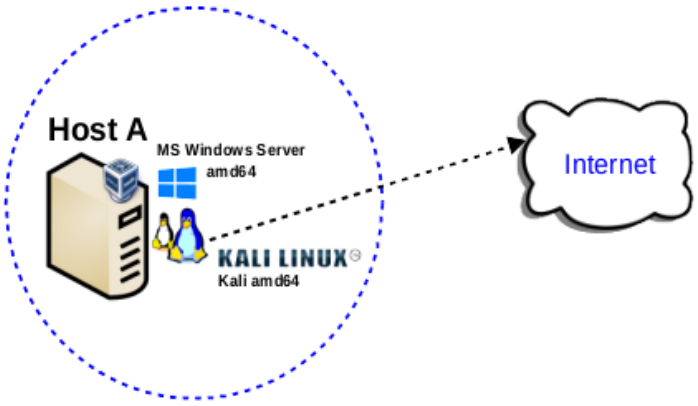
TALLER BRS - PRÁCTICA Auditar contrasinal usuarios DC: ntds	
Apelidos	**Nome**

ESCENARIO:

Host Alumnado: A
⊃ Máquina virtual

Máquinas virtuais:
⊂ Host



Máquina virtual Microsoft Windows DC:
RAM ≥ 2048MB
Disco duro: Windows Server 2019 amd64
Rede: Interna
IP/MS: 10.1.0.100/24
Controlador de dominio
Usuario/Contrasinal: administrador/abc123.
Usuario/Contrasinal: testing/rockstar#1

Máquina virtual GNU/Linux:
RAM ≥ 4096MB
ISO: Kali Live amd64
Rede: eth0 → NAT, IP/MS: 10.0.2.15/24
eth1 → Rede Interna, IP/MS: 10.1.0.10/24
BIOS: Permite arranque dispositivo extraíble: CD/DVD, USB
Servidor SSH

Material necesario	Práctica: Auditar contrasinal usuarios DC: ntds
■ Host alumnado ■ Máquina virtual MS Windows ■ Máquina virtual GNU/Linux Kali ■ [1] impacket ■ [2] hashes.com ■ [3] crackstation.net ■ [4] md5decrypt.net ■ [5] Práctica SI AD Enumeración ■ [6] ISO descarga Windows Server 2019 ■ [7] ISO descarga GNU/Linux Kali ■ [8] Dumping Active Directory Hashes - NTDS.dit	Host alumnado: a) Máquina virtual MS Windows Server 2019 amd64: ■ Crear seguindo especificacións do escenario. ■ Arrancar ■ Configurar a rede según o escenario ■ Configurar como controlador de dominio: Rol Servicios de dominio de Active Directory ■ Acceder como administrador e crear o usuario: Nome: testing Contrasinal: rockstar#1 ■ Con ntdsutil facer unha copia de ntds.dit b) Máquina virtual GNU/Linux Kali amd64: ■ Crear seguindo especificacións do escenario. ■ Arrancar ■ Configurar a rede según o escenario. ■ Arrancar servidor SSH c) Máquina virtual MS Windows Server 2019 amd64: ■ scp: Copiar de forma remota e mediante comunicación cifrada o volcado feito con ntdsutil á máquina virtual Kali. d) Máquina virtual GNU/Linux Kali amd64: ■ impacket-secretsdump: “Dumpear” os hashes das contas existentes no controlador de dominio a un ficheiro. e) Acceder a Internet, copiar os hashes do ficheiro anterior e comprobar se é posible averiguar os contrasinais a través das URLs [2][3][4]

Que é NTDS.dit?

NTDS.dit son as siglas de "NT Directory Services Database" (Base de Datos de Servizos de Directorio NT). É o arquivo central onde se almacena toda a información de Active Directory, un servizo de directorio de Microsoft que organiza e administra os recursos dunha rede.

Que información contén?

Este arquivo crucial contén unha gran variedade de datos, incluíndo:

- **Información de usuarios:** Nomes de usuario, contrasinais (en forma de hashes), grupos aos que pertencen, permisos e outros atributos.
- **Información de grupos:** Nomes de grupos, membros, permisos e atributos.
- **Obxectos de computador:** Información sobre os computadores da rede, como o seu nome, localización e configuración.
- **Obxectos de organización:** Estrutura xerárquica da organización, unidades organizativas e sitios.
- **Obxectos de configuración:** Configuración de Active Directory, como esquemas, particións e replicacións.

