POLO SCIENTIFICO TECNOLOGICO PROFESSIONALE "E. FERMI & G. GIORGI" LUCCA

INDIRIZZO: Informatica e Telecomunicazioni

DISCIPLINA: SISTEMI e RETI A.S. 2017/'18

Classe 5AIF **Docente: Lucia GIAMMARIO**

MODULO 1: Normativa relativa alla sicurezza dei dati

M1-U1-Normativa nazionale e comunitaria sulla sicurezzadei dati

OBIETTIVI:	**CONTENUTI:**	LABORATORIO:
•Conoscere la normativa sulla sicurezza informatica	•La sicurezza in un sistema informatico •Le normative ISO 27K •Il modello Plan Do Check Act •La normativa nazionale	

MODULO 2: Tecnologie informatiche per garantire la sicurezza e l'integrità dei dati e dei sistemi.

M2-U1- Strategie di sicurezza

OBIETTIVI:	**CONTENUTI:**	•LABORATORIO:
•Conoscere problematiche e rischi afferenti alla gestione della rete privata	•Il fenomeno degli hachers e dei crackers •Misure fisiche di sicurezza •Processi organizzativi • Sicurezza interna	•Controllo dei pacchetti in entrata ed in uscita da una rete, scrittura e configurazione delle Access Control List sui router Cisco con simulazione su PT

M2-U2- Tecniche di attacco

OBIETTIVI:	**CONTENUTI:**	**LABORATORIO:**
•Conoscere le varie tenciche di attacco ed il livello del modello ISO/OSI in cui possono essere sferrati	•Attacchi a livello data link •Attacchi a livello rete •Attacchi a livello trasporto •Attacchi a livello presentazione •Attacchi a livello applicativo	

M2-U3- Rete locale virtuale (VLAN)

OBIETTIVI:	**CONTENUTI:**	•LABORATORIO:
•Conoscere il significato di rete virtuale •Conoscere l'utilità delle reti virtuali in ambienti a particolare complessità •Conoscere lo strumento della lista di controllo degli accessi (ACL) per implementare la protezione della rete •Conoscere come implementare le varie facce della sicurezza nei N.O.S. •Installare, configurare e gestire sistemi operativi garantendone la sicurezza. • Saper configurare una VLAN •Saper configurare una serie di ACL	•Rete locale virtuale (VLAN) •Segmentazione delle reti tramite VLAN •Strategie di sicurezza basate sul controllo di accesso •Liste di controllo di accesso (ACL)	•Analisi dei pacchetti in entrata ed in uscita da una rete. •Configurazione di reti virtuali (VLAN) •Configurazione di liste di controllo di accesso (ACL) sui router Cisco con simulazione su PT •Standard ACL •Extended ACL •Aspetti relativi alla sicurezza nei S.O. Like Unix e Microsoft

M2-U4- Protocolli per la sicurezza		
OBIETTIVI:	**CONTENUTI:**	**LABORATORIO:**
Conoscere potenzialità e limiti dei protocolli che implementano la sicurezza	•Protocollo HTTPS • Protocollo CHAP •ProtocolloWAP2 •Protocollo RADIUS •Protocollo Kerberos •Protocollo Ipsec •Protocollo SSL/TLS	•Servizi Radius e TACACS+ nei sistemi Microsoft
Modulo 3: Tecniche di filtraggio del traffico di rete.		
M3-U1- Il traffico di rete		
OBIETTIVI:	**CONTENUTI:**	**LABORATORIO:**
•Saper individuare e controllare il traffico di rete	•Indirizzi IP di traffico unicast, multicast e brodcast •Il traffico su switch, bridge intelligenti e router •Il trafico in una rete paritaria •Il traffico in una rete WiFi •ISP e traffico	•Controllo dei pacchetti in entrata ed in uscita da una rete •Analisi del traffico con il SW Wireshark
M3-U2- Il traffico dei protocolli		
OBIETTIVI:	**CONTENUTI:**	**LABORATORIO:**
•Saper individuare e controllare il traffico generato dai protocolli di comunicazione	•Il Traffico HTTP e HTTPS •Violazione del traffico HTTP •Il traffico DNS •Il traffico LDAP sui server Microsoft e Like Unix	
M3-U3- Il traffico sulle interfacce		
OBIETTIVI:	**CONTENUTI:**	**LABORATORIO:**
•Saper individuare e controllare il traffico sulle inteffacce	•Traffico incoming e outgoing •Il network address translation •Le interfacce del firewall •La rete DMZ nei sistemi Microsoft	•Simulazione di una rete con firewall/ DMZ con Packet Tracer •Installazione di una rete DMZ
M3-U4- Il controllo del traffico		
OBIETTIVI:	**CONTENUTI:**	**LABORATORIO:**
•Conoscere i comandi ed i programmi che permettono di ispezionare il traffico	•Controllo del traffico verso la rete esterna •Ispezione del traffico •Comandi per il controllo del traffico •Il protocollo SNMP •L'Audit	• Il Comando NETSTAT •Netfilter •Iptables
M3-U5- Sistemi di Intrusion Detection		
OBIETTIVI:	**CONTENUTI:**	**LABORATORIO:**
•Comprendere potezialitità e limiti dei IDS •Conoscere la caratteristiche principali dei sistemi di prevenzione delle intrusioni	•Concetti di base •Componenti del sistema •Metodologie di lavoro	•

