Cyber Security

A Summer Training Project Report Submitted in Partial Fulfillment for the Award of the Degree of Bachelor of Technology in Computer Science and Engineering

Dr. A. P. J. ABDUL KALAM TECHNICAL UNIVERSITY, LUCKNOW

Submitted by:

Tanu Keshari (2300100100443)

UNDER THE SUPERVISION OF

Dr. Snehlata

Assistant Professor

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

UNITED COLLEGE OF ENGINEERING AND RESEARCH, PRAYAGRAJ

August,2025

CERTIFICATE

This is to certify that the project titled **"Cyber Security"** submitted by **Tanu Keshari** (2300100100443) in partial fulfillment of the requirement for the award of degree of the B. Tech. (Computer Science and Engineering) submitted to Dr. A. P. J Abdul Kalam Technical University, Lucknow at United College of Engineering and Research, Prayagraj is an authentic record of their own work carried out during a period from **31st July, 2025 to 20th August, 2025** under the guidance of **Dr. Snehlata**, Assistant Professor Department of Computer Science Engineering. The Summer Traing Project Viva-Voce Examination has been held on _____.

Signature of the Guide:
Dr. Snehlata

Signature of Project Coordinator:
Mr. Shyam Bahadur Verma

Signature of the Head of Department:
Dr. Vijay Kumar Dwivedi

Place: Prayagraj
Dated:

CANDIDATE'S DECLARATION

We, hereby certify that the project entitled **"Cyber Security"** submitted by us in partial fulfillment of the requirement for the award of degree of the B. Tech. (Computer Science Engineering) submitted to **Dr. A. P. J. Abdul Kalam Technical University, Lucknow** at **United College of Engineering and Research, Prayagraj**, is an authentic record of our own work carried out during a period from **31st July, 2025 to 20th August, 2025** under the guidance of **Dr. Snehlata, Assistant Professor**, Department of Computer Science Engineering. The matter presented in this project has not formed the basis for the award of any other degree, diploma, fellowship or any other similar titles.

Signature of the Student
Tanu Keshari(2300100100443)

Place: Prayagraj
Dated:

ACKNOWLEDGEMENTS

We express our sincere gratitude to Dr. A. P. J Abdul Kalam Technical University, Lucknow for giving us the opportunity to work on the Summer Training Project during our third year of B.Tech. (CSE) is an important aspect in the field of engineering.

We would like to thank **Dr. Swapnil Srivastav, Principal and Dr. Vijay Kumar Dwivedi, Head of Department, CSE at United College of Engineering and Research, Prayagraj** for their kind support.

We also owe our sincerest gratitude towards **Dr. Snehlata** for her valuable advice and healthy criticism throughout our project which helped us immensely to complete our work successfully.

We would also like to thank everyone who has knowingly and unknowingly helped us throughout our work. Finally, a word of thanks for the authors of all those books and papers which we have consulted during our project work as well as for preparing the report.

ABSTRACT

The creation of a Smart Campus at the United College of Engineering and Research was the brainchild of a visionary project aimed at establishing a comprehensive and fully operational campus. This prestigious institution of higher learning, located in Prayagraj City, Uttar Pradesh, has procured a reputation for excellence in all areas of engineering. With a commitment to keeping up with the latest technological advancements and trends, the college aims to spearhead an interdisciplinary initiative that will result in a Smart Campus of unparalleled functionality and efficiency. In keeping with this goal, we have proposed the incorporation of cutting-edge technologies such as blockchain to establish a micro-economy system that promises to be a game-changer in the development of the project.

Despite its immense potential, blockchain technology has only recently begun to make its mark on the engineering community. With its increasing influence and widespread social impact, this innovative technology has opened the door to a plethora of new applications and ways of thinking. We realized how crucial it is to get a better understanding of blockchain technology, and we wanted to use it in our Smart Campus Project at UCER. This game-changing technology has the potential to transform the education sector completely by providing new and cheaper ways to learn, participate and shaking up the old-school methods of working in academics. With blockchain, we can make it easier for students to pay for their extra-curricular activities, while also encouraging lifelong learning.

Contents

Chapter 1

Introduction

1.1 *Importance of Cyber Security*

Cyber security is critically important in today's digital world. Here's a clear breakdown of why cyber security matters:

1. Protection of Sensitive Data

Cyber security helps protect personal, financial, medical, and business data from unauthorized access and theft. This is essential for individuals, businesses, and governments.

Examples: Social Security numbers, bank account details, intellectual property, confidential emails.

2. Safeguarding Business Operations

Businesses rely on technology for communication, transactions, and data storage. Cyber attacks can disrupt operations, cause downtime, or even lead to permanent data loss.

Impact: Financial loss, reputational damage, loss of customer trust.

3. Preserving Privacy

Cyber security ensures that users' personal privacy is respected and protected. Without strong safeguards, individuals are vulnerable to identity theft and surveillance.

4. Defense Against Cyber crime

Cyber attacks are increasing in frequency and complexity. Cyber security protects against:

1. Phishing attacks
2. Ransomware
3. Malware

4. Hacking

5. Denial-of-Service (DOS) attacks

5. National Security

Governments must protect critical infrastructure (e.g., power grids, military systems) from cyber warfare and espionage. Cyber security is essential for national defense and public safety.

6. Protecting Emerging Technologies

As we adopt more smart devices (IOT), AI, and cloud computing, the attack surface expands. Cyber security is key to ensuring these technologies remain secure and trustworthy.

7. Compliance with Laws Regulations

Organizations must follow cyber security standards and legal requirements such as:

GDPR (EU)

HIPAA (US, health)

PCI-DSS (payment data)

ISO/IEC 27001 (international standard)

Non-compliance can lead to legal penalties and loss of certification.

1.2 *History of Cyber Security*

1. 1970s – The Beginning

First viruses threats: In 1971, the first known computer virus called Creeper appeared on ARPANET (the early internet).

Password security: Early operating systems started using basic password protection.

2. 1980s – Rise of Hacking

Hacking becomes public: The term ”hacker” gained popularity.

First antivirus: Tools like Reaper were created to remove Creeper.

In 1986, the Computer Fraud and Abuse Act was passed in the U.S.

3. 1990s – Internet Boom

Internet goes public: As the internet grew, so did cyber threats.

First major worms: The Morris Worm (1988) caused major damage.

Antivirus software became widely used (e.g., Norton, McAfee).

4. 2000s – Organized Cyber crime

Cyber attacks become professional: Hackers began forming groups and targeting businesses.

Phishing malware attacks increased.

Governments started building cyber security defense units.

5. 2010s – Data Breaches Ransomware

Major data breaches: Companies like Yahoo, Equi fax, and Target were hacked.

Rise of ransomware: Attackers lock systems and demand payment (e.g., Wanna Cry in 2017).

Cloud security became a new concern.

6. 2020s – AI, IOT Cyber Warfare

AI-driven attacks and defense systems emerge.

Nation-state attacks increase (e.g., Solar Winds hack).

More focus on cyber security laws, privacy, and critical infrastructure protection.

The shift to remote work during the COVID-19 pandemic increased vulnerabilities.

1.3 *Cyber Security threats and attacks*

Cybersecurity threats and attacks are malicious activities aimed at compromising digital systems, stealing data, or disrupting operations. These threats can come from hackers, criminal groups, insiders, or nation-states.

Main Types of Cyber Threats:

- Malware – Malicious software (e.g., viruses, ransomware) used to damage or control systems.
- Phishing – Deceptive messages tricking users into revealing sensitive information.
- Man-in-the-Middle (MitM) – Intercepting communications to steal or alter data.
- Denial-of-Service (DoS/DDoS) – Overloading systems to make them unavailable.
- SQL Injection – Inserting malicious code into databases via insecure input fields.
- Zero-Day Exploits – Attacks on unknown software vulnerabilities.
- Credential Stuffing – Using stolen login credentials to access user accounts.
- Insider Threats – Employees or partners misusing access.
- Ransomware – Encrypting data and demanding payment for its release.
- Social Engineering – Manipulating people into giving up confidential inform

Chapter 2

SPSS

2.1 *Introduction*

SPSS (Statistical Package for the Social Sciences) is a widely used software for statistical analysis, data management, and data visualization. It was originally developed by IBM and is now known as IBM SPSS Statistics.

It provides a user-friendly interface and allows both beginners and advanced users to perform complex data analysis without requiring deep programming knowledge.

2.2 *Key Features of SPSS*

- Data Management: Import, clean, and organize large datasets.
- Statistical Analysis: Perform descriptive, inferential, and advanced statistical tests.
- Visualization: Create charts, graphs, and tables for reporting.
- Syntax Editor: Automate tasks with SPSS syntax (similar to scripting).
- Add-ons: Extend functionality with advanced modules (e.g., regression, forecasting, decision trees).

2.3 *Common Uses of SPSS*

- Academic Research – analyzing survey data, experimental results.
- Business Marketing – customer behavior analysis, market research.

- Healthcare – medical research, patient data analysis.
- Social Sciences – psychology, sociology, and political science studies.
- Government Policy Making – census and demographic analysis.

2.4 *Advantages of SPSS*

- Easy-to-use GUI (Graphical User Interface).
- Supports large datasets.
- Wide range of built-in statistical tests.
- Can handle both qualitative and quantitative data.

Chapter 3

Email Header Analysis

3.1 *Introduction*

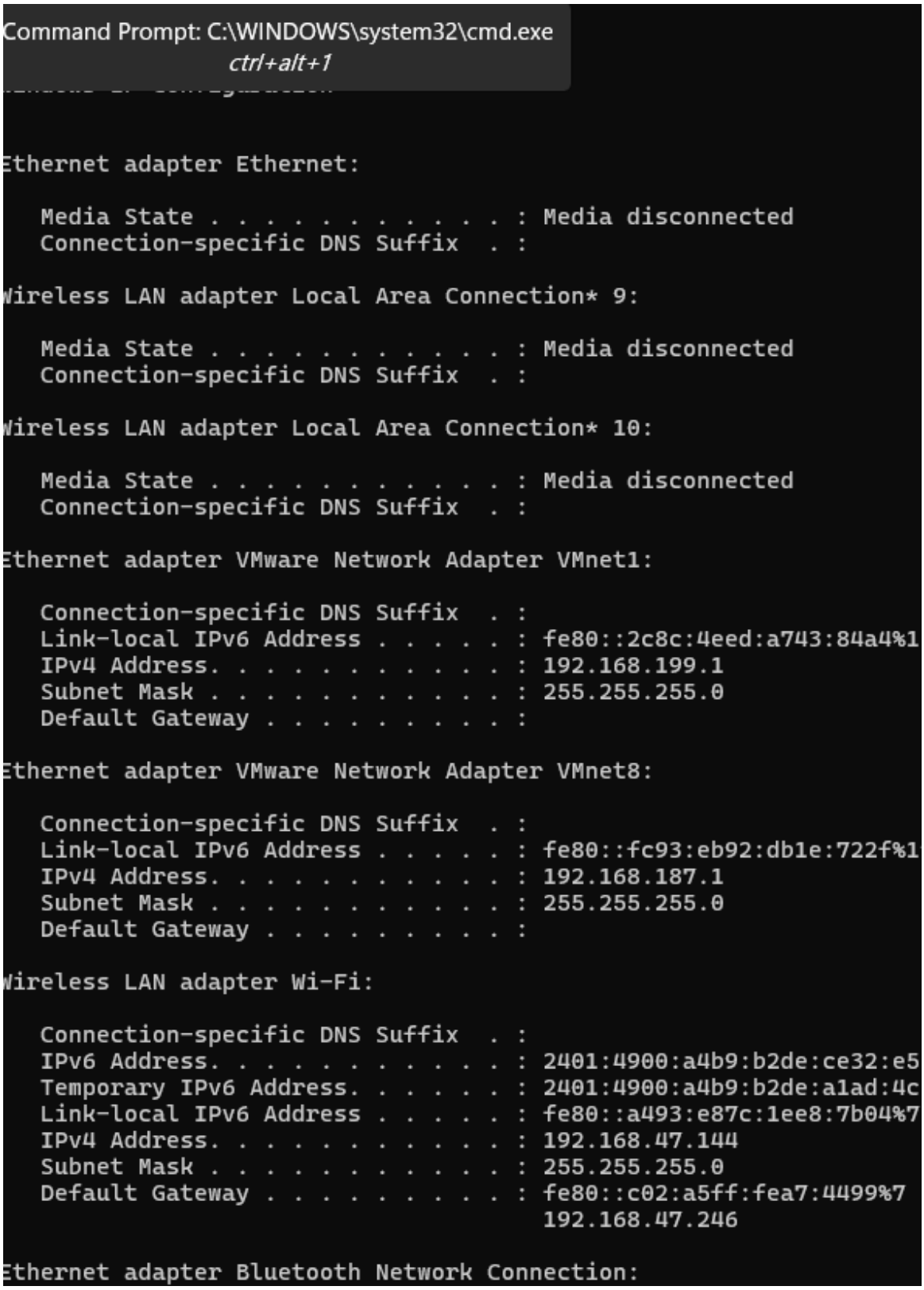
Email analysis is the process of examining email content, headers, attachments, and metadata to detect threats, investigate security incidents, or gather forensic evidence. It is commonly used in cybersecurity to:

- Identify phishing, spam, or malware
- Trace the sender's origin through email headers
- Analyze suspicious attachments or links
- Assist in incident response and digital forensics

Email analysis helps protect users and organizations by uncovering hidden risks and verifying the authenticity of messages.

