ACCEDERE A WINDOWS XP SENZA SAPERE LA PASSWORD

evilsocket
http://www.evilsocket.net

.: Introduzione

Molto spesso necessitiamo di accedere ad un computer windowz protetto da password, password che magari non sappiamo perchè ce la siamo dimenticata o magari perchè il pc non è ... ehm ... non è esattamente nostro XD .
In questo paper vedremo come poter risolvere questo problema tramite BackTrack, una distribuzione GNU/Linux live, quindi avviabile da cd, con un set mostruoso di strumenti di penetration test .

.: All'opera

Prima di tutto scarichiamo la iso di backtrack dal sito http://www.remote-exploit.org/ e masterizziamola su un cd vuoto .
Inseriamo il cd nella macchina windows in questione, resettiamola e facciamo il boot del cd .

All'avvio di backtrack usiamo le credenziali di default per entrare

username : root
password : toor

e facciamo partire il desktop manager con il comando 'startx' .

A questo punto, dobbiamo identificare la partizione NTFS dove risiede il sistema windows, per fare questo apriamo la console e digitiamo il comando 'mount' che stamperà una lista delle partizioni montate in automatico da backtrack .

Avremmo un output di questo tipo

```
/dev/sda5 on / type auto (rw)
...
/dev/sda1 on /mnt/sda1 type ntfs (ro,noatime)
...
```

come possiamo vedere la partizione /dev/sda1 è di tipo ntfs, quindi è lei !
Ma c'è un problema, di default le ntfs vengono montate in sola lettura (ro,noatime) mentre noi dobbiamo poterci scrivere .
Niente paura, basta rimontare la partizione con il modulo ntfs-3g dando i seguenti comandi

```
umount /dev/sda1
mkdir /mnt/windowz
mount -t ntfs-3g /dev/sda1 /mnt/windowz
```

così facendo dovremmo avere la partizione scrivibile montata nella directory da noi creata '/mnt/windowz', per verificare ridiamo il comando mount

/dev/sda1 on /mnt/windowz type ntfs (rw,noatime)

e notiamo che stavolta c'è il flag 'rw' ovvero sia lettura che scrittura .

Ora dobbiamo individuare il file SAM delle password di windows ... il path è 'WINDOWS/system32/config/SAM' .

E' ora di mettere mano alla mitica applicazione chntpw, che ci permetterà di modificare questo file impostando le password di sistema a nostro piacimento .

Prima di tutto cerchiamo la lista degli utenti di windows, quindi digitiamo

```
chntpw -l /mnt/windowz/WINDOWS/system32/config/SAM
```

il che ci darà un output di questo tipo

```
RID: 01f4, Username: <Administrator>
...
RID: 03ee, Username: <paperino>
RID: 03ef, Username: <pippo>
...
RID: 01f5, Username: <Guest>, *BLANK password*
```

Non ci rimane che decidere con quale utenza vogliamo entrare ... ma io sono un indovino sapete ? E so per certo che in questo momento starete pensando di usare l'account Administrator ! :D

Eheh scherzi a parte, per cambiare la sua password digitiamo

```
chntpw -u Administrator /mnt/windowz/WINDOWS/system32/config/SAM
```

o semplicemente

```
chntpw /mnt/windowz/WINDOWS/system32/config/SAM
```

dato che l'account di amministrazione è quello che il programma usa di default se non ne viene specificato uno da linea di comando .
Quando chntpw ce lo chiede digitiamo la nuova password et violà ! Possiamo riavviare il pc, far caricare windows ed entrare dentro il sistema con la password che abbiamo impostato pocanzi ^^ .

NOTA : Questo metodo è tanto efficace quanto invasivo, dato che l'utente al quale cambierete la password non sarà più in grado di accedere al sistema, quindi usatelo solo in casi di estrema necessità .

evilsocket