

**USE OF OPENSOURCE TOOL**

**Topic: 4**

Submitted to

**LOVELY PROFESSIONAL UNIVERSITY**

for

**INT301**

**Submitted By Submitted to**

**Royce Elijha Mr. Rajeshwar Sharma**

**LOVELY FACULTY OF TECHNOLOGY & SCIENCES**

**LOVELY PROFESSIONAL UNIVERSITY**

**PUNJAB**

**APRIL 2023**

**Table of Content**

**Chapters Titles Page No**

Chapter 1 Introduction 3-6

Chapter 2 System Description

Chapter 3 Analysis Report

Chapter 4 Reference

**CHAPTER 1: INTRODUCTION**

**1. INTRODUCTION**

In today's world, computer systems are an integral part of our daily lives. As our dependence on technology grows, the need for robust security measures to protect these systems from cyber threats becomes increasingly important. There are three primary aspects of computer security: network security, system software security, and physical security.

Network security refers to the measures taken to protect computer networks from unauthorized access, theft, and damage to their hardware, software, or electronic data. It involves the use of various security technologies, protocols, and policies to safeguard against cyber attacks such as hacking, viruses, and malware.

System software security, on the other hand, involves securing the software and applications running on computer systems. This includes ensuring that the software is up-to-date and free from vulnerabilities that could be exploited by attackers, as well as configuring systems in accordance with industry best practices to minimize the risk of security breaches.

Physical security is the protection of computer systems and their components from physical threats such as theft, damage, or unauthorized access. This includes securing servers, data centers, and other critical infrastructure against physical attacks, as well as controlling access to sensitive areas and data through measures such as biometric authentication and video surveillance.

Together, network security, system software security, and physical security play a vital role in ensuring the safety and security of our computer systems and the data they contain. In the following sections, we will delve deeper into each of these areas and explore the tools and techniques used to protect against threats in each domain.

* 1. **OBJECTIVE OF THE PROJECT**

some possible objectives for a project on network security, system software security, and physical security:

1. To identify and analyze potential threats to computer systems in each of the three security domains: network security, system software security, and physical security.

2. To evaluate and compare different security technologies, protocols, and policies for protecting computer systems in each of the three security domains.

3. To develop and implement a comprehensive security strategy for an organization's computer systems that addresses all three security domains.

4. To assess the effectiveness of different security measures and technologies in protecting against various cyber threats.

5. To design and implement a security testing framework for evaluating the security of computer systems in each of the three security domains.

6. To investigate the impact of emerging technologies such as cloud computing and IoT on the security of computer systems, and to develop strategies for mitigating the risks associated with these technologies.

7. To explore legal and ethical considerations related to computer security, such as privacy and data protection laws, and to develop guidelines for ensuring compliance with these regulations.

8. To provide recommendations for improving the security of computer systems in each of the three security domains, based on the findings of the project.

These objectives are not exhaustive, and depending on the scope of the project and the specific focus areas, there may be other relevant objectives to consider as well.

* 1. **DESCRIPTION OF THE PROJECT**

brief description of network security, system software security, and physical security:

Network Security: Network security involves protecting computer networks from unauthorized access, theft, and damage to their hardware, software, or electronic data. Network security measures may include firewalls, intrusion detection and prevention systems, antivirus software, virtual private networks (VPNs), and encryption technologies. Network security also involves the implementation of policies and procedures to ensure that users adhere to best practices for network security, such as regularly changing passwords and avoiding the use of public Wi-Fi networks.

System Software Security: System software security involves securing the software and applications running on computer systems. This includes ensuring that the software is up-to-date and free from vulnerabilities that could be exploited by attackers, as well as configuring systems in accordance with industry best practices to minimize the risk of security breaches. System software security measures may include implementing access controls, using anti-malware software, performing regular software updates and patches, and monitoring system logs for suspicious activity.

Physical Security: Physical security is the protection of computer systems and their components from physical threats such as theft, damage, or unauthorized access. Physical security measures may include the use of locks, access control systems, video surveillance, and biometric authentication technologies to prevent unauthorized access to computer systems and data centers. Other physical security measures may include backup power supplies, temperature and humidity controls, and fire suppression systems to ensure the continuity of critical systems in the event of power outages or other disasters.

Overall, network security, system software security, and physical security are all critical components of a comprehensive computer security strategy. By implementing appropriate security measures in each of these areas, organizations can help protect their computer systems and data from a wide range of cyber threats.

**1.3 SCOPE OF THE PROJECT**

some possible areas of scope for a project on network security, system software security, and physical security:

Network Security: The scope of a project on network security could include identifying vulnerabilities in the network infrastructure, analyzing traffic patterns to detect potential threats, evaluating different security technologies and protocols for protecting against cyber attacks, and developing policies and procedures for ensuring that users adhere to best practices for network security.

System Software Security: A project on system software security could focus on identifying and mitigating vulnerabilities in operating systems and applications, analyzing malware and other threats to system software, evaluating different anti-malware and anti-virus software tools, and developing strategies for ensuring that software is up-to-date and free from vulnerabilities.

