Whoami

Pwd

<https://openwall.info/wiki/john>

Extraer y descifrar contraseñas es una técnica avanzada utilizada en pruebas de penetración y auditorías de seguridad para evaluar la robustez de las contraseñas y la seguridad del sistema. Aquí describiré algunos métodos comunes para extraer y descifrar contraseñas utilizando herramientas como Metasploit, John the Ripper y Hashcat.

**Paso 1: Acceso al Sistema**

Antes de poder extraer contraseñas, necesitas tener acceso al sistema objetivo. Esto puede lograrse mediante la explotación de vulnerabilidades, como se explicó anteriormente. Una vez que tienes acceso, puedes proceder con la extracción de archivos de contraseñas.

**Paso 2: Extracción de Hashes de Contraseñas**

En sistemas Windows y Linux, las contraseñas se almacenan de manera encriptada (hashes). Aquí se explica cómo extraer estos hashes en ambos sistemas.

**En Sistemas Windows**

1. **Obtener Hashes con Metasploit**:

Si ya tienes una sesión Meterpreter en el sistema objetivo, puedes usar el módulo hashdump para extraer los hashes de contraseñas:

bash

Copy code

meterpreter > hashdump

Esto mostrará los hashes de todas las contraseñas almacenadas en el sistema.

1. **Extraer Hashes del SAM**:

Si tienes acceso al disco duro del objetivo, puedes extraer el archivo SAM que contiene los hashes de contraseñas:

bash

Copy code

reg save hklm\sam sam

reg save hklm\system system

Luego puedes usar una herramienta como creddump para extraer los hashes del archivo SAM.

**En Sistemas Linux**

1. **Obtener el archivo /etc/shadow**:

En Linux, las contraseñas están almacenadas en el archivo /etc/shadow. Necesitarás privilegios de root para acceder a este archivo:

bash

Copy code

cat /etc/shadow

**Paso 3: Descifrado de Contraseñas**

Una vez que tienes los hashes de contraseñas, puedes usar herramientas como John the Ripper o Hashcat para intentar descifrarlas.

**John the Ripper**

1. **Instalación**:

En sistemas basados en Debian:

bash

Copy code

sudo apt-get install john

1. **Uso Básico**:

Guarda los hashes en un archivo, por ejemplo, hashes.txt, y usa John the Ripper para intentar descifrarlos:

bash

Copy code

john hashes.txt

1. **Opciones Avanzadas**:

Puedes especificar reglas, diccionarios y otras opciones para mejorar el descifrado:

bash

Copy code

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

**Hashcat**

1. **Instalación**:

En sistemas basados en Debian:

bash

Copy code

sudo apt-get install hashcat

1. **Uso Básico**:

Guarda los hashes en un archivo, por ejemplo, hashes.txt, y usa Hashcat para intentar descifrarlos. Primero, debes identificar el tipo de hash que estás tratando de descifrar. Por ejemplo, para hashes NTLM:

bash

Copy code

hashcat -m 1000 -a 0 hashes.txt /usr/share/wordlists/rockyou.txt

* + -m 1000: Especifica el tipo de hash (1000 es NTLM).
  + -a 0: Especifica el modo de ataque (0 es diccionario).

1. **Opciones Avanzadas**:

Puedes usar diferentes modos de ataque, como fuerza bruta, combinaciones, etc.:

bash

Copy code

hashcat -m 1000 -a 3 hashes.txt ?a?a?a?a?a?a?a?a

* + -a 3: Modo de ataque de fuerza bruta.
  + ?a?a?a?a?a?a?a?a: Patrón de ataque para probar todas las combinaciones de 8 caracteres.

**Resumen**

1. **Acceso al Sistema**: Gana acceso al sistema objetivo mediante exploits.
2. **Extracción de Hashes**: Usa herramientas como Meterpreter y comandos del sistema para extraer hashes de contraseñas.
3. **Descifrado de Contraseñas**: Usa herramientas como John the Ripper y Hashcat para intentar descifrar los hashes y obtener las contraseñas en texto claro.

