Hacker è una figura che analizza e studia un sistema modificandone o migliorandone qualcosa in modo creativo. Questo termine nacque nei laboratori del MIT (Massachusetts Institute of Technology) Successivamente, con lo sviluppo dei computer, Unix (primo sistema operativo degli anni 70'), e di ARPANET, alcune figure (come Steve Jobs e Steve Wozniak che facevano parte del Homebrew Computer Club) iniziarono ad esplorare le possibilità che poteva dare il mondo informatico.

Anni '80
Esistono alcuni hacker "sociali" che hanno come scopo, utilizzando ingegneria sociale, di ottenere informazioni personali tramite l'inganno. Come Kevin Mitnick

Anni 2000
In questo periodo ci furono vari episodi di Hacktivismo e Cyberwarfare come quello di Edward Snowden che mise alla luce le pratiche di sorveglianza di massa da parte del governo americano portando a dibattito l'argomento della privacy e della sicurezza.

Withe e Black hat
Gli hacker possono essere divisi in due categorie di colori che si basano su dei principi come:
Con autorizzazione (withe)
Operano hacker che eseguono un accesso esplicito alla rete per poterne testare la sicurezza e sono ingaggiati dalle aziende che vogliono migliorare la propria sicurezza.
Senza autorizzazione (black)
Operano hacker senza il consenso dei proprietari dei sistemi e le loro attività sono considerate illegali e pericolose.
Fine buono (withe)
Gli hacker che utilizzano le loro competenze per scopi positivi e proteggere le organizzazioni migliorandone la sicurezza.
Fine cattivo (black)
Gli hacker che agiscono per creare danni rubando dati, compromettendo la privacy e causando disservizi.

Il pentesting
Il pentesting (penetration testing) è un processo in cui si simulano attacchi informatici contro un sistema o una rete per identificare vulnerabilità di sicurezza ed è composto da alcune fasi:
-Raccolta di informazioni (Reconnaissance)
vengono raccolte informazioni sul target come dominio, indirizzo IP, ecc.
-Scansione
Vengono utilizzati strumenti apposti per trovare le porte aperte, servizi in esecuzioni e vulnerabilità che possono essere sfruttate
-Accesso
Il pentester tenta di sfruttare tutte le vulnerabilità trovate tramite la fase di scansione per avere accesso al sistema
-Mantenimento dell'accesso
dopo l'accesso, il pentester mantiene l'accesso al sistema per ottenere ulteriori informazioni e potervi accedere successivamente
-Analisi e report
Dopo aver completato l'attacco viene fatto un report dettagliato che descrive le vulnerabili e i metodi utilizzati per sfruttarle dando raccomandazioni per mitigare i rischi.

La CIA (Confidenzialità Integrità e Disponibilità)
La sicurezza informatica si basa su questo triangolo di principi (non si possono avere tutti e tre)
Confidenzialità garantisce che le informazioni siano accessibili solo a coloro che sono autorizzati a vederle proteggendo i dati sensibili da accessi non autorizzati.
Come, ad esempio, la **Crittografia** dove i dati vengono convertiti in un formato illeggibile per chi non possiede una chiave di autorizzazione.
Integrità garantisce che le informazioni siano accurate e complete, e che non siano state alterate in modo non autorizzato. Protegge i dati da modifiche indebite.
Come, ad esempio, l'Hashing che ci permette di verificare che le informazioni non siano state modificate perché ad ogni modifica del file, viene modificato anche l'ash.
Disponibilità garantisce che le informazioni e i sistemi siano accessibili agli utenti autorizzati quando necessario e protegge i sistemi da interruzioni.
Ad esempio, sarebbe più opportuno effettuare regolari backup dei dati e avere un piano di ripristino per recuperare rapidamente i dati in caso di perdita.

Virtualizzazione
La virtualizzazione è una tecnologia che consente di creare versioni virtuali di risorse fisiche, come server, storage, reti e sistemi operativi.
Le macchine virtualizzate sono gestite e create dagli **Hypervisor** che possono essere di diverse categorie in base a come interagiscono con l'hardware e il sistema operativo host:
Bare-Metal (hypervisor di tipo 1)
funzionano direttamente sull'hardware fisico senza necessitare di un sistema operativo host. Offrono prestazioni superiori e minori latenze poiché hanno accesso diretto alle risorse hardware.
Hosted (hypervisor di tipo 2)
funzionano sopra un sistema operativo host esistente. Questo sistema operativo host gestisce l'accesso alle risorse hardware, mentre l'hypervisor gestisce le macchine virtuali. (VirtualBox)
Container Docker (hypervisor di tipo 3)
Questo tipo di hypervisor condivide lo stesso sistema operativo host, **ma isolano le applicazioni e le loro dipendenze in ambienti separati** dando anche la possibilità di poter eseguire delle applicazioni che non sarebbero compatibili con un determinato sistema operativo e di proteggere la macchina in caso di attacco proveniente da un determinato software.