Password Cracking Challenge 2

Challenge | 32 Solves

Jumbled

50

Password Cracking

I've found a hash of the password for the domain controller.

01F3273F68195C29A1A2365BE7AD2B1AAD469A73

I've also found this note:

Company Password Policy:

- 1 hex digit prepended
- 1 hex digit appended
- First letter capitalised
- An '@' appended to the end
- Leetspeak (a => 4, b => 6, e => 3, g => 9, i => 1, o => 0, s => 5, t => 7, z => 2) [Capital letters not included]
- Example: rockme => fR0ckm37@

Can you crack the hash using rockyou.txt?

The flag is HilltopCTF{password}

Unlock Hint for 10 points

Answer: We are given a hash and a set set of rules on how to crack it using the rockyou wordlist. Lets store the hash in a file called jumble.

The hash is identfied as a SHA1 hash. We can see this using the hashid command in kali. Command: hashid jumble

Next we're going to use hashcat to crack it but first we need to make a rule file to match the password policy: c sa4 sb6 se3 sg9 si1 so0 ss5 st7 sz5 $0 $@ ^0

c = Capitalize the first letter and lower the rest

sa4 = Replace all instances of a with 4

sb6 = Replace all instances of b with 6

se3 = Replace all instances of e with 3

sg9 = Replace all instances of g with 9

si1 = Replace all instances of i with 1

so0 = Replace all instances of o with 0

ss5 = Replace all instances of s with 2

st7 = Replace all instances of t with 7

sz5 = Replace all instances of z with 5

$0 = Append character 0 to end

$@ = Append character @ to end

^0 = Prepend character 0 to front

This string will match the password policy but we need more due to the different hex digits.

Full rule file can be found in jumble.rule.

Now we need to setup hashcat and let it crack the hash. Command: sudo hashcat -m 100 jumble --force rockyou.txt -r jumble.rule

FLAG: HilltopCTF{dCh47rum56@}