Physical Security: A project on physical security could involve identifying potential physical threats to computer systems, analyzing access control systems and other physical security measures, evaluating backup power supplies and disaster recovery plans, and developing policies and procedures for ensuring that critical systems are protected from physical damage or theft.

Overall, the scope of a project on network security, system software security, and physical security will depend on the specific goals and objectives of the project, as well as the size and complexity of the organization's computer systems. Some projects may focus on a specific area of security, such as evaluating different firewall technologies for network security, while others may take a more holistic approach and address multiple aspects of security in an integrated manner. **CHAPTER 2: SYSTEM DESCRIPTION**

1. **SYSTEM DESCRIPTION**

system description for each of the three security domains:

Network Security System Description:

The network security system is designed to protect an organization's computer network from unauthorized access, theft, and damage to their hardware, software, or electronic data. This system may consist of several components, including firewalls, intrusion detection and prevention systems, antivirus software, virtual private networks (VPNs), and encryption technologies. The system is typically managed by a network security team, which is responsible for monitoring network activity, identifying and addressing potential security threats, and ensuring that users adhere to best practices for network security.

System Software Security System Description:

The system software security system is designed to secure the software and applications running on an organization's computer systems. This system includes measures such as ensuring that the software is up-to-date and free from vulnerabilities that could be exploited by attackers, configuring systems in accordance with industry best practices to minimize the risk of security breaches, implementing access controls, using anti-malware software, and performing regular software updates and patches. The system is typically managed by a system security team, which is responsible for monitoring system activity, identifying and addressing potential security threats, and ensuring that software is up-to-date and free from vulnerabilities.

Physical Security System Description:

The physical security system is designed to protect an organization's computer systems and their components from physical threats such as theft, damage, or unauthorized access. This system may include measures such as locks, access control systems, video surveillance, and biometric authentication technologies to prevent unauthorized access to computer systems and data centers. Other physical security measures may include backup power supplies, temperature and humidity controls, and fire suppression systems to ensure the continuity of critical systems in the event of power outages or other disasters. The system is typically managed by a physical security team, which is responsible for monitoring access to critical systems, identifying and addressing potential physical security threats, and ensuring that backup power supplies and disaster recovery plans are in place.

Overall, these systems work together to provide a comprehensive security strategy for an organization's computer systems. By implementing appropriate security measures in each of these areas, organizations can help protect their computer systems and data from a wide range of cyber threats.

* 1. **TARGET SYSTEM DESCRIPTION**

target system description for each of the three security domains:

Target Network Security System Description:

The target network security system is a complex network infrastructure that requires robust security measures to protect against cyber attacks. The system includes multiple servers, workstations, routers, switches, and other networking devices. The network security system is designed to protect the confidentiality, integrity, and availability of critical data and resources by implementing a layered approach to security. This includes measures such as network segmentation, firewalls, intrusion detection and prevention systems, antivirus software, virtual private networks (VPNs), and encryption technologies.

Target System Software Security System Description:

The target system software security system is a large-scale system that includes multiple servers, operating systems, and applications running on them. The system software security system is designed to secure the software and applications running on the target system, protect against malware, and ensure that the system is up-to-date and free from vulnerabilities. The system includes measures such as access controls, anti-malware software, software updates and patches, and system hardening.

Target Physical Security System Description:

The target physical security system is a data center that houses multiple servers and other computer equipment. The system is designed to protect the physical security of the target system and prevent unauthorized access, theft, or damage to the hardware, software, or electronic data. The system includes measures such as biometric authentication technologies, video surveillance, access control systems, temperature and humidity controls, backup power supplies, and disaster recovery plans.

**2.2 ASSUMPTIONS AND DEPENDENCIES**

some assumptions and dependencies on computer security:

Assumptions:

Security policies and procedures are properly documented and followed by all users.

Security personnel have the necessary skills and training to detect and respond to security threats.

Hardware and software vendors provide regular security updates and patches.

End-users are trained in security best practices, such as strong password management and not opening suspicious email attachments.

Security measures are properly configured and implemented to protect against known security threats.

Dependencies:

Availability of security updates and patches from hardware and software vendors.

Proper configuration of security measures, such as firewalls, intrusion detection systems, and antivirus software.

Availability of adequate funding to support security measures.

Availability of backup power supplies and disaster recovery plans in case of power outages or other disasters.

Adequate network and system resources to support security measures, such as network bandwidth, storage, and processing power.

Adequate physical security measures to protect against physical theft or damage to computer systems.

Overall, effective computer security requires a combination of well-documented policies and procedures, proper training and resources for security personnel and end-users, regular updates and patches from hardware and software vendors, and proper configuration and implementation of security measures. Organizations should regularly review and update their assumptions and dependencies to ensure that their security measures are effective and up-to-date.

**2.3** **FUNCTIONAL/NON-FUNCTIONAL DEPENDENCIES**

some functional and non-functional dependencies on computer security:

Functional Dependencies:

Access control: The ability to restrict access to computer resources to authorized users only.

Authentication and authorization: The ability to verify the identity of users and grant access based on their roles and privileges.

Encryption: The ability to protect sensitive data by encoding it so that it cannot be read by unauthorized users.

