A REPORT OF ONE MONTH TRAINING

at

Sensation Software Solutions Pvt. Ltd.

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE AWARD OF THE DEGREE OF

BACHELOR OF TECHNOLOGY
(Computer Science and Engineering)

JUNE-JULY ,2025

SUBMITTED BY :

NAME : TARANVEER SINGH
UNIVERSITY ROLL NO : 2302703

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

GURU NANAK DEV ENGINEERING COLLEGE LUDHIANA

(An Autonomous College Under UGC ACT)

CERTIFICATE

CANDIDATE'S DECLARATION

I, Taranveer Singh (Roll No. 2302703), student of B.Tech in Computer Science and Engineering at Guru Nanak Dev Engineering College, Ludhiana, hereby declare that the report entitled

"A REPORT ON ONE MONTH TRAINING AT SENSATION SOFTWARE SOLUTIONS PVT. LTD."

is an authentic record of the work carried out by me during my one-month industrial training at Sensation Software Solutions Pvt. Ltd., Ludhiana.

This report has been prepared by me as part of the partial fulfillment of the requirements for the award of the Bachelor of Technology (B.Tech) degree in Computer Science and Engineering under IK Gujral Punjab Technical University (IKGPTU).

I further declare that this report is based on my personal training experience and has not been submitted previously, in part or full, for the award of any degree or diploma to any other institution or university.

(Taranveer Singh)
Roll No.: 2302703
B.Tech (Computer Science & Engineering)
Guru Nanak Dev Engineering College, Ludhiana

ABSTRACT

The one-month industrial training at Sensation Software Solutions Pvt. Ltd., Ludhiana provided an in-depth understanding of Cybersecurity fundamentals, networking, operating systems, and practical security tools. The training was designed to enhance both theoretical and practical knowledge of protecting systems, data, and networks against evolving cyber threats.

The program began with a detailed study of cybersecurity concepts, vulnerabilities, and attack types, followed by a thorough exploration of Linux and Windows operating systems, focusing on their security mechanisms and administrative controls. Trainees were introduced to essential tools such as Wireshark, Nmap, ip tables, Metasploit, and Procmon, which enabled hands-on experience in network analysis, packet inspection, and threat detection.

The training further covered cryptography, wireless security, vulnerability assessment, penetration testing, malware analysis, digital forensics, and incident response, providing exposure to real-world cybersecurity challenges. Additionally, emphasis was placed on defensive security techniques, including system hardening, SIEM monitoring, and threat hunting practices.

This training not only strengthened technical expertise but also improved analytical and problem-solving abilities, aligning with industry requirements for cybersecurity professionals. The experience gained through this program has contributed significantly to professional development and provided a solid foundation for future specialization in ethical hacking, digital forensics, and network defense.

ACKNOWLEDGMENT

I would like to express my heartfelt gratitude to Sensation Software Solutions Pvt. Ltd., Ludhiana, for providing me the opportunity to undertake my one-month industrial training in the field of Cybersecurity. This training has been a valuable learning experience, allowing me to bridge the gap between theoretical knowledge and practical applications in real-world environments.

I extend my sincere thanks to my training coordinator and the entire technical team at Sensation Software Solutions Pvt. Ltd. for their continuous guidance, support, and encouragement throughout the training period. Their mentorship helped me understand various cybersecurity concepts, tools, and practical implementations effectively.

I am also deeply thankful to Guru Nanak Dev Engineering College, Ludhiana, and the Department of Computer Science and Engineering for their support and for providing this wonderful opportunity to gain industrial exposure.

Lastly, I would like to thank my faculty mentors, colleagues, and friends for their valuable suggestions, motivation, and assistance during the completion of this training and report.

This experience has truly enhanced my technical skills and confidence, and I am grateful to everyone who contributed to the success of my training journey.

(Taranveer Singh)
Roll No.: 2302703
B.Tech (Computer Science & Engineering)
Guru Nanak Dev Engineering College, Ludhiana

ABOUT THE COMPANY / INSTITUTE

Sensation Software Solutions Pvt. Ltd. is a leading IT company based in Ludhiana, Punjab, specializing in software development, digital marketing, and cybersecurity services. Established with a vision to empower businesses through innovative technology, the company has built a strong reputation for delivering reliable, scalable, and secure digital solutions tailored to client needs.

The organization provides a wide range of IT services, including web and mobile application development, cloud computing, data analytics, IT consulting, and cybersecurity training. With a team of skilled professionals, Sensation Software Solutions aims to foster a learning environment that encourages creativity, technical growth, and real-world problem-solving.

The company's training division focuses on imparting practical knowledge to engineering and computer science students through hands-on industrial training programs. These programs are designed to align academic knowledge with industry standards, helping students develop the skills needed for a professional career in the IT sector.

During the one-month training on Cybersecurity Fundamentals and Operating System Basics, trainees were introduced to real-time security challenges and practical exposure to tools like Wireshark, Nmap, Nessus, Metasploit, and Firewalls. The training emphasized both defensive and offensive security concepts, ensuring that students understood how to identify, mitigate, and respond to modern cyber threats.

The company's learning environment promotes teamwork, technical exploration, and continuous improvement. Trainers at Sensation Software Solutions are experienced professionals with strong expertise in network security, ethical hacking, digital forensics, and secure software development. Their mentorship plays a crucial role in shaping students' technical competence and professional attitude.

Sensation Software Solutions Pvt. Ltd. maintains a culture of innovation and excellence. Its mission is to prepare future technologists capable of addressing emerging cybersecurity challenges while contributing to India's growing digital infrastructure. The company's commitment to practical learning and ethical values makes it a preferred destination for industrial training among students of top engineering institutions.

Through this training, I gained hands-on experience in implementing cybersecurity techniques, analyzing threats, configuring firewalls, and understanding real-world incident response scenarios. This experience has provided me with a deeper appreciation of the cybersecurity domain and inspired me to further pursue my career in this field.

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1 - INTRODUCTION

1.1 Introduction to Cybersecurity

In today's highly interconnected and technology-driven world, the internet has become an indispensable part of everyday life. People rely heavily on digital platforms for a wide range of activities such as online banking, financial transactions, e-commerce, social networking, cloud storage, remote education, and data sharing. Organizations and governments also depend on digital systems to store sensitive information and to carry out critical operations efficiently. However, this rapid growth in digitalization and increased dependence on technology has significantly expanded the attack surface, thereby opening the door to numerous cyber threats. These threats include hacking, identity theft, phishing attacks, malware infections, ransomware, denial-of-service attacks, and data breaches, all of which can lead to serious financial losses, privacy violations, and reputational damage.Cybersecurity refers to the comprehensive set of practices, technologies, tools, and processes designed to protect networks, computer systems, servers, mobile devices, applications, and data from cyber attacks, damage, or unauthorized access. It plays a crucial role in ensuring the confidentiality, integrity, and availability of information within the cyber domain. By implementing strong cybersecurity measures, organizations and individuals can safeguard sensitive data, prevent unauthorized activities, and maintain user trust in digital systems.The primary goal of cybersecurity is to minimize the risk of cyber attacks and protect systems from exploitation by malicious actors. Cybersecurity is not a one-time activity but a continuous and evolving process that adapts to emerging threats and vulnerabilities. It involves multiple stages, including prevention through security controls and policies, detection of potential threats, timely response to security incidents, and recovery measures to restore normal operations after an attack.

Figure 1.1 : introduction to cyber security

1.2 Importance of Cybersecurity

Cybersecurity plays a vital role in protecting digital systems, networks, and data in today's technology-driven world. As individuals, businesses, and governments increasingly rely on the internet for communication, financial transactions, data storage, and critical operations, the need for strong cybersecurity measures has become more important than ever.One of the primary reasons cybersecurity is important is the protection of sensitive data. Personal information such as bank details, passwords, identity documents, and confidential business data are valuable targets for cybercriminals. Cybersecurity helps prevent unauthorized access, data breaches, and identity theft, thereby ensuring privacy and data security.Cybersecurity is also essential for preventing cyber attacks and financial losses. Attacks such as phishing, ransomware, malware, and hacking can cause severe economic damage to individuals and organizations. By implementing effective security controls, firewalls, encryption, and monitoring systems, cybersecurity reduces the risk of such attacks and minimizes potential losses.Another important aspect of cybersecurity is maintaining trust and reliability in digital systems. Users expect online platforms, banking systems, and e-commerce websites to be safe and secure. Strong cybersecurity builds user confidence and ensures the smooth functioning of digital services without interruptions.Cybersecurity also protects critical infrastructure such as power grids, healthcare systems, transportation networks, and government services. A successful cyber attack on these systems can disrupt essential services and pose serious risks to public safety. Therefore, cybersecurity is crucial for national security and public welfare.Additionally, cybersecurity supports business continuity and operational stability. By preventing system failures and enabling quick recovery from cyber incidents, organizations can continue their operations with minimal downtime.In conclusion, cybersecurity is essential for safeguarding data, preventing cyber threats, ensuring trust in digital technologies, protecting critical infrastructure, and maintaining the stability of modern digital environments.

Figure 1.2 : importance of cyber security

1.3 Objectives of the Training

The primary objective of this training program on Cybersecurity Fundamentals and Operating System Basics is to develop a strong foundational understanding of core security principles, system architecture, and modern network protection techniques. This program is designed to equip learners with the essential knowledge required to identify, analyze, and mitigate security threats in today's complex digital environments.The main learning goals of the training program include gaining a clear understanding of the fundamental concepts of cybersecurity, including common cyber threats, vulnerabilities, and attack vectors. Participants learn how cyber attacks are carried out and how security measures are implemented to prevent, detect, and respond to such threats.Another key objective is to understand the architecture and built-in security mechanisms of both Linux and Windows operating systems. This includes user authentication, access control models, file system security, process management, and system hardening techniques that help protect operating systems from unauthorized access and exploitationThe training also focuses on networking fundamentals and network security, where learners explore concepts such as network protocols, firewalls, intrusion detection and prevention systems (IDS/IPS), and various network defense techniques. These topics help participants understand how to secure data transmission and protect networks from internal and external attacks.In addition, the program provides basic exposure to cryptography, including encryption techniques and their role in securing data, along with an introduction to penetration testing and vulnerability assessment. This helps learners understand how security weaknesses are identified and tested in a controlled and ethical manner.Participants also gain insight into incident response and malware analysis, learning how security incidents are handled, investigated, and mitigated, as well as how malicious software behaves and impacts systems.Furthermore, the training builds awareness of emerging security challenges related to cloud computing, Internet of Things (IoT), and mobile devices, highlighting the unique risks associated with modern technologies.Finally, the program emphasizes the practical application of knowledge by enabling learners to apply security concepts in **defensive scenarios**, helping them develop a security-oriented mindset and prepare for real-world cybersecurity challenges.

Figure 1.3: Objectives

1.4 Scope of the Training

The training program places strong emphasis on the foundational aspects of cybersecurity by integrating both theoretical concepts and practical implementation. It offers a comprehensive, hands-on introduction to essential cybersecurity tools and utilities such as Wireshark, Nmap, ip tables, Process Monitor (Procmon), and Metasploit, which are extensively used by cybersecurity professionals in real-world security operations and assessments. Through guided practical sessions, participants gain direct experience in using these tools to analyze network traffic, scan systems for vulnerabilities, monitor system activities, configure firewall rules, and simulate controlled attack scenarios.Participants are taken through a progressive and well-structured learning pathway that begins with an understanding of operating system fundamentals, including file systems, user management, and process handling, along with basic networking concepts such as protocols, ports, and data flow. As the training advances, learners are gradually introduced to more complex and specialized areas of cybersecurity, including vulnerability assessment, penetration testing methodologies, incident handling procedures, and threat detection techniques. This step-by-step approach ensures that learners develop confidence and competence at each stage of the program.Throughout the training, significant emphasis is placed on developing analytical thinking, problem-solving skills, and technical accuracy when dealing with security-related challenges. Participants learn not only how to identify system weaknesses and security gaps, but also how to implement effective countermeasures, apply security best practices, and ensure that systems remain robust and resilient against potential cyber threats.By the conclusion of the training program, participants acquire both technical and procedural skills required to analyze security vulnerabilities, protect digital infrastructure, investigate and respond to security incidents, and mitigate cyber attacks efficiently. This training thereby lays a strong foundation for advanced academic study, professional certifications, and a career in the rapidly evolving field of cybersecurity.This step-by-step approach ensures that learners develop confidence and competence at each stage of the program.Throughout the training, significant emphasis is placed on developing analytical thinking, problem-solving skills, and technical accuracy when dealing with security-related challengesThis step-by-step approach ensures that learners develop confidence and competence at each stage of the program.Throughout the training, significant emphasis is placed on developing analytical thinking, problem-solving skills, and technical accuracy when dealing with security-related challengesThis step-by-step approach ensures that learners develop confidence and competence at each stage of the program.Throughout the training, significant emphasis is placed on developing analytical thinking, problem-solving skills, and technical accuracy when dealing with security-related challengesThis step-by-step approach ensures that learners develop confidence and competence at each stage of the program.Throughout the training, significant emphasis is placed on developing analytical thinking, problem-solving skills, and technical accuracy when dealing with security-related challenges.

1.5 Outcome of the Training

- Upon successful completion of the training program, participants will be able to demonstrate a solid understanding of core cybersecurity principles, standards, and security frameworks, enabling them to recognize security requirements and apply best practices in real-world scenarios.
- Participants will develop the ability to operate, manage, and secure both Linux and Windows operating system environments, including user access control, file system security, process monitoring, and system configuration to prevent unauthorized activities.
- They will gain hands-on experience in performing network analysis and vulnerability assessments using industry-standard tools, allowing them to identify security gaps, analyze network traffic, and evaluate system weaknesses effectively.
- The training enables participants to identify, analyze, and mitigate common cyber threats and attacks such as malware infections, phishing, unauthorized access, and network-based attacks by implementing appropriate defensive and preventive measures.
- Learners will also acquire a foundational understanding of cryptography concepts, malware analysis techniques, and digital forensics, helping them understand how data is protected, how malicious software operates, and how digital evidence is collected and examined during investigations.
- Finally, participants will be able to apply system and network hardening techniques such as secure configuration, patch management, firewall implementation, and security policy enforcement to enhance the overall security posture of digital systems and networks.

Figure 1.4: outcomes of security programs

CHAPTER 2 – TRAINING WORK UNDERTAKEN

2.1 Overview of Training Methodology

The one-month cybersecurity training program was carefully designed to provide a comprehensive blend of theoretical understanding and practical skill development. A structured and systematic methodology was adopted to ensure effective learning and gradual skill enhancement. The training methodology comprised the following key components:

Classroom Lectures

Instructor-led sessions focused on introducing core cybersecurity fundamentals, including information security principles, operating system basics, networking concepts, cryptography, and ethical hacking methodologies. These sessions helped build a strong conceptual foundation and provided clarity on how cybersecurity theories are applied in real-world environments.

Hands-on Labs

Practical laboratory sessions were conducted to reinforce theoretical concepts through real-time implementation. Participants worked in controlled Linux and Windows environments using professional cybersecurity tools to perform tasks such as network analysis, system monitoring, vulnerability scanning, and security configuration. These labs enabled learners to gain direct experience and technical confidence.