**Consideraciones Éticas y Legales**

* **Permisos**: Asegúrate de tener permiso explícito para realizar estas acciones en el sistema objetivo.
* **Responsabilidad**: Utiliza estas técnicas de manera ética y legal, solo en entornos controlados o con el debido consentimiento.

Este proceso debe ser realizado con cuidado y responsabilidad, asegurando que se sigan todas las leyes y políticas de seguridad aplicables.

4o

como funcion ajohn the ripper?

ChatGPT

John the Ripper es una herramienta de descifrado de contraseñas extremadamente poderosa y versátil. Su funcionamiento se basa en intentar varias combinaciones de contraseñas para descifrar hashes previamente extraídos. Aquí te explico cómo funciona y cómo puedes usarlo paso a paso.

**Instalación**

**En Linux (Debian/Ubuntu)**

Puedes instalar John the Ripper utilizando el administrador de paquetes apt:

bash

Copy code

sudo apt-get update

sudo apt-get install john

**En macOS**

Utiliza Homebrew para instalar John the Ripper:

bash

Copy code

brew install john

**En Windows**

Puedes descargar el binario de John the Ripper desde Openwall y seguir las instrucciones de instalación en la página.

**Uso Básico de John the Ripper**

**1. Obtener Hashes**

Primero, necesitas obtener los hashes de las contraseñas que deseas descifrar. Por ejemplo, en un sistema Linux, los hashes se encuentran en /etc/shadow.

bash

Copy code

sudo cat /etc/shadow > hashes.txt

**2. Preparar el Archivo de Hashes**

Asegúrate de que el archivo de hashes esté en un formato que John pueda leer. Por ejemplo, puedes tener un archivo hashes.txt con el siguiente contenido:

perl

Copy code

user:$6$abcd1234$xyz...:18054:0:99999:7:::

**3. Ejecutar John the Ripper**

Para iniciar el proceso de descifrado, simplemente ejecuta:

bash

Copy code

john hashes.txt

Esto iniciará el proceso de descifrado utilizando un ataque de diccionario predeterminado.

**Opciones Avanzadas**

**Uso de Wordlists**

Puedes especificar un archivo de diccionario (wordlist) para mejorar la efectividad del descifrado:

bash

Copy code

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

**Ataque de Fuerza Bruta**

Para realizar un ataque de fuerza bruta, puedes usar:

bash

Copy code

john --incremental hashes.txt

**Reglas Personalizadas**

John the Ripper permite el uso de reglas personalizadas para generar variaciones de contraseñas. Estas reglas se definen en el archivo john.conf.

**Ver el Estado del Proceso**

Para ver el estado actual del proceso de descifrado:

bash

Copy code

john --status

**Continuar un Proceso**

Para continuar un proceso de descifrado que se ha detenido:

bash

Copy code

john --restore

**Ver las Contraseñas Descifradas**

Para ver las contraseñas descifradas hasta el momento:

bash

Copy code

john --show hashes.txt

**Ejemplo Completo**

Supongamos que tienes un archivo hashes.txt con los siguientes contenidos:

perl

Copy code

user:$6$abcd1234$xyz...:18054:0:99999:7:::

1. **Inicia John the Ripper con un diccionario específico**:

bash

Copy code

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

1. **Monitorea el Proceso**:

bash

Copy code

john --status

1. **Continúa el Proceso si se Interrumpe**:

bash

Copy code

john --restore

1. **Ver las Contraseñas Descifradas**:

bash

Copy code

john --show hashes.txt

**Consideraciones Éticas y Legales**

* **Permisos**: Asegúrate de tener permiso explícito para descifrar contraseñas en el sistema objetivo.
* **Responsabilidad**: Utiliza John the Ripper de manera ética y legal, solo en entornos controlados o con el debido consentimiento.

**Resumen**

John the Ripper es una herramienta poderosa que puede ser utilizada para descifrar contraseñas mediante diversas técnicas como ataques de diccionario y fuerza bruta. Su efectividad puede ser mejorada utilizando wordlists adecuadas y configuraciones personalizadas. Siempre asegúrate de usar esta herramienta de manera responsable y legal.