2024

XCODE

Ethical Elite Hacker v9

X-code Platinum Training (Online)

Ethical Elite Hacker v9

Pembelajaran teknik-teknik network hacking, web hacking, wireless hacking, serta melakukan safe guard dan defense. Selain itu juga bisa melakukan exploit development, penetration testing dan server security hardening.

Waktu Training: 20x pertemuan.

Objectives : Dengan Menyelesaikan training ini diharapkan peserta bisa melakukan teknik-teknik network hacking, web hacking, wireless hacking, serta melakukan safe guard dan defense. Selain itu juga bisa melakukan exploit development, penetration testing dan server security hardening.

X-code Platinum Training (Online)

Ethical Elite Hacker v9

No	Session	Objective
Performing Basic System Management Tasks		
1	Session 1	Sesi 1 - Computer Security & IT Security Awareness - Mengenal data & representasinya, hexdump pada file, ascii table, hexwrite - File Signature / Magic Number (pengenal file) - Network Fundamental - Dasar IP Address - ARP (Address Resolution Protocol) - MAC Address - Pengenalan 7 layer OSI - Subnetting (CIDR, perhitungan biner ke desimal, perhitungan subnneting, etc) - FTP (File Transfer Protocol) - SSH (Secure Shell) - Telnet (Teletype Network) - DNS (Domain Name System)

		- DHCP (Dynamic Host Configuration Protocol) - HTTP Server - SMB (Server Message Block) - POP3 (Post Office Protocol) - SMTP (Simple Mail Transfer Protocol) - MySQL Server - The Remote Framebuffer Protocol (RFB) - RDP (Remote Desktop Protocol) - Routing (NAT) - Port Forwarding - DMZ (Demilitarized Zone) - VPN (Virtual Private Network)
2	Session 2	Sesi 2 - Dasar Kriptografi - Mengenal encode / decode (base64) beserta perhitungannya - Melihat kasus PHPShell yang diencode dengan Base64 - Encode & decode Base64 disertai prakteknya dengan python - Mengenal dasar enkripsi & dekripsi pada kriptografi - Enkripsi 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 cracknya dengan menggunakan wordlist - Mendeteksi jenis hash secara otomatis dan contoh melakukan cracking dari situs cracking hash - Contoh crack hash MD5 dengan Hashcat - Contoh crack hash SHA1 dengan Hashcat - Mengenal reverse engineering dengan contoh prakteknya (source code, compile, binary (executable), disassembly & mendapatkan password pada contoh program login linux - Mengenal reverse engineering dengan contoh prakteknya (source code, compile, binary (executable), disassembly & mendapatkan password pada contoh program login windows - Firewall - Port Knocking - Forwarding pada managed switch - Proxy - TOR Windows

		- TOR Linux (Advanced) ~ Cara scan target agar terdeteksinya ip dari TOR - TOR Linux (Advanced) ~ Hacking Server seperti FTP Server koneksi TOR - SSH Tunnel
3	Session 3	Sesi 3 - 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 - Server Nginx

		Keamanan - Mematikan recovery mode pada GRUB - Firewall ufw - Blokir ip ke server dengan firewall ufw - Blokir semua ip client kecuali ip client tertentu pada port service tertentu (Kasusnya misal seperti website hanya bisa dibuka ip tertentu atau juga bisa misal untuk akses ssh hanya bisa diakses ip tertentu, tapi untuk web bisa diakses semua ip yang bisa terhubung) Pengawasan - Mengenali log-log server dan mengawasi client yang login - IDS (Intrusion detection system) dengan Snort (Linux)
4	Session 4	Sesi 4 - Instalasi Ubuntu Server 20.04.3 LTS - Instalasi Apache Server & MySQL Server di Ubuntu Server 20.04.3 LTS - Root pada MYSQL diberikan password - Instalasi PHPMyadmin di Ubuntu Server 20.04.3 LTS - Instalasi Wordpress di Apache Server di Ubuntu Server 20.04.3 LTS - Mengganti halaman login wordpress - Setting virtualhost di Apache Server di Ubuntu Server 20.04.3 LTS

