Cyber Attack Lifecycle & VAPT

29/07/2025

Aromal Kurup S G

Project Phase 1

CSA 2025

ICTAK March Batch

Index

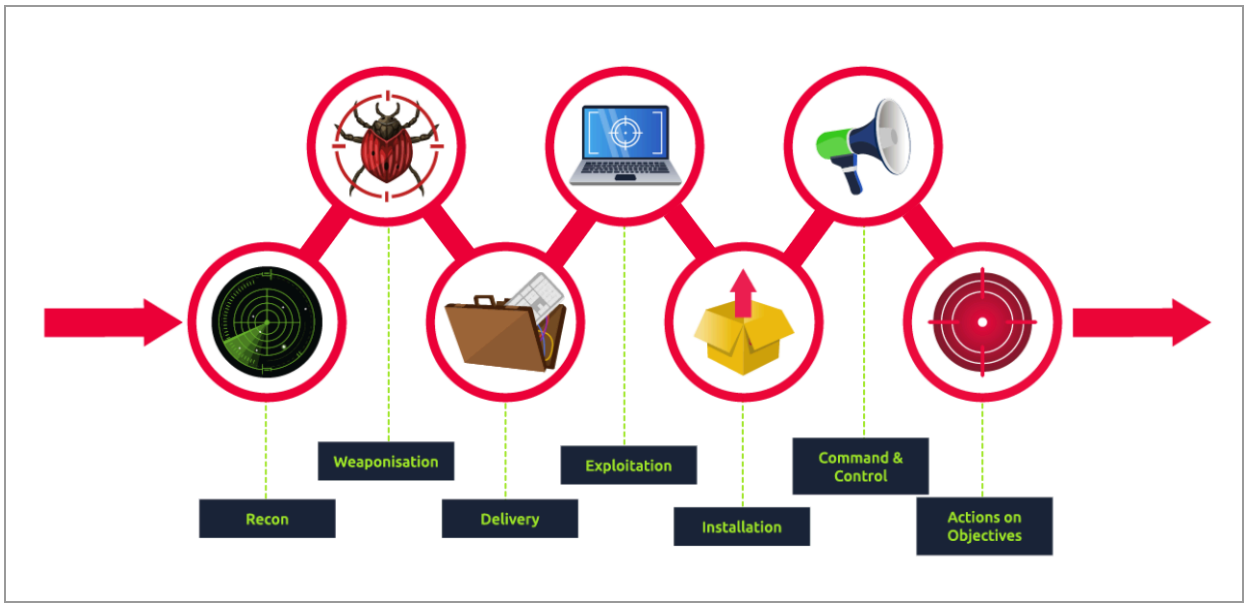
Introduction

As always,technology has been the stepping stone for the development of mankind. In this 21st century we all are driven by an evolved tech world. As technology became imperative, the need for security in the cyber world also became a necessity. That's where **Cybersecurity** comes into play.

Cybersecurity is essential for protecting systems, networks, and data from digital attacks, damage, or unauthorized access. In today's highly connected world, where almost every aspect of life depends on digital technologies, cybersecurity plays a **critical role** in ensuring safety, trust, and stability. To sum up, Cybersecurity is not just a technical necessity; it is a fundamental pillar of safety, trust, and progress in the digital age.

This phase 1 of the project is aimed at conducting a literature survey on Cyberattack Lifecycle and VAPT. It is a **critical summary and evaluation** of existing research, writings, and studies that helps to understand what is already known. Here we can also identify gaps or conflicts in knowledge, and build a foundation for the upcoming phases of the project. Thus this phase reviews existing literature and sets the tone for practical implementation.

Cyber Attack Lifecycle



The Cyber Attack Lifecycle is a conceptual model that outlines the steps an attacker takes to successfully carry out a cyberattack — from initial reconnaissance to achieving their end goal. Understanding this lifecycle enables defenders to map security controls to each phase, disrupting attacks before objectives are achieved.

