06-03

- Continuazione firewall e tipologie
- Utilizzo NAT: port forwarding e port triggering
- Politiche di accesso e sicurezza

11-03

- Ripasso argomenti in vista della verifica

13-03

- Verifica (1) Generale

15-03

- Recupero verifica per gli assenti
- Access Point, Protocolli di Sicurezza e Hotspot

18-03

- Introduzione al livello applicativo (7)
  - Architettura client-server e peer-to-peer
  - Principali protocolli (HTTP, FTP, SMTP, DNS)
  - Porte well-known

20-03

- Protocollo DNS
  - Spazio dei nomi e domini
  - Risoluzione diretta e inversa
  - Record DNS (A, CNAME, MX, NS)
- Posta elettronica
  - Formato dei messaggi (RFC 822, MIME)
  - Protocolli SMTP, POP3, IMAP
  - Configurazione client di posta
- Trasferimento file e accesso remoto
  - Protocollo FTP e sue evoluzioni (SFTP, FTPS)
  - SSH e confronto con Telnet
  - Esempi di utilizzo con tool a riga di comando

25-03

- Sicurezza informatica e tipologie di attacco
- Hacking etico
- Progettazione reti e rispetto normative vigenti
  - Privacy
  - Framework
- Open source vs closed source software

27-03

- Sicurezza informatica: concetti base
  - Riservatezza, integrità, disponibilità (CIA triad)
  - Vulnerabilità, minacce, attacchi
  - Malware (virus, worm, trojan, ransomware)

29-03

- Tecniche di autenticazione
  - Fattori di autenticazione (qualcosa che sai, possiedi, sei)
  - Autenticazione a più fattori
  - Sistemi biometrici

01-04

- Sicurezza delle reti wireless
  - Protocolli WEP, WPA, WPA2
  - Configurazione sicura di access point
  - Attacchi alle reti wireless (es. WPS attack, evil twin)

03-04

- Sicurezza delle applicazioni web
  - Principali vulnerabilità (es. SQL injection, XSS)
  - Tecniche di prevenzione (input validation, parametrized query)
- Web e HTTP
  - Struttura di una richiesta HTTP
  - Metodi GET, POST, PUT, DELETE
  - Cookie e sessioni
  - Cenni a HTTPS e SSL/TLS

05-04

- Normative sulla privacy e sulla sicurezza
  - GDPR europeo
  - Codice in materia di protezione dei dati personali
  - Standard ISO 27001

08-04

- Open source vs closed source in ambito sicurezza
  - Vantaggi e svantaggi
  - Impatto sulla trasparenza e affidabilità
  - Importanza di codice controllato

10-04

- Anonimato online e darknet
  - Proxy, TOR, I2P
  - Bitcoin e criptovalute
  - Cenni al cybercrime

12-04

- Hacking etico e test di penetrazione
  - Fasi di un pentest
  - Strumenti (es. Nmap, Metasploit)
  - Importanza delle autorizzazioni

15-04

- Gestione degli incidenti di sicurezza
  - Individuazione e contenimento
  - Analisi e ripristino
  - Prevenzione e lessons learned

17-04

- Ripasso generale e approfondimenti
- Preparazione ad un giro di interrogazioni

19-04

- Inizio interrogazioni (4 alla volta)