RINGKASAN MATERI & PANDUAN PRAKTIK

Bab 7–11: Akun Pengguna • VPN • Forensik Digital • Capture The Flag • Rangkuman

Versi Ringkas — Fokus Setup Praktik & Studi Kasus

Mata Pelajaran Keamanan Jaringan — Kelas XII TJKT (Jilid 2)

Catatan: Bab 2–6 (Hardening, Firewall, IDS/IPS, Kriptografi, Basis Data) merupakan bagian Jilid 1 (Kelas XI) dan tidak termasuk dalam berkas ini.

Panduan Umum Setup Laboratorium Praktik

Panduan ini berlaku untuk seluruh sesi praktik pada Bab 7–11, dipersiapkan sebelum masuk ke setup spesifik tiap bab.

Topologi Laboratorium

Mengapa harus terisolasi? Praktik keamanan jaringan sering melibatkan perubahan konfigurasi yang berisiko (mis. memblokir port, mengunci akun, mensimulasikan serangan). Bila dilakukan di jaringan produksi sekolah, kesalahan kecil bisa mengganggu layanan nyata. Jaringan lab yang terisolasi membuat peserta didik bebas bereksperimen dan boleh sampai gagal tanpa dampak ke luar lab.

- Gunakan software virtualisasi: VirtualBox, VMware Workstation, atau Proxmox VE.
- Minimal 3 VM per kelompok: (1) Server Target — yang di-hardening/dikonfigurasi, (2) Attacker/Tester — simulasi serangan (nmap, login gagal, dsb.), (3) Client VPN — uji konektivitas remote pada Bab 8.
- Seluruh VM berada di jaringan internal/host-only, terpisah dari jaringan sekolah & internet publik; aktifkan NAT sementara hanya saat instalasi paket.

Spesifikasi Minimal VM

Peran Mesin	OS & RAM Minimal
Server Target	Ubuntu Server 22.04 / Debian 12 — 1 GB RAM (instalasi minimal tanpa GUI)
Attacker/Tester	Kali Linux / Ubuntu Desktop — 2 GB RAM (nmap, wireshark, dsb.)
Client VPN	Ubuntu Desktop / Windows — 1 GB RAM

Jadwal & Manajemen Sesi

- Setiap elemen wajib disarankan 2 pertemuan (@2 JP): pertemuan 1 demonstrasi + praktik terpandu, pertemuan 2 praktik mandiri + uji kompetensi.
- CTF (Bab 10) cocok sebagai proyek akhir semester berbentuk kompetisi kelas.
- Gunakan fitur snapshot sebelum tiap sesi praktik baru — simpan kondisi "bersih" VM agar mudah rollback bila konfigurasi salah (mis. admin terkunci dari SSH), dan peserta didik bisa mengulang latihan dari kondisi default.

Verifikasi / Uji Coba: Lab Siap Digunakan

Sebelum masuk ke materi bab, pastikan dulu ketiga VM benar-benar bisa saling "melihat" satu sama lain di jaringan internal. Jalankan perintah berikut dari tiap VM untuk memastikan topologi sudah benar:

Perintah	Fungsi
ip addr show	Menampilkan alamat IP tiap VM — pastikan berada di subnet internal yang sama (mis. 192.168.56.0/24)
ping -c 3 <ip_vm_lain>	Menguji konektivitas antar VM dalam jaringan lab; balasan sukses = topologi benar
ping -c 3 8.8.8.8	Menguji akses internet sementara (hanya perlu saat instalasi paket, boleh gagal di luar itu)

Jika ping antar VM gagal, periksa kembali pengaturan network adapter (harus "Internal Network"/"Host-only" dengan nama yang sama pada seluruh VM), bukan "NAT" atau "Bridged".

