Security Assessment and Troubleshooting with SI6 IPv6 Toolkit v2.0

Fernando Gont

IPv6 Hackers #2
Prague, Czech Republic. July 21, 2015

About...

- Security Researcher and Consultant at SI6 Networks
- Published:
  - 20 IETF RFCs (9 on IPv6)
  - 10+ active IETF Internet-Drafts
- Author of the SI6 Networks' IPv6 toolkit
  - http://www.si6networks.com/tools/ipv6toolkit
- Admin of the IPv6 Hackers mailing-list
  - ipv6hackers@lists.si6networks.com
- More information at: http://www.gont.com.ar

Introduction

SI6 Networks' IPv6 Toolkit: Intro

- Brief history:
  - Produced as part of a project funded by UK CPNI on IPv6 security
  - Maintenance and extension taken over by SI6 Networks
- Goals:
  - Security analysis and trouble-shooting of IPv6 networks and implementations
  - Clean, portable, and secure code
  - Good documentation

SI6 Networks' IPv6 Toolkit: Intro (II)

- Supported OSes:
  - Linux, FreeBSD, NetBSD, OpenBSD, Mac OS, and OpenSolaris
- License:
  - GPL (free software)
- Home:
  - http://www.si6networks.com/tools/ipv6toolkit
- Collaborative development:
  - https://www.github.com/fgont/ipv6toolkit.git

SI6 Networks' IPv6 Toolkit: Philosophy

IDEAS TOOLS IPv6 NETWORK

"*an interface between your brain and your IPv6 network*"

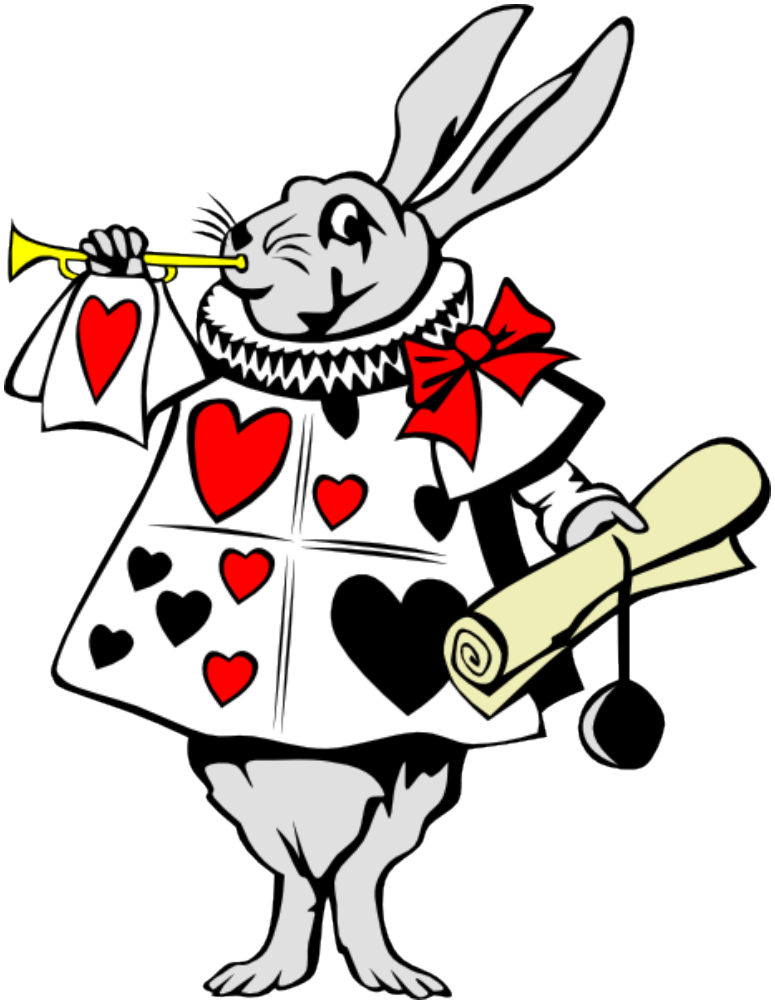
Some find this is NOT a useful approach, though! ☺

