



# Android Pen Testing Environment Setup ∞

**CHEAT-SHEET**

02 Jun 2021

Arr0way

This document covers the least exciting aspect of Android mobile app security testing, configuring the testing environment. It is both time consuming and an extremely important part of the assessment process to get right. This guide covers setup of GenyMotion with Burp Suite on Mac OS, but it should be trivial to replicate on Linux or Windows.

## Table of Contents

- [Install GenyMotion](#)
- [Setup Burp Proxy with GenyMotion](#)
  - [1. GenyMotion Burp Proxy Settings](#)
  - [2. Android 8.1 Proxy Settings](#)
  - [3. Android Burp Certificate Installation](#)
  - [4. Burp Proxy Settings](#)
  - [5. ADB](#)
  - [6. Installing APK Files](#)
  - [7. ADB Basic Commands](#)
  - [8. Open GApps](#)

## Install GenyMotion

GenyMotion is the android emulator of choice for dynamic android app security testing.

Installation on mac requires Virtual Box to be installed first, then run through the GenyMotion installer.

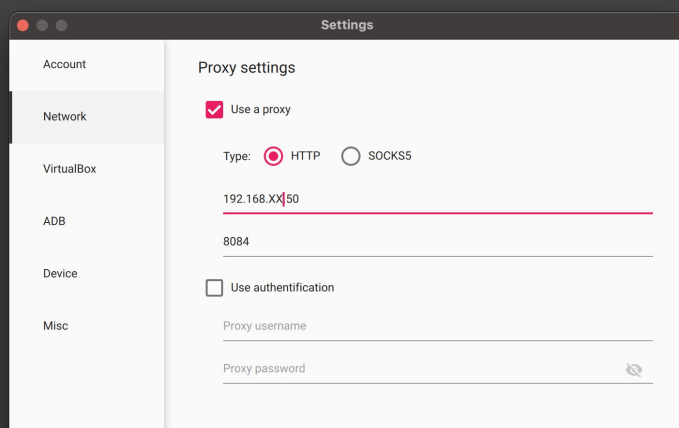
1. Install Android device (Nexus 4 works well)
2. Select Android 8.1 and deploy

## Setup Burp Proxy with GenyMotion

If you are using DHCP you may want to statically assign an address, as the IP randomly changing requires this process to be completed again (which can get extremely annoying...).

### 1. GenyMotion Burp Proxy Settings

1. Select GenyMotion
2. Preferences
3. Network
4. Proxy Settings and tick HTTP and add your local interface address and a different port to one that Burp is using



[All Blog](#)  
[Cheat Sheets](#)  
[Techniques](#)  
[Security Hardening](#)  
[WalkThroughs](#)

## CHEAT SHEETS

[Reverse Shell Cheat Sheet: PHP, Python, Powershell, Bash, NC, JSP, Java, Perl](#)  
[Nmap Cheat Sheet: Commands & Examples \(2022\)](#)  
[DNS Tunneling dnscat2 Cheat Sheet](#)  
[SSH Lateral Movement Cheat Sheet](#)  
[Android Pen Testing Environment Setup](#)  
[Password Reset Testing Cheat Sheet](#)  
[SSRF Cheat Sheet & Bypass Techniques](#)  
[Penetration Testing Tools Cheat Sheet](#)  
[LFI Cheat Sheet](#)  
[Vi Cheat Sheet](#)  
[Systemd Cheat Sheet](#)  
[nbtscan Cheat Sheet](#)  
[Linux Commands Cheat Sheet](#)  
[More »](#)

## WALKTHROUGHS

[InsomniHack CTF Teaser - Smartcat2 Writeup](#)  
[InsomniHack CTF Teaser - Smartcat1 Writeup](#)  
[FristiLeaks 1.3 Walkthrough](#)  
[SickOS 1.1 - Walkthrough](#)  
[The Wall Boot2Root Walkthrough](#)  
[More »](#)

## TECHNIQUES

[SSH & Meterpreter Pivoting Techniques](#)  
[More »](#)

## SECURITY HARDENING

[Security Harden CentOS 7](#)  
[More »](#)

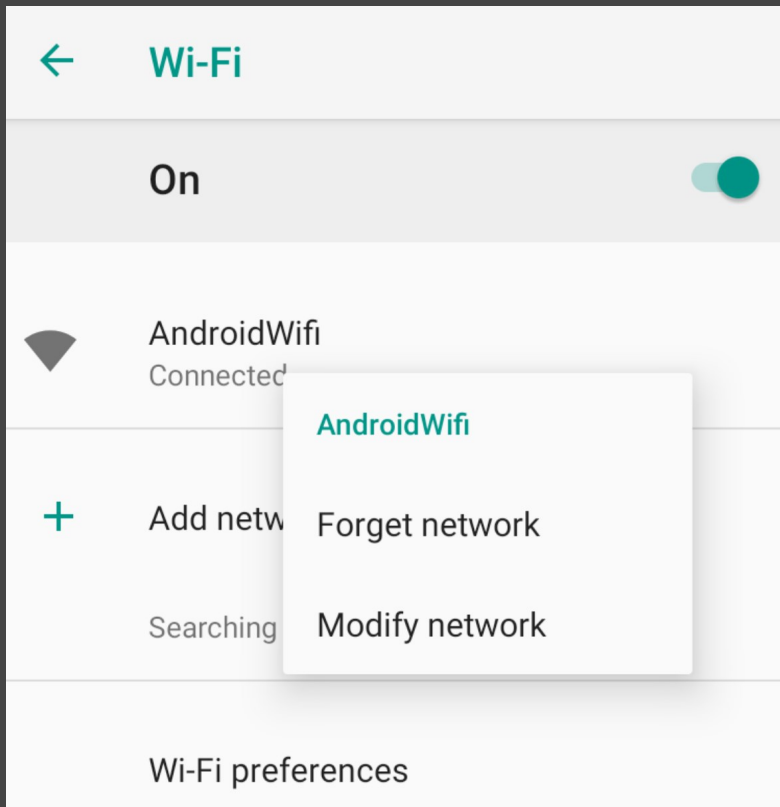
## /DEV/URANDOM

[MacBook - Post Install Config + Apps](#)

