# Advanced Penetration Testing with Kali Linux

*Unlocking industry-oriented VAPT tactics*

**Ummed Meel**

www.bpbonline.com

Every effort has been made in the preparation of this book to ensure the accuracy of the information presented. However, the information contained in this book is sold without warranty, either express or implied. Neither the author, nor BPB Online or its dealers and distributors, will be held liable for any damages caused or alleged to have been caused directly or indirectly by this book.

BPB Online has endeavored to provide trademark information about all of the companies and products mentioned in this book by the appropriate use of capitals. However, BPB Online cannot guarantee the accuracy of this information.

First published: 2024

Published by BPB Online
WeWork
119 Marylebone Road
London NW1 5PU

**UK | UAE | INDIA | SINGAPORE**

ISBN 978-93-55519-511

www.bpbonline.com

## Dedicated to

*My cherished mother and father*

***Dhanni Devi** and **Ratan Lal Meel***

*&*

*Respected big brother and sister-in-law*

***Vijendra Singh Meel** and **Anita***

# About the Author

**Ummed Meel** is a highly accomplished professional in the field of Cyber Security, boasting over a decade of expertise. He has played pivotal roles in numerous projects, emerging as a leader and a security practitioner. Ummed holds distinguished certifications such as *Certified Information Systems Auditor* (*CISA*), *Certified Ethical Hacker* (*CEH*), and *Certified Computer Hacking and Forensics Investigator* (*CHFI*), along with a *Diploma in Cyber Law* (*DCL*). With a remarkable track record, Ummed has conducted an impressive 150+ training sessions and workshops, honing his skills in cyber security, ethical hacking, intelligence, digital forensics, and cybercrime investigation. He has also excelled in establishing cyber security practices, contributing to multiple organizations. His audience spans state police departments across the country and prestigious organizations including the India Air Force, BSF, CISF, CAG, BPRD, CDTI, and various Ministries.

Ummed has accumulated extensive expertise, spanning both hands-on and managerial positions in various domains, such as Red Teaming, Vulnerability Assessment, Penetration Testing, Cyber Security Audits, Compliance, Gap Assessment, and Cyber Advisory. His vast experience extends across a multitude of sectors, encompassing telecommunications, manufacturing, logistics, hospitality, banking, fintech, power supply, stock exchange, aviation, and more.

Additionally, Ummed has made significant contributions by publishing articles in renowned global magazines and journals. He has shared his expert insights through interviews with numerous news channels and newspapers, shedding light on cyber-related solutions. Moreover, he has imparted knowledge through over a hundred seminars and lectures, actively raising awareness about cybercrime in educational institutions. His remarkable involvement extends to aiding investigating agencies in successfully resolving approximately 200 major cybercrime cases within the country. Ummed's academic qualifications include a *B Tech* (*Hons*) degree, *LLB* (*Cyber Law*), and ongoing pursuit of an *M Tech* in *Cyber Security* from BITS Pilani.

# About the Reviewer

**Darryn Brownfield** is a penetration tester and bug bounty hunter with over 10 years of experience in the IT industry. He holds industry-recognized and respected certifications such as the OSCP, PNPT, CRT, and CRTP. He publishes CTF write-ups, bug bounty findings, certification reviews across his social media and YouTube.

# Acknowledgement

I am deeply grateful to my family and friends for their unwavering support in creating this book, especially my parents, Dhanni Devi and Ratan Lal Meel. Heartfelt thanks to my inspiration, elder brother Vijendra Singh Meel, and Sister-in-law Anita, for their continuous encouragement, even during late-night writing. Special thanks to my sister Babita Meel and brother-in-law S.I. Ram Swaroop for their remarkable assistance.

I am thankful to BPB Publications for their guidance in bringing this book to life. Refining this work was a journey with reviewers, technical experts, and editors, each contributing valuably.

