ANDROID TAMER

https://androidtamer.com

WHAT

Virtual machine for Android (Security) Professionals

Supports

- VirtualBox
- VMWare
- Vagrant / Ansible

WHY

Saves time while

- Finding and installing tools
- Configuring them
- Ensuring all other tools are still working
- Managing updates of each tool

TOOLS INCLUDE

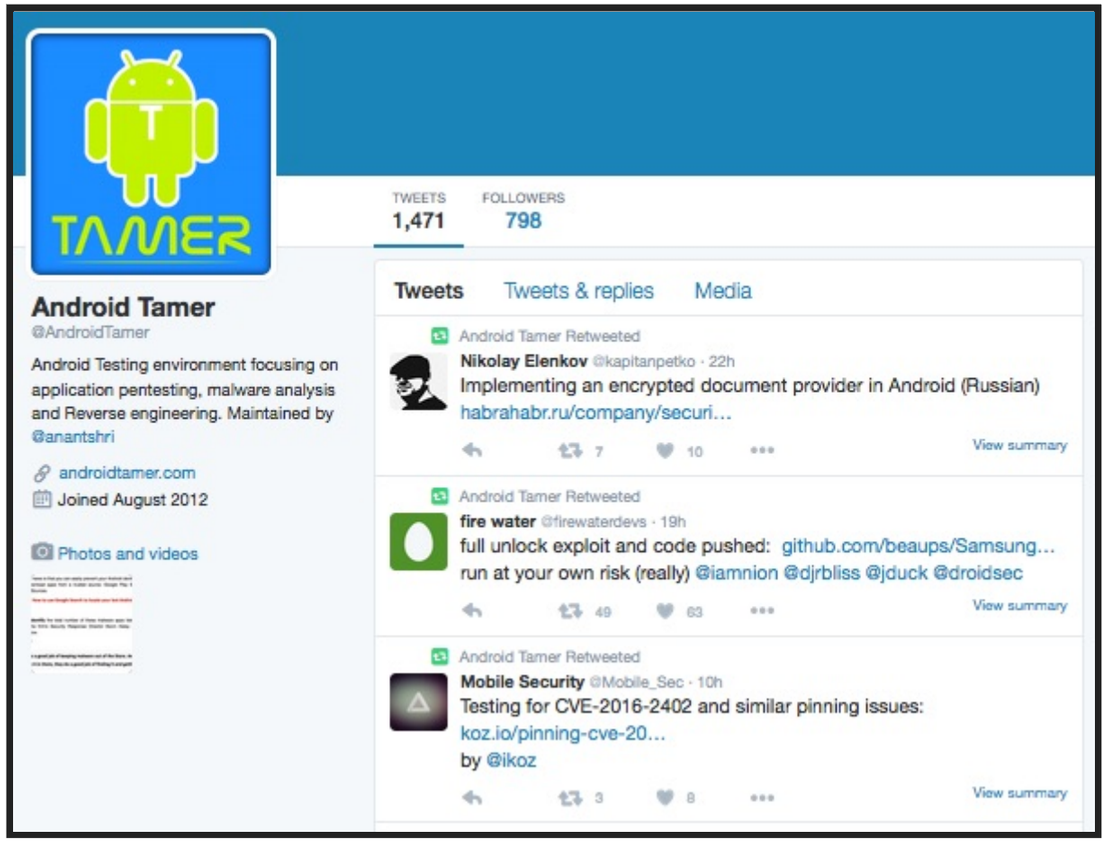
1. adb / fastboot / android-sdk
2. dex2jar / **enjarify**
3. apktool
4. jad / jd-gui / jadx / jadx-gui
5. drozer
6. DFF / ddrescueview
7. SQLiteManager / SQLiteMan
8. Burp Free / OWASP-ZAP
9. pidcat
10. MobSF (in-progress)
11. Cukoo-droid (in-progress)
12. and more....

