WiFi Internet Connection Hacking

WEP,WPA2 Penetration Testing

5/27/2012

For Myanmar IT Begineers (Myanmar version)

3thic0kiddi3

Wifi Hacking Basic By 3thic0kiddi3

ကျနော်တို့နိုင်ငံမှာ ဝိုင်ဖိုင်လိုင်းတွေပေါလာပါပြီ၊ဒါပေမယ့်အနည်းငယ်ဈေးမြင့်နေသေးတာကြောင့် လူတိုင်းမသုံးနိုင်သေးဖူး၊လူငယ်တွေအတွက်(တကယ်လေ့လာသူ)အင်တာနက်လိုင်းဆိုတာတောင့်တမိကြမှာပဲ။ယခုစာအုပ်က ဝိုင်ဖိုင်ခိုးယူသုံးစွဲဖို့ သင်ပေးတဲ့စာအုပ်မဟုတ်ပါ။ဖေါက်လို့ရတယ်။ပြီးတော့ဘယ်လိုကာကွယ်မယ်ဆိုတာကိုရှင်းပြထားတာလေးပါ။Educational Purpose Only ဖြစ်ပါတယ်။ဒီနည်းပညာကိုတတ်သွားတိုင်း ဝိုင်ဖိုင်လိုင်းအားလုံးကိုဖေါက်နိုင်မယ်လို့တော့မဆိုလိုပါ။အနည်းငယ်နားလည်သွားပါလိမ့်မည်။ဒီစာအုပ်ကို Beginner Level နှင့်လိုက်၍ရေးသားထားပါသည်။ကိုယ်တွေ့ သင်ခန်းစာများနှင့်အွန်လိုင်းသင်ခန်းစာများစုပေါင်း၍တည်းဖြတ်ထားပါသည်။တိုတိုနှင့်လိုရင်းကိုသာဖေါ်ပြသွားပါမည်။WEP ရော WPA ပါဟက်နည်းကိုဖေါ်ပြထားပါသည်။

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)။လိုအပ်သောဆော့ဝဲ Back Track 5 , VM ware ဒါပါပဲ။

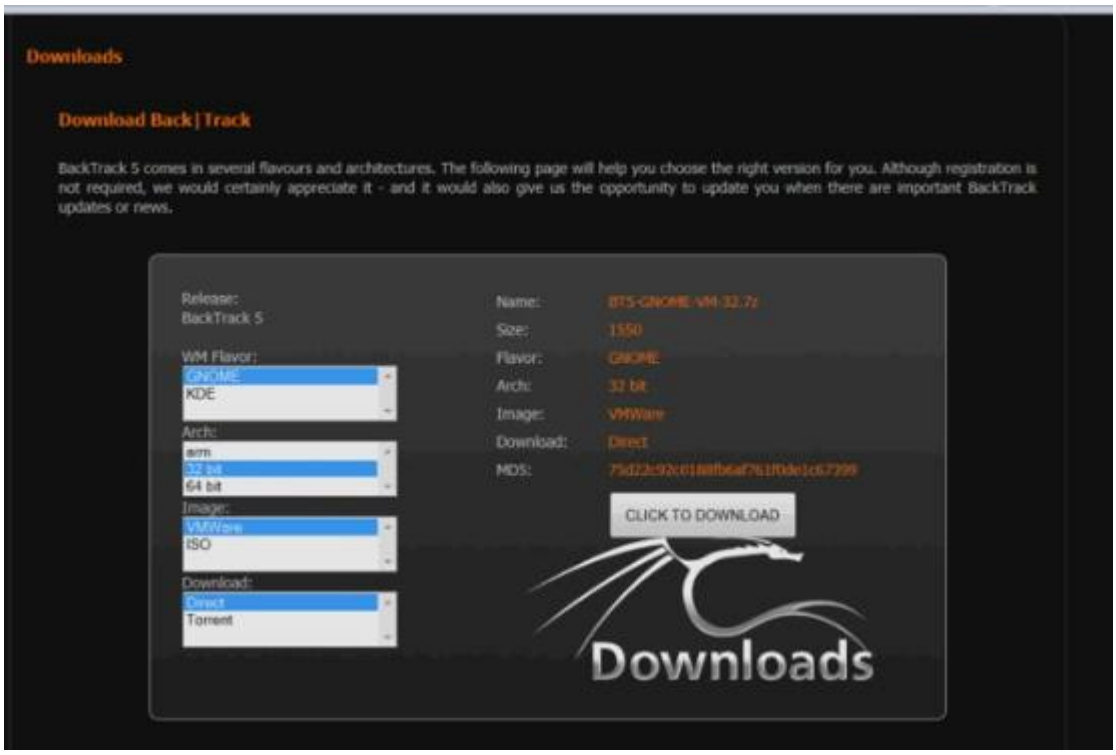
(လိုအပ်သောဆော့ဝဲဒေါင်းလုပ်ဆွဲရန် အင်တာနက်ရှိလျှင်ပိုကောင်းမည် :P)။မရှိပါကလဲအင်တာနက်ဆိုင်

တွင်အသုံးပြု၍ဒေါင်းလုပ်ဆွဲနိုင်ပါသည်။

စတင်ပြင်ဆင်ပုံ

Laptop ကိုဖွင့်ပါ။ပြီးတော့ လိုအပ်တဲ့ဆော့ဝဲတွေကိုဒေါင်းလုပ်ဆွဲဖို့ Browser တစ်ခုခုဖွင့်ပါ။

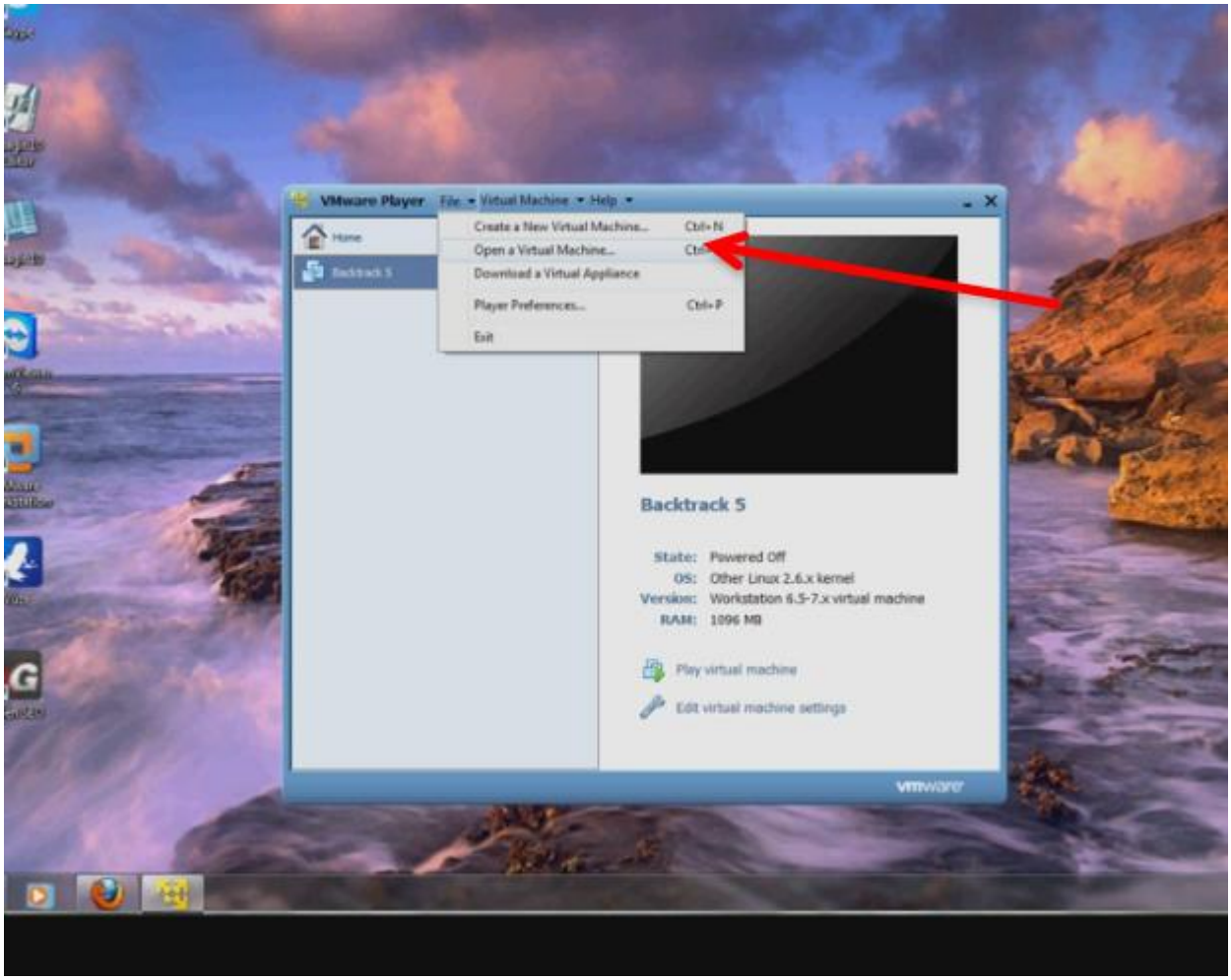
Back Track 5 ကို www.backtrack-linux.org မှာဒေါင်းလုပ်ဆွဲပါမယ်။အခုဒီစာရေးနေတဲ့အချိန်မှာ Back Track က 5R2 တောင်ထွက်နေပါပြီ။အခု Back Track 5 ဖြင့်ပြသွားပါ့မယ်။Download လုပ်ဖို့ သူတောင်းတဲ့ဒေတာတွေမထည့်လဲရပါတယ်။ပုံပါအတိုင်း GNOME ၊ 32 Bit ၊VM Ware၊ Direct ကိုရွေးပါ။



