SSTIC 2004, 2-4 juin, Rennes

Rump session : HoneyWRT

Cédric Blancher <sid@rstack.org>
French Honeynet Projet
Rstack Team

Proof of concept project :

- Use of embedded devices for honeynets

Why ?

- Cheap (~100/200€) and small devices
- Quick firmware upgrades
- Multi-purpose application

Should be profitable to solve some honeynets deployment issues :

- Expensiveness
- Time consuming (system install and so on)
- Space consuming ;)

Is possible because :

- Many network devices are Free Software (e.g. Linux) based systems (Buffalo, Linksys, NetGear, Fujitsu-Siemens, etc.)
- Thanks to some developers (e.g. Netfilter Core Team), GPL sources are available for download

Testbed device : wireless router Linksys WRT54G

- Profitable software
  - **Linux based**
  - **Almost complete GPL'ed source pack available**
  - **Build environment available**

- Profitable hardware
  - **MIPSEL architecture (cf. handhelds)**
  - **4Mo flash / 16Mo RAM (8/32 for GS) + NVRAM**
  - **VLAN aware ethernet switch ADM 6996 chip**
  - **Full featured proprietary WiFi 54g support**
  - **Some hardware enhancement (minipci wifi for v1.0, serial ports for V2.0+)**

Live RAM Distro

- BatBox
  - **http://www.batbox.org/wrt54g-linux.html**

Custom firmware enhancing Linksys build

- Wifi-Box
  - **http://wifi-box.sourceforge.net/**
- Sveasoft
  - **http://www.jsperkins.com/sveasoft/**

Mini distro with minimal firmware and ipkg support

- OpenWRT
  - **http://openwrt.ksilebo.net/**

- HoneyWRT will be OpenWRT based
  - **Minimal firmware with enhanced network capabilities**
  - **iPKG stuff aimed to specific honeynet needs**

- Project goals
  - **Provide purpose specific firmwares**
  - **Provide purpose specific packages**
  - **Provide all-in-one embedded toast'n'coffee machine with dish washing capabilities**

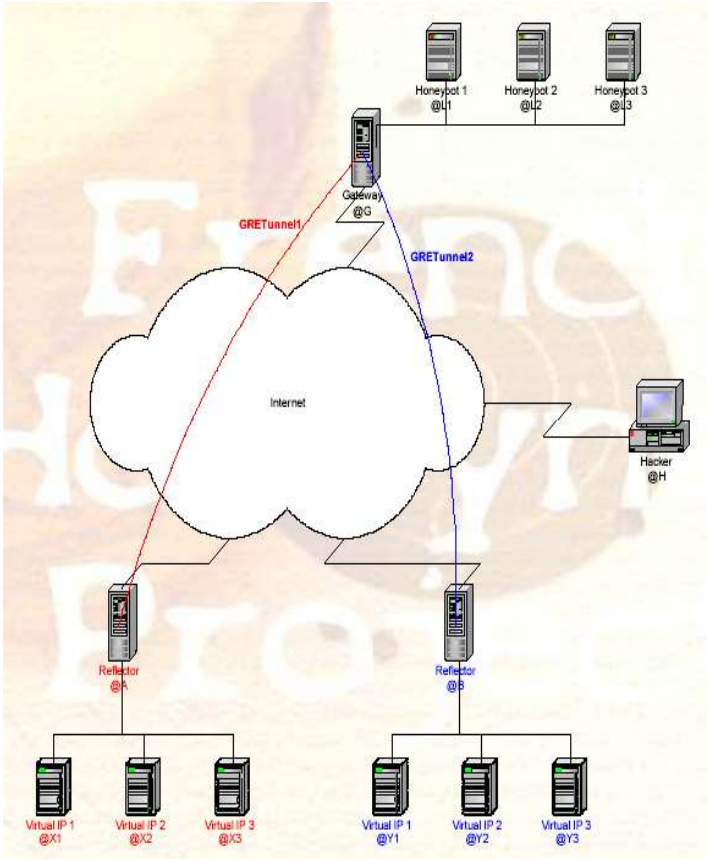
Main planned purposes

- Network flow monitoring (wired and wifi)
  - **Sniffer : tcpdump, Kismet drone**
  - **IDS : Snort**
  - **Traffic extraction and analysis : nProbe/nTop**
- Network containment
  - **Advanced firewalling : Netfilter + PoM**
  - **IPS : SnortInline**
- Traffic redirection
  - **Honeyd + GRE**
  - **IP tunnel based traffic redirectors**

Application example :

- Honeypots farm deployement
  - http://www.netexit.com/~sid/pres/0403_Eurosec_HoneypotsFarms.pdf

- Traffic redirectors
- Traffic dispatchers
- Containment



Future plans ?

- WRT54G honeypot (WTF ?)
- HoneyClusters ?
- What ever you can achieve with a small Linux based system
- Explore other devices (“donnez des sioux, pleins”)

Conclusion

- Pros
  - **Initial works seem promising**
  - **May be useful for people**
  - **Is definitely fun**
- Cons
  - **Heavy load handling**

Greetings

- rstack.org
  - http://www.rstack.org/

- French Honeynet Project
  - http://www.frenchhoneynet.org/