2012

[WiFi Internet Connection Hacking]

[WEP , WAP2 Penetration Test]

[ယခု စာအုပ်လေးဖြင့် မြန်မာနိုင်ငံမှ နည်းပညာ သမား ကိုညီမောင်နမများအား ကျွန်တော် မင်းစိုးရာစာမှ မိတ်ဆက်ခြင်းဖြစ်ပါသည်။ မှားသည်ရှိသော် ခွင့်လွှတ် နားလည်ပေးပါ။ မှန်ခဲ့တာများပါခဲ့ရင် ဖြစ်မြောက်အောင် လေ့လာပါ သင်ယူပါ။ စာဖတ်ပါသနာ ရှင်များ အားလုံးကို လေးစားလျှက်ပါ။]

-=[www.minsoeyarsar.com]=-

-= Myanmar0boy@gmail.com =-

မင်းစိုးရာစာ ၏ စမ်းသပ်ချက်များ စုစည်းမှု

N3tL0v3r
[Type the company name]

WiFi Hacking Basic အားဖောက်ထွင်းလေ့လာခြင်း

ကျနော်တို့ နိုင်ငံမှာ ဂိုင်ဖိုင်လိုင်းတွေ အရင်ထက်စာရင် တော်တော်လေး များလာပါပြီ။ ကြား မိတာကတော့ မြန်မာနိုင်ငံမှာ ၂၀၁၃ အတွင်း ရန်ကုန်မြို့ မှာ wifi free လိုင်းရရှိအောင်ပြု လုပ်ပေးမယ်လို့ တော့်ကြားနေရပါတယ်။ ဘယ်လောက်ဘဲဘာယ်လိုပြောပါစေဗျာ။ wifi free ပေးတယ်ဆိုတာ သူတို့ ပြောတာပါ။ လက်တွေ့ ကတော့ စောင့်ကြည့်ရအုံးမှာဘဲဖြစ်ပါတယ်။ဒီနည်းလေးကတော့ Educational Purpose Only အဖြစ်သာရေးသားပေးခြင်းဖြစ်ပါတယ်။ အခုနည်းကို အသုံးပြု ပြီး wifi လိုင်းအကုန်လုံးကို

ဖောက်ထွင်းနိုင်သည် ဟု ကျွန်တော်မဆိုလိုပါဘူး။ အခုနည်းကိုသိရင် အရင်က သင်သိထားသည်ထက် ပိုမိုနည်းလည်တတ်ကျွမ်းသွားမှာဖြစ်ပါတယ်။ ကျွန်တော် လေ့လာခဲ့သမျှ ကို မှတ်စုအနေနဲ့ ချရေးပေးတဲ့သဘောမျိုးသာဖြစ်ပါတယ်။ အခုစာအုပ်လေးကတော့ကို Ethicokiddie ရဲ့ စာအုပ်ကို ပြန်ပြီး update ပြု လုပ်ရေးသားခြင်းမျိုးသားဖြစ်ပါတယ်။

လိုအပ်သော သော Software များ

အခုအသုံးပြု သွားမှာကတော့ BackTrack 5 ကိုအသုံးပြု သွားမှာဖြစ်ပါတယ်။ Window boot ဖြစ်အသုံးပြု နိုင်သလို VMware များအားအသုံးပြု ပြီးတော့လည်း စမ်းသက်နိုင်ပါတယ်။

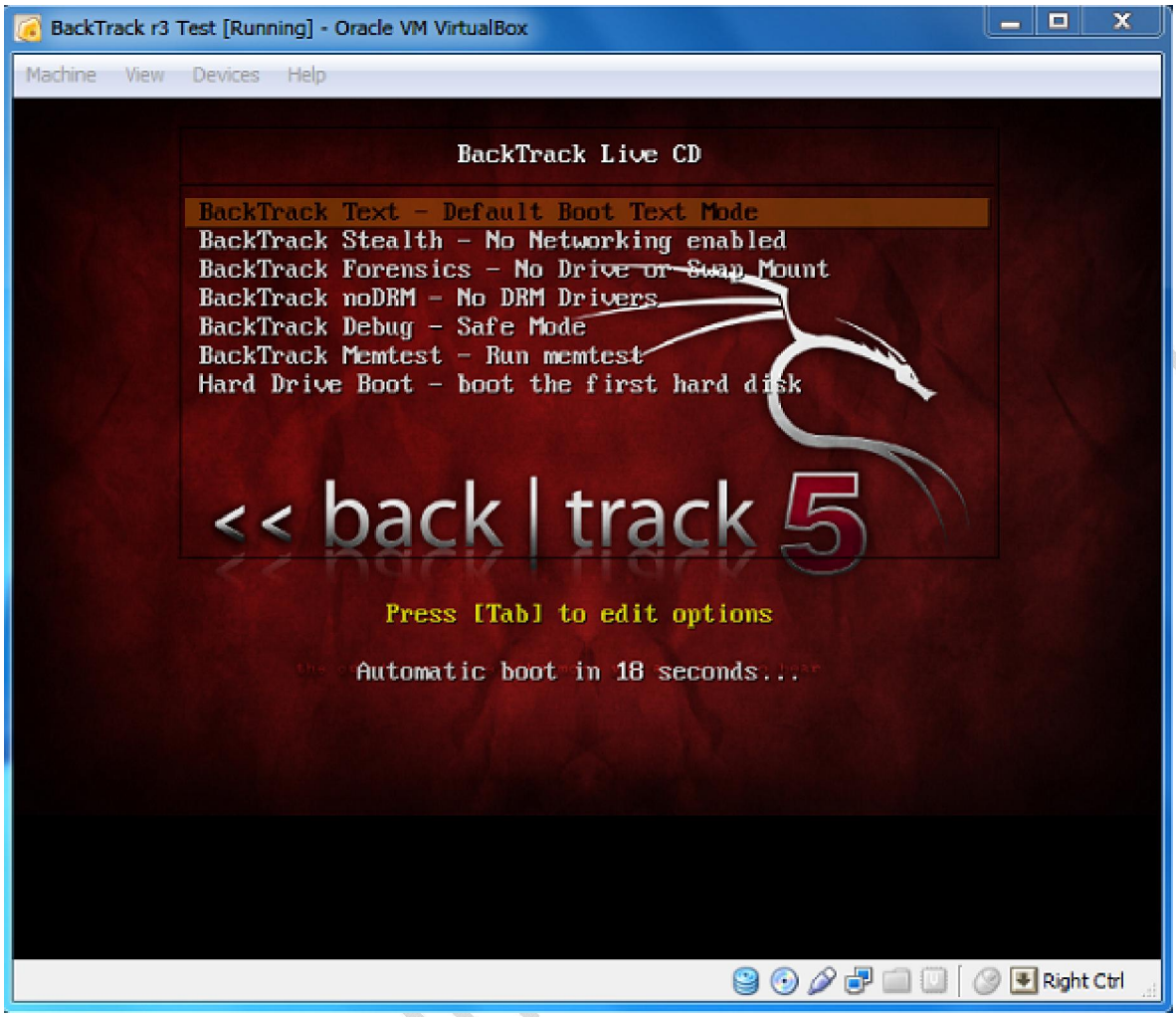
Back Track 5 အခွေတွေအခုဆိုရင် လူအများ စုလက်တည်းကိုရောက်ရှိနေပြီဖြစ်ပါတယ်။
မရှိသေးသူများကတော့ www.backtrack-linux.org တွင် Download ရယူနိုင်ပါတယ်။