SI6 Networks' IPv6 toolkit: Tools

- addr6: An IPv6 address analysis tool
- scan6: An IPv6 address scanner
- path6: A versatile IPv6-based traceroute
- frag6: Play with IPv6 fragments
- tcp6: Play with IPv6-based TCP segments
- udp6: Play with UDP datagrams
- ns6: Play with Neighbor Solicitation messages
- na6: Play with Neighbor Advertisement messages
- script6: Rather complex tasks made easy

SI6 Networks' IPv6 toolkit: Tools (II)

- rs6: Play with Router Solicitation messages
- ra6: Play with Router Advertisement messages
- rd6: Play with Redirect messages
- icmp6: Play with ICMPv6 error messages
- ni6: Play with Node Information messages
- flow6: Play with the IPv6 Flow Label
- jumbo6: Play with IPv6 Jumbograms



IPv6 Toolkit v2.0!

SI6 NETWORKS

What's new in SI6 IPv6 v2.0 (Guille)

- Lots of bug fixes!
- An additional supported platform
  - OpenSolaris
- New tools:
  - **`script6`**
  - **`blackhole6`**
  - **`path6`**
  - **`udp6`**
- New features:
  - **`tcp6`**'s --close-mode, --data, etc.
  - **`scan6`**'s automatic smart scanning

Address Scanning

Address Scanning

- scan6 is **the most comprehensive IPv6 address scanner**
- It now supports heuristic address scanning:
  - It automatically detects address patterns
  - Then automatically targets such address patterns
- Employing heuristic scanning:

```
scan6 -d DOMAIN/64

scan6 -d IPV6ADDR/64
```

Address Scanning

```
File  Edit  View  Search  Terminal  Help
root@fgont-outside:~# scan6 -v -d scanme.nmap.org/64
Rate-limiting probe packets to 1000 pps (override with the '-r' option if neces
sary)
Target address ranges (1)
2600:3c01:0:0:0:0:0-100:0-1500

Alive nodes:
2600:3c01::2
2600:3c01::3
2600:3c01::a
2600:3c01::4b
2600:3c01::2:1002
2600:3c01::2:1003
2600:3c01::2:1001
2600:3c01::21:1000
```

IPv6-base TCP/UDP port scanning

- scan6 incorporates all known TCP and UDP port-scanning techniques
- Specifying a protocol and port range:

  `--port-scan {tcp,udp}:port_low[-port_hi]`
- Specifying a TCP scan type:

  `--tcp-scan-type {syn,fin,null,xmas,ack}`
- Example:

  `--port-scan tcp:1-1024 --tcp-scan-type syn`

IPv6-base TCP/UDP port scanning

```
File  Edit  View  Search  Terminal  Help
fgont@satellite:~$ sudo scan6 -d freebsd-host-remote --port-scan tcp:1-1024 -
-tcp-scan-type syn
SI6 Networks' IPv6 Toolkit v2.0 (Guille)
scan6: An advanced IPv6 scanning tool

Rate-limiting probe packets to 1000 pps (override with the '-r' option if nec
essary)
PORT      STATE     SERVICE
22/tcp    open      ssh
fgont@satellite:~$
```

Playing with TCP Packets

tcp6: Introduction

- Tool originally developed out of “frustration”
  - There was not even an IPv6-based SYN flooder
- But continued as a kind of nice *deja vu*
  - My early work on protocols involved TCP
  - IPv4-based TCP attack tools were/are rather rudimentary