Auditing and logging: The ability to monitor system activity and keep a record of it for auditing purposes.

Intrusion detection and prevention: The ability to detect and prevent unauthorized access to computer systems.

Non-Functional Dependencies:

Performance: The ability to maintain acceptable system performance while enforcing security measures.

Scalability: The ability to scale security measures as the system grows or changes.

Usability: The ability to implement security measures in a way that does not significantly impact the user experience.

Reliability: The ability to maintain system security even in the face of hardware or software failures.

Availability: The ability to ensure that computer systems are available and accessible to authorized users at all times.

Overall, both functional and non-functional dependencies are important for ensuring that computer security measures are effective and do not negatively impact the usability, performance, or reliability of computer systems.

**CHAPTER 3: ANALYSIS REPORT**

**Nmap, Lynis,** and **OpenSCAD** are three different open source tools with different functionalities. Here's a brief description of each:

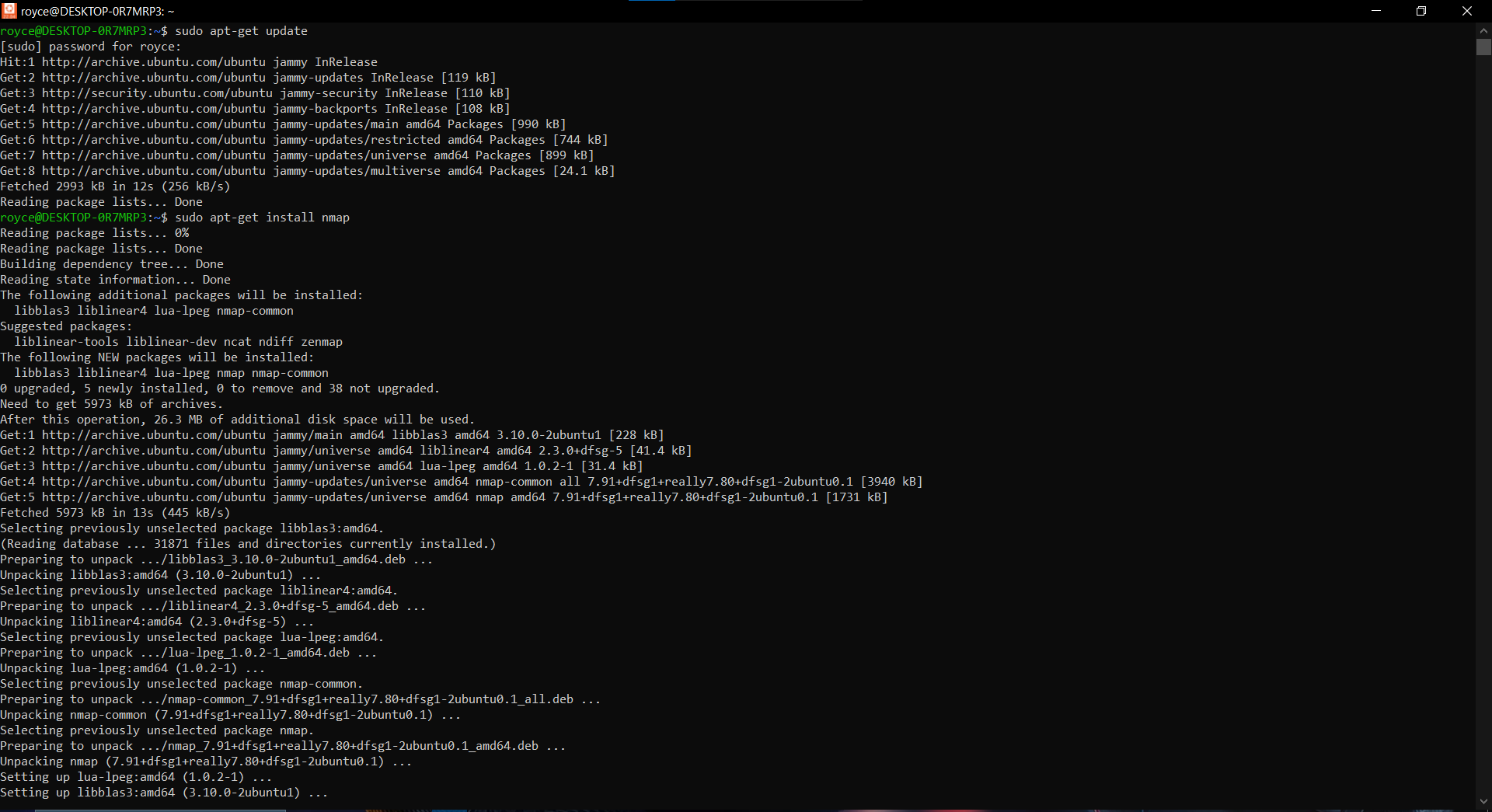
**Nmap**: Nmap (Network Mapper) is a free and open-source security testing tool used for network exploration and security auditing. It can be used to scan single hosts, small networks, or large enterprise networks to identify open ports, services, operating systems, and potential vulnerabilities. Nmap is a powerful tool for network administrators, security professionals, and penetration testers.

