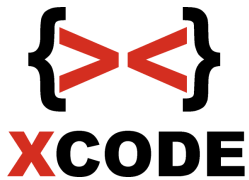


**Xcode Intensif Training**  
**Ethical Hacking & Security**



## **Ethical Hacking & Security**

Pembelajaran teknik-teknik network hacking, wireless hacking dan web hacking secara ethical. Penambahannya adalah pembahasan exploit development dan shellcode. Tambahan dari program materi ini adalah disertai pengamanannya sesuai silabus.

**Waktu Training:** 11 hari antara 2-5 jam.

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

## Ethical Hacking & Security

No	Session	Objective
<b>Performing Basic System Management Tasks</b>		
1	Session 1	<ul style="list-style-type: none"> <li>- Computer Security &amp; IT Security Awareness</li> <li>- Mengenal data &amp; representasinya, hexdump pada file, ascii table, hexwrite</li> <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 dasar enkripsi &amp; dekripsi pada kriptografi simetris pada caesar (prakteknya dengan python), substitusi (enkripsi dari penyedia layanan di web dan contoh cracknya dari penyedia layanan di web online),</li> </ul>

		<p>enkripsi dan dekripsi dengan XOR (prakteknya dengan python)</p> <ul style="list-style-type: none"> <li>- Mengetahui enkripsi pada kriptografi asimetris (public key &amp; private key), disertai prakteknya dengan python</li> <li>- Mengetahui fungsi hash disertai prakteknya untuk membangun hashnya dengan python dan cara cracknya dengan menggunakan wordlist</li> <li>- Contoh crack hash MD5 / SHA1 / lainnya dengan Hashcat</li> </ul>
2	Session 2	<ul style="list-style-type: none"> <li>- Firewall</li> <li>- Port Knocking</li> <li>- Forwarding pada managed switch</li> <li>- Proxy</li> <li>- TOR Windows</li> <li>- TOR Linux (Advanced) ~ Hacking Server seperti FTP Server, SSH Server, dst dengan koneksi TOR</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> </ul>

		<ul style="list-style-type: none"> <li>- Managemen 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> <li>- SAMBA (read only, writeable, valid users)</li> <li>- SMB Client</li> <li>- Server APACHE</li> <li>- Firewall ufw</li> </ul> <p>Keamanan</p> <ul style="list-style-type: none"> <li>- Mematikan recovery mode pada GRUB</li> <li>- Firewall ufw</li> <li>- Blokir ip ke server dengan firewall ufw</li> </ul> <p>Pengawasan</p> <ul style="list-style-type: none"> <li>- Mengenali log-log server dan mengawasi client yang login</li> <li>- IDS (Intrusion detection system) dengan Snort (Linux)</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 and Countermeasures</li> <li>- Mengenal Vulnerability Assessment &amp; Penetration Test</li> <li>- Strategi, metode &amp; langkah dasar</li> <li>- Scanning jaringan</li> </ul>

	<ul style="list-style-type: none"><li>- Tips dan trik untuk mengetahui Ip melalui nama komputer di kali linux, mengetahui ip dan mac di jaringan secara cepat di kali linux, dan sebagainya</li><li>- Scanning IP, port, service, OS yang digunakan, dan sebagainya</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>- Mengambil password-password seperti facebook, yahoo mail dan sebagainya yang disimpan pada browser seperti firefox (firefox baru) dan sebagainya, sampai FTP Server filezilla bisa diambil passwordnya melalui shell (post exploitation)</li><li>- Hacking suatu Web Server yang terinstall di Windows 7 (Step by step)</li><li>- Hacking suatu FTP Server yang terinstall di Windows 10 (Step by step)</li><li>- Hacking suatu router dengan routersploit</li><li>- Hacking suatu SSH Server dengan memanfaatkan situs mesin pencari (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></ul>
--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

		<ul style="list-style-type: none"> <li>- Scanning bug dengan Nessus dan contoh eksploitasinya dengan metasploit</li> <li>- Hacking pada service SMB Windows XP SP3 ber-firewall (Bypass firewall pada target Windows) (Step by step) untuk mendapatkan akses meterpreter / shell</li> <li>- Perintah-perintah meterpreter dasar</li> <li>- Hacking pada service SMB Windows Vista / Windows Server 2008 untuk mendapatkan akses shell</li> <li>- Hacking pada service SMB Windows 7 Full Version / Windows 7 SP1 untuk mendapatkan akses shell / meterpreter</li> <li>- Hacking pada service SMB Windows Server 2008 R2 Enterprise untuk mendapatkan akses shell</li> <li>- Hacking pada service SMB Windows 8.1 / 10 yang mengijinkan share folder tanpa password untuk mendapatkan akses shell (Bypass Windows Defender)</li> <li>- Hacking Mikrotik Router v6 pada service winbox (Langsung mendapatkan password mikrotik melalui jaringan, bukan brute force)</li> <li>- Hacking pada service SMB Windows Server 2012 / 2016 yang mengijinkan share folder tanpa password untuk mendapatkan akses shell</li> </ul>
4	Session 4	<ul style="list-style-type: none"> <li>- Hacking SAMBA pada suatu target Ubuntu Server untuk mendapatkan akses shell linux</li> <li>- Hacking pada suatu target FTP server dengan platform linux (Bypass firewall pada target linux)</li> </ul> <p>Pengamanan</p>