Two popular frameworks representing this lifecycle are:

- **Lockheed Martin's Cyber Kill Chain**
- **MITRE ATT&CK Framework**

Lockheed Martin Cyber Kill Chain

The Lockheed Martin's Cyber Kill Chain protects against attacks by providing a structured approach to understanding and countering the tactics, techniques, and procedures (TTPs) used by cyber adversaries. By breaking down an attack into its constituent phases, organizations can implement specific security measures tailored to each stage.

The various stages of the Lifecycle are;

1. Reconnaissance

Reconnaissance is the initial phase of the cyber kill chain, where attackers gather information about their target to plan their attack. This stage involves collecting data on vulnerabilities, network defenses, and potential entry points. Attackers may use various techniques such as social engineering, public information searches, and network scanning to accumulate valuable intelligence. This gathered information enables attackers to tailor their approach, select tools, and devise strategies that are most likely to succeed in compromising the target. Effective defense against reconnaissance efforts requires robust perimeter security, employee awareness training, and monitoring for unusual activity that could indicate a reconnaissance attempt in progress.

- **Tools**: Shodan, Google Dorking, or WHOIS.

2. Weaponization

Weaponization involves the attacker creating or repurposing a cyber weapon, such as malware or a virus, tailored to exploit vulnerabilities identified during the reconnaissance phase. This step combines the malicious payload with an exploit into a deliverable format that can be used to target the victim's system. The creation of this cyber weapon is done with the intent to ensure successful delivery and execution on the target network without detection.

The effectiveness of defensive measures against weaponization relies heavily on understanding and mitigating known vulnerabilities within systems and applications. Regularly updating software, employing vulnerability management programs, and utilizing threat intelligence can help in identifying potential threats before they are weaponized against an organization.

- **Example**: Creating a malicious Word document with a macro exploit.

3. Delivery

Delivery is the phase where the attacker transmits the weaponized content to the target. This can be achieved through various methods such as email attachments, websites, or direct network penetration. The goal is to ensure that the malicious payload reaches the intended victim and can be executed to further compromise the system. Defenses against delivery attempts include email filtering, web security solutions, and intrusion detection systems that can identify and block malicious transmissions.

In this stage, attackers may employ tactics like phishing or exploiting vulnerabilities in public-facing applications to deliver their payload. It's crucial for organizations to maintain a high level of vigilance through employee training on recognizing phishing attempts and maintaining robust patch management processes. By doing so, they reduce the risk of successful delivery of malicious payloads, thereby disrupting the attack chain at an early stage.

- **Example**: Phishing email with an infected attachment.

4. Exploitation

Exploitation occurs when the attacker's delivered payload activates on the victim's system, exploiting a vulnerability to execute malicious code. This phase marks the successful penetration of the target's defenses, allowing attackers to establish a foothold within the system. It often leverages software vulnerabilities that have not been patched or are unknown to software vendors.

Successful exploitation enables further malicious activities, such as installing malware or stealing sensitive information. Defenses against this phase include rigorous patch management, application whitelisting, and employing intrusion prevention systems that can detect and block attempts at exploiting known vulnerabilities.

- **Example**: Exploiting a browser vulnerability to run arbitrary code.

5. Installation

During the installation phase, attackers establish their presence on the victim's system by installing malware or other malicious tools. This step is crucial for maintaining control over the compromised system and executing further malicious activities. The malware installed can take various forms, including backdoors, keyloggers, or ransomware, depending on the attacker's objectives.

To counteract installation efforts, organizations must employ robust endpoint security solutions that include antivirus and anti-malware tools capable of detecting and removing unauthorized software. Regular system scans and updates, coupled with user education on safe computing practices, are essential in minimizing the risk of successful malware installation.

- **Example**: Dropping a remote access tool (RAT) on the system.

6. Command and Control (C2)

Command and Control (C2) is the stage where attackers establish a communication channel with the compromised system to control it remotely. This allows them to issue commands, exfiltrate data, or deploy additional malware. C2 activity often involves communicating with servers controlled by the attackers, which can be located anywhere in the world. Detection and disruption of these communication channels are vital for dismantling the control attackers have over compromised systems.

