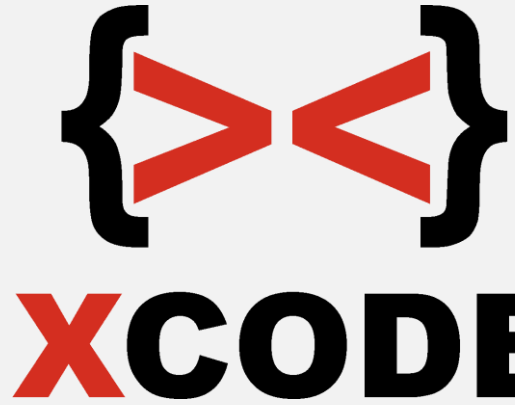
2026



Penetration Tester & Cyber Security Engineer

Bootcamp 2026 v7

2026

XCODE

X-code Bootcamp 2026 (Online)

Penetration Tester & Cyber Security Engineer v7.1

Penetration Tester (atau yang sering disebut **Ethical Hacker**) adalah seorang profesional keamanan siber yang bertugas untuk menguji dan mengevaluasi sistem, jaringan, aplikasi, dan infrastruktur TI organisasi dengan tujuan untuk menemukan kerentanannya sebelum para peretas jahat dapat mengeksploitasinya. Penetration tester melakukan serangkaian uji coba dan teknik untuk mensimulasikan serangan dunia nyata, memberikan wawasan kepada organisasi tentang potensi kelemahan yang ada dalam sistem mereka.

- Pengetahuan Mendalam tentang Keamanan Jaringan dan Sistem:
- Kemampuan Menggunakan Alat Pengujian Keamanan:
- Menguasai alat dan teknik untuk pengujian penetrasi, seperti: Kali Linux (sistem operasi yang dilengkapi dengan berbagai alat pengujian penetrasi).
- Pemrograman dan Scripting:
- Pemahaman tentang Sistem Operasi:
- Keahlian dalam Pengujian Aplikasi Web:
- Kemampuan Analisis dan Pemecahan Masalah:
- Mengidentifikasi masalah umum dalam kode aplikasi dan mencari cara untuk mengeksploitasi celah tersebut.

Cyber Security Engineer adalah profesional yang bertanggung jawab untuk merancang, mengimplementasikan, mengelola, dan memelihara sistem keamanan yang melindungi infrastruktur dan data organisasi dari ancaman dunia maya. Peran ini sangat penting untuk menjaga kerahasiaan, integritas, dan ketersediaan data serta sistem yang digunakan oleh perusahaan atau organisasi.

Apa saja yang dipelajari?

- Belajar pengetahuan Mendalam tentang Keamanan Jaringan: Paham tentang konsep dasar dan teknik perlindungan seperti firewall, dan enkripsi.
- Pemrograman dan Scripting: Kemampuan dalam bahasa pemrograman seperti Python dan Bash untuk membangun alat dan skrip keamanan.
- Kemampuan Analisis dan Penanggulangan Insiden: Mampu mendeteksi dan menganalisis ancaman serta merespons insiden dengan cepat.
- Keamanan Aplikasi dan Sistem: Pengalaman dalam pengujian penetrasi, analisis kerentanannya, dan menerapkan patch keamanan.
- Pengetahuan tentang Alat Keamanan: Familiaritas dengan berbagai alat dan perangkat lunak keamanan seperti IDS dan antivirus.

Waktu Bootcamp: 30x sesi zoom

Materi yang Dipelajari:

Alur Penetration Testing Lengkap (End-to-End Pentest Management):

- **Pra-Engangement & Legalitas:** Penyusunan proposal teknis dan finansial, pembuatan *Non-Disclosure Agreement* (NDA) untuk kerahasiaan data, penyusunan kontrak kerja (*Rules of Engagement*), dan penentuan ruang lingkup (*Scoping*).
- **Fase Eksekusi:** *Information Gathering*, *Vulnerability Assessment*, *Exploitation*, hingga *Post-Exploitation*.
- **Pelaporan (Reporting):** Penyusunan *Executive Summary* (laporan non-teknis untuk manajemen/C-Level) dan *Technical Report* (laporan detail, bukti eksploitasi, beserta langkah reproduksi untuk tim developer).
- **Manajemen Bisnis Keamanan:** Manajemen risiko, penentuan skor keparahan temuan menggunakan *Common Vulnerability Scoring System* (CVSS), serta komunikasi profesional dengan klien.

 Mode Penetration Testing (Pentest Modes):

- **Black-box Testing:** Simulasi serangan dari sudut pandang peretas luar tanpa informasi awal mengenai infrastruktur, kode sumber, atau arsitektur jaringan target.
- **Gray-box Testing:** Simulasi serangan dengan informasi terbatas, seperti memiliki akses akun pengguna biasa (*low-privilege*) atau dokumentasi arsitektur parsial untuk menguji eskalasi hak akses.

Eksploitasi Web Jaringan & Aplikasi (Web Exploitation & Mitigation):

- **Cross-Site Scripting (XSS):** Eksploitasi dan mitigasi *Stored XSS*, *Reflected XSS*, serta *DOM-based XSS*.
- **File Inclusion:** Eksploitasi *Local File Inclusion* (LFI) untuk membaca berkas sensitif sistem dan *Remote File Inclusion* (RFI) untuk mengeksekusi kode dari server luar.
- **SQL Injection (SQLi):** Teknik *In-band* (Union-based), *Inferential* (Boolean-based Blind, Time-based Blind).
- **Command Injection:** Injeksi perintah sistem operasi melalui input aplikasi web yang tidak divalidasi.
- **Cross-Site Request Forgery (CSRF):** Memanipulasi browser korban untuk mengeksekusi tindakan yang tidak diinginkan pada situs tempat mereka terautentikasi.
- **Server-Side Request Forgery (SSRF):** Memaksa server target melakukan permintaan HTTP ke jaringan internal (*Intranet*) atau layanan pihak ketiga yang terisolasi.
- **Clickjacking (UI Redressing):** Teknik penipuan manipulasi klik menggunakan lapisan transparan.

