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

This is to certify that the **One-Month Industrial Training Report** entitled

“CYBER SECURITY ”

has been successfully completed and submitted by

Name: Taranveer Singh
Roll No.: 2302703
Branch: B.Tech in Computer Science and Engineering
College: Guru Nanak Dev Engineering College, Ludhiana
Training Organization: Sensation Software Solutions Pvt. Ltd.

in partial fulfillment of the requirements for the award of the **Bachelor of Technology in Computer Science and Engineering** under the **IK Gujral Punjab Technical University, Jalandhar**.

It is certified that this report is the result of the student’s own effort and study carried out during the one-month industrial training period at **Sensation Software Solutions Pvt. Ltd.**, and has not been submitted elsewhere for any other degree or diploma.

(Dr. Kiran Jyoti)
Head of Department (CSE)
Guru Nanak Dev Engineering College, Ludhiana

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 world, the internet has become an essential part of our daily lives. From financial transactions to social networking and data sharing, nearly every activity depends on technology. However, this rapid digitalization has also opened the door to numerous cyber threats such as hacking, identity theft, phishing, and ransomware.

Cybersecurity refers to the collection of practices, technologies, and processes designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access. It ensures the safety, privacy, and integrity of information in the cyber domain.

The main goal of cybersecurity is to minimize the risk of cyber attacks and safeguard systems from exploitation. It is a continuous process that involves prevention, detection, response, and recovery measures to maintain trust in digital environments.

Figure 1.1 : introduction to cyber security

1.2 Importance of Cybersecurity

Cybersecurity is critical for individuals, organizations, and governments alike. Modern systems handle sensitive data such as personal information, financial records, and intellectual property. A single breach can cause severe financial loss, reputational damage, and even legal penalties.

Some key reasons why cybersecurity is essential include:

- Protection of data privacy – Preventing unauthorized access and misuse of personal and organizational data.
- Maintaining business continuity – Ensuring systems remain functional and secure against disruptions.
- Preventing cyber crime – Protecting individuals and organizations from fraud, identity theft, and data manipulation.
- National security – Defending against cyber warfare, espionage, and terrorism that target government or critical infrastructure.

Figure 1.2 : importance of cyber security

1.3 Objectives of the Training

The primary objective of this training program on *Cybersecurity Fundamentals & Operating System Basics* is to build foundational knowledge of security principles, system architecture, and network protection techniques.
The main learning goals include:

1. Understanding the fundamental concepts of cybersecurity, threats, and vulnerabilities.
2. Learning the architecture and security mechanisms of Linux and Windows operating systems.

3. Exploring networking concepts, firewalls, IDS/IPS, and network defense techniques.

4. Gaining basic exposure to cryptography, penetration testing, and vulnerability assessment.

5. Understanding how incident response and malware analysis are conducted.

6. Developing awareness of cloud, IoT, and mobile security challenges.

7. Learning to apply defensive scenarios.

Figure 1.3: Objectives

1.4 Scope of the Training

The training focuses on the **foundational aspects of cybersecurity**, covering both theoretical knowledge and practical implementation. It provides a **comprehensive, hands-on introduction** to essential tools and utilities such as **Wireshark**, **Nmap**, **ip tables**, **Procmon**, and **Metasploit**, which are widely used by security professionals in real-world environments.
Participants are guided through a **progressive and structured learning path** that begins with understanding **operating system fundamentals**, **file management**, and **networking basics**, and gradually advances toward more complex domains such as **vulnerability assessment**, **penetration testing**, **incident handling**, and **threat detection techniques**.

Throughout the training, emphasis is placed on **developing analytical thinking, problem-solving ability, and technical precision** in handling security challenges. Students learn not only how to identify vulnerabilities but also how to **implement countermeasures** and ensure that systems remain resilient against potential cyber threats.
By the end of this training, participants acquire the **technical and procedural skills necessary to analyze security weaknesses, protect digital infrastructure, investigate incidents, and respond effectively to cyberattacks** — thereby laying a strong foundation for advanced study and professional work in the field of cybersecurity.

1.5 Outcome of the Training

After completing the cybersecurity training, learners are expected to:

- Demonstrate an understanding of cybersecurity principles and frameworks.
- Operate and secure both Linux and Windows environments.
- Perform network and vulnerability analysis using professional tools.
- Identify and mitigate common cyber threats and attacks.
- Understand the basics of cryptography, malware analysis, and digital forensics.
- Apply system and network hardening techniques for improved security posture.

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 designed to provide a **comprehensive blend of theoretical knowledge and practical skills**. The methodology included:

1. **Classroom Lectures:** Focused on cybersecurity fundamentals, OS basics, networking, cryptography, and ethical hacking concepts.

2. **Hands-on Labs:** Practical exercises to reinforce concepts using professional tools and OS environments.

3. **Assignments & Exercises:** Each module included tasks to simulate real-world security scenarios.

4. **Documentation & Reporting:** Trainees maintained logs and reports for each exercise.

The training followed a **step-by-step progressive approach**, starting from basic concepts to advanced security practices, enabling participants to gain confidence in performing real-world cybersecurity tasks.

2.2 Cybersecurity Fundamentals and Operating System Basics

2.2.1 Linux Operating System

Objectives: Understand Linux architecture, commands, security features, and system administration.

Topics Covered:

- Linux OS Overview and File System

- Command-Line Basics: ls, cd, mkdir, chmod, chown, cat, grep

- User and Group Management: useradd, usermod, groupadd, passwd

- File Permissions & Security: read, write, execute permissions, SUID, SGID

Practical Exercises:

1. Create multiple users and assign groups.
2. Modify file permissions for secure access.
3. Use iptables to configure simple firewall rules.
4. Capture network traffic using **Wireshark** and analyze packet data.

