



UNIVERSITÉ
DE LORRAINE

UFR MATHÉMATIQUES INFORMATIQUE
MÉCANIQUE ET AUTOMATIQUE

MASTRANTONIO
CALOGERO

Progetto Network Security (Software Studio TrueCrypt)

Questo rapporto si propone di spiegare l'uso di TrueCrypt e studiare la sua sicurezza



TRUECRYPT

Sommario

Introduzione	2
Fine del supporto	2
Nota importante.....	3
Scelta di ambiente	3
➤ Essere Linux e in particolare Kali Linux.....	3
➤ Utilizzare la versione 7.1 TrueCrypt	4
➤ Utilizzare TrueCrack 3.0.....	5
Creare un blocco cifrato e selezionare le opzioni	6
➤ Prima di tutto scegliere una posizione "slot"	6
➤ Quindi fare clic su « Create Volume »	6
➤ Per un facile utilizzo, lasciare la scelta di default	7
➤ Selezionare il nome del blocco cifrato	7
➤ Selezionare l'algoritmo di crittografia e l'algoritmo di hash	8
➤ Impostazione la dimensione del blocco da cifrare	9
➤ Creare una password.....	10
➤ Format Options.....	10
➤ Volume Format.....	11
Come utilizzare TrueCrack per tentativo di trovare la password.....	12
Risultato.....	13
Conclusione	15

Introduzione

TrueCrypt è un noto programma applicativo open source usato per la crittazione on-the-fly di interi dischi rigidi o loro partizioni (OTFE/On-the-fly-Encryption). Lo sviluppo è terminato nel maggio 2014.

Crea un disco criptato virtuale in un file (contenitore) che può essere montato come un disco vero. Dalla versione 5 è capace di crittare la partizione di avvio (Boot) di Windows o un intero disco di avvio.

Dalla versione 6 può creare ed eseguire un hidden disk, nascosto all'interno della partizione crittata principale, la cui esistenza è impossibile da provare (negabilità plausibile).

È distribuito sotto la licenza TrueCrypt Collective, ed è disponibile per sistemi operativi Windows, Mac OS X e GNU/Linux.

Sono disponibili molti language pack, anche se alcuni ancora incompleti, per la versione Windows.

Gli algoritmi supportati da TrueCrypt sono l'AES il Serpent e il Twofish. È possibile però usarli in cascata (avendo così maggiore sicurezza), ad esempio: AES-Twofish, AES-Twofish-Serpent, Serpent-AES, Serpent-Twofish-AES e Twofish-Serpent.

Con la versione 7.0 TrueCrypt supporta l'accelerazione hardware per la cifratura e decifratura AES, utilizzando le apposite istruzioni di cui le CPU Intel Core i7/i5 dispongono.

La versione 7.1 del software è sotto auditing per verificarne la sicurezza. Ad aprile 2014 è stato rilasciato un riassunto dei risultati parziali di questa ricerca: non sono stati evidenziati problemi significativi.

Fine del supporto

Il 28 maggio 2014 i developers hanno annunciato la fine del supporto e dello sviluppo di TrueCrypt. L'ultima versione rilasciata, la 7.2, non permette di creare nuovi volumi cifrati, ma solo il montaggio degli stessi, ovvero l'accesso in lettura/scrittura dei volumi creati con versioni precedenti. Per la creazione di volumi cifrati è necessario l'utilizzo della versione 7.1.

Nota importante

Nonostante il rumore che questo ha causato e fino a prova contraria, TrueCrypt è sempre affidabile.

Qui non chiediamo se TrueCrypt è danneggiato o meno, l'obiettivo è quello di valutare il software per quello che è, vale a dire cifrare (una parte del disco, ecc ...) per proteggere le informazioni.