With profound gratitude, I extend my appreciation to the mentors, supervisors, colleagues, and fellow professionals in the Information Security sector, whose guidance has significantly enriched my understanding. I am fortunate to have received the blessings of my family members, Ramkaran Meel, Phool Chand Choudhary, and Dr. Sanju Choudhary. Additionally, I wish to express my heartfelt thanks to my younger brother, Brijendra Khyalia, for his invaluable technical advices.

To the trio of kid-mischief extraordinaires—Love, Kush, and Hridyansh—applause for turning my writing space into a lively haven.

Lastly, heartfelt thanks to readers for embracing my book. Your encouragement is priceless.

# Preface

In crafting this book, our intention is to provide readers with a comprehensive guide to the dynamic realm of Vulnerability Assessment and Penetration Testing (VAPT). Our purpose is twofold: to educate and empower. We aspire to equip a diverse readership, spanning from novices to seasoned IT professionals, with the knowledge and practical skills required to navigate the ever-evolving landscape of cybersecurity.

The scope of this book is ambitious yet focused. It delves deep into the intricacies of VAPT, from its foundational principles to advanced techniques. We explore VAPT project planning, governance, and the critical PPT (People, Process, and Technology) framework, offering a holistic understanding of this vital practice. Additionally, we elucidate the significance of pre-engagement strategies and the imperative of choosing appropriate security assessments.

Our hands-on approach guides readers in setting up a VAPT test lab, mastering reconnaissance, VA, and exploring practical network pentesting, web application exploitation, wireless network testing, privilege escalation, bypassing security controls, and report writing. It aims to ignite curiosity, foster skills, and equip readers for cybersecurity, making safeguarding digital assets a shared mission where theory meets practice.

**Chapter 1: Beginning with Advanced Pen Testing –** This chapter introduces readers to advanced penetration testing and its vital role in modern cybersecurity. It covers the core principles of VAPT, emphasizing the People, Process, and Technology (PPT) framework. Pre-engagement techniques for understanding client requirements and choosing appropriate security assessments are also discussed. This chapter sets the stage for a comprehensive exploration of advanced penetration testing techniques and principles in the subsequent chapters.

**Chapter 2: Setting up the VAPT Lab –** This chapter delves into the creation of an advanced VAPT test lab using open-source tools. Discover how to interconnect various computer systems and network devices, simulating real-world scenarios while maintaining security measures. The VAPT lab serves as a crucial environment for skill development, risk-free experimentation, and strategy formulation for cybersecurity professionals, emphasizing its pivotal role in the field.

**Chapter 3: Active and Passive Reconnaissance Tactics –** This chapter delves into the crucial role of reconnaissance tactics in successful penetration testing. Learn how to gather essential information about your target, adapting your approach to various components of a computer system and the unique characteristics of the target organization. Explore the treasure trove of data available on the internet and discover the power of Open Source Intelligence (OSINT) in collecting vital information from public sources, including email addresses, domain names, IP addresses, employee details, hostnames, and DNS records.

**Chapter 4: Vulnerability Assessment and Management –** This chapter delves into the realm of Vulnerability Assessment (VA) and its intricacies. Our primary aim is to empower penetration testers and security experts with invaluable knowledge in both manual and automated VA methodologies. By the chapter's end, you will have a comprehensive understanding of various VA techniques and best practices, enabling you to identify and address vulnerabilities across diverse computer infrastructures. Additionally, we explore the pivotal role of precise and targeted patch management in optimizing the overall effectiveness of VA initiatives.

**Chapter 5: Exploiting Computer Network –** This chapter delves deep into the practical realm of network penetration testing by actively exploiting vulnerabilities discovered in previous sections. Exploitation serves a critical role in assessing the true gravity of vulnerabilities and their potential consequences for the target environment. We emphasize the significance of gathering intelligence about the target environment before choosing a specific attack vector. Using open-source tools and manual scripts within a controlled testing environment, we provide hands-on experience that simulates real-world scenarios. Throughout this chapter, you will gain valuable insights into the operational aspects of exploitation tools, including Metasploit and Armitage.