- **Race Condition:** Eksploitasi celah waktu pada proses multi-threading untuk manipulasi data.
- **Mitigasi Komprehensif:** Penerapan *Input Validation*, HTTP Security Headers dan sebagainya.

Kegagalan Autentikasi & Manajemen Sesi (Broken Authentication & Session Management):

- **Injeksi & Kebocoran Sesi:** Pemanfaatan SQL Injection untuk bypass login, serta *XSS Cookie Theft* (pencurian cookie sesi menggunakan skrip jahat).
- **Insecure Direct Object References (IDOR):** Manipulasi parameter ID atau URL untuk mengakses data milik pengguna lain tanpa otorisasi.
- **Bypass Multi-Factor Authentication (2FA Bypass):** Contoh teknik melewati proteksi OTP.
- **Session Hijacking via MITM:** Penyadapan token sesi aktif melalui serangan *Man-in-the-Middle* pada jaringan yang tidak aman.
- **Privilege Escalation & Account Takeover:** Menaikkan hak akses dari pengguna biasa menjadi admin (*Horizontal & Vertical Privilege Escalation*), serta pengambilalihan akun secara penuh melalui *Credential Stuffing* (otomatisasi tebakan kata sandi hasil kebocoran data).
- **JSON Web Token (JWT) Manipulation:** Eksploitasi kelemahan JWT.

SIEM & Log Analysis (Security Information and Event Management):

- **Instalasi & Konfigurasi:** Proses implementasi platform SIEM menggunakan **Wazuh** (Wazuh Manager, Indexer, dan Dashboard) serta pemasangan *Wazuh Agent* pada endpoint target.
- **Deteksi Serangan Siber:** Pembuatan *rules* dan *decoders* untuk mendeteksi serangan *Brute-Force*, aktivitas pemindaian web, eksploitasi celah keamanan, hingga deteksi perubahan file sistem secara *real-time* (*File Integrity Monitoring* / FIM).

Kerangka Kerja Keamanan Terkini:

- **OWASP Top 10 2025:** Mempelajari dan membedah sepuluh risiko keamanan aplikasi web paling kritikal standar industri terbaru, mulai dari *Broken Access Control*, *Cryptographic Failures*, hingga kategori ancaman terbaru yang relevan dengan tren teknologi saat ini.

Penetration Testing pada API (API Pentest):

- **Authentication Bypass:** Menembus proteksi token atau kunci API yang tidak divalidasi dengan benar di sisi server.

- **Input Validation Flaws:** Eksploitasi parameter pada endpoint API yang rentan terhadap *injection* atau manipulasi data masukan.
- **REST API Exploitation:** Analisis arsitektur REST, pemetaan endpoint tersembunyi (*API Documentation Leaks*), dan pengujian metode HTTP.

Teknik Melewati Pengaman Web (WAF Bypass):

- **XSS & SQLi WAF Bypass:** Teknik mengelabui deteksi *Web Application Firewall*, pemanfaatan celah logika pada aturan (rules) WAF.

Keragaman Teknologi Target (Multi-Platform Targets):

- **PHP & Node.js Environment:** Pengujian tidak terbatas pada arsitektur monolitik PHP tradisional, melainkan mencakup ekosistem modern berbasis **Node.js**.

Pengembangan Eksploitasi Tingkat Rendah (Exploit Development):

- **Buffer Overflow (BOF):** Teknik membanjiri memori *stack* untuk mengambil alih register *Extended Instruction Pointer* (EIP/RIP) guna mengontrol alur eksekusi program.
- **Structured Exception Handling (SEH) Exploitation:** Memanfaatkan mekanisme penanganan *error* pada Windows untuk mengeksekusi kode buatan sendiri.
- **Mitigasi & Proteksi OS Bypass:** Teknik menembus proteksi modern seperti **SafeSEH**, **ASLR** (*Address Space Layout Randomization* - pengacakan alamat memori), dan **DEP/NX** (*Data Execution Prevention / No-Execute* - memori non-eksekusi).
- **Advanced Shellcode Placement:** Penggunaan teknik **Egghunter** (pencari kode di memori) dan instruksi **Jumpshort** untuk melompat ke alamat *shellcode* yang terbatas fungsinya.

Fuzzing & Eksploitasi Biner (Fuzzing & Exploitation):

- **Bug Finding:** Menggunakan teknik otomatisasi pengiriman data acak (*Fuzzing*) menggunakan *tools* khusus untuk mencari celah kerusakan memori (*crash/memory corruption*).
- **Shellcode Execution:** Proses injeksi dan pengeksekusian perintah *shell* langsung pada arsitektur sistem operasi Windows dan Linux.

Pembuatan Eksploitasi Kustom (Custom Exploit & Payload Engineering):

- **Custom Exploit Development:** Menulis skrip eksploitasi mandiri menggunakan bahasa pemrograman Python.

- **Custom Shellcode:** Pembuatan kode instruksi mesin tingkat rendah menggunakan Bahasa Assembly (asm).
- **Payload Generation:** Membuat dan mengonfigurasi koneksi *Bind Shell* (server membuka port) dan *Reverse Shell* (target menghubungi balik penyerang) menggunakan framework **MSFvenom**.

