Enterprise Cyber Range (Top Tier) Cybersecurity Lab 2026 v5

Why is a Cyber Security Lab considered one of the top-tier training environments?

Because each participant is provided with up to two VPS instances and works within a simulated real-world (enterprise) environment. It involves multi-layer attack scenarios rather than a single isolated machine. It includes advanced techniques such as pivoting, lateral movement, and privilege escalation.

This type of lab is typically used for exams, assessments, and red team simulations. It also supports Red Team vs Blue Team cyber war exercises in a controlled enterprise-like environment.

Cyber Security Lab Tier Levels :
1. Personal Lab (Basic offline learning environment)
2. Playground (Skill practice challenge platform)
3. Structured Lab **(**Guided structured learning path)
4. Advanced Lab **(**Multi-machine attack scenarios)
5. Enterprise Cyber Range (Red vs Blue): Highest Tier : Enterprise Cyber Range: Realistic enterprise environment with per-participant VPS, chaining exploits, pivoting, privilege escalation, and red blue simulation exercises

{><}XCODE XCODEHOSTER

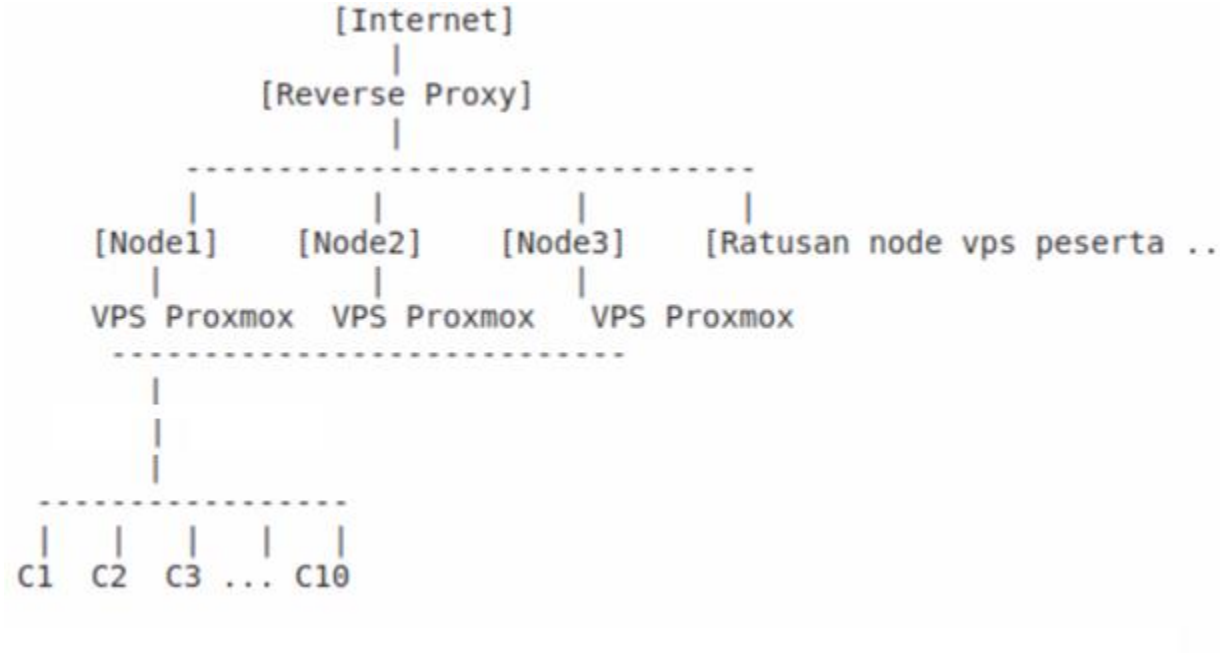
https://hackerbootcamp.asia

Bootcamp exam flow and general information

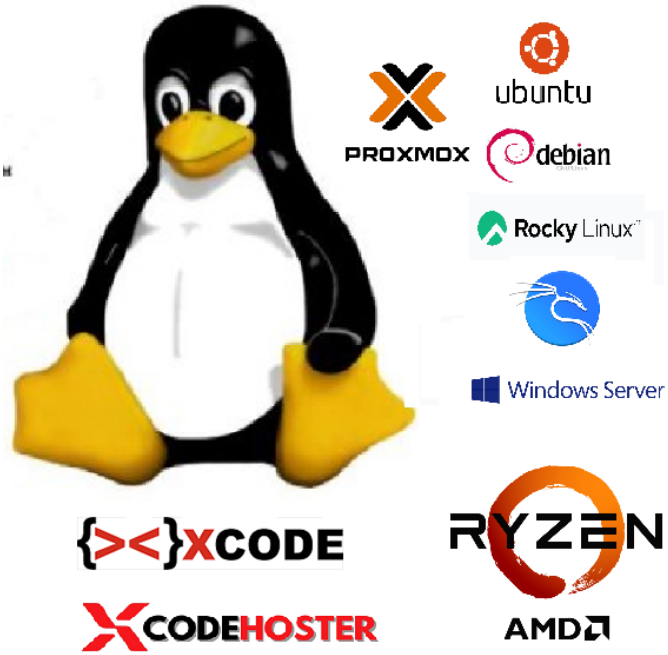
Each participant is provided with two VPS instances for the exam and can choose their own operating system, including Ubuntu Server, Debian, Rocky Linux, or FreeBSD.

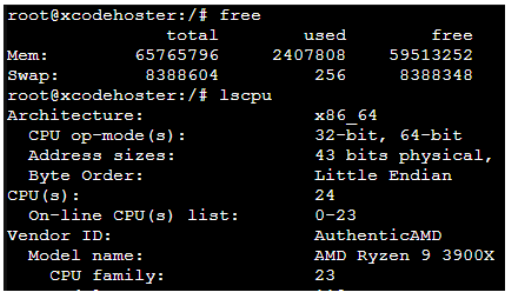
Remote Lab 1

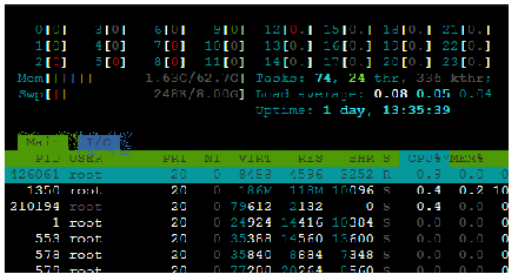
Advanced Lab for HackerBootcamp Asia participants.



Lab di atas mencakup beragam target, seperti web dan API.
Teknologi Data Center dengan 24 Server Baremetal menyediakan VPS dikembangkan secara mandiri oleh X-Code (PT Teknologi Server Indonesia).

