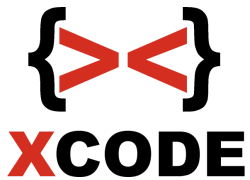


**Xcode Intensif Training**  
**Ethical Hacking Advanced**



## **Ethical Hacking – Advanced**

Pembelajaran teknik-teknik network hacking, wireless hacking dan web hacking secara ethical. Penambahannya adalah pembahasan exploit development dan shellcode lebih lanjut. 8,

**Waktu Training:** 8 hari antara 2-5 jam.

**Objectives :** Dengan Menyelesaikan training ini diharapkan peserta bisa melakukan teknik-teknik network hacking, web hacking dan wireless sesuai silabus. Selain itu peserta diharapkan dapat mengembangkan diri untuk pengembangan exploit.

## Ethical Hacking Advanced

No	Session	Objective
<b>Performing Basic System Management Tasks</b>		
1	Session 1	<ul style="list-style-type: none"> <li>- Network Fundamental</li> <li>- Dasar IP Address, Mac Address, pengenalan 7 layer OSI, etc</li> <li>- FTP, SSH, Telnet, DNS, DHCP, Web Server, SMB, POP3, SMTP, MySQL Server, VNC, RDP</li> <li>- Subnetting (CIDR, perhitungan biner ke desimal, perhitungan subnetting, etc)</li> <li>- Routing (NAT)</li> <li>- Port Forwarding</li> <li>- DMZ (Demilitarized Zone)</li> <li>- VPN (Virtual Private Network)</li> <li>- Dasar Kriptografi</li> <li>- Mengenal encode / decode (base64), disertai prakteknya dengan python</li> <li>- Mengenal salah satu enkripsi &amp; dekripsinya pada kriptografi simetris, disertai prakteknya dengan python</li> <li>- Mengenal enkripsi &amp; dekripsinya pada kriptografi asimetris (public key &amp; private key), disertai prakteknya dengan python</li> </ul>

		<ul style="list-style-type: none"> <li>- Mengetahui fungsi hash disertai prakteknya untuk membangun hashnya dengan python dan cara cracknya dengan menggunakan wordlist</li> <li>- Firewall</li> <li>- Port Knocking</li> </ul>
2	Session 2	<ul style="list-style-type: none"> <li>- Proxy</li> <li>- TOR Windows</li> <li>- TOR Linux (Advanced) ~ Hacking Server seperti FTP Server, SSH Server, dst dengan koneksi TOR</li> <li>- SSH Tunnel</li> <li>- Command prompt</li> <li>- Manajemen user (Command prompt)</li> <li>- Pembelajaran Shell Bash</li> <li>- Repository</li> <li>- Recovery mode di linux</li> <li>- Setting IP Client di linux (Permanen &amp; non permanen)</li> <li>- Menambah ip baru pada interface</li> <li>- Manajemen user dan group di linux</li> <li>- File Security : chown, chgrp, chmod (numeric coding, letter coding)</li> <li>- SSH Server (user &amp; admin)</li> <li>- Screen</li> </ul>

		<ul style="list-style-type: none"> <li>- SAMBA (read only, writeable, valid users)</li> <li>- Server APACHE</li> <li>- Firewall ufw</li> <li>- SSH Server (user &amp; admin)</li> <li>- SAMBA (read only, writeable, valid users)</li> <li>- Server APACHE</li> </ul> <p>Keamanan</p> <ul style="list-style-type: none"> <li>- Mematikan recovery pada GRUB</li> <li>- Firewall ufw</li> </ul> <p>Pengawasan</p> <ul style="list-style-type: none"> <li>- Mengenali log-log server dan mengawasi client yang login</li> </ul>
<p style="text-align: center;"><b>3</b></p>	<p style="text-align: center;">Session 3</p>	<ul style="list-style-type: none"> <li>- Ethical Hacking</li> <li>- Strategi, metode &amp; langkah dasar</li> <li>- Scanning jaringan</li> <li>- Scanning IP, port, service, OS yang digunakan, dll</li> <li>- Dasar Hacking (Step by step)</li> <li>- Hacking suatu Web Server dengan searchsploit / exploit-db (Step by step)</li> <li>- Shell (eksploitasi di shell seperti copy data)</li> <li>- Hacking suatu Web Server yang terinstall di Windows 7 (Step by step)</li> </ul>