Scelta di ambiente

Per lavorare su mio soggetto ho deciso:

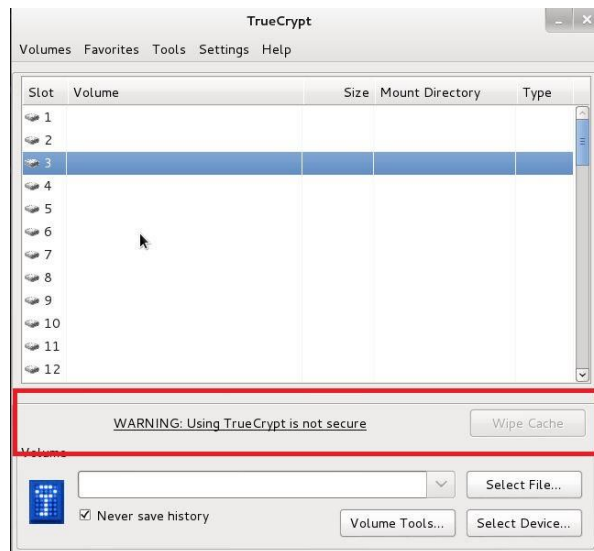
- Essere Linux e in particolare Kali Linux

```
root@Kalo:~# lsb_release -a
No LSB modules are available.
Distributor ID: Debian
Description:    Debian GNU/Linux Kali Linux 1.0.9
Release:        Kali Linux 1.0.9
Codename:       n/a
root@Kalo:~#
```

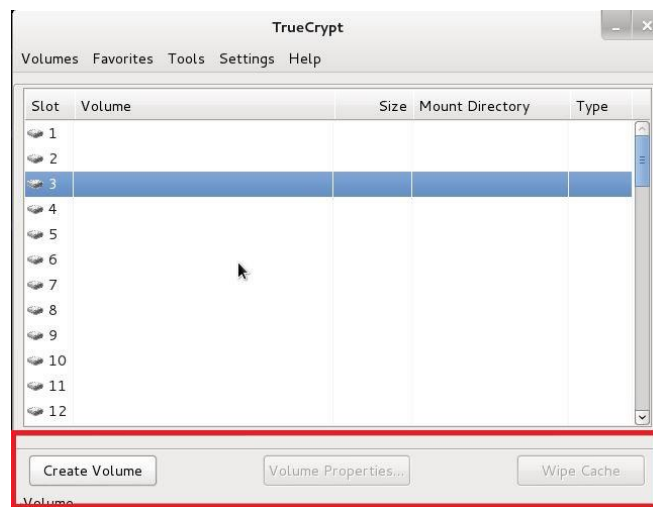
Per i miei test TrueCrypt avevo bisogno di essere su Linux e il fatto di utilizzare Linux Kali è stato grande perché il software aggiuntivo stavo usando "TrueCrack" base già installata.

➤ Utilizzare la versione 7.1 TrueCrypt

Esiste una versione 7.2 (l'ultima), ma (Linux) non mi permette di creare partizioni.



Mentre 7.1 si.



➤ Utilizzare TrueCrack 3.0

```
root@Kali:~# truecrack -v
TrueCrack v3.0
Website: http://code.google.com/p/truecrack
Contact us: infotruecrack@gmail.com
Bruteforce password cracker for Truecrypt volume. Optimized with Nvidia Cuda technology.
Based on TrueCrypt, freely available at http://www.truecrypt.org/
Copyright (c) 2011 by Luca Vaccaro.
```

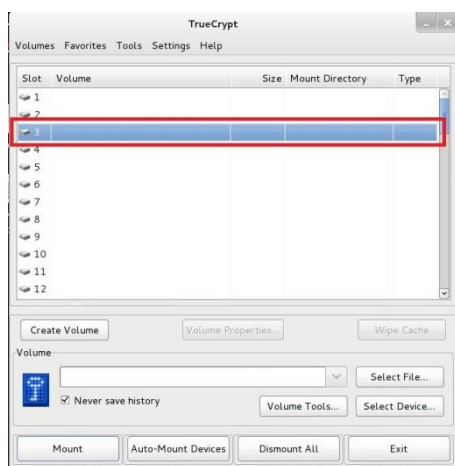
TrueCrack permette di decifrare le password. L'applicazione utilizza un metodo di forza bruta per tentare di trovare la password su base dizionario. TrueCrack è ottimizzato CUDA e supporta quindi nVidia GPU. Offre così un calcolo di potenza dieci volte riducendo la fase di ricerca di un fattore 20 a seconda della complessità della password.

