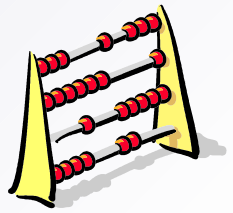
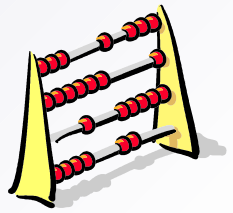
DenyHosts and IPBlock

Robert Spotswood



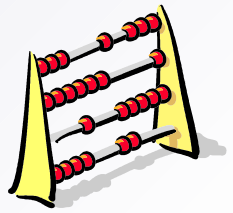
DenyHosts -> SSH

- What is SSH?
- SSH authentication methods
  - Password
  - Public Key
- Brute Force Attacks



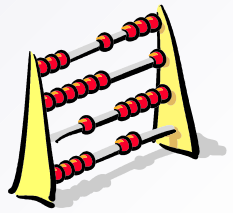
DenyHosts

- What is DenyHosts?
- Requirements
  - SSH with TCP wrappers support
  - Python 2.3 or higher
    - Bug: File "/usr/bin/denyhosts.py", line 5, in <module>
      import DenyHosts.python_version
      ImportError: No module named DenyHost-s.python_version



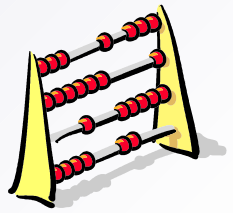
DenyHosts

- Edit the /etc/init.d/denyhosts and change PYTHON_BIN = "/usr/bin/python" to PYTHON_BIN = "/usr/bin/python2.4" (or what-ever your python version is)



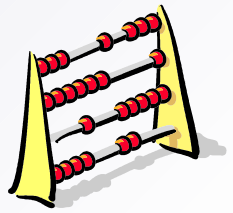
DenyHosts Login Types

- Invalid users
- Valid users
- Root
- Restricted users



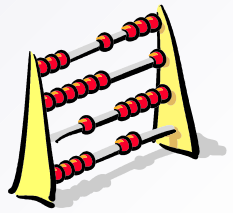
DenyHosts Resets

- Resets of login counts
  - Reset for valid users
  - Reset on success



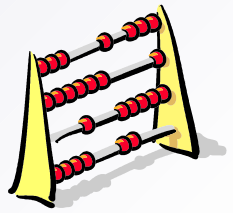
DenyHosts Blocking

- SSH only
- All TCP wrappers
- Run a script
- Whitelisting available



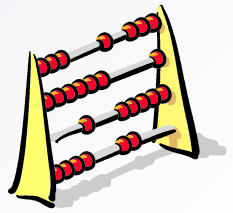
DenyHosts Unblocking

- Automatic
  - Can be limited
- Manual



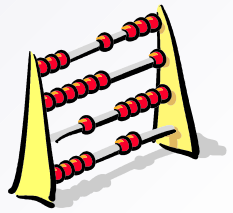
DenyHosts Options

- Default Config file: /usr/share/denyhosts/denyhosts.cfg
- Lots of option not covered, including email alerts.



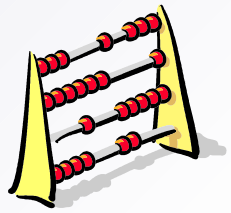
IPBlock

- What is it?
  - Homepage of IPList is http://iplist.sourceforge.net/
- Why use it?



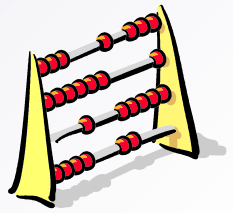
IPBlock – Block Lists

- 35 lists included, updated regularly
- Make your own lists
- Can whitelist ports and IP's
- My lists
  - DShield
  - Ad trackers
  - Spyware
  - DShield



