Pwn Pad User Manual

Note: The online version of this manual is maintained here:
http://pwnieexpress.com/pages/documentation

Table of Contents:

Introduction

Legal stuff

- All Pwnie Express / Rapid Focus Security products are for legally authorized uses only. By using this product you agree to the terms of the Rapid Focus Security EULA: (http://pwnieexpress.com/pdfs/RFSEULA.pdf)

- This product contains both open source and proprietary software: Proprietary software is distributed under the terms of the Rapid Focus Security EULA: (http://pwnieexpress.com/pdfs/RFSEULA.pdf). Open source software is distributed under one or more of the following licenses:

  - GNU PUBLIC LICENSE (HTTP://WWW.GNU.ORG/LICENSES/GPL.HTML).
  - BSD-3-CLAUSE LICENSE (HTTP://WWW.OPENSOURCE.ORG/LICENSES/BSD-3-CLAUSE):
  - OPENSSL TOOLKIT DUAL LICENSE (HTTP://WWW.OPENSSL.ORG/SOURCE/LICENSE.HTML)
  - APACHE LICENSE, VERSION 2.0 (HTTP://WWW.APACHE.ORG/LICENSES/LICENSE-2.0.HTML)

- As with any software application, any downloads/transfers of this software are subject to export controls under the U.S. Commerce Department's Export Administration Regulations (EAR). By using this software you certify your complete understanding of and compliance with these regulations.

Pwn Pad Features

Core Features

- Android OS 4.2 and Ubuntu 12.04
- Large screen, Powerful battery
- OSS-Based Pentester Toolkit
- Long Range Wireless Packet Injection

Included Accessories

- TP-Link High-gain 802.11b/g/n USB wireless adapter
- Sena High-gain USB Bluetooth adapter
- USB-Ethernet adapter
- USB OTG cable (for USB host-mode)

Wireless Tools

- Aircrack-ng
- Kismet
- Wifite-2
- Reaver
- MDK3
- EAPeak
- Asleap-2.2
- FreeRADIUS-WPE

- Hostapd
- Proxmark3 suite

Bluetooth Tools

- bluez-utils
- btscanner
- bluelog
- Ubertooth tools

Web Application Testing Tools

- Nikto
- Wa3f

Network Tools

- NET-SNMP
- Nmap
- Netcat
- Cryptcat
- Hping3
- Macchanger
- Tcpdump
- Tshark
- Ngrep
- Dsniff
- Ettercap-ng 7.5.3
- SSLstrip v9
- Hamster and Ferret
- Metasploit 4
- SET
- Easy-Creds v3.7.3
- John (JTR)
- Hydra
- Medusa 2.1.1
- Pyrit
- Scapy

Getting started

Things to be aware of

- **WARNING:** DO NOT UPGRADE THE ANDROID OS! Supported updates for the Pwn Pad will be provided by Pwnie Express (see http://pwnieexpress.com/pages/downloads for latest updates). Upgrading the Android OS directly is not supported and may affect wireless packet injection and external adapter capabilities.

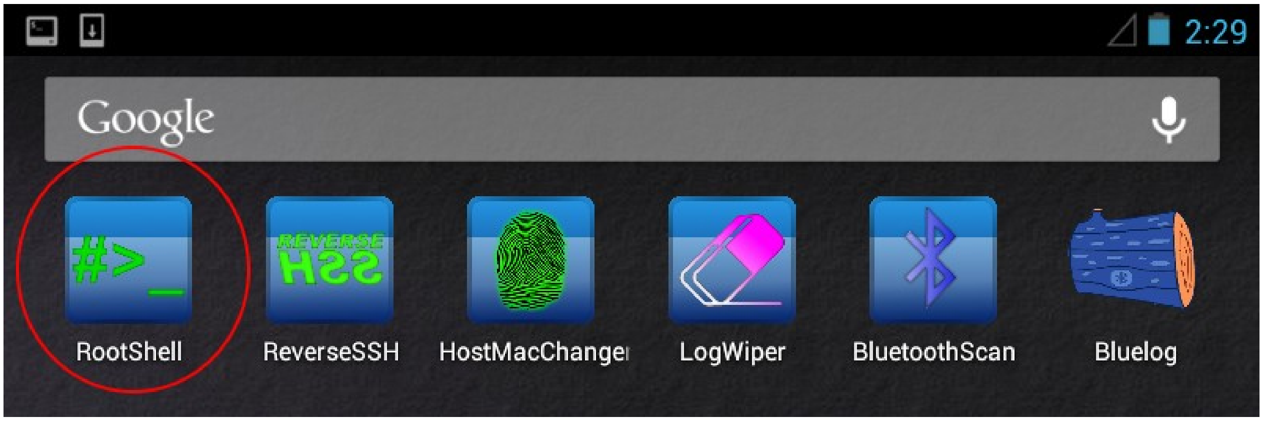
- Only one directly-attached external USB device is supported at a time. To attach multiple external USB adapters at once, an externally-powered USB hub is recommended, though a non-powered hub may support up to two devices at a time depending on power draw.
- The tablet's internal wireless and Bluetooth hardware does not support packet injection or monitor mode. The included external USB wireless/Bluetooth adapters are the only supported adapters offering packet injection and monitor mode at this time.
- Sometimes when the display goes into sleep mode it has trouble coming back on. Be aware the device may actually still be on and running, even if it doesn't instantly come back to life. Though this doesn't happen often, the display sleep timeout has been set to 30 minutes to avoid this until we have a fix. To turn screen off manually, press the power button once.
- There are two command terminals installed: "Android Terminal Emulator" and "Terminal IDE". All desktop apps currently use the Android Terminal Emulator (with this terminal, press the "Volume Down" button for the CTRL key).
- There are two SSH servers installed: the Android SSH server and openssh-server in the Ubuntu 12.04 chroot environment. The Ubuntu SSH server is set to listen on localhost only by default.
- In order for Android Terminal Emulator to have full root access, it must SSH into localhost (thus all current apps login to localhost before running any commands or pentest tools).
- You'll need to add a Google / Gmail account to access the Google Play store.

