

Libro di testo: Anelli, Macchi, Angiani, Ziccheri. GATEWAY 3 Sistemi e reti seconda edizione Petrini editore

Web e http e i Servizi Internet

Web e HTTP: Il mondo di Internet, la nascita del Web. Il livello di applicazione, funzionamento di un server web, architettura client-server, esempio di pagina Web dinamica.

Il protocollo http: URI e URL, la richiesta del client, la risposta del server, il passaggio di parametri, i metodi GET e POST.

Il DNS e la gerarchia di dominio, formato dei messaggi DNS e record delle risorse, struttura Interrogazione del DNS. La posta elettronica, caratteristiche e struttura di un messaggio e-mail, MIME, protocolli SMTP, POP3 e IMAP. Protocollo FTP: accesso, funzionamento del protocollo, comandi FTP.

La sicurezza informatica

Introduzione alla sicurezza, chi attacca e perché, come difendersi.

I principi della sicurezza informatica, il triangolo CIA (Confidentiality, Integrity, Availability). Vulnerabilità, minacce e attacchi.

Conoscere le minacce per difendersi, dove colpisce un attacco, classificazione degli attacchi. I malware e i keylogger. Attività di hacking.

Controllo dell'input: Buffer overflow, validità dell'input. SQL Injection, come proteggersi. Strumenti di monitoraggio e attacco.

Progettare la sicurezza. politiche di sicurezza, gli standard di riferimento. Il GDPR: la privacy e la protezione dei dati personali.

La Crittografia

La crittografia, obiettivi della crittografia. Un po' di storia: da Giulio Cesare a Enigma. Crittografia simmetrica a chiave segreta. Crittografia asimmetrica a chiave pubblica. L'algoritmo RSA.

Autenticazione e affidabilità, controllo degli accessi, autenticazione degli utenti. La firma digitale, i certificati digitali e le autorità di certificazione.

VPN e protocolli sicuri

Cos'è e perché utilizzare una VPN, tipi di VPN (trusted e secure VPN), I servizi di sicurezza nelle VPN.

Protocolli sicuri, IPSec, TLS/SSL, HTTPS. PGP: posta elettronica sicura.

Sicurezza perimetrale e applicazioni per la sicurezza

Sicurezza perimetrale. Le ACL: che cos'è una ACL e come funziona. Che cos'è un firewall. Gateway a livello applicazione e server proxy. Demilitarized Zone (DMZ), Port-forwarding. La sicurezza nelle reti Wi-Fi, consigli per la sicurezza Wi-Fi. Troubleshooting per la sicurezza.

Il Cloud Computing e l'IoT

Dal data center fisico a quello virtuale – Che cos'è un data center: come è fatto un data center, l'evoluzione dei data center, incidenti e interruzioni delle attività. L'astrazione logica dell'hardware: perché virtualizzare.

Il Cloud Computing – I modelli del Cloud Computing. Il modello dei servizi: SaaS, PaaS, IaaS. I modelli di distribuzione.

L'Internet of Things – cos'è l'Internet delle cose. Le tecnologie abilitanti e la raccolta dei dati. Gateway, edge e fog computing. L'accesso alla rete. L'analisi dei dati. I problemi di sicurezza

Lavori svolti in laboratorio

Progetto, configurazione e simulazione del funzionamento di reti LAN.

Implementazione della tecnica del NAT (Network Address Translation).

Simulazione del funzionamento di una rete protetta da Access Control List e DMZ.

Simulazione di configurazione di una rete Wan con accesso a Internet tramite modem, Cloud e Datacenter.