**Chapter 6: Exploiting Web Application –** This chapter provides a comprehensive introduction to web application exploitation, essential in today's digital landscape. It covers both fundamental and advanced vulnerability exploits, elucidating common attack vectors, threat modeling, and the identification of technical and business logic flows in web applications. By the chapter's end, readers will possess a thorough understanding of advanced web application exploitation techniques and the expertise to conduct sophisticated assessments.

**Chapter 7: Exploiting Wireless Network –** This chapter presents a comprehensive exploration of wireless network pentesting, targeting diverse networks like Wi-Fi and Bluetooth. Its primary focus is on revealing vulnerabilities and potential threats within these networks while establishing effective countermeasures to enhance security.

**Chapter 8: Hash Cracking and Post Exploitation –** This chapter takes you on an engaging journey into privilege escalation and network pivoting. It explores cutting-edge tools and techniques for password and hash cracking, as well as post-exploitation procedures. By the end, you will gain a comprehensive understanding of advanced penetration testing techniques to uncover vulnerabilities and enhance security measures with precision and expertise.

**Chapter 9: Bypass Security Controls –** This chapter delves into the art of bypassing security controls within computer networks, covering Windows security controls, antivirus measures, and firewall protections. It also explores social engineering and miscellaneous penetration testing techniques, offering valuable insights and skills to assess and enhance the efficacy of security controls in computer networks.

**Chapter 10: Revolutionary Approaches to Report Writing –** This chapter delves into the art of report writing, a crucial aspect of the industry. Assessments are incomplete without well-crafted reports that meet required standards. It provides insights through detailed reports, covering technical and logical vulnerabilities, along with recommendations. This chapter also offers guidance on calculating CVSS scores, assessing risk, prioritizing risks, and classifying severity. Additionally, it explores creating impactful presentations and security dashboards to effectively communicate assessment findings.

# Coloured Images

Please follow the link to download the
*Coloured Images* of the book:

## https://rebrand.ly/j6c2hib

We have code bundles from our rich catalogue of books and videos available at **https://github.com/bpbpublications**. Check them out!

# Errata

We take immense pride in our work at BPB Publications and follow best practices to ensure the accuracy of our content to provide with an indulging reading experience to our subscribers. Our readers are our mirrors, and we use their inputs to reflect and improve upon human errors, if any, that may have occurred during the publishing processes involved. To let us maintain the quality and help us reach out to any readers who might be having difficulties due to any unforeseen errors, please write to us at :

**errata@bpbonline.com**

Your support, suggestions and feedbacks are highly appreciated by the BPB Publications' Family.

## Piracy

If you come across any illegal copies of our works in any form on the internet, we would be grateful if you would provide us with the location address or website name. Please contact us at **business@bpbonline.com** with a link to the material.

## If you are interested in becoming an author

If there is a topic that you have expertise in, and you are interested in either writing or contributing to a book, please visit **www.bpbonline.com**. We have worked with thousands of developers and tech professionals, just like you, to help them share their insights with the global tech community. You can make a general application, apply for a specific hot topic that we are recruiting an author for, or submit your own idea.

## Reviews

Please leave a review. Once you have read and used this book, why not leave a review on the site that you purchased it from? Potential readers can then see and use your unbiased opinion to make purchase decisions. We at BPB can understand what you think about our products, and our authors can see your feedback on their book. Thank you!

For more information about BPB, please visit **www.bpbonline.com**.

