IBM Summer Training Report

On

Cyber Security

BTech – CSE

Submitted to

LOVELY PROFESSIONAL UNIVERSITY

PHAGWARA, PUNJAB

From 03/06/2024 to 15/07/2024

SUBMITTED BY

Name of the student: Jayant Kumar

Registration Number: 12217465

Signature of the student: Jayant

DECLARATION

I, **Jayant Kumar, 12217465** hereby declare that the work done by me on **"Network Taffic Analyzer"** from **June,2024** to **July,2024,** is record of original work for the partial fulfilment of the requirements for the award of the degree, **BTech Cyber Security.**

Name of the student: Jayant Kumar

Registration Number: 12217465

Signature: Jayant

Dated: July 2024

Allsoft Solutions

2024

A Pioneer organization& IBM Business Partner

Date: June, 2024

TO WHOM IT MAY CONCERN

This is to certify, Jayant Kumar student of Lovely Professional University, Phagwara has undergone 6 Weeks Summer Training on IBM project and technologies with us. The detailsare as follows: -

PROJECT NAME	Network Traffic Analyzer
TRAINING PERIOD	June 2024-July 2024
TECHNOLOGY	Python , Paramiko , Sockets , Threads , Virtual Machines
DURATION OF TRAINING	6 Weeks
REFERENCE NUMBER	AIP/CEP2024/IN/ 4052
SUBJECT MATTER EXPERT	Mr. Mahendra Rathaur
ACHIEVEMENTS	Project Completion Certificate and Declaration Letter

During the training, assessment and project period we find the students sincere, hardworking and having good behavior and moral character.

We wish intern all success in future endeavors.

Mr. S. K Garg
In charge | Delivery
Allsoft Solutions and Services

IBM Silver Business Partner

For Allsoft Solutions & Services

Authorised Signatory

Allsoft Solutions
An ISO 9001 : 2008 Certified Company

PROJECT COMPLETION CERTIFICATE

In recognition of the commitment to achieve professional excellence this is to certify that Ms./Mr.

Jayant Kumar

has successfully completed an Industry-oriented project.

Project Name	Network traffic analyzer
Technologies Used	Python
Reference No.	AIP/CEP2024/IN/ 4052
Training Date	3rd June to 15th July
Training Duration	6 Weeks
Training Location	Allsoft Solutions & Services Pvt. Ltd. (NCR/Mohali)

Program Co-ordinator
Industry/Academic Alliance

Business Partner IBM

Director
Training and Development
Allsoft Solutions and Services

BIG DATA - ANALYTICS | IoT | ORACLE | J2EE | PHP | CLOUD COMPUTING

IBM **SkillsBuild** Completion Certificate

This certificate is presented to

Jayant Kumar

for the completion of

Cybersecurity Fundamentals (New design; earn a credential!)

(PLAN-805005E992EA)

According to the Your Learning Builder - Plans system of record

Completion date: 15 Jul 2024 (GMT)

Contents

c. Various departments and their functions
d. Components Table

2. Overall Training Overview

a. Unit 1: Security Overview
b. Unit 2: IP Scanning, Foot-printing & Reconnaissance
c. Unit 3: Virtualization and Sniffing
d. Unit 4: Injection, Cross-Site Scripting, Missing Function Level Access Control
e. Unit 5: Web Application Security Fundamentals

3. Project

a) Introduction
b) Methodology
c) Implementation
d) Results and Analysis
e) Installation and Usage
f) Operational Workflow
g) Working Principle
h) Future Applications
i) Conclusion

1.INTRODUCTION OF IBM

a. Vision and Mission:

The mission of IBM is to lead in creating, developing, and manufacturing the industry's most advanced information technologies, including computer systems, software, networking systems, storage devices, and microelectronics. And our worldwide network of IBM solutions and services professionals translates these advanced technologies into business value for our customers. We translate these advanced technologies into value for our customers through our professional solutions, services, and consulting businesses worldwide. The Company reiterates its position and leadership responsibilities in the IT sector throughout its mission statement.

The vision of IBM is to be the world's most successful and vital information technology company. Successful in helping customers apply technology to solve their problems. Successful in introducing this extraordinary technology to new customers. Important, because we will continue to be the basic resource of much of what is invested in this industry. The IT firm stresses its influential position in the industry and its determination to retain it.