3.2 *Steps*

STEP 1:Find your IP Address
STEP 2:Open your email account
STEP 3:Open any Email
STEP 4:Click Right ,then select "Show Original"
STEP 5:Check the ip address in website 'iplookup'
STep 6:Check the Location of ip address


Command Prompt: C:\WINDOWS\system32\cmd.exe
ctrl+alt+1
Ethernet adapter Ethernet:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Wireless LAN adapter Local Area Connection* 9:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Wireless LAN adapter Local Area Connection* 10:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Ethernet adapter VMware Network Adapter VMnet1:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::2c8c:4eed:a743:84a4%1
IPv4 Address. . . . . : 192.168.199.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
Ethernet adapter VMware Network Adapter VMnet8:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::fc93:eb92:db1e:722f%1
IPv4 Address. . . . . : 192.168.187.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
Wireless LAN adapter Wi-Fi:
Connection-specific DNS Suffix . :
IPv6 Address. . . . . : 2401:4900:a4b9:b2de:ce32:e5
Temporary IPv6 Address. . . . . : 2401:4900:a4b9:b2de:a1ad:4c
Link-local IPv6 Address . . . . . : fe80::a493:e87c:1ee8:7b04%7
IPv4 Address. . . . . : 192.168.47.144
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::c02:a5ff:fea7:4499%7
192.168.47.246
Ethernet adapter Bluetooth Network Connection:

```
Delivered-To: tanukeshari429@gmail.com
Received: by 2002:a98:9e41:0:b0:239:ffb2:1a99 with SMTP id k1csp1154873eig;
        Sun, 3 Aug 2025 21:35:32 -0700 (PDT)
X-Received: by 2002:a17:907:7295:b0:ae0:a116:b9d3 with SMTP id a640c23a62f3a-af9401f48a8mr795077966b.60.1754282132256;
        Sun, 03 Aug 2025 21:35:32 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1754282132; cv=none;
        d=google.com; s=arc-20240605;
        b=Gy30c6djpkFNs0T+LOz6BAv5Ni0mIb7ed4S9K0yDzTms7RiQHH6NlWsXXI6ygfeEKF
         0nduXbZFE49aA1oktbL6zEt3rwD7/4HzclAVYm1cQs/Ery+LClkoYm7ncCMwRDCHAUPF
         vY1wrVCuwCoGV/S9BWGhBeic3JylsmAlcFeNd8nKLHyeX/wDoSAAArtIgP974nkqCHbw
         pS+gi0Oc3f2kqNOGYoUr+YKK7n1TVGWJx7lp1mPk5gygHtO9TwcfjhX713KLyMRd7va/
         1TMKBRDMVk6RawWxQEdxObo82hzbQeMxoDHWnGzAxDep7KdU/jWehnXoNdzjglcAAO7Q
         JIbw==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20240605;
        h=to:subject:message-id:date:from:mime-version:dkim-signature;
        bh=rroD6xDsQaxg+GbRShMVY3yIQHc6OaAofPrxvR/g7oI=;
        fh=gCATHadtWDuj2nmoom0SKBQYjdouRW00D0hrepQtZME=;
        b=hL4qw0tAv76i3V4gYXxRPDuoOeCHPDKgik1qSdzCf+vXKzWkCWDA5tJWeE4HqjyGUM
         xxT689whsZ71fm1gunKn8AcDP9OXJ2aL0kt0uYftc7I5yTuCtjkkd0MOacoUIZ+oEvVq
         67cFV2Cnw54EF4cDYjiqg/AkOHcubisCRb2HYhbPbAiY4VemImD5NPx9H1DuiTxn3tor
         zs5WkduBorxjEO0szvdIJ2/qwylsnD8C3PK/Z1CY7rilVws0P0jC9ylx1WyvWPzTXvZi
         q9u64nMbthS0MwyRSgjA3JU7WSMqaf6pYK4CgTrmJmeRjcUkbR/uWWyhg+CE9afblWS3
         xB3Q==;
        dara=google.com
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@gmail.com header.s=20230601 header.b=eXYKbaUO;
       spf=pass (google.com: domain of tkeshari06@gmail.com designates 209.85.220.41 as permitted sender) smtp.mailfrom=tkeshari06@gmail.com;
       dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=gmail.com;
       dara=pass header.i=@gmail.com
Return-Path: <tkeshari06@gmail.com>
Received: from mail-sor-f41.google.com (mail-sor-f41.google.com. [209.85.220.41])
        by mx.google.com with SMTPS id a640c23a62f3a-af91a0b968asor539525666b.2.2025.08.03.21.35.31
        for <tanukeshari429@gmail.com>
        (Google Transport Security);
        Sun, 03 Aug 2025 21:35:32 -0700 (PDT)
```


Original Message

Message ID	<CAAKe4XstexEd18JnM5jPtLCR5cP_UO8cpbgUA+CK9psMFjnHgw@mail.gmail.com>
Created at:	Mon, Aug 4, 2025 at 10:05 AM (Delivered after 14 seconds)
From:	Tanu Keshari <tkeshari06@gmail.com>
To:	Tanu Keshari <tanukeshari429@gmail.com>
Subject:	Ip address
SPF:	PASS with IP 209.85.220.41 Learn more
DKIM:	'PASS' with domain gmail.com Learn more
DMARC:	'PASS' Learn more

Chapter 4

Linux Commands

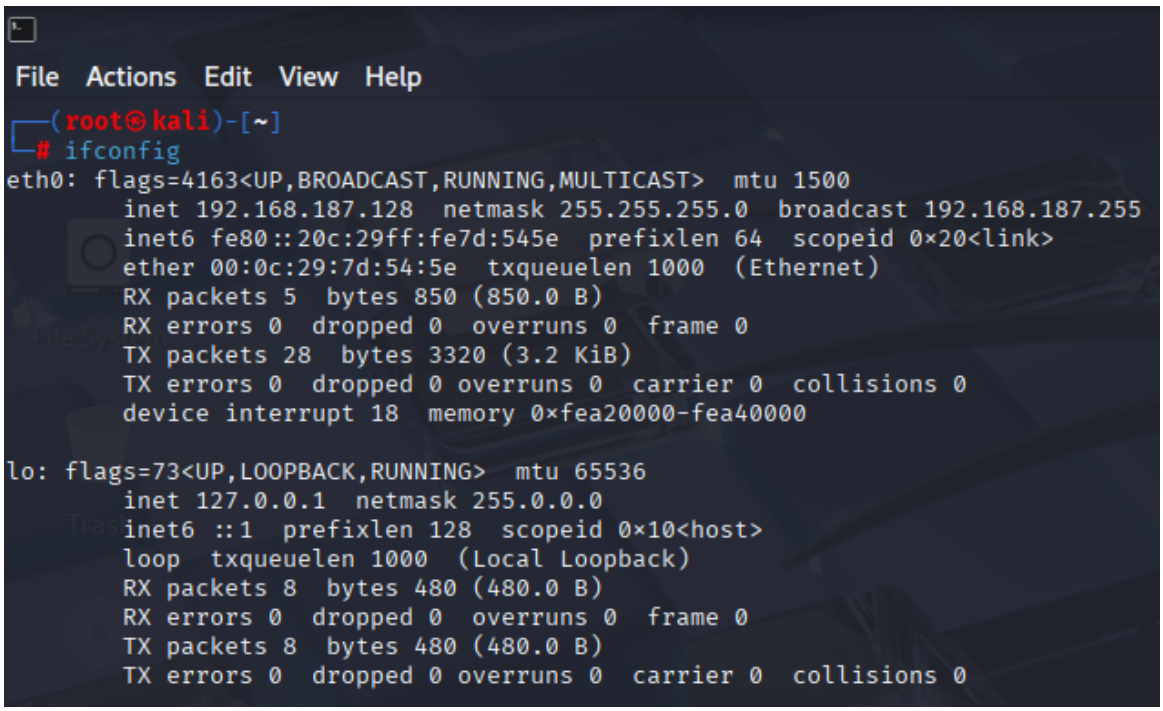
4.1 *Introduction*

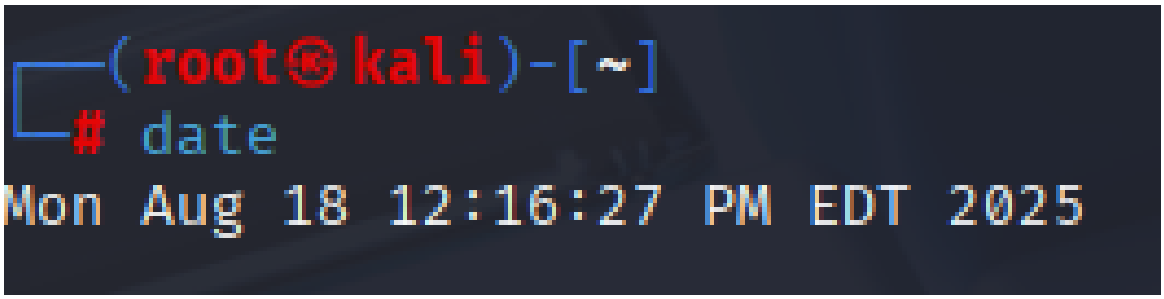
- All the Linux commands are run in the terminal provided by the Linux system.
- This terminal is just like command prompt of windows operating system.
- Linux commands are case-sensitive.
- The terminal can be used to accomplish all administrative tasks. This includes
- Package Installation
- File Manipulation
- User Management
- Execution of typed command is done only after we press the enter key.

4.2 *General Commands*

1. ifconfig: This command is used to find IP address in Linux
2. date: This command is used to display the current system date and time.
Syntax: date
Output: This command will display the Day, Month, Date, Time, Time-Zone and Year.

3.time : This command is used to display time





4. cal: This command is used to display the calendar of a specific month or a whole year.

Syntax: cal [[month] year]

Output: This command will display the calendar of current month.

5. who: This command is used to display the information about all currently logged in user on to system.

Syntax: who

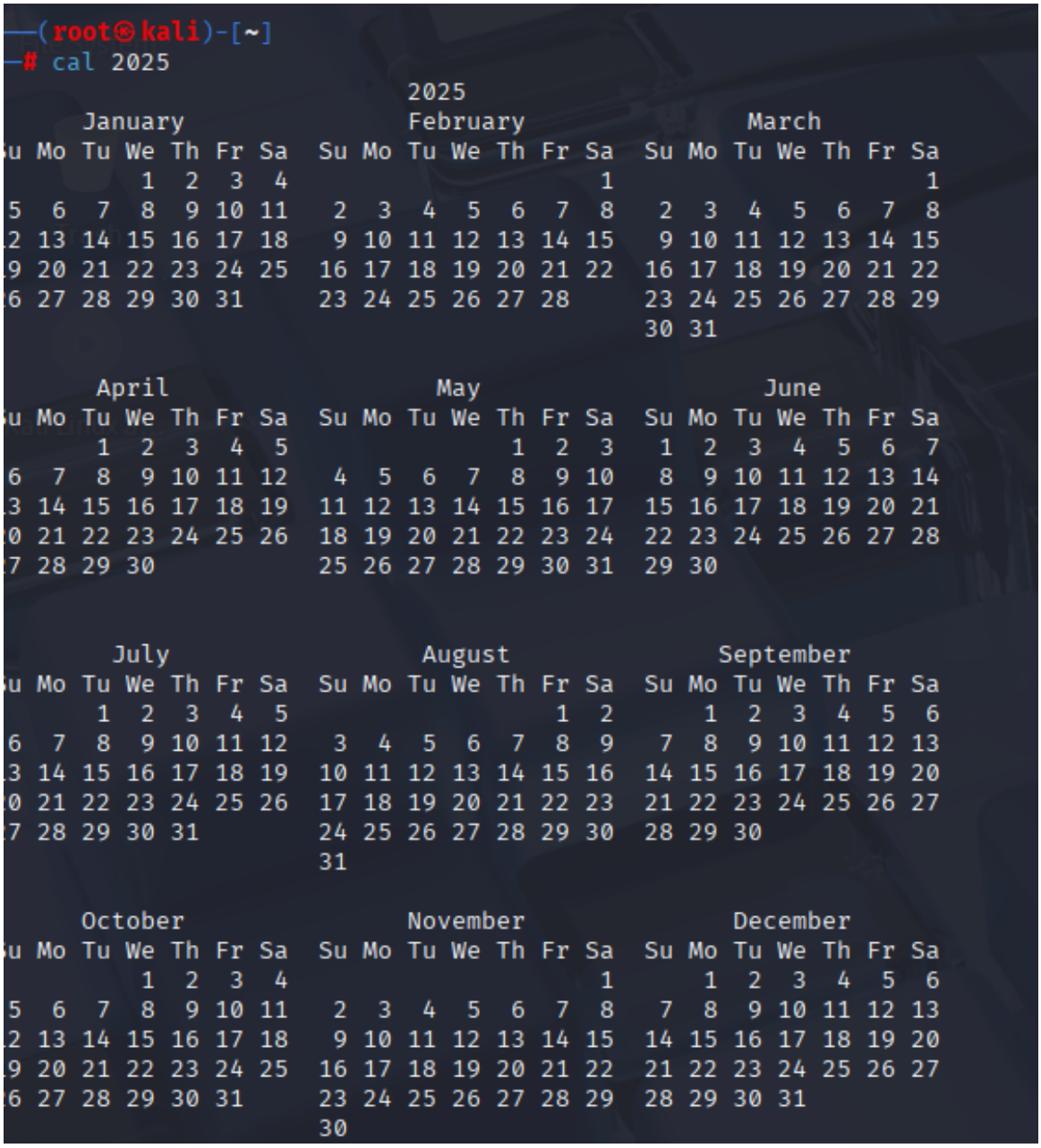
Output: This command will display the Username, Terminal Number, Login Date, Login Time of all currently logged in user on to system