Powering up for the first time

1. Power on device by holding power button until Google logo appears.

   WARNING: DO NOT UPGRADE THE ANDROID OS IF PROMPTED!

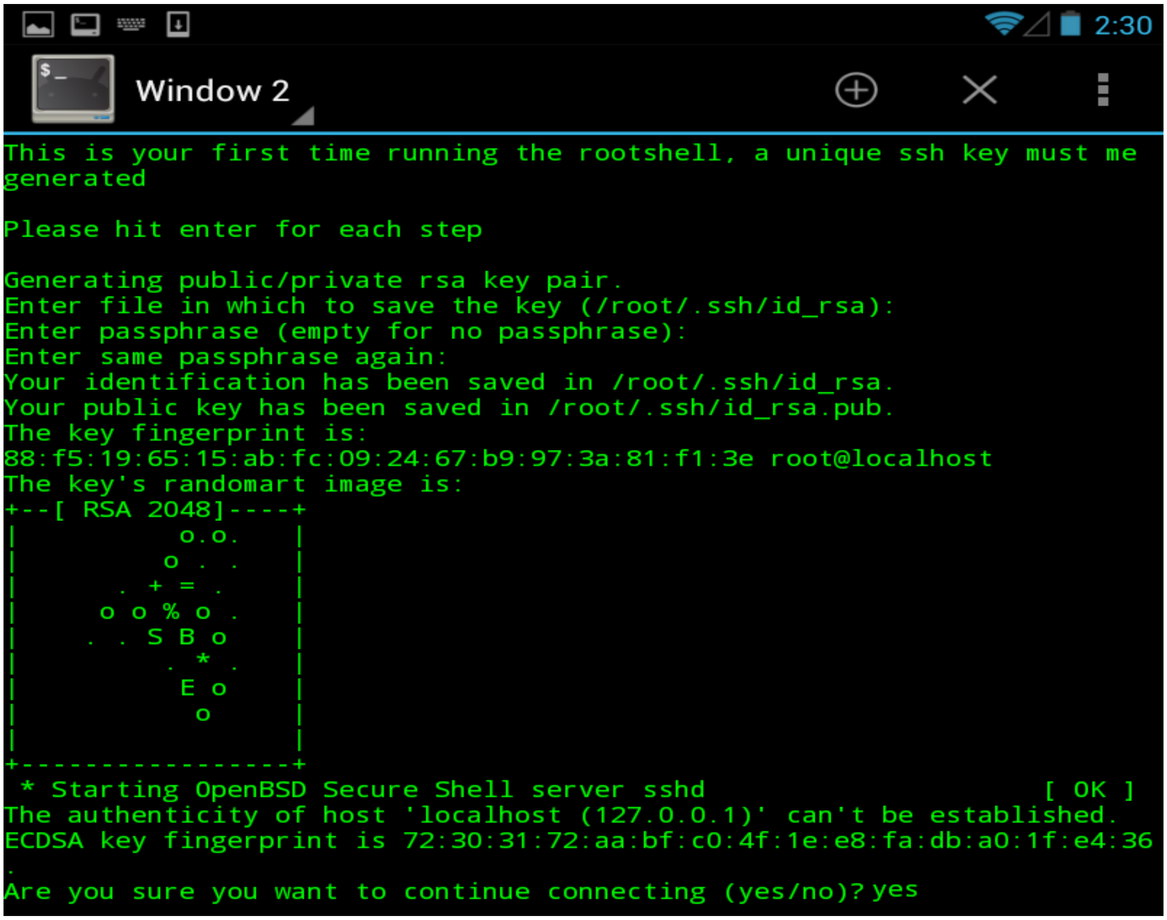
2. Once device is fully booted, open the "RootShell" app in the top left hand corner of the screen:



3. The first time the RootShell app is run it will generate a unique SSH key pair for the Ubuntu SSH server.
4. Press ENTER at each prompt to accept key generation defaults.

   NOTE: Setting a password for the SSH server private key is not recommended and will prevent the functionality of most Pwn Pad tools.