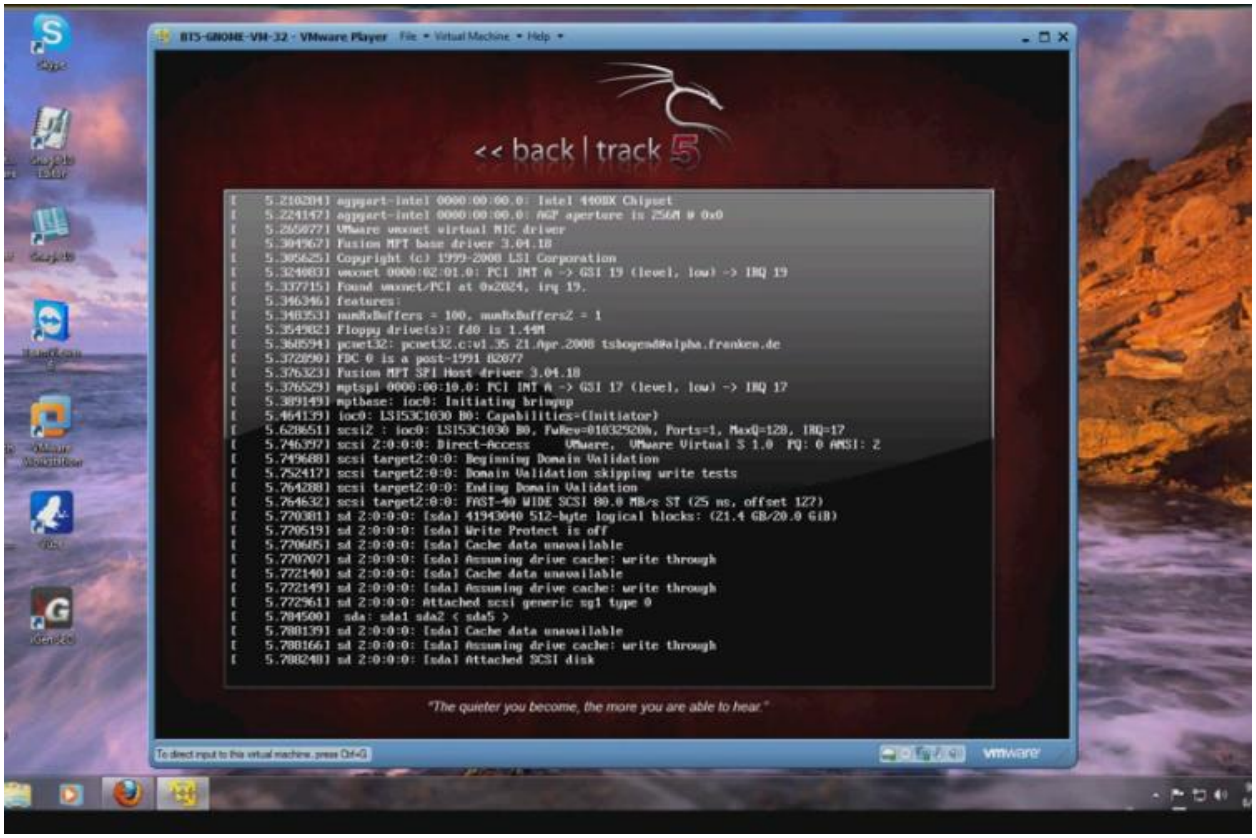
ဒေါင်းလုပ်ဆွဲပါလိမ့်မည်။ကျနော်ဒေါင်းလုပ်ဆွဲခဲ့တုန်းကအင်တာနက်ဆိုင်မှာပါ။ ဂုနာရီလောက်ကြာတယ်။

ဒေါင်းလုပ်ဆွဲဖို့ အတွက်အင်တာနက်ဆိုင်နဲ့ခင်ရင်တော့ဆွဲခိုင်းထားလို့ရတာပေါ့နော်။အဲဒီလောက်ကြာလို့ စိတ်ပျက်မသွားပါနဲ့၊ဖွဲလျော့ရင်ဘာမှလုပ်တတ်မှာမဟုတ်တော့ဖူး။Back Track 5ကိုရလာတာနဲ့ Zip ဖြည်လိုက်ပါ။ပြီးတော့ VM ware ကိုဒေါင်းလုပ်လုပ်ဖို့ www.vmware.com/products/player ကို သွားပါ။ဒေါင်းလုပ်ဆွဲပြီး VM ware ကိုစက်မှာအင်စတောလုပ်ပါ။

VM ware ကို Install လုပ်ရတာလွယ်ပါတယ်အခြားဆော့ဝဲများနည်းတူပါပဲ။အင်စတောလုပ်ပြီးပုံပါအတိုင်း File >open virtual machine ကိုရွေးပါ ။မိမိကွန်ပြူတာထဲက Back Track 5 zip ကိုဖြည်ထားတာကိုရွေးလိုက်ပါ။



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



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

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

ဒါဆို ကျနော်တို့ Windows 7 သုံးနေရင်းနဲ့ Back

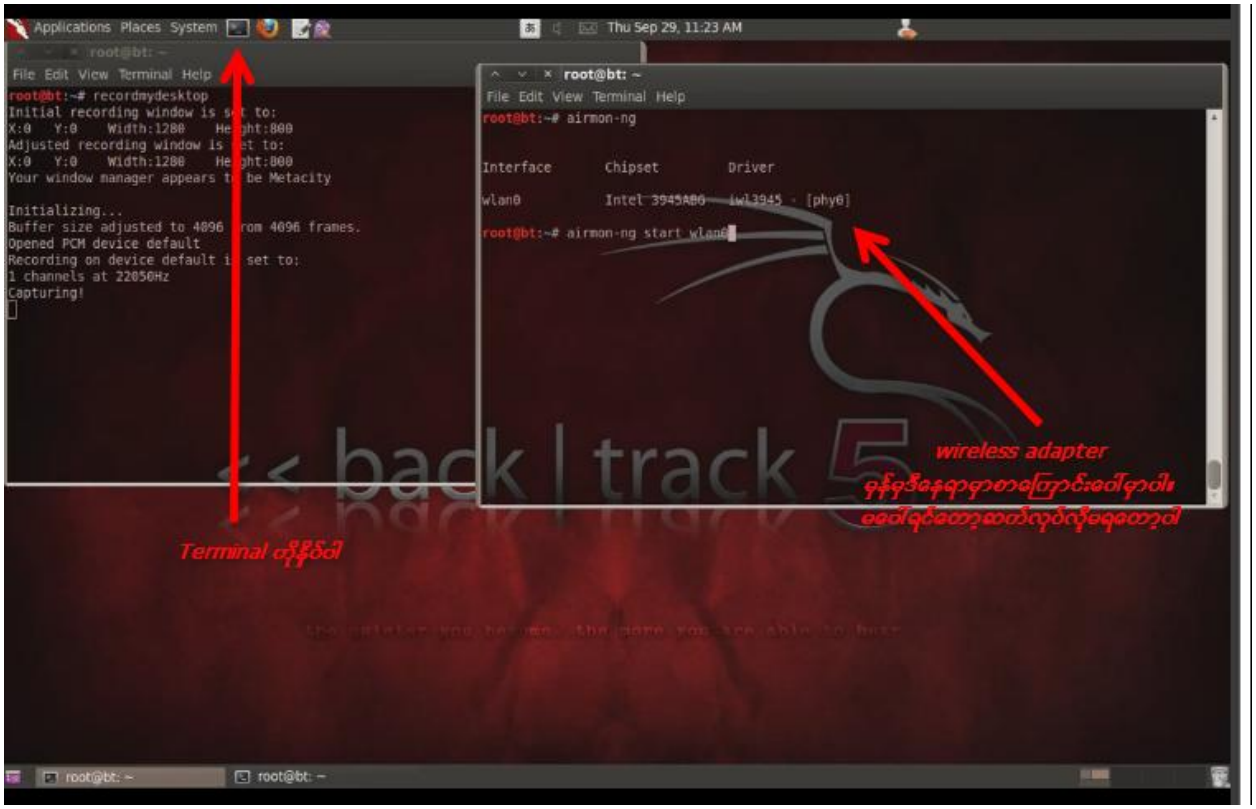
Track 5 သုံးနိုင်ပါပြီ။Back Track ဆိုတာ Linux အခြေယ်ဝင်တစ်ခုပါ Security သမားရော၊ Hacker တွေပါအသုံးပြုနေကြပါတယ်။Linux လေ့လာနေသူများအတွက် Back Track ကအထောက်အကူပေးမှာပါ။

ဝိုင်ဖိုင်လိုင်းတစ်ခုဟက်ကြည့်ခြင်း (WEP Cracking)

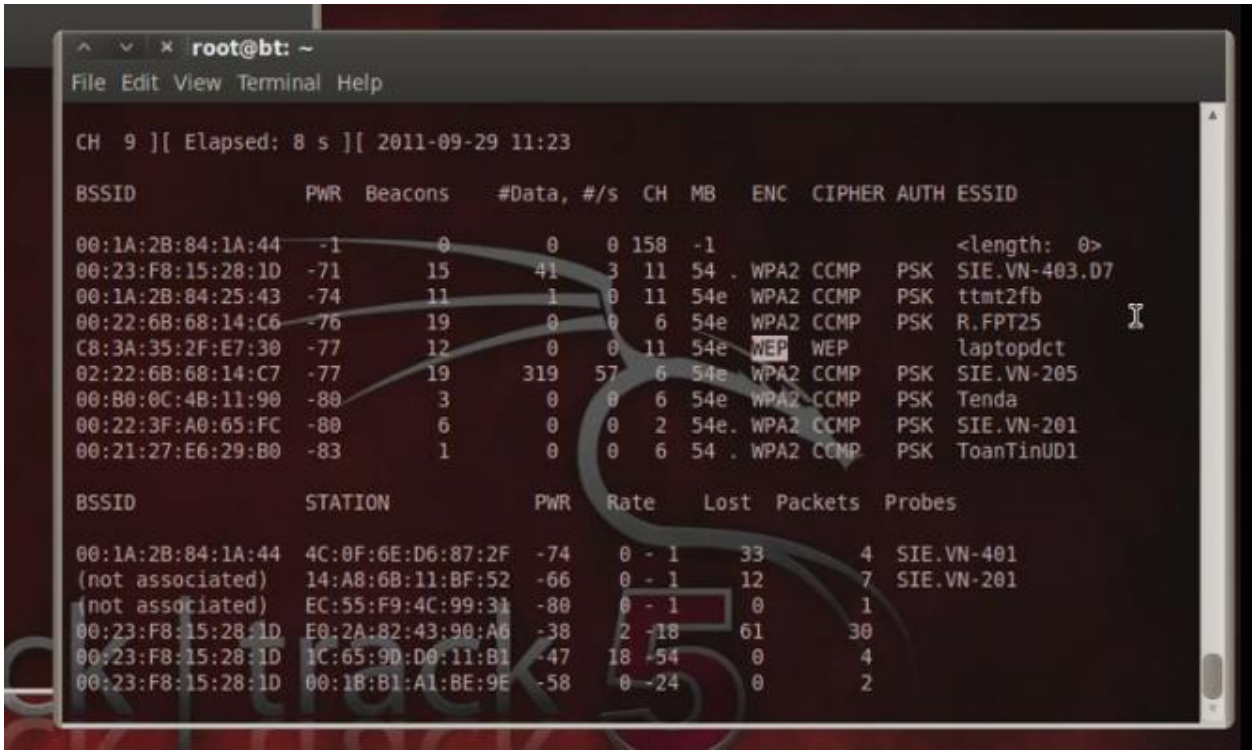
Wifi လိုင်းတွေကများသောအားဖြင့် WEP လိုင်း WPA လိုင်း WPA2 လိုင်းဆိုတာရှိကြပါတယ်။ အရှည်ကောက်တွေသိချင်ရင်တော့ Google မှာရှာဖတ်လိုက်ကြပါ။Beginner တစ်ယောက်အဖို့ ကတော့ WEP တို့ WPA တို့မသိကြပေမယ့်ပြဿနာမဟုတ်ပါ။WEP ကဖေါက်ရလွယ်ပါတယ်။ဆော့ဝဲတွေနည်းလမ်းတွေများကြီးရှိပါတယ်။မိမိဖေါက်ထွင်းမယ့်ပတ်ဝန်းကျင်မှာ WEP လိုင်းရှိလို့ကတော့ ပျော်ရမှာပါ။လက်တော့်ကဝိုင်ဖိုင် Connector လေးကိုထောက်ကြည့်တာနဲ့ အနီးနားကဝိုင်ဖိုင်လိုင်းတွေပေါ်နေတာတွေ့မှာ 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။

