

X-Code Offensive Security Certification

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.



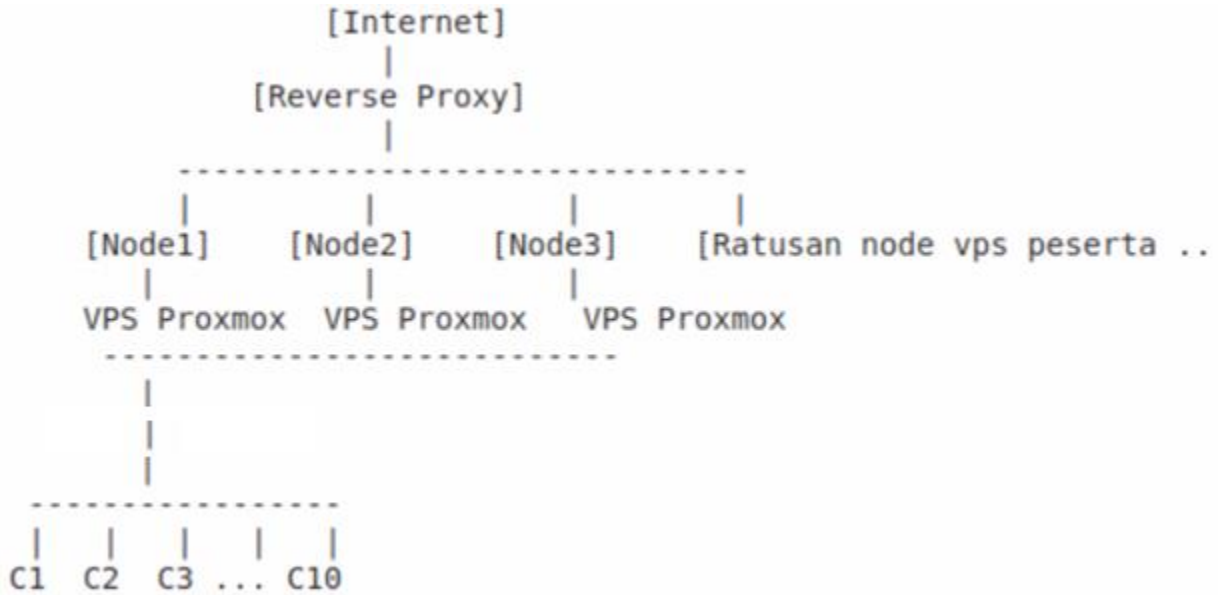
Cyber Security Lab Tier Levels :

