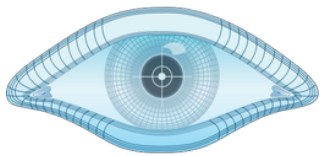
Advanced network scanning with Nmap 6

Henri Doreau
henri.doreau@gmail.com



13th LSM - Geneva 2012

Outline

Outline

Nmap Security Scanner

Full-featured Network scanner

- Port scanner
- Version and OS fingerprinting
- Lua scripting engine
- Companion tools (zenmap, ncat, nping, ndiff...)

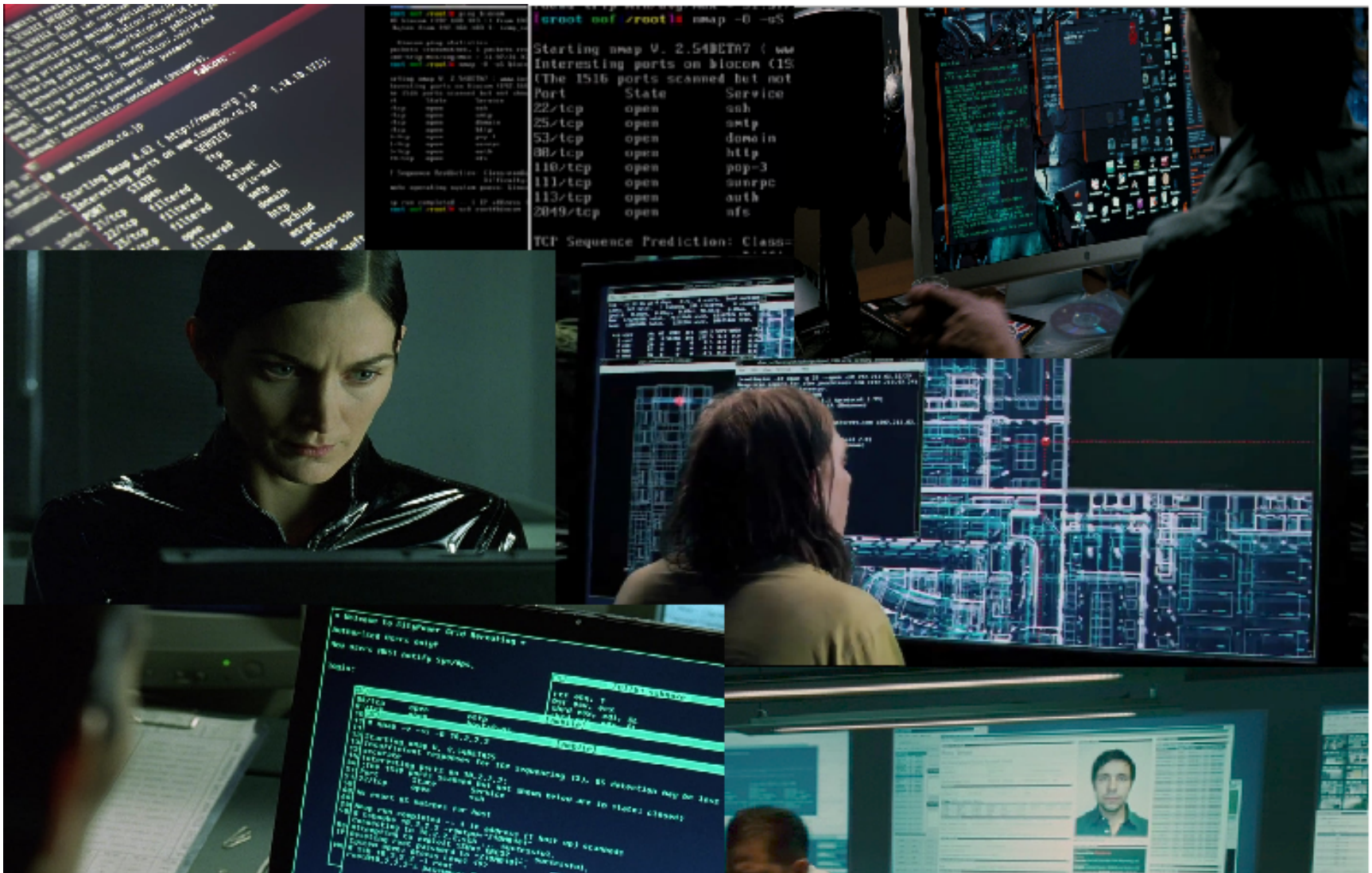