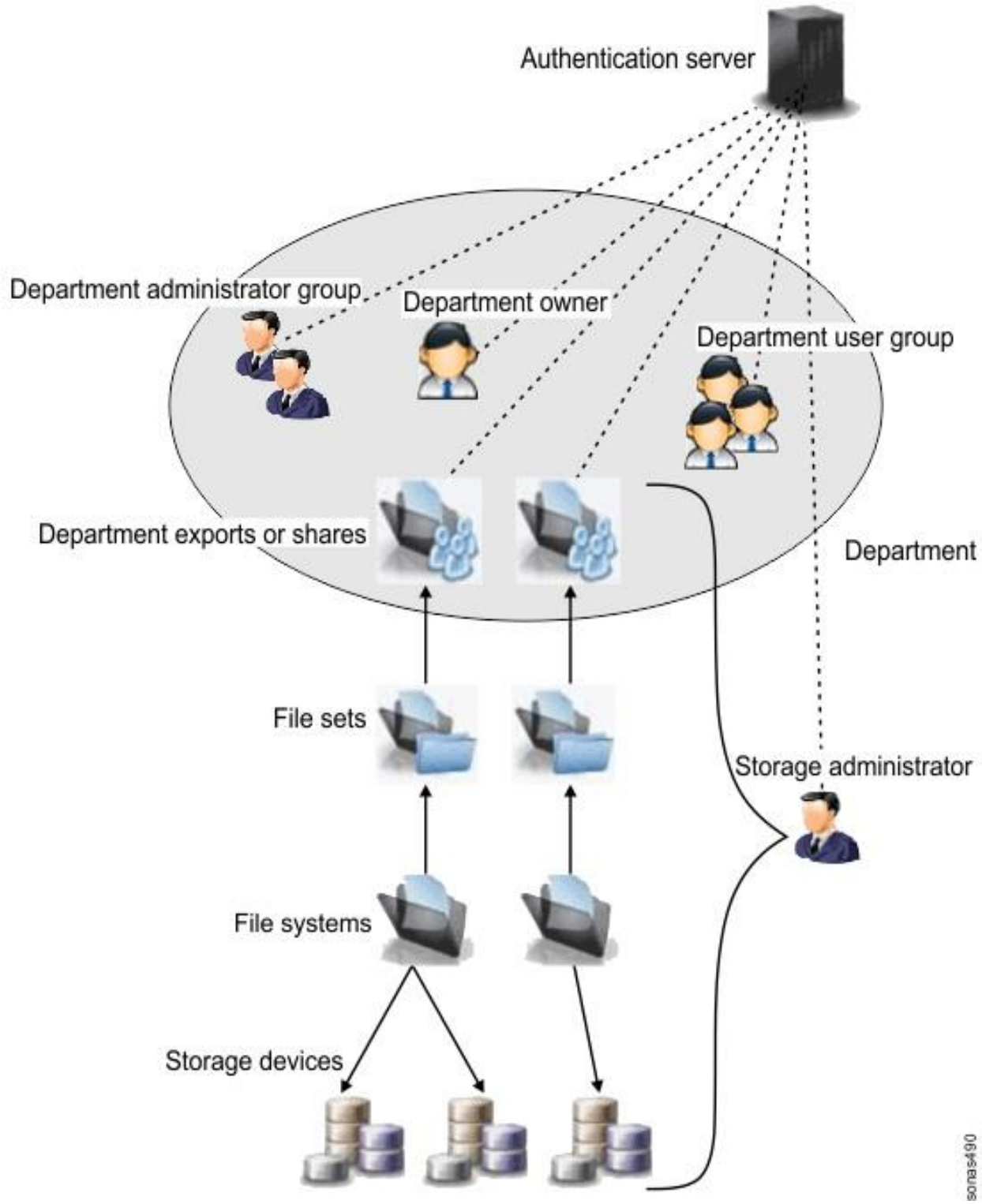
b. Origin and growth:

IBM was founded in 1911 in Endicott, New York; as the Computing-Tabulating-Recording Company (CTR) and was renamed "International Business Machines" in 1924.IBM is incorporated in New York and has operations in over 170 countries. In the 1880s, technologies emerged that would ultimately form the core of International Business Machines (IBM). Julius E. Pitrap patented the computing scale in
1885; Alexander Dey invented the dial recorder (1888); Herman Hollerith (1860–1929) patented the Electric Tabulating Machine; and Willard Bundy invented a time clock to record workers' arrival and departure times on a paper tape in 1889.On June 16, 1911, their four companies were amalgamated in New York State by Charles Randlett Flint forming a fifth company, the Computing-TabulatingRecording Company (CTR) based in Endicott, New York. The five companies had 1,300 employees and offices and plants in Endicott and Binghamton, New York; Dayton, Ohio; Detroit, Michigan; Washington, D.C and Toronto.

After pioneering the multipurpose microcomputer in the 1980s, which set the standard for personal computers, IBM began losing its market dominance to emerging competitors. Beginning in the 1990s, the company began downsizing its operations and divesting from commodity production, most notably selling its personal computer division to the Lenovo Group in 2005. IBM has since concentrated on computer services, software, supercomputers, and scientific research. Since 2000, its supercomputers have consistently ranked among the most powerful in the world, and in 2001 it became the first company to generate more than 3,000 patents in one year, beating this record in 2008 with over 4,000 patents. As of 2022, the company held 150,000 patents. As one of the world's oldest and largest technology companies, IBM has been responsible for several technological innovations, including the automated teller machine (ATM), dynamic random-access memory (DRAM), the floppy disk, the hard disk drive, the magnetic stripe card, the relational database, the SQL programming language, and the UPC barcode. The company has made inroads in advanced computer chips, quantum computing, artificial intelligence, and data infrastructure. IBM

employees and alumni have won various recognitions for their scientific research and inventions, including six Nobel Prizes and six Turing Awards.

