OSNE-6 - ELEMENTI DI CRITTOGRAFIA PER INTERNET

Categoria: **Networking**

INFORMAZIONI SUL CORSO

Durata:	Categoria:	Qualifica Istruttore:	Dedicato a:	Produttore:
3 Giorni	Networking	Docente Senior (min. 5 anni)	Professionista IT	PCSNET

OBIETTIVI

Fornire competenze sui protocolli crittografici utilizzati per garantire la sicurezza del flusso dati su Internet: crittografia a chiave simmetrica ed asimmetrica, concetto di certificato digitale e certification authority, protocolli di rete come SSH, HTTPS, TLS.

PREREQUISITI

Esperienza sistemistica di base.

CONTENUTI

Crittografia a chiave simmetrica.

Crittografia a chiave asimmetrica: concetto ed uso della chiave pubblica e privata.

Cifratura simmetrica: DES, 3DES, AES, IDEA.

Concetto di hashing: HMAC-MD5, HMAC-SHA.

Autenticazione e non ripudio.

Sessioni sicure in internet: protocolli di cifratura.

Concetto di certificato digitale. Architettura di una certification authority.

Formato x509.

Le transazioni su rete: Attacchi man in the middle e relativa mitigazione.

Protocolli TLS e SSL.

Protocollo HTTPS.

Protocollo SSH.

Architettura di una VPN.

Introduzione ai diversi tipi di VPN (remote access, lan to lan, etc.).

Modalità tunnel e di trasporto. Struttura del pacchetto dati.

Utilizzo della cifratura in una VPN.

Esempio di configurazione di una VPN IPSEC.

INFO

Materiale didattico: Materiale didattico e relativo prezzo da concordare
Costo materiale didattico: NON incluso nel prezzo del corso
Natura del corso: Operativo (previsti lab su PC)