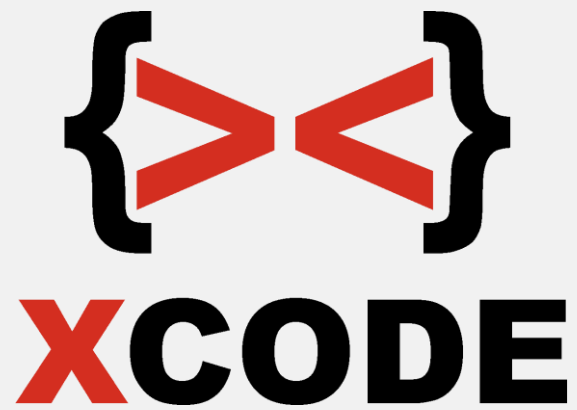


2024



**Elite Penetration
Testing Training
2024**



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: 7x pertemuan.



X-code Platinum Training

Elite Penetration Testing Training

No	Session	Objective
Performing Basic System Management Tasks		
1	Sesi 1	<p>Sesi 1</p> <p>Cyber Security Fundamental</p> <p>Dasar jaringan komputer</p> <p>Keamanan protokol jaringan</p> <ul style="list-style-type: none">- FTP- SSH- Telnet- SMTP- HTTP- POP3- SMB- MySQL <p>Dasar kriptografi</p> <ul style="list-style-type: none">- Encode & Decode- Encrypt & Decrypt (Simeteris & Asimetris)- Fungsi hash- Fungsi hash + Salt <p>Dasar Reverse Engineering</p> <ul style="list-style-type: none">- Target file binary Linux & Windows- TOR & Tsocks

		<p>Dasar terminal linux</p> <p>Firewall</p> <p>Snort (Membuat rules sendiri)</p>
2	Sesi 2	<p>Sesi 2</p> <p>Ethical Hacking</p> <p>Contoh langkah-langkah hacking pada aplikasi vulnerable di windows 10 untuk mendapatkan akses shell</p> <ul style="list-style-type: none"> - Scanning target di jaringan - Scanning target pada target - Pencarian informasi celah keamanan dan exploit - Eksploitasi celah service target <p>Contoh cara hacking router untuk mendapatkan username dan password dengan routersploit</p> <p>Nessus</p> <p>Langkah-langkah Hacking SMB Windows 7 32 bit dan 64 bit (Firewall aktif & Windows Defender aktif)</p> <p>Meterpreter</p> <ul style="list-style-type: none"> - Keylogger - VNC - Upload & download <p>Langkah-langkah Hacking SMB Windows 10 dengan sharing folder tanpa password</p> <p>Langkah-langkah pasang backdoor di Windows 10 – Otomatis aktif saat komputer target menjalankan Windows 10</p>

	<p>Langkah-langkah Hacking SMB Windows 10 dengan memanfaatkan celah SMBGhost</p> <p>Contoh langkah-langkah hacking FTP Server di target linux</p> <ul style="list-style-type: none">- Identifikasi aplikasi FTP Server- Pencarian exploit yang sesuai- Eksploitasi <p>Contoh langkah-langkah hacking SAMBA di target linux</p> <ul style="list-style-type: none">- Scanning- Identifikasi service samba dan versinya- Pencarian exploit yang sesuai- Eksploitasi <p>Pengamanan dengan firewall dan update</p> <p>ARP Spoofing (Ettercap & Wireshark)</p> <p>DNS Spoofing</p> <p>Stealing cookies through ARP spoofing to log into a website without a password</p>
--	---



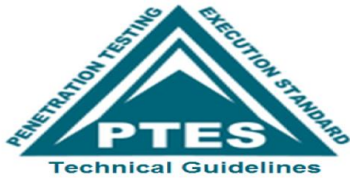
EXPLOIT DEVELOPMENT

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

4	Sesi 4	<p>Sesi 4</p> <p>Hacking Website secara beretika</p> <p>Information Gathering</p> <ul style="list-style-type: none">- Mencari berbagai informasi tentang web target- Mencari file-file sensitif- Mendeteksi WAF pada target- Scanning keberadaan subdomain pada web target <p>Contoh Teknik Bypass Cloudflare untuk mendapatkan ip address web target</p> <p>Denial of Service pada web server Apache & Nginx</p> <p>Pengamanan dari serangan Denial of Server pada Apache & Nginx</p> <p>XSS (Cross Site Scripting) – Non Persistent</p> <p>Pengamanan dari serangan XSS</p> <p>XSS (Cross Site Scripting) – Persistent</p> <p>Mengambil Cookie dengan memanfaatkan XSS untuk login tanpa password</p> <p>RFI (Remote File Inclusion)</p> <p>Pengamanan dari serangan RFI dari sisi pemrograman dan PHP.INI</p> <p>Privilege Escalation pada target linux</p> <p>Backdoor akun pada target linux</p>
---	--------	--

		<p>Rootkit</p> <p>Incident handling</p> <ul style="list-style-type: none"> - Analisa log - Mencari backdoor dengan cepat - Deteksi PHP Shell otomatis dengan cepat - Menghapus backdoor - Perbaiki celah keamanan pada aplikasi
5	Session 5	<p>Sesi 5</p> <p>LFI (Local File Inclusion)</p> <p>Contoh cara mendapatkan akses shell dari celah Local File Inclusion</p> <p>Pengamanan dari serangan LFI dari sisi pemrograman dan PHP.INI</p> <p>Brute force login pada web</p> <p>Brute force login pada CMS Wordpress & Joomla</p> <p>Contoh langkah-langkah Hacking CMS (Wordpress dan Joomla)</p> <p>Insecure Direct Object References (IDOR)</p> <p>SQL Injection (GET dan POST)</p> <p>Pengamanan dari serangan SQL Injection</p> <p>Bypass Web Application Firewall (WAF) – SQL Injection</p> <p>Bypass Web Application Firewall (WAF) – XSS</p> <p>Pengamanan maksimal dengan WAF</p>

		serangan disable function
6	Sesi 6	<p>Sesi 6</p> <ul style="list-style-type: none"> - 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 Honeygot (Di linux) - Mengganti url default URL pada PHPMyadmin (Linux) - PHPMyadmin Honeygot (Di linux) <p>Dasar Wireless LAN</p> <ul style="list-style-type: none"> - 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 7	<p>Sesi 7</p> <p>The Penetration Testing Execution Standard</p> <p>Dasar Pentest</p> <p>Pre-engagement Interactions</p> <p>General Questions</p> <p>Penetration testing offers</p> <p>Intelligence Gathering</p> <p>OSINT</p> <p>Threat Modeling</p> <p>Vulnerability Analysis</p> <p>Testing</p> <p>Exploitation</p> <p>CVSS Score</p> <p>Post Exploitation</p> <p>Vulnerability Impact and risks</p> <p>Recommendation</p> <p>Reporting</p>
---	--------	---