5. Type "yes" when prompted.



```
This is your first time running the rootshell, a unique ssh key must me
generated

Please hit enter for each step

Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
88:f5:19:65:15:ab:fc:09:24:67:b9:97:3a:81:f1:3e root@localhost
The key's randomart image is:
+--[ RSA 2048]----+
|          o.o.   |
|         o . .   |
|      . + = .    |
|     o o % o .   |
|    . . S B o    |
|         . * .   |
|          E o    |
|           o     |
|                 |
+-----------------+
 * Starting OpenBSD Secure Shell server sshd                     [ OK ]
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is 72:30:31:72:aa:bf:c0:4f:1e:e8:fa:db:a0:1f:e4:36
.
Are you sure you want to continue connecting (yes/no)? yes
```

The script will end by placing the user in /opt/pwnpad/. This is the main area where the Pwn Pad scripts, captures, logs and tools not found in /usr/bin reside.

NOTE: Most Pwn Pad apps automatically log to /opt/pwnpad/captures/

Basic navigation

All basic tablet navigation (outside of the command line) uses the front-end OS, Android Jellybean. Swiping, tapping, and tap and hold are all part of Android's intuitive navigation system that make using an Android device easy and natural.

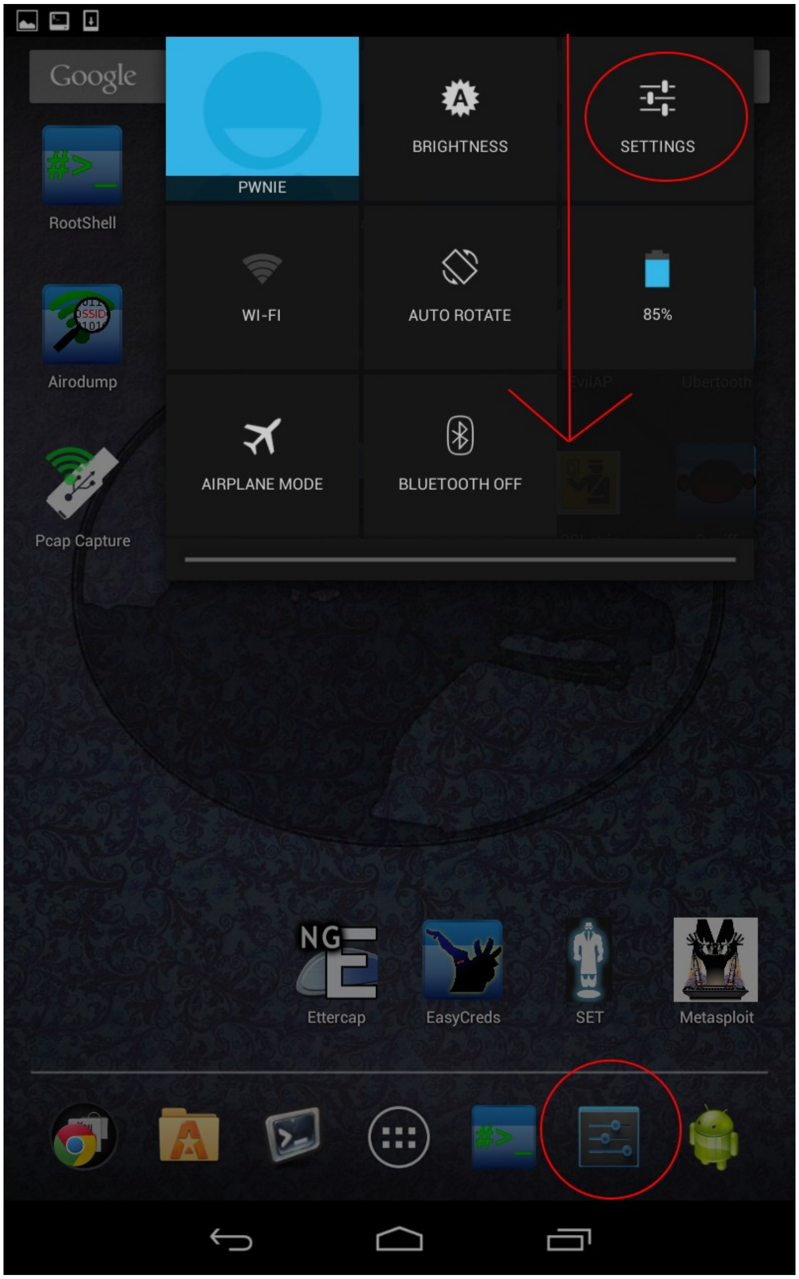
There are a few basic navigation steps that are essential to pentesting with the Pwn Pad. When opening multiple apps and spawning multiple terminal windows, simply swipe across the terminal window to switch to the next terminal window.

The best way to close an app is to tap the multi-view (double rectangle icon) in the bottom right hand corner. Then, from the listed window mode swipe the miniature window off the screen by swiping it to the right. To verify an app has really stopped running, use the app manager within 'Settings > Apps > Running', tap the 'Terminal Emulator', then tap 'Stop'. This will ensure the app has completely stopped. Below are a series of screenshots to illustrate this.

