John the ripper ed il crack delle pass di windows.

Ecco un sunto di come utilizzare john the ripper per provare a forzare le pass di un sistema windows non appartenente ad un dominio aziendale. Si tratta di un semplice sunto, molti punti non sono esposti.
Come prima cosa dobbiamo procuraci l'hash della password. Utilizzeremo il programma pwdump7 . Non mi dilungo sulla maniera di utilizzare tale programma. La rete e' piena di esempi. Ecco un ipotetico output di pwdump7

```
Administrator:500:NO PASSWORD*********************:31D6CFE0D16AE931B73C59D7E0C089C0:::
Guest:501:NO PASSWORD*********************:NO PASSWORD*********************:::
HomeGroupUser$:1002:NO PASSWORD*********************:2844A212BEE5F93FFE741D9355BCCA83:::
UT01:1004:NO PASSWORD*********************:NO PASSWORD*********************:::
UT02:1005:NO PASSWORD*********************:NO PASSWORD*********************:::
UT03:1006:NO PASSWORD*********************:NO PASSWORD*********************:::
poldo:1007:NO PASSWORD*********************:F492D5D64020D1E6CF36E6BF1E8F4EF1:::
```

Come vedete in questa prova, il sistema windows ha 3 utenti : UT01 , UT02, UT03, e c'e' anche l'utente administrator. Ora dobbiamo procurarci john the ripper. Lo troviamo all'indirizzo internet

https://www.openwall.com/john/

Sono presenti le versioni per linux e per windows. Inoltre e' possibile utilizzare la distribuzione linux kali , al cui interno vi e' john the ripper gia' installato. Gli esempi qui sotto proposti sono stati provati su un windows 7 pro.
Scaricato john the ripper, bisogna estrarre l'archivio, ottenendo la directory

john-1.9.0-jumbo-1-win64

All'interno di detta directory abbiamo tre sottodirectory, rispettivamente "doc" , "etc" , "run" . L'eseguibile john.exe si trova all'interno di "run" . Ed e' in questa posizione che copieremo il file di output di pwdump7. Assegniamo a questo file il nome ipotetico di dump.txt . Ora inizia la fase di forzatura vera e propria.

john.exe –single dump.txt

> l'elaborazione e' rapidissima, e purtroppo inconcludente.

john.exe –incremental dump.txt

> l'elaborazione potrebbe durare anche settimane, e non e' affatto garantito che si riesca a forzare una pass

john.exe –incremental –fork=3 –session=s1 dump.txt

come sopra, ma indichiamo a john di usare tre core della cpu, ed indichiamo espressamente la sessione attuale col nome “ s1 “ . se interrompessimo john, potremmo riprendere l’elaborazione dal punto ove e’ stata interrotta, tramite l’opzione –restore=s1

john.exe –incremental –fork=3 –progress-every=20 dump.txt

come sopra, ma chiedendo a john di mostrarci ogni 20 secondi la percentuale di elaborazione , ed anche una stima sul tempo rimanente al termine.

Ora vediamo l’utilizzo del file dizionario. Si tratta di un file da creare personalmente, al cui interno inserire le parole da passare a john come base di attacco. Detto file dizionario dal nome ipotetico “ dizionario.txt “ deve essere un file di testo piano, ordinato alfabeticamente, contenente il maggior numero possibile di parole, anche di senso non compiuto, utilizzabili come base di attacco. John utilizzera’ le parole presenti all’interno del file dizionario.txt , eventualmente applichera’ delle varianti, e provera’ a forzare le password. Nelle mie prove ho creato un dizionario di oltre 15 milioni di parole, contenente tutti i nomi e cognomi italiani, tutte le nazioni del mondo, tutti i fiumi e tutti i monti del mondo, tutti i laghi del mondo, tutte le combinazioni di 3 lettere , di 4 lettere , di 5 lettere e di 6 lettere. Nonostante cio’, rimane poco probabile trovare una password, a condizione che sia stata generata con un minimo di accortezza.

John.exe –fork=3 –progress-every=20 –rules=all –wordlist=dizionario.txt –dump.txt

john provera’ a craccare le pass utilizzando come base il contenuto del file wordlist.txt , ed applicando tutte le regole presenti nel file di configurazione john.conf

john.exe –fork=3 –wordlist=dizionario.txt –mask=?u –dump.txt

come sopra, ma l’opzione –mask=?u dice a john di forzare una lettera maiuscola in prima posizione.

John.exe –fork=3 –wordlist=dizionario.txt –mask=?u?w?d dump.txt

come sopra, dicendo a john di utilizzare in prima posizione una lettera maiuscola, aggiungere la parola presa da “ dizionario.txt “ ed aggiungere un numero. La parola cosi’ ottenuta e’ la base per il crack.

Non intendo aggiungere altro, poiche’ sono molto deluso da john the ripper. Nelle mia abbondanti prove ha trovato solo le password piu’ semplici e banali. La password

“ Italia2020 “ , non e’ stata forzata neppure con oltre tre settimane di funzionamento ininterrotto. Dopo questa delusione, ho deciso di abbandonare lo studio del programma.