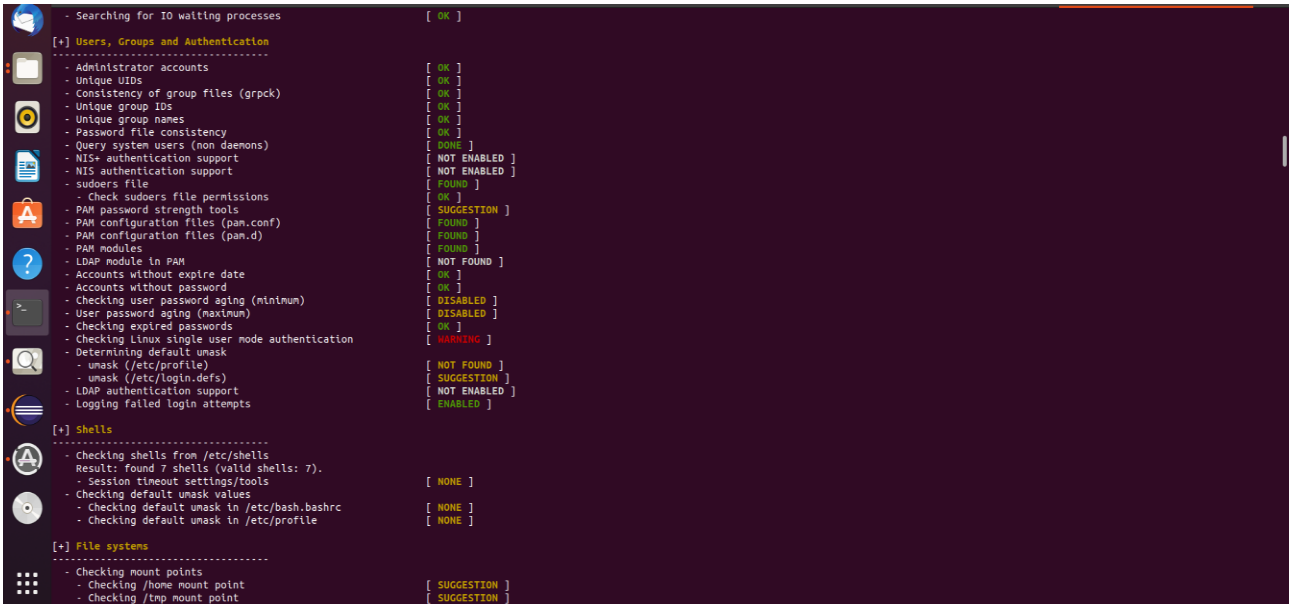
```
SriLakshmiPrasanna59@sri:~$ sudo apt-get install lynis
[sudo] password for SriLakshmiPrasanna59:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  menu
Suggested packages:
  apt-listbugs debsecan debsums tripwire samhain aide fail2ban menu-l10n gksu | kde-runtime | ktsuss
The following NEW packages will be installed:
  lynis menu
0 upgraded, 2 newly installed, 0 to remove and 196 not upgraded.
Need to get 537 kB of archives.
After this operation, 2,899 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 lynis all 2.6.2-1 [183 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 menu amd64 2.1.47ubuntu4 [354 kB]
Fetched 537 kB in 5s (107 kB/s)
Selecting previously unselected package lynis.
(Reading database ... 283754 files and directories currently installed.)
Preparing to unpack .../archives/lynis_2.6.2-1_all.deb ...
Unpacking lynis (2.6.2-1) ...
Selecting previously unselected package menu.
Preparing to unpack .../menu_2.1.47ubuntu4_amd64.deb ...
Unpacking menu (2.1.47ubuntu4) ...
Setting up lynis (2.6.2-1) ...
Setting up menu (2.1.47ubuntu4) ...
Processing triggers for mime-support (3.64ubuntu1) ...
Processing triggers for gnome-menus (3.36.0-1ubuntu1) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for install-info (6.7.0.dfsg.2-5) ...
Processing triggers for desktop-file-utils (0.24-1ubuntu3) ...
Processing triggers for menu (2.1.47ubuntu4) ...
SriLakshmiPrasanna59@sri:~$ sudo lynis audit system

[ Lynis 2.6.2 ]

################################################################################
  Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
  welcome to redistribute it under the terms of the GNU General Public License.
  See the LICENSE file for details about using this software.

  2007-2018, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)
################################################################################
```



```
  See the LICENSE file for details about using this software.

  2007-2018, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)
################################################################################


[+] Initializing program
------------------------------------
  - Detecting OS...                                           [ DONE ]
  - Checking profiles...                                      [ DONE ]

  ---------------------------------------------------
  Program version:           2.6.2
  Operating system:          Linux
  Operating system name:     Ubuntu Linux
  Operating system version:  20.04
  Kernel version:            5.15.0
  Hardware platform:         x86_64
  Hostname:                  sri
  ---------------------------------------------------
  Profiles:                  /etc/lynis/default.prf
  Log file:                  /var/log/lynis.log
  Report file:               /var/log/lynis-report.dat
  Report version:            1.0
  Plugin directory:          /etc/lynis/plugins
  ---------------------------------------------------
  Auditor:                   [Not Specified]
  Language:                  en
  Test category:             all
  Test group:                all
  ---------------------------------------------------
  - Program update status...                                  [ WARNING ]

      ===============================================================================
        Lynis update available
      ===============================================================================

        Current version is more than 4 months old

        Current version : 262   Latest version : 308

        Please update to the latest version.
        New releases include additional features, bug fixes, tests, and baselines.

        Download the latest version:
```