BAB 7 — Keamanan Akun Pengguna Sistem Operasi

Materi Inti (Ringkas)

- Bedakan user sistem (UID < 1000) dan user reguler (UID ≥ 1000); audit dengan cat /etc/passwd, awk, lastlog, who/w.
- chage: kebijakan masa berlaku password (-M maks hari, -m jarak minimal, -W peringatan).
- PAM pwquality: kompleksitas password (minlen, dcredit, ucredit, ocredit).
- pam_faillock: kunci akun otomatis setelah N kali gagal (beda dari fail2ban yang bekerja di level jaringan).
- 2FA (libpam-google-authenticator): OTP/TOTP tambahan pada login SSH.
- Siklus hidup akun: usermod -e (expire), -L (lock), -s nologin, deluser --remove-home.

Setup Praktik

Tujuan setup ini adalah menciptakan kondisi server yang realistis — bukan server "bersih" ideal, melainkan server yang sudah dipakai bertahun-tahun dan punya masalah kebersihan akun seperti umumnya ditemukan di lapangan (akun lama yang lupa dinonaktifkan, password lemah, dsb). Dengan begitu, peserta didik berlatih pada kondisi nyata, bukan skenario buatan yang terlalu rapi.

- Siapkan 1 VM Linux dengan minimal 3 akun dummy: 1 admin, 1 user aktif, 1 user "eks-siswa" yang seharusnya sudah nonaktif.
- Buat 1 akun sengaja memiliki password kosong/lemah sebagai temuan audit (untuk didemonstrasikan bahayanya).
- Instal modul: sudo apt install libpam-pwquality libpam-google-authenticator -y
- Siapkan smartphone/emulator dengan aplikasi authenticator (Google Authenticator/Authy/FreeOTP) untuk uji 2FA.
- Backup /etc/pam.d/sshd dan /etc/ssh/sshd_config sebelum praktik agar mudah rollback jika salah konfigurasi mengunci akses.

Verifikasi / Uji Coba

Setelah tiap langkah setup di atas dijalankan, gunakan perintah berikut untuk memastikan konfigurasi benar-benar aktif — jangan hanya berasumsi berhasil karena tidak ada pesan error:

Perintah	Yang Diverifikasi
sudo chage -l nama_user	Menampilkan kebijakan chage yang sedang berlaku — pastikan angka masa berlaku & peringatan sesuai yang diset
sudo cat /etc/security/pwquality.conf	Memastikan baris minlen/dcredit/ucredit/ocredit sudah tersimpan dan tidak typo
sudo faillock --user nama_user	Menampilkan riwayat percobaan gagal user — jumlah percobaan harus bertambah setiap kali login salah dicoba
sudo passwd -S nama_user	Mengecek status akun (L = locked, P = password aktif, NP = tanpa password)
ssh nama_user@ip_vm	Uji langsung: setelah 2FA aktif, seharusnya muncul prompt tambahan "Verification code:" setelah password

Studi Kasus

Skenario: Sekolah baru saja meluluskan satu angkatan siswa. Admin TI diminta membersihkan dan mengamankan akun-akun pada server lab sebelum tahun ajaran baru dimulai.

1. Audit seluruh user reguler pada sistem, identifikasi akun dengan password kosong.
2. Nonaktifkan (lock/expire) akun milik siswa yang sudah lulus tanpa menghapus data home directory-nya.
3. Terapkan kebijakan chage (masa berlaku 90 hari, peringatan 14 hari) pada seluruh akun aktif.
4. Konfigurasikan pam_pwquality agar password baru minimal 12 karakter dengan kombinasi huruf besar, angka, dan simbol.
5. Aktifkan pam_faillock (deny=5, unlock_time=600) dan uji dengan 5 kali percobaan login salah.
6. Aktifkan 2FA pada akun admin, lalu uji login SSH menggunakan password + kode OTP.

Pertanyaan reflektif: Mengapa akun yang tidak segera dinonaktifkan setelah penggunanya keluar dari organisasi dianggap risiko keamanan yang sering diabaikan?