c. Various departments and their functions:



d. Component Table

S. No.	Component Name	Component Description

1.	Storage devices	Storage devices are a set of storage disks on the IBM Storwize V7000 Unified system. File systems are created over storage disks.
2.	File systems	A file system is a collection of files and their attributes. File sets are created over file systems. The department model feature can be implemented over multiple file systems or on one file system, depending on the business scenario.
3.	Department	A department is an organizational unit with a specific business purpose. Hardware, software entities, and people are the assets of a department. Typically, every department is associated with a department owner. The department's members can be members of the department administrator group or the department user group. Every department gets a system-generated universal unique ID (UUID) that is associated with the department for its entire lifecycle. The UUID cannot be modified.
4.	Storage administrator	A storage administrator is an IBM Storwize V7000 Unified CLI user who manages departments and their associated storage resources. The storage administrators might need to set quota limits or manage quotas for file sets that are associated with a department, as directed by the department owner. A storage administrator performs the following tasks: • Create a department. • Modify a department. • List or view a department. • Verify that the properties of a department are correct. • Manage file sets and storage resources. • Manage department exports or shares
5.	Authentication server	All department users and user groups must be defined in the organization's authentication server such as Lightweight Directory Access Protocol (LDAP) and Microsoft Active Directory. If any of these definitions change in the authentication server, the storage administrator must manually update the department properties.

2. Overall Training Overview

a. Unit 1: Security Overview

Unit 1 serves as the foundational module in understanding information security, establishing essential principles that govern the protection of data in the digital age. The unit begins with a definition of information security, highlighting its importance in safeguarding against unauthorized access, use, disclosure, disruption, modification, or destruction of information.

i. Principles of Information Security

The unit covers the core principles of information security, often referred to as the CIA triad—Confidentiality, Integrity, and Availability:

- Confidentiality ensures that information is accessible only to those authorized to have access, through mechanisms like encryption and access controls.
- Integrity refers to maintaining the accuracy and reliability of data, which can be enforced through hashing algorithms and audit trails.
- Availability guarantees that authorized users have timely and reliable access to information and resources, achieved through redundant systems and backups.

These principles are fundamental in developing a comprehensive security strategy within organizations.

ii. Emerging Threats

As technology advances, so do the methods employed by cybercriminals. The unit identifies and discusses various emerging threats in today's digital landscape, such as:

- Ransomware: Malicious software that encrypts data and demands payment for decryption.
- Phishing: Attempts to acquire sensitive information by masquerading as trustworthy entities in electronic communications.
- Social Engineering: Techniques utilized by attackers to manipulate individuals into divulging confidential information.

A deeper understanding of these threats is essential for security professionals, as they create a framework from which preventive and responsive measures are developed.

iii. Attack Vectors

The concept of "attack vectors" is crucial, as it refers to the pathways that attackers utilize to infiltrate systems. These can include:

- Network Vulnerabilities: Unsecured networks or misconfigured devices can be exploited to gain unauthorized access.
- User Behavior: Poor practices such as weak password management or lack of awareness regarding phishing can create exploitable entry points.

This aspect of the unit emphasizes the importance of conducting thorough risk assessments to identify potential vulnerabilities and address them proactively.

iv. Defense in Depth

One of the core strategies emphasized in this unit is "Defense in Depth." This multi-layered security approach advocates that no single security measure is sufficient; rather, organizations need to implement multiple layers of security controls suited for different threats. Key components include:

- Technical Controls: Firewalls, intrusion detection systems (IDS), and anti-virus software.
- Administrative Controls: Policies, procedures, and training programs that foster security awareness among employees.
- Physical Controls: Securing physical access to systems and data through locks, surveillance, and secure data centers.

This strategy is complemented by a holistic organizational approach, ensuring all personnel understand the critical role they play in maintaining security.

v. Google Hacking

A unique topic introduced is Google hacking, which involves using advanced search techniques to gather sensitive information from the web. This section provides insights into the methods that attackers might employ to find misconfigured databases, exposed credentials, and other sensitive information that can aid in launching further attacks. Understanding these tactics is also vital for security professionals to better protect their information assets.

vi. Malware Analysis

The unit concludes with a discussion on various forms of malware, including:

- Trojans: Malicious software disguised as legitimate applications that can gain unauthorized access to systems.
- Viruses: Self-replicating programs that attach themselves to clean files, spreading across systems once activated.
- Worms: Standalone malware that replicates itself to spread to other devices without human intervention.

A thorough understanding of malware mechanics reinforces the necessity for consistent vigilance and implementation of preventive measures.

In summary, Unit 1 provides a comprehensive introduction to the complexities of information security, emphasizing the importance of understanding fundamental concepts, emerging threats, and robust defense strategies necessary for safeguarding information in an ever-evolving digital environment.

b. Unit 2: IP Scanning, Foot-printing, and Reconnaissance

Unit 2 dives deep into the essential practices of network reconnaissance, emphasizing its critical role in identifying vulnerabilities before they can be exploited by malicious actors. This unit breaks down the various methodologies and tools available for conducting thorough security assessments through effective data collection.

i. Foot printing

The first major topic is "footprinting," which involves gathering detailed information about a target system or network. This phase is crucial in the reconnaissance process, allowing security professionals to map out systems and identify possible vulnerabilities. The techniques discussed include:

- Passive Footprinting: Collecting information without directly interacting with the target, such as gathering data from public records, social media, and domain registration databases.
- Active Footprinting: Directly engaging with the target through queries and network probes, helping collect real-time data.

