ATTACCHI COMUNI

Essendo tra i metodi più ricorrenti, i sistemi di autenticazione basati su **password**, sono anche tra i più bersagliati.

Esistono semplici strategie che anche un attaccante con modeste conoscenze può utilizzare per cercare di violare un account.

- Spesso gli utenti poco esperti (talvolta anche i più esperti per pigrizia) tendono ad utilizzare la stessa password per l'accesso in sistemi diversi. Se uno tra questi dovesse accidentalmente essere violato l'utilizzo di una "**password multiuso**", comporterebbe la violazione di tutti i sistemi su cui è stata utilizzata.

- L'attaccante può anche, banalmente, tentare ripetutamente l'accesso con un'altro **ID** (noto), usando alcune tra le password più popolari (es. 123456, 000000, ...) oppure facendo varie permutazioni con le iniziali (maiuscole e minuscole) di nome, username, data di nascita, etc. , dell'utente bersaglio. Per evitare attacchi **mirati** verso particolari utenti, alcuni sistemi implementano dei **meccanismi di blocco**, facendo attendere alcuni minuti prima di ritentare l'accesso dopo un certo numero di tentativi falliti.

- Oltre al già citato (sul retro) attacco a dizionario, troviamo l'attacco con le **rainbow tables** (in italiano "tabelle arcobaleno"). L'idea è quella di usare una grossa quantità di memoria per memorizzare informazioni calcolate una volta per tutte (**tabella di hash precalcolati**), invece di impiegare molto per calcolare sul momento l'hash della password.
  Le tabelle arcobaleno consentono di risalire alle parole chiavi corrispondenti ad un dato hash. Tuttavia, le tecniche avanzate di memorizzazione con **sale** (vedi retro), hanno reso più complicato, a queste tabelle, il raggiungimento dei risultati sperati.

È IMPORTANTE SCEGLIERE DELLE BUONE PASSWORD

Alla luce degli usuali metodi di memorizzazione delle password nei sistemi e dei possibili attacchi, è necessario che gli utenti siano adeguatamente "**addestrati**" e/o **instradati** per la scelta di una buona password.

Per buona password si intende una password che, quanto meno, soddisfi dei requisiti minimi di sicurezza e che quindi è, in principio, più difficile da **violare**.
Per questo, nel tempo, sono stati definiti dei principi di buon senso (codificati tramite semplici regolette) da rispettare quando si crea la password da associare a un account in un sistema digitale.

Talvolta, le linee guida sono insufficienti per assicurare un certo grado di protezione ed è quindi opportuno che l'utente fare si sforzi di impostare, per il suo account, una password meno ovvia e facile da ricordare (vedi brochure "*Password e buone pratiche*").

RIFERIMENTI

➢ http://www.c3t.it/projects/awareness/articoli&brochure/autenticazione_password/

POR FESR 2014-2020 obiettivo Crescita e Occupazione (CreO)

AUTENTICAZIONE BASATA SU PASSWORD

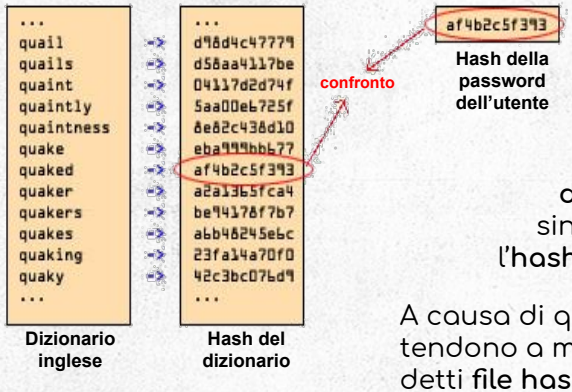
Scopri come e dove sono memorizzate le password nei sistemi informatici, quali sono le vulnerabilità e gli attacchi più comuni

LE PASSWORD

L'autenticazione basata su **password** è il metodo di autenticazione più antico e diffuso. A differenza di altre tecniche, non è stata eliminata dall'uso consuetudinario.

Le password rappresentano un serio rischio per l'integrità delle reti e offrono un punto di attacco facilmente sfruttabile dai malintenzionati per ottenere l'accesso non autorizzato alla rete o un sistema.
Il **furto di credenziali** è spesso citato come catalizzatore di violazioni dei dati che costano alle organizzazioni da migliaia a milioni di danni.