CUSTOM FEATURES

1. Easy Management of multiple devices
2. One liner commands (apk2java, drozer_start etc)
3. Scripts for automated analysis
4. Software update managed over apt-get repository (alpha phase) (http://repo.androidtamer.com/)
5. All Tools pre-configured in PATH (no need to switch directories)

THAT'S NOT IT

@ TWITTER



Follow Us @AndroidTamer to get Latest Android News

FB/ANDROIDTAMER

SECURITY ENHANCEMENTS

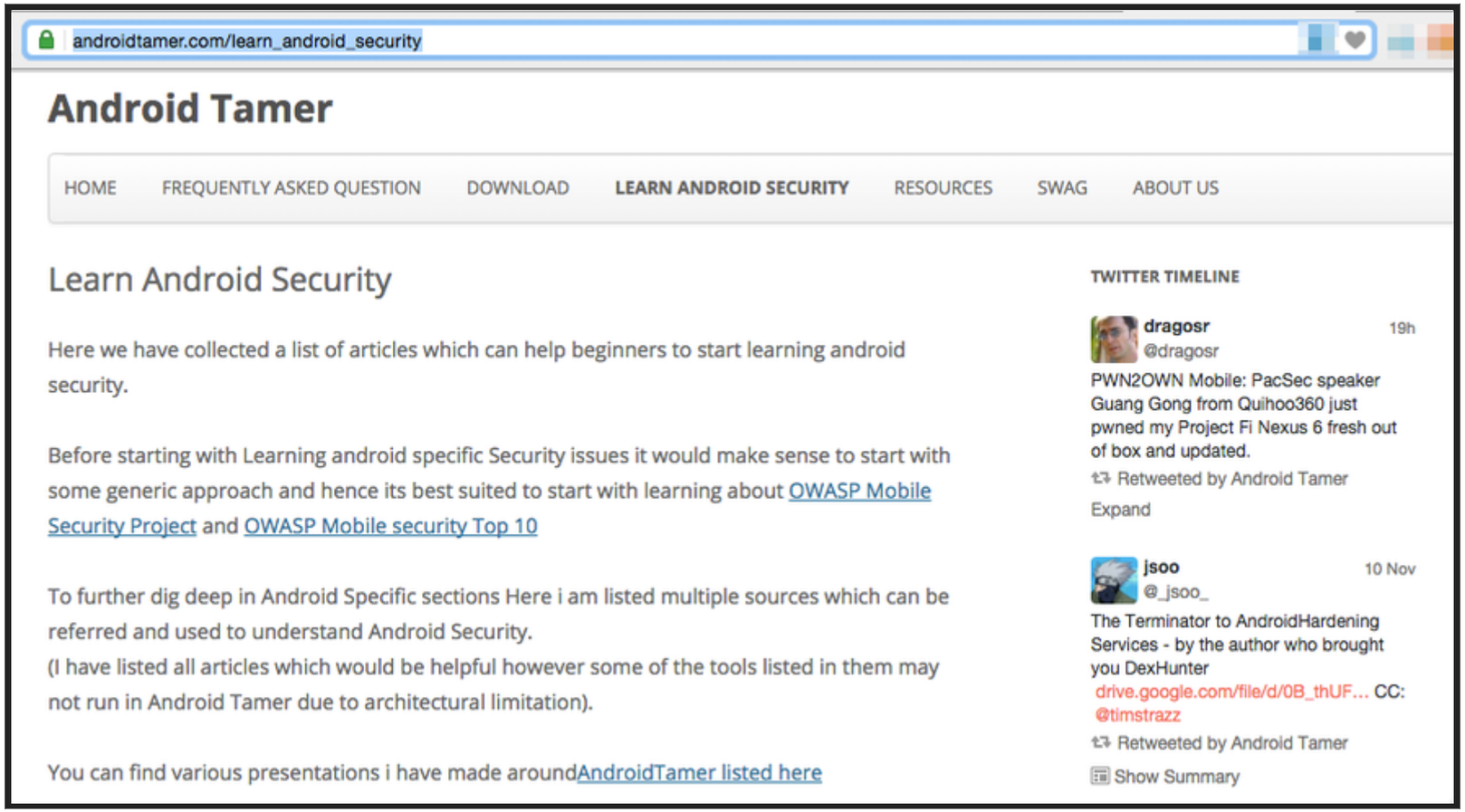
androidtamer.com/android-security-enhancements/

Android Security Enhancements

This page catalogues how android security has evolved over various versions of android. We strive to catalogue which version introduced a specific security feature or tweaked it as well as which version fixed a specific flaw.