To defend against C2 activities, organizations must monitor network traffic for unusual patterns that may indicate communication with malicious external servers. Implementing network segmentation can also limit the movement of attackers within a network, reducing the impact of compromised systems. Additionally, employing intrusion detection systems and regularly updating firewall rules are effective in identifying and blocking unauthorized communications.

- **Example**: Using Cobalt Strike to control compromised systems.

7. Actions on Objectives

Actions on Objective represents the final phase in the Cyber Kill Chain, where attackers achieve their primary goal, be it data exfiltration, destruction of data, or establishing a long-term presence within the target's network for espionage. At this stage, the attacker has successfully bypassed preceding security measures and executes actions to fulfill their intended objectives. These activities can range from encrypting critical files in ransomware attacks to extracting sensitive information or creating backdoors for future access.

To defend against these actions, organizations need to implement advanced threat detection and response systems that can identify and mitigate threats before they culminate in significant damage. Continuous monitoring of systems and networks for signs of unauthorized access or anomalies is crucial. Employing incident response protocols that can swiftly isolate affected systems and remediate threats ensures minimal impact and quick recovery from attacks.

- **Example**: Exfiltrating sensitive HR data or deploying ransomware.

MITRE ATT&CK Framework

The MITRE ATT&CK framework (MITRE ATT&CK) is a universally accessible, continuously updated knowledge base for modeling, detecting, preventing and fighting cybersecurity threats based on cybercriminals' known adversarial behaviors. MITRE ATT&CK catalogs cybercriminal tactics, techniques and procedures (TTPs) through each phase of the cyberattack lifecycle—from an attacker's initial information gathering and planning behaviors, through to the ultimate execution of the attack. The information in MITRE ATT&CK can help security teams accurately simulate cyberattacks to test cyber defenses and create more effective security policies.

MITRE ATT&CK Tactics

Each MITRE ATT&CK tactic represents a specific adversarial goal—something the attacker wants to accomplish at a given time. ATT&CK tactics correspond closely to stages or phases of a cyberattack. For example, ATT&CK tactics covered by the **Enterprise Matrix** include:

- **Reconnaissance**: Gathering information for planning an attack.
- **Resource Development**: Establishing resources to support attack operations.
- **Initial Access**: Penetrating the target system or network.
- **Execution**: Running malware or malicious code on the compromised system.
- **Persistence**: Maintaining access to the compromised system (in the event of shutdown or reconfigurations).
- **Privilege Escalation**: Gaining higher-level access or permissions (e.g., moving from user to administrator access).
- **Defense Evasion**: Avoiding detection once inside a system.
- **Credential Access**: Stealing usernames, passwords, and other logon credentials.
- **Discovery**: Researching the target environment to learn what resources can be accessed or controlled to support a planned attack.
- **Lateral Movement**: Gaining access to additional resources within the system.

- **Collection**: Gathering data related to the attack goal (e.g., data to encrypt and/or exfiltrate as part of a ransomware attack).

- **Command and Control**: Establishing covert/undetectable communications that enable the attacker to control the system.

- **Exfiltration**: Stealing data from the system.

- **Impact**: Interrupting, corrupting, disabling, or destroying data or business processes.

Tactics and techniques vary from matrix to matrix (and submatrix). For example, the **Mobile Matrix** does not include **Reconnaissance** and **Resource Development** tactics, but includes other tactics—**Network Effects** and **Remote Service Effects**—not found in the Enterprise Matrix.

MITRE ATT&CK Techniques

If MITRE ATT&CK tactics represent what attackers want to accomplish, MITRE ATT&CK techniques represent how they try to accomplish it. For example, drive-by compromise and spear phishing are types of initial access techniques; using fileless storage is an example of a defense evasion technique.The knowledge base provides the following information for each technique:

- A description and overview of the technique.
- Any known subtechniques associated with the technique. For example, subtechniques for phishing include spear phishing attachment, spear phishing link and spear phishing via service. At this writing, MITRE ATT&CK documents 196 individual techniques and 411 subtechniques.
- Examples of related procedures. These can include ways that attack groups use the technique, or types of malicious software used to execute the technique.
- Mitigations—security practices (e.g., user training) or software (e.g. antivirus software, intrusion prevention systems) that can block or address the technique.
- Detection methods. Typically these are log data or system data sources that security teams or security software can monitor for evidence of the technique.