		<ul style="list-style-type: none"> <li>- Hacking suatu FTP Server yang terinstall di Windows 10 (Step by step)</li> <li>- Hacking suatu FTP Server dengan metasploit framework (Step by step)</li> <li>- Perintah-perintah metasploit dasar dan contoh encode pada payload saat eksploitasi</li> <li>- Backdoor pada target Windows (Tiap target masuk windows, attacker langsung mendapatkan akses)</li> <li>- Scanning bug dengan Nexus dan contoh eksploitasinya dengan metasploit</li> <li>- Scanning bug dengan OpenVas dan contoh eksploitasinya dengan metasploit</li> <li>- Hacking pada SMB Windows XP SP3 ber-firewall (Bypass firewall pada target Windows) (Step by step)</li> <li>- Perintah-perintah meterpreter dasar</li> <li>- Hacking pada service SMB Windows Vista / Windows Server 2008</li> <li>- Hacking pada service SMB Windows 7 Full Version / Windows 7 SP1</li> <li>- Hacking pada service SMB Windows Server 2008 R2 Enterprise</li> <li>- Hacking pada target server dengan platform linux (Bypass firewall pada target linux)</li> </ul>
4	Session 4	<ul style="list-style-type: none"> <li>- Buffer Overflow</li> <li>- Fuzzer Development (Membuat fuzzer sendiri dengan Python)</li> </ul>

- EIP & SEH Handler
- Pattern create & pattern offset
- Cek proteksi SafeSEH & ASLR dan menghindarinya
- Uji coba perbedaan module yang terproteksi dan yang tidak terproteksi
- JMP ESP
- SEH & SafeSEH
- POP POP RETN (Bypass SEH)
- Mengenal Bad Character
- Jump Short
- Mengenal bahasa mesin, heksadesimal dan x86 assembler instruction set opcode table
- Tabel kebenaran XOR
- Shellcode Development untuk membuat CPU bekerja hingga 100% (Membuat dengan bahasa assembler dari awal)
- Shellcode Development untuk remote (Membuat dengan bahasa assembler dari awal)
- Penggunaan nasm dan objdump untuk shellcode yang dibuat
- Cara penyusunan shellcode secara cepat
- Shellcode generate dengan encode shikata\_ga\_nai
- Proof of concept pada exploit yang dibuat

5	Session 5	<ul style="list-style-type: none"> <li>- Scanning IP, port, service, OS dll</li> <li>- Denial of Service - Web Server (intranet &amp; internet)</li> <li>- Denial of Service - IP Publik (Koneksi internet target down)</li> <li>- Denial of Service SMBv1 - (SMB Windows XP, SMB Windows Server 2003)</li> <li>- Denial of Service SMBv2 - (SMB Windows Vista, SMB Windows Server 2008)</li> <li>- Denial of Service RDP (RDP Windows 7)</li> <li>- Serangan meningkatkan proses CPU melalui SMB secara cepat di Windows 8</li> <li>- Windows 7 SMB ATTACK (Target Windows 7 FULL VERSION)</li> <li>- Windows 8.1 / 10 SMB CLIENT DoS (Blue screen)</li> <li>- DHCP Flooding</li> <li>- Netcut</li> <li>- ARP Spoofing ( Sniffing http / telnet / pop3 / mysql &amp; crack with wordlist / smb &amp; crack with wordlist / ftp / Sniffing isi email (client ke smtp server)</li> <li>- Wireshark</li> <li>- Sniffing password dengan sertifikat SSL palsu pada HTTPS</li> <li>- Sniffing password dengan SSLStrip</li> </ul>
---	-----------	---

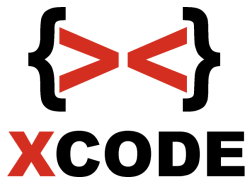


		<ul style="list-style-type: none"> <li>- Eksploitasi heartbleed untuk membaca memory dari server yang diproteksi oleh OpenSSL (Bisa mengambil password pengguna pada web dan sebagainya)</li> <li>- Cookies stealing (MITM + Wireshark)</li> <li>- Bypass login web tanpa memasukkan password (Wireshark cookie dump) ~ Session Hijacking (Cookie Hijacking)</li> </ul>
6	Session 6	<ul style="list-style-type: none"> <li>- DNS Spoofing (windows / linux)</li> <li>- Membuat fake login sendiri</li> <li>- Client side Attack ~ Browser IE (Windows XP/Windows 7)</li> <li>- Client side Attack ~ Browser Firefox</li> <li>- Client side Attack ~ Browser ~ Adobe Flash (Pengujian di IE 11 &amp; Windows 8.1)</li> <li>- Client side Attack ~ Browser ~ Adobe Acrobat (PDF)</li> <li>- Bypass login masuk windows (Berbagai versi windows seperti Windows 7 dan Windows 8.1))</li> <li>- Msfvenom untuk backdoor Windows 7 &amp; mendapatkan akses administrator (Local exploit)</li> <li>- Msfvenom untuk backdoor Windows 8.1 &amp; mendapatkan akses administrator (Local Exploit)</li> <li>- Msfvenom untuk backdoor Windows (Backdoor di inject kan ke file exe lain) – Tersembunyi / tidak terlihat</li> <li>- Membuat backdoor Android (Backdoor di injek kan ke file apk lain) – Tersembunyi / tidak terlihat</li> <li>- Meterpreter (Download, upload, keylogger, VNC, etc)</li> </ul>