[Insecure Direct Object Reference \(IDOR\): Definition, Examples & How to Find](#)  
[Encrypted Notes App Solution \(iOS, Android, MacOS, Linux, Windows\)](#)  
[HowTo: Kali Linux Chromium Install for Web App Pen Testing](#)  
[Jenkins RCE via Unauthenticated API](#)  
[MacBook - Post Install Config + Apps](#)  
[enum4linux Cheat Sheet](#)  
[Linux Local Enumeration Script](#)  
[HowTo Install Quassel on Ubuntu](#)  
[HowTo Install KeepNote on OSX Mavericks](#)

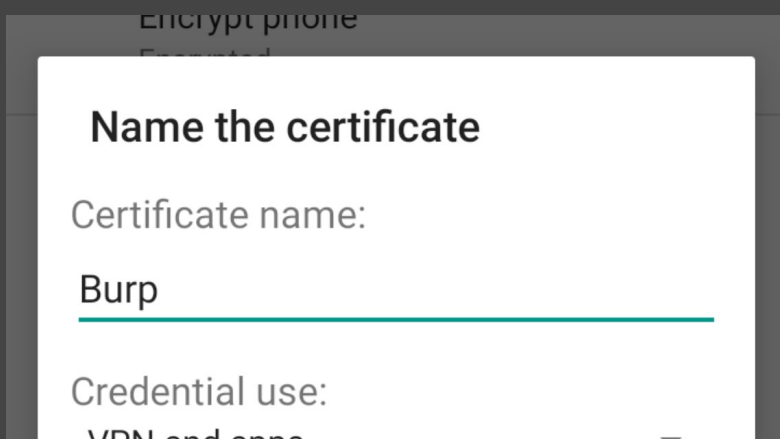
## 2. Android 8.1 Proxy Settings

1. Swipe down the top and select Settings
2. Tap Network & Internet > Wi-Fi > Long Tap on the connected Wi-Fi network and Select Modify Network
3. Tap Advanced > Proxy > Manual and enter the same Proxy settings you entered in step 1



## 3. Android Burp Certificate Installation

1. Go to your web browser and download the certificate file from <http://burp>
2. Rename it to .cer
3. Drag it into the running GenyMotion phone (this will place the file at /sd-card/)
4. On the phone go to Settings > Security & Location > Encryption & Location > Install from SD card (Install certificates from SD card)
5. Click Downloads on the left and select the .cer file
6. Install the certificate and call it Burp



The package contains:  
one CA certificate

CANCEL

OK

Install from SD card

Install certificates from SD card

1. You will need to set a pin code, set one

#### 4. Burp Proxy Settings

Add a Burp proxy on the interface with the IP and port used at step 1

#### 5. ADB

1. Install brew
2. `brew install android-platform-tools`
3. `adb devices`

```
List of devices attached
192.168.XX.XXX:5555 device
```

1. `adb shell`

```
vbox86p:/ # ls
```

Your id should be root on GenyMotion.

#### 6. Installing APK Files

There are two options for installing APK files, using adb or dragging and dropping.

Using ADB:

```
adb install file.apk
```

Or drag and drop the apk file into the running GenyMotion Android device.

#### 7. ADB Basic Commands

Installed Android application location:

```
cd /data/data
```

#### 8. Open GApps

If you are assessing an application from the Play Store then you can install open gapps in GenyMotion by clicking on the icon on the right hand menu.

Enjoy.

## Share this on...


 Twitter  Facebook  Google+  Reddit

# Follow Arr0way

 Twitter  GitHub

Also...

You might want to read these



CATEGORY	POST NAME
<code>cheat-sheet</code>	<a href="#">Reverse Shell Cheat Sheet: PHP, Python, Powershell, Bash, NC, JSP, Java, Perl</a>
<code>Web App Security</code>	<a href="#">Insecure Direct Object Reference (IDOR): Definition, Examples &amp; How to Find</a>
<code>cheat-sheet</code>	<a href="#">Nmap Cheat Sheet: Commands &amp; Examples (2022)</a>
<code>SecOps</code>	<a href="#">Encrypted Notes App Solution (iOS, Android, MacOS, Linux, Windows)</a>
<code>cheat-sheet</code>	<a href="#">DNS Tunneling dnscat2 Cheat Sheet</a>
<code>cheat-sheet</code>	<a href="#">SSH Lateral Movement Cheat Sheet</a>
<code>cheat-sheet</code>	<a href="#">Password Reset Testing Cheat Sheet</a>
<code>cheat-sheet</code>	<a href="#">SSRF Cheat Sheet &amp; Bypass Techniques</a>
<code>cheat-sheet</code>	<a href="#">Penetration Testing Tools Cheat Sheet</a>
<code>cheat-sheet</code>	<a href="#">LFI Cheat Sheet</a>