ကို 3thic0kiddi3 ဒီထက်မက အောင်မြင်ပါစေ

ကိုးကား

Network Hacking Testing

Armitage with Backtrack 5

5/27/2012

3thic0kiddi3

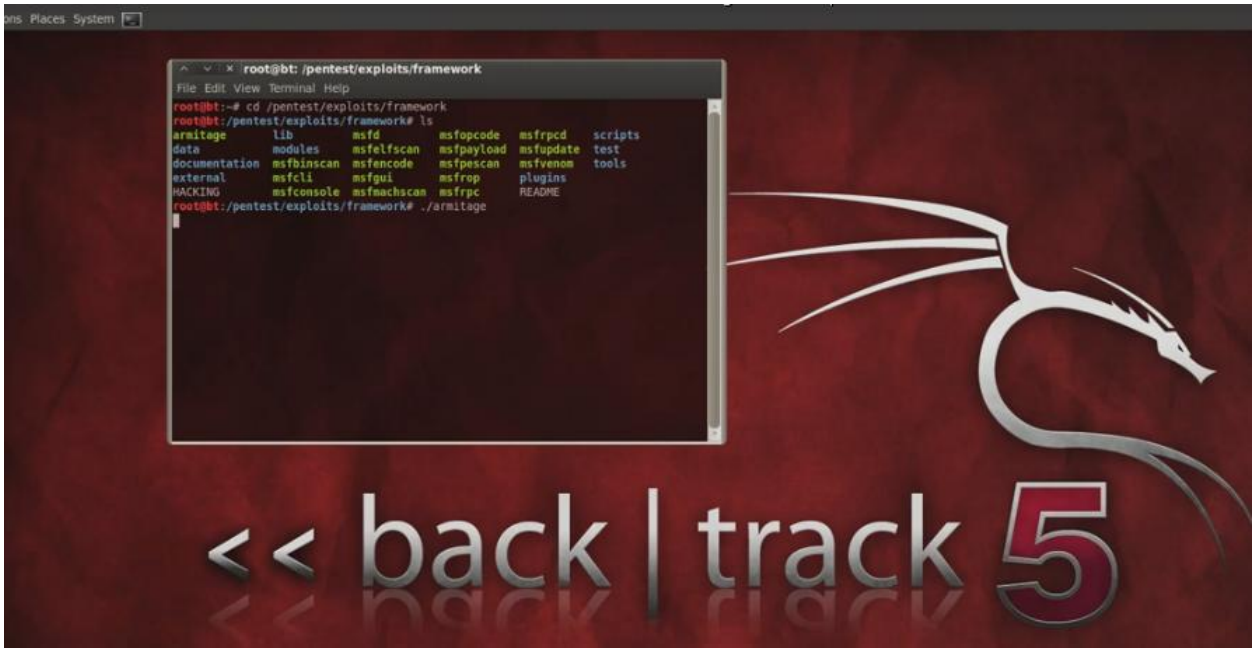
Network Hacking ကို Backtrack 5 ၏ Bulit in Tools Armitageဖြင့်စမ်းသပ်ခြင်း

BY 3thic0kiddi3

Armitage ဆိုတာ Back Track ရဲ့ Built in Hacking Tool တစ်ခုပါ။ Metasploit လို့လဲခေါ်ပါတယ်။အသေးစိတ်အချက်အလက်ကိုတော့ အွန်လိုင်းမှာရှာဖတ်ကြည့်ပါ။ကျနော်တို့ ဟာ Armitage ကိုသုံးပြီးနက်ဟက်ချိတ်ဆက်မှုရှိနေတဲ့ ကွန်ပြူတာတွေကိုဟက်လို့ရပါတယ်။ဒီထက်ဘာတွေစွမ်းဆောင်နိုင်သေးလဲတော့ကျနော်လဲသေချာမသိပါ။ခုစမ်းသပ်တဲ့အခါမှာကျနော်တို့ Back Track ကို BT5ဒါမှမဟုတ် 5R1,5R2 တို့သုံးပြီးအလုပ်လုပ်နိုင်ပါတယ်။ကျနော်တို့ ကအင်တာနက်ဆိုင်မှာသုံးနေရင်းအခြားကွန်ပြူတာများကိုထိန်းချုပ်ချင်တာဖြစ်ဖြစ်၊ကိုယ့်ဂိုင်ဖိုင်ကွန်ယက်မှာအခြားကွန်ပြူတာများကို(ဆာဗာအပါအဝင်)ထိန်းချုပ်ချင်တာပဲဖြစ်ဖြစ်ဒီနည်းကိုအသုံးပြုနိုင်ပါတယ်။သိပ်ကိုဆန်းကြယ်တယ်လို့ ထင်ရပေမယ့်အရမ်းကိုလွယ်ကူပါတယ်။