Download ပြု လုပ်ပြီးသား ဖိုင်အား DvD အခွေ အဖြင် Burn ရပါမယ်.. ပြီးရင် Window First boot ကို CD ROM (or) DVD ROM သို့ ပြောင်းပေးထားရပါမယ်..အခွေ အနေဖြင့် boot တတ်ပြီဆိုတာနဲ့ startx ကို နှိပ်ပြီး ဂင်ရောက်ရမှာဖြစ်ပါတယ်။

VMware တည်းမှာ အသုံးပြု သူများအတွက် အခွေကို DVD Boot အနေဖြင့် အသုံးပြု ပါက OS ၏ Full Speed ကိုရရှိနိုင်မည်မဟုတ်ပါဘူး။ ဒါကြောင့် VMware တည်းတွင် BackTrack OS ကို Install ပြု လုပ်ပြီးအသုံးပြု လျှင် ပိုမို အဆင်ပြေမယ်ဖြစ်ပါတယ်။ ပြီးတော့ wifi adapter တစ်ခုလိုပါမယ် ။
လက်တော့တွေမှာတော့ပါပြီးသားပါ။

BackTrack 5 အား Install ပြု လုပ်ပုံ

အရင်ဆုံး BackTrack 5 အား DVD ခွေဖြင့် VMware တည်းတွင် Boot တင်ပါ။ အမြဲရောင်Box လေးတစ်ခု ကျလာပါမယ် ။ Boot: ဆိုပြီးတော့ ကျလာခဲ့ရင် ဘာမှ မနှိပ်ဘဲ Enter ခေါက်လိုက်ပါ အောက်ကပုံအတိုင်း ထပ်မံ ကျလာပါလိမ့်မယ်။



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

အခုဆိုရင်တော့ ကျွန်တော်တို့ BackTrack 5 ကိုအသုံးပြု နိုင်ပြီဖြစ်ပါတယ်။

Back Track ဆိုတာ Linux အခွယ်ပင်တစ်ခုပါ Security သမားရော ၊ Hacker တွေပါအသုံးပြု နေကြပါတယ်။

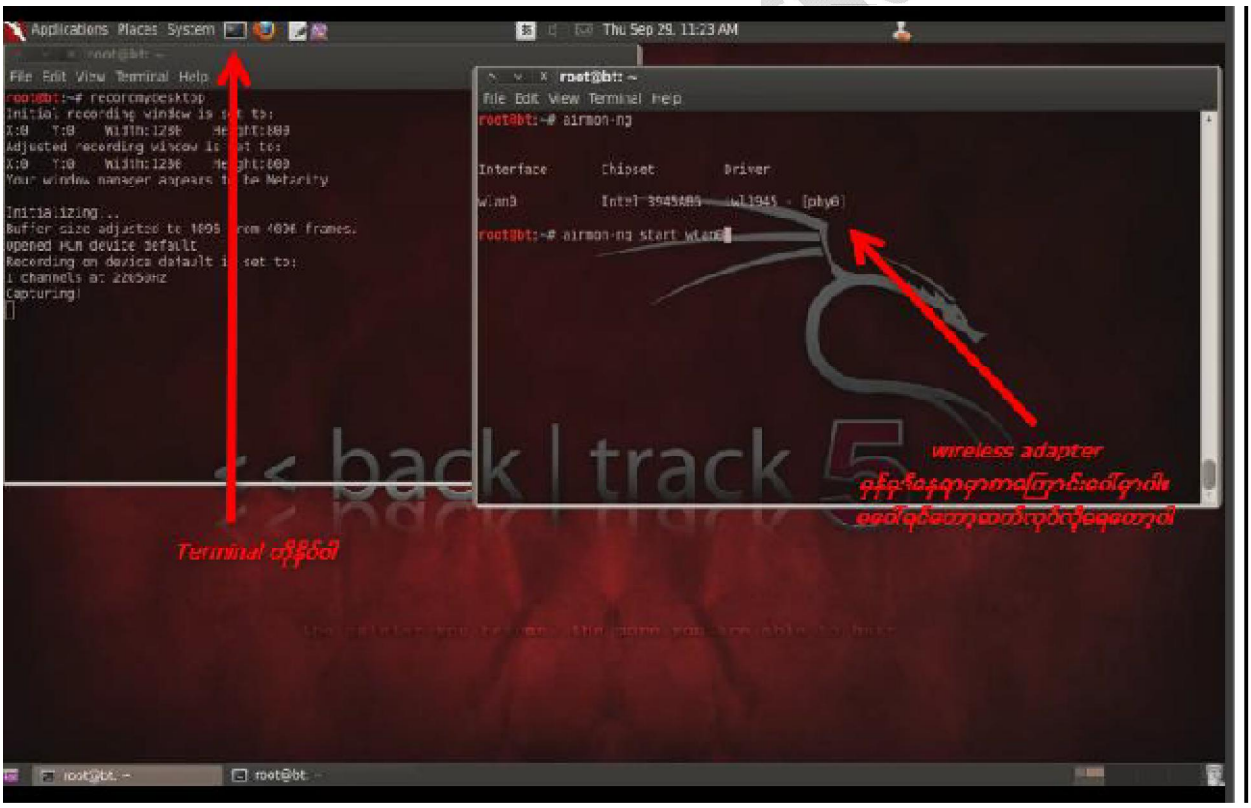
Linux လေ့လာနေသူများအတွက် Back Track ကအထောက်အကူပေးမှာပါ။

WEP အား Crack ခြင်း

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

ကဲ စတင်ရအောင်ဗျာ။

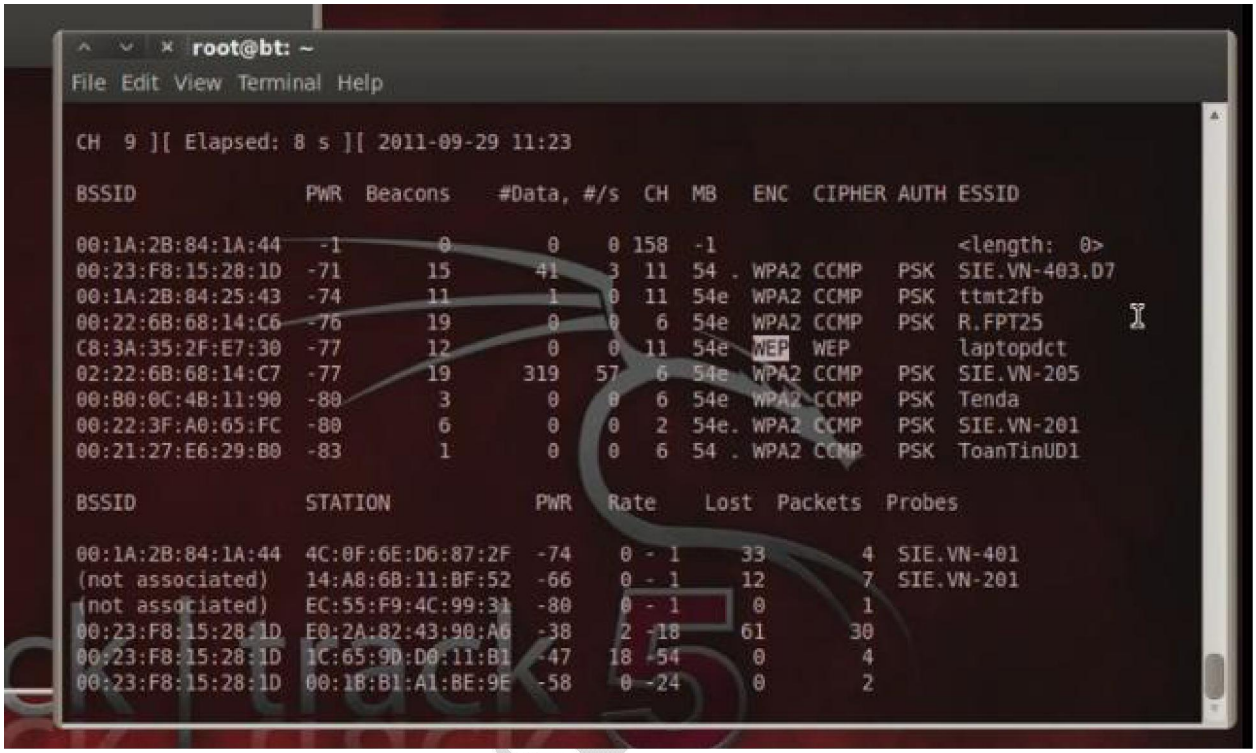
အရင်ဆုံး Back Track က Terminal ကိုဖွင့်ပါ ။ Terminal ဆိုတာ Windows က Command Line(CMD) နဲ့ သဘောတရားခြင်း တူတူပါဘဲ။ ပထမဆုံး Command ရိုက်ပါမယ်။ airmon-ng လို့ ရိုက်ပါ enter ခေါက်ပါ။ အဲ့မှာ Interface , Chipset တို့ အောက်မှာ wlan0 လို့ Adapter ရဲ့ Detail တစ်ကြောင်းကို ပြပါလိမ့်မယ်။ အဲ့ဒါဆိုရင် Adapter ကို Bt5 က သိနေပြီဖြစ်ပါတယ်။



