Cybersecurity

* Slide del corso

Principio del formulario

Final del formulario

[01. Cybersecurity (3.2.1)](https://fad.its-ictpiemonte.it/mod/resource/view.php?id=22741&redirect=1" \t "_blank)

Principio del formulario

Final del formulario

[02. Password management (3.4)](https://fad.its-ictpiemonte.it/mod/resource/view.php?id=22742&redirect=1" \t "_blank)

Principio del formulario

Final del formulario

Lezione 1 - mercoledì 13 aprile 2022

Argomenti trattati a lezione:

* + Il concetto di **sicurezza**: valutazione del *rischio*, la *minaccia*, il *danno* e la *probabilità*.
  + La **sicurezza informatica**: implicazioni e responsabilità a livello *personale*, *aziendale* e *nazionale*.
  + **Cyberwarfare**: la guerra cibernetica e l'esempio del malware *Stuxnet*.
  + La triade **C.I.A.**: *confidenzialità* e *integrità* dei dati, *disponibilità* del servizio.
  + Tipologie di **attacchi informatici**: *attivi* (mascheramento, ripetizione, modifica e DOS) e *passivi* (intercettazione e analisi dei metadati).
  + Tipologie di **attaccanti**: "script kiddies", white/gray/black hat, organizzazioni e hacktivism, le minacce interne all'azienda.
  + **Terminologia** di base: le *vulnerabilità* (zero-day, exploit, rootkit, backdoor)

Principio del formulario

Final del formulario

Lezione 2 - mercoledì 20 aprile 2022

Argomenti trattati a lezione (Blocco slide 1):

* + Differenza tra vulnerabilità software, hardware e dei protocolli;
  + Tipologie di malware: **virus**, **trojan**, **worm**, **ransomware**, **botnet**, **spyware**, **keylogger**, **scareware**;
  + Scenari di attacco estremi: **thermal attack** e **keystroke attack**.

Blocco Slide 2:

* + Il controllo degli accessi: **autenticazione** e **autorizzazione**;
  + Principali tecniche di intrusione: **password di default**, **social engineering**, **attacchi a dizionario**, **attacchi a forza bruta**;

Principio del formulario

Final del formulario

Lezione 3 - mercoledì 27 aprile 2022

Argomenti trattati a lezione (blocco slide 2)

* + Definizione e misura dell'**entropia** di una stringa per la costruzione di una **password casuale**;
  + Calcolo dei **tempi di brute-force** per una password casuale a seconda della lunghezza e dell'alfabeto;
  + Brute-force con **ricerca euristica** quando le password non sono casuali;
  + Il problema del **credential stuffing**: statistiche e problemi derivanti dal riutilizzo delle password;
  + Il **phishing**, le varie tipologie e strumenti di prevenzione;
  + Uso dei **password manager** per gestire in sicurezza le password;
  + Definizione e uso dell'**autenticazione multifattore**.