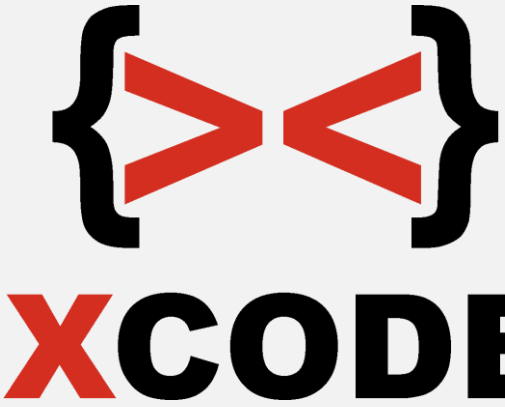
2020



Xcode Intensive Training

Ethical Hacking & Security

XCODE

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.

Jumlah pertemuan : 11x pertemuan.

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.

XCODE

Ethical Hacking & Security

No	Session	Objective
Performing Basic System Management Tasks		
1	Session 1	- 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 subnneting, 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),

		enkripsi dan dekripsi dengan XOR (prakteknya dengan python) - Mengenal enkripsi pada kriptografi asimetris (public key & private key), disertai prakteknya dengan python - Mengenal fungsi hash disertai prakteknya untuk membangun hashnya dengan python dan cara crack nya dengan menggunakan wordlist - Mendeteksi jenis hash secara otomatis dan contoh melakukan cracking dari situs cracking hash - Contoh crack hash MD5 / SHA1 dengan Hashcat
2	Session 2	- 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 - Managemen user (Command prompt) - Pembelajaran Shell Bash - Repository - Recovery mode di linux - Setting IP Client di linux (Permanen & non permanen)

		- Menambah ip baru pada interface - 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 Keamanan - Mematikan recovery mode pada GRUB - Firewall ufw - Blokir ip ke server dengan firewall ufw Pengawasan - Mengenali log-log server dan mengawasi client yang login - IDS (Intrusion detection system) dengan Snort (Linux)
3	Session 3	- Ethical Hacking and Countermeasures - Mengenal Vulnerability Assessment & Penetration Test - Strategi, metode & langkah dasar - Scanning jaringan

		- 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)

		- 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 7 Full Version / Windows 7 SP1 untuk mendapatkan akses shell / meterpreter - Hacking pada service SMB Windows 8.1 / 10 / 2012 / 2016 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)
4	Session 4	- Hacking SAMBA pada suatu target Ubuntu Server untuk mendapatkan akses shell linux (Target Samba dalam kondisi ada yang dishare foldernya tanpa password dengan hak akses writeable) - Hacking pada suatu target FTP server dengan platform linux (Bypass firewall pada target linux) Pengamanan - 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 (Linux)

		- Scanning dan pembangunan komputer lab untuk fuzzing hingga pengembangan expoit - 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 - 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	- 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) - Denial of Service SMB Windows 7 (Blue Screen) - Denial of Service Windows 8.1 / 10 / 2012 / 2016 pada SMB Service yang mengijinkan 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

		- Sniffing password dengan SSLStrip - Eksploitasi heartbleed untuk membaca memory dari server yang diproteksi oleh OpenSSL (Bisa mengambil password pengguna pada web dan sebagainya) Pengamanan - Mengamankan Web Server dari serangan DoS tertentu (Pengujian sebelum diamankan dan setelah diamankan) (Linux) - Mengatasi serangan Netcut di Windows (Pengujian sebelum diamankan dan setelah diamankan) - Pengamanan di linux dari serangan netcut dan serangan sniffing password dengan ARP Spoofing (Pengujian sebelum diamankan dan setelah diamankan)
6	Session 6	- DNS Spoofing - Membuat fake login sendiri - Client side Attack ~ Browser IE atau firefox - Eksploitasi celah remote pada Microsoft Word 2010 / 2013 / 2016) - Bypass password login masuk windows 7 dan 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) - 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 - Cara mendapatkan password login windows 7 / 8 secara langsung dengan akses administrator (Mengambil dari memory, bukan brute force) - Cara mendapatkan password login pada Linux Ubuntu Desktop secara langsung dengan akses root (Mengambil dari memory, bukan brute force) - John the ripper pada Windows - John the ripper pada Linux - Brute force attack dengan wordlist (VNC / telnet / ftp / pop3 / http / mysql / rdp / ssh / vnc / samba linux) - Membangun wordlist dengan berbagai kriteria sendiri secara cepat (generate) Pengamanan - Pengamanan umum - SSH Honeypot (Linux) Tambahan : - Cara mendeteksi SSH Honeypot
7	Session 7	- 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 - Scan untuk mendeteksi nama web server yang digunakan serta versinya, sistem operasi apa yang digunakan, jika menggunakan PHP maka menggunakan PHP versi berapa, jika menggunakan CMS maka apa nama CMS yang digunakan, jika CMS wordpress maka versi berapa wordpressnya dan sebagainya - Whois - Reverse domain - Teknik-teknik bypass cloudflare - Scanning sub domain - Google hacking - Google hacking untuk kasus-kasus khusus (mendapatkan file-file dari folder yang terbuka,dst) - Mencari situs sesuai kriteria dengan cepat pada bing (Menampilkan semua yang dicari dalam 1 halaman) - Mencari halaman login admin (Secara otomatis mencari halaman web login admin berdasarkan dengan mencoba-coba nama-nama file halaman login admin yang umum) - Dirbuster - Dirsearch - Dirhunt - Mendeteksi Web Application Firewall pada website- Memahami Get Method & post method - Cross-site scripting (XSS)