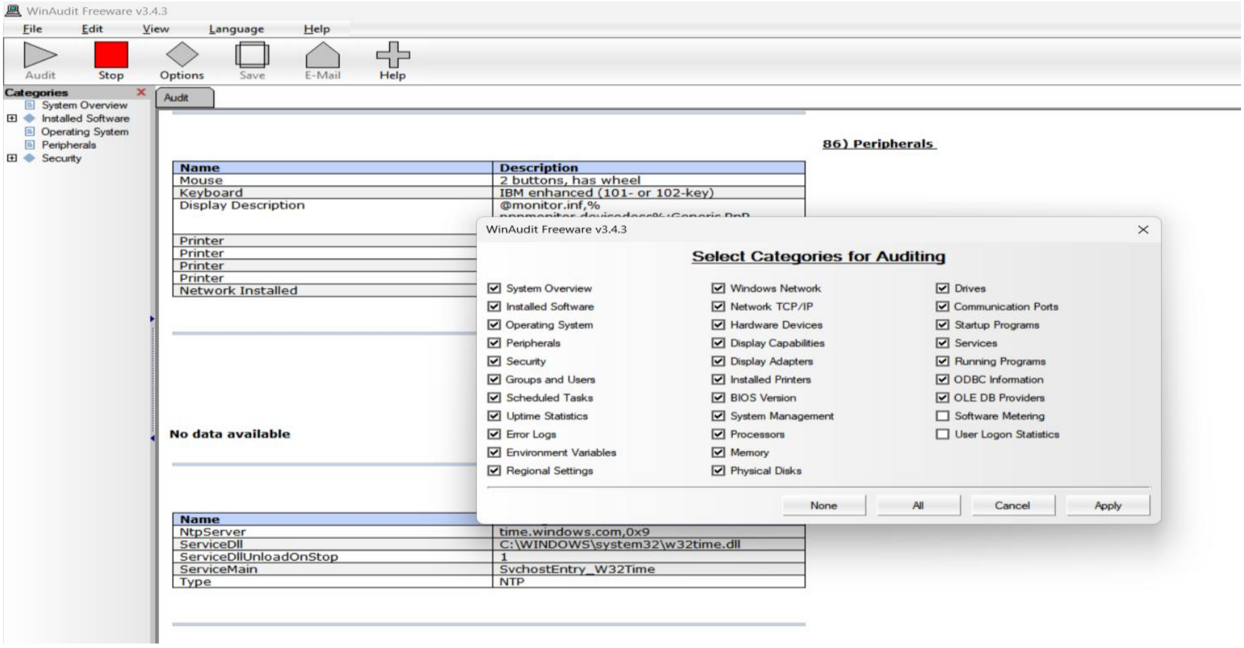
```
------------------------------------
  - Scanning available tools...
  - Checking system binaries...
tr: extra operand 'c'
Try 'tr --help' for more information.

[+] Plugins (phase 1)
------------------------------------
 Note: plugins have more extensive tests and may take several minutes to complete

  - Plugin: debian
    [
[+] Debian Tests
------------------------------------
  - Checking for system binaries that are required by Debian Tests...
    - Checking /bin...                                          [ FOUND ]
    - Checking /sbin...                                         [ FOUND ]
    - Checking /usr/bin...                                      [ FOUND ]
    - Checking /usr/sbin...                                     [ FOUND ]
    - Checking /usr/local/bin...                                [ FOUND ]
    - Checking /usr/local/sbin...                               [ FOUND ]
  - Authentication:
    - PAM (Pluggable Authentication Modules):
      - libpam-tmpdir                                           [ Not Installed ]
      - libpam-usb                                              [ Not Installed ]
  - File System Checks:
    - DM-Crypt, Cryptsetup & Cryptmount:
  - Software:
    - apt-listbugs                                              [ Not Installed ]
    - apt-listchanges                                           [ Not Installed ]
    - checkrestart                                              [ Not Installed ]
    - needrestart                                               [ Not Installed ]
    - debsecan                                                  [ Not Installed ]
    - debsums                                                   [ Not Installed ]
    - fail2ban                                                  [ Not Installed ]
]

[+] Boot and services
------------------------------------
  - Service Manager                                             [ SysV Init ]
  - Checking UEFI boot                                          [ DISABLED ]
  - Checking presence GRUB2                                     [ FOUND ]
    - Checking for password protection                          [ WARNING ]
  - Check running services (systemctl)                          [ DONE ]
        Result: found 34 running services
  - Check enabled services at boot (systemctl)                  [ DONE ]
```



```
  - Searching for IO waiting processes                          [ OK ]

[+] Users, Groups and Authentication
------------------------------------
