

Forum:[Hack Forums](#)

Thread: [\[TUT\] Hacking WEP-WPA-WPA2 \[TUT\] NOOB FRIENDLY](#)

kodamafire - May 29, 2014, 11:10 am

THIS TUTORIAL IS (HOPEFULLY) GOING TO TEACH YOU HOW TO CRACK WEP,WPA(2) USING BACKTRACK/ KALI LINUX

Step 1: Downloading VMware Workstation, and installing it correctly. and this can be found here: <http://www.vmware.com/products/workstation>

Step 1.5: Once you have step 1 complete it should look something like this:

[img]http://4.bp.blogspot.com/-5XBLme77III/UkTzOfGHVsI/AAAAAABGlo/X7_y29xtyO8/s1600/VMware+Workstation+Version+10.0.0+Captura+1.jpg[/img]

Step 2: You will need to download Kali Linux/ Backtrack. Which you can download from here: <http://www.kali.org/>

Step 2.5: Once you have downloaded Kali run it through VMware and it, and it should look somewhere along the lines of this

[IMG]<http://i461.photobucket.com/albums/qq331/Kodamafire/Untitled-1.png>[/IMG]
side note; Username:root Password:toor

Step 3: Once you have all these steps completed open up Kali and type in your password and username, and open a new terminal up (which is in top left corner, looks like command prompt) once you have done that, should look something like this:

[IMG]<http://i461.photobucket.com/albums/qq331/Kodamafire/Untitled-2.png>[/IMG]

Step 3: These next steps we are getting onto commands. Read carefully because one misspelt word or not putting punctuation will make you hate life.

In the terminal type "airmon-ng" Nooo space. And you'll get something that looks like this:

[IMG]<http://i461.photobucket.com/albums/qq331/Kodamafire/Untitled1-1.png>[/IMG]

Side note; you have to a wireless adapter that will pick up and transmit a signal. Not all wireless cards have this capability.

Step 4: Once you have that all done type "airmon-ng start wlan0" you'll get a list and you'll have to start the process of "looking" In this case mine is called Wlan0. Yours could be different. It'll look like this:

[IMG]<http://i461.photobucket.com/albums/qq331/Kodamafire/Untitled11.png>[/IMG]

Step 5: Now hit enter and it will give you some mumbo jumbo. Now its time to "wash" which means now we start looking for points to access. type "wash -l mon0" and then you'll get this:

[IMG]<http://i461.photobucket.com/albums/qq331/Kodamafire/Untitled3.png>[/IMG]

SIM-1550131 - May 29, 2014, 11:12 am

That's nice, but where is the tutorial? o.O

Threat? - May 29, 2014, 11:12 am

Thanks OP for the title suggestion, will use in the future

kodamafire - May 29, 2014, 11:14 am

Sorry hit post. instead of post preview :/ will be done after a while

SIM-1550131 - May 29, 2014, 11:14 am

(May 29, 2014 11:14 AM)kodamafire Wrote: [\[CITE\]](#) Sorry hit post. instead of post preview :/ will be done after a while

Haha its okay, everyone makes mistakes. Looking forward to seeing it.

Mr. Mayhem - May 29, 2014, 11:35 am

(May 29, 2014 11:14 AM)kodamafire Wrote: [\[CITE\]](#) Sorry hit post. instead of post preview :/ will be done after a while

Ok man ,take your time buddy. hope is worth it ?.

kodamafire - May 29, 2014, 1:04 pm

DAMNIT! did it again :/ sorry guys! :/
still not finished yet. Soon tho :)

Hidden™ - May 29, 2014, 1:05 pm

Nice tutorial but it needs a bit more added on to it.

shrekyboi - July 8, 2018, 6:29 pm

The wash command is to find routers with wps enabled, which is useful for pixiedust attacks and reaver in general.

one you have the bssid and channel of the routers listed from the wash command you can run

Normal attack: Reaver -i (wireless interface e.g. wlan0mon) -b (bssid # of router u want to get) -c (channel of router)

Pixiedust attack:(much faster attack, typically takes less then 30 seconds but does not work on all routers)

Reaver -i (wireless interface e.g. wlan0mon) b (bssid # of router u want to get) -c (channel of router) -K

and obviously their are more options if you type reaver -h

just some starting points, not trying to hijack the thread though, just trying to help some people who are waiting for the full guide.

SchwererGustav - July 9, 2018, 4:06 am

it s not complete yet , we are looking forward for it ,but hopefully not the same method of aireplay-ng or else i will cry cause it won t work unless you have a wordlist and these things couldn t work anymore

L33TV13W3R - July 31, 2018, 1:23 pm

Thanks for sharing dude!!!!