

Projecte ASIX 2k22

Escola Del Treball

2HISX 2021-2022

Aaron Andal & Cristian Condolo

CryptoSEC: “*Careful where you step in*”



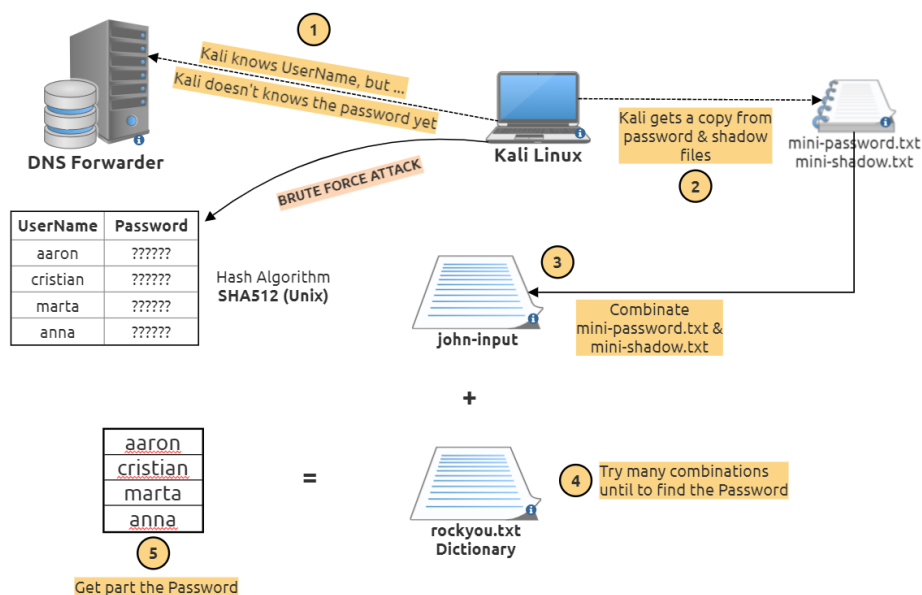
Index

- Brute Force:-> readME <-
- Practica:-> readME <-
 - Prova improvisada:-> readME <-
- Bibliografia:-> readME <-

Brute Force

Que no engagi el nom de **Força Bruta**, es un **atac criptogràfic** que **prova totes les solucions possibles** o molts d'elles. També coneguda per la seva **recerca exhaustiva** y es molt **utilitzada pels hackers** per **dexifrar passwords**, i d'aquesta forma, **obtenir accés a dades externes**. Per això s'utilitza **un programari amb un algorisme** simple que realitza la successió de diverses combinacions de caràcters compostos per dígits, espais i lletres fins a una longitud màxima definida.

No podem prendre'ns a la lleugera, ja que per un hacker es **facil trobar el fitxer necessari per trobar el password**. Tot i que els **passwords** no estan **en format text**, doncs han sigut **codificats** previament **utilitzen algoritme criptografic**, el hacker pot **accedir als fitxers** si aquest **no estan protegits** contra accesos no autoritzats. Aquest pot **crear una copia del fitxers** i executar en ells diferents atacs de Brute Force sense mantenir la connexio amb el sistema. Actualment, nomes existeixen **tres variables** que faciliten al hacker compleix el seu cometit: + La **duració** de cada pas de la verificació + La **longitud** del password + La **complexitat** del password



Com prevenir-ho?

Quan mes curta siguin els passwords, mes rapidsseran descoberts per el metode de Brute Force. Es per aixó que se recomana utilitzar passwords mes complexo i llargs, que incluin diferents caracters i per aixó la majoria de sistemes de xifrat de contrasenyes utilitzen claus molt llargues.

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

Practica

Nota: totes les ordres ha de ser executades per root. En cas de no estar com a root, posar sempre al principi sudo.