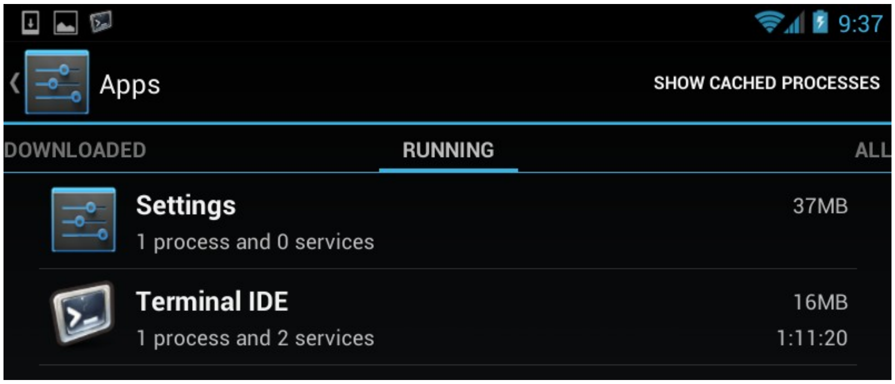
NOTE: This is how to properly end all pentesting apps on the Pwn Pad.

Typical open close scenario when running Pwn Pad apps on desktop: (Example: Closing RootShell)

Keep the app manager open in the background to easily kill tasks by switching to multiview. To open app manager go to ‘Settings > Apps > Running’ (access settings icon in the tray on the bottom right or you can swipe from the top right side of the screen down):



Next, go to ‘Apps’ then tap ‘RUNNING’ in the top right. These are the only apps that need to be running:



9:37

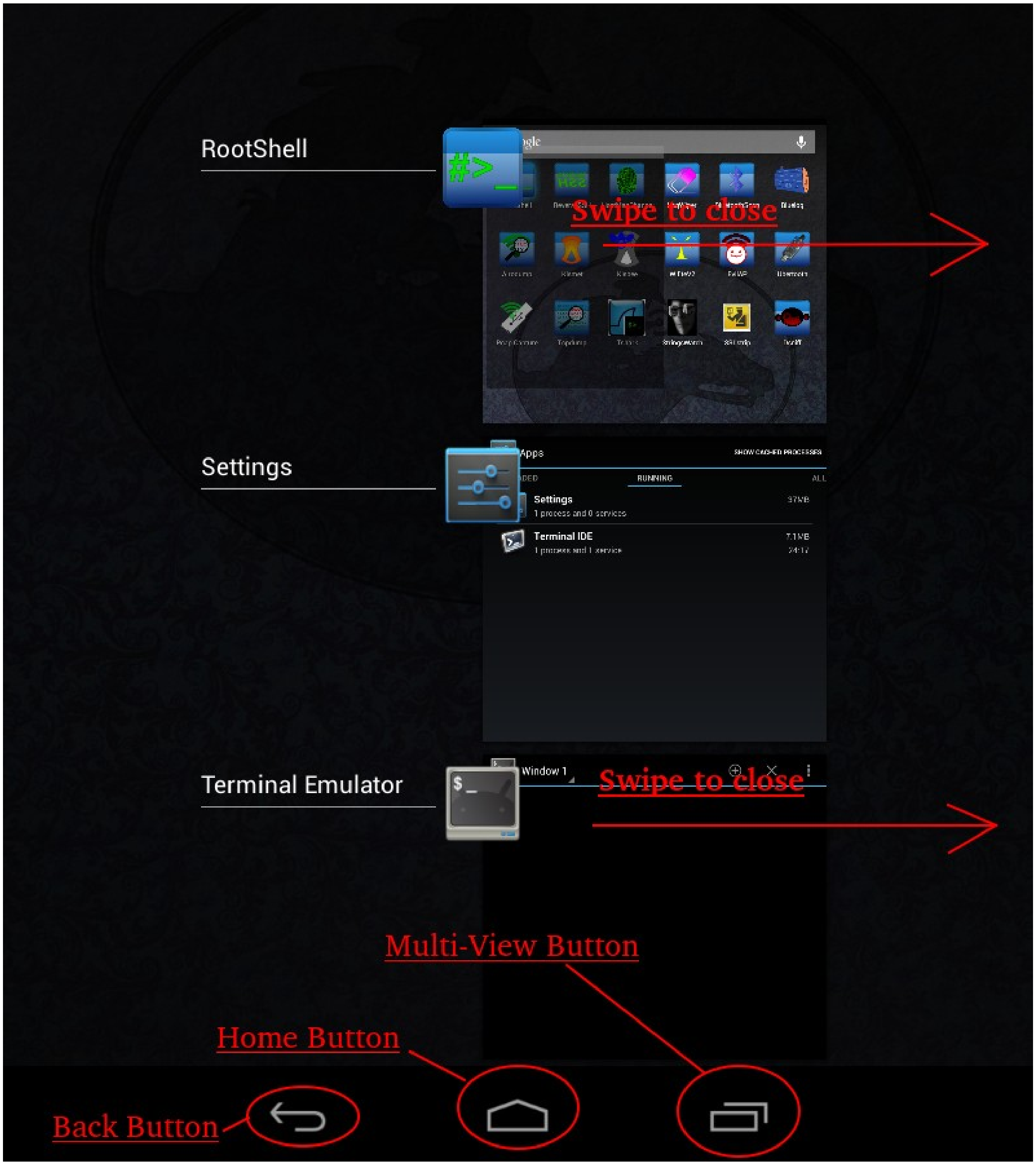
Apps

SHOW CACHED PROCESSES

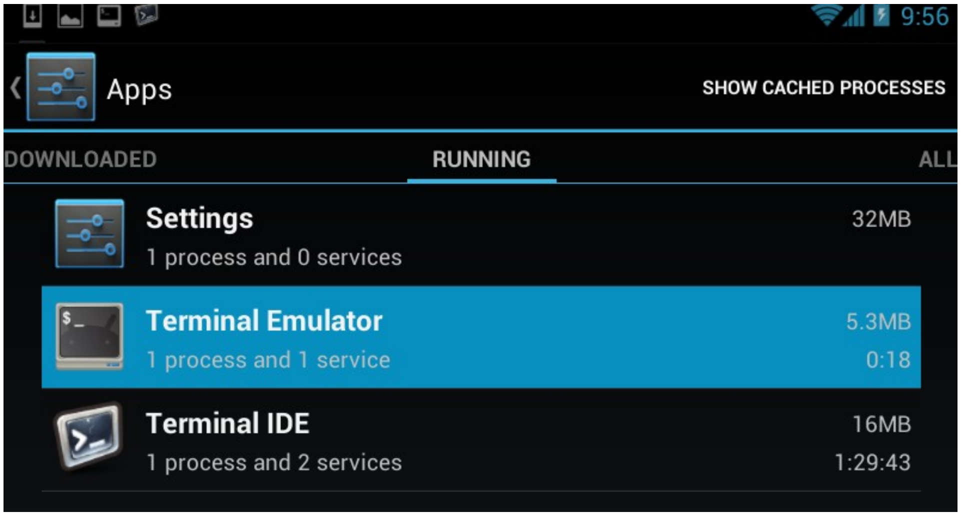
DOWNLOADED | RUNNING | ALL

Settings 1 process and 0 services	37MB
Terminal IDE 1 process and 2 services	16MB 1:11:20

Select the ‘Home’ button (the house icon located in the center of the screen at the very bottom) to get back to the Pwn Pad desktop. Now select ‘RootShell’. To close ‘RootShell’ tap the multi-view icon in the bottom right hand corner (double rectangle icon):



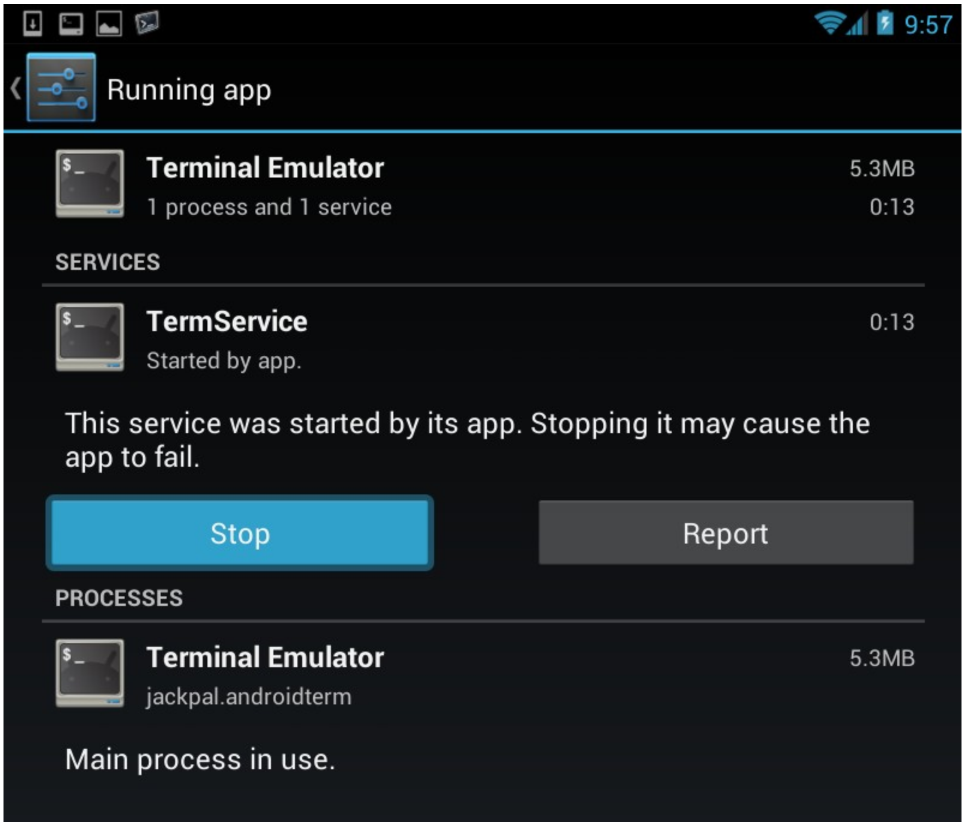
Every app will spawn both the app name and the Terminal Emulator. Swipe Terminal Emulator and the app name off the screen to close initially. Then tap the settings window showing ‘Running apps’ to kill the Terminal Emulator process completely:



Settings 32MB
1 process and 0 services

Terminal Emulator 5.3MB
1 process and 1 service 0:18

Terminal IDE 16MB
1 process and 2 services 1:29:43



Terminal Emulator 5.3MB
1 process and 1 service 0:13

TermService 0:13
Started by app.