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



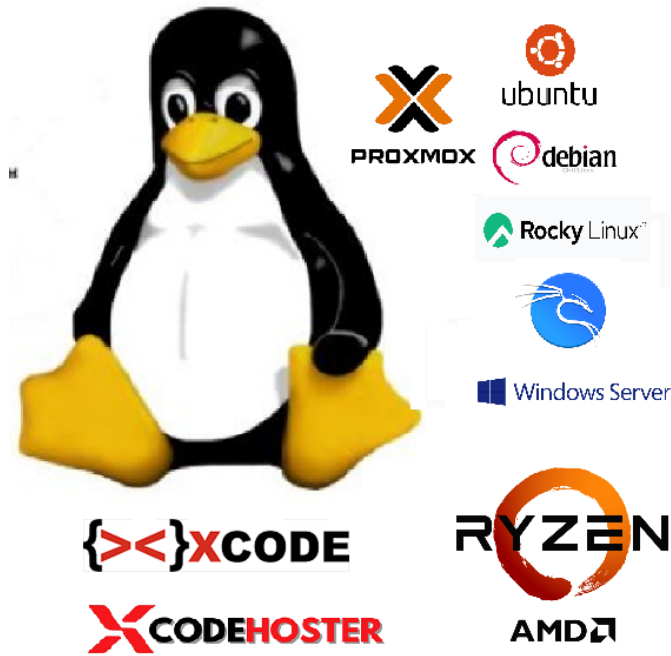
Remote Lab 1

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).



```

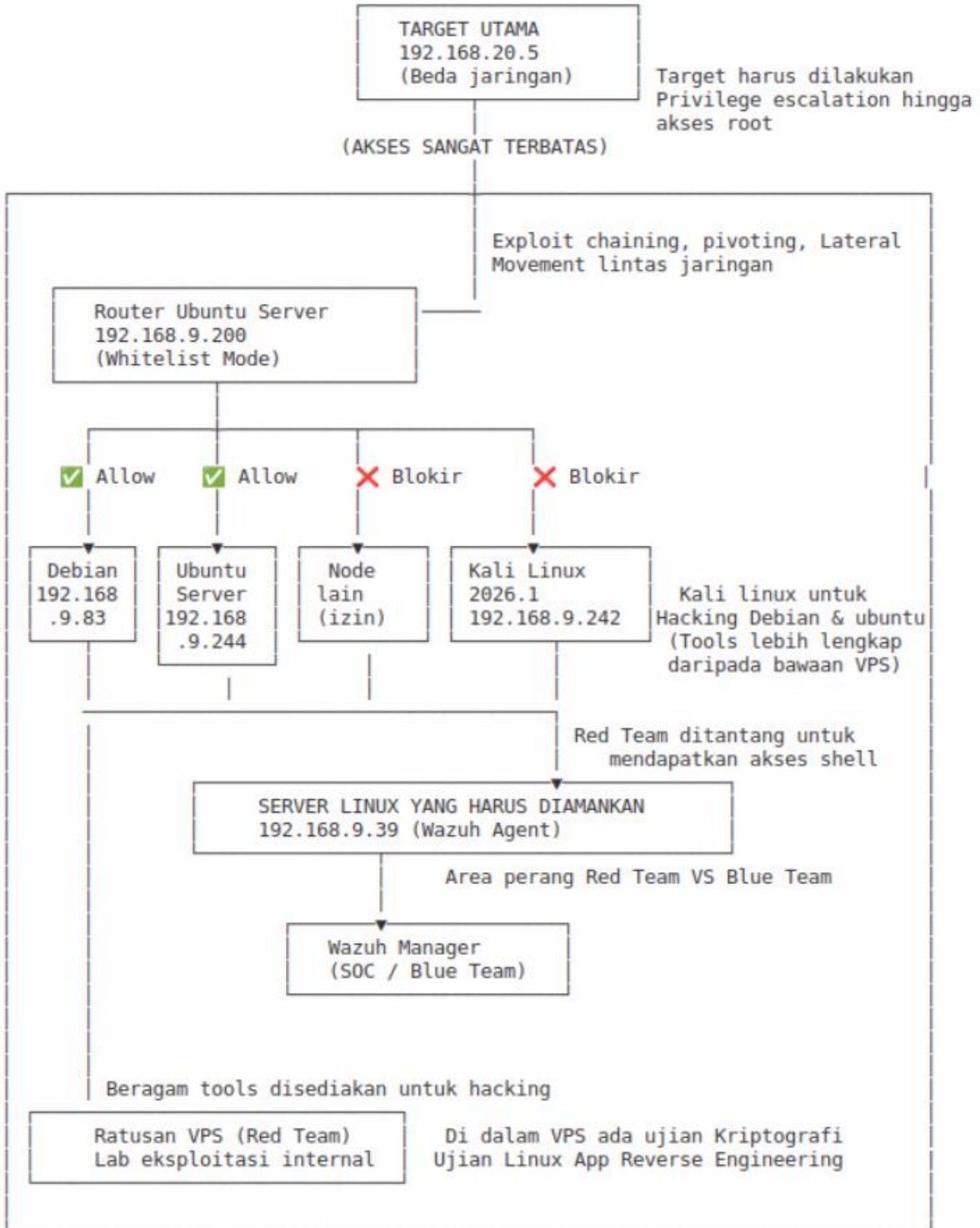
root@xcodehoster:/$ free
              total        used        free
Mem:           65765796      2407808      59513252
Swap:          8388604         256         8388348
root@xcodehoster:/$ lscpu
Architecture:          x86_64
CPU op-mode(s):        32-bit, 64-bit
Address sizes:          43 bits physical,
Byte Order:             Little Endian
CPU(s):                 24
On-line CPU(s) list:   0-23
Vendor ID:              AuthenticAMD
Model name:             AMD Ryzen 9 3900X
CPU family:             23
  
```

```

01[ ]  3[0]  6[0]  9[0]  12[0]  15[0]  18[0]  21[0]
1[ ]  4[0]  7[0]  10[0]  13[0]  16[0]  19[0]  22[0]
2[ ]  5[0]  8[0]  11[0]  14[0]  17[0]  20[0]  23[0]
Mem| | | | | 1.69G/62.7G| Tasks: 74, 24 thr, 398 kthbr|
Swp| | | | | 248K/8.00G| Total uptime: 0.08 0.05 0.04
                                     Uptime: 1 day, 13:35:39
  
