

Advances in IPv6 Network Reconnaissance

Fernando Gont



NGI @ Troopers 2018
Heidelberg, Germany. March 12-13, 2018


About...

- Security Researcher and Consultant at SI6 Networks
- Published:
 - 30 IETF RFCs (10+ 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

Network Reconnaissance

reconnaissance

/rɪˈkɒnɪs(ə)ns/ 

noun

military observation of a region to locate an enemy or ascertain strategic features.

"an excellent aircraft for low-level reconnaissance"

synonyms: preliminary survey, [survey](#), [exploration](#), [observation](#), [investigation](#), [examination](#), [inspection](#), [probe](#), [scrutiny](#), [scan](#); [More](#)

- preliminary surveying or research.
"conducting client reconnaissance"

Network reconnaissance:

Locate possible targets and/or learn network information/features that can be leveraged for performing network-based attacks

Where we were at

Where we were at

- Smart host address scans
 - via SI6 Toolkit's scan6
- DNS reverse enumeration
 - via THC-IPv6 dnsrevenue6 et al
- DNS sec zone walking
- Others borrowed from the IPv4 world

Moving things forward

Moving things forward

- Leverage search engines
 - suggested in RFC7707
- Smart discovery of prefixes
 - suggested in RFC7707
- Stateful address analysis
 - Ref Plonka
- Try to put all the above together

Leveraging Search Engines

Introduction

- Most search engines support this sort of query:

site: *DOMAIN*

- Very useful for:
 - pentesting a specific site
- Somewhat useful for:
 - Obtaining zone data
- Challenges:
 - Some engines obfuscate the results
 - Some require you to keep state (cookie-like)
 - Some will ban you if they assume you are a robot

Challenges

- Some engines obfuscate the results
 - Google is a notable example
- Some will ban you if they assume you are a robot
 - Teoma will ban you for about a day
- Some require you to keep state (cookie-like)
 - Just scrypt the first page for the “cookie”, and use it in the actual query
- Some complain if they think you are a robot
 - Fake the user-agent
 - Fly low, if necessary

Playing with Bing

- Good search results
- No obfuscation of results page
 - Improvements in scanning techniques
 - Improvements in IPv6 addressing to mitigate these attacks
- No banning upon multiple queries
- Example:

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

Playing with Teoma

- Good search results
- No obfuscation of results page
 - Improvements in scanning techniques
 - Improvements in IPv6 addressing to mitigate these attacks
- Banning upon lots of queries
 - Limits usefulness for a single target
- Example:

```
script6 get-teoma navy.mil
```

Working with IPv6 Addresses

Introduction

- addr6 lets you do lots of things with IPv6 addresses
 - Filter based on address properties (type, scope, etc)
 - Remove duplicate addresses
- More features added
 - Some requested by friends
 - Others for my own needs

IPv6 address presentation “styles”

- Canonic format:
 - Useful for comparing addresses for “equality”
 - Useless for virtually everything else

addr6 -c -a ADDRESS

- Fixed-size (constant length):
 - A hassle for humans
 - Awesome for scripting

addr6 -f -a ADDRESS

Generating IPv6 prefixes

- You have a bunch of addresses
- You want to produce unique /something prefixes

```
cat addresses.txt | addr6 -i -P /32
```

- What's the use of this?
 - Fixed-size (constant length):
 - A hassle for humans
 - Awesome for scripting

```
addr6 -f -a ADDRESS
```

Integrating IPv6 Network Reconnaissance

Introduction

- Most network reconnaissance is manual
- Our 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

Questions?

Thanks!

Fernando Gont

fgont@si6networks.com

IPv6 Hackers mailing-list

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



www.si6networks.com