Assignments and Practical Exercises

Each module included structured assignments and exercises designed to simulate real-world cybersecurity scenarios. These tasks encouraged learners to analyze security problems, identify vulnerabilities, apply defensive measures, and document their findings, thereby strengthening problem-solving and analytical skills.

Documentation and Reporting

Participants were required to maintain detailed logs, reports, and observations for each exercise and lab session. This practice helped develop professional documentation skills, enhanced understanding of incident analysis, and emphasized the importance of record-keeping in cybersecurity operations.The one-month cybersecurity training program was carefully designed to provide a comprehensive blend of theoretical understanding and practical skill development. A structured and systematic methodology was adopted to ensure effective learning and gradual skill enhancement. The training methodology comprised the following key components

2.2 Cybersecurity Fundamentals and Operating System Basics

2.2.1 Linux Operating System

Objectives **:-** The objective of this module is to develop a strong understanding of Linux system architecture, command-line operations, security features, and basic system administration. This module equips learners with the skills required to manage Linux systems securely, which is essential for cybersecurity professionals working in server and networked environments.

Topics Covered :- Linux Operating System Overview and File System
Introduction to Linux architecture, kernel components, directory structure, and the Linux file system hierarchy. Understanding how files and directories are organized and managed in a Linux environment.Command-Line BasicsHands-on practice with essential Linux commands such as ls, cd, mkdir, cat, grep, chmod, and chown for file navigation, management, and permission handling.User and Group Management Managing users and groups using commands like useradd, usermod, groupadd, and passwd. Emphasis on access control, role-based permissions, and secure account management.

Practical Exercises :- Create multiple user accounts and assign them to appropriate groups. Modify file and directory permissions to enforce secure access controls.Configure basic firewall rules using iptables to control network traffic.Capture live network traffic using Wireshark and analyze packet data for security insights.

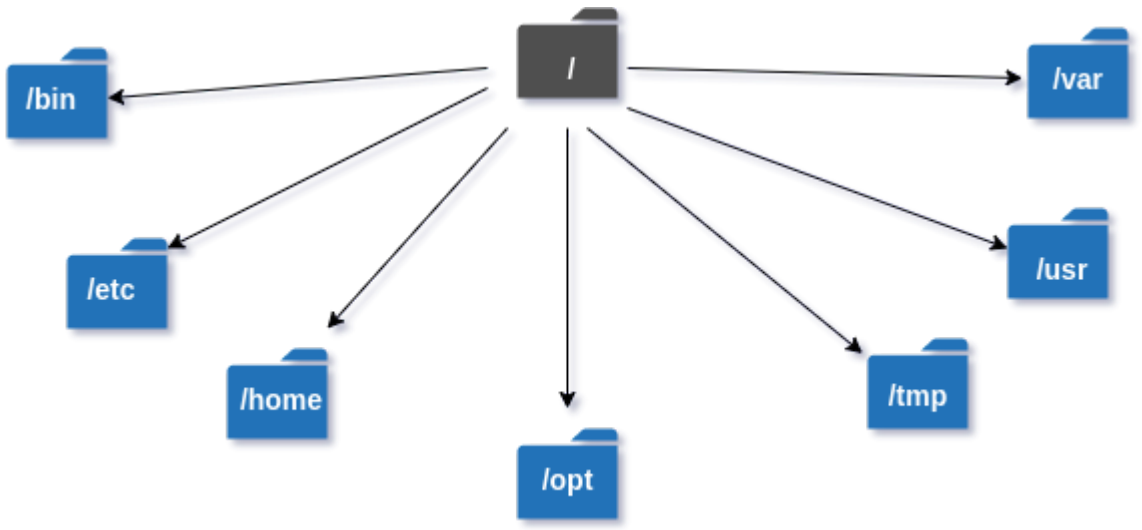


Figure 2.1: Linux file structure hierarchy

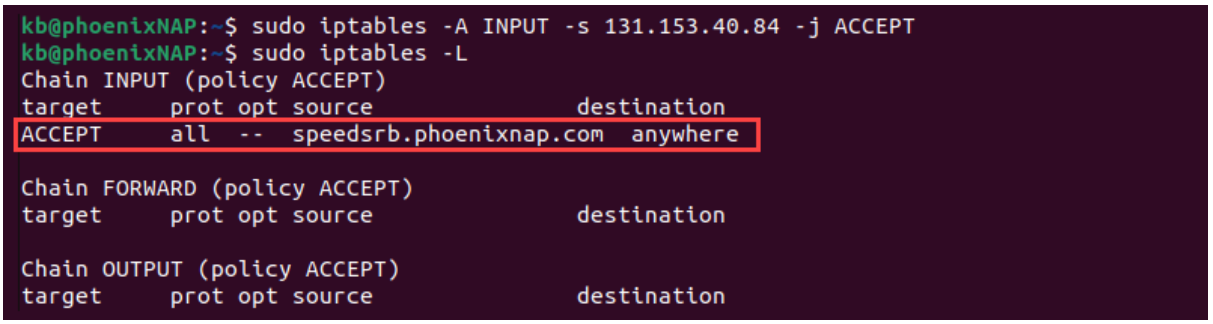


Figure 2.2: Sample ip tables rule setup

Table 2.1: Linux commands with description and usage examples

S.No.	Command	Description	Example Usage
1	ls	Lists files and directories in the current directory	Ls -l displays detailed file info
2	cd	Changes the current working directory	cd /home/user/Documents
3	pwd	Displays the current working directory path	pwd
4	mkdir	Creates a new directory	mkdir projects
5	rmdir	Removes an empty directory	rmdir old_folder
6	cp	Copies files or directories	cp file1.txt /home/user/backup/
7	mv	Moves or renames files and directories	mv oldname.txt newname.txt
8	rm	Deletes files or directories	rm files.txt
9	cat	Displays file content	cat notes.txt

		on the terminal	
10	grep	Searches text or patterns within files	grep "error" log.txt
11	chmod	Changes file permissions	chmod 755 script.sh
12	chown	Changes file ownership	chown user:group file.txt
13	ps	Displays running processes	ps aux
14	kill	Terminates processes using PID	kill 1234
15	top	Shows real-time system processes	top
16	df	Displays disk space usage	df -h
17	du	Displays directory and file size	du -sh *
18	ifconfig	Displays and configures network interface	ifconfig eth0
19	ping	Tests connectivity with a host	ping google.com

2.2.2 Windows Operating System

Objectives :-The aim of this section is to provide trainees with a comprehensive understanding of Windows OS architecture, administrative tools, and security monitoring techniques. By the end of this module, participants were able to manage users, monitor system processes, and analyze security logs to detect potential threats.

Topics Covered

Kernel:-The kernel is the core component of the Windows operating system. It is responsible for managing system resources such as CPU scheduling, memory management, hardware communication, and process execution. The kernel ensures stable and efficient operation by coordinating between hardware and software components.It is responsible for managing system resources such as CPU scheduling, memory management, hardware communication, and process execution.

Registry:-The Windows Registry is a centralized hierarchical database that stores configuration settings and options for the operating system, hardware devices, user preferences, and installed applications. It plays a crucial role in system configuration, security settings, and application behavior .hardware devices, user preferences, and installed applications.

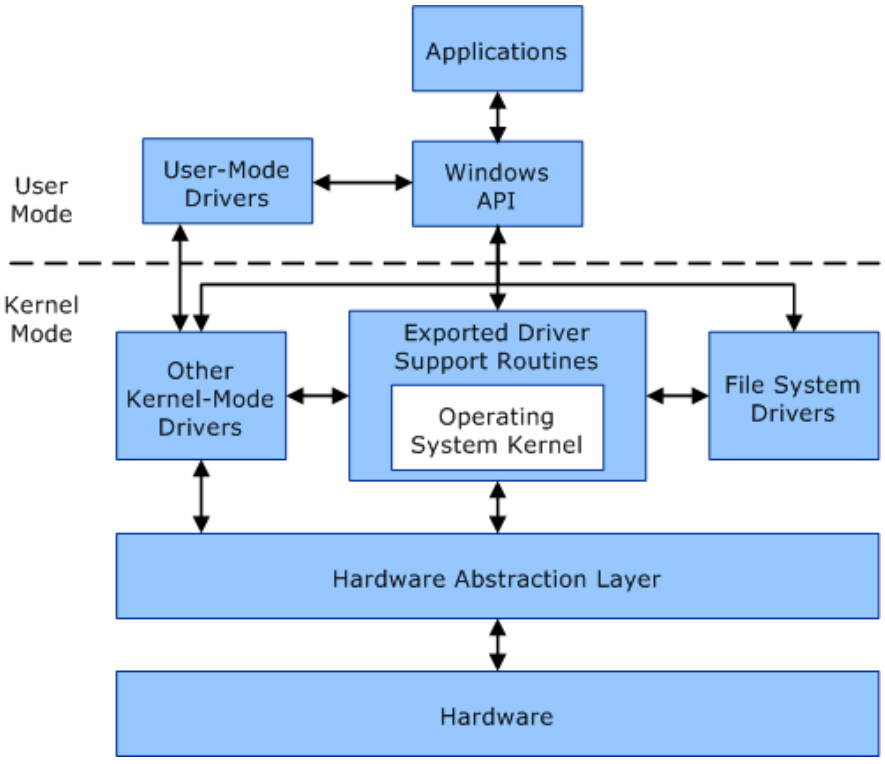


Figure 2.3: Windows architecture diagram (Kernel, User Mode, Services, UI)

2. User Privileges, Event Logs, and Registry Management

User Privileges :-Windows operating systems implement a role-based access control model to manage user permissions and enhance system security. Different user privilege levels determine what actions a user can perform on the system.

Administrator :-Administrator accounts have full control over the system. They can install and uninstall software, configure system settings, manage user accounts, access all files, and modify security policies. Due to their elevated privileges, administrator accounts must be protected with strong authentication to prevent misuse.

Standard Users :-Standard user accounts have limited privileges and are restricted from making system-wide changes. They can run applications and access personal files but cannot install system software or modify critical settings. This limitation helps reduce the risk of accidental or malicious system changes.

Guest Accounts :-Guest accounts provide minimal access and are typically used for temporary users. These accounts have very limited permissions, cannot install software, and have restricted access to system resources, making them suitable for short-term or public.

Event Logs :-Windows maintains detailed event logs that record activities related to system operations, applications, and security events. These logs are categorized into Security Logs, System Logs, and Application Logs.Event logs are extremely useful for monitoring system behavior, detecting unauthorized access attempts, identifying system errors, and investigating malicious activities. Security professionals frequently analyze event logs during incident response and forensic investigations to trace suspicious actions.

Registry Management :-The Windows Registry stores critical configuration information related to the operating system, installed applications, user preferences, and security settings. Registry keys and values control how software and hardware components behave within the system.

Table 2.2: Common Windows User Privileges

Privilege Level	Access Rights	Use Case Example
Administrator	Full system access	Installing software, changing security policies
Standard User	Limited access	Using applications without changing system settings
Guest	Minimal access	Temporary access for visitors

3. Security Tools: Procmon, PsExec, Task Scheduler

Process Monitor (Procmon) :-Process Monitor (Procmon) is an advanced Windows monitoring tool used to observe real-time activity related to process execution, file system access, registry modifications, and network interactions. It is widely used by security professionals to troubleshoot system issues, detect unauthorized changes, and identify suspicious or malicious behavior. Procmon provides detailed event-level visibility, making it an essential tool for malware analysis and incident investigation.

PsExec :-PsExec is a command-line utility from the Sysinternals suite that allows administrators to execute processes remotely with administrative privileges. It is commonly used for remote system administration, maintenance, and troubleshooting. From a security perspective, PsExec is also important because attackers may misuse it for lateral movement within a network. Understanding PsExec helps learners identify both legitimate and malicious usage scenarios.

Task Scheduler :-Task Scheduler is a built-in Windows utility that enables users to automate tasks, scripts, and programs at specified times or in response to specific system events. In cybersecurity, Task Scheduler is often used for legitimate automation tasks such as backups, updates, and security scans. However, it can also be abused by malware to maintain persistence, making it a key component to monitor during security investigation.

Practical Exercises

1. Monitoring System Processes Using Procmon :-Participants launch Process Monitor and apply filters based on specific process names such as explorer.exe. By observing real-time registry access, file system changes, and network activity, learners gain insight into normal system behavior. This exercise helps identify suspicious processes or unusual activities that may indicate malware presence or unauthorized actions.

2. Managing User Accounts and Privileges :-Using Computer Management → Local Users and Groups, participants create new user accounts and assign them either Standard User or Administrator privileges. Existing user privileges are modified to simulate different security scenarios, helping learners understand the impact of privilege levels on system security and access control.

3. Investigating Windows Event Logs for Suspicious Activities :-Participants use Event Viewer → Windows Logs → Security to analyze system events. Filters are applied to identify login failures, potential privilege escalation attempts, and system errors. Observations and findings are documented in a structured table format for report submission, reinforcing professional investigation and reporting practices.

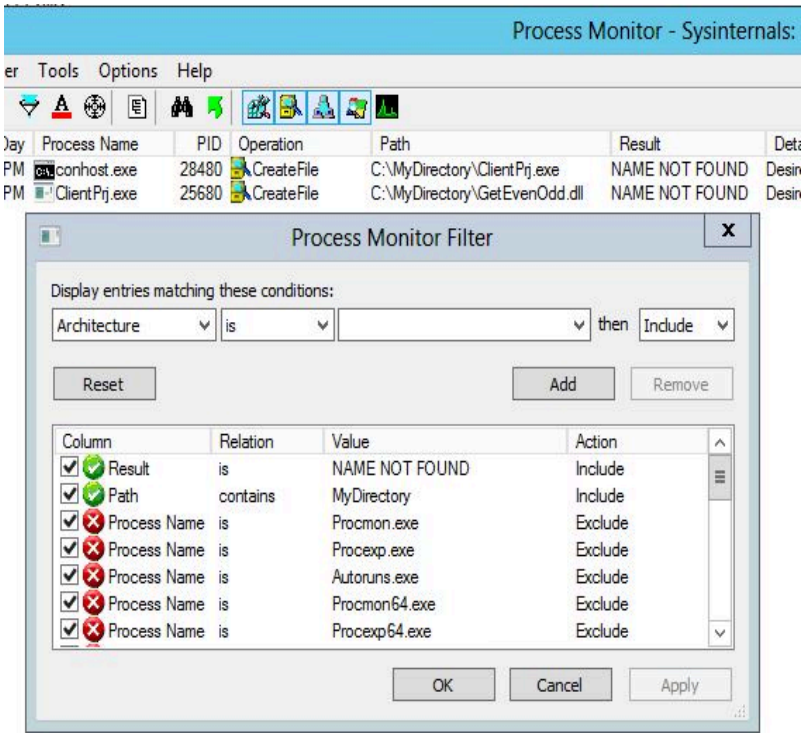


Figure 2.4: Procmon monitoring a sample process

Summary

This module provided trainees with a practical and in-depth understanding of Windows operating system security and administrative operations. Through hands-on activities and guided exercises, participants developed the ability to monitor, manage, and secure Windows-based systems effectively.By the end of this section, participants were able to :-Analyze system processes for anomalies using security and monitoring tools to identify suspicious or malicious activities.Manage user accounts and assign appropriate privilege levels, ensuring proper access control and minimizing security risks.Examine Windows event logs and registry settings to support continuous security monitoring, incident detection, and system auditing.Overall, this module strengthened the participants' ability to perform essential Windows security tasks and prepared them to handle real-world administrative and security challenges in professional environments..Overall, this module strengthened the participants' ability to perform essential Windows security tasks and prepared them to handle real-world administrative and security challenges in professional environments..Overall, this module strengthened the participants' ability to perform essential Windows security tasks and prepared them to handle real-world administrative and security challenges in professional environments..Overall, this module strengthened the participants' ability to perform essential Windows security tasks and prepared them to handle real-world administrative and security challenges in professional environments.

