PERTEMUAN 12 · SUB-CPMK 3.4

Keamanan Sistem & Hardening Server

CIA Triad, defense in depth, firewall, SSH hardening & kebijakan sandi

Administrasi Sistem (CEN3303) · D3 Teknik Komputer · Politeknik Negeri Padang
Ir. H. A. Mooduto, M.Kom. · Semester Ganjil 2026/2027

Target hari ini

Sub-CPMK 3.4

Mahasiswa mampu menerapkan keamanan sistem dasar dan hardening server (firewall lokal, SSH hardening, kebijakan password).

- Memahami CIA Triad & defense in depth
- Mengonfigurasi firewall (UFW/iptables)
- Menerapkan hardening SSH & sandi

Alur pertemuan

1	Prinsip keamanan	20'
2	Firewall	25'
3	Hardening SSH & sandi	35'
4	Audit & studi kasus	20'
5	Praktikum lab	170'

Server diretas bukan karena hacker jenius

Sebagian besar insiden berawal dari konfigurasi dasar yang lemah — bukan eksploitasi zero-day yang canggih.

Sandi lemah

admin/admin, 123456, atau sandi bawaan yang tidak pernah diganti

Port terbuka

Layanan yang tidak dipakai tetap mendengarkan di internet

Patch tertunda

Celah sudah diumumkan dan diperbaiki, tapi tidak dipasang (Bab 6)

Bot otomatis memindai seluruh alamat IP internet tanpa henti. Server baru yang terhubung ke internet biasanya mulai menerima percobaan login SSH dalam hitungan menit.

CIA Triad: tiga tujuan keamanan

C



Confidentiality

Kerahasiaan

Hanya pihak berwenang yang bisa membaca data

Kontrol yang sudah kita pelajari:

Permission & ACL · SFTP/HTTPS · SSH key

I



Integrity

Integritas

Data tidak diubah secara tidak sah

Kontrol yang sudah kita pelajari:

Permission tulis · TLS · log audit · checksum paket

A



Availability

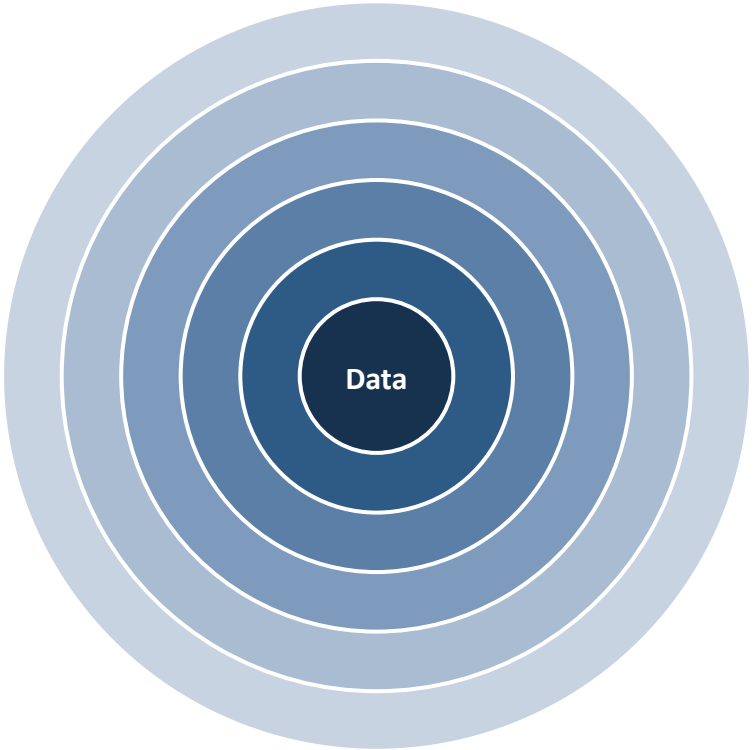
Ketersediaan

Layanan tetap bisa diakses saat dibutuhkan

Kontrol yang sudah kita pelajari:

Backup (Bab 12) · monitoring · fail2ban · patching

Defense in depth: pertahanan berlapis



Kebijakan & fisik
Ruang server terkunci, kebijakan sandi, pelatihan staf

Perimeter
Firewall jaringan, VPN untuk akses jarak jauh

Jaringan
Pemisahan VLAN, DHCP snooping (Pertemuan 9)

Host / server
UFW, SSH hardening, patching, fail2ban

Aplikasi
HTTPS, SFTP, akun layanan least privilege

Data
Permission, enkripsi, backup terpisah (Bab 12)

01

Firewall: penjaga gerbang server

Tolak semua yang masuk, lalu buka hanya pintu yang benar-benar dibutuhkan

Merancang aturan firewall dari layanan kita

Kebijakan default

Masuk: deny
Keluar: allow

Lalu tambahkan pengecualian hanya untuk layanan yang memang dijalankan server.