Nmap Security Scanner

Vibrant community

- Fingerprint DBs
- CPEs
- Scripts and NSE libraries

Nmap Security Scanner

Hollywood movie star



Outline

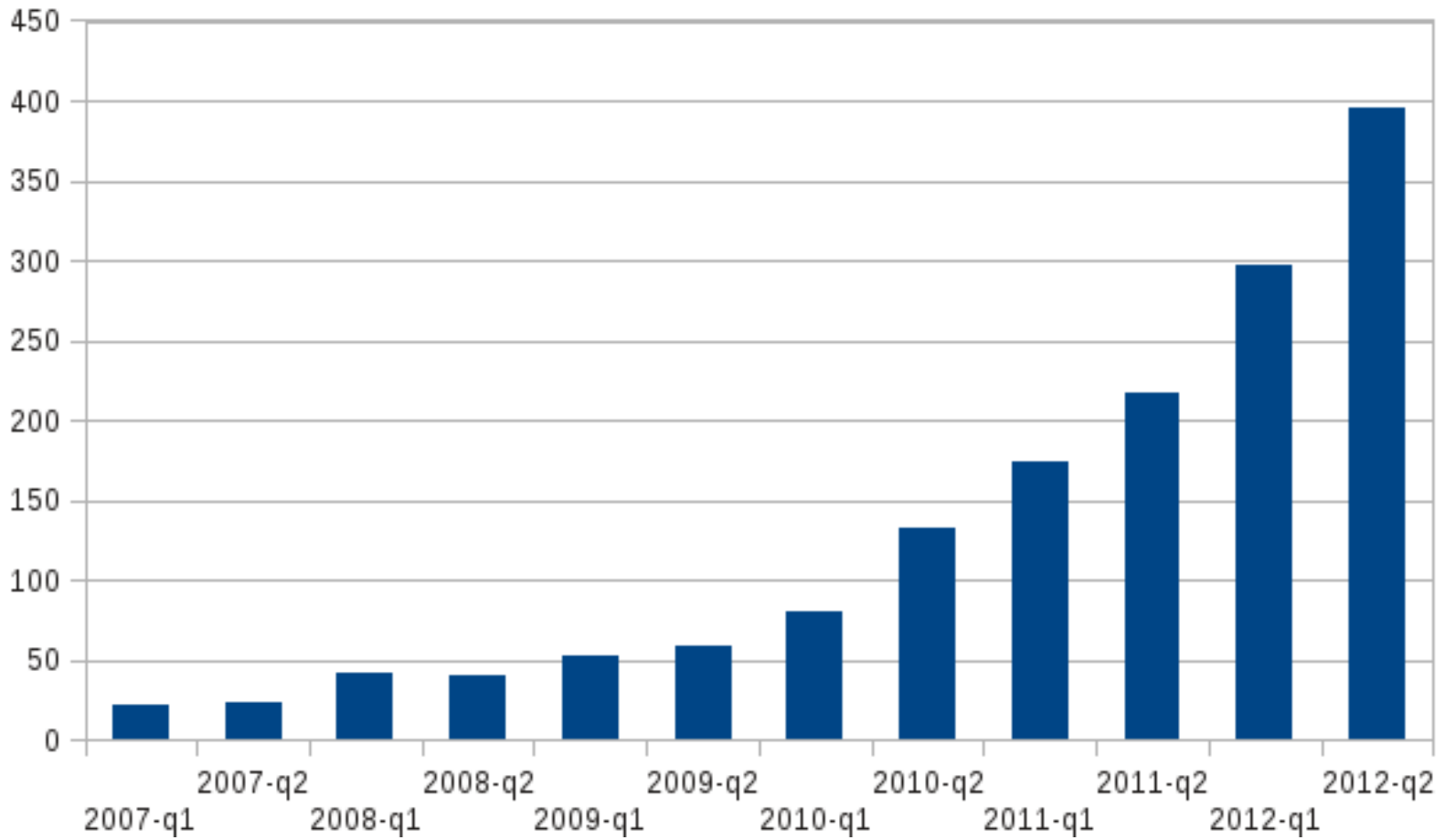
Introduction

Built-in lua scripting engine

- Network exploration
- Sophisticated version detection
- Vulnerability detection
- Scan results post-processing