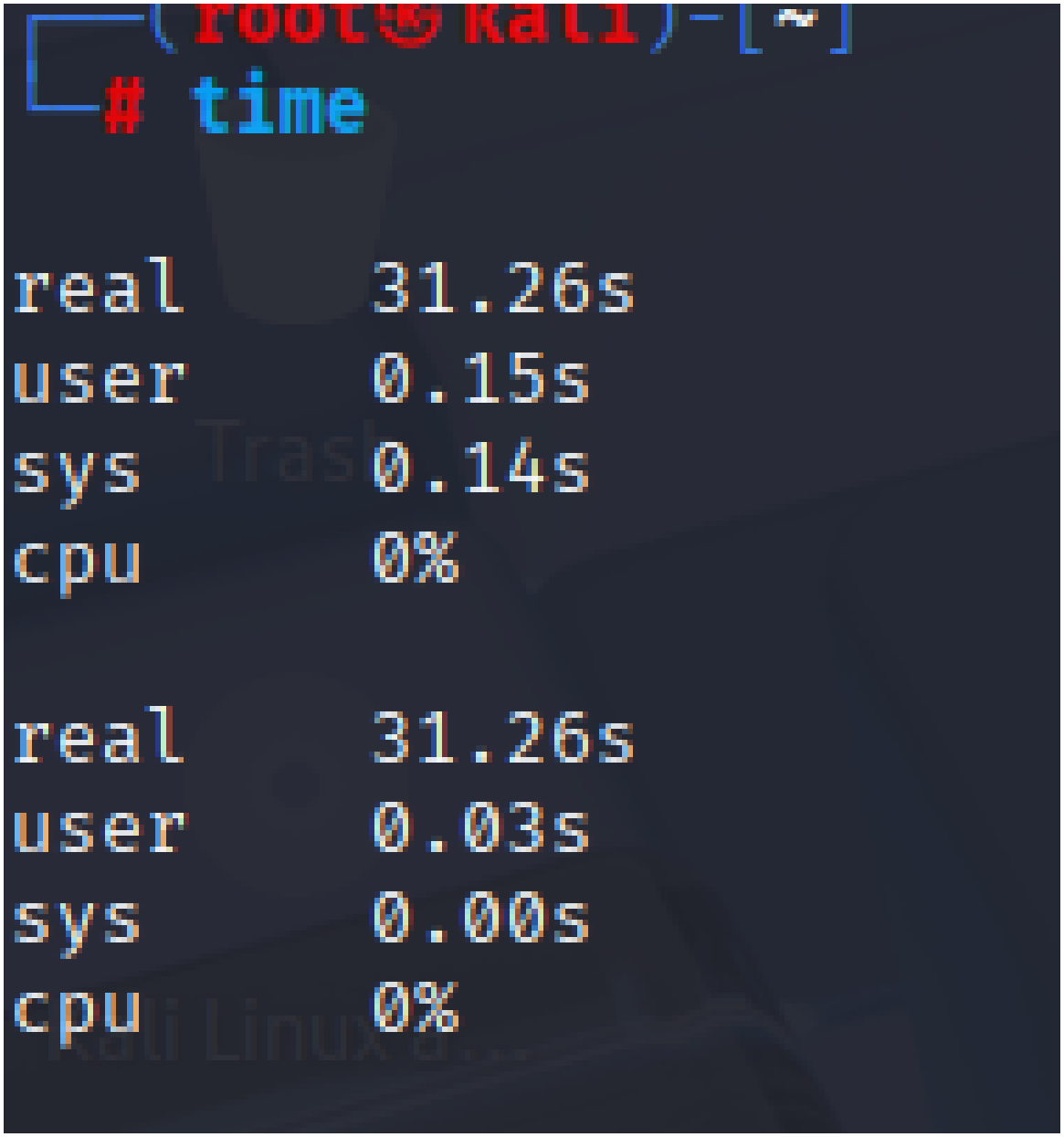
6. whoami: This command is used to display the username of the current user who invoked this command.

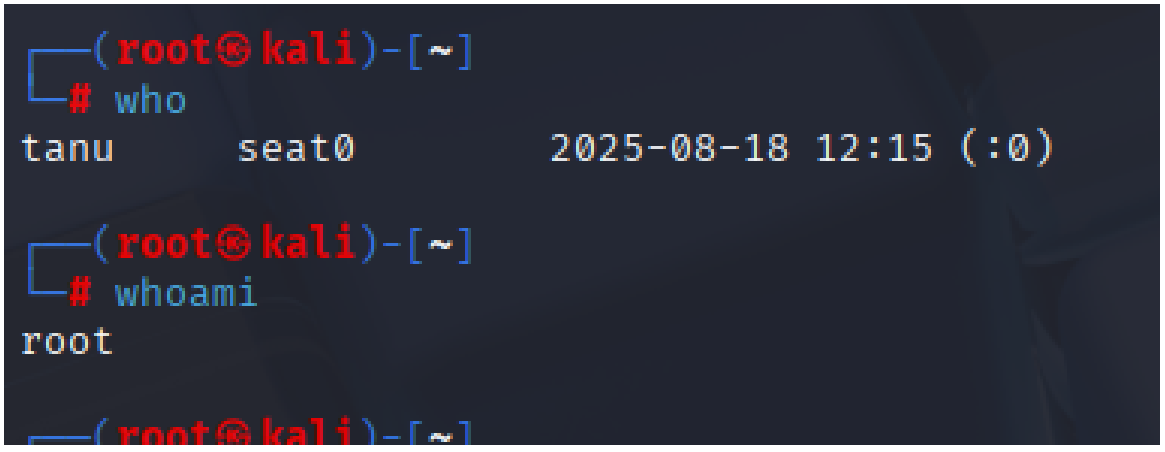
Syntax: whoami

Output: This command will display the username of the user who invoked this command.

7. history: This command is used to display the previously executed command.
Syntax: history
Output: This command will display the history of executed commands.
8. Banner: This command is used to print the string in large letter to standard output. Double quote is optional. Maximum 10 characters are displayed in a single line.
Syntax: banner "Message"
Output: This command will display the "sachin" in large letter 9. mkdir: This command is used to create directories. It is also used to create multiple directories at once.
Syntax: mkdir ¡directory name¿ 10. rmdir: This command is used to remove empty directory.
Syntax: rmdir ¡directory name¿
11. cat: This command is used to create file, display content of file and append data into file.
Syntax: cat ¿ ¡file$_{n}ame >$
$Output : Thiscommandwillcreateafile\abc.txt".Usectrl + dtosavethefilecontent.$


┌──(root㉿kali)-[~]
└─# cal 2025
2025
January
Su Mo Tu We Th Fr Sa
1 2 3 4
5 6 7 8 9 10 11
12 13 14 15 16 17 18
19 20 21 22 23 24 25
26 27 28 29 30 31
February
Su Mo Tu We Th Fr Sa
1
2 3 4 5 6 7 8
9 10 11 12 13 14 15
16 17 18 19 20 21 22
23 24 25 26 27 28
March
Su Mo Tu We Th Fr Sa
1
2 3 4 5 6 7 8
9 10 11 12 13 14 15
16 17 18 19 20 21 22
23 24 25 26 27 28 29
30 31
April
Su Mo Tu We Th Fr Sa
1 2 3 4 5
6 7 8 9 10 11 12
13 14 15 16 17 18 19
20 21 22 23 24 25 26
27 28 29 30
May
Su Mo Tu We Th Fr Sa
1 2 3
4 5 6 7 8 9 10
11 12 13 14 15 16 17
18 19 20 21 22 23 24
25 26 27 28 29 30 31
June
Su Mo Tu We Th Fr Sa
1 2 3 4 5 6 7
8 9 10 11 12 13 14
15 16 17 18 19 20 21
22 23 24 25 26 27 28
29 30
July
Su Mo Tu We Th Fr Sa
1 2 3 4 5
6 7 8 9 10 11 12
13 14 15 16 17 18 19
20 21 22 23 24 25 26
27 28 29 30 31
August
Su Mo Tu We Th Fr Sa
1 2
3 4 5 6 7 8 9
10 11 12 13 14 15 16
17 18 19 20 21 22 23
24 25 26 27 28 29 30
31
September
Su Mo Tu We Th Fr Sa
1 2 3 4 5 6
7 8 9 10 11 12 13
14 15 16 17 18 19 20
21 22 23 24 25 26 27
28 29 30
October
Su Mo Tu We Th Fr Sa
1 2 3 4
5 6 7 8 9 10 11
12 13 14 15 16 17 18
19 20 21 22 23 24 25
26 27 28 29 30 31
November
Su Mo Tu We Th Fr Sa
1
2 3 4 5 6 7 8
9 10 11 12 13 14 15
16 17 18 19 20 21 22
23 24 25 26 27 28 29
30
December
Su Mo Tu We Th Fr Sa
1 2 3 4 5 6
7 8 9 10 11 12 13
14 15 16 17 18 19 20
21 22 23 24 25 26 27
28 29 30 31


(root㉿kali)-[~]
time
real 31.26s
user 0.15s
sys 0.14s
cpu 0%
real 31.26s
user 0.03s
sys 0.00s
cpu 0%


(root㉿kali)-[~]
who
tanu seat0 2025-08-18 12:15 (:0)
(root㉿kali)-[~]
whoami
root

```
┌──(root㉿kali)-[~]
└─# history
    1  ifconfig
    2  date
    3  time
    4  sudo apt install ncal
    5  cal
    6  cal 2025
    7  who -m -H
    8  who -a
    9  who -all
   10  who -p -H
   11  whoami
   12  bc
```

```
┌──(root㉿kali)-[~]
└─# banner sachin

 #####      ##      #####   #     #      #     #     #
#          #  #    #    #  #     #      #     ##    #
 #####    #    #   #    #  #######      #     # #   #
      #   #######  #       #     #      #     #  # #
#     #   #     #  #    #  #     #      #     #   ##
 #####    #     #   #####   #     #      #     #    #
```

```
┌──(root㉿kali)-[~]
└─# mkdir mata

┌──(root㉿kali)-[~]
└─# ls
cryptr  line.txt  mata  sita.txt  supriya

┌──(root㉿kali)-[~]
└─# ls -a
..  .bashrc  .bashrc.original  .cache  .config  cryptr  .dbus  .face  .face.icon  .gvfs  line.txt  mata  .msf4  .profile  sita.txt  .ssh  supriya  .zsh_h

┌──(root㉿kali)-[~]
└─#
```

Chapter 5

A Practical Approach to Network Monitoring

5.1 *Introduction*

Network monitoring is the process of continuously checking a computer network's performance, availability, and security. It helps detect problems like slow connections, downtime, or suspicious activity early, ensuring smooth and secure network operations.

Key Purposes:

- **Ensure network uptime and performance**
- **Detect cyber threats and unusual activity**
- **Optimize resource usage**
- **Maintain security and compliance**

Main Functions:

- **Monitor traffic and devices**
- **Generate alerts for issues**
- **Record logs for analysis**
- **Track key metrics (e.g., bandwidth, latency)**

Network monitoring is essential for keeping networks reliable, fast, and secure

Tools of network monitoring

- **Nmap**
- **Wireshark**
- **Metasploit Framework**
- **Aircrack**
- **Hashcat**
- **Burpsuit**
- **Nesses Professional**
- **Kali Linux**
- **Snort**
- **Intruder**