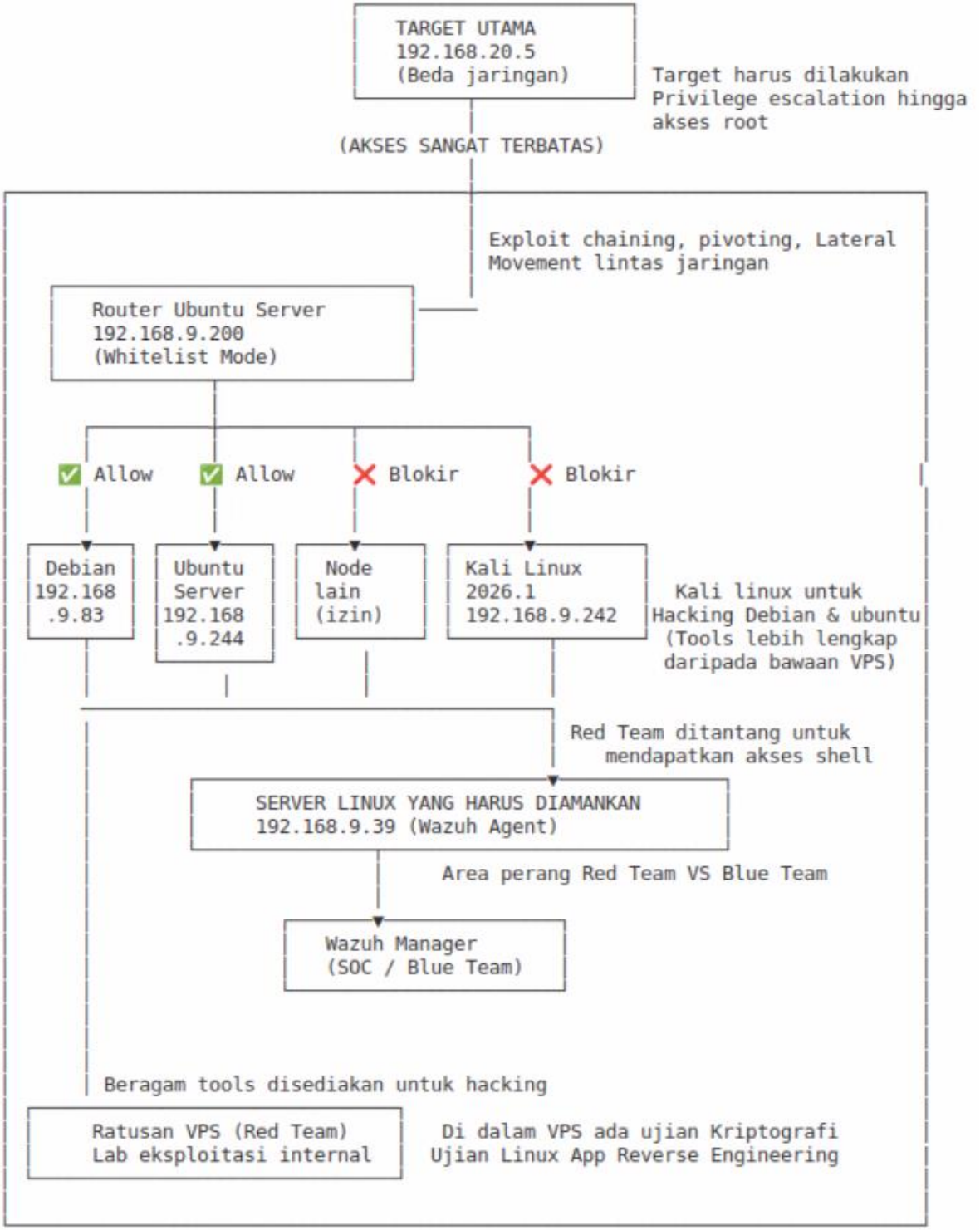






Remote Lab 2

Enterprise Lab / Cyber Range (Full) for HackerBootcamp Asia participants

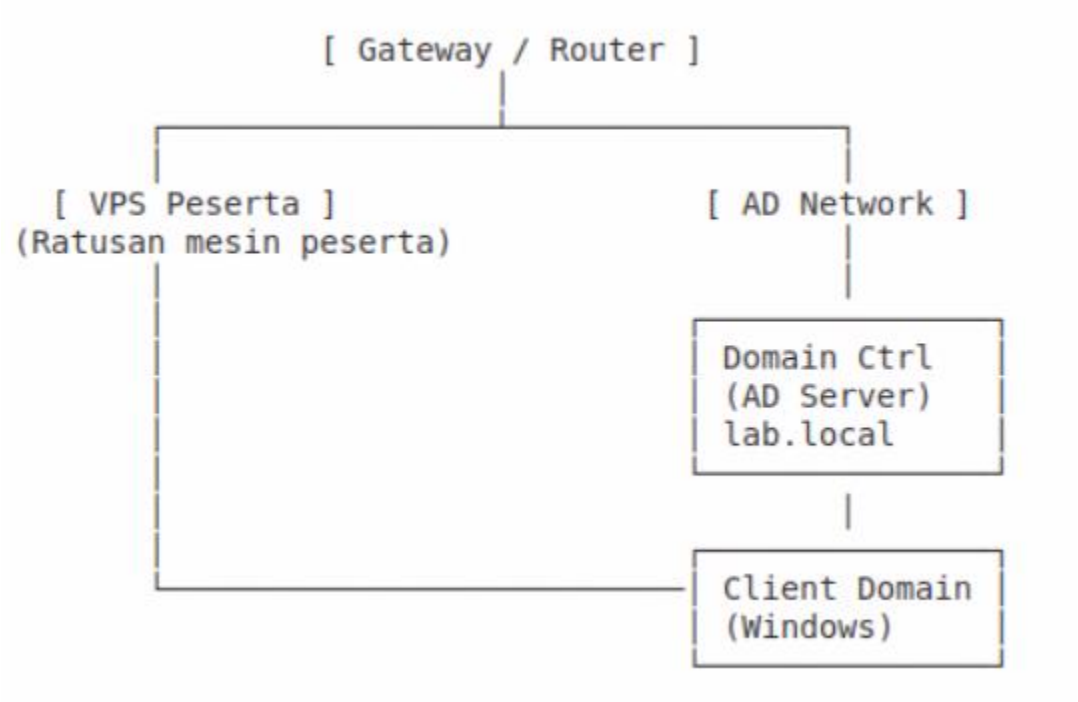


Node lain di Lab 2: Target Server Joomla, Server Apache, dan sebagainya.

