

Romper contraseñas

A.D.G.

1) Busca si tu contraseña está en RockYou:

```
(kali@kali)-[/usr/share/wordlists]
$ sudo gzip -d rockyou.txt.gz
[sudo] password for kali:
$ sudo nano rockyou.txt
$ grep andreidani /usr/share/wordlists/rockyou.txt
andreidaniel
haiduandreidaniel
biruandreidaniel
```

2) Buscar si habéis sido pawneados:

Un correo que lo usaba para 1001 cosas. Otro correo Outlook sólo para trabajo y temas administrativos como ciudadano.

The image shows two screenshots of the 1Password security check interface. The left screenshot is for the email address 'andreidani...@gmail.com' and shows a 'pwned?' status with a message 'Oh no — pwned!' and 'Pwned in 3 data breaches and found no pastes'. It lists three steps to better security: 1. Protect yourself using 1Password, 2. Enable 2 factor authentication, and 3. Subscribe to notifications. It also lists breaches you were pwned in: Daily Quiz, Jobandtalent, and Nitro. The right screenshot is for the email address 'Andre...@outlook.com' and shows a 'pwned?' status with a message 'Good news — no pwnage found!' and 'No breached accounts and no pastes'.

3) Buscar el algoritmo hash más seguro de estos: HMAC-SHA512,PBKDF2-HMAC-SHA256,bcrypt,LM,NT:

```
$ john --test --format=HMAC-SHA512,PBKDF2-HMAC-SHA256,bcrypt,LM,NT
Created directory: /home/kali/.john
Will run 2 OpenMP threads
Benchmarking: HMAC-SHA512 [password is key, SHA512 128/128 SSE2 2x]... (2xOMP) DONE
Many salts: 3334K c/s real, 1685K c/s virtual
Only one salt: 1666K c/s real, 843961 c/s virtual

Benchmarking: PBKDF2-HMAC-SHA256 [PBKDF2-SHA256 128/128 SSE2 4x]... (2xOMP) DONE
Speed for cost 1 (iteration count) of 1000
Raw: 10578 c/s real, 4096 c/s virtual

Benchmarking: bcrypt ("2a$05", 32 iterations) [Blowfish 32/64 X3]... (2xOMP) DONE
Speed for cost 1 (iteration count) of 32
Raw: 3427 c/s real, 1467 c/s virtual

Benchmarking: LM [DES 128/128 SSE2]... (2xOMP) DONE
Raw: 94176K c/s real, 47406K c/s virtual

Benchmarking: NT [MD4 128/128 SSE2 4x3]... DONE
Raw: 51877K c/s real, 51877K c/s virtual

5 formats benchmarked.
```

El algoritmo hash más seguro sería **"bcrypt"** por el hecho de que está probando menos claves por segundo que los demás (al menos en mi portátil con mi hardware actual), lo cual tanto a mí como a un ciberdelincuente le dificultaría más conseguir la clave por la espera, a comparación de otros algoritmos hash que prueban muchísimas más claves por segundo, por tanto bcrypt es más seguro y más difícil de descryptar.

4) Rompe las contraseñas del zip, (we will rock you):

Usamos John the Ripper para lograr descubrir posteriormente la contraseña de un zip. El resultado lo guardo en shadow.txt:

```
Simbolo del sistema
C:\Users\Andrei\Desktop\john-1.9.0-jumbo-1-win64\run>zip2john.exe c:\Users\Andrei\Desktop\john-1.9.0-jumbo-1-win64\shadow.zip > c:\Users\Andrei\Desktop\john-1.9.0-jumbo-1-win64\shadow.txt
ver 5.1 c:\Users\Andrei\Desktop\john-1.9.0-jumbo-1-win64\shadow.zip\shadow.txt is not encrypted, or stored with non-handled compression type
```