2.3 Networking & Network Security

Objectives :-This module aimed to provide trainees with a clear and practical understanding of networking fundamentals, network security principles, and the use of security tools to monitor, analyze, and protect network infrastructures. The module emphasized both conceptual knowledge and hands-on skills required in real-world cybersecurity environments. By the end of this section, participants were able to analyze network traffic, configure basic security devices, and simulate cyber attacks in a controlled laboratory environment to better understand attacker techniques and defensive strategies.

OSI Model (Open Systems Interconnection – 7 Layers):
The OSI model provides a conceptual framework for understanding how data moves across a network. The seven layers include Physical, Data Link, Network, Transport, Session, Presentation, and Application, each responsible for specific network functions. Understanding these layers helps in troubleshooting network issues and identifying the layer at which a security breach may occur.TCP/IP Model :-The TCP/IP model represents the practical implementation of networking used on the internet. It consists of four layers: Network Interface, Internet, Transport, and Application. This model explains how data is transmitted and routed across interconnected networks.

Network Devices :-The module also covered essential network devices such as routers, switches, firewalls, and intrusion detection/prevention systems (IDS/IPS). These devices play a crucial role in directing traffic, enforcing security policies, and detecting or preventing unauthorized network activities.This model explains how data is transmitted and routed across interconnected networks.

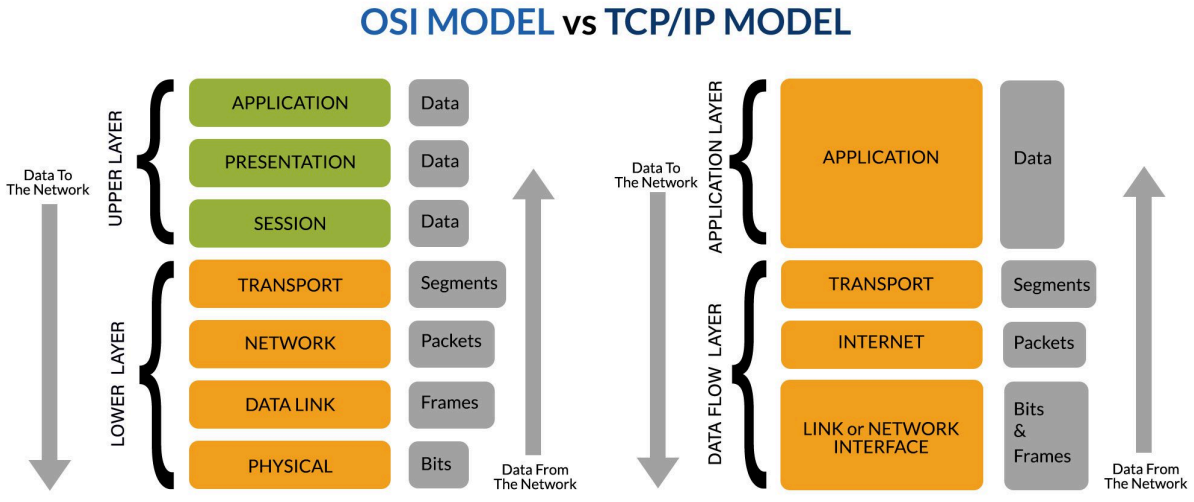


Figure 2.5: OSI and TCP/IP model diagram

TCP (Transmission Control Protocol)

TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) are transport layer protocols used for data communication over networks. Both serve different purposes based on reliability, speed, and application requirements.TCP is a connection-oriented and reliable protocol. It establishes a connection between sender and receiver before data transmission and ensures that all data packets are delivered accurately and in the correct order.Both serve different purposes based on reliability, speed, and application requirements.TCP is a connection-oriented and reliable protocol. Both serve different purposes based on reliability, speed, and application requirements.TCP is a connection-oriented and reliable protocol.

Features :-It establishes a connection between the sender and receiver using a three-way handshake before data transmission begins.TCP ensures that data is delivered accurately, completely, and in the correct order.It performs error detection and retransmission of lost or corrupted packets.TCP uses flow control and congestion control mechanisms to prevent network overload.Due to these reliability features, TCP is slower than UDP but highly dependable.TCP is commonly used in applications where data integrity is critical, such as HTTP/HTTPS, FTP, SMTP, and SSH.TCP uses flow control and congestion control mechanisms to prevent network overload.Due to these reliability features, TCP is slower than UDP but highly dependable.TCP is commonly used in applications where data integrity is critical, such as HTTP/HTTPS, FTP, SMTP, and SSH.

UDP (User Datagram Protocol)

UDP is a connectionless and unreliable protocol. It sends data without establishing a connection and does not guarantee delivery, order, or error correction, making it faster and more efficient for real-time applications..It is suitable for real-time applications where speed is more important than reliability.UDP is commonly used in video streaming, online gaming, VoIP, DNS, and live broadcasts. UDP has low latency and minimal overhead, making it faster than TCP .It is suitable for real-time applications where speed is more important than reliability.

Features :-It does not establish a connection before sending data packets.UDP does not guarantee delivery, order, or error correction of data packets.There is no retransmission of lost or corrupted packets. UDP has low latency and minimal overhead, making it faster than TCP .It is suitable for real-time applications where speed is more important than reliability.UDP is commonly used in video streaming, online gaming, VoIP, DNS, and live broadcasts.UDP has low latency and minimal overhead, making it faster than TCP.It is suitable for real-time applications where speed is more important than reliability.UDP is commonly used in video streaming, online gaming, VoIP, DNS, and live broadcasts.UDP has low latency and minimal overhead, making it faster than TCP.It is suitable for real-time applications where speed is more important than reliability.UDP is commonly used in video streaming, online gaming, VoIP, DNS, and live broadcasts.

2.3.2 Network Security Fundamentals

Overview **:-**Network security is essential to ensure the confidentiality, integrity, and availability of data in any computing environment. Protecting networks from unauthorized access, cyber attacks, and data breaches is a key responsibility for cybersecurity professionals. This module provided trainees with practical knowledge and skills to implement firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS) to secure network infrastructure effectively.

Firewalls :-Firewalls are network security devices that monitor and control incoming and outgoing traffic based on predefined rules. Key types of firewalls include:Packet Filtering: Examines individual packets and allows or blocks them based on IP addresses, ports, or protocols.Stateful Inspection: Tracks the state of active connections and makes filtering decisions based on connection context.Proxy Firewalls: Acts as an intermediary between internal users and external networks, inspecting traffic at the application layer.

IDS/IPS Concepts :-Intrusion Detection System (IDS): Monitors network traffic in real-time to identify suspicious patterns, anomalies, or known attack signatures. IDS alerts administrators but does not automatically block traffic. Intrusion Prevention System (IPS): Extends IDS functionality by detecting and automatically blocking malicious traffic to prevent attacks before they reach critical systems.

Security Monitoring :-Trainees also learned to monitor network security by configuring logging, generating alerts, and preparing reports. This includes detecting anomalies, unusual traffic patterns, and possible security breaches.

Practical Exercises :-Firewall Configuration: Set rules to allow or block specific IP addresses, ports, or protocols to control network access.Deploying IDS: Use Snort IDS to monitor network traffic for malicious patterns and potential attacks.Simulated Attacks: Generate controlled cyber attacks in the lab environment and observe IDS/IPS responses.

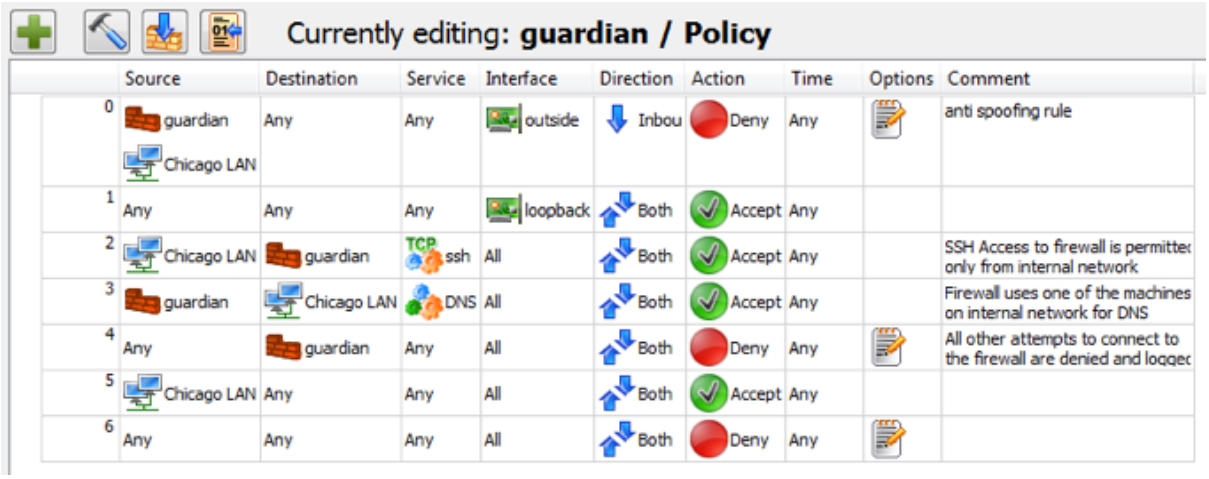


Figure 2.6: Example firewall configuration interface

Intrusion Detection System (IDS :-) is a network security tool designed to monitor network traffic and system activities for suspicious behavior, policy violations, or known attack patterns. It works by analyzing incoming and outgoing traffic and comparing it against a database of known threats or abnormal patterns. IDS generates alerts to notify administrators when potential security incidents are detected but does not take automatic action to block the threat. This makes IDS a valuable tool for identifying intrusions, conducting forensic analysis, and improving overall network security posture.It works by analyzing incoming and outgoing traffic and comparing it against a database of known threats or abnormal patterns. IDS generates alerts to notify administrators when potential security incidents are detected but does not take automatic action to block the threat. This makes IDS a valuable tool for identifying intrusions, conducting forensic analysis, and improving overall network security posture.IPS can automatically block malicious traffic, drop harmful packets, or terminate sessions that exhibit signs of an attack. It is deployed inline within the network so that all traffic passes through it, enabling real-time threat mitigation. By combining detection and prevention, IPS helps reduce the risk of data breaches, service disruption, and other cyber threats while maintaining network integrity and availability.It is deployed inline within the network so that all traffic passes through it, enabling real-time threat mitigation. By combining detection and prevention, IPS helps reduce the risk of data breaches, service disruption, and other cyber threats while maintaining network integrity and availability.

Intrusion Prevention System (IPS) :- builds on the capabilities of IDS by not only detecting suspicious activities but also taking **proactive measures to prevent attacks**. IPS can automatically block malicious traffic, drop harmful packets, or terminate sessions that exhibit signs of an attack. It is deployed inline within the network so that all traffic passes through it, enabling real-time threat mitigation. By combining detection and prevention, IPS helps reduce the risk of data breaches, service disruption, and other cyber threats while maintaining network integrity and availability.IPS can automatically block malicious traffic, drop harmful packets, or terminate sessions that exhibit signs of an attack. It is deployed inline within the network so that all traffic passes through it, enabling real-time threat mitigation. By combining detection and prevention, IPS helps reduce the risk of data breaches, service disruption, and other cyber threats while maintaining network integrity and availability.IPS can automatically block malicious traffic, drop harmful packets, or terminate sessions that exhibit signs of an attack. It is deployed inline within the network so that all traffic passes through it, enabling real-time threat mitigation. By combining detection and prevention, IPS helps reduce the risk of data breaches, service disruption, and other cyber threats while maintaining network integrity and availability.It is deployed inline within the network so that all traffic passes through it, enabling real-time threat mitigation. By combining detection and prevention, IPS helps reduce the risk of data breaches, service disruption, and other cyber threats while maintaining network integrity and availability.

2.3.3 Network Security Best Practices

Key Concepts :- To maintain a secure network environment, it is essential to use strong, complex passwords for routers, administrative accounts, and other critical devices to prevent unauthorized access. Enabling logging on all security devices is crucial for monitoring network activity, detecting anomalies, and investigating potential security incidents. Additionally, network segmentation helps limit exposure by isolating critical systems and sensitive data from less secure parts of the network, reducing the impact of any potential breach. Finally, it is important to regularly update firmware and apply security patches to all network devices and software, ensuring that known vulnerabilities are addressed and systems remain protected against emerging threats.