Eskalasi Hak Akses Sistem (Privilege Escalation):

- **Linux & BSD Privilege Escalation:** Eksploitasi kerentanan pada level **Kernel** (OS *exploit*), penyalahgunaan hak akses perintah **Sudo** (*Sudoers misconfiguration*), eksploitasi kerentanan komponen keamanan sistem seperti **Polkit** (PolicyKit), serta pemanfaatan salah konfigurasi hak akses file (*SUID/SGID binaries, writable cronjobs*).

Serangan Infrastruktur Jaringan (Network Attack & Reconnaissance):

- **ARP Spoofing & Sniffing:** Manipulasi tabel ARP untuk memposisikan diri di tengah lalu lintas data jaringan guna menyadap informasi sensitif (*cleartext credentials*).
- **Network Exploitation:** Serangan *Brute-Force* massal pada protokol remote (SSH, RDP, FTP), eksekusi serangan *Denial of Service* (DoS), eksploitasi kerentanan *firmware* perangkat Router, hingga eksploitasi celah keamanan pada kamera pengawas berbasis IP (*IPcam Exploitation*).

Pemindaian & Framework Eksploitasi Otomatis (Nessus & Metasploit):

- **Nessus Vulnerability Scanner:** Mengonfigurasi, menjalankan, dan menganalisis hasil pemindaian celah keamanan otomatis skala korporasi.
- **Metasploit Framework:** Pemanfaatan modul *auxiliary* untuk pemindaian/intelijen, serta modul eksploitasi untuk penetrasi otomatis dan manajemen sesi *Session/Meterpreter*.

Keamanan Jaringan Nirkabel (Wireless Pentest):

- **Wireless Reconnaissance & Deauthentication:** Pemetaan jaringan Wi-Fi sekitar (*Sniffing*) dan pemutusan koneksi pengguna secara paksa menggunakan paket *Deauth*.
- **WPA/WPA2 Testing:** Teknik penangkapan Handshake, hingga proses *offline brute-force/dictionary attack* terhadap enkripsi nirkabel, dilengkapi dengan metode mitigasi pengamanannya.

Pengodingan Aman & Respon Insiden (Secure Coding & Incident Response):

- **Hot Patching:** Teknik melakukan perbaikan kode program (*patching*) secara cepat tanpa menghentikan layanan aplikasi web yang sedang berjalan.
- **Audit Sistem Kontinu:** Penggunaan perkakas bawaan seperti **auditctl** (Audit Daemon Linux) untuk memonitoring akses file dan eksekusi perintah mencurigakan.
- **Real-Time Incident Response:** Langkah-langkah taktis dalam mengisolasi host yang terkompromi, menganalisis proses yang berjalan, dan membersihkan ancaman secara instan.

Pengerasan Sistem & Pertahanan Siber (Hardening & Defensive Engineering):

- **Implementasi Keamanan:** Konfigurasi tingkat lanjut pada *Web Application Firewall* (WAF), sistem proteksi terhadap serangan tebakan kata sandi (*Anti-Brute-Force* seperti Fail2ban), mekanisme penipuan/blokir pemindaian port (*Anti-Port-Scanner*), manajemen aturan lalu lintas *Firewall* (iptables/ufw), serta manajemen pembaruan keamanan (*security patch*).

Aturan Simulasi Tim (Team Simulation Rule):

- **Blue Team Full Access:** Aturan khusus simulasi di mana Tim Bertahan diberikan akses administratif penuh ke platform SIEM **Wazuh** dan server utama untuk melakukan pemantauan, analisis log, pertahanan aktif, dan penutupan celah secara langsung saat serangan terjadi (*Live Defense*).

Kesiapan Karir & Keterampilan Interpersonal (Career & Soft Skills):

- **STAR Interview Method:** Pelatihan menghadapi wawancara kerja menggunakan metode terstruktur *Situation, Task, Action, Result*.
- **Careers in Pentesting:** Pemetaan jalur karir industri keamanan siber (Junior/Senior Pentester, Security Consultant, Red Teamer).
- **Soft Skills for Business:** Teknik menerjemahkan temuan teknis yang rumit menjadi bahasa bisnis yang dipahami oleh pemangku kepentingan finansial dan manajemen (*Translating tech to business value*).

Pembelajaran Laboratorium Praktis Tingkat Lanjut (Advanced Lab Exploitation):

- **Exploit Chain & Pivoting:** Menggabungkan beberapa kerentanan kecil menjadi satu dampak besar (*Exploit Chain*), serta menggunakan komputer yang telah diretas sebagai jembatan untuk menyerang jaringan internal terisolasi lainnya (*Pivoting*).
- **Lateral Movement:** Teknik berpindah dari satu mesin ke mesin lain di dalam jaringan internal setelah berhasil masuk.

- **JWT Exploitation:** Lab eksploitasi JWT.
- **Mobile Application Exploitation:** Analisis statis dan dinamis pada aplikasi mobile (Android) untuk melakukan bypass login.
- **Container Escape:** Contoh Teknik menjebol isolasi lingkungan virtualisasi berbasis kontainer (seperti Docker) untuk mendapatkan akses penuh ke sistem operasi *Host*.
- **Active Directory (AD) Takeover:** Contoh Simulasi serangan total pada infrastruktur Windows Domain, termasuk pembuatan **Golden Ticket** (tiket Kerberos palsu dengan hak akses tertinggi), eksploitasi hubungan kepercayaan antar domain (*Cross-Domain AD Takeover*), serta eksploitasi infrastruktur manajemen identitas berbasis Linux (**FreeIPA Exploitation**).
- **Malware Analysis:** Analisis dasar perilaku perangkat lunak berbahaya (malware) melalui teknik analisis statis dan dinamis (pemantauan aktivitas di lingkungan terisolasi).