Vulnerability Assessment and Penetration Testing (VAPT)

VAPT is a structured cybersecurity process that combines two complementary services—Vulnerability Assessment (VA) and Penetration Testing (PT)—to identify, evaluate, and remediate security weaknesses before they can be exploited by real attackers.The core components are;

- Vulnerability Assessment (VA):
  Automated scans and manual techniques detect and catalog potential vulnerabilities—misconfigurations, missing patches, default credentials, insecure settings.
- Penetration Testing (PT):
  Ethical hackers actively exploit identified weaknesses (and potential zero-days) to determine real-world impact and attack paths

VAPT Methodology

There are three main methods or strategies used to conduct Vulnerability Assessment and Penetration Testing (VAPT): **Black Box Testing**, **White Box Testing**, and **Gray Box Testing**. Each approach offers different levels of access and insight into the system being tested.

1. Black Box Testing

In black box penetration testing, the tester is given no prior knowledge about the target system. This method simulates the actions of an external attacker attempting to breach the system from the outside. The penetration tester starts from scratch, mimicking real-world attacks to discover vulnerabilities through reconnaissance, scanning, exploitation, and post-exploitation—all without any internal credentials or architecture knowledge.

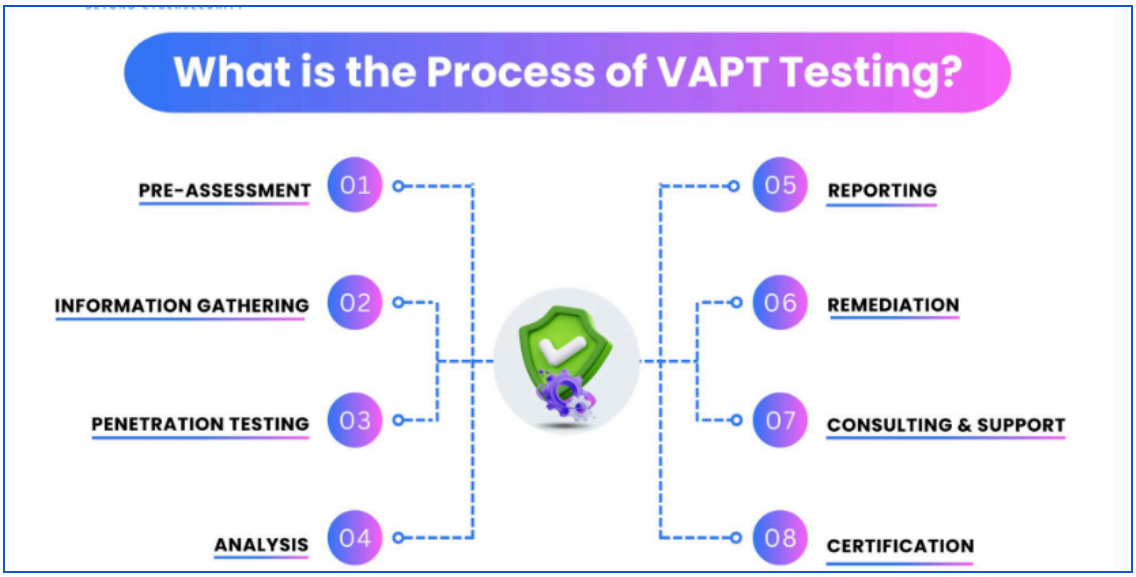
2. White Box Testing

White box testing provides the tester with full knowledge of the system's internal workings, including source code, architecture diagrams, and credentials. The tester has the perspective of an insider and can perform a thorough code-level security analysis. This approach allows for deep testing of logic flaws, insecure configurations, and vulnerabilities that would not be apparent from an external view. It's highly effective for evaluating the system's resistance to various real-time attacks.

3. Gray Box Testing

Gray box testing is a hybrid approach where the tester is given limited information about the system, such as user credentials or partial access. Also known as transparent box testing, this method simulates an attack by a user with some level of trust or access within the organization—like an employee or contractor. It helps assess what a semi-privileged attacker could exploit and how much damage they could cause from that position.