	<ul style="list-style-type: none"><li>- Teknik untuk meminimalisir serangan ke server dan pengamanannya secara umum</li><li>- Teknik melakukan banned otomatis pada ip target yang melakukan scanning menggunakan NMAP dengan option seperti misal -sV dan -A</li><li>- Scanning dan pembangunan komputer lab untuk fuzzing hingga pengembangan exploit</li><li>- Mengenal Memory layout</li><li>- Buffer Overflow</li><li>- Fuzzer Development (Membuat fuzzer sendiri dengan Python)</li><li>- EIP &amp; SEH Handler</li><li>- Pattern create &amp; pattern offset</li><li>- JMP ESP</li><li>- Mengenal Bad Character</li><li>- Mengenal bahasa mesin, heksadesimal dan x86 assembler instruction set opcode table</li><li>- Tabel kebenaran XOR</li><li>- Shellcode Development untuk remote (Membuat dengan bahasa assembler dari awal)</li><li>- Penggunaan nasm dan objdump untuk shellcode yang dibuat</li><li>- Cara penyusunan shellcode secara cepat</li><li>- Proof of concept pada exploit yang dibuat</li><li>- Shellcode generate dengan encode shikata_ga_nai</li></ul>
--	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------



		<ul style="list-style-type: none"> <li>- Tugas untuk membuat exploit remote buffer overflow pada suatu web server</li> <li>- Pembahasan tugas pembuatan exploit remote buffer overflow pada web server</li> <li>- SEH (Structured Exception Handling)</li> <li>- Latihan target program yang memiliki proteksi SEH</li> <li>- Cek proteksi SafeSEH / ASLR dan menghindarinya</li> <li>- POP POP RETN (Bypass SEH)</li> </ul>
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). Contoh pada apache server, web dari OS mikrotik dan access point tp-link</li> <li>- Denial of Service - IP Publik (Koneksi internet target down)</li> <li>- Denial of Service SMBv1 - (SMB Windows XP, SMB Windows Server 2003) (Blue Screen)</li> <li>- Denial of Service SMBv2 - (SMB Windows Vista, SMB Windows Server 2008) (Blue Screen)</li> <li>- Denial of Service RDP (RDP Windows 7)</li> <li>- Serangan meningkatkan proses CPU melalui SMB secara cepat di Windows 8</li> <li>- Denial of Service SMB Windows 7 (Blue Screen)</li> <li>- Windows 8.1 / 10 SMB CLIENT DoS (Blue screen)</li> </ul>

	<ul style="list-style-type: none"><li>- Denial of Service Windows 8.1 / 10 pada SMB Service yang memungkinkan share folder tanpa password (Blue Screen)</li><li>- Denial of Service Windows 2012 / 2016 pada SMB Service yang memungkinkan share folder tanpa password (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>- Mengenal HTTPS</li><li>- Memahami keamanan dari Page URL &amp; Form URL</li><li>- Sniffing password dengan sertifikat SSL palsu pada HTTPS</li><li>- Sniffing password dengan SSLStrip</li><li>- Eksploitasi heartbleed untuk membaca memory dari server yang diproteksi oleh OpenSSL (Bisa mengambil password pengguna pada web dan sebagainya)</li></ul> <p>Pengamanan</p> <ul style="list-style-type: none"><li>- Mengamankan Web Server dari serangan DoS tertentu (Pengujian sebelum diamankan pada serangan sebelumnya dan setelah diamankan) (Linux)</li><li>- Pengamanan dari serangan ARP Spoofing dan pengamanan lainnya (Linux)</li></ul> <p>Penggantian FTP dengan SFTP</p>
--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

6	Session 6	<ul style="list-style-type: none"> <li>- DNS Spoofing (windows / linux)</li> <li>- Membuat fakedologin sendiri</li> <li>- Client side Attack ~ Browser IE (Windows XP/Windows 7) / Client side Attack ~ Browser Firefox / Client side Attack ~ Browser ~ Adobe Flash (Pengujian di IE 11 &amp; Windows 8.1) / Client side Attack ~ Browser ~ Adobe Acrobat (Document PDF)</li> <li>- Eksploitasi celah remote pada Microsoft Word 2010 / 2013 / 2016)</li> <li>- Bypass password login masuk windows (Berbagai versi windows seperti Windows 7 dan Windows 8.1)</li> <li>- Membangun backdoor untuk remote Windows 10 dan bypass antivirus internal Windows 10 (Windows Defender)</li> <li>- Msfvenom untuk backdoor Windows (Backdoor di inject kan ke file exe lain) – Tersembunyi / tidak terlihat</li> <li>- Meterpreter (Download, upload, keylogger, VNC, etc)</li> <li>- Privilege escalation (Menaikkan hak akses dari user biasa menjadi akses admin pada Windows Server 2008 / Windows 7 SP1 / Windows 8.1 / Windows 10 / Windows Server 2012 R2 / Windows server 2016</li> <li>- John the ripper pada Windows / linux</li> <li>- Brute force attack dengan wordlist (VNC / telnet / ftp / pop3 / http / mysql / rdp / ssh / vnc / samba linux)</li> <li>- Brute force attack tanpa wordlist tapi dengan semua kemungkinan pada kriteria tertentu, contoh praktek pada FTP Server</li> </ul>
---	-----------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