		<ul style="list-style-type: none"> <li>- Privilege escalation</li> <li>- John the ripper pada Windows / linux</li> <li>- Brute force attack (VNC / telnet / ftp / pop3 / http / mysql / ssh / vnc / samba linux)</li> <li>- Membangun wordlist dengan berbagai kriteria sendiri secara cepat (generate)</li> <li>- Covering Track (Menghapus jejak)</li> </ul>
7	Session 7	<ul style="list-style-type: none"> <li>- Pengenalan web dan database (HTML, PHP, MySQL)</li> <li>- Mengetahui web hacking</li> <li>- Reverse domain</li> <li>- Google hacking</li> <li>- Mendeteksi jenis hash secara otomatis dan contoh melakukan cracking dari situs-situs cracking hash</li> <li>- Mendeteksi Web Application Firewall pada website</li> <li>- Cross-site scripting (XSS)</li> <li>- Scanning XSS - di linux dan windows</li> <li>- Eksploitasi XSS non persistent untuk remote target melalui client side attack (browser ~ metasploit framework)</li> <li>- Eksploitasi XSS persistent untuk menggunakan account target tanpa password login (Mengambil cookie dari target), masukkan ke browser lalu akses account target</li> <li>- Cross-Site Request Forgery (CSRF)</li> </ul>

	<ul style="list-style-type: none"><li>- Local File Inclusion</li><li>- LFI untuk mendapatkan akses PHPMyadmin pada kasus celah pada plugin wordpress</li><li>- LFI untuk mendapatkan username pada linux</li><li>- WPScan</li><li>- WPScan for brute force (Advanced) ~ Username Enumeration + crack password (Wordlist)</li><li>- Admin login scanner</li><li>- Scanning SQL Injection - di Linux dan Windows</li><li>- Remote File Inclusion</li><li>- Scanning RFI - di linux dan windows</li><li>- PHP Shell Development (Membuat PHP Shell sendiri dari awal untuk RFI)</li><li>- Remote shell target dengan celah RFI</li><li>- Bind Shell &amp; Reverse shell</li><li>- SQL Injection manual (Dasar)</li><li>- SQL Injection - bypass login wp</li><li>- PHP upload &amp; logger Login</li><li>- Havij di Windows</li><li>- SQLMAP di Linux</li><li>- SQL Injection pada web halaman login</li><li>- Tabel kebenaran gerbang "AND" dan "OR"</li></ul>
--	--

		<ul style="list-style-type: none"> <li>- Variasi SQL Injection pada login</li> </ul> <p>Websploit untuk scan PMA</p> <ul style="list-style-type: none"> <li>- PhpMyAdmin Exploitation Advanced</li> <li>- Ngeroot Linux</li> </ul>
	<p>Session 8</p>	<ul style="list-style-type: none"> <li>- Dasar Wireless LAN</li> <li>- Mengenal keamanan wireless pada access point</li> <li>- Mac changer</li> <li>- Bypass mac filtering (Deny the stations specified by any enabled entries in the list to access)</li> <li>- Bypass mac filtering (Allow the stations specified by any enabled entries in the list to access)</li> <li>- Bypass SSID Hidden (teori)</li> <li>- Analisa dasar paket wireless untuk mengetahui ip address yang ada di jaringan</li> </ul> <p>SSID Flooding</p> <ul style="list-style-type: none"> <li>- Jamming</li> <li>- Hacking WEP</li> <li>- Hacking password WPA-PSK dengan menggunakan wordlist</li> <li>- Cracking dengan paket WPA-PSK dengan VGA Card (CUDA)</li> <li>- Hacking password WPA-PSK melalui WPS (tidak sampai 1 menit - tidak semua AP bisa)</li> </ul>



		<ul style="list-style-type: none"><li>- Hacking password WPA-PSK pada router ADSL melalui eksploitasi Wifi.id</li><li>- Hacking password WPA-PSK dengan LINSET</li></ul>
--	--	--