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

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

BAB 8 — Keamanan Koneksi Remote (VPN)

Materi Inti (Ringkas)

Aspek	OpenVPN vs WireGuard
Kompleksitas	OpenVPN: PKI penuh (CA, sertifikat) — WireGuard: pasangan kunci publik/privat, lebih sederhana
Performa	WireGuard lebih cepat (desain minimalis di kernel)
Kematangan	OpenVPN lebih matang & fleksibel; WireGuard modern & populer sejak 2020-an

- PKI OpenVPN: CA → sertifikat server → sertifikat client → parameter Diffie-Hellman (easy-rsa).
- IP forwarding + NAT (nftables masquerade) diperlukan agar client VPN bisa mengakses jaringan lokal di balik server.
- tls-auth/pre-shared key: lapisan HMAC tambahan menolak paket tanpa signature valid sebelum TLS handshake.

Setup Praktik

Alasan menggunakan 2 NIC pada server: satu antarmuka mensimulasikan sisi "internet" tempat client VPN terhubung dari luar, dan satu lagi mensimulasikan jaringan lokal kantor yang ingin dilindungi. Pemisahan ini penting supaya peserta didik memahami perbedaan antara "terhubung ke server VPN" dan "bisa mengakses jaringan di baliknya" — dua hal yang sering tertukar oleh pemula.

- Siapkan 2 VM: "vpn-server" (2 NIC — 1 ke "internet"/WAN lab, 1 ke jaringan lokal simulasi) dan "vpn-client" (hanya terhubung ke NIC WAN, tidak punya akses langsung ke jaringan lokal).
- Instal paket: sudo apt install openvpn easy-rsa -y (di server); siapkan juga wireguard sebagai perbandingan bila waktu memungkinkan.
- Buat direktori kerja Easy-RSA (make-cadir ~/easy-rsa) dan pastikan peserta didik memahami tiap tahap PKI sebelum lanjut ke konfigurasi server.
- Siapkan skenario "server internal" (mis. VM ketiga di jaringan lokal) sebagai target ping/test setelah VPN aktif.
- Aktifkan IP forwarding sementara di /etc/sysctl.conf dan siapkan rule nftables masquerade sebagai referensi.

Verifikasi / Uji Coba

VPN yang "terlihat jalan" belum tentu benar-benar berfungsi. Lakukan pengecekan bertahap berikut, dari sisi server dulu baru client, agar mudah menemukan di titik mana masalah terjadi bila koneksi gagal:

Perintah	Yang Diverifikasi
sudo systemctl status openvpn@server	Memastikan service OpenVPN aktif (status: active/running) di sisi server
ip addr show tun0	Memastikan interface tunnel VPN terbentuk di server setelah service dijalankan
sudo journalctl -u openvpn@server -f	Memantau log server secara live saat client mencoba connect — error koneksi akan terlihat di sini

openvpn --config client1.ovpn	Menjalankan koneksi dari sisi client; cari baris "Initialization Sequence Completed" sebagai tanda sukses
ip addr show tun0 (di client)	Memastikan client menerima IP virtual dari range 10.8.0.0/24
ping 10.8.0.1	Menguji client bisa menjangkau server VPN itu sendiri melalui tunnel
ping 192.168.1.1	Menguji client bisa menjangkau jaringan lokal di balik server (baru berhasil setelah IP forwarding+NAT aktif)

Urutan uji yang disarankan: pastikan dulu tunnel terbentuk (tun0 muncul) → baru cek ping ke server (10.8.0.1) → baru cek ping ke jaringan lokal (192.168.1.1). Jika langkah kedua gagal, masalah ada di PKI/sertifikat; jika langkah ketiga gagal, masalah ada di IP forwarding/NAT.

Studi Kasus

Skenario: Sebuah perusahaan kecil memiliki 3 pekerja remote yang perlu mengakses server internal kantor (berisi aplikasi & file share) secara aman dari luar kantor.