tcp6: Connection flooding attacks

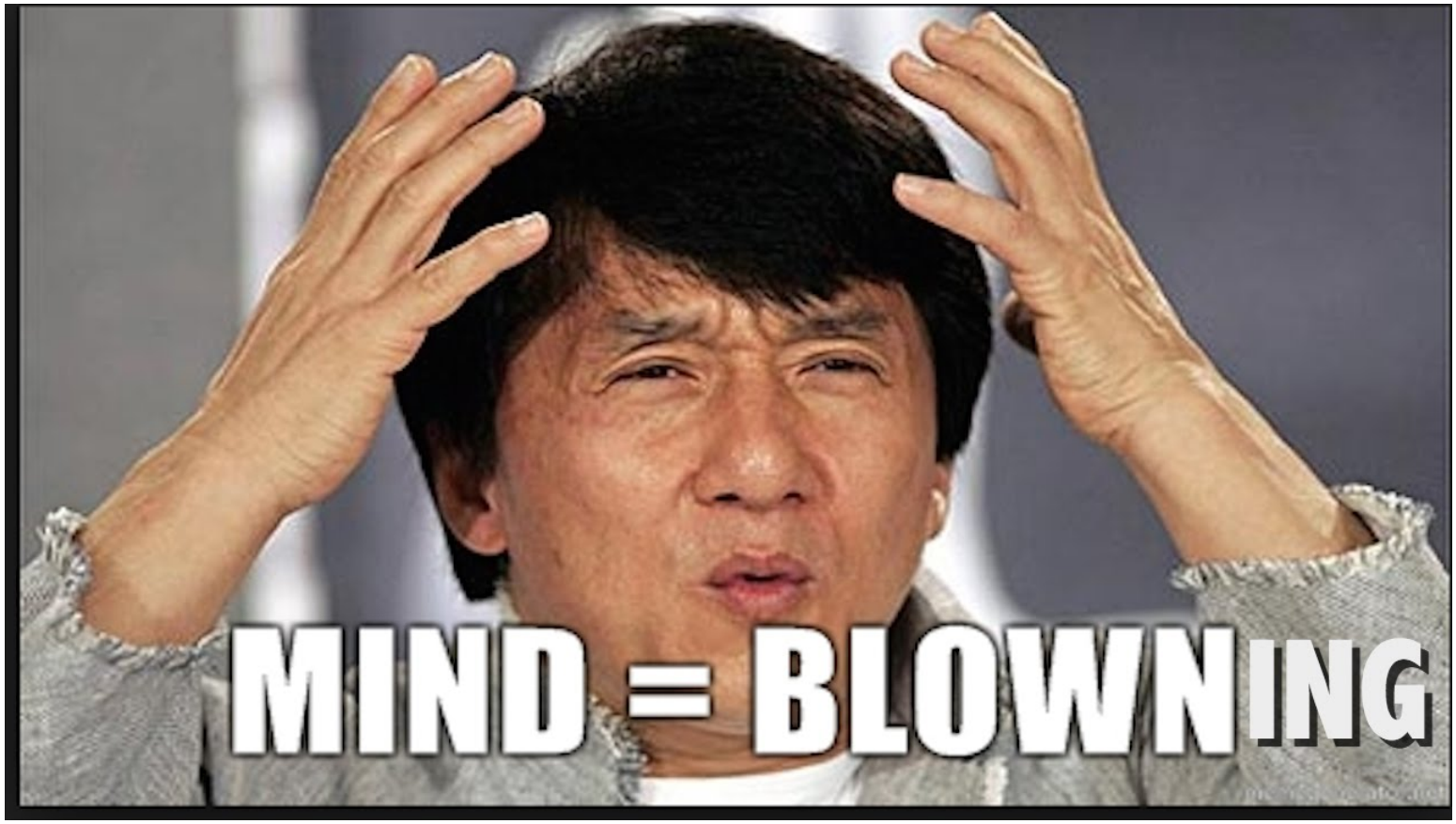
- SYN-floods:

```
tcp6 -i IFACE -s SRCPRF -d TARGET -a DSTPORT -X
S -F 100 -l -z 1 -v
```

- Connection floods:

```
tcp6  -i  IFACE  -s SRCPRF -d TARGET -a DSTPORT
-L -l --flood-sources 10 -z 1 --tcp-flags auto
-v
```

More about TCP-based attacks?