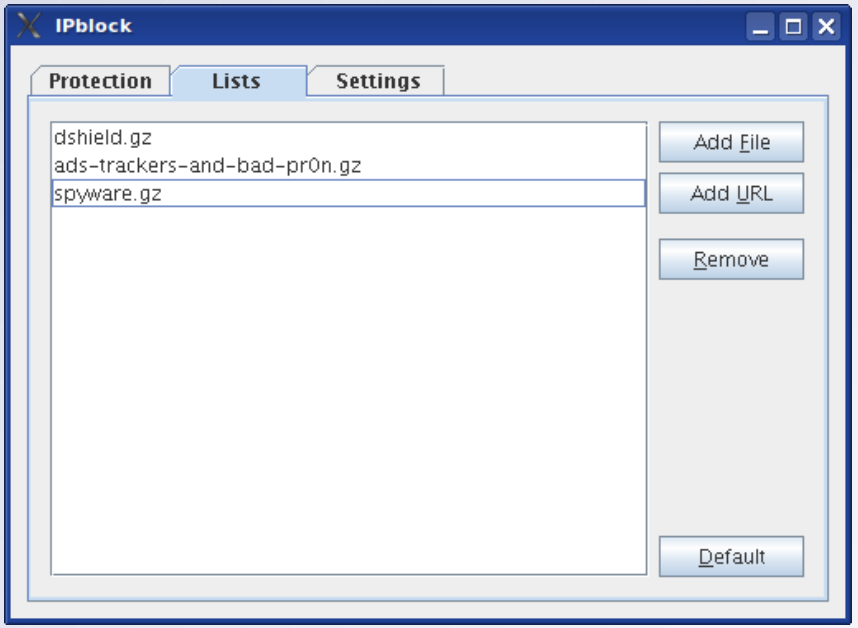
IPBlock Usage

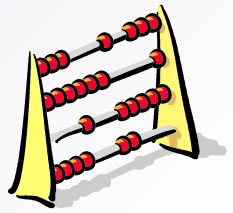
- Requires Sun JRE 1.5 or higher
- Does not stop blocking when you close.
- If IPBlock won't start, for Ubuntu run the following command:
  - sudo update-alternatives --config java
- Must start after other firewalls.



IPBlock – List Tab

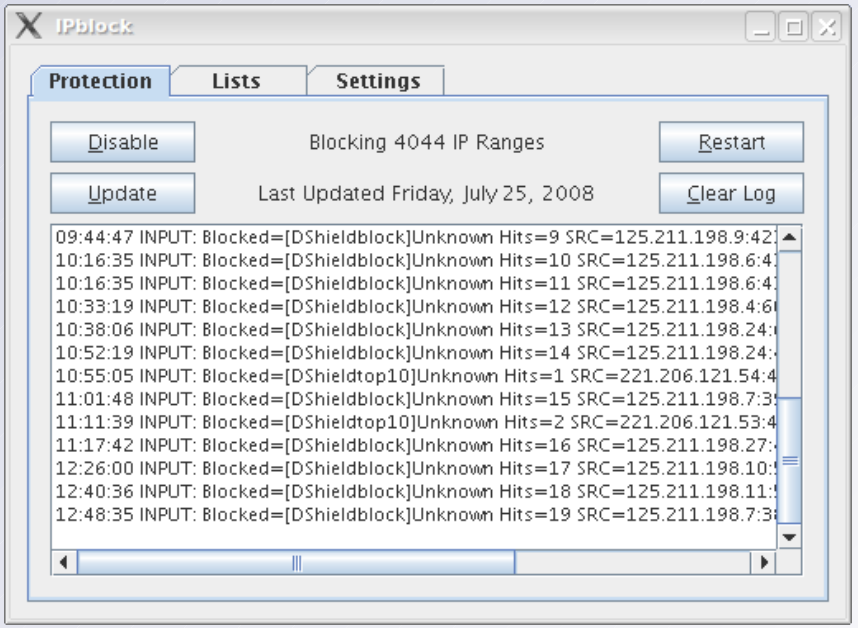
- Use Add Url!
- Only use Add File if you maintain your own lists.

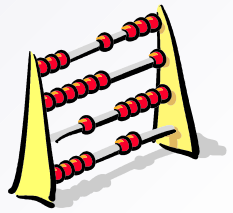




IPBlock – Protection Tab

- Must disable and enable to use changed lists.





IPBlock – Settings Tab

- Most important settings
  - Autostart
  - Auto-update