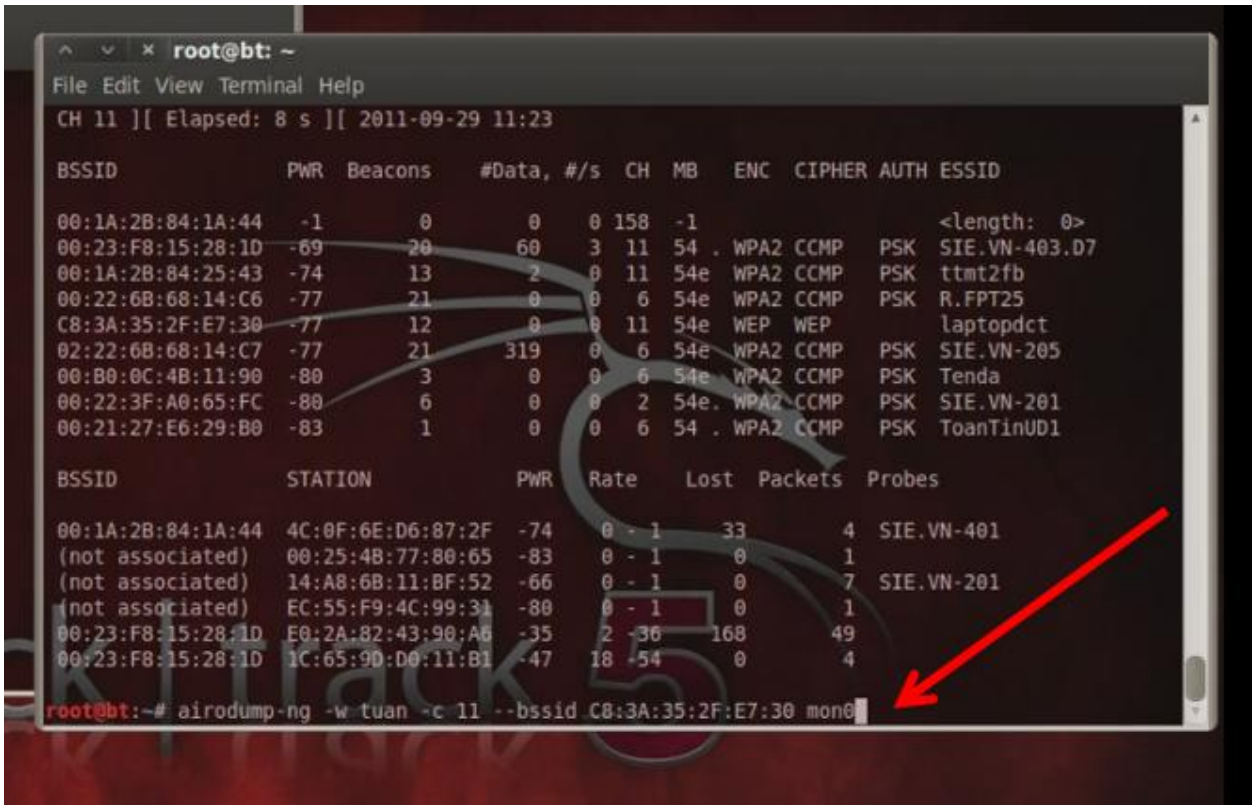
airmon-ng လို့ ရိုက်ပါ Enter ခေါက်ပါ။အဲဒီမှာ Interface ,Chipset တို့အောက်မှာ wlan0 လို့ adapter ရဲ့ detail တစ်ကြောင်းကိုပြပါလိမ့်မယ်။အဲဒါဆို Adapter ကို BT5 ကသိပါပြီ။ဆက်လုပ်လို့ ရပါပြီ။



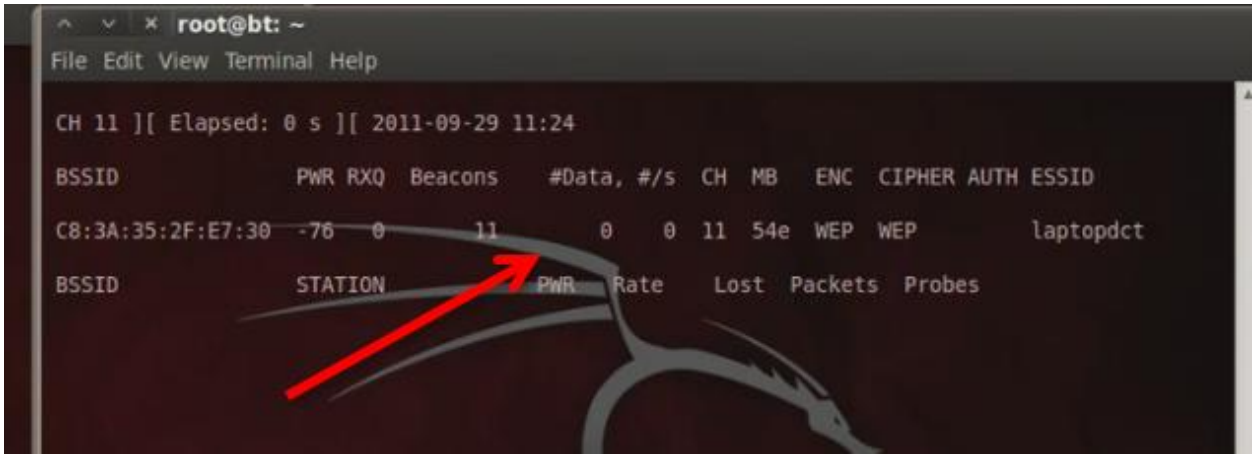
ဒုတိယ Command ရိုက်ပါမယ်။ airmon-ng start wlan0 ပါ Enter ခေါက်ပါ။ နောက်တစ်ကြောင်း တတိယ Command ရိုက်ပါမယ်။ airodump-ng mon0 ပါ Enter ခေါက်ပါ။အဲဒီ ကွန်မန်းကိုရိုက်တာနဲ့ ကိုယ့် အနီးနားက ဝိုင်ဖိုင်လိုင်းမှန်သမျှပြပါပြီ။အဲဒီမှာ ဘယ်လိုင်းကတော့ဖြင့် WEP ဘယ်လိုင်းကတော့ WPA2 ဆိုတာပြနေမှာပါ သင့်ရဲ့ Target wifi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



ကျနော်ထဲမှာတော့ laptopdct ဆိုတဲ့လိုင်းက WEP လိုင်းဗျ။ကျန်တဲ့ဝိုင်ဖိုင်လိုင်းတွေက WPA2 လိုင်းတွေချည်း ဒီတော့ ကျနော် Laptopdct ဆိုတဲ့လိုင်းကိုဖေါက်ကြည့်မယ်။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။



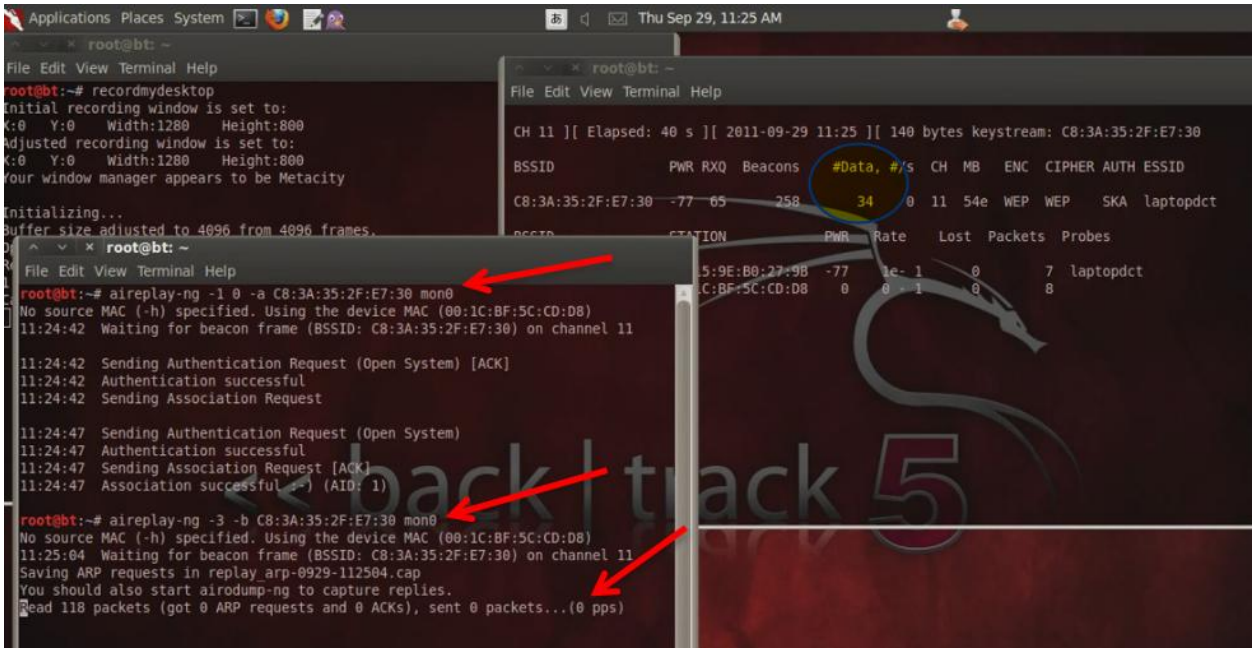
ဒီနေရာမှာ tuan ဆိုတာဖိုင်နိမ်း (File name) ပါကြိုက်တဲ့နာမည်ထည့်လို့ရပါတယ်။ -c ရဲ့နောက်မှာတော့မိမိ Terget ရဲ့ CH နံပါတ်ကိုထည့်ရပါမယ်။ C8:3A:35:2F:E7:30 ရဲ့ နေရာမှာလဲ မိမိ Terget ရဲ့ BSSID ကိုထည့်ရပါမယ်။ပြီးရင် Enter ခေါက်ပါ။အဲဒီအခါ ကိုယ့် Target ရဲ့လိုင်း Data အနေအထားသီးသန့်ပေါ်လာပါမယ်။ ပုံမှာကြည့်ပါ။