Process of VAPT



Vulnerability Assessment and Penetration Testing (VAPT) follows a structured approach to identify and fix security flaws. Below is a step-by-step breakdown of the process:

1. Pre-Assessment

Before starting, the security team defines the scope, objectives, and rules of the test. This involves:

- Understanding the system's architecture, purpose, and potential risks.
- Setting up the testing environment.
- Getting required approvals and access credentials.

2. Information Gathering

The security team collects technical and non-technical details about the system. This includes:

- Scanning for public and internal information related to the system.
- Understanding the technology stack, APIs, and third-party integrations.
- Conducting reconnaissance to map out possible attack points.

3. Penetration Testing

Testers simulate real-world cyberattacks to find security weaknesses. The key areas tested include:

- Authentication & Access Control – Checking login mechanisms, session management, and user roles.
- Data Storage & Transmission – Evaluating encryption and data protection measures.
- Business Logic Flaws – Testing for logic errors that hackers can exploit.
- API & Third-Party Integrations – Assessing risks from connected services.

- Automated & Manual Testing – Using security tools alongside expert-driven testing for deeper insights.

4. Analysis

Each vulnerability is assessed based on three key factors:

- Likelihood of Exploitation – How easy it is for an attacker to exploit the flaw.
- Impact on Business & Users – Confidentiality, integrity, and availability risks.
- Severity Rating – Categorized using OWASP, CVSS, and real-world attack impact.

5. Reporting

The penetration testing team provides a detailed VAPT report that includes:

- A summary of vulnerabilities and their severity levels.
- Technical details on how each issue was discovered.
- Recommended fixes with step-by-step remediation guidance.
- Compliance alignment (e.g., ISO 27001, SOC 2, GDPR, PCI-DSS, FDA).

6. Remediation & Retesting

Developers fix the vulnerabilities based on the recommendations. Security testers retest to confirm that:

- Fixes are properly implemented.
- No new security risks have emerged.
- The system is now more secure.

7. Consulting & Support

Post-testing consultation helps teams understand:

- How to strengthen security in future updates.
- Secure coding best practices.
- Compliance measures for ongoing protection.

8. Certification & Attestation

After successful testing and remediation, companies receive:

- A VAPT Security Certificate confirming compliance.
- A Letter of Attestation proving the system was tested against the latest cybersecurity standards

Types of VAPT

There are 8 significant types of VAPT;

1. Web Application Penetration Testing

This type of testing focuses on identifying vulnerabilities in web-based applications. It involves analyzing input fields, authentication mechanisms, session management, and business logic to uncover security flaws like SQL Injection, XSS, and CSRF.

Tools: Burp Suite, OWASP ZAP, Nikto, Acunetix

2. Mobile Application Penetration Testing

Mobile app pentesting targets vulnerabilities in Android and iOS applications. It assesses both the app's frontend (user interface) and backend (API communication, data storage) for weaknesses.

Tools: MobSF (Mobile Security Framework), Frida, Drozer, Burp Suite

3. Cloud Application Penetration Testing

This testing evaluates the security posture of applications hosted on cloud platforms like AWS, Azure, or GCP. It checks for misconfigured storage, insecure APIs, identity and access management flaws, and exposed services.

Tools: ScoutSuite, Prowler, Pacu, AWS Inspector, CloudSploit

4. IoT Penetration Testing

IoT pentesting involves analyzing internet-connected devices and their ecosystems. It includes testing the firmware, communication protocols, mobile apps, and cloud integrations.

Tools: Shodan, Wireshark, Binwalk, Firmalyzer, Ghidra

5. API Penetration Testing

APIs are often a target due to poor access control and input validation. This testing examines endpoints, request/response handling, rate limits, and data exposure.

Tools: Postman, Burp Suite, Insomnia, OWASP Amass, SoapUI

6. Desktop Application Penetration Testing

This type focuses on software installed on Windows, macOS, or Linux systems. It identifies vulnerabilities in how the application handles files, user input, memory, and system calls.