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

တတိယ command ရိုက်ရပါအုံးမယ်။ airodump-ng mon0 ပါ။ အဲ့ဒီကွန်မန်းကိုရိုက်တာနဲ့

ကို ယ့်အနီးနားမှာရှိတဲ့ ဝိုင်ဖိုင် လိုင်းမှန်သမျှကို ပြသပေးမှာဖြစ်ပါတယ်။ အဲ့ဒီမှာ ဘယ်လိုင်းကတော့ WEP ဘယ်လိုင်းကတော့WPA2 ဆိုတာကိုပြနေမှာဖြစ်ပါတယ်။ ကဲ ဒီတော့အခု ကျွန်တော်တို့ က WEP လိုင်းတစ်ခုကိုရွေးပြီး စတင် Crack ပါတော့မယ်။



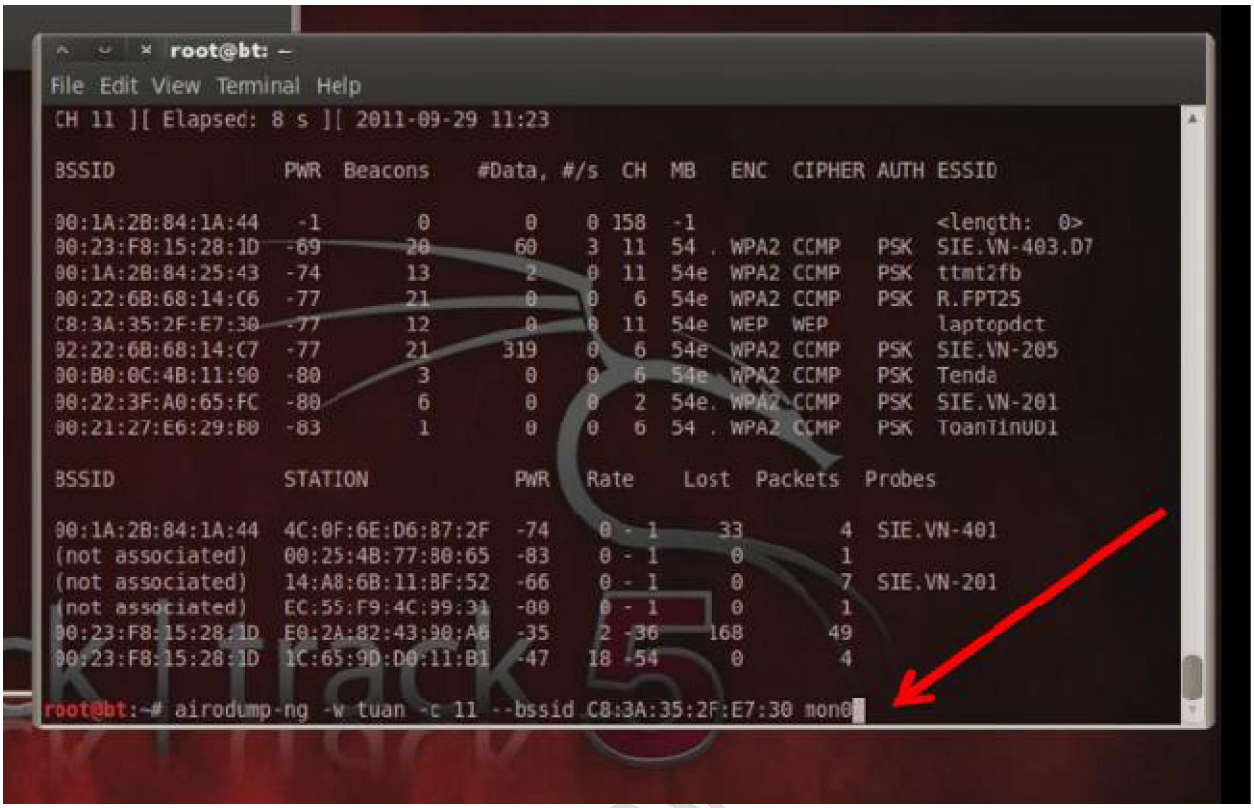
ဟောတွေ့ ပါပြီ ပုံသုံလို့ ဗျာ ။ ဒီတော့ WEP လိုင်းတစ်ခုဖြစ်တဲ့ Laptopdct ဆိုတာကိုရွေးလိုက်ပါမယ်။

သူနဲ့ ပတ်သတ်တဲ့ BSSID နံပတ်တွေကိုကူးယူရပါမယ်။ C8:3A35:2F:E7:30 ဘဲဖြစ်ပါတယ်။

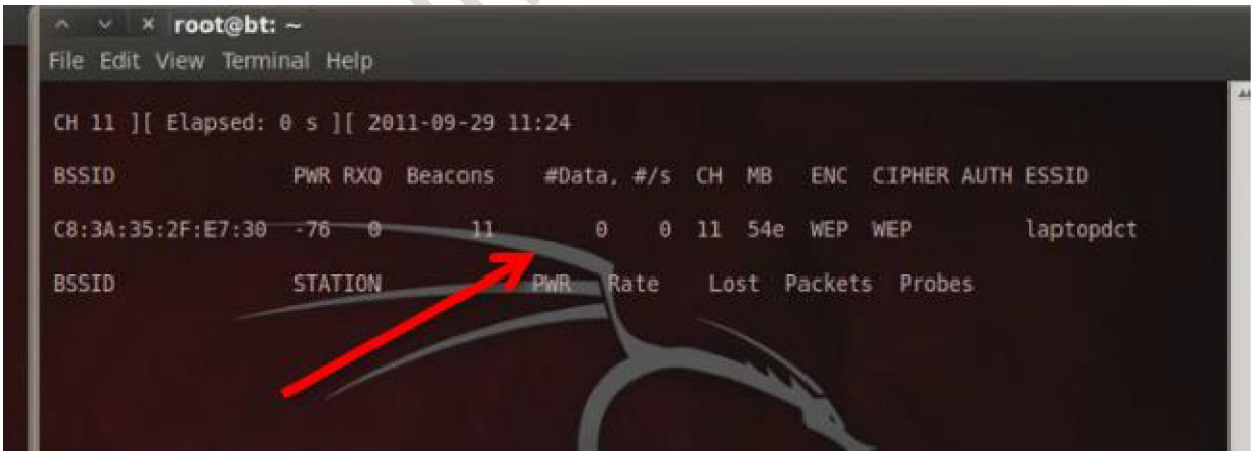
လိုင်းတစ်ခုနဲ့ တစ်ခု BSSID မတူကြပါဘူး ပြီးတော့ CH ကို မှတ် Cheannel (CH) ။ Laptopdct ရဲ့ Cheannel (CH) က 11 ဖြစ်ပါတယ်။ ပြီးတော့ ကျွန်တော်တို့ က Command နောက်တစ်ကြောင်းကို ထပ်မံအသုံးပြု ရပါတော့မယ်။

