Advanced Penetration Testing Course New Syllabus 2021

- **Module 1: Networking** •MAC Address •IP Address •Subnet Mask •Gateway •Classification of IP Addresses •Network Address Translation •Domain Name Server

- **Module 2: Cryptography** •Encryption •Hashing •Encoding •Obfuscation •Hash vs Cryptographic Hash •Classification of Hash functions •MD5, SHA, HMAC

- **Module 3: Foot-printing** Module 4: Network Scanning •Scanning for Live Single Systems •Scanning for Live Multiple Systems •Scanning for Open Ports •Nmap •Nikto •Port scanning

- **Module 4: Network Scanning** •Scanning for Live Single Systems •Scanning for Live Multiple Systems •Scanning for Open Ports •Nmap •Nikto •Port scanning

- **Module 5: Spoofing and System Hacking** •IP Address Spoofing •MAC Address Spoofing •Call Spoofing •URL Spoofing •Email Spoofing -ARP Spoofing •DNS Spoofing

- **Module 6: Web Application Hacking** •Basics of Web Application •Burp suite •Insecure Direct Object reference •Brute force •OTP bypass •Privilege escalation •SQL injection •Command Injection Attack •TML injection •Host header injection •Missing spf •LFI/RFI •File Upload attack •Insufficient Transport Layer Protection •Security Misconfiguration •Insecure Cryptographic Storage •Buffer Overflow •Cross Site Request Forgery attack -(CSRF) •Cross Site Scripting (XSS) •Redirection Attack •Improper Error Handling •Information Leakage

- **Module 7: SQL Injection** •Introduction to SQL Injection •Types of SQL Injection

- **Module 8: - Mobile Application Security** •Android Emulators and Devices and Android Debug Bridge (ADB) •Downloading and installing applications with ADB •Setting Up a Proxy for Android •Mobile Security Framework (Mobsf) •Data Capturing (MITM Attack) •Download and Install CA Certificate -SSL •Data Capturing (MITM Attack) •Android APK Reverse Engineering •OWASP top 10 Mobile Vulnerabilities Module 9: -Web Server Hacking and Network Pentesting •Scanning port with nmap •Kioptrix server (attack) •Windows (eternal blue attack) •Pumpkin garden (attack) •Sniffing Packets •MITM •DNS Poising •ARP Spoofing •Jamming LAN Network •Cut Internet of Whole Network and access full internet. •Browser Exploitation

- **Module 10: Firewall, IDS and IPS** •What is firewall •Types of Firewall •Evading using ip spoofing •IDS •IPS •Honey pots

- **Module 11: Malwares** •What is malware •Types of malware •How to create malware and virus? •Manually detecting virus Module 12: -MetaSploit •Introduction to Metasploit •Hacking windows system •Using Virtual Network Computing •Using exe+payload •Sniffing keystroke of remote system Module 13: -Wireless Hacking •Introduction to wireless networks •Encryption used in wireless •Wi-Fi Attacks •Jamming Attacks •Dictionary Attack •Testing and countermeasure Module 14: -Hacking Mobile Phones •Security Application •Accessing mobile phone remotely •Capturing Call log and SMS •WhatsApp Spoofing •Introduction to termux •Some termux commands