Non vi è alcun motivo particolare per utilizzare questa versione, ma come è già installato sul mio Kali Linux ed è non vi era alcun motivo per cambiare.

Creare un blocco cifrato e selezionare le opzioni

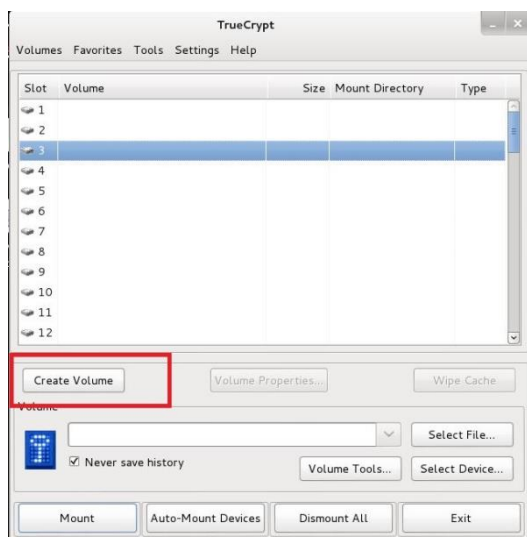
Per una migliore comprensione e facilità di scrittura vi spiegherò come montare un blocco cifrato con la gamma di opzioni che presenterò per evitare la ridondanza in questo rapporto.

- **Prima di tutto scegliere una posizione "slot"**

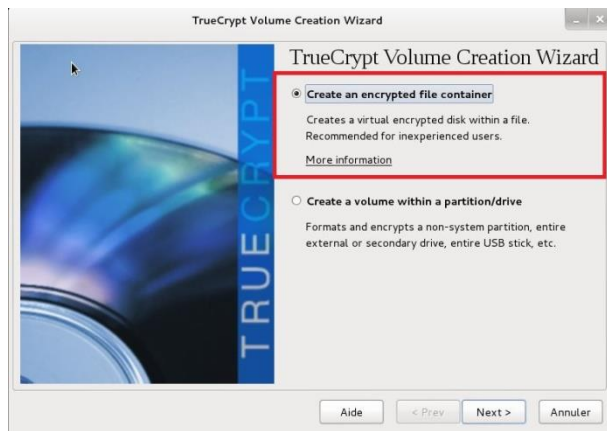


(La scelta del numero non ha importanza)

- **Quindi fare clic su « Create Volume »**

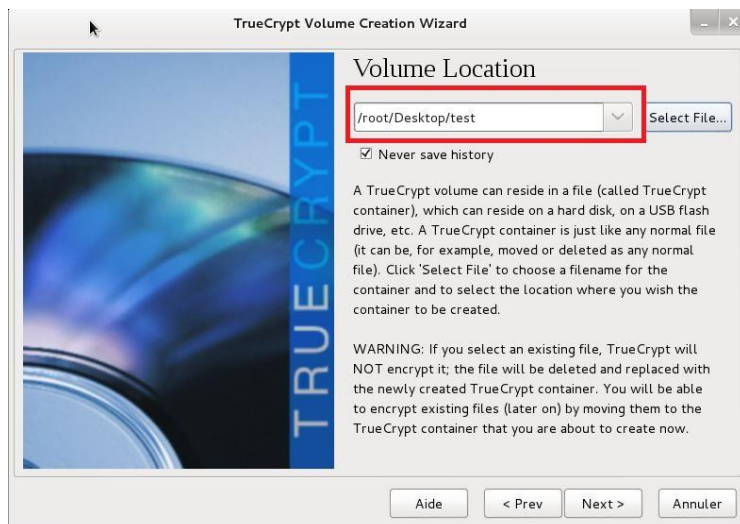


- **Per un facile utilizzo, lasciare la scelta di default**



- **Selezionare il nome del blocco cifrato**

Devi dare il blocco della strada, con l'ultima parola come il nome del blocco cifrato.



➤ **Selezionare l'algoritmo di crittografia e l'algoritmo di hash**

Per il nostro progetto è qui che saranno effettuate le scelte e studiate. Anzi metteremo a confronto i tipi di algoritmi e tipi di hash per verificare se una determinata password, è meglio concentrarsi una scelta piuttosto che un'altra.