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

လို့ ရိုက်ထည့်လိုက်ပါ။



ဒီနေရာမှာ tuan ဆိုတာက 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။ အဲ့ဒီအချိန်မှာကိုက Target ထားတဲ့လိုင်းရဲ့ Data အနေအထားသီးသန့် ပေါ်လာပါမယ်။



ပြီးရင်တော့ Termainal အသစ်တစ်ခုခေါ်ပါ။ အဲ့တည်းမှာ

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

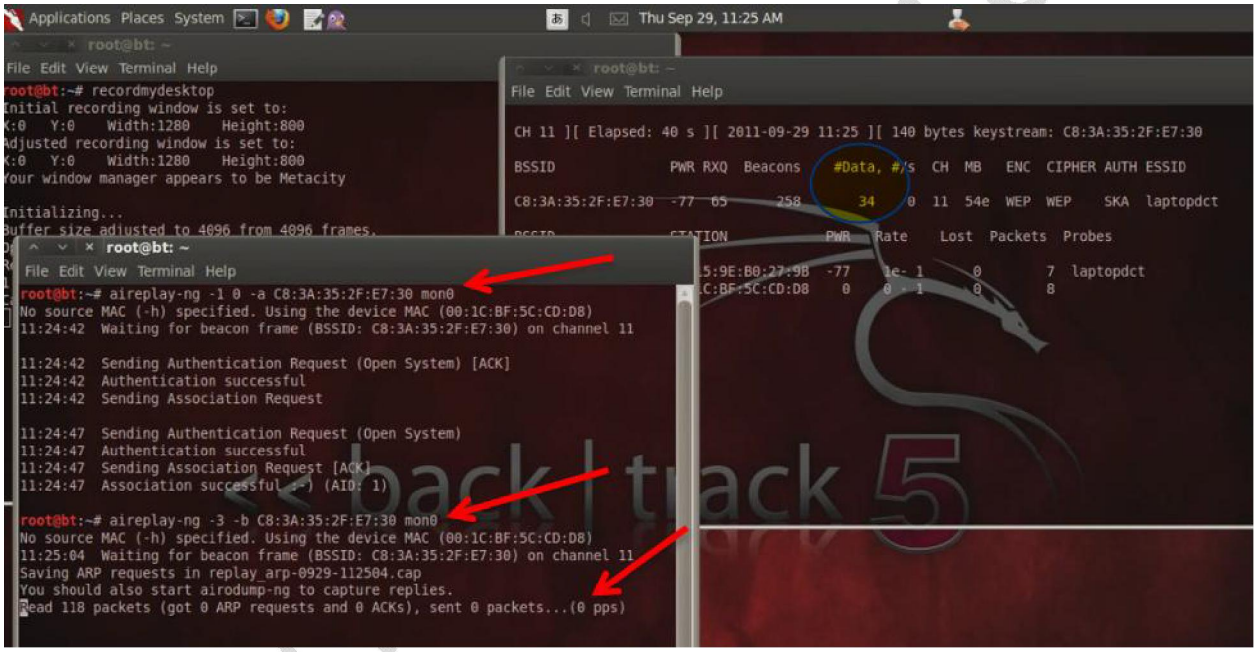
အခုဒီအခါ မိမိ request တွေကို send လုပ်တာတွေ့ ရမှာ ဖြစ်ပါတယ်။ ပြီးတဲ့အချိန်မှာတော့ command နောက်တစ်ကြောင်းကိုထပ်မံအစားသွင်းရမှာဖြစ်ပါတယ်။

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

လို့ ရိုက်ထည့်ပေးရမှာပါ။ ထိုအခါ ကို ပို့ လိုက်တဲ့ requesဒိုင်တွေ့ read လုပ်နေတာကိုတွေ့ ရပါလိမ့်မယ်။

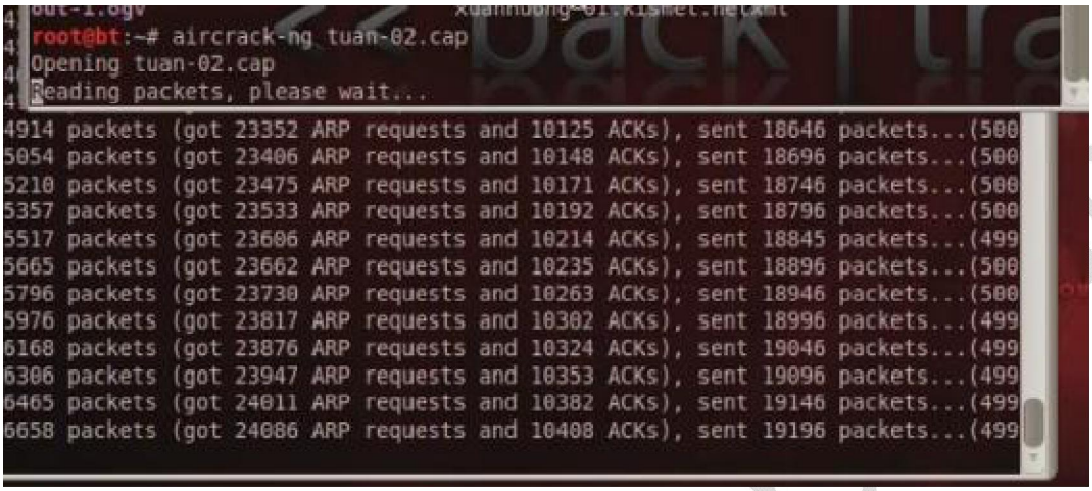
read ရတာများလေ ကို့ Target ရဲ့ Data တတ်လာလေလေ ကို့ target ရဲ့ လိုင်းထိုးကျလာလေလေ စြိုလာပါတယ်။