1. Un cop a dins del Kali entrem dins del dir **demo**, on es troben dos fitxer. Son dos copies dels files **passwd** i **shadow** d'algun client.

```
(anonymous@cristian-cryptosec)-[~]
$ cd demo/

(anonymous@cristian-cryptosec)-[~/demo]
(anonymous@cristian-cryptosec)-[~/demo]
$ ll
total 8
-rw-r--r-- 1 root root 688 May 16 16:25 mini-passwd2.txt
-rw-r--r-- 1 root root 929 May 16 16:25 mini-shadow2.txt

(anonymous@cristian-cryptosec)-[~/demo]
$ cat *
systemd-coredump:x:999:999:systemd Core Dumper:/:usr/sbin/nologin
cryptosec:x:1000:1000:cryptosec:/home/cryptosec:/bin/bash
lxd:x:998:100:/var/snap/lxd/common/lxd:/bin/false
bind:x:118:118:/var/cache/bind:/usr/sbin/nologin
dnsmasq:x:114:65534:dnsmasq,,/var/lib/misc:/usr/sbin/nologin
dhcpcd:x:115:120:/var/run/usr/sbin/nologin
aaron:x:1001:1001:Aaron,03,6597565656,3659889789,Hola:/home/aaron:/bin/bash
cristian:x:1002:1002:Cristian,54,54564564,534545646,53424:/home/cristian:/bin/bash
pere:x:1003:1003:Pere,pere,pere,pere,pere:/home/pere:/bin/bash
anna:x:1004:1004:anna,anna,anna,anna:/home/anna:/bin/bash
marta:x:1005:1005:marta,marta,marta,marta:/home/marta:/bin/bash
systemd-coredump:!!:19108:19108:
cryptosec:$6$VCz5SW3NvrkaM0fZ$9w0QfWC1Hitu7pVhxJR1xfvYJwa5JK0t00vZL5/NWCy1FkcxIEY1Xs2gJ0RC1T1U4Py6Pcj2sJ0Q.DHZRLJQB1:19110:0:99999:7:::
lxd:!:19108:19108:
bind:!:19114:0:99999:7:::
dnsmasq:*:19121:0:99999:7:::
dhcpcd:*:19124:0:99999:7:::
aaron:$6$0x5d18NYGmgn..w0$GMIZVYTM0..saBCHdKoTndvPgctcVqf8qJ4zF642W0FucLpQz18AR56DjKqZkrz9HrF.JjYQG..so2tWGJVF20JN.:19128:0:99999:7:::
cristian:$6$1VIV..10..PwFP0tCBV$PdxjACMvR1gdb/1a5UeAfKs84../uP1Pzv3b4IXEY12yfdIHBHhYHxEBNnuFWJmnoxB8MchjM3ocPCIBa/FvH.:19128:0:99999:7:::
pere:$6$DabvFVG1w..Byi8uc$90myr04Pdpf9MjJq9DgDMuifgH/1lba5eV68pm3FKVtUq00J2FRxxJqsybmYfiKQ0ISK85E/60bBLdihqoyok.:19128:0:99999:7:::
anna:$6$Q05gf5rpQKw2aWk$dlWsiK1SWJlp..Nrm07q7p36cUxzFSYQ9JrgQY2BM4NzJcG1DV8EhNz9TFRy0iCRxP8wrThyLWUhwcrI82.B.:19128:0:99999:7:::
marta:$6$0NrL4Errv1L6JUF0$FVlWP..gFr08GrtcseQmS..LW6BU9R/531L8moTohtdQIFrZXC35FoH0XD8PZ3xd6PPTMgFaG994RLS8PrBauC0:19128:0:99999:7:::
```

2. Como aquest es una atac offline, necessitem a juntar els dos fitxer (**passwd** + **shadow**), per tenir el **username** y **password** junts.

