BUKU BAHAN AJAR SISWA

KEAMANAN JARINGAN

Program Keahlian Teknik Jaringan Komputer dan Telekomunikasi (TJKT)

Disusun berdasarkan Naskah Soal LKS SMK Tingkat Kabupaten Tasikmalaya Tahun 2026

Bidang Cyber Security (Hardening & Capture the Flag) dan Firewall/VPN pada Bidang IT Network System Administration

Untuk Jenjang Kelas XI SMK — Jilid 1 (Elemen 1–5)

Yusuf Burhani, S.Pd., S.Kom

Kata Pengantar

Buku ini disusun sebagai bahan ajar bagi peserta didik mata pelajaran Keamanan Jaringan pada Program Keahlian Teknik Jaringan Komputer dan Telekomunikasi (TJKT) di Sekolah Menengah Kejuruan kelas XI, sebagai Jilid 1 dari dua jilid buku ini.
Jilid 1 ini mencakup Bab 1 sampai Bab 6 (Elemen 1–5). Jilid 2 untuk kelas XII melanjutkan Bab 7 sampai Bab 11 (Elemen 6–9), dilengkapi glosarium dan lampiran. Penyusunan materi mengacu pada kisi-kisi soal Lomba Kompetensi Siswa (LKS) SMK Tingkat Kabupaten Tasikmalaya Tahun 2026, khususnya Bidang Cyber Security (sesi Hardening dan Capture the Flag) serta bagian keamanan infrastruktur (firewall nftables dan VPN) pada Bidang IT Network System Administration.

Materi dalam buku ini disusun ke dalam sembilan elemen kompetensi, delapan di antaranya bersifat wajib karena merupakan kompetensi inti yang diujikan pada sesi Tes Praktik Hardening, meliputi keamanan akses perangkat, firewall dan keamanan port, deteksi dan pencegahan intrusi, kriptografi terapan, keamanan basis data, keamanan akun pengguna, keamanan koneksi remote (VPN), serta forensik digital dasar. Satu elemen tambahan bersifat pengayaan, yaitu Capture The Flag, yang memperkuat pola pikir problem-solving keamanan siber setelah kedelapan elemen wajib dikuasai.

Setiap bab disusun dengan struktur yang konsisten, yaitu tujuan pembelajaran, uraian materi dilengkapi contoh perintah (command) yang dapat dipraktikkan langsung, aktivitas pembelajaran, rangkuman, serta soal latihan/refleksi. Struktur ini dimaksudkan untuk memudahkan peserta didik memahami konsep keamanan siber secara bertahap sekaligus mempersiapkan diri menghadapi praktik hardening sistem nyata maupun kompetisi keahlian seperti LKS.

Semoga buku ini bermanfaat sebagai pegangan belajar yang sistematis, aplikatif, dan relevan dengan kebutuhan dunia kerja serta perkembangan ancaman keamanan siber yang terus berkembang.

Akhir kata, keamanan siber bukanlah tujuan akhir yang dapat dicapai sekali dan selesai, melainkan proses berkelanjutan yang menuntut kewaspadaan, pembelajaran terus-menerus, dan adaptasi terhadap ancaman baru yang senantiasa berkembang. Semangat inilah yang diharapkan tertanam pada diri peserta didik setelah mempelajari buku ini, bukan sekadar penguasaan teknis semata.

Penyusun

Daftar Isi

Peta Kompetensi Buku

Tabel berikut memetakan setiap bab terhadap elemen target pembelajaran sebagaimana termuat dalam dokumen Target Pembelajaran Keamanan Jaringan.

Bab	Judul	Elemen	Fokus Utama
1	Pendahuluan	-	Orientasi mata pelajaran
2	Keamanan Akses Perangkat (Hardening Dasar)	Elemen 1	SSH hardening, user administratif, penonaktifan layanan
3	Firewall dan Keamanan Port Jaringan	Elemen 2	UFW/nftables, TCP Wrappers, deteksi port scan, NAT
4	Deteksi dan Pencegahan Intrusi (IDS/IPS)	Elemen 3	fail2ban, auditd, Snort
5	Keamanan Komunikasi dan Kriptografi Terapan	Elemen 4	GPG, key pair, enkripsi, digital signature
6	Keamanan Basis Data	Elemen 5	mysql_secure_installation, user privilege terbatas
7	Kemanan Akun	Elemen 6	
8	Keamanan Akses VPN	Elemen 7	

BAB 1 — Pendahuluan

Keamanan Jaringan merupakan mata pelajaran lanjutan pada Program Keahlian Teknik Jaringan Komputer dan Telekomunikasi (TJKT) yang membekali peserta didik kelas XI dan XII dengan kompetensi mengamankan sistem dan infrastruktur jaringan dari berbagai ancaman siber. Mata pelajaran ini menjadi kelanjutan langsung dari Jaringan Dasar dan Administrasi Infrastruktur Jaringan yang telah dipelajari sebelumnya, dengan fokus bergeser dari membangun konektivitas menuju melindungi konektivitas tersebut.

Buku ini disusun dengan mengacu pada kisi-kisi soal Lomba Kompetensi Siswa (LKS) SMK Tingkat Kabupaten Tasikmalaya Tahun 2026, khususnya Bidang Cyber Security (meliputi sesi Hardening dan Capture the Flag) serta bagian keamanan infrastruktur pada Bidang IT Network System Administration (firewall nftables dan VPN). Sembilan elemen kompetensi dalam buku ini disusun berjenjang dari pengamanan dasar perangkat hingga analisis forensik dan simulasi capture the flag.

Tujuan Pembelajaran

- Peserta didik memahami kedudukan mata pelajaran Keamanan Jaringan dan keterkaitannya dengan kompetensi jaringan yang telah dipelajari sebelumnya.
- Peserta didik memahami sembilan elemen kompetensi yang menjadi cakupan buku ini.
- Peserta didik memahami cara menggunakan buku ini sebagai bahan belajar teori maupun praktik langsung di laboratorium.

1.1 Kedudukan Mata Pelajaran Keamanan Jaringan

Keamanan Jaringan mengajarkan cara mengidentifikasi, mencegah, mendeteksi, dan merespons ancaman terhadap sistem dan jaringan komputer. Berbeda dengan mata pelajaran sebelumnya yang berfokus pada bagaimana membangun dan mengoperasikan jaringan, mata pelajaran ini berfokus pada bagaimana jaringan dan sistem yang sudah berjalan dapat dilindungi dari akses tidak sah, kebocoran data, dan gangguan operasional.

Materi keamanan jaringan sesungguhnya bertumpu pada penguasaan sistem operasi Linux, konsep jaringan TCP/IP, serta layanan-layanan jaringan (DNS, DHCP, web server, database) yang telah dipelajari pada mata pelajaran sebelumnya. Peserta didik yang belum menguasai dasar administrasi sistem Linux disarankan meninjau kembali materi tersebut sebelum mendalami buku ini secara mendalam, khususnya terkait perintah dasar command line, manajemen user, dan manajemen layanan (service/daemon).

1.2 Sembilan Elemen Kompetensi

Target pembelajaran buku ini disusun ke dalam sembilan elemen, delapan di antaranya bersifat wajib karena merupakan kompetensi inti hardening dan keamanan infrastruktur yang diujikan pada sesi Tes

Praktik Hardening LKS (berbobot 60% nilai praktik), sementara satu elemen bersifat pengayaan sebagai penguatan pola pikir problem-solving keamanan siber.

No	Elemen	Status
1	Keamanan Akses Perangkat (Hardening Dasar)	Wajib
2	Firewall dan Keamanan Port Jaringan	Wajib
3	Deteksi & Pencegahan Intrusi (IDS/IPS)	Wajib
4	Keamanan Komunikasi & Kriptografi Terapan	Wajib
5	Keamanan Basis Data	Wajib

1.3 Struktur Buku

Buku Jilid 1 ini memuat Bab 1 sampai Bab 6: Bab 1 sebagai pendahuluan, Bab 2 hingga Bab 6 membahas Elemen 1 sampai 5 secara berurutan. Elemen 6 sampai 9 (Bab 7–11) dibahas pada Jilid 2 untuk kelas XII. Setiap bab memuat komponen yang konsisten.

- **Tujuan Pembelajaran** — kompetensi yang ingin dicapai peserta didik pada bab tersebut.
- **Uraian Materi** — penjelasan konsep dilengkapi contoh perintah (command) yang dapat dipraktikkan langsung pada Linux.
- **Aktivitas Pembelajaran** — kegiatan praktik langsung pada mesin virtual/server Linux di laboratorium.
- **Rangkuman** — inti sari materi untuk memudahkan review sebelum evaluasi.
- **Soal Latihan/Refleksi** — bahan evaluasi formatif bagi peserta didik.

1.4 Petunjuk Penggunaan bagi Guru dan Peserta Didik

1. Setiap elemen sebaiknya disertai praktik langsung di laboratorium menggunakan mesin virtual atau server Linux, agar target kompetensi dapat diukur secara objektif, sejalan dengan format penilaian praktik pada LKS (skala 100, dengan ambang nilai 90/80/70).
2. Gunakan distribusi Linux berbasis Debian/Ubuntu sebagai lingkungan praktik utama, karena paling umum digunakan pada kompetisi dan dunia kerja, meskipun konsep yang dipelajari juga berlaku pada distribusi turunan Red Hat dengan penyesuaian nama paket dan perintah.

3. Bab 2–6 (Elemen 1–5) merupakan materi wajib pada Jilid 1 ini yang sebaiknya dikuasai tuntas sebelum melanjutkan ke Jilid 2 (Bab 7–11, Elemen 6–9 dan CTF) pada kelas XII.
4. Materi firewall gateway (nftables, NAT, port forwarding) pada Bab 3 beririsan dengan mata pelajaran Administrasi Sistem Jaringan — disarankan dikoordinasikan dengan guru pengampu mata pelajaran tersebut agar tidak terjadi duplikasi materi.
5. Lanjutkan ke Jilid 2 (Kelas XII) untuk Bab 7 hingga Bab 11 sebagai kelanjutan pembelajaran, termasuk konsolidasi dan evaluasi akhir.

1.5 Persiapan Lingkungan Praktik: Instalasi VMware dan Ubuntu Server

Sebelum memulai praktik pada Bab 2 dan seterusnya, peserta didik perlu menyiapkan lingkungan virtualisasi di komputer/laptop masing-masing. Buku ini menggunakan VMware (Workstation Pro pada Windows, atau Fusion pada macOS) sebagai hypervisor utama, karena antarmukanya relatif mudah dipelajari pemula dan banyak digunakan di dunia kerja maupun kompetisi. Satu mesin virtual Ubuntu Server yang dibuat pada tahap ini akan dipakai secara berkelanjutan sebagai target hardening dari Bab 2 sampai Bab 6, sehingga konfigurasi keamanan yang diterapkan pada setiap bab menumpuk secara realistis di atas mesin yang sama.

1.6 Instalasi VMware Workstation Player/Pro

VMware Workstation Player tersedia gratis untuk penggunaan pribadi/pendidikan, sedangkan VMware Workstation Pro menyediakan fitur tambahan seperti snapshot bercabang dan jaringan virtual yang lebih fleksibel. Untuk kebutuhan praktik pada buku ini, versi Player sudah mencukupi.

Langkah	Tindakan
Unduh installer	Unduh VMware Workstation Player/Pro untuk Windows dari situs resmi vmware.com/products/workstation-player
Jalankan installer	Jalankan file .exe yang diunduh, ikuti wizard instalasi dengan pengaturan default
Terima lisensi	Pilih 'I accept the terms in the License Agreement' lalu klik Next
Pilih mode penggunaan	Pilih 'Use VMware Workstation Player for free for Non-commercial use' untuk kebutuhan pendidikan
Selesaikan instalasi	Klik Finish, lalu restart komputer apabila diminta agar driver virtualisasi aktif
Aktifkan virtualisasi di BIOS/UEFI	Pastikan fitur Intel VT-x/AMD-V sudah diaktifkan di BIOS apabila VMware menampilkan peringatan virtualisasi tidak aktif

1.7 Mengunduh Image Ubuntu Server

Ubuntu Server dipilih sebagai sistem operasi target karena bersifat open source, ringan (tanpa antarmuka grafis), dan merupakan distribusi yang paling umum digunakan pada praktik hardening maupun ujian praktik LKS Bidang IT Network System Administration.

Langkah	Tindakan

Unduh berkas ISO	Unduh Ubuntu Server LTS (format .iso) dari situs resmi ubuntu.com/download/server
Simpan lokasi berkas	Catat lokasi penyimpanan berkas ISO karena akan diminta saat membuat mesin virtual baru di VMware

1.8 Membuat Mesin Virtual Baru di VMware

Langkah	Tindakan
Buka VMware, pilih Create a New Virtual Machine	Pada halaman utama VMware Player/Workstation, klik Create a New Virtual Machine
Pilih jenis instalasi	Pilih Installer disc image file (iso), lalu arahkan ke berkas ISO Ubuntu Server yang telah diunduh
Isi identitas mesin virtual	Isi nama mesin virtual, misalnya 'Ubuntu-Server-Hardening', dan tentukan lokasi penyimpanan berkas VM
Tentukan ukuran disk	Alokasikan disk minimal 20 GB, pilih 'Store virtual disk as a single file' untuk kemudahan backup/pemindahan
Sesuaikan spesifikasi VM	Klik Customize Hardware, atur RAM minimal 2 GB dan 2 CPU core agar performa cukup untuk praktik
Atur jaringan VM	Pilih mode jaringan NAT untuk akses internet standar, atau Bridged apabila VM perlu tampil sebagai host terpisah di jaringan LAN
Mulai instalasi	Klik Finish, VMware akan otomatis menyalakan VM dan mem-boot installer Ubuntu Server dari ISO

1.9 Instalasi Sistem Operasi Ubuntu Server

Setelah VM menyala dan boot dari ISO, installer Ubuntu Server (berbasis teks/TUI) akan memandu proses instalasi melalui beberapa tahap berikut.