Common resources for passive footprinting include WHOIS databases, DNS records, and social engineering methods to gather intelligence.

ii. Techniques for Data Collection

The unit outlines various techniques for footprinting relevant to different layers of network technology:

- Website Footprinting: Using tools to analyze the structure of a target web application, including its technologies, subdomains, and vulnerabilities.
- Email Footprinting: Investigating email addresses and associated servers to discover misconfigurations that could be exploited.
- DNS Footprinting: Leveraging DNS queries to discover underlying network structures, identifying DNS servers, and checking for zone transfers that might reveal sensitive information.
- Network Footprinting: Mapping out network architecture and identifying devices and their roles within the network.

These techniques provide a comprehensive view of a target's technological landscape, which is vital for identifying potential security gaps.

iii. Scanning Techniques

Building on footprinting, the unit delves into scanning techniques essential for discovering open ports and identifying system vulnerabilities. Key scanning methodologies include:

- Port Scanning: Identifying open ports on a target machine to see which services are running. Tools like Nmap are extensively used for this purpose.
- Vulnerability Scanning: Conducting analysis to identify known vulnerabilities within systems and applications, utilizing tools like Nessus and OpenVAS to automate this process.

iv. Network Diagramming

The practice of network diagramming is introduced, allowing security professionals to visualize network structures effectively. This visual representation helps assess security risks and devise strategies for mitigation. Proper network diagrams can assist in identifying potential choke points, single points of failure, and areas that may be oversaturated with security risks.

v. Concealment Techniques

The unit also discusses techniques that attackers may employ to conceal their identities during reconnaissance efforts. Techniques such as:

- Proxy Chaining: Using multiple proxy servers to mask the origin of a connection, complicating the tracing of malicious activities.
- IP Spoofing: Sending packets from a false (or "spoofed") IP address, which can obscure the real IP of the attacker, making detection more challenging.

Understanding these techniques is critical for security professionals seeking to defend against such tactics.

vi. Countermeasures

Finally, this unit emphasizes the implementation of countermeasures against footprinting and scanning techniques. Key strategies include:

- Network Hardening: Strengthening network configurations to limit the exposure of critical resources and services.
- Monitoring and Alerting: Continuously monitoring network traffic for unusual activity that may indicate reconnaissance efforts.
- Access Control Lists (ACLs): Implementing rigorous ACLs to restrict unauthorized requests and limiting exposure to potential attackers.

Unit 2 synthesizes the principles of proactive security assessments and the importance of reconnaissance techniques, equipping learners with the skills necessary to identify and mitigate risks effectively in their organizational environments.

c. Unit 3: Virtualization and Sniffing

Unit 3 provides an in-depth examination of virtualization technologies and network sniffing, two critical aspects of modern network security. The unit begins with a focus on web server security, underscoring the vulnerabilities that can arise from misconfigurations or inadequate security practices. Security professionals are guided on implementing best practices for securing web servers, including patch management, proper access control, and ongoing monitoring for suspicious activities.

i. Virtualization

Virtualization is a transformative technology that enables organizations to run multiple operating systems on a single physical machine. This unit explores the several benefits that virtualization affords, including resource optimization, improved efficiency, and operational cost savings. Through virtualization, organizations can achieve better isolation of applications, thus minimizing the risk that a breach in one environment could compromise others.

The unit focuses on configuring virtual machines using VMware, a widely adopted platform, detailing the processes for installation, resource allocation, and network integration. Best practices for managing virtual environments are also underscored, including:

- Isolation: Ensuring that virtual machines operate in isolated environments to mitigate risks of cross-contamination.
- Backup and Recovery: Implementing robust backup strategies to ensure quick recovery in the event of a failure or breach.
- Monitoring and Management: Using tools to monitor the performance and security of virtual environments.

ii. Network Sniffing

The exploration of network sniffing introduces learners to techniques utilized by attackers to capture and analyze network traffic. The unit describes specific methods of network sniffing, such as ARP poisoning, where an attacker sends forged ARP messages over a local area network. This deceives systems into associating the attacker's MAC address with the IP address of a legitimate device, allowing the attacker to intercept and manipulate traffic.

Another significant topic is DNS (Domain Name System) poisoning, where attackers corrupt DNS records to redirect users to malicious websites. This practice can perform various attacks, including phishing and data exfiltration.

Countermeasures against sniffing attacks are emphasized throughout the unit. Key strategies include employing:

- Encryption: Implementing protocols such as SSL/TLS to secure data in transit.
- Network Segmentation: Dividing networks into segments to limit attacker access to sensitive data.
- Intrusion Detection Systems (IDS): Implementing IDS tools to monitor network traffic for anomalies and alert administrators of potential breaches.

The human factor in security, including social engineering attacks, is also addressed, highlighting the necessity of employee training to recognize and respond to manipulative tactics.

