PROGRAMMA DEL CORSO DI RETI DI CALCOLATORI E CYBERSECURITY

SETTORE SCIENTIFICO

INF/01

CFU

12

OBIETTIVI

/**/

La prima parte del corso ha lo scopo di fornire le basi concettuali delle Reti di Calcolatori con particolare riferimento ai protocolli ed alla architettura di Internet. Vengono analizzate le architetture standard per le reti di calcolatori, e descritto il funzionamento dei protocolli standard di Internet e dei meccanismi per la gestione e la trasmissione in rete di contenuti di vario tipo (es. multimediali audio-video). Nella seconda parte del corso vengono presentati i principali aspetti della Cybersecurity relativi a: sicurezza dei sistemi informativi e della loro difesa da attacchi informatici via rete, tecniche di rilevamento delle intrusioni, classificazione di virus e malware e tecniche e strumenti per la loro analisi ed individuazione, firewall e loro configurazione.

PROGRAMMA DIDATTICO: ELENCO VIDEOLEZIONI/MODULI

Reti di calcolatori

1.Introduzione alle Reti di calcolatori 2.Accesso a Internet 3.Trasmissione dei dati in Internet 4.Ritardi nelle Reti a commutazione di pacchetto 5.Throughput nelle reti di calcolatori 6.Internet: una rete di reti 7.Architettura a livelli: suite di protocolli ISO/OSI e TCP/IP 8.Incapsulamento nella suite dei protocolli Internet 9.Sicurezza in Internet 10.I certificati X.509 11.IPSec e il protocollo ESP 12.Sicurezza della posta elettronica e PGP 13.IPSec 14.Il protocollo SSL 15.I protocolli TLS e HTTPS 16.SET - Secure Electronic Transaction 17.I firewall 18.Comunicazioni anonime: i protocolli Crowds e Mix 19.Comunicazioni anonime: Tor e Deep Web Modulo 2: Cybersecurity 1.Concetti base di sicurezza 2.Servizi e meccanismi di sicurezza 3.Crittografia simmetrica 4.Crittografia simmetrica: tecniche di sostituzione e di trasposizione 5.Cifratura a blocchi 6.La cifratura DES: Data Encryption Standard 7.La cifratura AES - Advanced Encryption Standard 8.La crittografia multipla 9.Modalità di funzionamento della cifratura a blocchi 10.Segretezza e crittografia simmetrica 11.Crittografia asimmetrica 12.L'algoritmo RSA 13.Gestione delle chiavi e scambio Diffie-Hellman 14.Autenticazione dei messaggi 15.Codici MAC e funzioni hash 16.L'algoritmo SHA-512 17.Gli algoritmi HMAC e CMAC 18.Le firme digitali 19.Autenticazione in ambienti distribuiti 20.Intrusioni e software doloso 21.Tipi di malware e DDoS 22.Multimedia forensics 23.MM-forensics: identificazione della sorgente 24.MM-forensics: rilevazione di fake 25.Blockchain e Proof-of-Work 26.Blockchain e il Ledger Distribuito