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

Enter ခေါက်။အဲဒီအခါမိမိ Request တွေကို Send လုပ်တာတွေ့ ရမယ် (sending auth)။ပြီးရင်နောက် Command တစ်ကြောင်းထပ်ရိုက်မယ်

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

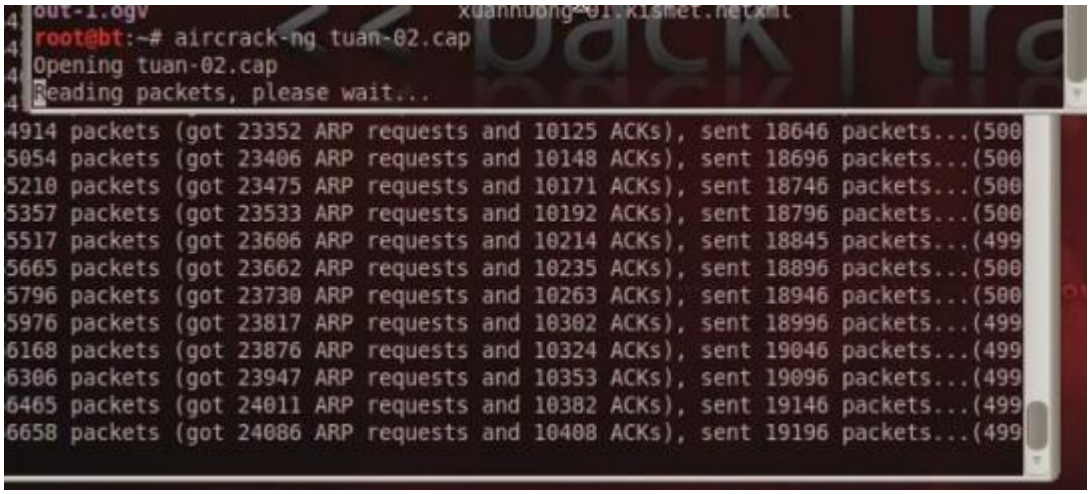


Data များများတက်လာအောင်စောင့်ပါ။ဖေါက်ဖို့အခွင့်ရေးပိုကောင်းပါတယ်။ဒီနေရာမှာ C8:3A:35:2F:E7:30 ကိုအသေမှတ်မထားနဲ့လိုင်းပေါ်မူတည်ပြီး BSSID ပြောင်းပါတယ်။ပြီးတော့ Aireplay command တွေမှာ -1 တို့ 0 တို့မရရင် အခြားကိန်းဂဏန်းများထည့်စမ်းကြည့်ပါ ဥပမာ 2တို့ 3 တို့ ပေါ့။တားဂတ်ရဲ့ အခြေနေပေါ်မူတည်ပြီးအနည်းငယ်လိုက်ပြောင်းနိုင်ပါတယ်။သဘောတရားခြင်းကတော့တူတူပါပဲ။ပုံမှာ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

မည်ပြန်ထည့်ရပါမယ်။ဥပမာ ethickiddie ဆိုရင် Command က aircrack-ng ethickiddie-01.cap ပါ။

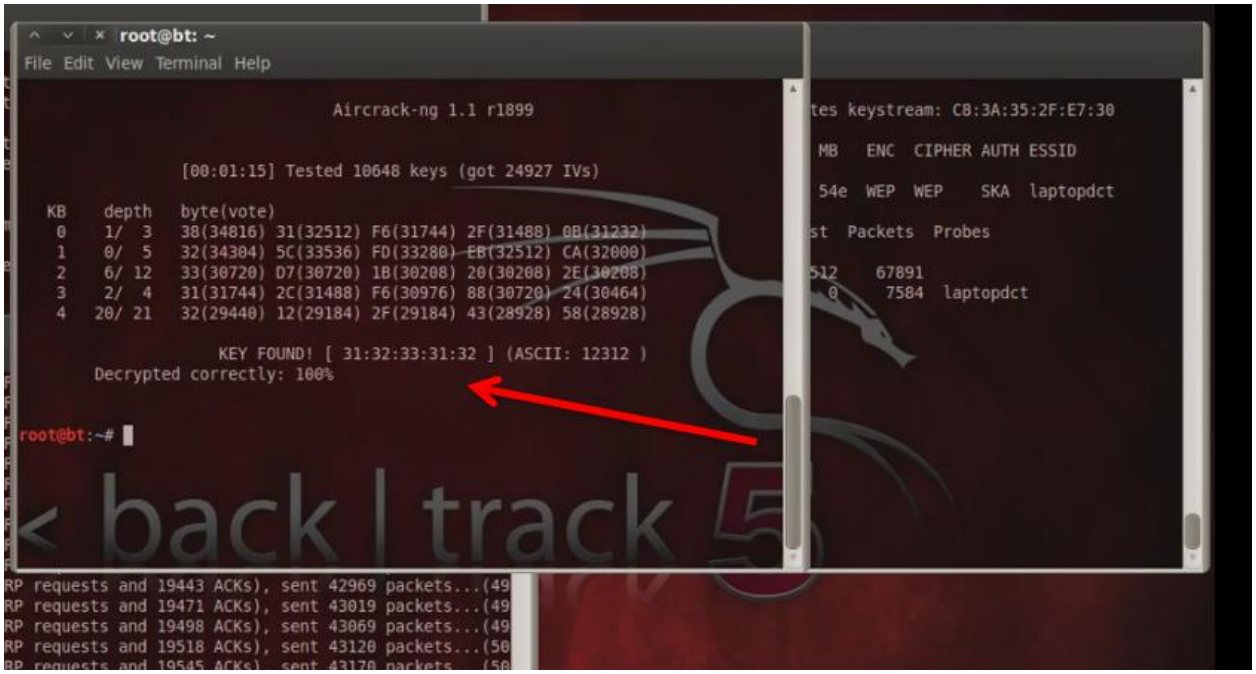
မိမိဘာနာမည်ပေးခဲ့လည်းမသိရင် Terminal မှာ ls လို့ ရိုက်ပြီးကြည့်လို့ရပါတယ်။ပုံမှာ aircrack ကွန်မန်း

ကိုရိုက်လိုက်ပါပြီ Opening tuan-01.cap ကို Crack လုပ်နေပါပြီ။



နောက်ဆုံးမှာတော့ Aircrack ကပက်ဆဝက်တွေကိုအလိုလိုရှာပေးနေပါလိမ့်မယ်။Key Found

ဆိုရင်တော့အတော်ပျော်ရမှာပါ။ပုံမှာ Key ကိုCrack လုပ်ပြီးအောင်မြင်တဲ့ပုံပါ။



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

A3:B5:C11:34:U7:F8:9Q:33 အစရှိသဖြင့်ပြပါလိမ့်မယ်ဒါဆို ပက်ဆ်ဝက်က A3B5C1134U7F89Q33 ပါ WEP Cracking ပြီးပါပြီ။

WEP ပိုင်ရှင်များလုံခြုံစေရန်

Wifi လိုင်းပိုင်ရှင်များအနေဖြင့် မိမိလိုင်းက WEP ဖြစ်နေရင် WPA2 သို့ပြောင်းလဲသုံးသင့်ပါတယ်။ WEP ဟာဖေါက်ဖို့ ရာလွယ်ကူနေပါပြီ။ပြီးတော့ မိမိလိုင်းကို BSSID ဖျောက်ထားခြင်းဖြင့်လဲကာကွယ်နိုင်ပါလိမ့်မယ်။မိမိအင်တာနက်လိုင်းလေးလွန်းလာပြီဆို Restart ချပါ။မိမိ Network အတွင်းမှာ ချိတ်ဆက်နေတဲ့ကွန်ပြူတာများပုံမှန်ဟုတ်မဟုတ်လေ့လာပါ။နက်ဝက်မှာလာရောက် Crack လုပ်တဲ့ Computer များရဲ့ Mac address ကို Filter လုပ်ပစ်ပါ။ဒါမှမရရင် ပေးသုံးလိုက်ပါ။သနားပါတယ်ဗျာ။

.....

WPA2 Cracking (အနည်းငယ်ခက်သောလိုင်းအားခရက်လုပ်ခြင်း)

နည်းလမ်း(၁)

WEP ရဲ့သဘောတရားအတိုင်းဆင်တူပါတယ်။ဒါပေမယ့် WPA ကလုံခြုံရေးတင်းကျပ်တယ်။ဆရာ့ဆရာဟက်ကာကြီးတွေတောင်မှချွေးပြန်လောက်တ.ယ်။WPA2 ကို ဟက်ဖို့ က Packet Sniffing လုပ်မလား?Dictionary attack နဲ့လုပ်မလားဆိုတာပါပဲ Beginner တွေအတွက်ကတော့ Dictionary attack ကအသင့်တော်ဆုံးပါ။ Packet Sniffing ကိုကျနော်နောက်တော့ရေးပါ့မယ်။Dictionary attack ကတော့ရိုးရှင်းတဲ့နည်းတစ်ခုပါ မိမိဖေါက်မယ့်လိုင်းရဲ့ password ကို မိမိမှာရှိတဲ့ Wordlist နဲ့တိုက်ဆိုင်ယူပြီး Crack ယူတာပါ။ WPA2 ကိုအဲဒီနည်းနဲ့ဖေါက်နိုင်ပါတယ်။ဒါပေမယ့် special character တွေပါတဲ့ Strong ဖြစ်တဲ့ Password တွေကိုတွေ့ ရတဲ့အခါအချိန်ပေးရပါတယ်။မိမိမှာ wordlist တွေများများရှိရင်တော့ ခရက်တဲ့အခါအဆင်ပြေပါတယ်။WPA2 ကို Dictionary att နဲ့တိုက်ဖို့စိတ်ရှည်ရပါမယ်။ရပ်ပစ်လို့မရဖူးဆက်တိုက်တိုက်ခိုက်နေရမယ်။ ကံကောင်းမှရတတ်သလို ခဏလေးရသွားတာမျိုးရှိပါတယ်။မိမိ Target ကပက်ဆဝက်ရိုးရှင်းလေးတွေထားရင်တော့ ကံကောင်းတာပေါ့ ခဏလေးနဲ့ ဖေါက်နိုင်ပါမယ်။wordlist တွေကိုအင်တာနက်ပေါ်မှာဒေါင်းလုပ်

