

Special Modules

1. Basic
 - 1.1. Linux Basic
 - 1.2. Bash Scripting
 - 1.3. Python Basic
 - 1.4. Working with powershell
 - 1.5. Note Taking
2. Information Gathering
 - 2.1. Passive
 - 2.1.1. Google Hacking
 - 2.1.2. Recon-ng
 - 2.1.3. Spiderfoot
 - 2.1.4. SSL Testing
 - 2.1.5. Pastebin, Archive, Job posting, LinkedIn
 - 2.1.6. Email Information
 - 2.1.7. OSINT Framework
 - 2.2. Active Information Gathering
 - 2.2.1. Forward & Reverse enumeration
 - 2.2.2. Zone Transfer
 - 2.2.3. Finding hidden directories/files
 - 2.2.4. Port scanning
 - 2.2.5. SMTP Enumeration
 - 2.2.6. Network file system enumeration
 - 2.3. Working other information gathering tools & technique
 - 2.4. Building an attack plan
3. Vulnerability Scanning
 - 3.1. Various scanning methods
 - 3.2. Manual Scanning
 - 3.3. Scanning using nessus
4. Web Application Testing
 - 4.1. Enumeration
 - 4.2. Tools
 - 4.2.1. Gobuster
 - 4.2.2. Nikto
 - 4.2.3. Burp suite Pro
 - 4.2.4. Exploit Web Vulnerabilities
 - 4.2.4.1. XSS
 - 4.2.4.2. SQLi
 - 4.2.4.3. RCE
 - 4.2.4.4. XXE
 - 4.2.4.5. SSTI
 - 4.2.5. Hacking Wordpress

5. Red Teaming
 - 5.1. Open-source C2 Framework
 - 5.1.1. Meterpreter
 - 5.1.2. Poshc2
 - 5.1.3. Silver
 - 5.2. HTA based Payload
 - 5.3. Microsoft Office Payload
 - 5.4. Password Cracking
 - 5.5. Privilege Escalation
 - 5.6. Tunneling
 - 5.7. Active Directory
 - 5.7.1. Enumerate Using PowerView
 - 5.7.2. Enumerate using Bloodhound
 - 5.7.3. Exploiting ACL and ACE
 - 5.7.4. Pass the hash
 - 5.7.5. Golden tickets
6. Windows Buffer Overflow
 - 6.1. Stack Overflow
 - 6.2. SEH Based Overflow
 - 6.3. EGG Hunting
7. Writing Report
8. Bonus
 - 8.1. How to improve
 - 8.2. What next?