Network Reconnaissance: Adventures in IPv6-Land

Fernando Gont

SI6 NETWORKS

H2HC 2019
Sao Paulo, Brazil. October 26-27, 2019

About...

- Security Researcher and Consultant at SI6 Networks
- Published:
  - 30 IETF RFCs (15+ on IPv6)
  - 10+ active IETF Internet-Drafts
- Author of the SI6 Networks' IPv6 toolkit
  - https://www.si6networks.com/tools/ipv6toolkit
- I have worked on security assessment of communication protocols for:
  - UK NISCC (National Infrastructure Security Co-ordination Centre)
  - UK CPNI (Centre for the Protection of National Infrastructure)
- More information at: https://www.gont.com.ar

Introduction

What is IPv6 all about?

- The main driver for IPv6 is its increased address space
- IPv6 uses 128-bit addresses
- Virtually all other “advantages” are marketing claims

Network Reconnaissance in IPv6

- IPv6 changes the “Network Reconnaissance” game
- Brute force address scanning attacks undesirable (if at all possible)
- We need to evolve in how they do net reconnaissance
  - Pentests/audits
  - Deliberate attacks
- Network reconnaissance support in security tools has traditionally been **very poor**

IPv6 Address Scanning

IPv6 Addressing in a Nutshell

- Different address types:
  - **unicast → most useful!**
  - anycast
  - multicast
- Different address scopes:
  - **global → most useful!**
  - link-local
  - unique-local
- Different lifetime properties:
  - **stable → most useful!**
  - temporary

IPv6 Addressing in a Nutshell (II)

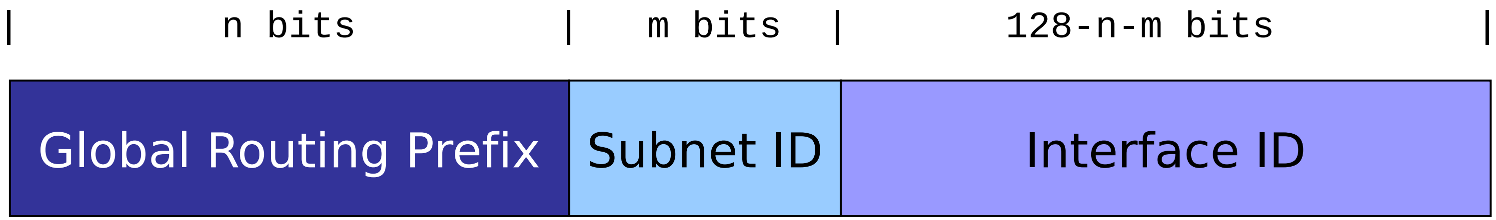
- Hosts normally configure:
  - one link-local address
  - one (stable) global address
  - one (temporary) global address
- For remote audits/attacks, mostly interested in:

stable global unicast addresses

IPv6 Address Scanning

- Larger address space has implications on address scanning
  - brute-force approach not feasible!
  - Networks address-scannable only if addresses have patterns
- Not all scope/type/stability combinations are of use in all scenarios. e.g.
  - a “private” (local) address may be of no use from a remote network
  - a temporary address may be of no use if persistance is desired

IPv6 Global Unicast Addresses



- A number of possibilities for generating the Interface ID:
  - Embed the MAC address (traditional SLAAC)
  - Stable-privacy (Hash(Prefix,Secret))
  - Embed the IPv4 address (e.g. 2001:db8::192.168.1.1)
  - Low-byte (e.g. 2001:db8::1, 2001:db8::2, etc.)
  - Wordy (e.g. 2001:db8::dead:beef)
  - According to a transition/co-existence technology (6to4, etc.)

