# Overview Workshop & Pengenalan Infrastruktur Jaringan dan Server

Tim ITB

# Outline

1. Latar Belakang
2. Objective Pelatihan
3. Output dan Outcome Pelatihan
4. Pendekatan dan Metodologi
5. Infrastruktur Jaringan dan Server
6. Tools yang Digunakan: Server, Tools Serangan, Tools Pertahanan
7. Topologi Jaringan dan Server

# Latar Belakang Permasalahan

1. Serangan siber, seperti **defacing** dan **brute force attacks**, semakin sering menargetkan situs pemerintah.
2. Banyak situs pemerintah yang diretas dan disalahgunakan untuk **iklan judi online** atau konten ilegal.
3. Kelemahan dalam **pengelolaan keamanan jaringan dan server** sering menjadi titik lemah yang dieksploitasi hacker.

# Objective Pelatihan

1. Pemahaman dasar tentang isu defacing situs pemerintah untuk iklan judi online.
2. Pemahaman dan best practices untuk pengamanan jaringan dan server di situs pemerintah.
3. Meningkatkan kemampuan peserta dalam menangani dan mencegah serangan cyber khususnya defacing situs pemerintah.

# Output Pelatihan

1. Peserta mampu melakukan **konfigurasi keamanan** server dan jaringan.
2. Peserta memahami penggunaan **tools** untuk mendeteksi, mencegah, dan mengatasi serangan.
3. Peserta dapat mengidentifikasi potensi serangan dan mengambil langkah preventif.

# Outcome Pelatihan

1. Infrastruktur jaringan dan server institusi pemerintah lebih **aman** dari serangan cyber, khususnya defacing judi online.
2. Penguatan sistem keamanan yang mengurangi potensi menurunnya reputasi institusi pemerintah.
3. Meningkatnya produktivitas karena memiliki waktu luang yang bisa digunakan untuk hal yang lebih produktif dari pada mengatasi insiden cyber security terus-menerus.

# Pendekatan dan Metodologi

1. Menggunakan **best practices** dalam keamanan infrastruktur jaringan dan server.
2. Sesi akan fokus pada **konsep singkat** yang diikuti dengan **praktik langsung**.
3. Peserta tidak perlu melakukan instalasi, semua tools sudah diinstal sebelumnya, tinggal melakukan **konfigurasi** dan **menjalankan command line**.

# Infrastruktur Jaringan dan Server

1. Server dijalankan di atas **cloud**, dengan setiap peserta mengakses **VM** yang sudah disiapkan.
2. Terdapat 6 kelompok, masing-masing kelompok memiliki **blok IP ( x.x.x.x – y.y.y.y**).
3. **DNS Primary** disiapkan untuk setiap kelompok, serta **DNS Resolver** yang digunakan bersama.
4. Setiap hosts memiliki server, serta tools untuk menyerang dan bertahan

# Server

1. Sistem Operasi Ubuntu 22.04
2. **Apache**: Web server untuk hosting aplikasi web dan simulasi serangan.
3. **MySQL**: Database server yang digunakan dalam aplikasi seperti DVWA (Damn Vulnerable Web App).
4. **Bind9**: DNS server untuk mengelola dan mensimulasikan serangan DNS dan implementasi DNSSEC

# Tools untuk Serangan

1. **SQLMap**: Untuk melakukan serangan **SQL Injection** otomatis pada website yang rentan.
2. **Hydra**: Tool brute force attack yang digunakan untuk mencoba menebak login admin pada layanan **SSH**.
3. **dnsspoof**: Tool untuk mensimulasikan serangan **DNS spoofing** sebelum implementasi DNSSEC.

