Techonquer

Techonquer Certified Advanced Penetration Tester (TAPT) with AI

Master the Art of Ethical Hacking and Penetration Testing

Learn More

Introduction to TAPT

Who Should Take This Course?

This intensive program is designed for cybersecurity professionals, aspiring penetration testers, and anyone seeking advanced skills in ethical hacking and penetration testing. This course equips you with the knowledge and practical experience needed to conduct comprehensive penetration tests, uncover vulnerabilities, and safeguard sensitive information.

Course Syllabus

The TAPT curriculum covers a wide range of topics, from foundational concepts to advanced techniques. We explore various attack vectors, including code execution, network exploitation, and privilege escalation. You'll learn how to identify and exploit vulnerabilities across different platforms and environments, including Windows, Linux, and web applications.

Crafting Powerful Exploits

1 Code Execution Flow

Understanding how code executes in different environments, including Windows and Linux, is crucial for creating effective exploits. You'll learn how to manipulate code flow to achieve remote code execution and gain control over vulnerable systems.

2 VBA Code and MSHTA Exploit Development

Explore the world of VBA code and MSHTA, leveraging these technologies to develop sophisticated exploits that bypass security controls and achieve malicious goals. Gain practical experience in crafting exploits that exploit vulnerabilities in these widely used applications.

3 PowerShell & Macros

Uncover the power of PowerShell and Macros for developing robust and evasive exploits. Learn techniques to craft custom payloads, bypass security mechanisms, and execute commands within the target environment.

4 regsvr32 Execution and AMSI Evasion

Master the art of using regsvr32 for code execution and explore advanced techniques to evade Anti-Malware Scan Interface (AMSI), a security mechanism that often prevents malicious code execution. Gain hands-on experience with real-world scenarios.

Open Server Exploitation

- Taking Initial Recon for Web
- Understanding OWASP Top 10
- Breaking Intigrity File Upload Vulnerability
- No need for Port Forwarding..? (Advance File Upload Exploit)
- Understanding Code Flow to Gain RCE
- Injecting Code Flow to gain RCE via SQLi(SQLi to RCE)
- Stealing Cookie vai SQL Injection
- Fetching Internal Server File Using SQLi (SQLi to LFI)

Open Server Exploitation

Breaking Authorisation/Authentication (Broken Authentication)

- Gaining Admin Session (XSS Session hijacking)
- Exposing Internal File - (LFI/RFI)
- Greping Session via LFI
- Decoding JWT to gain admin
- Are you in XXEi ? (XXE Inection to RCE)
- We got the Admin... hehe IDOR(Insecure Direct Object Refrence)
- again 401.. Got it..!(Verb Tempering)

Initial Recon: Network Compromise

SMB Exploitation

Learn to exploit vulnerabilities in the Server Message Block (SMB) protocol, often used for file sharing and network communication. Master techniques to gain unauthorized access to shared resources and potentially compromise the entire network.

SNMP Exploitation

Discover the power of Simple Network Management Protocol (SNMP) for network exploration. Understand how to extract sensitive information, manipulate network devices, and even launch denial-of-service attacks.

FTP Exploitation

Explore vulnerabilities in File Transfer Protocol (FTP) servers, enabling you to gain unauthorized access to sensitive files, upload malicious content, and potentially compromise the entire network.

MySQL Exploitation

Delve into the world of MySQL databases and learn how to exploit vulnerabilities in these critical systems. Discover techniques to gain unauthorized access, manipulate data, and potentially gain control over the entire database.

Local Internal Enumeration

PowerShell Enumeration

Leverage the power of PowerShell for in-depth enumeration of a compromised system. Gain mastery in utilizing native commands and scripts to gather information about user accounts, installed software, system configuration, and network connections.

Command Prompt Techniques

Learn to utilize the command prompt effectively for gathering information. Discover advanced techniques for analyzing system logs, identifying running processes, and extracting sensitive data.

Running Enumeration Scripts

Explore and implement various enumeration scripts designed to automate the process of gathering information. Understand how to modify and adapt these scripts to your specific needs and objectives.