Example: IPv6 Addresses with IPv4 IIDs

- They simply embed an IPv4 address in the IID
- Two variants found in the wild:
  - 2000:db8::192.168.0.1 <- Embedded in 32 bits
  - 2000:db8::192:168:0:1 <- Embedded in 64 bits
- Search space: same as the IPv4 search space – feasible!
- Examples:

```
# scan6 -d fc00::/64 -B all -Q 10.10.0.0/16
```

Example: IPv6 addr. with “low-byte” IIDs

- The IID is set to all-zeros, “except for the last byte”
  - e.g.: 2000:db8::1
- Other variants have been found in the wild:
  - 2001:db8::n1:n2 <- where n1 is typically greater than n2
- Search space: usually 2^8 or 2^{16} – feasible!
- Example:

```
# scan6 -d fc00::/64 --tgt-low-byte
```

Example: IPv6 addr with IEEE IIDs

24 bits	16 bits	24 bits
IEEE OUI	**FF FE**	Lower 24 bits of MAC
Known or guessable	Known	Unknown

- In practice, the search space is at most ~2^{24} bits – **feasible!**
- The low-order 24-bits are not necessarily random:
  - An organization buys a large number of boxes
  - In that case, MAC addresses are usually consecutive
- Examples:

```
# scan6 -d fc00::/64 -K 'Dell Inc' -v
```

scan6 coolness

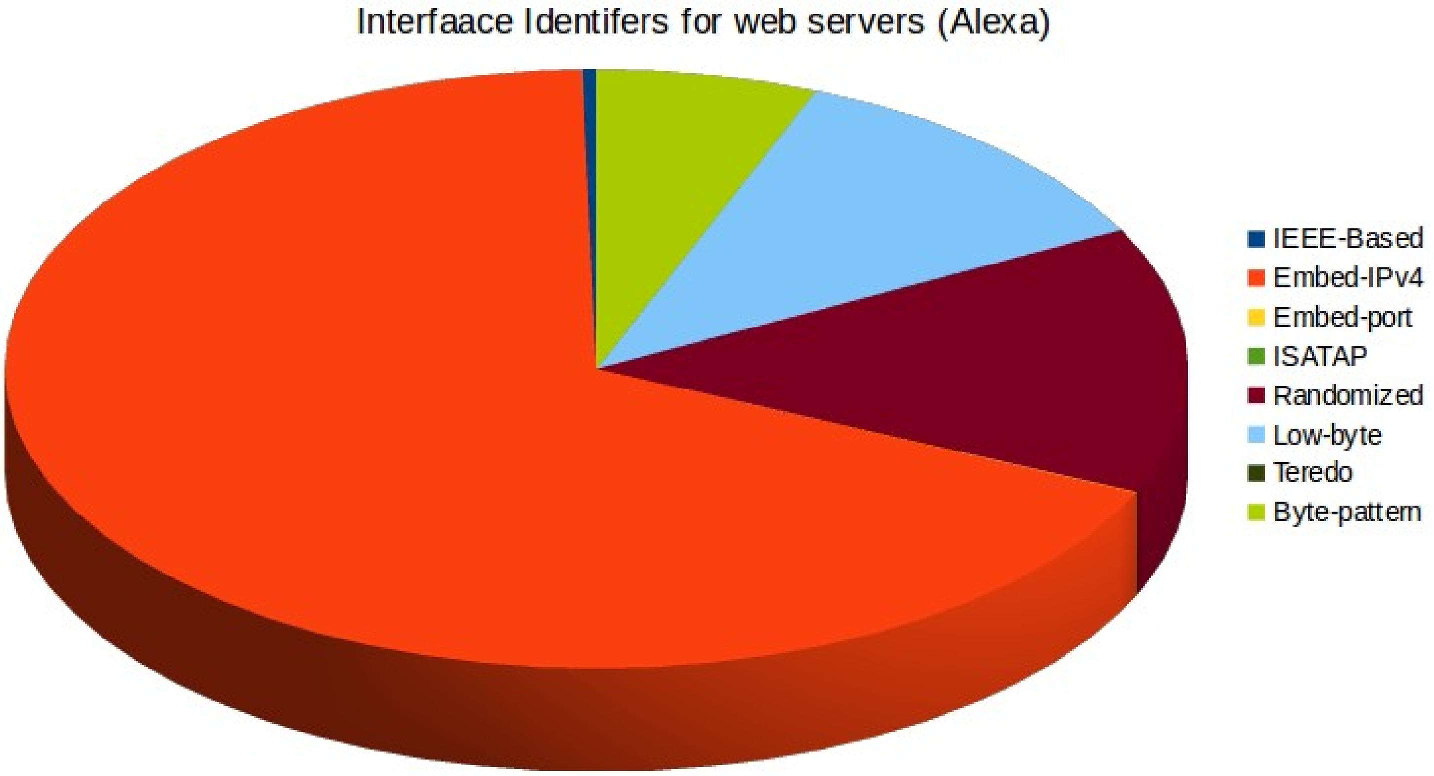
- “What if I'm lazy enough to 'set' an appropriate address pattern?”
  - scan6 infers the address pattern for you!
- Examples:

```
sudo scan6 -d DOMAIN/64 -v

sudo scan6 -d ADDRESS/64 -v
```