  - Administrator accounts                                      [ OK ]
  - Unique UIDs                                                 [ OK ]
  - Consistency of group files (grpck)                          [ OK ]
  - Unique group IDs                                            [ OK ]
  - Unique group names                                          [ OK ]
  - Password file consistency                                   [ OK ]
  - Query system users (non daemons)                            [ DONE ]
  - NIS+ authentication support                                 [ NOT ENABLED ]
  - NIS authentication support                                  [ NOT ENABLED ]
  - sudoers file                                                [ FOUND ]
    - Check sudoers file permissions                            [ OK ]
  - PAM password strength tools                                 [ SUGGESTION ]
  - PAM configuration files (pam.conf)                          [ FOUND ]
  - PAM configuration files (pam.d)                             [ FOUND ]
  - PAM modules                                                 [ FOUND ]
  - LDAP module in PAM                                          [ NOT FOUND ]
  - Accounts without expire date                                [ OK ]
  - Accounts without password                                   [ OK ]
  - Checking user password aging (minimum)                      [ DISABLED ]
  - User password aging (maximum)                               [ DISABLED ]
  - Checking expired passwords                                  [ OK ]
  - Checking Linux single user mode authentication              [ WARNING ]
  - Determining default umask
    - umask (/etc/profile)                                      [ NOT FOUND ]
    - umask (/etc/login.defs)                                   [ SUGGESTION ]
  - LDAP authentication support                                 [ NOT ENABLED ]
  - Logging failed login attempts                               [ ENABLED ]

[+] Shells
------------------------------------
  - Checking shells from /etc/shells
    Result: found 7 shells (valid shells: 7).
    - Session timeout settings/tools                            [ NONE ]
  - Checking default umask values
    - Checking default umask in /etc/bash.bashrc                [ NONE ]
    - Checking default umask in /etc/profile                    [ NONE ]

[+] File systems
------------------------------------
  - Checking mount points
    - Checking /home mount point                                [ SUGGESTION ]
    - Checking /tmp mount point                                 [ SUGGESTION ]
```