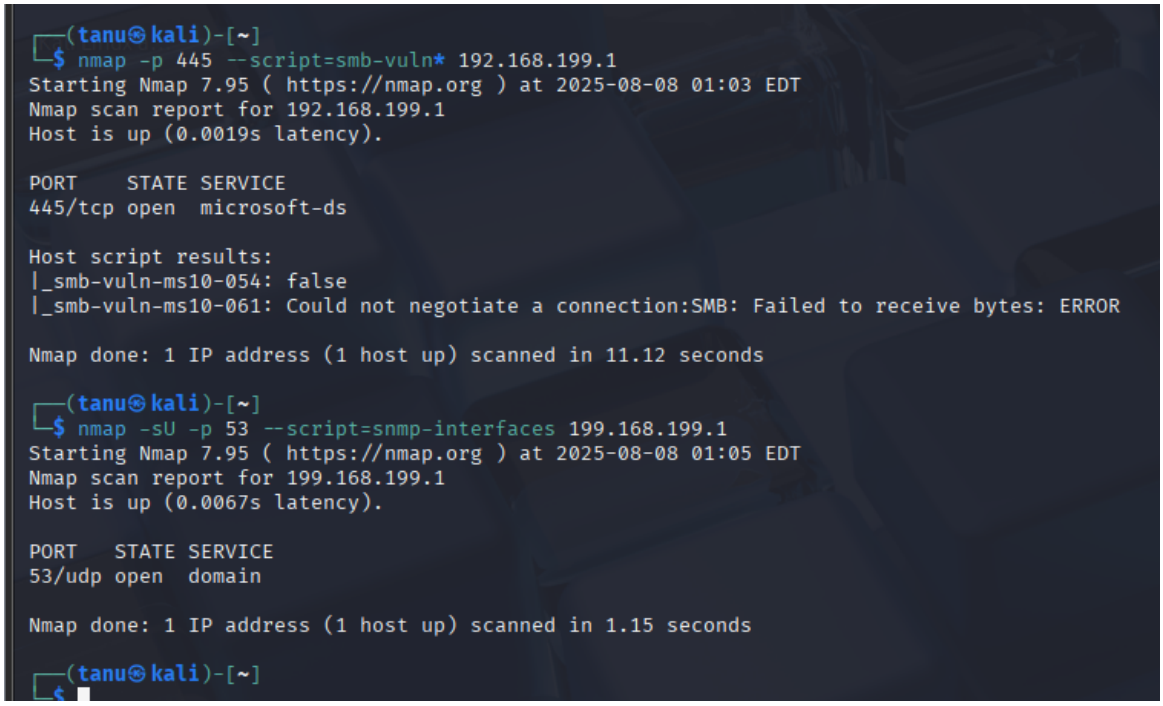
5.2 General Commands

STEP 1: FIND LIVE MACHINES
nmap –sP target
STEP 2: DISCOVER OPEN PORTS
nmap –p port -v target
For example:
nmap –p 1-65535 –v 172.16.4.51
a) TCP Connect Scan [-sT]
nmap –sT target
b) SYN Stealth Scan [-sS]
nmap –sS –A –O target –p port
c) UDP Scan [-sU]
nmap –sU target
d) Idle Scan [-sI]
nmap -V -Pn –sI zombie-address :port no. victim's address

```
└─$ nmap -sP 192.168.199.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-08 00:42 EDT
Nmap scan report for 192.168.199.1
Host is up (0.0018s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds

┌──(tanu㉿kali)-[~]
└─$ nmap -p 1-65535 -v 192.168.199.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-08 00:43 EDT
Initiating Ping Scan at 00:43
Scanning 192.168.199.1 [4 ports]
Completed Ping Scan at 00:43, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 00:43
Completed Parallel DNS resolution of 1 host. at 00:43, 0.03s elapsed
Initiating SYN Stealth Scan at 00:43
Scanning 192.168.199.1 [65535 ports]
Discovered open port 135/tcp on 192.168.199.1
Discovered open port 139/tcp on 192.168.199.1
Discovered open port 445/tcp on 192.168.199.1
Discovered open port 912/tcp on 192.168.199.1
SYN Stealth Scan Timing: About 20.10% done; ETC: 00:45 (0:02:03 remaining)
Discovered open port 49668/tcp on 192.168.199.1
SYN Stealth Scan Timing: About 44.22% done; ETC: 00:45 (0:01:17 remaining)
Increasing send delay for 192.168.199.1 from 0 to 5 due to 22 out of 71 dropped probes since last increase.
Increasing send delay for 192.168.199.1 from 5 to 10 due to 58 out of 193 dropped probes since last increase.
Increasing send delay for 192.168.199.1 from 10 to 20 due to 99 out of 328 dropped probes since last increase.
Increasing send delay for 192.168.199.1 from 20 to 40 due to max_successful_tryno increase to 4
Increasing send delay for 192.168.199.1 from 40 to 80 due to max_successful_tryno increase to 5
Increasing send delay for 192.168.199.1 from 80 to 160 due to max_successful_tryno increase to 6
Increasing send delay for 192.168.199.1 from 160 to 320 due to max_successful_tryno increase to 7
Increasing send delay for 192.168.199.1 from 320 to 640 due to max_successful_tryno increase to 8
SYN Stealth Scan Timing: About 9.62% done; ETC: 00:59 (0:14:15 remaining)
Increasing send delay for 192.168.199.1 from 640 to 1000 due to max_successful_tryno increase to 9
Warning: 192.168.199.1 giving up on port because retransmission cap hit (10).
SYN Stealth Scan Timing: About 8.81% done; ETC: 01:06 (0:20:52 remaining)
SYN Stealth Scan Timing: About 8.82% done; ETC: 01:11 (0:26:01 remaining)
SYN Stealth Scan Timing: About 8.83% done; ETC: 01:17 (0:31:09 remaining)
SYN Stealth Scan Timing: About 8.84% done; ETC: 01:23 (0:36:16 remaining)
SYN Stealth Scan Timing: About 8.85% done; ETC: 01:28 (0:41:23 remaining)
SYN Stealth Scan Timing: About 8.86% done; ETC: 01:34 (0:46:29 remaining)
SYN Stealth Scan Timing: About 8.86% done; ETC: 01:39 (0:51:35 remaining)
Stats: 0:05:19 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 8.87% done; ETC: 01:43 (0:54:38 remaining)
Stats: 0:05:24 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 8.87% done; ETC: 01:44 (0:55:29 remaining)
```

```
tanu@kali: ~
File  Actions  Edit  View  Help
┌──(tanu㉿kali)-[~]
└─$ nmap -sT 192.168.199.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-08 00:52 EDT
Nmap scan report for 192.168.199.1
Host is up (0.0027s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
912/tcp open  apex-mesh

Nmap done: 1 IP address (1 host up) scanned in 9.30 seconds

┌──(tanu㉿kali)-[~]
└─$ nmap -sS -A -O 192.168.199.1 -p 135
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-08 00:54 EDT
Nmap scan report for 192.168.199.1
Host is up (0.0036s latency).

PORT    STATE SERVICE VERSION
135/tcp open  msrpc   Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized
Running: Microsoft Windows XP|7|2012, VMware Player
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2012 cpe:/a:vmware:player
OS details: Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012, VMware Player virtual NAT device
Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE (using port 135/tcp)
HOP RTT     ADDRESS
1   5.48 ms 192.168.187.2
2   5.54 ms 192.168.199.1

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.41 seconds

┌──(tanu㉿kali)-[~]
└─$ nmap -sU 199.168.199.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-08 00:55 EDT
Nmap scan report for 199.168.199.1
Host is up (0.0036s latency).
Not shown: 999 open|filtered udp ports (no-response)
PORT   STATE SERVICE
53/udp open  domain

Nmap done: 1 IP address (1 host up) scanned in 5.93 seconds
```


```
└─$ nmap -T5 192.168.199.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-08 00:58 EDT
Nmap scan report for 192.168.199.1
Host is up (0.0030s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
902/tcp open  iss-realsecure
912/tcp open  apex-mesh

Nmap done: 1 IP address (1 host up) scanned in 8.07 seconds

┌──(tanu㉿kali)-[~]
└─$ nmap -T4 192.168.199.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-08 00:59 EDT
Warning: 192.168.199.1 giving up on port because retransmission cap hit (6).
Nmap scan report for 192.168.199.1
Host is up (0.029s latency).
Not shown: 929 closed tcp ports (reset), 66 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
902/tcp open  iss-realsecure
912/tcp open  apex-mesh

Nmap done: 1 IP address (1 host up) scanned in 63.87 seconds
```


┌──(tanu㉿kali)-[~]
└─$ nmap -p 445 --script=smb-vuln* 192.168.199.1
Starting Nmap 7.95 (https://nmap.org) at 2025-08-08 01:03 EDT
Nmap scan report for 192.168.199.1
Host is up (0.0019s latency).
PORT STATE SERVICE
445/tcp open microsoft-ds
Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
Nmap done: 1 IP address (1 host up) scanned in 11.12 seconds
┌──(tanu㉿kali)-[~]
└─$ nmap -sU -p 53 --script=snmp-interfaces 199.168.199.1
Starting Nmap 7.95 (https://nmap.org) at 2025-08-08 01:05 EDT
Nmap scan report for 199.168.199.1
Host is up (0.0067s latency).
PORT STATE SERVICE
53/udp open domain
Nmap done: 1 IP address (1 host up) scanned in 1.15 seconds
┌──(tanu㉿kali)-[~]
└─$

Chapter 6

Encryption and Decryption

6.1 *Introduction*

In today's digital world, where vast amounts of sensitive data are shared and stored electronically, ensuring the security and privacy of that information is critical. Encryption and decryption are two essential processes used to protect data from unauthorized access Encryption is the process of converting plain text or readable data into an unreadable format called ciphertext. This transformation is done using an algorithm and a key, ensuring that only authorized parties with the correct key can understand the original content.

- **Purpose: To protect data confidentiality.**
- **Example: If you send a message like "HELLO" and encrypt it, it might become something like "XKQZF" which looks meaningless to anyone intercepting it.**

6.2 *What is Decryption?*

Decryption is the reverse process of encryption. It transforms the ciphertext back into the original plain text using the appropriate key.

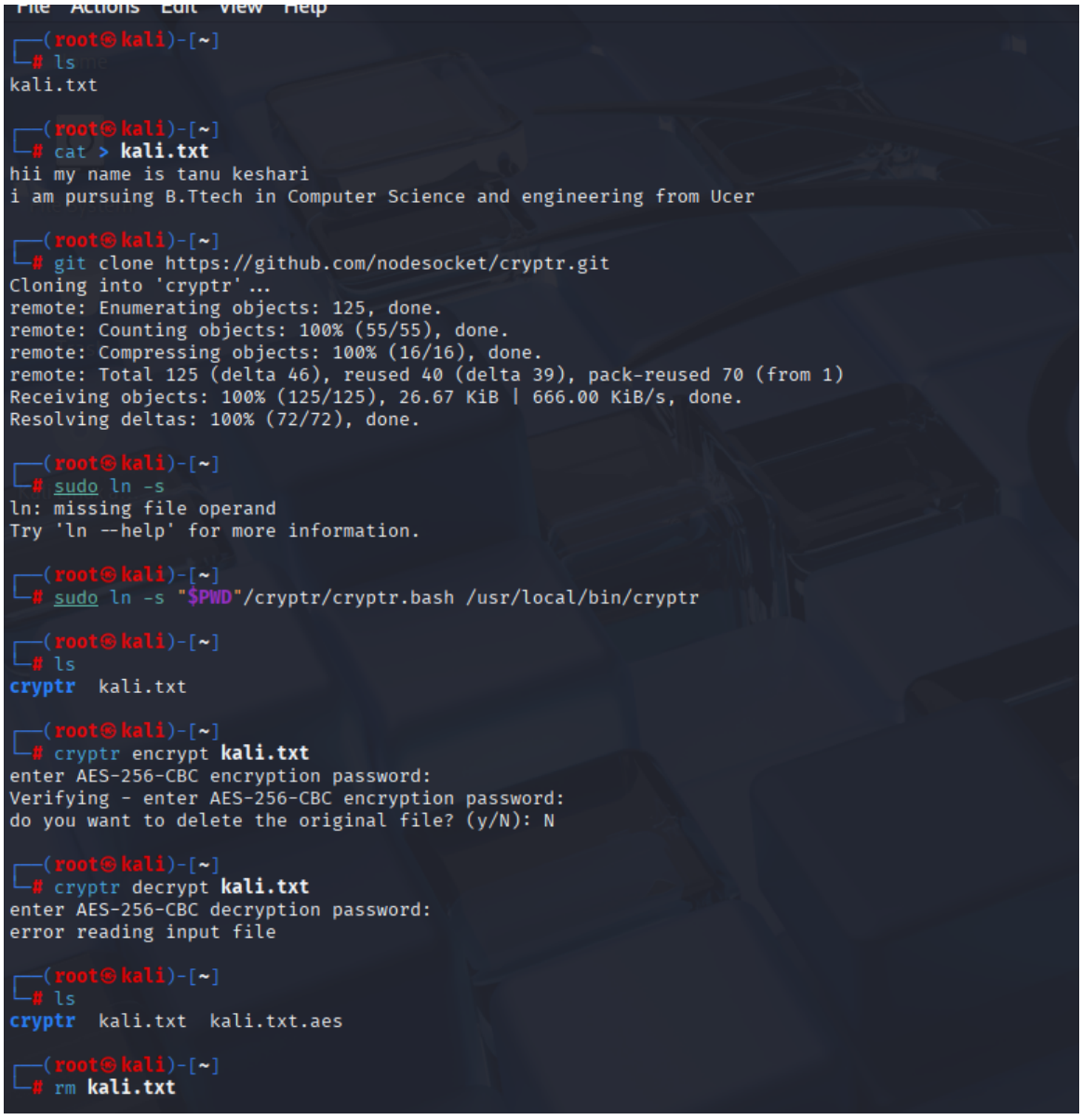
- **Purpose: To allow authorized users to access the original information.**
- **Example: Taking the encrypted message "XKQZF" and converting it back to "HELLO" using the right key.**

