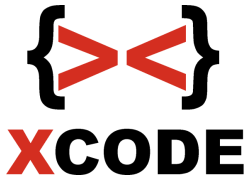


Xcode Intensif Training
Ethical Hacking & Security



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
Performing Basic System Management Tasks		
1	Session 1	<ul style="list-style-type: none"> - Computer Security & IT Security Awareness - Mengenal data & representasinya, hexdump pada file, ascii table, hexwrite - Network Fundamental - Dasar IP Address, Mac Address, pengenalan 7 layer OSI, etc - FTP, SSH, Telnet, DNS, DHCP, Web Server, SMB, POP3, SMTP, MySQL Server, VNC, RDP - Subnetting (CIDR, perhitungan biner ke desimal, perhitungan subnetting, etc) - Routing (NAT) - Port Forwarding - DMZ (Demilitarized Zone) - VPN (Virtual Private Network) - Dasar Kriptografi - Mengenal encode / decode (base64), disertai prakteknya dengan python - Mengenal dasar enkripsi & 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),

		<p>enkripsi dan dekripsi dengan XOR (prakteknya dengan python)</p> <ul style="list-style-type: none"> - Mengetahui enkripsi pada kriptografi asimetris (public key & private key), disertai prakteknya dengan python - Mengetahui fungsi hash disertai prakteknya untuk membangun hashnya dengan python dan cara cracknya dengan menggunakan wordlist - Contoh crack hash MD5 / SHA1 / lainnya dengan Hashcat
2	Session 2	<ul style="list-style-type: none"> - Firewall - Port Knocking - Forwarding pada managed switch - Proxy - TOR Windows - TOR Linux (Advanced) ~ Hacking Server seperti FTP Server, SSH Server, dst dengan koneksi TOR - Command prompt - Manajemen user (Command prompt) - Pembelajaran Shell Bash - Repository - Recovery mode di linux - Setting IP Client di linux (Permanen & non permanen) - Menambah ip baru pada interface

		<ul style="list-style-type: none"> - Managemen user dan group di linux - File Security : chown, chgrp, chmod (numeric coding, letter coding) - SSH Server (user & admin) - Screen - SAMBA (read only, writeable, valid users) - SMB Client - Server APACHE - Firewall ufw <p>Keamanan</p> <ul style="list-style-type: none"> - Mematikan recovery mode pada GRUB - Firewall ufw - Blokir ip ke server dengan firewall ufw <p>Pengawasan</p> <ul style="list-style-type: none"> - Mengenali log-log server dan mengawasi client yang login - IDS (Intrusion detection system) dengan Snort (Linux)
3	Session 3	<ul style="list-style-type: none"> - Ethical Hacking and Countermeasures - Mengenal Vulnerability Assessment & Penetration Test - Strategi, metode & langkah dasar - Scanning jaringan

	<ul style="list-style-type: none">- 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- Scanning IP, port, service, OS yang digunakan, dan sebagainya- Dasar Hacking (Step by step)- Hacking suatu Web Server dengan searchsploit / exploit-db (Step by step)- Shell (eksploitasi di shell seperti copy data)- 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)- Hacking suatu Web Server yang terinstall di Windows 7 (Step by step)- Hacking suatu FTP Server yang terinstall di Windows 10 (Step by step)- Hacking suatu router dengan routersploit- Hacking suatu SSH Server dengan memanfaatkan situs mesin pencari (Step by step)- Hacking suatu FTP Server dengan metasploit framework (Step by step)- Perintah-perintah metasploit dasar dan contoh encode pada payload saat eksploitasi- Backdoor pada target Windows (Tiap target masuk windows, attacker langsung mendapatkan akses)
--	--

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

- Teknik untuk meminimalisir serangan ke server dan pengamanannya secara umum
- Teknik melakukan banned otomatis pada ip target yang melakukan scanning menggunakan NMAP dengan option seperti misal -sV dan -A
- Scanning dan pembangunan komputer lab untuk fuzzing hingga pengembangan exploit
- Mengenal Memory layout
- Buffer Overflow
- Fuzzer Development (Membuat fuzzer sendiri dengan Python)
- EIP & SEH Handler
- Pattern create & pattern offset
- JMP ESP
- Mengenal Bad Character
- Mengenal bahasa mesin, heksadesimal dan x86 assembler instruction set opcode table
- Tabel kebenaran XOR
- Shellcode Development untuk remote (Membuat dengan bahasa assembler dari awal)
- Penggunaan nasm dan objdump untuk shellcode yang dibuat
- Cara penyusunan shellcode secara cepat
- Proof of concept pada exploit yang dibuat
- Shellcode generate dengan encode shikata_ga_nai

		<ul style="list-style-type: none"> - Tugas untuk membuat exploit remote buffer overflow pada suatu web server - Pembahasan tugas pembuatan exploit remote buffer overflow pada web server - SEH (Structured Exception Handling) - Latihan target program yang memiliki proteksi SEH - Cek proteksi SafeSEH / ASLR dan menghindarinya - POP POP RETN (Bypass SEH)
5	Session 5	<ul style="list-style-type: none"> - Scanning IP, port, service, OS dll - Denial of Service - Web Server (intranet & internet). Contoh pada apache server, web dari OS mikrotik dan access point tp-link - Denial of Service - IP Publik (Koneksi internet target down) - Denial of Service SMBv1 - (SMB Windows XP, SMB Windows Server 2003) (Blue Screen) - Denial of Service SMBv2 - (SMB Windows Vista, SMB Windows Server 2008) (Blue Screen) - Denial of Service RDP (RDP Windows 7) - Serangan meningkatkan proses CPU melalui SMB secara cepat di Windows 8 - Denial of Service SMB Windows 7 (Blue Screen) - Windows 8.1 / 10 SMB CLIENT DoS (Blue screen)