ဆွဲယူနိုင်ပါတယ် နာမည်ကြီး wordlist တွေကတော့ 1.1million wordlist.txt နဲ့ darkc0de.lst တို့ပါ။

Googleမှာလဲ WPA2 Crack wordlists လို့ရှာပြီးဒေါင်းလုပ်ဆွဲနိုင်ပါသေးတယ်။

4sharedမှာလဲရှာဆွဲနိုင်ပါတ.ယ်။အခုတော့ 1.1 million wordlist နဲ့ darkc0de.lst ကိုအသုံးပြုပြပါမယ်။

(1)1.1million wordlist.txt download

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

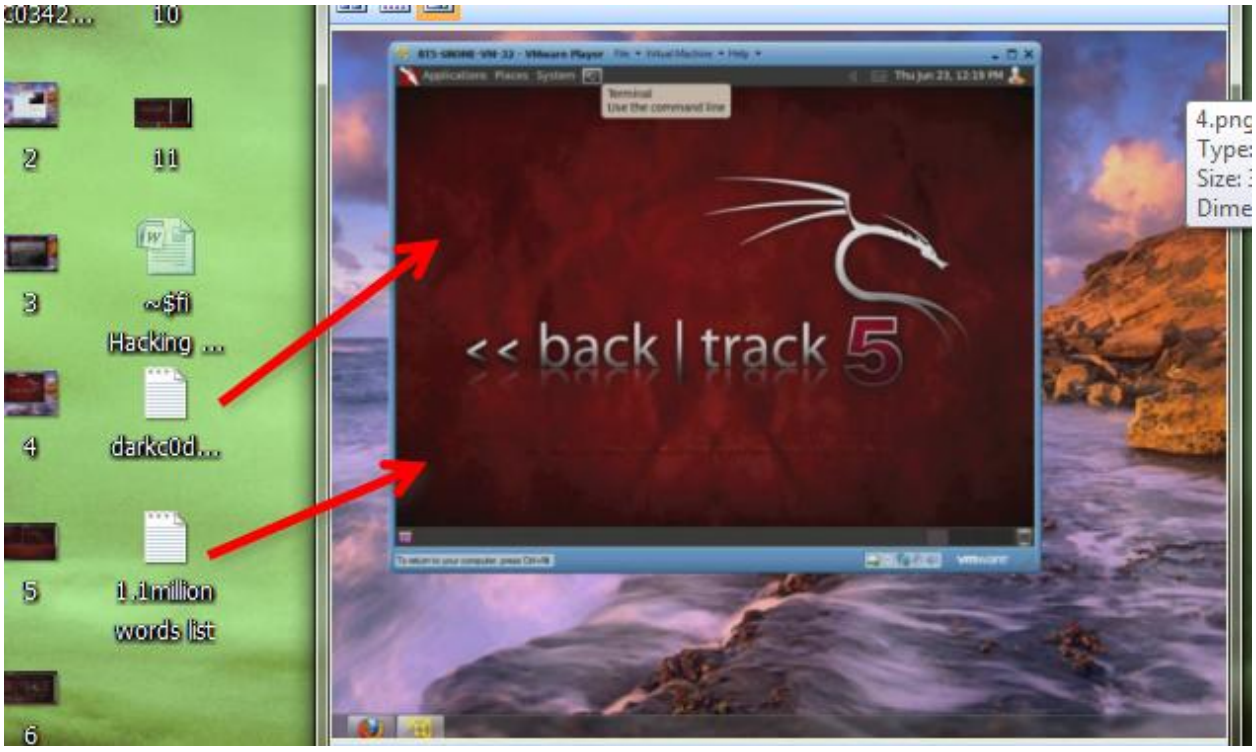
(2)darkc0de.lst download

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

ပထမဦးဆုံး Back Track 5 ကိုပြန်ဖွင့်ပါ။ဒေါင်းလုပ်ဆွဲလို့ရရှိလာတဲ့ 1.1 million list နဲ့ darkc0de ဖိုင်၂ဖိုင်

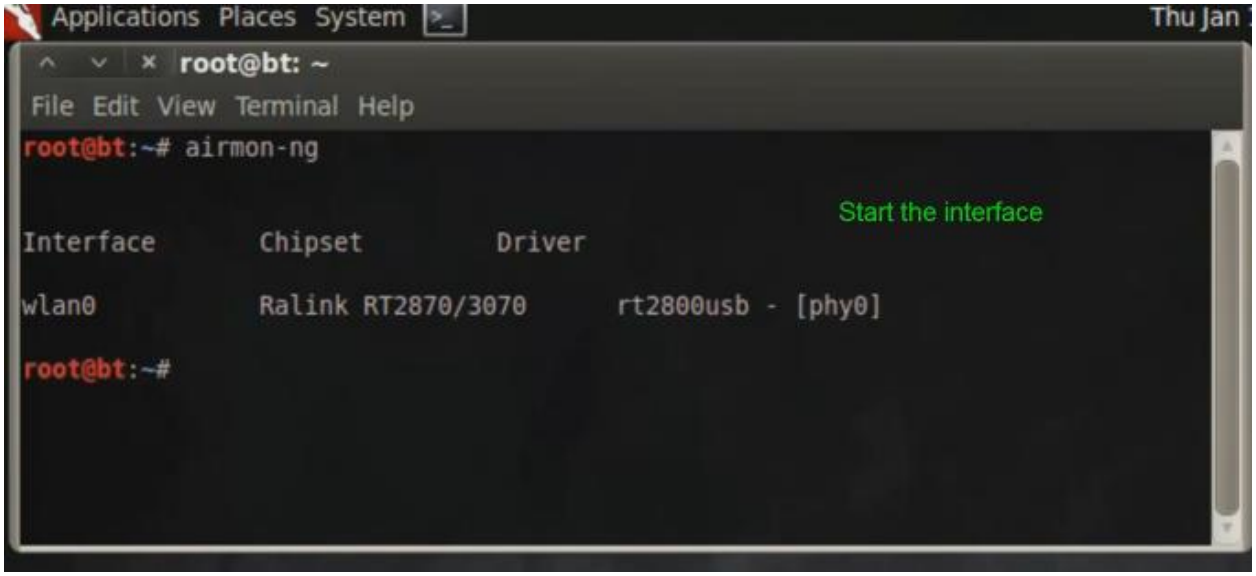
ကို Backtrack 5ထဲသို့ မောက်စ်ဖြင့်ဆွဲယူလိုက်ပါ(move)လုပ်လိုက်တာဖြစ်ပါတယ်။ပုံမှာပြထားပါတယ်။

Windows desktop ကနေဆွဲယူလိုက်တာပါ။



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

Adapter Name ကိုပြရင်ဆက်သွားလို့ရပါပြီ။



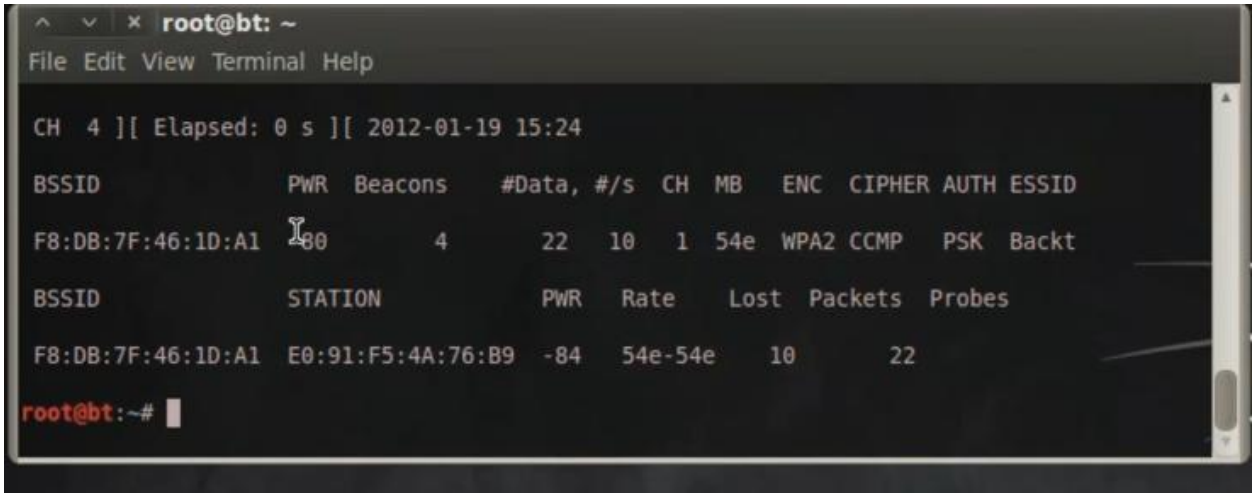
နောက် Command က airmon-ng start wlan0 ပါ Enter ခေါက်ပါ။

နောက်Command က airodump-ng mon0 ပါ Enter ခေါက်လိုက်ရင် မိမိအနီးကဝိုင်ဖိုင်လိုင်းများကို

ဖော်ပြနေပါမည်။မိမိဟက်ချင်တဲ့လိုင်းတစ်ခု (WPA2-PSK) လိုင်းတစ်ခုခုကိုရွေးချယ်လိုက်ပါ။

