

PTI · Batch 2

Pentest Intermediate

Tingkatkan Skill Pentest & Ethical Hacking ke Level Berikutnya

14 · Via Zoom & Youtube Exclusive · 1 Agt 2023 – 23 Sep 2023

Ringkasan Eksekutif

Nama Program	Pentest Intermediate
Kode Program	PTI · Batch 2
Durasi	14
Tanggal Pelaksanaan	1 Agt 2023 – 23 Sep 2023
Format & Platform	Via Zoom & Youtube Exclusive
Mentor	Anggrahito, (CEH, ECSA, CHFI) MBA.
Bahasa	Bahasa Indonesia
Sertifikat	e-Certificate Taalenta (sesuai paket)

Kenapa Wajib Ikut

1. Ancaman Cyber Meroket

Dengan digitalisasi yang semakin luas, ancaman cybercrime juga semakin meningkat. Memahami pentest dapat membantu kita menemukan celah keamanan lebih cepat daripada pelaku kejahatan siber.

2. Jangan Lewatkan Peluang Karir

Kebutuhan untuk profesional keamanan cyber semakin besar. Mempelajari pentest membuka banyak peluang karir.

3. Praktek Langsung

Kelas Hacking/Pentesting Taalenta menekankan pada praktik langsung dan simulasi untuk mempersiapkan kamu dalam situasi nyata.

4. Komunitas yang Aktif

Berbagi pengalaman dan diskusi dengan sesama peserta kelas dan mentor dapat membantu mempercepat proses pembelajaranmu.

5. Siap Hadapi Transformasi Digital

Memahami penetration testing menjadi satu keahlian praktis yang dibutuhkan untuk melindungi infrastruktur digital dan memastikan keandalan sistem di era digital.

Outline Materi

1. Introduction

- Penetration Testing Introduction Knowledge Base (About OS Pentest and Essential Tools) Legal and Opportunity
- Methodology and Standard Hacking Methodology, Bug Bounty Workflows, OWASP Standard
- Reporting Common Vulnerability Scoring Systems (CVSS), Report Structure

2. Information Gathering

- Passive Method Online Information Gathering, Email Harvesting, Tools Pentest (Burp suite), Additional Resources
- Active Method DNS Enumeration, Sub Domain Enumeration, Port Scanning, SSL & TLS Enumeration

3. Vulnerability Scanning

- Automated Tools, CMS Scanning & Vulnerabilities

4. Buffer Overflows

- Fuzzing, Win32 Buffer Overflow Exploitation, Linux Buffer Overflow Exploitation

5. Privilege Escalation

- Linux Local Privilege Escalation, Windows Local Privilege Escalation

6. Web Application Attacks

- Burp Suite Tools, XSS, Command Injection

7. Web Application Attacks

- Command Injection, File Inclusion, Password Attacks, SQL Injection

Profil Mentor

Anggrahito

Anggrahito, MBA, adalah seorang Expert di bidang Cybersecurity dan Penetration Testing dengan latar belakang akademis dan profesional yang kuat di keamanan siber. Keahliannya meliputi vulnerability assessment, ethical hacking, network security, dan penyusunan kebijakan keamanan informasi. Dengan 1 batch kelas di Taalenta, Anggrahito mengajar peserta memahami metodologi penetration testing, teknik identifikasi celah keamanan, serta strategi mitigasi risiko siber. Pendekatannya menggabungkan perspektif bisnis dari latar MBA dengan kompetensi teknis, relevan bagi profesional IT dan manajemen keamanan organisasi.

Investasi Program

Pilihan paket yang tersedia untuk program ini:

Elite Rp 300.000 Rp 155.000 per peserta	Supreme Rp 400.000 Rp 175.000 per peserta
---	---

Jadwal & Sesi

Sesi 1 4 Sep 2023	Introduction Introduction > Penetration Testing Introduction - Knowledge Base (About OS Pentest and Essential Tools) - Legal and Opportunity > Methodology and Standard - Hacking Methodology - Bug Bounty Workflows - OWASP Standard > Reporting - Common Vulnerability Scoring Systems (CVSS) - Report Structure 1. > Penetration Testing Introduction 2. Knowledge Base (About OS Pentest and Essential Tools) - Legal and Opportunity 3. > Methodology and Standard 4. Hacking Methodology - Bug Bounty Workflows - OWASP Standard 5. > Reporting 6. Common Vulnerability Scoring Systems (CVSS) - Report Structure
Sesi 2 6 Sep 2023	Information Gathering Information Gathering > Passive Method - Online Information Gathering - Email Harvesting - Tools Pentest (Burp suite) - Additional Resources > Active Method - DNS Enumeration - Sub Domain Enumeration - Port Scanning - SSL & TLS Enumeration 1. > Passive Method 2. Online Information Gathering - Email Harvesting - Tools Pentest (Burp suite) - Additional Resources 3. > Active Method 4. DNS Enumeration - Sub Domain Enumeration - Port Scanning - SSL & TLS Enumeration
Sesi 3 9 Sep 2023	Vulnerability Scanning Vulnerability Scanning - Automated Tools - CMS Scanning & Vulnerabilities 1. Automated Tools - CMS Scanning & Vulnerabilities
Sesi 4 10 Sep 2023	Buffer Overflows Buffer Overflows - Fuzzing - Win32 Buffer Overflow Exploitation - Linux Buffer Overflow Exploitation 1. Fuzzing - Win32 Buffer Overflow Exploitation - Linux Buffer Overflow Exploitation
Sesi 5 16 Sep 2023	Privilege Escalation Privilege Escalation - Linux Local Privilege Escalation - Windows Local Privilege Escalation Web Application Attacks - Burp Suite Tools - XSS - Command Injection 1. Linux Local Privilege Escalation - Windows Local Privilege Escalation 2. Web Application Attacks 3. Burp Suite Tools - XSS - Command Injection

Sesi 6

17 Sep 2023

Web Application Attacks

Web Application Attacks - Command Injection - File Inclusion - Password Attacks - SQL Injection

1. Command Injection - File Inclusion - Password Attacks - SQL Injection

Sesi 7

23 Sep 2023

Final Test (Optional)

Final Test (Optional) - CTF Challenge - Reporting - Presentation

1. CTF Challenge - Reporting - Presentation

Perlengkapan

- Koneksi internet
- Zoom meeting
- PC / Laptop RAM minimal 8GB(Direkomendasikan 16 GB)
- PC / Laptop terinstall VirtualBox / VM Ware

Pendaftaran

Daftar di halaman program:

taalenta.id/pti

Atau scan QR di samping untuk membuka langsung.



Kontak

PT Taalenta Digital Inteleksia

Jl. Prof. Herman Yohanes, Depok, Sleman, D.I. Yogyakarta

WhatsApp / Telepon: 0851-8313-3328

Email: halo@taalenta.id

Dokumen ini di-generate otomatis dari data terkini di sistem Taalenta. Harga, jadwal, dan ketersediaan paket dapat berubah; mohon konfirmasi ulang melalui WhatsApp/email di atas sebelum pengajuan resmi.

© 2023-2026 PT Taalenta Digital Inteleksia. Versi: 2026-09-04 13:58