11. Bangun PKI lengkap (CA, sertifikat server, sertifikat 2 client) menggunakan Easy-RSA.
12. Konfigurasikan server.conf (port, proto, dev tun, blok IP virtual 10.8.0.0/24, push route ke jaringan lokal kantor).
13. Hasilkan file konfigurasi client (.ovpn) untuk masing-masing pekerja dan uji koneksi dari VM client.
14. Aktifkan IP forwarding dan rule NAT agar client VPN dapat mem-ping server internal di jaringan lokal.
15. Tambahkan tls-auth dengan pre-shared key pada server & client, lalu uji ulang koneksi memastikan tetap berfungsi.
16. Dokumentasikan hasil pengujian: waktu koneksi berhasil, IP virtual yang diterima client, dan hasil ping ke jaringan lokal.

Pertanyaan reflektif: Jika perusahaan ingin menambah 20 pekerja remote lagi, pertimbangan apa yang perlu diperhatikan dalam skalabilitas PKI dan manajemen sertifikat client?

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

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

BAB 9 — Forensik Digital Dasar

Materi Inti (Ringkas)

- Forensik digital: proses investigasi bukti digital setelah insiden terjadi (reaktif) — beda dari prevention/detection yang proaktif.
- Fokus: menelusuri riwayat login, log autentikasi, file/proses mencurigakan, lalu menyusun laporan.
- Chain of custody: dokumentasikan setiap langkah, jangan ubah bukti asli, gunakan checksum (sha256sum), simpan bukti di tempat aman.

Perintah Kunci

Perintah	Fungsi
last / lastb	Riwayat login berhasil / gagal
grep 'Failed password' /var/log/auth.log	Cari percobaan login gagal
find / -mtime -1 -type f	File yang berubah 24 jam terakhir
find / -perm -4000 -type f	Cari file berbit SUID (potensi eskalasi)
ps aux --sort=-%cpu | head	Proses dengan CPU tertinggi (indikasi cryptomining)
ss -tulnp / netstat -tulnp	Port listening & proses pemiliknya
sha256sum <file>	Checksum bukti untuk chain of custody

Setup Praktik

Inti dari setup ini adalah menyembunyikan "jawaban" dari peserta didik terlebih dahulu — guru berperan sebagai "penyerang" yang meninggalkan jejak, dan peserta didik berperan sebagai analis yang harus menemukannya tanpa diberi tahu di mana letaknya. Ini melatih proses investigasi yang sesungguhnya, bukan sekadar mengikuti instruksi.

- Siapkan 1 VM Linux (Debian/Ubuntu) sebagai "korban", bridged/NAT ke jaringan lab.
- Guru menanam skenario sebelum kelas: beberapa percobaan login SSH gagal dari 2–3 IP berbeda (bisa disimulasikan dengan beberapa percobaan ssh salah password dari VM lain).
- Tambahkan 1 file mencurigakan di /tmp (mis. skrip bernama acak) dengan timestamp mtime terbaru.
- Jalankan 1 proses dummy dengan nama tidak lazim yang listening di port tidak umum, sebagai simulasi backdoor.
- Pastikan peserta didik punya akses sudo ke VM korban dan salinan /var/log/auth.log untuk dianalisis.
- Siapkan template laporan singkat (ringkasan, kronologi, bukti, dampak, rekomendasi).

Verifikasi / Uji Coba (untuk Guru, Sebelum Kelas Dimulai)

Sebelum sesi dimulai, guru perlu memastikan skenario yang ditanam benar-benar terekam dan bisa ditemukan — jangan sampai peserta didik kesulitan bukan karena kurang teliti, tapi karena jejaknya tidak benar-benar tersimpan:

Perintah	Yang Diverifikasi
sudo tail -20 /var/log/auth.log	Memastikan percobaan login gagal yang disimulasikan benar-benar tercatat di log
sudo grep -c 'Failed password' /var/log/auth.log	Menghitung jumlah baris gagal login — harus sesuai jumlah percobaan yang disimulasikan
stat /tmp/nama_file_mencurigakan	Memastikan mtime file "jejak" benar-benar dalam 24 jam terakhir
ps aux | grep nama_proses_dummy	Memastikan proses simulasi backdoor benar-benar berjalan dan terlihat di daftar proses
ss -tulnp | grep <port_dummy>	Memastikan port dummy benar-benar dalam status listening sebelum kelas dimulai

Studi Kasus

Skenario: Tim IT mendapat laporan server internal "web-01" melambat sejak semalam. Sebagai analis, Anda diminta menginvestigasi kemungkinan penyusupan.