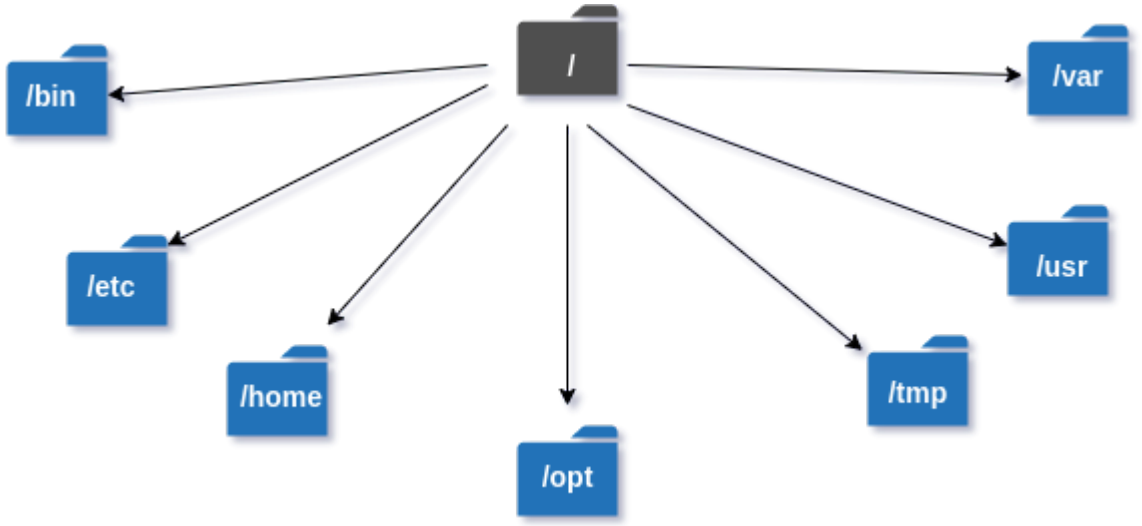


Figure 2.1: Linux file structure hierarchy

```
kb@phoenixNAP:~$ sudo iptables -A INPUT -s 131.153.40.84 -j ACCEPT
kb@phoenixNAP:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  speedsrb.phoenixnap.com  anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

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 on the terminal	cat notes.txt
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 and usage	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

1. Windows OS Overview and Components

- Windows operating system is a **graphical-based OS** widely used in enterprises and personal systems.
- Key components include:
    - **Kernel:** Core system managing hardware resources, memory, and processes.
    - **Registry:** Central database storing system settings and application configurations.

- **User Interface (UI):** Desktop, Start Menu, Taskbar for user interaction.
- **Services & Processes:** Background tasks enabling system and application functionalities.

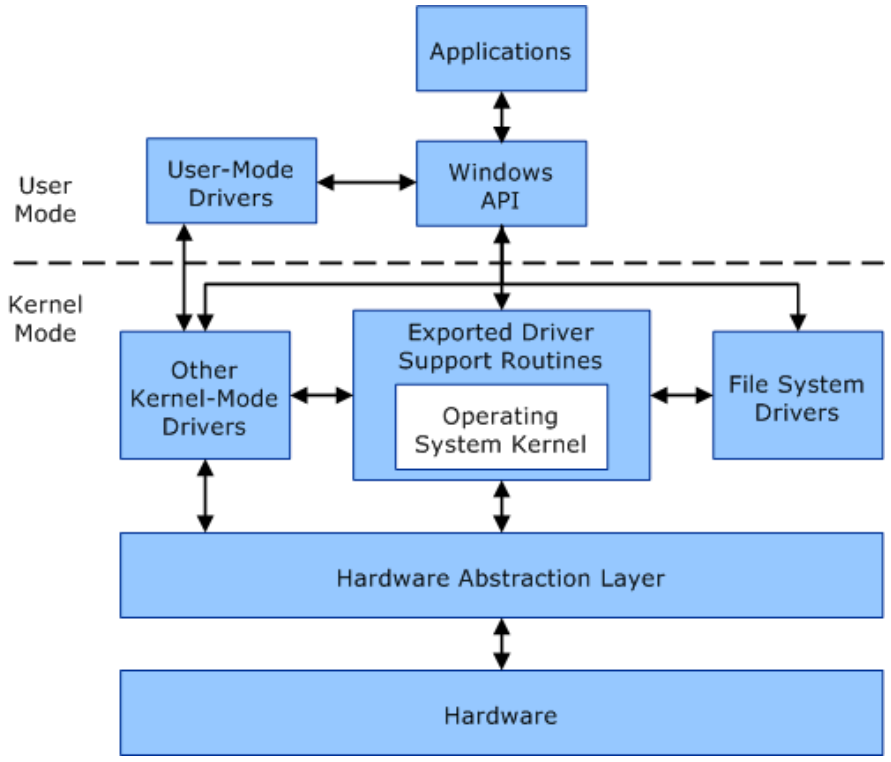


Figure 2.3: Windows architecture diagram (Kernel, User Mode, Services, UI)

2. User Privileges, Event Logs, and Registry Management

- **User Privileges:**
  - Administrators: Full access, can install software, manage accounts.
  - Standard Users: Limited access to system settings.
  - Guest Accounts: Minimal access, mainly for temporary users.
- **Event Logs:**

    - Windows maintains logs for security, system, and application events.
    - Useful for detecting unauthorized access, system errors, or malicious activity.
- **Registry Management:**
    - Registry keys store system, application, and security configurations.
    - Editing registry must be done carefully as incorrect changes can crash 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

- **Procmon (Process Monitor):** Monitors real-time file system, registry, and process activity.
- **PsExec:** Executes processes remotely with administrative privileges.
- **Task Scheduler:** Automates tasks and scripts at scheduled times; useful for security automation.

Practical Exercises

1. Monitor System Processes using Procmon

- Launch **Procmon** and filter by process names (e.g., `explorer.exe`)
- Observe registry, file system, and network activity.
- Detect suspicious processes that might indicate malware.

2. Manage User Accounts and Privileges

- Open **Computer Management → Local Users and Groups**
- Create a new user and assign Standard or Administrator privileges
- Modify existing user privileges to simulate different security scenarios

3. Investigate Windows Event Logs for Suspicious Activities

- Open **Event Viewer → Windows Logs → Security**
- Filter for login failures, privilege escalation, or system errors
- Document findings in a table for report submission

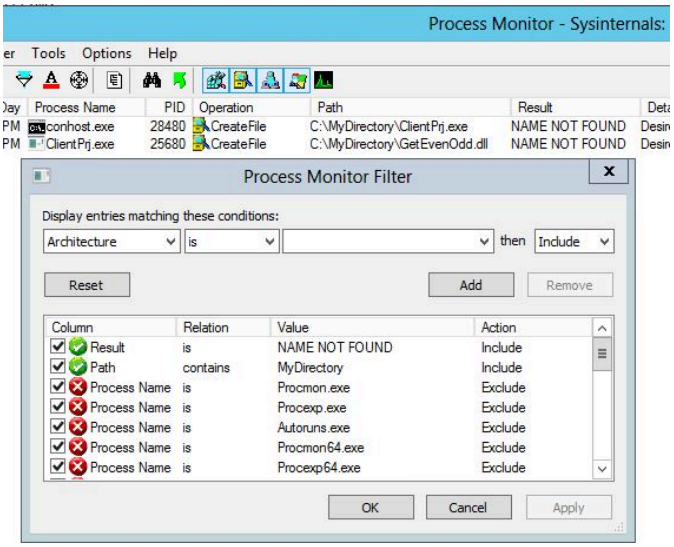


Figure 2.4: Procmon monitoring a sample process

Summary

This module provided trainees with a practical understanding of **Windows OS security and administrative operations**.
By the end of this section, participants were able to:

- Analyze system processes for anomalies
- Manage user accounts with appropriate privileges
- Examine event logs and registry settings for security monitoring

2.3 Networking & Network Security

Objectives:
This module aimed to provide trainees with a clear understanding of **networking fundamentals, network security principles, and the use of security tools** to monitor and protect networks. By the end of this section, participants were able to analyze network traffic, configure security devices, and simulate cyber attacks in a controlled environment.

2.3.1 Networking Basics

Overview:

- Networking is the process of connecting multiple devices to **share resources and communicate**.

- Understanding networking fundamentals is critical for cybersecurity professionals to identify vulnerabilities and secure systems.

Topics Covered:

- **OSI Model (7 Layers):** Physical, Data Link, Network, Transport, Session, Presentation, Application

- **TCP/IP Model:** Network Interface, Internet, Transport, Application

- **Common Protocols:**

    - **IP (Internet Protocol):** Addressing and routing

    - **TCP/UDP:** Reliable vs. connectionless communication

    - **HTTP/HTTPS, DNS:** Web and domain communication

- **Network Devices:** Routers, Switches, Firewalls, IDS/IPS

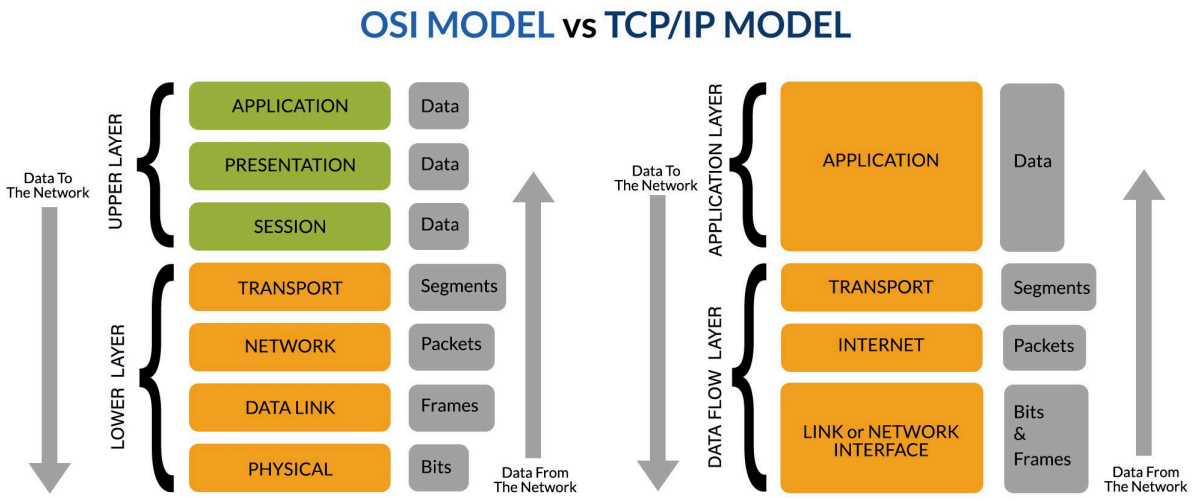


Figure 2.5: OSI and TCP/IP model diagram

Protocol Comparison: TCP vs UDP

- **Type:**
    - TCP: Connection-oriented
    - UDP: Connectionless
- **Reliability:**
    - TCP: Reliable, ensures data delivery with acknowledgments
    - UDP: Unreliable, no guarantee of delivery
- **Data Flow:**
    - TCP: Stream-oriented
    - UDP: Message-oriented
- **Error Checking:**
    - TCP: Yes, with retransmission of lost packets
    - UDP: Minimal, only basic checksum

- **Ordering of Packets:**
    - TCP: Ensures packets arrive in correct order
    - UDP: No guarantee of order
- **Speed:**
    - TCP: Slower due to additional overhead
    - UDP: Faster because of minimal overhead
- **Use Cases:**
    - TCP: Web browsing (HTTP/HTTPS), Email (SMTP), File Transfer (FTP)
    - UDP: Streaming, VoIP, Online gaming
- **Connection Setup:**
    - TCP: Requires handshake (3-way handshake)
    - UDP: No handshake required
- **Overhead:**
    - TCP: Higher due to headers and acknowledgment mechanisms
    - UDP: Lower due to minimal headers
- **Examples:**
    - TCP: HTTP, HTTPS, FTP, SMTP
    - UDP: DNS queries, Video streaming, VoIP

2.3.2 Network Security Fundamentals

Overview:

- Network security is critical to **protect data integrity, confidentiality, and availability**.

- Trainees learned to implement firewalls, intrusion detection systems, and intrusion prevention systems.

Topics Covered:

- **Firewalls:**
    - Packet Filtering
    - Stateful Inspection
    - Proxy Firewalls
- **IDS/IPS Concepts:**
    - Intrusion Detection System (IDS): Monitors network for suspicious activity
    - Intrusion Prevention System (IPS): Detects and blocks malicious traffic
- **Security Monitoring:**
    - Logging, alerts, and reporting
    - Detecting anomalies and possible breaches

Practical Exercises:

1. Configure firewall rules to allow/block specific IP addresses or ports
2. Deploy **Snort IDS** to monitor network traffic for malicious patterns
3. Generate simulated attacks and observe IDS/IPS responses
4. Document firewall and IDS configuration rules

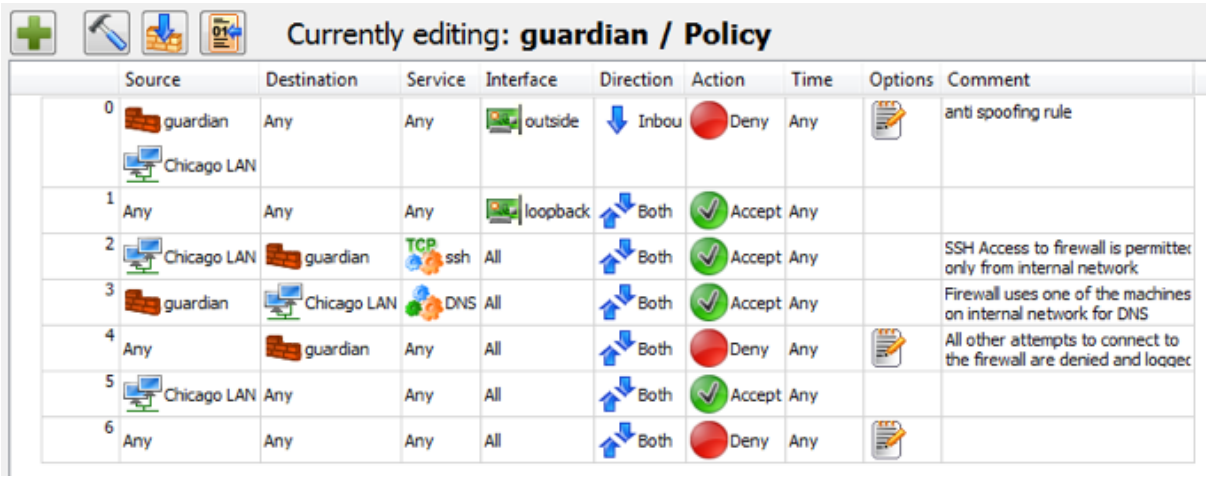


Figure 2.6: Example firewall configuration interface

Intrusion Detection System (IDS)

- Monitors network or system activities for **suspicious behavior**.
- Operates in **passive mode**; does not block traffic.
- Generates **alerts** for detected intrusions or anomalies.
- Can be **signature-based** (detect known threats) or **anomaly-based** (detect unusual behavior).