# Join our book's Discord space

Join the book's Discord Workspace for Latest updates, Offers, Tech happenings around the world, New Release and Sessions with the Authors:

**https://discord.bpbonline.com**

# Table of Contents

1. **Beginning with Advanced Pen Testing ..... 1**

Introduction ..... 1

Structure ..... 2

Objectives ..... 2

Fundamentals of VAPT ..... 3

*Vulnerability Assessment ..... 3*

*Penetration Testing ..... 4*

Advanced penetration testing techniques and strategies ..... 4

Business and compliance requirements for VAPT ..... 6

Industrial approach and methodology in VAPT ..... 7

*Goals and objectives ..... 7*

*Kickoff call ..... 8*

*Intelligence gathering ..... 8*

*Passive intelligence ..... 8*

*Active intelligence ..... 9*

*Threat modeling ..... 9*

*Vulnerability assessment ..... 9*

*Automated VA scan ..... 10*

*Manual VA scan ..... 10*

*Penetration testing ..... 10*

*Post exploitation ..... 10*

*Reporting ..... 11*

*Security posture: Executive summary ..... 11*

*Detailed technical report ..... 11*

*Vulnerability management tracker ..... 12*

Security audit standards and frameworks: Best practices ..... 12

*Open web application security project standard ..... 12*

*CWE/SANS Top 25 ..... 12*

*Penetration Testing Execution Standard ..... 13*

*Open-source security testing methodology manual ..... 13*

*NIST Cybersecurity Framework ..... 14*

*ISO 27001 standards ..... 14*

*CIS benchmarks*......15

*ISACA standards and guidelines*......15

*MITRE framework*......16

Pre-engagement interaction with customers......16

*Define audit scope*......16

*Exercise nature*......17

*Testing method*......17

*Black box*......17

*Grey box*......18

*White box*......18

*Environment selection*......18

*Approach and methodology selection*......18

*Exercise time selection*......18

*Project timeline*......19

*Rules of engagement*......19

*Deliverables*......19

Designing the Scope of Work for security audits......19

Project planning and governance in VAPT......20

*Project planning*......20

*Project management*......21

*Project governance*......23

Delivery and customer success tactics in VAPT......23

Conclusion......24

References......24

**2. Setting up the VAPT Lab......27**

Introduction......27

Structure......28

Initiating with Kali Linux......28

*Kali Linux features*......28

Establishing the virtualization landscape......30

*How is it useful in VAPT*......30

Deploying Kali Linux 2023.2......30

*Installing Kali Linux on VMware workstation*......31

*Installing Kali Linux on VirtualBox*......35

Arranging network services....................37

Enabling ProxyChains....................39

*Use cases of ProxyChains*....................*41*

Personalizing Kali Linux....................41

*Changing the desktop environment*....................*41*

*Installing additional applications*....................*42*

*Modifying system settings*....................*42*

*Changing the login screen*....................*43*

Refreshing Kali Linux....................44

Enabling third-party VAPT tools....................45

*MobSF framework*....................*46*

*Trivy*....................*51*

Setting up vulnerable machines and applications....................52

*Setting up Metasploitable 2*....................*52*

*Setting Up BWAPP*....................*54*

Conclusion....................57

**3. Active and Passive Reconnaissance Tactics....................59**

Introduction....................59

Structure....................60

What is reconnaissance....................60

Why is reconnaissance so important....................61

Types of reconnaissance....................61

*Passive reconnaissance*....................*62*

*Active reconnaissance*....................*62*

Passive reconnaissance tools and tactics....................62

