2025

XCODE

Penetration Tester & Cyber Security Engineer Bootcamp v2

XCODE

X-code Bootcamp (Online)

Penetration Tester & Cyber Security Engineer v2

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 Training: 22x pertemuan

X-code Bootcamp (Online)

Penetration Tester & Cyber Security Engineer v2

No	Session	Objective
Sessions		
1	Session 1	Sesi 1 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 testing 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
2	Session 2	Sesi 2 Cara masang vm di virtualbox Cara masang vm di vmware Cara setting ip manual di windows Cara setting ip otomatis di windows Cara setting ip manual di linux ubuntu (netplan) Cara setting ip otomatis di linux ubuntu (netplan Cara setting ip manual di kali linux Cara setting ip otomatis di kali linux
3	Session 3	Sesi 3 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 Belajar Instalasi Kali Linux di virtualbox
4	Session 4	Sesi 4 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 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
4	Session 5	Sesi 5 Belajar jaringan komputer Belajar ARP, ip address, mac address dan berbagai hal yang berhubungan dengan jaringan Belajar keamanan FTP dari protokol hingga melihat kerentanan jika memiliki bug stack overflow 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 keamanan SMB di windows dan SAMBA di linux (Keamanan protokol hingga melihat kerentanan jika memiliki kerentanan dari Microsot Bulleting untuk Windows dan CVE untuk lebih luas)
6	Session 6	Sesi 6 Belajar instalasi Nessus (Dari download hingga aktivasi nessus) 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 eksplorasi target di windows 10 Belajar dasar Meterpreter
7	Session 7	Sesi 7 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 & DEP) Mengenal berbagai strategi jika exploit tidak jalan

8	Session 8	Sesi 8 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 (dari scanning sampai masuk yang halaman admin) Belajar exploit development di linux
9	Session 9	Sesi 9 Belajar berbagai hal yang dibutuhkan Cyber Security Engineer Belajar Secure Coding Belajar cara cepat analisa kode sumber untuk mencari kerentanan Pengenalan tentang Bug Bounty Cara merespon laporan bug bounty untuk perusahaan Cara menguji kerentanan dari laporan yang diberikan untuk perusahaan Cara patch secara cepat jika ada laporan kerentanan
10	Session 10	Sesi 10

		HTTP methods (GET & POST) Information gathering pada website (Menggunakan berbagai tools dari kali linux, website yang menyediakan information gathering, search engine dan sebagainya) 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
11	Session 11	Sesi 11 Pengenalan OWASP Top 10 2021 A1: Broken Access Control (Teori dan demo praktek) A2: Cryptographic Failures (Teori dan demo praktek) A3: Injection (Teori dan demo praktek) A4: Insecure Design (Teori dan demo praktek) A5: Security Misconfiguration (Teori dan demo praktek)
12	Session 12	Sesi 12 A6: Vulnerable and Outdated Components (Teori dan demo praktek) A7: Identification and Authentication Failures (Teori dan demo praktek)

		A8: Software and Data Integrity Failures (Teori dan demo praktek) A9: Security Logging and Monitoring Failures (Teori dan demo praktek) A10: Server-Side Request Forgery (SSRF) (Teori dan demo praktek)
13	Session 13	Sesi 13 Dasar XSS Contoh eksploitasi XSS dan pengamanannya Scanning XSS Secara otomatis dengan banyak tools Pengujian XSS secara manual XSS non persistent XSS persistent Cara mengambil cookies dari kerentanan XSS dan login ke web target menggunakan cookies (tanpa password) Bypass WAF untuk serangan XSS (Otomatis & manual)
14	Session 14	Sesi 14 File inclusion 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
15	Session 15	Sesi 15 Insecure Direct Object Reference (IDOR) & Insecure File Upload Mengenal Insecure File Upload Contoh eksploitasi Insecure File Upload Contoh pengamanan dari eksploitasi Insecure File Upload Mengenal Insecure Direct Object Reference (IDOR) Contoh eksploitasi Insecure Direct Object Reference (IDOR) Contoh pengamanan dari Insecure Direct Object Reference (IDOR)
16	Session 16	Sesi 16 Pengenalan dan teori Tautology-based SQL Injection (POST), praktek scanning, eksploitasi dan pengamanannya Tautology-based SQL Injection (POST) Boolean-based Blind SQL Injection (Manual) untuk mendapatkan username dan password Mengenal Time-based Blind SQL Injection secara manual dan eksploitai otomatis dengan SQLMAP untuk

		mendapatkan username dan password
17	Session 17	Sesi 17 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 Bypass WAF untuk serangan SQL Injection Pemilihan rules pada WAF yang tepat untuk menangani serangan bypass WAF SQL Injection
18	Session 18	.Sesi 18 Apa beda API PHP dan PHP biasa? Pengenalan Struktur RESTful API Scanning otomatis dan pengujian manual endpoint serta parameter API menggunakan teknik fuzzing Contoh eksploitasi SQL Injection pada API PHP Contoh eksploitasi Local File Inclusion (LFI) pada API PHP Contoh eksploitasi Command Injection pada API PHP Contoh Information Disclosure pada API PHP
19	Session 19	Sesi 19 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
20	Session 20	Sesi 20 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 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
21	Session 21	Sesi 21 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
22	Session 22	Sesi 22 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 Impact and risks Recommendation Reporting

Media

– Zoom

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

– Program-program pendukung

– Gratis konsultasi kapan saja

– Akses ke X-code Premium Video

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

Biaya

– 1.500.000 IDR

Pendaftaran (Online)

Informasi & pendaftaran melalui online (Whatsapp)

– WA Admin 1 : 0857 2891 7933

– WA Admin 2 : 0895 4207 54477