Tahap Instalasi	Pengaturan yang Disarankan
Pemilihan bahasa	Pilih English agar istilah teknis pada dokumentasi dan pesan error lebih mudah dicari solusinya
Konfigurasi keyboard	Gunakan layout default English (US) kecuali terdapat kebutuhan khusus
Jenis instalasi	Pilih Ubuntu Server (bukan minimized), agar paket-paket umum yang dibutuhkan Bab 2--6 sudah tersedia
Konfigurasi jaringan	Biarkan pengaturan DHCP otomatis dari VMware, catat alamat IP yang diberikan untuk keperluan akses SSH nanti
Konfigurasi proxy dan mirror	Kosongkan proxy, biarkan mirror APT default terisi otomatis
Partisi disk	Pilih 'Use an entire disk' dengan layout LVM default untuk kemudahan pemula
Profil pengguna	Isi nama lengkap, nama server (hostname), username, dan password administratif yang akan dipakai sebagai user pertama
Instalasi OpenSSH Server	Centang 'Install OpenSSH server' agar VM dapat langsung diakses melalui SSH setelah instalasi, sesuai

	kebutuhan praktik Bab 2
Featured Server Snaps	Lewati (skip) pemasangan paket snap tambahan agar instalasi tetap ringan
Selesaikan instalasi	Tunggu proses instalasi selesai, pilih Reboot Now, lalu lepas ISO installer ketika diminta

1.10 Verifikasi Instalasi dan Akses Pertama

Perintah	Fungsi
ip a	Menampilkan alamat IP yang diperoleh VM, digunakan untuk mengakses VM melalui SSH dari luar
sudo apt update && sudo apt upgrade -y	Memperbarui daftar paket dan seluruh paket terpasang agar sistem dalam kondisi mutakhir sebelum praktik hardening dimulai
ssh nama_user@alamat_ip_vm	Mengakses VM dari luar (mis. dari terminal host atau aplikasi seperti PuTTY/Terminal) menggunakan kredensial yang dibuat saat instalasi

Setelah VM Ubuntu Server berhasil diakses melalui SSH, mesin virtual ini dianggap siap dan menjadi 'mesin target' yang akan digunakan berulang kali pada seluruh praktik Bab 2 sampai Bab 6. Peserta didik sangat disarankan membuat snapshot VMware (menu VM > Snapshot > Take Snapshot) pada kondisi bersih ini, sebagai titik pemulihan apabila konfigurasi pada bab tertentu perlu diulang dari awal.

Rangkuman

Keamanan Jaringan merupakan kelanjutan kompetensi TJKT yang berfokus pada perlindungan sistem dan infrastruktur jaringan, disusun dalam sembilan elemen mulai dari hardening dasar hingga forensik digital dan capture the flag. Penguasaan dasar Linux dan jaringan TCP/IP dari mata pelajaran sebelumnya menjadi prasyarat penting sebelum mendalami buku ini secara praktik langsung di laboratorium.

BAB 2 — Keamanan Akses Perangkat (Hardening Dasar)

Tujuan Pembelajaran

- Peserta didik mampu mengonfigurasi SSH agar root tidak dapat login langsung dan memahami alasan keamanannya.
- Peserta didik mampu mengganti port default layanan SSH serta memverifikasi layanan tetap berjalan.
- Peserta didik mampu membuat dan mengelola user administratif dengan hak sudo sesuai kebutuhan.
- Peserta didik mampu mengidentifikasi dan menonaktifkan layanan yang tidak diperlukan untuk mengurangi attack surface.

2.1 Konsep Hardening dan Attack Surface

Hardening adalah proses memperkuat konfigurasi sebuah sistem untuk mengurangi celah keamanan yang dapat dimanfaatkan penyerang, dengan cara menonaktifkan fitur tidak perlu, memperketat kontrol akses, dan menerapkan konfigurasi sesuai praktik keamanan terbaik. Konsep kunci dalam hardening adalah **attack surface**, yaitu keseluruhan titik yang berpotensi dimanfaatkan penyerang untuk mendapatkan akses ke sebuah sistem — semakin sedikit layanan, port, dan akun aktif yang tidak diperlukan, semakin kecil attack surface sebuah sistem, dan semakin sulit bagi penyerang menemukan celah masuk.

2.2 Menonaktifkan Login Root Langsung via SSH

Akun root memiliki hak akses penuh terhadap seluruh sistem, sehingga menjadi target utama serangan brute force. Praktik keamanan standar mewajibkan login root langsung melalui SSH dinonaktifkan, dan administrator diwajibkan login menggunakan akun biasa terlebih dahulu sebelum meningkatkan hak akses menggunakan `sudo` atau `su`. Pendekatan ini menambahkan lapisan autentikasi tambahan dan mempermudah audit karena setiap aktivitas administratif tercatat atas nama user yang sesungguhnya melakukan login, bukan tercatat sebagai root secara langsung.

Langkah	Perintah/Konfigurasi
Buka file konfigurasi SSH daemon	sudo nano /etc/ssh/sshd_config
Ubah baris directive PermitRootLogin	PermitRootLogin no
Simpan file dan mulai ulang layanan SSH	sudo systemctl restart sshd
Verifikasi status layanan	sudo systemctl status sshd

2.3 Mengganti Port Default Layanan SSH

Port default SSH (22) sangat umum menjadi sasaran pemindaian otomatis (automated scanning) oleh penyerang maupun bot. Mengganti port default ke port kustom bukan merupakan pengganti autentikasi yang kuat, melainkan lapisan tambahan yang dikenal sebagai **security through obscurity**, yang secara signifikan mengurangi jumlah percobaan login otomatis yang tidak relevan pada log sistem.

Langkah	Perintah/Konfigurasi
Ubah baris directive Port pada sshd_config	Port 2222
Pastikan firewall mengizinkan port baru	sudo ufw allow 2222/tcp
Mulai ulang layanan SSH	sudo systemctl restart sshd
Uji koneksi dari client menggunakan port baru	ssh -p 2222 user@alamat_server

Perlu diperhatikan urutan langkah di atas — firewall harus mengizinkan port baru **sebelum** layanan SSH dimulai ulang dengan konfigurasi port baru, agar administrator tidak terkunci (locked out) dari akses remote ke server.

2.4 Membuat dan Mengelola User Administratif

Sebagai pengganti akses root langsung, administrator perlu membuat user biasa yang diberi hak `sudo` untuk menjalankan perintah administratif ketika diperlukan.

Perintah	Fungsi
sudo adduser teknisi	Membuat user baru bernama teknisi beserta home directory
sudo usermod -aG sudo teknisi	Menambahkan user teknisi ke grup sudo (Debian/Ubuntu)
sudo visudo	Membuka file /etc/sudoers dengan aman untuk pengaturan hak akses sudo
teknisi ALL=(ALL) NOPASSWD:ALL	Baris pada sudoers agar user tidak diminta password saat sudo (bila diperlukan skenario tertentu)

Penggunaan `NOPASSWD` sebaiknya diterapkan secara selektif dan hanya pada skenario yang benar-benar membutuhkannya (misalnya otomatisasi skrip), karena mengurangi lapisan autentikasi pada akses administratif sehari-hari.

2.5 Menonaktifkan Layanan yang Tidak Diperlukan

Setiap layanan (service/daemon) yang berjalan pada sebuah sistem berpotensi menjadi celah masuk, sehingga layanan yang tidak esensial bagi fungsi server sebaiknya dinonaktifkan atau dihapus.

Perintah	Fungsi
systemctl list-units --type=service --state=running	Menampilkan seluruh layanan yang sedang aktif
sudo systemctl stop cups	Menghentikan layanan cups (print server) yang sedang berjalan
sudo systemctl disable cups	Mencegah layanan cups dijalankan otomatis saat boot
sudo systemctl stop avahi-daemon && sudo systemctl disable avahi-daemon	Menghentikan dan menonaktifkan layanan avahi-daemon (network discovery)
sudo apt purge cups avahi-daemon	Menghapus paket layanan tersebut sepenuhnya dari sistem (opsional, lebih permanen)

Layanan seperti `cups` (pencetakan) dan `avahi-daemon` (penemuan layanan jaringan otomatis) umum ditemukan aktif secara default pada instalasi desktop Linux namun jarang dibutuhkan pada server, sehingga menjadi kandidat utama untuk dinonaktifkan dalam proses hardening.

2.6 Hardening SSH Lanjutan

Selain menonaktifkan login root dan mengganti port, beberapa pengaturan tambahan pada sshd_config dapat memperkuat keamanan akses SSH secara signifikan.

Directive sshd_config	Rekomendasi Nilai	Manfaat
PasswordAuthentication	no	Mewajibkan autentikasi berbasis kunci publik (key-based), jauh lebih kuat dibanding password
PubkeyAuthentication	yes	Mengaktifkan autentikasi berbasis kunci publik SSH
MaxAuthTries	3	Membatasi jumlah percobaan autentikasi per koneksi sebelum ditolak
ClientAliveInterval	300	Memutus sesi SSH yang tidak aktif setelah periode waktu tertentu
Banner /etc/issue.net	-	Menampilkan pesan peringatan hukum sebelum proses login
AllowUsers	teknisi	Membatasi login SSH hanya untuk user tertentu yang didaftarkan secara eksplisit

Kombinasi PasswordAuthentication no dengan autentikasi berbasis kunci publik merupakan salah satu praktik hardening SSH paling efektif, karena menghilangkan sepenuhnya risiko serangan brute force terhadap password — penyerang harus memiliki private key yang sesuai, yang secara praktis mustahil ditebak.

Aktivitas Pembelajaran

6. Peserta didik melakukan praktik hardening dasar secara berurutan pada mesin virtual Linux: membuat user administratif baru, menonaktifkan login root SSH, mengganti port SSH, kemudian menguji akses SSH menggunakan user baru dan port baru dari komputer lain.
7. Peserta didik menjalankan `systemctl list-units --type=service --state=running` untuk mengidentifikasi seluruh layanan aktif pada mesin virtual, kemudian mendiskusikan dalam kelompok layanan mana yang dapat dinonaktifkan dengan aman.
8. Simulasi: setelah hardening selesai, peserta didik mencoba login sebagai root secara langsung dan mengamati bahwa percobaan tersebut ditolak oleh sistem.

Studi Kasus dan Praktik (VMware)

Studi Kasus: Sebuah SMK menerima laporan bahwa server latihan siswa sering menerima percobaan login dari alamat IP yang tidak dikenal, terlihat pada berkas log autentikasi. Sebagai teknisi jaringan magang, kalian diminta mengamankan akses ke server tersebut sebelum insiden yang lebih serius terjadi.

Praktik berikut dilakukan pada VM Ubuntu Server yang telah dibuat di VMware sesuai Bab 1. Disarankan membuat snapshot baru setelah praktik ini selesai sebagai titik pemulihan sebelum lanjut ke bab berikutnya.

Langkah	Perintah/Tindakan pada VM Ubuntu (VMware)
Nyalakan VM dan masuk sebagai user awal	Buka VMware, jalankan snapshot 'Bab1-Bersih', login menggunakan user yang dibuat saat instalasi
Periksa percobaan login pada log	sudo grep 'Failed password' /var/log/auth.log
Buat user administratif baru	sudo adduser teknisi_jaringan lalu sudo usermod -aG sudo teknisi_jaringan
Nonaktifkan login root langsung	sudo nano /etc/ssh/sshd_config -> ubah PermitRootLogin menjadi no
Ganti port SSH default	Ubah baris Port menjadi Port 2222 pada berkas yang sama
Terapkan perubahan	sudo systemctl restart sshd
Verifikasi dari luar VM	ssh -p 2222 teknisi_jaringan@alamat_ip_vm, pastikan login root pada port 22 ditolak
Simpan snapshot baru	Menu VM > Snapshot > Take Snapshot, beri nama 'Bab2-Selesai'

Bandingkan jumlah percobaan login gagal pada log sebelum dan sesudah hardening sebagai bukti bahwa attack surface server berkurang.

Rangkuman

Hardening dasar meliputi penonaktifan login root langsung via SSH, penggantian port default SSH, pembuatan user administratif dengan hak sudo, dan penonaktifan layanan yang tidak diperlukan, seluruhnya bertujuan mengurangi attack surface sebuah sistem. Kompetensi ini menjadi fondasi wajib sebelum mempelajari konfigurasi firewall pada bab berikutnya.

Soal Latihan / Refleksi

9. Jelaskan mengapa login root langsung melalui SSH sebaiknya dinonaktifkan, meskipun password root tetap kuat.
10. Tuliskan langkah-langkah mengganti port SSH dari 22 menjadi 2200 beserta urutan yang benar agar administrator tidak terkunci dari akses remote.
11. Apa fungsi perintah `visudo` dibanding mengedit file /etc/sudoers menggunakan editor teks biasa?
12. Jelaskan konsep attack surface dan bagaimana penonaktifan layanan yang tidak diperlukan dapat menguranginya.