Ejecuto john para que descubra la contraseña a partir de mi documento de texto generado:

```
C:\Users\Andrei\Desktop\john-1.9.0-jumbo-1-win64\run>john shadow.txt
Warning: detected hash type "ZIP", but the string is also recognized as "ZIP-openc1"
Use the "--format=ZIP-openc1" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 256/256 AVX2 8x])
Will run 8 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 18 candidates buffered for the current salt, minimum 64 needed for performance.
Proceeding with wordlist:password.lst, rules:Wordlist
123456 (shadow.zip/shadow.txt)
lg 0:00:00:00 DONE 2/3 (2022-11-01 22:51) 1.739g/s 84765p/s 84765c/s 123456..faithfaith
Use the "--show" option to display all of the cracked passwords reliably
Session completed
C:\Users\Andrei\Desktop\john-1.9.0-jumbo-1-win64\run>
```

Obtenemos un documento texto con:

```
1 $6$yMJT8Nf23i7Z1WkF$ChxmECeWS3W80r10gf4e-
apPz5FNcBM4SBvZG.
21fI0wpNUMR1yCmK71r7sYFMXCL3deD5BWD0/
6A4WU66cjv0
2 $6$xonBhxEl9HmG8.DR$LdediY0FTHMUPyeQAiEFV-
gUR6rKVr0GcCECn.EQuIwH2EyZqib3gc5k3fuw/
ppLJY41Ap5KEUF7Rck3T400
3 $6$ooYV5Z5dEaDfyPom$VnKneoTa7s7DJRFFaye2
sJZiWbrr1jQ28Lzw360GaAChy1K14GY6BEFTABLG-
jZ8Xs4i5mbaZdfDXyF19ED71
4 $6$a5m5M9J/
FEJGzyrd$shv36BN0S58W8VQbbjLKEs1/
3QjJxomkBB84j9Mw2g04JW3TIVGstOmJQFT5wdp11
soe9XjI3YjDNNH6uXv7s1
```

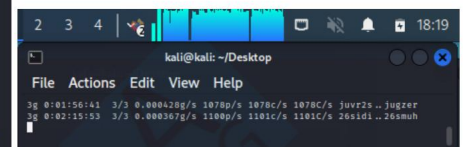
Ahora uso John the Ripper para descubrir el o los algoritmos de hash que tienen esas 4 líneas, para descryptarlos:

```
(kali@kali)-[~/Desktop]
$ john shadow.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with 4 different salts (sha512crypt
, crypt(3) $6$ [SHA512 128/128 SSE2 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for statu
s
Almost done: Processing the remaining buffered candidate pas
swords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
dragon (?)
whatever (?)
princesa (?)
Proceeding with incremental:ASCII
```

Podemos comprobar las claves obtenidas, la otra lleva ya más de dos horas en el mismo estado anterior:

```
(kali@kali)-[~/Desktop]
$ john --show shadow.txt
?:whatever
?:dragon
?:princesa
3 password hashes cracked, 1 left
```

Cancelo, tarda mucho y me ralentiza las tareas



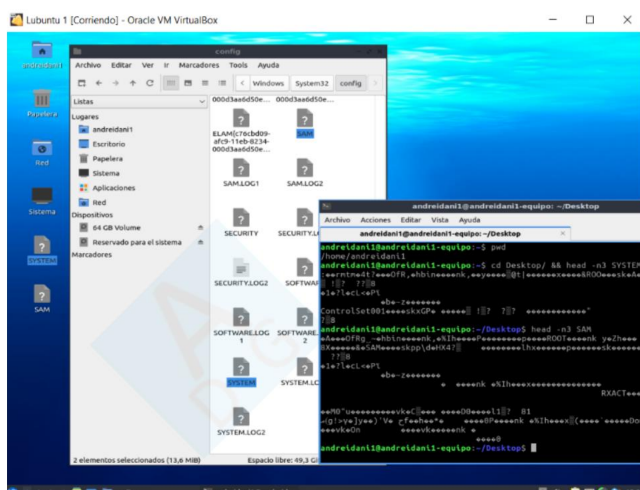
5) De la máquina de Windows sacar los usuarios y contraseñas

Iniciando una consola con permisos de Administrador, copiamos desde el registro el archivo SAM y SYSTEM, ó accedemos manualmente a la ruta: `C:\Windows\System32\config`, que es donde encontraremos los archivos y los copiamos:

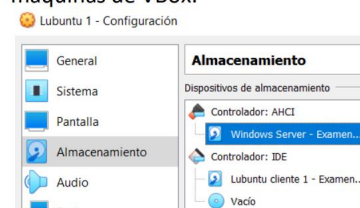
*******IMPORTANTE*******

Al final del video tuyo ví que también pedías sacar la contraseña de oscar para acceder (es que rápido de primeras probé iniciar sesión con oscar y la super fuerza bruta mental de probar poner de contraseña lo que tienes de usuario 😊 pensé que la habías dicho por ser así de fácil y continué el proceso desde la misma sesión iniciada con oscar).

----- **ACTUALIZACIÓN:** Después de intentar probarlo en **VMWare** te comenté que se me bloquea al instalar sistemas operativos tanto Ubuntu como Lubuntu (para posteriormente meter el disco duro de tu máquina de Windows con los usuarios) así que probé hacer una prueba en **VirtualBox** para probar este método con un S.O. Lubuntu, y un disco que tenía yo de un Windows de otra máquina virtual:

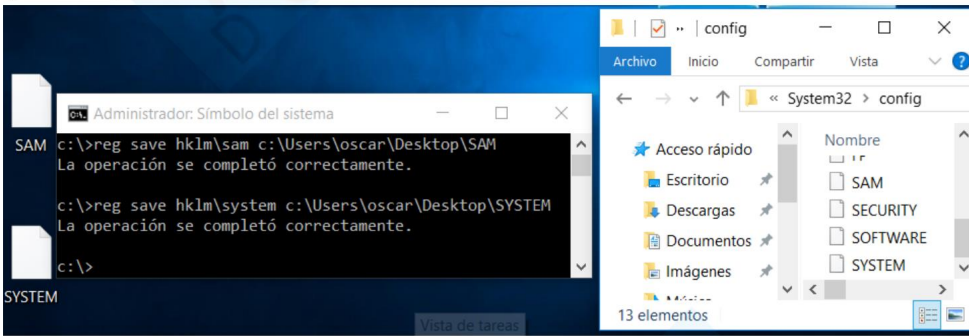


Únicamente lo conecté como AHCI para poder detectar los discos de las máquinas de VBox:



Inicié sesión en mi Lubuntu, y en el Explorador de archivos podía ver el apartado de la foto de la izquierda de **64 GB Volume**, ese es el disco duro del Windows. Pude entrar hasta ver los archivos SYSTEM y SAM todo bien, lo único que en Lubuntu no encontraba ningún editor/lector de documentos de texto, no funcionaba ni con LibreOffice Write ni nada así que imprimí un par de muestras de 3 líneas de cada por consola.

🚩 Aquí ya continué con oscar averiguado al tuntún por lo explicado anteriormente:



Los pasamos del Windows a Kali, y después nos situamos en la consola donde los hayamos copiado y escribimos el comando de SamDump2 junto a SYSTEM SAM, en orden, guardándolo en un archivo .txt obteniendo lo siguiente:

```
(kali@kali)~/Desktop
$ samdump2 SYSTEM SAM > SYSTEMSAM.txt

(kali@kali)~/Desktop
$ cat SYSTEMSAM.txt
*disabled* Administrador:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
*disabled* Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
*disabled* :503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
oscar:1000:aad3b435b51404eeaad3b435b51404ee:b32db29f51c06e0b7ae42f8355dab807 :::
:1001:aad3b435b51404eeaad3b435b51404ee:a2212d8b2bb5a18c1f0f9343956b3f23 :::
:1002:aad3b435b51404eeaad3b435b51404ee:9ab721ecba25a83055ea8ba89c7c717b :::
:1003:aad3b435b51404eeaad3b435b51404ee:edba5cbe1ed46b673a7f0a86fdbfca2f :::
:1004:aad3b435b51404eeaad3b435b51404ee:cf74007f626c01b74c94f0e95423ab50 :::
:1005:aad3b435b51404eeaad3b435b51404ee:93609de8c3eeaa8113d33131230a192f :::
:1006:aad3b435b51404eeaad3b435b51404ee:6a5d34a235d3553fb8aa3b1c036ff684 :::
:1007:aad3b435b51404eeaad3b435b51404ee:186cb09181e2c2ecaac768c47c729904 :::
:1008:aad3b435b51404eeaad3b435b51404ee:cadceffac32144a358cbd798d8c132f :::
```

