ISTITUTO D'ISTRUZIONE SUPERIORE "L. EINAUDI" – ALBA
ANNO SCOLASTICO 2023/2024

CLASSE 5° L Disciplina: Sistemi e Reti

Docenti: Davide Odierna – Carmelo Vassallo Todaro

MODULI COSTITUENTI IL PROGRAMMA SVOLTO

MODULI

M_1 Reti ISO/OSI livello 3, livello Rete

M_2 Reti ISO/OSI livello 4, livello di trasporto

M_3 Reti modello TCP/IP, il livello delle applicazioni

M_4 Sicurezza di un sistema informatico, in rete e perimetrale

M_5 Progettazione ed amministrazione reti

DETTAGLIO DEL PROGRAMMA

MODULO 1: Reti ISO/OSI livello 3: livello Rete

Contenuti:

- Il modello IOS/OSI e TCP/IP a confronto.
- Introduzione: servizi e protocolli del livello IP e del livello TCP, i concetti chiave di "Comunicazione orientata alla connessione" o "senza connessione", "comunicazione affidabile" o "non affidabile", segmento, datagramma, trama.
- I protocolli TCP e UDP, differenze.
- Il protocollo IP (Internet Protocol), i principali campi della intestazione IPv4.
- L'indirizzamento IP: struttura degli indirizzi, la divisione degli indirizzi per classi (indirizzamento classful), caratteristiche di ogni classe in termini di numero di reti/host e intervallo di indirizzi ammissibili; network ID, host ID, indirizzo di host, indirizzo di rete, indirizzo di broadcast.
- (sub)net mask: scopo ed utilizzo; operazione di and bit a bit per la determinazione di un indirizzo di rete.
- Indirizzi privati e pubblici: differenza, funzioni, l'esaurimento degli indirizzi IP, concetto di NAT.
- (Classful) Subnetting: partizionamento delle reti; indirizzamento di sottoreti, uso della maschera di sottorete per l'individuazione degli indirizzi di sottorete di appartenenza.
- Subnetting VLSM: uso delle maschere a lunghezza variabile, differenti per ogni sottorete.
- Indirizzamento IP classless (CIDR) o "supernetting": definizione, indicazione della maschera; individuazione delle reti classless; confronto tra l'indirizzamento classless e classful.
- Router e default gateway: introduzione, funzione; configurazione delle sue interfacce, indirizzo di gateway, configurazione degli host connessi ai router; forwarding diretto (Direct Connected Network) ed indiretto; la comunicazione tra host nella stessa rete ed in reti differenti (il viaggio di un pacchetto attraverso le reti); differenza tra router "utente" (di rete periferica), router edge (di rete di accesso) e router core (di rete di trasporto).
- Tabella di routing: costituzione, sua lettura ed utilizzo; le regole di routing statico, assegnazione delle rotte in presenza di una rete complessa connessa da più router; la distanza amministrativa; la tabella di routing dei router CISCO.
- Algoritmi di routing: classificazione e caratteristiche dei principali algoritmi e protocolli usati; la differenza tra protocollo RIP v2 e v1.

MODULO 2: Reti ISO/OSI livello 4, livello di trasporto

Contenuti:

- Lo strato di trasporto, i compiti, i servizi offerti, il multiplexing/demultiplexing.
- Il Protocollo TCP: le porte e i socket TCP, le porte well known, registered e Dynamic and/or Private Ports; il preambolo del segmento TCP con significato dei principali campi; gestione delle connessioni TCP, apertura e chiusura di una connessione TCP, handshake a 3 vie e 4 vie; la gestione degli errori in TCP, i problemi di efficienza di Nagle e Clark, il problema della congestione.
- Il Protocollo UDP: cenni e differenze col TCP.
- Il protocollo ARP (Address Resolution Protocol): le funzioni ARP e RARP (Reverse ARP), principio di funzionamento, la tabella ARP, risoluzione degli indirizzi di stazioni presenti nella stessa rete o in reti differenti; il comando “arp” di sistema operativo.
- Il protocollo NAT (Network Address Translation): scopo de NAT, la separazione tra indirizzi pubblici e privati; l’utilizzo delle porte nel processo di NAT; la tabella di NAT, il viaggio di un pacchetto attraverso il servizio NAT.
- Il protocollo DHCP (Dynamic Host Configuration Protocol): le 4 fasi per la assegnazione di un indirizzo dinamico, il concetto di lease dell’indirizzo, il lease time.
- Introduzione alle VLAN e loro configurazione, Port based VLAN (untagged), VLAN 802.1Q (tagged VLAN).

MODULO 3: Reti modello TCP/IP, il livello delle applicazioni

Contenuti:

- Il livello applicazione, il WWW, documenti ipertestuali e ipermediali, il linguaggio HTML caratteristiche aggiuntive con HTML v5.
- Architettura client-server e architettura multi-tier
- Il Protocollo HTTP, demone HTTP, differenza tra pagine statiche e dinamiche; la richiesta dal client al server, sintassi e commento dei campi; il passaggio di parametri con protocollo HTTP, i metodi GET e POST; la risposta del server al client, sintassi e commento dei campi; differenza tra la versione HTTP1.0 e HTTP1.1.
- Il servizio DNS, storia e struttura, gerarchia di dominio; il record delle risorse; struttura e interrogazione del DNS.
- Il servizio di posta elettronica, architettura di un sistema di posta elettronica e i suoi protocolli; differenza tra Mail User Agent e Mail Transfer Agent; struttura di un messaggio di posta elettronica, lo standard MIME; il protocollo SMTP con e senza autenticazione, descrizione dei comandi principali; il protocollo POP3, i comandi principali, differenza col protocollo IMAP.
- Il protocollo FTP, architettura e funzione, utilizzo dei principali comandi.

