Securing Small Registries
(Handy Hints)

Nigel Roberts
nigel@roberts.gg

About.Me/Nigel.Roberts

@nigelrbrts

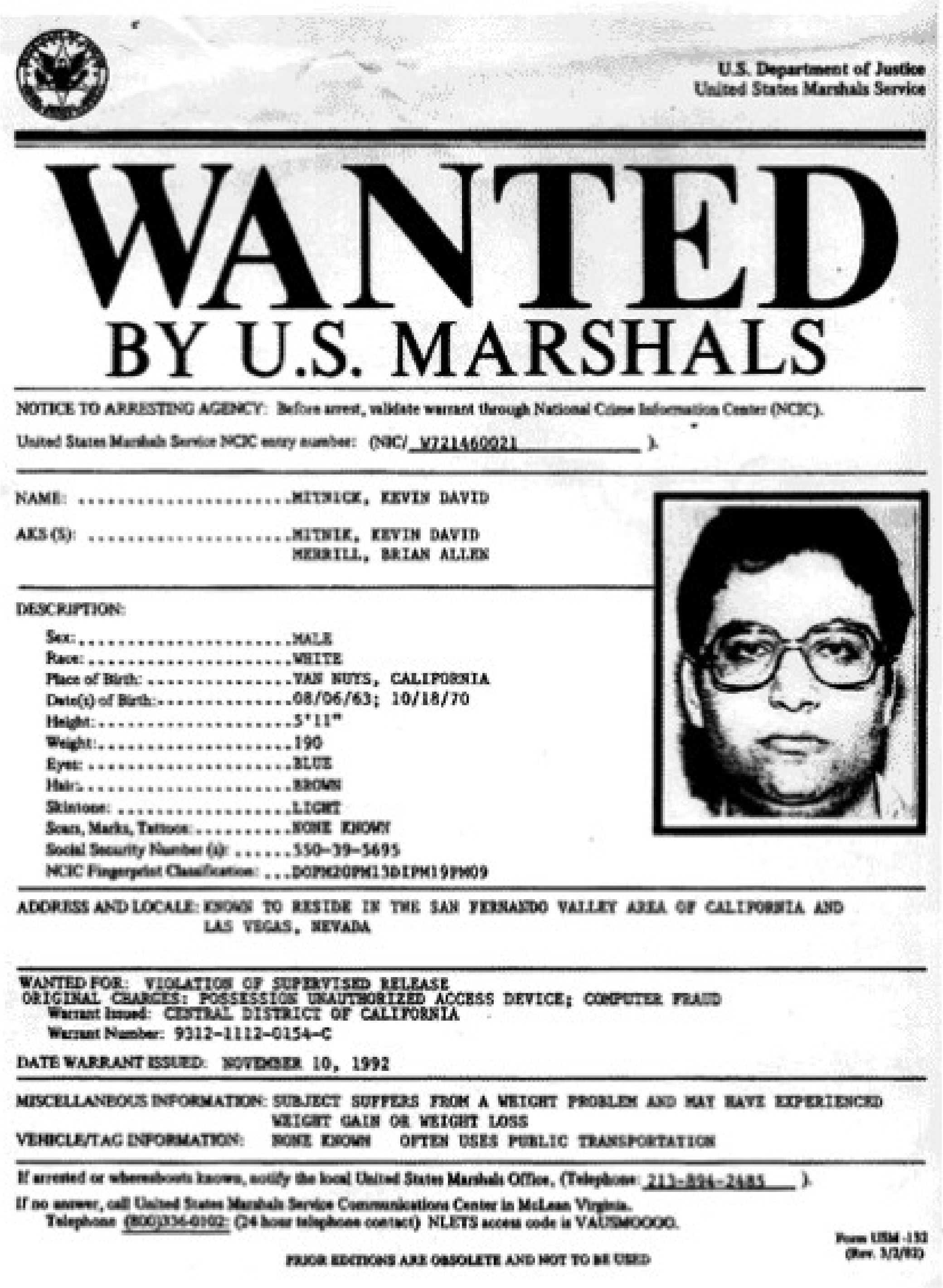
Two or three handy hints!

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 . . .”



U.S. Department of Justice
United States Marshals Service

WANTED
BY U.S. MARSHALS

NOTICE TO ARRESTING AGENCY: Before arrest, validate warrant through National Crime Information Center (NCIC).

United States Marshals Service NCIC entry number: (NIC/ W721460021).