http://www.gont.com.ar/papers/tn-03-09-security-assessment-TCP.pdf

Playing with UDP datagrams

udp6: Play with UDP datagrams

- Can send arbitrary IPv6-based UDP datagrams
  - Use EHs
  - Flood a specific endpoint with datagrams from different sources and ports
  - Supports customized filters
  - Supports a **`--data`** option to embed a payload
- New in SI6 Networks IPv6 toolkit v2.0 (Guille)

Get interesting addresses

Get domains and IPv6 addresses

- **`script6`** can do batch-processing of domain names
- Available commands:
  - **`get-aaaa`**
  - **`get-mx`**
  - **`get-ns`**

Get domains and IPv6 addresses (II)

- Get mailserver domains:

```
$ cat domains.txt | script6 get-mx
```

- Get IPv6 addresses:

```
$ cat domains.txt | script6 get-aaaa
```

- Get mailserver addresses:

```
$ cat domains.txt | script6 get-mx | script6 get-aaaa
```

Get domains and IPv6 addresses (II)

```
File  Edit  View  Search  Terminal  Help
fgont@satellite:~$ cat sites.txt
www.si6networks.com
scanme.nmap.org
www.facebook.com
fgont@satellite:~$ cat sites.txt | script6 get-aaaa
# www.si6networks.com (www.si6networks.com.)
2a00:8240:6:a::1
# scanme.nmap.org (scanme.nmap.org.)
2600:3c01::f03c:91ff:fe93:cd19
fgont@satellite:~$ cat sites.txt | script6 get-mx
# si6networks.com (si6networks.com.)
02.mx.mail-scanner.eu.
01.mx.mail-scanner.eu.
# facebook.com (facebook.com.)
msgin.vvv.facebook.com.
fgont@satellite:~$ cat sites.txt | script6 get-mx | script6 get-aaaa
# 01.mx.mail-scanner.eu. (01.mx.mail-scanner.eu.)
2a00:d10::25:1
# 02.mx.mail-scanner.eu. (02.mx.mail-scanner.eu.)
2a00:d10:3::25:2
2001:898:2000:1000::2
fgont@satellite:~$
```