	<ul style="list-style-type: none">- Denial of Service Windows 8.1 / 10 pada SMB Service yang memungkinkan share folder tanpa password (Blue Screen)- Denial of Service Windows 2012 / 2016 pada SMB Service yang memungkinkan share folder tanpa password (Blue Screen)- DHCP Flooding- Netcut- ARP Spoofing (Sniffing http / telnet / pop3 / mysql & crack with wordlist / smb & crack with wordlist / ftp / Sniffing isi email (client ke smtp server)- Wireshark- Mengenal HTTPS- Memahami keamanan dari Page URL & Form URL- Sniffing password dengan sertifikat SSL palsu pada HTTPS- Sniffing password dengan SSLStrip- Eksploitasi heartbleed untuk membaca memory dari server yang diproteksi oleh OpenSSL (Bisa mengambil password pengguna pada web dan sebagainya) <p>Pengamanan</p> <ul style="list-style-type: none">- Mengamankan Web Server dari serangan DoS tertentu (Pengujian sebelum diamankan pada serangan sebelumnya dan setelah diamankan) (Linux)- Pengamanan dari serangan ARP Spoofing dan pengamanan lainnya (Linux) <p>Penggantian FTP dengan SFTP</p>
--	---

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

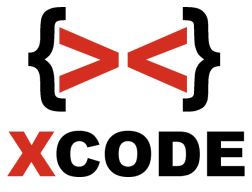
		<ul style="list-style-type: none"> - Membangun wordlist dengan berbagai kriteria sendiri secara cepat (generate) <p>Pengamanan</p> <ul style="list-style-type: none"> - Pengamanan umum - SSH Honeypot - Membatasi jumlah login SSH yang salah <p>Tambahan</p> <ul style="list-style-type: none"> - Cara mendeteksi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

		<ul style="list-style-type: none">- Cross-site scripting (XSS)- Pengamanan XSS dari sisi pemrograman- Scanning XSS - di linux dan windows- Eksploitasi XSS non persistent untuk remote target melalui client side attack (browser ~ metasploit framework)- Eksploitasi XSS persistent untuk menggunakan account target tanpa password login (Mengambil cookie dari target), masukkan ke browser lalu akses account target- Bypass filter upload image dengan tamper data- Pengamanan upload dengan .htaccess- Variasi teknik-teknik bypass filter upload
	Session 8	<ul style="list-style-type: none">- Local File Inclusion- LFI untuk mendapatkan akses PHPMyadmin pada kasus celah pada plugin wordpress- LFI untuk mendapatkan username pada linux- Contoh pengamanan LFI dari sisi programming- Contoh pengamanan LFI dari sisi konfigurasi PHP.INI- WPScan- Admin login scanner (Perl)- Scanning SQL Injection - di Linux dan Windows- Remote File Inclusion

		<ul style="list-style-type: none"> - Scanning RFI - di linux dan windows - PHP Shell Development (Membuat PHP Shell sendiri dari awal untuk RFI) - Remote shell target dengan celah RFI - Bind Shell & Reverse shell - Contoh pengamanan terhadap serangan Remote File Inclusion dari sisi pemrograman - Contoh pengamanan terhadap serangan Remote File Inclusion dari sisi konfigurasi PHP.INI
	<p>Session 9</p>	<ul style="list-style-type: none"> - SQL Injection union - SQL Injection untuk BYPASS WAF (ADVANCED) - Contoh pengamanan SQL Injection dari sisi pemrograman - Havij di Windows - SQLMAP di Linux - SQL Injection pada web halaman login - Contoh pengamanan pada web login dari SQL Injection dari sisi pemrograman (pengecekan dengan input password) - Contoh pengamanan pada web login dari SQL Injection dari sisi pemrograman (Filter pada input variable) - Hacking wordpress secara default pada versi tertentu, bukan pada celah dari plugin atau theme (Mengganti isi content)

		<ul style="list-style-type: none"> - Hacking Joomla secara default pada versi-versi tertentu, bukan pada celah component atau tambahan lainnya (Mengakses shell linux secara langsung dengan reverse shell)
	<p>Session 11</p> <ul style="list-style-type: none"> - Websploit untuk scan PMA - PhpMyAdmin Exploitation Advanced - Ngeroot Linux - Contoh alur mendapatkan password user dengan akses root dari hasil eksploitasi web yang vulnerable <p>Mempelajari covering tracks</p> <ul style="list-style-type: none"> - Menghapus log server, menghapus history, menghapus php shell dan sebagainya <p>Session 10</p> <p>Pengamanan</p> <ul style="list-style-type: none"> - 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) 	

		<ul style="list-style-type: none"> - 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
	<p>Session 11</p>	<ul style="list-style-type: none"> - Dasar Wireless LAN - Mengenal keamanan wireless pada access point - Mac changer - Bypass mac filtering (Deny the stations specified by any enabled entries in the list to access) - Bypass mac filtering (Allow the stations specified by any enabled entries in the list to access) - Bypass SSID Hidden (teori) - Analisa dasar paket wireless untuk mengetahui ip address yang ada di jaringan <p>SSID Flooding</p> <ul style="list-style-type: none"> - Jamming - Hacking WEP - 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
--	--	--