NAME: ....MITNICK, KEVIN DAVID

AKS (S): ....MITNIK, KEVIN DAVID
MERRILL, BRIAN ALLEN

DESCRIPTION:

Sex: ....MALE
Race: ....WHITE
Place of Birth: ....VAN NUYS, CALIFORNIA
Date(s) of Birth: 08/06/63; 10/18/70
Height: ....5'11"
Weight: 190
Eyes: ....BLUE
Hair: ....BROWN
Skintone: ....LIGHT
Scars, Marks, Tattoos: ....NONE KNOWN
Social Security Number (s): 550-39-5695
NCIC Fingerprint Classification: ...DOPM20PM13DIPM19PM09

ADDRESS AND LOCALE: KNOWN TO RESIDE IN THE SAN FERNANDO VALLEY AREA OF CALIFORNIA AND LAS VEGAS, NEVADA

WANTED FOR: VIOLATION OF SUPERVISED RELEASE
ORIGINAL CHARGES: POSSESSION UNAUTHORIZED ACCESS DEVICE; COMPUTER FRAUD
Warrant Issued: CENTRAL DISTRICT OF CALIFORNIA
Warrant Number: 9312-1112-0154-C

DATE WARRANT ISSUED: NOVEMBER 10, 1992

MISCELLANEOUS INFORMATION: SUBJECT SUFFERS FROM A WEIGHT PROBLEM AND MAY HAVE EXPERIENCED WEIGHT GAIN OR WEIGHT LOSS

VEHICLE/TAG INFORMATION: NONE KNOWN OFTEN USES PUBLIC TRANSPORTATION

If arrested or whereabouts known, notify the local United States Marshals Office, (Telephone: 213-894-2485).

If no answer, call United States Marshals Service Communications Center in McLean Virginia.
Telephone (800)336-0102: (24 hour telephone contact) NLETS access code is VAUSMOOOO.

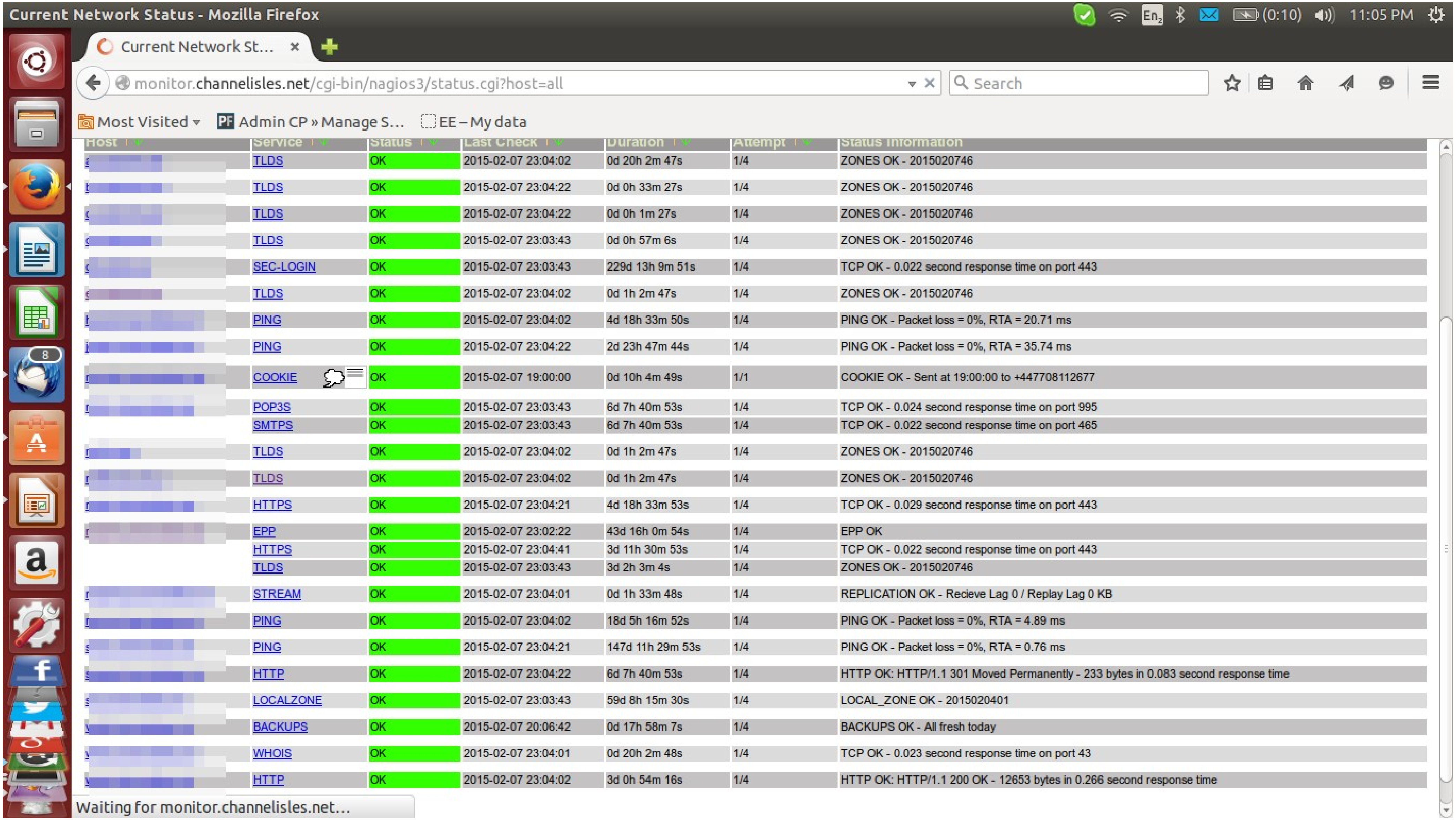
Form USM-132
(Rev. 3/2/92)