BAB 3 — Firewall dan Keamanan Port Jaringan

Tujuan Pembelajaran

- Peserta didik mampu mengonfigurasi firewall berbasis host untuk mengizinkan hanya port esensial (default deny).
- Peserta didik mampu menerapkan pembatasan akses layanan berdasarkan IP/subnet menggunakan TCP Wrappers.
- Peserta didik mampu mendeteksi aktivitas port scanning menggunakan psad/portsentry.
- Peserta didik mampu mengonfigurasi firewall gateway menggunakan nftables untuk NAT dan port forwarding.

3.1 Konsep Firewall dan Kebijakan Default Deny

Firewall adalah sistem yang mengontrol lalu lintas jaringan masuk dan keluar berdasarkan seperangkat aturan (rule) yang telah ditetapkan. Praktik keamanan terbaik menerapkan kebijakan **default deny**, yaitu menolak seluruh lalu lintas secara default dan hanya mengizinkan lalu lintas yang secara eksplisit diperlukan (misalnya SSH, HTTP, HTTPS), berbeda dengan kebijakan default allow yang mengizinkan semua lalu lintas kecuali yang secara eksplisit diblokir dan jauh lebih rentan terhadap celah keamanan yang tidak disadari.

3.2 Firewall Berbasis Host dengan UFW

Uncomplicated Firewall (UFW) adalah antarmuka penyederhana bagi iptables yang umum digunakan pada distribusi Ubuntu/Debian karena kemudahan sintaksnya.

Perintah	Fungsi
sudo ufw default deny incoming	Menetapkan kebijakan default menolak seluruh koneksi masuk
sudo ufw default allow outgoing	Mengizinkan seluruh koneksi keluar secara default
sudo ufw allow 22/tcp	Mengizinkan port SSH (22) masuk
sudo ufw allow 80/tcp	Mengizinkan port HTTP (80) masuk
sudo ufw allow 443/tcp	Mengizinkan port HTTPS (443) masuk
sudo ufw enable	Mengaktifkan firewall dengan aturan yang telah ditetapkan
sudo ufw status verbose	Menampilkan status dan daftar aturan firewall aktif

3.3 Firewall Berbasis Host dengan iptables/nftables

nftables merupakan penerus iptables pada kernel Linux modern, menawarkan sintaks yang lebih terstruktur dan performa lebih baik, meskipun iptables masih banyak digunakan dan didukung secara luas. Contoh berikut menunjukkan penerapan kebijakan default deny menggunakan nftables.

Perintah	Fungsi
sudo nft add table inet filter	Membuat tabel filter untuk keluarga alamat inet (IPv4 & IPv6)
sudo nft add chain inet filter input { type filter hook input priority 0 \; policy drop \; }	Membuat chain input dengan kebijakan default drop
sudo nft add rule inet filter input tcp dport 22 accept	Mengizinkan lalu lintas masuk ke port 22
sudo nft add rule inet filter input ct state established,related accept	Mengizinkan lalu lintas balasan dari koneksi yang sudah terbentuk
sudo nft list ruleset	Menampilkan seluruh aturan nftables yang aktif

3.4 Menonaktifkan Respons ICMP dari Luar

Menonaktifkan respons terhadap permintaan ping (ICMP Echo Request) dari jaringan luar merupakan salah satu teknik hardening yang membuat server lebih sulit dideteksi keberadaannya oleh pemindaian jaringan otomatis, meskipun teknik ini juga memiliki kekurangan karena dapat menyulitkan troubleshooting jaringan yang sah.

Perintah	Fungsi
sudo ufw deny proto icmp	Menolak seluruh lalu lintas ICMP pada UFW
sudo nft add rule inet filter input icmp type echo-request drop	Menolak permintaan ping pada nftables

3.5 TCP Wrappers (hosts.allow dan hosts.deny)

TCP Wrappers adalah mekanisme kontrol akses tingkat aplikasi yang membatasi akses ke layanan tertentu berdasarkan alamat IP atau subnet klien, dikonfigurasi melalui dua file: `/etc/hosts.allow` yang mendaftar akses yang diizinkan, dan `/etc/hosts.deny` yang mendaftar akses yang ditolak. Aturan pada hosts.allow diproses lebih dahulu dan memiliki prioritas lebih tinggi dibanding hosts.deny.

File	Contoh Isi	Keterangan
/etc/hosts.allow	sshd: 192.168.0.0/24	Mengizinkan akses SSH hanya dari subnet 192.168.0.0/24

File	Contoh Isi	Keterangan
/etc/hosts.deny	sshd: ALL	Menolak seluruh akses SSH selain yang diizinkan pada hosts.allow

3.6 Membatasi Akses SSH Berdasarkan Subnet

Selain menggunakan TCP Wrappers, pembatasan akses berdasarkan subnet juga dapat diterapkan langsung pada firewall, memberikan lapisan kontrol tambahan yang lebih terintegrasi dengan kebijakan firewall secara keseluruhan.

Perintah	Fungsi
sudo ufw allow from 192.168.0.0/24 to any port 22	Mengizinkan akses SSH hanya dari subnet 192.168.0.0/24
sudo ufw delete allow 22/tcp	Menghapus aturan lama yang mengizinkan SSH dari seluruh alamat

3.7 Mendeteksi Port Scanning dengan Nmap, PSAD, dan Portsentry

Port scanning adalah teknik yang digunakan penyerang (maupun administrator untuk audit keamanan) untuk memeriksa port mana saja yang terbuka pada sebuah sistem. **Nmap** adalah alat pemindaian port paling populer yang digunakan untuk simulasi pengujian, sedangkan **psad** (Port Scan Attack Detector) dan **portsentry** adalah alat yang berjalan pada sisi target untuk mendeteksi dan merespons aktivitas pemindaian tersebut secara otomatis.

Perintah	Fungsi
nmap -sS 192.168.1.10	Melakukan SYN scan untuk memeriksa port terbuka pada target (dari sisi penguji)
sudo apt install psad	Menginstal psad pada sistem target
sudo psad --sig-update && sudo systemctl restart psad	Memperbarui signature dan memulai ulang layanan psad
sudo psad -S	Menampilkan status pemindaian yang terdeteksi oleh psad
sudo apt install portsentry	Menginstal portsentry sebagai alternatif pendeteksi port scan

3.8 Firewall Gateway dengan nftables: NAT dan Port Forwarding

Pada perangkat yang berfungsi sebagai gateway (menghubungkan jaringan internal ke internet), nftables juga digunakan untuk menerapkan NAT masquerade agar perangkat internal dapat mengakses internet, serta port forwarding agar layanan pada server internal (misalnya di DMZ) dapat diakses dari luar.

Perintah	Fungsi
sudo nft add table ip nat	Membuat tabel nat
sudo nft add chain ip nat postrouting { type nat hook postrouting priority 100 \; }	Membuat chain postrouting untuk NAT keluar
sudo nft add rule ip nat postrouting oifname "eth0" masquerade	Menerapkan NAT masquerade pada interface keluar eth0
sudo nft add chain ip nat prerouting { type nat hook prerouting priority -100 \; }	Membuat chain prerouting untuk port forwarding
sudo nft add rule ip nat prerouting tcp dport 8080 dnat to 192.168.100.10:80	Meneruskan port 8080 gateway ke port 80 server DMZ

3.9 Logging dan Pemantauan Aktivitas Firewall

Selain menerapkan aturan, firewall yang baik juga perlu mencatat (logging) aktivitas penolakan lalu lintas, agar administrator dapat memantau pola percobaan akses yang ditolak dan mendeteksi potensi serangan sejak dini.

Perintah	Fungsi
sudo ufw logging on	Mengaktifkan logging pada UFW
sudo tail -f /var/log/ufw.log	Memantau log UFW secara real-time
sudo nft add rule inet filter input log prefix "dropped: " drop	Menambahkan logging pada rule nftables sebelum paket ditolak
sudo journalctl -k | grep dropped	Memeriksa log kernel untuk entri yang dicatat dengan prefix tertentu

Logging firewall yang aktif menjadi sumber data penting yang saling melengkapi dengan alat deteksi intrusi (fail2ban, auditd, Snort) yang akan dipelajari pada bab berikutnya, membentuk gambaran menyeluruh mengenai aktivitas mencurigakan yang menyasar sebuah sistem.

Aktivitas Pembelajaran

13. Peserta didik mengonfigurasi UFW pada mesin virtual dengan kebijakan default deny incoming, kemudian mengizinkan hanya port SSH, HTTP, dan HTTPS, lalu menguji dengan mencoba mengakses port lain yang seharusnya diblokir.

14. Peserta didik mengonfigurasi TCP Wrappers agar akses SSH hanya diizinkan dari subnet laboratorium, kemudian menguji akses dari luar subnet tersebut untuk memastikan ditolak.
15. Peserta didik melakukan simulasi port scan menggunakan nmap dari satu mesin virtual ke mesin virtual lain yang telah dipasang psad, kemudian memeriksa log psad untuk memverifikasi deteksi berhasil.
16. Peserta didik mengonfigurasi firewall gateway sederhana dengan nftables yang menerapkan NAT masquerade dan satu aturan port forwarding menuju server web pada jaringan DMZ simulasi.

Studi Kasus dan Praktik (VMware)

Studi Kasus: Server web sekolah yang sama ternyata juga menjalankan basis data pada port default, dan dapat diakses langsung dari jaringan luar. Tim IT sekolah meminta firewall diterapkan agar hanya layanan yang benar-benar diperlukan yang dapat diakses dari luar.

Praktik berikut dilakukan pada VM Ubuntu Server yang telah dibuat di VMware sesuai Bab 1. Disarankan membuat snapshot baru setelah praktik ini selesai sebagai titik pemulihan sebelum lanjut ke bab berikutnya.

Langkah	Perintah/Tindakan pada VM Ubuntu (VMware)
Lanjutkan dari snapshot Bab 2	Buka VM 'Bab2-Selesai' pada VMware
Aktifkan UFW dengan kebijakan default deny	sudo ufw default deny incoming lalu sudo ufw default allow outgoing
Izinkan hanya port yang diperlukan	sudo ufw allow 2222/tcp lalu sudo ufw allow 80/tcp dan sudo ufw allow 443/tcp
Aktifkan firewall	sudo ufw enable, konfirmasi dengan y
Uji port yang seharusnya tertutup dari host	nmap -p 3306,22 alamat_ip_vm (dijalankan dari terminal host, bukan di dalam VM)
Verifikasi status aturan	sudo ufw status verbose
Simpan snapshot baru	Beri nama 'Bab3-Selesai' setelah firewall terverifikasi bekerja

Jika VMware diatur pada mode jaringan Bridged, praktik nmap dari komputer host akan lebih merepresentasikan pengujian dari 'luar' jaringan VM secara nyata.

Rangkuman

Firewall menerapkan kontrol lalu lintas jaringan dengan kebijakan default deny sebagai praktik terbaik, dikonfigurasi menggunakan UFW atau nftables pada level host, dilengkapi TCP Wrappers dan pembatasan subnet untuk kontrol akses tambahan. Deteksi port scanning menggunakan psad/portsentry serta konfigurasi NAT dan port forwarding pada firewall gateway melengkapi kompetensi keamanan jaringan tingkat infrastruktur pada bab ini.

Soal Latihan / Refleksi

17. Jelaskan perbedaan kebijakan default deny dan default allow pada firewall beserta alasan default deny lebih disarankan.
18. Tuliskan perintah UFW untuk mengizinkan akses SSH hanya dari subnet 10.10.10.0/24.

19. Jelaskan fungsi file /etc/hosts.allow dan /etc/hosts.deny pada mekanisme TCP Wrappers.
20. Apa perbedaan fungsi psad dan nmap dalam konteks pengujian dan deteksi port scanning?
21. Jelaskan konsep NAT masquerade pada firewall gateway menggunakan nftables.

BAB 4 — Deteksi dan Pencegahan Intrusi (IDS/IPS)

Tujuan Pembelajaran

- Peserta didik mampu memasang dan mengonfigurasi fail2ban untuk memblokir percobaan login gagal berulang.
- Peserta didik mampu mengaktifkan audit log sistem menggunakan auditd.
- Peserta didik mampu memasang dan mengonfigurasi Snort sebagai IDS untuk mendeteksi port scan.
- Peserta didik mampu menganalisis log hasil deteksi IDS dan menyusun laporan ringkas.

4.1 Konsep IDS dan IPS

Intrusion Detection System (IDS) adalah sistem yang memantau lalu lintas jaringan atau aktivitas sistem untuk mendeteksi tanda-tanda serangan atau aktivitas mencurigakan, kemudian memberikan peringatan (alert) kepada administrator tanpa secara otomatis memblokir lalu lintas tersebut. Intrusion Prevention System (IPS) melangkah lebih jauh dengan secara otomatis mengambil tindakan pencegahan, seperti memblokir alamat IP penyerang, ketika aktivitas mencurigakan terdeteksi.

4.2 Fail2ban: IPS Sederhana untuk SSH

Fail2ban adalah salah satu contoh implementasi IPS sederhana yang bekerja dengan memantau file log sistem (misalnya log autentikasi SSH), mendeteksi pola percobaan login gagal berulang dari alamat IP yang sama dalam rentang waktu tertentu, kemudian secara otomatis memblokir alamat IP tersebut menggunakan firewall untuk periode waktu yang dapat dikonfigurasi.

