

**ISTITUTO INDUSTRIALE STATALE
"MICHELANGELO BUONARROTI"**

Guspini- CA

Anno Scolastico 2015-2016

Programma Finale : Sistemi e Reti e Laboratorio

Classe 5BI- Ind.: Inf. e Telec.

I Docenti: Viviana Manca e Serge Fonnesu

Modulo ripasso

Servizi offerti e funzioni dal L. Trasporto. Il protocollo TCP e UDP.

Livello di trasporto e Livello di applicazione

Il servizio di trasferimento affidabile. Problematiche di connessione. Problematiche di congestione: finestra di congestione, algoritmo low start e congestion avoidance. Funzioni e protocolli principali del L. Applicativo: DNS, HTTP, FTP, POP3, SMTP e Telnet.

La configurazione dei sistemi in rete

Il protocollo DHCP: configurazione automatica e dinamica. Gli stati del DHCP Client. Rinnovo del lease dell'indirizzo IP. Configurazione di un computer Windows in LAN.

Laboratorio: assegnazione automatica dell'indirizzo IP, assegnazione manuale, assegnazione dinamica mediante il DHCP, configurazione dei servizi di un server con l'emulatore CiscoPacket Tracer.

Tecniche crittografiche per la protezione dei dati

La sicurezza nelle reti. Crittografia. Crittoanalisi. Storia della crittografia fino alla seconda guerra mondiale.

Crittografia moderna

Crittografia a chiave simmetrica (o privata): a sostituzione e a trasposizione. Cenni sugli algoritmi: DES, 3-DES, AES. Crittografia a chiave asimmetrica (o pubblica). Algoritmo RSA con fattorizzazione. Chiave di sessione. Sintesi (o digest) di messaggi: funzione di hash. Algoritmi MD5 e SHA1 e 2. Autenticazione di un utente: password, autenticazione asimmetrica. Segretezza del messaggio. Firma digitale. Certificati digitali. Identità e distribuzione delle chiavi.

Principali tipologie di minacce informatiche modalità di prevenzione.

Sicurezza delle mail. Il protocollo S/MIME. Caratteristiche principali del software PGP. Sicurezza nelle connessioni a livello di sessione: protocollo SSL/TLS. Il protocollo SET per le transazioni finanziarie.

La difesa perimetrale con i firewall

Firewall: personal, network. Regole ACL. Packet Filter. Firewall di tipo Stateful Inspection. Proxy Application. DMZ e le tre possibili architetture. Sicurezza con il servizio NAT source e destination.

Laboratorio: esercizi di configurazione delle regole ACL e del servizio sNAT e dNAT con Packet Tracer

VPN

VLAN ripasso. VPN Remote-access e VPN site-to-site. Modalità di realizzazione: tunnel e transport. Il protocollo IPSEC: AH, ESP, IKE. Il protocollo HTTPS.

Laboratorio: Configurazione di VPN Server e Client con computer Windows.

Wireless e reti mobili (cenni)

Comunicazione wireless e standard di riferimento 802.11. Reti PAN E WLAN. Protocolli di crittografia: WEP E WPA.

Laboratorio: Connessione wireless con Packet Tracer e configurazione di un router wireless.

Modello Client/Server e distribuito per i servizi di rete

Le applicazioni e i sistemi distribuiti. Architetture dei sistemi Web. Amministrazione di una rete.

Servizio DHCP, DNS, autenticazione degli utenti tramite workgroup e a dominio.

Guspini, 10/06/2016

Docenti

Alunni