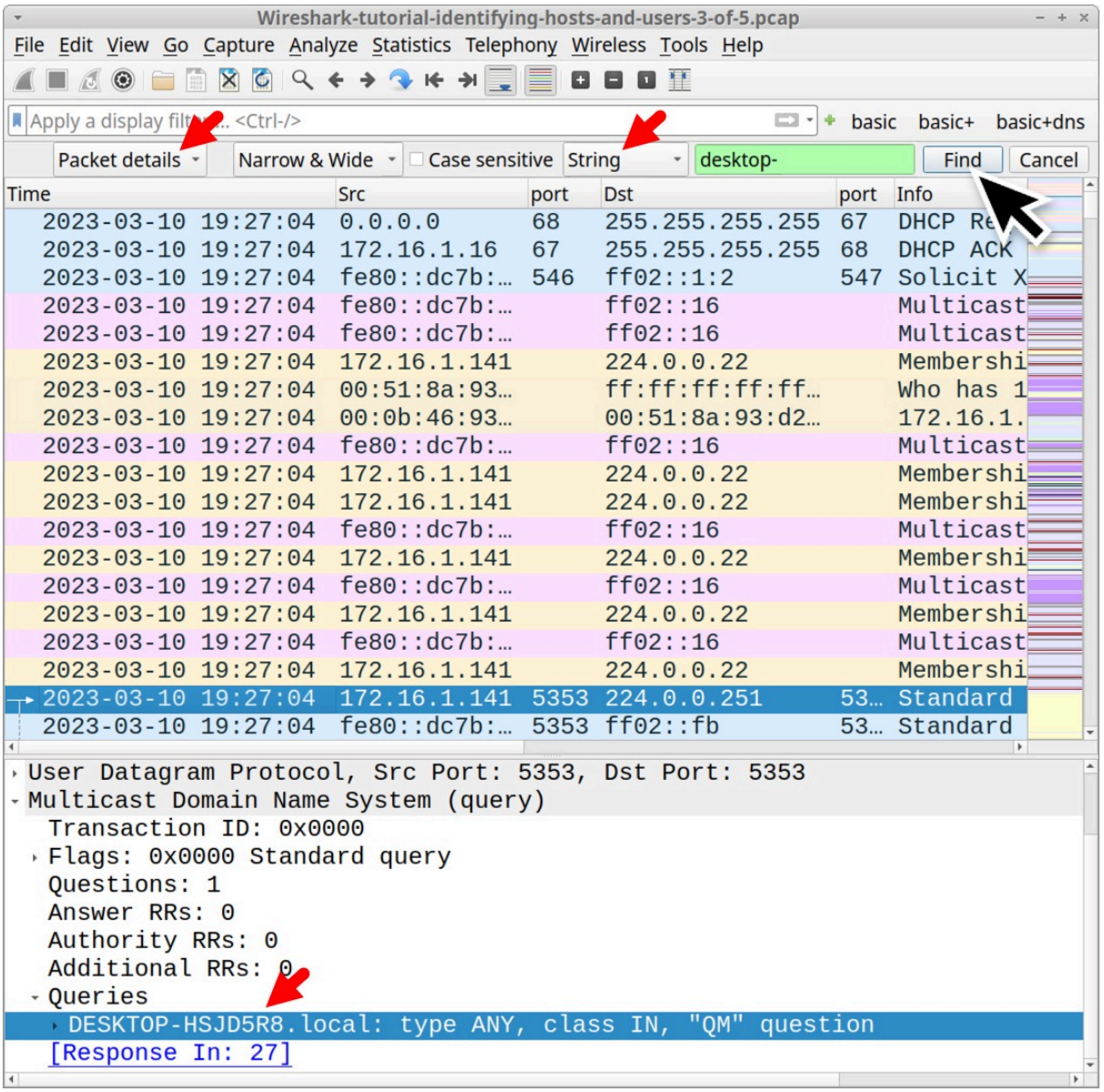


Figure 2.7: Wireshark packet capture

Summary of Networking and Network Security Module

This module provided trainees with a practical and comprehensive foundation in networking principles and network security concepts. It began with an in-depth study of the OSI and TCP/IP models, which form the basis of understanding how data flows through a network. Trainees explored the seven layers of the OSI model—Physical, Data Link, Network, Transport, Session, Presentation, and Application—as well as the four layers of the TCP/IP model. By understanding these models, participants were able to grasp the roles of various protocols and services, such as IP, TCP, UDP, HTTP, HTTPS, and DNS, in ensuring effective and secure network communication.An essential part of the module was network traffic analysis using Wireshark, a widely used packet-sniffing tool. Trainees learned how to capture live network traffic, filter packets by protocols, analyze packet headers, and identify abnormal patterns that could indicate security threats. This hands-on experience enabled participants to understand how data traverses a network, detect suspicious activities, and gain insights into potential vulnerabilities or misconfigurations in real-world network environments.

The module also emphasized practical implementation of security measures, including firewall configuration and the deployment of Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS). Trainees were guided to create rules for allowing or blocking specific IP addresses, ports, and protocols, as well as monitor network traffic to detect malicious patterns. This practical exposure helped participants understand how to prevent unauthorized access, detect attacks in real-time, and take corrective actions to protect critical network resources.Overall, this module strengthened trainees' ability to analyze, monitor, and secure network infrastructures. By combining theoretical knowledge with hands-on exercises, participants gained confidence in identifying network vulnerabilities, implementing protective measures, and using professional tools to maintain a secure environment. The skills acquired in this module provide a strong foundation for advanced study in cybersecurity, as well as practical expertise applicable to real-world network security operations.

An essential part of the module was network traffic analysis using Wireshark, a widely used packet-sniffing tool. Trainees learned how to capture live network traffic, filter packets by protocols, analyze packet headers, and identify abnormal patterns that could indicate security threats. This hands-on experience enabled participants to understand how data traverses a network, detect suspicious activities, and gain insights into potential vulnerabilities or misconfigurations in real-world network environments.This hands-on experience enabled participants to understand how data traverses a network, detect suspicious activities, and gain insights into potential vulnerabilities or misconfigurations in real-world network environments.This hands-on experience enabled participants to understand how data traverses a network, detect suspicious activities, and gain insights into potential vulnerabilities or misconfigurations in real-world network environments.This hands-on experience enabled participants to understand how data traverses a network, detect suspicious activities, and gain insights into potential vulnerabilities or misconfigurations.

2.4 Cryptography and Wireless Security

Objectives :-The objective of this module was to introduce trainees to encryption techniques for data security and methods for securing wireless networks. By the end of the section, participants were able to implement encryption mechanisms, configure secure Wi-Fi networks, and detect potential wireless threats, ensuring that sensitive information remains protected from unauthorized access.By the end of the section, participants were able to implement encryption mechanisms, configure secure Wi-Fi networks, and detect potential wireless threats, ensuring that sensitive.

2.4.1 Cryptography :-Cryptography is the science of protecting data by converting it into unreadable formats, thereby ensuring confidentiality, integrity, and authenticity. It provides a foundation for secure communication in digital systems and is widely used in networking, email, and file storage. Cryptography can be broadly classified into symmetric and asymmetric encryption techniques. Symmetric encryption uses a single key for both encryption and decryption, making it fast and efficient for handling large volumes of data. A common example of this is the Advanced Encryption Standard (AES), which can be used to encrypt files and share the same key with authorized recipients for decryption. On the other hand, asymmetric encryption employs a pair of keys—a public key for encryption and a private key for decryption. This approach allows secure communication without the need to share the private key, making it suitable for applications such as email encryption. A widely used algorithm in this category is RSA (Rivest-Shamir-Adleman), which ensures that only the intended recipient can decrypt and access the information, thereby maintaining the privacy and security of communications.

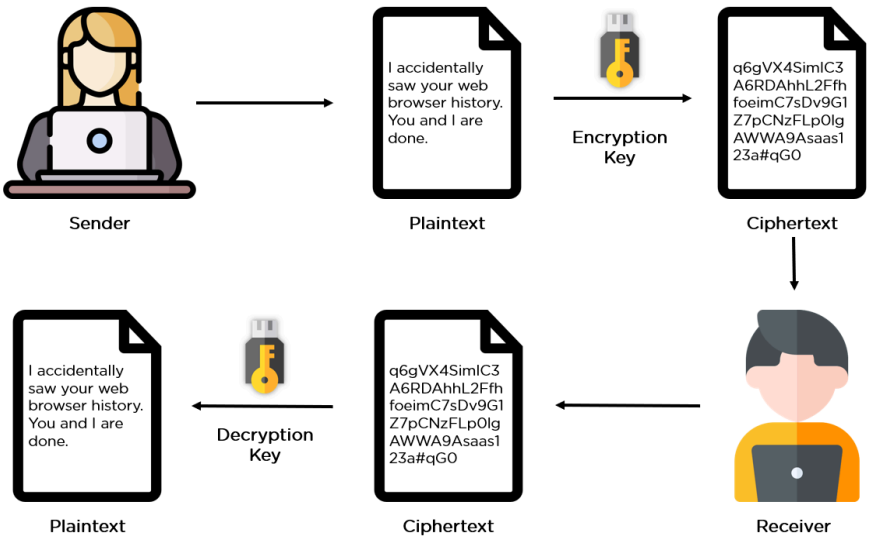


Figure 2.8 : Sample encrypted vs decrypted data

Table 2.3: Comparison of Encryption Algorithms

Algorithm	Type	Key size	speed	Security level	Use case
AES	Symmetric	128,192,256	Fast	High	File encryption, VPN
RSA	Asymmetric	1024,2048,4096	Moderate	Very high	Email encryption, Digital signatures
SHA-256	Hash	N/A	Fast	High	Data integrity, Password storage

2.4.2 Wireless Security

Wireless networks are inherently vulnerable due to their open transmission medium, which allows signals to be intercepted more easily than wired networks. Securing Wi-Fi networks is therefore critical to prevent unauthorized access, data theft, and potential compromise of sensitive information. Trainees were introduced to wireless security protocols such as WPA2 (Wi-Fi Protected Access 2), which provides strong encryption using AES, and WPA3, the latest protocol offering enhanced encryption, forward secrecy, and improved protection against brute-force attacks. Understanding these protocols helps ensure that wireless communications remain secure in both personal and organizational environments.

Another important aspect of wireless security covered in this module was the detection of rogue access points. Rogue APs are unauthorized devices attempting to mimic legitimate Wi-Fi networks to trick users into connecting, potentially exposing sensitive data. Trainees learned to identify such threats using tools like Wi-Fi scanners and network monitoring utilities. Practical steps included scanning networks, checking MAC addresses, and validating access points against known infrastructure to ensure that only authorized devices are allowed access to the network.

The module also emphasized hands-on practical exercises to reinforce theoretical concepts. Participants practiced encrypting and decrypting files using both AES (symmetric) and RSA (asymmetric) encryption methods to secure data. They also configured a secure Wi-Fi network with WPA3 encryption, assigned strong passwords, and enabled MAC filtering for additional protection. Finally, trainees used tools such as Kismet and NetS.

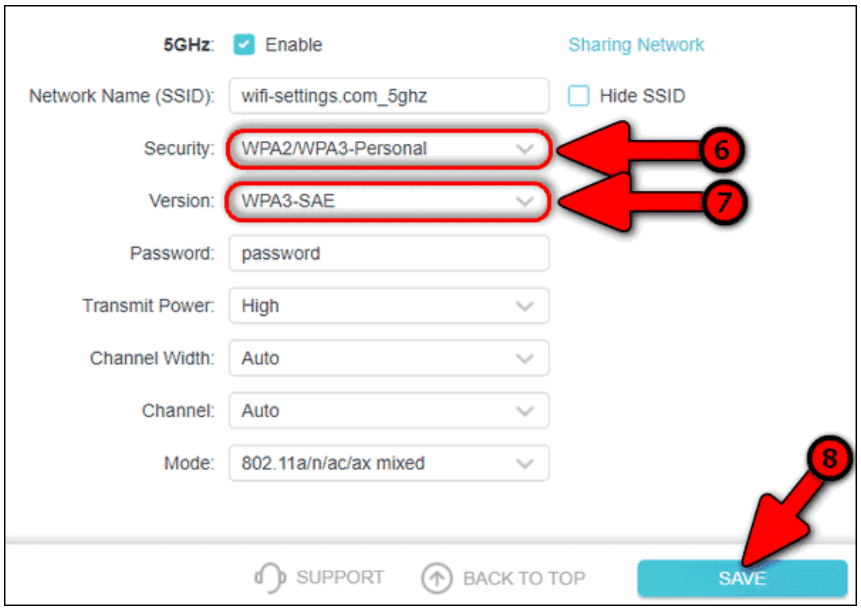


Figure 2.9: Screenshot of WPA3 secured network configuration

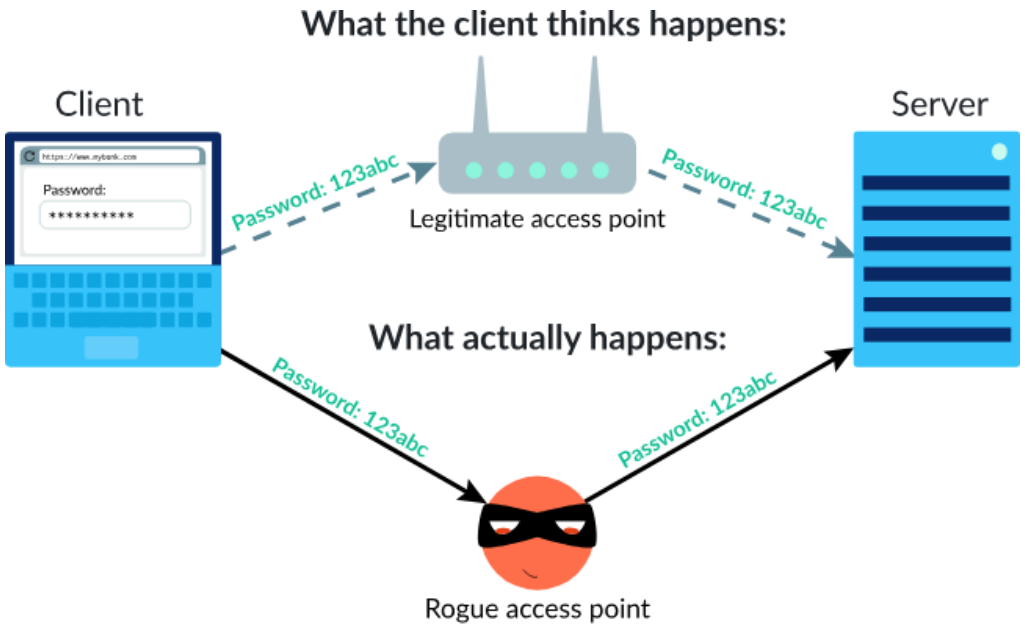


Figure 2.10: Example scan detecting a rogue access point

2.5 Vulnerability Assessment and Penetration Testing

2.5.1 Vulnerability Assessment

Objectives and topics covered :- The objective of this module was to enable trainees to identify, analyze, and classify vulnerabilities in computer systems and networks. Participants learned about Common Vulnerabilities and Exposures (CVE) and the Common Vulnerability Scoring System (CVSS), which provide standardized methods for identifying and rating the severity of security flaws. The module also introduced various vulnerability scanning tools such as Nessus, OpenVAS, and Qualys, which are widely used by cybersecurity professionals to detect potential weaknesses and assess the overall security posture of systems. Additionally, trainees gained knowledge about reporting and risk assessment, learning how to communicate findings effectively and recommend remediation strategies based on severity and impact.

Practical Exercises :-In the practical exercises, trainees performed vulnerability scans on lab machines using the aforementioned tools, analyzing the generated reports to identify and document security gaps. They practiced prioritizing vulnerabilities according to their CVSS scores, which helped in understanding which issues required immediate attention and which could be addressed later. These hands-on activities provided participants with the skills to conduct systematic vulnerability assessments, interpret results accurately, and make informed decisions for mitigating risks in real-world environments.

