DOCUMENTAZIONE LABORATORIO 2
FONDAMENTI DI CYBERSECURITY

Manuel Castiglia

Thomas Westerman

ESERCIZIO 1

Una volta installato rainbowcrack, creata una rainbow table e aver capito come funzionassero i vari comandi, siamo passati a decifrare il primo hash, usando il comando

‘rcrack /usr/share/rainbowcrack -h 6e6bc4e49dd477ebc98ef4046c067b5f‘

trovando la parola ‘ciao’

Una volta risolto il primo hash, siamo passati al secondo, utilizzando lo stesso procedimento, ossia utilizzando il comando

“rcrack /usr/share/rainbowcrack -h 427ade9c15ec643751860eba9899355b’

trovando la parola ‘gatto’

Per risolvere il terzo hash, abbiamo cambiato procedimento: inizialmente abbiamo utilizzato il comando **man** per trovare l’hash code da utilizzare, abbiamo aggiunto il salt alla fine dell’hash e, utilizzando il dizionario rockyou.txt, al secondo tentativo abbiamo trovato che quello giusto era –m 1710, trovando la parola ‘markinho’, come si può osservare qui sotto

```
┌──(kali㉿kali)-[~]
└─$ hashcat -m 1710 -a 0 '6c00f2d6e1610bfc9b415daf80d45855f2c56443c2dc2f71e7ef27168d1f2857d6168f4d374ed8eca34
9f2debd18d4ccac339218ca70446adf999060395742b4:hjt88q' /usr/share/wordlists/rockyou.txt --show
6c00f2d6e1610bfc9b415daf80d45855f2c56443c2dc2f71e7ef27168d1f2857d6168f4d374ed8eca349f2debd18d4ccac339218ca704
46adf999060395742b4:hjt88q:markinho
```

Per risolvere il quarto e il quinto hash, abbiamo utilizzato la stessa metodologia, con l’aggiunta del ruleset Insidepro-PasswordsPro.rule, oltre che il solito dizionario, abbiamo utilizzato il comando **man** per trovare l’hash code giusto e dopo un paio di tentativi, i risultati sono stati i seguenti:

- Hashcat – m 0 /home/kali/Downloads/InsidePro-Passwords.pro ‘0e8ae09ae169926a26b031c18c01bafa’ /usr/share/wordlists/rockyou.txt
    - Risultato → ILOVEME8320
- Hashcat – m 0 /home/kali/Downloads/InsidePro-Passwords.pro ‘c73fceaab80035a75ba3fd415ecb2735/usr/share/wordlists/rockyou.txt
    - Risultato → soccer23!

Per risolvere il sesto hash invece, visto che vengono fornite delle regole specifiche, siamo andati a creare un nostro ruleset, chiamato ‘lab2.rule’ dentro il quale abbiamo definito le regole che concatenano alla fine della parola uno o due numeri, e abbiamo usato il parametro C per invertire il case della parola

La struttura del ruleset è questa:

C$0

C$1

....

C$1 $0

C$1 $1

...

Una volta definito il ruleset, siamo andati a richiamare il comando **man** per identificare l’hash mode e tramite il comando

‘hashcat -m 0 -a 0 -r /home/kali/Desktop/lab2.rule 'dc612dc12fb4540a88b88875c2bee3b4' /usr/share/wordlists/rockyou.txt’

siamo arrivati alla soluzione ‘dANIELEGUAPO16’

```
dc612dc12fb4540a88b88875c2bee3b4:dANIELELGUAPO16

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 0 (MD5)
Hash.Target......: dc612dc12fb4540a88b88875c2bee3b4
Time.Started.....: Mon May  6 20:24:35 2024 (32 secs)
Time.Estimated...: Mon May  6 20:25:07 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Mod........: Rules (/home/kali/Desktop/lab2.rule)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  5676.8 kH/s (6.23ms) @ Accel:128 Loops:100 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 188121600/1434438500 (13.11%)
Rejected.........: 0/188121600 (0.00%)
Restore.Point....: 1880832/14344385 (13.11%)
Restore.Sub.#1...: Salt:0 Amplifier:0-100 Iteration:0-100
Candidate.Engine.: Device Generator
Candidates.#1....: dANIELELGUAPO0 → dANIE081899
Hardware.Mon.#1..: Util: 85%
```

ESERCIZIO 2

Level 0:

Per iniziare, è fondamentale stabilire una connessione sicura con il server utilizzando il protocollo SSH (Secure Shell):
Aprire il terminale e digitare il seguente comando:

```
root@kali:~# ssh bandit1@bandit.labs.overthewire.org
```

Dopo aver ottenuto la password per un determinato livello, è necessario utilizzarla per accedere al livello successivo. Per fare ciò, bisogna sostituire il nome utente prima del simbolo “@” con quello del livello successivo. Ad esempio, se si hai completato il livello 0 e si hai ottenuta la password, per accedere al livello 1, il comando diventerà:

```
root@kali:~# ssh bandit1@bandit.labs.overthewire.org
```

Per accedere al livello bisogna usare la password acquisita dal livello precedente per autenticarsi.Ricordarsi di digitare exit per disconnettersi dal livello attuale prima di procedere al successivo.

```
root@kali:~# ssh bandit0@bandit.labs.overthewire.org
```

Level 0 -> Level 1:

Nel prossimo livello possiamo trovare la password in un file chiamato readme nella cartella home del server.

```
bandit0@bandit:~$ ls
readme
bandit0@bandit:~$ cat readme
boJ9jbbUNNfktd78OOpsqOltutMc3MY1
```

Level 1 -> Level 2:

La password del prossimo livello è situata in un file nella cartella home.

```
bandit1@bandit:~$ ls
-
bandit1@bandit:~$ cat ./-
CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9
```

Level 2 -> 3:

La password del prossimo livello è in un file della home chiamato: **spaces in this filename** .

```
bandit2@bandit:~$ dir
spaces\ in\ this\ filename
```

```
bandit2@bandit:~$ cat spaces\ in\ this\ filename
UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK
```

Level 3 -> Level 4:

La password del prossimo livello è situata in un file nascosto dentro la cartella **inhere.**

```
bandit3@bandit:~$ ls
inhere
bandit3@bandit:~$ cd inhere
bandit3@bandit:~/inhere$ ls -a
.  ..  .hidden
bandit3@bandit:~/inhere$ cat .hidden
pIwrPrtPN36QITSp3EQaw936yaFoFgAB
```

Level 4 - > Level 5:

La password del prossimo livello è dentro un file con un particolare formattazione nella cartella **inhere.**

```
bandit4@bandit:~$ ls -a
.  ..  .bash_logout  .bashrc  .profile  inhere
bandit4@bandit:~$ cd inhere
bandit4@bandit:~/inhere$ ls -a
-file00  -file02  -file04  -file06  -file08  .
-file01  -file03  -file05  -file07  -file09  ..
bandit4@bandit:~/inhere$ file ./-*
./-file00: data
./-file01: data
./-file02: data
./-file03: data
./-file04: data
./-file05: data
./-file06: data
./-file07: ASCII text
./-file08: data
./-file09: data
bandit4@bandit:~/inhere$ cat ./-file07
koReBOKuIDDepwhWk7jZC0RTdopnAYKh
```

Level 5 -> Level 6:

La password del prossimo livello si trova nella directory **inhere** e ha tutte le seguenti proprietà: - leggibile dall'uomo - dimensione 1033 byte - non eseguibile.

```
bandit5@bandit:~$ ls
inhere
bandit5@bandit:~$ cd inhere
bandit5@bandit:~/inhere$ ls -a
.            maybehere02  maybehere06  maybehere10  maybehere14  maybehere18
```

```
..           maybehere03  maybehere07  maybehere11  maybehere15  maybehere19
maybehere00  maybehere04  maybehere08  maybehere12  maybehere16
maybehere01  maybehere05  maybehere09  maybehere13  maybehere17
bandit5@bandit:~/inhere$ find -type f -size 1033c
./maybehere07/.file2
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
DXjZPULLxYr17uwoI01bNLQbtFemEgo7
```

Level 6 -> Level 7:

La password per il livello successivo è memorizzata sul server e ha le seguenti proprietà: - di proprietà dell'utente bandit7 - di proprietà del gruppo bandit6 - 33 byte di dimensione.

```
bandit6@bandit:~$ find / -user bandit7 -group bandit6 -size 32c 2>/dev/null
/var/lib/dpkg/info/bandit7.password
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs
```

Level 7 -> Level 8:

La password per il livello successivo è memorizzata nel file **data.txt** accanto alla parola **millionth.**

```
bandit7@bandit:~$ ls
data.txt bandit7@bandit:~$ cat data.txt | head
stripes ZwoAbav24aKageEnorHYKB9vx0NWUst
notched QI7c1ckBq47CEZdMnQGQk6QcHNw7oiD
Armstrong's rUWxU2IDq8debiXsNOUK7Q002xL9dlts
Frightens G1611Zov2U6KdfLWyF0Eyfo3jywMF14g
Shuttered qs8qWr]85CCG3wmOLNNCuGDWYWWjlSi
Prakrit's HV8XkpDaUp08uLofbczyRstbbr057ZtV
Tapeworms jkJdvjWn5ruqP5IKaZVs r99Eu6NTWBOI
Gamble rGpYkHUc2BvCDoi7ZHOL2Jham57ehRUb
Anchovies IyOuvBzQrSfIzjZuXM5sIFvS0NDNkdiv
Adelaide's qnWisXg®ExqA7ULLWd8qwV4xyCnxSyWk
bandit7@bandit:~$ cat data.tt | grep millionth
millionth cvX2JJa4CFALtqS87jk27qwqGhBM9plV
```

Level 8 -> Level 9:

La password per il livello successivo è memorizzata nel file **data.txt** ed è l'unica riga di testo che è presente tramite una sola occorrenza.

```
bandit8@bandit:~$ sort data.txt | uniq -u
UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR
```

Level 9 -> Level 10:

La password del livello successivo è situate al interno del file **data.txt** in una delle poche stringhe leggibili dall'uomo, che inizia con diversi caratteri "=".

```
bandit9@bandit:~$ ls -a
.  ..  .bash_logout  .bashrc  .profile  data.txt
bandit9@bandit:~$ strings data.txt | grep "="
epr~F=K
7?YD=
?M=HqAH
/(Ne=
C=_"
I========== the6
z5Y=
`h(8=`
n\H=;
========== password
========== ism
N$=&
l/a=L)
f=C(
========== truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk
ie)=5e
```