

# Sicurezza nelle Reti

- Denial of service (disponibilità)
- Intercettazione (confidenzialità)
- Creazione di traffico (integrità)
- Modifica dei dati (integrità)

Principali attacchi:

- Sniffing passivo
- Sniffing attivo (wiretap)
  - Invio falsi messaggi
  - Modifica metadati
  - Replay di messaggi precedenti
  - Reindirizzamento
  - Eliminazione
- Violazioni autenticazioni
  - Intercettazione password
  - DoS authentication system
  - Bruteforce
- Falsificazione identità
  - Pharming (impersonare un altro nodo, fake pages)
    - \* alterazione DNS
    - \* Phishing
    - \* URL simili
  - IP spoofing
    - \* Creazione di traffico ip con un indirizzo sorgente (header) falso)
  - Fake public key identity
    - \* Man in the middle
  - Hijacking sessione
    - \* Man in the middle
  -
- DoS
  - Attacchi fisici o apparati di rete
  - Flooding
    - \* Syn flooding TCP/UDP
    - \* Flooding ping (ICMP)
    - \* Smurf (ping broadcast + IP spoofing)
  - DNS attacks
    - \* traffic rerouting
  - DDos
    - \* Flooding da sistemi distribuiti / malware distribuito

## Prima dell'attacco

- Scansione porte
- Social Engineering
- OS/Applicaiton fingerprint
- Studio debolezza documentazione software

- Studio debolezze note

## **Difesa**

### **Firewall**

todo

### **Proxy**

todo

## **Protocolli di rete con crittografia**

### **SSL**

todo

### **IPsec**

todo

### **VPN**

todo