Android Security & Exploitation

Aditya Gupta (@adi1391)

Founder, Attify (http://attify.com)

adi@attify.com

Certifications : http://securitytube-training.com
Pentester Academy : http://PentesterAcademy.com

ADB

ADB

- Android Debug Bridge
- Used to interact with the device / emulator
- Adb daemon
- Could be used to debug apps, install applications, do file system modifications etc.

© 2015 - Pentester Academy and Attify

ADB

```
# ps
USER      PID   PPID  VSIZE  RSS     WCHAN    PC         NAME
root      1     0     368    220   c0077dc0 000090cc S /init
root      2     0     0      0     c009015c 00000000 S kthreadd
root      3     2     0      0     c007aeec 00000000 S ksoftirqd/0
root      4     2     0      0     c00aeac4 00000000 S watchdog/0
root      5     2     0      0     c008c214 00000000 S events/0
```

```
system    19682 1304  135620 15020 ffffffff ffff0520 S com.sec.android.providers.drm
app_78    19770 1304  146072 23376 ffffffff afd0c5bc S com.whatsapp
radio     19788 1304  138720 20488 ffffffff afd0c5bc S com.wssyncmldm
app_41    19807 1304  135888 16740 ffffffff afd0c5bc S com.sec.android.widgetapp.dualclock
app_39    19816 1304  157876 23580 ffffffff afd0c5bc S com.google.android.apps.maps:GoogleLocat
```

adb devices

```
MathBook Pro:~ adityagupta$ adb devices
List of devices attached
emulator-5554   device
```

adb kill-server
adb start-server

```
MathBook Pro:~ adityagupta$ adb kill-server
MathBook Pro:~ adityagupta$ adb start-server
* daemon not running. starting it now on port 5037 *
* daemon started successfully *
MathBook Pro:~ adityagupta$
```

adb shell

```
MathBook Pro:~ adityagupta$ adb shell
# id
uid=0(root) gid=0(root)
#
```

Some more commands

- `adb logcat`
- `adb install [appname].apk`
- `adb push srcaddr destaddr`
- `adb pull srcaddr destaddr`

© 2015 - Pentester Academy and Attify

Some important locations

- **/data/data :** All applications data installed by user
- **/data/app :** APKs of applications installed by user
- **/system/app :** System Applications
- **/data/system :** Files such as gesture.key
- **/data/local/tmp :** Writeable (without root)

© 2015 - Pentester Academy and Attify

PM

```
root@hacking:~# adb shell pm --help
Error: unknown command '--help'
usage: pm list packages [-f] [-d] [-e] [-s] [-3] [-i] [-u] [FILTER]
       pm list permission-groups
       pm list permissions [-g] [-f] [-d] [-u] [GROUP]
       pm list instrumentation [-f] [TARGET-PACKAGE]
       pm list features
       pm list libraries
       pm path PACKAGE
       pm install [-l] [-r] [-t] [-i INSTALLER_PACKAGE_NAME] [-s] [-f]
                  [--algo <algorithm name> --key <key-in-hex> --iv <IV-in-hex>
] PATH
       pm uninstall [-k] PACKAGE
       pm clear PACKAGE
       pm enable PACKAGE_OR_COMPONENT
       pm disable PACKAGE_OR_COMPONENT
       pm disable-user PACKAGE_OR_COMPONENT
       pm grant PACKAGE PERMISSION
       pm revoke PACKAGE PERMISSION
       pm set-install-location [0/auto] [1/internal] [2/external]
       pm get-install-location
       pm set-permission-enforced PERMISSION [true|false]
```