*WHOIS*....................*63*

*DNS reconnaissance*....................*65*

*IP reconnaissance*....................*68*

*Shodan*....................*70*

*Route mapping*....................*72*

*Email address*....................*74*

*Name and number*....................*75*

*Password or breach data dump*....................*75*

Active reconnaissance tools and tactics....76

*Host discovery*....76

*Port scanning*....79

*Port scanning techniques*....79

*Running services and version detection*....81

*OS fingerprinting*....82

*Directory enumeration*....83

*Hard-coded information*....84

Additional resources for reconnaissance....85

*Maltego*....85

*SPARTA*....88

Conclusion....91

**4. Vulnerability Assessment and Management....93**

Introduction....93

Structure....93

Overview of vulnerability assessment....94

Vulnerability nomenclature....96

Vulnerability management life cycle....96

Vulnerability assessment....97

*Web application*....97

*OWASP ZAP*....98

*Burp suite*....100

*Computer network*....104

*Nessus*....104

*Legion*....109

*NMAP*....111

*Mobile application*....115

*MobSF*....116

*Container*....120

*Trivy*....120

Vulnerability management....124

Application security....126

Conclusion....126

**5. Exploiting Computer Network....129**
Introduction....129
Structure....130
Objectives....130
Understanding network pen testing....130
Introduction to Metasploit....131
Metasploit database and workspace management....132
Integrating NMAP scans with Metasploit....135
Metasploit automation....138
Starting with auxiliary and exploits....140
*Auxiliary modules....140*
*Exploit modules....141*
*Post-exploitation modules....141*
Manual exploitation....146
Exploitation using Armitage....147
*Setting up Armitage....148*
Conclusion....153

**6. Exploiting Web Application....155**
Introduction....155
Structure....156
Objectives....156
What is web application pen testing....156
*Web application pen testing approach....157*
*Web application pen testing attack vectors....158*
*OWASP top 10 for web application....158*
Web application pen testing threat modeling....159
Web application pen testing mind map....160
Detecting web app firewalls and load balancers....162
Exploiting application-specific vulnerabilities....163
*SQL injection....164*
*PHP code execution....169*
*Brute force at login....171*
*Broken authentication....174*
*Insecure Direct Object Reference....177*

*XSS using XSS validator*......179
*Backdoor via unrestricted file upload*......184
*HTTP parameter pollution*......187
Business logic flaws......189
Conclusion......194

**7. Exploiting Wireless Network......195**
Introduction......195
Structure......195
Objectives......196
Introduction to wireless pentesting......196
Wireless network fundamentals......197
*Wireless networks and protocols overview*......197
*Wireless network topologies and architectures*......197
*Radio Frequency fundamentals*......198
Wireless security threats and standards......198
*Common wireless security threats*......198
*Wireless security overview*......198
Wireless pen testing methodology......198
*Steps involved in wireless pentesting*......199
*Approach to wireless pentesting*......199
Wireless pen testing tools......200
*Overview of wireless pen testing tools*......201
*Common wireless pen testing tools*......201
Configuring Kali Linux for wireless pentesting......202
*Configuring Kali Linux for wireless attacks*......203
Wireless network exploitation techniques......207
*Compromising WPA/WPA2 encryption*......208
*Man-in-the-middle attacks with rogue access points*......211
*Bypassing hidden SSIDs*......212
*Bypassing MAC and open authentication*......214
*Denial-of-service attacks*......216
Advanced wireless attacks......218
*Attacking wireless routers with Reaver*......218
Conclusion......219