Finally, the unit discusses Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, detailing their mechanisms and potential impacts on organizations. These attacks overwhelm systems with traffic, rendering them unusable. Organizations are encouraged to adopt prevention and response strategies, such as rate limiting, redundant systems, and effective incident response plans.

d. Unit 4: Injection, Cross-Site Scripting, Missing Function Level Access Control

Unit 4 focuses intensely on vulnerabilities prevalent in web applications, with particular emphasis on injection flaws and cross-site scripting (XSS) attacks. By illuminating these vulnerabilities, the unit aims to enhance learners' ability to identify, assess, and mitigate security risks associated with modern web applications.

i. SQL Injection

The unit begins with an exploration of SQL injection, one of the most notorious web application vulnerabilities. Learners gain a comprehensive understanding of how attackers can exploit applications by injecting malicious SQL queries through input fields. The steps taken by attackers to manipulate databases through unsanitized inputs are meticulously illustrated, enhancing awareness of the consequences that can arise from such breaches.

To counter SQL injection vulnerabilities, the unit reviews:

- Input Validation: Ensuring that all inputs to an application are checked and sanitized before processing.
- Prepared Statements and Parameterized Queries: Using these methods to separate SQL code from data inputs, thereby preventing malicious data from altering the intended execution of SQL commands.

ii. Cross-Site Scripting (XSS)

Cross-Site Scripting attacks are thoroughly examined next. These attacks enable attackers to inject malicious scripts into web pages viewed by other users, potentially compromising user sessions or stealing sensitive cookies. The unit details how XSS attacks can manifest in various forms, including stored, reflected, and DOM-based XSS, each requiring distinct mitigation strategies.

Countermeasures against XSS include:

- Content Security Policy (CSP): Implementing CSP to control resources the user agent is allowed to load, thereby mitigating the impact of XSS.
- Input Encoding: Ensuring outputs are properly encoded so that any scripts are rendered harmless when presented to users.

iii. Insecure Direct Object References

The unit also addresses Insecure Direct Object References (IDOR), where attackers gain unauthorized access to resources or data by manipulating parameters in requests. This discussion emphasizes the need for proper access control mechanisms to validate user permissions before granting access to sensitive objects.

Further considerations include security misconfigurations, which can lead to exposure of sensitive data through neglected security settings, such as default credentials or overly permissive settings for S3 buckets. Techniques to defend against these vulnerabilities are explored.

Moreover, the unit highlights the critical importance of protecting sensitive data through encryption and secure transmission protocols. Learners are educated on best practices for managing sensitive data, reinforcing the notion that data protection is paramount in web security.

iv. Cross-Site Request Forgery (CSRF)

Finally, the unit concludes with an overview of Cross-Site Request Forgery (CSRF) attacks. The discussion focuses on how attackers can trick users into executing unwanted actions on authenticated applications. To combat CSRF, the necessity of incorporating anti-CSRF tokens in forms, maintaining user session integrity, and leveraging the SameSite cookie attribute is elaborated.

In summary, Unit 4 equips learners with a robust understanding of prevalent application vulnerabilities and effective security practices. By the end of this unit, participants will be better prepared to implement strategies aimed at fortifying web applications against common threats.

e. Unit 5: Web Application Security Fundamentals

Unit 5 provides a comprehensive exploration of web application security, centering around the OWASP Top 10—an essential framework that highlights the most significant security risks to web applications. This unit articulates a holistic approach to securing applications from inception to deployment.

i. OWASP Top 10

The unit begins by unpacking the OWASP Top 10 vulnerabilities, including injection flaws, authentication issues, sensitive data exposure, and insecure direct object references. Each vulnerability is examined, providing learners with an in-depth understanding of its impact, characteristics, and remedial actions. This foundational knowledge arms developers and security professionals with the insights required to prioritize security throughout the software development lifecycle.

ii. Practical Vulnerability Testing

Participants are engaged in practical exercises that involve the installation and setup of web application vulnerability testing solutions. Emphasis is placed on utilizing various tools to conduct security assessments and identify vulnerabilities in web applications actively. Lessons cover configuring and optimizing scans, which enable learners to remedy vulnerabilities efficiently before application deployment.

iii. Session Hijacking and Countermeasures

The unit further delves into session hijacking tactics, where attackers eavesdrop on user sessions to gain unauthorized access. Techniques such as session fixation and cookie theft are discussed in detail, alongside preventive measures like:

- HTTPS: Enforcing the use of HTTPS to encrypt sessions and protect transmitted cookies.
- Secure and Http Only Flags: Using these cookie attributes to limit exposure to client-side scripts.

iv. Intrusion Detection Systems (IDS)

An introduction to Intrusion Detection Systems (IDS) is a foundational component of this unit. The importance of these systems lies in their ability to monitor and analyze network traffic for suspicious activities. Participants learn how IDS can alert security teams to potential breaches and facilitate rapid response efforts.

v. Incident Response and Computer Forensics

Computer forensics and incident response procedures are outlined, highlighting the critical steps organizations must take following a security incident. This includes preserving evidence, performing investigations, and preparing reports that can be used for remediation and possible legal action. The discussion stresses the importance of maintaining a chain of custody for digital

evidence to support thorough investigations and maintain integrity in legal scenarios.

vi. Building a Security Culture

The unit emphasizes building a security culture within organizations, highlighting the importance of ongoing employee training, awareness programs, and the implementation of security policies that encourage vigilance among personnel.

