CYBERSECURITY

EXPLOITATION: HASHES

Hashing is easy, but unhashing does require calculation power. For this exercise, use a password from one of the wordlists, the rockyou.txt (/usr/share/wordlists/rockyou.txt).

HASH

Choose a password from the rockyou list.

Create a MD5 hash using: https://www.md5hashgenerator.com/

Your String/password:

Your Hash:

Create a NTLM hash using: https://www.browserling.com/tools/all-hashes

Your String/password:

Your Hash:

As you see there are many hash-mechanisms. (This can be a study in itself.)

Put these hashes in different files on your KALI machine.

UNHASH

HASHCAT

Try to unhash your hashes.

Type: hashcat -m 0 hash_md5 /usr/share/wordlists/rockyou.txt –force
Note: use hashcat -h to check the options and explain them.
Document your findings.

How do you unhash your NTLM hash?

Extra:

Which types of attacks can hashcat perform? (use the documentation)

JOHN THE RIPPER

Try to crack the hashes by using “john the ripper”
Type: john --format=raw-md5 -wordlist=/usr/share/wordlists/rockyou.txt hash_md5
Check & document the options: use “john -h” or “man john”
Which 3 modes can john the ripper use to crack passwords?
Retry the command to crack the md5 hash?
What’s the result?
Find the FAQ to see what’s going on.

Find the file that stores the cracked passwords.
Try to delete the found hash and retry.

What command do you use to crack the NTLM hash?
Note this is “difficult” & you have to search for the options…
Document your answer.

IDENTIFYING

MANUALLY

What if you found a key that could be a hash, but you don’t know of which type it is?
A first indication may be given by the length.
See if you can find a list that relates hash-types to their length. Document this.

A second indication might be given by the program which generated the hash.
See if you can find relations between programs and their hash-types. Document this.

AUTOMATICALLY

Use: hash-identifier.
Find out how it works.
Test it with your hashes.
Document your results.

So the NTLM hash isn’t really correctly identified…

Check/try some online hashing identifiers. Document the ones that seem the best.