Enterprise Cyber Range (Red vs Blue):

Participants are divided into two roles: the red team and the blue team.
The blue team is equipped with a monitoring system using Wazuh SIEM along with auditctl, which are integrated with Wazuh to enable centralized system activity monitoring and analysis.

Remote Lab 3
Active Directory Attack Chain Lab



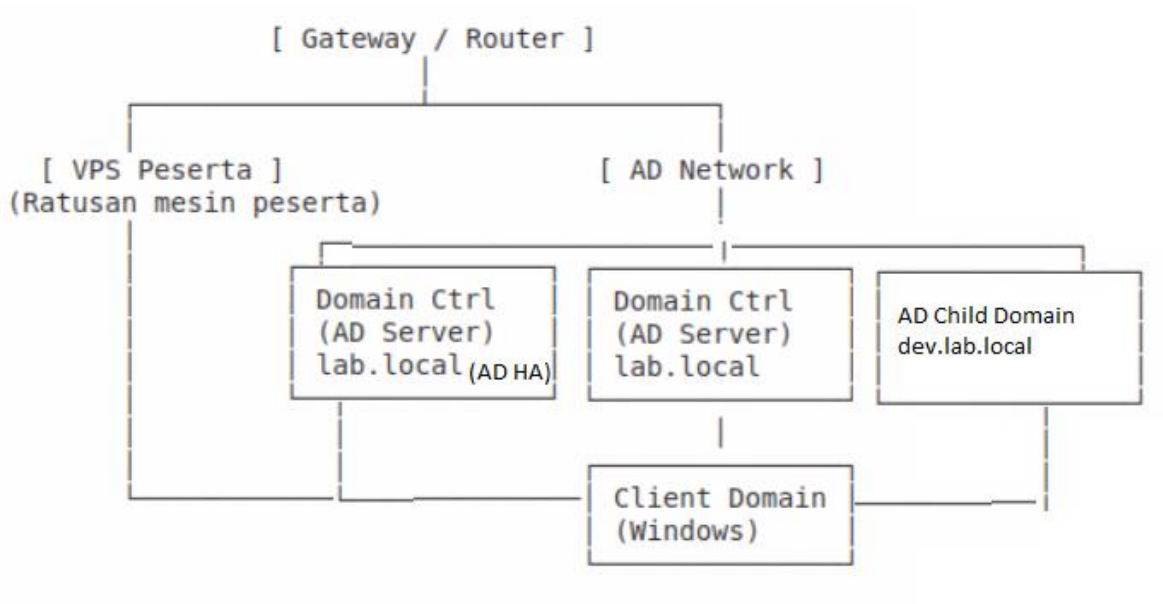
Advanced Active Directory Attack Techniques: Full-Chain Domain Compromise via Lateral Movement and Kerberos Ticket Forgery (Golden Ticket) for Persistent Administrative Access.

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 Windows
   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

Remote Lab 4

Kiamat Infrastruktur: Runtuhnya Benteng Terakhir Otoritas Active Directory

Inter-Domain Trust Relationship Exploitation (Cross Domain)



Cross-Domain Escalation (Expert Level)

Golden Ticket attack

Cross-Node Security Identifier (SID) Harvesting (ExtraSID)

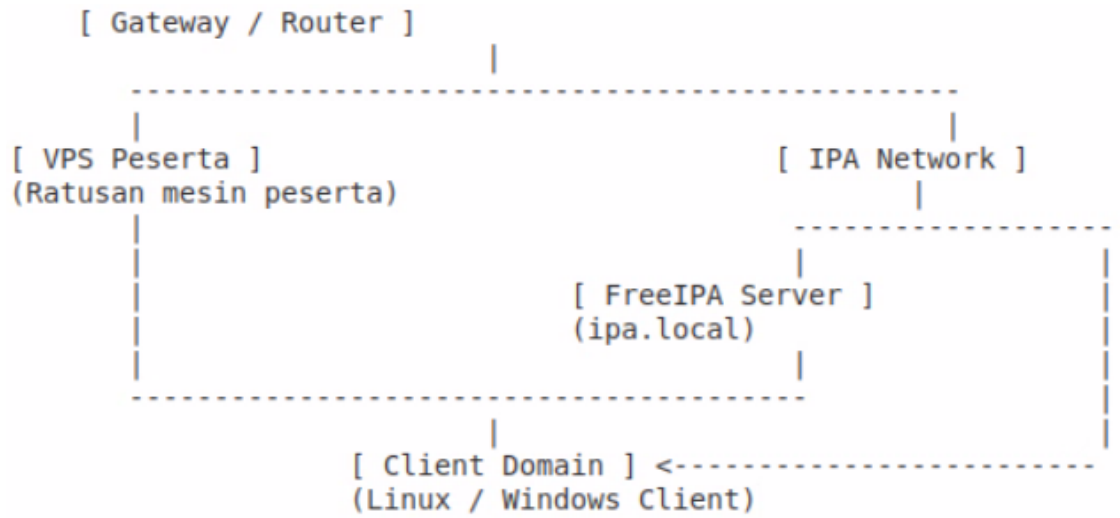
Parent-Child trust exploitation

Enterprise Admin takeover.