ကျနော်ထဲမှာတော့တလိုင်းပဲရှိတယ် Backt ဆိုတဲ့လိုင်းပါ။ WPA2-CCMP-PSk ပါ။

ပုံမှာပြထားပါတယ်။

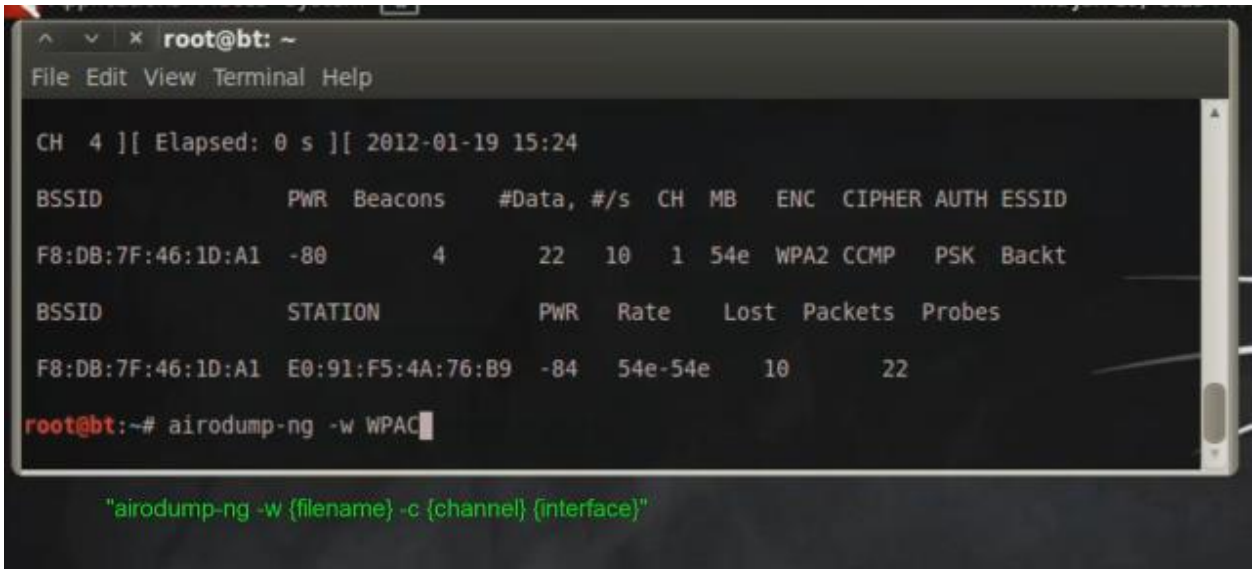


ကျနော်ဖေါက်မယ့် Backt လိုင်းရဲ့ BSSID က F8:DB:7F:46:1D:A1 ဖြစ်ပါတယ်။ Channel (CH)က 1 ပါ။

မိမိ Target ရဲ့Data ကိုသေချာကော်ပီလုပ်ထားပါ။ပြီးရင်နောက် Command ရိုက်ပါပြီ။

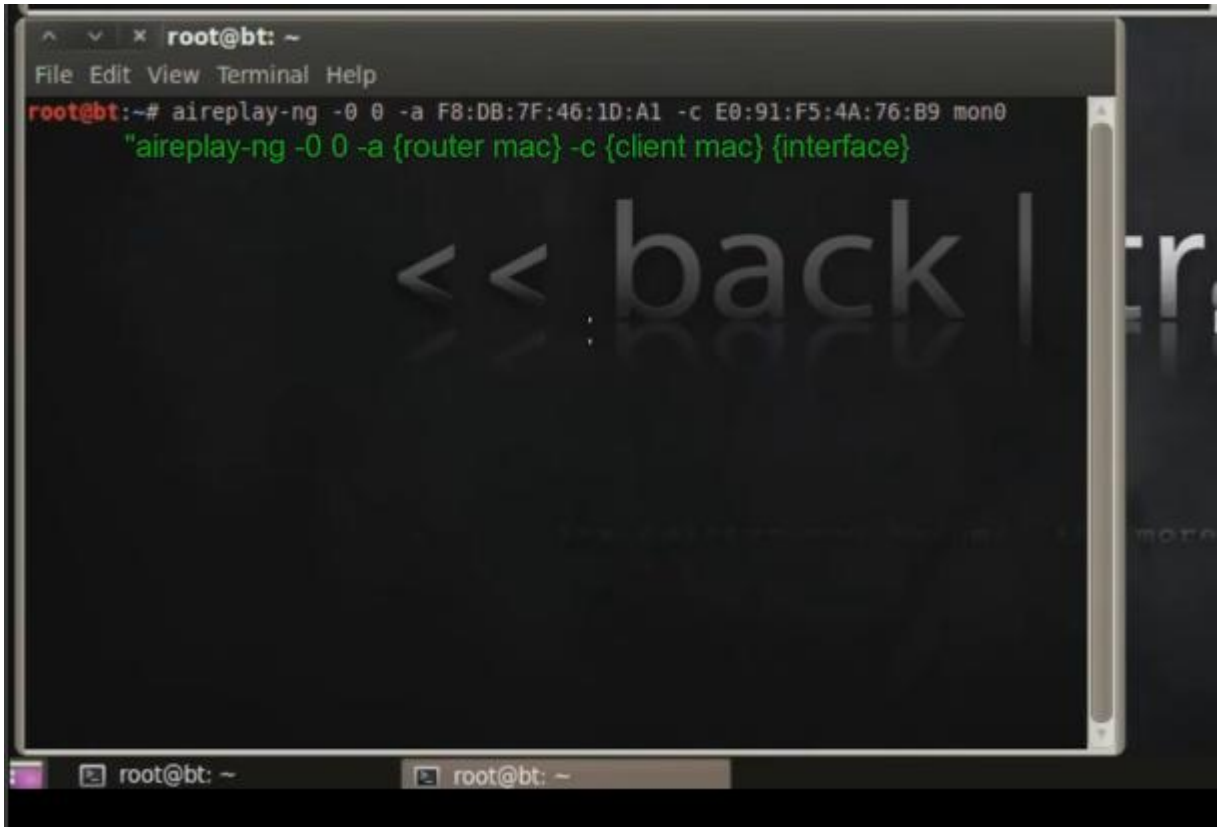
airodump-ng -w WPACap -c 1 mon0 ပါ WPACap နေရာမှာ မိမိနှစ်သက်ရာဖိုင်နိမ်းကိုထည့်ပါ။