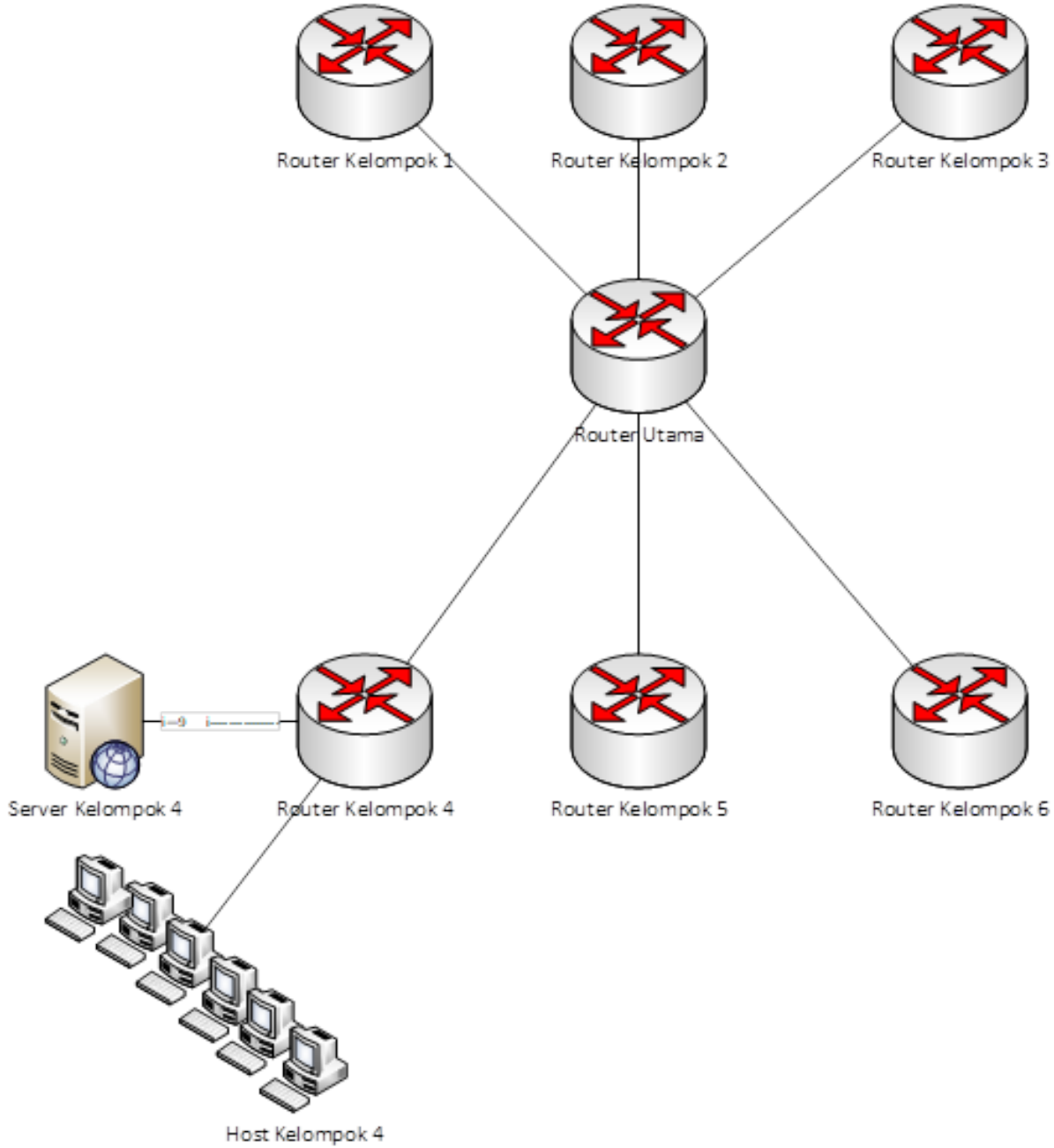
# Tools untuk Defense

1. **iptables**: Firewall untuk memfilter traffic jaringan, memblokir IP mencurigakan, dan melindungi akses ke port penting.
2. **Fail2ban**: Tool untuk memonitor percobaan brute force attack pada SSH dan secara otomatis memblokir IP yang melakukan percobaan login berulang-ulang.
3. **ModSecurity**: Web Application Firewall (WAF) yang digunakan untuk mencegah serangan web seperti SQL Injection dan XSS.
4. **DNSSEC**: Digunakan untuk memastikan integritas DNS dan mencegah serangan DNS spoofing.