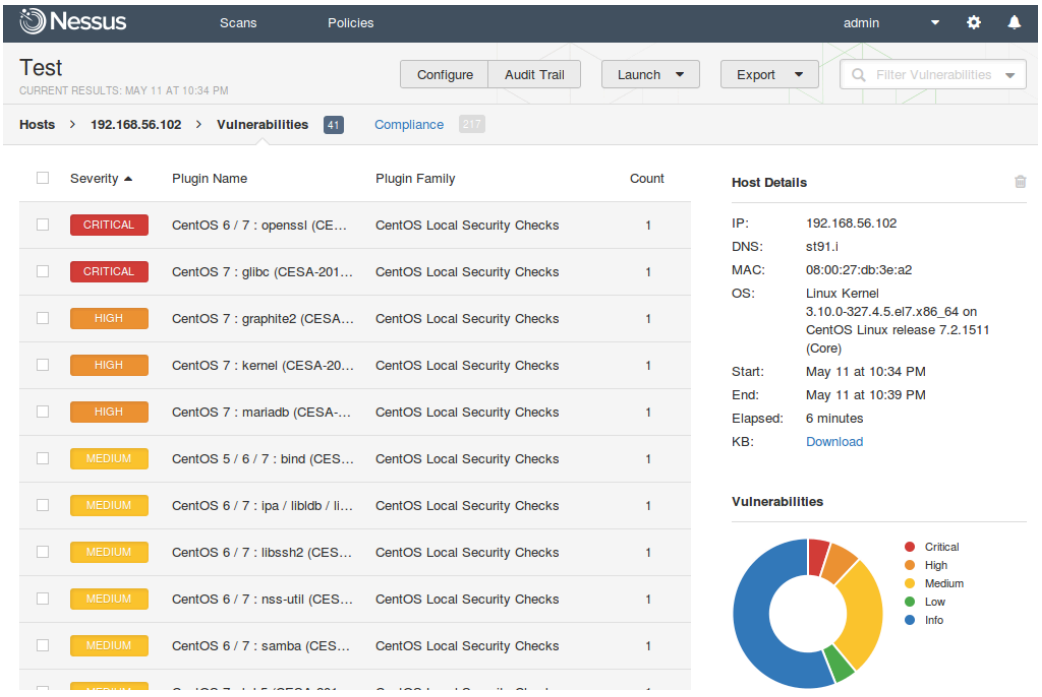


Figure 2.11: Nessus scan report screenshot

2.5.2 Penetration Testing

Objectives :-The objective of this module was to equip trainees with the skills to perform controlled and ethical attacks on systems and networks in order to test their defenses. Participants learned the importance of penetration testing as a proactive approach to identify security weaknesses before attackers can exploit them. The module emphasized adherence to ethical hacking guidelines, ensuring that all testing is conducted legally, safely, and in a controlled environment.

TopicsCovered :-The training covered the phases of penetration testing, including reconnaissance, where trainees gathered information about target systems; scanning, to identify open ports, services, and vulnerabilities; and exploitation, where controlled attacks were executed to test system defenses. Participants also became familiar with widely used penetration testing tools such as Nmap for network reconnaissance, Metasploit for exploiting vulnerabilities, and Burp Suite for assessing web application security.

Practical Exercises :-In the practical exercises, trainees conducted network reconnaissance using Nmap to map networks and detect open ports or services. They then used Metasploit in controlled lab environments to exploit identified vulnerabilities safely and observe system responses.

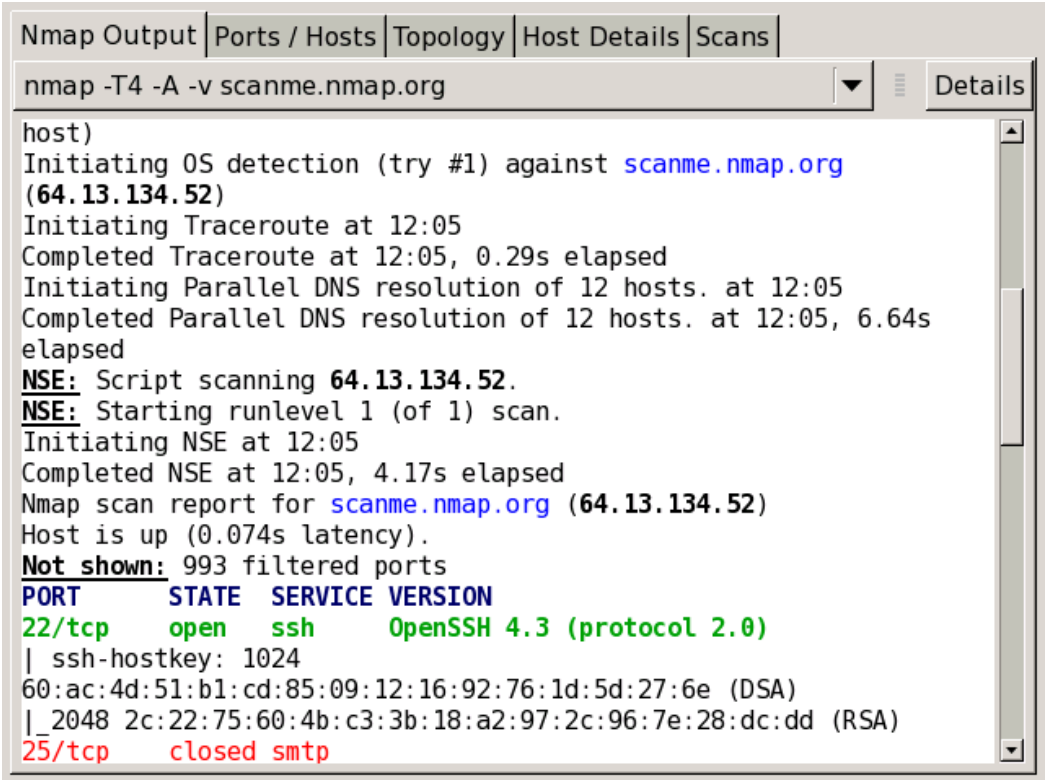


Figure 2.12: Nmap scan output

Table 2.4 : Metasploit commands with description

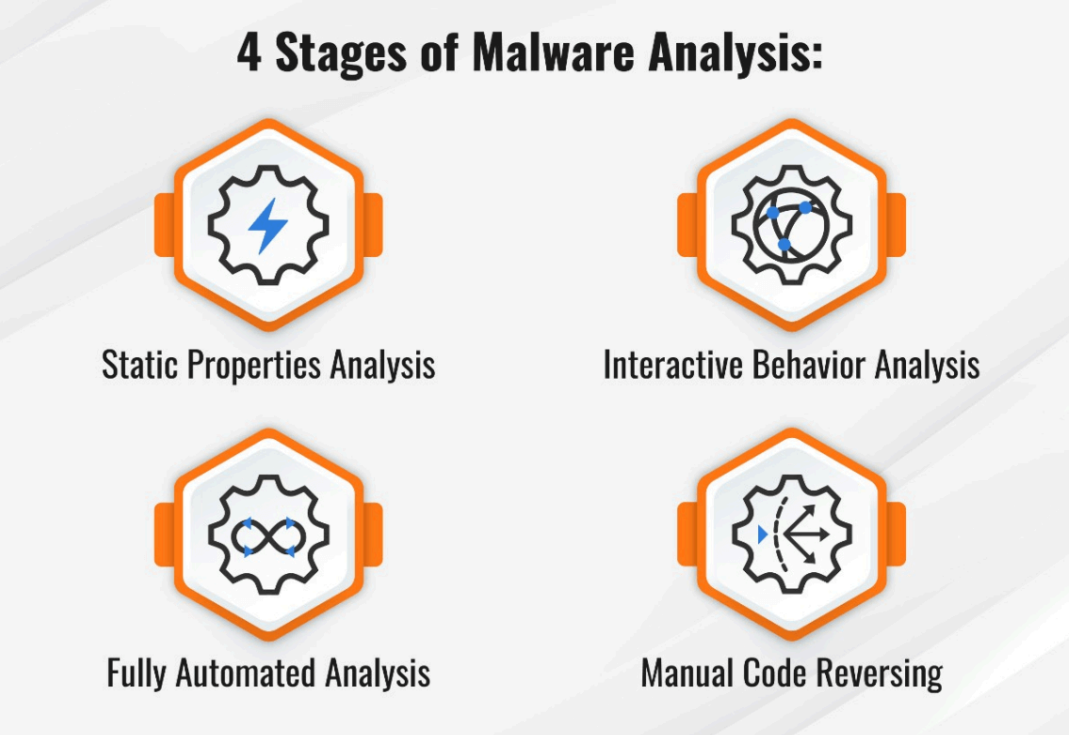
S.No.	Command / Context	Description	Example / Notes
1	msfconsole	Launches the Metasploit Framework interactive console.	msfconsole
2	search	Searches exploit/payload/module names and descriptions in the module database.	search type:exploit name:tomcat
3	use	Loads a specific module (exploit/auxiliary/post).	use exploit/windows/smb/ms17_010_eternalblue
4	info	Shows detailed information about the currently selected module.	info
5	Show options	Displays configurable options (RHOST, RPORT, payload, etc.) for the selected module.	show options
6	set	Sets a module option or payload option (e.g., RHOST, LHOST).	set RHOST 192.168.1.10
7	Exploit / run	Executes the currently configured exploit against the target. run is an alias.	Exploit or run

2.6 Incident Response and Malware Analysis

Objectives:-The objective of this module was to train participants to respond effectively to security incidents and conduct malware analysis to understand threats. Trainees learned the significance of a structured approach to incident response, which helps minimize damage, restore systems efficiently, and prevent future attacks. The module emphasized practical skills for identifying, analyzing, and mitigating security threats in controlled and safe environments.

Topics Covered :-Participants were introduced to the incident response lifecycle, which includes preparation, detection, containment, and recovery. They also learned about various types of malware, such as viruses, trojans, and ransomware, which can compromise system integrity, steal data, or disrupt operations. The module covered static and dynamic malware analysis techniques, enabling trainees to examine malicious software without executing it, as well as observing its behavior in an isolated environment to understand its impact.

Practical Exercises :-In practical exercises, participants analyzed malware samples in a controlled lab environment, carefully documenting detection methods and mitigation steps. They also practiced creating a basic incident response plan for a simulated cyberattack, which included identification of the threat, containment measures, system recovery procedures, and post-incident reporting. These exercises provided hands-on experience in both technical analysis and procedural response, equipping trainees with the foundational skills required to handle real-world cybersecurity incidents.



F **Figure 2.13:** Malware analysis workflow

2.7 Digital Forensics

Objectives :-The objective of this module was to equip trainees with the skills to collect, preserve, and analyze digital evidence in a forensically sound manner. Participants learned the importance of adhering to proper procedures during evidence handling to ensure that collected data remains admissible in legal or investigative contexts. The module emphasized both theoretical knowledge and practical application of digital forensics techniques.

Topics Covered :-Trainees were introduced to the chain of custody, which documents the handling of evidence from collection to analysis and storage, ensuring that its integrity is maintained. They also learned evidence collection procedures, including proper identification, preservation, and documentation of digital artifacts. The module covered the use of professional forensic tools such as FTK Imager and EnCase, which enable secure acquisition and analysis of digital data from storage devices, memory, and other digital sources.

Practical Exercises :-In practical exercises, participants captured disk images using FTK Imager, ensuring that the original data remained unaltered. They also practiced recovering deleted files and analyzing them to extract relevant information. Throughout the exercises, trainees maintained detailed logs documenting their findings and chain of custody, reinforcing best practices for evidence integrity and accountability. These hands-on activities provided essential experience in applying forensic principles to real-world scenarios, preparing participants for professional work in digital investigations.

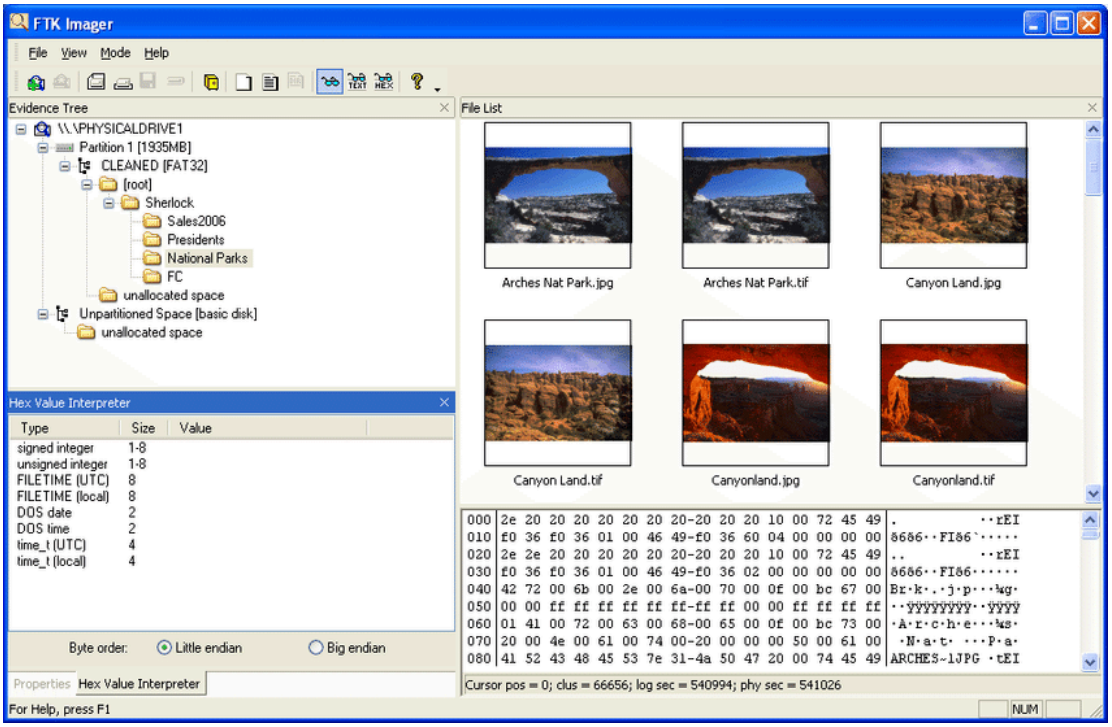


Figure 2.14 : FTK Imager screenshot

Table 2.5: Evidence collection checklist

S.No	Evidence Type	Description / Purpose	Collection Method / Tool	Notes / Remarks
1	Hard Drives / Storage Media	Physical drives containing system data, documents, logs	Disk imaging using **FTK Imager, dd, EnCase**	Create **forensic image**; verify hash
2	RAM / Memory	Volatile memory containing running processes, malware	Memory dump using **FTK Imager, Volatility**	Capture before system shutdown
3	System Logs	Event logs, security logs, application logs	Export from **Event Viewer, Linux /var/log**	Document timestamp and source
4	Network Traffic	Packets for analysis of attacks	Capture using **Wireshark, tcpdump**	Store in PCAP format
5	Emails / Messages	Communications relevant to the investigation	Export from email client or server	Include headers, attachments
6	USB / Removable Devices	Portable storage containing evidence	Copy contents, create hash value	Maintain chain of custody
7	System Configuration	Registry, user accounts, firewall settings	Export using **regedit, command-line tools**	Take screenshots of critical settings

2.8 Mobile, IoT, and Cloud Security

Objectives :-The objective of this module was to provide trainees with an understanding of modern security challenges associated with mobile devices, Internet of Things (IoT) systems, and cloud computing platforms. Participants explored the unique risks and vulnerabilities inherent to these environments and learned strategies to protect data, applications, and devices from unauthorized access, exploitation, and other cyber threats.

Topics Covered :-In the mobile security section, trainees studied Android and iOS operating systems, learning about security mechanisms, common vulnerabilities, and best practices for securing applications and devices. The IoT security portion focused on identifying vulnerabilities in connected devices, such as weak authentication, unpatched firmware, and insecure communication protocols, which can be exploited to gain unauthorized access or disrupt services. The cloud security section introduced models such as IaaS, PaaS, and SaaS, and key security concepts including Identity and Access Management (IAM) and Multi-Factor Authentication (MFA), emphasizing strategies for protecting cloud resources and sensitive data.

