PROGRAMMA SVOLTO
A.S. 2023/2024

DOCENTE:	Casali Enea - Cirioni Vittorio
DISCIPLINA:	Sistemi e Reti
CLASSE:	5A INFO

Per ogni Modulo svolto vengono indicati i relativi contenuti affrontati.

MODULO	CONTENUTI
U0 Libro di quarta	Protocolli di livello 4: Protocollo connesso TCP Protocollo non connesso UDP Three way handshake Sliding Windows Porte e servizi: well known port, registered port, dynamic port
U1	Tecniche di crittografia per l'internet sicurity Requisiti: autenticità, confidenzialità/segretezza, integrità, non ripudiabilità Classificazione dei metodi crittografici In particolare: tecniche di sostituzione/trasposizione Antica/moderna: studio autonomo dell'antica; parallelo con la moderna dove la sostituzione di lettere nell'antichità è divenuta tecnica dello xor con una chiave nella criptografia moderna Crittografia Simmetrica/Asimmetrica Algoritmi simmetrici più noti 3DES, AES, IDEA solo nomi senza la descrizione dell'algoritmo se non l'idea sommaria di ripetuti passaggi di sostituzione xor con una o più chiavi e trasposizione Algoritmi asimmetrici RSA non svolta la teoria matematica alla base, solo la nozione di fattorizzazione con numeri primi con un grande numero di cifre, per cui grande dispendiosità in termini di calcolo; concetto di invertibilità reciproca della due funzioni $K^{+}(m)$ $K^{-}(m)$ notazione per indicare rispettivamente

	chiave pubblica + e chiave privata – applicate al messaggio dei soggetti A e B i cosiddetti Alice e Bob Gli schemi di utilizzo della chiave pubblica del mittente/destinatario per garantire autenticità/segretezza/entrambe (importante) Definizione di hash di un documento (anche detto impronta, fingerprint, digest) e principali algoritmi MD5 SHA1 SHA2 Utilizzo dell'hash per garantire l'integrità di un documento trasmesso Firma digitale Schema di funzionamento riferibile alla tecnica dell'hash del documento Importanza di una CA (certification authority) imprescindibile per scongiurare la possibilità di certificati falsi e quindi della presenza di un Mim (man in the middle)
U2	Efficienza e sicurezza delle reti locali VLAN Firewall ACL Attacchi: arp-spoofing, portscanning, DoS, DDoS, Warm, SQL injection Proxy Server Compiti Tipi di proxy (non svolto) Nat e Pat DMZ
U3	VPN Introduzione Tipi Fattori di sicurezza: autenticazione dell'identità, cifratura Tunneling (concetto di incapsulamento di protocolli) Ipsec (AH, ESP, IKE) Svolta solo la differenza tra i tre protocolli in termini di garantire autenticazione e/o segretezza SSL/TLS VPN: passi necessari ed uso di tecnica sia asimmetrica nella fase handshake che simmetrica durante la comunicazione BGP/MPLS VPN non svolto per mancanza di tempo Trusted vpn / Secure vpn / Hybrid vpn (non svolto per mancanza di tempo consigliato lo studio autono in vista della seconda prova) Vpn per lo streaming, gaming, home banking (non svolto per mancanza di tempo consigliato lo studio autonomo in vista della seconda prova)
U4	**Le reti wireless** non svolto per mancanza di tempo consigliato lo studio autonomo in vista della seconda prova in particolare di: Classificazione studio autonomo WLAN studio autonomo in particolare della terminologia WT wireless terminal - AP access point - BSS basic server set - SSID WWAN studio autonomo wmax ricordare distanza e velocità in vista della seconda prova

	WWAN studio autonomo Rischi per la sicurezza studio autonomo Critptografia criptografia WEP RC4 conoscere che non è più ritenuta sicura, tralasciare il funzionamento WPA2 3 conoscere come metodi sicuri Autenticazione studio autonomo
U5	**Reti mobile ip e reti cellulari per utenti mobili** non svolto per mancanza di tempo consigliato lo studio autonomo in vista della seconda prova in particolare dei paragrafi La telefonia cellulare La rete 5G
U6	**Progettare strutture di rete dal cablaggio al cloud** Ripasso del cablaggio strutturato: esempi di progetto di rete: “Un giornale online” “un ospedale con cartella clinica elettronica via wifi” “Una Scuola riprogettazione” simulazione della seconda prova “un servizio a supporto di start-up” Progettare la collocazione dei server (FileServer, Data Base Server, Web Server, Application Server, DHCP server, DNS server…) (presentazione su classroom in cui inclusa anche architettura 3-tier per web-app) Studio dei protocolli http mail dns (presentazione su classroom) Active Directory e DC Domain Controller (presentazione su classroom) I Servizi offerti dalle server farm -Hosting / Housing -Server dedicati -Server virtuali (Virtual Box) La soluzione cloud Modelli di servizi cloud (SaaS, DaaS, PaaS, IaaS) Il cloud nella pubblica amministrazione
Laboratorio	Ripasso su Routing, DHCP e NAT
Laboratorio	Lo strato di trasporto 1 - Le PORTE e CONNESSIONI virtuali necessarie per identificare le comunicazioni 2 - Le CONNESSIONI tcp e le TRASMISSIONI (unicast/multicast) udp 3 - Esercitazione NETSTAT su Windows
Laboratorio	Cybersecurity - KALI Linux e uso di wireshark 1 - La VIRTUALIZZAZIONE di Macchine 2 - Kali LINUX: lo sniffer WIRESHARK 3 - Analisi a L3 di un pacchetto ICMP con WIRESHARK

	4 - Analisi a L4 dei segmenti TCP: i 3 scambi di strette di mano 5 - Analisi a L5->7: intercettazione trasmissione HTTP
Laboratorio	I SERVIZI di rete essenziali 1 - Le componenti HARDWARE essenziali di un SERVER 2 - Linux come sistema operativo per server 3 - Configurazione iniziale di server VIRTUALE LINUX 4 - I SERVIZI di rete: le applicazioni tipiche di un server 5 - Servizio DNS e DHCP: servizio di attribuzione di NOMI alle risorse di rete
Laboratorio	Architettura WEB a LIVELLI (Tier) 1 - Installazione Servizio HTTP - Apache 2 2 -Rafforzare la sicurezza di Apache 4 - Controllo dell'accesso al proprio SITO WEB pubblicato 5 - Integrazione modulo PHP
Educazione Civica	L'argomento indicato nella programmazione di classe "identità digitale" è stato svolto solo dal punto di vista tecnico e senza implicazioni con educazione civica, per mancanza di tempo.

Il programma è stato visionato e approvato dai rappresentanti degli studenti della classe in data 7 giugno 2024