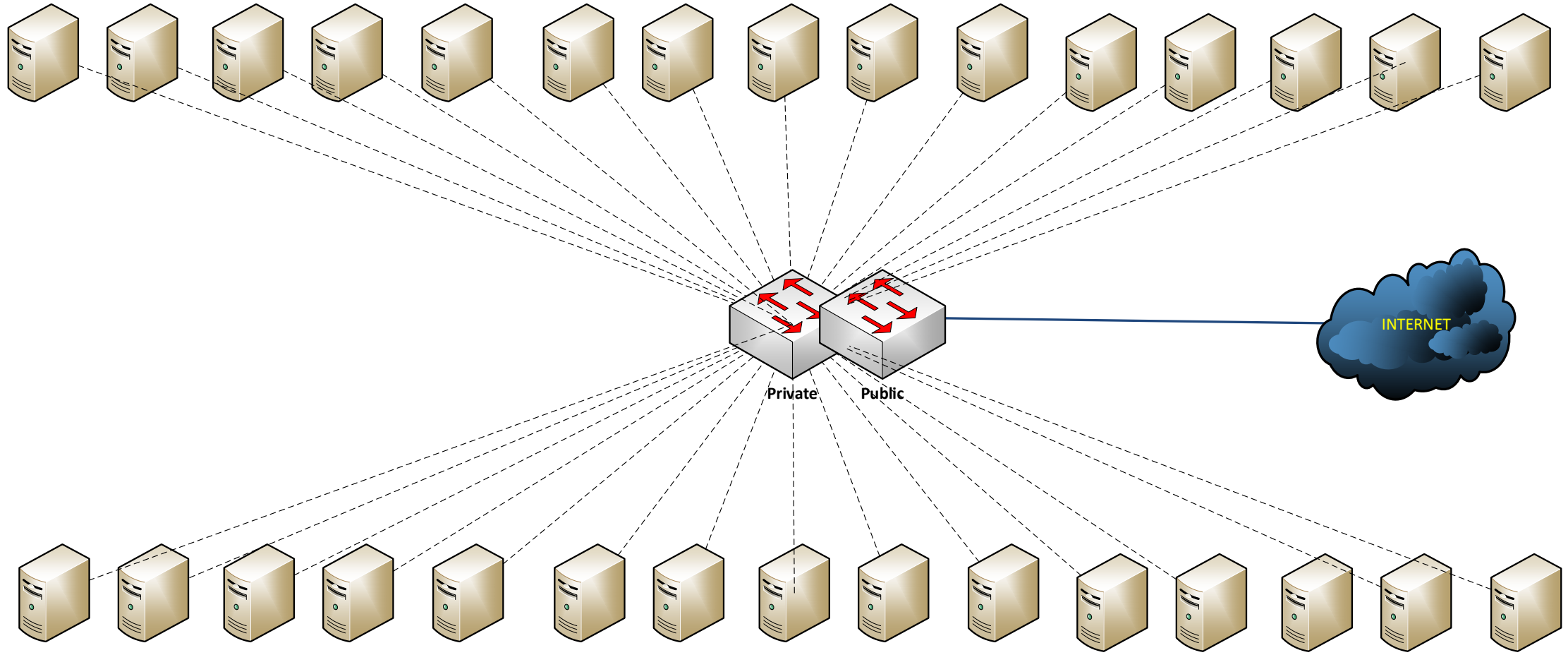
# Topologi Jaringan dan Server

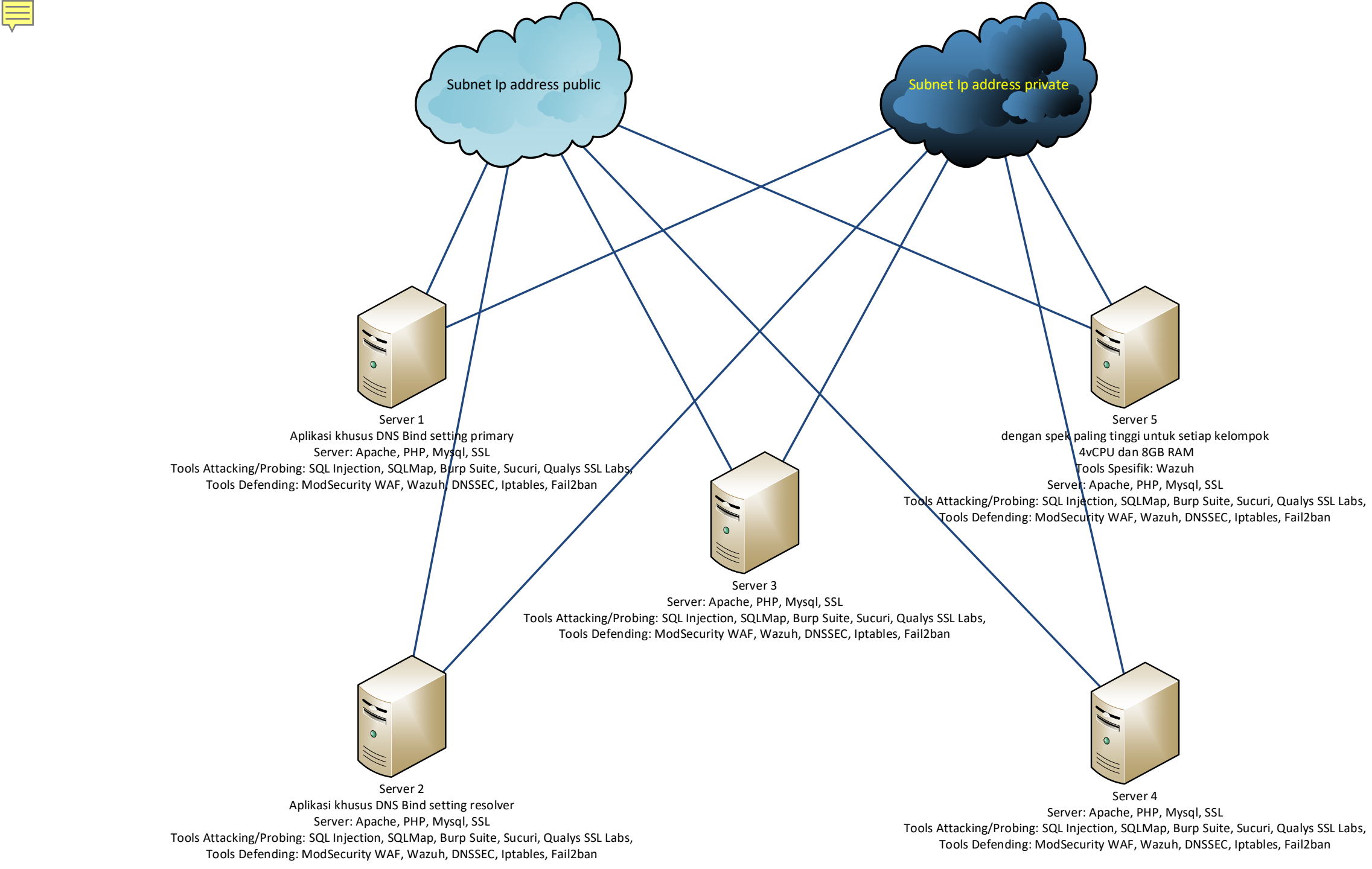
1. Setiap kelompok menggunakan **subnet terpisah** (misalnya **192.168.10.0/24** untuk kelompok 1).
2. Terdapat **DNS Primary** per kelompok dan **DNS Resolver** terpisah untuk query DNS bersama.
3. Infrastruktur ini memungkinkan peserta untuk melakukan simulasi serangan dan pertahanan dalam jaringan yang terisolasi dengan VM.

# Topologi Ideal



# Topologi Alternatif




Subnet Ip address public
Subnet Ip address private
Server 1
Aplikasi khusus DNS Bind setting primary
Server: Apache, PHP, Mysql, SSL
Tools Attacking/Probing: SQL Injection, SQLMap, Burp Suite, Sucuri, Qualys SSL Labs,
Tools Defending: ModSecurity WAF, Wazuh, DNSSEC, Iptables, Fail2ban
Server 5
dengan spek paling tinggi untuk setiap kelompok
4vCPU dan 8GB RAM
Tools Spesifik: Wazuh
Server: Apache, PHP, Mysql, SSL
Tools Attacking/Probing: SQL Injection, SQLMap, Burp Suite, Sucuri, Qualys SSL Labs,
Tools Defending: ModSecurity WAF, Wazuh, DNSSEC, Iptables, Fail2ban
Server 3
Server: Apache, PHP, Mysql, SSL
Tools Attacking/Probing: SQL Injection, SQLMap, Burp Suite, Sucuri, Qualys SSL Labs,
Tools Defending: ModSecurity WAF, Wazuh, DNSSEC, Iptables, Fail2ban
Server 2
Aplikasi khusus DNS Bind setting resolver
Server: Apache, PHP, Mysql, SSL
Tools Attacking/Probing: SQL Injection, SQLMap, Burp Suite, Sucuri, Qualys SSL Labs,
Tools Defending: ModSecurity WAF, Wazuh, DNSSEC, Iptables, Fail2ban
Server 4
Server: Apache, PHP, Mysql, SSL
Tools Attacking/Probing: SQL Injection, SQLMap, Burp Suite, Sucuri, Qualys SSL Labs,
Tools Defending: ModSecurity WAF, Wazuh, DNSSEC, Iptables, Fail2ban

# QnA