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

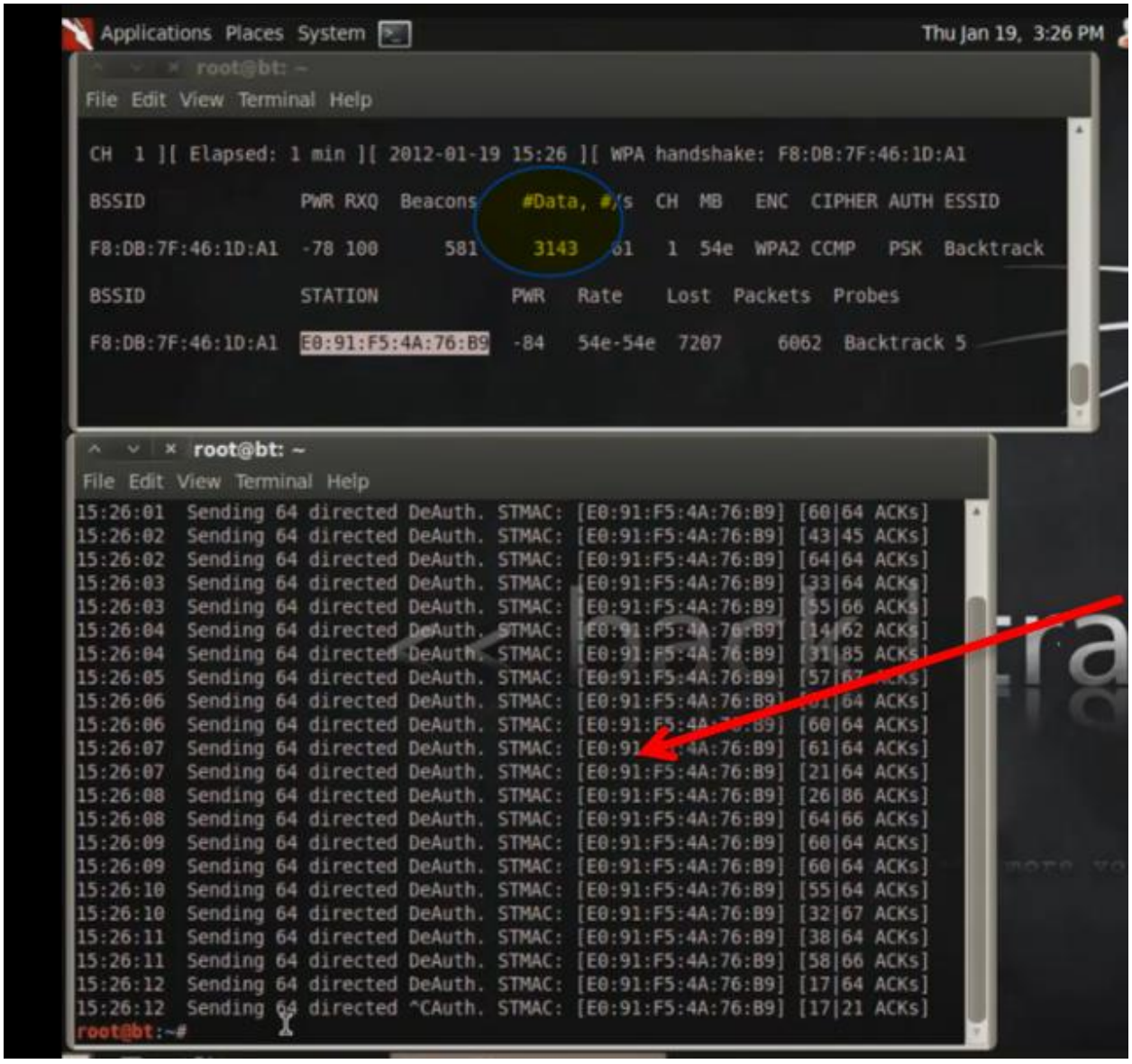


ပြီးရင်နောက် Command ရိုက်ပါမယ်။Terminal အသစ်တစ်ခုဖွင့်ပါ။

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

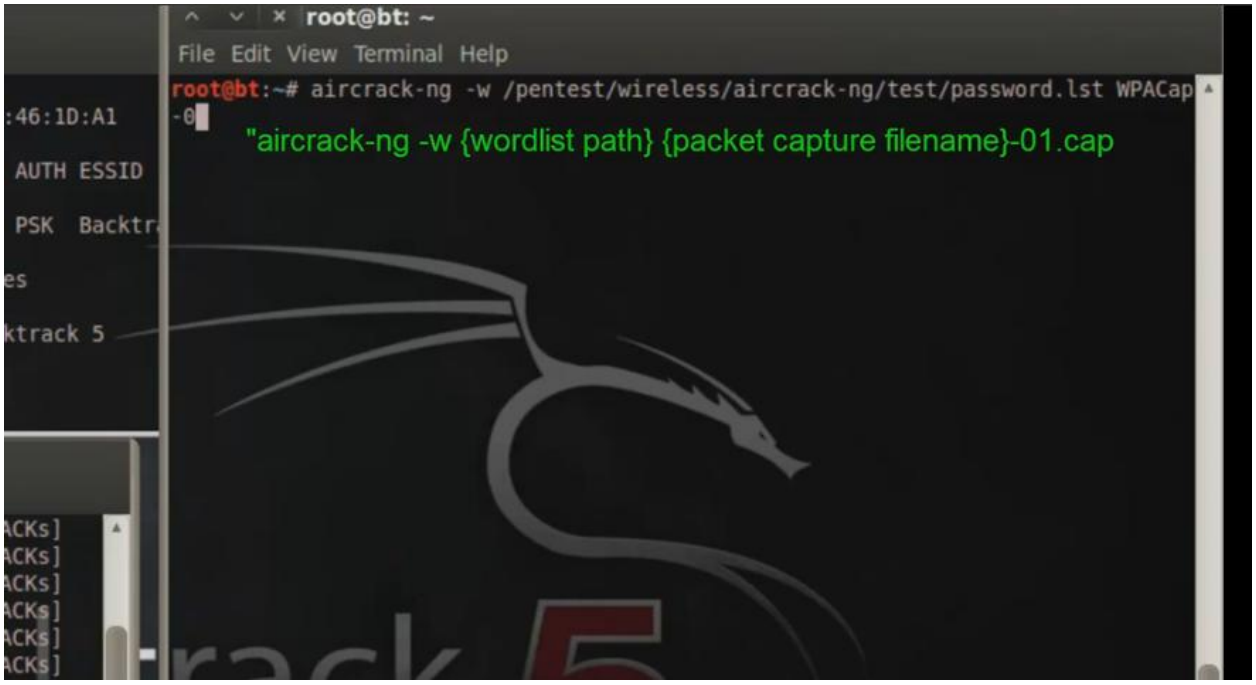


ဒီနေရာမှာမှတ်ထားဖို့က {router mac}နေရာမှာ မိမိ Target ရဲ့ BSSID နံပါတ်ပါ။{Client Mac}ဆိုတာက မိမိ Target ရဲ့ STATION အောက်က နံပါတ်ဖြစ်ပါတယ်။ဒီလောက်ဆိုရှင်းပြီထင်ပါတယ်။မရှင်းသေးရင် ပုံတွေကိုကြည့်ပြီးမိမိ Target ရဲ့ Data တွေနဲ့အစားထိုးသွားပါ။သိပ်မခက်ပါဖူးခင်ဗျာ။ဒီ Aireplay Command ရိုက်အပြီးမှာ Data တွေ Send လုပ်နေတာကိုတွေ့ရမှာပါ။ဒေတာပို့တာများလာတာနဲ့အမျှ 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 ပေါ်မှာ1.1 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 လို့ရိုက်ပြီးကြည့်နိုင်ပါတယ်။ဥပမာ မိမိမှတ်ခဲ့တဲ့ဖိုင်နိမ်းက 3thic0kiddi3 ဆိုပါစို့ 3thic0kiddi3-01.cap လို့ပြန်လည်ခေါ်ယူရမှာဖြစ်ပါတယ်။



ဒီ Aircrack ရိုက်အပြီးမှာ မိမိ Wordlist နဲ့တိုက်ဆိုင်စစ်ဆေးပြီးဖြစ်နိုင်ခြေ Password တွေနဲ့ မိမိ Target ကိုဖေါက်နေမှာဖြစ်ပါတယ်။Wordlist ကုန်သွားတယ်ပက်ဆက်မရသေးဖူးဆိုရင် darkc0de.lst နဲ့ထပ်ရှာပါ။ဒါမှမရသေးရင်အခြား Wordlist တွေနဲ့ဆက်ရှာပါ။ဖွဲ့ရှိဖို့ တော့လိုပါမည်။ ဝိုင်ဖိုင်ပိုင်ရှင်တော်တော်များများကမိမိတို့ကိုယ်တိုင်မမှတ်မိမှာစိုးလို့ ပက်ဆက်တွေကိုလွယ်လွယ်ပေးထားတတ်ကြတယ်။ဒါမျိုးဆိုရင်တော့အမြန်ရမှာပါ။လိုတာရဖို့ဆိုရင်တော့လွယ်လွယ်နဲ့လက်မလျော့ဖို့ပါပဲ။ ကြိုးစားမှအောင်မြင်မှာပါ။ WPA2 Hacking ပြီးပါပြီ။

WPA2 Cracking နည်းလမ်း(၂)

WPA2 လိုင်းကို Crack လုပ်နိုင်တဲ့နောက်နည်းလမ်းတစ်ခုပါ Mac Changer Method လို့ခေါ်ပါတယ်။

Mac ကို Change လုပ်ပြီး Client ဘက်ကနေဖေါက်တဲ့နည်းလမ်းတစ်ခုပါ။

နည်းလမ်း ၁နဲ့တူတူပါပဲ၊အနည်းငယ်ကွာတာပါ။တမျိုးမရတမျိုးစမ်းကြည့်ပေါ့နော်။

ပထမဆုံး Command က airmon-ng start wlan0 ဖြစ်ပါတယ်။

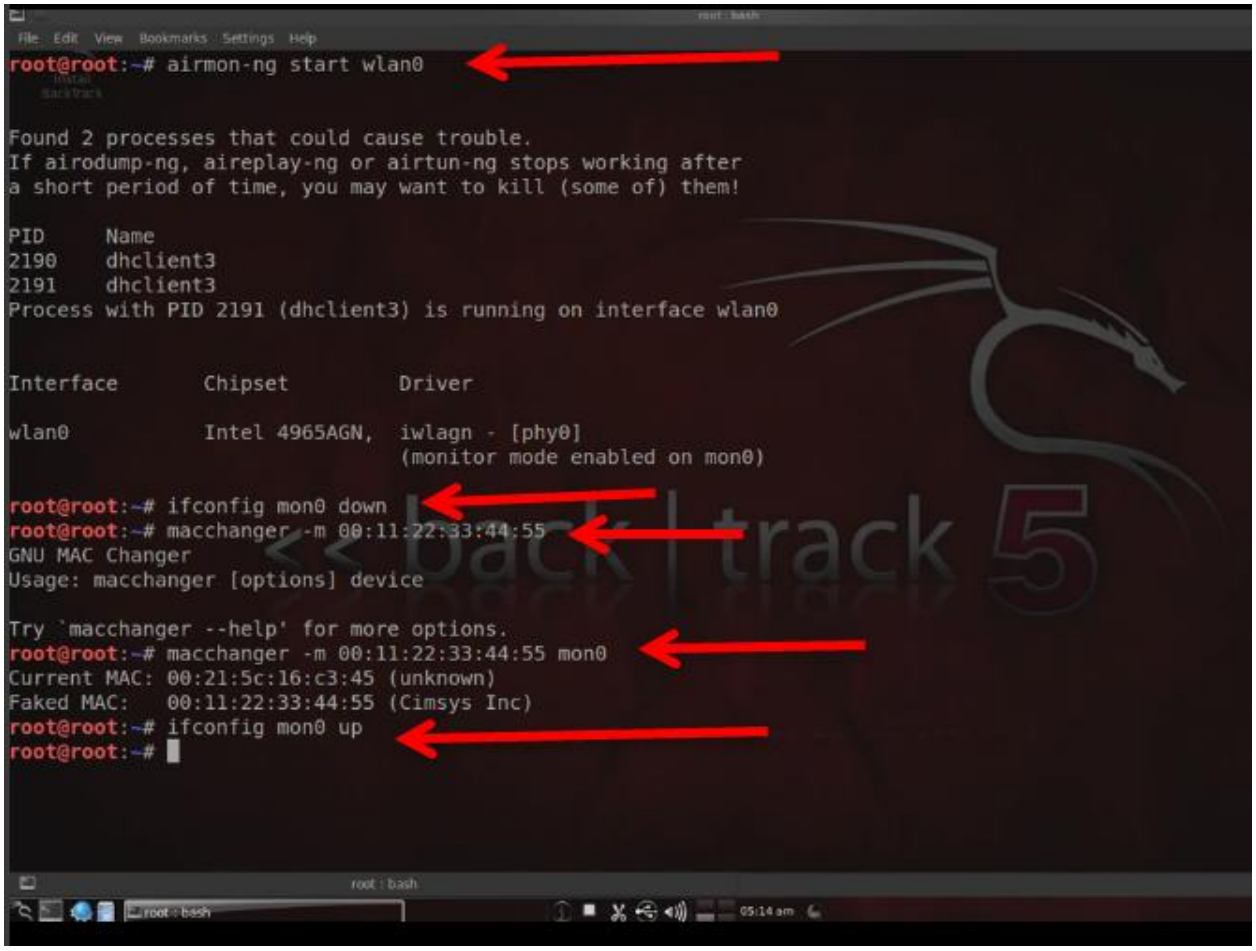
ပြီးနောက် ifconfig mon0 down လို့ရိုက်ပါ Enter ခေါက်

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။



နောက်တစ်ကြောင်းကတော့ airodump-ng mon0 ပါ။ရှိသမျှလိုင်းတွေပြပေးနေပါပြီ။

ကျနော်စက်မှာတော့ WPA2 လိုင်းတွေချည်းပြနေတယ်။ကျနော်က Victima ဆိုတဲ့လိုင်းကို Targetထား

လိုက်ပါပြီ။

မိမိ Target ရဲ့ဒေတာကိုမှတ်ထားပါ။ရိုက်ရမယ့် Command က

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

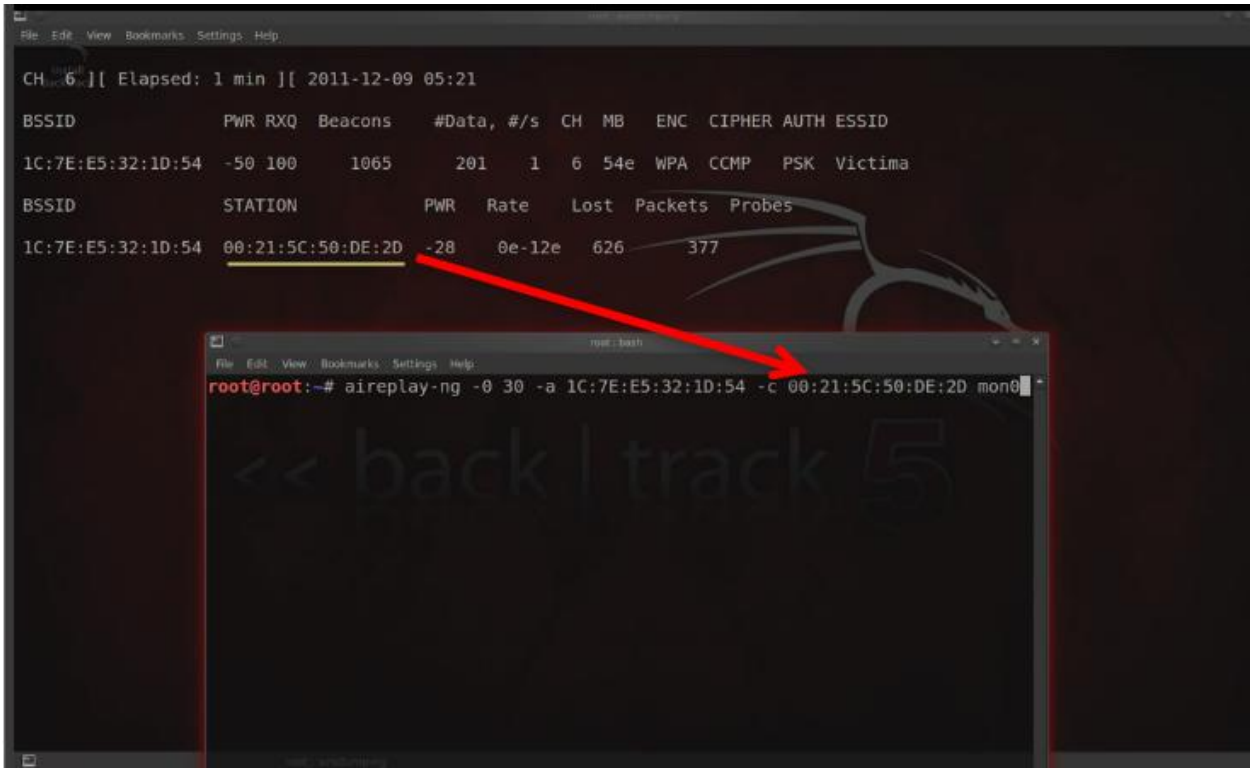
(မှတ်ချက်- Channel No.နဲ့ BSSID No.ကိုတော့မိမိ Target အတိုင်းပြောင်းထည့်ပါရန်)