Perintah/Konfigurasi	Fungsi
sudo apt install fail2ban	Menginstal fail2ban
sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local	Membuat file konfigurasi lokal agar tidak menimpa file default
[sshd]\nenabled = true\nport = 22\nmaxretry = 5\nbantime = 3600	Contoh konfigurasi jail sshd pada jail.local: aktif, port 22, maksimal 5 percobaan gagal, blokir 3600 detik
sudo systemctl restart fail2ban	Menerapkan konfigurasi dengan memulai ulang layanan
sudo fail2ban-client status sshd	Menampilkan status dan daftar IP yang diblokir pada jail sshd
sudo fail2ban-client set sshd unbanip 192.168.1.50	Membuka blokir sebuah alamat IP secara manual

4.3 Audit Log Sistem dengan auditd

auditd (Linux Audit Daemon) adalah komponen kernel Linux yang mencatat aktivitas sistem secara terperinci, seperti akses file, eksekusi perintah, dan perubahan konfigurasi, yang sangat berguna untuk keperluan audit keamanan dan investigasi insiden.

Perintah	Fungsi
sudo apt install auditd audispd-plugins	Menginstal auditd beserta plugin pendukung
sudo systemctl enable --now auditd	Mengaktifkan dan memulai layanan auditd
sudo auditctl -w /etc/passwd -p wa -k passwd_changes	Memantau perubahan (write/attribute) pada file /etc/passwd dengan label passwd_changes
sudo ausearch -k passwd_changes	Mencari log audit berdasarkan label (key) yang telah ditetapkan
sudo aureport --summary	Menampilkan ringkasan seluruh aktivitas yang tercatat oleh auditd

4.4 Snort sebagai Network IDS

Snort adalah perangkat lunak IDS/IPS berbasis jaringan (Network-based IDS) yang menganalisis lalu lintas jaringan secara real-time berdasarkan seperangkat aturan (rule) untuk mendeteksi pola serangan yang dikenal, seperti port scan, eksploitasi kerentanan tertentu, maupun lalu lintas mencurigakan lainnya.

Perintah/Konfigurasi	Fungsi
sudo apt install snort	Menginstal Snort (akan meminta konfigurasi jaringan awal seperti HOME_NET)
alert tcp any any -> $HOME_NET any (msg:"Possible port scan detected"; flags:S; threshold: type both, track by_src, count 20, seconds 60; sid:1000001;)	Contoh rule sederhana pada local.rules untuk mendeteksi indikasi port scan (20 paket SYN dalam 60 detik dari sumber sama)
sudo snort -c /etc/snort/snort.conf -i eth0	Menjalankan Snort pada interface eth0 menggunakan file konfigurasi utama
sudo tail -f /var/log/snort/alert	Memantau log alert Snort secara real-time

4.5 Menganalisis Log Hasil Deteksi

Kemampuan menganalisis log hasil deteksi IDS sama pentingnya dengan kemampuan memasang alat tersebut. Analisis log yang baik melibatkan identifikasi alamat IP sumber serangan, jenis dan pola serangan yang terdeteksi, waktu kejadian, serta tingkat urgensi (severity) yang memerlukan tindak lanjut. Peserta didik perlu terbiasa menyusun laporan ringkas berisi ringkasan temuan, bukti (log/alert terkait), dan

rekomendasi tindakan yang sesuai, sebagai bagian dari keterampilan analis keamanan siber yang komprehensif.

4.6 Perbandingan Alat Deteksi dan Pencegahan

Setiap organisasi perlu memilih kombinasi alat deteksi yang sesuai dengan skala dan kebutuhan infrastrukturnya. Tabel berikut merangkum karakteristik ketiga alat yang telah dipelajari sebagai bahan pertimbangan.

Alat	Cakupan	Jenis Respons	Kompleksitas
fail2ban	Log aplikasi tertentu (SSH, web, dll.)	Otomatis (blokir IP via firewall)	Rendah
auditd	Aktivitas sistem (file, syscall)	Pencatatan (pasif, perlu ditinjau manual)	Sedang
Snort	Lalu lintas jaringan (network-wide)	Peringatan (dapat diperluas jadi IPS)	Tinggi

Pada praktiknya, ketiga alat ini sering digunakan secara bersamaan sebagai bagian dari strategi pertahanan berlapis: fail2ban menangani ancaman brute force pada layanan spesifik secara otomatis, auditd menyediakan jejak audit terperinci untuk investigasi, dan Snort memberikan visibilitas menyeluruh terhadap lalu lintas jaringan yang mencurigakan.

Aktivitas Pembelajaran

22. Peserta didik memasang dan mengonfigurasi fail2ban pada mesin virtual, kemudian mensimulasikan beberapa percobaan login SSH gagal dari mesin lain untuk menguji apakah IP tersebut secara otomatis diblokir.
23. Peserta didik mengaktifkan auditd dan memantau perubahan pada file /etc/passwd, kemudian melakukan perubahan uji coba dan memverifikasi log tercatat menggunakan ausearch.
24. Peserta didik memasang Snort dan membuat satu rule sederhana untuk mendeteksi port scan, kemudian menjalankan nmap dari mesin lain dan memeriksa log alert yang dihasilkan.
25. Peserta didik menyusun laporan ringkas (1 halaman) berdasarkan hasil deteksi IDS pada aktivitas sebelumnya, mencakup ringkasan temuan dan rekomendasi tindak lanjut.

Studi Kasus dan Praktik (VMware)

Studi Kasus: Beberapa hari setelah firewall diterapkan, log autentikasi pada VM masih menunjukkan percobaan login SSH berulang dari satu alamat IP yang sama dalam waktu singkat, mengindikasikan upaya brute force yang belum tertangani oleh firewall saja.

Praktik berikut dilakukan pada VM Ubuntu Server yang telah dibuat di VMware sesuai Bab 1. Disarankan membuat snapshot baru setelah praktik ini selesai sebagai titik pemulihan sebelum lanjut ke bab berikutnya.

Langkah	Perintah/Tindakan pada VM Ubuntu (VMware)

Lanjutkan dari snapshot Bab 3	Buka VM 'Bab3-Selesai' pada VMware
Pasang fail2ban	sudo apt install fail2ban -y
Aktifkan jail SSH	sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local, atur [sshd] enabled = true, port = 2222
Terapkan konfigurasi	sudo systemctl restart fail2ban
Simulasikan percobaan gagal	Dari komputer host, jalankan ssh ke port 2222 dengan password salah sebanyak 5-6 kali berturut-turut
Verifikasi IP terblokir	sudo fail2ban-client status sshd
Aktifkan auditd untuk memantau file penting	sudo apt install auditd -y lalu sudo auditctl -w /etc/passwd -p wa -k user_modification
Simpan snapshot baru	Beri nama 'Bab4-Selesai' setelah fail2ban dan auditd terbukti bekerja

Perhatikan bahwa IP host akan ikut terblokir oleh fail2ban setelah simulasi; gunakan sudo fail2ban-client set sshd unbanip <ip_host> untuk membuka blokir kembali sebelum melanjutkan praktik lain dari komputer yang sama.

Rangkuman

Deteksi dan pencegahan intrusi melibatkan fail2ban sebagai IPS sederhana berbasis log autentikasi, auditd untuk pencatatan audit sistem terperinci, dan Snort sebagai IDS berbasis jaringan yang mendeteksi pola serangan menggunakan rule tertentu. Kemampuan menganalisis log hasil deteksi dan menyusun laporan menjadi keterampilan pelengkap yang esensial bagi seorang analis keamanan siber.

Soal Latihan / Refleksi

26. Jelaskan perbedaan mendasar antara IDS dan IPS.
27. Jelaskan cara kerja fail2ban dalam mendeteksi dan memblokir percobaan login gagal berulang.
28. Apa fungsi auditd, dan berikan satu contoh skenario penggunaannya untuk memantau file sensitif.
29. Jelaskan komponen utama sebuah rule Snort sederhana untuk mendeteksi port scan.

BAB 5 — Keamanan Komunikasi dan Kriptografi Terapan

Tujuan Pembelajaran

- Peserta didik mampu menginstal dan menggunakan GnuPG (GPG) pada sistem Linux.
- Peserta didik mampu membuat pasangan kunci PGP dan mengekspor public key untuk didistribusikan.
- Peserta didik mampu mengenkripsi dan mendekripsi pesan menggunakan GPG.
- Peserta didik mampu membuat dan memverifikasi digital signature terhadap sebuah file.

5.1 Konsep Dasar Kriptografi Asimetris

Kriptografi asimetris (juga dikenal sebagai kriptografi kunci publik) menggunakan sepasang kunci matematis yang saling berkaitan: **kunci publik (public key)** yang dapat dibagikan secara bebas dan digunakan untuk mengenkripsi pesan atau memverifikasi tanda tangan, serta **kunci privat (private key)** yang harus dijaga kerahasiaannya dan digunakan untuk mendekripsi pesan atau membuat tanda tangan digital. Pendekatan ini menyelesaikan masalah mendasar pada kriptografi simetris, yaitu bagaimana dua pihak dapat berkomunikasi secara aman tanpa harus bertukar kunci rahasia melalui saluran yang aman terlebih dahulu.

GNU Privacy Guard (GPG) adalah implementasi perangkat lunak bebas dari standar OpenPGP, digunakan secara luas untuk mengenkripsi komunikasi (seperti email), memverifikasi keaslian perangkat lunak yang diunduh, serta menandatangani dokumen secara digital.

5.2 Instalasi GnuPG

Perintah	Fungsi
sudo apt update && sudo apt install gnupg	Menginstal GPG pada distribusi berbasis Debian/Ubuntu
gpg --version	Memverifikasi GPG telah terinstal beserta versinya

5.3 Membuat Pasangan Kunci PGP

Pembuatan pasangan kunci (key pair) dilakukan secara interaktif, di mana pengguna diminta menetapkan jenis dan ukuran kunci, masa berlaku, serta identitas (nama dan alamat email) yang akan melekat pada kunci tersebut.

Perintah	Fungsi
gpg --full-generate-key	Memulai proses pembuatan key pair secara interaktif

Perintah	Fungsi
Pilihan jenis kunci: (1) RSA and RSA	Direkomendasikan untuk kompatibilitas luas
Ukuran kunci: 4096	Ukuran 4096 bit memberikan tingkat keamanan lebih tinggi dibanding default 2048 bit
Masa berlaku: mis. 1y (1 tahun)	Menetapkan periode validitas kunci sebelum perlu diperbarui
gpg --list-keys	Menampilkan daftar public key yang tersimpan pada keyring pengguna
gpg --list-secret-keys	Menampilkan daftar private key yang tersimpan

5.4 Mengekspor dan Mendistribusikan Public Key

Agar pihak lain dapat mengirimkan pesan terenkripsi kepada pemilik kunci atau memverifikasi tanda tangannya, public key perlu diekspor ke sebuah file yang dapat dibagikan secara bebas, misalnya melalui email atau diunggah ke server kunci publik (keyserver).

Perintah	Fungsi
gpg --armor --export nama@email.com > publickey.asc	Mengekspor public key ke file teks ASCII (armor) bernama publickey.asc
gpg --import teman_publickey.asc	Mengimpor public key milik pihak lain ke dalam keyring sendiri
gpg --edit-key nama@email.com	Membuka mode edit key, termasuk untuk menandatangani (sign) kunci pihak lain guna membangun web of trust

5.5 Mengenkripsi dan Mendekripsi Pesan

Perintah	Fungsi
gpg --encrypt --armor -r teman@email.com rahasia.txt	Mengenkripsi file rahasia.txt menggunakan public key milik penerima, menghasilkan rahasia.txt.asc
gpg --decrypt rahasia.txt.asc > rahasia_terbuka.txt	Mendekripsi file terenkripsi menggunakan private key milik penerima (akan diminta passphrase)

Proses enkripsi menggunakan public key milik penerima memastikan hanya pemilik private key yang berpasangan (yaitu penerima yang dituju) yang dapat mendekripsi pesan tersebut, meskipun pesan terenkripsi tersebut dicegat oleh pihak ketiga selama proses pengiriman.

5.6 Membuat dan Memverifikasi Digital Signature

Digital signature (tanda tangan digital) berfungsi membuktikan keaslian dan integritas sebuah file — bahwa file tersebut benar berasal dari pemilik kunci privat tertentu dan tidak mengalami perubahan sejak ditandatangani. Berbeda dengan enkripsi yang menggunakan public key penerima, proses penandatanganan menggunakan private key milik pengirim, dan verifikasinya menggunakan public key milik pengirim yang sama.

Perintah	Fungsi
gpg --detach-sign --armor dokumen.pdf	Membuat file tanda tangan terpisah (dokumen.pdf.asc) tanpa mengubah file asli
gpg --verify dokumen.pdf.asc dokumen.pdf	Memverifikasi keaslian file menggunakan file tanda tangan dan public key pengirim

5.7 Konsep Web of Trust dan Tingkat Kepercayaan Kunci

Salah satu tantangan pada kriptografi kunci publik adalah memastikan bahwa sebuah public key benar-benar milik orang yang diklaim, bukan milik pihak yang menyamar. OpenPGP menyelesaikan masalah ini melalui konsep **web of trust**, yaitu jaringan kepercayaan di mana pengguna dapat menandatangani (sign) kunci milik orang lain yang identitasnya telah mereka verifikasi secara langsung, sehingga pihak ketiga yang mempercayai penanda tangan tersebut juga dapat mempercayai kunci yang ditandatangani.