In conclusion, Unit 5 serves as a comprehensive guide that combines theoretical knowledge with practical skills, empowering learners to identify, assess, and address vulnerabilities within web applications. By the end of the unit, participants will be well-equipped to enhance the security posture of their organizations, mitigating risks and protecting valuable digital assets effectively.

3. PROJECT

Abstract

This project focuses on developing a Network Traffic Analyzer tool using Python. The tool captures and analyzes network packets to provide insights into network activity. Utilizing libraries such as Scapy, Pyshark, and Psutil, the tool performs packet sniffing, filtering, and analysis. This report details the design, implementation, and results of the project, highlighting its significance in understanding network traffic patterns.

Introduction

Network traffic analysis is the process of capturing and examining network packets to understand the data flow across a network. It is essential for diagnosing network issues, monitoring performance, and ensuring network security.

1. Importance of Network Traffic Analysis

Analyzing network traffic is crucial for identifying potential security threats, optimizing network performance, and ensuring compliance with network policies.

2. Objectives of the Project

The primary objective of this project is to develop a tool that captures and analyzes network packets, providing insights into network traffic patterns and helping in identifying potential security threats.

Methodology

1. Tools and Technologies Used

Python: The primary programming language used for developing the tool.
Scapy: A Python library for packet manipulation and sniffing.
Pyshark: A Python wrapper for the Wireshark packet analysis engine.
Psutil: A Python library for retrieving information on system utilization and network interfaces.

2. Development Environment and Setup

The development environment includes Python 3.x, along with the necessary libraries installed via pip. The setup also involves configuring network interfaces for packet capture.

3. Workflow and Design of the PacketAnalyzer Tool

The tool is designed with a modular approach, using classes and functions to handle different aspects of packet capturing and analysis.

4. Packet Capturing Techniques

The tool uses Scapy for packet capturing, allowing for flexible filtering based on protocols.

Implementation

Code Explanation and Snippets

Class: PacketAnalyzer

```python
import logging
import pyshark
import psutil
from scapy.all import sniff, wrpcap

class PacketAnalyzer:
    def __init__(self):
        self.captured_packets = []

    def packet_callback(self, packet):
        self.captured_packets.append(packet)
        print(packet.summary())

    def capture_packets(self, interface="eth0", count=100, filter=""):
        logging.info(f"Starting packet capture on {interface} with filter {filter}")
        try:
            packets = sniff(iface=interface, count=count, filter=filter, prn=self.packet_callback)
            wrpcap("captured_packets.pcap", packets)
            logging.info(f"Packet capture complete. {len(packets)} packets captured.")
        except Exception as e:
            logging.error(f"Error capturing packets: {e}")

    def analyze_packets(self, pcap_file):
        try:
            cap = pyshark.FileCapture(pcap_file)
            for packet in cap:
                print(f"Packet: {packet}")
                print(f"Source: {packet.ip.src}, Destination: {packet.ip.dst}")
        except Exception as e:
            logging.error(f"Error analyzing packets: {e}")

    def list_network_interfaces(self):
        try:
            interfaces = psutil.net_if_addrs()
            for interface, addrs in interfaces.items():
                print(f"Interface: {interface}")
                for addr in addrs:
                    print(f"  Address: {addr.address}")
        except Exception as e:
            logging.error(f"Error listing network interfaces: {e}")

```

Main Function:

```python
def main():
    parser = argparse.ArgumentParser(description="Network Traffic Analyzer Tool")

    parser.add_argument('-i', '--interface', type=str, help="Network interface to capture packets from")
    parser.add_argument('-p', '--protocol', type=str, help="Protocol to filter (e.g., tcp, udp, http)")
    parser.add_argument('-c', '--count', type=int, default=100, help="Number of packets to capture")
    parser.add_argument('-o', '--output', type=str, default="captured_packets.pcap", help="Output file for captured packets")
    parser.add_argument('--list-interfaces', action='store_true', help="List available network interfaces")

    args = parser.parse_args()

    analyzer = PacketAnalyzer()

    if args.list_interfaces:
        logging.info("Listing Network Interfaces:")
        analyzer.list_network_interfaces()
        return

    if args.interface and args.protocol and args.count:
        logging.info(f"Capturing Packets on Interface: {args.interface}, Protocol: {args.protocol}, Count: {args.count}")
        analyzer.capture_packets(interface=args.interface, count=args.count, filter=args.protocol)
        logging.info(f"Packets captured and saved to {args.output}")

    logging.info("Execution complete. Here are the results:")
    total_packets = len(analyzer.captured_packets)
    protocols = set(packet.payload.name for packet in analyzer.captured_packets)
    logging.info(f"Total Packets Captured: {total_packets}")
    logging.info(f"Protocols Analyzed: {', '.join(protocols)}")

if __name__ == "__main__":
    main()
```