Gaining Admin Access: Privilege Escalation

Windows Privilege Escalation

Registry Attacks(3 methods)

- **Impersonation Attacks(2 Methods)**
- **Kernal Exploit**

Linux Privilege Escalation

- **Kernal Exploit**
- **Crontab**
- **SUID/GUID Binaries**
- **Docker Exploit**
- **NFS Exploit**
- **Capabilities Exploit**

Persist YourSelf inside System(windows)

Logon Scripts

Learn how to manipulate logon scripts, which execute automatically when a user logs in, to maintain persistent access to a compromised system. Explore methods to inject malicious code and establish a backdoor.

1

2

DLL Sideloading

Discover the technique of DLL sideloading, where attackers can exploit vulnerabilities in the way applications load dynamic link libraries (DLLs) to gain persistent access and execute malicious code.

3

Login Screen Backdooring

Explore techniques to manipulate the login screen, either by modifying existing components or injecting malicious code, allowing attackers to intercept login credentials and gain unauthorized access.

Persist YourSelf inside System(windows)

Persist YourSelf inside System(linux)

- SubheCrontab
- Shell rc poisoning
- User addition
- Custom service development
- APT Poisoningading

Credential Dumping

- Fake Service Impersonation
- Mimikatz In-Memory Elfiltration
- Registry Crawiling
- SSP
- Hunting LSA/LSASS.exe
- CredsPhish Locally
- Browser Dumping

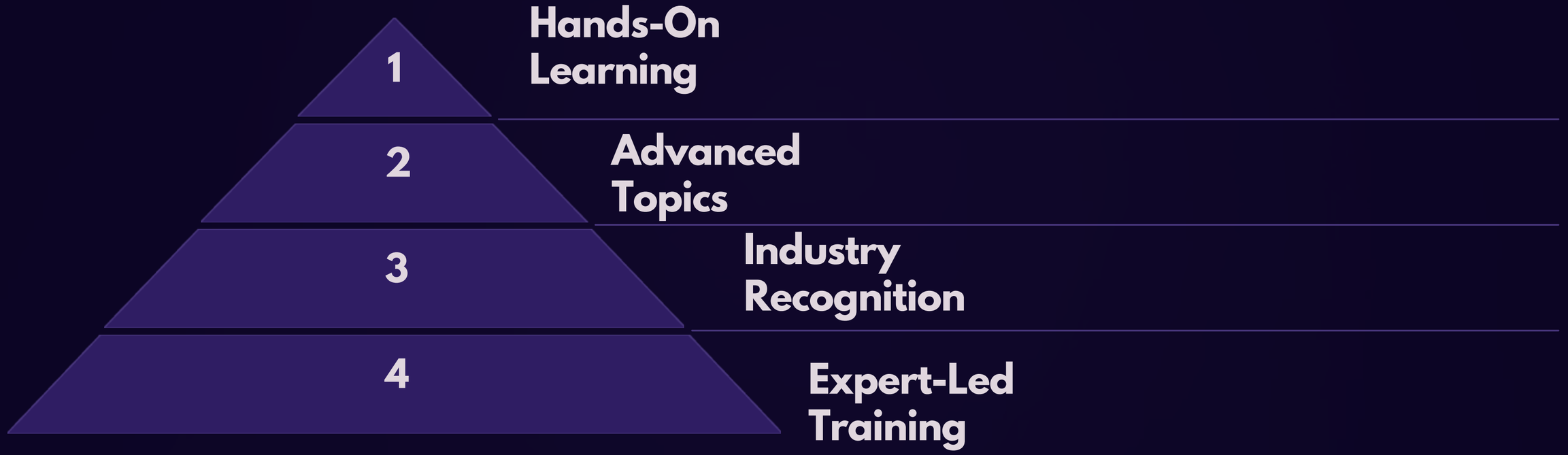
Lateral Movement

- RDP Hijacking using Task Manager
- RDP Hijacking using Tscon
- PsExec SMB RCE
- exe SMB RCE
- SSH Port Forwarding
- New-PSSession Powershell
- Evil-Winrm
- Lateral Movement through WMI

Eradicating Footprints

- Logs Correction
- Erasing EventViewer
- Webtutil Clearing
- Registry Resetting

Why TAPT Stands Out



Contact Techonquer

1

Email

team@techonquer.org

2

Phone

6367098233

3

Website

https://techonquer.org/blackhat

4

Join Now

Don't miss this opportunity to become a certified advanced penetration tester!