WPAssword

Our surveillance team from the cybercrime unit of X , based on their intelligence documents, are inside an operations van in the area of a location owned by criminal organization Y . They succeed to deauthenticate a persona that is connected to a wireless network owned by the criminal organization Y in order to catch a wi-fi handshake . Also from the intelligence , they found out that the security of the wireless network is WPA2. Help the law enforcement to take the next step in their investigation by cracking the wireless password.

Clue:

On the van , a cat hired by the criminal organization , appeared and jumped through the air …... cracking the van’s roof and compromising the whole operation .

Files:

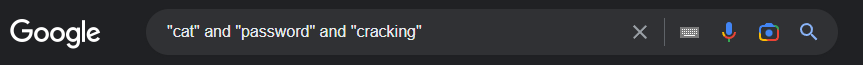
handshake.cap

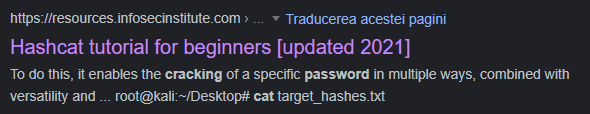
Solve:

If I look at the title of the challenge one of the tags and the format of the flag , I could see that a certain password is involved , a wireless security passphrase .

Secondly , I see that , in the clue , are 3 words that ring in my mind , `cat` , `air` and `cracking` . If I search the web with wildcards I get:

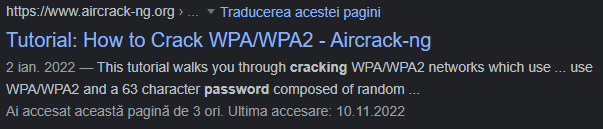
For the `cat`:





For the `air` and `crack`:





So , using OSINT techniques , I found out 2 tools that could crack the password .

Let’s see if WPA/WPA2 has vulnerabilities that I could use to add for the passphrase cracking .

I found a repository on github and a document from an university that includes the cracking of WPA and explains how the vulnerability works :

<https://github.com/koutto/pi-pwnbox-rogueap/wiki/05.-WPA-WPA2-Personal-(PSK)-Authentication>

http://www.cs.toronto.edu/~arnold/427/15s/csc427/tools/aircrack/Aircrack.pdf

Cracking Process:

1. Guess a given Passphrase (PSK)
2. Compute PMK for this Passphrase using: PMK = PBKDF2(HMAC−SHA1, PSK, SSID, 4096, 256)
3. Derivate PTK from the assumed PMK using: PTK = Hash(PMK||ANonce||SNonce||MAC\_AP||MAC\_Client)
4. Use generated PTK to compute a MIC for packet 2,3 or 4 of the captured handshake
5. If computed MIC = MIC of the captured packet => PSK guess is correct
6. Otherwise, go back to 1 & make a new guess.

I will need to validate the MIC with the KCK (Key Confirmation Key) , derived from the PTK .

From the first step , it says that I need to guess a given passphrase . I can create password lists to proceed to a dictionary attack or I can search for one online . A famous dictionary of passwords is rockyou.txt . It can be found at :

<https://github.com/brannondorsey/naive-hashcat/releases/download/data/rockyou.txt>

I will try to crack the password with this dictionary , if is not possible , I could do some social engineering but the SSID does not provide much information provided about the user that uses the WAP .

SOLUTION 1:

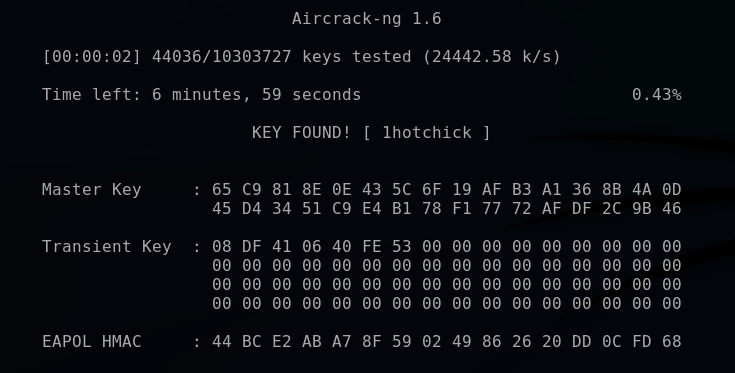
First , let s try with aircrack-ng and then I will provide a second solution to the problem using hashcat.



-w : the wordlist that I use to create the keys and finally to compare the MICs .

-b : the target AP’s MAC address

koko-01.cap : handshake captured



SOLUTION 2:

The hashcat tool doesn’t understand the pcapng , pcap or cap file , we will need to convert the file to a format understandable to hashcat .

With an easy search on the search engine , I found this website that converts my .cap in .hc22000 format that I will use to crack the password with this tool .



-m : the hash type , in my case is WPA-PBKDF2-PMKID+EAPOL (22000)

-w : the workload profile , in my case is High



After I got the password in plaintext , I could easily get a hash from it with a tool or an online generator .

The format of the output is : `MIC HASH`:`S’MAC`:`A’MAC`:`SSID`:`password` .

Flag : CTF{80a3045d4d9aa5b35c97b72b761c69009acfdfb87d806c3e03cb3b04addbb659}

The conclusion is understanding how WPA2 works and that multiple tools can be used for cracking password hashes . Doing this , I have helped the cybercrime unit to continue their investigation .