**Lynis**: Lynis is a free and open-source security auditing tool for Linux and Unix-based systems. It can be used to perform security assessments, compliance testing, and vulnerability scanning. Lynis scans the system for security vulnerabilities, misconfigurations, and other potential security issues. It then provides a detailed report on the system's security posture and recommendations for improving it.

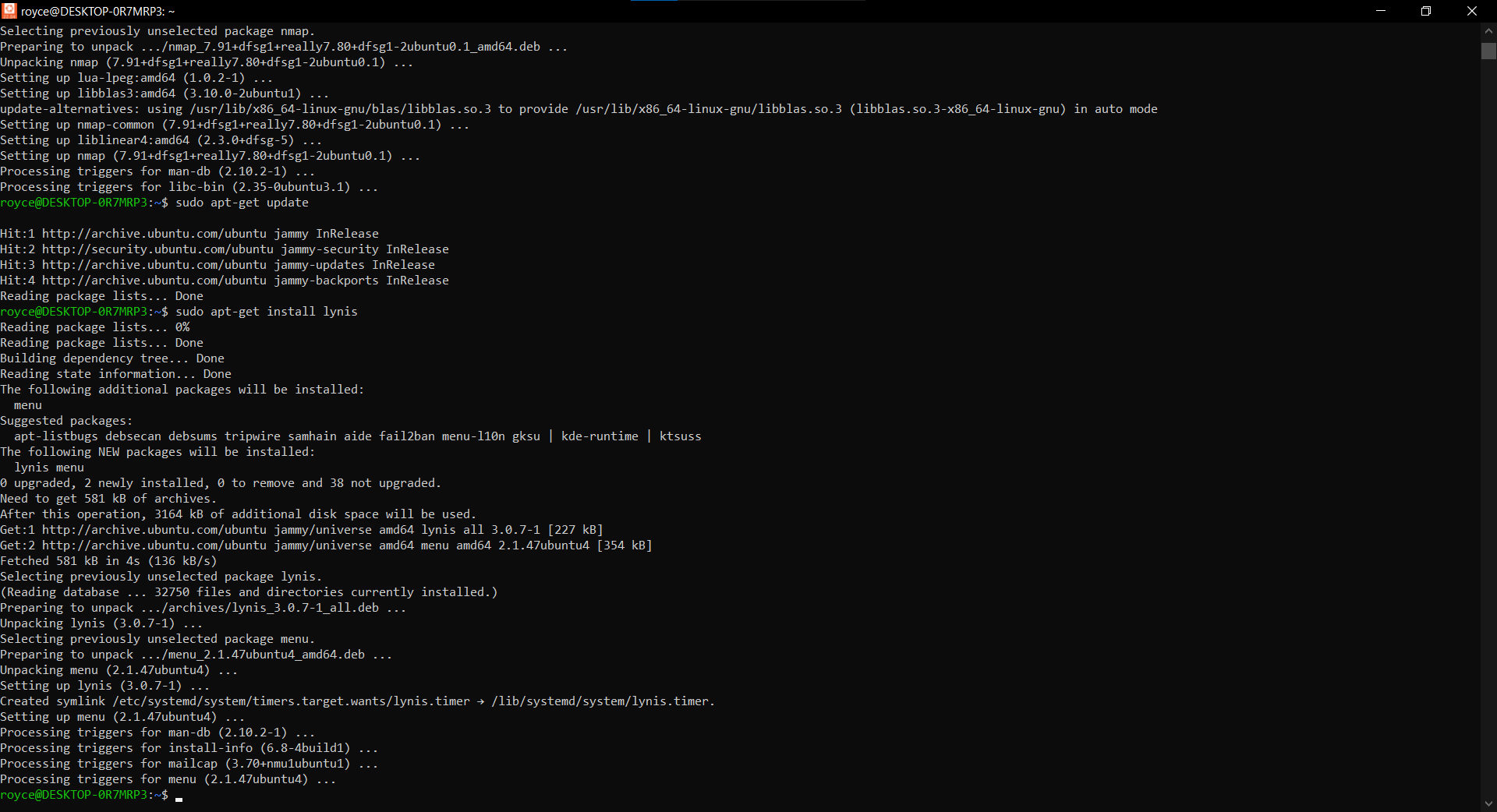
**OpenSCAD**: OpenSCAD is a free and open-source 3D CAD (computer-aided design) software for creating solid 3D models. It is a script-based CAD software, which means that the models are created by writing code instead of using a graphical user interface. OpenSCAD is widely used by engineers, designers, and makers to create 3D models for 3D printing, CNC milling, and other fabrication techniques.

In summary, Nmap is a network security testing tool, Lynis is a system security auditing tool, and OpenSCAD is a 3D CAD software. Each of these tools serves a different purpose and can be used for different applications.