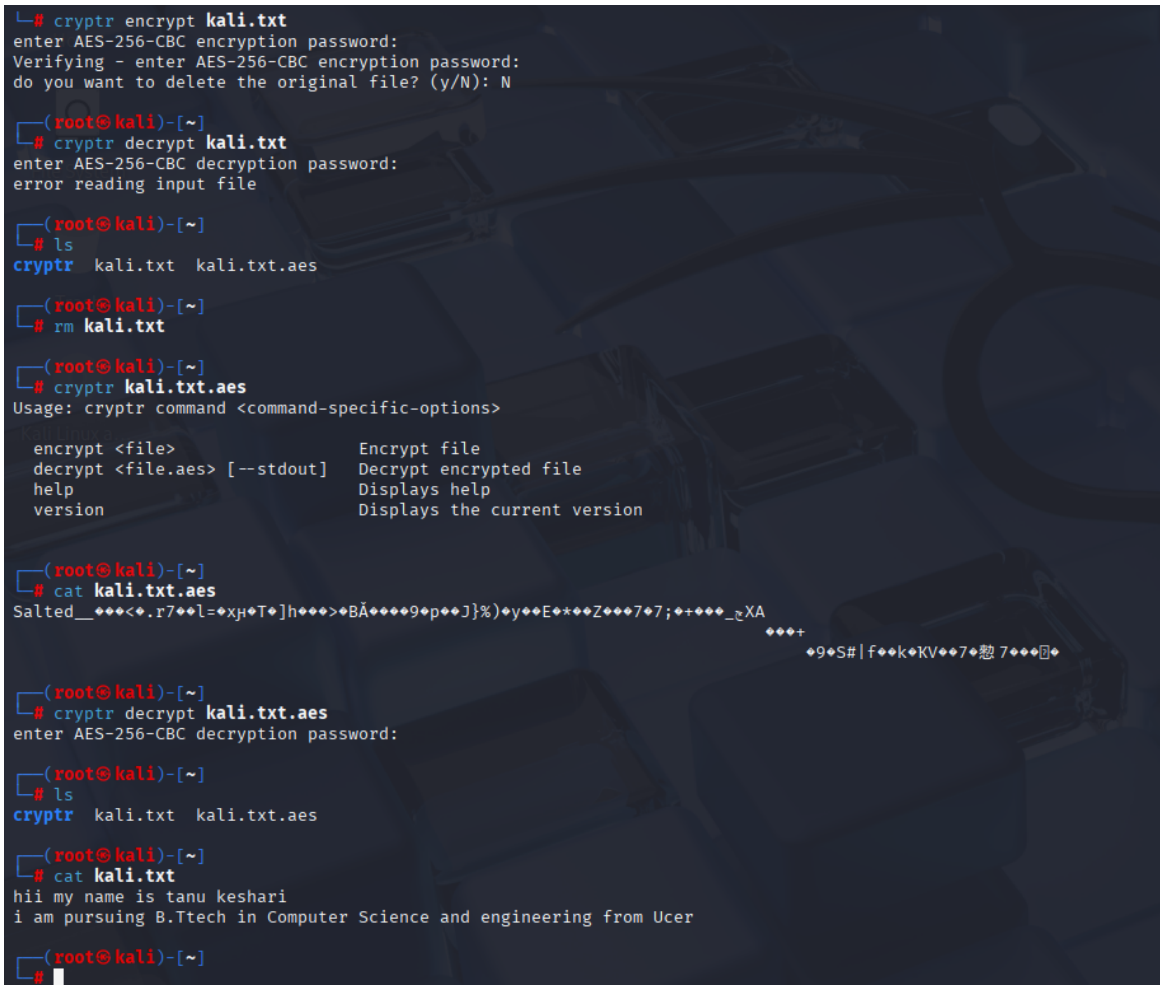
6.3 *Importance of Encryption and Decryption*

- **Data Security: Protects sensitive information like financial data, personal information, and communication.**
- **Privacy: Ensures that only intended recipients can read the information.**
- **Authentication: Confirms the identity of the sender and receiver.**
- **Data Integrity: Verifies that the information has not been altered.**

6.4 *Common Uses*

- **Online Banking and E-commerce**
- **Messaging Apps (e.g., WhatsApp, Signal)**
- **Email Encryption**
- **Secure File Storage and Transfer**


File Actions Edit View Help
┌──(root㉿kali)-[~]
└─# ls
kali.txt
┌──(root㉿kali)-[~]
└─# cat > kali.txt
hii my name is tanu keshari
i am pursuing B.Ttech in Computer Science and engineering from Ucer
┌──(root㉿kali)-[~]
└─# git clone https://github.com/nodesocket/cryptr.git
Cloning into 'cryptr' ...
remote: Enumerating objects: 125, done.
remote: Counting objects: 100% (55/55), done.
remote: Compressing objects: 100% (16/16), done.
remote: Total 125 (delta 46), reused 40 (delta 39), pack-reused 70 (from 1)
Receiving objects: 100% (125/125), 26.67 KiB | 666.00 KiB/s, done.
Resolving deltas: 100% (72/72), done.
┌──(root㉿kali)-[~]
└─# sudo ln -s
ln: missing file operand
Try 'ln --help' for more information.
┌──(root㉿kali)-[~]
└─# sudo ln -s "$PWD"/cryptr/cryptr.bash /usr/local/bin/cryptr
┌──(root㉿kali)-[~]
└─# ls
cryptr kali.txt
┌──(root㉿kali)-[~]
└─# cryptr encrypt kali.txt
enter AES-256-CBC encryption password:
Verifying - enter AES-256-CBC encryption password:
do you want to delete the original file? (y/N): N
┌──(root㉿kali)-[~]
└─# cryptr decrypt kali.txt
enter AES-256-CBC decryption password:
error reading input file
┌──(root㉿kali)-[~]
└─# ls
cryptr kali.txt kali.txt.aes
┌──(root㉿kali)-[~]
└─# rm kali.txt


└─# cryptr encrypt kali.txt
enter AES-256-CBC encryption password:
Verifying - enter AES-256-CBC encryption password:
do you want to delete the original file? (y/N): N
┌──(root㉿kali)-[~]
└─# cryptr decrypt kali.txt
enter AES-256-CBC decryption password:
error reading input file
┌──(root㉿kali)-[~]
└─# ls
cryptr kali.txt kali.txt.aes
┌──(root㉿kali)-[~]
└─# rm kali.txt
┌──(root㉿kali)-[~]
└─# cryptr kali.txt.aes
Usage: cryptr command <command-specific-options>
encrypt <file> Encrypt file
decrypt <file.aes> [--stdout] Decrypt encrypted file
help Displays help
version Displays the current version
┌──(root㉿kali)-[~]
└─# cat kali.txt.aes
Salted__◆◆◆<◆.r7◆◆l=◆xH◆T◆]h◆◆◆>◆BÅ◆◆◆◆9◆p◆◆J}%)◆y◆◆E◆*◆◆Z◆◆◆7◆7;◆+◆◆◆_ᵴXA
◆◆◆+
◆9◆S#|f◆◆k◆KV◆◆7◆憨 7◆◆◆□◆
┌──(root㉿kali)-[~]
└─# cryptr decrypt kali.txt.aes
enter AES-256-CBC decryption password:
┌──(root㉿kali)-[~]
└─# ls
cryptr kali.txt kali.txt.aes
┌──(root㉿kali)-[~]
└─# cat kali.txt
hii my name is tanu keshari
i am pursuing B.Ttech in Computer Science and engineering from Ucer
┌──(root㉿kali)-[~]
└─#

Chapter 7

Metasploit Framework

7.1 *Introduction*

The Metasploit Framework is one of the most powerful and widely used tools in the field of penetration testing, ethical hacking, and cybersecurity research. Developed and maintained by Rapid7, it is an open-source framework that helps security professionals identify, exploit, and validate vulnerabilities in systems and networks.

7.2 *What is Metasploit Framework?*

The Metasploit Framework (MSF) is a modular platform that provides a wide collection of tools, exploits, payloads, and auxiliary modules used to simulate real-world attacks on computer systems.

- **It allows ethical hackers and penetration testers to:**
- **Detect security vulnerabilities**
- **Test the effectiveness of security defenses**
- **Exploit weaknesses in a controlled and legal environment**

7.3 *Why Metasploit is Popular*

- **Open-source and free (with a commercial version available)**
- **Extensive module library (thousands of exploits and tools)**

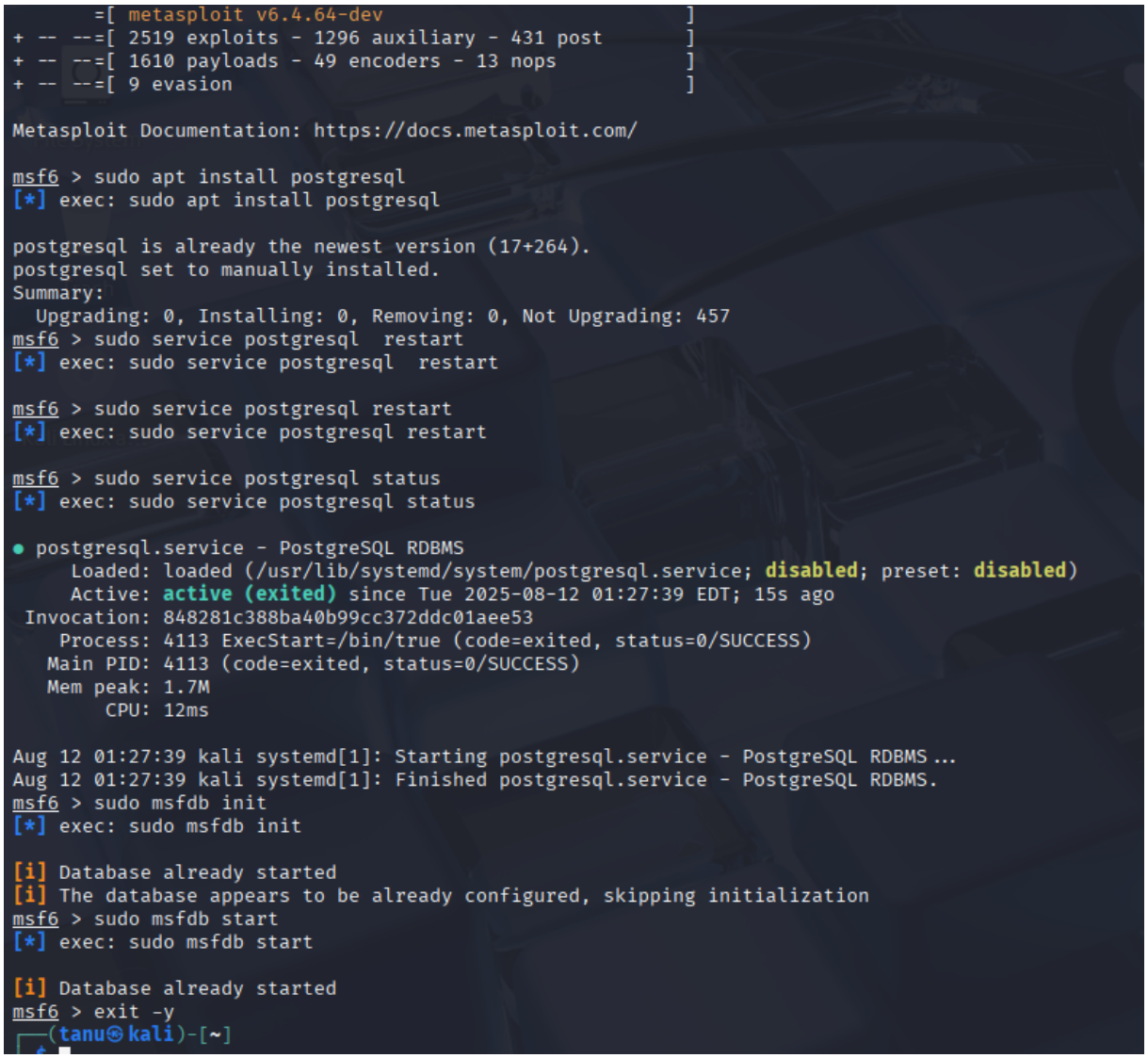
- **Regular updates from the security community**
- **Cross-platform support (Linux, Windows, macOS)**
- **Integration with other tools like Nmap, Nessus, and Burp Suite**

7.4 *Common Uses*

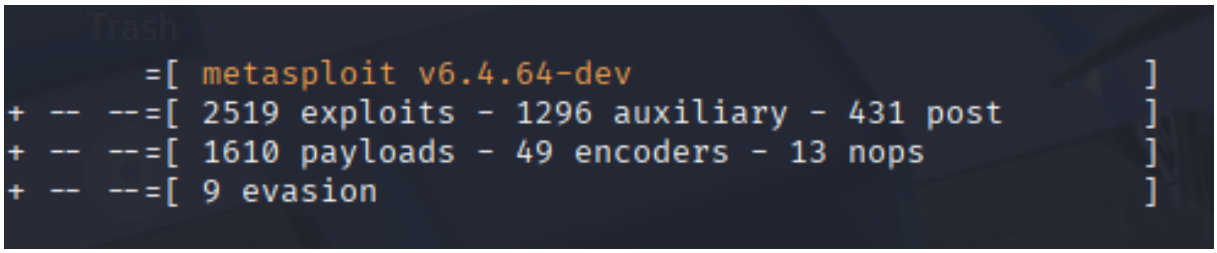
- **Penetration Testing: Simulate attacks to identify vulnerabilities before malicious hackers do.**
- **Security Research: Test and analyze vulnerabilities in software and systems.**
- **Exploit Development: Create and test custom exploits in a safe environment.**
- **Training and Education: Teach cybersecurity skills and attack techniques.**

7.4.1 Step-1 : Installation of metasploit framework in Kali Linux

7.4.2 Step-2 : Installation of package of metasploit framework



7.4.3 Step-3


=[metasploit v6.4.64-dev]
+ -- --=[2519 exploits - 1296 auxiliary - 431 post]
+ -- --=[1610 payloads - 49 encoders - 13 nops]
+ -- --=[9 evasion]

Chapter 8

Hashcat

8.1 *Introduction*

Hashcat is a powerful and open-source password recovery tool widely used in cybersecurity. It is designed to crack hashed passwords using various attack modes and algorithms. Hashcat is considered one of the fastest password cracking tools, leveraging both CPU and GPU acceleration for high-speed computations.

8.2 *Key Features of Hashcat*

- **Supports multiple hash algorithms**
- **(MD5, SHA-1, SHA-256, bcrypt, NTLM, etc.)**
- **GPU acceleration**
- **Utilizes NVIDIA/AMD GPUs for faster cracking.**
- **Flexible attack modes**
- **Brute-force attack**
- **Dictionary attack**
- **Hybrid attack (dictionary + mask)**
- **Rule-based attack**
- **Combinator attack**

- **Cross-platform (Windows, Linux, macOS).**
- **Community-supported and regularly updated**

8.3 *Uses of Hashcat in Cybersecurity*

- **Password auditing: Test strength of stored passwords.**
- **Forensics: Recover lost/forgotten credentials.**
- **Penetration testing: Identify weak passwords in security assessments.**
- **Research: Study hashing algorithms and password security.**

Chapter 9

Aircrack

9.1 *Introduction*

Aircrack-ng is a powerful, open-source suite of tools used for auditing and securing wireless networks. It is widely used by ethical hackers, penetration testers, and network administrators to assess the security of Wi-Fi networks, especially those using WEP and WPA/WPA2 encryption.