		- Implementasi dengan DNS Server - Log Server pada Apache di Ubuntu Server 20.04.3 - Install Nginx & MySQL Server di Ubuntu Server 20.04.3 LTS - Log Server pada Nginx di Ubuntu Server 20.04.3 LTS - Instalasi wordpress di Nginx di Ubuntu Server 20.04.3 LTS - Setting virtualhost di Nginx di Ubuntu Server 20.04.3 LTS - Setting ip address dengan netplan - Menambah ip baru dengan netplan - Instalasi dan konfigurasi DNS Server di Ubuntu Server 20.04.3
5	Session 5	Sesi 5 - Ethical Hacking - 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 - CVE dan situs-situs penyedia exploit - 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 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 router dengan routersploit - Hacking suatu SSH Server dengan memanfaatkan situs mesin pencari (Step by step) - Hacking Apache Server 2.4.49 untuk mendapatkan akses shell (cgi-bin nyala) - Hacking pada web server memanfaatkan celah log4shell untuk mendapatkan akses shell - Hacking suatu FTP Server di Windows 10 dengan memodifikasi shellcode (Dari X-code Premium Video) - 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 berfirewall (Bypass firewall pada target Windows) (Step

		by step) untuk mendapatkan akses meterpreter / shell - Scanning dengan OpenVAS (Dari X-code Premium Video) - Hacking pada service SMB Windows Vista / Windows Server 2008 (Dari X-code Premium Video) - Hacking pada service SMB Windows 7 SP1 untuk mendapatkan akses shell / meterpreter - 32 bit
6	Session 6	Sesi 6 - Hacking pada service SMB Windows 7 SP1 untuk mendapatkan akses meterpreter - 32 bit untuk melihat camera webcam - Hacking pada service SMB Windows 7 SP1 untuk mendapatkan akses shell / meterpreter - 64 bit - Hacking pada service SMB Windows Server 2008 R2 Enterprise untuk mendapatkan akses shell - Hacking pada service SMB Windows 8.1 / 10 / 2012 R2 yang mengijinkan share folder tanpa password untuk mendapatkan akses shell (Bypass Windows Defender) - Hacking pada service SMB Windows 10 memanfaatkan celah CVE-2020-0796 (SMBGhost) untuk mendapatkan akses shell - Hacking Mikrotik Router v6 pada service winbox (6.29 to 6.42) (Langsung mendapatkan password mikrotik melalui jaringan, bukan brute force) - 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 di linux pada ip target yang melakukan scanning menggunakan NMAP dengan option seperti misal -sV dan -A (Linux)
7	Session 7	Sesi 7 - Scanning dan pembangunan komputer lab untuk fuzzing hingga pengembangan expoit - Mengenal Memory layout - Buffer Overflow - Membuat program Fuzzer dengan python - Pattern create & pattern offset - Extended Instruction Pointer - Extended Stack Pointer - NOPSleed - Mengenal Bad Character - Implementasi shellcode bind shell - Proof of concept pada exploit yang dibuat - Mengenal Bad Character - 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 - Proof of concept pada exploit yang dibuat - Shellcode generate dengan encode shikata_ga_nai - SEH (Structured Exception Handling) - SafeSEH (Safe Structured Exception Handling) - Bypass SEH (Structured Exception Handling) - Bypass SafeSEH (Safe Structured Exception Handling) - Tugas untuk membuat exploit remote buffer overflow pada suatu web server
8	Session 8	Sesi 8 - Pembahasan tugas pembuatan exploit remote buffer overflow pada web server – ASLR (Address Space Layout Randomization) – Bypass ASLR (Address Space Layout

		Randomization) - Mengenal Jump Short – Generate reverse shell (bypass firewall) untuk dipasang pada exploit. - Contoh membuat exploit dari awal pada suatu aplikasi yang berjalan di Windows 10 - Uji coba perbedaan module yang terproteksi dan yang tidak terproteksi ASLR - Mengenal Egg Hunter - Implementasi Egg Hunter dengan shellcode DEP - Mengenal proteksi DEP (Data Execution Prevention) - Menghadapi mitigasi DEP dengan hasil generate ROP pada *.DLL - Membangun exploit untuk metasploit berdasarkan exploit python yang dibuat sebelumnya. Contoh Buffer overflow di linux - Gdb & belajar perintah-perintah GDB (list main, disasmain) - Fuzzing dengan GDB (seg fault) & memeriksa alamat eip - PoC untuk menjalankan shellcode dari menghitung jumlah byte shellcode, nop dan jumlah alamat yang diinjeksikan - Menjalankan exploit buffer overflow di shell (Terminal bukan di gdb)