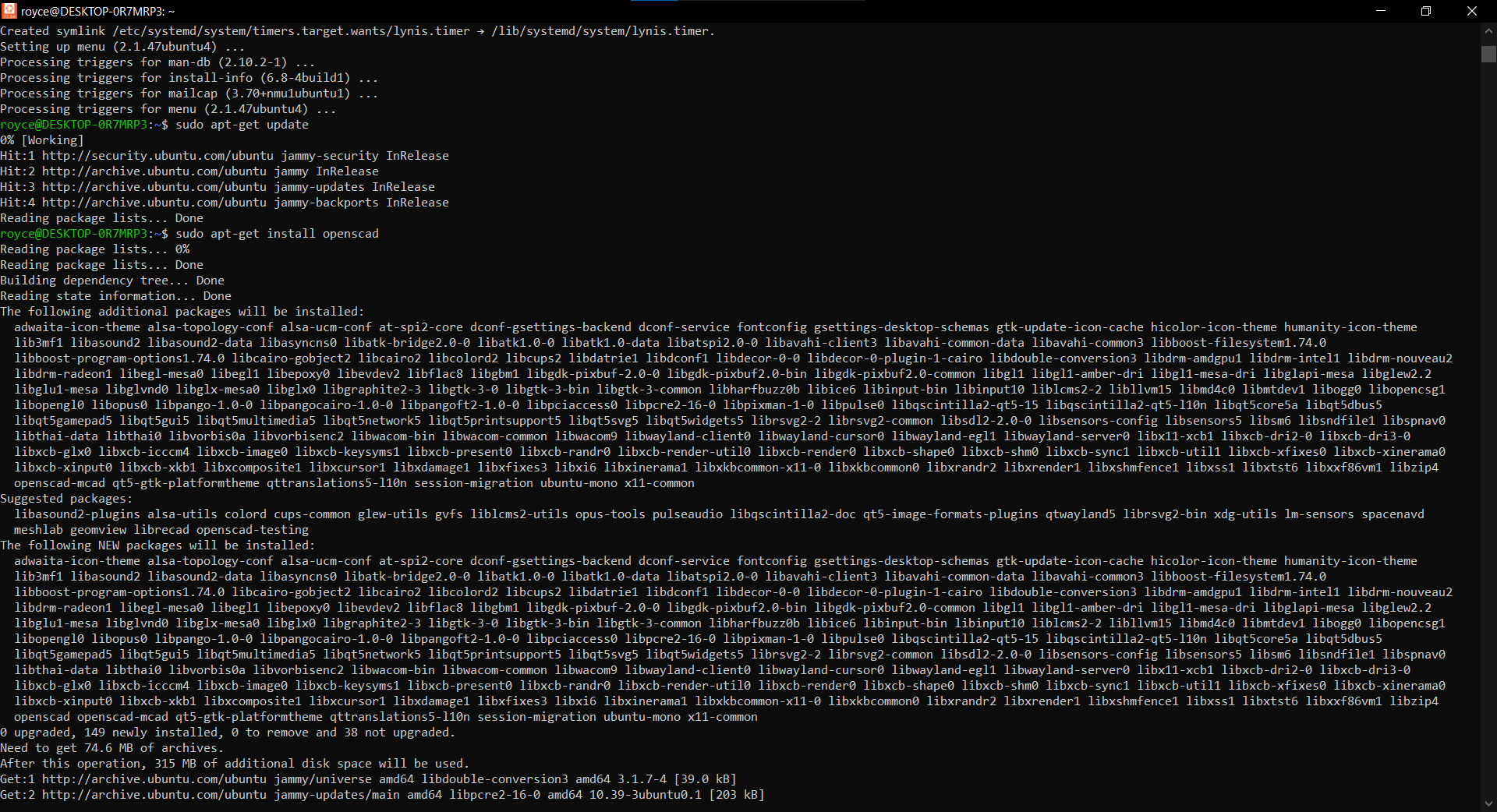
**ANALYSIS:**



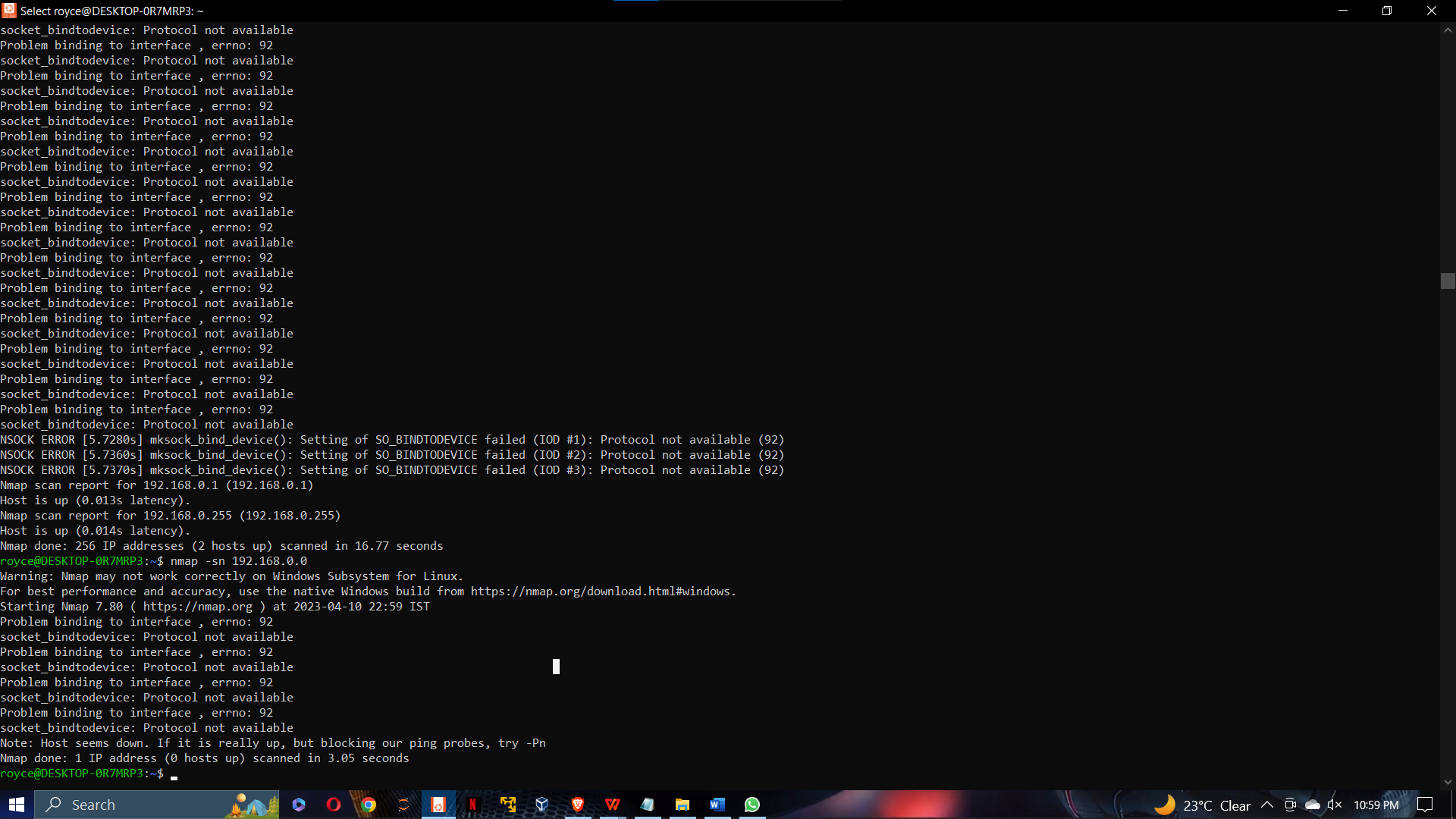
* In this I’m installing Nmap by using command “sudo