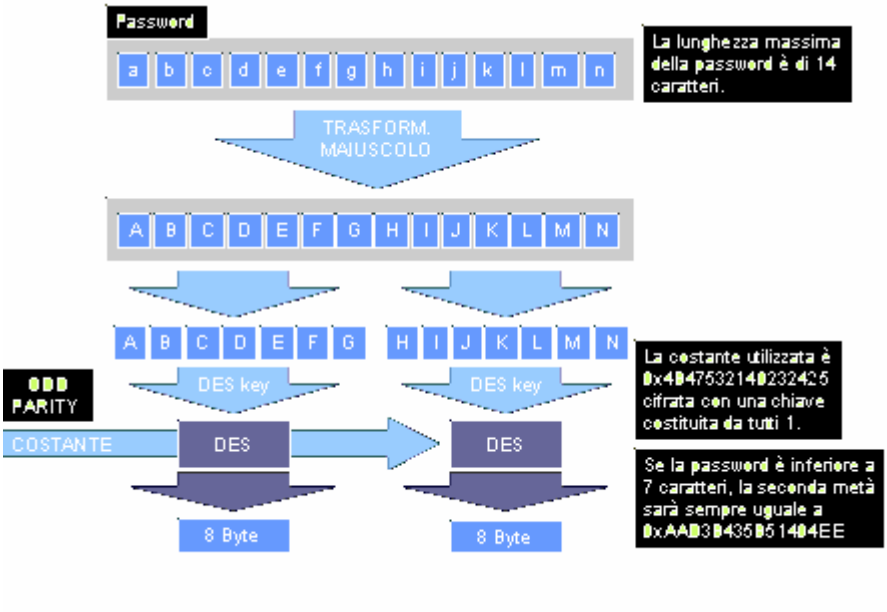
Lan Manager (LM)

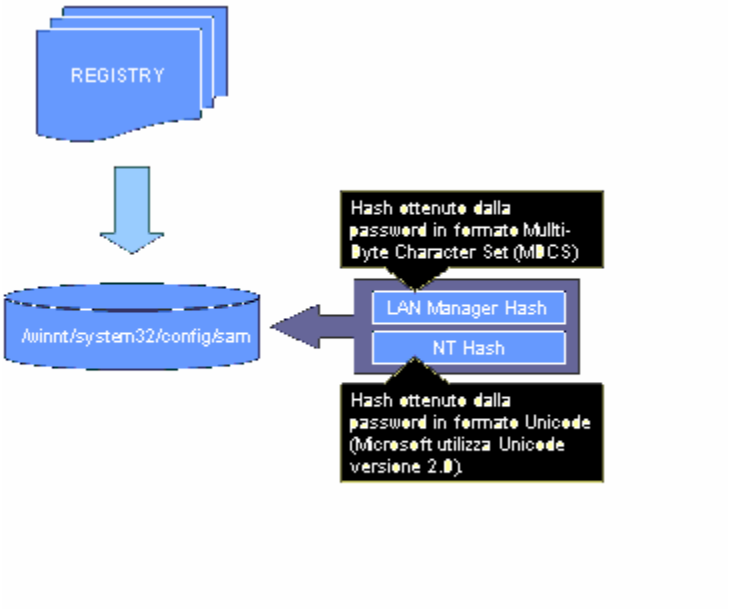
Il procedimento utilizzato per l'autenticazione Lan Manager è il seguente:

- la lunghezza massima della parola chiave consentita dall'algoritmo è di 14 caratteri di tipo OEM, se quella scelta dall'utente è inferiore a questo valore, verranno concatenati degli zeri fino al raggiungimento del numero dei caratteri previsto. Se invece è più lunga, avverrà un troncamento al quattordicesimo carattere;
- i caratteri alfabetici costituenti la parola chiave verranno convertiti in lettere maiuscole e la stringa ottenuta verrà suddivisa in due metà di sette caratteri ciascuna;
- dalle due metà ottenute al passo precedente, verranno costruite due chiavi DES aggiungendo un bit di controllo (disparità);
- ognuna delle chiavi DES a 8 byte verrà quindi utilizzata per cifrare in modalità ECB un “numero magico”, 0x4B47532140232425 corrispondente alla stringa "KGS!@#$%", precedentemente cifrato con una chiave di tutti uno;
- se il numero dei caratteri componenti la password è uguale o inferiore a sette, la seconda parte sarà sempre uguale a 0xAAD3B435B51404EE.
- i risultati ottenuti dalle precedenti elaborazioni verranno concatenati in modo da ottenere il valore finale Lan Manager a 16 byte

In pratica, semplificando:



Per terminare, i dati ottenuti, verranno cifrati con l'algoritmo DES in modalità ECB oppure, se si utilizza MS Windows NT 4.0 con SysKey oppure MS Windows 2000, con l'RC4 e come chiave il RID dell'utente. Fatto questo, il tutto verrà memorizzato all'interno del registro di configurazione seguito dal risultato della relativa elaborazione dell'NT Hash.



Verifica della password

Per verificare la robustezza delle password, basterà utilizzare il programma pwdump2 e la versione a linea di comando del programma L0phtCrack.
Il risultato sarà qualcosa di simile:

```
C:\>pwdump2 > dump.txt
C:\>type dump.txt
administrator:500:e52cac67419a9a224a3b108f3fa6cb6d:
8846f7eaee8fb117ad06bdd830b7586c:::

C:\>lc_cli -p dump.txt -w wfile.txt
User: [administrator] Lanman PW: [PASSWORD] NT
dialect PW: [password]
```

Il programma pwdump3 espande le capacità di pwdump2 permettendo l'estrazione delle credenziali di tutti gli utenti da un sistema remoto, previa connessione alla condivisione amministrativa ADMIN$, per fare ciò è necessario possedere quindi i relativi diritti di amministratore affinchè l'operazione abbia esito positivo.
Esempio:

```
C:\pwdump3v2>net use \\pro2k-01\ADMIN$
The password or user name is invalid for \\pro2k-
01\ADMIN$.

Enter the user name for 'pro2k-01': Administrator
Enter the password for pro2k-01:
The command completed successfully.


C:\pwdump3v2>pwdump3 pro2k-01 pro2k-01.txt

pwdump3 (rev 2) by Phil Staubs, e-business
technology, 23 Feb 2001
Copyright 2001 e-business technology, Inc.
...
Completed.

C:\pwdump3v2>type pro2k-01.txt
Administrator:500:<LAN MANAGER HASH>:<NTLM HASH>:::
```