How I hacked into my neighbour's WiFi and harvested login credentials?

Aditya Anand Follow
Jul 30, 2018 · 5 min read

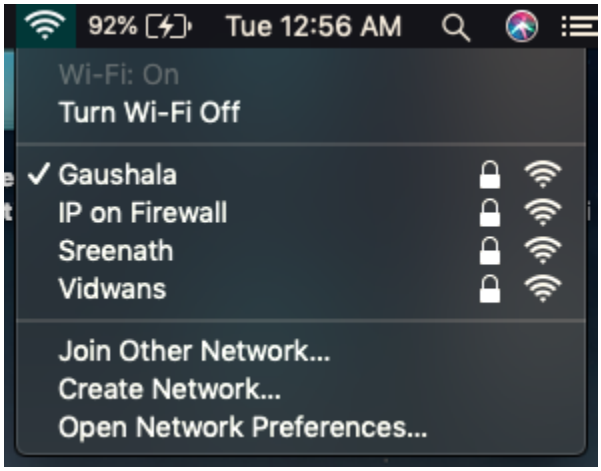
It has been almost a week since I wrote my last article, which gained a lot of attraction.

> *How I pranked my friend using DNS Spoofing?*

Since, then I have been playing around with network sniffing tools and trust me there is a different kind of high you get when you sniff the traffic of networks. The thing is it's not much fun when you are sniffing your own network, you know what's the traffic is going to be and all. The fun begins when you are on someone's else network, that's when the thrill starts. You go through each and every Wireshark packet carefully, hoping to find login credentials or something valuable of sorts. That's when I decided let's hack into the nearby WiFi network and sniff out the packets.

Let's begin!

So, to begin with the hack first I had to search for different WiFi signals in the nearby area, there were a few of them.

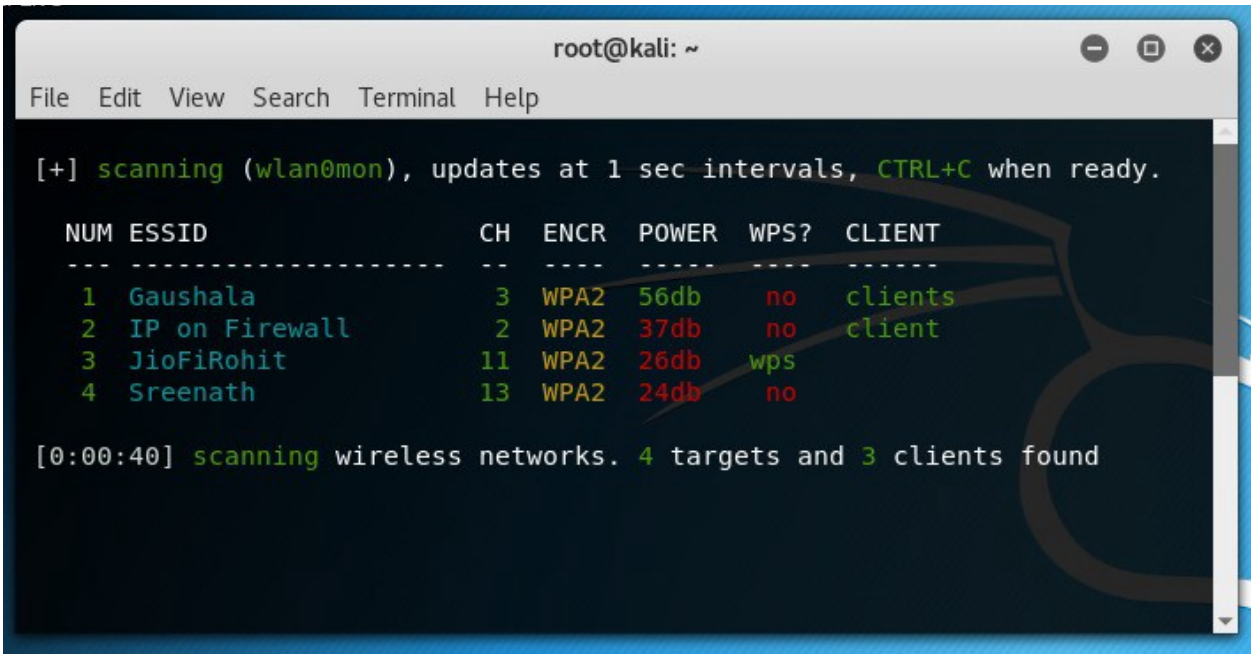


WiFi Networks

Once, I checked for the WiFi networks then I turned on my Kali machine to hack into one of these networks. I opened up my terminal and typed in