ကဲကျနော်တို့ စလိုက်ရအောင်- Back Track Terminal ကိုဖွင့်ပါ။

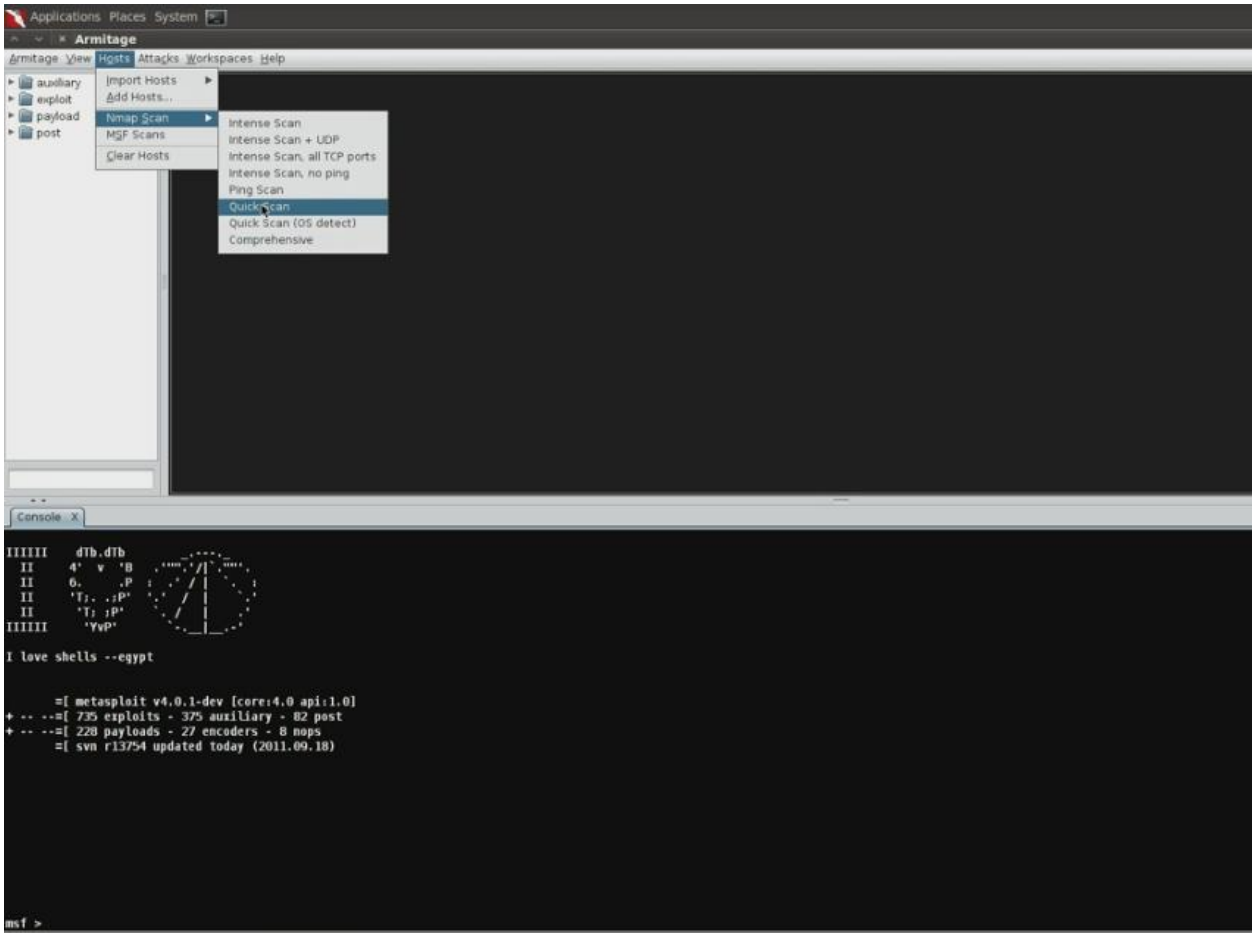
ပထမဆုံး cd /pentest/exploits/framework ကိုရိုက်ပါ။ပုံမှာပြထားတယ်ပြီးတော့ ls ကိုရိုက်ကြည့် armitage ကိုတွေ့လိုက်မယ် ။Armitag ကိုခေါ်မယ်။ ./armitage ဆိုရင်ခေါ်လိုက်ပါပြီ။ပုံမှာကြည့်ပါ။