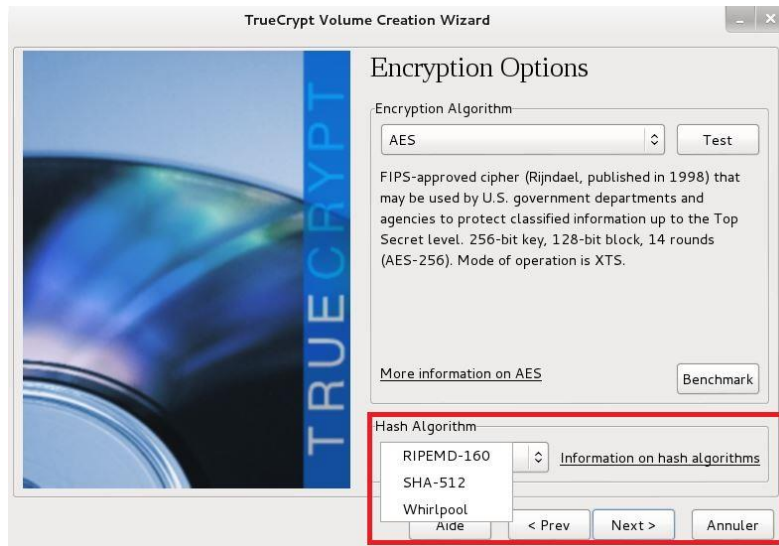
TrueCrypt ci offre una scelta di 8 algoritmo per crittografare

- AES
- Serpent
- Twofish
- AES-Twofish
- AES-Twofish-Serpent
- Serpent-AES
- Serpent-Twofish-AES
- Twofish-Serpent



E 3 algoritmi per hashing :

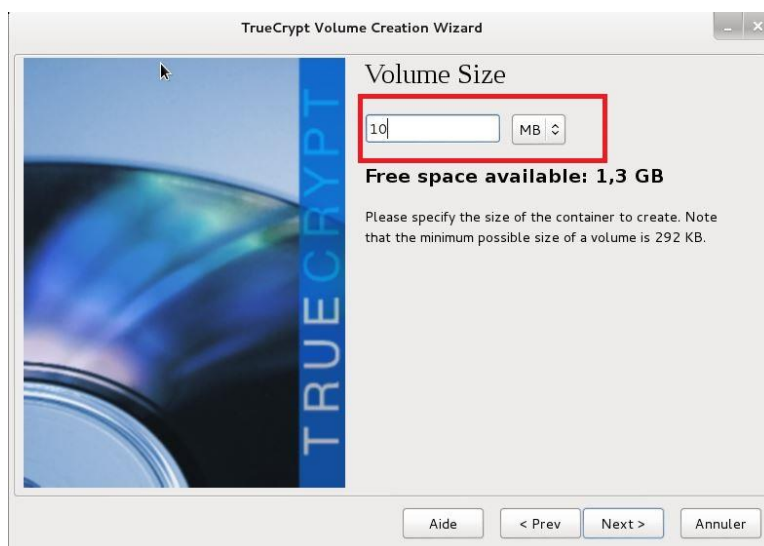
- RIPEMD-160
- SHA-512
- Whirlpool



Per finire il tutorial che ho scelto AES e RIPEMD-160 (cliccare “next” per passare alla fase successiva)