ANDROID VERSION	SECURITY ENHANCEMENT	DETAILS	REFERENCE / BYPASS (IF APPLICABLE)
5.0	Webview : de-coupled from core and OTA based upgrade	WebView can now be updated independent of the framework and without a system OTA. This will allow for faster response to potential security issues in WebView	Chrome developers G+ Post WebView for android
5.0	Fixed : SQL injection vulnerability in WAPPushManager	In Android <5.0, a SQL injection vulnerability exists in the opt module WAPPushManager, attacker can remotely send malformed WAPPush message to launch any activity or service in the victim's phone (need permission check)	Fixed commit POC : CVE-2014-8507
5.0	Fixed : Privilege Escalation using ObjectInputStream	In Android <5.0, java.io.ObjectInputStream did not check whether the Object that is being deserialized is actually serializable.	Fixed Commit POC : CVE-2014-7911
5.0	Fixed : SMS resend vulnerability	Applications can send SMS without privilege leading to undesired cost to user or be used for data exfiltration	Fixed commit POC for CVE-2014-8610
5.0	FORTIFY_SOURCE improvements	Protection against memory-corruption vulnerabilities involving stpcpy(), stpncpy(), read(), recvfrom(), FD_CLR(), FD_SET(), and FD_ISSET() libc functions	
5.0	non-PIE linker support removed	Enhancing Address Space Layout Randomization (ASLR) by requiring all dynamically linked executables to support PIE (Position-Independent Executables)	

LEARN ANDROID



https://androidtamer.com/learn_android_security

DEMO TIME

1. Application decompiling
2. Automated assessment (drozer_checks)
3. Multi devices management (adb list)
4. MobSF
5. Build your own Distro (Debian compatible Repository)

DEMO: APK2JAVA

```
android@tamer:~/Desktop/Arsenal/demo7$ apk2java CMFileManager.apk
APK TO JAVA source code extraction script
This is a script created by Anant Shrivastava
http://anantshri.info
This script will work on automating the work of extracting the source code
Starting APK Decompile
/usr/local/bin/apk2java CMFileManager.apk
CMFileManager.apk
APK to JAVA/SRC conversion Utility
CMFileManager
CMFileManager.apk
/home/android/Desktop/Arsenal/demo7/CMFileManager.apk
/home/android/Desktop/Arsenal/demo7
APK TOOLS extracting files
Doing APKtool now
apktool decode -f -o /home/android/Desktop/Arsenal/demo7/CMFileManager.apk
leManager.apk_src/
I: Using Apktool 2.1.0-25bc46-SNAPSHOT on CMFileManager.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /home/android/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...
```