unshadow mini-password.txt mini-shadow.txt > john-input 'cat

john-input

```
(root@cristian-cryptosec) [/home/anonymous/demo]
# unshadow mini-passwd2.txt mini-shadow2.txt > john-input
[cr]
[cr]
[cr]
total 12
-rw-r--r-- 1 root root 1319 May 20 07:14 john-input
-rw-r--r-- 1 root root 688 May 16 16:25 mini-passwd2.txt
-rw-r--r-- 1 root root 929 May 16 16:25 mini-shadow2.txt
[cr]
# cat john-input
systemd-coredump: 11:999:999:systemd Core Dumper:/:usr/sbin/nologin
cryptosec:$6$vcZ55W3MvRkaM0fZ39wQfWcHitu7pVhxJRx1fdJ3W5Jk0t00vZ15/NWCy1fKcxIEY1Xs2gJorC1T1U4Py6PcJ2sJ0Q,DH2RL3Q81:1000:1000:cryptosec:/home/cryptosec:/bin
/bash
lxd:l:998:100::/var/snap/lxd/common/lxd:/bin/false
bind:*:113:118::/var/cache/bind:/usr/sbin/nologin
dnsmasq:*:114:6534:dnsmasq,,,:/var/lib/dnsmasq:/usr/sbin/nologin
dhcpd:*:115:120::/var/run:/usr/sbin/nologin
aaron:$6$0xd51RhY6msn.wM0$GMI2VYTN8.sabCHdKoTndvPgTcVqf8qJ4zF642WofuLpQz1BAR56DJKqZkRZ9Hrf.JJYQG.so2tW6JVF20JN.:1001:1001:Aaron,03,6597565656,3659889789,Hola:/home/aaron:/bin/bash
cristian:$6$1VV.10.PwP0TcBV5PdxjACMvri9db/1a5UeAFks84..uP1Pzv3b4IxEY12yfdIHBHYHJXEBNnUfWJmmoxB68MCHJ3ocPCIBa/FVH.:1002:1002:Cristian,54,54564564,534545646,53424:/home/cristian:/bin/bash
pere:$6$0abv7VG1w.Byl8uc$90myr04Pdpf9MjJq0d0MuIfGH/1lba5eV6Bpm3FKVIUQ0J2FRxXJqsybmYfIKQ1SK85E/60bBLdihqayoyk.:1003:1003:Pere,pere,pere,pere,pere:/home/pere:/bin/bash
anna:$6$0Q0g5rPQKwx2aWk$dNlwsIK1SW3lwp.Nrmo7q7p36cUxzFSYQ9JrgQV2BM4NzJcG1DV8EhNz9TFRy01CRxP8wRThyLWUhwcr182.B.:1004:1004:anna,anna,anna,anna,anna:/home/anna:/bin/bash
marta:$6$0Nrl4Errv1L6JUF0$FVLWP.gFr08GrtcseQm5..Lw6BU9R/531l8moTohtdQIFRZXC3SfoH0XdBP23xd6PPTMga6994RL58RbAuC0:1005:1005:marta,marta,marta,marta,marta:/home/marta:/bin/bash
```

3. Ara passem a descriptar el passwords, amb l'eina John. . Mitjançant un diccionari, on va provar moltes combinacion fins trobar un coincidenci.

Nota: John The Ripper es un eina de recuperacio de passwords, es molt utilitzada pels hackers, que admet centenars de tipus **hash** i de **xifratge** per **passwords de Unix**, en el nostre cas esta descriptant amb **hash SHA215Unix**.

john john-input --wordlist=/usr/share/wordlists/rockyou.txt

```
(root@cristian-cryptosec) [/home/anonymous/demo]
# john john-input --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 different salts (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Remaining 4 password hashes with 4 different salts
Cost 1 (iteration count) is 5000 for all loaded hashes
Press 'q' or Ctrl-C to abort, almost any other key for status
marta (marta)
anna (anna)
```

4. Durant el proces, es pot veure com va troban la password de cada username.
5. Lo que faltaria seria espera fins que acabi, i quan acabi podem veure de nou el fitxer john-input.

```
(root@cristian-cryptosec) [/home/anonymous/demo]
# john john-input --show
aaron:aaron:1001:1001:Aaron,03,6597565656,3659889789,Hola:/home/aaron:/bin/bash
cristian:cristian:1002:1002:Cristian,54,54564564,534545646,53424:/home/cristian:/bin/bash
anna:anna:1004:1004:anna,anna,anna,anna,anna:/home/anna:/bin/bash
marta:marta:1005:1005:marta,marta,marta,marta,marta:/home/marta:/bin/bash

4 password hashes cracked, 2 left
```