IPv6 Addresses in the Real World

IPv6 web servers: Alexa Dataset



Client addresses

- SLAAC stable and temporary addresses result in randomized IIDs
  - When performing passive analysis, it's hard to tell one from another
  - Difficult to infer hosr IID generation policy
- Many deployments employ a border "diode" firewall:
  - Hosts employ global addresses
  - Host are not globally reachable unless they initiate communications
  - Address scanning attempts get blocked

Some take-aways

- Servers tend to use manually-configured addresses
  - as opposed to SLAAC or DHCPv6
- Patterns vary from service to service
  - e.g. web servers vs. DNS servers vs. mail servers
- When address-scanning:
  - Find servers with any possible technique
  - Leverage address patterns to address-scan

Complementary Techniques

Complementary Techniques
Leveraging Search Engines

Search Engines (Bing)

- Good search results
- No obfuscation of results page
- No banning upon multiple queries
- Example:

```
script6 get-bing navy.mil
```

- Performance is much increased with the help of a dictionary
- Example:

```
script6 get-bing-dict navy.mil english.dic
```

Complementary Techniques
Leveraging Certificate Transparency

Introduction

- Goals of the Certificate Transparency Framework:
  - Make it difficult for CAs to issue certificates that are not visible to the owner of the domain
  - Provide an open auditing an monitoring system to determine malicious or mistakenly issued certificates
  - Protect users from such certificates
- Main components:
  - Certificate logs
  - Monitors
  - Auditors

Leveraging CTF logs

- Logs can be searched for subdomains of a specific zone
  - e.g. with https://crt.sh/
- Available with:

```
script6 get-crt ZONE
```

- If search would lead to tons of results, it must be partitioned into sub-zones

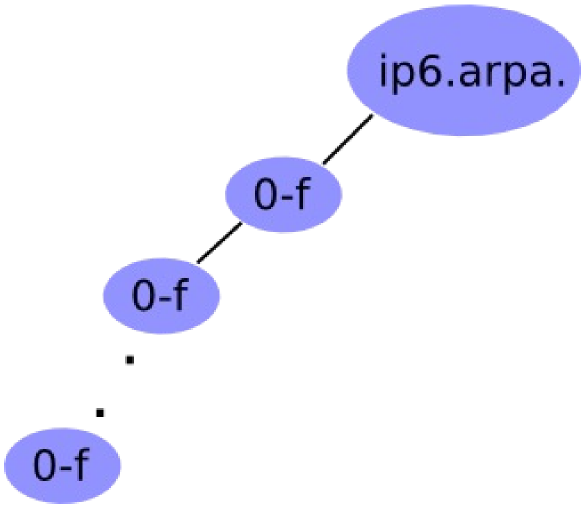
Leveraging CTF logs (II)

- Example:

```
fgont@satellite:~$ script6 get-crt lacnic.net
charts.dev.lacnic.net
monitor.dev.lacnic.net
natmeter.labs.lacnic.net
simon.labs.lacnic.net
simon.v4.labs.lacnic.net
simon.v6.labs.lacnic.net
cdn.dev.lacnic.net
ghwww.labs.lacnic.net
milacnic.dev.lacnic.net
labs.lacnic.net
transfer-stats.labs.lacnic.net
portaldedatos.dev.lacnic.net
simon.lacnic.net
icav6.dev.lacnic.net
jekyll-template.dev.lacnic.net
rdap-web.lacnic.net
hackathon.dev.lacnic.net
```