		<ul style="list-style-type: none"> <li>- Membangun wordlist dengan berbagai kriteria sendiri secara cepat (generate)</li> </ul> <p>Pengamanan</p> <ul style="list-style-type: none"> <li>- Pengamanan umum</li> <li>- SSH Honeypot</li> <li>- Membatasi jumlah login SSH yang salah</li> </ul> <p>Tambahan</p> <ul style="list-style-type: none"> <li>- Cara mendeteksi SSH Honeypot</li> </ul>
<b>7</b>	Session 7	<ul style="list-style-type: none"> <li>- Pengenalan web dan database (HTML, PHP, MySQL)</li> <li>- Form, action, metode post, input type text dan submit, koneksi database, mysqli_connect, mysqli_query, pengkondisian &amp; mysql_num_rows, create database, use, create table, insert, select, alter, update, drop.</li> <li>- Mengenal web hacking</li> <li>- Reverse domain</li> <li>- Google hacking (umum)</li> <li>- Google hacking untuk kasus-kasus khusus (mendapatkan file-file dari folder yang terbuka, mendapatkan potensi keberadaan halaman login)</li> <li>- Mendeteksi jenis hash secara otomatis dan contoh melakukan cracking dari situs-situs cracking hash</li> <li>- Dirbuster</li> <li>- Mendeteksi Web Application Firewall pada website</li> <li>- Memahami Get Method &amp; post method</li> </ul>

		<ul style="list-style-type: none"> <li>- Cross-site scripting (XSS)</li> <li>- Pengamanan XSS dari sisi pemrograman</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>- Bypass filter upload image dengan tamper data</li> <li>- Pengamanan upload dengan .htaccess</li> <li>- Variasi teknik-teknik bypass filter upload</li> </ul>
	<p>Session 8</p>	<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>- Contoh pengamanan LFI dari sisi programming</li> <li>- Contoh pengamanan LFI dari sisi konfigurasi PHP.INI</li> <li>- WPScan</li> <li>- Admin login scanner (Perl)</li> <li>- Scanning SQL Injection - di Linux dan Windows</li> <li>- Remote File Inclusion</li> </ul>

		<ul style="list-style-type: none"> <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>- Contoh pengamanan terhadap serangan Remote File Inclusion dari sisi pemrograman</li> <li>- Contoh pengamanan terhadap serangan Remote File Inclusion dari sisi konfigurasi PHP.INI</li> </ul>
	Session 9	<ul style="list-style-type: none"> <li>- SQL Injection union</li> <li>- SQL Injection untuk BYPASS WAF (ADVANCED)</li> <li>- Contoh pengamanan SQL Injection dari sisi pemrograman</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> <li>- Contoh pengamanan pada web login dari SQL Injection dari sisi pemrograman (pengecekan dengan input password)</li> <li>- Contoh pengamanan pada web login dari SQL Injection dari sisi pemrograman (Filter pada input variabel)</li> </ul>
	Session 10	Session 11

- Websploit untuk scan PMA
- PhpMyAdmin Exploitation Advanced
- Ngeroot Linux
- Contoh alur mendapatkan password user dengan akses root dari hasil eksploitasi web yang vulnerable

Mempelajari covering tracks

- Menghapus log server, menghapus history, menghapus php shell dan sebagainya

Pengamanan

- Pengamanan web server dari PHP Shell (Pengujian sebelum diamankan dan setelah diamankan)
- Periksa celah kernel dan update kernel (Mengamankan kernel dari rooting exploit yang sebelum berhasil di rooting)
- Deteksi PHP Shell di web server secara otomatis
- Menonaktifkan Directory Listing
- Mengganti url default URL pada PHPMyadmin
- Instalasi dan konfigurasi WAF (A web application firewall)
- Cara agar SQL Injection khusus bypass WAF tidak mampu bypass WAF
- Pengujian XSS, RFI & SQL Injection (Termasuk SQL Injection yang ditujukan untuk bypass WAF)
- Teknik melakukan banned pada ip attacker secara otomatis yang melakukan serangan brute force pada SSH

	Session 11	<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 di linux</li><li>- Cracking password WPA-PSK dengan semua kemungkinan pada kriteria tertentu di linux (bukan daftar kata yang ada pada file text / wordlist)</li><li>- Hacking password WPA-PSK dengan LINSET</li></ul>
--	------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------