3.1.4 WinAudit

I have used WinAudit to check the physical security of my system and it performs the scan of system and gives the complete information of the system.



86) Peripherals

Name	Description
Mouse	2 buttons, has wheel
Keyboard	IBM enhanced (101- or 102-key)
Display Description	@monitor.inf,% pnpmonitor.devicedesc%;Generic PnP
Printer	
Printer	
Printer	
Printer	
Network Installed	

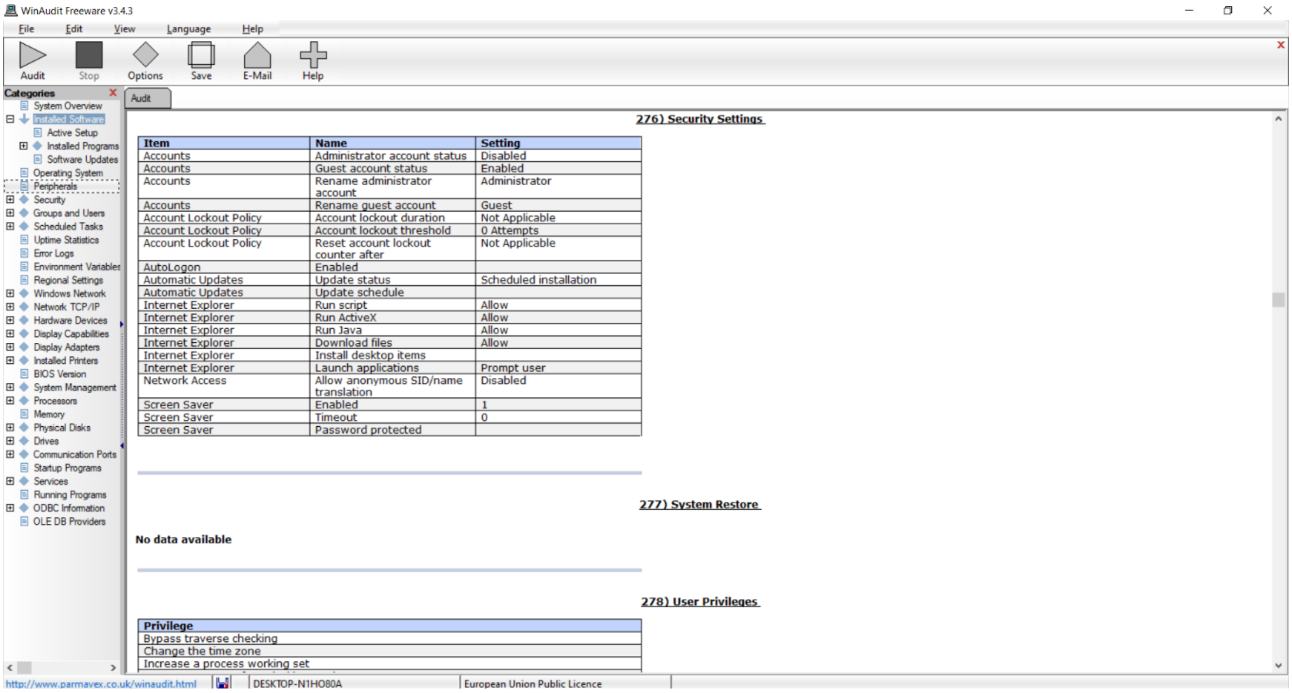
No data available

Name	
NtpServer	time.windows.com,0x9
ServiceDll	C:\WINDOWS\system32\w32time.dll
ServiceDllUnloadOnStop	1
ServiceMain	SvchostEntry_W32Time
Type	NTP