ပုံပါအတိုင်း Box တက်လာရင် Start MSF ကိုနှိပ်ပါ။ Default user အတိုင်းပဲဆိုတော့ဘာမှပြောင်းစရာမလိုပါ။

အဲဒီမှာပုံပါအတိုင်း Armitage ပဂိုဂရမ်ပေါ်လာပါပြီ။ကျနော်တို့ပုံပါအတိုင်းပြုလုပ်ရအောင်

အပေါ်က Tools Bar ထဲက Hosts > Namp Scan >Quick scan(Os detect) ကိုရွေးပါမယ်။

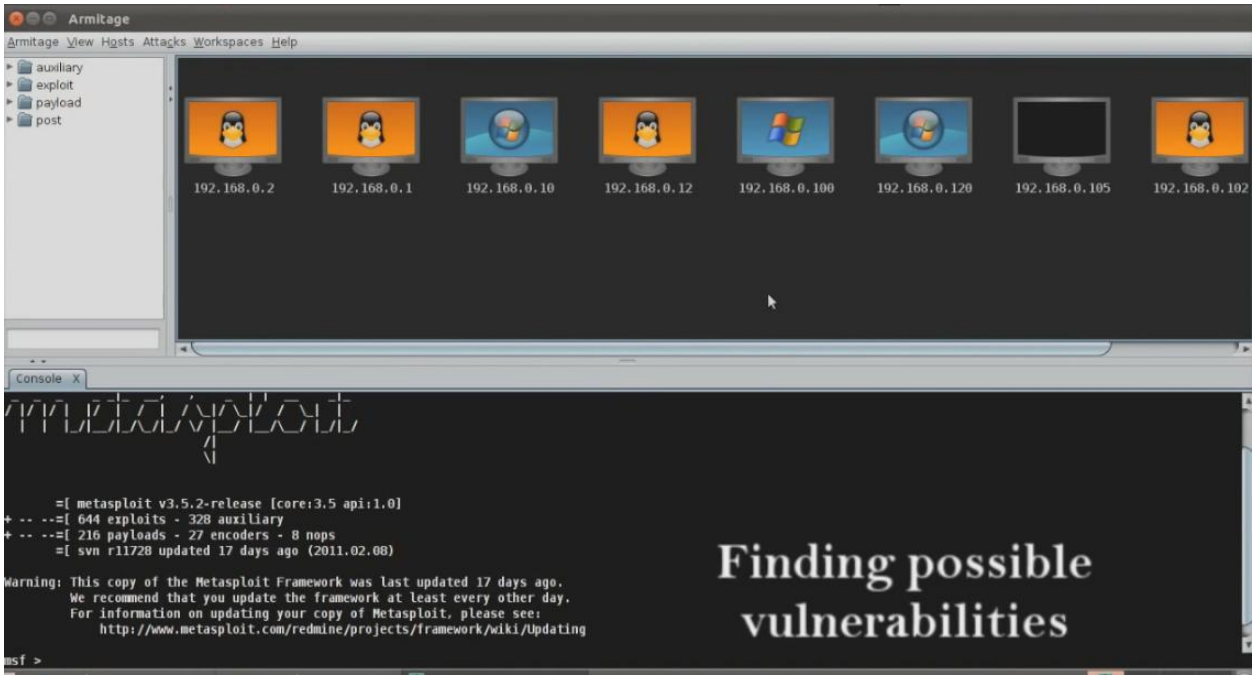


အဲဒီမှာ ip ထည့်စရာ Box လေးပေါ် လာ ပါ မယ်။ 192.168.1.0/24 လို့ထည့်ပါ။

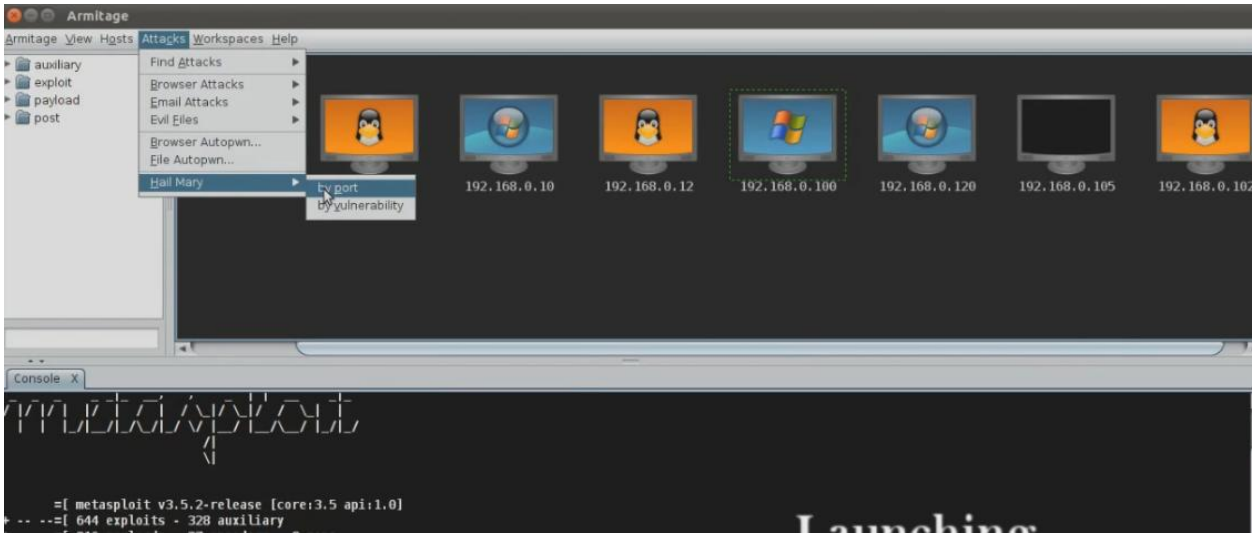
IP ထည့်တာနဲ့မိမိနက်ဟက်အတွင်းက ယူဇာကွန်ပြူတာတွေကိုပြပါတော့မယ်။Alert တက်လာပြီးဘယ်နလုံးရှိ