21. Periksa riwayat login (last, lastb) — identifikasi apakah ada login berhasil dari IP yang tidak dikenal.
22. Analisis /var/log/auth.log — hitung dan urutkan IP dengan percobaan gagal terbanyak.
23. Cari file yang dimodifikasi dalam 24 jam terakhir di seluruh sistem.
24. Periksa proses berjalan dan port listening — temukan proses/port yang tidak wajar.
25. Susun laporan forensik singkat (maks. 1 halaman): ringkasan, kronologi, bukti, dampak, dan rekomendasi remediasi.

Pertanyaan reflektif: Berdasarkan bukti yang ditemukan, langkah mitigasi segera apa yang perlu diambil, dan bagaimana mencegah insiden serupa terulang?

Studi Kasus Lanjutan (Variasi)

Skenario: Setelah insiden pertama teratasi, 1 minggu kemudian ditemukan file cron job asing di /etc/cron.d/ yang menjalankan skrip tidak dikenal setiap 5 menit.

- Identifikasi isi skrip tersebut menggunakan cat/strings, dan tentukan sha256sum-nya sebagai bukti sebelum dihapus.
- Telusuri kembali /var/log/auth.log pada rentang waktu file cron tersebut dibuat — cari korelasi dengan sesi login mencurigakan.
- Perbarui laporan forensik dengan bagian baru: "Temuan Lanjutan" beserta kronologi tambahan.

Rangkuman

Forensik digital dasar meliputi penelusuran riwayat login menggunakan last/lastb, analisis log autentikasi untuk mendeteksi anomali, identifikasi perubahan file dan proses mencurigakan menggunakan perintah find dan ps, hingga penyusunan laporan hasil analisis yang sistematis. Kompetensi ini menjadi bekal penting bagi analis keamanan dalam merespons insiden, sekaligus menjadi dasar bagi materi Capture The Flag pada bab berikutnya.

Soal Latihan / Refleksi

26. Jelaskan perbedaan antara pendekatan pencegahan (prevention), deteksi (detection), dan forensik (forensics) dalam keamanan siber.

27. Tuliskan perintah untuk menampilkan seluruh percobaan login SSH yang gagal pada file /var/log/auth.log.
28. Jelaskan bagaimana perintah find dapat digunakan untuk menemukan file yang baru dimodifikasi dalam 24 jam terakhir.
29. Sebutkan empat bagian utama yang sebaiknya terdapat dalam sebuah laporan hasil analisis forensik.

BAB 10 — Capture The Flag (Dasar Analisis Keamanan)

Materi Inti (Ringkas)

CTF melatih pola pikir problem-solving & attacker mindset lewat 5 kategori tantangan mencari 'flag' (format umum FLAG{...}).

Kategori	Tools Utama
Steganografi	file, strings, exiftool, steghide, binwalk
Kriptografi	base64 -d, xxd -r -p, CyberChef, analisis frekuensi huruf
Forensik Jaringan	Wireshark, tshark, Follow TCP Stream
Eksploitasi Web Dasar	View Source, DevTools (F12), curl robots.txt
Eksploitasi Biner Dasar	file, strings, strace/ltrace

Etika: teknik hanya untuk sistem/lab latihan resmi (mis. PicoCTF, OverTheWire, TryHackMe, HackTheBox) — tidak boleh dipakai menyerang sistem pihak lain tanpa izin.