Results and Analysis

1. Summary of Captured Data

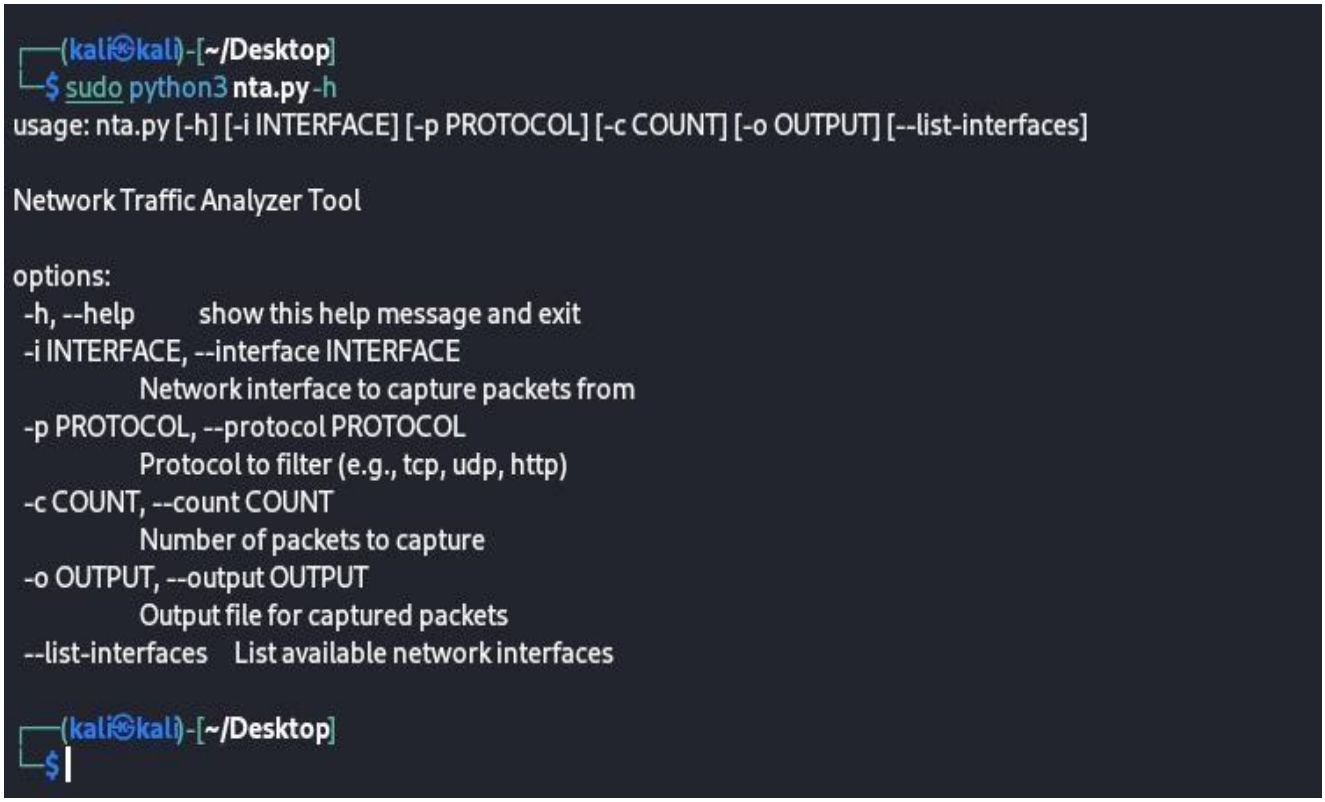
The tool captured a total of 20 packets on the specified network interface.

