

DISCIPLINA Sistemi e Reti

DOCENTE/I **PROF.** Stefania Concas-Piermario CarboniTESTO **SISTEMI E RETI** (LO RUSSO- BIANCHI) – EDITORE HOEPLI

Appunti dei docenti (vedi Classroom)

RECUPERO PROGRAMMA DI QUARTA: IL LIVELLO DI TRASPORTO

Ripasso sul routing. Multiplexing e demultiplexing, il protocollo UDP e il protocollo TCP.

IL LIVELLO DI APPLICAZIONE

Le applicazioni di rete. Architetture per applicazioni di rete. Servizi offerti dallo strato di trasporto alle applicazioni. Il WWW. I protocolli http e HTTPS. Il protocollo FTP. Il servizio email: SMTP, POP3 E IMAP. DNS. Telnet

VLAN: VIRTUAL LOCAL NETWORK

Virtual LAN e standard IEEE 802.1Q. Realizzazione di una VLAN: port based e tagged. Il protocollo VTP e l'interVLAN Routing.

TECNICHE CRITTOGRAFICHE PER LA PROTEZIONE DEI DATI

La sicurezza nelle reti. La crittografia. La crittoanalisi. Cifrari e chiavi. La crittografia simmetrica. Il cifrario DES. 3-DES. IDEA e AES. Limiti degli algoritmi simmetrici. La crittografia asimmetrica. L'algoritmo RSA: modalità confidenziale e autenticazione. La crittografia ibrida. Certificati e firma digitale. Funzioni di hash: MD5, SHA. Certificati digitali

LA SICUREZZA DELLE RETI

La sicurezza dei sistemi informativi ed informatici e analisi dei rischi. Principali tipologie di minacce. Firewall e loro classificazione: personal firewall e Network firewall (packet-filtering, circuit gateway e proxy server). Application proxy e bastion host. DMZ.

VPN

Generalità. Remote Access VPN e Site-to-Site VPN. Implementazione mediante la suite IPsec. Security association, modalità trasporto e modalità tunnel.

Progettazione di una rete

Il cablaggio strutturato degli edifici secondo lo standard ISO/IEC 11801

RETI WIRELESS E RETI MOBILI

La comunicazione senza fili: classificazione su scala dimensionale. Lo standard IEEE 802.11. La sicurezza nelle reti wireless. La crittografia: WEP, WPA e WPA2. Standard IEEE 802.1X e server radius. Lo scanning di una rete. Architettura di una rete wireless (BSS ed ESS). Ruolo dell'Access Point e modalità di funzionamento.

Analisi di prove d'esame

Un numero considerevole di ore è stato dedicato all'analisi e/o svolgimento di prove d'esame in preparazione alla seconda prova. In tale occasione sono stati approfonditi concetti non esplicitamente affrontati nei vari moduli e anche analizzati nelle altre materie di indirizzo: interfacciamento di sistemi tramite web application, collocazione dei server (hosting, housing e soluzione interna), acquisizione di dati di vario tipo (codice a barre, qr code). Cenni di acquisizione di dati tramite sensori e gestione tramite applicazioni.

Attività di Laboratorio

Tutti i moduli sono stati accompagnati da lezioni pratiche di supporto ai contenuti teorici precedentemente illustrati. Lo strumento utilizzato in laboratorio, conformemente alla programmazione iniziale è Cisco Packet Tracer. Le esercitazioni svolte riguardano in particolare: Utilizzo e configurazione dei protocolli a livello di applicazione (dhcp, ftp, http, pop3 e imap). VLAN (configurazione base, Vlan Routing e protocollo VTP). VPN:

implementazione di Remote Access VPN. ACL standard ed estese per definizione di firewall packet filter e per la realizzazione di DMZ.

Educazione Civica

La firma digitale e la sicurezza in rete. La posta elettronica certificata

Serramanna, 1 Giugno 2024

Gli studenti

I DOCENTI

Prof.ssa Stefania Concas

Prof. Piermario Carboni