

PROGRAMMA FINALE

SISTEMI E RETI

Classe 5 F

Prof. Giuliano Latina

A.S. 2020/2021

TEORIA

Modulo 1 – LIVELLO 4 TRASPORTO

- Livello 4 Trasporto: caratteristiche generali; concetti di connessione e three-way handshake.
- Protocollo UDP: caratteristiche generali e concetto di porta; pacchetto UDP; comunicazioni UDP; protocollo IGMP.
- Protocollo TCP: caratteristiche generali; pacchetto TCP; connessione e disconnessione TCP; Sliding Window TCP con ACK cumulativi e piggybacking; controllo di flusso con finestra di trasmissione e Selective Repeat; gestione delle congestioni con timeout ed algoritmi per il controllo di congestione (Slow Start, Congestion Avoidance, Fast Retransmit e Fast Recovery).
- Programmazione: caratteristiche generali; concetto di socket e principali funzioni; concetti di programmazione sequenziale e concorrente; chiamate delle funzioni per le comunicazioni UDP e per le connessioni e disconnessioni TCP.

Modulo 2 – LIVELLO 7 APPLICAZIONE

- Protocollo DHCP e problemi legati alla sicurezza (address starvation e rogue server); protocollo DNS e problemi legati alla sicurezza (cache poisoning); cenni sul protocollo mDNS.
- Protocollo HTTP: caratteristiche generali; metodi GET e POST; problemi legati alla sicurezza (Web spoofing e hijacking).
- Reti Microsoft: concetti di rete workgroup e rete a dominio; protocollo SMB con servizio NBT; protocollo LDAP con interfaccia amministrativa MMC.
- Posta elettronica: caratteristiche generali; protocolli SMTP, IMAP e POP3; architettura del sistema di posta elettronica in trasmissione ed in ricezione.

Modulo 3 – INTERNETWORKING - PROCESSI

- Processo NAT; sicurezza NAT.
- Processo firewall: tipi di firewall; livelli di controllo; regole di una ACL; problemi legati alla sicurezza (IP spoofing e IP smurfing).
- Processo proxy: reverse proxy; confronto con NAT e firewall; sicurezza proxy.

Modulo 4 – INTERNETWORKING – MODELLI DI CONFIGURAZIONE

- Reti residenziali; reti single-homed e dual-homed; reti trust/DMZ; rete modello Microsoft.
- Virtualizzazione: macchina virtuale; vantaggi della virtualizzazione (gestione, costo, manutenzione, configurazione e gestione remota).

Modulo 5 – INTERNETWORKING – ACCESSO DA REMOTO

- Concetto di amministrazione remota; tecnica di tunneling.
- Terminale remoto; desktop remoto.
- VPN (Virtual Private Network).
- Cloud computing: costi di gestione; organizzazione di un sistema cloud; servizi cloud.

Modulo 6 – SICUREZZA INFORMATICA - QUADRO NORMATIVO IN ITALIA

- Norma ISO 27001: sistema di gestione per la sicurezza delle informazioni; terminologia essenziale.
- Frode e crimini informatici: sanzioni previste dal Codice penale; tipologie di reato; programmi utilizzati per compiere i crimini; precauzioni necessarie per contrastare i reati (**SVOLTO NELL'AMBITO DELL'INSEGNAMENTO DI EDUCAZIONE CIVICA**).
- Riservatezza dei dati: differenza tra dati sensibili e giudiziari; ruoli essenziali in materia di trattamento di dati personali.
- Pubblica Amministrazione: codice dell'amministrazione digitale; posta elettronica certificata (PEC); concetto di firma elettronica.

Modulo 7 – SICUREZZA INFORMATICA – TECNICHE PER LA SICUREZZA

- Crittografia a chiave simmetrica: concetto di chiave; cifratura con codice a sostituzione; cifratura con codice a trasposizione.
- Crittografia a chiave asimmetrica: chiave privata e chiave pubblica; operazione di fattorizzazione.
- Sintesi di messaggi: funzioni di hash.
- Autenticazione: password e One-Time Password; protocollo sfida/risposta; protocollo di Diffie-Hellman per lo scambio di chiavi tramite operazione di logaritmo discreto.
- Firma digitale con smart card; concetti di identità, autorità di certificazione e centro di distribuzione delle chiavi.

Modulo 8 – SICUREZZA INFORMATICA – PROTOCOLLI PER LA SICUREZZA

- CHAP; WPA2 nelle modalità personal ed enterprise; RADIUS; Kerberos.
- IPsec e sottoprotocolli IKE ed ESP; SSL/TLS: fasi di Handshake e di Record; protocollo HTTPS; certificati digitali.

LABORATORIO

- *Port scanner Nmap*: comandi per effettuare la scansione delle porte UDP e TCP e per ottenere informazioni su protocolli e servizi in esecuzione.
- *Programma Netstat*: comandi per controllare le comunicazioni UDP e le connessioni TCP attive e per visualizzare le statistiche relative ad entrambi i protocolli.
- *Programma Ipconfig*: comandi per individuare l'indirizzo IP di un server DHCP e per ispezionare la cache del DNS.
- *Programma Nslookup*: comando per ottenere l'indirizzo IP corrispondente ad un nome di dominio.

- *Analizzatore di protocollo Wireshark*: selezione dell'interfaccia di rete; valutazione dei campi di pacchetti TCP in transito su una rete, misurazione del Round Trip Time, confronto con il valore ottenuto tramite il programma Ping ed interpretazione di statistiche e grafici; valutazione dei campi di pacchetti UDP in transito su una rete ed interpretazione di statistiche e grafici; valutazione dei campi di pacchetti DHCP e DNS in transito su una rete; valutazione dei metodi GET e POST relativi ai pacchetti HTTP; valutazione dei campi di pacchetti TLS in transito su una rete.
- *Programma Nbtstat*: comando per visualizzare lo stato NBT di un client Microsoft.
- *Interfaccia amministrativa Microsoft Management Console (MMC)*: visualizzazione degli snap-in per avviare o fermare i servizi di sistema e per gestire la console di un client Microsoft.
- *Interfaccia amministrativa MicroSoft Terminal Services Client (MSTSC)*: visualizzazione delle principali impostazioni di Connessione Desktop remoto per un client Microsoft.
- *Programma Telnet*: comandi per l'invio di una e-mail tramite una sessione SMTP, con autenticazione codificata in Base64; comandi per la lettura di una e-mail tramite una sessione POP, con autenticazione non codificata.
- *Due algoritmi in Linguaggio C++* sulla cifratura con codice a sostituzione.

N.B. Vari argomenti sono stati trattati tramite Didattica Digitale Integrata, prevalentemente sincrona.

Libro di testo: "Corso di sistemi e reti - Vol. 3", *Ollari*, Tecnologia Zanichelli

Bolzano, 27/5/2021

Firma docente Giuliano Latina