```

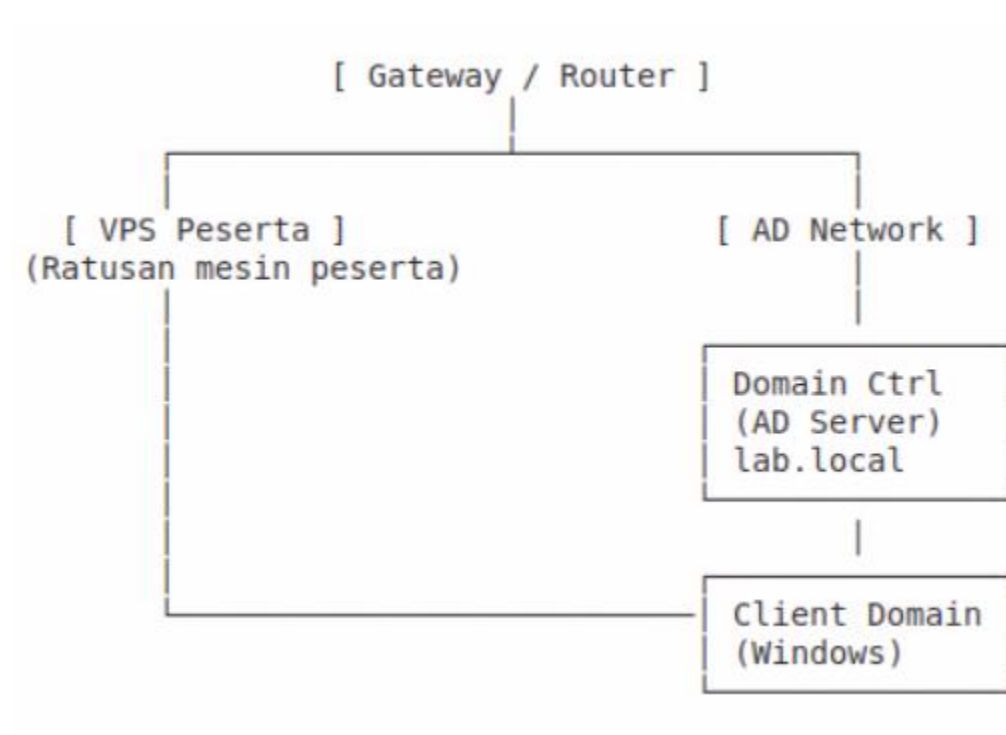
pid	USER	PR	NI	VIRT	RES	SHR	S	CPUS	MEM%
126061	root	20	0	8458	4536	3252	R	0.3	0.0
1350	root	20	0	786V	118M	10096	S	0.4	0.2
210194	root	20	0	79612	2132	0	S	0.4	0.0
1	root	20	0	24924	2416	10304	S	0.0	0.0
553	root	20	0	35368	4560	15600	S	0.0	0.0
573	root	20	0	35840	8834	7348	S	0.0	0.0
573	root	20	0	37200	20264	5560	S	0.0	0.0

Remote Lab 2
Enterprise Lab / Cyber Range (Full) for HackerBootcamp Asia participants



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

Remote Lab 3
Active Directory Attack Chain Lab



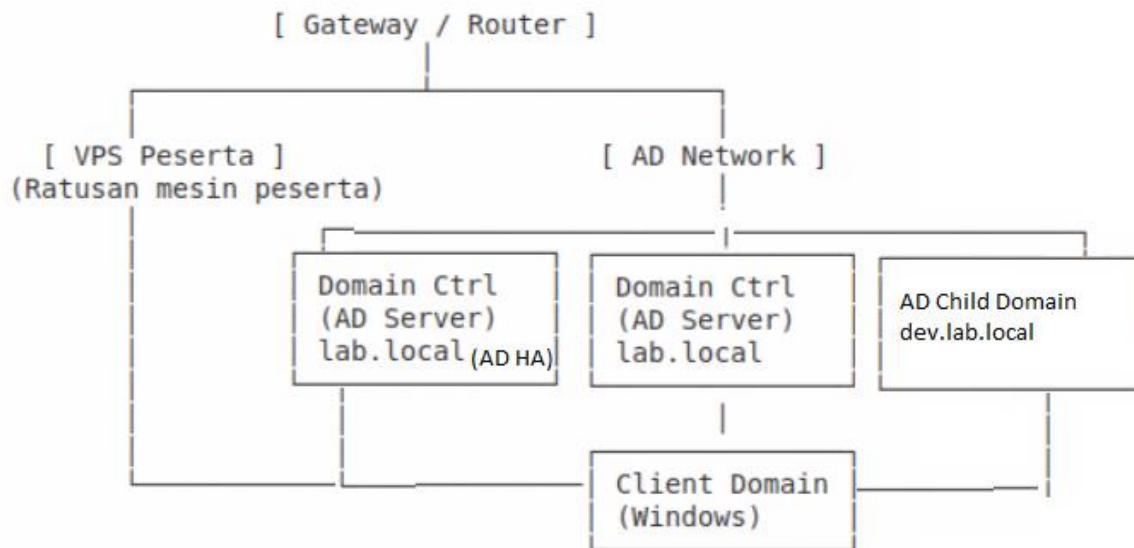
Advanced Active Directory Attack Techniques: Full-Chain Domain Compromise via Lateral Movement and Kerberos Ticket Forgery (Golden Ticket) for Persistent Administrative Access.