- Typically deployed **out-of-band**, monitoring traffic copies rather than live traffic.
- Useful for **forensic analysis and auditing** after incidents.
- Minimal impact on network performance since it does not interfere with traffic.
- Examples: Snort (IDS mode), Suricata (IDS mode).

Intrusion Prevention System (IPS)

- Monitors network traffic and **actively blocks malicious activity**.
- Operates in **inline mode**, inspecting live network traffic.

- Can prevent attacks in **real-time** based on detection rules.
- Uses **signature-based** or **anomaly-based** detection methods.
- Can enforce **security policies** automatically.
- May introduce **latency** if misconfigured or under heavy load.
- Examples: Cisco Firepower, Snort (IPS mode), Palo Alto Threat Prevention.
- Essential for **real-time defense** in enterprise networks.

2.3.3 Network Security Best Practices

Key Concepts:

- Use **strong passwords** for routers and administrative access
- Enable **logging** on all security devices
- Segment networks to limit exposure
- Regularly update firmware and security patches

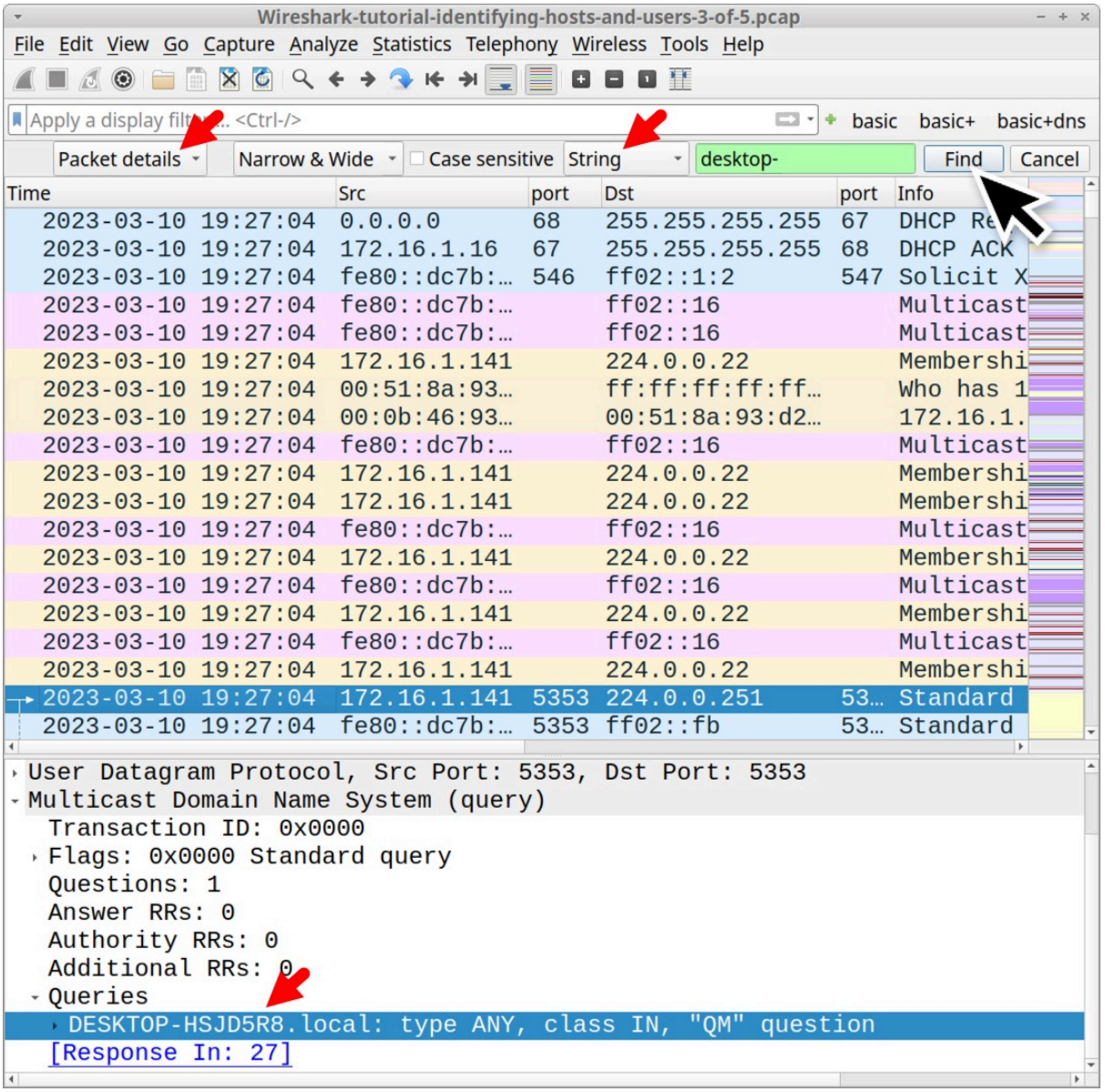


Figure 2.7: Wireshark packet capture

Summary

This module provided a practical foundation in **networking principles and security**. Trainees learned to:

- Understand OSI/TCP-IP models and common protocols
- Analyze network traffic using Wireshark
- Configure firewalls and monitor IDS/IPS systems

2.4 Cryptography and Wireless Security

Objectives:
The purpose of this module is to introduce trainees to **encryption techniques for data security** and **methods for securing wireless networks**. By the end of this section, participants were able to implement encryption, configure secure Wi-Fi networks, and detect potential wireless threats.

2.4.1 Cryptography

Overview:
Cryptography is the science of **securing data** by converting it into unreadable formats. It ensures **confidentiality, integrity, and authenticity** of data. Two main types of encryption are commonly used:

1. **Symmetric Encryption:**
    - Uses a **single key** for both encryption and decryption.
    - Faster and efficient for large amounts of data.
    - Common algorithms: **AES (Advanced Encryption Standard)**.
    - Practical Example: Encrypting a file using AES and sharing the same key for decryption.
2. **Asymmetric Encryption:**
    - Uses a **pair of keys**: public key for encryption, private key for decryption.
    - Ensures secure communication without sharing the private key.
    - Common algorithms: **RSA (Rivest-Shamir-Adleman)**.
    - Practical Example: Encrypting emails so that only the intended recipient can decrypt.

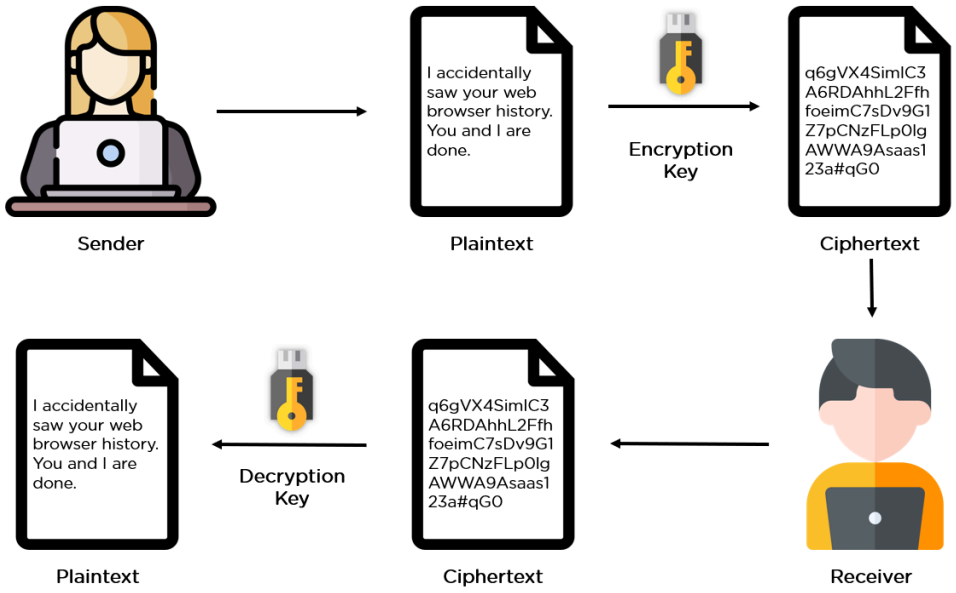


Figure 2.8 : Sample encrypted vs decrypted data

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

Overview:
Wireless networks are prone to attacks due to **open transmission medium**. Securing Wi-Fi is essential to prevent unauthorized access and data theft.

Topics Covered:

1. **Wireless Security Protocols:**
    - **WPA2 (Wi-Fi Protected Access 2):** Strong encryption (AES), widely used.
    - **WPA3:** Latest protocol offering stronger encryption, forward secrecy, and protection against brute-force attacks.
2. **Detection of Rogue Access Points:**
    - Rogue APs are unauthorized devices trying to mimic legitimate Wi-Fi networks.
    - Detection tools include Wi-Fi scanners and network monitoring utilities.