X-code Bootcamp 2026 (Online)

Penetration Tester & Cyber Security Engineer v7.1

No	Session	Objective
Sessions		
1	Introduction session	Sesi Pengantar Oleh Kurniawan **Live Class** Sesi awal atau perkenalan yang bertujuan menjelaskan tujuan dan alur dari Bootcamp.untuk memberikan gambaran umum tentang apa yang akan dipelajari/dilakukan **Video Class** - 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, 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 - Mengenal reverse engineering dengan contoh prakteknya (source code, compile, binary (executable), disassembly & mendapatkan password pada contoh program login windows dan linux).
2		Sesi 2

		Live Class Apa itu cyber security Mengapa cyber security itu ada? Mengenal Blue Team dan Red Team serta perbedaannya Safe Guard & Defends Apa itu ethical hacking Apa itu penetration testing? Alasan dan kebutuhan penetration testing Mengenal berbagai Penetration Testing methodolgies and Standards Gambaran pekerjaan penetration testing Skill yang dibutuhkan menjadi seorang penetration testing Tips dan trik dalam penetration tssting Apa itu Tim Infrastruktur? Apa itu SOC Analyst Tier 1 dan SOC Analyst Tier 2? Mengenal Tim Infrastruktur, SOC Analyst Tier 1, dan SOC Analyst Tier 2 dalam Studi Kasus Layanan Public Cloud di PT. Teknologi Server Indonesia: Cara Kerja dan Tugas Masing-Masing **Video Class** - Firewall - Port Knocking

		- Forwarding pada managed switch - Proxy - TOR Windows - TOR Linux (Advanced) ~ Hacking Server seperti FTP Server, SSH Server, dst dengan koneksi TOR - SSH Tunnel - 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)
3	Session 3	Sesi 3 **Live Class** Cyber Security Fundamental - Miss GIzka **Video Class** - 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 (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 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 ber-firewall (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 - 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 - Instalasi Ubuntu Server 20.04.3 LTS - Install Apache Server & MySQL Server di Ubuntu Server 20.04.3 LTS - 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 - 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 - DNS Server di Ubuntu Server 20.04.3
4	Session 4	Sesi 4 **Live Class** Mengenal Virtualbox, VMWare, KVM (Proxmox), LXC (Proxmox), Docker dan MicroCloud - Cara masang vm di virtualbox serta beragam konfigurasinya Cara masang vm di vmware serta beragam konfigurasinya Cara setting ip address secara manual di windows Cara menambah ip baru di ip address manual di

		Windows Cara setting ip address secara otomatis di windows Cara setting ip address manual di linux ubuntu (netplan) Cara menambah ip baru di ip address manual di netplan (Ubuntu) Cara setting ip address secara otomatis di linux ubuntu (netplan Cara setting ip address secara manual di kali linux Cara menambah ip baru di ip address manual di Windows Cara setting ip otomatis di kali linux **Video Class** - 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 (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 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 ber-firewall (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 - 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
5	Session 5	Sesi 5 **Live Class** Apa itu linux, FreeBSD & OpenBSD Memahami Linux, FreeBSD, & OpenBSD Melihat kelemahan dan kelebihan Linux, FreeBSD, & OpenBSD Distro Kali Linux Mengenal dan belajar file system linux

		Belajar instalasi Ubuntu Server di virtualbox Belajar Instalasi FreeBSD di virtualbox (Video dengan hardening: : Download belajar freebsd dan security hardening Belajar Instalasi Kali Linux di virtualbox **Video Class** - 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) - 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 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 - Tugas untuk membuat exploit remote buffer overflow pada suatu web server
6	Session 6	Sesi 6 **Live Class** Belajar Kali linux Belajar menggunakan tool-tool di kali linux Belajar shell di kali linux / ubuntu server dan freeBSD

		(cd , ls, mkdir, rmdir, rm, cp, mv, dll) Belajar tentang user, group dan managemennya di linux (useradd, groupadd, chown, chgrp, chmod, dll) Belajar menggabungkan TOR dan Proxychains untuk anonim Belajar Web Server Apache dan belajar log pada apache2 web server Belajar Web Server Nginx dan belajar log pada Nginx Web Server Belajar Melihat berbagai log di linux **Video Class** - 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) - Mengenal Jump Short - Uji coba perbedaan module yang terproteksi dan yang tidak terproteksi EggHunter - 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.
7	Session 7	Sesi 7 **Live Class** Belajar jaringan komputer Belajar ARP, ip address, mac address dan berbagai hal yang berhubungan dengan jaringan Mengenal protokol, port, service, serta contoh aplikasi / nama service. Switching & Routing Belajar keamanan FTP dari protokol hingga melihat kerentanan jika memiliki bug stack overflow untuk attacker: Eksploitasi kerentanan yang ditemukan melalui CVE dan membuat exploit-nya sendiri. Membuat exploit sendiri dari python untuk remote shell dengan shellcode membuat sendiri dari bahasa assembly Contoh cara memasukkan exploit yang dibuat ke metasploit Belajar keamanan protokol SSH hingga kemungkinan untuk dihack Belajar keamanan telnet dibandingkan SSH

		Belajar keamanan SMTP dan POP3 (Dari instalasi mail server sampai keamanan protokol) Belajar SSLStrip untuk mendapatkan username dan browser Belajar keamanan SMB di windows dan SAMBA di linux (Keamanan protokol hingga melihat kerentanan jika memiliki kerentanan dari Microsot Bulletin untuk Windows dan CVE untuk lebih luas)Belajar **Video Class** Contoh Buffer overflow di linux - Gdb & belajar perintah-perintah GDB (list main, disas main) - 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 - Bypass DEP (Data Execution Prevention) dengan ROP (Return Oriented Programming) secara manual (Ngoding manual, bukan generate) pada target Windows - Generate reverse shell (bypass firewall) untuk dipasang pada exploit. - 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 CVE-2020-0796 (Blue screen)
8	Session 8	Sesi 8 **Live Class** Belajar instalasi Nessus (Dari download hingga aktivasi nessus) Halaman 1038 bawah Belajar menggunakan Nessus untuk mencari bug Belajar cara memanfaatkan informasi di nessus untuk melakukan hacking Belajar menggunakan metasploit

