Lab - Recuperar contraseñas

Objetivos

- Utilice una herramienta para recuperar las contraseñas de los usuarios.
- Cambiar una contraseña de usuario a una contraseña más segura.

Aspectos básicos/situación

Existen cuatro cuentas de usuario: Alice, Bob, Eve y Eric, en un sistema Linux. También está la cuenta de superusuario Cisco. Las cuentas de usuario en la VM no están destinadas a ser seguras, ya que la VM es un entorno de espacio aislado y no está diseñada para aplicaciones del mundo real. En esta práctica de laboratorio, utilizará John the Ripper, una herramienta de recuperación de contraseña de código abierto, para recuperar las contraseñas de las cinco cuentas.

Recursos necesarios

PC con **CSE-LABVM** instalada en VirtualBox

Instrucciones

Parte 1: Abra una ventana de terminal en CSE-LABVM.

a. Inicie **CSE-LABVM**.

b. Haga doble clic en el icono de **Terminal** para abrir un terminal.

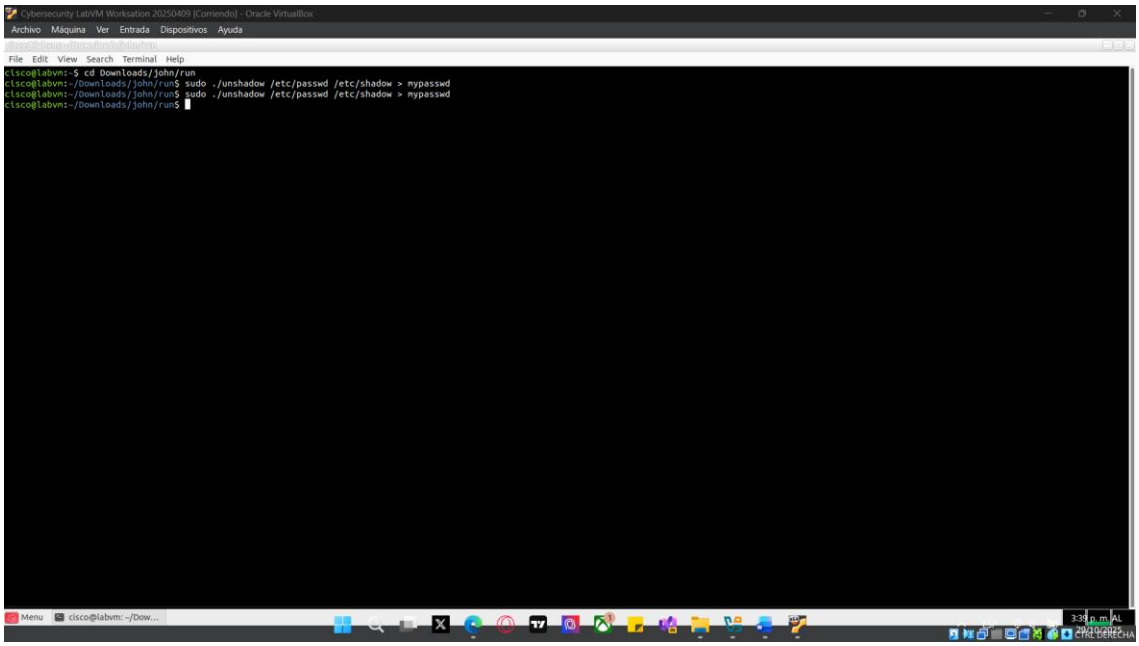
Parte 2: Combinar contraseñas y nombres de usuario en un archivo de texto.

a. Ingrese el siguiente comando para cambiar el directorio donde se encuentra John el Destripador:

```
cisco@labvm:~$ cd Downloads/john/run
cisco@labvm:~/Downloads/john/run$
```

b. Utilice el comando **unshadow** para combinar el archivo **/etc/passwd** donde se almacenan las cuentas de usuario, con el archivo **/etc/shadow** donde se almacenan las contraseñas de usuarios, en un nuevo archivo denominado “**mypasswd**”. Introduzca "**password**" como contraseña de superusuario, si se le solicita. La sintaxis del comando **unshadow** es la siguiente:

```
cisco@labvm:~/Downloads/john/run$ sudo ./unshadow /etc/passwd /etc/shadow > mypasswd
[sudo] password for cisco: password
cisco@labvm:~/Downloads/john/run$
```



Parte 3: Ejecute John the Ripper para recuperar las contraseñas.

a. Para ver que las contraseñas aún no se han recuperado (descifradas), ingrese el comando **./john --show mypasswd**.

```
cisco@labvm:~/Downloads/john/run$ ./john --show mypasswd
Created directory: /home/cisco/.john
0 password hashes cracked, 5 left
cisco@labvm:~/Downloads/john/run$
```

b. El programa, John the Ripper, utiliza un diccionario predefinido llamado **password.lst** con un conjunto estándar de «reglas» predefinidas para administrar el diccionario y recuperar todos los hashes de la contraseña de md5crypt y el tipo de cifrado. En el commando prompt, introduzca el siguiente comando para recuperar las contraseñas almacenadas en el archivo **mypasswd**.