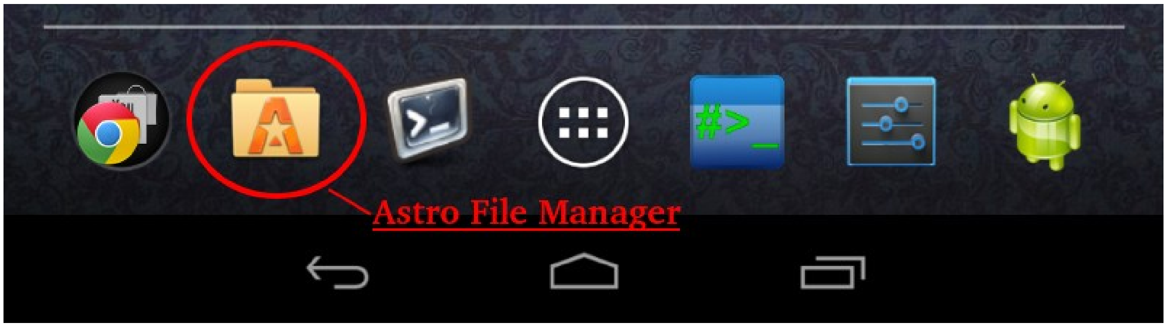
This service was started by its app. Stopping it may cause the app to fail.

Terminal Emulator 5.3MB
jackpal.androidterm

Main process in use.

Multi-view can also be very useful for switching between app (equivalent to ALT+TAB on a computer).

To file browse using the GUI, open the ‘Astro File Manager’ app (shortcut in the tray on the bottom):



Connecting USB devices

How to connect OTG cable and included accessories:

Any USB accessories included with the Pwn Pad can be connected to the device and attached via velcro to the back of the case. Each app that corresponds to the attached device will set up the device for you.

Included adapters will show up as the following in the Ubuntu chroot environment:

TP-Link Wireless - **wlan0**

Sena Bluetooth - **hci0**

USB-Ethernet - **eth0**

How to connect USB flash drives:

1. Connect a USB flash drive to the Pwn Pad via OTG cable.
2. Once connected, ‘ USB OTG Helper’ will appear, tap ‘OK’
3. Once ‘USB OTG Helper’ has loaded, select ‘MOUNT’
4. Once mounted, USB drive will show up under /storage/UsbOtgDrives/drive1/
5. Access from command line or ‘Astro File Manager’
6. To unmount safely open ‘USB OTG Helper’ and select ‘UNMOUNT’

NOTE: USB drives can be accessed through Astro File Manager by going to ‘My Files’ once properly mounted. The folder ‘UsbOtgDrive’ will appear in ‘Storage’ within Astro File Manager.

Recommended apps from Google Play

For added functionality, we recommend downloading these additional Android apps from the Google Play store. While these apps are free, they are released under third-party licensing (and thus we are not able to bundle them into the Pwn Pad image).

- Android SSH server
- Astro file manager
- USB OTG helper
- IPv4 subnet calculator

- Connect Cat

Command terminals & SSH

Android Terminal Emulator

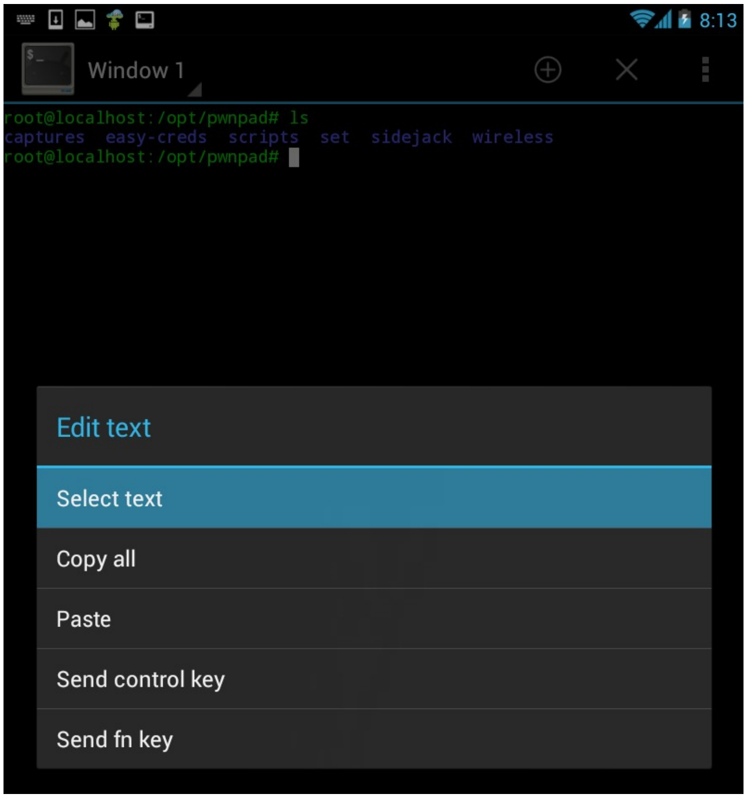
All Pwn Pad apps on the desktop run scripts by launching Android Terminal Emulator. As true root access isn’t available through this terminal, each script starts by SSHing into localhost to gain root access. If you open Terminal Emulator on it’s own, you must type the following to have true root access:

```
# su
root@android:/ # bootubuntu
root@localhost:/# ssh root@localhost
```

Now you will have full root access to run commands.