အဲဒီကွန်မန်းရိုက်အပြီးမှာ မိမိ Target ရဲ့သီးသန့် Data ကိုပဲပြမှာပါ။

Terminal အသစ်တစ်ခုဖွင့်ပါ။

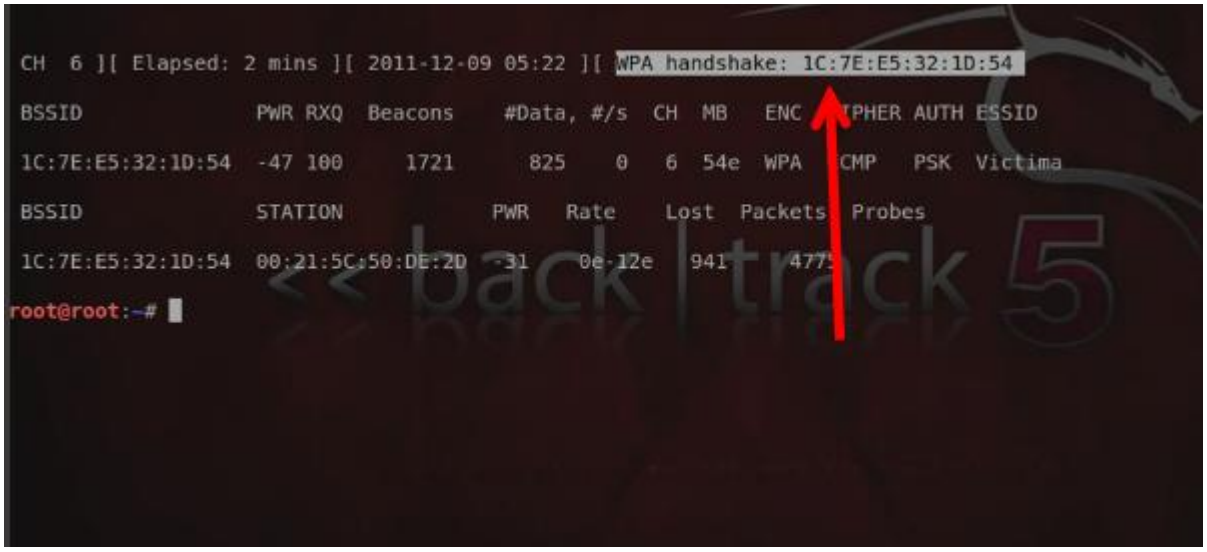
aireplay-ng -0 30 -a {မိမိတားဂတ်ရဲ့BSSID} -c {Client Macနံပါတ်} mon0 ကိုရိုက်ပါ။

ပုံမှာကြည့်ပြီးနမူနာယူပါဦး။



အဲဒီ Aireplay အပြီးမှာ မိမိ Target ဆီကို Request တွေ Sending လုပ်နေတာကိုတွေ့ရမှာပါ။

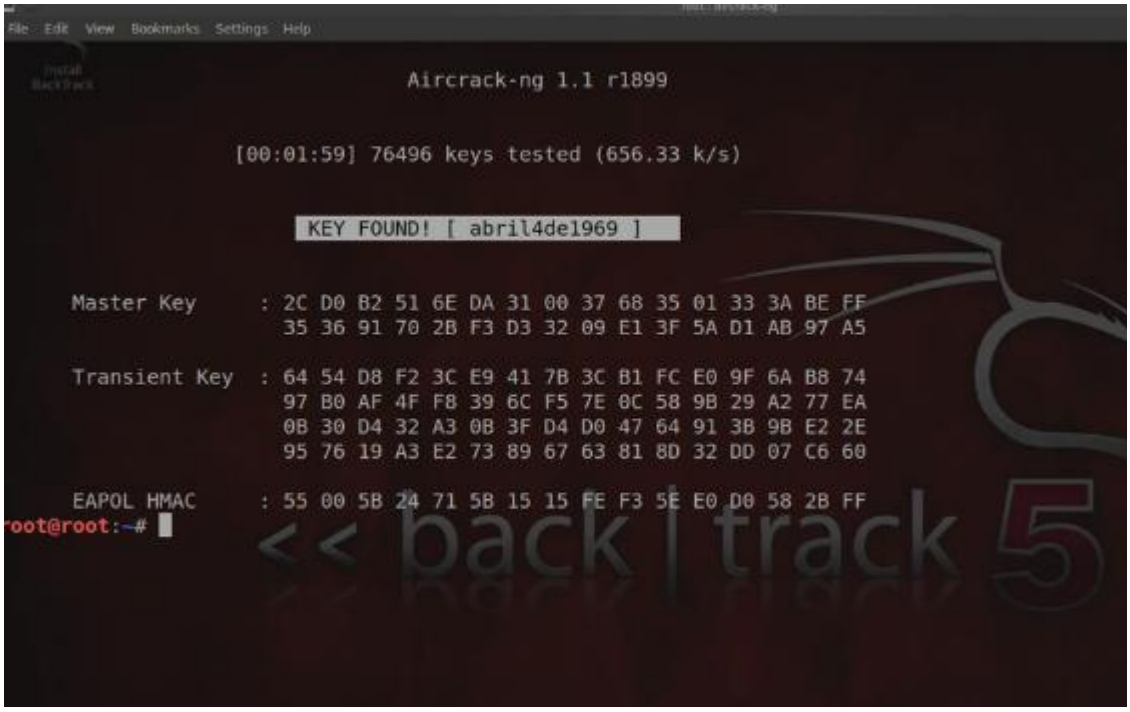
တဖြေးဖြေးနဲ့ပုံပါအတိုင်း WPA Handshake လို့ပေါ်လာတဲ့အခါ Crack လုပ်လို့ရနိုင်ပါပြီ။



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။ဒီင်း aircrack ရိုက်ပြီးလျှင် Words List တွေထဲက Password တွေနဲ့ Crack လုပ်နေတာမြင် ရပါမယ်။နောက်ဆုံးမှာတော့ပုံပါအတိုင်း Key ကိုရရှိလိုက်ပါတယ်။



Key Found=abril4de1969 ပါ။ဤသို့နဲ့ရှုပ်ထွေးတာတောင်ခဏနဲ့တိုက်ဆိုင်ရှာဖွေရရှိနိုင်ပါတယ် Cracking Time ကသိပ်ကိုမြန်ဆန်ပါတယ်။တချို့ခက်ခဲလွန်းသောပက်ဆက်များသာကြာတတ်ပါ တယ်။

WPA2 Cracking နည်းလမ်း(၂)ပြီးပါပြီ။

WPA2 ပိုင်ရှင်များလုံခြုံစိတ်ချရဖို့

WPA 2 ပိုင်ရှင်များအနေဖြင့် မိမိတို့၏ Password များကို Default ထားသုံး၍သော်၄င်း၊

Password အရှည်ကြီးစကားလုံးရှုပ်ရှုပ်ထွေးထွေးများပေး၍သော်၄င်း၊Mac address ကို

Filter လုပ်၍သော်၄င်း၊မိမိဝိုင်ဖိုင်လိုင်းကို နက်ဝက်မှ Hideလုပ်ထား၍သော်၄င်း။ပက်ဆဝက်ပေးရာ

တွင် မြန်မာဖေါင့်ကဲ့သို့စာလုံးများသုံးပါက Wordlist ထဲတွင်မပါသောကြောင့် လွယ်လွယ်နှင့်

Hackလို့ရမည်မဟုတ်ပါ။ထို့ ပြင်မိမိလိုင်းလေးလာလျှင် restart ချလိုက်ပါ။

MY Book Ref: Youtube(WEP,WPA2) Hacking,BT 5 wireless penetration testing book

You Tube တွင်ဆက်လက်လေ့လာနိုင်မည့် Video Training များ ::::::..... :::.....:: ....

http://www.youtube.com/watch?v=y9XV2MBPM5M

http://www.youtube.com/watch?v=FZso9pofw-0

http://www.youtube.com/watch?v=rzzgzP4hEo0

http://www.youtube.com/watch?v=T3iDWP2xeFw

http://www.youtube.com/watch?v=dB21RAvbcDQ

http://www.youtube.com/watch?v=aKQiAAzmW90&feature=fvsr

http://www.youtube.com/watch?v=BiJp9ZajJlg&feature=fvsr

အထက်ပါ Video Link များကို Download ဆွဲပြီးလေ့လာကြည့်ပါ WEP,WPA2 များကို Crackလုပ်ပြ

တဲ့ Video များဖြစ်ပါတယ်။

.....

ကျနော်လေ့လာမိသလောက်ပြန်လည် Share လုပ်ပေးသည့်နည်းပညာများကို နားမလည်ပါက

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

မှုမရှိပါ။ထို့ကြောင့်ဆင်ခြင်တရားလက်ကိုင်ထား၍စမ်းသပ်ကြပါ။အမှားအယွင်းများပါဝင်ပါကအကြံပြုစာများ

စိတ်ကြိုက်ပေးပို့ နိုင်ပါသည်။၄င်းအကြံပြုစာများအရ 2nd Edition တွင်ပြန်လည်ဖြည့်စွက်ဖေါ်ပြသွားပါမည်။

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