Setup Praktik

Berbeda dari Bab 9 (peserta didik mencari jejak di sistem), pada CTF peserta didik mencari "pesan tersembunyi" di dalam file. Guru perlu menyiapkan file challenge dengan hati-hati agar tingkat kesulitannya sesuai — terlalu mudah membuat bosan, terlalu sulit membuat frustrasi tanpa belajar apa-apa.

- Instal tools di VM lab: sudo apt install steghide binwalk exiftool wireshark tshark xxd -y
- Siapkan folder "challenge" berisi: 1 file gambar dengan pesan steghide/EXIF tersembunyi, 1 string ter-encode berlapis (Base64+Hex), 1 file .pcap kecil berisi HTTP plaintext, 1 halaman HTML statis dengan komentar tersembunyi, 1 binary sederhana dengan string 'flag' tertanam.
- Beri passphrase sederhana untuk file steghide (informasikan atau sembunyikan sebagai clue tambahan).
- Pastikan Wireshark/tshark bisa membuka file .pcap tanpa perlu izin root (chmod file capture agar terbaca).
- Opsional: siapkan akses ke CyberChef (offline build atau gordonlesti.github.io/CyberChef) bila lab tanpa internet.

Verifikasi / Uji Coba (untuk Guru, Sebelum Kelas Dimulai)

Guru wajib mencoba sendiri seluruh challenge sebelum diberikan ke peserta didik, memakai perintah yang sama persis yang nanti dipakai peserta didik, untuk memastikan flag benar-benar bisa ditemukan dan tidak ada file yang rusak/salah proses pembuatan:

Perintah	Yang Diverifikasi
steghide extract -sf gambar.jpg	Memastikan pesan tersembunyi berhasil diekstrak dengan passphrase yang telah ditentukan
echo 'STRING_ENCODE' | base64 -d | xxd -r -p	Menjalankan urutan decode berlapis untuk memastikan hasil akhirnya adalah flag yang valid (format FLAG{...})
tshark -r file.pcap -Y "http"	Memastikan paket HTTP yang berisi flag benar-benar terekam dan bisa difilter

grep -o 'FLAG{.*}' index.html	Memastikan flag tersembunyi di komentar HTML dapat ditemukan dengan pencarian pola sederhana
strings program_biner | grep -i flag	Memastikan string flag benar-benar tertanam dan terbaca di file biner

Jika salah satu perintah di atas tidak menghasilkan flag yang diharapkan, perbaiki file challenge tersebut sebelum kelas dimulai — jangan biarkan peserta didik mencoba memecahkan challenge yang sebenarnya rusak.

Studi Kasus — Mini CTF

Skenario: Kelas dibagi kelompok, setiap kelompok mendapat 5 file challenge (1 per kategori) dan diberi waktu 45 menit untuk menemukan seluruh flag.

30. Steganografi: ekstrak pesan tersembunyi dari file gambar yang diberikan.
31. Kriptografi: decode string ter-encode berlapis menjadi flag asli.
32. Forensik Jaringan: temukan flag dalam komunikasi HTTP plaintext pada file .pcap.
33. Web: temukan flag yang disembunyikan dalam komentar HTML/encoding Base64 pada halaman latihan.
34. Biner: jalankan/analisis file biner untuk menemukan string flag.

Kelompok tercepat menyelesaikan seluruh flag dengan bukti langkah kerja (screenshot/perintah) menjadi pemenang simulasi.

Studi Kasus Lanjutan (Variasi — Chained Challenge)

Skenario: 1 flag "final" tersembunyi berlapis — hasil decode Base64 dari sebuah komentar HTML ternyata adalah passphrase untuk file steghide, dan isi file steghide berisi potongan flag yang harus digabung dengan hasil analisis file .pcap.

- Latih peserta didik mengenali pola "chained challenge" yang umum di kompetisi CTF tingkat lanjut/LKS.
- Tekankan pencatatan setiap langkah (tool + output) karena satu langkah yang terlewat menghentikan seluruh rantai penyelesaian.

