Attacchi di Rete e Contromisure

Attacchi attivi vs passivi su canale di comunicazione

Tipo	Descrizione	Proprietà CIA violate	Esempi classici
Passivo	Solo ascolto / osservazione	Confidenzialità	Eavesdropping, traffic analysis
Attivo	Modifica, interruzione, iniezione dati	Confidenzialità + Integrità + Disponibilità	DoS/DDoS, ARP poisoning, MITM, packet injection

Esempi concreti e contromisure

DoS / DDoS

- **Proprietà violate**: Disponibilità
- **Tecniche**: SYN flood, UDP flood, applicativo (HTTP flood)
- **Contromisure**: rate limiting, scrubbing center, anycast, CDN, WAF

ARP spoofing / ARP poisoning

- **Ambiente**: LAN Ethernet/Wi-Fi
- **Effetto**: reindirizzamento traffico (prerequisito per MITM)
- **Contromisure**: Dynamic ARP Inspection (switch), ARP statico, VPN end-to-end

Man-in-the-Middle (MITM)

Altri attacchi comuni

- **DNS spoofing** → falsifica risoluzione nome
- **SSL stripping** → downgrade HTTPS → HTTP
- **Session hijacking** → furto cookie/token di sessione
- **Replay attack** → riutilizzo di pacchetti validi

Difese generali (best practice)

- **Cifratura**: TLS, VPN (WireGuard/IPsec), SSH
- **Autenticazione forte**: 2FA/MFA, certificati client
- **Monitoraggio continuo**: IDS/IPS, SIEM, log analysis
- **Patch management**: aggiornare sistemi e librerie
- **Principio del minimo privilegio**: ruoli e permessi
- **Segmentazione di rete**: VLAN, firewall interni
- **Hardening**: disabilitare servizi non necessari, change defaults

Strumenti operativi per test e analisi

Strumento	Uso tipico
Wireshark	Cattura e analisi pacchetti (con SSLKEYLOGFILE per TLS)
tcpdump	Cattura da CLI
OpenSSL	Test connessioni TLS, generazione certificati
mitmproxy	Proxy per MITM, manipolazione traffico HTTPS
nmap	Scansione porte e servizi
netcat	Test connessioni, banner grabbing
BetterCAP / Ettercap	Attacchi MITM su LAN
hping3	Crafting pacchetti custom, DoS test

Esercitazioni pratiche consigliate

1. Cattura traffico HTTP vs HTTPS con Wireshark → confronto
2. Simulare MITM con `bettercap` su rete locale → osservare ARP spoofing
3. Test firma digitale con OpenSSL (`openssl dgst`, `openssl rsautl`)
4. Configurare WireGuard tra due VM → verificare cifratura
5. Usare `sslyze` per scansione certificati/TLS di un server
6. Simulare attacco DoS con `hping3` (solo in laboratorio isolato!)

Riepilogo: sicurezza è difesa in profondità. Comprendere attacchi ↔️ contromisure è essenziale per penetration testing etico.