DEFENCE IN DEPTH

What is defence in depth?

Defence in depth is a concept used in information security in which multiple layers of security controls are placed throughout an information technology system.

Layers

There are 6 layers of security are:

Physical security

Secure Networks and System

Network security

Data security

Active attacks

Passive attacks

Needs for defence in depth?

Defence in depth helps you ensure that you are protecting your system as effectively as possible. It forces you to account for security even when your various tools and solution have been compromised.

Example:

Host encryption

Anti-virus

Firewall

E-mail gateway

Password management

Password management is a set of principles and best practice to be followed by users while storing and managing password in an efficient manner to secure password as much as they can to prevent unauthorized access.

HoneyPot

A honeypot is a cybersecurity mechanism that uses a manufactured attack target to lure cybercriminals away fromlegitimate targets.they also gather intelligence about the identity,methods and motivations of adversaries.

Multi Factor Auth

Multi-Factor authentication is a layered approach to security data and application where a system requires a user to present a combination of two or more credentials to verify a user’s identity for login.

