**OS Security**

La sicurezza di un sistema è determinata da una policy di sicurezza

Immagine che contiene testo

Descrizione generata automaticamente

Il sistema operativo si protegge;

* con spazi di indirizzamento separati per ogni processo
* separazione dei contesti di esecuzione kernel/user
* autenticazione
* controllo accessi(autorizzazione)
* identificazione di minacce e tecniche di difesa.

**Autenticazione e autorizzazione**

Autenticazione: procedura che identifica l’utente sulla macchina

Autorizzazione: processo che determina cosa un utente autenticato può fare sul sistema o rete.

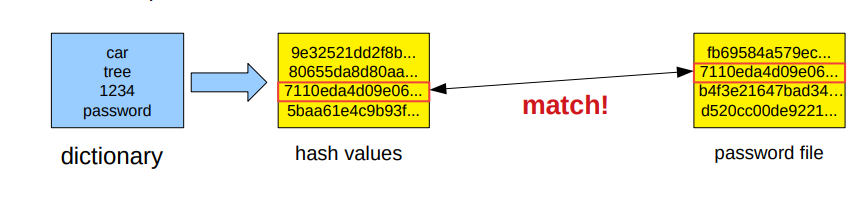
* Tipi di autenticazione:  
  password based auth
* Token based auth
* Biometric auth

le tecniche possono essere combinate.

**Password based authentication**

Hashare le password su db

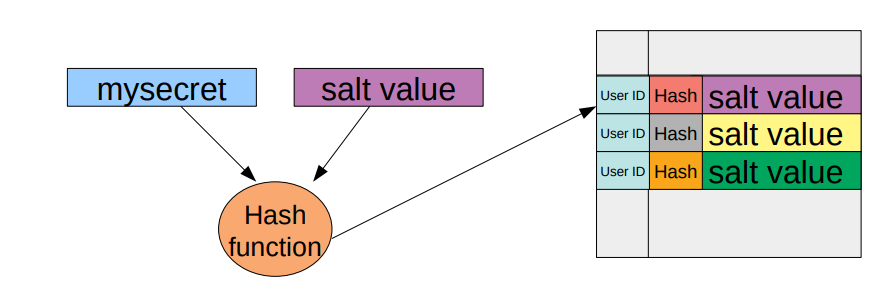
Attenzione che se si hanno gli hash di alcune password si po' capire se l’utente è uguale alla password