Perintah	Fungsi
gpg --fingerprint nama@email.com	Menampilkan sidik jari (fingerprint) kunci untuk verifikasi identitas secara manual/lisan
gpg --sign-key nama@email.com	Menandatangani public key milik pihak lain setelah identitasnya diverifikasi
gpg --edit-key nama@email.com trust	Menetapkan tingkat kepercayaan (trust level) terhadap sebuah kunci dalam keyring

Aktivitas Pembelajaran

30. Peserta didik membuat pasangan kunci PGP RSA 4096 bit dengan identitas masing-masing, kemudian saling bertukar public key dengan rekan sebangku.
31. Peserta didik mengenkripsi sebuah file teks menggunakan public key milik rekannya, mengirimkan file terenkripsi tersebut, dan meminta rekannya mendekripsi menggunakan private key miliknya.
32. Peserta didik membuat digital signature terhadap sebuah file, kemudian mengubah sedikit isi file tersebut dan mencoba memverifikasi ulang untuk mengamati bahwa verifikasi gagal karena file telah berubah.

Studi Kasus dan Praktik (VMware)

Studi Kasus: Seorang guru perlu mengirimkan berkas rekap nilai siswa yang bersifat rahasia kepada wali kelas lain melalui email, namun khawatir isi berkas dapat terbaca apabila email tersebut disadap atau salah kirim.

Praktik berikut dilakukan pada VM Ubuntu Server yang telah dibuat di VMware sesuai Bab 1. Disarankan membuat snapshot baru setelah praktik ini selesai sebagai titik pemulihan sebelum lanjut ke bab berikutnya.

Langkah	Perintah/Tindakan pada VM Ubuntu (VMware)
Lanjutkan dari snapshot Bab 4	Buka VM 'Bab4-Selesai' pada VMware
Buat pasangan kunci PGP	gpg --full-generate-key, pilih RSA 4096 bit, isi nama dan email sebagai identitas
Ekspor public key	gpg --armor --export email@sekolah.sch.id > publickey.asc
Simulasikan rekan menerima public key	Salin publickey.asc ke folder terpisah (mewakili komputer rekan), lalu impor dengan gpg --import publickey.asc
Enkripsi berkas rekap nilai	gpg --encrypt --armor -r email@sekolah.sch.id rekap_nilai.txt
Simulasikan proses dekripsi oleh rekan	gpg --decrypt rekap_nilai.txt.asc > rekap_nilai_terbuka.txt
Buat dan verifikasi digital signature	gpg --detach-sign --armor rekap_nilai.txt lalu gpg --verify rekap_nilai.txt.asc rekap_nilai.txt
Simpan snapshot baru	Beri nama 'Bab5-Selesai' setelah proses enkripsi dan verifikasi berhasil

Karena praktik ini dilakukan pada satu VM yang sama, gunakan dua folder kerja terpisah (mis. folder_guru dan folder_rekan) untuk mensimulasikan peran pengirim dan penerima secara berdampingan.

Rangkuman

Kriptografi asimetris menggunakan pasangan kunci publik dan privat untuk mengamankan komunikasi tanpa perlu bertukar kunci rahasia. GnuPG (GPG) mengimplementasikan standar OpenPGP untuk membuat key pair, mengenkripsi/mendekripsi pesan, serta membuat dan memverifikasi digital signature guna menjamin keaslian dan integritas data. Kompetensi ini menjadi dasar keamanan komunikasi sebelum mempelajari topik keamanan basis data pada bab berikutnya.

Soal Latihan / Refleksi

33. Jelaskan perbedaan fungsi kunci publik dan kunci privat pada kriptografi asimetris.
34. Mengapa proses enkripsi pesan menggunakan public key milik penerima, sedangkan proses penandatanganan menggunakan private key milik pengirim?
35. Jelaskan tujuan pembuatan digital signature terhadap sebuah file.
36. Tuliskan perintah GPG untuk mengekspor public key ke dalam format file ASCII armor.

BAB 6 — Keamanan Basis Data

Tujuan Pembelajaran

- Peserta didik mampu mengamankan akses root MySQL dengan membatasi akses hanya dari localhost.
- Peserta didik mampu membuat user database dengan hak akses terbatas sesuai kebutuhan.
- Peserta didik mampu menghapus akun anonymous dan menjalankan audit konfigurasi menggunakan mysql_secure_installation.
- Peserta didik mampu membatasi akses port database menggunakan firewall.

6.1 Risiko Keamanan pada Basis Data

Basis data sering menyimpan informasi paling sensitif dalam sebuah organisasi, seperti data pengguna, kredensial, dan data transaksi, sehingga menjadi target utama serangan. Konfigurasi default pada perangkat lunak basis data seperti MySQL/MariaDB umumnya belum dioptimalkan untuk keamanan produksi, sehingga proses hardening menjadi langkah wajib segera setelah instalasi.

6.2 Menjalankan mysql_secure_installation

MySQL/MariaDB menyediakan skrip bawaan bernama `mysql_secure_installation` yang memandu administrator melalui beberapa langkah pengamanan dasar secara interaktif segera setelah instalasi.

Langkah Interaktif	Rekomendasi
Set root password	Tetapkan password root yang kompleks dan unik
Remove anonymous users?	Jawab Yes — akun anonymous memungkinkan siapa saja login tanpa kredensial valid
Disallow root login remotely?	Jawab Yes — root sebaiknya hanya dapat login dari localhost
Remove test database and access to it?	Jawab Yes — database test bersifat publik dan tidak diperlukan pada produksi
Reload privilege tables now?	Jawab Yes — menerapkan seluruh perubahan segera

6.3 Mengamankan Akses Root MySQL

Selain melalui mysql_secure_installation, administrator dapat memverifikasi dan memastikan akses root secara manual melalui perintah SQL berikut, dijalankan setelah login ke MySQL menggunakan `mysql -u root -p`.

Perintah SQL	Fungsi
SELECT user, host FROM mysql.user;	Menampilkan daftar user dan host yang diizinkan mengaksesnya
DELETE FROM mysql.user WHERE user='root' AND host NOT IN ('localhost');	Menghapus akses root dari host selain localhost
ALTER USER 'root'@'localhost' IDENTIFIED BY 'PasswordKompleks!23';	Mengganti password root menjadi kompleks
FLUSH PRIVILEGES;	Menerapkan perubahan hak akses secara langsung

6.4 Membuat User Database dengan Hak Akses Terbatas

Prinsip **least privilege** (hak akses minimal) mewajibkan setiap user database hanya diberikan hak akses yang benar-benar diperlukan sesuai fungsinya, alih-alih menggunakan akun root untuk seluruh keperluan aplikasi.

Perintah SQL	Fungsi
CREATE USER 'app_web'@'localhost' IDENTIFIED BY 'PasswordAman!45';	Membuat user baru bernama app_web yang hanya dapat login dari localhost
GRANT SELECT, INSERT, UPDATE, DELETE ON toko_online.* TO 'app_web'@'localhost';	Memberikan hak akses terbatas hanya pada database toko_online
SHOW GRANTS FOR 'app_web'@'localhost';	Menampilkan hak akses yang dimiliki user tersebut untuk verifikasi
REVOKE DROP ON toko_online.* FROM 'app_web'@'localhost';	Mencabut hak akses tertentu (mis. DROP) yang tidak diperlukan aplikasi

6.5 Membatasi Akses Port Database dengan Firewall

Port default MySQL (3306) sebaiknya tidak dapat diakses dari jaringan luar kecuali benar-benar diperlukan (misalnya untuk replikasi database antar server), karena aplikasi umumnya mengakses database melalui localhost pada server yang sama.

Perintah	Fungsi
sudo ufw deny 3306/tcp	Menolak akses port 3306 dari jaringan luar pada UFW
bind-address = 127.0.0.1	Baris pada file konfigurasi MySQL (my.cnf) agar MySQL hanya mendengarkan pada localhost
sudo systemctl restart mysql	Menerapkan perubahan konfigurasi bind-address

6.6 Backup Basis Data Terenkripsi

Selain mengamankan akses langsung ke database, administrator juga perlu memastikan salinan cadangan (backup) database turut terlindungi, karena file backup yang tidak terenkripsi dapat menjadi celah kebocoran data apabila jatuh ke tangan yang tidak berwenang.

Perintah	Fungsi
mysqldump -u root -p toko_online > backup.sql	Membuat backup database toko_online ke file SQL
gpg --encrypt --armor -r admin@sekolah.sch.id backup.sql	Mengenkripsi file backup menggunakan GPG (memanfaatkan kompetensi Bab 5)
gpg --decrypt backup.sql.asc > backup_restore.sql	Mendekripsi file backup saat diperlukan untuk pemulihan

Praktik ini menunjukkan bagaimana kompetensi kriptografi terapan pada Bab 5 dapat diintegrasikan langsung dengan kompetensi keamanan basis data, memperkuat pemahaman bahwa keamanan siber merupakan disiplin yang saling terhubung antar elemen.

Aktivitas Pembelajaran

37. Peserta didik menjalankan `mysql_secure_installation` pada instalasi MySQL/MariaDB baru di mesin virtual, mengikuti seluruh langkah pengamanan yang direkomendasikan.
38. Peserta didik membuat sebuah database contoh beserta user dengan hak akses terbatas (hanya SELECT dan INSERT), kemudian menguji bahwa user tersebut tidak dapat menjalankan perintah DROP TABLE.
39. Peserta didik mengonfigurasi firewall agar port 3306 tidak dapat diakses dari mesin virtual lain, kemudian memverifikasi menggunakan percobaan koneksi dari luar.

Studi Kasus dan Praktik (VMware)

Studi Kasus: Aplikasi pendataan siswa di sekolah ternyata masih menggunakan akun root MySQL tanpa password dan dapat diakses dari komputer mana pun di jaringan, sehingga berisiko tinggi mengalami kebocoran data siswa apabila ditemukan pihak yang tidak berwenang.

Praktik berikut dilakukan pada VM Ubuntu Server yang telah dibuat di VMware sesuai Bab 1. Disarankan membuat snapshot baru setelah praktik ini selesai sebagai titik pemulihan sebelum lanjut ke bab berikutnya.

Langkah	Perintah/Tindakan pada VM Ubuntu (VMware)
Lanjutkan dari snapshot Bab 5	Buka VM 'Bab5-Selesai' pada VMware
Pasang MariaDB	sudo apt install mariadb-server -y
Jalankan pengamanan dasar	sudo mysql_secure_installation, jawab Yes pada seluruh rekomendasi keamanan

Buat user aplikasi dengan hak terbatas	CREATE USER 'app_siswa'@'localhost' IDENTIFIED BY 'PasswordAman!23'; lalu GRANT SELECT, INSERT, UPDATE ON data_siswa.* TO 'app_siswa'@'localhost';
Batasi akses port database	sudo ufw deny 3306/tcp, lalu pastikan bind-address = 127.0.0.1 pada berkas konfigurasi MariaDB
Terapkan perubahan	sudo systemctl restart mariadb
Backup terenkripsi	mysqldump -u root -p data_siswa > backup.sql lalu gpg --encrypt --armor -r email@sekolah.sch.id backup.sql
Simpan snapshot baru	Beri nama 'Bab6-Selesai' sebagai kondisi akhir mesin virtual hardening

Langkah backup terenkripsi ini sekaligus menggabungkan kompetensi kriptografi (Bab 5) dengan keamanan basis data (Bab 6) pada satu VM yang sama, menunjukkan bagaimana lapisan-lapisan keamanan saling melengkapi.

Rangkuman

Keamanan basis data mencakup penjalanan mysql_secure_installation untuk pengamanan dasar, pembatasan akses root MySQL hanya dari localhost, penerapan prinsip least privilege melalui pembuatan user dengan hak akses terbatas, serta pembatasan akses port database menggunakan firewall. Kompetensi ini melengkapi lapisan keamanan aplikasi berbasis data sebelum mempelajari keamanan akun pengguna sistem operasi pada bab berikutnya.

Soal Latihan / Refleksi

40. Jelaskan lima langkah utama yang dilakukan oleh skrip mysql_secure_installation.
41. Apa yang dimaksud dengan prinsip least privilege dalam konteks manajemen user database?
42. Tuliskan perintah SQL untuk membuat user bernama 'staff_db' yang hanya dapat melakukan SELECT pada database 'inventaris'.

43. Mengapa port MySQL (3306) sebaiknya tidak diakses langsung dari jaringan luar?

Pembelajaran Keamanan Jaringan dilanjutkan pada Buku Jilid 2 untuk Kelas XII, yang membahas Bab 7 (Keamanan Akun Pengguna Sistem Operasi) sampai Bab 11 (Rangkuman dan Evaluasi Akhir), dilengkapi glosarium dan lampiran praktik.

BAB 7 — Keamanan Akun Pengguna Sistem Operasi

Tujuan Pembelajaran

- Peserta didik mampu mengaudit daftar user aktif pada sistem dan memeriksa kelemahan password.
- Peserta didik mampu menerapkan kebijakan password menggunakan chage dan konfigurasi PAM.
- Peserta didik mampu mengonfigurasi penguncian akun otomatis setelah percobaan login gagal berulang.
- Peserta didik mampu menerapkan autentikasi dua faktor (2FA) untuk user tertentu.

7.1 Mengaudit Daftar User Aktif

Langkah pertama dalam mengamankan akun pengguna adalah memahami akun apa saja yang ada pada sistem. Linux membedakan antara user sistem (system account, umumnya UID di bawah 1000, digunakan oleh layanan) dan user reguler (UID 1000 ke atas, digunakan oleh manusia).