တယ်ဆိုတာပြပါလိမ့်မယ်။

ပုံမှာနက်ဟက်ထဲကကွန်ပြူတာတွေကိုပြနေတဲ့ပုံပါ။

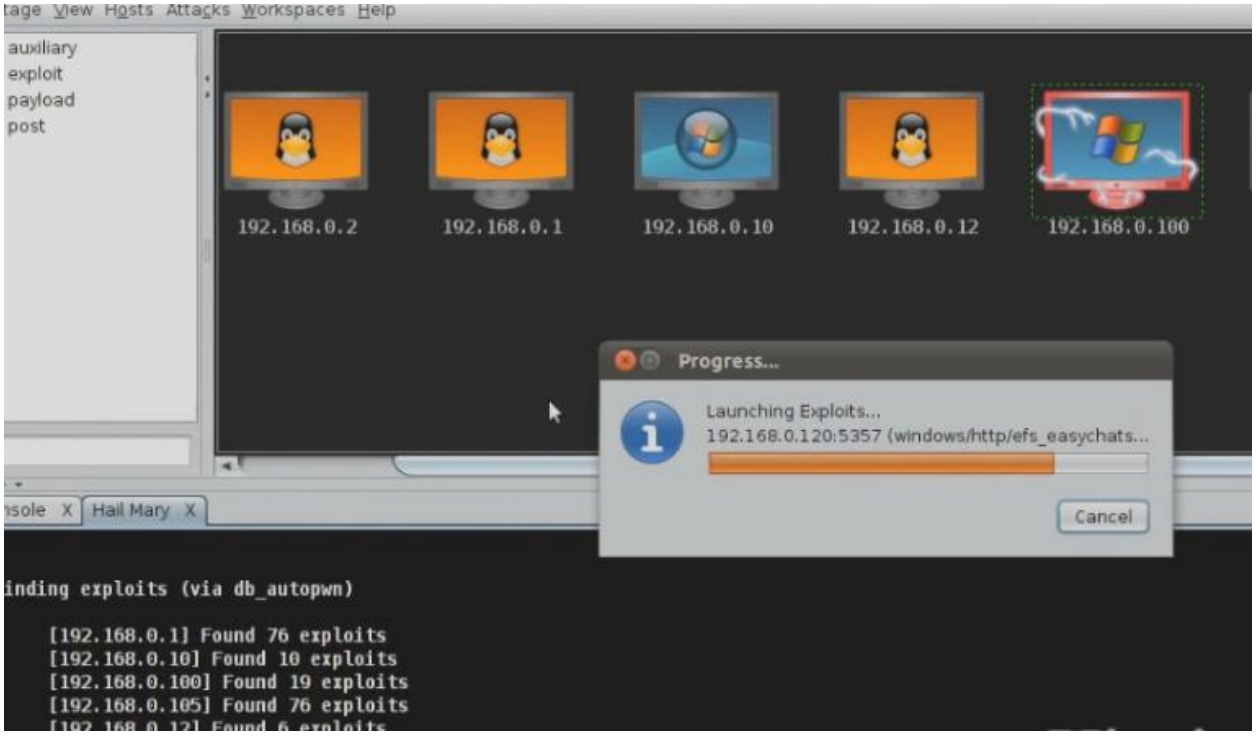


မိမိ Terget Computer ကိုကလစ်ထောက်ပါပြီးတော့ Tool bar က attack>Hail Mary>By port ကိုရွေးပါ