9.2 *What is Aircrack-ng?*

Aircrack-ng stands for "Aircrack next generation" and is primarily used to test the strength of wireless encryption by capturing packets and attempting to crack the network's password or encryption key. It is a command-line-based toolset available for Linux, Windows, macOS, and even Android (with some limitations).

9.3 *Components of Aircrack-ng Suite*

1. **airmon-ng – Enables monitor mode on wireless interfaces.**
2. **airodump-ng – Captures packets and displays information about nearby networks.**
3. **aireplay-ng – Performs packet injection and deauthentication attacks.**
4. **aircrack-ng – Uses captured data to attempt to crack WEP/WPA keys.**
5. **airbase-ng – Creates rogue access points for testing.**

9.4 *Why Aircrack-ng is Popular*

- **Free and open-source**
- **Widely supported by cybersecurity tools and Linux distros (e.g., Kali Linux)**
- **Lightweight and fast**
- **Flexible and scriptable for automation**

9.5 *Common Use Cases*

- **Wi-Fi Security Testing: Ensure your network is not vulnerable to known attacks.**
- **Password Strength Evaluation: Test how easily a Wi-Fi password could be guessed or cracked.**
- **Learning and Training: Used in cybersecurity courses and ethical hacking certifications.**
- **Red Team Exercises: Simulate attacks during authorized security assessments.**
- **Packet Capture: Capture packets from a wireless network in monitor mode.**
- **WEP and WPA/WPA2 Cracking: Break encryption keys using captured data and dictionary attacks.**
- **Deauthentication Attacks: Disconnect clients to capture handshake data.**
- **Replay Attacks: Resend captured packets to generate traffic for analysis.**
- **Fake Access Points: Simulate fake Wi-Fi networks for testing.**
- **Monitoring and Detection: Identify network devices, channels, and signal strengths.**

9.6 *Commands*

1. **iwconfig**
2. **airmon-ng -help**

3. **airmon-ng check kill**

4. **airmon-ng dump-ng wlan0mon**

Chapter 10

SQLmap

10.1 *Introduction*

SQLMap is an open-source penetration testing tool that automates the process of detecting and exploiting SQL injection vulnerabilities in web applications. It is one of the most widely used tools by ethical hackers, security researchers, and penetration testers to identify database security flaws and perform database takeovers during authorized security assessments.

10.2 *What is SQL Injection?*

SQL Injection is a common web vulnerability that allows attackers to interfere with the queries an application makes to its database. Exploiting this flaw can lead to unauthorized access, data leakage, or even full control over the database server.

10.3 *What is SQLMap?*

SQLMap is a command-line tool designed to detect and exploit SQL injection vulnerabilities with minimal user input. It is capable of performing automated attacks, making it easier and faster for security professionals to test the security of database-driven applications.

10.4 *Common Use Cases*

- **Web Application Penetration Testing**

- **Security Audits of Database-driven Applications**
- **Vulnerability Assessment**
- **Capture the Flag (CTF) Challenges and Cybersecurity Training**

10.5 *Why SQLMap is Popular*

- **Free and Open Source**
- **Highly Automated – requires minimal configuration**
- **Supports a wide range of databases**
- **Regularly updated and maintained**
- **Powerful and flexible, suitable for both beginners and advanced users**

10.6 *Key Features of SQLMap*

Automatic Detection of various types of SQL injection techniques (e.g., boolean-based, time-based blind, error-based, UNION-based). Database Fingerprinting to identify the database type and version (MySQL, PostgreSQL, Oracle, MSSQL, etc.). Data Extraction from the database, such as table names, columns, and records. Database Takeover, including reading and writing files on the server, executing operating system commands, and spawning a reverse shell. Bypass Techniques for web application firewalls (WAFs) and input sanitization.

10.7 *Commands*

1. **sqlmap -u**
2. **sqlmap -u ”http://example.com/page.php?id=1” –dbs**
3. **sqlmap -u ”http://example.com/page.php?id=1” -D database-name –tables**
4. **sqlmap -u ”http://example.com/page.php?id=1” -D database-name -T table-name –columns**

5. **sqlmap -u ”http://example.com/page.php?id=1” -D database-name -T table-name –dump**

6. **sqlmap -u ”http://example.com/page.php?id=1” –dump-all**

Chapter 11

BurpSuit

11.1 *Introduction*

Burp Suite is one of the most widely used tools for web application security testing. It is developed by PortSwigger and provides a powerful platform for performing security testing of web applications. Ethical hackers, penetration testers, and cybersecurity professionals use it to identify vulnerabilities such as SQL injection, Cross-Site Scripting (XSS), CSRF, insecure authentication, and more.

11.2 *Key Features of Burp Suite*

1. **Proxy – Acts as an intercepting proxy between the browser and the target application. It allows testers to inspect, modify, and replay HTTP/S requests and responses.**

2. **Spider (Crawl) – Automatically crawls the application to discover pages, links, and parameters.**

3. **Scanner (Pro only) – Scans the web application for common vulnerabilities.**

4. **Intruder – Automates customized attacks, such as brute force, fuzzing, and parameter manipulation.**

5. **Repeater – Allows manual testing by sending modified requests repeatedly to observe the response.**

6. **Sequencer – Tests randomness in session tokens.**

7. **Comparer – Compares two requests or responses to find differences.**
8. **Extender – Supports extensions written in Python, Java, or Ruby to add more functionality.**

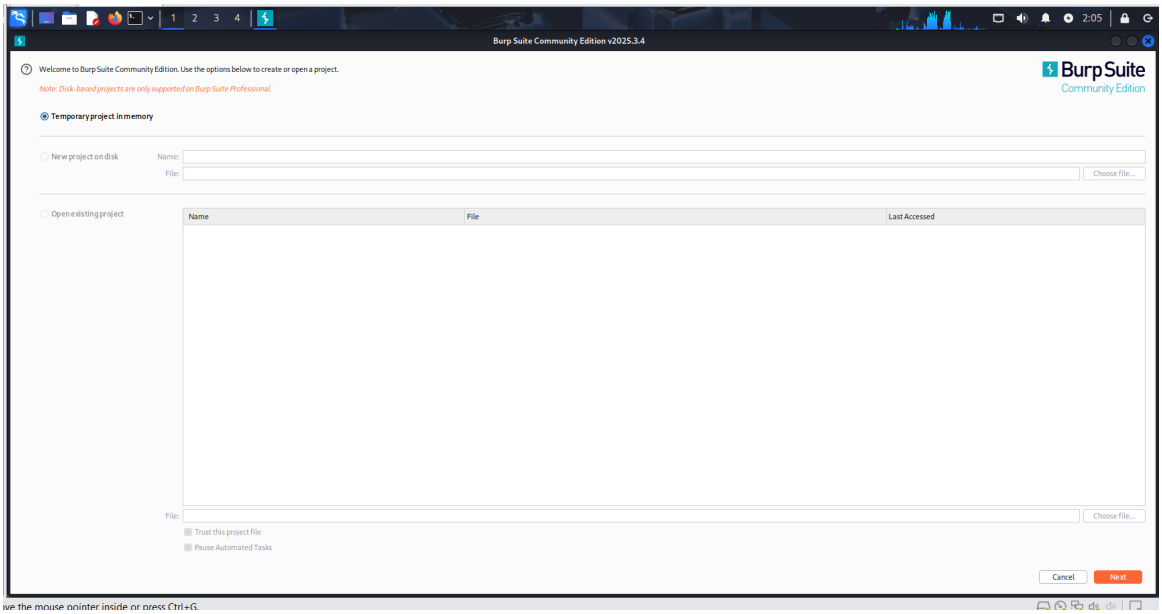
11.3 *Importance in Cybersecurity*

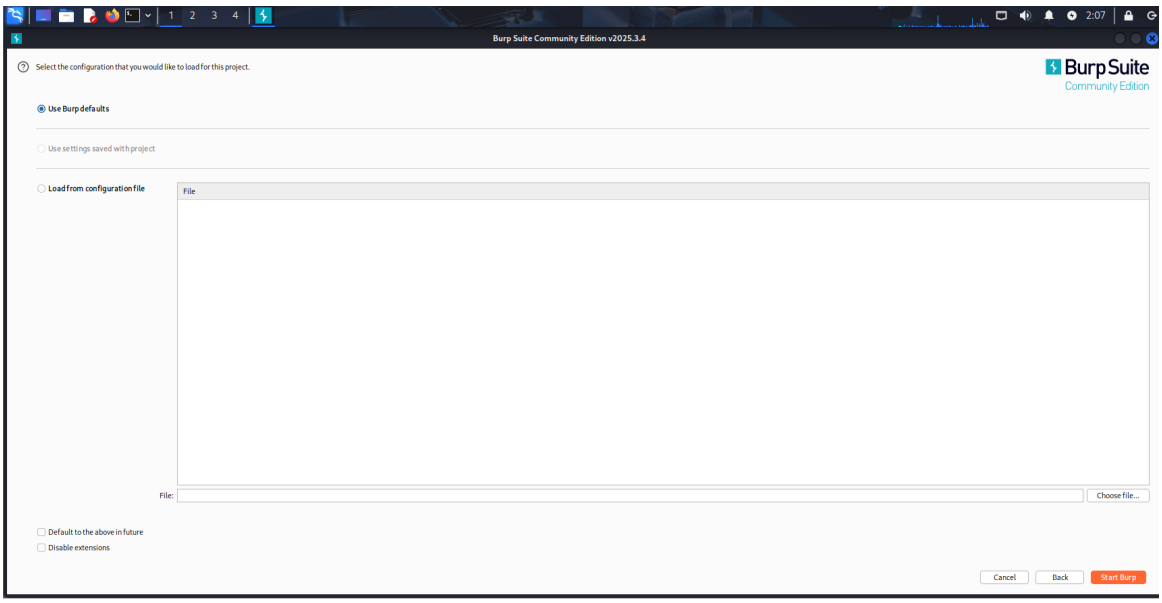
- **Helps in identifying security loopholes in web applications.**
- **Provides both manual and automated testing tools.**
- **Assists penetration testers in simulating real-world attacks safely.**
- **Widely used in bug bounty programs to find critical vulnerabilities.**

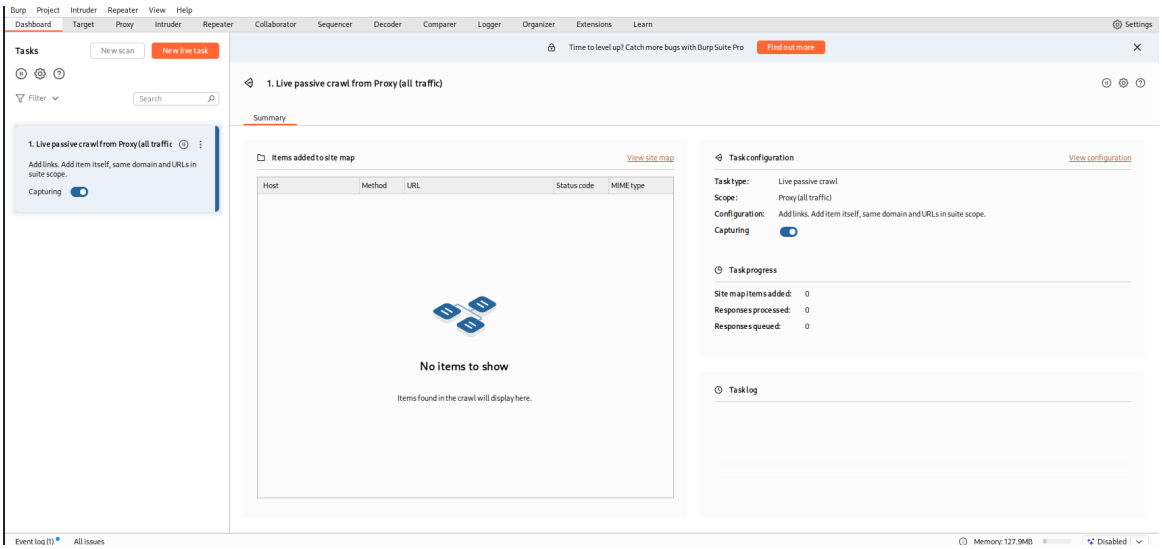
11.4 *Uses*

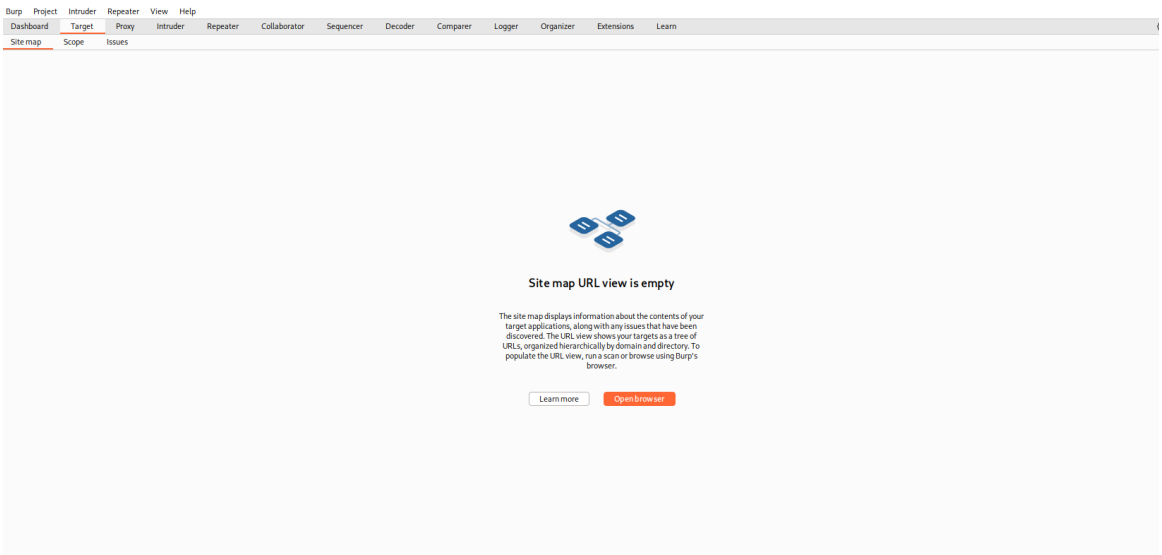
- **Intercepting and Modifying Traffic**
- **Acts as a proxy between your browser and the target web application.**
- **Lets you capture, view, and change HTTP/S requests and responses before they reach the server or client.**
- **Web Application Security Testing**
- **Identifies vulnerabilities like:**
- **SQL Injection**
- **Cross-Site Scripting (XSS)**
- **Cross-Site Request Forgery (CSRF)**
- **Broken Authentication**
- **Insecure Direct Object References (IDOR)**
- **Automated Vulnerability Scanning**
- **(Pro/Enterprise editions) Burp can scan web apps for common vulnerabilities automatically, saving time for testers.**

