

Sistemi e reti

Relazione finale

La classe è composta da venticinque studenti e presenta al suo interno un buon livello di coesione. Gli alunni si sono dimostrati nell'arco degli ultimi due anni di studi collaborativi e favorevoli ad un dialogo educativo proficuo. I rapporti interpersonali sono sempre stati rispettosi e cordiali e non si sono osservate problematiche significative all'interno del gruppo classe. Questo atteggiamento, una buona partecipazione degli alunni alle lezioni e un impegno sufficientemente costante hanno favorito i processi di apprendimento come dimostrato dalle poche insufficienze presenti nel quadro di voti degli alunni.

Dal punto di vista del comportamento, gli studenti hanno tenuto una condotta corretta sia nelle attività in aule che in quelle di laboratorio. Il profitto della classe è generalmente positivo, ma i risultati non sono omogenei. Alcuni alunni si sono infatti distinti per interesse, partecipazione e merito, altri non hanno raggiunto lo stesso livello di profitto.

Programma svolto

Obiettivi Conseguiti:

Progettazione e simulazione di reti di computer e sistemi di comunicazione negli elementi essenziali; comprensione dei concetti di architettura di rete, di protocolli di comunicazione, di sicurezza delle reti e di gestione delle risorse di rete. L'obiettivo finale cui si è teso, tra gli altri, è il raggiungimento della capacità di utilizzare la logica, la conoscenza e la ragione per risolvere problemi, nell'ambito dei sistemi, in modo efficace.

Metodi di Insegnamento:

Si sono orientate le attività al fine di sviluppare la logica attraverso l'analisi dei dati e la didattica guidata; organizzare il processo di apprendimento in moduli in sequenza logica; presentare gli argomenti nella forma teorica ed in seguito metterli in pratica in laboratorio; sviluppare i temi in logica deduttiva, dal generale al particolare.

Contenuti disciplinari:

Gli elementi centrali della disciplina sono costituiti da tre differenti macro aree intercomunicanti fra loro e suddivise in nove moduli: networking; protocolli di applicazione; sistemi di sicurezza.

I moduli didattici sono stati distribuiti nei due quadrimestri nella seguente maniera:

(1°quadrimestre)

- Modulo 1 – Virtual Local Area Network: progettazione e strutturazione di VLAN, utilizzo di protocolli specifici tra cui il Virtual Trunking Protocol e set dei device necessari.
- Modulo 2 – Crittografia: concetto di sicurezza informatica, cifrari e sistemi di crittografia, crittografia a chiave simmetrica ed asimmetrica, firma digitale, DES, RSA;
- Modulo 3 – Protocolli SSH e SSL/TLS: confidenzialità attraverso la rete, funzionamento e scopo dei protocolli, concetto di tunneling;
- Modulo 4 – Protocolli di livello applicazione ISO-OSI: telnet, http, smtp, pop3, imap, ftp, snmp, dhcp, dns;

(2° quadrimestre)

- Modulo 5 – VPN: realizzazione e configurazione nelle modalità site-to-site e remote-access, protocollo IPSec;
- Modulo 6 – Firewall e Proxy: controllo degli accessi e monitoring, ACL, Firewall, DMZ, Proxy e Nat;
- Modulo 7 – Sistemi di autenticazione: rete cablata e wireless, il servizio AAA, Radius. IOT
- Modulo 8 – Sistemi di archiviazione e server: archiviazione e backup, sistema Raid, Nas.
- Modulo 9 – Cloud: housing e hosting, server farm e data center, cloud computing e modelli di servizi, multi-tier application.

Metodi (spazi, tempi):

le lezioni sono state organizzate fra aula e laboratorio per un monte ore previsto di 4 ore settimanali.

Attività di aula (1 ora settimanale): le attività di aula sono state orientate alla comprensione dei

fondamenti disciplinari, alla radicazione delle conoscenze tecnologiche. Strategie adottate: lezione frontale, discussione guidata, studio di caso.

Attività di laboratorio (3 ore settimanali): le attività di laboratorio, intese come integranti e complementari delle lezioni teoriche d'aula, sono state svolte nel laboratorio LT dell'Istituto per un totale di 3 ore settimanali. I contenuti hanno riguardato principalmente seguenti argomenti: simulazione di progettazione di rete e configurazione devices attraverso l'utilizzo del software Cisco Packet tracer; moduli di simulazione e virtualizzazione di proxy e O.S. server, attività complementari alla sicurezza: packet sniffing, spoofing. A completamento delle attività sono state proposte esercitazioni

riguardanti il cloud e servizi. Strategie adottate: didattica laboratoriale, learn by doing, problema di realtà.