		Hacking Windows 10 yang memiliki kerentanan Belajar eksploitasi target di windows 10 Belajar dasar Meterpreter Scanning bug pada Web Server Apache yang memiliki kerentanan Contoh Eksploitasi kerentanan yang ditemukan dengan exploit yang tersedia di internet Scanning bug pada Aplikasi web yang memiliki kerentanan dengan Nessus Eksploitasi kerentanan yang ditemukan dengan SQLMAP **Video Class** - 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)
8	Session 9	Sesi 9 **Live Class** Binary Exploitation Mengenal Buffer Overflow, Stack Overflow (Subtipe buffer overflow: terjadi di heap), Heap Corruption (Subtipe buffer overflow: terjadi di heap), Format String & Use After Free Belajar membuat tool hacking sendiri dengan python Exploit Development dasar

		Membuat program Fuzzing Belajar tentang Stack, memory dan registers Mengenal berbagai keamanan di Windows (SEH, SafeSEH, ASLR (Address Space Layout Randomization), DEP / NX (Data Execution Prevention / No Execute), CET (Control-flow Enforcement Technology), Stack Canary dan Control Flow Guard (CFG). Mengenal Jump Short dan Egghunter Mengenal berbagai strategi jika exploit tidak jalan Contoh membuat exploit dengan python untuk target yang mempunyai kerentanan yang berjalan di Windows 10 (Bypass SEH, bypass SafeSEH dan bypass ASLR) Memasang shellcode bind shell pada exploit Membangun shellcode reverse shell dengan msfvenom untuk dipasang pada exploit **Video Class** - 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 - 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 kernel 5.8 - Update Kernel Ubuntu 20.04.2 versi 5.4 ke kernel baru (Di x-code video) - Privilege escalation pada ubuntu server 20.04.3 pada celah polkit (exploit dari bulan Januari 2022) - Pengamanan pada ubuntu server 20.04.3 pada celah polkit (exploit dari bulan Januari 2022) - Privilege Escalation pada target linux memanfaatkan

		celah CVE-2022-0847
10	Session 10	Sesi 10 **Live Class** Mengenal berbagai aplikasi populer di linux Belajar Hacking linux server dan router Belajar hacking Samba di linux (dari scanning sampai remote shell) Belajar hacking FTP di linux (dari scanning sampai remote shell) Belajar hacking router untuk mendapatkan password (dari scanning sampai masuk yang halaman admin) Belajar bagaimana belajar eksploitasi router secara lebih mendalam Belajar beragam teknik hacking pada router dari memanfaatkan ARP Spoofing untuk mendapatkan password, brute force untuk mendapatkan passworddan sebagainya Belajar mematikan seluruh koneksi jaringan local secara cepat baik computer / server yang menggunakan ip manual ataupun otomatis (Dari DHCP) dengan Kali Linux Belajar exploit development di linux **Video Class** - 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
11	Session 11	Sesi 11 **Live Class** Belajar berbagai hal yang dibutuhkan Cyber Security Engineer Pengenalan Wazuh SIEM, fungsinya sebagai SIEM Arsitektur Wazuh: Manager, Agent serta persiapan Infrastruktur Kebutuhan sistem & topologi sederhana (1 server + beberapa agent) Instalasi Wazuh Manager, Wazuh Indexer, Wazuh Dashboard Validasi service berjalan Instalasi WAF ModSecurity di Ubuntu Server 24.04

		untuk menangkal beragam serangan seperti SQL Injection dan sebagainya Instalasi dan Koneksi Wazuh Agent Instalasi Wazuh Agent di mesin client (Ubuntu) Registrasi dan sinkronisasi key Agent ke Manager Konfigurasi koneksi Agent Verifikasi koneksi berhasil (Agent aktif & terbaca) Pengujian dilakukan untuk mendeteksi percobaan brute force pada layanan SSH, DoS, serangan webs dan sebagainya Pengujian deteksi dilakukan untuk mengetahui jika terdapat aktivitas seperti: Pembuatan user baru, pembuatan password, instalasi aplikasi dan sebagainya Monitoring & Analisis Belajar Secure Coding Belajar cara cepat analisa kode sumber untuk mencari kerentanan Pengenalan tentang Bug Bounty untuk kebutuhan perusahaan Cara merespon laporan bug bounty untuk perusahaan Cara menguji kerentanan dari laporan yang diberikan untuk perusahaan Cara patch secara cepat jika ada laporan kerentanan **Video Class** - 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)
12	Sesi 12	WAR – Red Team vs Blue Team Peserta akan dibagi menjadi dua kelompok, yaitu Red Team dan Blue Team. • Blue Team dibekali akses ke server target serta sistem monitoring keamanan menggunakan Wazuh SIEM untuk mendeteksi dan menganalisis aktivitas serangan. Peserta dapat menerapkan berbagai mekanisme pengamanan, namun layanan pada server harus tetap dapat diakses dan berjalan normal. • Red Team dibekali berbagai tools hacking yang tersedia pada VPS. Selain itu, Red Team juga dapat memanfaatkan SSH Tunnel untuk melancarkan serangan dari PC atau laptop pribadi, sehingga dapat menggunakan tools tambahan seperti Burp Suite dan lainnya.
13	Session 13	Sesi 13 **Live Class** Client-Server Side Web Server Model, dari komponen, fungsi, alur kerja, http request & http response, Belajar protokol http, https, proxy server, DNS, firewall, API