    - Practical Steps: Scan networks, check MAC addresses, validate access points with known infrastructure.

Practical Exercises

1. **Encrypt and Decrypt Files using AES and RSA:**
    - Encrypt a text or document file using AES (symmetric).
    - Encrypt another file using RSA (asymmetric) and decrypt with private key.
2. **Configure a Secure Wireless Network:**
    - Set up a Wi-Fi network with **WPA3 encryption**.
    - Assign strong passwords and enable MAC filtering for additional security.
3. **Detect Rogue Access Points:**
    - Use Wi-Fi scanning tools like **Kismet** or **NetSpot**.

- Identify unauthorized networks and take preventive action.

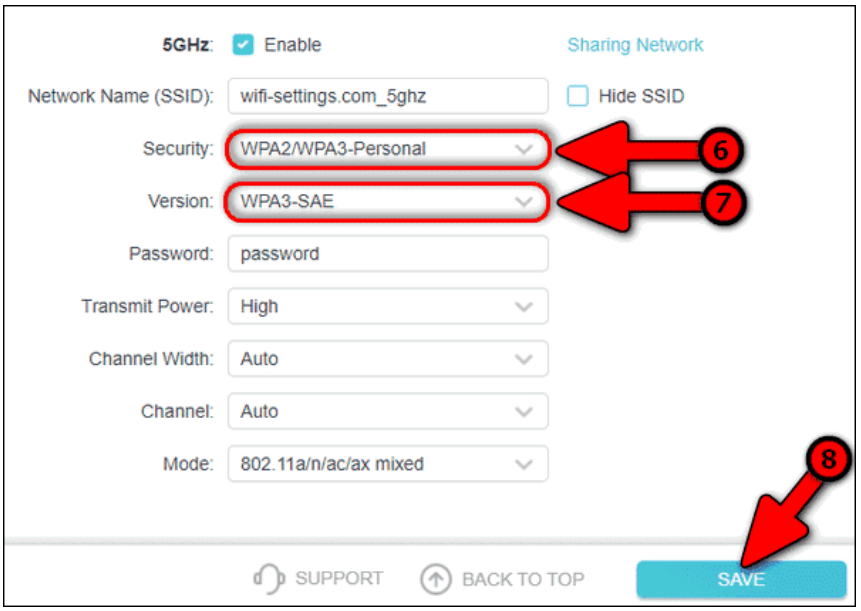


Figure 2.9: Screenshot of WPA3 secured network configuration

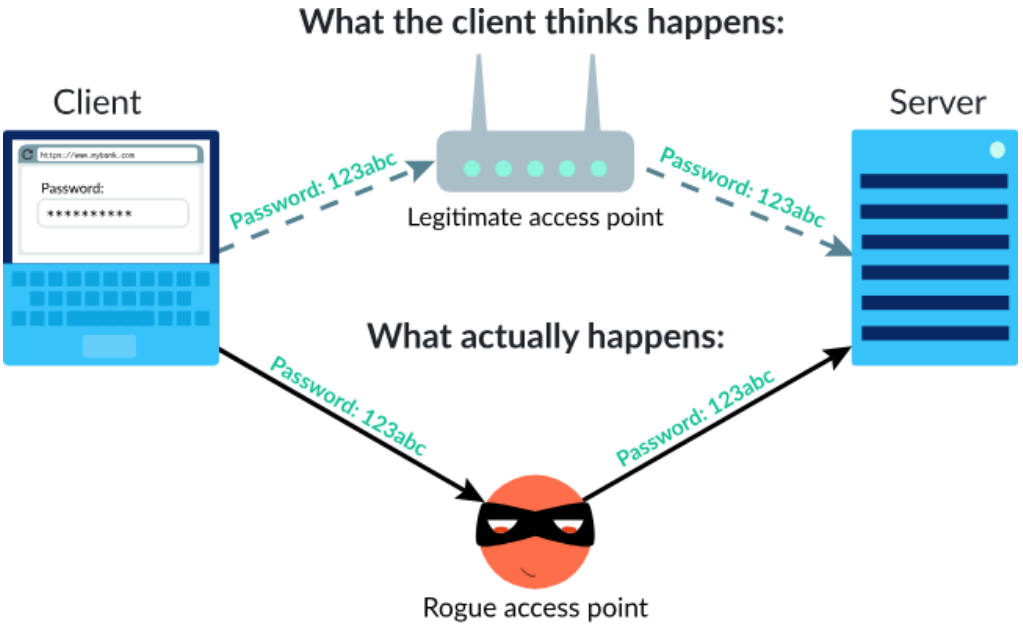


Figure 2.10: Example scan detecting a rogue access point

2.5 Vulnerability Assessment and Penetration Testing

2.5.1 Vulnerability Assessment

Objectives: Identify and classify vulnerabilities in systems and networks.

Topics Covered:

- CVE and CVSS for vulnerability scoring
- Vulnerability scanning using **Nessus, OpenVAS, Qualys**
- Reporting and risk assessment

Practical Exercises:

1. Run vulnerability scans on lab machines.
2. Analyze scan reports and document findings.
3. Prioritize vulnerabilities using CVSS scores.

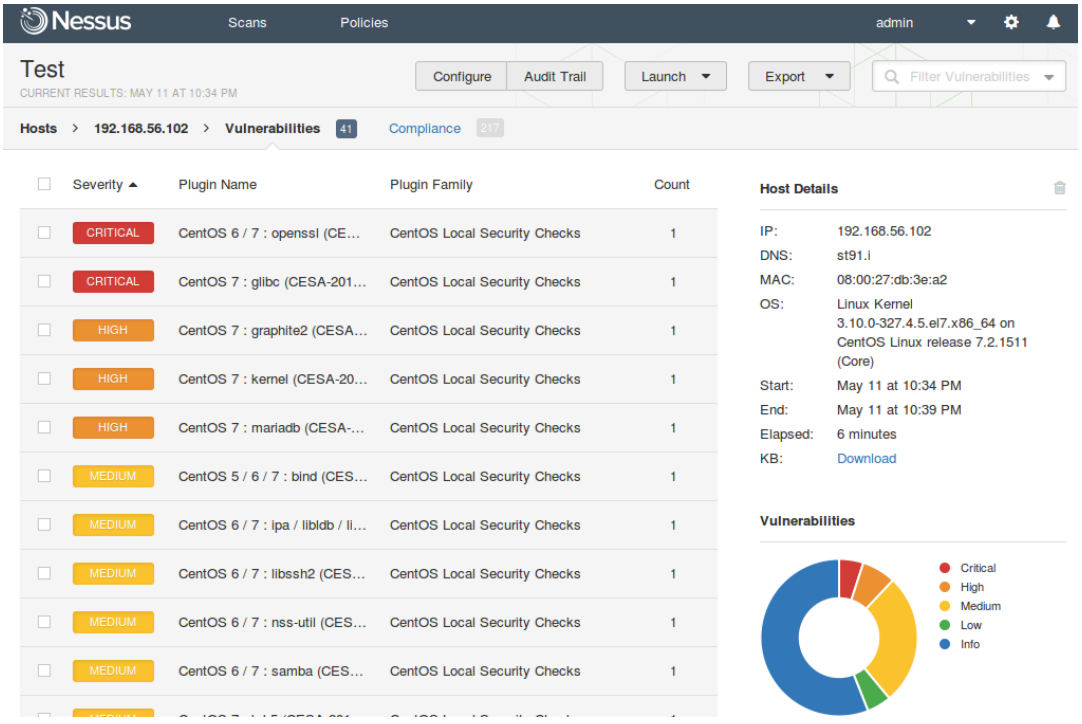


Figure 2.11: Nessus scan report screenshot

2.5.2 Penetration Testing

Objectives: Perform controlled attacks to test system defenses.

Topics Covered:

- Phases: Reconnaissance, Scanning, Exploitation
- Tools: Nmap, Metasploit, Burp Suite
- Ethical hacking guidelines

Practical Exercises:

1. Conduct network reconnaissance with Nmap.
2. Exploit vulnerabilities in controlled lab environments using Metasploit.
3. Perform web application testing with Burp Suite.

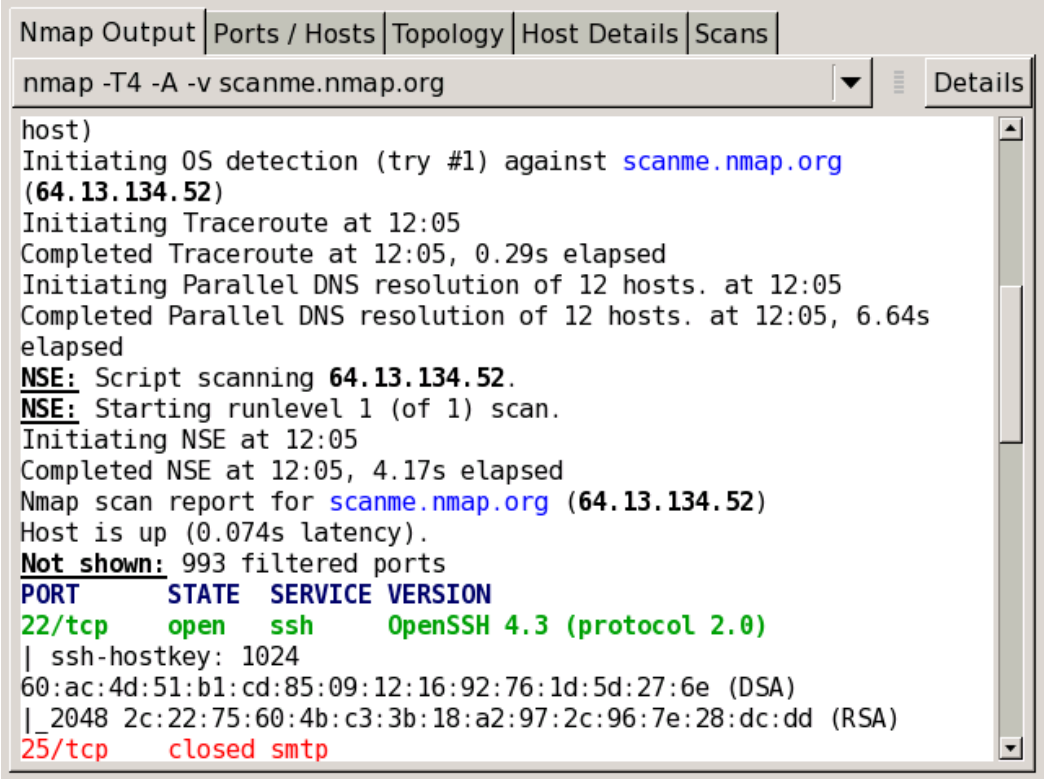


Figure 2.12: Nmap scan output

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: Respond to security incidents and analyze malware.

Topics Covered:

- Incident Response Lifecycle: Preparation, Detection, Containment, Recovery
- Malware Types: Viruses, Trojans, Ransomware
- Static and Dynamic Malware Analysis

Practical Exercises:

1. Analyze malware samples in isolated lab.
2. Document detection and mitigation steps.
3. Create a basic incident response plan for a simulated attack.

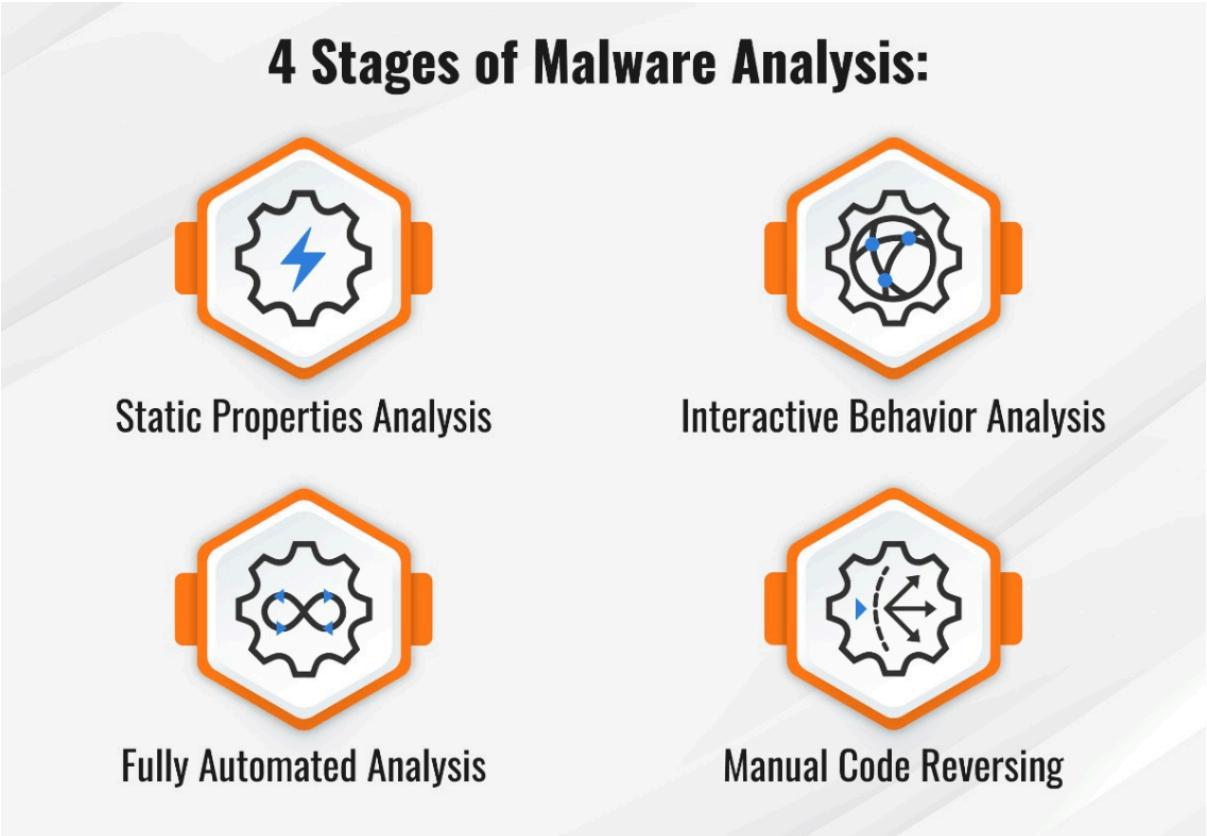


Figure 2.13: Malware analysis workflow

2.7 Digital Forensics

Objectives: Learn evidence collection and analysis techniques.

Topics Covered:

- Chain of Custody
- Evidence Collection Procedures
- Tools: FTK Imager, EnCase

Practical Exercises:

1. Capture disk images using FTK Imager.
2. Recover deleted files.
3. Document findings and maintain chain of custody logs

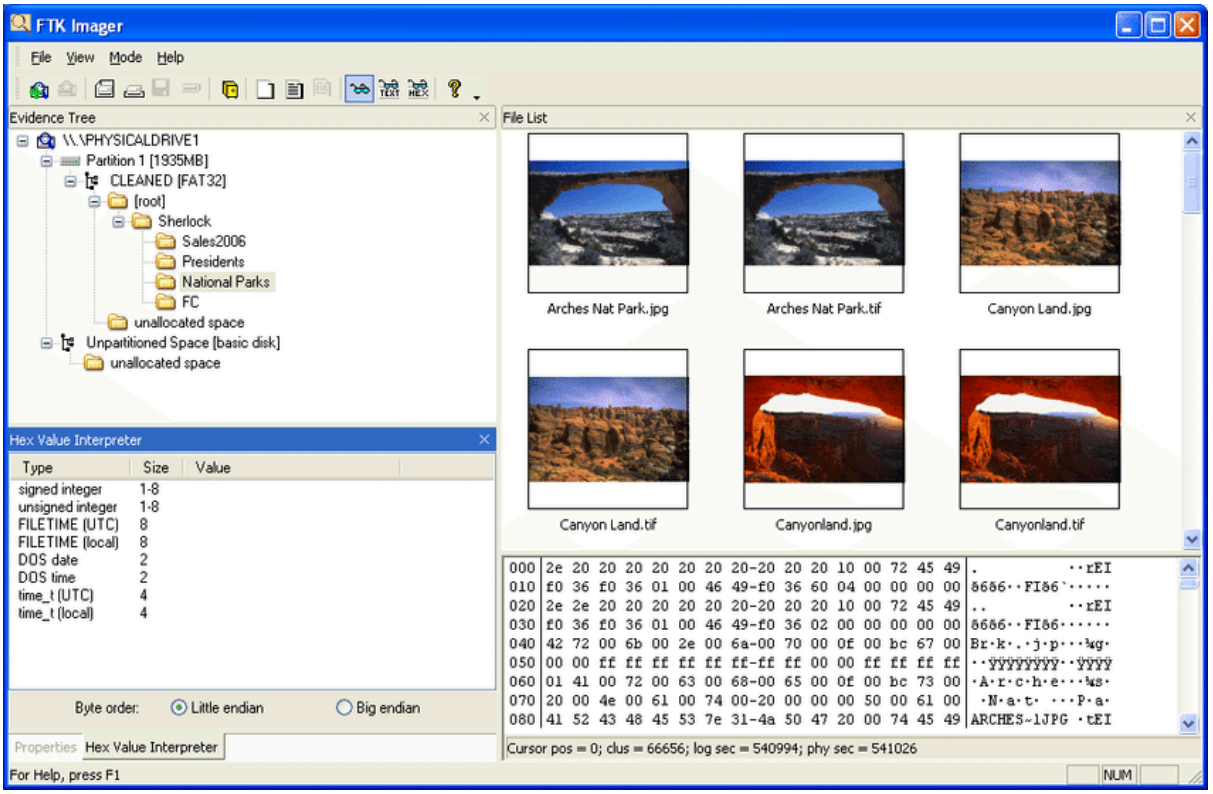


Figure 2.14 : FTK Imager screenshot

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: Understand modern security challenges and solutions.

Topics Covered:

- Mobile OS Security: Android, iOS
- IoT Device Security and Vulnerabilities
- Cloud Security: IaaS, PaaS, SaaS, IAM, MFA

Practical Exercises:

1. Test a mobile app for security flaws.
2. Scan IoT devices for vulnerabilities.
3. Configure secure IAM and MFA in a cloud lab environment.

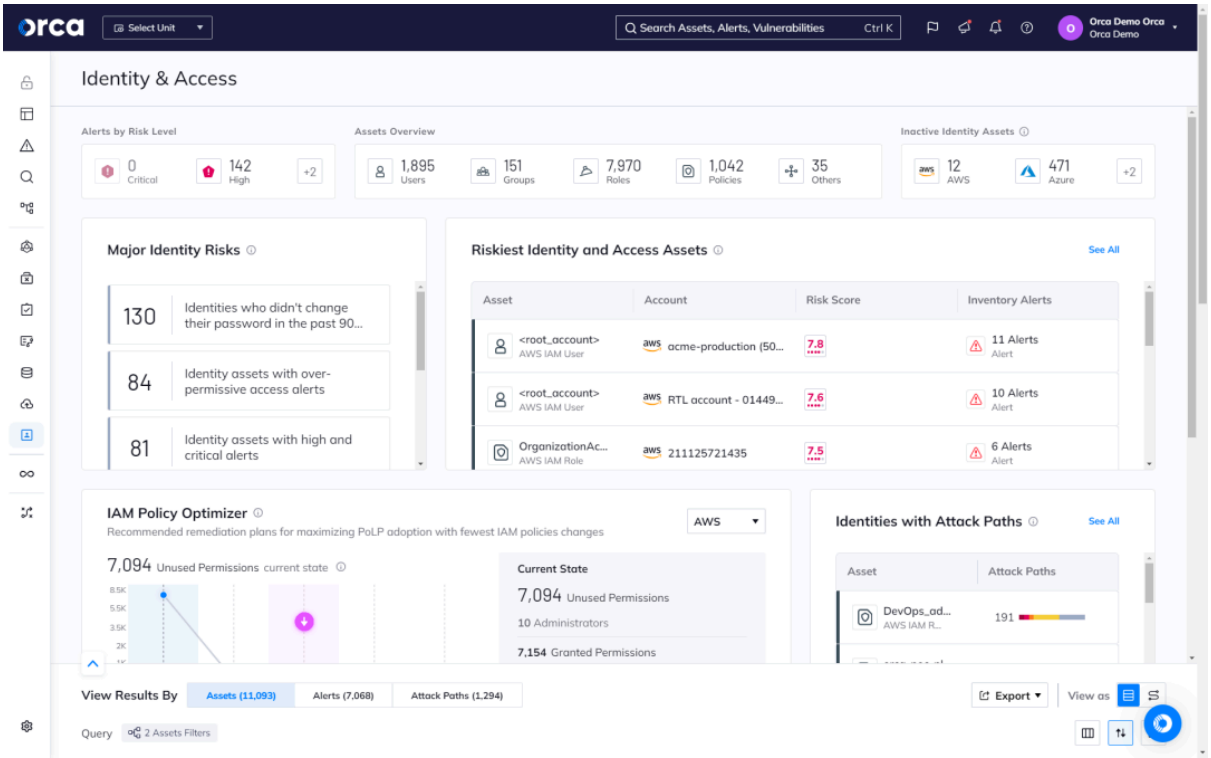


Figure 2.15: Evidence collection checklist

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.

Topics Covered