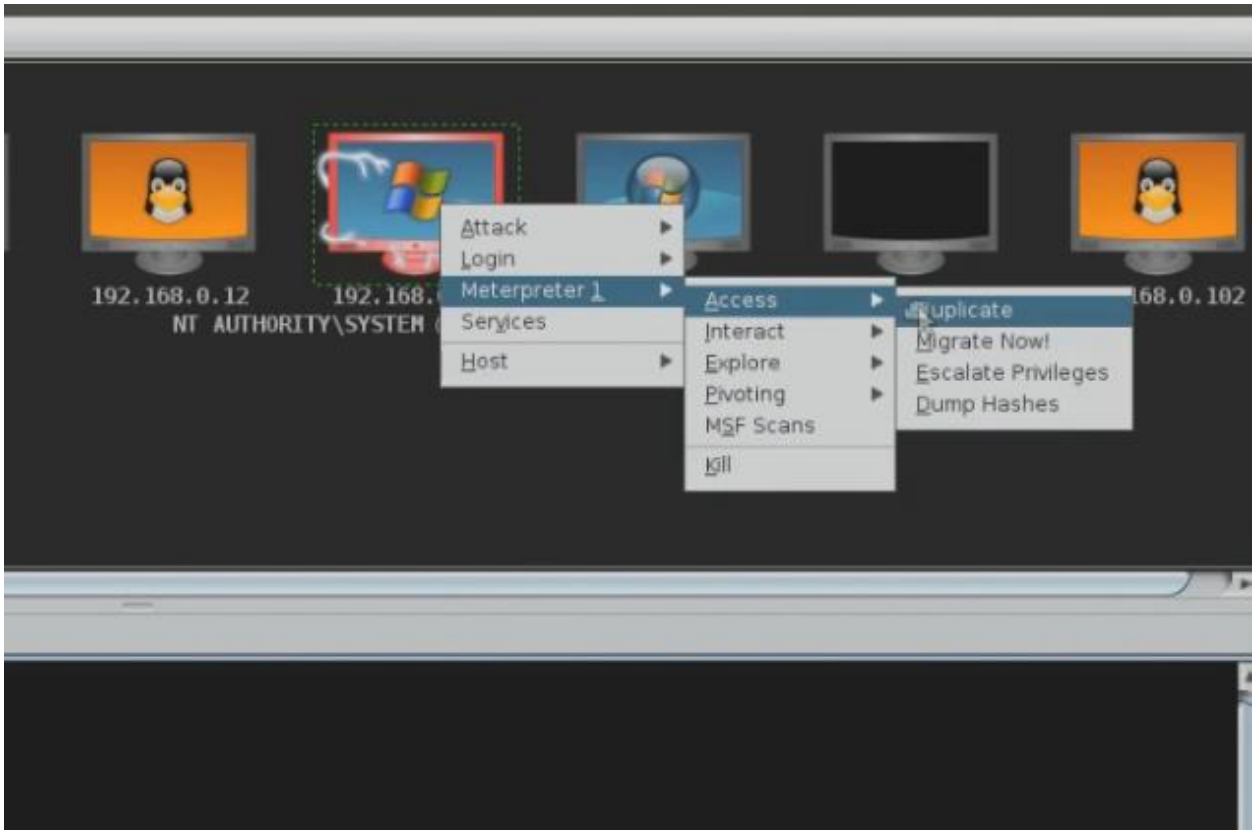


အဲဒီအခါ Exploit တွေကို Scan ဖတ်နေတာကိုတွေ့ရမှာပါ။အဲမှာ Port attack ခံရတဲ့ Target ကွန်ပြူတာဟာ

