Pwn Plug Academic Edition Update Guide

The following steps are for use with the Pwnie Express Pwn Plug Academic Edition or the Pwn Plug Elite.

Required materials for installation:

- *Pwn Plug Academic Edition or Pwn Plug Elite running Release 1.1 or newer*
- *Ethernet cable (included with Pwn Plug)*
- *Serial cable (included with Pwn Plug)*
- *Power cable (included with Pwn Plug)*
- *Internet connection*
- *Host machine with Screen installed*

Setup:

1. Attach the Pwn Plug Academic Edition or Pwn Plug Elite to the host machine using the serial cable and connect it to the network via Ethernet cable. A DHCP server must be accessible on the LAN to assign an IP address to the Pwn Plug.

2. Next, connect to the Pwn Plug Academic Edition or Pwn Plug Elite from the host machine via Screen. First, enter the following command as root *without executing*:

   ```
   screen /dev/ttyUSB0 115200
   ```

   Then, power on and attach to the Pwn Plug Academic Edition or Pwn Plug Elite from the host machine by plugging in the power cable and quickly executing the above command.

3. Now login using your username and password (username: *root*, password: *pwnplug8000* by default).

Installation:

1. First execute the following **command block**:

```
dhclient eth0; echo `ifconfig eth0 |grep HWaddr |awk '{print$5}' |awk -F":"
'{print$1$2$3$4$5$6}'` > /etc/hostname; /etc/init.d/hostname.sh; touch
/var/pwnplug/script_configs/sms_message_config.sh; echo -e "\n### BEGIN INIT
INFO\n# Provides: atheros-reset\n# Required-Start: \$remote_fs \$syslog\n#
Required-Stop: \$remote_fs \$syslog\n# Default-Start: 0 1 2 3 4 5 6\n#
Default-Stop: 0 1 6\n# Short-Description: Resets atheros device so it loads
properly at next boot\n### END INIT INFO\n\nifconfig wlan0 up && ifconfig
wlan0 down\n" > /etc/init.d/athreset; chmod +x /etc/init.d/athreset;
update-rc.d athreset defaults; sed -i 's/\/etc\/init.d\/ssh
stop/\/etc\/init.d\/ssh stop\nservice ifplugd stop/g'
/var/pwnplug/scripts/bypass_mode.sh
```

2. Now test for connectivity:

```
ping www.google.com
```

3. If connected, create a directory to download the update into using:
   Note: create this directory outside of the /root directory or it will be deleted before you are able to completely apply 1.1.3

```
mkdir <update_directory_here>
```

4. then:

```
cd <update_directory_here>
```

5. Download the update and patch to v1.1.2 by executing:

```
dhclient eth0; wget
https://updates.pwnieexpress.com/pwnplug/pwnplug-update.tar.xz
--no-check-certificate; tar xvf pwnplug-update.tar.xz; chmod +x
pwnplug_patch*; ./pwnplug_patch_1.1.2_INTERNAL_TFTP.sh
```

6. Then execute the following command block:

```
aptitude remove --purge ettercap ettercap-common w3af-console cryptcat sipsak
miredo yersinia smbclient sslsniff tcptraceroute pbnj netdiscover netmask
udptunnel dnstracer sslscan medusa ipcalc dnswalk socat onesixtyone tinyproxy
dmitry fcrackzip ssldump fping ike-scan gpsd darkstat swaks arping tcpreplay
sipcrack proxychains proxytunnel siege sqlmap wapiti skipfish w3af;
/var/pwnplug/scripts/Free_up_space_on_rootfs.sh; rm
/var/cache/apt/pkgcache.bin* /var/cache/apt/srcpkgcache.bin*; rm -rf
/usr/share/w3af
```

7. Then patch to v1.1.3 by executing:

```
apt-get update; PWNIE_POWER=true; chmod +x pwnplug_patch_1.1.3.sh;
./pwnplug_patch_1.1.3.sh
```

8. Confirm the update completed successfully using:

```
cat /etc/motd
```