PRIOR EDITIONS ARE OBSOLETE AND NOT TO BE USED

November 1992

IWDRM

1: Monitoring/SMS Alerting

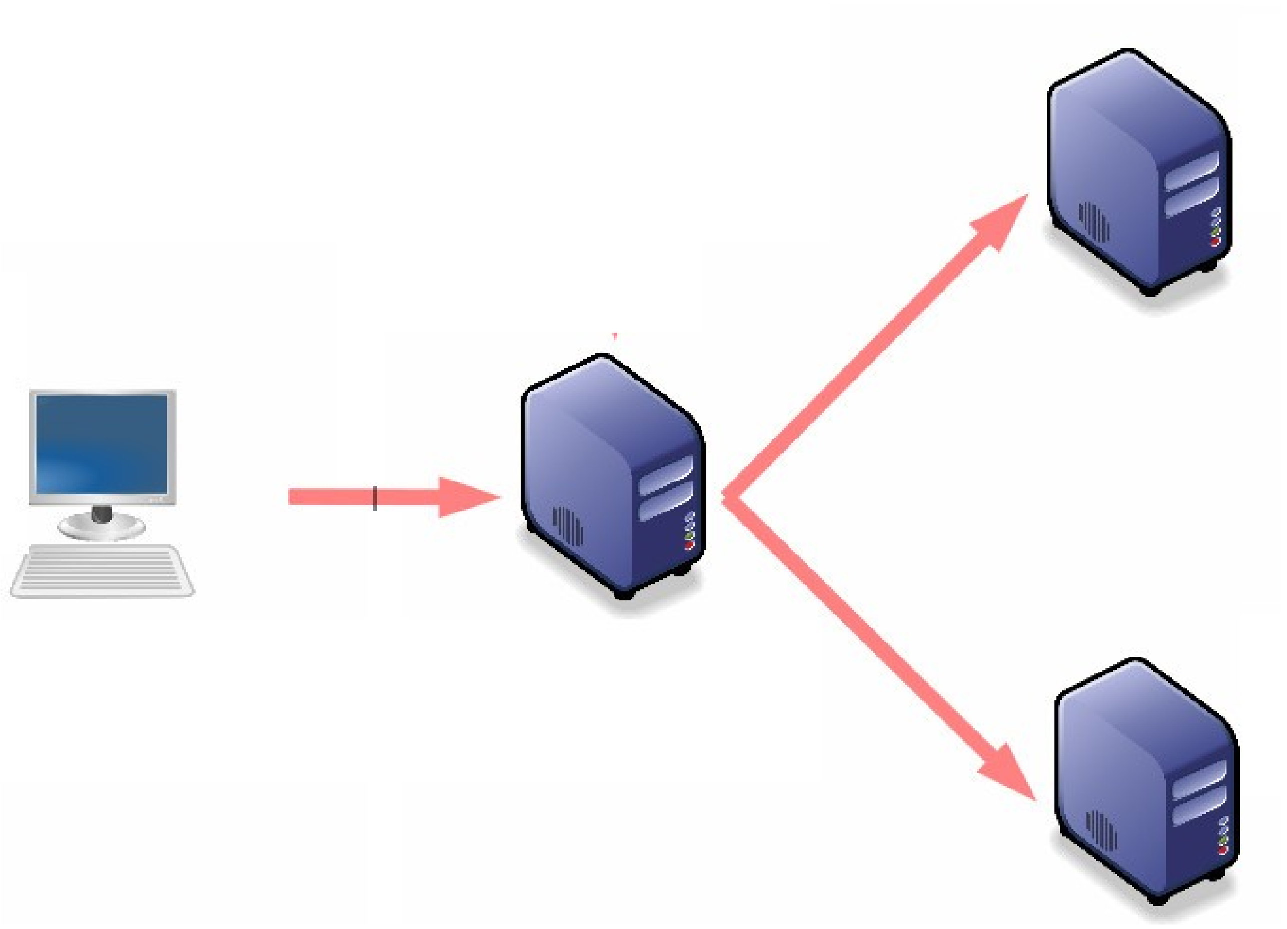


monitor.channelisles.net/cgi-bin/nagios3/status.cgi?host=all

Host	Service	Status	Last Check	Duration	Attempt	Status Information
[redacted]	TLDS	OK	2015-02-07 23:04:02	0d 20h 2m 47s	1/4	ZONES OK - 2015020746
[redacted]	TLDS	OK	2015-02-07 23:04:22	0d 0h 33m 27s	1/4	ZONES OK - 2015020746
[redacted]	TLDS	OK	2015-02-07 23:04:22	0d 0h 1m 27s	1/4	ZONES OK - 2015020746
[redacted]	TLDS	OK	2015-02-07 23:03:43	0d 0h 57m 6s	1/4	ZONES OK - 2015020746
[redacted]	SEC-LOGIN	OK	2015-02-07 23:03:43	229d 13h 9m 51s	1/4	TCP OK - 0.022 second response time on port 443
[redacted]	TLDS	OK	2015-02-07 23:04:02	0d 1h 2m 47s	1/4	ZONES OK - 2015020746
[redacted]	PING	OK	2015-02-07 23:04:02	4d 18h 33m 50s	1/4	PING OK - Packet loss = 0%, RTA = 20.71 ms
[redacted]	PING	OK	2015-02-07 23:04:22	2d 23h 47m 44s	1/4	PING OK - Packet loss = 0%, RTA = 35.74 ms
[redacted]	COOKIE	OK	2015-02-07 19:00:00	0d 10h 4m 49s	1/1	COOKIE OK - Sent at 19:00:00 to +447708112677
[redacted]	POP3S	OK	2015-02-07 23:03:43	6d 7h 40m 53s	1/4	TCP OK - 0.024 second response time on port 995
	SMTPS	OK	2015-02-07 23:03:43	6d 7h 40m 53s	1/4	TCP OK - 0.022 second response time on port 465
[redacted]	TLDS	OK	2015-02-07 23:04:02	0d 1h 2m 47s	1/4	ZONES OK - 2015020746