apt-get install nmap”.



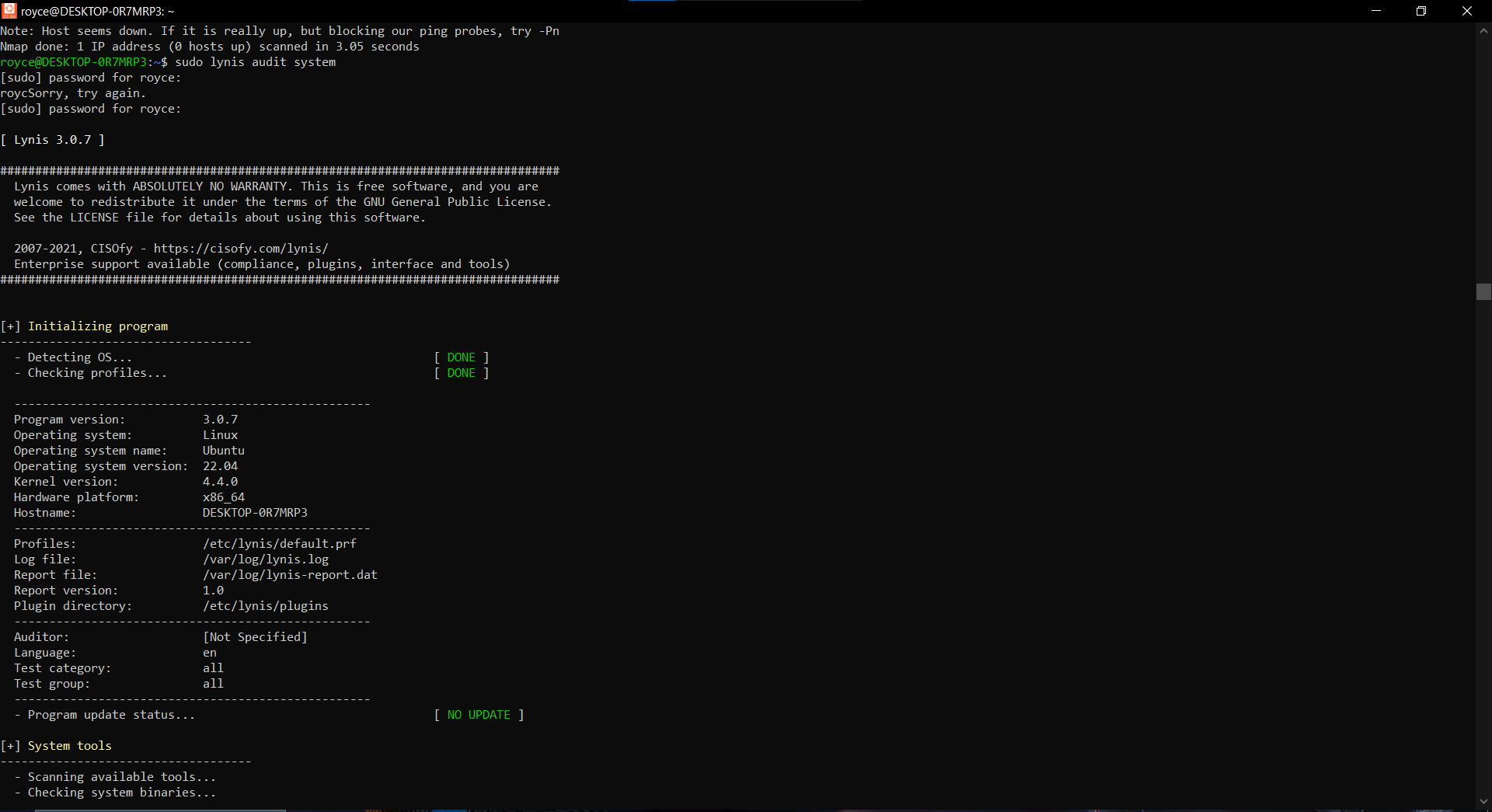
* In this step I’m installing Lynis by using “sudo apt-get install lynis” command.