		- Implementasi shellcode bind shell linux - PoC bypass ASLR pada target Linux (Video)
9	Session 9	Sesi 9 – Data Execution Prevention (DEP) – Return-oriented programming – Pemanfaatan EDI, ESI, EBP, ESP dalam bypass DEP – Bypass Data Execution Prevention (DEP) dengan Return-oriented programming (ROP) – Manual (Tidak pakai generate) - Denial of Service - Web Server. Contoh pada apache server, web server Nginx, web dari OS mikrotik, router ZTE dan access point tp-link - Serangan cara membuat semua komputer dalam 1 jaringan lokal terputus koneksinya secara cepat. - (Dari X-code Premium Video) - 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) - Serangan membuat CPU pada Windows 8 menjadi naik - Denial of Service Windows 8.1 / 10 / 2012 R2 / 2016 pada SMB Service yang mengijinkan share folder tanpa

		password (Blue Screen) - Denial of Service SMB Windows 10 pada celah CVE2020-0796 (Blue screen)
10	Session 10	Sesi 10 - Netcut - ARP Spoofing - Wireshark - MITM user & pass ip camera (Sniffing). - Hacking Server IP Camera untuk melihat isinya (MITM) - (Dari X-code Premium Video) - MITM user & pass router (sniffing) TP-Link. - Sniffing isi e-mail yang dikirim ke SMTP server dan sniffing username dan password POP3 - (Dari X-code Premium Video) - Sniffing hash samba di jaringan dan melakukan crack (Dari X-code Premium Video) - Sniffing password dengan SSLStrip - Eksploitasi heartbleed untuk membaca memory dari server yang diproteksi oleh OpenSSL (Bisa mengambil password pengguna pada web dan sebagainya) Pengamanan - 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) - Cookie stealing dengan MITM (Cain + Wireshark) untuk bypass login web tanpa memasukkan password (Session Hijacking) - DNS Spoofing - Membuat fake login sendiri - Client side Attack ~ Browser IE (Windows XP/Windows 7) / Client side Attack ~ Browser Firefox (Windows XP)
11	Session 11	Sesi 11 - Bypass login Windows 7 / 8.1 / 10 / 11 / Server 2022 / dengan reset password - Eksploitasi celah remote pada Microsoft Word 2010) - (Dari X-code Video Premium) - Eksploitasi celah remote pada Microsoft Word 2013 / 2016) - Eksploitasi akses remote pada Microsoft Word 2019 di Windows 11 memanfaatkan MSDT (CVE-2022-30190) - Msfvenom untuk backdoor Windows (Backdoor di inject kan ke file exe lain) - Membangun backdoor untuk remote Windows 10 dan bypass antivirus internal Windows 10 (Windows Defender) - 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 - Privilege escalation Windows 10 1909 / Windows Server 2019 - Mengenal Linpeas (X-code Video) - Privilege escalation pada Ubuntu 20.04.1 pada celah SUDO - Privilege escalation pada Ubuntu 18.04.1 LTS / privilege escalation Ubuntu 19.04 / Privilege escalation pada Linux Mint 19 / privilege escalation pada MX Linux 18.3 / privilege escalation Manjaro linux 18.1 / Privilege escalation pada CentOS 8 - Privilege escalation pada CentoS 7 - Privilege escalation pada FreeBSD 12.1 - Privelege escalation pada OpenBSD 6.6 - Privilege escalation pada ubuntu 20.04.2 LTS kernel 5.8 - Update Kernel Ubuntu 20.04.2 LTS versi 5.4 ke kernel baru (Di x-code video) - Privilege escalation pada ubuntu server 20.04.3 LTS pada celah polkit (exploit dari bulan Januari 2022) - Pengamanan pada ubuntu server 20.04.3 LTS pada celah polkit (exploit dari bulan Januari 2022) - Privilege Escalation pada target linux memanfaatkan celah CVE-2022-0847
12	Session 12	Sesi 12 - 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) - Cara mendapatkan NTLM hash windows 10 dengan akses administrator (Mengambil dari memory), lalu crack NTLM hashnya dengan hashcat (brute force) - Crack password Windows dengan John the ripper - Crack password Linux dengan John the ripper - Brute force attack dengan wordlist (VNC / telnet / ftp / pop3 / http / mysql / rdp / ssh / vnc / samba linux) - Brute force dengan menggunakan proxy agar ip address attacker tidak terkena log (Dari X-code Premium Video) - Membangun wordlist dengan berbagai kriteria sendiri secara cepat (generate) Pengamanan - Pengamanan umum - SSH Honeypot (Linux) - Membatasi jumlah login SSH yang salah (Linux) - Port Knocking pada SSH (Linux) Tambahan - Cara mendeteksi SSH Honeypot - 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. - Managemen user pada MySQL - 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
13	Session 13	Sesi 13 - 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 - Scan lebih dalam untuk mendapatkan versi pada suatu CMS, untuk kasus jika tidak terdeteksi menggunakan salah satu tool dari bawaan kali linux - 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 - Advanced XSS untuk target di windows tidak jalan tapi di linux jalan (XSS untuk Pop up a JavaScript alert() dan redirect). - Variasi teknik-teknik injeksi pada target dengan celah XSS - Eksploitasi XSS persistent untuk menggunakan akun target tanpa password login (Mengambil cookie dari target), masukkan ke browser lalu akses akun target - Memahami keamanan cookie dengan mengenal session cookie httponly dan session cookie secure - Bypass filter upload image dengan burp suite - Pengamanan upload dengan .htaccess - Variasi teknik-teknik bypass filter upload - Cross-Site Request Forgery (CSRF)