DEMO: DROZER_CHECK

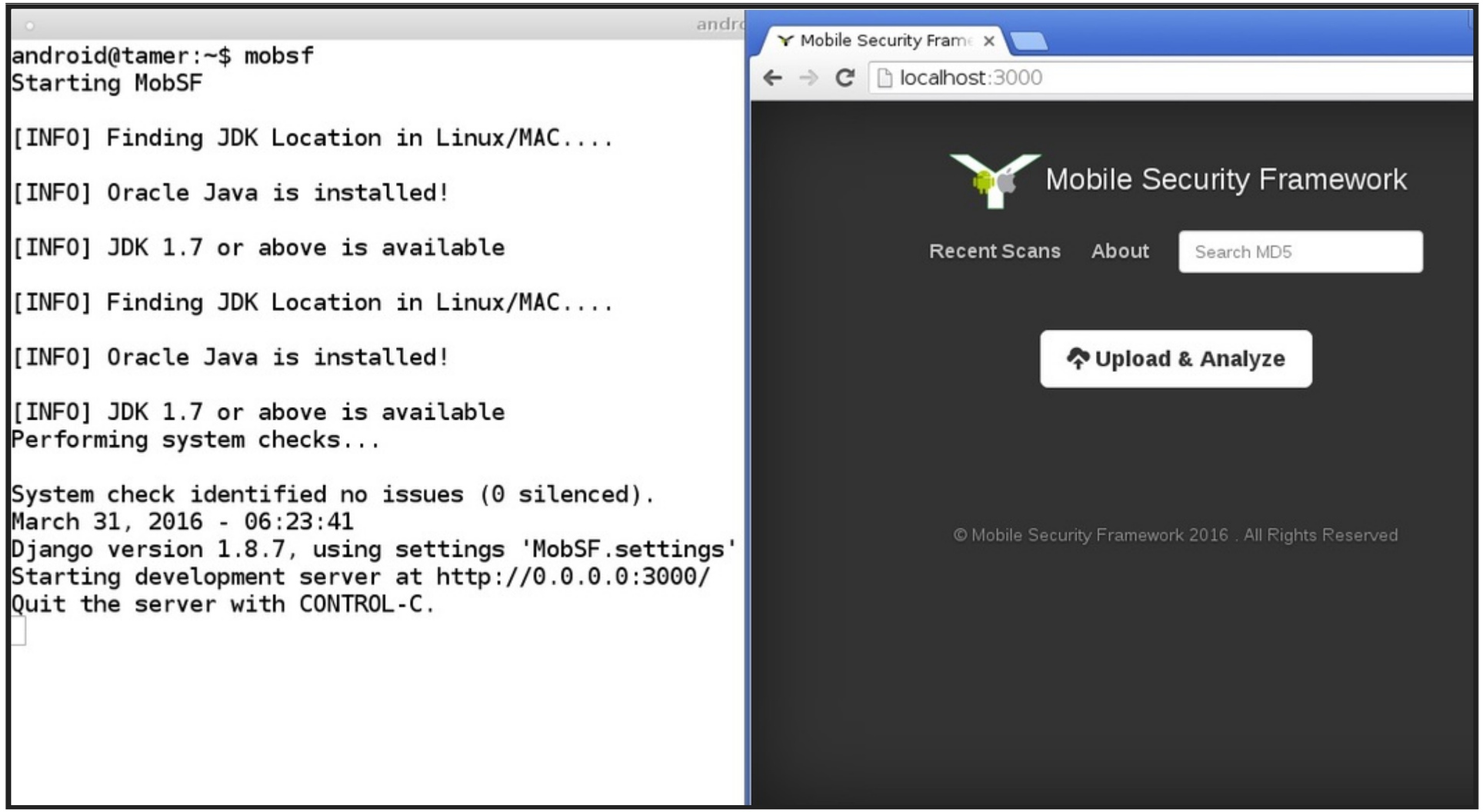
```
android@tamer:~$ drozer_check.sh jakhar.aseem.diva
Selecting dadcb63e00e6dbf9 (Genymotion Xtreme_Android_Exploitation_Lab 4.4.4)

Package: jakhar.aseem.diva
  Application Label: Diva
  Process Name: jakhar.aseem.diva
  Version: 1.0
  Data Directory: /data/data/jakhar.aseem.diva
  APK Path: /data/app/jakhar.aseem.diva-1.apk
  UID: 10090
  GID: [1028, 1015, 3003]
  Shared Libraries: null
  Shared User ID: null
  Uses Permissions:
  - android.permission.WRITE_EXTERNAL_STORAGE
  - android.permission.READ_EXTERNAL_STORAGE
  - android.permission.INTERNET
  Defines Permissions:
  - None

Selecting dadcb63e00e6dbf9 (Genymotion Xtreme_Android_Exploitation_Lab 4.4.4)

<manifest versionCode="1"
          versionName="1.0"
          package="jakhar.aseem.diva"
```