1. 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.

Key practices included:

- **Patch Management:** Regularly updating the operating system and installed software to fix security vulnerabilities.
- **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 aims to strengthen the security posture of network devices, routers, and firewalls to protect data in transit and prevent unauthorized access.

The following concepts were covered:

- **Virtual Private Networks (VPNs):** Configuring VPN tunnels to encrypt traffic between remote clients and corporate networks. This ensures secure communication even over untrusted networks.

- **Firewall Rules:** Setting inbound and outbound traffic rules to control which applications or ports are accessible.

- **Network Segmentation:** Dividing large networks into smaller segments (subnets) to contain potential breaches.

- **Intrusion Prevention Systems (IPS):** Implementing IPS mechanisms to detect and block suspicious traffic patterns.

- **Secure Protocols:** Replacing insecure protocols such as FTP and Telnet with SSH and SFTP.

Practical exercises included creating custom firewall policies using **iptables**, verifying rules with ufw status, and testing VPN configurations to ensure encryption and tunneling functionality.

---

3. Threat Hunting Basics using EDR and SIEM Tools

Threat hunting involves proactively searching for indicators of compromise (IOCs) within networks or systems before automated tools detect them.
This process combines analytical thinking with threat intelligence to identify hidden or stealthy attacks that evade traditional defenses.

Key components discussed were:

- **EDR (Endpoint Detection and Response):** Tools such as Microsoft Defender for Endpoint and CrowdStrike Falcon monitor endpoint activities, detect anomalies, and support response actions like isolating infected devices.

- **SIEM (Security Information and Event Management):** Platforms like Splunk and IBM QRadar aggregate logs from multiple sources, correlate events, and generate alerts for suspicious behaviors.

- **Threat Intelligence Feeds:** Integration of real-world attack patterns and indicators from open-source intelligence to enhance detection.

- **Incident Response Workflow:** Identifying, analyzing, containing, and eradicating threats from affected systems.

Hands-on activities included simulating log monitoring using **Wazuh** (an open-source SIEM tool) and identifying suspicious PowerShell commands or failed login attempts in Windows Event Logs.

Practical Exercises

1. **Apply Hardening Techniques on Lab Machines**
    - Disabled unused services and user accounts.
    - Implemented password complexity and lockout policies.
    - Configured firewalls and automatic updates.
2. **Monitor Network Traffic for Suspicious Activity**
    - Used Wireshark to observe network packets and detect anomalies.
    - Set up IDS rules to generate alerts on unauthorized access attempts.
3. **Document Threat Hunting Steps and Outcomes**
    - Recorded identified IOCs (Indicators of Compromise).
    - Documented mitigation actions and lessons learned for future improvement.

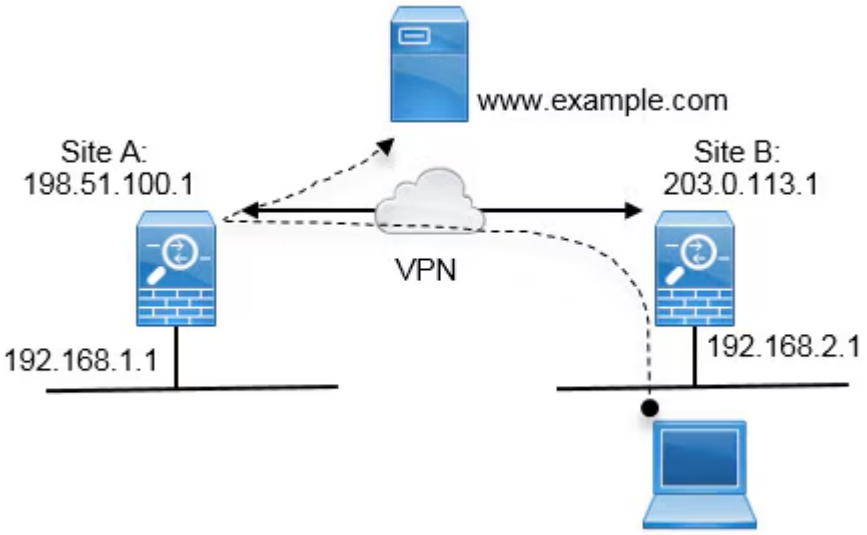


Figure 2.16: Example VPN configuration

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 provided a **structured progression from fundamentals to advanced techniques**.
Trainees gained **hands-on experience** with Linux and Windows OS, network configurations, vulnerability assessment, penetration testing, malware analysis, and defensive strategies.