		- Pengamanan XSS dari sisi pemrograman - Scanning celah XSS di linux - Eksploitasi XSS persistent untuk menggunakan account target tanpa password login (Mengambil cookie dari target), masukkan ke browser lalu akses account target
	Session 8	- Remote File Inclusion Contoh alur mendapatkan password user dengan akses root dari hasil eksploitasi web yang vulnerable - Scanning celah RFI di linux - Remote shell target dengan celah RFI - Bind Shell & Reverse shell - Ngeroot linux - Contoh pengamanan terhadap serangan Remote File Inclusion dari sisi pemrograman - Contoh pengamanan terhadap serangan Remote File Inclusion dari sisi konfigurasi PHP.INI - Bypass filter upload image dengan tamper data - Bypass filter upload image dengan Burp Suite - Pengamanan upload dengan .htaccess - Variasi teknik-teknik bypass filter upload - Local File Inclusion - LFI untuk mendapatkan akses PHPMyadmin pada kasus celah pada plugin wordpress

		- Scanning celah LFI - LFI untuk mendapatkan username pada linux - Contoh pengamanan LFI dari sisi programming - Contoh pengamanan LFI dari sisi konfigurasi PHP.INI - WPScan - PHP Shell Development (Membuat PHP Shell sendiri dari awal untuk RFI)
	Session 9	- Scanning celah SQL Injection di Linux - SQL Injection union - Havij di Windows - SQLMAP di Linux - SQL Injection - bypass login wp - PHP upload & logger Login - 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 variablel) - Contoh pengamanan SQL Injection dari sisi pemrograman - SQL Injection untuk BYPASS WAF (ADVANCED)

		- Hacking untuk mendapatkan akses shell dengan memanfaatkan celah shellsock - Hacking wordpress secara default pada versi tertentu, bukan pada celah dari plugin atau theme (Mengganti isi content) - Hacking Joomla secara default pada versi-versi tertentu, bukan pada celah component atau tambahan lainnya (Mengakses shell linux secara langsung dengan reverse shell)
	Session 10	- Websploit untuk scan PMA - PhpMyAdmin Exploitation (Advanced) Mempelajari covering tracks - Menghapus log server dan menghapus history Pengamanan - Pengamanan web server dari PHP Shell (Pengujian sebelum diamankan dan setelah diamankan) (Linux) - Periksa celah kernel linux dan update kernel (Mengamankan kernel dari rooting exploit yang sebelum berhasil di rooting) - Deteksi PHP Shell di web server secara otomatis (Linux) - Menonaktifkan Directory Listing (Linux) - Mengganti url default URL pada PHPMyadmin (Linux) - PHPMyadmin Honeypot (di linux)

		- Teknik melakukan banned pada ip attacker secara otomatis yang melakukan serangan brute force pada SSH (Linux) - Instalasi dan konfigurasi WAF (A web application firewall) (Linux) - Cara agar SQL Injection khusus bypass WAF tidak mampu bypass WAF (Linux) - Pengujian pengamanan maksimal pada WAF untuk serangan XSS, RFI & SQL Injection (Termasuk serangan SQL Injection untuk bypass WAF)
	Session 11	- 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) - SSID Flooding - 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