ATTACCHI A DIZIONARIO E MEMORIZZAZIONE (avanzata) NEI SISTEMI



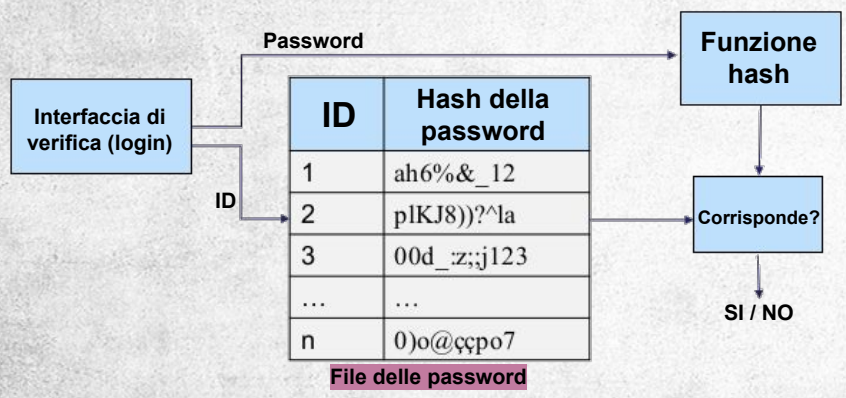
Nel caso tradizionale, la memorizzazione del file delle password con la sola coppia **ID - hash**, lascia far pensare ad un possibile "**attacco a dizionario offline**". In questo tipo di attacco viene usato un file che contiene le parole di un intero dizionario (può essere più o meno conforme al dizionario reale di una certa lingua), partendo da esso si calcola l'**hash del dizionario** (applicando la funzione di hash ad ogni singola parola), e si cerca così una corrispondenza con l'**hash della password dell'utente** bersaglio.

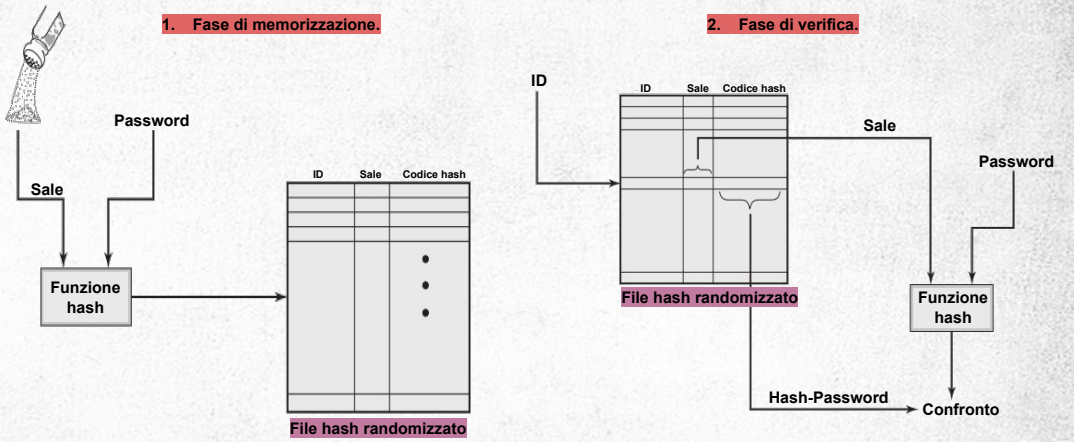
A causa di questa possibile vulnerabilità, oggi i sistemi moderni tendono a memorizzare le password di sistema in quelli che sono detti **file hash randomizzanti**.

MEMORIZZAZIONE (tradizionale) NEI SISTEMI

Per meglio sfruttare la semplicità del meccanismo di autenticazione tramite **password**, è meglio comprenderne nel dettaglio il loro funzionamento, andando ad osservare, in particolare, come avviene la loro memorizzazione all'interno di un generico sistema digitale (prendendo in esame il caso più classico del Personal Computer - PC).

Nel meccanismo tradizionale più classico e generale, in un PC, il sistema memorizza un "**file delle password**".
Contrariamente a quanto può far pensare il nome di questo file, esso non contiene le password vere e proprie associate agli utenti del sistema; bensì contiene una lista di righe con identificativo e valore hash calcolato per la corrispondente password.





Al momento della **memorizzazione** di una nuova password si "aggiunge un pò di sale" alla funzione che calcola l'hash. Si può pensare al **sale** come una piccola quantità generata casualmente dal sistema.
Per ogni **ID** dell'utente si memorizza il **sale** ed il codice **hash** calcolato.

Nella fase di **verifica**, l'utente che vuole autenticarsi fornisce la sua password all'interfaccia (che si assume fidata). Il sistema cerca nel **file hash randomizzato** il **sale** e il **codice hash** corrispondenti all'**ID dell'utente**. Ricalcola il codice hash fornendo sale e password (inserita dall'utente) alla funzione di hash, ed infine confronta se il codice hash ricalcolato e quello recuperato dal file sono uguali.
La randomizzazione ha due scopi principali:

1. prevenire il riconoscimento di password duplicate (poiché i sali saranno diversi);
2. aumentare drasticamente la complessità di un **attacco a dizionario**: l'attaccante dovrebbe, per ogni possibile password del dizionario, fare la prova con tutti i possibili sali.