Rangkuman

Capture The Flag melatih kemampuan problem-solving keamanan siber melalui lima kategori tantangan dasar: steganografi (data tersembunyi dalam file), kriptografi (pemecahan ciphertext), forensik jaringan (analisis file pcap), eksploitasi web dasar (pemeriksaan kode sumber), dan eksploitasi biner dasar (analisis string dan perilaku program). Sebagai materi pengayaan, bab ini memperkuat pola pikir analitis yang melengkapi seluruh kompetensi hardening yang telah dipelajari pada bab-bab sebelumnya.

Soal Latihan / Refleksi

35. Jelaskan perbedaan mendasar antara steganografi dan kriptografi.
36. Tuliskan perintah untuk mendekode string Base64 'S2VhbWFuYW4=' menjadi teks aslinya menggunakan command line.
37. Jelaskan bagaimana fitur 'Follow TCP Stream' pada Wireshark dapat membantu menemukan flag pada tantangan forensik jaringan.

38. Sebutkan dua teknik dasar yang dapat digunakan untuk menemukan flag tersembunyi pada tantangan web tanpa memerlukan eksploitasi lanjutan.

BAB 11 — Rangkuman dan Evaluasi Akhir

Materi Inti (Ringkas)

Sembilan elemen membentuk pertahanan berlapis (defense in depth): akses & firewall (lapisan pertama) → deteksi intrusi → kriptografi, database, akun pengguna → VPN → forensik digital (respons insiden) → CTF (penguatan pola pikir, pengayaan).

Checklist Hardening Komprehensif (versi cepat)

- Root SSH login nonaktif; user admin + sudo dibuat; port SSH diganti.
- Firewall default-deny aktif; hanya port esensial dibuka.
- Fail2ban + auditd aktif memantau login gagal & perubahan file.
- MySQL secure-installation dijalankan; akses root dibatasi localhost.
- Kebijakan password (chage, PAM pwquality) & faillock aktif.
- VPN (OpenVPN/WireGuard) terkonfigurasi dan teruji dari client.
- Kemampuan investigasi log (last, lastb, auth.log) dikuasai.

Setup Praktik — Simulasi Ujian Akhir

Bab ini mensimulasikan kondisi ujian sesungguhnya: server benar-benar "kosong" tanpa hardening apapun, dan peserta didik mengerjakan semuanya dari awal sampai akhir dalam satu sesi panjang — persis seperti format Tes Praktik Hardening pada kompetisi LKS. Tujuannya bukan mempelajari hal baru, melainkan melatih kecepatan dan ketepatan menerapkan seluruh kompetensi Bab 2–10 secara berurutan dan mandiri.

- Siapkan 1 VM Linux "bersih" (fresh install, belum di-hardening) sebagai server ujian.
- Beri peserta didik akses awal sebagai root/user default, mirip kondisi server baru.
- Sediakan lembar soal yang mencakup seluruh elemen: hardening akses, firewall, IDS/IPS, GPG, database, akun pengguna, VPN, forensik, dan 1 tantangan CTF ringan.
- Batasi waktu pengerjaan (mis. 3–4 jam) untuk mensimulasikan kondisi Tes Praktik Hardening LKS.
- Siapkan skrip verifikasi otomatis sederhana (opsional) untuk mengecek beberapa poin checklist di akhir sesi.