Cal é a súa importancia?

O arquivo NTDS.dit é o corazón de Active Directory. Sen el, non sería posible autenticar usuarios, administrar recursos de rede nin manter unha estrutura organizada da información. Calquera dano ou corrupción neste arquivo pode ter consecuencias graves para o funcionamento de toda a rede.

Onde se atopa?

Por defecto, o arquivo NTDS.dit atópase na seguinte ruta no controlador de dominio:

```
C:\Windows\NTDS\NTDS.dit
```

Por que é un obxectivo para os atacantes?

Debido á gran cantidade de información sensible que contén, o arquivo NTDS.dit é un obxectivo atractivo para os atacantes. Ao obter acceso a este arquivo, un atacante pode:

- **Roubar contrasinais:** Ao extraer os hashes das contrasinais, un atacante pode intentar descifralas e obter acceso ás contas de usuario.
- **Realizar ataques de Pass the Hash:** Utilizar os hashes directamente para autenticarse en outros sistemas.
- **Tomar o control do dominio:** Ao modificar a información contida no arquivo, un atacante pode tomar o control de todo o dominio de Active Directory.

Como protexelo?

Para protexer o arquivo NTDS.dit, é fundamental implementar medidas de seguridade sólidas, como:

- **Cópias de seguridade regulares:** Realizar copias de seguridade do arquivo NTDS.dit e de toda a base de datos de Active Directory.
- **Controis de acceso:** Restringir o acceso ao controlador de dominio e ao arquivo NTDS.dit a usuarios autorizados.
- **Auditoría de seguridade:** Monitorear a actividade no controlador de dominio e detectar calquera intento de acceso non autorizado.
- **Parches de seguridade:** Manter o sistema operativo e as aplicacións actualizadas cos últimos parches de seguridade.

En resumo:

O arquivo NTDS.dit é un compoñente crítico de Active Directory que almacena unha gran cantidade de información sensible. Comprender a súa importancia e as ameazas ás que está exposto é fundamental para protexer a infraestrutura dunha organización.

Procedemento:

(1) Hosts alumnado. Máquina virtual MS Windows Server 2019[6] 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 [6]
vi. Nome: Practica-Windows-Auditar-DC

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

(c) Configurar a rede según o escenario. Abrir unha consola e executar:

```
> systeminfo #Amosar información de configuración detallada sobre o equipo e o seu sistema operativo
> ipconfig /all #Amosar a configuración TCP/IP completa de todas as interfaces de rede.
```

