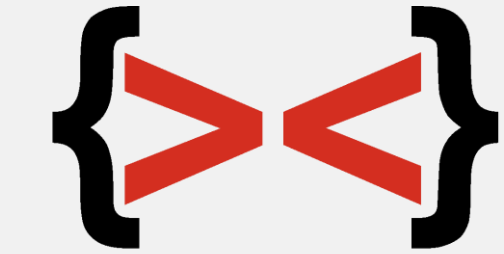
2025



XCODE

Elite Penetration Testing Training 2025

X-code Platinum Training

Elite Penetration Testing Training

Pembelajaran teknik-teknik yang berhubungan cyber security, network hacking, web hacking, exploit development untuk kebutuhan penetration testing.

Waktu Training: 10x pertemuan.

X-code Platinum Training

Elite Penetration Testing Training

No	Session	Objective
Training sessions and materials		
1	Sesi 1	**Sesi 1** Cyber Security Fundamental Dasar jaringan komputer Keamanan protokol jaringan - FTP - SSH - Telnet - SMTP - HTTP - POP3 - SMB - MySQL Dasar kriptografi - Encode & Decode - Encrypt & Decrypt (Simeteris & Asimetris) - Fungsi hash - Fungsi hash + Salt Dasar Reverse Engineering - Target file binary Linux & Windows - TOR & Tsocks

		Dasar terminal linux Firewall Snort (Membuat rules sendiri)
2	Sesi 2 & 3	**Sesi 2** Ethical Hacking Contoh langkah-langkah hacking pada aplikasi vulnerable di windows 10 untuk mendapatkan akses shell - Scanning target di jaringan - Scanning target pada target - Pencarian informasi celah keamanan dan exploit - Eksploitasi celah service target Contoh cara hacking router untuk mendapatkan username dan password dengan routersploit Nessus Langkah-langkah Hacking SMB Windows 7 32 bit dan 64 bit (Firewall aktif & Windows Defender aktif) Meterpreter - Keylogger - VNC - Upload & download Langkah-langkah Hacking SMB Windows 10 dengan sharing folder tanpa password Langkah-langkah pasang backdoor di Windows 10 – Otomatis aktif saat komputer target menjalankan Windows 10

		Sesi 3 Langkah-langkah Hacking SMB Windows 10 dengan memanfaatkan celah SMBGhost Contoh langkah-langkah hacking FTP Server di target linux - Identifikasi aplikasi FTP Server - Pencarian exploit yang sesuai - Eksploitasi Contoh langkah-langkah hacking SAMBA di target linux - Scanning - Identifikasi service samba dan versinya - Pencarian exploit yang sesuai - Eksploitasi Pengamanan dengan firewall dan update ARP Spoofing (Ettercap & Wireshark) DNS Spoofing Stealing cookies through ARP spoofing to log into a website without a password

XCODE

EXPLOIT DEVELOPMENT

3	Sesi 4	**Sesi 4** Exploit Development pada target Windows 10 Buffer Overflow Membuat program Fuzzer dengan python Pattern create & pattern offset Extended Instruction Pointer (EIP) Extended Stack Pointer (ESP) NOPSleed Mengenal Bad Character Bypass SEH Bypass SafeSEH Bypass ASLR (Address Space Layout Handling) Generate shell reverse shell dengan msfvenom Egghunter Bypass DEP (Data Exection Prevention) Adding our custom exploit to Metasploit Jumpshort PoC

4	Sesi 5 & 6	**Sesi 5** Hacking Website secara beretika Information Gathering - Mencari berbagai informasi tentang web target - Mencari file-file sensitif - Mendeteksi WAF pada target - Scanning keberadaan subdomain pada web target Contoh Teknik Bypass Cloudflare untuk mendapatkan ip address web target Denial of Service pada web server Apache & Nginx Pengamanan dari serangan Denial of Server pada Apache & Nginx XSS (Cross Site Scripting) – Non Persistent Pengamanan dari serangan XSS XSS (Cross Site Scripting) – Persistent Mengambil Cookie dengan memanfaat XSS untuk login tanpa password **Sesi 6** RFI (Remote File Inclusion) Pengamanan dari serangan RFI dari sisi pemrograman dan PHP.INI Privilege Escalation pada target linux Backdoor akun pada target linux

		Rootkit Incident handling - Analisa log - Mencari backdoor dengan cepat - Deteksi PHP Shell otomatis dengan cepat - Menghapus backdoor - Perbaikan celah keamanan pada aplikasi
5	Session 7	**Sesi 7** LFI (Local File Inclusion) Contoh cara mendapatkan akses shell dari celah Local File Inclusion Pengamanan dari serangan LFI dari sisi pemrograman dan PHP.INI Brute force login pada web Brute force login pada CMS Wordpress & Joomla Contoh langkah-langkah Hacking CMS (Wordpress dan Joomla) Insecure Direct Object References (IDOR) SQL Injection (GET dan POST) Pengamanan dari serangan SQL Injection Bypass Web Application Firewall (WAF) – SQL Injection Bypass Web Application Firewall (WAF) – XSS Pengamanan maksimal dengan WAF Contoh serangan pada bypass disable function (PHP)

6	Sesi 8 & 9	**Sesi 8** - Contoh cari mencari celah kernel linux dan update kernel (Mengamankan kernel dari rooting exploit yang sebelum berhasil di rooting) - Menonaktifkan Directory Listing (Linux) – Ubuntu - Deteksi PHP Shell di web server secara otomatis (Linux) - Menghapus otomatis PHP Shell di server Antivirus di Linux - PHPMyadmin Honeypot (Di linux) - Mengganti url default URL pada PHPMyadmin (Linux) - PHPMyadmin Honeypot (Di linux) **Sesi 9** Dasar Wireless LAN - Mengenal keamanan wireless pada access point - Macchanger - Bypass mac filtering (Deny the stations specified by any enabled entries in the list to access) - Cara sniffing SSID Hidden pada hotspot target dengan airodump-ng. (Dari X-code Premium Video) - Jamming - Hacking password WPA-PSK dengan menggunakan wordlist di linux - Cracking password WPA-PSK dengan semua kemungkinan pada kriteria tertentu di linux (bukan daftar kata yang ada pada file text / wordlist) - Hacking password WPA-PSK dengan LINSET

7	Sesi 10	**Sesi 10** The Penetration Testing Execution Standard Dasar Pentest Pre-engagement Interactions General Questions Penetration testing offers Intelligence Gathering OSINT Threat Modeling Vulnerability Analysis Testing Exploitation CVSS Score Post Exploitation Vulnerability Impact and risks Recommendation Reporting