**8. Hash Cracking and Post Exploitation ...221**

Introduction...221

Structure...221

Objectives...222

Exploring hash functions...222

*Purpose and properties of modern hash functions ...223*

*Unveiling common hash algorithms ...223*

Mastering password hashing...224

*Art of securing passwords...224*

*Cutting-edge techniques - Salting and key stretching...225*

Unleashing hash cracking techniques ...226

*Strategic approaches...226*

Empowering hash cracking arsenal...227

*Elite tools for hash warriors ...227*

*Hash-identifier ...227*

*John the Ripper ...228*

*John the Ripper Jumbo...230*

*Hashcat ...230*

*Online tools for hash warriors ...232*

*CrackStation ...232*

*Hashes...233*

Difference between hashing, encryption and encoding...235

Post exploitation and lateral movement...235

*Understanding post exploitation ...236*

*Significance of lateral movement ...236*

Privilege escalation techniques...236

*Privilege escalation on Linux...236*

*Phase 1: Initial access ...237*

*Phase 2: Preparing for privilege escalation using a Udev exploit ...237*

*Phase 3: Escalating privileges...239*

*Privilege escalation on Windows ...241*

*Phase 1: Initial access ...242*

*Phase 2: Preparing for privilege escalation using bypass UAC ...244*

*Phase 3: Escalating privileges...245*

Exploring network pivoting...246

*Pivoting approach* ....................247
*Phase 1: Gain (initial) access to Windows 7* ....................247
*Phase 2: Network info gathering and pivot connection establishment* ....................248
*Phase 3: Network pivoting by exploiting Metasploitable 2 machine* ....................250
Persistence and lateral movement ....................251
*Strategies for persistent access and lateral movement* ....................252
*Persistence through hashdump techniques* ....................253
*Exploring RDP for lateral movement* ....................254
Unleashing the power of Mimikatz in meterpreter ....................256
Conclusion ....................259

**9. Bypass Security Controls ....................261**
Introduction ....................261
Structure ....................261
Objectives ....................262
Significance of bypassing security controls ....................262
Advancements in security controls ....................263
*Cutting-edge technologies* ....................263
*Intelligent systems* ....................264
*Evolving threat landscape* ....................264
*Cloud specific security controls* ....................264
Security control bypass in network recon ....................265
*Source port manipulation* ....................265
*IP address spoofing / decoy IP* ....................266
*Packet fragmentation* ....................266
*Spoofing MAC address* ....................267
*Custom packet creation* ....................267
*Nmap Scripting Engine scripts* ....................269
Outsmarting Windows Defender ....................270
Antivirus evasion techniques and tools ....................277
*Antivirus evasion techniques* ....................278
*Antivirus evasion tools* ....................278
*Harnessing Metasploit templates and custom binaries for antivirus evasion* ....................279
*Shellter* ....................290
*Unicorn* ....................294

*Phantom-Evasion*......296
*Invoke-Stealth*......299
Cutting-edge WAF evasion tactics......302
Evolving social engineering tactics......306
*Phishing simulation*......308
*Phishing approach and methodology*......308
*Gophish*......310
Conclusion......316

**10. Revolutionary Approaches to Report Writing......317**
Introduction......317
Structure......317
Objectives......318
Overview of report writing......318
*Importance of report writing in cybersecurity*......318
*Integrating reports in comprehensive assessments*......319
Components of well-crafted reports......319
*Vulnerability Assessment report*......332
*Penetration Testing report*......332
Risk assessment and prioritization......333
*Quantifying risks for effective assessment*......333
Utilizing CVSS scores......334
*Factors influencing CVSS scores*......335
*Interpreting and applying CVSS scores appropriately*......336
Types of cybersecurity assessment reports......339
*Executive summary report*......339
*Detailed technical assessment report*......340
*Vulnerability management tracker*......340
Examples of detailed reports......340
*Web application VAPT report writing example*......341
*Network VAPT report writing example*......343
Automated vulnerability management with DefectDojo......347
Conclusion......350

**Index......353-363**

# Chapter 1
# Beginning with Advanced Pen Testing

## Introduction

**Penetration Testing** (**PT**) is a legally authorized practice that aims to identify technical and logical flaws within computer systems, as well as to evaluate an organization's security controls, monitoring capabilities, and incident response procedures. As technology continues to advance, the complexity of attack surfaces increases, making **Vulnerability Assessment and Penetration Testing** (**VAPT**) a crucial and well-established method for mitigating potential threats. By providing insight into an organization's security posture and accurate remediation solutions, VAPT can safeguard businesses from data breaches and unauthorized access.

Today, adopting zero trust policies has become a crucial component of organizational security, and VAPT is no exception. It plays an important role in ensuring proper validation of inputs received from applications and devices.

This chapter covers the fundamental principles of VAPT project planning, management, and governance. It also delves into the **People, Process, and Technology** (**PPT**) framework, which helps to clarify the role of individuals, processes, and technology in VAPT practice. The chapter further explores VAPT methodology and approach in detail, equipping Pen testers with an industry-oriented understanding of the practice. With this understanding and an agile approach, Pen testers can execute enterprise-level testing practices smoothly and efficiently.