Complementary Techniques
DNS reverse mappings

Introduction



- Technique:
  - Given a zone X.ip6.arpa., try the labels [0-f].X.ip6.arpa.
  - If an NXDOMAIN is received, that part of the "tree" should be ignored
  - Otherwise, if NOERROR is received, "walk" that part of the tree
- Example (using dnsrevenum6 from THC-IPv6):

```
$ dnsrevenum6 DNSSERVER IPV6PREFIX
```

DNS Reverse Mappings

- Example:

```
fgont@satellite:~$ dnsrevenum6 1.1.1.1 2001:13c7:7002:4128::/48
Starting DNS reverse enumeration of 2001:13c7:7002:4128:: on server 1.1.1.1
Warning: packet loss, increasing response timeout to 3 seconds
Found: 2001:13c7:7002:2000::2 is lo1.gw02.lacnic.net.
Found: 2001:13c7:7002:2000::1 is lo1.gw01.lacnic.net.
Warning: packet loss, increasing response timeout to 4 seconds
Found: 2001:13c7:7002:3000::1 is ge13.gw.lacnic.net.
Found: 2001:13c7:7002:3000::11 is ns2.lacnic.net.
Found: 2001:13c7:7002:3000::10 is ns.lacnic.net.
Found: 2001:13c7:7002:3000::12 is d.ip6-servers.lacnic.net.
Found: 2001:13c7:7002:3000::14 is ns3.lacnic.net.
Warning: packet loss, increasing response timeout to 8 seconds
Found: 2001:13c7:7002:3000::253 is ge13.gw01.lacnic.net.
Found: 2001:13c7:7002:3000::254 is ge13.gw02.lacnic.net.
Warning: packet loss, increasing response timeout to 9 seconds
Found: 2001:13c7:7002:4000::1 is ge11.gw.lacnic.net.
Found: 2001:13c7:7002:4000::10 is registro.lacnic.net.
Found: 2001:13c7:7002:4000::11 is mail.lacnic.net.
Found: 2001:13c7:7002:4000::62 is ge11.gw02.lacnic.net.
Found: 2001:13c7:7002:4000::61 is ge11.gw01.lacnic.net.
```

Lessons learned: “Noise”

- Large number of dynamically generated reverse mappings for some networks:

```
Found: 2001:4998:c:80d::4062 is hz-network-migration-50568-89.gq1.yahoo.com.
Found: 2001:4998:c:80d::4064 is hz-network-migration-50568-91.gq1.yahoo.com.
Found: 2001:4998:c:80d::406d is hz-network-migration-50568-100.gq1.yahoo.com.
Found: 2001:4998:c:80d::4061 is hz-network-migration-50568-88.gq1.yahoo.com.
Found: 2001:4998:c:80d::4066 is hz-network-migration-50568-93.gq1.yahoo.com.
Found: 2001:4998:c:80d::4060 is hz-network-migration-50568-87.gq1.yahoo.com.
Found: 2001:4998:c:80d::4063 is hz-network-migration-50568-90.gq1.yahoo.com.
Found: 2001:4998:c:80d::4068 is hz-network-migration-50568-95.gq1.yahoo.com.
Found: 2001:4998:c:80d::4069 is hz-network-migration-50568-96.gq1.yahoo.com.
Found: 2001:4998:c:80d::406b is hz-network-migration-50568-98.gq1.yahoo.com.
Found: 2001:4998:c:80d::4065 is hz-network-migration-50568-92.gq1.yahoo.com.
Found: 2001:4998:c:80d::406f is hz-network-migration-50568-102.gq1.yahoo.com.
Found: 2001:4998:c:80d::406c is hz-network-migration-50568-99.gq1.yahoo.com.
```

Lessons learned: Reliability

- Reverse mappings of /48s were more reliable than those of /32s
- May make sense to split /32s into multiple /48s for reliability purposes

Integrating IPv6 Network Reconnaissance

Introduction

- Most network reconnaissance is manual
- Out goal was to try to integrate different techniques into the same tool