Modificamos con nano y vemos que hay 3 cuentas deshabilitadas las eliminamos, y en el nombre de usuarios aparecen ^T y los cambiamos por userX respectivo:

GNU nano	GNU nano 6
disabled	oscar:1000:a
disabled	user1:1001:a
disabled	user2:1002:a
oscar:100	oscar:100
^T:1001::	user3:1003:a
^T:1002::	user4:1004:a
^T:1003::	user5:1005:a
^T:1004::	user6:1006:a
^T:1005::	user7:1007:a
^T:1006::	user8:1008:a
^T:1007::	
^T:1008::	

Se prueba sacar contraseñas por **fuerza bruta** (uso John The Ripper en Windows, ya que no podía encontrar el archivo john.pot para borrar lo descubierto por tantas pruebas y así poder hacer las capturas: (renombré SYSTEMSAM.txt a SYSTEMSAM1.txt)

```
Administrador: Símbolo del sistema
C:\john\run>john --format=NT SYSTEMSAM1.txt
Using default input encoding: UTF-8
Loaded 9 password hashes with no different salts (NT [MD4 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=8
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
oscar
(oscar)
Warning: Only 17 candidates buffered for the current salt, minimum 24 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 8 candidates buffered for the current salt, minimum 24 needed for performance.
Proceeding with wordlist:password.lst, rules:Wordlist
a
(user7)
Proceeding with incremental:ASCII
2g 0:00:03:22 3/3 0.009864g/s 27597Kp/s 27597Kc/s 193184KC/s lcbdoc09..lcbdoz09
2g 0:00:04:36 3/3 0.007228g/s 29316Kp/s 29316Kc/s 205214KC/s kjisf2u..kjisfjb
2g 0:00:05:53 3/3 0.005658g/s 30264Kp/s 30264Kc/s 211851KC/s lhd1pll..lhd1p98
carlos2023
(user6)
3g 0:00:06:38 3/3 0.007537g/s 30573Kp/s 30573Kc/s 213396KC/s p0sk195m..p0sk1na6
3g 0:00:07:19 3/3 0.006830g/s 30618Kp/s 30618Kc/s 210870KC/s rigudhno..rigucno3
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session aborted

C:\john\run>john --show --format=NT
Password files required, but none specified

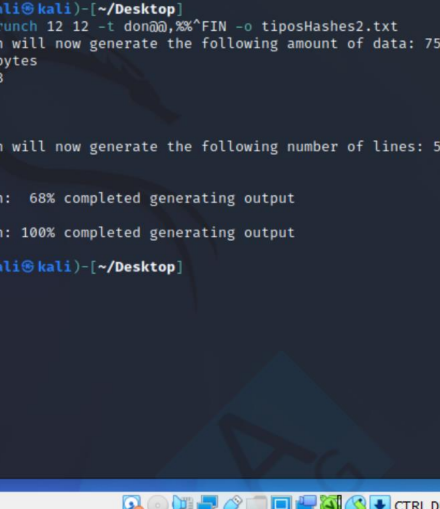
C:\john\run>john --show --format=NT SYSTEMSAM1.txt
oscar:oscar:1000:aad3b435b51404eeaad3b435b51404ee:b32db29f51c06e0b7ae42f8355dab807:::
user6:carlos2023:1006:aad3b435b51404eeaad3b435b51404ee:6a5d34a235d3553fb8aa3b1c036ff684:::
user7:a:1007:aad3b435b51404eeaad3b435b51404ee:186cb09181e2c2ecaac768c47c729904:::

3 password hashes cracked, 6 left
```

En dos horas no sacó más de aquello, lo paro para continuar con los siguientes.

