



Modulo 1 – CyberSecurity - 50 ore

- **Lezione 1: Introduzione alla sicurezza dei sistemi informativi (6 ore)**
 - Concetti e requisiti
 - Intelligenza Artificiale a supporto della Sicurezza Informatica
 - Minacce, attacchi e risorse
 - Principi di progettazione e strategie
 - Standard e normative
- **Lezione 2: Software malevolo (7 ore)**
 - Tipologie di software malevolo
 - Tecniche di propagazione (virus, worm, ingegneria sociale, spam, trojan)
 - Tipologie di payload (corruzione del sistema, distruzione dei dati, DoS, botnet, furto di dati/identità, ecc.)
 - Tecniche di persistenza (backdoor, rootkit, ecc.)
 - Logica e Reverse Engineering di un Ransomware
 - Contromisure
- **Lezione 3: Attacchi di tipo Denial-of-service (DoS) (5 ore)**
 - Introduzione e classificazione
 - Attacchi di flooding
 - Attacchi DoS distribuiti (DDoS)
 - Attacchi a livello applicativo basati sulla larghezza di banda
 - Attacchi reflector e amplifier
 - Difesa e risposta
- **Lezione 4: Approcci crittografici (6 ore)**
 - Riservatezza: crittografia simmetrica
 - Autenticazione dei messaggi e funzioni di hash
 - Crittografia a chiave pubblica
 - Scambio di chiavi
 - Firma digitale
 - Certificati a chiave pubblica
 - Password Cracking and Wireless Security
 - Compromissione del sistema password
 - Social Engineering
 - Wireless Security
- **Lezione 5: Generatori di numeri casuali (6 ore)**
 - Casualità e imprevedibilità
 - Generatori di numeri pseudocasuali (PRNG)
 - Generatori di numeri casuali veri (TRNG)



- PRNG crittografici

- **Lezione 6: Autenticazione (5 ore)**

- Principi e problematiche
- Autenticazione basata su password
- Autenticazione basata su token
- Autenticazione biometrica
- Autenticazione remota dell'utente

- **Lezione 7: Controllo degli accessi (5 ore)**

- Principi e concetti
- Soggetti, oggetti e diritti di accesso
- Controllo degli accessi discrezionale
- Caso di studio: controllo degli accessi in UNIX
- Controllo degli accessi basato sui ruoli (RBAC)
- Controllo degli accessi basato sugli attributi (ABAC)

- **Lezione 8: Sicurezza del software di basso livello (5 ore)**

- Principi e problematiche
- Panoramica del linguaggio di programmazione C
- Undefined behavior e relativi rischi
- Indirizzi, puntatori, array e loro sicurezza
- Allocazione dinamica della memoria e problemi di sicurezza

- **Lezione 9: Vulnerabilità di memory safety (5 ore)**

- Introduzione, layout della memoria, stack frame
- Corruzione dello stack (buffer overflow, stack smashing, format string, errori di conversione)
- Corruzione dell'heap
- Tecniche avanzate (return-oriented programming, heap spraying)
- Mitigazioni (write xor execute, stack canaries, randomizzazione del dello spazio degli indirizzi, autenticazione dei puntatori)

Modulo 2 – Reti - 30 ore

- **Lezione 10: Perimeter Security (5 ore)**

- Intrusion Detection Systems e Intrusion Prevention Systems
- Botnet
- Firewall
- Netfilter e Iptables

- **Lezione 11: RADIUS (5 ore)**

- Generalità
- Sequence diagram basato su PAP, PAP (Proxy), CHAP
- Struttura dei messaggi



- Autenticazione dei pacchetti
- Accounting
- Configurazione

- **Lezione 12:** Kerberos (5 ore)
 - Kerberos per realm distribuiti
 - Configurazione

- **Lezione 13:** IPSEC (5 ore)
 - Modalità di Funzionamento di IpSec
 - IP Security Policy
 - Authentication Header
 - Encapsulating Security Payload

- **Lezione 14:** VPN (5 ore)
 - IPsec e VPN
 - Open VPN
 - Configurazione Server e Client

- **Lezione 15:** Perimeter Security (5 ore)
 - Intrusion Detection
 - Packet Filtering Gateway
 - Proxy Server
 - Transport Gateway