Introduzione alla Cyber e Network Security

Descrizione

Il corso si prefigge di fornire ai partecipanti i concetti, gli strumenti e le metodologie di approccio alle problematiche di sicurezza riguardanti le reti di calcolatori. Partendo dai concetti basilari riguardanti la sicurezza informatica, si analizzeranno in maniera approfondita le caratteristiche dei sistemi di ultima generazione per il rilevamento delle intrusioni.

Durata: 3 giorni

A chi si rivolge

- È indirizzato a tecnici con pregresse conoscenze di networking, fortemente interessati ad investire su se stessi per acquisire nuove competenze, diventare più competitivi nel mondo del lavoro e accelerare il proprio percorso di carriera.

La sicurezza dei sistemi informativi:

Concetti base della sicurezza ICT.
Introduzione alla sicurezza nelle reti di calcolatori.
Valutazione delle minacce e delle vulnerabilità più comuni.

Sicurezza delle reti IP:

Principi di crittografia.
Crittografia a chiave pubblica e privata.
Protocolli di rete per autenticazione, cifratura e controllo di integrità:

- RADIUS (Remote Authentication Dial-In User Service).
- Kerberos.
- IPSec.
- SSL/TLS.

Lo standard X.509.
Public key infrastructure (PKI).
Cenni su VPN.
Protezione da attacchi e rilevamento delle intrusioni.

La sicurezza perimetrale:

Firewall:

- Concetti generali.
- Tecnologia dei firewall.
- Progettazione di un firewall.

Intrusion Detection and Prevention System (IDPS).
Principi di intrusion detection e prevention.
Metodi di intrusion detection:

- Signature-Based Detection.
- Anomaly-Based Detection.
- Stateful Protocol Analysis.

Componenti e architettura.
Funzioni di sicurezza.
Implementazione e amministrazione dell'IDPS.
Tipi di tecniche di IDPS:

- Network-Based IDPS.
- Wireless IDPS.
- Network Behavior Analysis (NBA) System.
- Host-Based IDPS.

Integrazione di molteplici tecniche IDPS.
Scelta dei prodotti IDPS.

Esercitazioni:

Applicazione dei concetti appresi durante le lezioni teoriche.