> **NOTE:** Volume Down button is the CTRL key for Terminal Emulator (use with all Pwn Pad apps). Example: For ‘CTRL+C’ press ‘Volume Down’ and ‘C’. The CTRL key on the onscreen keyboard only works with Terminal IDE.

To copy/paste simply tap and hold in the terminal window, tap ‘Select text’. To paste tap and hold and select ‘paste’



```
root@localhost:/opt/pwnpad# ls
captures  easy-creds  scripts  set  sidejack  wireless
root@localhost:/opt/pwnpad# 
```

NOTE: Selecting text works best when placing your finger directly below the text, so the tip of your finger is at the bottom of the text you are selecting.

Moving between terminal windows is as simple as swiping across the screen. Be sure to kill Terminal Emulator in the app manager when you close the terminal as described in the navigation section.

Terminal IDE

Terminal IDE gives you full root access, without having to ssh into itself. It is very nice with a lot of different options but unfortunately has a limited copy/paste ability. The only copy/paste options are to select all text and copy paste. Terminal IDE does however support pasting from selected copied text from Android Terminal Emulator.

Terminal window navigation is swipeable, and if you tap and hold on the screen it will let you select one of four windows. Only four open windows are possible, and also always open.

To gain root access on Android via Terminal IDE type the following:

```
terminal++@localhost: $ su
```

To gain root access to the Ubuntu chroot environment type:

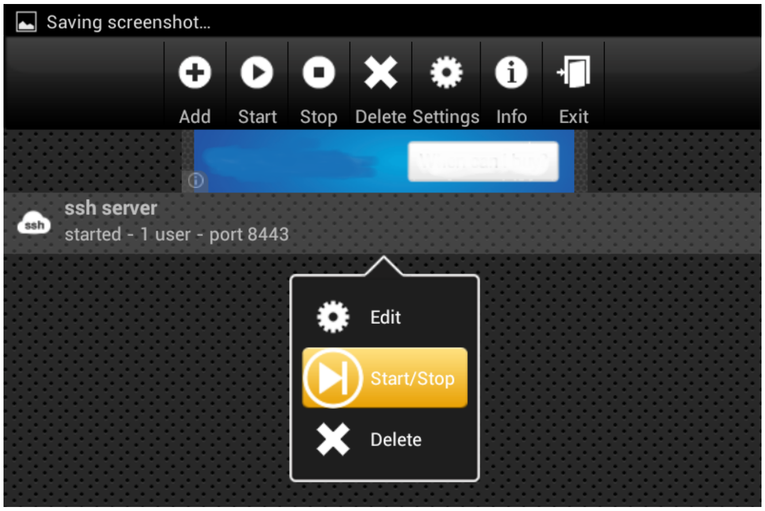
```
root@localhost:/data/data/com.spartacusrex.spartacuside/files # bootubuntu
```

Android SSH Server

The Android SSH Server installed can be useful for gaining access to the Android file system via SSH. Unfortunately it has some bugs on the Nexus 7; it may be incredibly slow for a local network connection and has issues when trying to exit from the command line. Below are the details of how best to utilize this app.

To start the Android SSH server: Tap the ‘SSH Server’ icon on the desktop to the left (access by swiping over - from right to left from the main screen)

Once the app is open tap the ‘ssh server’ listed and select ‘Start/Stop’. A little window will then pop up stating ‘The server has been started.’



Saving screenshot...

ssh server
started - 1 user - port 8443

NOTE: Once stopped there is a bug that doesn't let the SSH server properly start up again. To restart the SSH server simply kill the SSH Server app from the app manager. Once it has been killed you can open it again and start the server successfully. Even if you tap 'exit' the server will not successfully start again until it has been killed via app manager.

To access the Android file system via the Android SSH server use the following port and credentials:

From linux computer:

```
# ssh root@{ip address of Pwn Pad} -p 8443
```

Example: ssh root@192.168.1.100 -p 8443

Default username: **root**
Default password: **pwnplug8000**

To gain root access type:

```
# su
```

To gain access to the Ubuntu chroot with Pwn Pad tools type:

```
# bootubuntu
```

Ubuntu SSH server (OpenSSH)

By default OpenSSH-Server is installed within the Ubuntu chroot environment. In order to access it over the network you must edit the sshd_config file and the restart the SSH service:

From rootshell:

```
# nano /etc/ssh/sshd_config
```

Comment out the line that says 'ListenAddress 127.0.0.1' by adding a # in front of it.

```
#ListenAddress 127.0.0.1
```

Type 'CTRL O' then 'hit enter' then 'CTRL X' to save changes to the file.

To restart the SSH server type:

```
# /etc/init.d/ssh restart
```

To access the Ubuntu chroot file system via the Ubuntu SSH server use the following port and credentials:

From linux computer:

```
# ssh root@{ip address of Pwn Pad}
```

Example: ssh root@192.168.1.100

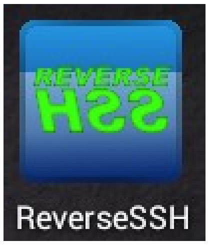
Default username: **root**
Default password: **pwnplug8000**

> **NOTE:** To access internal Android storage from the Ubuntu chroot side ‘cd /sdcard/’.