[illegible]

6) Deshasea las contraseñas del txt dado,
don+dosletrasminuscultas+unamayuscula+dosnumero+unsimbolo+FIN ej donniK12\$FIN, HELP tomate un crunch



```
kali@kali: ~/Desktop
File Actions Edit View Help

(kali@kali)-[~/Desktop]
$ crunch 12 12 -t don@,%%^FIN -o tiposHashes2.txt
Crunch will now generate the following amount of data: 75401
0400 bytes
719 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 5800
0800

crunch: 68% completed generating output
crunch: 100% completed generating output

(kali@kali)-[~/Desktop]
$
```

(ACTUALIZACIÓN: Sólo desde esta parte volví a hacer/modificar mi documento enviado el 06/11/2022 poniendo “FIN” con mayúsculas en vez de “fin” en minúsculas ya que se me fue al leerlo en el enunciado pero la sintaxis del comando era buena en general 😊 sólo que con fin no me saldría ninguna clave ni en 1 mes encendido.

Uso el John The Ripper para probar el diccionario junto a las hashes que tú has dado (lo llamé oscar-tiposhashtxt), aunque falte el . antes de txt no significa un cambio de formato sigue siendo un nombre por tanto no afecta: Pruebo con el formato RAW-SHA1:

```
(kali@kali)-[~/Desktop]
$ john --wordlist=tiposHashes2.txt oscar-tiposhashtxt --
format=RAW-SHA1
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA1 [SHA1 128/128 SSE2 4x])
Warning: no OpenMP support for this hash type, consider --fo
rk=6
Press 'q' or Ctrl-C to abort, almost any other key for statu
s
0g 0:00:00:03 42.17% (ETA: 14:26:31) 0g/s 8098Kp/s 8098Kc/s
8098KC/s donkzB80 FIN..donkzB81#FIN
donpa099,FIN (?)
1g 0:00:00:04 DONE (2022-11-07 14:26) 0.2262g/s 7581Kp/s 758
1Kc/s 7581KC/s donpa099'FIN..donpa099,FIN
Use the "--show --format=Raw-SHA1" options to display all of
the cracked passwords reliably
Session completed.
```

Se puede ver que prueba de forma correcta las combinaciones, pero si lo pongo a probar todos los formatos sigue tardando demasiado (8 días 24/7 encendido tardaría para ser más exactos)

```
0g 0:00:38:49 0.34% (ETA: 2022-11-15 11:51) 0g/s 85.44p/s 170.8c/s 170.8C/s donac132"FIN..donac134.FIN
Session aborted

C:\john\run>john --wordlist=tiposHashes2.txt oscar-tiposhashes.txt
Warning: detected hash type "bcrypt", but the string is also recognized as "bcrypt-openc1"
Use the "--format=bcrypt-openc1" option to force loading these as that type instead
Warning: only loading hashes of type "bcrypt", but also saw type "HMAC-SHA256"
Use the "--format=HMAC-SHA256" option to force loading hashes of that type instead
Warning: only loading hashes of type "bcrypt", but also saw type "LW"
Use the "--format=LW" option to force loading hashes of that type instead
Warning: only loading hashes of type "bcrypt", but also saw type "Raw-SHA1"
Use the "--format=Raw-SHA1" option to force loading hashes of that type instead
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 1024 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:14 0.00% (ETA: 2022-11-14 12:50) 0g/s 87.34p/s 174.6c/s 174.6C/s donaaA39)FIN..donaaA41~FIN
0g 0:00:00:27 0.00% (ETA: 2022-11-15 01:47) 0g/s 86.75p/s 173.5c/s 173.5C/s donaaA72]FIN..donaaA74*FIN
0g 0:00:00:45 0.01% (ETA: 2022-11-15 07:10) 0g/s 86.34p/s 172.6c/s 172.6C/s donaaB17>FIN..donaaB19 FIN
0g 0:00:01:06 0.01% (ETA: 2022-11-15 08:42) 0g/s 85.55p/s 172.2c/s 172.2C/s donaaB72+FIN..donaaB74]FIN
0g 0:00:03:17 0.03% (ETA: 2022-11-15 11:40) 0g/s 85.37p/s 170.7c/s 170.7C/s donaaF10{FIN..donaaF12;FIN
```