

Forum:[Hack Forums](#)

Thread: [\[TUT\] Passive sniffing with real-time package decryption](#)

pomwtin - November 28, 2014, 1:22 pm

After a HF member presented his problem, I decided to look deeper into it as I found it very interesting.

Why ?

Unlike sniffing while performing MITM attack with ARP poisoning, ICMP redirection, DHCP spoofing and port stealing, it can not be detected.

But there is one big disadvantage- our monitor can easily miss a package.

First you have to find out AP password- it is needed for package decryption.

After that start monitor mode:

PHP Code

```
<?php
airmon-ng start wlanX -c Y
```

Then open Wireshark and make sure that decryption is disabled!



Ok now you have to find your victim, use airodump-ng to find out who is connected to access point:

PHP Code

```
<?php
airodump-ng monX
```



For real-time decryption we need to capture victim's handshake.

You will only be able to decrypt traffic of victim from who you captured handshake.

If there are multiple victims on AP, you need to capture handshake from all of them.

If that can not be done, you can still capture handshake later, add it into capture file and then use airdecap-ng to decrypt captured packages later.

Here is tutorial about non-real-time package decryption:

<https://hackforums.net/showthread.php?tid=2351236&highlight=sniffing>

We can capture handshakes with deauth attack:

PHP Code

```
<?php
aireplay-ng -0 0 -a accesspointMAC -c victimMAC monX
```

Second "0" means unlimited number of sent packages. Set this to 10 or something for it to stop automatically.

After that, our victim will try to reconnect back to AP, and this will show up in Wireshark:

[img]http://shrani.si/f/2d/124/32u1vE0Z/1-2-3-4.png[/img]

If you do not get all handshake parts, decryption won't be successful:

[img]http://shrani.si/f/44/zr/BAe80Hl/1-3-4.png[/img]

If you do not capture full handshake, repeat deauth attack.
Remember to capture handshake for every specific victim.

Now we need to set WPA/WPA2 password in Wireshark and enable decryption:

[img]http://shrani.si/f/0/RS/1iX39q4w/setting-password.png[/img]

and non-SSL packages will be decrypted:

[img]http://shrani.si/f/p/ds/3mWTWmgB/decrypted-data.png[/img]

As I mentioned before, this is sniffing without performing MITM attack, so it can not be detected. But it is only useful if victims and AP signal strength is very good.

This works on WEP and WPA/WPA2 encryption, for presentation I used WPA2 protected network.

Hope somebody finds it useful or at least informative ?

TheCyb3rAlpha - November 28, 2014, 11:05 pm

very informative!

Good work mate!

but I have a question.

Why do we need a complete 4-way handshake when we can do it in 2 messages? If I recall, for cracking WPA2 password using dictionary attack, one needs to have just Message 1 and 2 EAPOL packets. The cracking would be successful in this way too. And in the above tutorial, you mentioned that you need to have a complete 4-way handshake for live sniffing but again how did you get the password? Did you crack it? Even for cracking, like I said, needs only Message 1 and 2 is required at the least. After finding out the password, you set it to the decryption keys in Wireshark so I don't think that all the messages are needed.

pomwtin - November 29, 2014, 3:35 am

thanks :)

about handshake:

That's what I taught, but I did not manage to capture only 1 and 2, so I look it up on link below, where it says that you need complete 4-way handshake.

link: <http://wiki.wireshark.org/HowToDecrypt802.11>

Yes password was already known.

However without handshake Wireshark is unable to calculate keys for decryption.

TheCyb3rAlpha - November 29, 2014, 4:14 am

oh ok. thanks for the info.

As we are monitoring the live session, wireshark CAN decrypt with the 2 messages BUT ONLY IF there was NO multicast or broadcast packets in the flow (which is obviously impossible because those packets will be there) so i guess for decrypting the whole live session, wireshark needs to have the GTK from message 3 for decryption.

Did you try the same with only message 1,2 & 3?

I think it should work that way.

what do you think?

TheCyb3rAlpha - November 29, 2014, 4:16 am

oh ok. thanks for the info.