WinAudit Freeware v3.4.3

Select Categories for Auditing

☑ System Overview
☑ Installed Software
☑ Operating System
☑ Peripherals
☑ Security
☑ Groups and Users
☑ Scheduled Tasks
☑ Uptime Statistics
☑ Error Logs
☑ Environment Variables
☑ Regional Settings
☑ Windows Network
☑ Network TCP/IP
☑ Hardware Devices
☑ Display Capabilities
☑ Display Adapters
☑ Installed Printers
☑ BIOS Version
☑ System Management
☑ Processors
☑ Memory
☑ Physical Disks
☑ Drives
☑ Communication Ports
☑ Startup Programs
☑ Services
☑ Running Programs
☑ ODBC Information
☑ OLE DB Providers
□ Software Metering
□ User Logon Statistics



276) Security Settings

Item	Name	Setting
Accounts	Administrator account status	Disabled
Accounts	Guest account status	Enabled
Accounts	Rename administrator account	Administrator
Accounts	Rename guest account	Guest
Account Lockout Policy	Account lockout duration	Not Applicable
Account Lockout Policy	Account lockout threshold	0 Attempts
Account Lockout Policy	Reset account lockout counter after	Not Applicable
AutoLogon	Enabled	
Automatic Updates	Update status	Scheduled installation
Automatic Updates	Update schedule	
Internet Explorer	Run script	Allow
Internet Explorer	Run ActiveX	Allow
Internet Explorer	Run Java	Allow
Internet Explorer	Download files	Allow
Internet Explorer	Install desktop items	
Internet Explorer	Launch applications	Prompt user
Network Access	Allow anonymous SID/name translation	Disabled
Screen Saver	Enabled	1
Screen Saver	Timeout	0
Screen Saver	Password protected	