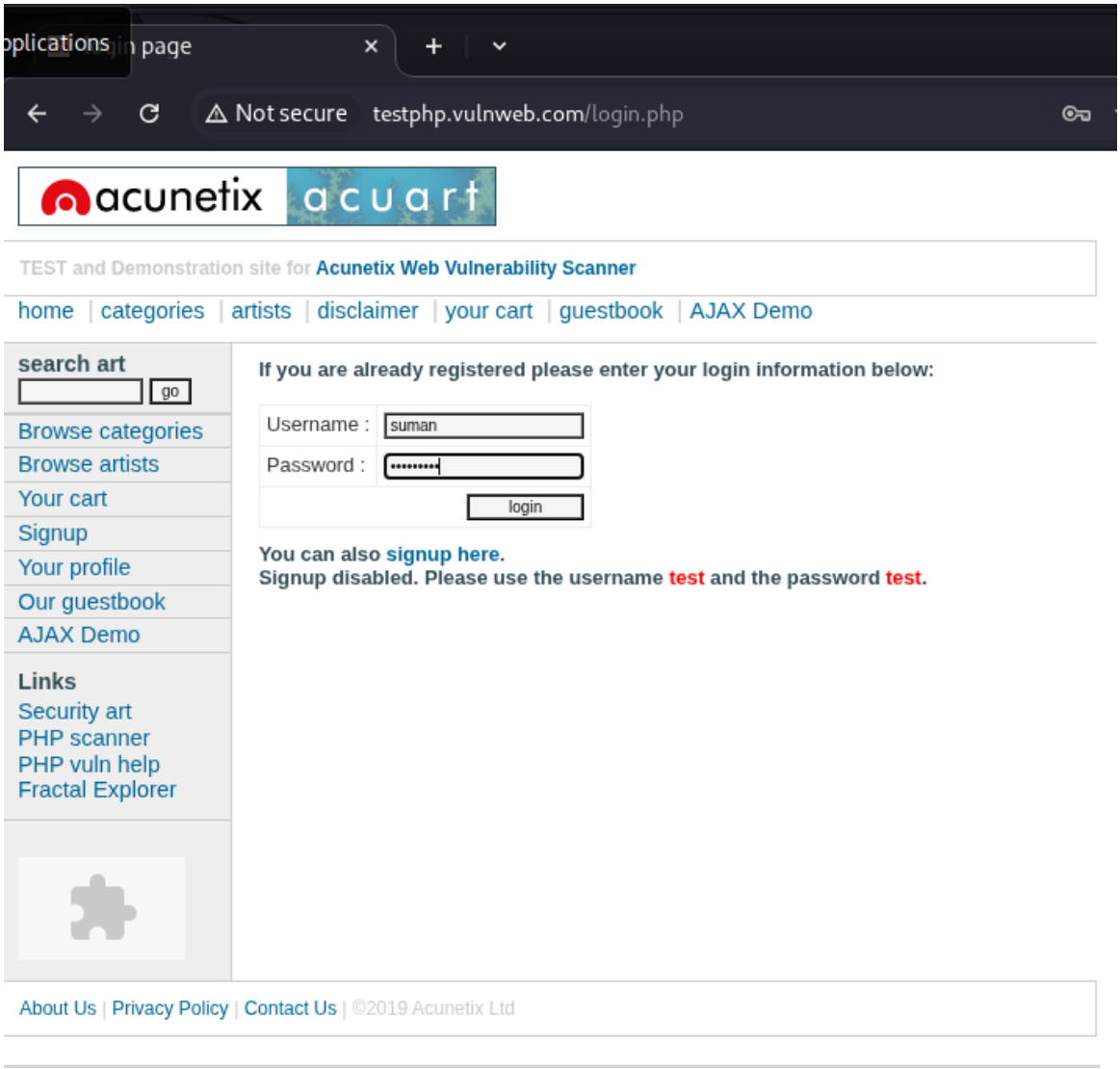
- **Fuzzing and Brute Forcing**
- **With Intruder, Burp can send large numbers of requests to test login forms, parameters, and hidden inputs for weaknesses.**
- **Manual Request Manipulation**
- **Repeater tool allows you to craft and resend modified requests to check how the server responds to changes.**
- **Testing Authentication and Session Management**
- **Sequencer analyzes session tokens (like cookies) to see if they are random and secure.**
- **Helps find flaws in login, logout, and session expiration.**
- **Crawling Web Applications**
- **The Spider automatically maps out web applications, discovering pages, forms, and parameters to test.**
- **Analyzing Application Logic**
- **Helps testers understand how an app processes requests, making it easier to detect logic flaws that automated scanners might miss.**
- **Comparing Responses**
- **The Comparer tool highlights differences between two requests/responses, useful for testing privilege escalation or response changes.**
- **Extending Functionality**
- **Burp supports extensions through the Burp Extender API, allowing integration with custom scripts and tools.**

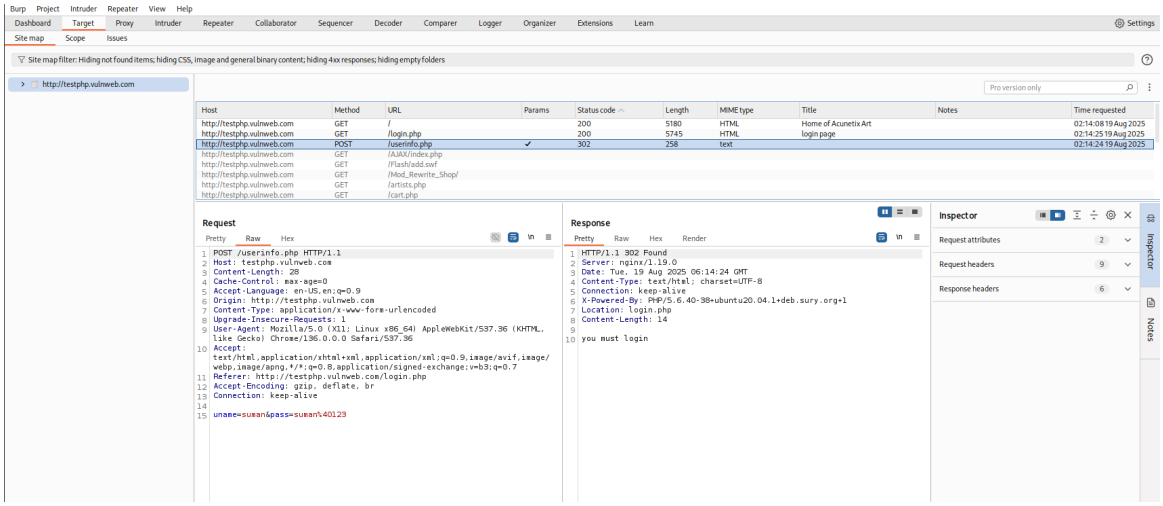

Burp Suite Community Edition v2025.3.4
Welcome to Burp Suite Community Edition. Use the options below to create or open a project.
Note: Disk-based projects are only supported on Burp Suite Professional.
Burp Suite
Community Edition
Temporary project in memory
New project on disk
Name:
File:
Choose file...
Open existing project
Name
File
Last Accessed
File:
Choose file...
Trust this project file
Pause Automated Tasks
Cancel
Next


Burp Suite Community Edition v2025.3.4
Select the configuration that you would like to load for this project.
Burp Suite
Community Edition
Use Burp defaults
Use settings saved with project
Load from configuration file
File
File:
Choose file...
Default to the above in future
Disable extensions
Cancel
Back
Start Burp


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Tasks
New scan
New live task
Time to level up? Catch more bugs with Burp Suite Pro
Find out more
Filter
Search
1. Live passive crawl from Proxy (all traffic)
Summary
1. Live passive crawl from Proxy (all traffic
Add links. Add item itself, same domain and URLs in suite scope.
Capturing
Items added to site map
View site map
Host
Method
URL
Status code
MIME type
No items to show
Items found in the crawl will display here.
Task configuration
View configuration
Task type: Live passive crawl
Scope: Proxy (all traffic)
Configuration: Add links. Add item itself, same domain and URLs in suite scope.
Capturing
Task progress
Site map items added: 0
Responses processed: 0
Responses queued: 0
Task log
Event log (1)
All issues
Memory: 127.9MB
Disabled


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Site map Scope Issues
Site map URL view is empty
The site map displays information about the contents of your target applications, along with any issues that have been discovered. The URL view shows your targets as a tree of URLs, organized hierarchically by domain and directory. To populate the URL view, run a scan or browse using Burp's browser.
Learn more
Open browser


Not secure testphp.vulnweb.com/login.php
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer
If you are already registered please enter your login information below:
Username : suman
Password :
login
You can also signup here.
Signup disabled. Please use the username test and the password test.
About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd


Request
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
Content-Length: 28
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Origin: http://testphp.vulnweb.com
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36
Referer: http://testphp.vulnweb.com/login.php
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
uname=suman&pass=suman%40123
Response
HTTP/1.1 302 Found
Server: nginx/1.19.0
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Location: login.php
Content-Length: 14
you must login
Inspector

Chapter 12

Wireshark

12.1 *Introduction*

Wireshark is the world's most popular open-source network protocol analyzer, designed to capture, filter, and analyze network traffic in real-time. It enables users to look inside live network data or previously saved capture files at a granular level, making it an invaluable tool in the fields of network administration, cybersecurity, and research.

12.2 *Origins and Development*

Wireshark was originally released in 1998 under the name Ethereal by Gerald Combs. Due to trademark issues, the project was renamed Wireshark in 2006. Since then, it has been continuously developed and maintained by a global community, becoming the industry standard for network packet analysis.

12.3 *Key Features*

1. **Packet Capture – Wireshark captures packets directly from the network interface and displays them in real-time.**
2. **Deep Packet Inspection – It allows detailed analysis of hundreds of protocols, including TCP/IP, HTTP, FTP, DNS, VoIP, and many more.**
3. **Filtering and Searching – Advanced filters help users focus only on relevant traffic, reducing noise and making analysis easier.**

4. **Reassembly – Wireshark can reconstruct complete data streams (e.g., web pages, VoIP calls, or file transfers) for further analysis.**
5. **Cross-Platform Support – Available on Windows, Linux, macOS, and UNIX.**
6. **Visualization – Provides statistics, flow graphs, and I/O graphs to help identify traffic patterns and anomalies.**

12.4 *Applications of Wireshark*

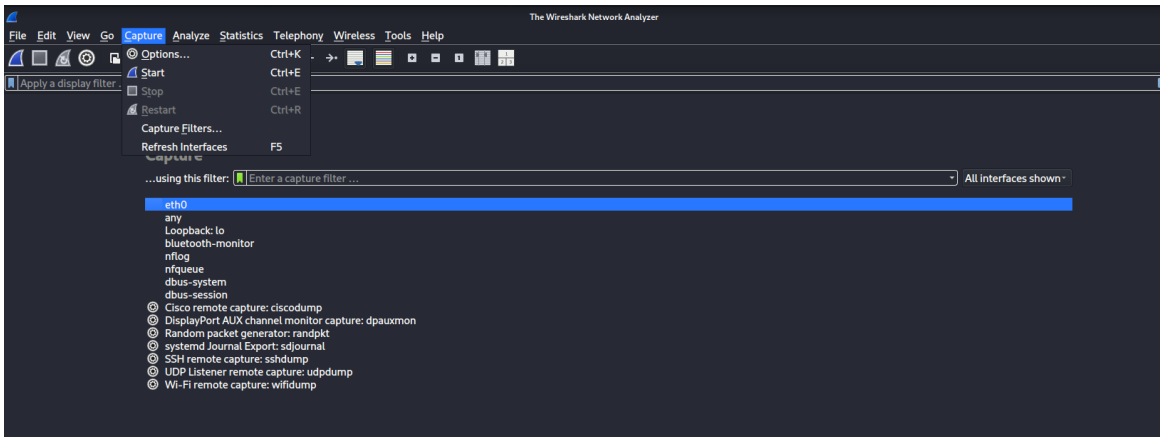
- **Network Troubleshooting: Identifying latency, dropped packets, or misconfigured devices.**
- **Cybersecurity: Detecting malicious traffic, intrusion attempts, and data exfiltration.**
- **Protocol Development: Testing and debugging new network protocols.**
- **Education and Research: Teaching networking concepts and analyzing network behavior in labs.**