		HTTP methods (GET & POST) HTTP Header Manipulation Information gathering pada website (Menggunakan berbagai tools dari kali linux, website yang menyediakan information gathering, search engine dan sebagainya) Bypass Cloudflare dengan beragam cara Scanning pada website (Scanning bug dengan berbagai tools baik dari kali linux ataupun dari Memeriksa masalah konfigurasi, beradaan file-file sensitif seperti file backup, dan sebagainya Mencari file sensitive dengan Dirbuster, Gobuster, Dirsearch dan Dirhunt Mencari halaman login dengan brute force Mendeteksi keberadaan WAF pada target Mencari subdomain pada suatu domain dengan beragam cara Melihat kemungkinan dari mana saja kerentanan didapat Scanning pada website (Scanning bug dengan berbagai tools baik dari kali linux ataupun dari luar) Memeriksa masalah konfigurasi, beradaan file-file sensitif seperti file backup, dan sebagainya Broken Authentication & Session Management Security Missconfiguration Captcha Bypass

		Two-Factor Authentication (2FA) Bypass **Video Class** - 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
14	Session 14	Sesi 14 **Live Class** Pengenalan OWASP Top 10 2025 A01:2025 - Broken Access Control A02:2025 - Security Misconfiguration A03:2025 - Software Supply Chain Failures A04:2025 - Cryptographic Failures A05:2025 – Injection **Video Class** A01 2021 - Broken Access Control A02 2021 - Cryptographic Failures A03 2021 - Injection A04 2021 - Insecure Design A05 2021 - Security Misconfiguration
15	Session 15	Sesi 15 **Live Class** A06:2025 - Insecure Design A07:2025 - Authentication Failures A08:2025 - Software or Data Integrity Failures

		A09:2025 - Security Logging and Alerting Failures A10:2025 - Mishandling of Exceptional Conditions **Video Class** A06 2021 - Vulnerable and Outdated Components A07 2021 - Identification and Authentication Failures A08 2021 - Software and Data Integrity Failures A09 2021 - Security Logging and Monitoring Failures A10 2021 - Server Side Request Forgery (SSRF)
16	Session 16	Sesi 16 **Live Class** Konsep Dasar Clickjacking Analisis Celah, Simulasi Clickjacking serta pencegahan Konsep Dasar Race Condition Analisis Celah dan Simulasi Race Condition Dasar XSS (Cross-Site Scripting) Contoh eksploitasi XSS dan pengamanannya Scanning XSS Secara otomatis dengan banyak tools Pengujian XSS secara manual XSS non persistent XSS persistent

		DOM-Based XSS Cara mengambil cookies dari kerentanan XSS dan login ke web target menggunakan cookies (tanpa password) Tips cara pentest dengan metode blackbox dan graybox pada XSS untuk mendapatkan pengujian optimal. Bypass WAF untuk serangan XSS Pemilihan rules pada WAF yang tepat untuk menangani serangan bypass XSS **Video Class** Memasukkan file ISO ubuntu server ke proxmox Membuat VM dan instalasi Ubuntu Server Membangun backup secara otomatis untuk semua file website dan database Membangun backup secara otomatis untuk semua file website dan database ke server berbeda Restore backup file dan website Membangun backup otomatis di proxmox untuk VM Membangun backup otomatis di proxmox untuk VM ke server berbeda Restore backup VM
17	Session 17	Sesi 17 **Live Class**

		File inclusion Membangun PHP Shell sendiri Scanning bug file incluson dengan berbagai tool dari kali linux Scanning bug file inclusion dengan ZAP Scanning bug file inclusion Burpsuite Eksplotasi RFI (Remote File Inclusion), pengamanan dari koding, pengamanan dari sisi konfigurasi PHP Eksplotasi LFI (Local File Inclusion), pengamanan dari koding, pengamanan dari sisi konfigurasi LFI Tips cara pentest dengan metode blackbox dan graybox pada LFI untuk mendapatkan pengujian optimal. Eksploitasi LFI untuk mendapatkan akses shell (Bind Shell & Reverse Shell) **Video Class** FreeBSD Server Hardening - Pengenalan FreeBSD - Instalasi FreeBSD - Pengenalan Shell di FreeBSD: cd, ls, mkdir, rmdir, rm, cp, mv, dll. - Konfigurasi IP Statis di FreeBSD - Instalasi Apache Web Server, PHP, MySQL Server, dan Konfigurasinya, serta Instalasi WordPress di FreeBSD

		- Pengujian Keamanan Apache Web Server terhadap Serangan DoS - Penerapan Security Hardening pada Apache Web Server di FreeBSD dengan IPFW untuk Mitigasi Serangan DoS - Konfigurasi VirtualHost di FreeBSD - Konfigurasi DMZ pada Router (Teori & Praktik) - Implementasi Mode Enkripsi Flexible SSL/TLS Cloudflare pada Apache Web Server di FreeBSD (Teori & Praktik)
18	Session 18	Sesi 18 **Live Class** Insecure Direct Object Reference (IDOR) & Insecure File Upload Mengenal Improper Input Validation dan Unrestricted Upload of File with Dangerous Type Contoh eksploitasi Insecure File Upload Contoh pengamanan dari eksploitasi Insecure File Upload Bypassing File Upload Restrictions via .htaccess Override Pengamanan .htaccess Mengenal Insecure Direct Object Reference (IDOR) Contoh eksploitasi Insecure Direct Object Reference (IDOR) Memahami IDOR secara lebih mendalam dan

		kemungkinan eksploitasi lebih jauh dalam pentest Contoh pengamanan dari Insecure Direct Object Reference (IDOR) Belajar Command Injection dan demo prakteknya Belajar CSRF (Cross-Site Request Forgery) dan demo prakteknya Belajar SSRF (Server-Side Request Forgery) dengan target web native dan CMS **Video Class** Linux Server Hardening – Instalasi Ubuntu Server 24.04 LTS – Instalasi Apache Web Server – Instalasi PHP (Web Apache Server) – Instalasi MySQL (Web Apache Server) – Memberikan password untuk akses root di MySQL – Instalasi PHPMyAdmin (Web Apache Server) – Instalasi WordPress terbaru (Web Apache Server) – Virtualhost di Web Apache server – Security Hardening untuk PHPMyadmin – Pengujian mematikan Web Apache Server dengan DoS – Hardening Web Server Web Apache dari DoS dengan iptables