Verifikasi / Uji Coba — Checklist Akhir Sesi

Setelah waktu pengerjaan selesai, gunakan rangkaian perintah berikut untuk menilai secara objektif apakah tiap poin checklist benar-benar diterapkan, bukan hanya mengecek dari pengakuan peserta didik:

Perintah	Yang Diverifikasi
sudo grep PermitRootLogin /etc/ssh/sshd_config	Memastikan login root SSH sudah dinonaktifkan (harus bernilai 'no')
sudo nft list ruleset	Memastikan firewall default-deny aktif dan hanya port esensial yang diizinkan
sudo systemctl status fail2ban	Memastikan fail2ban aktif dan berjalan (status: active/running)
sudo systemctl status auditd	Memastikan auditd aktif memantau perubahan sistem

sudo mysql -u root -e "SELECT user,host FROM mysql.user;"	Memastikan akun anonymous MySQL sudah dihapus dan akses root dibatasi localhost
sudo chage -l nama_user	Memastikan kebijakan masa berlaku password sudah diterapkan
sudo systemctl status openvpn@server	Memastikan VPN server aktif dan siap menerima koneksi client
last -a | head	Memastikan peserta didik mampu menampilkan riwayat login sebagai bagian investigasi forensik

Skrip ini bisa digabung menjadi satu file bash sederhana yang dijalankan sekali di akhir sesi, sehingga guru mendapat ringkasan cepat status seluruh poin sebelum memberi nilai.

Studi Kasus — Simulasi Tes Praktik LKS

Skenario: Anda ditugaskan meng-hardening server produksi baru dalam waktu terbatas, sekaligus menyiapkan akses remote yang aman dan mendokumentasikan seluruh pekerjaan.

39. Lakukan hardening akses dasar (nonaktifkan root login, ganti port SSH, buat user admin).
40. Terapkan firewall default-deny dan buka hanya port yang diperlukan.
41. Aktifkan fail2ban dan auditd untuk deteksi & pencegahan intrusi.
42. Amankan database (jika ada) dan terapkan kebijakan password/akun pengguna.
43. Konfigurasikan VPN agar 1 client dapat mengakses server secara aman.
44. Simulasikan insiden kecil (mis. beberapa percobaan login gagal) lalu lakukan investigasi forensik singkat.
45. Susun dokumentasi akhir: checklist yang telah diselesaikan + laporan singkat temuan forensik.

Kriteria penilaian: kelengkapan checklist, ketepatan konfigurasi, serta kualitas dokumentasi/laporan yang disusun.

Studi Kasus Lanjutan (Variasi — Skenario Insiden Pasca-Hardening)

Skenario: 2 hari setelah server berhasil di-hardening dan dinyatakan lulus penilaian, muncul alert dari fail2ban menunjukkan lonjakan percobaan login gagal dari satu IP tunggal dalam waktu singkat.

- Verifikasi apakah fail2ban sudah otomatis memblokir IP tersebut; periksa status jail dengan fail2ban-client status sshd.
- Telusuri auth.log untuk memastikan tidak ada login yang berhasil di antara percobaan-percobaan gagal tersebut.
- Susun ringkasan evaluasi: apakah lapisan hardening yang telah diterapkan (Bab 2–8) efektif menahan percobaan serangan ini, dan lapisan mana yang paling berperan.

Soal Latihan / Refleksi

46. Sebuah server Linux baru perlu di-hardening sebelum digunakan sebagai server produksi. Susun urutan langkah hardening yang sebaiknya dilakukan, mulai dari akses dasar hingga firewall, beserta alasan urutan tersebut.
47. Jelaskan bagaimana fail2ban, auditd, dan Snort saling melengkapi dalam strategi deteksi dan pencegahan intrusi.
48. Sebuah organisasi ingin mengizinkan tiga pekerja remote mengakses server internal secara aman. Rancang solusi menggunakan VPN, mencakup jenis VPN yang dipilih beserta alasannya, dan langkah konfigurasi utama yang diperlukan.

49. Setelah sebuah insiden keamanan terdeteksi, jelaskan langkah-langkah forensik digital dasar yang sebaiknya dilakukan untuk mengidentifikasi sumber dan dampak insiden tersebut.
50. Jelaskan bagaimana latihan Capture The Flag dapat memperkuat kompetensi hardening yang telah dipelajari pada elemen-elemen sebelumnya, meskipun sifatnya pengayaan.