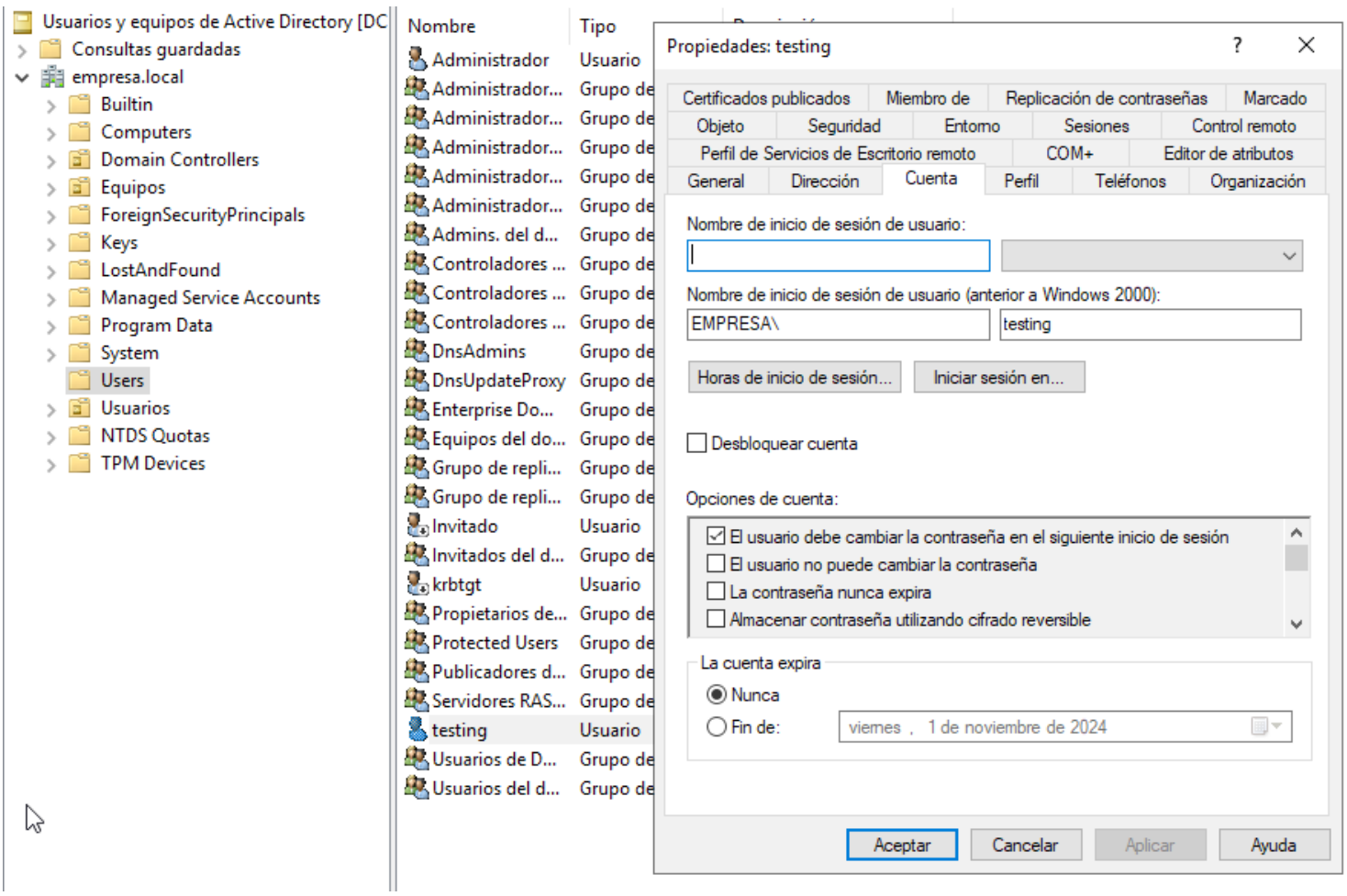
(d) Configurar como controlador de dominio: Rol Servicios de dominio de Active Directory

(e) Crear o usuario según o escenario. Abrir unha consola como administrador e executar:

```
> net user testing rockstar#1 /add /passwordchg:yes /logonpasswordchg:yes /active:yes
```

NOTA: O contrasinal xerado para o usuario testing é rockstar#1

(f) Comprobar a existencia do usuario `testing` en Usuarios y equipos de Active Directory



(g) Abrir unha consola e executar:

```
> powershell "ntdsutil.exe 'ac i ntds' 'ifm' 'create full c:\temp' q q" #Executa a ferramenta ntdsutil.exe e realiza as seguintes accións: activa o modo de directorio, inicia o modo de importación, crea unha copia completa do directorio activo na carpeta c:\temp e finalmente sae dos modos de importación e directorio.
```

Explicación detallada:

- **powershell:** É o intérprete de comandos de PowerShell, unha ferramenta de liña de comandos para automatizar tarefas en sistemas operativos Windows.
- **ntdsutil.exe:** É unha ferramenta de liña de comandos que se usa para administrar o directorio activo de Windows.
- **ac i ntds:** Activa o modo de directorio dentro de Ntdsutil.
- **ifm:** Inicia o modo de importación, que permite crear copias de seguridade do directorio activo.
- **create full c:\temp:** Crea unha copia completa do directorio activo e garda a copia na carpeta c:\temp.
- **q q:** Sae do modo de importación e do modo de directorio.

En resumo:

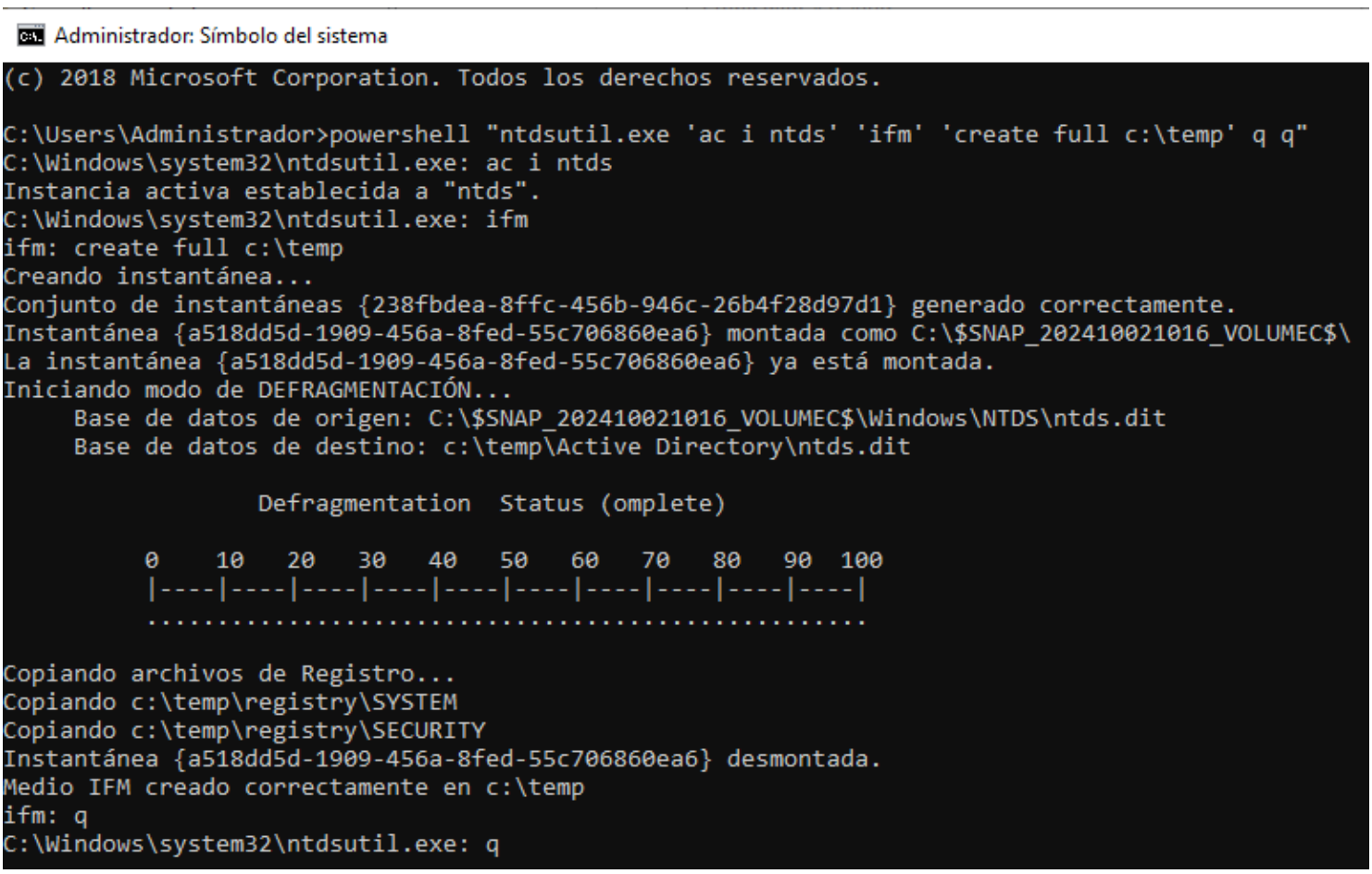
Este comando crea unha copia de seguridade completa do directorio activo nun servidor Windows e garda esa copia nunha carpeta específica. Esta copia pode ser útil para realizar restauracións, análises forenses ou outras tarefas de administración.

Importancia de entender este comando:

- **Seguridade:** Este comando pode ser utilizado para realizar copias de seguridade do directorio activo, o que é fundamental para a recuperación en caso de desastre.
- **Administración:** Permite crear copias para realizar pruebas ou análises sen afectar o sistema en produción.
- **Forense:** As copias creadas con este comando poden ser utilizadas para investigar incidentes de seguridade.

Advertencia:

Este comando debe ser utilizado con coidado, xa que unha copia incorrecta do directorio activo pode causar problemas graves no sistema. Recoméndase ter coñecementos avanzados de administración de sistemas Windows e directorio activo antes de executar este comando.