Remote Lab 5

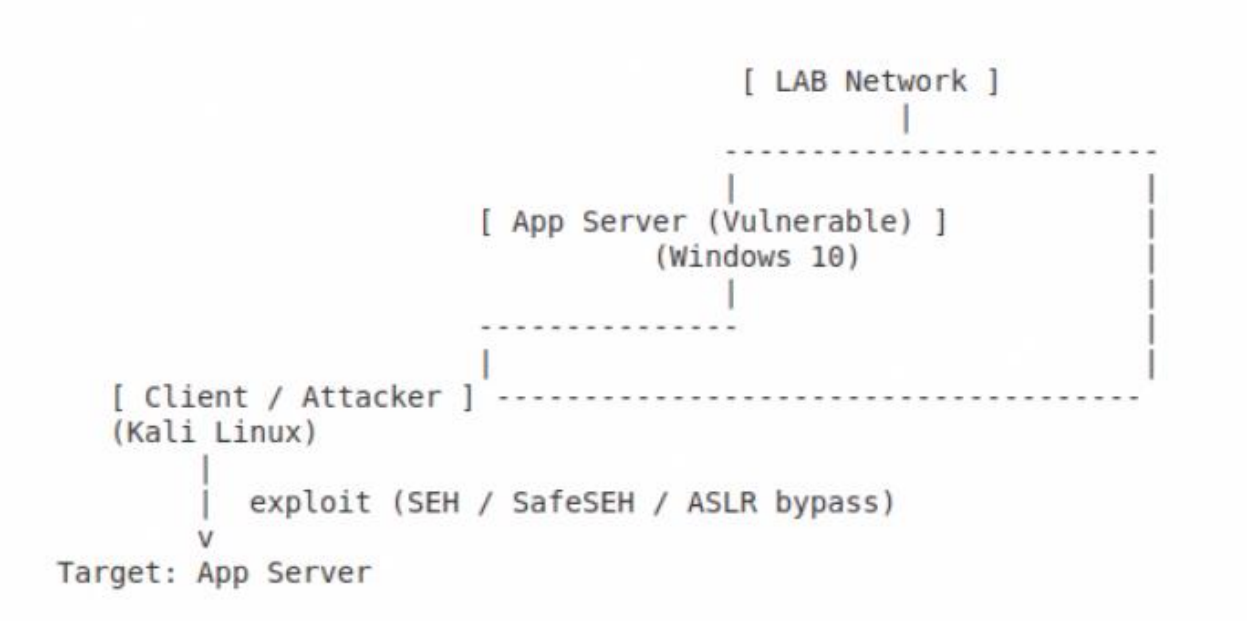
Enterprise Identity Security: Compromising FreeIPA Domain Controller through Credential Validation

Full Domain Takeover: Exploiting Identity Management in FreeIPA



Lab 6

Exploit Development Lab



Additional learning support
You not only get access to download more than 50 virtual machines that you can install on your own PC or laptop to support hands-on learning throughout the bootcamp, but you also get access to remote lab environments, along with dozens of hacking tools and exploits.

Support for Ethical Hacking & Security modules with over 2,000 pages of material, along with a variety of slides from X-code (PT. Teknologi Server Indonesia) for bootcamp sessions.

Internship for bootcamp participants

.

The internship is conducted with a direct industry immersion approach as a SOC Analyst responsible for monitoring the company's cloud VPS and shared web hosting services. Within the SOC structure, roles are divided into SOC L1 and SOC L2.

In addition, for participants focusing on becoming pentesters, the tasks include performing penetration testing on the company's own systems to identify and evaluate security vulnerabilities.

The monitoring tools used are comprehensive, including Wazuh SIEM, Splunk, Zabbix, Prometheus, Grafana, Netdata, as well as various supporting tools for monitoring, logging, and observability.

