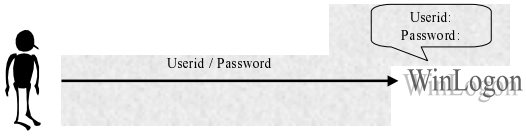
Le password in Windows NT

Speaker:
Francesco Auriemma

Tratteremo

- **Gestione delle password in Windows NT**
- **Differenze rispetto a Unix**
- **Attacchi al database SAM**
- **Alcune tecniche utilizzate per il riconoscimento in rete**
- **Codifica forte**

Password



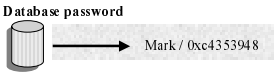
Questo schema, anche se molto utilizzato, è debole perché gli utenti scelgono solitamente delle cattive password (cioè password che possono essere facilmente scoperte) oppure cedono o scrivono password in modo che utenti maliziosi ne possono entrare in possesso.

Password

Ogni sistema che utilizzi una forma di autenticazione attraverso le password, deve memorizzare una rappresentazione della password, in modo da controllare quando un tentativo di logon (locale o attraverso la rete) è consentito.

Di base, ci sono tre modi per memorizzare una password:

Memorizzazione del valore hash della password

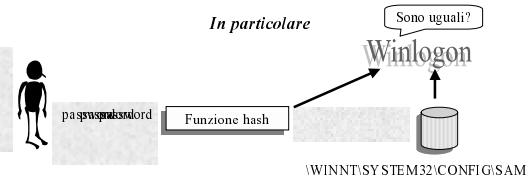


Questo è il metodo che viene utilizzato nei moderni Sistemi Operativi.

Password

Windows NT utilizza questo terzo metodo per memorizzare la password

In particolare



Quindi per rendere valido un logon, il sistema utilizza la password inserita dall'utente, calcola una funzione matematica sul valore inserito e quindi confronta il valore appena calcolato con il valore hash memorizzato nel database delle password.

Funzioni hash

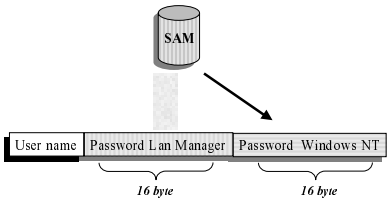
Un fattore importante nella sicurezza delle password è la qualità della funzione hash. Essa è solitamente una funzione irreversibile che genera un unico valore hash per una data password.

Unix

Unix utilizza un algoritmo simile al DES per calcolare il valore hash. La password è utilizzata come una chiave DES (otto caratteri a 7 bit formano una chiave DES a 56 bit) per codificare un blocco binario di zeri. Il risultato di questa codifica è il valore hash. Da notare che la password non è cifrata, ma è la chiave utilizzata per effettuare l'operazione di codifica. Una delle caratteristiche più importanti di UNIX è che esso introduce due caratteri random nell'algoritmo.

Funzione hash di Windows NT

In Windows NT sono memorizzati sul server due valori hash della password: il valore ***Lan Manager*** e il valore ***Windows NT***.

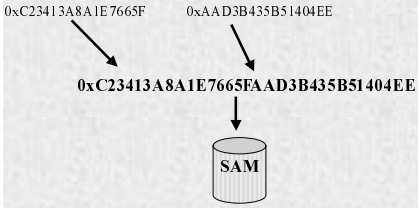


Anche se la dimensione è limitata a **14 caratteri** dalla GUI utilizzata da UserManager.

Lan Manager

1. Lan Manager utilizza una password a 14 byte. Se la password è più piccola di 14 byte, ad essa vengono concatenati degli zeri. Altrimenti viene troncata al 14° byte.
2. La password viene convertita in lettere maiuscole e divisa in due metà di sette byte ciascuna.
3. Aggiungendo un bit di parità viene costruita una chiave DES da ognuna delle due metà di 7 byte costruite in precedenza.
4. Ognuna delle chiavi DES a 8 byte viene utilizzata per codificare un "numero magico" (**0x4B47532140232425** codificato con una chiave di tutti 1).
5. I risultati della codifica del numero magico sono concatenati nel valore hash a 16 byte.

Esempio



La password memorizzata è il risultato della concatenazione di questi due numeri ottenuti cifrando il magic number.

Password locali

Una regolare password Windows NT è ottenuta:

Password locali

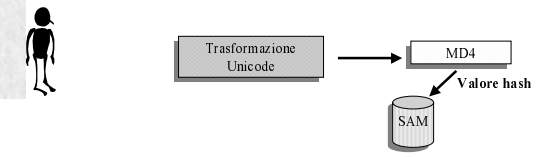
Una regolare password Windows NT è ottenuta:

- Convertendo la password dell'utente in Unicode

Password locali

Una regolare password Windows NT è ottenuta:

- Convertendo la password dell'utente in Unicode
- Utilizzando MD4 per ottenere il valore a 16 byte.