14	Session 14	Sesi 14 - Remote File Inclusion - WPScan - Scanning celah RFI di linux - Contoh alur mendapatkan akses root dari hasil eksploitasi web yang vulnerable - Remote shell target dengan celah RFI - Bind Shell & Reverse shell - Ngeroot Linux - Menambah user dan menjadikan user menjadi admin dari reverse shell - Membuat backdoor (binary) linux dan memasangnya di crontab untuk reverse shell - Crack password dengan john the ripper - Mengambil username dan password linux dari memory (Target : Ubuntu Desktop) - Menyisipkan backdoor upload ke file php dan memasang backdoor php shell - Teknik-teknik melacak backdoor dengan cepat (Backdoor php, backdoor akun, netstat, dst) - Cara membuat backdoor PHP lebih sulit dilacak - Cara melacak backdoor PHP jika sulit dilacak - Cara melacak backdoor di user dengan akses berbahaya di database secara otomatis

		- Cara melacak log perintah yang diketikkan attacker yang berhasil masuk di server linux dengan ACCT melalui web - Cara attacker menghapus jejak log di server dari program ACCT - Contoh pengamanan terhadap serangan Remote File Inclusion dari sisi pemrograman - Contoh pengamanan terhadap serangan Remote File Inclusion dari sisi konfigurasi PHP.INI - Local File Inclusion - LFI untuk mendapatkan akses PHPMyadmin pada kasus celah pada plugin wordpress - Scanning celah LFI di linux - LFI untuk mendapatkan username pada linux - Contoh pengamanan LFI dari sisi programming - Contoh pengamanan LFI dari sisi konfigurasi PHP.INI - Variasi teknik-teknik injeksi pada target dengan celah LFI - Cara mendapatkan akses shell dari LFI dengan reverse shell - WPScan for brute force (Advanced) ~ Username Enumeration + crack password (Wordlist) - PHP Shell Development (Membuat PHP Shell sendiri dari awal untuk RFI) - Command Injection dan teknik-teknik variasinya