By the end of the program, participants were confident in:

- Operating securely in both Linux and Windows environments
- Conducting vulnerability scans and penetration tests
- Performing malware analysis and incident response
- Implementing hardening and defensive security measures

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:
To identify active hosts, open ports, and running services on a target network using Nmap.

Tools Used:

- Nmap
- Zenmap (GUI interface)
- Wireshark

Procedure:

1. Open terminal and execute basic scan command:

   —> nmap -sP 192.168.1.0/24

   This command detects all live hosts in the subnet.

2. Perform service version detection:

   —> nmap -sV 192.168.1.10

   It identifies open ports and corresponding service versions

3. Conduct OS detection and vulnerability scan:

   —>nmap -A -T4 192.168.1.10

Observations:

- Multiple devices were discovered within the local subnet.
- Ports **22 (SSH)**, **80 (HTTP)**, and **445 (SMB)** were open on specific hosts.
- Version detection indicated outdated Apache server software, a potential vulnerability.

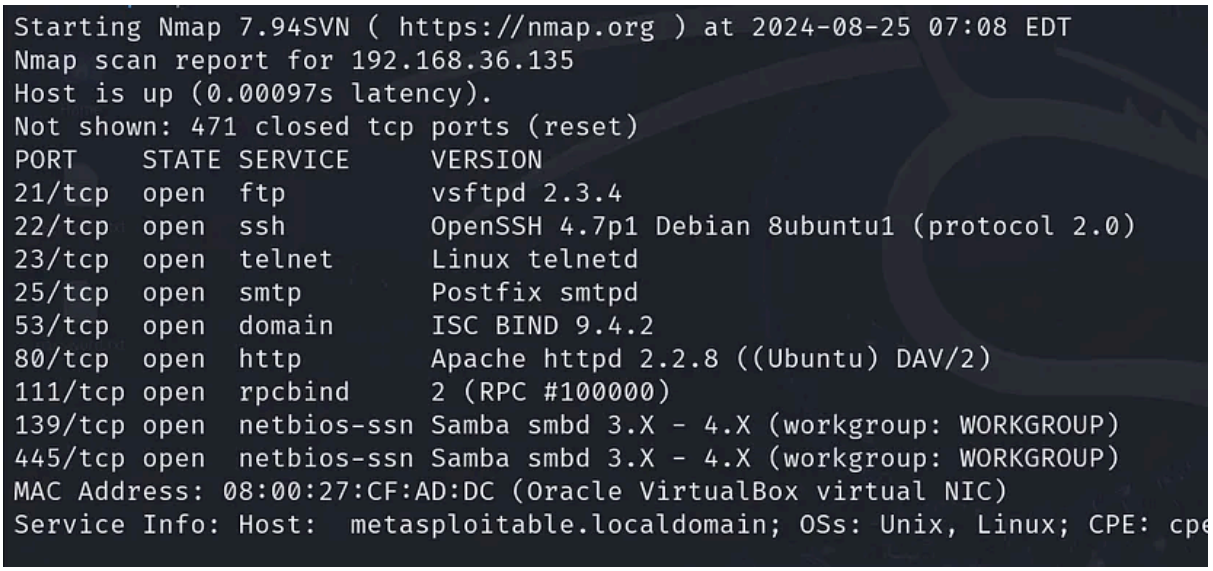


Figure 3.1: Sample Nmap Scan Output

3.3 Packet Capture and Analysis (Wireshark)

Objective:
To analyze live network traffic and identify potential anomalies or malicious packets.

Tools Used:
Wireshark (Network Protocol Analyzer)

Procedure:

1. Launch Wireshark and start capture on active interface (e.g., eth0 or Wi-Fi).
2. Apply filters for specific protocols like HTTP, DNS, and TCP.

3. Inspect captured packets for suspicious payloads or repeated retransmissions.

Observations:

- DNS requests were observed for normal browsing activity.
- Some TCP retransmissions indicated packet loss in network communication.
- No suspicious IPs or ARP spoofing attempts were detected during normal traffic.
-

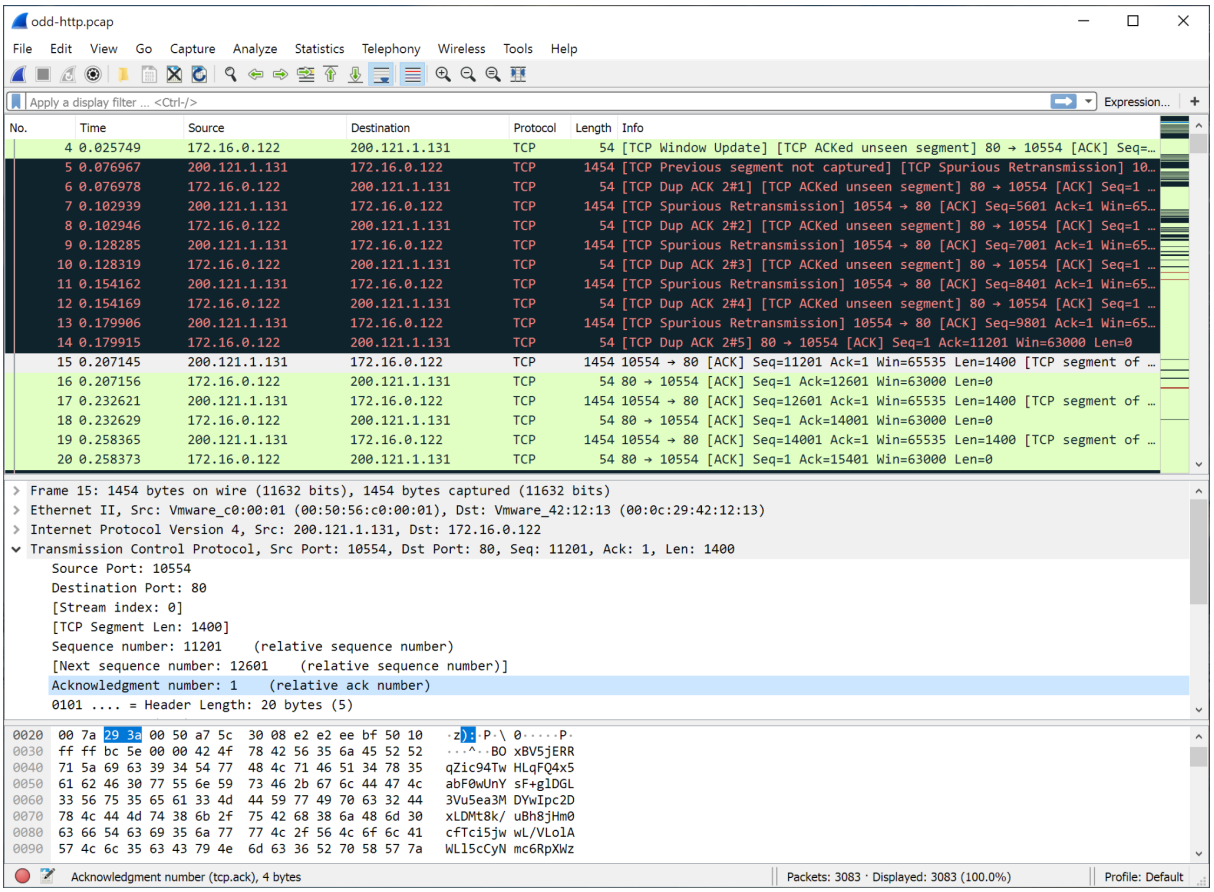


Figure 3.2: Captured Packets in Wireshark

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.

3.4 Vulnerability Assessment

Objective:
To identify system and network vulnerabilities using automated scanning tools.

Tools Used:

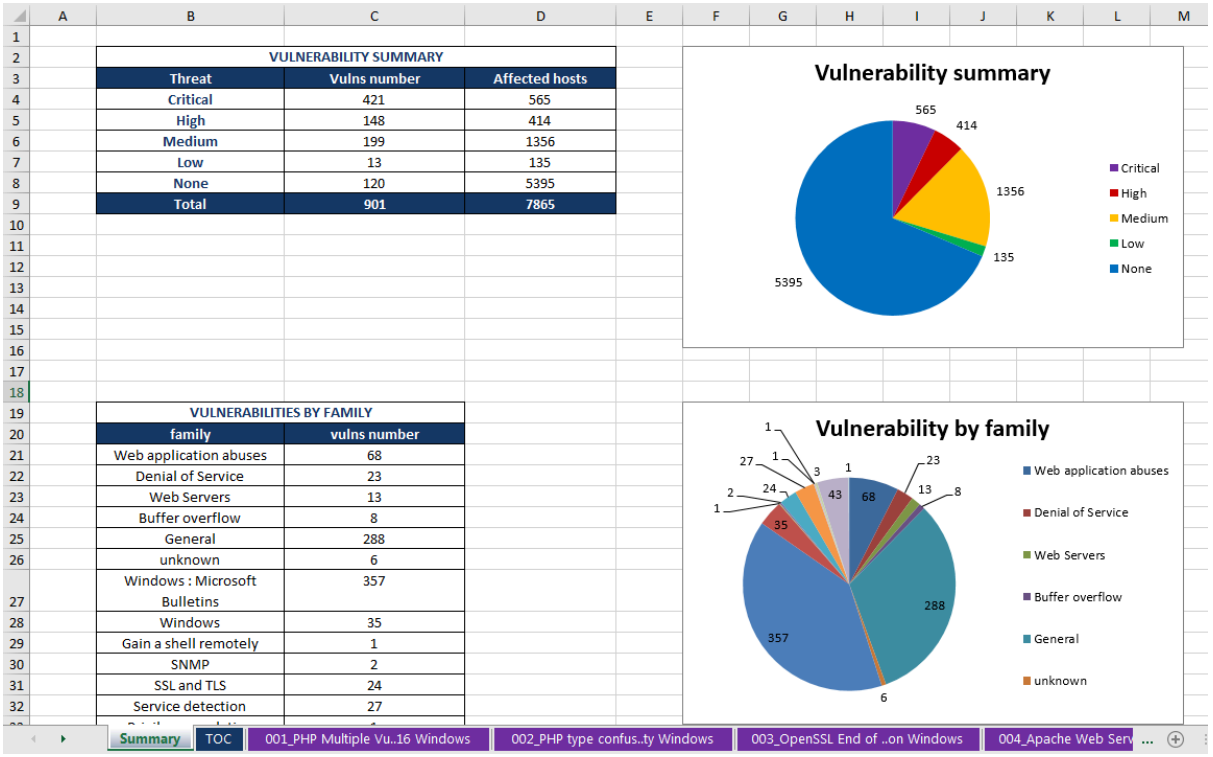
- OpenVAS / Nessus
- CVSS Calculator
- Nmap Scripts

Procedure:

1. Run vulnerability scan using OpenVAS against selected target.
2. Export results in HTML or PDF format for review.
3. Map vulnerabilities using CVSS base scores.

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 vulnerability scan results emphasize the importance of timely patching and disabling outdated services. Mapping results with **CVSS** provides a quantitative measure for prioritizing remediation steps.

3.5 Firewall and IDS Configuration

Objective:

To configure firewall rules and intrusion detection mechanisms for proactive defense.

Procedure:

1. Configured **iptables** rules on Linux to block all incoming connections except SSH and HTTP.

2. Installed and configured **Snort IDS** for packet inspection.

3. Tested detection by generating simulated attack traffic.

Results:

- Firewall blocked unauthorized pings and FTP attempts.
- Snort successfully logged alert messages for ICMP flood simulation.

Discussion:
The configuration demonstrated how rule-based systems prevent unauthorized access and detect malicious activities, forming a strong line of defense in network security.

3.6 Malware Analysis and Forensics