Perintah	Fungsi
cat /etc/passwd	Menampilkan seluruh akun user pada sistem beserta detailnya
awk -F: '$3 >= 1000 && $3 != 65534 {print $1}' /etc/passwd	Menampilkan hanya user reguler (bukan user sistem)
lastlog	Menampilkan waktu login terakhir setiap user, membantu identifikasi akun yang tidak lagi digunakan
who / w	Menampilkan user yang sedang login pada sistem saat ini

7.2 Memeriksa Kelemahan Password

User tanpa password atau dengan password kosong merupakan celah keamanan serius yang harus segera diidentifikasi dan diperbaiki.

Perintah	Fungsi
sudo awk -F: '($2 == "") {print $1}' /etc/shadow	Menampilkan user dengan field password kosong pada /etc/shadow
sudo passwd -S nama_user	Memeriksa status password (locked, aktif, atau kosong) pada user tertentu

sudo passwd -l nama_user	Mengunci akun user (menonaktifkan login menggunakan password)

7.3 Menerapkan Kebijakan Password dengan chage

Perintah `chage` (change age) digunakan untuk mengatur kebijakan masa berlaku password pada level user, memaksa user mengganti password secara berkala sebagai praktik keamanan standar.

Perintah	Fungsi
sudo chage -l nama_user	Menampilkan kebijakan password yang berlaku saat ini pada user tersebut
sudo chage -M 90 nama_user	Menetapkan masa berlaku password maksimal 90 hari
sudo chage -m 7 nama_user	Menetapkan jarak minimal 7 hari sebelum password dapat diganti kembali
sudo chage -W 14 nama_user	Menetapkan peringatan 14 hari sebelum password kedaluwarsa

7.4 Kebijakan Kompleksitas Password melalui PAM

Pluggable Authentication Modules (PAM) adalah kerangka kerja modular pada Linux yang mengatur proses autentikasi sistem, termasuk penerapan aturan kompleksitas password (panjang minimal, kombinasi huruf besar/kecil, angka, simbol) menggunakan modul `pam_pwquality`.

Perintah/Konfigurasi	Fungsi
sudo apt install libpam-pwquality	Menginstal modul pwquality untuk PAM
minlen = 12	Baris pada /etc/security/pwquality.conf: panjang password minimal 12 karakter
dcredit = -1	Mewajibkan minimal 1 karakter angka pada password
ucredit = -1	Mewajibkan minimal 1 karakter huruf besar pada password
ocredit = -1	Mewajibkan minimal 1 karakter simbol pada password

7.5 Penguncian Akun Otomatis dengan faillock

Modul `pam_faillock` memungkinkan sistem secara otomatis mengunci sebuah akun setelah sejumlah percobaan login gagal dalam rentang waktu tertentu, melindungi akun dari serangan brute force pada level login sistem operasi (berbeda dengan fail2ban yang bekerja pada level jaringan/layanan).

Perintah/Konfigurasi	Fungsi
deny = 5	Baris pada konfigurasi PAM faillock: kunci akun setelah 5 kali percobaan gagal
unlock_time = 600	Akun otomatis terbuka kembali setelah 600 detik
faillock --user nama_user	Menampilkan riwayat percobaan gagal pada user tertentu
sudo faillock --user nama_user --reset	Membuka kunci akun secara manual sebelum unlock_time berakhir

7.6 Mengaktifkan Autentikasi Dua Faktor (2FA)

Autentikasi dua faktor (2FA) menambahkan lapisan verifikasi kedua di luar password, umumnya berupa kode sekali pakai (One-Time Password/OTP) yang dihasilkan oleh aplikasi authenticator pada perangkat terpisah. Modul `libpam-google-authenticator` memungkinkan penerapan 2FA berbasis TOTP (Time-based One-Time Password) pada login SSH.

Perintah	Fungsi
sudo apt install libpam-google-authenticator	Menginstal modul PAM untuk 2FA berbasis TOTP
google-authenticator	Menjalankan wizard pembuatan kunci rahasia 2FA untuk user yang login, menghasilkan QR code
auth required pam_google_authenticator.so	Baris yang ditambahkan pada /etc/pam.d/sshd untuk mewajibkan 2FA
ChallengeResponseAuthentication yes	Baris pada sshd_config agar SSH mendukung autentikasi tambahan (2FA)

7.7 Manajemen Siklus Hidup Akun (Account Lifecycle)

Keamanan akun pengguna bukan hanya soal pengaturan awal, melainkan juga pengelolaan berkelanjutan sepanjang siklus hidup akun tersebut, mulai dari pembuatan, penggunaan aktif, hingga penonaktifan ketika sudah tidak diperlukan (misalnya karyawan/siswa yang keluar dari organisasi). Akun yang tidak dinonaktifkan tepat waktu menjadi celah keamanan yang sering diabaikan.

Perintah	Fungsi
sudo usermod -e 2026-12-31 nama_user	Menetapkan tanggal kedaluwarsa akun (expire date)
sudo usermod -L nama_user	Mengunci akun (setara passwd -l) tanpa menghapus data/home directory

Perintah	Fungsi
sudo usermod -s /usr/sbin/nologin nama_user	Mencegah user login secara interaktif dengan mengubah shell default
sudo deluser --remove-home nama_user	Menghapus akun beserta home directory-nya secara permanen

Aktivitas Pembelajaran

2. Peserta didik mengaudit daftar user reguler pada mesin virtual menggunakan perintah awk, kemudian memeriksa apakah terdapat user dengan password kosong.
3. Peserta didik menerapkan kebijakan chage pada sebuah user dengan masa berlaku password 60 hari dan peringatan 7 hari sebelum kedaluwarsa.
4. Peserta didik mengonfigurasi pam_faillock dengan deny=3 dan unlock_time=300, kemudian menguji dengan sengaja memasukkan password salah tiga kali berturut-turut untuk memverifikasi akun terkunci.
5. Peserta didik memasang dan mengaktifkan 2FA menggunakan Google Authenticator pada login SSH, kemudian menguji login menggunakan password dan kode OTP dari aplikasi authenticator pada ponsel.

Studi Kasus dan Praktik (VMware)

Studi Kasus: Sekolah menemukan bahwa akun seorang siswa magang yang sudah menyelesaikan praktik kerja lapangan beberapa bulan lalu ternyata masih aktif pada server latihan, dengan password lemah dan tanpa masa berlaku. Sebagai teknisi jaringan, kalian diminta mengaudit seluruh akun yang ada, menerapkan kebijakan password yang lebih ketat, serta menonaktifkan akun yang tidak lagi digunakan.

Praktik berikut dilanjutkan pada VM Ubuntu Server yang sama, sesuai persiapan lingkungan praktik pada Bab 1. Disarankan membuat snapshot baru setelah praktik ini selesai sebagai titik pemulihan sebelum lanjut ke bab berikutnya.

Langkah	Perintah/Tindakan pada VM Ubuntu (VMware)
Nyalakan VM dan masuk sebagai user admin	Buka VMware, jalankan snapshot 'Bab6-Selesai', login sebagai teknisi_jaringan
Audit daftar user reguler pada sistem	awk -F: '$3 >= 1000 && $3 != 65534 {print $1}' /etc/passwd
Periksa akun dengan password kosong	sudo awk -F: '($2 == "") {print $1}' /etc/shadow
Terapkan kebijakan masa berlaku password	sudo chage -M 90 -m 7 -W 14 siswa_magang
Pasang modul kompleksitas password	sudo apt install libpam-pwquality
Atur aturan kompleksitas password	sudo nano /etc/security/pwquality.conf -> minlen=12, dcredit=-1, ucredit=-1, ocredit=-1
Konfigurasi penguncian akun otomatis	sudo nano /etc/security/faillock.conf -> deny=3, unlock_time=300
Uji penguncian akun	Masukkan password salah 3 kali berturut-turut, lalu verifikasi dengan faillock --user siswa_magang

Aktifkan autentikasi dua faktor pada SSH	sudo apt install libpam-google-authenticator lalu jalankan google-authenticator
Nonaktifkan akun yang tidak lagi digunakan	sudo usermod -L siswa_magang lalu sudo chage -E 0 siswa_magang
Simpan snapshot baru	Menu VM > Snapshot > Take Snapshot, beri nama 'Bab7-Selesai'

Bandingkan status akun siswa_magang sebelum dan sesudah praktik ini, lalu pastikan akun tersebut tidak lagi dapat digunakan untuk login sebagai bukti bahwa manajemen siklus hidup akun berhasil diterapkan.

Rangkuman

Keamanan akun pengguna sistem operasi mencakup audit daftar user aktif dan pemeriksaan kelemahan password, penerapan kebijakan masa berlaku password menggunakan chage, kebijakan kompleksitas password melalui PAM pwquality, penguncian akun otomatis menggunakan pam_faillock, hingga penerapan autentikasi dua faktor sebagai lapisan keamanan tambahan. Kompetensi ini melengkapi hardening akses pada level akun sebelum mempelajari keamanan koneksi remote (VPN) pada bab berikutnya.

Soal Latihan / Refleksi

6. Jelaskan perbedaan user sistem dan user reguler pada Linux beserta cara membedakannya melalui UID.
7. Tuliskan perintah chage untuk menetapkan masa berlaku password maksimal 60 hari pada user 'siswa1'.
8. Jelaskan perbedaan fungsi pam_faillock dengan fail2ban yang telah dipelajari pada Bab 4.
9. Mengapa autentikasi dua faktor dianggap lebih aman dibanding autentikasi berbasis password saja?

BAB 8 — Keamanan Koneksi Remote (VPN)

Tujuan Pembelajaran

- Peserta didik mampu menginstal OpenVPN/WireGuard beserta komponen pendukungnya pada server Linux.
- Peserta didik mampu membangun Public Key Infrastructure (PKI) untuk kebutuhan VPN.
- Peserta didik mampu mengonfigurasi server VPN dan menguji koneksi client.
- Peserta didik mampu mengaktifkan IP forwarding dan menerapkan pre-shared key sebagai lapisan keamanan tambahan.

8.1 Konsep VPN dan Manfaatnya

Virtual Private Network (VPN) menciptakan sebuah 'terowongan' (tunnel) terenkripsi antara dua titik melalui jaringan publik seperti internet, sehingga data yang dikirimkan tidak dapat dibaca oleh pihak yang tidak berwenang meskipun melewati jaringan yang tidak dipercaya. VPN umum digunakan untuk menghubungkan pekerja remote ke jaringan kantor secara aman, menghubungkan kantor cabang ke kantor pusat (site-to-site VPN), maupun melindungi privasi pengguna saat mengakses internet publik.

8.2 OpenVPN vs WireGuard

Aspek	OpenVPN	WireGuard
Usia teknologi	Matang, sejak awal 2000-an	Relatif baru, diadopsi luas sejak 2020-an
Kompleksitas konfigurasi	Lebih kompleks, memerlukan PKI penuh	Lebih sederhana, berbasis pasangan kunci
Performa	Baik, namun umumnya lebih lambat	Sangat cepat karena desain minimalis di kernel
Basis kriptografi	OpenSSL (fleksibel, banyak cipher)	Cryptography modern tetap (fixed, lebih sederhana)

OpenVPN cocok pada skenario yang membutuhkan fleksibilitas konfigurasi tinggi dan kompatibilitas luas, sedangkan WireGuard menjadi pilihan populer untuk implementasi modern yang mengutamakan kesederhanaan dan performa.

8.3 Instalasi OpenVPN dan Easy-RSA

Perintah	Fungsi
sudo apt install openvpn easy-rsa	Menginstal OpenVPN beserta Easy-RSA untuk manajemen PKI

Perintah	Fungsi
make-cadir ~/easy-rsa && cd ~/easy-rsa	Membuat direktori kerja Easy-RSA
./easyrsa init-pki	Menginisialisasi struktur Public Key Infrastructure

8.4 Membangun Public Key Infrastructure (PKI) untuk OpenVPN

PKI pada OpenVPN terdiri atas Certificate Authority (CA) sebagai otoritas penerbit sertifikat, sertifikat dan kunci server, sertifikat dan kunci untuk setiap client, serta parameter Diffie-Hellman untuk pertukaran kunci yang aman.

Perintah	Fungsi
./easyrsa build-ca	Membuat Certificate Authority (akan meminta passphrase CA)
./easyrsa gen-req server nopass	Membuat permintaan sertifikat (CSR) untuk server tanpa passphrase
./easyrsa sign-req server server	Menandatangani CSR server menggunakan CA, menghasilkan sertifikat server
./easyrsa gen-req client1 nopass	Membuat CSR untuk client bernama client1
./easyrsa sign-req client client1	Menandatangani CSR client1 menggunakan CA
./easyrsa gen-dh	Menghasilkan parameter Diffie-Hellman (proses ini memakan waktu cukup lama)

8.5 Mengonfigurasi Server VPN

Setelah PKI terbentuk, file konfigurasi server OpenVPN (server.conf) perlu menunjuk pada file-file sertifikat dan kunci yang telah dibuat, serta menentukan protokol, port, dan skema alamat IP virtual yang akan diberikan kepada client.