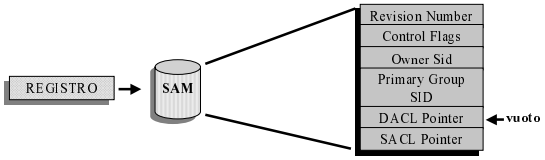


Considerazioni

La cosa interessante è che a differenza di Unix, in cui per il calcolo dei valori hash vengono inseriti degli elementi random in modo che password uguali abbiano valori hash diversi, in Windows NT se due password sono uguali, le funzioni hash genereranno lo stesso valore.

Questo significa che le password sono ***equivalenti***.

SAM

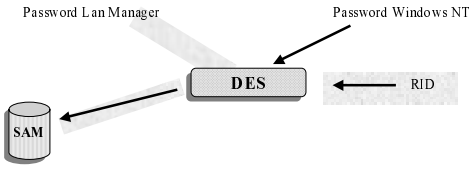


In Windows NT, le informazioni sugli utenti e sulle password sono memorizzate nel SAM che è parte del registro.

Le sottochiavi di SAM sono protette con le Access Control List che negano a tutti (anche all'amministratore del sistema) l'accesso alle informazioni memorizzate.

SAM

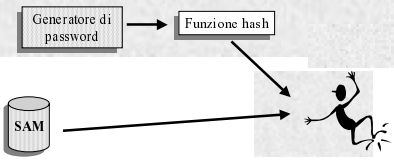
Per dare un ulteriore protezione alle informazioni contenute nel SAM, a queste viene applicata un ulteriore codifica.



Infatti prima di essere memorizzate nel SAM sia la password Lan Manger che la password Windows NT vengono codificati con il DES, utilizzando come chiave un attributo dell'utente (RID).

Attacchi

*Tali sistemi sono vulnerabili ad attacchi chiamati di **forza bruta***



Dato che le funzioni hash sono ben documentate, un hacker può generare tutte le possibili password, calcolare il loro valore hash e confrontare questo valore con il valore memorizzato nel database delle password del sistema.

Attacchi

Gli attacchi di forza bruta condotti contro Windows NT operano nel seguente modo:

Lo stesso procedimento viene ripetuto fino a quando il generatore delle combinazioni non fornisce il valore WELCOME e si scopre che la prima parte della password corrisponde al valore hash appena calcolato.

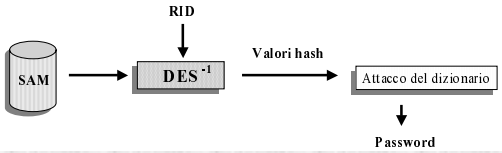
Osservazioni

Il potere computazionale per lanciare un attacco di questo tipo non è generalmente disponibile. In un sistema che utilizza una password formata da 8 caratteri ASCII, ci sono approssimativamente $7{,}2e^{16}$ password possibili. Per cui dato un computer che può generare, calcolare il valore hash e confrontare 1 milione di possibili password al secondo, allora sarebbero necessari 2258 anni per analizzare l'intero spazio delle password.

Solitamente gli utenti scelgono password semplici (pronunciabili) che limitano il numero delle password da generare. Questo ha portato ad un attacco noto come ***attacco del dizionario*** in cui le password da provare sono prese da database contenenti interi dizionari o nomi di automobili sulle quali vengono applicate anche regole di logica.

Attacchi

Dato che in Windows NT i valori hash delle password sono protetti ulteriormente dalla codifica DES, per realizzare un attacco del dizionario bisogna prima decodificare i valori.



La codifica produce i valori hash, ai quali è possibile applicare l'attacco del dizionario.

Attacchi

*Gli attacchi del dizionario condotti contro **Windows NT** operano nel modo seguente:*

- Il contenuto del dizionario viene codificato utilizzando la funzione hash di LanManager.
- Il valore ottenuto viene confrontato con il valore hash della password dell'utente.
- Se viene trovato il match, si cerca di scoprire il valore della password Windows NT , andando a verificare tutte le $2^{|password|}$ combinazioni delle lettere alfabetiche.

Osservazioni

Una limitazione di questi programmi è che per funzionare devono essere eseguiti sotto il contesto di sicurezza dell'amministratore. Infatti per poter leggere la chiave del registro, essi devono cambiare la ACL ad essa associata.

Questo limita enormemente l'utilizzo di questo attacco dato che se un hacker fosse in grado di ottenere i privilegi dell'amministratore, potrebbe fare cose ben peggiori, invece di andare incontro ad un lungo attacco del dizionario

Crack di NT

Dopo aver ottenuto una copia del database SAM, un hacker può dare vita ad un attacco offline di tipo dizionario. Questo implica la generazione di password (solitamente prese da una lista di parole) e l'esecuzione del Lan Manager (DES) o della funzione hash MD4 (Windows NT).

