Fondamenti di Sicurezza Informatica per il Pentesting

Triade CIA e Terminologia di Base

- **Confidenzialità** → solo autorizzati leggono i dati
- **Integrità** → i dati non vengono modificati non autorizzatamente
- **Disponibilità** → i sistemi/dati sono accessibili quando servono

Terminologia chiave:

- **Minaccia** (threat) → evento potenzialmente dannoso
- **Vulnerabilità** → debolezza sfruttabile
- **Attacco** → sfruttamento concreto di una vulnerabilità
- **Contromisura** → misura di protezione

Principi fondamentali della difesa

Rendere **impossibile** all’attaccante:

1. **Sapere** direttamente la chiave/segreto
2. **Indovinare** (brute force, dictionary)
3. **Deducere** (side-channel, pattern, leak di metadati)

Principi correlati:

- Kerckhoffs → algoritmo pubblico, solo chiave segreta
- Perfect Forward Secrecy
- High entropy
- No side-channel leakage
- Traffic masking / padding

Principi per l'identificazione e autenticazione

- **Univocità**
- **Persistenza** nel tempo
- **Verificabilità** (collegamento a entità reale)
- **Non ripudiabilità** (quando serve firma digitale)

Fattori di autenticazione:

- Qualcosa che **si sa** (password, PIN)
- Qualcosa che **si ha** (token, smartcard, phone)
- Qualcosa che **si è** (biometria)

Crittografia per la riservatezza

Cifrario classico – Cesare

- Spostamento fisso k lettere
- Es: k=3 → A→D, B→E, …, Z→C
- “CIA” → “F L D”
- Vulnerabile a frequency analysis

Cifrari moderni – Simmetrica vs Asimmetrica

Simmetrica (stessa chiave)	Asimmetrica (pubblica/privata)
DES → 56 bit – **rotto**	RSA → fattorizzazione (2048-4096 bit)
	Usi: scambio chiavi, firma

Integrità → Funzioni hash

Algoritmo	Lunghezza	Stato attuale (2026)
MD5	128 bit	**rotto** – collisioni facili
SHA-1	160 bit	**rotto**
SHA-256	256 bit	ancora sicuro (SHA-2 family)
SHA-3	variabile	alternativa moderna (Keccak)

Cifratura ibrida (standard de facto)

1. Asimmetrica → autentica + scambia chiave di sessione
2. Simmetrica → cifra il grosso del traffico (molto più veloce)

- Esempi reali: TLS/HTTPS, SSH, OpenPGP, S/MIME

Certificati digitali e CA

- **Certificato digitale** = chiave pubblica + identità + firma CA
- **Certification Authority (CA)** → entità fidata che emette certificati
- **Problema fiducia**: se root CA compromessa → catena fiducia collassa
- **Mitigazioni moderne**: Certificate Transparency, pinning, OCSP Stapling, CRL

Struttura certificato X.509 (campi principali)

- Version, Serial Number, Signature Algorithm, Issuer
- Validity (Not Before / Not After), Subject
- Subject Public Key Info
- Extensions (SAN, KeyUsage, ExtendedKeyUsage, …)
- Signature (dalla CA)

Firma digitale (con chiave pubblica)

1. Hash del documento
2. Cifratura hash con **chiave privata** → firma
3. Verifica: decifra firma con **pubblica** → confronta hash calcolato

Garantisce: **integrità** + **autenticità** + **non ripudio**

HTTPS (in breve)

HTTP + **TLS**

- Autenticazione server (certificato X.509)
- Scambio chiavi (solitamente ECDHE)
- Cifratura simmetrica (AES-GCM)
- Integrità (HMAC o AEAD)

VPN – Panoramica

Crea tunnel cifrato su rete non sicura

- **Tipi**: Remote Access (utente→sede), Site-to-Site (sede↔️sede)
- **Protocolli moderni (2026):** WireGuard (semplice, veloce), OpenVPN, IKEv2/IPSec

IPSec (livello 3 – IP)

- **IKE** → negozia chiavi e SA
- **AH** → solo autenticazione + integrità
- **ESP** → cifratura + integrità + autenticazione
- **Modalità**: Transport (solo payload), Tunnel (intero pacchetto IP)

Note finali: Concetti fondamentali per pentesting e sicurezza reti. Laboratori pratici usano Wireshark, OpenSSL, mitmproxy, tcpdump, SSLKEYLOGFILE.