Passwords en Sistemas operativos

Para esta práctica se necesita:

- Kali Linux versión mayor a 2.0 instalado ya sea en una máquina virtual o nativo.
- John the Ripper instalado
- Archivos diccionario almacenados por defecto en Kali Linux

Parte 1:

En todo sistema operativo al manejar cuentas locales, existe un archivo con la contraseña, en el caso de Windows es el archivo SAM.

En Linux las contraseñas de almacenan en la siguiente dirección /etc/passwd. Adicional a esto, en /etc/shadow existe información sobre las claves que cifran el archivo passwd, y otras contraseñas o tokens importantes del sistema.

Se desea obtener la contraseña de Linux, en una ubicación que podamos manipular fácilmente, para ello se puede utilizar el siguiente comando, que, en este caso, va a tomar el archivo de contraseñas y lo colocará en el escritorio concatenando la información del archivo shadow, con el nombre que le demos, en este caso es "MyPassword" sin ninguna extensión en particular:

cat /etc/passwd > Desktop/myPassword && cat /etc/shadow >> Desktop/MyPassword

Parte 2:

John the ripper es utilizado para encontrar contraseñas cifradas con distintos algoritmos, algunos de ellos:

- UNIX crypt(3)
- Traditional DES-based
- "bigcrypt"
- BSDI extended DES-based
- FreeBSD MD5-based (linux and Cisco IOS)
- OpenBSD Blowfish-based
- Kerberos/AFS
- Windows LM (DES-based)
- DES-based tripcodes
- SHA-crypt hashes (newer versions of Fedora and Ubuntu)
- SHA-crypt and SUNMD5 hashes (Solaris)

Utilizando ya sea John the Ripper o Johnny the ripper, se intentará encontrar la contraseña, siguiendo las instrucciones a continuación:

1. Ejecutar la aplicación utilizando la opción del menú de aplicaciones, apartado de contraseñas.

```
Created directory: /root/.john
John the Ripper 1.9.0-jumbo-1 [linux-gnu 64-bit x86_64 AVX2 AC]
Copyright (c) 1996-2019 by Solar Designer and others
Homepage: http://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]
--single[=SECTION[,..]]   "single crack" mode, using default or named
 rules
--single=:rule[,..]       same, using "immediate" rule(s)
--wordlist[=FILE] --stdin  wordlist mode, read words from FILE or stdi
n
                  --pipe   like --stdin, but bulk reads, and allows ru
les
--loopback[=FILE]          like --wordlist, but extract words from a .
pot file
--dupe-suppression         suppress all dupes in wordlist (and force p
reload)
--prince[=FILE]            PRINCE mode, read words from FILE
--encoding=NAME            input encoding (eg. UTF-8, ISO-8859-1). See
 also
                           doc/ENCODINGS and --list=hidden-options.
--rules[=SECTION[,..]]     enable word mangling rules (for wordlist or
 PRINCE
                           modes), using default or named rules
--rules=:rule[;..]]        same, using "immediate" rule(s)
```

2. Este comando puede utilizarse de diferentes formas, ejecutar la primera que consiste en:
    a. Ubicarse en donde se ha guardado el archivo de contraseñas
    b. Ejecutar el comando john MyPassword
3. Hacer la misma prueba, pero esta vez, utilizando un listado de diccionario existente en Kali, en la ubicación: /usr/share/wordlists/metasploit/unix_passwords.txt
    a. El comando es: john --wordlist="/usr/share/wordlists/metasploit/unix_passwords.txt"

¿Luego del paso 3 ha encontrado la contraseña? Si no, ¿Qué debería hacer para encontrarla con este ataque de tipo diccionario?

Parte 3:

En Windows, el archivo de contraseñas puede encontrarse en la siguiente ubicación: %SystemRoot%\system32\config

Utilizando herramientas como PwDump se pueden obtener los hashes de este archivo SAM.

1. Tome el archivo SamHash adjunto a la práctica e intente encontrar la contraseña utilizando John the Ripper.

Referencias:

https://www.varonis.com/blog/john-the-ripper/

https://www.top-password.com/blog/crack-windows-password-with-john-the-ripper/