🛡️ Module 1: Introduction Module

1. Red Team Engagements
2. Red Team Threat Intelligence
3. Red Team OPSEC (Operations Security)
4. Intro to Command and Control (C2)

🧠 Module 2: Initial Access – Gaining Entry Like a Real Adversary

1. Intro to Initial Access
2. Social Engineering 101
3. Macro-Based Documents Attack
4. Other File-Based Payload Vectors
5. Antivirus Bypass Techniques

🌐 Module 3: Web-Based Initial Access – Breaching Through the Front Door(Real Life Target)

1. Web Entry Points in Enterprise Environments
2. Common Web-Based Initial Access Techniques
3. Real World SQLi Exploitation & WAF Bypass
4. XSS Exploitation and Account takeover
5. LFI/RFI Exploitation to Internal Network
6. Broken Access Control Life Exploitation
7. Broken Authentication & Session Management
8. Wordpress Exploitation
9. Drupal Exploitation
10. Jenkins Exploitation
11. File Upload Exploitation
12. JWT Exploitation to ATO

🔥 Module 4: Post-Compromise Attack – Owning the System Silently

1. Living Off The Land (LotL)
2. Local Enumeration (Recon After Compromise)
3. Privilege Escalation
4. Persistence
5. Credential Dumping
6. Lateral Movement & Pivoting
7. Data Exfiltration

🏰 Module 5: Active Directory Attacks – Owning the Enterprise

1. AD Enumeration (Internal / External)
2. Initial Access
3. Local Privilege Escalation
4. Domain Privilege Escalation
5. Lateral Movement
5. Lateral Movement
6. Domain Dominance
7. Persistence in AD
8. Credential Harvesting (Domain-Wide)

Module 6: In-Memory Antivirus Evasion

1. AMSI Bypass
2. EWT Bypass
3. ScriptBlock Loggin bypass
4. ShellCode Development

5. ShellCode Injection