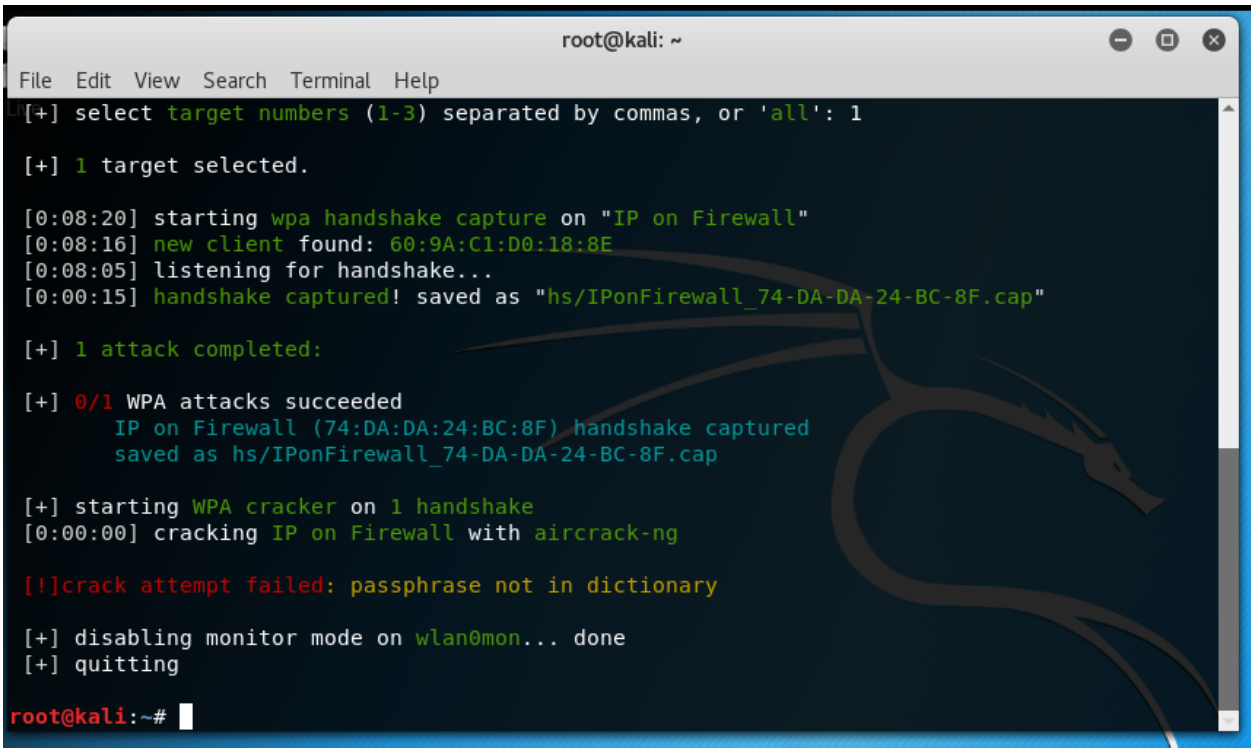
> *wifite*

Wifite, is one of the most user friendly tool out there you can use for hacking WiFi (that's just my opinion). The information shown below popped up.



WiFi Networks

Now if you are a hacker, then you already know which network I would have tried to hack in. Yes, "IP on Firewall". I mean if you name your WiFi, Firewall then it is like asking nearby hackers to mess with you, and so I choose it.



WiFite Packet Capture

As soon, as the target was selected " wifite " ran the packet capture for "IP on Firewall", it found the hosts connected to it and sent out de-auth packets for a few moments till the time the device was disconnected. Once the device got disconnected, the device tried to connect back to the WiFi router and during this process " wifite " captured the packet with the password for the WiFi in encrypted form.

Now, that once the capture file was present with me. I ran it against the rockyou.txt wordlist file using aircrack-ng, the command was as follows.

> *aircrack-ng -w rockyou.txt -b <bssid> <capture file name>*

I let it run for a few minutes at max, when I got a hit on the password.

Aircrack-ng Password Crack

Once, I obtained the password, the next thing was to go ahead and sniff-out their traffic and look for interesting things.

Sniffing the packets

I was feeling ecstatic as soon as I figured out the password of IP on Firewall. The reason was, if they had not used such a simple password which was present in the rockyou.txt file, then the whole process would have been bogged down, I guess it was my lucky day.

Once I got into the network then I started ettercap, (one of the best tool out there to sniff packets). I wanted to capture each and every packet on their network, so I opened up terminal and typed in the following command.

> *ettercap -T -M arp -i eth0 /// -w test.cap*

(To refer the ettercap tutorial visit here : Ettercap Packet Sniffing)

As soon as I initiated the ettercap, tons and tons of traffic was passing through on my terminal screen. I saved it all to the test.cap so that I can later on go through each and every packet on my device using Wireshark for detailed inspection.

If you want to go through the traffic on your Kali machine then you can use the following commands

> *cat test.cap | grep -a <keyword>*

Using the above command you can search for the keyword you want to search for, the below command gave me the following output

> *cat test.cap | grep -a password*

Capture from test.cap document

Once, I transferred the file to my laptop for further inspection I picked up many other login credentials which were entered on HTTP websites. The websites the users were visiting and many other interesting information.

test.cap on wireshark

So, now you know why there is such a high about intercepting other people’s traffic.

Moral

The biggest take away from this hack is to never use HTTP websites and above all never use your credentials to login on those websites. You may never know who else might be sniffing the network and they will pick up your login credentials all just by viewing the network traffic. If feasible then use your VPN services to encrypt your traffic,

they provide you with security no matter where you are. So the next time you encounter websites that are not https, just run away or be really careful to not leak anything personal information.

If you enjoyed it please do clap & let's collaborate. Get, Set, Hack!

Website : aditya12anand.com | Donate : paypal.me/aditya12anand

Telegram : https://t.me/aditya12anand

Twitter : twitter.com/aditya12anand

LinkedIn : linkedin.com/in/aditya12anand/

E-mail : aditya12anand@protonmail.com