The Technologies We Use in Our Work

Technology & Infrastructure: Virtualisasi, Network Architecture, Security Stack & Monitoring System

21+ Years of Experience, 5,000+ Clients Served, 129,000+ Community Members, Cybersecurity Community Since 2004

We are an Indonesian technology company building an independent ecosystem in cybersecurity, encompassing penetration testing, security hardening, SOC services, public cloud and VPS, shared hosting, self managed servers, R&D platforms and automation, IT consulting, AI services, cybersecurity education and bootcamps, as well as software development projects.

Our technologies include a wide range of systems, algorithms, codebases, panels, and infrastructure built entirely from scratch, enabling us to operate as a comprehensive and modern technology innovator.

Our cloud infrastructure is designed with reliability, scalability, and security in mind. Parts of our storage architecture utilize triple replication with Ceph to ensure data redundancy and high availability. Our public cloud platforms are powered by technologies such as OpenStack, Canonical MicroCloud, Proxmox, and other supporting systems, combined with custom automation and security frameworks developed internally from the ground up, from architecture design, algorithms, and system engineering to core coding implementations.

For infrastructure and security monitoring, we utilize various technologies such as Wazuh SIEM, Splunk SIEM, Grafana, Prometheus, Netdata, and Zabbix, along with other observability and monitoring platforms. For container management and Docker-based system orchestration, we also use Docker management interfaces such as Portainer, along with various automation and system management tools.

For backend development, we utilize modern technologies including PHP, Node.js, Next.js, Rust, and other advanced development stacks to build scalable, secure, and high performance platforms.

We operate across multiple technology domains as an IT and technology consultancy and service company, infrastructure and cloud company, cybersecurity company, AI service provider, and software product company.

As a cybersecurity learning platform, we were founded on June 5, 2004. We also operate the largest cybersecurity forum in Indonesia, with more than 129,000 members.

We have extensive experience conducting penetration testing for various companies and have handled a wide range of cybersecurity incident cases. We have proudly served over 5,000 clients, who have consistently provided nearly flawless testimonials, a true testament to the quality, reliability, and trust we deliver.

X-Code Bootcamp - Penetration Testing & Cyber Security Engineer
Tersedia program magang! Pemagang akan terjun langsung di Pentest & SOC, menggunakan tools industri modern:. Proxmox, Wazuh SIEM, Splunk SIEM, Grafana, Prometheus, Netdata dan sistem internal milik PT

Bagi peserta yang ingin mendapatkan pengalaman industri nyata yang langsung bisa dimasukkan ke portofolio!

Materi yang Dipelajari:
Alur Penetration Testing Lengkap: Mulai dari penyusunan proposal, NDA, kontrak, eksekusi pentest, penyusunan laporan teknis & non-teknis, manajemen bisnis. Pentest modes: Learn Black-box & Gray-box. Web Exploitation: XSS, LFI, RFI, SQLi, Command Injection, CSRF, dll (+mitigasi), SIEM & Log Analysis: Instalasi Wazuh, deteksi brute-force, serangan web, perubahan sistem. Belajar OWASP Top 10. API Pentest: Auth bypass, input validation flaws, REST API exp. WAF Bypass: XSS & SQLi bypass. Target tidak hanya PHP, tapi juga Node.js. Exploit Dev: BOF, SEH, SafeSEH, ASLR, DEP/NX bypass, egghunter, jumpshort, dll. Fuzzing & Exploitation: Bug finding & shellcode execution (Windows/Linux). Custom Exploit: Buat exploit sendiri, bind/reverse shell (msfvenom) Privilege Escalation: Kernel, sudo, polkit, misconfig (Linux & BSD). Network Attack: ARP spoof, bruteforce, sniffing, DoS, router exploit, IPcam Exploitation. Nessus & Metasploit: Scanning & eksploitasi. Wireless Pentest: recon, deauth, WPA/WPA2 testing, mitigasi. Advanced Active Directory Attack Techniques: Full-Chain Domain Compromise via Lateral Movement and Kerberos Ticket Forgery (Golden Ticket) for Persistent Administrative Access., Secure Coding & IR: Patch cepat, respon insiden real-time. Hardening & Defensive Eng: WAF, anti-bf, anti-port-scanner, firewall, patch. STAR interview method, careers in pentesting, & soft skills for translating tech to business

Belajar langsung: Menjadi:Pentester, SOC Level 1, SOC Level 2.
Pendaftaran & Info:
- WA Admin 1: 0857-2891-7933, - WA Admin 2: 0895-4207-54477