MODULO 4: Sicurezza di un sistema informatico, in rete e perimetrale

Contenuti:

- Sicurezza informatica: introduzione e obiettivi; concetto di vulnerabilità, minacce e attacchi.
- Gli aspetti di un sistema informatico, e/o le sue informazioni, da proteggere da qualsiasi eventuale minaccia: la terna “CIA”, Confidenciality (Riservatezza), Integrity (Integrità), Availability (Disponibilità).
- Classificazione delle minacce rispetto ai diversi aspetti del servizio erogato (CIA), sui quali avranno impatto e rispetto ai livelli della pila ISO/OSI sui quali avranno impatto.
- Classificazione degli attacchi, attività di hacking, SQL Injection, Social Engineering
- L’attacco Advanced Persistent Threat (ATP), definizione, le quattro fasi in cui si mette in atto: Preparation, Infection, Deployment, Persistence..
- Gestione della sicurezza aziendale: introduzione, analisi del rischio e politiche di sicurezza; il piano di sicurezza, la policy, pianificazione, piano di ripristino e contromisure; tutela dei dati personali, normative sulla privacy.
- Crittografia: ambiti di applicazione, sistemi monoalfabetici e polialfabetici, il concetto di chiave di cifratura; crittografia simmetrica a chiave segreta; crittografia asimmetrica a chiavi pubblica e privata, descrizione dell’algoritmo RSA..
- Autenticazione degli utenti ed affidabilità: controllo degli accessi, autenticazione degli utenti; la firma digitale e la non ripudiabilità, i certificati digitali e le autorità di certificazione.
- I protocolli sicuri nei diversi livelli ISO/OSI: I protocolli IPSec, struttura, funzione, differenze tra protocollo AH e ESP; implementazione in modalità transport o tunnel; intestazione AH e ESP, i principali campi;
- I protocolli sicuri nei diversi livelli ISO/OSI: Il protocollo SSL/TLS, scopo, campo di applicazione, funzionalità; lo strato “SSL handshake”: descrizione delle 4 fasi di handshake, caratteristiche dei messaggi; lo strato “SSL Record Protocol”: la manipolazione e preparazione dei dati consegnati al livello TCP; Il protocollo HTTPS, caratteristiche e funzionamento.
- il protocollo PGP per la posta sicura, dettagli funzionali, la rete “Web of Trust” a garanzia di una democratica ed imparziale certificazione delle chiavi.
- Le reti private virtuali (Virtual Private Network - VPN): scopo e funzione di una VPN, modalità site-to-site e ad accesso remoto; tipi di VPN Trusted, Secure e Hybrid, differenze.
- Firewall, definizione e funzione, il filtraggio dei dati nei diversi livelli della pila TCP/IP: il packet filtering, lo stateful packet inspection e il gateway application level (o proxy server); la funzione di caching del proxy server; Demilitarized Zone (DMZ) e port forwarding.
- La sicurezza nelle reti Wi-Fi: filtraggio dell’indirizzo MAC, autenticazione, la chiave PSK, i protocolli WEP, WPA/Personal e WPA/Enterprise (standard 802.1x/EAP); le tre macrofasi di autenticazione del protocollo EAP.

MODULO 5: Progettazione ed amministrazione reti

Contenuti:

- Il software di progettazione e simulazione di reti Packet-Tracer: funzionalità ed utilizzo; analisi dei pacchetti mediante simulatore Packet tracer.
- Progettazione di una rete di PC, connessioni, creazione di sottoreti, indirizzamento IP classful e classless.
- Cenni al sistema operativo CISCO IOS (Internetwork Operating System) e alla Command Line Interface (CLI) per la scrittura di comandi nei router CISCO, i comandi base e fondamentali per la configurazione e gestione delle principali funzioni dei router.
- Configurazione di uno o più router, utente, edge e core.

Attività di laboratorio (in ambiente simulato Packet Tracer):

- Progetto di una rete di calcolatori organizzata in isole indipendenti mediante l'uso di classful subnetting e VLSM subnetting.
- Connessione tra reti mediante router: installazione e configurazione del router attraverso la CLI.
- Connessione di reti remote attraverso router utente, edge e core: configurazione di rotte statiche, la regola “last resort”; configurazione di rotte dinamiche mediante protocollo RIP (v2 inclusa).
- Connessione di reti remote attraverso router edge e core: creazione di una maglia per l’osservare le azioni di modifica delle rotte dinamiche messe in atto dai router in caso di guasto di uno o più nodi della rete (scambio di informazioni tra i router, modifica e aggiornamento delle tabelle di routing).
- Gestione della funzione di NAT: progettazione, attivazione e configurazione del Network Address Translation (NAT) nei router CISCO.
- Realizzazione di una rete divisa in più VLAN.
- Gestione e configurazione dei servizi di DHCP, FTP e HTTP su un server.
- Scrittura e applicazione di una Access Control List (ACL) “semplice” per il controllo del traffico in una rete locale o tra reti locali/remote: programmazione del router.
- Scrittura e applicazione di una Access Control List (ACL) “avanzata” per il controllo di traffico “specifico” in una rete locale o tra reti locali/remote: programmazione del router.