

Corso di Formazione

Codice: **KLA-SECUR**Durata: **4 giorni**

Livello: ■■■□

IP Security

LABORATORIO DIDATTICO

■ OBIETTIVI

Il corso fornisce gli elementi per valutare la sicurezza delle reti IP nei confronti di accessi indesiderati e DoS (Denial of Service), analizza le tecniche di Hacking e fornisce le linee guida per aumentare la sicurezza delle applicazioni basate su reti IP attraverso una scelta adeguata di apparati e protocolli di comunicazione. Vengono effettuate diverse sessioni pratiche relative agli argomenti trattati teoricamente.

■ PREREQUISITI

E' richiesta una conoscenza di base delle reti locali e dei protocolli della famiglia TCP/IP...

■ CHI E' ATTESO

Questo corso è rivolto ai tecnici che operano nell'ambito della protezione delle reti e dei sistemi di elaborazione, così come ai progettisti di sistemi di sicurezza informatica.



CONTENUTI

Firewall

- Funzione di un Firewall
- NAT e PAT
- Tipi di Firewall: Packet Filtering, Stateful Inspection, Application Proxy
- Concetto di zone: Trusted, Untrusted e DMZ
- Concetto di policy
- Sessione pratica di configurazione
- Cluster di Firewall
- Virtualizzazione dei Firewall
- High-Availability: Active/Passive, Active/Active, full meshed

Firewall Testing

- RFC 2647: Definizioni
- RFC 3511: Security Benchmarking
- Sessioni pratiche di Test di Firewall
- Generazione attacchi

IDS (Intrusion Detection System)

- Collocazione dei sistemi IDS in rete
- Tipologie di IDS
- Falsi Positivi e Falsi Negativi
- Architetture evolute: bilanciatori di NIDS
- Sessione pratica di utilizzo e test di un IDS
- IPS (Intrusion Prevention System): funzioni e criticità d'impiego
- Operational IDS (HoneyPot)

Tecniche di Autenticazione e Crittografia

- Cifratura dei dati
- Crittografia a chiave simmetrica ed asimmetrica
- Meccanismo di firma elettronica
- Autenticazione, Riservatezza, Integrità e non Ripudio
- Algoritmi di crittografia: DES, 3DES, AES, RSA, ecc.
- Algoritmo Diffie-Hellman
- Integrità dei dati: MD5, SHA, ecc.
- Public-Key Infrastructure (PKI)
- Certificati digitali: ITU-T X.509
- Certification Authority (CA)
- Gestione dei certificati digitali
- CRL: Certificate Revocation List
- LDAP e X.500: cenni
- Servizio HTTPS e protocollo SSL (Secure Socket Layer)
- Transazioni con carta di credito: 3D Secure e MasterCard SPA
- Sessioni pratiche di crittanalisi

AAA (Authentication, Authorization, Accounting)

- PPP (Point to Point Protocol)
- Protocollo PAP
- Protocollo CHAP
- RADIUS (Remote Authentication Dial-in User Service)
- TACACS (Terminal Access Controller Access Control System)

VPN IPsec

- Protocollo IPSEC
- AH ed ESP
- Transport mode e Tunnel mode
- IKE
- Fase 1: Main mode & Aggressive mode
- Fase 2: Quick mode
- ISAKMP
- Sessione pratica di instaurazione di VPN IPsec
- Architetture VPN: Lan-to-Lan, Hub and Spoke, Backup, Client-to-Lan

VPN SSL (Clientless VPN)

- Confronto con VPN IPsec
- Implementazione in rete
- Architettura Single DMZ
- Architettura Dual DMZ

Wireless LAN: IEEE 802.11b (WiFi)

- Analisi delle vulnerabilità su WLAN
- Protocollo WEP
- Riservatezza ed integrità con WiFi
- Autenticazione con WiFi: Open System e Shared Key
- Tipi di attacchi alla WLAN
- WiFi Protected Access (WPA)
- Autenticazione e gestione delle chiavi (IEEE 802.11i e IEEE 802.1x)
- Extensible Authentication Protocol (EAP)
- Architetture evolute di sicurezza nelle WLAN