

**Advanced Penetration Testing (APT) — Course Content**

**Module 1 – Introduction to Advanced Pentesting**

* How advanced pentesting differs from standard pentests
* Red teaming vs. penetration testing vs. vulnerability assessment
* Rules of engagement and operational security (OPSEC)

**Module 2 – Advanced Reconnaissance & OSINT**

* Deep OSINT collection (subdomain takeovers, metadata harvesting)
* Advanced DNS enumeration & pivoting through recon data
* Automating recon with custom scripts and frameworks

**Module 3 – Advanced Network Mapping & Enumeration**

* Layer 2 & Layer 3 network mapping techniques
* Enumerating segmented networks
* SNMP, LDAP, and custom protocol enumeration

**Module 4 – Bypassing Perimeter Defenses**

* Advanced firewall & IDS/IPS evasion
* Covert channels and tunneling (DNS, ICMP, HTTPS)
* Proxy chaining and traffic obfuscation

**Module 5 – Exploiting Internal Networks**

* Post-perimeter network pivoting
* VLAN hopping and rogue DHCP servers
* Advanced ARP spoofing and MITM attacks

**Module 6 – Web Application Advanced Exploitation**

* Chaining multiple web vulnerabilities
* Server-side request forgery (SSRF) to cloud exploitation
* Deserialization RCE and sandbox escapes

**Module 7 – Active Directory Advanced Attacks**

* Kerberos attacks (Silver Ticket, Golden Ticket, AS-REP Roasting)
* Delegation abuse and DCSync attacks
* Domain trust abuse and cross-forest exploitation

**Module 8 – Advanced Wireless Attacks**

* WPA3 exploitation & downgrade attacks
* Rogue AP with captive portal credential harvesting
* Wireless client attacks and exploitation

**Module 9 – Advanced Exploitation & Shellcode**

* Custom exploit creation for unpatched vulnerabilities
* Advanced buffer overflow and heap exploitation
* Shellcode encoding and AV/EDR evasion

**Module 10 – Lateral Movement Techniques**

* Pass-the-Hash, Pass-the-Ticket, and Overpass-the-Hash
* WMI, WinRM, and PSRemoting abuse
* Using compromised accounts for privilege escalation

**Module 11 – Cloud & Hybrid Environment Attacks**

* Pivoting between on-premises and cloud environments
* Exploiting misconfigured cloud IAM roles
* Persistence in cloud infrastructure

**Module 12 – Persistence Mechanisms**

* Fileless persistence
* DLL search order hijacking
* Scheduled tasks and service abuse

**Module 13 – Evasion & Anti-Forensics**

* Bypassing AV/EDR/XDR with custom loaders
* Timestomping and log tampering
* Living-off-the-land (LOTL) techniques

**Module 14 – Attacking Enterprise Applications**

* Exploiting ERP and CRM systems
* Attacks on Microsoft Exchange & SharePoint
* Exploiting middleware and message queues

**Module 15 – Physical Penetration Testing**

* Bypassing physical locks and access controls
* Rogue device attacks (Rubber Ducky, Bash Bunny)
* Social engineering with physical access

**Module 16 – Advanced Social Engineering**

* Multi-stage phishing campaigns
* Spear phishing with malicious documents
* Voice phishing (vishing) and deepfake-based attacks

**Module 17 – Red Team Operations**

* Planning & executing red team campaigns
* Blending in with normal user activity
* Long-term engagement OPSEC

**Module 18 – Purple Teaming**

* Working with defenders to improve detection
* Using MITRE ATT&CK for defense validation
* Joint red-blue exercises

**Module 19 – Advanced Reporting & Executive Briefings**

* Writing reports for high-stakes stakeholders
* Mapping findings to business risk
* Communicating without revealing operational tradecraft

**Module 20 – Final APT Simulation**

* End-to-end adversary simulation in a live enterprise lab
* Multi-vector attack scenario (network, cloud, social engineering)
* Final report & stakeholder presentation