ပုံလေး ကိုကြည့်ကြည့်ပါအုံး။။

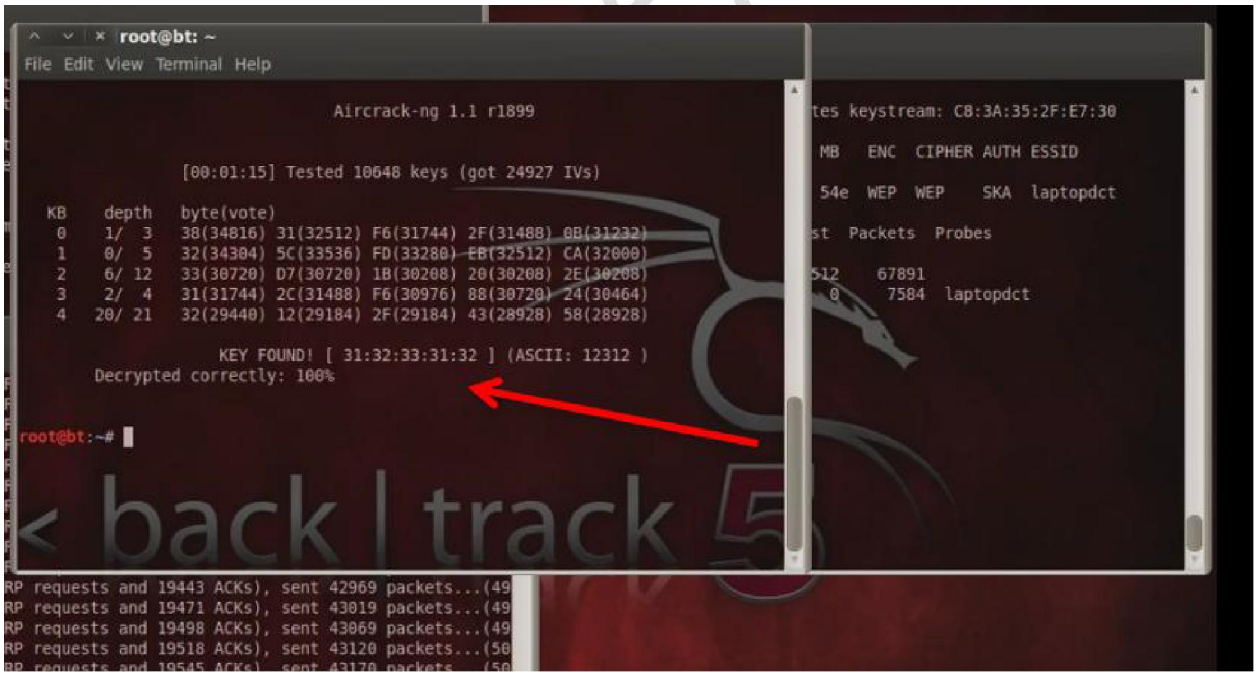


Data များများတက်လာအောင်စောင့်ပါ ။ ဖောကို့ အခွင့်အရေး ပိုကောင်းပါတယ်။ ဒီနေရာမှာ C8:3A:35:2F:E7:30ကိုအသေမှတ်မထားဘဲ လိုင်းပေါ်မူတည်ပြီး BSSID ပြောင်းပါတယ်။ ပြီးတော့ Aireplay Command တွေမှာ-1 တို့ 0 တို့ မရရင် အခြား ကိန်းဂဏန်းများထည့်စမ်းကြည့်ပါ ဥပမာ ၂ တို့ ၃ တို့ ကိုပါ။ Target ရဲ့ အခြေအနေပေါ်မူတည်ပြီးအနည်းငယ်လိုက်ပြောင်းနိုင်ပါတယ်။ သဘောတရားခြင်းကတော့ တူတူပါဘဲ။ ပုမှာ Command ၂ကြောင်းရိုက်အပြီး Data တွေ တက်လာတာကိုတွေ့ ရမှာပါ။ ကဲနောက်ဆုံးအဆင့်ကိုရောက်ပါပြီ Data တော်တော်လေးတက်လာပြီ ဆိုရင် read packet တွေလဲတော်တော်ဖတ်နေပြီဆိုရင် Crack လို့ ရလောက်ပါပြီ ဒီတော့ aircrack-ng tuan-01.cap လို့ ရိုက်ပါ။ စောစော ကကျနော်ပြောခဲ့သလိုပါပဲ။ Tuan နေရာမှာကြိုက်တဲ့နမည်ကို 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 ကိုရိုက်လိုက်ပါပြီ Opening tuan-01.cap ကို Crack လုပ်နေပါပြီ။



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



ကျွန်တော် ခုရှိခဲ့တဲ့ Key က 3132333132 ပါ။ အခဲ့ဒါမိမိ target ရဲ့ Password ပါပဲ။ တစ်ခါတစ်ရံမှာ တော့ Key က A3:B5:C11:34:U7:F8:9Q:33 အစရှိသဖြင့် ပြပါလိမ့်မယ် ဒါဆိုရင်တော့ password က A3B5C1134U7F89Q33 ဘဲဖြစ်ပါတယ်။

ကဲ အားလုံးဘဲ ပျော်ရွှင်စရာ့ Wep Cracking လေးပြီးဆုံးသွားပါပြီ။

WPA2 Cracking

WEP ရဲ့ သဘောတရားအတိုင်း ပါဘဲ ကွာခြားမှုက ဘာမှသိပ်မရှိပါဘူး။ ဒါပေမယ့် WPA က လုံခြုံရေးပိုမိုတင်းကျပ်ပါတယ်။WPA ကို Hack ဖို့ က Packet Sniffing လုပ်မလား ? Dictionary Attack နဲ့ လုပ်မလားဆိုတာပါဘဲ?စတင်လေ့လာစ ညီကိုတွေအတွက်ကတော့ Dictionary Attack က အသင့်တော်ဆုံးပါ။Packet Sniffing ကိုနောက်ပိုင်း ရေး ဖြစ်ရင်ဂေးပေးပါဒုံးမယ်။Dictionary Attack ကတော့ ရိုးရှင်းတဲ့နည်းတစ်ခုပါ ။ မိမိဖောက်မယ့်လိုင်းရဲ့ Password ကို မိမိမှာရှိတဲ့ wordlist နဲ့ တိုက်စစ်ပြီး ရယူတာပါဘဲ။WPA2 ကိုအခဲ့နည်းနဲ့ ဖောက်နိုင်ပါတယ်။ ဒါပေမယ့် Special Character တွေပါတဲ့ Strong ဖြစ်တဲ့ Password တွေကို တွေ့ ရတဲ့အခါ အချိန်ပေးရပါတယ်။ မိမိမှာ wordlist တွေများများရှိရင်တော့ Crack တဲ့အခါ အဆင်ပြေပါတယ်။ WPA 2 ကို Dictionary Attack နဲ့ တိုက်ို့ စိတ်ရှည်ရပါတယ်။ ရပ်ပစ်မယ်ဆိုတဲ့ အတွေးကိုမထားဘဲ ဆက်တိုက်ခိုက်နေရမယ်။ ကံကောင်းမှ ရတတ်သလို ခဏလေးရသွားတာမျိုးရှိပါတယ်။ မိမိ Target က Password ရိုးရှင်း လေးတွေထားရင်တော့ ကံကောင်းတာပေါ့ ခဏလေး 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။