Tools: IDA Pro, Ghidra, OllyDbg, Immunity Debugger

7. AI/ML Penetration Testing

With the rise of AI-based applications, this testing identifies how attackers might exploit ML models (e.g., model poisoning, evasion, or data leakage). It evaluates model behavior under malicious input.

Tools: Adversarial Robustness Toolbox (ART), CleverHans, TensorFlow Security Toolkit

8. Network Penetration Testing

Network pentesting checks internal and external infrastructure for vulnerabilities like open ports, weak credentials, outdated services, and insecure configurations.

Tools: Nmap, Metasploit, Nessus, OpenVAS, Wireshark

Environments of VAPT

VAPT can be conducted across diverse environments, each presenting unique security challenges and requiring specialized approaches. Understanding these environments helps organizations implement comprehensive security testing strategies tailored to their specific technology stacks and infrastructure.

It's very important to note that for different environments we will be tailoring different tools and threat modelling accordingly. Below shown is the Environment comparison table.

Environment	Tools Used	Primary Risks	Testing Approach	Safety Concerns
Web Applications	Burp Suite, OWASP ZAP, Nikto	SQL injection, XSS, broken authentication	Automated scanning + manual business-logic testing	Low risk; tests run in staging/QA environments to avoid live disruption
Network Infrastructure	Nmap, Nessus, OpenVAS, Wireshark	Lateral movement, privilege escalation	Network discovery → vulnerability scanning → controlled exploitation	Medium risk; may disrupt services—use off-hours or isolated network segments
IoT Devices	JTAGulator, Binwalk, Scapy, Wireshark	Device takeover, botnet recruitment	Hardware interface analysis + firmware reverse-engineering + protocol testing	High risk; physical testing can damage hardware—use lab-grade devices
Mobile Applications	MobSF, APKTool, Frida, Burp Mobile Assistant	Data leakage, insecure storage, auth bypass	Static analysis (SAST) + dynamic testing (DAST) + interactive testing	Low-medium; emulators are safe, real-device tests risk data loss if unisolated
Cloud Environments	ScoutSuite, Prowler, AWS CLI, Azure CLI, GCP gcloud	IAM misconfigurations, exposed buckets	Continuous configuration assessment + API security testing	Medium; testing misconfigs may trigger alerts—use test accounts
ICS/SCADA Systems	Wireshark, PLCScan, ModbusPal, passive network TAPs	Safety system disruption, physical damage	Passive monitoring → controlled active tests on isolated OT networks	Very high; must avoid process interference—use simulators or testbeds

Difference Between Cyberattack Lifecycle and VAPT

Feature	Cyberattack Life Cycle	VAPT
Definition	Model describing stages of a real cyberattack	Security testing methodology (assessment + simulated attack)
Purpose	Understand how attacks unfold to improve detection and response	Proactively identify and fix vulnerabilities
Perspective	Attacker-focused (what real attackers do step-by-step)	Defender-focused (how to identify and mitigate weaknesses)
Process	Series of attack stages: Recon → Exploit → Execute	VA: Scan/identify flaws; PT: Simulated hacker tries to exploit
Usage	Incident response, threat modeling, defense strategy	Regular security audits, compliance, risk reduction
Goal	Disrupt or prevent actual attacks at each phase	Strengthen security by fixing exploitable vulnerabilities
Cycle Example	Recon, Weaponize, Deliver, Exploit, Install, C2, Action	Plan → Gather Info → Scan → Exploit → Report/Remediate

Conclusion

The Cyber Kill Chain and Vulnerability Assessment & Penetration Testing (VAPT) frameworks together provide a comprehensive roadmap for understanding and securing modern IT environments. The Kill Chain outlines the sequential stages an attacker follows—reconnaissance, weaponization, delivery, exploitation, installation, command & control, and actions on objectives—enabling defenders to anticipate and disrupt hostile activities at each phase. VAPT complements this defensive approach by systematically identifying and validating vulnerabilities through automated scanning, manual analysis, exploitation, and remediation planning. Integrating insights from the Kill Chain into VAPT engagements ensures that assessments not only uncover technical weaknesses but also simulate real-world attack pathways, thereby strengthening an organization's security posture across web applications, networks, IoT devices, mobile and cloud platforms, and industrial control systems. Together, these methodologies foster a proactive, intelligence-driven defense strategy that reduces risk, meets compliance requirements, and enhances resilience against evolving cyber threats.