➤ **Impostazione la dimensione del blocco da cifrare**

Inserire il numero desiderato e scegliere il formato tra KB, MB, GB



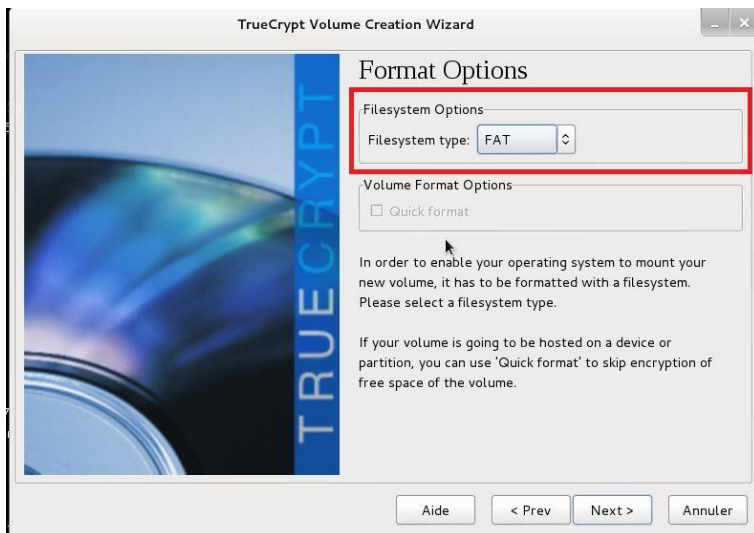
➤ Creare una password

La scelta di una buona password è molto importante.



➤ Format Options

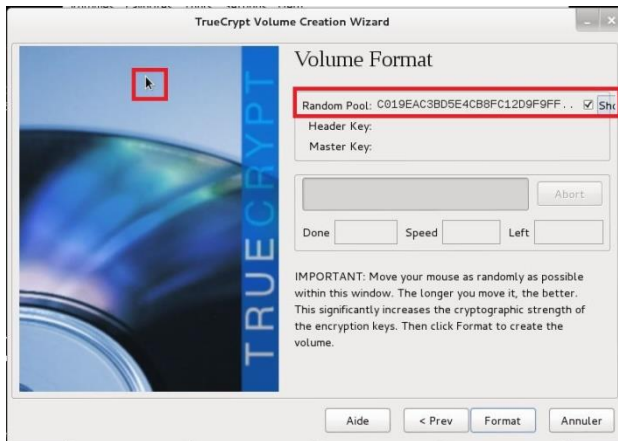
Scegliere il default (FAT) è il più utilizzato.



➤ Volume Format

Muovi il mouse permette a caso per rendere più difficile la crittografia vulnerabile.

Quindi, più si sposta il meglio del mouse sarà il risultato.



Questo sta creando un blocco cifrato è completata.

Come utilizzare TrueCrack per tentativo di trovare la password

Per utilizzare TrueCrack deve essere 2 cose. Conoscendo il blocco modo crittografato e hanno un attacco dizionario.

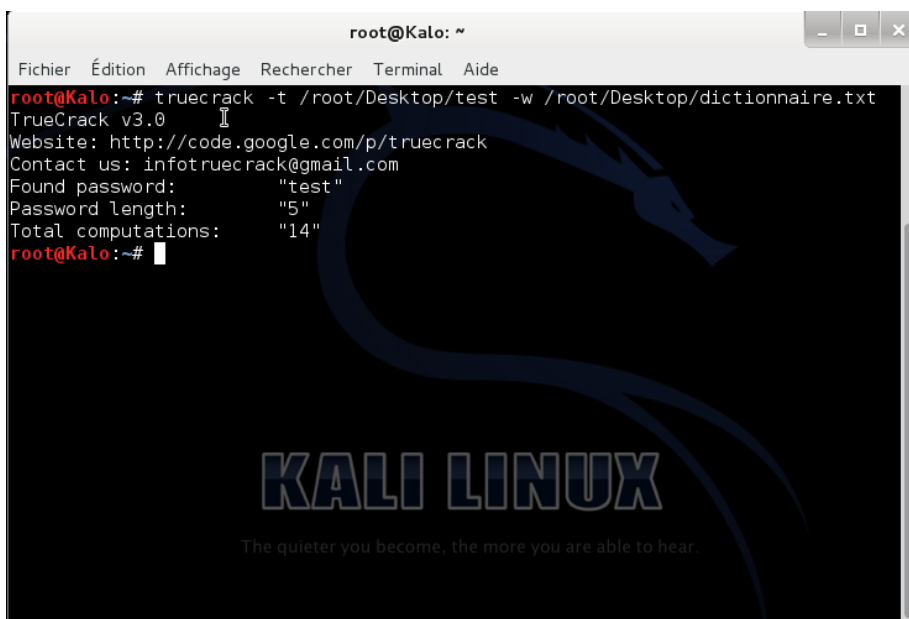
Il -t diciamo che si tratta di un blocco TrueCrypt criptato

Il -w diciamo usiamo l'attacco dizionario

Il percorso che termina con /test è il percorso del blocco cifrato.