Obtaining AS-related info

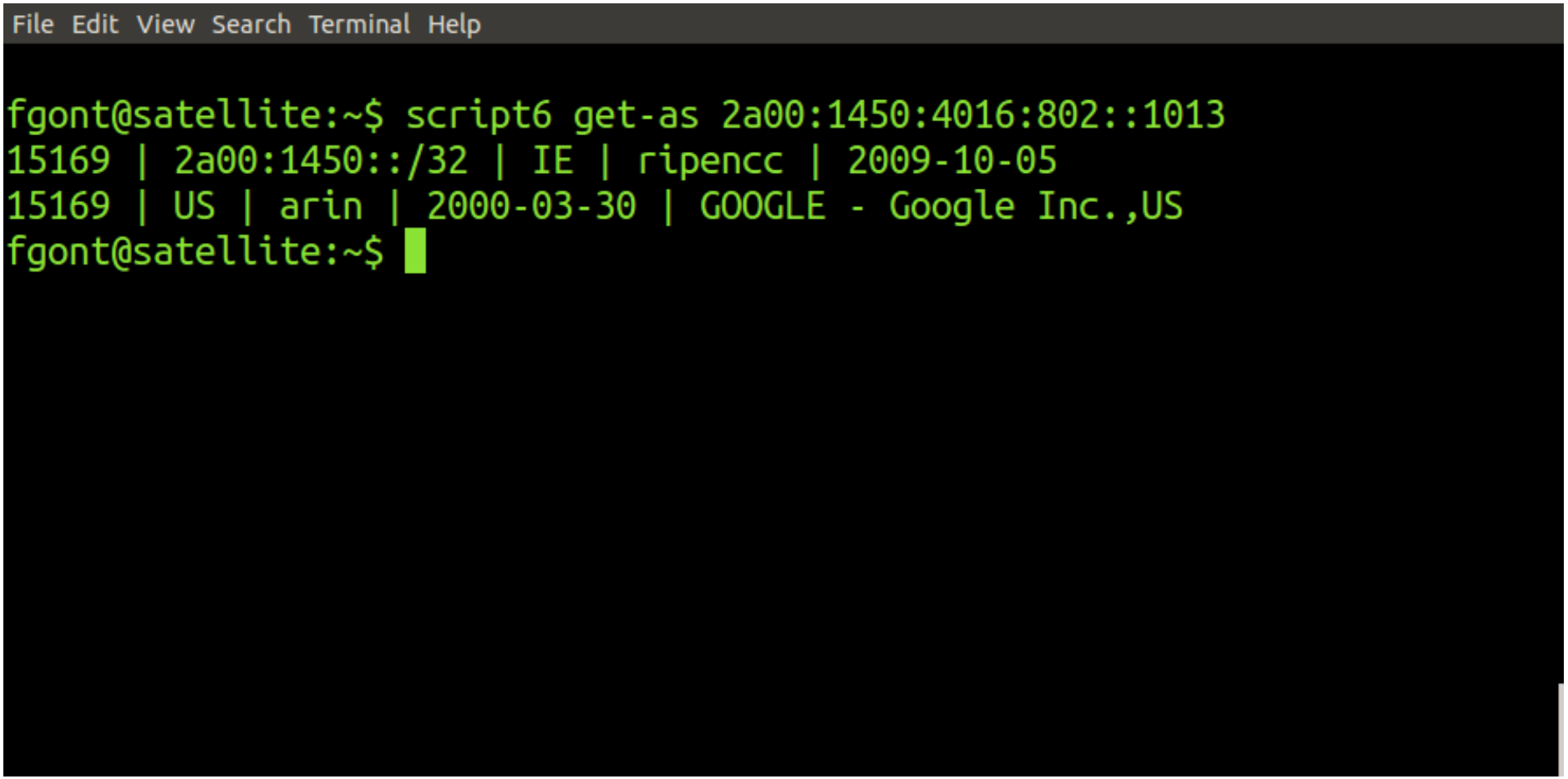
Obtaining AS-related info

- Given an IPv6 address, the corresponding AS identifies the corresponding organization, e.g.
  - who should I contact when an IPv6 address is attacking me?
  - who should I contact when a given router is dropping my packets?
- script6 can query AS-related information:

```
script6 get-as

script6 get-asn
```

Obtaining AS-related info



Tracing IPv6 Routes

path6 tool

- No existing traceroute tool supported IPv6 extension headers
  - e.g., How far do your IPv6 EH-enabled packets get?
- Hence we produced our path6 tool
  - Supports IPv6 Extension Headers
  - Can employ TCP, UDP, or ICMPv6 probes
  - It's faster ;-)
- Example:

```
# path6 -u 100 -d fc00:1::1
```

Dst Opt Hdr

path6 tool

```
File  Edit  View  Search  Terminal  Help
fgont@satellite:~$ sudo path6 -v -u 72 -d www.si6networks.com
IPv6 Source Address: 2001:1291:200:42e::2
IPv6 Destination Address: 2a00:8240:6:a::1
Destination Options Header: 72 bytes
Tracing path to www.si6networks.com (2a00:8240:6:a::1)...

  1 (2001:1291:200:42e::1)  59.3 ms  61.7 ms  60.7 ms
  2 (2001:1291:2::b)  61.6 ms  81.4 ms  80.4 ms
  3 ()  *  *  *
  4 ()  *  *  *
  5 ()  *  *  *
  6 ()  *  *  *
  7 (2001:1291:0:45::b)  274.7 ms  286.4 ms  290.9 ms
  8 (2001:478:124::176)  291.3 ms  290.2 ms  289.1 ms
  9 (2001:470:0:a6::2)  267.2 ms  266.2 ms  265.2 ms
 10 (2001:470:0:1b5::1)  284.5 ms  283.4 ms  282.2 ms
 11 (2001:470:0:299::2)  280.9 ms  279.8 ms  286.4 ms
 12 (2001:470:0:2cf::1)  354.6 ms  356.9 ms  356.6 ms
 13 (2001:470:0:2d0::2)  375.5 ms  375.3 ms  374.1 ms
 14 (2001:7f8:1::a502:9396:1)  351.8 ms  351.1 ms  367.6 ms
 15 (2a02:120:0:200::3:1b)  369.6 ms  368.5 ms  367.5 ms
 16 (2a00:8240:6:a::1)  366.2 ms  365.0 ms  363.8 ms
fgont@satellite:~$
```