Both the Cyber Kill Chain and VAPT suffer from rigid, point-in-time approaches that struggle with today's dynamic, multi-vector threats—Kill Chain's linear stages miss complex attack paths and insider actions, while VAPT scans often generate false positives, inconsistently scope assessments, and overlook emerging vulnerabilities in cloud-native, serverless, OT/ICS, and IoT environments. To improve, organizations should integrate MITRE ATT&CK for granular TTP mapping, embed continuous testing into CI/CD pipelines, leverage AI/ML to reduce false alarms, standardize methodologies (e.g., PTES, OSSTMM), and develop specialized modules for cloud-native, OT, and IoT security testing.

Moving forward to other phases of the project which include Reconnaissance,Vulnerability assessment & Pentesting, it's very important to map and analyze the environment and resources we have. The various stages of Cyber Attack Lifecycle and processes in VAPT should be mastered along with familiarizing vital tools like Nmap, Wireshark, Burpsuite, Metasploit,Netcat etc. It's very important to adapt to the environment and select tools according to the requirements. As the Cyberattack Lifecycle showcases the path of attackers, VAPT provides structured guidance to walk along that path for effective testing. It's imperative to follow ethical behaviour all along as we are granted access to sensitive systems, networks, and data. Ethical decision-making is critical to ensure **trust, integrity, and lawful conduct** which contributes to the backbone of Cybersecurity.

References

The following sources were referred to during the preparation of this report.

- Aquasec - Lockheed Martin Cyber Kill Chain
  https://www.aquasec.com/cloud-native-academy/application-security/cyber-kill-chain/

- Tryhackme - Cyber Kill Chain
  https://tryhackme.com/room/cyberkillchainzmt

- Varonis - Cyber Kill Chain and how to use it effectively
  https://www.varonis.com/blog/cyber-kill-chain

- Qualisec - VAPT & Methodologies
  https://qualysec.com/what-is-vapt-testing-its-methodology-importance-for-business

- IBM - MITRE ATT&CK Framework
  https://www.ibm.com/think/topics/mitre-attack

- Chat GPT

- Perplexity

Annexure A

Phase 2: Reconnaissance Phase Report

1. Title Page
    - Project Name, Team Name, Date, Target Environment (e.g., Web App/IoT/Cloud)
2. Executive Summary
    - Objective of Reconnaissance
3. Work Allocation Table
    - Team Member | Role | Tasks Performed | Public IP Used
4. Target Overview
    - Target IP/URL (if assigned)
    - Description of Target Environment
5. Methodology
    - Tools & Techniques Used
6. Information Gathered
    - System/network mapping
    - Services/ports identified
    - Publicly available info
    - Application structure (for web)
7. Findings and Observations
8. Screenshots/Evidence
9. Challenges/Limitations
10. Summary
11. Appendix

Annexure B

Phase 3: Vulnerability Assessment Report

1. Title Page
2. Executive Summary
3. Work Allocation Table
4. Target Overview
5. Purpose & Scope
6. Assessment Methodology
    - Tools/Scanners Used
    - Approaches referencing Phase 1 & 2
7. Vulnerabilities Identified
    - Name | Severity | Description | Source/Reference
8. Supporting Evidence
    - Screenshots, Log Entries
9. Remediation Recommendations
10. Limitations
11. Summary
12. Appendix

Annexure C

Phase 4: Penetration Testing Report

1. Title Page
2. Executive Summary
3. Work Allocation Table
4. Target Details
5. Testing Scope
6. Methodology
    - Steps to Confirm Recon/VA Findings
    - New Pentesting Steps
7. Findings
    - Vulnerability | Exploitation Steps | Impact | Proof/Screenshot | Mitigation
8. Validation of Previous Phases
    - Are initial findings still valid?
9. Screenshots/Evidence
10. Summary of Recommendations
11. Conclusion
12. Appendix