**I.I.S.S.** ***"Luigi dell'Erba"*** **Castellana Grotte**

PROGRAMMA

**MATERIA: SISTEMI ERETI (ore settimanali: 4).**

**Classe: V Di**
**Anno scolastico: 2019/2020**

**Indirizzo: INFORMATICA E TELECOMUNICAZIONI – Articolazione: Informatica**
**Docenti: Prof.ssa MELIOTA CARMELA**
**Prof. DANIELE AMENDOLARE**

**Libro di testo: SISTEMI e RETI Vol. 2 e 3 – autore: Luigi Lo Russo, Elena Bianchi–Ed:Hoepli**

## Argomenti svolti fino al 4 marzo 2020 (DIDATTICA IN PRESENZA)

- ## Lo strato di Trasporto

Servizi e funzioni dello strato di trasporto
I protocolli del livello di trasporto di Internet: UDP, TCP
TCP: problematiche di connessione e congestione ;
Compiti del livello trasporto - servizi del livello trasporto
Livello trasporto nel modello TCP/IP : porte e socket,
TCP : segmenti, intestazione, creazione connessione, chiusura connessione, controllo del flusso, controllo della congestione ;
UDP: intestazione

- ## Le Virtual LAN (VLAN)

Definizione e funzioni di una VLAN
Realizzazione tramite due modalità: port based, tagged
Porte ibride
Il protocollo VTP e l'Inter-VLAN routing
VLAN condivise su più di uno switch
Realizzazione delle VLAN con CISCO Packet Tracer

- ## Principi di crittografia

La sicurezza nelle reti
Crittografia
Crittoanalisi
Trasformazioni e trasposizioni

- ## Crittografia simmetrica (o a chiave privata)

Generalità
Definizione di chiave
Il criterio DES ; 3-DES; IDEA; AES;
Limiti degli algoritmi simmetrici

- ## Crittografia asimmetrica (o a chiave pubblica)

Definizione di chiave pubblica e chiave privata

Utilizzo per garantire la segretezza
Utilizzo per garantire l'autenticità •
Doppia crittografia •
Algoritmo RSA
Crittografia ibrida
Limiti della crittografia asimmetrica

- **Certificati e firma digitale**

La firma digitale secondo la direttiva 199/93/CE
Apposizione e controllo della firma digitale: funzione HASH
Certificati

- **La sicurezza nei sistemi informativi**

Minacce naturali, umane
Minacce in rete
Tipologie di attacchi: attivi e passivi
Modalità di attacco: virus, worm, trojan, backdoor
Hacker e Cracker • Evoluzione degli attacchi
La sicurezza di un sistema informatico
Valutazione dei rischi
La sicurezza nei sistemi informativi distribuiti

- **La difesa perimetrale con i firewall**

I firewall
Classificazione ingress/egress
Livello di intervento: routing, proxy
Personal firewall
Network firewall
Packet filter router
Access control list
Controllo orientato alla connessione (firewall stateful inspection)
Applicazione Proxy
La DMZ

***LABORATORIO***

- Programmazione di applicazioni in architettura client-server
- Utilizzo delle API di java per la realizzazione di applicazioni basate sulla crittografia simmetrica e asimmetrica.

**Argomenti svolti dal 5 marzo 2020 (DIDATTICA A DISTANZA)**

- **Reti private e reti private virtuali VPN**

Generalità La VPN:tipologie di VPN
Il protocollo Ipsec: Transport mode, Tunnel mode,
Authentication Header (AH), Encapsulating Security Payload (ESP), IKE.
Classificazione delle VPN

- **La sicurezza delle connessioni con SSL/TLS**

Generalità
Il protocollo SSL/TLS ; SSL Handshake,  SSL Record Protocol
Il funzionamento di TLS

***LABORATORIO***

- Progettazione e sviluppo di un sistema distribuito e sicuro in collaborazione multidisciplinare con Informatica e T.I.P.S.T.

Castellana Grotte, 31-05-2020

I  docenti

*Carmela Meliota*
*Daniele Amendolare*

Gli alunni