

Ringkasan materi Ancaman jaringan, hardening router, IDS, keamanan Wi-Fi

Kelas XI–XII TKJ · Disusun oleh Bayu Setiawan

Modul keamanan jaringan untuk siswa TKJ yang dirancang dari KD AIJ dan ASJ: jenis ancaman seperti DDoS, brute force, port scanning, dan sniffing; teknik hardening router MikroTik dan server Linux; firewall berlapis; keamanan Wi-Fi; hingga monitoring log dan deteksi intrusi. Semua praktik dilakukan di lab virtual milik sendiri.

Bab 1. Mengenal Ancaman Jaringan

Memahami jenis ancaman adalah langkah pertama melindungi jaringan. Sebagian besar insiden berawal dari kata sandi lemah dan layanan yang dibiarkan terbuka tanpa perlindungan.

- Malware dan ransomware
- DDoS
- Brute force dan password lemah
- Sniffing dan man in the middle

Bab 2. Hardening Router MikroTik

Hardening berarti mengurangi celah. Matikan service seperti telnet dan ftp, buat user baru pengganti admin, batasi akses manajemen hanya dari IP tertentu, dan selalu perbarui RouterOS.

- Menonaktifkan service yang tidak dipakai
- Mengganti user default admin
- Membatasi akses Winbox
- Update RouterOS

```
/ip service disable telnet,ftp,www,api
/ip service set winbox address=192.168.88.0/24
/user add name=adminlab group=full password=*****
/user remove admin
```

Bab 3. Firewall Berlapis dan Proteksi Serangan

Firewall dapat mendeteksi pola serangan, misalnya memasukkan IP yang terlalu sering mencoba login ke address list lalu memblokirnya dalam jangka waktu tertentu.

- Proteksi brute force SSH
- Deteksi port scan
- Drop invalid connection
- Rate limit ICMP

Bab 4. Keamanan Wi-Fi dan Monitoring Log

Jaringan nirkabel sekolah sebaiknya memisahkan SSID guru dan siswa, menerapkan isolasi klien, serta mengirim log ke server terpusat agar kejadian mencurigakan cepat diketahui.

- WPA2/WPA3 dan kata sandi kuat
- Isolasi klien
- Logging ke syslog server

- Membaca log serangan