

- Lab Setup and Installing VMs:
 - Virtualization
 - Installing Kali Linux
 - Installing Metasploitable2
 - Installing Metasploitable3
 - penetration testing methodologies
 - OSI Model
- Information Gathering:
 - Passive information gathering
 - OSINT
 - Anonymizing your traffic
 - WHOIS
 - Hunter.io
 - Recon-ng
 - The-Harvester
 - Instaloader
 - Sherlock
 - Shodan.io
 - Censys
 - Maltego
 - NetCraft
 - Active information gathering
 - Google Hacking (dorks)
 - Google Hacking Database (GHDB)
 - Metagoofil
 - DNS Pen-testing

- DNS Enumeration
 - DNS Zone Transfer Attack
- DNS Attacks
 - DNS Tunneling
 - DNS Amplification
 - DNS Flood Attack
 - DNS Spoofing
- SpiderFoot
- Subdomains Enumeration
 - DNSmap
 - Amass
- EyeWitness
- Active scanning techniques
 - Spoofing mac address
- Discovering Live hosts
- Probing open service ports
- Scanning:
 - Port scanning Basics
 - Scanning Tools
 - Nmap
 - Hping2, Hping3
 - Host Discovery
 - ARP ping scan and UDP ping scan
 - ICMP Ping Scan
 - TCP Ping Scan
 - Port and Service Discovery
 - TCP Connect/Full Open Scan
 - Stealth Scan
 - Invert TCP Flag Scan

- Xmas Scan
 - IDLE/IPID Header scan
 - UDP Scanning
 - SCTP INIT Scanning
 - IPV6 Scanning
 - Service Version Discovery
 - Time Reduction Techniques
- Port scanning countermeasures
- OS Discovery
 - Wireshark
 - Nmap
- Firewalls, IDS, WAF
 - Scanning beyond IDS and Firewall
 - Software and Hardware Firewall
- Enumeration:
 - NetBIOS Enumeration
 - nmap
 - SNMP enumeration
 - Snmpcheck
 - FTP enumeration
 - Banner Grabbing
 - Nmap NSE
 - SSH enumeration
 - Banner Grabbing
 - SSH-audit
 - SSH-Keyscan
 - Nmap NSE

- SMB enumeration
 - Smbmap
 - EnumLinux4
 - NSE
- MYSQL Enumeration
 - Nmap NSE
- RDP Enumeration
 - Nmap NSE
- Vulnerability Assessment:
 - Nessus
 - Scanning with Nessus
 - Analyzing Nessus results
 - Vulnerability discovery using Nmap
 - Greenbone Vulnerability manager
 - Web application scanners
 - Whatweb
 - Nmap
 - Nikto
 - WPScan
- System Hacking:
 - Password Cracking
 - Active Online attacks
 - Creating Our Wordlist
 - Crunch
 - Cewl
 - CUPP
 - THC Hydra
 - Ncrack

- Medusa
- Passive Online attacks
- Offline Attacks
 - John The Ripper
 - Hashcat
- Vulnerability Exploitation
 - Exploit-DB
 - Metasploit
 - MSFConsole
 - Hacking Metasploitable2
 - Hacking Metasploitable3
 - Buffer Overflow
 - Buffer Overflow Exploitation
 - Introducing to Immunity Debugger
 - Overflowing the Buffer
 - Windows Buffer Overflows
 - Discovering the Vulnerability
 - Win32 Buffer Overflow Exploitation
- Creating Malware
 - Netcat
 - Socat
 - PowerShell and Powercat
 - Creating Custom Malware
 - Meterpreter vs Shell
- Antivirus Bypass Technique
 - Bypass the Dynamic Engine
 - Shellter
 - Bypass the Static Engine
 - YARA

- Crypter
 - Pyminifier
 - Other Antivirus Bypass Techniques
 - PowerSploit
 - Invoke-Obfuscation
- Privilege Escalation Techniques
 - Windows enumeration
 - Linux enumeration
 - Windows Kernel Exploits
 - Windows Password Mining
 - Mimikatz
 - Exploiting Services
 - DLL Hijacking
 - Windows Registry
 - PowerUp
 - Linux Kernel Exploits
 - Privilege Escalation using sudo version
 - Privilege Escalation using SUID
 - Privilege Escalation using Cron Jobs
 - Privilege Escalation using PATH
 - Process memory
- Maintaining access
- Covering tracks
- Sniffing and Spoofing:
 - Network Protocols
 - File protocols
 - Remote access protocols
 - Email protocols

- HTTP and HTTPS
- SQL database protocols
- LDAP
- SIP
- Network Protocol types
- Network Services
- Decoding TCP
- Decoding UDP
- DHCP
- ARP
- Decode HTTP
- Analyzing FTP packets
- Analyzing TFTP packets
- Analyzing SMB packets
- Analyzing Telnet packets
- reassembling a SIP telephone conversation
- MAC Attacks
 - MAC Flooding Attack
 - MAC Spoofing Attack
- DHCP Attacks
 - DHCP Flooding
 - DHCP Spoofing
- ARP Attacks
 - ARP spoofing/Poisoning
- DNS Attacks
 - DNS Spoofing

- Social Engineering:
 - Phishing
 - Tunneling
 - Ngrok
 - Serveo
 - Zphisher
 - Beef tool
 - Email Phishing
- Web Hacking:
 - Web Application Architecture
 - Fundamentals of HTTP
 - HTTPS
 - HTTPS Testing
 - Nmap
 - SSLScan
 - Qualys SSL Labs
 - Foxy Proxy and Burp Suite
 - OWASP Top 10
 - Juice Shop
 - Finding the Score Board
 - Gobuster
 - Content Discovery using JavaScript
 - Injection
 - SQL Injection attack
 - Blind SQL Injection
 - SQLMap tool

- NoSQL
 - Command execution
 - Server-Side Template Injection (SSTI)
- Broken Authentication
- Sensitive Data Exposure
 - Wappalyzer
 - Robots.txt/sitemap.xml
 - Humans.txt
 - Facvico.ico fingerprint
 - Exiftool
- Improper Input Validation
- Broken Access Control
 - IDOR
 - Web Storage API
 - CSRF
 - HTTP Parameter Pollution (HPP)
 - SSRF
- Security Misconfiguration
- XML External Entities (XXE)
- Cross Site Scripting (XSS)
- Insecure Deserialization
- Vulnerable Components
- The art of effective penetration testing:
 - Penetration testing Tips
 - CTF (Capture the Flag)