Istituto Statale di Istruzione Secondaria
di Secondo Grado
*POLO TECNOLOGICO IMPERIESE*
**I.T.I.** "G.Galilei"- **I.T.T.L.**. "A.Doria" - **I.P.S.S.C.** "U.Calvi"
Via Santa Lucia 31 – 18100 Imperia – C.F. 80011330083
Tel. 0183.29.59.58
email:imis002001@istruzione.it
PEC: imis002001@pec.istruzione.it
sito:www.polotecnologicoimperiese.edu.it

Erasmus+

**A.S. 2023-24**
**CLASSE 5B INF**

**Programma di SISTEMI E RETI**

**Prof. Simone ZANELLA (Docente)**
**Prof. Marco DE ROSSI (ITP)**

- **I servizi di rete**
  - Modello client/server.
  - Porte e servizi: well known ports, registered ports.
    - Laboratorio: il protocollo ICMP e il comando ping.
  - Il WWW e il protocollo HTTP: caratteristiche principali, motori di ricerca, spider web. Vulnerabilità di sicurezza, il defacciamento di siti web.
    - Laboratorio: analisi tramite Firefox dei flussi messaggi HTTP, GET, POST, Altervista come server web; analisi di rete con Wireshark, analisi degli scambi di dati HTTP, funzionamento dei cookies.
    - Laboratorio: il linguaggio di scripting PHP e la gestione dei database MySQL, realizzazione di un sito web dinamico (Lavoro di gruppo I quadrimestre con metodologia jigsaw a gruppi esperti).
  - Protocollo FTP: caratteristiche principali.
  - Protocollo POP3, SMTP, IMAP: caratteristiche principali, vantaggi, svantaggi, lo spam, tecniche di phishing, filtraggio dello spam con tecniche euristiche
  - Servizio DNS: caratteristiche del funzionamento, DNS poisoning.
    - Laboratorio: utilizzo del comando tracert/traceroute per individuazione del routing verso un sito web, strumenti di geolocalizzazione degli IP – Ip Lookup, strumenti per visualizzare i record di un DNS – "DNS Lookup".
  - Servizio VOIP: caratteristiche principali, gateway, collegamento a reti PSTN, vulnerabilità di sicurezza.
    - Approfondimento: i servizi di rete decentralizzati, la "degooglizzazione", il fediverso.
    - Approfondimento: TOR e il deep web, differenza tra surface web e deep web, dark web.
    - Laboratorio: hacking etico, Wireshark e analisi di catture di rete contenenti malware.

- **Sicurezza delle informazioni**
  - Triade CIA e protocolli di tipo AAAA
  - Normative: X800, GDPR
    - Approfondimento: corso CISCO Introduction to Cybersecurity

        - Laboratorio: attività CTF – “Capture the Flag” su OliCyber.it Consorzio Interuniversitario di Cybersecurity
    - Crittografia e crittoanalisi: crittografia a chiave privata (sincrona), a chiave pubblica (asincrona), problema dello scambio delel chiavi e crittografia ibrida. Firma digitale.
    - Cenni su storia di crittografia: cifrari a sostituzione di Cesare e di Vigenere, cifrari a rotori e la macchina Enigma.
        - Laboratorio: attacco Man in The Middle tramite protocollo ARP su autenticazione in chiaro e con crittografia tramite form di pagina web, confronto tramite catttura di rete con Wireshark.
        - Laboratorio: scansione di rete per la ricostruzione della topologia della rete, e individuazione di servizi non sicuri tramite NMAP su Linux.
        - Approfondimento: tecniche di analisi delle frequenze per attacco a un crittogramma. esperienza semplificata su un cruciverba crittografato della Settimana Enigmistica.
    - Funzioni di hashing: caratteristiche, problema delle collisioni, “attacco di compleanno”, fingerprint, campi di utilizzo.
        - Laboratorio: applicazione di algoritmi di hashing in PHP con la funzione Crypt, algoritmo SHA256 e MD5, implementazione nei propri siti dinamici di autenticazione tramite password memorizzata tramite hashing.
        - Laboratorio: cracking di password tramite rainbow table. strumenti di verifica dei data breach (Have I Been Pwned, Mozilla Monitor).

- **Sicurezza delle reti**
    - Principali tipologie di minacce nei livelli ISO/OSI.
    - Protocollo SSL/TLS: caratteristiche, impiego nel protocollo HTTPS, certificati, CA – Certification Authority.
    - Firewall: tipologie incominig/outgoing, software vs hardware, Stateful Inspection, Packet Filter, Personal, Application Firewall, Next Generation.
    - ACL: Access Control List, comandi principali, strutturazione di una semplice ACL.
        - Laboratorio: ricerca di esposizione di dati di accesso a reti e sistemi su motori, “Google Dorks”.
    - VPN: tipologie e caratteristiche principali, tunneling.

- **Modello distribuito per servizi di rete**
    - Modello Client-Server: caratteristiche, programmazione Client Side/Server Side
    - Sistemi Distribuiti: architetture web, risorse condivise, confronto tra soluzione monolitica e soluzione distribuita, requisiti, IntraNet ed ExtraNet.
    - Middleware: caratteristiche principali.
    - Autenticazione nei sistemi distribuiti: autenticazione nei sistemi Linux, caratteristiche e criticità, Windows Active Directory: caratteristiche principali, dominio, protocollo SMB.
        - Laboratorio: autenticazione degli utenti in Linux, file passwd, file shadow, attacco alle password con tool John the Ripper e attacchi a dizionario/wordlist.

- **Progettazione di rete**
    - Il cablaggio strutturato delle reti, cablaggio verticale e orizzontale, normative.
    - Topologia logica e fisica di una rete.
    - Piano di indirizzamento IPv4.
    - Routing statico e tabelle di routing.
    - Tecniche di separazione del traffico di rete, VLAN. InterVLAN routing, tecnica del Router-on-a-stick.
    - Progettazione di una rete LAN cablata integrata con WiFi, scelta dei servizi di rete.
    - Analisi/audit di sicurezza di una rete, implementazione di servizi di rete a difesa dalle minacce interne ed esterne.
        - Laboratorio: progettazione di una rete con CISCO Packet Tracer.
        - Approfondimento: corso CISCO CCNA-1 Introduction to Networks.
        - Analisi di prove di esame di Sistemi e Reti dei precedenti A.S.

*Riferimenti:*

- *Libro di testo: SISTEMI E RETI – D. Tomassini - Vol. 2 – Hoepli.*
- *Slides fornite dal docente su piattaforma Moodle scolastica.*
- *Piattaforma di e-learning CISCO Net Academy.*

Imperia, 15 Maggio 2024