NSE development

Script collection growth



Script phases

Four execution modes

- Prerules
- Service
- Host
- Postrules

- NSE Pre-scan
  1. Host enumeration
  2. Host discovery
  3. Reverse DNS resolution
  4. Port scan
  5. Version detection / RPC grind
  6. OS fingerprinting
  7. Traceroute
  8. Script scan
  9. Output
- NSE Post-scan

Script structure

When to run?

```
hostrule = function(host)
  return host.directly_connected
end
```

```
portrule = shortport.http
```

$\Rightarrow$ script can have several rule and action functions

Sample output

```
Nmap scan report for scanme.nmap.org (74.207.244.221)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 5.3p1 Debian 3ubuntu7
80/tcp open  http    Apache httpd 2.2.14 ((Ubuntu))
|_http-title: Go ahead and ScanMe!
Service Info: OS: Linux; CPE: cpe:/o:linux:kernel

Host script results:
| firewalk:
| HOP  HOST          PROTOCOL  BLOCKED PORTS
| 0    192.168.0.15  tcp       139
|_10   64.62.250.6   tcp       135,445
```

Design

NSE parallelism

- Single nmap thread
- lua coroutines

⇒ Lightweight and efficient non-blocking mechanism

⇒ Script writers get parallelism for free

⇒ No concurrent memory access concerns *ever*

Adaptive workflow

Two ways to invoke scripts

Point and shoot

```
nmap --script samba-vuln-cve-2012-1182 <target>
nmap --script +mongodb-info -p80 <target>
```

$\Rightarrow$ No silent dependencies

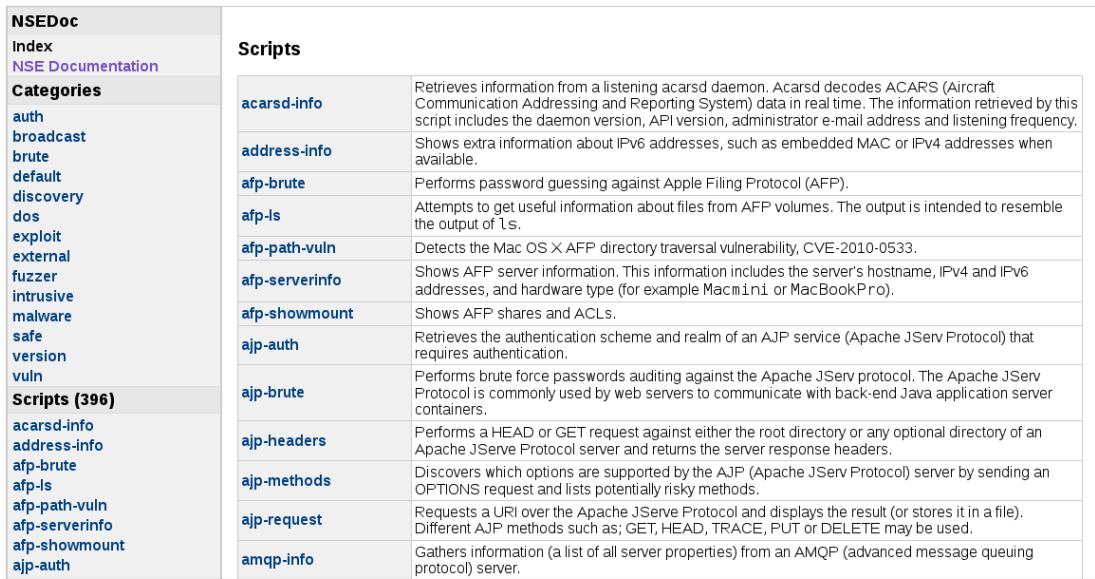
Aim oriented

```
nmap --script "http-* and not brute" <target>
```

Script categories

Grouped by categories

- `default`
- `intrusive`
- `external`
- `...`



NSEDoc

Index
NSE Documentation

Categories

auth
broadcast
brute
default
discovery
dos
exploit
external
fuzzer
intrusive
malware
safe
version
vuln

Scripts (396)

acarsd-info
address-info
afp-brute
afp-ls
afp-path-vuln
afp-serverinfo
afp-showmount
ajp-auth