Directive	Contoh Nilai	Keterangan
port	1194	Port default OpenVPN
proto	udp	Protokol transport, UDP umum digunakan untuk performa lebih baik
dev	tun	Jenis interface virtual (tun untuk routing layer 3)
server	10.8.0.0 255.255.255.0	Blok alamat IP virtual yang akan diberikan kepada client VPN

Directive	Contoh Nilai	Keterangan
push "route"	192.168.1.0 255.255.255.0	Memberi tahu client rute menuju jaringan lokal yang dapat diakses melalui VPN

Perintah	Fungsi
sudo systemctl start openvpn@server	Memulai layanan server OpenVPN sesuai file server.conf
sudo systemctl enable openvpn@server	Mengaktifkan OpenVPN agar berjalan otomatis saat boot

8.6 Mengaktifkan IP Forwarding dan Menguji Koneksi Client

Agar client VPN dapat mengakses jaringan lokal di balik server VPN (bukan hanya berkomunikasi dengan server itu sendiri), server perlu mengaktifkan **IP forwarding** pada level kernel, yang memungkinkan server meneruskan paket antar interface.

Perintah/Konfigurasi	Fungsi
net.ipv4.ip_forward = 1	Baris pada /etc/sysctl.conf untuk mengaktifkan IP forwarding secara permanen
sudo sysctl -p	Menerapkan perubahan sysctl.conf tanpa perlu boot ulang
sudo nft add rule ip nat postrouting oifname "eth0" masquerade	Menerapkan NAT agar lalu lintas dari client VPN dapat keluar ke jaringan lokal/internet
openvpn --config client1.ovpn	Menjalankan koneksi VPN dari sisi client menggunakan file konfigurasi client
ping 192.168.1.1	Menguji dari client VPN apakah dapat mengakses jaringan lokal di balik server

8.7 Pre-Shared Key sebagai Lapisan Keamanan Tambahan

Selain autentikasi berbasis sertifikat, OpenVPN mendukung penambahan **pre-shared key (tls-auth/tls-crypt)** sebagai lapisan keamanan HMAC tambahan yang melindungi terhadap serangan tertentu seperti DoS dan port scanning terhadap layanan VPN itu sendiri, karena paket yang tidak memiliki HMAC signature yang valid akan langsung ditolak sebelum diproses lebih lanjut oleh proses TLS handshake.

Perintah	Fungsi
openvpn --genkey secret ta.key	Menghasilkan pre-shared key (ta.key) untuk lapisan HMAC tambahan
tls-auth ta.key 0	Baris pada server.conf: mengaktifkan tls-auth dengan ta.key (arah 0 untuk server)
tls-auth ta.key 1	Baris pada file konfigurasi client: arah 1 untuk client

8.8 Contoh Konfigurasi Dasar WireGuard

Sebagai perbandingan praktis terhadap kompleksitas OpenVPN, berikut contoh konfigurasi minimal WireGuard yang menunjukkan kesederhanaan pendekatannya, hanya membutuhkan pasangan kunci publik-privat tanpa PKI penuh.

Perintah	Fungsi
sudo apt install wireguard	Menginstal WireGuard pada server dan client
wg genkey | tee privatekey | wg pubkey > publickey	Menghasilkan pasangan kunci privat dan publik WireGuard
[Interface]\nPrivateKey = [kunci_privat_server]\nAddress = 10.9.0.1/24\nListenPort = 51820	Contoh isi file konfigurasi server (wg0.conf) bagian Interface
[Peer]\nPublicKey = [kunci_publik_client]\nAllowedIPs = 10.9.0.2/32	Contoh bagian Peer pada server yang mendefinisikan client yang diizinkan
sudo wg-quick up wg0	Mengaktifkan interface WireGuard sesuai konfigurasi wg0.conf

Aktivitas Pembelajaran

10. Peserta didik membangun server OpenVPN lengkap di mesin virtual, mulai dari instalasi, pembuatan PKI (CA, sertifikat server dan client), hingga konfigurasi server.conf.
11. Peserta didik menghasilkan file konfigurasi client (.ovpn) dan menguji koneksi dari mesin virtual client, memverifikasi client menerima alamat IP virtual dari server.
12. Peserta didik mengaktifkan IP forwarding dan NAT pada server VPN, kemudian menguji client VPN dapat melakukan ping ke jaringan lokal di balik server.
13. Peserta didik menambahkan tls-auth dengan pre-shared key pada konfigurasi server dan client, kemudian menguji ulang koneksi untuk memastikan tetap berfungsi dengan lapisan keamanan tambahan tersebut.

Studi Kasus dan Praktik (VMware)

Studi Kasus: Beberapa siswa perlu mengerjakan tugas praktik dari rumah dengan mengakses server latihan sekolah, namun membuka akses SSH langsung ke internet dinilai berisiko tinggi terhadap serangan

brute force. Sebagai teknisi jaringan, kalian diminta membangun jalur akses remote yang aman menggunakan VPN sebelum akses dari luar sekolah diizinkan.

Praktik berikut dilanjutkan pada VM Ubuntu Server yang sama, sesuai persiapan lingkungan praktik pada Bab 1. Disarankan membuat snapshot baru setelah praktik ini selesai sebagai titik pemulihan sebelum lanjut ke bab berikutnya.

Langkah	Perintah/Tindakan pada VM Ubuntu (VMware)
Nyalakan VM dan masuk sebagai user admin	Buka VMware, jalankan snapshot 'Bab7-Selesai', login sebagai teknisi_jaringan
Instal OpenVPN dan Easy-RSA	sudo apt install openvpn easy-rsa
Bangun direktori dan inisialisasi PKI	make-cadir ~/easy-rsa && cd ~/easy-rsa && ./easyrsa init-pki
Buat Certificate Authority dan sertifikat server	./easyrsa build-ca nopass lalu ./easyrsa build-server-full server nopass
Salin sertifikat ke direktori OpenVPN	sudo cp pki/ca.crt pki/issued/server.crt pki/private/server.key /etc/openvpn/server/
Konfigurasi server VPN	sudo nano /etc/openvpn/server/server.conf -> atur port, proto udp, dev tun, path ca/cert/key
Aktifkan IP forwarding	sudo sysctl -w net.ipv4.ip_forward=1 lalu tambahkan net.ipv4.ip_forward=1 pada /etc/sysctl.conf
Jalankan dan aktifkan layanan OpenVPN	sudo systemctl start openvpn@server lalu sudo systemctl enable openvpn@server
Buat sertifikat client untuk siswa	./easyrsa build-client-full siswa1 nopass lalu susun berkas siswa1.ovpn
Uji koneksi dari sisi client	openvpn --config siswa1.ovpn lalu ping ke alamat IP jaringan lokal server
Simpan snapshot baru	Menu VM > Snapshot > Take Snapshot, beri nama 'Bab8-Selesai'

Bandingkan hasil percobaan akses SSH langsung dari internet dengan akses melalui terowongan VPN, lalu jelaskan mengapa VPN dianggap sebagai jalur akses remote yang lebih aman bagi siswa yang belajar dari rumah.

Rangkuman

VPN membangun terowongan komunikasi terenkripsi melalui jaringan publik, dengan OpenVPN dan WireGuard sebagai dua implementasi populer yang memiliki karakteristik berbeda. Konfigurasi OpenVPN melibatkan pembangunan PKI (CA, sertifikat server/client, parameter Diffie-Hellman), konfigurasi server, pengaktifan IP forwarding untuk akses jaringan lokal, serta penambahan pre-shared key sebagai lapisan keamanan tambahan. Kompetensi ini melengkapi kemampuan mengamankan akses remote sebelum mempelajari forensik digital pada bab berikutnya.

Soal Latihan / Refleksi

14. Jelaskan perbedaan utama antara OpenVPN dan WireGuard.
15. Sebutkan komponen utama Public Key Infrastructure (PKI) yang dibutuhkan untuk membangun server OpenVPN.
16. Mengapa IP forwarding perlu diaktifkan pada server VPN agar client dapat mengakses jaringan lokal?
17. Jelaskan manfaat penambahan tls-auth/pre-shared key pada konfigurasi OpenVPN.

LAMPIRAN — SIMULASI KEAMANAN JARINGAN MENGGUNAKAN GNS3

Tujuan Pembelajaran

- Peserta didik mampu menjelaskan fungsi GNS3 sebagai simulator jaringan berbasis perangkat nyata (Cisco IOS, Docker, QEMU) untuk kebutuhan praktik keamanan jaringan.
- Peserta didik mampu memasang (instalasi) GNS3 pada sistem operasi Windows maupun Ubuntu beserta komponen pendukungnya (GNS3 VM, Dynamips, Docker).
- Peserta didik mampu membangun topologi simulasi jaringan bertingkat (LAN, DMZ, dan gateway) menggunakan GNS3 sebagai wadah praktik hardening, firewall, dan deteksi intrusi.
- Peserta didik mampu mengintegrasikan mesin virtual hardening (VirtualBox/VMware) yang telah dipelajari pada Bab 2 sampai Bab 6 ke dalam topologi simulasi GNS3.

Seluruh praktik pada Bab 2 sampai Bab 6 sejauh ini dilakukan pada satu mesin virtual tunggal atau jaringan sederhana antar mesin virtual dalam satu segmen. Pada praktiknya, ujian praktik Hardening LKS maupun kondisi kerja nyata menuntut peserta didik memahami topologi jaringan yang lebih kompleks, misalnya jaringan dengan beberapa segmen (LAN, DMZ, WAN) yang dihubungkan oleh router/gateway. GNS3 (Graphical Network Simulator-3) hadir sebagai alat bantu open source untuk mensimulasikan topologi semacam ini secara visual, tanpa memerlukan perangkat jaringan fisik.

6.7 Mengenal GNS3 sebagai Simulator Jaringan

GNS3 adalah perangkat lunak simulasi jaringan yang memungkinkan pengguna merangkai topologi jaringan secara grafis (drag-and-drop) menggunakan node berupa router, switch, firewall, maupun komputer virtual. Berbeda dengan simulator sederhana seperti Packet Tracer, GNS3 dapat menjalankan citra (image) sistem operasi jaringan yang sesungguhnya, seperti Cisco IOS, serta mengintegrasikan mesin virtual VirtualBox/VMware dan kontainer Docker sebagai node di dalam topologi. Karakteristik inilah yang membuat GNS3 relevan untuk mensimulasikan skenario hardening, firewall gateway, dan deteksi intrusi yang telah dipelajari pada bab-bab sebelumnya secara lebih realistis.

Komponen	Fungsi dalam Simulasi
GNS3 GUI (Client)	Antarmuka grafis untuk merancang topologi, menambah node, dan menghubungkan tautan antar perangkat
GNS3 Server	Mesin yang benar-benar menjalankan node simulasi (dapat berupa mesin lokal atau GNS3 VM terpisah)
GNS3 VM	Mesin virtual Linux siap pakai yang menjalankan server GNS3 beserta Docker dan Dynamips secara terisolasi
Dynamips/IOU	Komponen emulator yang menjalankan citra Cisco IOS/IOS pada node router
Docker Node	Node berbasis kontainer (mis. Ubuntu, Alpine) yang ringan untuk mensimulasikan host/server
Cloud/NAT Node	Menjembatani topologi simulasi dengan jaringan fisik/host asli, termasuk mesin virtual VirtualBox

6.8 Instalasi GNS3 di Windows

Pada sistem operasi Windows, GNS3 dipasang melalui installer all-in-one yang tersedia di situs resmi gns3.com. Karena Windows tidak memiliki dukungan native untuk menjalankan Dynamips, IOU, maupun kontainer Docker secara penuh, disarankan menambahkan GNS3 VM (berbasis VirtualBox atau VMware) sebagai server simulasi agar seluruh jenis node dapat berjalan dengan baik.

Langkah	Perintah/Tindakan
Unduh installer GNS3	Unduh GNS3 All-in-one installer for Windows dari situs resmi gns3.com/software/download
Pasang GNS3 dan Npcap	Jalankan installer, sertakan komponen Npcap/WinPcap saat diminta agar antarmuka jaringan host terdeteksi
Pasang VirtualBox	Instal VirtualBox sebagai hypervisor untuk menjalankan GNS3 VM dan mesin virtual hardening
Unduh GNS3 VM	Unduh berkas GNS3 VM (format .ova) dari halaman download GNS3, lalu impor melalui File > Import Appliance pada VirtualBox
Hubungkan GNS3 ke GNS3 VM	Pada GNS3 GUI, buka Edit > Preferences > GNS3 VM, aktifkan opsi Enable the GNS3 VM dan pilih VirtualBox sebagai virtualization engine
Uji koneksi server	Klik Test Settings pada Preferences untuk memastikan GNS3 GUI berhasil terhubung ke GNS3 VM sebagai server simulasi

6.9 Instalasi GNS3 di Ubuntu

Pada Ubuntu, GNS3 dapat dipasang langsung sebagai aplikasi native karena sistem operasi ini sudah mendukung Dynamips, Docker, dan KVM/QEMU tanpa lapisan virtualisasi tambahan, sehingga performa simulasi umumnya lebih ringan dibandingkan pada Windows.

Perintah	Fungsi
sudo add-apt-repository ppa:gns3/ppa	Menambahkan repository resmi GNS3 ke daftar sumber paket Ubuntu
sudo apt update	Memperbarui indeks paket setelah repository GNS3 ditambahkan
sudo apt install gns3-gui gns3-server	Memasang aplikasi GUI dan server GNS3 sekaligus
sudo usermod -aG ubridge,libvirt,kvm,wireshark,docker $USER	Menambahkan pengguna ke grup yang diperlukan agar GNS3 dapat mengakses bridge jaringan, virtualisasi KVM, dan Docker tanpa sudo
sudo apt install docker.io	Memasang Docker sebagai mesin kontainer untuk node berbasis image ringan (mis. Ubuntu, Alpine)
newgrp docker	Menerapkan keanggotaan grup docker pada sesi terminal aktif tanpa perlu logout

Setelah instalasi selesai, GNS3 server dapat dijalankan secara lokal (localhost) tanpa memerlukan GNS3 VM tambahan, karena Ubuntu sudah mampu menjalankan Dynamips dan Docker secara native. Konfigurasi server lokal ini dipilih pada GNS3 GUI melalui Edit > Preferences > Server dengan opsi Local Server.