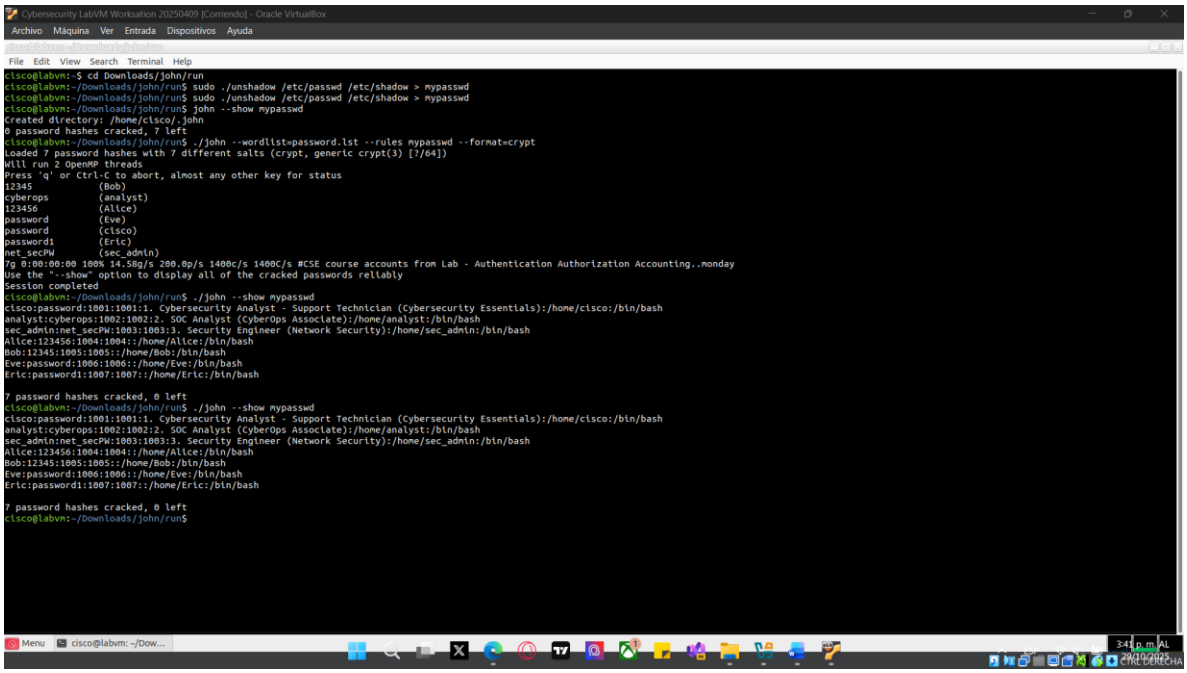
```
cisco@labvm:~/Downloads/john/run$ ./john --wordlist=password.lst --rules
mypasswd --format=crypt
Loaded 5 password hashes with 5 different salts (crypt, generic crypt(3) [?/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
password1        (Eric)
password         (cisco)
password         (Eve)
12345            (Bob)
123456           (Alice)
5g 0:00:00:00 100% 6.097g/s 117.0p/s 585.3c/s 585.3C/s #CSE course accounts from Lab -
Authentication Authorization Accounting..natasha
Use the "--show" option to display all of the cracked passwords reliably
Session completed
cisco@labvm:~/Downloads/john/run$
```

c. Ingrese el comando **./john --show mypasswd** nuevamente para ver si las contraseñas están descifradas.

```
cisco@labvm:~/Downloads/john/run$ ./john --show mypasswd
cisco:password:900:900:Cybersecurity Analyst,,,:/home/cisco:/bin/bash
```

```
Alice:123456:1000:1000::/home/Alice:/bin/bash
Bob:12345:1001:1001::/home/Bob:/bin/bash
Eve:password:1002:1002::/home/Eve:/bin/bash
Eric:password1:1003:1003::/home/Eric:/bin/bash

5 password hashes cracked, 0 left
cisco@labvm:~/Downloads/john/run$
```



Parte 4: Cambie la contraseña de un usuario a una versión más segura e intente recuperarla.

a. Cree su propia contraseña segura o utilice un generador de contraseñas en línea para crear una.

b. Busque un "verificador de seguridad de la contraseña" en línea para probar la seguridad de su contraseña. Su contraseña debería tardar al menos miles de años en descifrarse.

c. Utilice sus privilegios de superusuario para cambiar la contraseña de Eric de **password1** al valor de su nueva contraseña segura. Asegúrese de recibir el mensaje "La contraseña se actualizó correctamente".

```
cisco@labvm:~/Downloads/john/run$ sudo passwd Eric
[sudo] password for cisco: password
New password: <your_new_strong_password>
Retype new password: <your_new_strong_password>
passwd: password updated successfully
cisco@labvm:~/Downloads/john/run$
```

d. Ejecute **unshadow** y luego vuelva a ver a John para ver si puede descifrar la contraseña de Eric. Si cambió la contraseña de Eric por una que sea lo suficientemente sólida como para demorar miles de años en descifrarla, esperará mucho tiempo. Cuando haya terminado de esperar, introduzca **q** o **Ctrl+C** para detener a John the Ripper.

```
cisco@labvm:~/Downloads/john/run$ ./john --wordlist=password.lst --rules
mypasswd --format=crypt
Loaded 5 password hashes with 5 different salts (crypt, generic crypt(3) [?/64])
```

```
Remaining 1 password hash
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:17 7% 0g/s 599.6p/s 599.6c/s 599.6C/s reddog1..mark1
Session aborted
```

e. Ingrese el comando **./john --show mypasswd** para ver que solo se descifraron cuatro contraseñas y que queda una.

```
cisco@labvm:~/Downloads/john/run$ ./john --show mypasswd
cisco:password:900:900:Cybersecurity Analyst,,,:/home/cisco:/bin/bash
Alice:123456:1000:1000::/home/Alice:/bin/bash
Bob:12345:1001:1001::/home/Bob:/bin/bash
Eve:password:1002:1002::/home/Eve:/bin/bash

4 password hashes cracked, 1 left
cisco@labvm:~/Downloads/john/run$
```