Practical Exercises :-Practical exercises enabled trainees to test a mobile application for security flaws, scan IoT devices to detect vulnerabilities, and configure secure IAM and MFA settings in a cloud lab environment. These hands-on activities provided essential experience in applying security principles across emerging technology platforms, preparing participants to address real-world security challenges in mobile, IoT, and cloud environments.

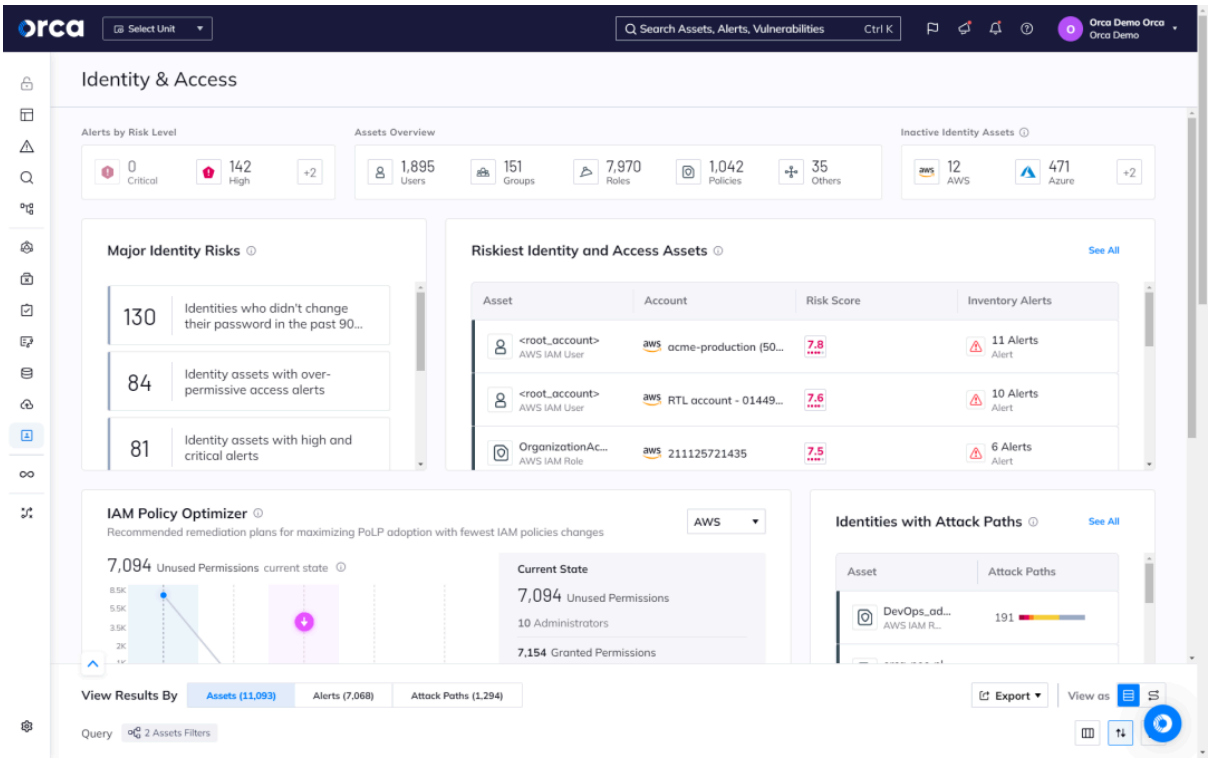


Figure 2.15: Evidence collection checklist

2.9 Defensive Security and Hardening

Objectives :-The objective of this module was to understand and implement proactive defense mechanisms designed to protect systems and networks before attacks occur. Defensive security involves adopting a preventive approach to minimize vulnerabilities, enhance monitoring capabilities, and ensure rapid detection and response to potential threats.

System hardening focuses on reducing the attack surface by eliminating unnecessary services, applying security patches, enforcing access controls, and ensuring proper configuration of operating systems, networks, and applications.System hardening focuses on reducing the attack surface by eliminating unnecessary services, applying security patches, enforcing access controls, and ensuring proper configuration of operating systems, networks, and applications.

Operating System Hardening (Linux and Windows) :-Operating System (OS) hardening is the process of securing an operating system by minimizing its vulnerabilities. It involves configuring system settings, controlling user privileges, and ensuring that only essential services are enabled.The cloud security section introduced models such as IaaS, PaaS, and SaaS, and key security concepts including Identity and Access Management (IAM) and Multi-Factor Authentication (MFA), emphasizing strategies for protecting cloud resources and sensitive data.System hardening focuses on reducing the attack surface by eliminating unnecessary services, applying security patches, enforcing access controls, and ensuring proper configuration of operating systems, networks, and applications.

- **Patch Management:** Regularly updating the operating system and installed software to fix security vulnerabilities.
- **Firewall Configuration:** Enabling Windows Defender Firewall or Linux iptables/ufw for traffic filtering
- **User Account Management:** Creating least-privilege user accounts and disabling unused or default accounts.
- **Service Optimization:** Disabling unnecessary background services that could be exploited by attackers.
- **File and Directory Permissions:** Configuring appropriate access rights for users and groups to prevent unauthorized modifications.
- **Firewall Configuration:** Enabling Windows Defender Firewall or Linux iptables/ufw for traffic filtering.
- **Audit and Logging:** Configuring audit policies to record user activities, failed login attempts, and configuration changes.
- **Antivirus and Endpoint Protection:** Installing and maintaining updated antivirus software for real-time protection.

  On Linux systems, tools like chown, chmod, and iptables were utilized for access control and network rule configuration. On Windows systems, Group Policy Editor, Windows Security Center, and PowerShell commands were applied to strengthen system security.

2. Network Security Hardening (VPNs and Firewalls)

Network hardening focuses on strengthening the security posture of network devices, routers, and firewalls to protect data in transit and prevent unauthorized access. Trainees learned several key concepts to achieve this objective. Virtual Private Networks (VPNs) were configured to create encrypted tunnels between remote clients and corporate networks, ensuring secure communication even over untrusted networks. Firewall rules were implemented to control inbound and outbound traffic, specifying which applications or ports were allowed or blocked. Network segmentation was covered as a strategy to divide large networks into smaller subnets, limiting the impact of potential breaches. Participants also explored Intrusion Prevention Systems (IPS) to detect and automatically block suspicious traffic patterns, as well as the importance of using secure protocols, replacing insecure protocols like FTP and Telnet with SSH and SFTP for safer data transmission.

In the practical exercises, trainees applied these concepts hands-on by creating custom firewall policies using iptables, verifying rule implementation with commands such as `ufw status`, and testing VPN configurations to ensure proper encryption and tunneling functionality. These activities provided participants with the skills to harden network infrastructure, control access, and protect sensitive data against real-world cyber threats.

3. Threat Hunting Basics using EDR and SIEM Tools

Threat hunting is the proactive practice of searching for indicators of compromise (IOCs) within networks or systems before automated tools can detect them. This process combines analytical thinking with threat intelligence to uncover hidden or stealthy attacks that may bypass traditional security defenses. Trainees were introduced to several key components that support effective threat hunting. Endpoint Detection and Response (EDR) tools, such as Microsoft Defender for Endpoint and CrowdStrike Falcon, monitor endpoint activities, detect anomalies, and assist in response actions like isolating infected devices. Security Information and Event Management (SIEM) platforms, including Splunk and IBM QRadar, aggregate logs from multiple sources, correlate events, and generate alerts for suspicious behaviors. Additionally, integrating threat intelligence feeds provides real-world attack patterns and indicators from open-source intelligence to enhance detection capabilities.

The module also emphasized the importance of following a structured incident response workflow, which includes identifying, analyzing, containing, and eradicating threats from affected systems. Trainees learned how threat hunting is closely linked to incident response, helping organizations respond faster and mitigate the impact of cyber attacks. Hands-on activities included simulating log monitoring using Wazuh, an open-source SIEM tool, and identifying suspicious activities such as unusual PowerShell commands or repeated failed login attempts in Windows Event Logs.

Practical Exercises :-The practical exercises for this module focused on applying network hardening, monitoring, and threat hunting techniques on lab machines. Trainees began by implementing hardening measures, such as disabling unused services and user accounts, enforcing password complexity and account lockout policies, and configuring firewalls along with automatic updates to ensure system resilience. These activities reinforced the importance of securing endpoints and minimizing potential attack surfaces.

Participants also learned to monitor network traffic for suspicious activity using tools like Wireshark to capture and analyze network packets, identifying anomalies that could indicate security threats. In addition, they configured IDS rules to generate alerts on unauthorized access attempts, gaining hands-on experience in real-time detection of potential attacks and understanding how intrusion detection systems support overall network security.
Finally, trainees practiced documenting threat hunting steps and outcomes, recording identified Indicators of Compromise (IOCs), and documenting mitigation actions taken during exercises. This process helped develop the ability to maintain detailed logs, analyze patterns, and learn from each scenario, thereby improving preparedness for real-world cybersecurity incidents and ensuring continuous improvement in organizational security practices.

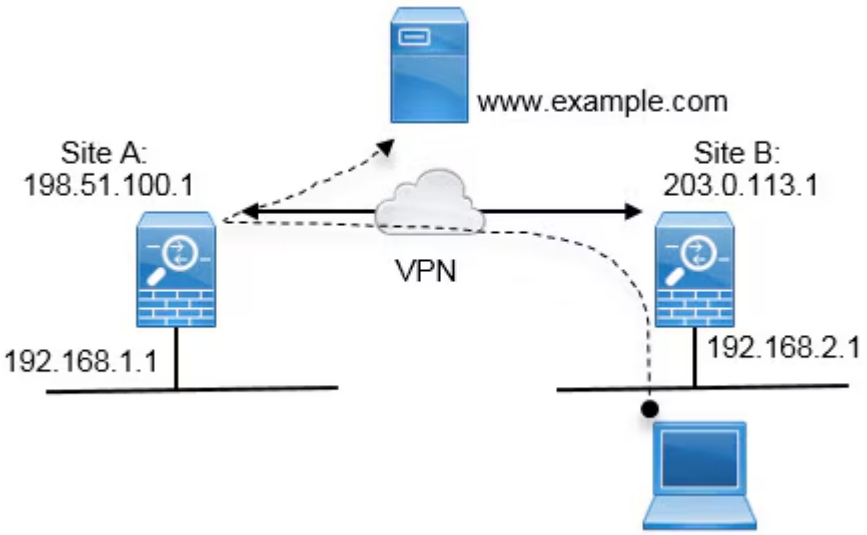


Figure 2.16: Example VPN configuration

Conclusion -Defensive security and hardening represent a crucial layer in cybersecurity defense. Through this training, participants gained practical exposure to securing systems and networks, monitoring endpoints, and understanding proactive defense mechanisms. The knowledge and hands-on practice provided the foundation to anticipate and counter cyber threats effectively in real-world environments.

2.10 Summary of Training Work

The training program offered a comprehensive and structured learning path, guiding participants from foundational cybersecurity concepts to advanced defensive and offensive techniques. Trainees gained both theoretical knowledge and hands-on experience with Linux and Windows operating systems, including system administration, security configurations, and process monitoring. The program also covered network configurations, vulnerability assessments, and penetration testing, equipping participants with the skills to identify, analyze, and remediate potential security weaknesses in real-world environments.
security configurations, and process monitoring. The program also covered network configurations, vulnerability assessments, and penetration testing, equipping participants with the skills to identify, analyze, and remediate potential security weaknesses in real-world environments.security configurations, and process monitoring. The program also covered network configurations, vulnerability assessments, and penetration testing, equipping participants with the skills to identify, analyze, and remediate potential security weaknesses in real-world environments.

In addition to system and network security, the training provided practical exposure to malware analysis, incident response, and threat hunting, enabling participants to understand attack methodologies, detect malicious activity, and respond effectively to security incidents. Trainees also learned to implement hardening measures, configure firewalls, monitor network traffic, and apply defensive security strategies, ensuring systems remained resilient against unauthorized access and cyber threats. to security incidents. Trainees also learned to implement hardening measures, configure firewalls, monitor network traffic, and apply defensive security strategies, ensuring systems remained resilient against unauthorized access and cyber threats. to security incidents. Trainees also learned to implement hardening measures, configure firewalls, monitor network traffic, and apply defensive security strategies, ensuring systems remained resilient against unauthorized access and cyber threats.

By the end of the program, participants were confident in operating securely within both Linux and Windows environments, conducting thorough vulnerability scans and penetration tests, performing malware analysis and incident response, and applying defensive measures to strengthen overall security posture. The combination of theory, hands-on labs, and practical exercises provided a solid foundation for pursuing further studies or professional roles in cybersecurity.The combination of theory, hands-on labs, and practical exercises provided a solid foundation for pursuing further studies or professional roles in cybersecurity.
The combination of theory, hands-on labs, and practical exercises provided a solid foundation for pursuing further studies or professional roles in cybersecurity.The combination of theory, hands-on labs, and practical exercises provided a solid foundation for pursuing further studies or professional roles in cybersecurity.

CHAPTER 3 – RESULTS AND DISCUSSION

3.1 Overview

This chapter presents the outcomes of the practical sessions conducted during the one-month cybersecurity training program. Each exercise and experiment was designed to provide hands-on exposure to cybersecurity tools, network analysis, vulnerability assessment, and ethical hacking fundamentals.The results reflect the understanding of concepts explained in earlier chapters and demonstrate the ability to apply theoretical knowledge to real-world scenarios.

3.2 Network Scanning and Enumeration (Nmap Results)

Objective :-The objective of this exercise was to identify active hosts, open ports, and running services on a target network using Nmap, a widely used network scanning tool. Trainees employed both Nmap command-line utility and its GUI counterpart Zenmap, along with Wireshark for network traffic analysis, to gain a comprehensive understanding of the network's structure and potential vulnerabilities.

Tools used :-The procedure began with a basic scan to detect live hosts within the subnet by executing the command `nmap -sP 192.168.1.0/24`. This scan revealed multiple active devices on the local network. Next, a service version detection scan was performed using `nmap -sV 192.168.1.10`, which allowed trainees to identify open ports and the versions of the services running on those ports. Finally, an advanced scan incorporating OS detection and vulnerability assessment was conducted using the command `nmap -A -T4 192.168.1.10`, providing detailed information about the target system.

Procedure :-Observations from the scans indicated that several devices were active within the local subnet. Specific hosts had ports 22 (SSH), 80 (HTTP), and 445 (SMB) open, exposing potential entry points for attackers. Additionally, version detection revealed that some hosts were running outdated Apache server software, highlighting a possible vulnerability that would require patching or mitigation. This exercise provided trainees with practical experience in network enumeration, identifying vulnerabilities, and understanding how attackers might gather information for reconnaissance.