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

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

i. RAM ≥ 4096MB
ii. CPU ≥ 2
iii. PAE/NX habilitado
iv. Rede: 2 tarxetas de rede,
   - eth0 → NAT
   - eth1 → Rede Interna
v. ISO: Kali Live amd64 [7]
vi. Nome: Practica-Kali-Auditar-DC

(b) O xestor de redes NetworkManager está habilitado. Por defecto, está xerada unha conexión da interface eth0 solicitando a configuración de rede mediante DHCP, e como temos a tarxeta eth0 en modo NAT deberiamos obter a IP 10.0.2.15 e ter conexión a Internet. Así, executar nunha consola:

```
$ setxkbmap es #Configurar teclado en español

$ ip addr show #Amosar información sobre as NIC existentes no sistema, é dicir, verificar a configuración de rede para as NIC: lo, eth0 e eth1

$ ip addr show eth0 #Amosar información sobre a NIC eth0. Verificar que a configuración de rede para a NIC eth0 é a seguinte: IP=10.0.2.15, MS=255.255.255.0

$ ip route #Ver a táboa de rutas do sistema.Verificar que GW=10.0.2.2

$ cat /etc/resolv.conf #Ver o contido do ficheiro /etc/resolv.conf, o cal contén a configuración os servidores DNS a empregar para a resolución de nomes.
```

(c) Imos xerar unha configuración de rede manual. Así, executar na consola anterior:

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

  # /etc/init.d/avahi-daemon stop || systemctl stop avahi-daemon #Parar o demo avahi-daemon(control resolución de nomes) para poder configurar de forma manual a configuración de rede e non ter conflicto con este demo.

  # /etc/init.d/network-manager stop || pkill NetworkManager #Parar o demo network-manager(xestor de rede) ou o script NetworkManager (executado sen ser demo) para poder configurar doutro xeito (co comando ip(ifconfig) de forma manual ou mediante networking (ficheiros /etc/init.d/networking, /etc/init.d/networking.d) a configuración de rede e non ter conflicto con este xestor.

  # ip addr add 10.1.0.10/24 dev eth1 #Configurar a tarxeta de rede eth1, coa IP: 10.1.0.10 e máscara de subrede: 255.255.255.0

  # ip addr show eth1 #Amosar información sobre a NIC eth1. Verificar a configuración de rede para a NIC eth1

  # /etc/init.d/ssh start || systemctl start ssh #Arrancar o servidor SSH

  # exit #Saír da shell

  $
```

(3) Hosts alumnado. Máquina virtual MS Windows Server 2019[6] amd64:

(a) Na anterior consola do usuario administrador executar:

```
> scp -r c:\temp kali@10.1.0.12: #Copiar mediante unha comunicación cifrada o cartafol c:\temp a través do servidor SSH en $HOME(/home/kali) da máquina virtual GNU/Linux Kali amd64 (Practica-Kali-Auditar-DC)
```

```
C:\Users\Administrador>scp -r c:\temp kali@10.1.0.12:
The authenticity of host '10.1.0.12 (10.1.0.12)' can't be established.
ECDSA key fingerprint is SHA256:sVm+bvo7t2HffpShsBDBgeragpkjZVPaRP2RR+0hsJw.
Are you sure you want to continue connecting (yes/no)?
Warning: Permanently added '10.1.0.12' (ECDSA) to the list of known hosts.
kali@10.1.0.12's password:
ntds.dit                                      100%   24MB  96.2MB/s   00:00
ntds.jfm                                      100%   16KB  16.0KB/s   00:00
SECURITY                                      100%   32KB  32.0KB/s   00:00
SYSTEM                                        100%   15MB 185.0MB/s   00:00
```

(4) Hosts alumnado. Máquina virtual GNU/Linux Kali:

(a) Executar nunha consola:

```
$ tree temp #Ver a estrutura arbórea do cartafol temp
temp
├── Active Directory
│   ├── ntds.dit
│   └── ntds.jfm
└── registry
    ├── SECURITY
    └── SYSTEM
3 directories, 4 files
```