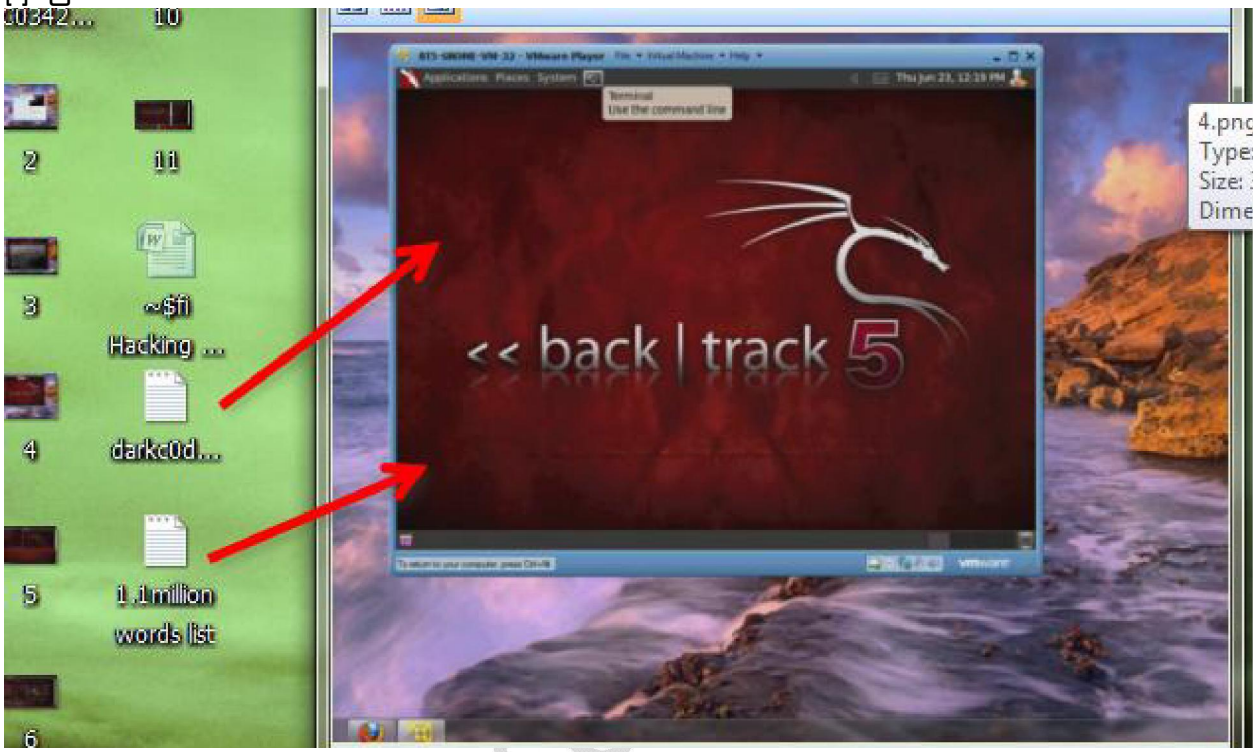
(1)1.1million wordlist.txt download

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

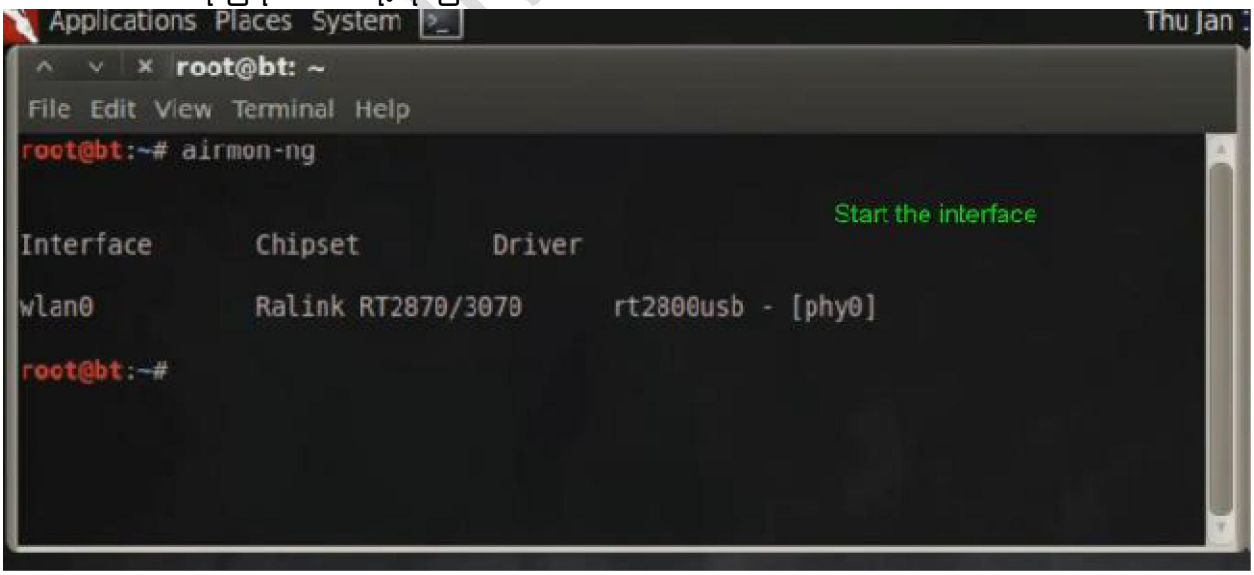
(2)darkc0de.lst download

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

ပထမဦးဆုံး back track 5 ကိုဖွင့်ပါ။ ပြီးရင်တော့ 1.1 million list and darkc0de ဖိုင် ၂ခုကို backtrack 5 ထဲသို့ mouse ဖြင့် ဆွဲယူလိုက်ပါ။
ပုံမှာပြထားပါတယ်..



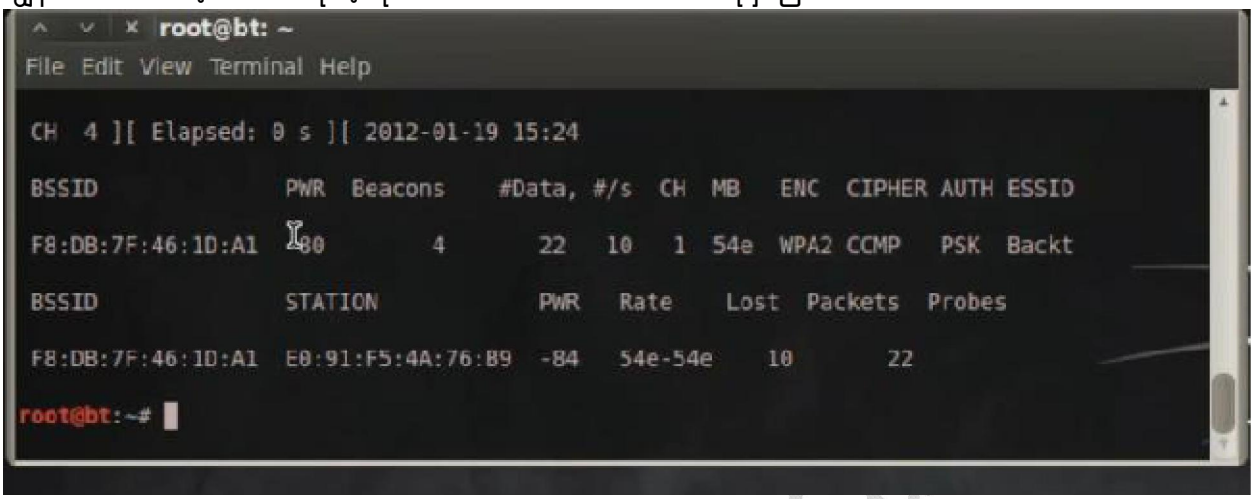
command box (terminal) ကို ဖွင့်ပါ။ airmon-ng ကိုရိုက်ပါ။ အောက်ကပုံပြထားတဲ့အတိုင်းလေး မိမိ adapter name ကို ပြရင် ဆက်လို့ ရပါပြီ...