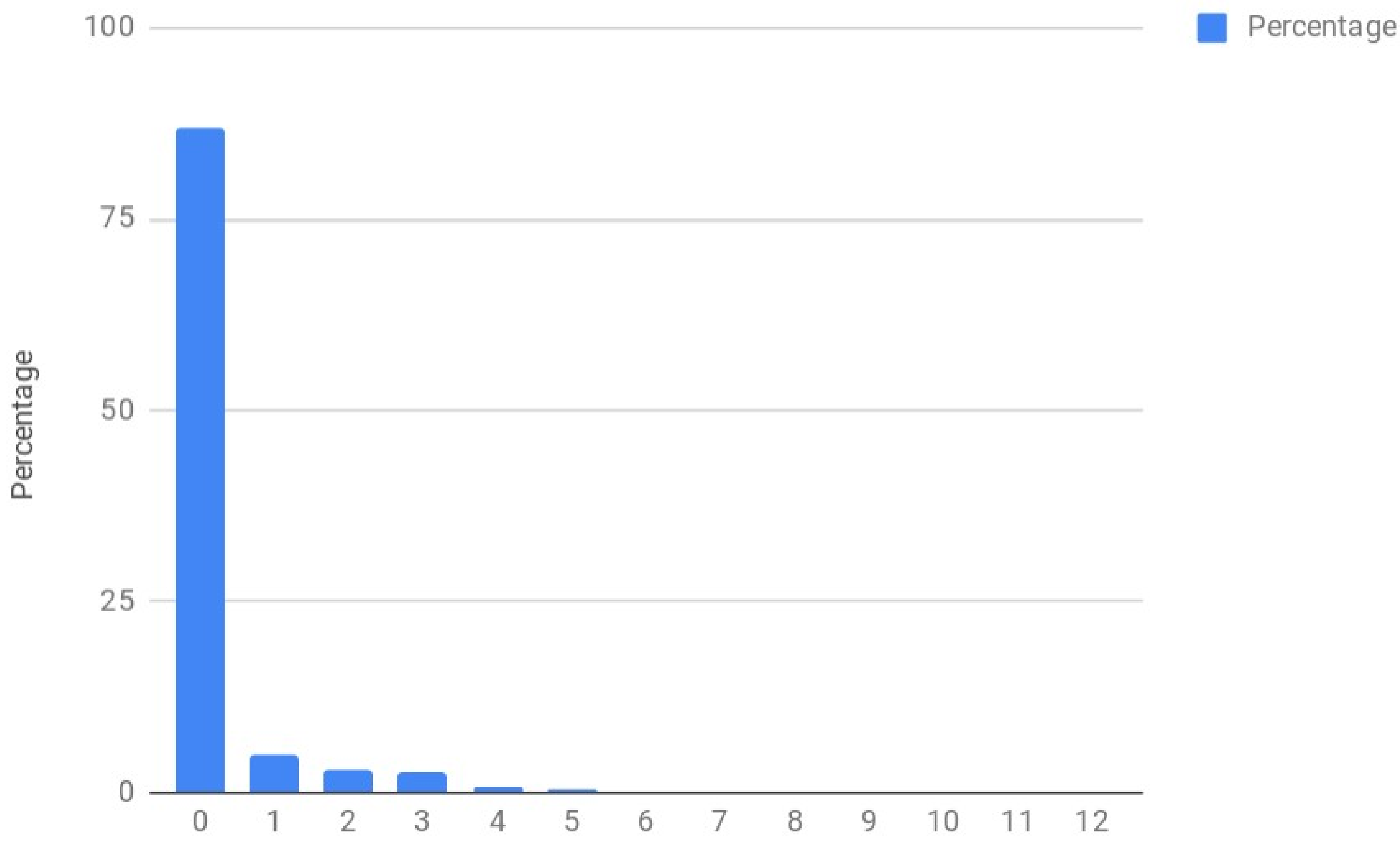
Messi: IPv6 net reconnaissance tool

- If you have access to a local node, it might be of use:
- What the tool does:
  1) Obtain domains from search engines
  2) Obtain NS and MX records
  3) Obtain IPv6 addresses for all those names
  4) Build prefixes out of those addresses
  5) Do DNS reverse enumeration
  6) Go back to step #1
- Eventually we converge to results
- Implemented as:

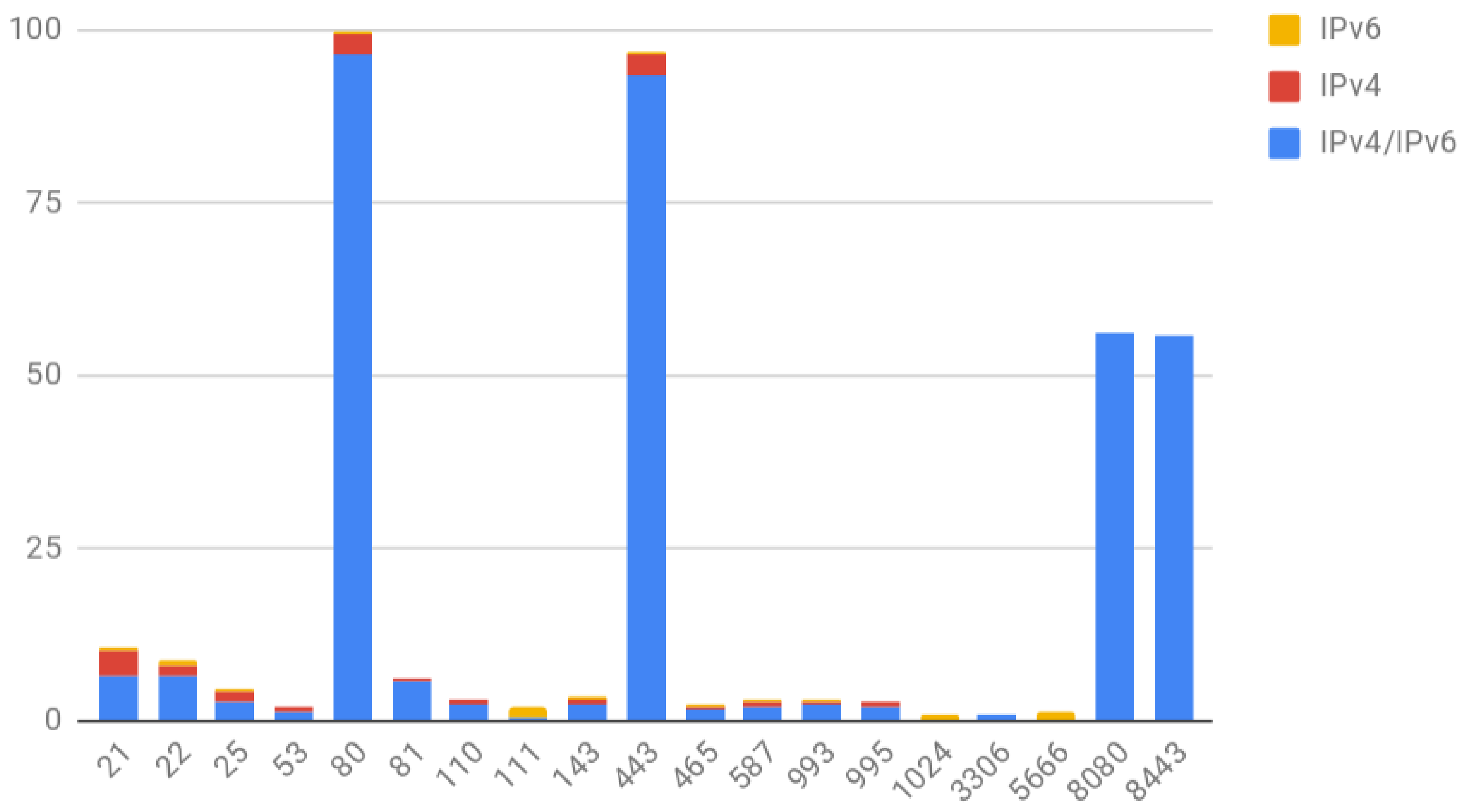
```
messi -Hgont.com.ar -H2001:db8:1::/64 -F2002:db8:1::/6
```

Why bother finding IPv6 addresses?