Before beginning a project, pre-engagement techniques can help auditing organizations to clearly understand the scope and requirements of their clients and accordingly, enlist the necessary toolsets, manpower, and deliverables. Additionally, to choose the most appropriate security assessments for your organization, you must be well-versed in the cybersecurity offerings available in the market and understand the differences between them.

> Note: Regular vulnerability assessments and penetration testing are essential exercises for identifying, prioritizing, reporting, and remediating weak security practices, threats, and vulnerabilities in your computer infrastructure. By performing these exercises on a regular basis, organizations can proactively mitigate potential threats and safeguard their systems against malicious attacks.

# Structure

In this chapter, we will discuss the following topics:

- Fundamentals of VAPT
- Advanced penetration testing techniques and strategies
- Business and compliance requirements for VAPT
- Industrial approach and methodology in VAPT
- Security audit standards and frameworks: Best practices
- Pre-engagement interaction with customers
- Designing the Scope of Work for security audits
- Project planning and governance in VAPT
- Delivery and customer success tactics in VAPT

# Objectives

The primary aim of this chapter is to provide cyber security professionals and organizations with an in-depth understanding of advanced VAPT approaches and methods. By reading this chapter, you will learn not only about the VAPT approach but also about its standards, frameworks, scope designing, customer engagement, project management, governance, and customer success strategies.

Advanced VAPT approaches and methods can effectively identify and prioritize vulnerabilities based on their severity, enabling organizations to focus their efforts on addressing the most critical vulnerabilities. This approach can enhance the overall efficiency of the VAPT process and lead to more successful outcomes. This chapter is also beneficial for individuals and organizations seeking to understand why they need VAPT services, as well as which services would be most beneficial to their business based on relevant regulatory or industry standards.

# Fundamentals of VAPT

**Vulnerability Assessment and Penetration Testing** (**VAPT**) is a methodical and risk-based approach for identifying security vulnerabilities within computer infrastructure. VAPT audits utilize a combination of automated tools and manual efforts to detect all potential vulnerabilities that malicious actors may exploit.

The vulnerability life cycle refers to a vulnerability's stages, from its discovery to its resolution. *Figure 1.1* provides a visual representation of this process:

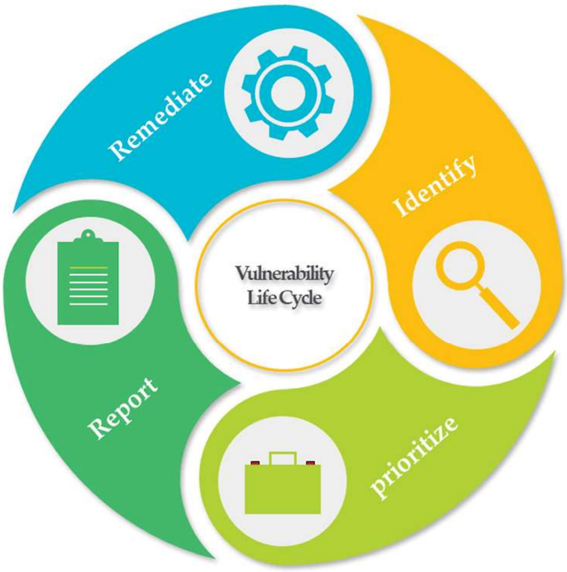

***Figure 1.1**: Vulnerability Life Cycle*

# Vulnerability Assessment

**Vulnerability Assessment** (**VA**) can only detect weaknesses in the targeted system. However, it cannot differentiate between findings that have the potential to be exploited and cause damage to the system.

## Penetration Testing

**Penetration Testing** (**PT**) is a sequential exercise that builds on vulnerability assessment results. In this process, the pen tester identifies vulnerabilities and exploits them to gain access and exfiltrate data. Additionally, penetration testing evaluates the system through the access gained after exploitation to determine the sensitivity of the accessible data.