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

နောက်ပြီးရင်မိမိ အနီးနားက wifi လိုင်းများကို ပြနေတာကိုမြင်ရပါမယ်.။မိမိ ဟက်ချင်တဲ့ လိုင်းတစ်ခု ကိုရွေးလိုက်ပါ။

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

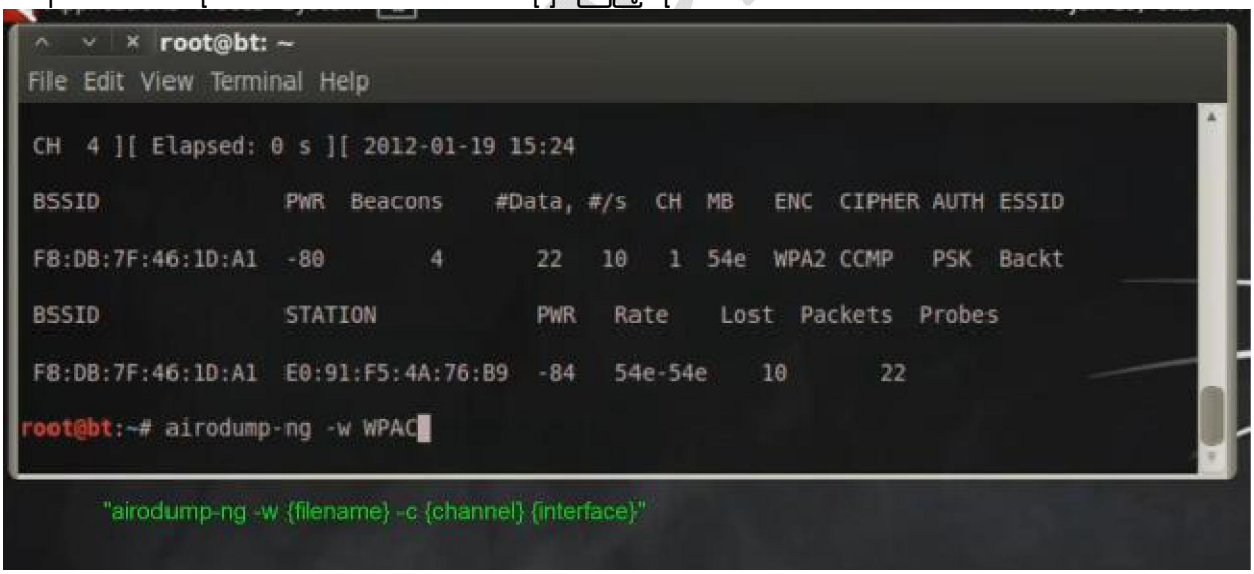


ကျွန်တော် စမ်းပြမယ့်လိုင်းကတော့ Backt လိုင်းပါ။ BSSID ကတော့ F8:DB:7F:46:1D:A1 ဖြစ်ပါတယ်။ CH (Channel) က 1 ပါ။

မိမိ target ရဲ့ Data ကိုသေချာ copy လုပ်ထားပါ။ နောက်ပြီးရင်တော့ command ရိုက်ပါမယ်.

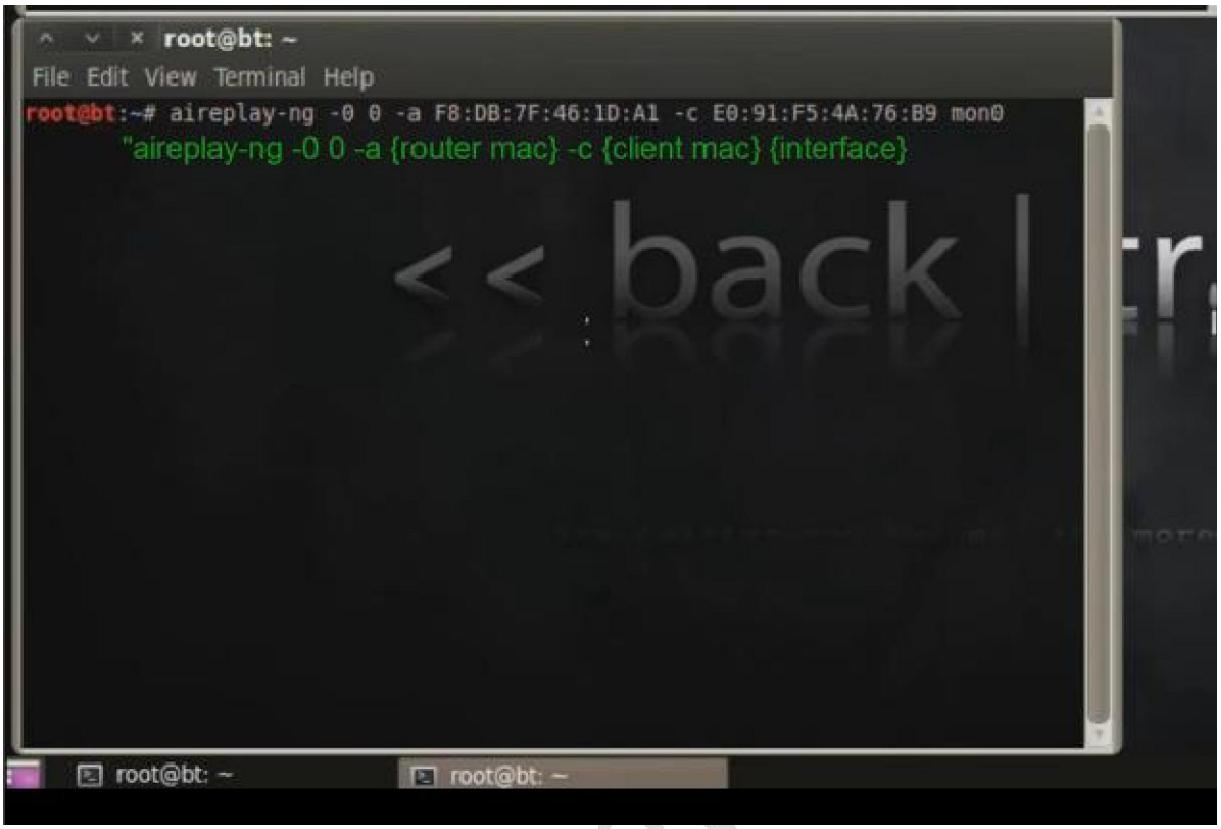
airodump-ng -w WPACap -c 1 mon0 ပါ WPACap နေရာမှာ မိမိနှစ်သက်ရာ file name ကိုထည့်ပါ...