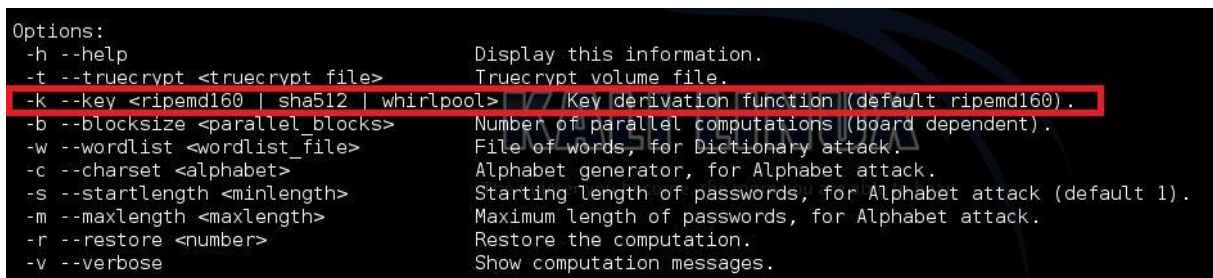
Il percorso termina con /Dictionnaire è il modo (attacco del dizionario)

In questo esempio TrueCrack trovare la password.



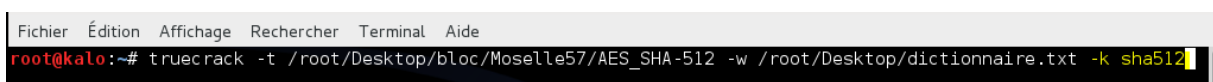
```
root@Kalo: ~  
Fichier Édition Affichage Rechercher Terminal Aide  
root@Kalo:~# truecrack -t /root/Desktop/test -w /root/Desktop/dictionnaire.txt  
TrueCrack v3.0  
Website: http://code.google.com/p/truecrack  
Contact us: infotruetrack@gmail.com  
Found password: "test"  
Password length: "5"  
Total computations: "14"  
root@Kalo:~#
```

Il -k permette di testare in base al hash che vogliamo.



```
Options:  
-h --help Display this information.  
-t --truecrypt <truecrypt file> Truecrypt volume file.  
-k --key <riplemd160 | sha512 | whirlpool> Key derivation function (default ripemd160).  
-b --blocksize <parallel_blocks> Number of parallel computations (board dependent).  
-w --wordlist <wordlist_file> File of words, for Dictionary attack.  
-c --charset <alphabet> Alphabet generator, for Alphabet attack.  
-s --startlength <minlength> Starting length of passwords, for Alphabet attack (default 1).  
-m --maxlength <maxlength> Maximum length of passwords, for Alphabet attack.  
-r --restore <number> Restore the computation.  
-v --verbose Show computation messages.
```

Esempio: ci prova l'algoritmo di hash SHA512 in opzionale



```
Fichier Édition Affichage Rechercher Terminal Aide  
root@Kalo:~# truecrack -t /root/Desktop/bloc/Moselle57/AES_SHA-512 -w /root/Desktop/dictionnaire.txt -k sha512
```

Risultato

Come accennato in precedenza nella relazione, TrueCrypt ci offre una scelta di 8 algoritmi di crittografia e 3 algoritmi per tritare.

È-tutti gli algoritmi per un dizionario di password e data equivalente?