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

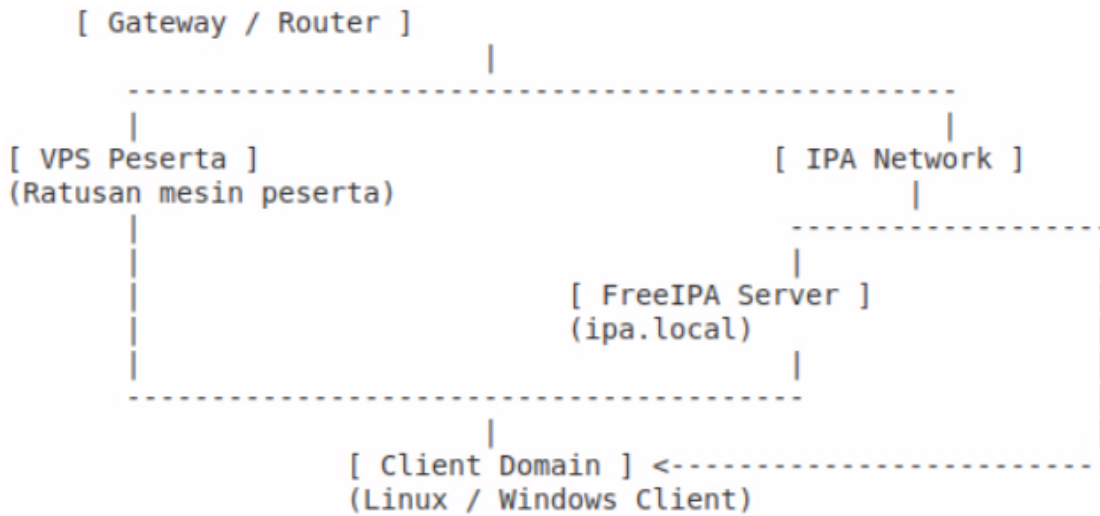
Cross-Node Security Identifier (SID) Harvesting (ExtraSID)

Parent-Child trust exploitation

Enterprise Admin takeover.

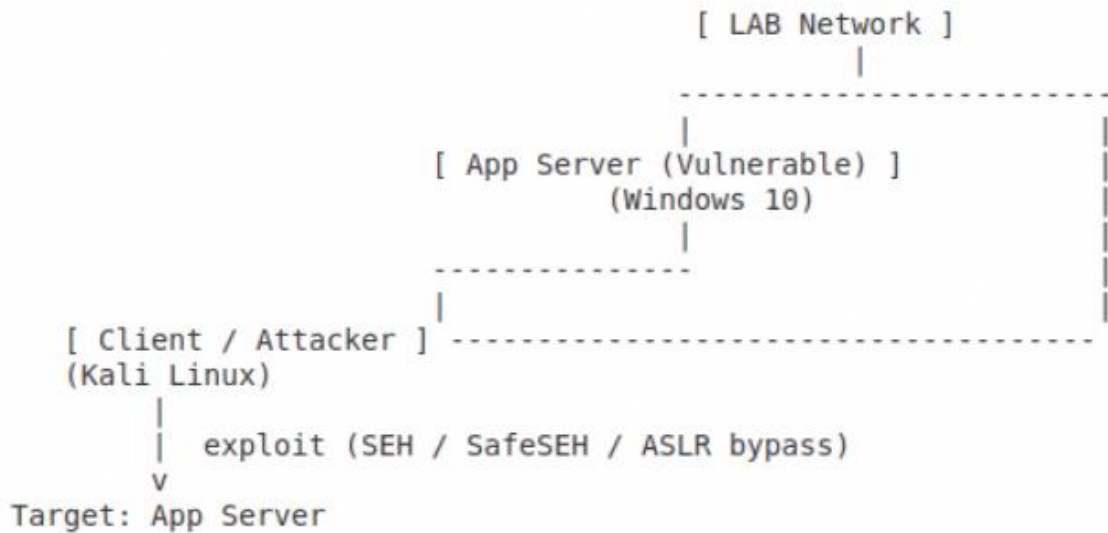
Remote Lab 5

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.



This video-based course consists of 16 sessions and is available free of charge. The full syllabus can be accessed at the following link: https://kelashacker.com/elitehackerv3_online.pdf. The Active Directory (AD) and FreeIPA topics will be delivered live in a single session.

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

.

Pendaftaran & Info:

- WA Admin 1: 0857-2891-7933

- WA Admin 2: 0895-4207-54477