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

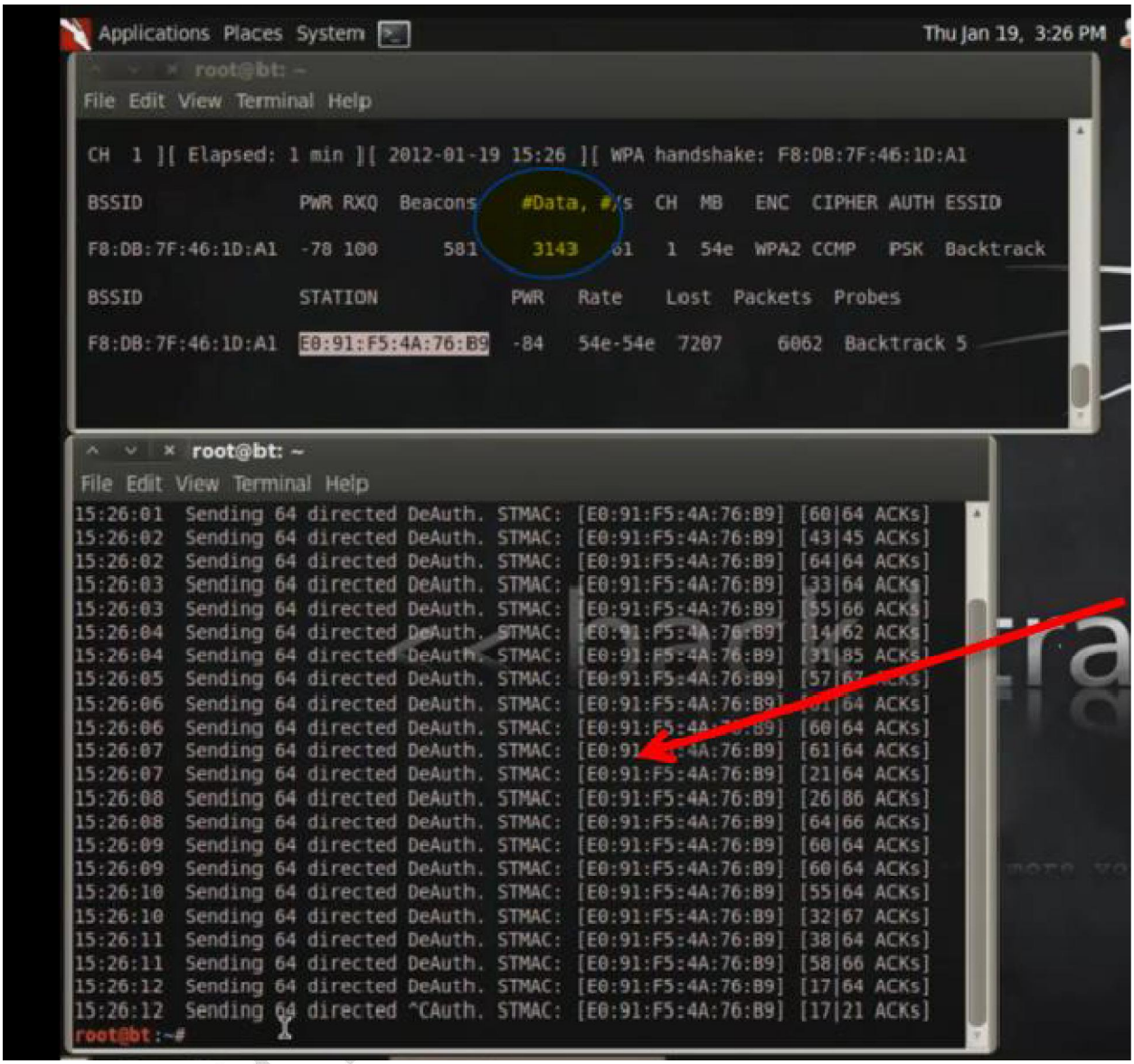


ပြီးရင်နောက် command ရိုက်ပါ။ ဒီအတွက် terminal အသစ်တစ်ခုကိုဖွင့်ပါ...

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

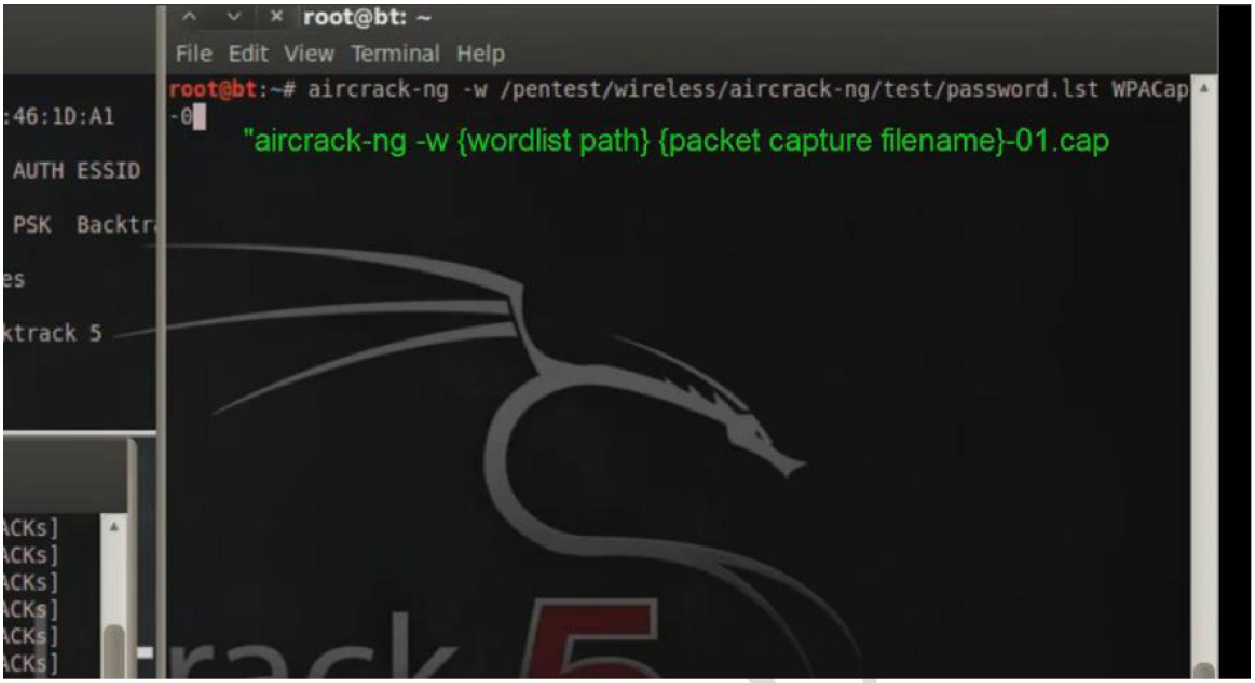


ဒီနေရာမှာ မှတ်ထားဖို့ က router mac နေရာမှာ မိမိ target ရဲ့ BSSID နံပတ်ပါဘဲ။
Client Mac ဆိုတာ မိမိ target ရဲ့ Station အောက်ကနံပတ် ဖြစ်ပါတယ်။ ဒီလောက်ဆို အဆင်ပြေမယ်ထင်ပါတယ်.မရှင်းဘူးဆိုရင်တော့ အောက်က ပုံလေးကိုကြည့်ရင် ရှင်းမယ်ထင်ပါတယ်..
Airplay command ရိုက်အပြီးမှာ Data တွေ send လုပ်နေတာကို တွေ့ ရမှာပါ။ Data ပို့ တာများလာသည်နှင့် အမျှ Target ဆီကို စုပုံရောက်ရှိသွားပြီး မိနစ်အနည်းငယ်အတွင်း မှာကို လိုင်းကျစေမှာပါ.. ပုံမှာ Data sending လုပ်နေပုံပါ...



ပြီးရင် နောက်ဆုံး Command ဖရိုက်ပါမယ်။ aircrack-ng -w /root/desktop/1.1.million wordlist.txt WPACap-01.cap ပါ။ကျွန်တော်တို့ က desktop ပေါ်မှာ 1.1.million wordlist.txt ကိုတင်ခဲ့လို့ ဖိုင်တည်နေရာ ပြောင်းသွားတာပါ။ ပုံမှာပြထားပါတယ်။ ပုံမှာကတော့ wordlist file ကို /pentest အောက်မှာထားလို့ Pentest အောက်လှမ်းခေါ်ရတဲ့သဘောပါ။ 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..



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 passwrod တွေကိုအလွယ်တကူပေးထားတတ်ကြပါတယ်။ ဒီလိုမျိုးဆိုရင်တော့ အမြန်ရမှာပါ။

လိုတာကတော့ ရဖို့ မလွယ်ကူတာကြောင့် ဖွဲ ရှိဖို့ လိုပါတယ်။ ကြိုးစားမှုအောင်မြင်မှာပါ။..

အားလုံးဘဲ ပျော်ရွှင်စွာလေ့လာနိုင်ပါစေ..

www.minsoeyarsar.com

myanmar0boy@gmail.com