```
$ mkdir hashes && cp -pv temp/*/SYSTEM temp/*/SECURITY temp/*/ntds.dit hashes && cd hashes
#Preparar os ficheiros necesarios para poder "dumpear" os hashes das contas de usuarios do DC
$ impacket-secretsdump -system SYSTEM -security SECURITY -ntds ntds.dit local | tee -a hashes.txt
#"Dumpear" os hashes das contas de usuarios do DC do sistemaa operativo Microsoft Windows.
```

O comando `impacket-secretdump` é unha ferramenta poderosa empregada en probas de penetración e auditorías de seguridade para **extraer contrasianis e outra información sensible** dun sistema operativo Windows. Este en concreto, enfócase en extraer os datos almacenados no arquivo **NTDS.dit**, que é unha base de datos fundamental para o funcionamento de Active Directory, o servizo de directorio de Windows, onde:

- **impacket-secretsdump:** É o nome da ferramenta, que forma parte do conxunto de ferramentas Impacket. Esta
- **-system SYSTEM:** Indica que se utilizará a conta de sistema "SYSTEM" para acceder ao archivo NTDS.dit. Esta conta ten os privilexios mais altos no sistema e, polo tanto, pode acceder a calquera recurso.
- **-security SECURITY:** Similar ao anterior, pero neste caso empregase a conta "SECURITY", que tamén ten altos privilexios de acceso.
- **-ntds ntds.dit:** Especifica o nombre do arquivo NTDS.dit que se vai a analizar. Este arquivo soe atoparse no directorio de sistema de Windows.
- **local:** Indica que o arquivo NTDS.dit atópase no sistema local onde está axecutándose o comando.

En resumo:

Este comando, ao executarse, intentará acceder ao archivo NTDS.dit empregando as contas "SYSTEM" e "SECURITY" para extraer información como:

- **Hashes de contraseñas:** Representacións cifradas dos contrasinais dos usuarios.
- **Tickets Kerberos:** Credenciais utilizadas para a autenticación en contornas de rede.
- **Outros secretos del sistema:** Información confidencial almacenada no archivo NTDS.dit.

Importante:

- **Uso autorizado:** Este comando debe utilizarse unicamente coa autorización en sistemas que te perterzan ou nos que teñas permiso explícito para realizar probas de seguridade.
- **Consecuencias legales:** O emprego non autorizado desta ferrramenta pode ser considerado un delito e ter consecuencias legais.
- **Seguridade:** A información obtida con este comando debe tratarse coa máxima confidencialidade e utilizarse unicamente con fins lexítimos.

(b) Copiar da saída anterior os hashes NTLM de `administrador` e `testing` e auditalos nas URLs [2][3][4], é dicir, comprobar nesas URLs se os contrasinais son recoñecidos:

```
3ec585243c919f4217175e1918e07780
a01dc1593b28e5b01cd802fadffb4d5b
```

```
Administrador:500:aad3b435b51404eeaad3b435b51404ee:3ec585243c919f4217175e1918e07780:::
testing:1122:aad3b435b51404eeaad3b435b51404ee:a01dc1593b28e5b01cd802fadffb4d5b:::
```

Cada liña segue o seguinte esquema:

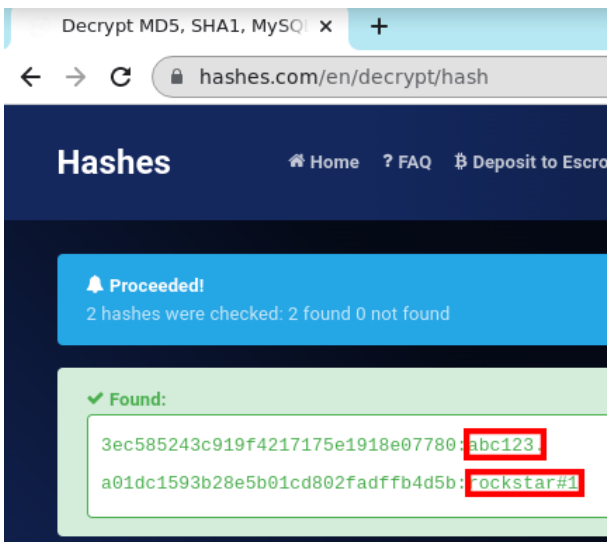
<nome de usuario>:<RID>:<LM hash>:<NT hash>:::

Explicación de cada campo:

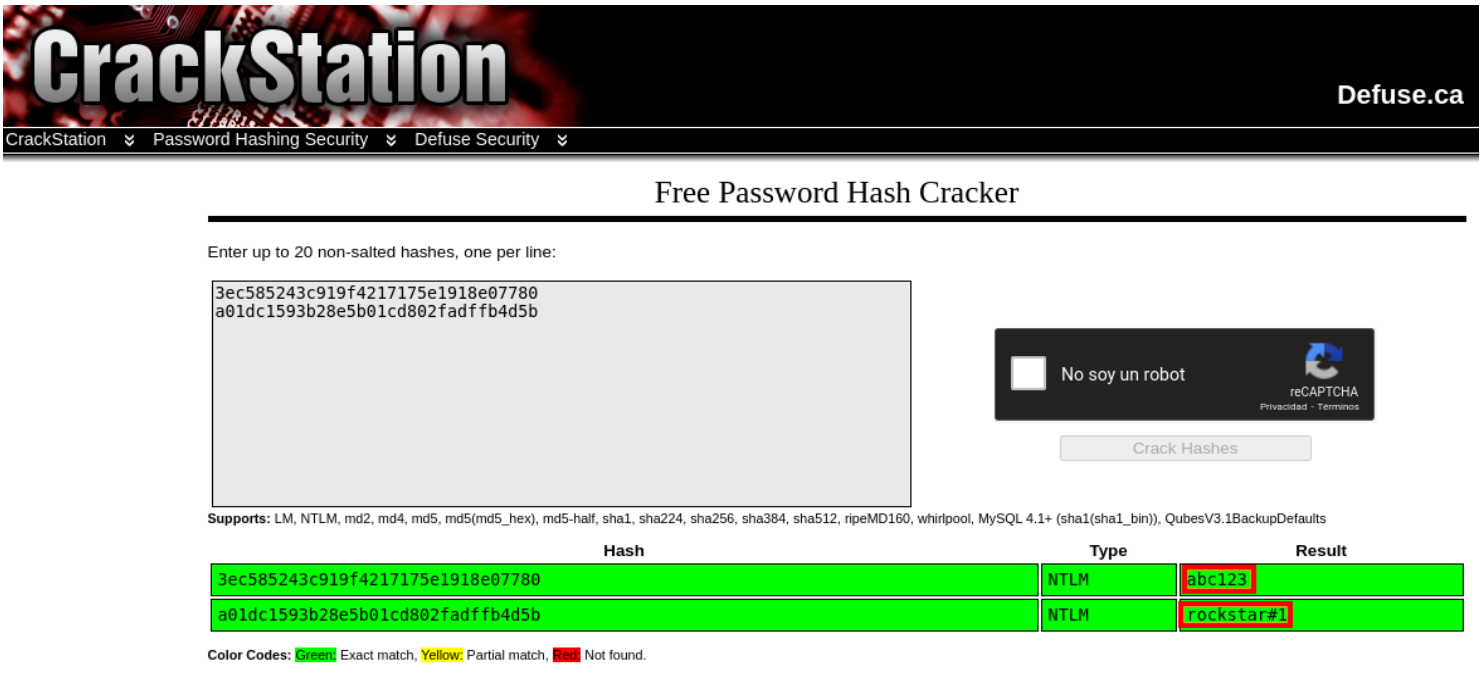
1. **Primeiro campo <nome de usuario>:** Este é o **nome de usuario** da conta.
2. **Segundo campo RID:** Este é o **RID (Relative Identifier)** do usuario. O RID é un número único que identifica de forma inequívoca unha entidade de seguridade nun dominio de Windows. O RID 500 asígnase por defecto á conta do Administrador do sistema local en equipos independentes como ao Administrador de dominio en contornas de Active Directory. Os RIDs a partir do 1000 asígnanse ás contas de usuario e grupos creadas no dominio.
3. **Terceiro campo <LM hash>:** É o **hash LM (LAN Manager)** do contrasinal. O valor `aad3b435b51404eeaad3b435b51404ee` é un valor comunmente empregado para indicar que non se configurou un hash LM. Nos sistemas modernos de Active Directory, o almacenamento de hashes LM soe estar deshabilitado debido ás debilidades de seguridade asociadas con este tipo de hash.
4. **Cuarto campo <NT hash>:** Este é o **hash NTLM (NT LAN Manager)** da conta. Este hash é empregado por Windows para autenticar aos usuarios no dominio. Un atacante que obteña este hash pode intentar usalo para realizar ataques de "pass-the-hash", o que lle permitiría autenticarse no sistema sen necesidade de coñecer o contrasinal en texto claro, ou ben intentar averiguar o contrasinal a partir dese hash mediante ataques por diccionario, forza bruta ou ben páxinas web que posúen unha base de datos de hashes.
5. **:::** Estes campos adicionais poden variar e xeralmente conteñen información sobre as opcións de contrasinal, como se a contrasinal caduca ou se se require cambiar.

(c) Capturar 3 imaxes:

i. imaxe1.png onde ser vexa a través da URLs [2] que os contrasinais foron atopados



ii. imaxe2.png onde ser vexa a través da URLs [3] que os contrasinais foron atopados



iii. imaxe3.png onde ser vexa a través da URLs [4] que os contrasinais foron atopados