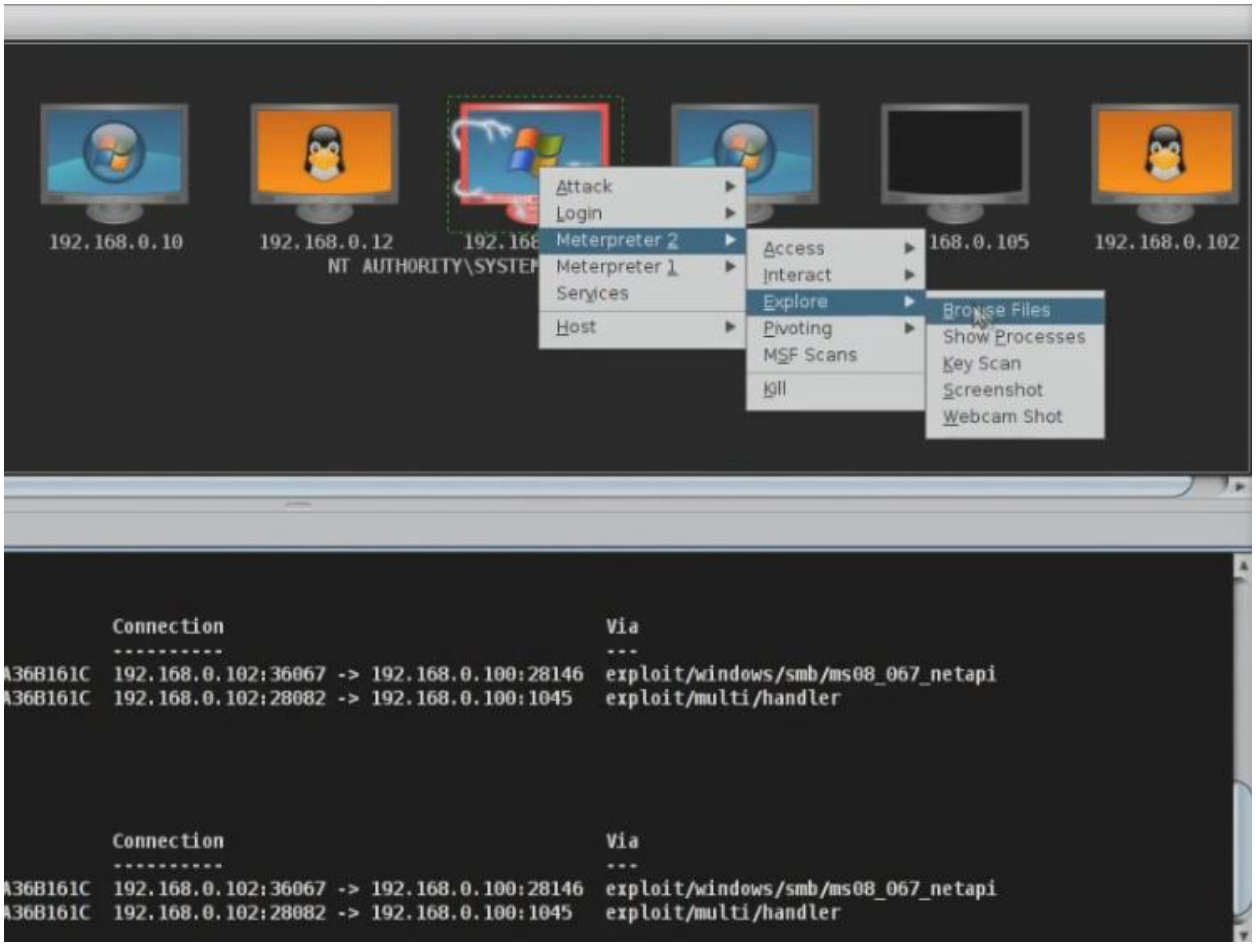
မိုးကြိုးပုံနဲ့ပြနေမှာပါ။ပုံမှာကြည့်ပါ။



ပျော်ဖို့ကောင်းမှာပါ။ Lunching Exploits လုပ်ပြီးသွားရင်ကျနော်တို့ Target Computer ကို Right Click ထောက်ပြီး ပုံပါအတိုင်း Duplicate လုပ်ပါ။



အဲလိုမျိုး Accessရသွားဂျင် Right Click နှိပ်ပြီး ပါတဲ့ Function တွေကိုစမ်းနေပါ။ကျနော် System 32 အောက်ကို အောက်ပါအတိုင်းသွားပြပါမယ်။ Browse File လုပ်လိုက်တာပါ။



Admin password

တွေ၊ Screen shot တွေကိုကျနော်တို့လိုသလိုယူလို့ရပါတယ်။အခြားနက်ဟက်ချိတ်နေတဲ့ကွန်ပြူတာတွေ၊ ပရင်တာတွေ၊ကိုသုံးလို့ရပါတယ်။အခြေနေတမျိုးနဲ့တမျိုးကမတူနိုင်လို့မိမိဘာသာဆက်လက်စမ်းကြည့်ကြပါ။ Computer တစ်ခုလုံးကို Full access ကိုရနိုင်ပါတယ်။

Armitage နဲ့ပါတ်သတ်တဲ့ Tutorial from Youtube

Video တွေကြည့်ပြီးရင်ကျနော်ပြောပြတာထက်ပိုရှင်းပိုသိလာမှာပါ။အောက်မှာ Metasploits နဲ့ပါတ်သတ်တဲ့ဘီဒီယိုတွေကျနော်လင့်ပေးထားပါတယ်။ကြိုးစားလေ့လာလိုက်ကြပါဦး

http://www.youtube.com/watch?v=j7uLBzULOE0