Ecco le parole al mio dizionario (dictionnaire.txt) che verrà utilizzato:

















































































































































dictionnaire.txt				
Fichier	Édition	Rechercher	Options	Aide
Aurai				
-				
je				
une				
bonne				
note				
(
20				
)				
pour				
mon				
projet				
test				
?				
Luxembourg				
MIM				
Moselle				
ParisNew-York20!				
France				
Italie				
Manger				
Cigarette				
facile				
maladroit				

Nota: La password è nel dizionario questo è volontaria

 Password trovati

 Password non trovati

 Non testato (spiegazione nella conclusione)

Algoritmo uso	Password utilizzata					
	test	test123	Moselle	Moselle57	ParisNew-York20!	Los-AngelesTokyo10?
AES_RIPEMD-160						
Serpent_RIPEMD-160						
Twofish_RIPEMD-160						
AES-Twofish_RIPEMD-160						
AES-Twofish-Serpent_RIPEMD-160						
Serpent-AES_RIPEMD-160						
Serpent-Twofish-AES_RIPEMD-160						
Twofish-Serpent_RIPEMD-160						
AES_SHA-512						
Serpent_SHA-512						
Twofish_SHA-512						
AES-Twofish_SHA-512						
AES-Twofish-Serpent_SHA-512						
Serpent-AES_SHA-512						
Serpent-Twofish-AES_SHA-512						
Twofish-Serpent_SHA-512						
AES_Whirlpool						
Serpent_Whirlpool						
Twofish_Whirlpool						
AES-Twofish_Whirlpool						
AES-Twofish-Serpent_Whirlpool						
Serpent-AES_Whirlpool						
Serpent-Twofish-AES_Whirlpool						
Twofish-Serpent_Whirlpool						

Conclusione

Come possiamo vedere gli stessi fattori ritornano quando viene trovata la password:

- ❖ La password è presente nel dizionario
- ❖ L'algoritmo di crittografia è AES

Così per i miei test tutti gli algoritmi sono equivalenti tranne AES viene evitato.

Per algoritmi di hash sono tutti equivalenti

La versione di TrueCrack utilizzato ci permette di scegliere l'hash, ma non l'algoritmo di crittografia per cercare di trovare la password.

Solo l'algoritmo AES è considerato così dopo un primo test con altri algoritmi non era necessario provare con le password più forti, questo è inutile TrueCrack non avrebbe trovato.

Esiste un'altra versione di TrueCrack (o estensione) che viene utilizzata per aggiungere la possibilità di selezionare l'algoritmo di cifratura.

Dopo numerosi test sul mio computer non sono riuscito ad installare un'altra versione o l'estensione, ma il principio e il risultato **della mia conclusione sarebbe la stessa.**

Con una versione di TrueCrack con la possibilità di scegliere l'algoritmo di cifratura (-e) tutti gli algoritmi diventano equivalenti (a differenza dei miei esami quando è stato evitato AES).

Se l'opzione permette di selezionare un algoritmo preferito quindi un algoritmo di scelta che combina diversi algoritmi di crittografia (AES-Twofish-Serpent, per esempio) per proteggersi dagli attacchi.

Quindi, se TrueCrack conosce l'algoritmo di crittografia e l'algoritmo hash e la password è nel dizionario utilizzato è trovata la password.

Prova quale combinazione di algoritmo di crittografia e l'algoritmo di hash non fa male l'attaccante ($8 * 3 = 24$ combinazioni)

(Nel mio test $1 * 3 + \text{AES}$ come un hash di scelta)

Per proteggersi dagli attacchi in modo da avere una password che non è un attacco dizionario.

L'obiettivo qui non è quello di dare un corso su come scegliere una buona password, ma ecco alcuni suggerimenti:

- ❖ Scegliere una buona lunghezza (10 caratteri minimo)
- ❖ Una suite di carattere con minuscole, maiuscole, il numero e il carattere speciale (-!, \$, ...)
- ❖ Nessuna parola da un dizionario
- ❖ Non scegliere qualcosa di troppo facili

Il mio consiglio da ricordare una buona password: Scegli una frase e prendere la prima lettera di ogni parola, alternando maiuscole e minuscole.

Esempio: Scherzi cosa ne pensi del mio rapporto è 20/20?

Password: ScCnPdMrE20??

Prima relazione che ho TrueCrack era considerato uno dei migliori software per crittografare i propri dati (ancora senza parlare del dibattito se è compromessa o meno dall'inizio)

Con la password corretta per il software di sicurezza è molto buono e incontra la sua reputazione.

Definizioni : [wikipedia.it](https://it.wikipedia.org/)