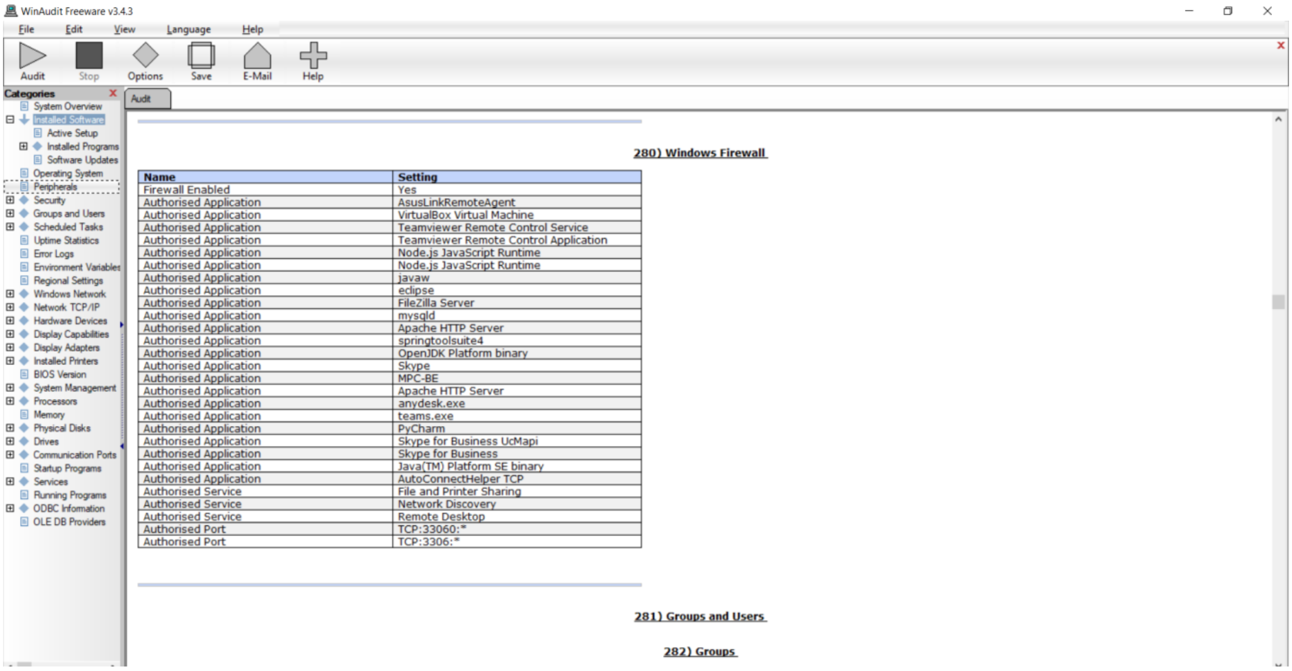
277) System Restore

No data available

278) User Privileges

Privilege
Bypass traverse checking
Change the time zone
Increase a process working set

http://www.parmavex.co.uk/winaudit.html | DESKTOP-N1HO80A | European Union Public Licence

