# tool

NANOG 29

Danny McPherson & Aaron Klink
danny@arbor.net

# About tool…

- Free!
- Developed by Aaron Klink & Danny McPherson many, many moons ago.
- Written in PERL, includes modules that enable interaction with various platforms and tools that employ those modules.
- Multi-vendor support:
  - Cisco IOS & catOS
  - Juniper
  - Foundry
  - Other…

# Motivation

- Needed simple tool (hence the name) to perform lots of different router-oriented functions
  - config audit
  - mass configuration tasks
  - basic monitor stuff with “self-defined” triggers
  - others as they arise
- Wasn’t aware of rancid at the time

# tool functions..

- basic CLI interaction
- configDiff
- cpuMon
- uptimeMon
- massConfig

# Basic CLI Interaction

- Accomplishes several tasks, including downloading and uploading of configs and execution of commands on single or multiple routers of various types.

```
danny@rambler% ./tool
usage:  tool -co command
or      tool -d config_repo [-ar]
or      tool -f tftp_filename [-s tftp_server]
or      tool -p local_filename

All variations take the following options:
  -a router_list or -r cisco_router or -j juniper_router or -cat
   cisco_switch
  -c class
  -o output_file (starttime appended) or -of output_file
```

# hostlist defines router list

```
danny@rambler% more Example.hostlist
10.0.0.1|br1.tcb.net|cisco|7500|ios|rr-client
10.0.0.2|br2.tcb.net|cisco|6509|catos|rr-client
10.0.0.3|ar1.tcb.net|juniper|M-160|junos|rr-server
```

# configDiff & configHash

- configDiff downloads configs based on a hostlist (and pattern, if desired), calls configHash to get the differences between the new config and the latest in the archive, and emails the results out.

# Sample configDiff

```
To: config-diffs@tcb.net
From: configDiff@tooth.tcb.net
Subject: Config Diffs
-------
131 - access-list 3 permit 10.0.1.9

131 + access-list 3 permit 10.0.1.8

abc-core-01
  + ! NVRAM config last updated at 09:12:31 UTC Sun Jul 11 1999 by danny
  - ! NVRAM config last updated at 09:12:30 UTC Sat Jul 10 1999 by danny
  + ! Last configuration change at 09:12:30 UTC Sun Jul 11 1999 by danny
  - ! Last configuration change at 09:12:29 UTC Sat Jul 10 1999 by danny
  - interface POS0/3  isis metric 29 level-2
  + interface POS0/3  isis metric 37 level-2
  - interface POS1/3  isis metric 22 level-2
  + interface POS1/3  isis metric 28 level-2 2

xyz-edge-02
  + ! NVRAM config last updated at 12:51:17 UTC Tue Nov 23 1999C by danny
  - ! NVRAM config last updated at 12:53:09 UTC Mon Nov 22 1999C by danny
  + ! Last configuration change at 23:31:41 UTC Mon Nov 22 1999C by danny
  - ! Last configuration change at 12:53:08 UTC Mon Nov 22 1999C by danny
 + interface Serial6/0/0/23:0  ip route-cache distributed
  + interface Serial6/0/0/23:0  no cdp enable
  + interface Serial6/0/0/23:0  no ip route-cache optimum
  + interface Serial6/0/0/23:0
```

# cpuMon

- Polls routers (specified in a hostlist) for 5 min CPU util averages. If util exceeds the specified threshold, sends mail out with further debug information pulled from the device.

# uptimeMon

- Polls routers (specified in a hostlist) for current uptime. If the device has rebooted since the last time the code ran, sends mail out with further debug information pulled from the device.

# massConfig

- Uses a config file and hostlist to update configs on a number of routers

```
danny@rambler% ./massConfig
usage: ./massConfig command_file hostlist [-c class]
   [debug]
```

# Comments & Where To Get It…

- Sourceforge: http://tool.sourceforge.net

- Send comments to tool@aklink.cx

www.CISecurity.org

THE CENTER FOR INTERNET SECURITY℠

*presents*

snmp-server community pub

# rat

# Router Audit Tool

## Version 2.0

# About RAT

- Free!
- RAT downloads configurations of devices to be audited (optionally), and then checks them against the settings defined in the benchmark.
- Just released “Gold Standard” (SANS/CIS marketing term) benchmark for IOS
- Currently working on PIX & Juniper rulesets
- See URL in previous slide for more information.

Thanks!