Programma del corso

Durante il corso saranno affrontati i seguenti argomenti:

- Introduzione e terminologia
- Parte I: Introduzione alla offensive security
    - Richiami concettuali sul sistema Unix
    - L'uso della shell interattiva
    - Introduzione al linguaggio assembler
    - Introduzione allo shell coding
    - I memory error exploit
    - Un esempio di attacco buffer overflow
    - Il Malware
    - Attacchi di rete
- Parte II: Introduzione alla Defensive Security
    - Elementi di crittografia
    - Tecnologie: EDR, Firewall, IDS, SIEM
    - IPSEC, TLS
- Parte III: Elementi di Privacy

Testo di riferimento:

Il corso non adotta un testo particolare, lo studente potrà consultare come testo di riferimento per una serie di approfondimenti il seguente:

> W. Stallings, L. Brownie, "Computer Security: principles and practice", Global Edition, Pearson.

Modalità d'Esame

Il voto finale dell'esame sarà così determinato:

- sino a 5 punti per lo svolgimento degli homework
- sino a 5 punti per lo svolgimento degli esercizi della prova pratica
- sino a 23 punti per la prova orale.

AULE e ORARIO

Il corso di svolgerà con il seguente orario:

- Martedì dalle 14.30 alle 17.30 Aula E presso il Dipartimento di Fisica
- Giovedì dalle 14.30 alle 16.30 Aula V8, Didatteca via Venezian