Layanan	Port	Dari	Pert.
SSH (admin)	`22/tcp`	Subnet lab saja	12
DNS	`53/tcp, 53/udp`	LAN	7
DHCP	`67/udp`	LAN	9
Web HTTP/HTTPS	`80, 443/tcp`	Semua	10
Samba	`445/tcp`	LAN	11
NFS	`2049/tcp`	Server tertentu	11
Telnet, FTP	`23, 21`	**Tutup**	—

Menerapkan dengan UFW

```
sudo ufw default deny incoming
sudo ufw default allow outgoing

# SSH hanya dari subnet lab — WAJIB sebelum enable!
sudo ufw allow from 192.168.10.0/24 to any port 22 proto tcp

sudo ufw allow 80,443/tcp
sudo ufw allow from 192.168.10.0/24 to any port 445 proto tcp
sudo ufw allow from 192.168.10.0/24 to any port 53
sudo ufw allow 67/udp

sudo ufw enable
sudo ufw status numbered
sudo ufw delete 3        # hapus aturan nomor 3
```



Jangan terkunci!

Izinkan SSH sebelum ufw enable, dan uji login dari sesi kedua sebelum menutup sesi pertama.

Di bawahnya: iptables/nftables

```
iptables -A INPUT \
  -p tcp --dport 22 \
  -s 192.168.10.0/24 \
  -j ACCEPT
```

UFW menulis aturan ini untuk kita.

02

Hardening: menutup celah akses

SSH, kebijakan sandi, pemblokiran otomatis, dan mengurangi permukaan serangan

SSH hardening: pintu utama administrasi

Urutan aman

1. **Buat kunci di laptop admin**

```
ssh-keygen -t ed25519
```

2. **Salin kunci publik ke server**

```
ssh-copy-id admin@192.168.10.30
```

3. **Uji login dengan kunci**

```
ssh admin@192.168.10.30
```

4. **Baru matikan login sandi & root**

```
sudo sshd -t && sudo systemctl reload ssh
```

```
# /etc/ssh/sshd_config
PermitRootLogin no
PasswordAuthentication no
PubkeyAuthentication yes
MaxAuthTries 3
LoginGraceTime 30
AllowUsers admin
Port 2222          # opsional
```

Ganti port = lapisan tambahan, bukan keamanan utama. Mengurangi kebisingan bot, tetapi tetap bisa ditemukan pemindai.

Kebijakan sandi yang benar-benar ditegakkan

Kualitas sandi

```
sudo apt install \
  libpam-pwquality
# /etc/security/pwquality.conf
minlen = 12
minclass = 3
dictcheck = 1
```

Batas percobaan gagal

```
# /etc/security/faillock.conf
deny = 5
unlock_time = 900

sudo faillock --user andi
```

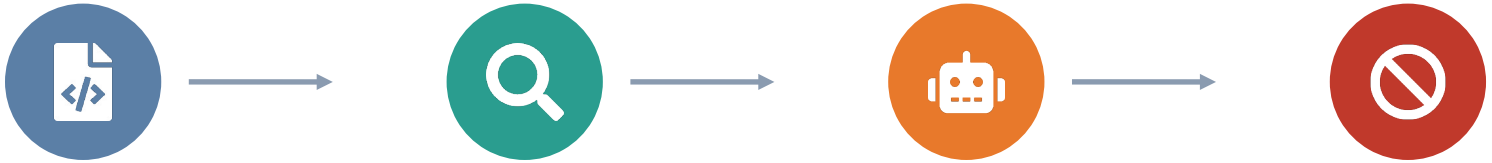
Masa berlaku akun

```
sudo chage -M 180 -W 14 andi
sudo chage -l andi

# kunci akun yang tidak aktif
sudo usermod -L mantan_staf
```

Panjang lebih penting daripada kerumitan. Frasa sandi 15+ karakter lebih kuat dan lebih mudah diingat daripada P@ssw0rd! — dan untuk akses admin, kunci SSH tetap lebih baik dari sandi apa pun.

fail2ban: memblokir penyerang secara otomatis



Baca log
auth.log / journal

Cocokkan pola
“Failed password”

Hitung
5× dalam 10 menit

Blokir IP
aturan firewall 1 jam

```
sudo apt install fail2ban

# /etc/fail2ban/jail.local
[sshd]
enabled  = true
maxretry = 5
findtime = 10m
bantime  = 1h
ignoreip = 127.0.0.1/8 192.168.10.0/24
```

```
sudo systemctl enable --now fail2ban
sudo fail2ban-client status sshd
sudo fail2ban-client set sshd \
  unbanip 203.0.113.7
```

Kurangi permukaan serangan

Apa yang mendengarkan?

```
sudo ss -tulnp
```

Setiap port terbuka harus punya alasan

Layanan yang aktif saat boot?

```
systemctl list-unit-files \
  --state=enabled
```

Matikan yang tidak dipakai:
systemctl disable --now <svc>

Patch keamanan otomatis

```
sudo apt install \
  unattended-upgrades
```

Pembaruan keamanan terpasang tanpa menunggu admin (Bab 6)

