

Forum:[Hack Forums](#)

Thread: [\[Tut\] WPA/WPA2 handshake Capture \[For Noobs\] \[Very detailed\] \[Kali/ BT5\]](#)

Shashwat7 - June 14, 2014, 12:52 am

Yesterday someone asked me to write a tutorial on WPA handshake capturing on my blog. Most of the WPA hacking tutorials have just a few lines devoted to capturing handshake and rest of the tutorial focuses on cracking the handshake instead. However, many times people face problems in what seems to be a very easy step. To start with, some people complain that wlan interface does not show up on their machine. This is because they are using Kali/BT5 on virtual machine, and it doesn't use internal wireless hardware. Secondly, sometimes deauth doesn't work, as the card doesn't support it. Also, sometimes the clients and AP are too far, so the router's wireless signals can reach us (router has more power), but our AP's packet injection doesn't have enough range. This tutorial discusses all such problems faced during handshake capture, and I personally used poor adapters to demonstrate the failure practically, before using good adapters and finally capturing the handshake. Also, this tutorial shows you how to use wifite as well as airodump-ng to capture the handshake, and use aireplay-ng for deauthentication.

I tried to copy and paste the tutorial from my blog to this thread, but the copied version here was devoid of font colors and size, and all the pics were missing. It wasn't readable at all, and considering the huge length of tutorial (beginner friendly), I decided formatting it again here to help people read through the length and breadth of the tutorial will be very tough and time consuming. So I guess I'll just post the link to the tutorial here. It'll do me some good too, as you can check out other good posts, and you are surely going to love it (if you're a beginner especially), so I'll get new audience for my blog. So here's the tutorial.

[Capture Wpa handshake](#)

^Click here or use this URL

<http://www.kalitutorials.net/2014/06/hack-wpa-2-psk-capturing-handshake.html>

Also guys, if you take a look at the post, and think it is really what it claims to be, please reply to this thread with somewhat of a vouch (like yes it really is beginner friendly, not a scam, OP isn't lying). People usually hesitate to visit external sites so this will help them. It also keeps the thread alive, and pays off the effort I took in writing that post. Thank you ?

Boshi - June 14, 2014, 1:47 am

ok great, so wheres the tut? hf link or such pl0xxx sounds good tho +rep if informative

(Jun 14, 2014 12:52 AM)Shashwat7 Wrote: [\[CITE\]](#) Yesterday someone asked me to write a tutorial on WPA handshake capturing on my blog. Most of the WPA hacking tutorials have just a few lines devoted to capturing handshake and rest of the tutorial focuses on cracking the handshake instead. However, many times people face problems in what seems to be a very easy step. To start with, some people complain that wlan interface does not show up on their machine. This is because they are using Kali/BT5 on virtual machine, and it doesn't use internal wireless hardware. Secondly, sometimes deauth doesn't work, as the card doesn't support it. Also, sometimes the clients and AP are too far, so the router's wireless signals can reach us (router has more power), but our AP's packet injection doesn't have enough range. This tutorial discusses all such problems faced during handshake capture, and I personally used poor adapters to demonstrate the failure practically, before using good adapters and finally capturing the handshake. Also, this tutorial shows you how to use wifite as well as airodump-ng to capture the handshake, and use aireplay-ng for deauthentication.

I tried to copy and paste the tutorial from my blog to this thread, but the copied version here was devoid of font colors and size, and all the pics were missing. It wasn't readable at all, and considering the huge length of tutorial (beginner friendly), I decided formatting it again here to help people read through the length and breadth of the tutorial will be very tough and time consuming. So I guess I'll just post the link to the tutorial here. It'll do me some good too, as you can check out other good posts, and you are surely going to love it (if you're a beginner especially), so I'll get new audience for my blog. So here's the tutorial.

[Capture Wpa handshake](#)

Also guys, if you take a look at the post, and think it is really what it claims to be, please reply to this thread with somewhat of a vouch (like yes it really is beginner friendly, not a scam, OP isn't lying). People usually hesitate to visit external sites so this will help them. It also keeps the thread alive, and pays off the effort I took in writing that post. Thank you ?

Ahhh very sorry mate, i read this a few minutes later on a computer, the link didnt display on on tablet. I suggest keeping this away from beginners, skuds are starting to read and will abuse shit like that making life harder for everyone. +Rep for the tut tho

SW4T - June 14, 2014, 1:51 am

(Jun 14, 2014 01:47 AM)Boshi Wrote: [\[CITE\]](#) ok great, so wheres the tut? hf link or such pl0xxx sounds good tho +rep if informative

There is the words "Capture WPA handshake". If you click on that, you'll find the tutorial.

Also you can't +rep.

Shashwat7 - June 14, 2014, 2:56 am

(Jun 14, 2014 01:47 AM)Boshi Wrote: [\[CITE\]](#) ok great, so wheres the tut? hf link or such pl0xxx sounds good tho +rep if informative

Ahhh very sorry mate, i read this a few minutes later on a computer, the link didnt display on on tablet. I suggest keeping this away from beginners, skuds are starting to read and will abuse shit like that making life harder for everyone. +Rep for the tut tho

Yeah the link wasn't really obvious (too many colors and the link doesn't stand out). Might not be clearly visible on the tablet.