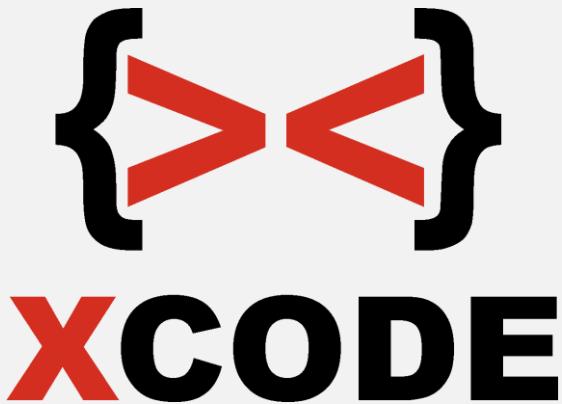
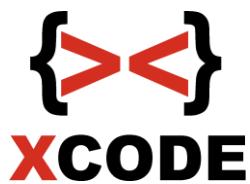


2024



**Ethical Hacking & Security**  
**Excellence**

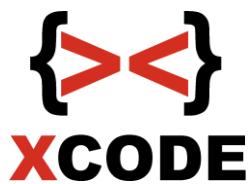


## X-code Platinum Training

### Ethical Hacking & Security Excellence

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

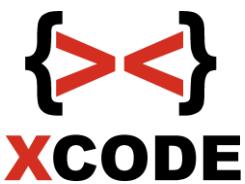
**Waktu Training:** 6x pertemuan.



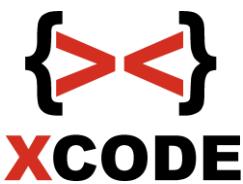
# X-code Platinum Training

## Ethical Hacking & Security Excellence

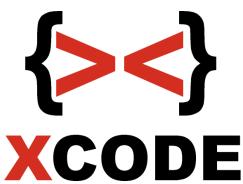
No	Session	Objective
<b>Performing Basic System Management Tasks</b>		
1	Sesi 1	<p>Sesi 1</p> <p>Cyber Security Fundamental</p> <p>Dasar jaringan komputer</p> <p>Keamanan protokol jaringan</p> <ul style="list-style-type: none"><li>- FTP</li><li>- SSH</li><li>- Telnet</li><li>- SMTP</li><li>- HTTP</li>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



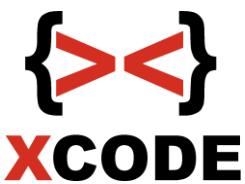
		<p>Dasar terminal linux</p> <p>Firewall</p> <p>Snort</p>
2	Sesi 2	<p>Sesi 2</p> <p>Ethical Hacking</p> <p>Contoh langkah-langkah hacking pada aplikasi vulnerable di windows 10 untuk mendapatkan akses shell</p> <ul style="list-style-type: none"><li>- Scanning target di jaringan</li><li>- Scanning target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



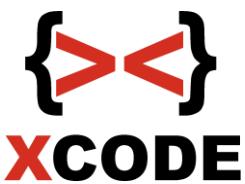
		<ul style="list-style-type: none"><li>- Pencarian exploit yang sesuai</li><li>- Eksloitasi</li></ul> <p>Contoh langkah-langkah hacking SAMBA di target linux</p> <ul style="list-style-type: none"><li>- Scanning</li><li>- Identifikasi service samba dan versinya</li><li>- Pencarian exploit yang sesuai</li><li>- Eksloitasi</li></ul> <p>Pengamanan dengan firewall dan update</p>
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 &amp; 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>Jumpshort</p>



		PoC
4	Sesi 4	<p>Sesi 4</p> <p>Hacking Website secara beretika</p> <p>Information Gathering</p> <ul style="list-style-type: none"><li>- Mencari berbagai informasi tentang web target</li><li>- Mencari file-file sensitif</li><li>- Mendeteksi WAF pada target</li><li>- Scanning keberadaan subdomain pada web target</li></ul> <p>Contoh Teknik Bypass Cloudflare untuk mendapatkan ip address web target</p> <p>Denial of Service pada web server Apache &amp; Nginx</p> <p>Pengamanan dari serangan Denial of Server pada Apache &amp; 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 memanfaat 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"><li>- Analisa log</li><li>- Mencari backdoor dengan cepat</li><li>- Deteksi PHP Shell otomatis dengan cepat</li><li>- Menghapus backdoor</li><li>- Perbaikan celah keamanan pada aplikasi</li></ul>
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 &amp; 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> <p>Pengamanan dari sisi serangan PHP Shell dan</p>



		serangan disable function
6	Sesi 6	<p>Sesi 6</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>