Scripts

acarsd-info	Retrieves information from a listening acarsd daemon. Acarsd decodes ACARS (Aircraft Communication Addressing and Reporting System) data in real time. The information retrieved by this script includes the daemon version, API version, administrator e-mail address and listening frequency.
address-info	Shows extra information about IPv6 addresses, such as embedded MAC or IPv4 addresses when available.
afp-brute	Performs password guessing against Apple Filing Protocol (AFP).
afp-ls	Attempts to get useful information about files from AFP volumes. The output is intended to resemble the output of `ls`.
afp-path-vuln	Detects the Mac OS X AFP directory traversal vulnerability, CVE-2010-0533.
afp-serverinfo	Shows AFP server information. This information includes the server's hostname, IPv4 and IPv6 addresses, and hardware type (for example `Macmini` or `MacBookPro`).
afp-showmount	Shows AFP shares and ACLs.
ajp-auth	Retrieves the authentication scheme and realm of an AJP service (Apache JServ Protocol) that requires authentication.
ajp-brute	Performs brute force passwords auditing against the Apache JServ protocol. The Apache JServ Protocol is commonly used by web servers to communicate with back-end Java application server containers.
ajp-headers	Performs a HEAD or GET request against either the root directory or any optional directory of an Apache JServe Protocol server and returns the server response headers.
ajp-methods	Discovers which options are supported by the AJP (Apache JServ Protocol) server by sending an OPTIONS request and lists potentially risky methods.
ajp-request	Requests a URI over the Apache JServe Protocol and displays the result (or stores it in a file). Different AJP methods such as; GET, HEAD, TRACE, PUT or DELETE may be used.
amqp-info	Gathers information (a list of all server properties) from an AMQP (advanced message queuing protocol) server.

see `http://nmap.org/nsedoc`

Outline

Full IPv6 support

Long standing wish

- All features (provided it makes any sense)
- All supported platforms

Full IPv6 support

Long standing wish

- All features (provided it makes any sense)
- All supported platforms

YEAH!!!

Brand new OS fingerprinting engine

Innovative approach: machine learning techniques

- Reduced dataset
- Increased adaptiveness
- Very accurate

⇒ See `http://nmap.org/book/osdetect`

IPv6 support

Honestly, who cares?

IPv6 support

Honestly, who cares?

The future is already there!

Enhanced performances

Three main axis of improvement

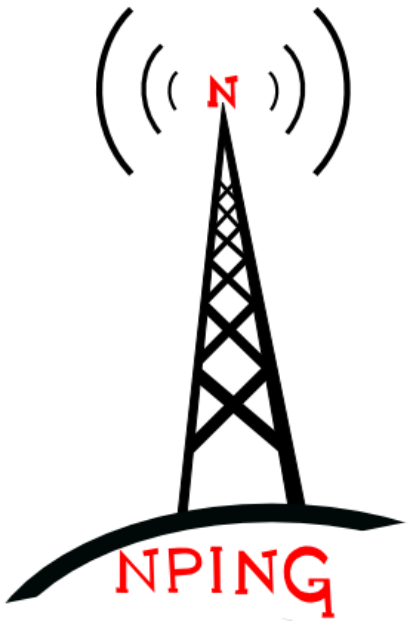
- Memory footprint
- High performance and scalable I/O notification facities
- Application-specific optimizations (NSE)

cf. *Scanning the Internet*, by Fyodor

Nping

Reimplementation of the venerable hping2

- Modern, high performance tool
- Leverages nmap libraries
- Provides new packet crafting classes to nmap