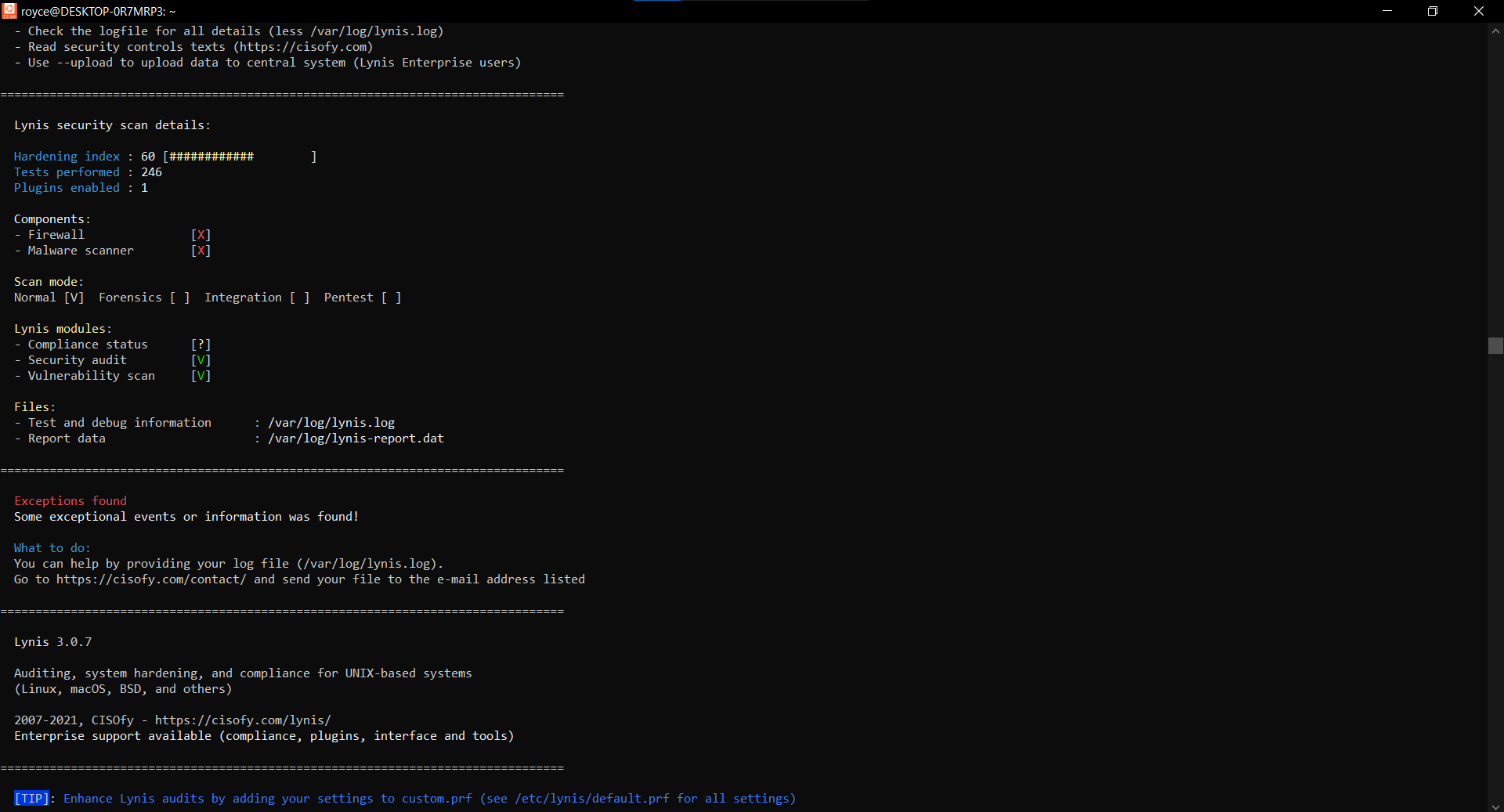
* In this step I’m installing openSCAD by using “sudo apt-get install openSCAD” command.