Observations :-Observations from the scans indicated that several devices were active within the local subnet. Specific hosts had ports 22 (SSH), 80 (HTTP), and 445 (SMB) open, exposing potential entry points for attackers. Additionally, version detection revealed that some hosts were running outdated Apache server software, highlighting a possible vulnerability that would require patching or mitigation. This exercise provided trainees with practical experience in network enumeration, identifying vulnerabilities, and understanding how attackers might gather information for reconnaissance.

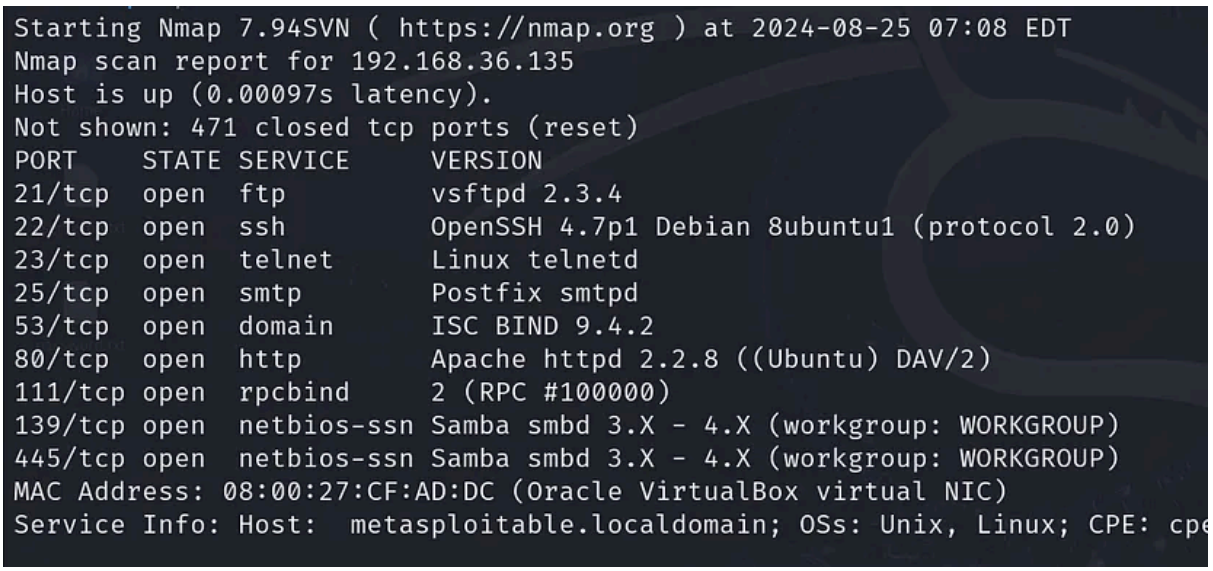


Figure 3.1: Sample Nmap Scan Output

3.3 Packet Capture and Analysis (Wireshark)

Objective :-The objective of this exercise was to analyze live network traffic and identify potential anomalies or malicious packets using Wireshark, a widely used network protocol analyzer. Trainees launched Wireshark and initiated packet capture on an active network interface, such as eth0 or Wi-Fi, to monitor real-time network activity. Filters were applied to focus on specific protocols including HTTP, DNS, and TCP, allowing for detailed inspection of relevant traffic and identification of unusual patterns.

Tools Used :-During the analysis, trainees carefully inspected captured packets for suspicious payloads, abnormal retransmissions, or repeated connection attempts that could indicate network issues or potential security threats. Observations showed that DNS requests reflected normal browsing activity, with typical domain resolutions occurring without anomalies. Some TCP retransmissions were noted, which suggested minor packet loss within the network, a common occurrence in routine communication.

Procedure :-No malicious activity was detected during the capture period; specifically, there were no suspicious IP addresses or ARP spoofing attempts, indicating that the network was functioning normally and securely. This exercise provided trainees with hands-on experience in monitoring network traffic, interpreting protocol-level information, and understanding how packet-level analysis can be used to detect both performance issues and potential security incidents.

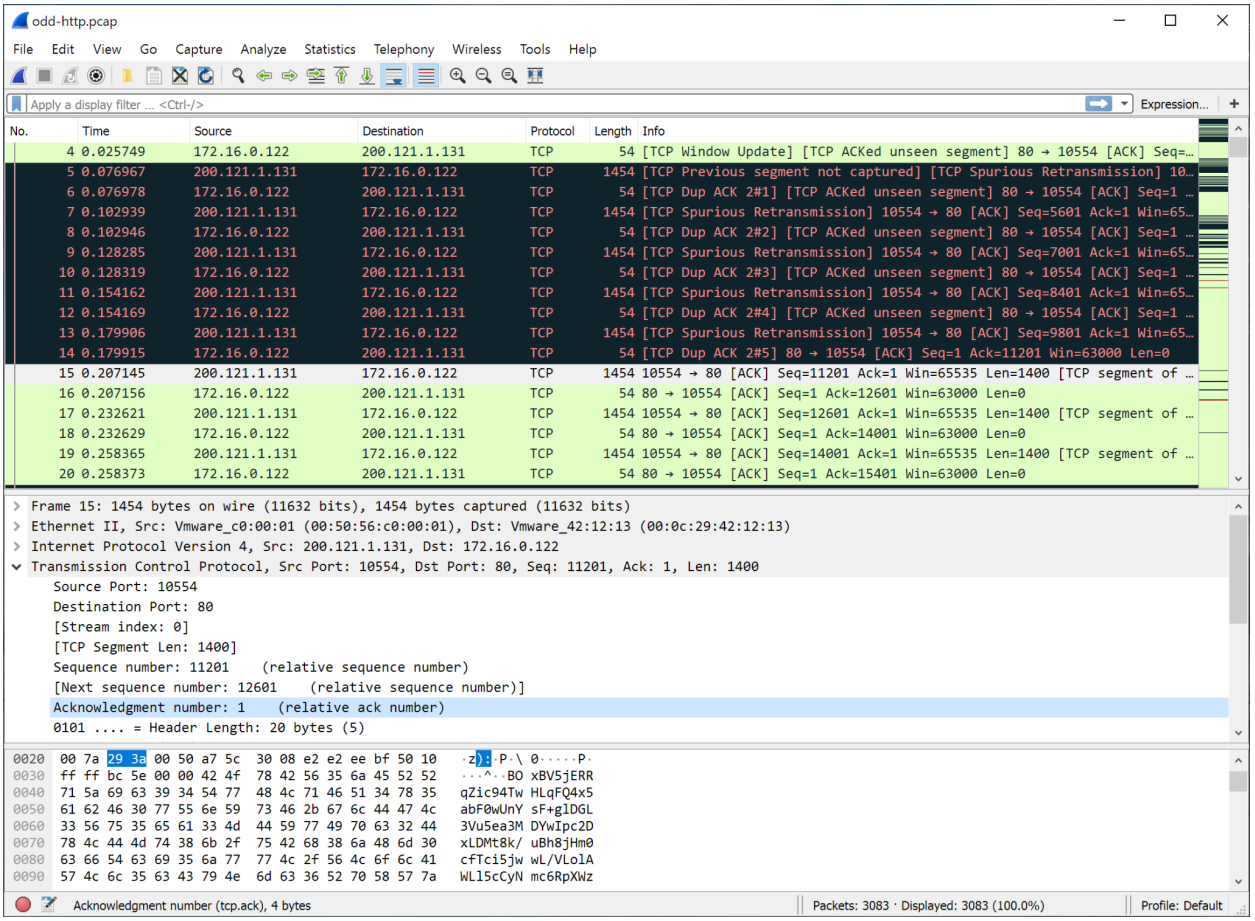


Figure 3.2: Captured Packets in Wireshark

Observations :-No malicious activity was detected during the capture period; specifically, there were no suspicious IP addresses or ARP spoofing attempts, indicating that the network was functioning normally and securely. This exercise provided trainees with hands-on experience in monitoring network traffic, interpreting protocol-level information, and understanding how packet-level analysis can be used to detect both performance issues and potential security incidents.No malicious activity was detected during the capture period; specifically, there were no suspicious IP addresses or ARP spoofing attempts, indicating that the network was functioning normally and securely.

Discussion :-Packet analysis helped understand real-time communication between systems. It demonstrated how attackers could sniff credentials or inject malicious packets, highlighting the importance of encryption and HTTPS protocols.Packet analysis helped understand real-time communication between systems. It demonstrated how attackers could sniff credentials or inject malicious packets, highlighting the importance of encryption and HTTPS protocols.Packet analysis helped understand real-time communication between systems. It demonstrated how attackers could sniff credentials or inject malicious packets, highlighting the importance of encryption and HTTPS protocols.

3.4 Vulnerability Assessment

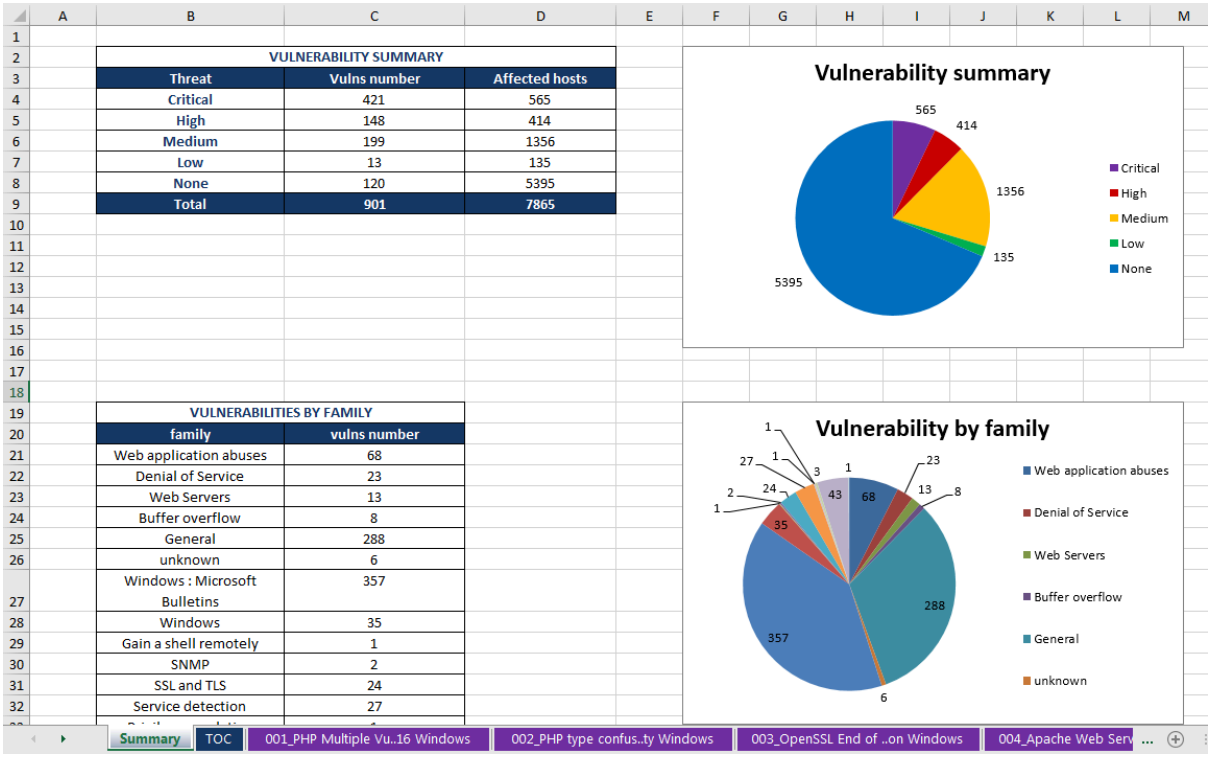
Objective **:-**The objective of this exercise was to identify system and network vulnerabilities using automated scanning tools, enabling trainees to assess security risks in a structured and systematic manner. Tools such as OpenVAS and Nessus were employed to perform comprehensive vulnerability scans, while the CVSS (Common Vulnerability Scoring System) calculator was used to evaluate and prioritize the severity of identified issues. Additionally, Nmap scripts were utilized to gather detailed information on open ports and services that could expose potential weaknesses.

Tools Used :-The procedure involved running a vulnerability scan with OpenVAS against selected target systems, allowing trainees to detect misconfigurations, missing patches, and exploitable vulnerabilities. Scan results were then exported in HTML or PDF format, providing a clear and organized report of findings for review and documentation.This hands-on exercise provided practical experience in conducting vulnerability assessments, interpreting automated scan results, and applying standardized scoring methods to inform effective risk management strategies.

Procedure :-To assess the impact of the discovered vulnerabilities, trainees used CVSS base scores to map and prioritize risks, highlighting which issues required immediate remediation. This hands-on exercise provided practical experience in conducting vulnerability assessments, interpreting automated scan results, and applying standardized scoring methods to inform effective risk management strategies.

Table 3.1 : Results Summary

Vulnerability	Severity	CVSS Score	Description
Outdated Apache version	High	9.0	Allows remote code execution
SMB v1 enabled	Medium	6.5	Outdated protocol vulnerable to EternalBlue
Weak password policy	Medium	5.8	Could allow brute-force login attempts



VULNERABILITY SUMMARY		
Threat	Vulns number	Affected hosts
Critical	421	565
High	148	414
Medium	199	1356
Low	13	135
None	120	5395
Total	901	7865

VULNERABILITIES BY FAMILY	
family	vulns number
Web application abuses	68
Denial of Service	23
Web Servers	13
Buffer overflow	8
General	288
unknown	6
Windows : Microsoft Bulletins	357
Windows	35
Gain a shell remotely	1
SNMP	2
SSL and TLS	24
Service detection	27

Figure 3.3: Sample OpenVAS Report

Discussion :-The results obtained from the vulnerability scans underscore the critical importance of timely patch management and proactive system maintenance. Vulnerabilities detected in the scanned systems, such as outdated software versions, unpatched services, and misconfigured applications, highlight potential entry points that attackers could exploit. Left unaddressed, these weaknesses can lead to unauthorized access, data breaches, or system disruptions. The exercise demonstrates that regular scanning and prompt remediation of vulnerabilities are essential components of an effective cybersecurity strategy, ensuring that systems remain resilient against evolving threats.

Mapping the identified vulnerabilities using the Common Vulnerability Scoring System (CVSS) adds significant value to the assessment process by providing a quantitative measure of risk severity. CVSS scores allow security teams to prioritize remediation efforts based on the potential impact and exploitability of each vulnerability. For example, high-scoring vulnerabilities indicate critical weaknesses that require immediate attention, while lower-scoring issues may be scheduled for routine updates. This structured approach ensures that limited resources are allocated efficiently and that the most serious risks are mitigated first, reducing the overall attack surface of the network.

3.5 Firewall and IDS Configuration

Objective :-The objective of this exercise was to provide trainees with practical experience in configuring firewall rules and intrusion detection mechanisms to establish a proactive defense for networked systems. The module emphasized the importance of combining preventive and detective security measures, ensuring that systems are both protected from unauthorized access and monitored for malicious activity. By the end of this exercise, participants were able to configure and test firewalls and IDS systems, gaining hands-on exposure to essential network security tools

Procedure :-The procedure began with configuring iptables rules on a Linux system, setting the firewall to block all incoming connections except for essential services such as SSH and HTTP. This allowed authorized users to access the system securely while minimizing exposure to potential attacks. Trainees also installed and configured Snort, an open-source Intrusion Detection System (IDS), to monitor network traffic, inspect packets, and generate alerts for suspicious patterns.