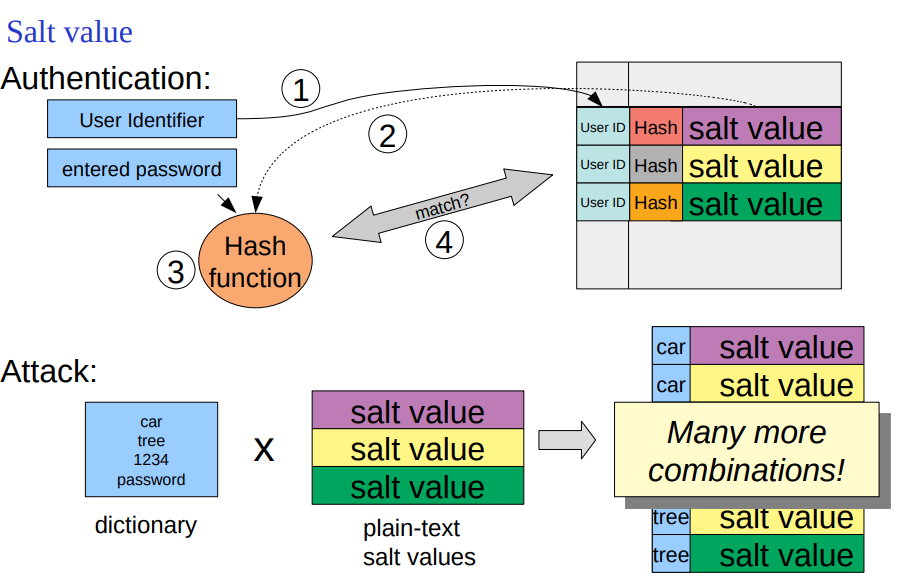


Salt value

Si aggiunge un valore alla password casuale

Si fa l’hash della password e del salt value





Si può effettuare l’hash delle password

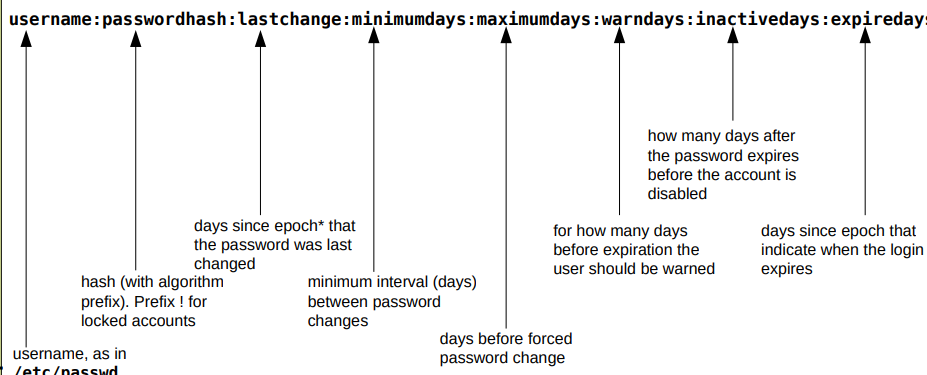
Nei vecchi sistemi unix le password erano in etc/passwd ed era visibile a tutti gli utenti,

struttura:

Immagine che contiene testo

Descrizione generata automaticamenteoggi è su etc/shadow ed è accessibile solo dall’utente root,

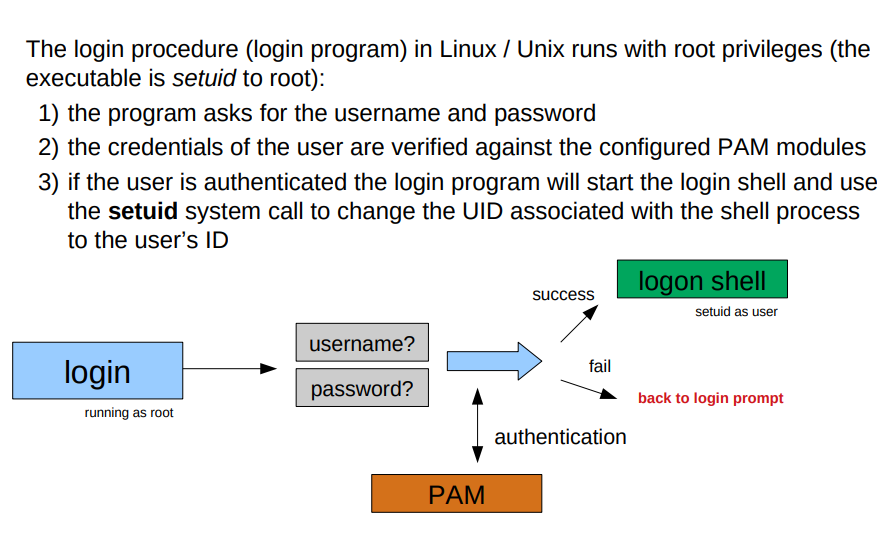
struttura:



**PAM (pluggable authentication modules)**

Immagine che contiene testo

Descrizione generata automaticamente



Challenge response protocol

Immagine che contiene testo

Descrizione generata automaticamente

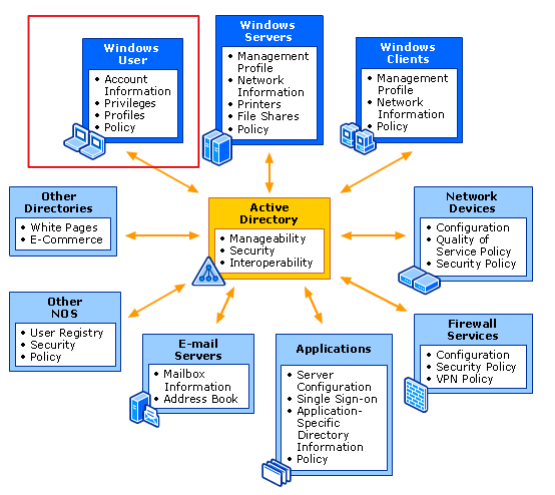
Meccanismo domanda-risposta

Il challenge serve a evitare di utilizzare la stessa autenticazione più volte

KGS!@#$% è fisso

Immagine che contiene testo

Descrizione generata automaticamente



**Kerberos**

È un sistema SSO

Autenticazione mutuale, il server verifica il client tramite certificati

Immagine che contiene testo

Descrizione generata automaticamente

Il passaggio tra i vari servizi si usa un TGT (ticket granting ticket)

Quando si prova a collegarsi ai servizi e si è loggati non si richiede più l’accesso alla infrastruttura di autenticazione ed i servizi non hanno interesse a sapere le credenziali del client, sene occupa il server di autenticazione (KDC).

I servizi verificano il certificato dell’utente.