Objective:
To identify and analyze malware behavior using sandbox and forensic techniques.

Procedure:

1. Executed sample malware in a **controlled virtual machine**.

2. Observed process creation, registry modification, and network activity.

3. Used **Procmon** and **Wireshark** for real-time monitoring.

Results:

- Malware attempted to modify startup entries in Windows registry.
- Created suspicious connections to unknown IP addresses.
- Forensic analysis revealed persistence mechanisms used by malware.

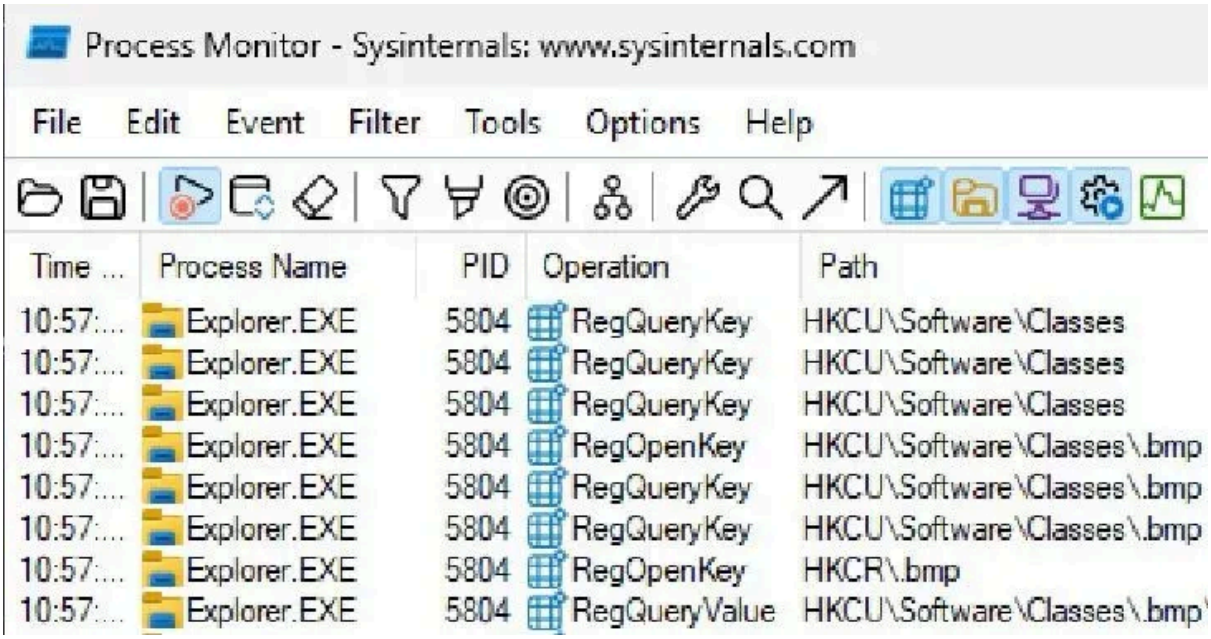


Figure 3.4: Procmon Capture of Malware Activity

Discussion:

The exercise enhanced understanding of malware behavior and emphasized the need for controlled sandbox environments to prevent real-world infections.

3.8 Summary

The experiments and results discussed in this chapter provided hands-on experience across various cybersecurity domains — network analysis, vulnerability detection, encryption, and digital forensics.

Through practical implementation, participants gained a deeper understanding of how different tools and techniques interconnect to create a complete security framework.

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 marks an important step in understanding the real-world challenges of cybersecurity.
By applying the techniques learned — from system hardening to vulnerability management — participants are now equipped to implement and maintain secure computing environments.
Continuous learning, ethical responsibility, and awareness will be key in adapting to the future landscape of cybersecurity.

REFERENCES

[1] William Stallings, *Cryptography and Network Security: Principles and Practice*, 8th Edition, Pearson, 2019.

[2] Andrew S. Tanenbaum, David J. Wetherall, *Computer Networks*, 5th Edition, Pearson, 2011.

[3] Behrouz A. Forouzan, *Data Communications and Networking*, 5th Edition, McGraw-Hill, 2012.

[4] Georgia Weidman, *Penetration Testing: A Hands-On Introduction to Hacking*, 2nd Edition, No Starch Press, 2014.

[5] Michael T. Simpson, et al., *Computer Forensics: Cybercriminals, Laws, and Evidence*, Cengage Learning, 2018.

[6] NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, 2018. [Online]. Available: https://www.nist.gov/cyberframework

[7] OWASP, *OWASP Top Ten Security Risks*, 2021. [Online]. Available: https://owasp.org/www-project-top-ten

[8] Wireshark Foundation, *Wireshark User's Guide*, 2023. [Online]. Available: https://www.wireshark.org/docs/wsug_html/

[9] Offensive Security, *Metasploit Unleashed: Metasploit Framework Guide*, 2022. [Online]. Available: https://www.offensive-security.com/metasploit-unleashed/

[10] CVSS Special Interest Group, *Common Vulnerability Scoring System v3.1*, 2019. [Online]. Available: https://www.first.org/cvss/

THANK YOU

I would like to express my sincere gratitude to everyone who supported me during the completion of this one-month industrial training and report.

A special thanks to **Sensation Software Solutions Pvt. Ltd., Ludhiana**, for providing a practical platform to learn and apply cybersecurity concepts.

I am also thankful to **Guru Nanak Dev Engineering College, Ludhiana**, my project guide, faculty members, and peers for their guidance, encouragement, and continuous support.

This experience has been invaluable in enhancing my knowledge, skills, and confidence in the field of **Cybersecurity**.

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