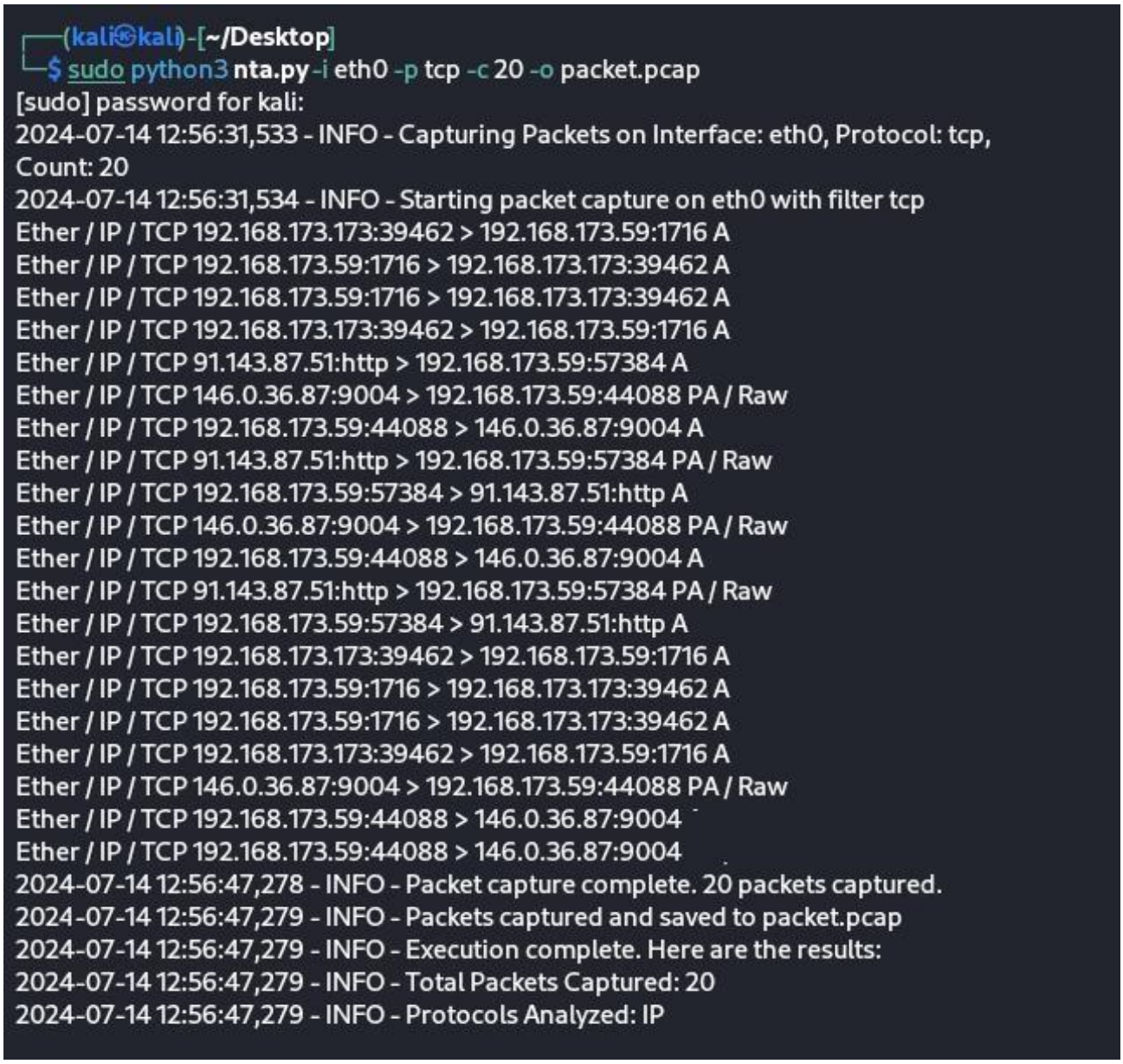
2. Analysis of Captured Packets

The captured packets include various protocols such as TCP, UDP, and HTTP. Each packet's source and destination IP addresses were logged for further analysis.

3. Screenshots of the Tool in Action

(Include screenshots showing the tool capturing and analyzing packets.)





Installation and Usage Instructions

Installation

1. Install Python 3
2. Install required libraries:

- ***pip install scapy pyshark psutil***

Usage

To capture packets on a specific interface:

- ***python analyzer.py -i eth0 -p tcp -c 100***

To list available network interfaces:

- ***python analyzer.py --list-interfaces***

Operational Workflow

The Network Traffic Analyzer tool can be initiated and configured via command-line arguments, enabling administrators to specify parameters for packet capture, analysis, or network interface listing. The following command serves as an example of how the script can be executed:

Terminal args -> Python network_traffic_analyzer.py -i eth0 -p tcp -c 100 -o captured_packets.pcap

In this example, the script captures TCP packets on interface "eth0," capturing a total of 100 packets and saving them in a file named "captured_packets.pcap." Executing the script with these parameters triggers the packet capture process, with real-time logging providing updates on the captured packets.

Working Principle

Upon command-line execution, the script parses the provided arguments and operates in the following modes:

1. Packet Capture Mode:

   The script captures packets based on specified parameters such as the network interface, protocol filter, and packet count. It leverages Scapy's functionality to capture and store packets in a PCAP file for subsequent analysis.

2. Packet Analysis Mode:

   Post packet capture, the script utilizes PyShark to conduct detailed analysis of captured packets, extracting critical data such as source and destination IP addresses, protocol information, and packet payloads.

3. Network Interface Listing Mode:

   Upon initiating the listing of network interfaces, the script uses Psutil to enumerate available interfaces and associated IP addresses, providing comprehensive information to administrators for network configuration and management.

Future Applications

The network traffic analyzer tool presents a wealth of potential applications and enhancements for advancing network monitoring, security, and performance optimization. Prominent future applications include:

1. Enhanced Security Monitoring:

   Future iterations of the tool could integrate advanced anomaly detection algorithms andthreat intelligence feeds to bolster security monitoring capabilities, enabling swift iden-tification and response to security breaches.

2. Predictive Network Maintenance:

   Through the utilization of machine learning algorithms and predictive analytics, the tool could predict network failures and issues before they occur, allowing proactive maintenance and mitigation strategies.

3. Automation and Orchestration:

   By integrating with automation frameworks, the tool could automate incident response,network configuration changes, and remediation, streamlining network management processes and enhancing operational efficiency.

4. Cloud Infrastructure Support:

   Extending the tool's capabilities to support cloud environments and virtualized net- works would enable administrators to monitor network traffic and security across hy- brid cloud infrastructures seamlessly.

Conclusion

This project successfully developed a Network Traffic Analyzer tool using Python, which captures and analyzes network packets. The tool provides valuable insights into network trafficpatterns and can be a useful resource for network administrators and cybersecurity professionals. Future enhancements will further improve its capabilities and usefulness.