As we are monitoring the live session, wireshark CAN decrypt with the 2 messages BUT ONLY IF there was NO multicast or broadcast packets in the flow (which is obviously impossible because those packets will be there) so i guess for decrypting the whole live session, wireshark needs to have the GTK from message 3 for decryption. Could this be the case?

Did you try the same with only message 1,2 & 3?

I think it should work that way.

what do you think?

TheCyb3rAlpha - November 29, 2014, 4:17 am

oh ok. thanks for the info.

As we are monitoring the live session, wireshark CAN decrypt with the 2 messages BUT ONLY IF there was NO multicast or broadcast packets in the flow (which is obviously impossible because those packets will be there) so i guess for decrypting the whole live session, wireshark needs to have the GTK from message 3 for decryption. Could this be the case?

Did you try the same with only message 1,2 & 3?

I think it should work that way.

what do you think?

sorry about so many posts. network problem here.

pomwtin - November 29, 2014, 4:49 am

Well since the fourth part is only station sending confirmation to AP, i think you are right about that there is no need of fourth part.

Step 4 is not really necessary to decrypt packages, but if there is no 4/4, then station and AP won't start using encryption key.

Wireshark may stop decrypting data because of this.

I think that we would need to study wireshark manual first, so we know how exactly its made (lets say there is if loop counting eapol messages and it do not allow decryption until there are all four of them, or maby 1/4, 2/4 and confirmation 4/4... this may be stupid but is possible)

TheCyb3rAlpha - November 29, 2014, 4:56 am

There is one more option that we can choose to decrypt the live session but its a long shot!

We can run Airodump (i prefer airodump because it monitors the packets in the air very effectively

but wireshark have some issues with that, it does miss some packets) and at the same time we can use airdecap-ng on the file in which airodump is writing the packets and simultaneously opening that file in wireshark.

LOL i know its a very long shot but if there can be a program which can do all of this at run-time would be something!

pomwtin - November 29, 2014, 5:07 am

Hehe yes that would be very nice :D

Nagga - July 1, 2015, 3:14 pm

Is it important to deauth all victims in AP ?

I tried in home

First captured handshake with airodump-ng and starting wireshark

then i deauth my pc and reconnecting him while typing the password ,but i can't find in wireshark key messages im doing something wrong

I have 2 more devices connect to AP

Good work btw ?

pomwtin - July 1, 2015, 3:33 pm

I think you misunderstood this tutorial a bit.

Thos tutorial is for passive sniffing- wifi password must already be known.

You need to capture handshake of each target you wish to decrypt traffic.

These are 4 EAPOL messages.

After that, you enter wifi key into wireshark and decrypt data.

If you do not have wifi password, you would need to get it first (handshake cracking, wps, fake AP, rat,...)

If you are having trouble with EAPOL capture, make sure that you hear (good signal) both, client and AP well.

This may be solved with "airmon-ng check kill" before monitor creation- it will kill any processes which could interfere with airmon-ng

Nagga - July 1, 2015, 3:55 pm

(Jul 1, 2015 03:33 PM)pomwtin Wrote: [\[CITE\]](#) I think you misunderstood this tutorial a bit.

Thos tutorial is for passive sniffing- wifi password must already be known.

You need to capture handshake of each target you wish to decrypt traffic.

These are 4 EAPOL messages.

After that, you enter wifi key into wireshark and decrypt data.

If you do not have wifi password, you would need to get it first (handshake cracking, wps, fake AP, rat,...)

If you are having trouble with EAPOL capture, make sure that you hear (good signal) both, client and AP well.

This may be solved with "airmon-ng check kill" before monitor creation- it will kill any processes which could interfere with airmon-ng Oh yea i see now ... i though you can steal wifi password with wireshark when you get handshake and i was so happy because i don't have much success with reaver and cracking .cap ^^

This is great gonna try it now

pomwtin - *July 1, 2015, 4:53 pm*

Oh well, sadly it is not so simple to get wifi password :)

Long story short, this is just a method to capture client<-->ap traffic without leaving any traces