



## PROGRAMMA EFFETTIVAMENTE SVOLTO

Anno Scolastico 2023 / 2024

**Classe/Sede:** 5D2 ITI

**Docente:** LUCA BATTISTIN

**Codocente (ITP):** ANDREA MISITI

**Materia insegnata:** SISTEMI E RETI

**Testi adottati:** cisco.netcada.com e www.v-learning.it

### CONTENUTI DISCIPLINARI

**Certificazione CCNA R&S** (completamento : cap 11-16) – settembre/novembre (29 ore)

Livello Transport (TCP e UDP). Porte logiche (well known, registered e dynamic). 3-way-handshake; 4-way-handshake; affidabilità e controllo di flusso. Confronto tra protocolli best effort e connessi e affidabili.

Servizi di rete e dettagli su alcuni protocolli di livello Application: HTTP, DNS , DHCP.

Hardening dei sistemi: comandi Cisco per la sicurezza dei dispositivi.

Introduzione alla sicurezza informatica.

Ripasso in vista della certificazione: piano di indirizzamento (IPv4 oIPv6), configurazione dei dispositivi intermedi (router e switch) mediante CLI anche da remoto (telnet e ssh)

**VLAN (CLIL)** dicembre/gennaio (22 ore di cui 11 CLIL)

*L0: introduction to VLAN technology; definition and Advantages of subnetting; benefits of VLAN technology*

*L1: Port-based VLAN : access port (untagged)*

*L2: trunk link (tagged) ports. IEEE802.1Q frame*

*L3: inter VLAN routing with L3 subinterfaces.*

*L4: inter VLAN routing with multilayer switch.*

*L 5: introduction to (standard) Access Control Lists.*

ACL su multilayer switch e su router

NAT e port forwarding mediante ACL

DMZ su router Cisco come e introduzione al firewall

## Crittografia febbraio/aprile (24 ore)

Cenni storici: Cifrario di Cesare, Scitila spartana, Vigenere, Enigma.  
Cifrari di flusso e cifrari a blocchi; cifrario perfetto.  
Dettaglio sugli algoritmi DES e AES (modalità EBC o CBC)  
Crittografia a chiave pubblica: principio di funzionamento del "Diffie-Hellman Key Exchange" e del sistema RSA.  
Funzioni di HASH e loro proprietà.  
Confronto tra famiglie crittografiche.  
Firma digitale e HMAC  
HTTPS : TLS handshake e certificati X509. PKI  
PGP e e web of trust.  
Protocolli di Autenticazione challenge/response : Kerberos e EAPoL  
Cenni alla crittografia applicata alle VPN

## Sicurezza informatica, progettazione e configurazione delle reti aziendali - trasversale (19 ore)

Definizione di Sicurezza informatica (CIA). Descrizione di alcune vulnerabilità, relativi attacchi e mitigazioni.  
Hypervisor di tipo 1 e 2. Server LAMP su VirtualBox. Configurazione di base del file server Samba  
Modelli di cloud computing (XaaS).  
Vantaggi della virtualizzazione dell'hardware.  
Servizi di rete e misure per la continuità di servizio. Ridondanza hardware, monitoraggio (IDS/IPS), backup/restore, difesa perimetrale, segmentazione della rete, controllo degli accessi.  
Strumenti per verificare la robustezza delle password (lookup hash tables e attacco del dizionario).  
Cenni alla normativa (GDPR)

## Wireless e IoT maggio/giugno (7 ore)

Problema della stazione nascosta. CSMA/CA. Autenticazione WPA2 Pre-shared-key ed Enterprise con server RADIUS.  
Cenni all'evoluzione del WiFi fino alla 802.11ax .  
Cenni ai Protocolli Zigbee e LoRaWAN per l'IoT.

## PCTO - periodo trasversale (8 ore )

Indicazioni sulla relazione di tirocinio e presentazione dei PCTO. Incontro con ex-studenti ora universitari. Incontri con aziende del campo dell'automazione e IoT. Prova delle presentazioni.

Valdagno, 7 giugno 2024

*Firma degli studenti  
rappresentanti di classe*

\_\_\_\_\_  
\_\_\_\_\_

*Firma dei Docenti*

\_\_\_\_\_  
\_\_\_\_\_