		– Instalasi Web Nginx Web Server – Instalasi PHP (Nginx Web Server) – Instalasi MySQL (Nginx Web Server) – Memberikan password untuk akses root di MySQL – Instalasi WordPress terbaru (Nginx Web Server) – Virtualhost di Nginx Web server – Pengujian mematikan Nginx Web Server dengan DoS – Hardening Web Server Nginx dari DoS dengan iptables – Hardening untuk pengamanan dari PHP Shell – Pengamanan secara umum untuk server – Instalasi anti portscan dan cara penggunaannya – Instalasi anti bruteforce (SSH) dan cara penggunaannya – Konfigurasi untuk anti clickjacking – Firewall UFW di Ubuntu Server 24.04 – Pengamanan Web Server dari PHP Shell – Instalasi tool untuk dukungan monitoring – Instalasi Antivirus dan cara penggunaanya untuk server – Analisa Log web server, SSH dan lainnya
19	Session 19	Sesi 19

		Live Class Pengenalan dan teori Tautology-based SQL Injection (POST), praktek scanning, eksploitasi dan pengamanannya Cara scanning otomatis untuk mendapat kerentanan SQL Injection Cara scanning semi otomatis untuk menemukan kerentanan SQL Injection Scanning SQL Injection (POST) dengan Burpsuite Cara scanning otomatis untuk menemukan kerentanan SQL Injection Cara cek manual untuk mengetahui kerentanan SQL Injection Demo Tautology-based SQL Injection (POST) Boolean-based Blind SQL Injection (Manual) untuk mendapatkan username dan password pada kasus login Mengenal Time-based Blind SQL Injection secara manual dan eksploitai otomatis dengan SQLMAP untuk mendapatkan username dan password pada kasus login SQL Injection pada kasus pencarian dengan Burp Suite Eksploitasi SQL Injection secara otomatis pada kasus pencarian dengan SQLMAP. Melewati keamanan pada SQL Injection dengan teknik bypass lebih lanjut pada suatu kasus **Video Class**

		- 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 - Tabel kebenaran gerbang AND dan OR - 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)
20	Session 20	Sesi 20 **Live Class** Pengenalan dan teori SQL Injection Union-based

		(GET), scanning, eksploitasinya serta pengamanannya SQL Injection Union-based (GET) untuk mendapatkan password user untuk masuk dalam database melalui phpmyadmin dengan SQLMAP Mengenal SQL Injection Blind pada metode GET serta demo contohnya Mengenal SQL Injection Time-Based pada metode GET serta demo contohnya Membangun lab untuk belajar Bypass WAF dari instalasi WAF dan menggunakan Generic Attacks.Rules. Instalasi WAF ModSecurity di Ubuntu Server Konfigurasi WAF ModSecurity Bypass WAF untuk serangan SQL Injection Pemilihan rules pada WAF yang tepat untuk menangani serangan bypass WAF SQL Injection Tips cara pentest dengan metode blackbox dan graybox pada SQL Injection untuk mendapatkan pengujian optimal. **Video Class** - 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) - Websploit untuk scan PMA - PhpMyAdmin Exploitation (Advanced) Covering tracks - Menghapus log server dan menghapus history.
21	Session 21	.Sesi 21 **Live Class** STAR interview method, careers in pentesting, red/blue team, GRC, portfolio building, and soft skills for translating tech to business Apa beda API PHP dan PHP biasa? Pengenalan Struktur RESTful API Scanning otomatis dan pengujian manual endpoint serta parameter API menggunakan teknik fuzzing Mengenal SQL Injection pada API PHP Contoh eksploitasi SQL Injection pada API PHP

		Mengenal Local File Inclusion (LFI) pada API PHP Contoh eksploitasi Local File Inclusion (LFI) pada API PHP Mengenal Command Injection pada API PHP Contoh eksploitasi Command Injection pada API PHP Contoh Information Disclosure pada API PHP **Video Class** - 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
22	Session 22	Sesi 22 **Live Class** Pengenalan Node.js

		Contoh eksploitasi SQL Injection pada Aplikasi Node.js Contoh Eksploitasi Local File Inclusion (LFI) pada Node.js Contoh eksploitasi Command Injection pada Aplikasi Node.js DoS web server dan pengamanannnya PHP Shell dan eksploitasinya dari PHP 5 hingga PHP 8 hingga pengamanannya dari PHP.INI dan Virtualhost Bypass disable function LD_PRELOAD, GC, CONCAT, FILTER Pengamanan dari serangan bypass disable function **Video Class** 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 Server lama - 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) - Teknik melakukan banned secara otomatis pada ip target yang melakukan scanning otomatis atau cek

		celah pada variabel secara manual pada web yang diamankan (Linux)
23	Session 23	Sesi 23 **Live Class** Mengenal privilege escalation privilege escalation dari kerentanan kernel linux privilege escalation dari kerentanan polkit privilege escalation dari kerentanan sudo Privilege Escalation via Insecure Permissions and Misconfigured Access Control privilege escalation pada freebsd dan openbsd yang memiliki kerentanan Incident Response Auditctl, instalasi dan cara penggunaannya Monitoring server dengan htop / top, ps dan sebagainya Pemeriksaan log jika ada yang berhasil mendapatkan akses shell di server Pemeriksaan malware secara otomatis di server Pemeriksaan file-file terbaru yang diupload attacker Rootkit, backdoor reverse shell otomatis, phpshell, backdoor akun, dst