For example, if banner grabbing identifies an outdated version of a service and the pen tester has included all relevant CVEs/CWEs in their report, that would be classified as a vulnerability assessment. However, if the pen tester is able to gain access to the server or obtain a desired response through the use of an exploit, then this would fall under the category of Penetration Testing.

> Note: A pen tester should not be content with identifying only the obvious vulnerabilities and then stop working. Given the ever-increasing complexity of attack surfaces, a great deal of effort is required to thoroughly test and secure systems against potential threats.

## Advanced penetration testing techniques and strategies

A decade ago, when organizations did not prioritize cyber security, basic technical knowledge was enough to conduct a vulnerability assessment scan using automated tools. However, this approach can now only identify known and technical vulnerabilities. As technology and VAPT methodology have evolved, modernization is crucial. For instance, the attack payload must be advanced and **Fully Undetectable** (**FUD**) to bypass security controls effectively. It is essential to have objective-oriented testing approaches that define why a network firewall or web application firewall needs to be bypassed during the audit. Advanced VAPT approaches use more sophisticated tools and techniques to detect and exploit vulnerabilities, offering numerous benefits, as shown in *Figure 1.2*.

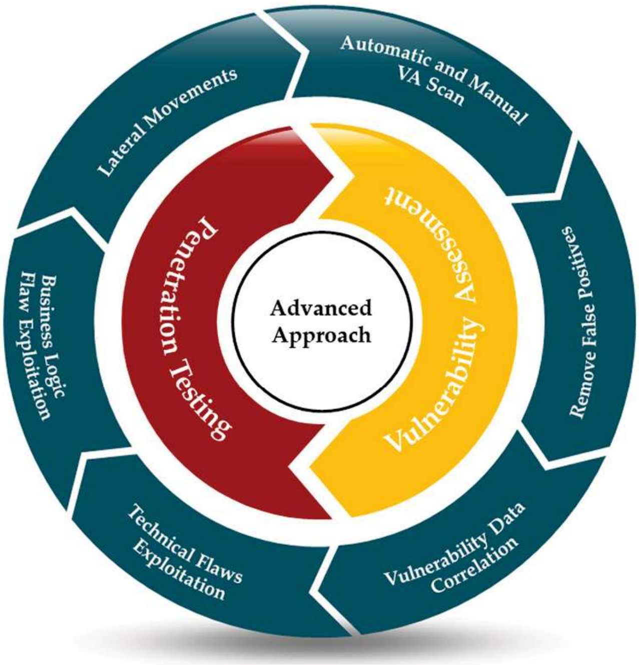
Advanced Approach
Penetration Testing
Vulnerability Assessment
Automatic and Manual VA Scan
Remove False Positives
Vulnerability Data Correlation
Technical Flaws Exploitation
Business Logic Flaw Exploitation
Lateral Movements

***Figure 1.2:*** *Advanced approach for VAPT*

To ensure timely and comprehensive detection of all vulnerabilities, your risk-based approach must be both agile and advanced. Advanced penetration testing can help you not only detect vulnerabilities but also identify the most effective security controls for your computer infrastructure. Pen testers must possess a comprehensive understanding and skill set to accurately audit key sensitive areas of the business.

The traditional VAPT phase of asset discovery, which was once considered the most essential, has evolved into attack surface management. This is a well-planned approach to continuously discovering, inventorying, tagging, and monitoring the status of IT assets in an organization's infrastructure. The attack surface is constantly changing and is a critical consideration for organizations of all sizes. By implementing effective attack surface management practices, both system owners and CISOs can gain visibility into their organization's IT infrastructure.

> Note: In some cases, vulnerabilities in a system's business logic flow can result in a greater impact than technical vulnerabilities, as these types of vulnerabilities may require less technical expertise and a smaller toolset to exploit.