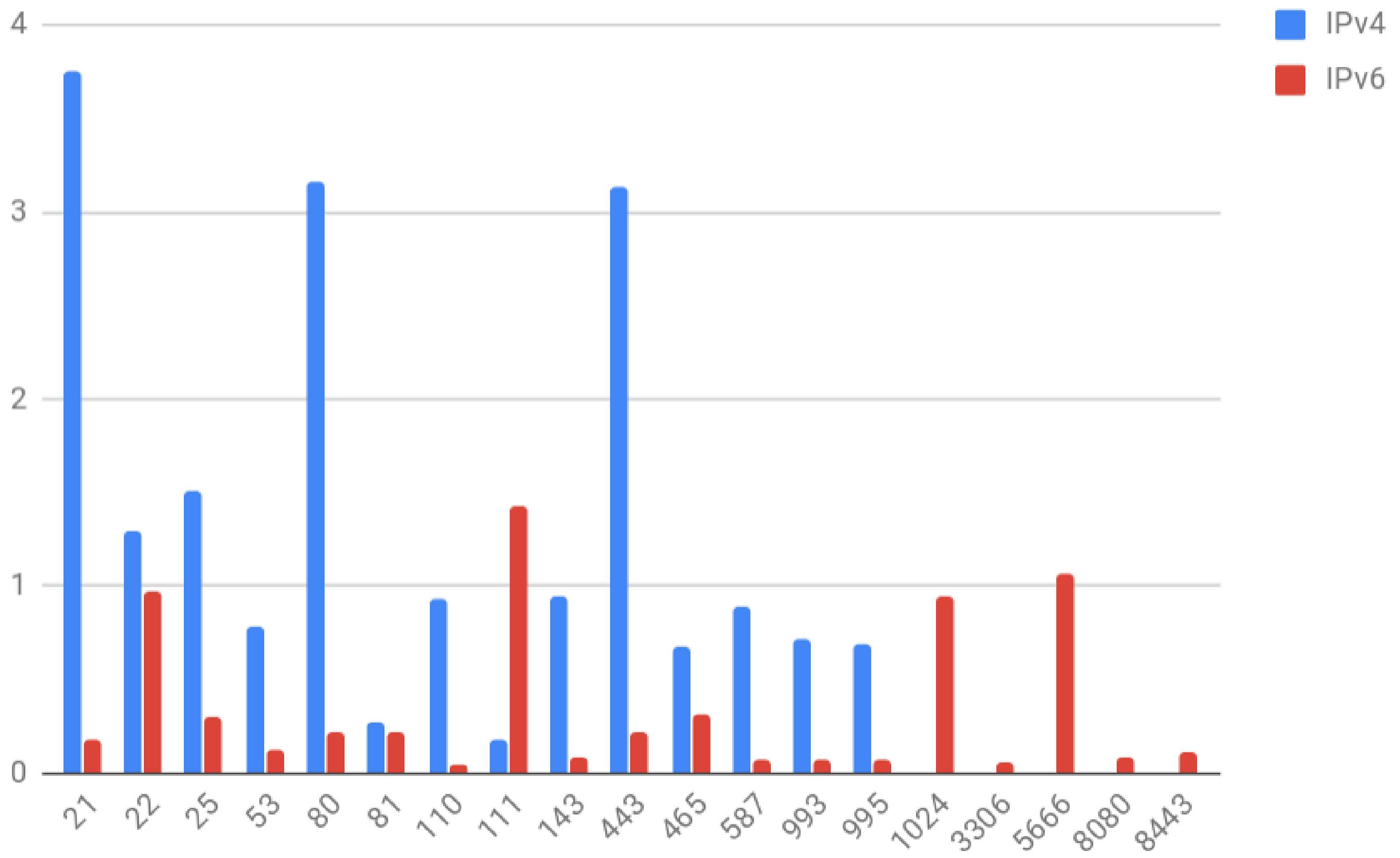
Policy mismatches across IPv4/IPv6



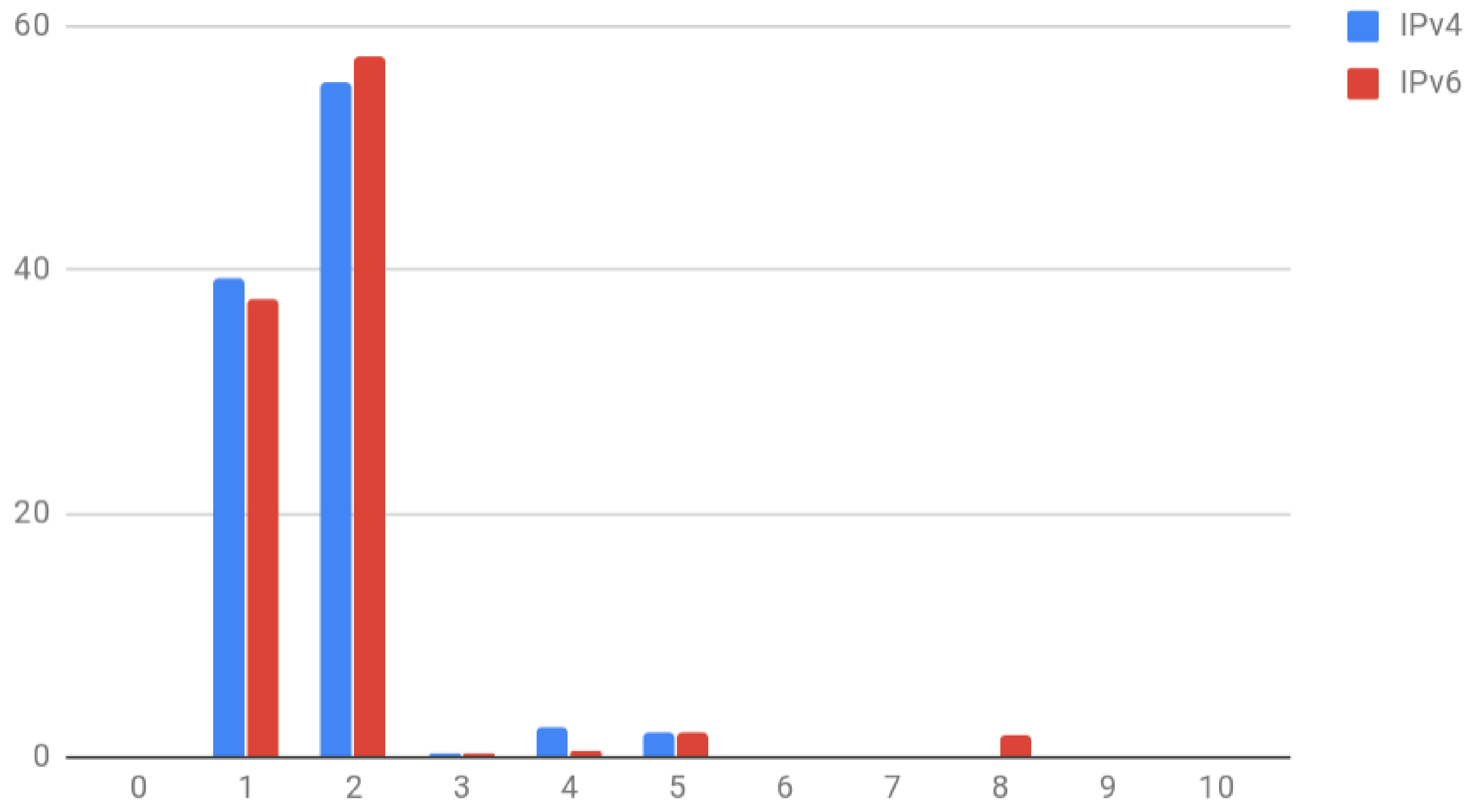
Open ports on IPv4/IPv6 (cumulative)



Open ports (differential)



Typical number of addresses per domain



Conclusions

Conclusions

- IPv6 is becoming an important attack surface
- Traditional brute-force address-scanning not feasible for IPv6
  - Pattern-based address-scanning possible in many cases
- There is an ongoing move towards randomized addresses
- Complementary reconnaissance techniques become more important
- Mismatches in IPv6/IPv4 security policies do exist
  - But they don't favor any protocol

Questions?

Thanks!

Fernando Gont

fgont@si6networks.com

IPv6 Hackers mailing-list

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

www.si6networks.com