DEMO: ADB LIST

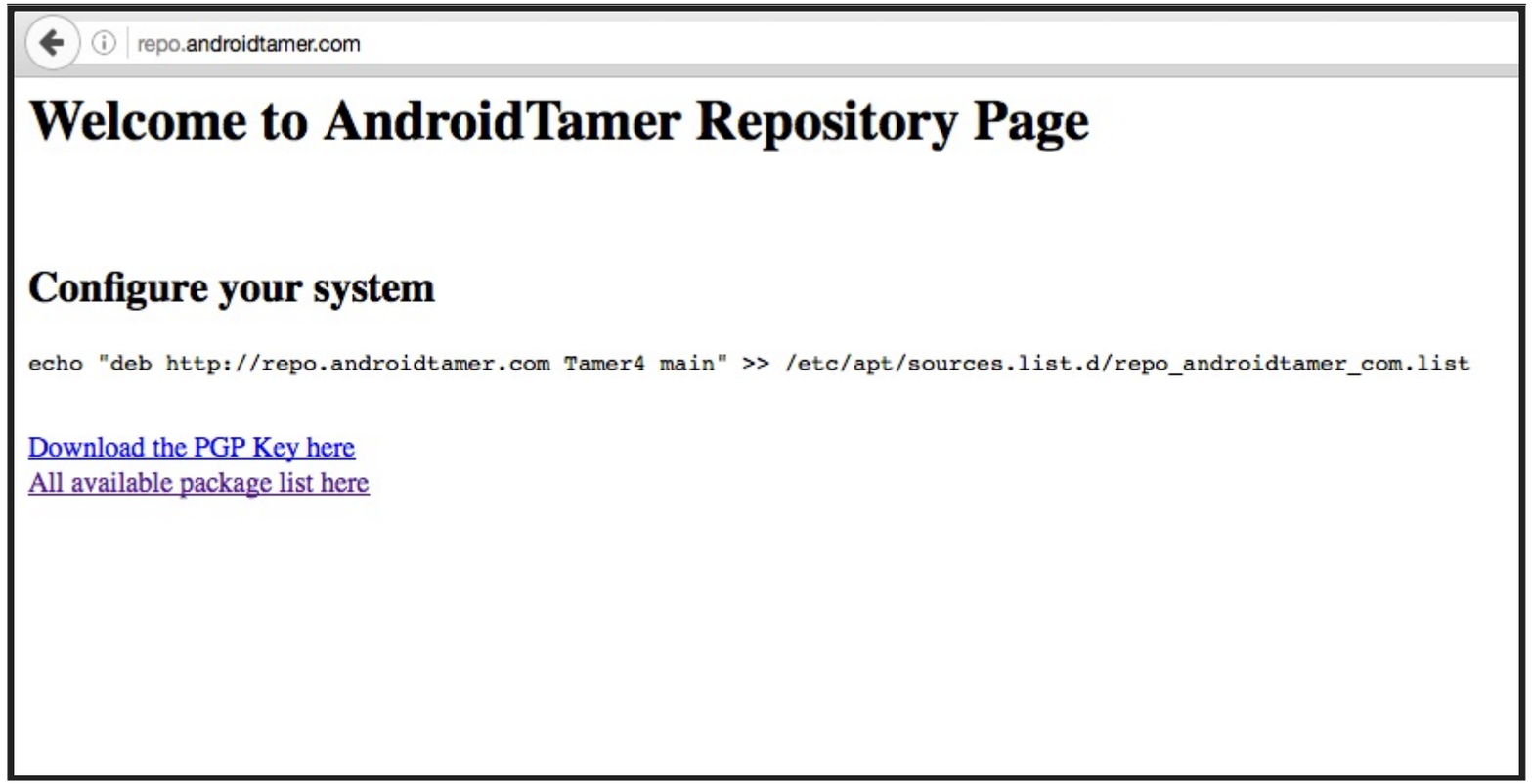
```
android@tamer:~$ adb list
ADB Status  : DeviceName  : Device SerialNo
device      : geny        : 192.168.57.101:5555
unknown     : nexus4      :
unknown     : spice       :
unknown     : nexus4      :
unknown     : nexus7      :
unknown     : oneplusx    :
unknown     : oneplus     :
unknown     : redmi       :
unknown     : geny2       : 192.168.56.102:5555
unknown     : geny3       : 192.168.56.103:5555
unknown     : grand2      :
unknown     : genynew     : 172.28.128.3:5555
android@tamer:~$
```