Admin pakai sudo, bukan root

```
sudo usermod -aG sudo admin
```

Setiap tindakan tercatat atas nama pengguna

Checklist hardening server produksi

Area	Langkah hardening	Cara verifikasi
Akses SSH	Root login off, key-based auth	`sshd -T | grep -i permitroot`
Firewall	Default deny, buka port seperlunya	`ufw status verbose`
Pembaruan	Patching rutin & otomatis	`apt list --upgradable`
Sandi	Panjang minimum & batas gagal	`chage -l <user>`
Layanan	Nonaktifkan yang tidak perlu	`ss -tulnp`
Brute force	fail2ban untuk SSH	`fail2ban-client status`
Log & audit	Catat akses, tinjau berkala	`lastb · journalctl`

Audit: memeriksa sebelum diserang

Siapa yang login?

```
last -n 10
sudo lastb -n 10      # login gagal
```

Jejak percobaan SSH

```
sudo grep "Failed password" \
  /var/log/auth.log | tail
```

Pantau berkas penting

```
sudo apt install auditd
sudo auditctl -w /etc/passwd \
  -p wa -k akun
sudo ausearch -k akun
```

Pemindaian otomatis

```
sudo apt install lynis
sudo lynis audit system
```

Studi kasus: brute force pada SSH

```
$ sudo grep "Failed password" /var/log/auth.log | tail -4
Oct 6 02:14:07 sshd: Failed password for root from 203.0.113.7
Oct 6 02:14:09 sshd: Failed password for root from 203.0.113.7
Oct 6 02:14:11 sshd: Failed password for admin from 198.51.100.4
Oct 6 02:14:12 sshd: Failed password for root from 203.0.113.7
$ sudo grep -c "Failed password" /var/log/auth.log
4817
```

Akar masalah: port 22 default + login root diizinkan + autentikasi sandi



Root login off



Key-based auth



fail2ban aktif



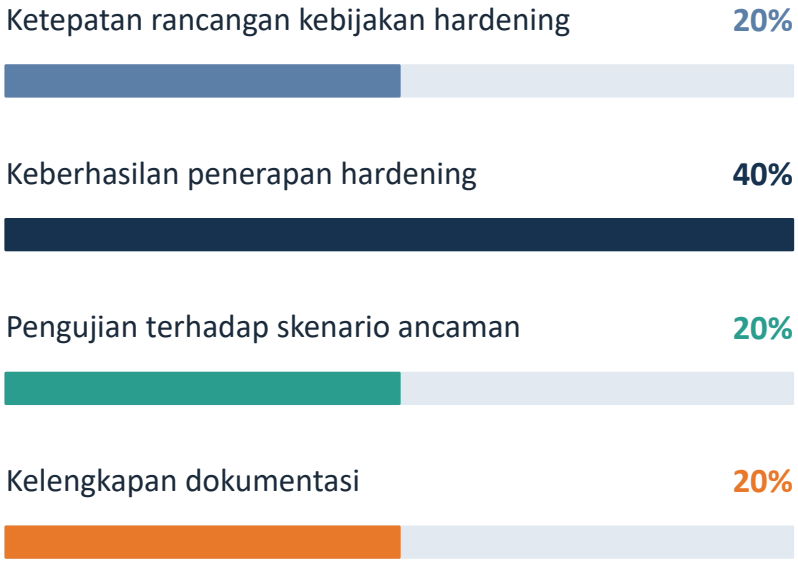
SSH hanya dari IP kantor/VPN

Praktikum & penilaian (170 menit)

Tugas lab

1. Snapshot VM, lalu jalankan lynis (skor awal)
1. Terapkan UFW sesuai tabel aturan layanan
1. Hardening SSH: key-based, root & sandi off
1. Kebijakan sandi (pwquality, faillock) + fail2ban
1. Uji: login root ditolak, IP terblokir, port tertutup; lynis ulang

Rubrik Pertemuan 12 · bobot 2,5% nilai akhir



Cek pemahaman

1	**Prinsip agar data tidak diubah secara tidak sah?**	Integrity
2	**Antarmuka sederhana di atas iptables/nftables?**	UFW
3	**Cegah akses langsung sebagai superuser lewat SSH?**	Nonaktifkan login root langsung (PermitRootLogin no)
4	**Contoh defense in depth pada server?**	Firewall + SSH key + fail2ban + patching + backup
5	**Checklist server web publik sebelum produksi?**	Tabel checklist + HTTPS + hanya port 80/443/SSH terbatas

Rangkuman

Prinsip

CIA Triad sebagai tujuan; defense in depth sebagai strategi berlapis.

Firewall

Default deny, buka port seperlunya, batasi alamat asal.

Hardening

SSH key, root off, kebijakan sandi, fail2ban, audit berkala.

Pertemuan 13

Backup, Restore & Disaster Recovery Dasar. Baca Bab 12 Buku Ajar sebelum kelas.

Referensi: Buku Ajar Bab 11 · Nemeth et al. (2021) · CIS Benchmarks · Frisch (2002)