



## Sicurezza Informatica

- Scopo del corso:** Conoscere e comprendere i metodi per difendere i dati aziendali.
- Durata:** 60 ore.
- Metodologia:** Lezioni frontali interattive, confronto tra i partecipanti ed esercitazioni pratiche.
- Requisiti:** Per seguire con profitto il corso è necessario possedere nozioni di base sul funzionamento delle comunicazioni fra computer.
- Sono requisiti preferenziali ma non indispensabili la conoscenza dei principali servizi Internet (server, posta elettronica) e la conoscenza della logica di creazione di una rete Internet.

### Contenuti del corso:

#### Concetti di base:

- Il problema della sicurezza nel settore IT
- Le risorse da proteggere: dati, sistemi, reti
- Ridondanza delle risorse
- Concetti di sicurezza relativi agli utenti
- Concetti di sicurezza relativi ad amministratori e sistemisti
- Gestione dei bug

#### Tecniche di protezione , trasmissione sicura e autenticazione dati

- Autenticità, affidabilità, integrità dei dati
- Riservatezza dei dati
- Tecniche di protezione dei dati
- Cifratura di dati e protocolli
- Autenticità/integrità della comunicazione
- Tecniche di autenticazione: password, smart card, riconoscimento biometrico
- Autenticazione forte
- Regole di sicurezza generale
- Regole per l'hardening dei sistemi operativi
- Policy di sicurezza
- Tecniche per ripristinare il servizio: backup e recovery

#### Analisi , diagnosi e organizzazione di una rete

- Le vulnerabilità dell'IP
- IP Fragmentation
- Utilizzo di ARP
- Affidabilità dei sistemi
- Analisi dei rischi
- Implementazione e monitoraggio
- Hardening dei Servizi
- LAN Virtuali
- La "Zona demilitarizzata" (DMZ)
- Router e firewall
- Application proxy
- Trap zone
- Tecniche di instradamento e vulnerabilità
- Sostituzione dell'identità Internet: IP spoofing

#### Concetti di sicurezza applicata

- Hardening dei servizi (SMTP, POP3, IMAP, HTTP)
- E-mail spam e e-mail spoofing
- Sistemi per la rilevazione di intrusioni: IDS
- ISS
- Analisi dei log
- Strumenti di rilevazione delle vulnerabilità
- Test di vulnerabilità



### **Tecniche di violazione e contromisure**

- Masquerading
- Buffer overflow
- Spoofing (IP spoofing, DNS spoofing, UDP spoofing)
- Sniffing
- ICMP redirection
- Worm, Virus e trojan horse
- Individuazione di tentativi di attacco
- Analisi e contromisure
- Intercettazione dati, man-in-the-middle
- Attacchi DOS e DDOS

### **Installare e configurare componenti HD e SW per la protezione di una rete locale**

- Installazione hardware
- installazione schede NIC
- Installazione periferiche (stampanti, CD-Rom, ecc...), analizzatori di protocollo su reti locali
- monitoraggio del traffico in rete
- gestione reti
- pianificazione delle risorse hardware e software di una rete Ethernet
- creazione, assegnazione e gestione degli account utente e gruppi di lavoro
- criteri di scelta nella formazione di gruppi di lavoro, gruppi locali e gruppi globali
- profilo utente
- impostazione delle protezioni, permessi e dei livelli di condivisione
- gestione di file e dischi rigidi
- visualizzazione degli altri computer e delle risorse
- amministratore di dominio: ruolo e funzione
- gestione della posta elettronica
- soluzioni per l'accesso ad Internet (router, proxy server)
- gestione della sicurezza in rete (Firewall)