MiniPwner Instructions:

Your new MiniPwner comes setup and ready-to-use out of the box. By default, your new MiniPwner is configured in AP mode. It has DHCP configured on the physical Ethernet port and it will automatically create a wireless network named ACEHACKWARE (unsecured) when powered on. To get started, connect to the wireless network (or plug in the Ethernet port and determine the IP address assigned by your DHCP server) then login via SSH with the following credentials.

Default SSID: **ACEHACKWARE**
login: **root**
passwd: **acehackware**

Packages pre-installed include:
- Nmap network scanner
- Tcpdump sniffer
- Netcat Hacker's swiss army knife
- aircrack Wireless network analysis
- kismet Wireless network analysis
- perl Perl Scripting Language
- openvpn VPN Client and Server
- dsniff suite of sniffing and spoofing tools, including arpspoof
- nbtscan NetBIOS Network Scanner
- snort Sniffer, Packet Logger, Intrusion Detection System
- ***karma*** Wireless Sniffing Tool - not working yet....
- samba2-client Windows File Sharing Client
- elinks Text Based Web Browser
- yafc FTP Client
- openssh-sftp-client Secure File Transfer Client

To change the name of the wireless network (defaults to ACEHACKWARE) edit:
`/etc/config/wireless`

To install new packages, use ‘opkg’:

```
opkg update                              # updates the list of available packages
opkg -dest usb install packagename # will install ‘packagename’ to USB
```

If you have problems with installed packages not being able to find their libraries, modules, or other resources, you may need to create symlinks, as follows:

```
ln -s /mnt/usb/usr/share/nmap /usr/share/nmap   # nmap example
```

For more ways to use the MiniPwner, visit the ACE Hackware blog at:
http://acehackware.com/blog/

and the MiniPwner forums at:
http://minipwner.com/index.php/forum/index