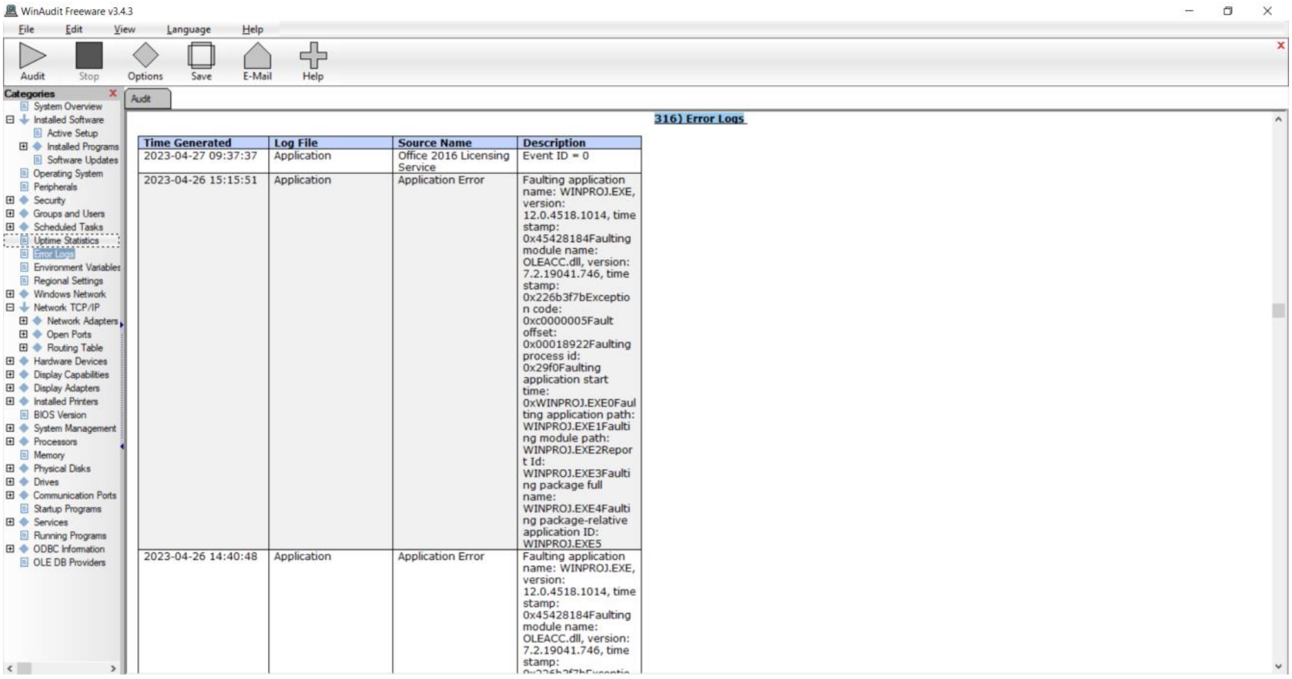


280) Windows Firewall

Name	Setting
Firewall Enabled	Yes
Authorised Application	AsusLinkRemoteAgent
Authorised Application	VirtualBox Virtual Machine
Authorised Application	Teamviewer Remote Control Service
Authorised Application	Teamviewer Remote Control Application
Authorised Application	Node.js JavaScript Runtime
Authorised Application	Node.js JavaScript Runtime
Authorised Application	javaw
Authorised Application	eclipse
Authorised Application	FileZilla Server
Authorised Application	mysqld
Authorised Application	Apache HTTP Server
Authorised Application	springtoolsuite4
Authorised Application	OpenJDK Platform binary
Authorised Application	Skype
Authorised Application	MPC-BE
Authorised Application	Apache HTTP Server
Authorised Application	anydesk.exe
Authorised Application	teams.exe
Authorised Application	PyCharm
Authorised Application	Skype for Business UcMapi
Authorised Application	Skype for Business
Authorised Application	Java(TM) Platform SE binary
Authorised Application	AutoConnectHelper TCP
Authorised Service	File and Printer Sharing
Authorised Service	Network Discovery
Authorised Service	Remote Desktop
Authorised Port	TCP:33060:*
Authorised Port	TCP:3306:*