[redacted]	TLDS	OK	2015-02-07 23:04:02	0d 1h 2m 47s	1/4	ZONES OK - 2015020746
[redacted]	HTTPS	OK	2015-02-07 23:04:21	4d 18h 33m 53s	1/4	TCP OK - 0.029 second response time on port 443
[redacted]	EPP	OK	2015-02-07 23:02:22	43d 16h 0m 54s	1/4	EPP OK
	HTTPS	OK	2015-02-07 23:04:41	3d 11h 30m 53s	1/4	TCP OK - 0.022 second response time on port 443
	TLDS	OK	2015-02-07 23:03:43	3d 2h 3m 4s	1/4	ZONES OK - 2015020746
[redacted]	STREAM	OK	2015-02-07 23:04:01	0d 1h 33m 48s	1/4	REPLICATION OK - Recieve Lag 0 / Replay Lag 0 KB
[redacted]	PING	OK	2015-02-07 23:04:02	18d 5h 16m 52s	1/4	PING OK - Packet loss = 0%, RTA = 4.89 ms
[redacted]	PING	OK	2015-02-07 23:04:21	147d 11h 29m 53s	1/4	PING OK - Packet loss = 0%, RTA = 0.76 ms
[redacted]	HTTP	OK	2015-02-07 23:04:22	6d 7h 40m 53s	1/4	HTTP OK: HTTP/1.1 301 Moved Permanently - 233 bytes in 0.083 second response time
[redacted]	LOCALZONE	OK	2015-02-07 23:03:43	59d 8h 15m 30s	1/4	LOCAL_ZONE OK - 2015020401
[redacted]	BACKUPS	OK	2015-02-07 20:06:42	0d 17h 58m 7s	1/4	BACKUPS OK - All fresh today
[redacted]	WHOIS	OK	2015-02-07 23:04:01	0d 20h 2m 48s	1/4	TCP OK - 0.023 second response time on port 43
[redacted]	HTTP	OK	2015-02-07 23:04:02	3d 0h 54m 16s	1/4	HTTP OK: HTTP/1.1 200 OK - 12653 bytes in 0.266 second response time

Waiting for monitor.channelisles.net...

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