6.10 Membangun Topologi Simulasi Hardening dan Firewall

Topologi simulasi dirancang agar mencerminkan skenario yang telah dipelajari pada Bab 2 sampai Bab 6, yaitu jaringan dengan segmen LAN (tempat client/attacker berada), segmen DMZ (tempat server yang dihardening berada), serta sebuah node gateway yang menjalankan firewall nftables/UFW sebagaimana dibahas pada Bab 3.

Node	Peran dalam Topologi Simulasi
Cloud	Menjembatani topologi ke adaptor jaringan host, memungkinkan mesin virtual hardening (VirtualBox) ikut serta dalam simulasi
Switch (Ethernet Switch)	Menghubungkan beberapa node dalam satu segmen jaringan (LAN atau DMZ)
Router/Gateway (VM Ubuntu Server)	Node bertindak sebagai gateway yang menjalankan firewall nftables/UFW dan NAT/port forwarding (Bab 3)
VM Server DMZ (VM Ubuntu Server)	Target hardening yang telah dikonfigurasi SSH, fail2ban, dan MySQL sesuai Bab 2, 4, dan 6
VPCS (Virtual PC Simulator)	Node ringan bawaan GNS3 untuk mensimulasikan client biasa yang menguji konektivitas
Kali Linux (VM/Docker)	Node penyerang untuk mensimulasikan port scanning (nmap) sesuai aktivitas pembelajaran Bab 3

Langkah umum menyusun topologi ini di GNS3 GUI adalah: (1) tarik node Cloud, Switch, dan VM appliance yang telah diimpor ke kanvas kerja; (2) hubungkan tautan antar node sesuai segmen LAN dan DMZ; (3) atur node gateway agar memiliki dua antarmuka jaringan, satu menghadap LAN dan satu menghadap DMZ, meniru konfigurasi NAT dan port forwarding pada Bab 3; (4) jalankan (start) seluruh node, lalu masuk ke konsol masing-masing VM untuk menerapkan konfigurasi hardening, firewall, dan IDS/IPS yang telah dipelajari.

6.11 Menjalankan Simulasi Deteksi Intrusi dan Pengujian Firewall

Setelah topologi berjalan, peserta didik dapat mensimulasikan skenario pengujian keamanan secara end-to-end di dalam GNS3, misalnya menjalankan port scanning dari node Kali Linux menuju VM server DMZ, mengamati bagaimana aturan firewall gateway (Bab 3) menahan atau meneruskan trafik, serta memeriksa apakah Snort atau fail2ban (Bab 4) berhasil mendeteksi dan mencatat percobaan tersebut pada log.

Perintah/Tindakan	Tujuan Pengujian
nmap -sS -p 1-1000 <IP_VM_DMZ>	Menjalankan port scan dari node Kali Linux untuk menguji port mana saja yang tampak terbuka dari luar DMZ
sudo tail -f /var/log/auth.log	Memantau log autentikasi pada VM server DMZ untuk melihat percobaan akses yang tercatat
sudo fail2ban-client status sshd	Memeriksa apakah fail2ban telah memblokir IP node penyerang setelah beberapa percobaan gagal
Klik kanan tautan > Start capture (Wireshark)	Menangkap paket pada tautan GNS3 tertentu untuk menganalisis trafik secara langsung dari GUI

6.12 Menyimpan dan Mendokumentasikan Proyek Simulasi

Setiap topologi yang telah disusun dapat disimpan sebagai berkas proyek (.gns3project) yang memuat konfigurasi node, tautan, dan posisi topologi, sehingga dapat dibuka kembali atau dibagikan kepada peserta didik/guru lain melalui menu File > Export Portable Project. Dokumentasi topologi dalam bentuk tangkapan layar dan penjelasan alur pengujian sebaiknya disertakan pada laporan praktik sebagai bukti kompetensi simulasi jaringan.

6.13 Simulasi VPN Akses Remote Menggunakan WireGuard di GNS3

Topologi LAN-Gateway-DMZ yang telah dibangun sejauh ini mensimulasikan kompetensi hardening, firewall, dan deteksi intrusi (Bab 2 sampai Bab 6), namun belum mencakup kompetensi keamanan koneksi remote (VPN) yang dipelajari pada Bab 8. Bagian ini memperluas topologi dengan menambahkan segmen WAN dan sebuah node client remote, sehingga peserta didik dapat mensimulasikan skenario siswa yang mengakses VM server DMZ dari luar sekolah melalui tunnel WireGuard, sekaligus membuktikan bahwa firewall gateway (Bab 3) hanya membuka satu celah masuk yaitu port WireGuard.

Node	Peran dalam Topologi Simulasi VPN
Cloud (WAN/Internet)	Node tambahan yang menjembatani node client remote ke antarmuka luar node gateway, mensimulasikan jaringan publik/internet yang memisahkan siswa di rumah dari jaringan sekolah
Ubuntu Server VM (Gateway)	Peran node gateway diperluas: selain menjalankan firewall nftables/UFW (Bab 3), node ini juga dipasangi WireGuard server pada interface wg0 sebagai titik akhir (endpoint) tunnel VPN
VM/Docker Client Remote (mis. Ubuntu Server atau Alpine Linux)	Node baru yang mensimulasikan komputer siswa yang belajar dari rumah, dipasangi WireGuard client untuk membangun tunnel menuju gateway sekolah sebelum mengakses VM server DMZ

Susun topologi dengan menghubungkan node client remote ke node Cloud (WAN), kemudian node Cloud ke antarmuka luar node gateway; antarmuka dalam gateway tetap terhubung ke segmen DMZ seperti topologi sebelumnya. Setelah tautan tersusun, jalankan konfigurasi WireGuard pada node gateway dan node client remote berikut, mengikuti konsep yang telah dipelajari pada Bab 8.

Perintah/Konfigurasi pada Node Gateway	Fungsi
sudo apt install wireguard	Memasang WireGuard pada node gateway GNS3
wg genkey | tee /etc/wireguard/privatekey | wg pubkey > /etc/wireguard/publickey	Menghasilkan pasangan kunci privat dan publik server, sesuai prosedur Bab 8
sudo nano /etc/wireguard/wg0.conf -> isi [Interface] PrivateKey, Address = 10.9.0.1/24, ListenPort = 51820	Membuat konfigurasi interface WireGuard pada sisi server
Tambahkan [Peer] PublicKey = <kunci_publik_client>, AllowedIPs = 10.9.0.2/32	Mendaftarkan node client remote sebagai peer yang diizinkan membentuk tunnel
sudo ufw allow 51820/udp	Mengizinkan port WireGuard pada firewall gateway (Bab 3) sebagai satu-satunya celah masuk dari segmen WAN
sudo nft add rule ip nat postrouting oifname "eth1" masquerade	Menerapkan NAT masquerade agar trafik dari tunnel wg0 dapat diteruskan menuju segmen DMZ

sudo wg-quick up wg0	Mengaktifkan interface WireGuard pada node gateway
Perintah/Konfigurasi pada Node Client Remote	**Fungsi**
sudo apt install wireguard	Memasang WireGuard pada node client remote
wg genkey | tee privatekey | wg pubkey > publickey	Menghasilkan pasangan kunci privat dan publik client
sudo nano /etc/wireguard/wg0.conf -> isi [Interface] PrivateKey, Address = 10.9.0.2/24	Membuat bagian Interface pada konfigurasi client
Tambahkan [Peer] PublicKey = <kunci_publik_gateway>, Endpoint = <IP_WAN_gateway>:51820, AllowedIPs = 192.168.100.0/24, PersistentKeepalive = 25	Menunjuk endpoint gateway sekolah melalui segmen WAN/Cloud serta membatasi rute hanya menuju subnet DMZ
sudo wg-quick up wg0	Mengaktifkan tunnel VPN dari sisi client remote
Perintah/Tindakan Pengujian	**Tujuan Pengujian**
sudo wg show (dijalankan pada node gateway maupun client remote)	Menampilkan status handshake dan statistik trafik pada interface wg0, memastikan tunnel berhasil terbentuk
ping 192.168.100.10 (dari node client remote menuju VM server DMZ)	Menguji bahwa client remote dapat menjangkau server DMZ melalui tunnel WireGuard yang telah aktif
ssh -p 2222 teknisi_jaringan@192.168.100.10 (dijalankan setelah tunnel aktif)	Memverifikasi akses SSH ke server DMZ hanya berhasil melalui jalur VPN, bukan langsung dari segmen WAN
Klik kanan tautan node Cloud-Gateway > Start capture (Wireshark)	Menangkap paket pada segmen WAN untuk membuktikan lalu lintas yang melintas hanya berupa paket UDP terenkripsi pada port 51820, bukan trafik SSH/HTTP polos
nmap -p 1-1000 <IP_WAN_gateway> (dijalankan dari node Cloud/luar)	Membuktikan bahwa seluruh port pada gateway tertutup dari jaringan luar kecuali port UDP 51820, sesuai kebijakan default deny (Bab 3)

Hasil pengujian di atas menunjukkan bahwa client remote wajib membentuk tunnel WireGuard terlebih dahulu sebelum dapat menjangkau layanan pada VM server DMZ, karena firewall gateway hanya membuka port WireGuard dan menolak seluruh port lain secara default. Simulasi ini mengintegrasikan kompetensi keamanan koneksi remote (Bab 8) ke dalam topologi GNS3 secara menyeluruh, melengkapi simulasi hardening, firewall, dan deteksi intrusi yang telah dibangun sebelumnya.

Aktivitas Pembelajaran

44. Peserta didik memasang GNS3 pada salah satu sistem operasi (Windows atau Ubuntu) sesuai perangkat yang tersedia, termasuk GNS3 VM apabila menggunakan Windows.
45. Peserta didik membangun topologi sederhana terdiri atas satu segmen LAN, satu node gateway, dan satu segmen DMZ menggunakan node Cloud, Switch, dan VM appliance.
46. Peserta didik mengimpor mesin virtual hardening hasil praktik Bab 2 dan Bab 6 ke dalam topologi GNS3 menggunakan node Cloud sebagai penghubung ke VirtualBox.
47. Peserta didik menjalankan simulasi port scanning dari node Kali Linux menuju VM server DMZ, kemudian memverifikasi bahwa firewall gateway (Bab 3) dan fail2ban (Bab 4) merespons sesuai konfigurasi yang telah diterapkan.
48. Peserta didik menyimpan topologi sebagai berkas .gns3project dan menyusun laporan singkat berisi tangkapan layar topologi beserta hasil pengujian.

49. Peserta didik memperluas topologi GNS3 dengan menambahkan node Cloud (WAN) dan satu node client remote, kemudian memasang serta mengonfigurasi WireGuard pada node gateway dan node client remote sesuai konsep yang telah dipelajari pada Bab 8.
50. Peserta didik menguji bahwa VM server DMZ hanya dapat diakses melalui tunnel WireGuard yang aktif, dengan membandingkan hasil port scanning dari node Cloud sebelum dan sesudah tunnel VPN terbentuk, serta menangkap trafik menggunakan Wireshark untuk membuktikan bahwa data yang melintas telah terenkripsi.

Rangkuman

GNS3 merupakan simulator jaringan open source yang memungkinkan peserta didik merangkai topologi multi-segmen menggunakan node router, switch, serta mesin virtual/Docker, dan dapat dipasang baik di Windows (dengan bantuan GNS3 VM) maupun Ubuntu (secara native). Dengan mengintegrasikan mesin virtual hardening yang telah dibangun pada Bab 2 sampai Bab 6 ke dalam topologi GNS3, peserta didik dapat mensimulasikan skenario jaringan LAN-DMZ-gateway secara lebih realistis, mempraktikkan pengujian firewall, deteksi intrusi, dan dokumentasi hasil simulasi sebagai persiapan menghadapi ujian praktik maupun kondisi kerja nyata. Penambahan segmen WAN dan tunnel VPN WireGuard pada topologi ini turut mengintegrasikan kompetensi keamanan koneksi remote (Bab 8), sehingga simulasi mencakup seluruh lapisan keamanan jaringan yang telah dipelajari pada jilid ini.

Soal Latihan / Refleksi

51. Jelaskan perbedaan mendasar antara GNS3 dan simulator jaringan sederhana seperti Packet Tracer.
52. Mengapa instalasi GNS3 di Windows umumnya memerlukan GNS3 VM, sedangkan di Ubuntu tidak?
53. Sebutkan minimal tiga jenis node yang dapat digunakan dalam topologi simulasi GNS3 beserta fungsinya.
54. Rancang topologi sederhana (LAN - Gateway - DMZ) menggunakan node GNS3, lalu jelaskan bagaimana Anda akan menguji efektivitas firewall gateway terhadap percobaan port scanning.
55. Jelaskan mengapa node client remote pada topologi GNS3 hanya dapat mengakses VM server DMZ setelah tunnel WireGuard aktif, dikaitkan dengan kebijakan firewall default deny pada node gateway.
56. Bandingkan kompleksitas penambahan node VPN WireGuard pada simulasi GNS3 dengan penambahan node OpenVPN, ditinjau dari jumlah langkah konfigurasi yang diperlukan.