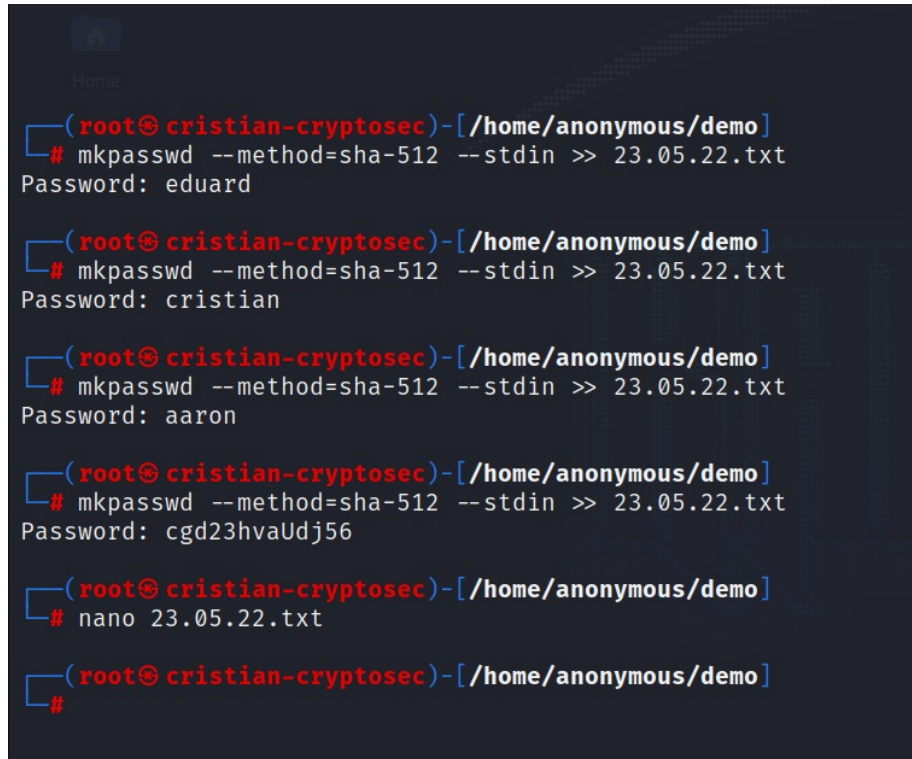
6. Una manera de comprovar si els passwords son certes seria entrar per ssh a la maquina.

ssh marta@192.168.3.102

Prova improvisada

1. Com el cas anterior estava preparat, llavors demostrarem com seria una prova en viu amb noves **passwords** encriptades, ho rediriguem a un fitxer i dins d'aquest l'hi fem el **username**.

```
mkpasswd --method=sha-512 --stdin >> passwd.txt
```



```
(root@ cristian-cryptosec)-[/home/anonymous/demo]
# mkpasswd --method=sha-512 --stdin >> 23.05.22.txt
Password: eduard

(root@ cristian-cryptosec)-[/home/anonymous/demo]
# mkpasswd --method=sha-512 --stdin >> 23.05.22.txt
Password: cristian

(root@ cristian-cryptosec)-[/home/anonymous/demo]
# mkpasswd --method=sha-512 --stdin >> 23.05.22.txt
Password: aaron

(root@ cristian-cryptosec)-[/home/anonymous/demo]
# mkpasswd --method=sha-512 --stdin >> 23.05.22.txt
Password: cgd23hvaUdj56

(root@ cristian-cryptosec)-[/home/anonymous/demo]
# nano 23.05.22.txt

(root@ cristian-cryptosec)-[/home/anonymous/demo]
#
```

2. I tornem a descriptar-lo amb l'eina **john**.

```
john passwd.txt --wordlist=/usr/share/wordlists/rockyou.txt
```

3. Durant el procés de descriptació, prems **Enter** per poder veure com intenta amb cada combinació.
4. Tornem a esperar i veure com ha resultat.

Bibliografia

- <https://www.ionos.es/digitalguide/servidores/seguridad/brute-force-definicion-y-medidas-de-proteccion/>
- <https://www.zonasystem.com/2020/06/password-cracking-en-linux-john-the-ripper-hashcat.html>

- <https://www.openwall.com/john/>
- https://www.youtube.com/watch?v=z4_oqTZJqCo&t=509s