	•Sistemi NIDS, HBIDS, HIDS •IDS attivi e passivi •Intrusion Prevention System	
Modulo 4: Tecniche crittografiche applicate alla protezione dei sistemi e delle reti		
M4-U1- Servizi di crittografia Integrità di base, Autenticità e Riservatezza		
OBIETTIVI:	**CONTENUTI:**	**LABORATORIO:**
•Descrivere i requisiti di sicurezza delle comunicazioni tra cui l'integrità, l'autenticazione e la riservatezza. •Descrivere la crittografia, la crittoanalisi e la crittologia. •Descrivere l'importanza delle funzioni hash . •Descrivere le caratteristiche e le funzioni l'algoritmo MD5 e SHA •Descrivere come abilitare l'autenticità con HMAC. •Descrivere i componenti di gestione delle chiavi. •Descrivere la funzione degli algoritmi DES, 3DES e AES, SEAL, RC e DH	•Funzione hash •Integrità con MD5 and SHA-1 •Autenticazione con HMAC •Caratteristiche di gestione delle chiavi •Algoritmi di Crittografia simmetrica •Tecniche di crittografia Simmetrica •Scambio di chiavi Diffie-Hellman	•Installare, configurare e gestire reti in riferimento alla privatezza, alla sicurezza e all'accesso ai servizi
M4-U2- Crittografia a Chiave pubblica		
OBIETTIVI:	**CONTENUTI:**	**LABORATORIO:**
•Spiegare le differenze tra crittografia simmetrica e asimmetrica •Spiegare la funzionalità delle firme digitali •Descrivere il ruolo delle Autorità di Certificazione e dei Certificati Digitali	•Algoritmi a chiavi a chiave asimmetrica •Chiave pubblica e Privata •Crittografia a chiave pubblica •Firma digitale •Il framework PKI •Le autorità di certificazione •La gestione dei certificati •I protocolli standard ed i protocolli alternativi	•Analisi di un certificato digitale
Modulo5 : Reti private virtuali.		
M5-U1-Le reti VPN		
OBIETTIVI:	**CONTENUTI:**	**LABORATORIO:**
•Descrivere i benefici di una VPN ed i loro benefici. •Configurare una VPN site-to-site con tunnel GRE •Configurare le ACL crypto utilizzando CLI. •Configurare una mappa crittografica utilizzando CLI. •Spiegare come il panorama aziendale sta cambiando per supportare il telelavoro. •Configurare un server VPN •Collegare un client VPN utilizzando un software specifico	•Caratteristiche generali •Tipi di VPN: remote access, site to site •Il tunnel GRE •Gestione della sicurezza:autenticazione, crittografia, tunnelling	•Configurazione su Packet Tracer di una VPN site-t-site tra due router Cisco 2811
M5-U2- Tecnologie di implementazione di una VPN		

OBIETTIVI:	CONTENUTI:	LABORATORIO:
•Descrivere il protocollo IPsec e le sue funzioni di base. •Descrivere le fasi di negoziazione e configurazione di IPsec. •Preparare IPsec per rendere compatibili le ACL. •Confrontare l' accesso remoto con IPsec e SSL •Spiegare come SSL viene utilizzato per stabilire una connessione VPN sicura.	•Protocollo Ipsec •Protocollo SSL •Protocollo MPLS •Classificazione in base ai protocolli:trusted,secure,hybrid	

Modulo 6: Modello client/server e distribuito per i servizi di rete.

M6-U1- Il Modello Client/ Server per i servizi di rete

OBIETTIVI:	CONTENUTI:	LABORATORIO:
•Identificare le caratteristiche di un servizio di rete nel modello Client/server. •Selezionare, installare, configurare e gestire un servizio di rete locale	•Il modello client server •Funzionalità e caratteristiche dei principali servizi di rete nel modello client /server	

M6-U2- Il Modello distribuito per i servizi di rete

OBIETTIVI:	CONTENUTI:	LABORATORIO:
•Identificare le caratteristiche di un servizio di rete. •Selezionare, installare, configurare e gestire un servizio di rete ad accesso pubblico	•Il modello distribuito •Funzionalità e caratteristiche dei principali servizi di rete nel modello distribuito	

Modulo 7: Funzionalità e caratteristiche dei principali servizi di rete.

M7-U1-Rete e servizi in Internet

OBIETTIVI:	CONTENUTI:	LABORATORIO:
Saper installare e configurare i principali servizi di rete	•La struttura di Internet •I servizi di Internet •Comunicazione in Internet •Telnet: collegamento ad un host remoto tramite •FTP:trasferimento dei file •Posta elettronica •HTTP •Newsgroup e chat	•Identificare le caratteristiche di un servizio di rete. •Utilizzare i servizi di rete

Modulo 6: Strumenti e protocolli per la gestione ed il monitoraggio delle reti

M6-U1- Strumenti e protocolli per la gestione delle reti

OBIETTIVI:	CONTENUTI:	LABORATORIO:
•Conoscere i protocolli per la gestione delle reti •Saper utilizzare gli strumenti per la gestione delle reti	•La gestione di una rete •Le utility di gestione	•Integrare differenti sistemi operativi in rete

Modulo 7: Macchine e servizi virtuali, reti per la loro implementazione

M7-U1-Macchine virtuali

OBIETTIVI:	CONTENUTI:	LABORATORIO:
•Comprendere il significato di macchina virtuale •Saper installare e configurare una VM	•Le macchine virtuali: caratteristiche e funzionalità.	•Installazione e configurazione di VM