		Video Class - 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 X-code Premium Video) - Jamming (User yang terkoneksi ke hotspot mengalami terputus koneksi) - 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) - 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
24	Session 24	Sesi 24

		Live Class Wirelsss hacking Bypass Mac Filtering Sniffing SSID Hidden Jamming Cracking WPA-PSK2 dengan wordlist Cracking WPA-PSK2 dengan kriteria sendiri untuk percobaan brute force Cracking WPA-PSK2 dengan wordlist dengsn IGPU / APU / Graphics Card Evil Twin Attack **Video Class** Malware Analysis Building a malware analysis laboratory Building a DNS server and a mail server Sample malware (Windows) Dynamic Analysis – Behavioural analysis Dynamic Analysis – Network traffic analysis Static Analysis – Code analysis (Reverse Engineering)
25	25	Sesi 25 **Live Class** Pembahasan Lab 2

		Initial Access & foothold pada network terbatas Exploit chaining (multi-step exploitation) Network pivoting antar subnet Lateral movement antar host Privilege escalation sampai root access Web / service exploitation pada Linux server Internal host enumeration & discovery Access control bypass (whitelist filtering scenario) Logically segmented network traversal (router-based restrictions) Cryptography challenge (di VPS Red Team environment) Linux application reverse engineering Internal infrastructure exploitation lab tasks
26	Session 26	Sesi 26 **Live Class** Pembahasan Lab 3 JWT Retrieval from API to Application Flaw Mobile Static Analysis and Dynamic Analysis to SQL Injection Popular CMS Core RCE into Remote Shell Web Server RCE into Remote Shell

		From CVE-2026 to Host: Container Escape Chain (Ubuntu Server 24.04.4)
27	Sesi 27	Sesi 27 **Live Class** Pembahasan Lab 4 Advanced Active Directory Attack Techniques: Full-Chain Domain Compromise via Lateral Movement and Kerberos Ticket Forgery (Golden Ticket) for Persistent Administrative Access. 1. Initial Access & Foothold Establishment 2. Database Extraction (The Source) Non-Interactive Credential Database Dumping Automated SAM & LSA Secret Extraction Cryptographic Material Harvesting 3. Operational Base Expansion (The Pivot) Exploitation of Domain-Joined Windows Client Workstation Control & Environment Preparation 4. Identity Mapping Local & Domain Security Identifier (SID) Analytics Whoami Identity Verification Relative Identifier (RID) Mapping 5. Ticket Forging & Internal Domain Persistence In-Memory Kerberos Ticket Injection Standardized Authentication Protocol Alignment Remote File System Enumeration via UNC Paths
28	Sesi 28	Sesi 28

		Live Class Pembahasan Lab 5 Cross-Domain Escalation (Expert Level) Golden Ticket attack Cross-Node Security Identifier (SID) Harvesting (ExtraSID) Parent-Child trust exploitation Enterprise Admin takeover.
29	Sesi 29	Sesi 29 **Live Class** Pembahasan Lab 6 – Mengenal FreeIPA • Melakukan scanning target untuk mendeteksi penggunaan FreeIPA • Persiapan proses eksploitasi • Melakukan eksploitasi terhadap target Objective: Peserta harus mendapatkan akses ke target berikut: https://ipa.ctf-lab.local/ipa/ui/ Catatan: • Target hanya dapat diakses melalui jaringan internal. • Konfigurasi target telah dimodifikasi manual untuk kebutuhan lab/praktik.

30	Sesi 30	Sesi 30 **Live Class** General Questions Penetration testing offers Intelligence Gathering OSINT Threat Modeling Vulnerability Analysis Testing Exploitation Common Weakness Enumeration (CWE) CVSS Score Post Exploitation Vulnerability Impact and risks Recommendation Reporting

Media

– Zoom

Mentor Bootcamp

– Mentor utama: Master Kurniawan (Mentor semua sesi kecuali sesi 2)

– Mentor: Miss Gizka (Mentor sesi 2)

Mentor untuk Magang

– Mentor utama: Master Kurniawan

– Mentor: Miss Gizka

Fasilitas:

– Grup forum dan relasi baru– Rekaman saat training

– Modul training ethical hacking & security lebih dari 2000 halaman

– Download lebih dari 50 files virtual machine

– 1 Peserta 1 VPS untuk target server-server di lab

– Program-program pendukung

– Gratis konsultasi kapan saja

– Akses ke X-code Premium Video

– E-sertifikat X-code Bootcamp & E-sertifikat Magang bagi yang magang

Program Magang – Pentest & SOC Analyst

Fasilitas & Materi:

1. SOP untuk SOC Analyst

2. Template Laporan Pentest, SOC Analyst, PKS (Perjanjian Kerja Sama), dan NDA (Non-Disclosure Agreement)

Pengalaman Praktis:

Pemagang akan langsung terjun di bidang Pentest & SOC, menggunakan tools industri modern seperti:

Proxmox dengan ratusan VPS, Wazuh SIEM, Splunk SIEM, Grafana, Prometheus,

Netdata, serta sistem internal perusahaan, untuk menjaga ratusan VPS dan layanan shared hosting milik PT.

Keahlian yang Dipelajari:

Pentester

SOC Level 1

SOC Level 2

Biaya

– 2.000.000 IDR

Pendaftaran (Online)

Informasi & pendaftaran melalui online (Whatsapp)

– WA Admin 1 : 0857 2891 7933

– WA Admin 2 : 0895 4207 54477