15	Session 15	Sesi 15 - IDOR (Insecure Direct Object References) - Scanning celah SQL Injection di linux - SQL Injection union (MANUAL) - BLIND SQL Injection (MANUAL) - TIME BASED SQL Injection (MANUAL) - Havij di Windows - SQLMAP di Linux hingga crack hash password login dengan brute force - SQLMAP di Linux untuk masuk ke akses phpmyadmin - Contoh pengamanan SQL Injection dari sisi pemrograman - 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 (Filter pada input variablel) - Contoh pengamanan pada web login dari SQL Injection dari sisi pemrograman (pengecekan dengan input password)
16	Session 16	Sesi 16 - Instalasi dan konfigurasi WAF (A web application

		firewall) - SQL Injection untuk BYPASS WAF (ADVANCED) - XSS redirect url untuk BYPASS WAF (ADVANCED) - Brute force dengan Burp Suite - Hacking untuk mendapatkan akses shell dengan memanfaatkan celah shellsock - Hacking Laravel 8 (Debug Mode) untuk mendapatkan akses shell (Linux) - Hacking wordpress secara default pada versi tertentu, bukan pada celah dari plugin atau themes (Mengganti isi content) - Hacking Joomla secara default pada versi-versi tertentu, bukan pada celah component atau tambahan lainnya (Mengakses shell linux) - Hacking Joomla 4 untuk masuk ke database target - CVE-2023-23752 - Websploit untuk scan PMA - PhpMyAdmin Exploitation (Advanced) Covering tracks - Menghapus log server dan menghapus history.
17	Session 17	Sesi 17 Pengamanan - Pengamanan web server dari PHP Shell (Pengujian sebelum diamankan dan setelah diamankan) (Linux) - Eksploitasi PHP 7 (bypass disable_function &

		open_basedir) serta pengamanannya) - Exploit reverse shell dengan memanfaatlah celah PHP 7 (Menggunakan metasploit) - Hacking untuk mendapatkan akses reverse shell pada PHP 8 dan versi 7 (All version) saat tidak diamankan lebih lanjut, selain itu juga sekaligus cara pengamanannya. (Cara 1) - Eksploitasi memanfaatkan GCC untuk compile exploit lalu hasil compile dijalankan lewat PHP. - Hacking untuk mendapatkan akses reverse shell pada PHP 8 dan versi 7 (All version) saat tidak diamankan lebih lanjut, selain itu juga sekaligus cara pengamanannya. (Cara 2) - Exploit dari bulan Oktober 2021 - Hacking untuk mendapatkan akses reverse shell pada PHP 8 dan versi 7 (All version) saat tidak diamankan lebih lanjut, selain itu juga sekaligus cara pengamanannya. (Cara 3) - Exploit dari bulan Januari 2022 - 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) – Ubuntu - Menonaktifkan Directory Listing (Linux) – Ubuntu Server baru

		- Mengganti url default URL pada PHPMyadmin (Linux) - PHPMyadmin Honeypot (Di linux) - Instalasi dan konfigurasi WAF (A web application firewall) (Linux) - Cara agar teknik 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) - Teknik melakukan banned pada ip attacker secara otomatis yang melakukan serangan brute force pada SSH (Linux)
18	Session 18	Sesi 18 - Pertahanan dengan cloudflare - Setting name servers di domain dengan name server dari cloudflare - Set SSL / TLS encryption mode is Full (Strict) - pengamanan dengan cloudflare origin CA certificate on the server - Under Attack Mode di cloudflare - Setting virtualhost di web server - 2 Teknik bypass ip cloudflare disertai pengamanannya - Teknik agar web tidak bisa diakses lewat ip - Log pada web server jika diakses lewat domain / subdomain

19	Session 19	Sesi 19 - Dasar Wireless LAN - Mengenal keamanan wireless pada access point - Macchanger - 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) - Cara sniffing SSID Hidden pada hotspot target dengan airodump-ng. (Dari X-code Premium Video) - Cara melakukan SSID flooding di hotspot. (Dari Xcode Premium Video) - Jamming (User yang terkoneksi ke hotspot mengalami terputus koneksi) - Hacking WEP (Wired Equivalent Privacy) - 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) - Cracking password WPA-PSK dengan GPU/APU - Hacking password WPA-PSK melalui WPS (tidak sampai 1 menit - tidak semua AP bisa)

		- Hacking password WPA-PSK dengan LINSET
20	Session 20	Sesi 20 - The Penetration Testing Execution Standard - Dasar Pentest - Pre-engagement Interactions - General Questions - Penetration testing offers - Intelligence Gathering - OSINT - Threat Modeling - Vulnerability Analysis - Testing - Exploitation - CVSS Score - Post Exploitation - Vulnerability impacts and risks - Recommendation - Reporting