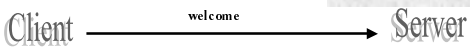
Alcune applicazioni che effettuano questo sono:

Crack 5.0a per NT

Utilizza un algoritmo particolarmente potente ed una lista di parole provenienti da linguaggi diversi. La caratteristica di questa applicazione è che utilizza dei filtri per le parole che aumentano notevolmente lo spazio delle possibili password.

Spiare le password dalla rete

Un altro modo per ottenere le password o informazioni sulle password (valori hash) è spiare la rete (locale o Internet) quando una connessione client/server viene stabilita.



Il protocollo standard SMB, ora utilizzato da Windows NT e Lan Manager, non invia le informazioni sulla password direttamente sulla rete, ma utilizzano un meccanismo di tipo Challenge/Response.

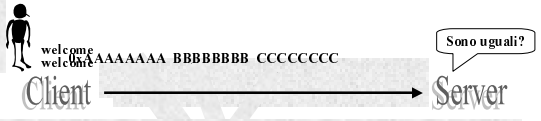
Challenge / Response

Letteralmente Challenge/Response significa Sfida/Risposta

4. Gli 8 byte random (challenge) vengono codificati utilizzando il DES con ognuna delle tre chiavi DES generate in precedenza, ottenendo 24 byte da utilizzare come risposta (la response).
5. Questa risposta viene restituita al server, il quale prende il valore hash dell'utente dal suo database delle password ed effettua gli stessi calcoli.
6. Se il risultato di 24 byte del server è lo stesso della risposta del client il logon ha successo, altrimenti la richiesta viene respinta.

Challenge / Response

Esempio:



Il risultato della codifica viene inviato al Server il quale effettua le stesse operazioni sul valore hash memorizzato nel suo database. Se il risultato coincide con la risposta inviata dal Client, allora il collegamento ha esito positivo, altrimenti viene rifiutato.

Osservazioni

Qualcuno che spia la rete intermediaria vede soltanto gli 8 byte della sfida e i 24 byte della risposta.

Sfida
0x0001020304050607

Risposta
0xAAAAAAAABBBBBBBBCCCCCCCC

Password
0xC23413A8A1E766 AC435F2DD90417 CCD60000000000

Se la password non è più piccola di 8 byte, allora è comunque possibile scoprire gli ultimi due byte del valore hash della password generando tutti i possibili valori(65535), codificando la sfida e confrontando il risultato con la risposta restituita.

Client modificato

Questo porta ad un attacco chiamato del Client modificato

È da osservare che il Client ha ottenuto questo senza conoscere il valore originale (il testo in chiaro) della password. Questo significa che anche una buona password (cioè una password che è resistente all'attacco del dizionario) può essere utilizzata in modo sbagliato.

Firma dei pacchetti

Un modo per evitare un attacco di questo tipo è mediante la firma dei pacchetti.

In questo modo, i Client e i Server sono sicuri che le parti ai due estremi della comunicazione sono realmente quelli che hanno detto di essere.

Codifica forte

- La codifica forte protegge le informazioni sugli account codificando i dati sulle password utilizzando una chiave crittografica random a 128 bit, chiamata ***password encryption key***
- La password encryption key è essa stessa codificata utilizzando una chiave di sistema (***System key***)

Codifica forte

La chiave del sistema è definita utilizzando il comando Syskey.exe che può essere eseguito soltanto dai membri del gruppo dell'amministratore. Questa utility viene usata per inizializzare o cambiare la chiave del sistema.

Ci sono tre modi per gestire la chiave del sistema

3

Utilizzare una password scelta dall'amministratore per derivare la chiave del sistema.

Solitamente viene utilizzato MD5 della password come chiave principale per proteggere la chiave di codifica delle password.

Codifica forte

La chiave del sistema è definita utilizzando il comando Syskey.exe che può essere eseguito soltanto dai membri del gruppo dell'amministratore. Questa utility viene usata per inizializzare o cambiare la chiave del sistema.

Ci sono tre modi per gestire la chiave del sistema

3

Utilizzare una password scelta dall'amministratore per derivare la chiave del sistema.

Solitamente viene utilizzato MD5 della password come chiave principale per proteggere la chiave di codifica delle password.

Codifica forte

La codifica forte può essere configurata in maniera del tutto indipendente sul Primary e ogni Backup Domain Controller. Ogni controllore di dominio dovrebbe avere un'unica chiave di codifica della password ed un'unica chiave di sistema.

Per esempio

- Prima di abilitare la codifica forte su un PDC, si deve garantire che un BDC completamente aggiornato sia disponibile per essere utilizzato fino a quando i cambiamenti del PDC non sono completati e verificati.

Gestione delle password