One-touch pentesting

RootShell: Provides root access via Android Terminal Emulator and places user in the /opt/pwnpad/ folder.

ReverseSSH: Allows user to create a reverse SSH shell connection to a SSH server on desired port.



HostMacChanger: Randomizes the hostname and MAC address of selected interface.

LogWiper: Securely wipes all captures, logs, tmp files, and or bash history if desired.

BluetoothScan: Scans for bluetooth devices using ‘hcitool -i hci0 scan --flush --class --info’ showing detailed bluetooth data about each devices found, including device type, class, and services available.

Logs to /opt/pwnpad/captures/bluetooth/ **NOTE:** Must have SENA UD100 bluetooth adapter attached to Pwn Pad

Bluelog: Bluetooth scanning tool which logs device name, MAC address, and class id. Logs to /opt/pwnpad/captures/bluetooth/ **NOTE:** Must have SENA UD100 bluetooth adapter attached to Pwn Pad

Airodump: Runs ‘airodump-ng wlan1’ to show current surrounding wireless in real time with clients connected and probe requests from clients. **NOTE:** Must have TPlink wireless adapter attached to Pwn Pad (Use ‘Volume Down’ button and ‘C’ key to close gracefully)

Kismet: Wireless packet sniffer for logging all wireless data seen. Ubertooth supported. Start sequence once TPlink adapter has been plugged in: Enter, Enter, Enter, Tab, Put keyboard down with down arrow in bottom left hand corner. **NOTE:** Must have TPlink wireless adapter attached to Pwn Pad (Hit ESC and use arrow keys to select ‘close’ to close gracefully)

Kisbee: Zigbee wireless packet capturing and mapping tool. (Android app) **NOTE:** Must have a Kisbee adapter (NOT INCLUDED) connected to Pwn Pad

WifiteV2: Automated wireless attack / auditing tool. Front end automation for Aircrack-NG suite. After attaching TPlink wireless adapter open WifiteV2 and select ‘3. wlan1’ to place into monitor mode. Hit ‘Volume Down Button C’ to select targets. **NOTE:** Must have TPlink wireless adapter attached to Pwn Pad (Use ‘Volume Down’ button and ‘C’ key to close gracefully)

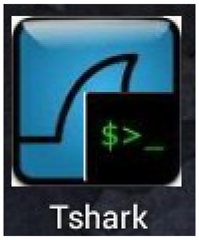
EvilAP: Aggressive wireless access point used to forcefully associate wireless clients in range with vulnerable preferred network list. **NOTE:** Must have TPlink wireless adapter attached to Pwn Pad (Use ‘Volume Down’ button and ‘C’ key to close gracefully)

Ubertooth: Bluetooth full packet sniffing using Ubertooth toolsuite. **NOTE:** Must have an Ubertooth adapter (NOT INCLUDED) connected to Pwn Pad

Pcap Capture: App to capture packets via attached usb adapter. (Android app) **NOTE:** Must have TPlink wireless adapter attached to Pwn Pad

Tcpdump: TCP Packet sniffer used to sniff network traffic on selected interface. Option to log to /opt/pwnpad/captures/tcpdump/ **NOTE:** must have corresponding adapter attached for selected interface

Tshark: Terminal version of Wireshark used for sniffing network traffic. Option to log to /opt/pwnpad/captures/tshark/ **NOTE:** must have corresponding adapter attached for selected interface



StringsWatch: Tshark cmd piped to Strings cmd to show human readable strings in clear text being sniffed on selected interface. Option to log to /opt/pwnpad/captures/stringswatch/. **NOTE:** must have corresponding adapter attached for selected interface

SSLstrip: Tool used to strip SSL connections and serve HTTP versions of requested URLS on selected interface. Logs to /opt/pwnpad/captures/sslstrip/ **NOTE:** must have corresponding adapter attached for selected interface

Dsniff: Used to watch for clear text username and passwords in transit on selected interface. (dsniff toolsuite installed, though app uses ettercap to provide dsniff functionality currently broken in the dsniff tool) Option to log to /opt/pwnpad/captures/sniffed$date.log. **NOTE:** must have corresponding adapter attached for selected interface

Ettercap-NG: MITM Toolsuite. App on desktop provides a quick menu to perform arp cache poisoning with known target IP addresses. Option to log to /opt/pwnpad/captures/ettercap/ **NOTE:** must have corresponding adapter attached for selected interface

EasyCreds: Menu driven MITM attack suite for automating the setup and configuration of several wireless and network level attacks. *FreeRadius-WPE attack fully functional* **NOTE:** FreeRadius attack is the primary function and use of this tool at this time, all other attacks have not been fully tested. Must have TPlink wireless adapter attached to Pwn Pad (Use ‘Volume Down’ button and ‘C’ key to close gracefully)

SET: Social Engineering Toolkit used for many MITM attacks combined with social engineering. Incredibly extensive toolkit.

Metasploit: Metasploit framework 4 latest up to date stable release. Exploitation framework.

Additional pentesting tools

All remaining command line tools not in the path can be found in **/opt/pwnpad/**

Pwn Pad Resources

Latest Pwn Pad user manual:
http://pwnieexpress.com/pages/documentation

Latest software updates:
http://pwnieexpress.com/pages/downloads

Technical support:
http://pwnieexpress.com/pages/support