Results :-Testing the configurations involved simulating attack traffic to validate the effectiveness of both the firewall and IDS. Results showed that the firewall successfully blocked unauthorized pings and FTP attempts, preventing unpermitted connections. Simultaneously, Snort logged alerts for ICMP flood simulations, demonstrating its capability to detect potential denial-of-service attacks and other malicious behaviors in real time. These results confirmed that combining preventive controls (firewall) with detective mechanisms (IDS) provides a more robust security posture.

Discussion :-The configuration clearly demonstrated the effectiveness of rule-based security systems in safeguarding networked environments. By carefully defining and enforcing firewall rules, unauthorized access attempts were systematically blocked, ensuring that only legitimate traffic could reach critical services. At the same time, the deployment of an Intrusion Detection System (IDS) like Snort allowed for continuous monitoring of network activity, enabling the identification and alerting of potentially malicious behaviors in real time. Together, these preventive and detective controls form a complementary security strategy, providing multiple layers of protection that not only stop attacks from penetrating the network but also allow rapid detection of abnormal or suspicious activity. This hands-on exercise highlighted that rule-based systems are an essential part of a defense-in-depth approach, reinforcing organizational security by combining access control, traffic filtering, and active monitoring to maintain the integrity, confidentiality, and availability of network resources.This hands-on exercise highlighted that rule-based systems are an essential part of a defense-in-depth approach, reinforcing organizational security by combining access control, traffic filtering, and active monitoring to maintain the integrity, confidentiality, and availability of network resources.

3.6 Malware Analysis and Forensics

Objective :- The objective of this exercise was to provide trainees with practical experience in configuring firewall rules and intrusion detection mechanisms to establish a proactive defense for networked systems. The module emphasized the importance of combining preventive and detective security measures, ensuring that systems are both protected from unauthorized access and monitored for malicious activity. By the end of this exercise, participants were able to configure and test firewalls and IDS systems, gaining hands-on exposure to essential network security tools.

Procedure :-The procedure began with configuring iptables rules on a Linux system, setting the firewall to block all incoming connections except for essential services such as SSH and HTTP. This allowed authorized users to access the system securely while minimizing exposure to potential attacks. Trainees also installed and configured Snort, an open-source Intrusion Detection System (IDS), to monitor network traffic, inspect packets, and generate alerts for suspicious patterns.

Results :-Testing the configurations involved simulating attack traffic to validate the effectiveness of both the firewall and IDS. Results showed that the firewall successfully blocked unauthorized pings and FTP attempts, preventing unpermitted connections. Simultaneously, Snort logged alerts for ICMP flood simulations, demonstrating its capability to detect potential denial-of-service attacks and other malicious behaviors in real time. These results confirmed that combining preventive controls (firewall) with detective mechanisms (IDS) provides a more robust security posture.

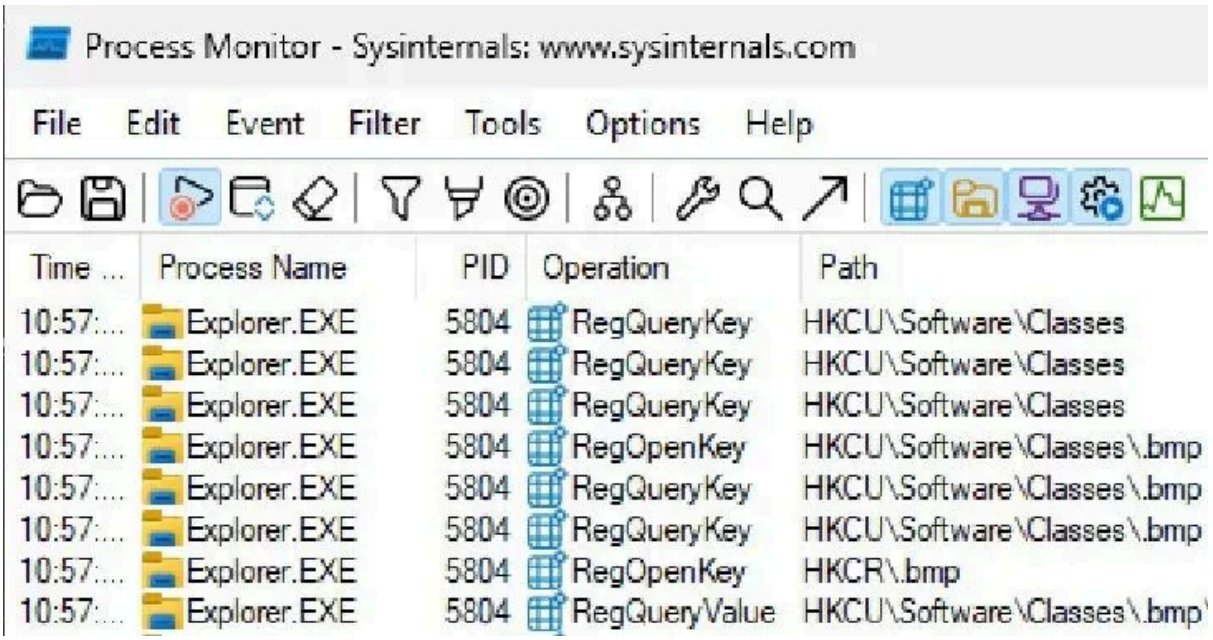


Figure 3.4: Procmon Capture of Malware Activity

Discussion :-The exercise highlights the importance of rule-based security systems in protecting networks. Firewalls enforce strict access control, while IDS tools monitor for abnormal activity, allowing security teams to respond quickly to threats. Trainees learned how to implement, test, and document security rules, reinforcing the principle that proactive configuration and continuous monitoring are key to maintaining secure and resilient network infrastructures.exercise highlights the importance of rule-based security systems in protecting networks. Firewalls enforce strict access control, while IDS tools monitor for abnormal activity, allowing security teams to respond quickly to threats. Trainees learned how to implement, test, and document security rules, reinforcing the principle that proactive configuration and continuous monitoring are key to maintaining secure and resilient network infrastructures.Trainees learned how to implement, test, and document security rules, reinforcing the principle that proactive configuration and continuous monitoring are key to maintaining secure and resilient network infrastructures.

3.7 Summary

The experiments and results presented in this chapter provided participants with extensive hands-on experience across multiple key domains of cybersecurity, including network analysis, vulnerability detection, penetration testing, encryption, malware analysis, and digital forensics. By actively engaging with tools such as Nmap, Wireshark, OpenVAS, Nessus, FTK Imager, and Snort, trainees were able to simulate real-world scenarios and understand how theoretical concepts are applied in practice. This practical exposure allowed them to observe the direct impact of configuration choices, scanning techniques, and monitoring strategies on system security, enhancing their analytical and problem-solving skills.

Through these exercises, participants developed a holistic understanding of cybersecurity workflows, learning how individual tools and techniques interconnect to form a comprehensive security framework. For example, network scanning identified potential vulnerabilities, which could then be exploited in controlled penetration tests and monitored using IDS systems. Similarly, digital forensics exercises complemented incident response practices by teaching participants how to collect, preserve, and analyze evidence from compromised systems. The combination of theory, practical application, and structured experimentation reinforced the importance of proactive defense, continuous monitoring, and systematic response in maintaining a secure digital environment.

Overall, the hands-on approach of this training helped participants internalize the relationships between different cybersecurity components, demonstrating that effective protection requires integration of multiple tools, strategies, and analytical skills rather than reliance on isolated solutions. This comprehensive learning experience prepared trainees to approach real-world cybersecurity challenges with confidence, technical competence, and state.

CHAPTER 4 – CONCLUSION AND FUTURE SCOPE

4.1 Conclusion

The one-month training on Cybersecurity Fundamentals and Operating System Basics provided valuable insight into the principles, tools, and practices essential for protecting digital infrastructure. The training effectively combined theoretical concepts with practical exposure, helping to bridge the gap between academic learning and real-world applications. Through hands-on sessions, participants explored multiple domains — including network analysis, vulnerability assessment, cryptography, malware analysis, and incident response. The exposure to tools such as Wireshark, Nmap, Metasploit, FTK Imager, and Snort offered practical understanding of threat detection and mitigation strategies.

A major takeaway from this training was the importance of defense-in-depth — a layered approach to cybersecurity involving proactive monitoring, regular patching, access control, and strong encryption mechanisms.

Additionally, concepts such as the CIA triad (Confidentiality, Integrity, Availability) and frameworks like NIST and ISO 27001 helped in understanding how enterprises maintain security compliance and resilience.Overall, the training experience enhanced technical competency, analytical skills, and awareness of evolving cyber threats. It prepared the participants to think like both defenders and ethical hackers, capable of identifying and resolving vulnerabilities in a responsible and systematic manner.

4.2 Future Scope

Cybersecurity is a constantly evolving field, with new attack vectors and technologies emerging every day. Therefore, the skills and concepts learned during this training form a foundation that can be expanded through continuous learning and specialization.

Future advancements and learning areas include:

- **Advanced Penetration Testing:** Learning advanced exploitation techniques, red teaming, and post-exploitation strategies using tools like Burp Suite Pro and Cobalt Strike.
- **Cloud Security and DevSecOps:** Understanding secure cloud deployment, identity management (IAM), and integration of security in the software development lifecycle.
- **Digital Forensics and Threat Intelligence:** Expanding into forensic investigation, log correlation, and malware reverse engineering to identify root causes of cyber incidents.

- **AI and Machine Learning in Cybersecurity:** Using intelligent systems for anomaly detection, predictive threat analysis, and automated response.
- **Incident Response and SOC Operations:** Developing skills in Security Information and Event Management (SIEM) tools, threat hunting, and building automated defense workflows.

As organizations increasingly migrate to cloud-based systems and IoT environments, there is a growing need for skilled cybersecurity professionals who can manage complex infrastructures securely.With further training, certifications, and research, participants can contribute effectively to this domain as Security Analysts, Penetration Testers, Forensic Experts, or Network Security Engineers.

4.3 Final Remarks

The successful completion of this training program represents a significant milestone in developing a practical and comprehensive understanding of cybersecurity in real-world contexts. Over the course of the program, participants were exposed to a wide range of concepts, tools, and techniques that are fundamental to protecting digital systems and networks. From the basics of operating system administration in Linux and Windows, to advanced practices such as network scanning, vulnerability assessment, penetration testing, malware analysis, and digital forensics, the training provided a structured and immersive learning experience. By actively engaging in hands-on exercises and simulations, trainees were able to observe how theoretical knowledge is applied to identify risks, mitigate threats, and enhance system resilience against cyberattacks.

Through practical application, participants gained valuable skills in implementing system hardening measures, configuring firewalls, monitoring network traffic, and managing access controls, all of which contribute to creating secure computing environments. They also learned to conduct structured vulnerability assessments and penetration tests, enabling them to proactively identify and prioritize risks using frameworks such as CVSS. Additionally, exercises in incident response, threat hunting, malware analysis, and digital forensics instilled a deeper understanding of how to respond effectively to security incidents, investigate breaches, and maintain the integrity of critical systems. These competencies collectively provide a strong foundation for addressing both current and emerging cybersecurity challenges.

The training also emphasized the importance of continuous learning, ethical responsibility, and professional awareness. Cybersecurity is a constantly evolving field, with new threats, vulnerabilities, and technologies emerging every day. Participants were encouraged to stay updated with industry best practices, engage in ongoing skill development, and approach every task with ethical consideration, recognizing that the protection of digital assets and user privacy is a fundamental responsibility of security professionals.

REFERENCES

[1] **William Stallings**, *Cryptography and Network Security: Principles and Practice*, 8th Edition, Pearson, 2019.
This book provides a comprehensive introduction to cryptography and network security principles, covering symmetric and asymmetric encryption, key management, digital signatures, authentication protocols, and modern network security practices. It is widely regarded as a foundational text for understanding secure communication in computer networks.

[2] **Andrew S. Tanenbaum, David J. Wetherall**, *Computer Networks*, 5th Edition, Pearson, 2011.
Tanenbaum and Wetherall present a detailed exploration of computer network architecture, protocols, and data communication principles. Topics include the OSI and TCP/IP models, routing algorithms, error detection, congestion control, and practical network implementation strategies.

[3] **Behrouz A. Forouzan**, *Data Communications and Networking*, 5th Edition, McGraw-Hill, 2012.
Forouzan's text provides an in-depth study of data communications and networking fundamentals, emphasizing network topologies, transmission methods, network devices, IP addressing, and modern network protocols. The book also introduces practical networking scenarios and troubleshooting techniques.

[4] **Georgia Weidman**, *Penetration Testing: A Hands-On Introduction to Hacking*, 2nd Edition, No Starch Press, 2014.
This practical guide covers ethical hacking and penetration testing techniques. Topics include reconnaissance, scanning, exploitation, post-exploitation, and reporting. The book emphasizes hands-on exercises using tools such as Metasploit, Nmap, and Wireshark to simulate real-world attacks in controlled environments.

[5] **Michael T. Simpson, et al.**, *Computer Forensics: Cybercriminals, Laws, and Evidence*, Cengage Learning, 2018.
Simpson and colleagues provide a detailed overview of computer forensics, including evidence collection, analysis, and legal considerations. The book addresses investigative techniques, forensic tools, and the process of maintaining the chain of custody for digital evidence.

[6] **National Institute of Standards and Technology (NIST)**, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, 2018. [Online]. Available: https://www.nist.gov/cyberframework
The NIST Cybersecurity Framework provides guidelines for managing and reducing cybersecurity risks in critical infrastructure.

THANK YOU

I would like to express my **sincere gratitude** to everyone who has supported me throughout the successful completion of this one-month industrial training program and the preparation of this report. This experience has been both enriching and transformative, providing me with a practical understanding of cybersecurity concepts and hands-on exposure to real-world applications.

A special thanks is extended to **Sensation Software Solutions Pvt. Ltd., Ludhiana**, for providing me with an excellent platform to **learn, explore, and apply cybersecurity principles** in a professional setting. The guidance and resources offered by the organization allowed me to gain practical insights into network security, system hardening, vulnerability assessment, penetration testing, and incident response, which have greatly enhanced my technical proficiency and problem-solving abilities.

I am also deeply thankful to **Guru Nanak Dev Engineering College, Ludhiana**, for their continuous support and encouragement throughout the training. I sincerely appreciate the valuable guidance provided by my **project guide, faculty members, and peers**, whose constructive feedback and mentorship were instrumental in helping me understand complex concepts and successfully complete this training. Their encouragement motivated me to approach challenges confidently and learn effectively.

This industrial training experience has been invaluable in **enhancing my knowledge, skills, and confidence in the field of cybersecurity**. It has not only provided practical exposure to modern security tools and techniques but has also inspired me to continue learning and pursuing a professional career in cybersecurity, with a strong foundation in both theoretical understanding and practical application.

(Taranveer Singh)
Roll No : 2302703
B.Tech (Computer Science & Engineering)
Guru Nanak Dev Engineering College, Ludhiana