http://www.youtube.com/watch?v=Z0x_O75tRAU

http://www.youtube.com/watch?v=2rQfNfoQVCQ

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

http://www.youtube.com/watch?v=EACo2q3kgHY

http://www.youtube.com/watch?v=wq30OrCd-9s

http://www.youtube.com/watch?v=zF91ucpE1Tw&feature=related

http://www.youtube.com/watch?v=T01SgKqL9Is&feature=related

http://www.youtube.com/watch?v=PQyGPar580s&feature=related

ဤစာအုပ်ကိုဟက်ကင်းလေ့လာနေသော မြန်မာလူငယ်များ၊ဆက္ကူရတီသမားများ၊နက်ဂက်သမားများ အတွက်ရည်ရွယ်ထားပါသည်။Educational Purpose Only ဖြစ်ပါသည်။သိထားဂုန်ပြောပြခြင်းဖြစ်သဖြင့် မိမိကလိလို့ပျက်စီးသောဆိုးကျိုးဖြစ်ထွန်းမှုအတွက်တာဂန်မယူပါ။

စာဖတ်သူများအားအစဉ်လေးစားလျက်

3thic0kiddi3

3thic0kiddi3@gmail.com

www.ethickiddie.blogspot.com (my book store)

ထွက်ရှိပြီးသည့်စာအုပ်များ-

(1) Wireless Hacking Basic (download)
(2) DNN hacking (download)
(3) IIS hacking (download)