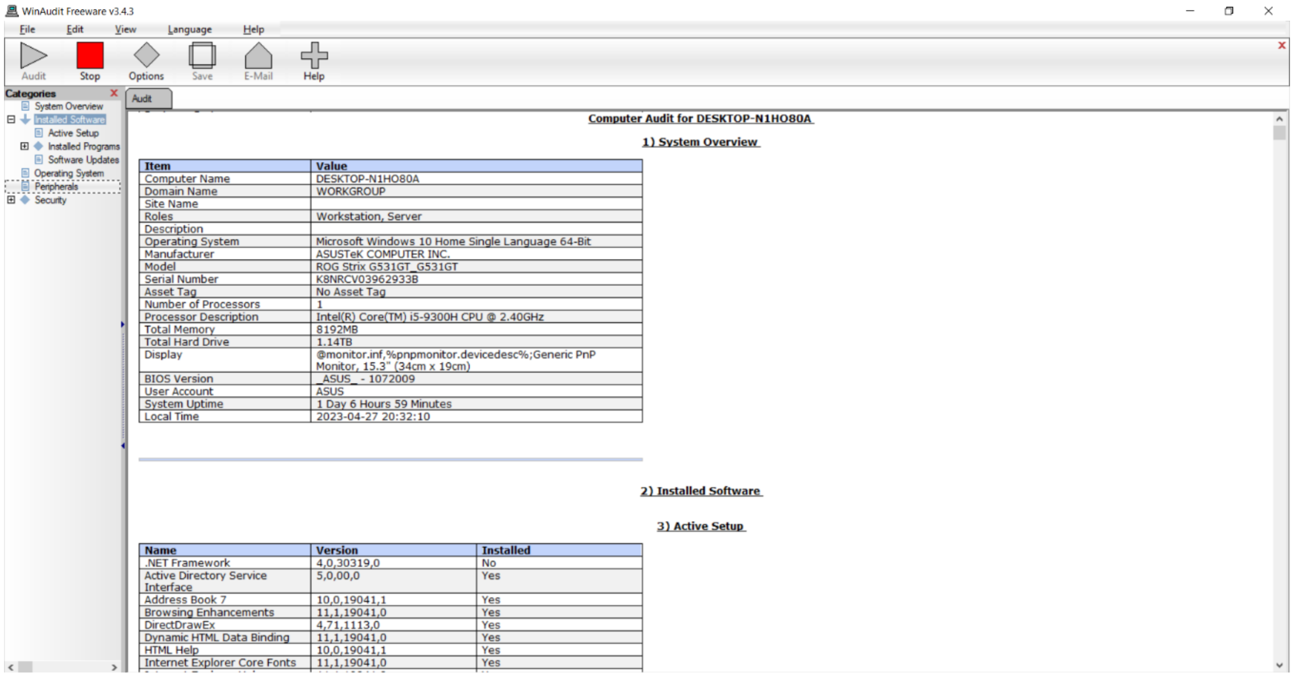
281) Groups and Users

282) Groups



316) Error Logs

Time Generated	Log File	Source Name	Description
2023-04-27 09:37:37	Application	Office 2016 Licensing Service	Event ID = 0
2023-04-26 15:15:51	Application	Application Error	Faulting application name: WINPROJ.EXE, version: 12.0.4518.1014, time stamp: 0x45428184Faulting module name: OLEACC.dll, version: 7.2.19041.746, time stamp: 0x226b3f7bException code: 0xc0000005Fault offset: 0x00018922Faulting process id: 0x29f0Faulting application start time: 0xWINPROJ.EXE0Faulting application path: WINPROJ.EXE1Faulting module path: WINPROJ.EXE2Report Id: WINPROJ.EXE3Faulting package full name: WINPROJ.EXE4Faulting package-relative application ID: WINPROJ.EXE5
2023-04-26 14:40:48	Application	Application Error	Faulting application name: WINPROJ.EXE, version: 12.0.4518.1014, time stamp: 0x45428184Faulting module name: OLEACC.dll, version: 7.2.19041.746, time stamp:



Computer Audit for DESKTOP-N1HO80A

1) System Overview

Item	Value
Computer Name	DESKTOP-N1HO80A
Domain Name	WORKGROUP
Site Name	
Roles	Workstation, Server
Description	
Operating System	Microsoft Windows 10 Home Single Language 64-Bit
Manufacturer	ASUSTeK COMPUTER INC.
Model	ROG Strix G531GT_G531GT
Serial Number	K8NRCV03962933B
Asset Tag	No Asset Tag
Number of Processors	1
Processor Description	Intel(R) Core(TM) i5-9300H CPU @ 2.40GHz
Total Memory	8192MB
Total Hard Drive	1.14TB
Display	@monitor.inf,%pnpmonitor.devicedesc%;Generic PnP Monitor, 15.3" (34cm x 19cm)
BIOS Version	_ASUS_ - 1072009
User Account	ASUS
System Uptime	1 Day 6 Hours 59 Minutes
Local Time	2023-04-27 20:32:10

2) Installed Software

3) Active Setup

Name	Version	Installed
.NET Framework	4,0,30319,0	No
Active Directory Service Interface	5,0,00,0	Yes
Address Book 7	10,0,19041,1	Yes
Browsing Enhancements	11,1,19041,0	Yes
DirectDrawEx	4,71,1113,0	Yes
Dynamic HTML Data Binding	11,1,19041,0	Yes
HTML Help	10,0,19041,1	Yes
Internet Explorer Core Fonts	11,1,19041,0	Yes

4. Conclusion

In conclusion, the project aimed to assess the security of a system using open-source software tools and provide recommendations for improving its security posture. Overall, the project helped to improve the security posture of the system by identifying and addressing security vulnerabilities. It helped to reduce the risk of security breaches and protect the confidentiality, integrity, and availability of the system and its data. The project demonstrated the importance of regularly assessing the security of systems and taking appropriate measures to address identified security vulnerabilities.

GitHub Link: https://github.com/srilakshmi777/OpenSource

5. Bibliography

1. https://www.cisco.com/ (accessed on 23rd April 2023)
2. https://www.vmware.com/topics/glossary/content/network-security.html (accessed on 23rd April 2023)
3. https://www.openpath.com/physical-security-guide (accessed on 23rd April 2023)
4. https://www.geeksforgeeks.org/system-security/ (accessed on 24th April 2023)
5. https://nmap.org/ (accessed on 24th April 2023)
6. http://www.parmavex.co.uk/winaudit.html (accessed on 24th April 2023)
7. https://www.wireshark.org/ (accessed on 24th April 2023)