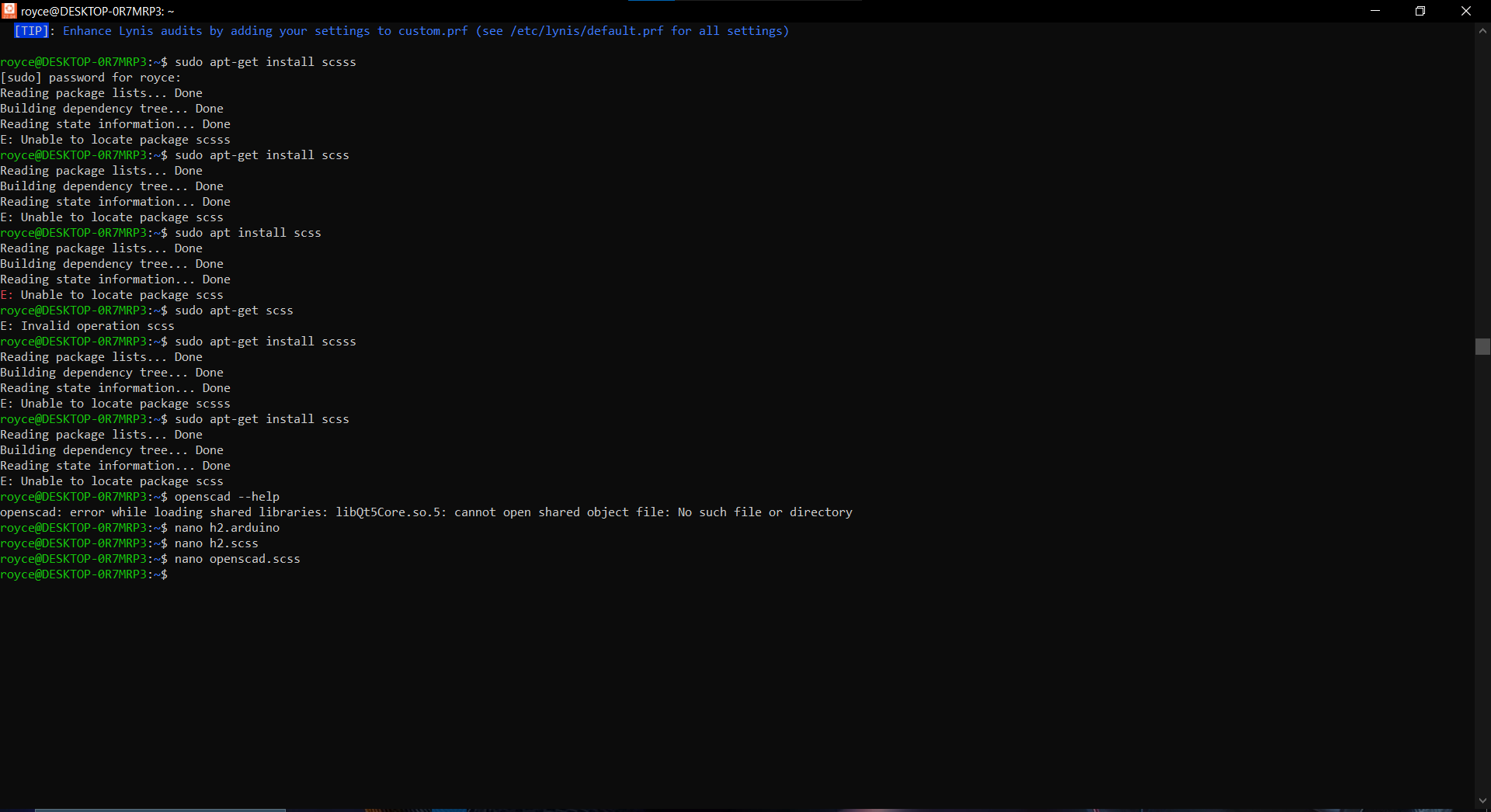
* In this Screenshot we are using Nmap for Network security.



* In this Step we are using lynis to analyze system security.



* Second step for analyzing system security with lynis.



* This is the step for openSCAD



* Inside the nano file of OpenSCAD.

**CHAPTER 4: REFRENCES**

* **https://www.sans.org/**
* **https://www.cisco.com/c/en/us/solutions/enterprise-networks/network-security.html**
* **https://owasp.org/**
* **https://www.nist.gov/topics/cybersecurity**
* **https://www.cisecurity.org/**
* **https://www.microsoft.com/en-us/security/business**
* **https://iapsc.org/resources/white-papers/**
* **https://www.asisonline.org/professional-development/resource-center/physical-security/**
* **https://www.securityinfowatch.com/security-executives/physical-security**
* **https://github.com/RoyceElijha/project\_ca3\_int301.git**