# Segmentazione e Segregazione

# Indice

- Tecniche di autenticazione e multi-factor authentication
- Protocolli di autenticazione
- Gestione delle password e dei certificati.
- Modelli e tecniche per autorizzazione e controllo dell’accesso
- Privileged Identity and Access Management (PAM)
- Cenni sulla segregazione e segmentazione delle reti

# Indice

- Tecniche di autenticazione e multi-factor authentication
- Protocolli di autenticazione
- Gestione delle password e dei certificati.
- Modelli e tecniche per autorizzazione e controllo dell'accesso
- Privileged Identity and Access Management (PAM)
- Cenni sulla segregazione e segmentazione delle reti

# Segregazione e segmentazione delle reti

- Analogia con
  - Compartimentazione scafi
  - Compartimentazione ambienti per prevenzione incendi
  - Suddivisione in circuiti di un impianto elettrico
  - ecc.
- Obiettivo: separare in modo fisico o logico parti di rete in modo da regolarne le comunicazioni

# Segregazione e segmentazione delle reti

- **Segregazione**
  sviluppo e applicazione di regole per il controllo della comunicazione fra sistemi

- **Segmentazione**
  partizionamento di una rete in sottoreti

# Realizzazione di segmentazione e segregazione

- A livello di rete, attraverso router, firewall e switch
  - Definizione di reti private in termini di gruppi di indirizzi IP
  - Definizione di regole di accesso a server e host (basate su IP o su gruppi di IP, porta)
- A livello applicativo attraverso virtualizzazione
  - server virtuali
  - reti virtuali (software-defined-networks - SDN)

# Realizzazione di segmentazione e segregazione

- A livello di rete, attraverso router, firewall e switch
  - Definizione di reti private in termini di gruppi di indirizzi IP
  - Definizione di regole di accesso a server e host (basate su IP o su gruppi di IP, porta)
- A livello applicativo attraverso virtualizzazione
  - server virtuali
  - reti virtuali (software-defined-networks - SDN)

# Realizzazione di segmentazione e segregazione

- Principio del *minimo privilegio*
  - Valutare a quale livello effettuare separazione, a partire dal livello fisico fino a quello applicativo

- La segmentazione deve seguire la definizione di livelli di riservatezza di dati e applicazioni

# Realizzazione di segmentazione e segregazione

- Accesso ai sistemi sempre realizzato attraverso specifiche autorizzazioni
  - Approcci *whitelisting* e non *blacklisting*
- Regole per l'accesso alle sottoreti
  - a livello di indirizzi IP e regole di routing
  - basati sullo stato corrente
  - a livello di porta e protocollo

# Segregazione delle applicazioni a maggior rischio

- Quando è preponderante la presenza di dati e applicazioni *sensibili,* può essere conveniente segregare applicazioni e sistemi a maggior rischio
- Utenti che devono accedere a Internet
  - remote desktop di una macchina virtuale opportunamente segregata
- Connessioni verso host interni via macchina virtuale con sistema operativo *hardened*