1. Add entries in ~/.adb_list
2. format of entries "ABC;SERIALNO"
3. echo "abc;1234567890" >> ~/.adb_list

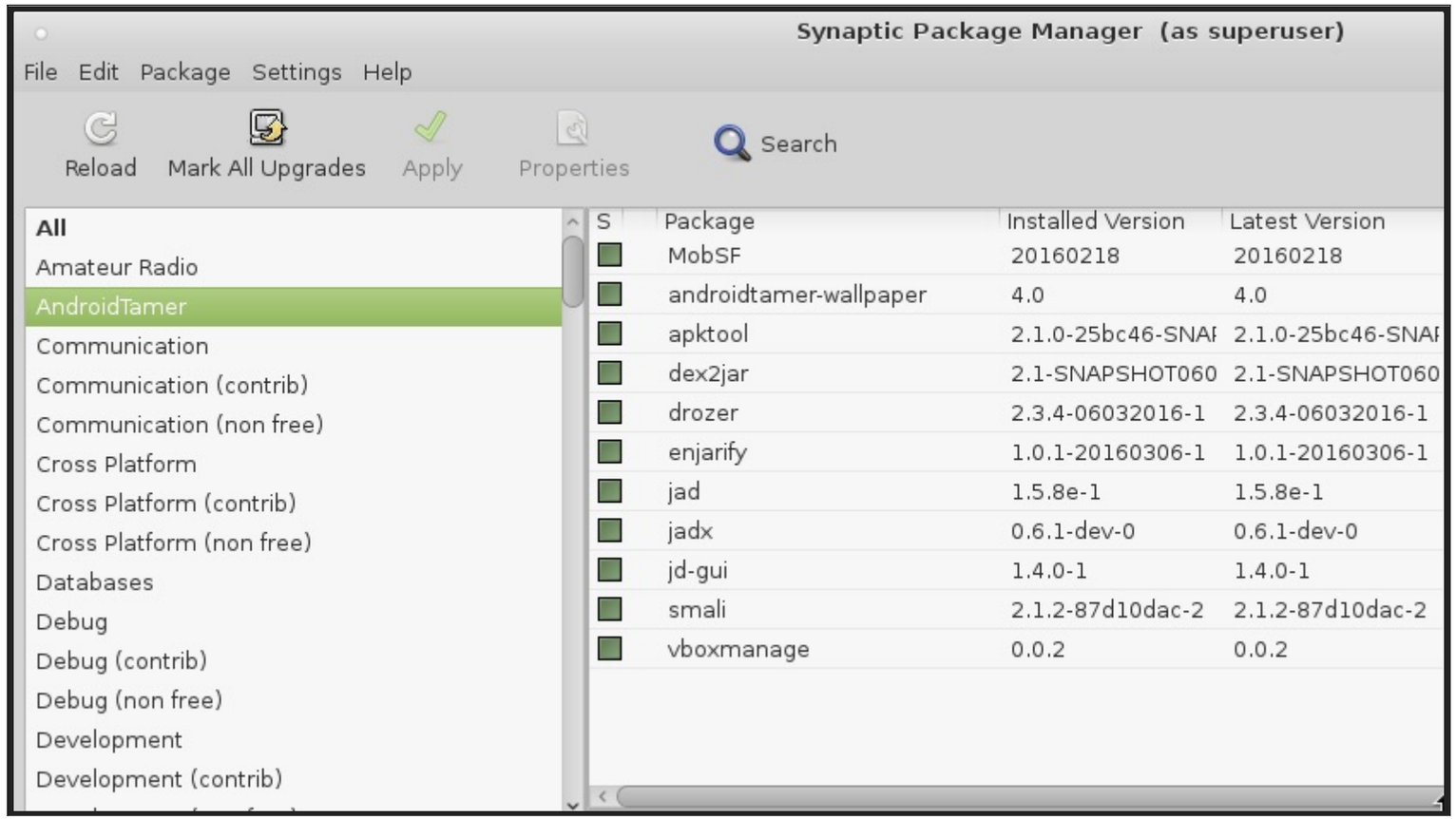
DEMO: MOBSF


android@tamer:~$ mobsf
Starting MobSF
[INFO] Finding JDK Location in Linux/MAC....
[INFO] Oracle Java is installed!
[INFO] JDK 1.7 or above is available
[INFO] Finding JDK Location in Linux/MAC....
[INFO] Oracle Java is installed!
[INFO] JDK 1.7 or above is available
Performing system checks...
System check identified no issues (0 silenced).
March 31, 2016 - 06:23:41
Django version 1.8.7, using settings 'MobSF.settings'
Starting development server at http://0.0.0.0:3000/
Quit the server with CONTROL-C.
Mobile Security Fram
localhost:3000
Mobile Security Framework
Recent Scans
About
Search MD5
Upload & Analyze
© Mobile Security Framework 2016 . All Rights Reserved

BUILD YOUR OWN



PACKAGE REPOSITORY



SUGGESTIONS & SUPPORT

1. Suggest more tools
2. Issues / Challenges faced
3. Support by contributing to the project
4. Write articles & blogposts

THANKS

Follow @AndroidTamer for all Updates