Securing Small Registries
(Handy Hints)

Nigel Roberts
nigel@roberts.gg

About.Me/Nigel.Roberts

@nigelrbrts
Two or three handy hints!
Story

• Once upon a time,
  – there was a story of Little Red Riding Hood, who is a small registry operator;
  – her grandma
  – …. and a Big Bad Wolf

• (OK .. I made up the bit about the grandmother)
“I know my place . . .”
1: Monitoring/SMS Alerting
2: Streaming/Hot Standby
3: Rule based fortifications
IP Sets

$ apt-get install ipset

- Framework inside the kernel (since 2.4)
- IP addresses, port sequences or IP/MAC address pairs
- in a way which ensures lightning fast match speed
Custom Security Perimeter

- TRUSTED - certain IP addresses have no restrictions
- REGISTRARS - can see ports 443 and port 700 only
- BUT to anyone else ....

registry system simply appears not to exist

-A INPUT -m set --match-set trusted src -j ACCEPT
-A INPUT -p tcp -m set --match-set registrar src -m tcp --dport 443 -j ACCEPT
-A INPUT -p tcp -m set --match-set registrar src -m tcp --dport 700 -j ACCEPT
Other advantages

- Allows management of the authorised IP blocks (which can be single IP addresses OR CIDR blocks) separately from the firewall rules.
- IPTABLES rules can dynamically create IP sets – so this allows us to place different resource restrictions e.g. on WHOIS, DAC and WHOIS2, and
- automatically drop abusive WHOIS queries at the network level which is much more efficient than at application level.
Example WHOIS rules

-A INPUT -p tcp -m tcp --dport 43 -j ACCEPT
-A INPUT -p tcp -m set --match-set whois2 src -m tcp --dport 1043 -j ACCEPT

-A INPUT -p tcp -m set --match-set dac src -m tcp --dport 2043 -j ACCEPT

-A INPUT -i eth0 -p tcp -m tcp --dport 43 -m state --state NEW -m recent --update --seconds 120 --hitcount 12 --name pilgrims --mask 255.255.255.255 --rsource -j LOG --log-prefix "port43_block:" --log-level 6

-A INPUT -i eth0 -p tcp -m tcp --dport 43 -m state --state NEW -m recent --update --seconds 120 --hitcount 12 --name pilgrims --mask 255.255.255.255 --rsource -j DROP

-A INPUT -i eth0 -p tcp -m tcp --dport 43 -m state --state NEW -m recent --set --name pilgrims --mask 255.255.255.255 --rsource
Concluding

• . . . the story of the big bad wolf.

• The woodcutter built a big fence. So the wolf went away to figure out another way in . . .

• Leaving Little Red Riding Hood never to forget . . .
He'll be back!
Nigel Roberts
nigel@roberts.gg
About.Me/Nigel.Roberts
@nigelrbrts