Finding IPv6 blackholes

blackhole6: Finding IPv6 blackholes

- It is useful to find out who is dropping specific packets:
  - Troubleshooting
  - Network reconnaissance
  - ... or just checking if you EH-enabled attacks would work
- blackhole6 does this (and more) auto-magically:

```
blackhole6 DESTINATION [EHTYPE[EHSIZE]]
[PROTOCOL [PORT]]]
```

blackhole6: Methodology

1) Run “normal” path6 to target (D), and save route (ROUTE)
2) Check that last “hop” in route is D
3) Run EH-enabled path6, and find last responding address (M)
4) Find “M” in “ROUTE” -> dropping system is next in ROUTE (M+1)
5) Compare AS(M) with AS(M+1), and produce other stats

blackhole6: Methodology (II)

- Given the output of path6 for no-EH and EHs:

	No EHs	With EHs
	1. fc00:1:1:1000::1	1. fc00:1:1:1000::1
	2. fc00:1:1:2000::4	2. fc00:1:1:2000::4
	3. fc00:1:2:4000::1	3. fc00:1:2:4000::1
	4. fc00:2:1:4000::1	4. fc00:2:1:4000::1
	5. fc00:a:2:1000::1	5. fc00:a:2:1000::1
	6. fc00:a:4:4000::1	6. fc00:a:4:4000::1
DROP	7. fc00:b:1:1000::1	
	8. fc00:b:2:5000::1	
	9. fc00:b:4:5000::1	
	10. fc00:d::1	

blackhole6: Methodology (II)

```
File  Edit  View  Search  Terminal  Help
root@fgont-outside:~# blackhole6 www.google.com do8
SI6 Networks IPv6 Toolkit v2.0
blackhole6: A tool to find IPv6 blackholes
Tracing www.google.com (2404:6800:4008:c02::69)...

Dst. IPv6 address: 2404:6800:4008:c02::69 (AS15169 - GOOGLE - Google Inc.,US)
Last node (no EHs): 2404:6800:4008:c02::69 (AS15169 - GOOGLE - Google Inc.,US)
(18 hop(s))
Last node (DO 8): 2a00:ee0:0:215::2 (AS5603 - SIOL-NET Telekom Slovenije d.d.,S
I) (5 hop(s))
Dropping node: 2a00:ee0:5:26::2 (AS5603 - SIOL-NET Telekom Slovenije d.d.,SI ||
 AS15169 - GOOGLE - Google Inc.,US)
root@fgont-outside:~#
```

Statistics about IPv6 EH Support

Introduction

- A number of questions surrounded the use of IPv6 EHs:
  - Can be reliably employed on the public IPv6 Internet?
  - Anyway, are they effective for penetration-testing/attack purposes?
- There was not much real world data
- Tools we had to produce:
  - **`path6`**: EH-enabled traceroute
  - **`script6 get-alexa-domains`**: Obtain domains from Alexa's Top-1M file
  - **`script6 get-`**{**`mx`**,**`ns`**,**`aaaa`**}: Obtain different types of DNS RRs
  - **`addr6`**: Filter out uninteresting addresses (we had this one! ;-))
  - **`script6 get-trace6`**: Produce trace record for a number of targets
  - **`script6 get-trace6-stats`**: Produce stats based on the get-trace6 data

Some conclusions

Some conclusions

- Coding IPv6 tools:
  - Portability harder than expected (harder than it “should”)
  - Increased usage -> increased code quality
- Using IPv6 tools
  - There is a lot to learn through practice
- **Please use the toolkit and report back to us**

Questions?

Acknowledgements

- Jan Zorz & Go6 Institute

Thanks!

Fernando Gont

fgont@si6networks.com

IPv6 Hackers mailing-list

http://www.si6networks.com/community/

www.si6networks.com