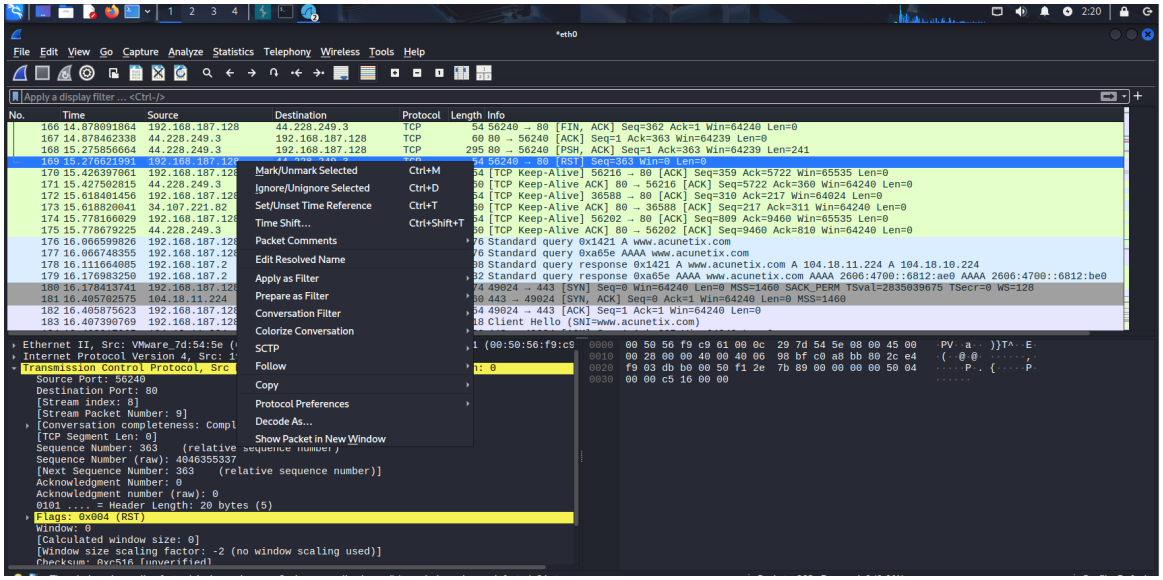
12.5 *Advantages*

- **Free and open-source with active community support.**
- **Intuitive graphical user interface (GUI) and command-line options.**
- **Supports hundreds of protocols with frequent updates.**

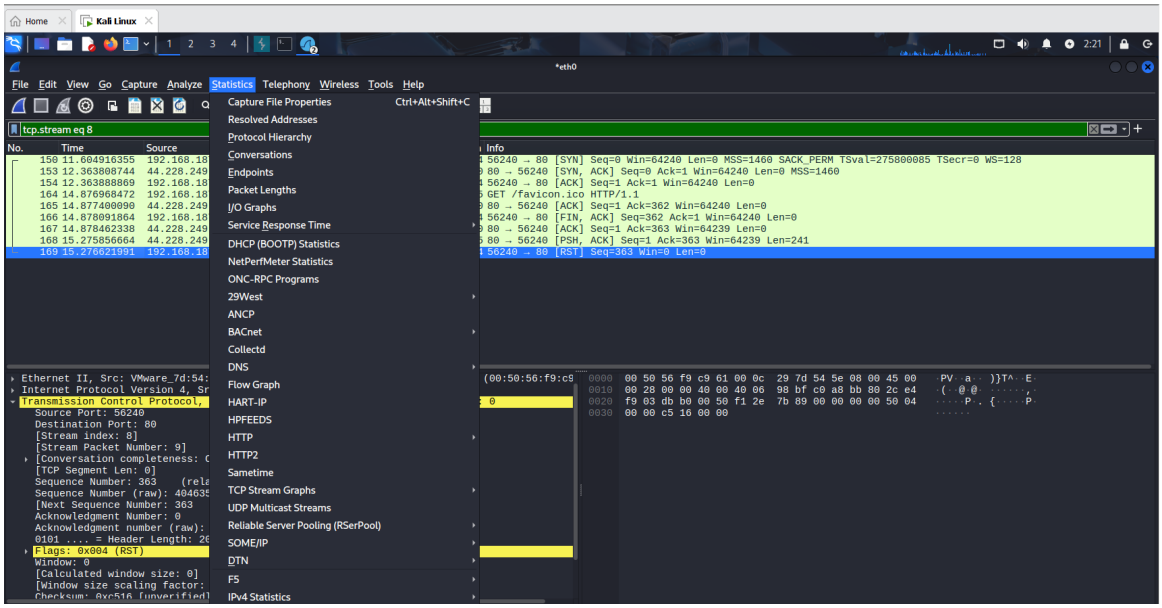
12.6 *Limitations*

- **Requires administrative privileges to capture live traffic.**
- **Large capture files can become difficult to manage.**
- **Cannot decrypt encrypted traffic (like HTTPS) without proper keys.**

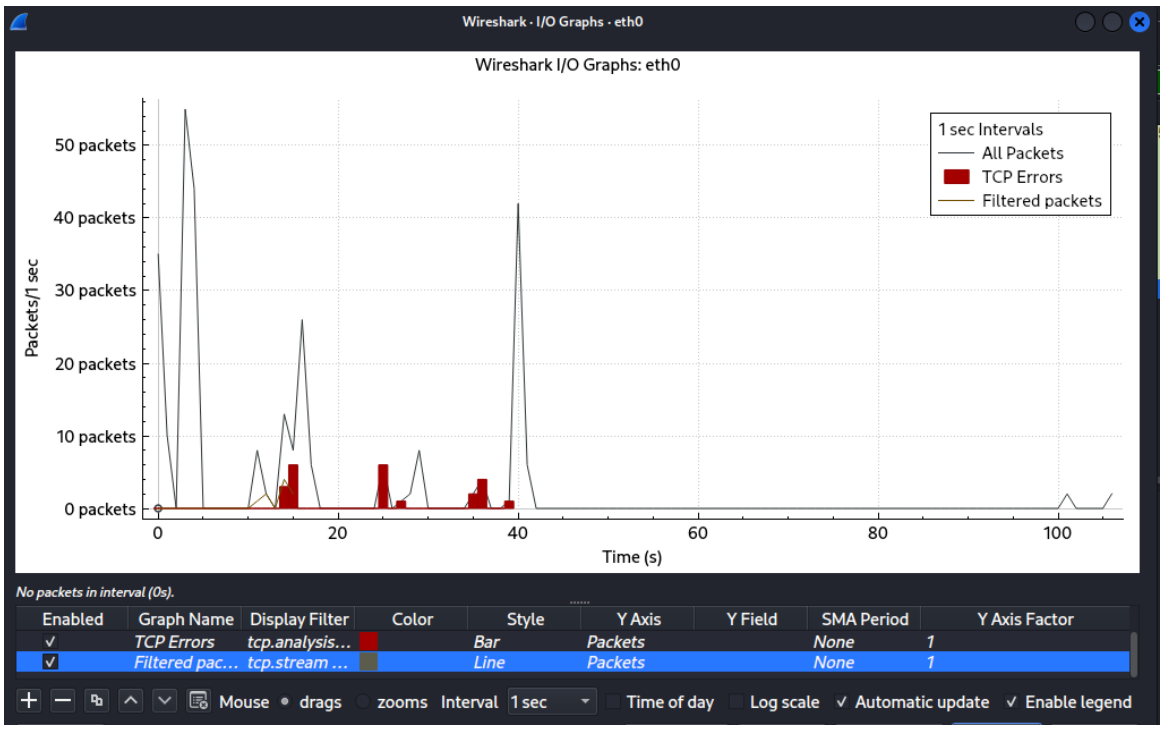

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Options... Ctrl+K
Start Ctrl+E
Stop Ctrl+E
Restart Ctrl+R
Capture Filters...
Refresh Interfaces F5
...using this filter: Enter a capture filter ...
All interfaces shown
eth0
any
Loopback: lo
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
Cisco remote capture: ciscodump
DisplayPort AUX channel monitor capture: dpauxmon
Random packet generator: randpkt
systemd Journal Export: sdjournal
SSH remote capture: sshdump
UDP Listener remote capture: udpdump
Wi-Fi remote capture: wifidump

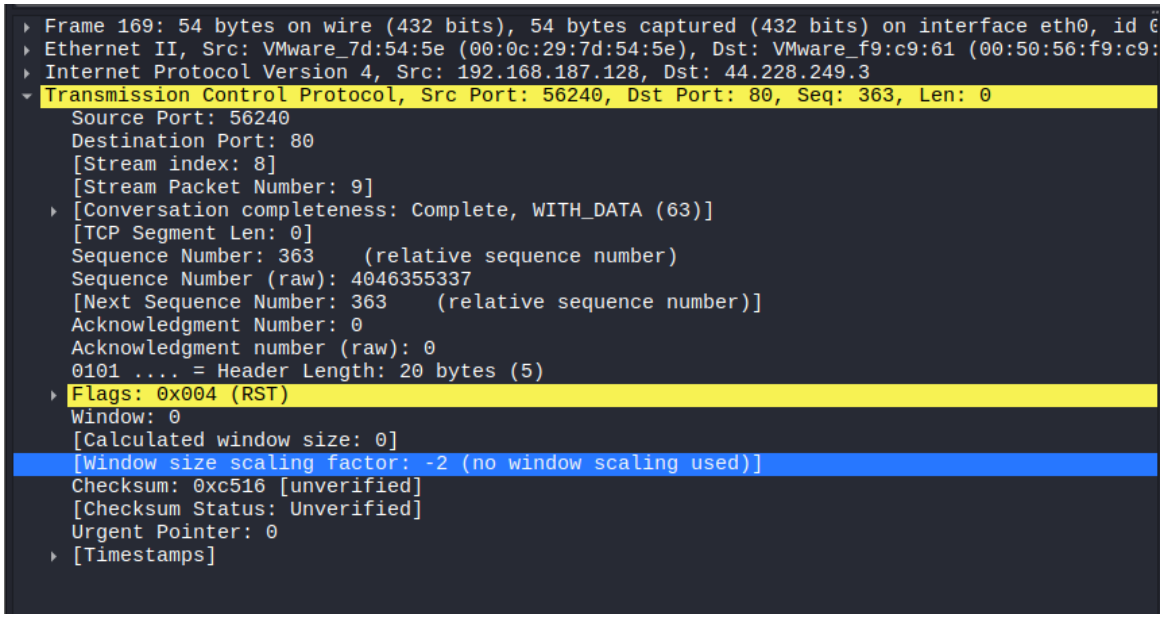

*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
Mark/Unmark Selected Ctrl+M
Ignore/Unignore Selected Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comments
Edit Resolved Name
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window


GET /favicon.ico HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: image/avif,image/webp,image/png,image/svg+xml,image/*;q=0.8,*/*;q=0.5
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://testphp.vulnweb.com/
Priority: u=6
HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Mon, 18 Aug 2025 06:07:15 GMT
Content-Type: image/x-icon
Content-Length: 894
Last-Modified: Wed, 11 May 2011 10:27:48 GMT
Connection: keep-alive
ETag: "4dca64a4-37e"
Accept-Ranges: bytes



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	9	100.0	1126	2,453	0	0	0	9
Ethernet	100.0	9	12.4	140	305	0	0	0	9
Internet Protocol Version 4	100.0	9	16.0	180	392	0	0	0	9
Transmission Control Protocol	100.0	9	18.1	204	444	8	184	400	9
Hypertext Transfer Protocol	11.1	1	32.1	361	786	1	361	786	1




Frame 169: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
Ethernet II, Src: VMware_7d:54:5e (00:0c:29:7d:54:5e), Dst: VMware_f9:c9:61 (00:50:56:f9:c9:
Internet Protocol Version 4, Src: 192.168.187.128, Dst: 44.228.249.3
Transmission Control Protocol, Src Port: 56240, Dst Port: 80, Seq: 363, Len: 0
Source Port: 56240
Destination Port: 80
[Stream index: 8]
[Stream Packet Number: 9]
[Conversation completeness: Complete, WITH_DATA (63)]
[TCP Segment Len: 0]
Sequence Number: 363 (relative sequence number)
Sequence Number (raw): 4046355337
[Next Sequence Number: 363 (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0
0101 .... = Header Length: 20 bytes (5)
Flags: 0x004 (RST)
Window: 0
[Calculated window size: 0]
[Window size scaling factor: -2 (no window scaling used)]
Checksum: 0xc516 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]

Chapter 13

References

@inproceedingsthakur2015investigation, title=An investigation on cyber security threats and security models, author=Thakur, Kutub and Qiu, Meikang and Gai, Keke and Ali, Md Liakat, booktitle=2015 IEEE 2nd international conference on cyber security and cloud computing, pages=307–311, year=2015, organization=IEEE

@articlekaur2022recent, title=The recent trends in cyber security: A review, author=Kaur, Jagpreet and Ramkumar, KR, journal=Journal of King Saud University-Computer and Information Sciences, volume=34, number=8, pages=5766–5781, year=2022, publisher=Elsevier

@articleghelani2022cyber, title=Cyber security, cyber threats, implications and future perspectives: A Review, author=Ghelani, Diptiben, journal=Authorea Preprints, year=2022, publisher=Authorea