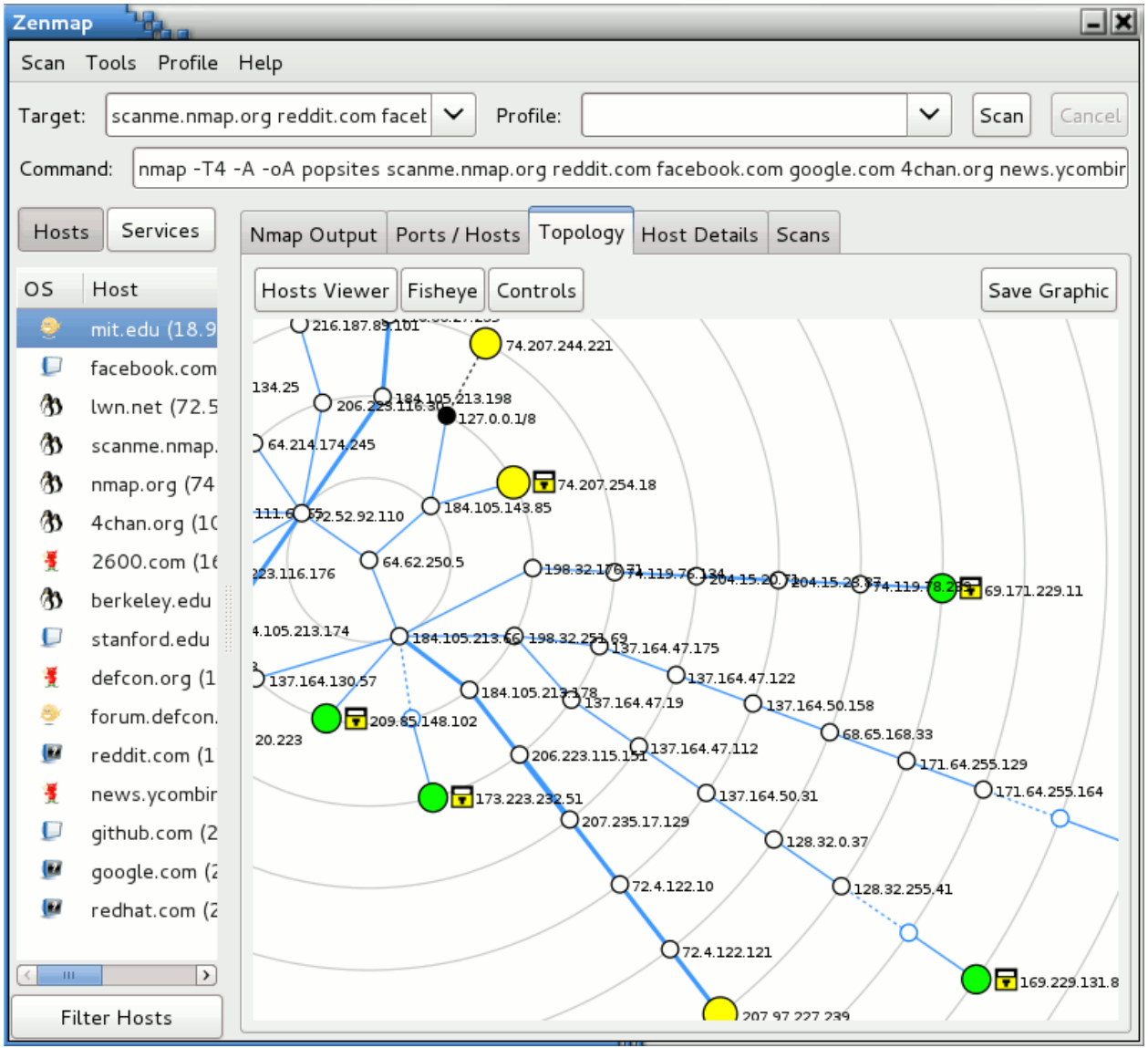
Nping Echo mode

Replacement for ping+tcpdump

1. nping in server mode on target
2. client probes the target
3. server returns captured probes to the client(s) as encrypted payloads

Zenmap tologoy tab

Finally: actual network maps from the network mapper!



Better web scanning

Big focus on web technologies

- Pipelining
- Built-in web crawler
- Caching
- Web-specific security checks

NSE frameworks

Implemented as NSE libraries

brute

Parallel network authentication cracking module.

credentials

Leverage and report discovered credentials.

vulns

Consistent vulnerability reports and efficient post-processing.

Outline

Upcoming: web scanning

Continued effort on HTTP

- Implement latest performance-related protocols and paradigms
- WebSocket mode to ncat

Upcoming: extend NSE

Expand the role and features of NSE

- Leveraging native libraries from lua
- NSE-based port scanning
- Re-implementing older code within NSE
- Adapting NSE to the companion tools

Upcoming: misc

but also...

- Combining IP v4/v6 scans
- Improving scalability
- Scanning through proxies
- Remote checks through authenticated SSH connections
- Updater

Get involved!

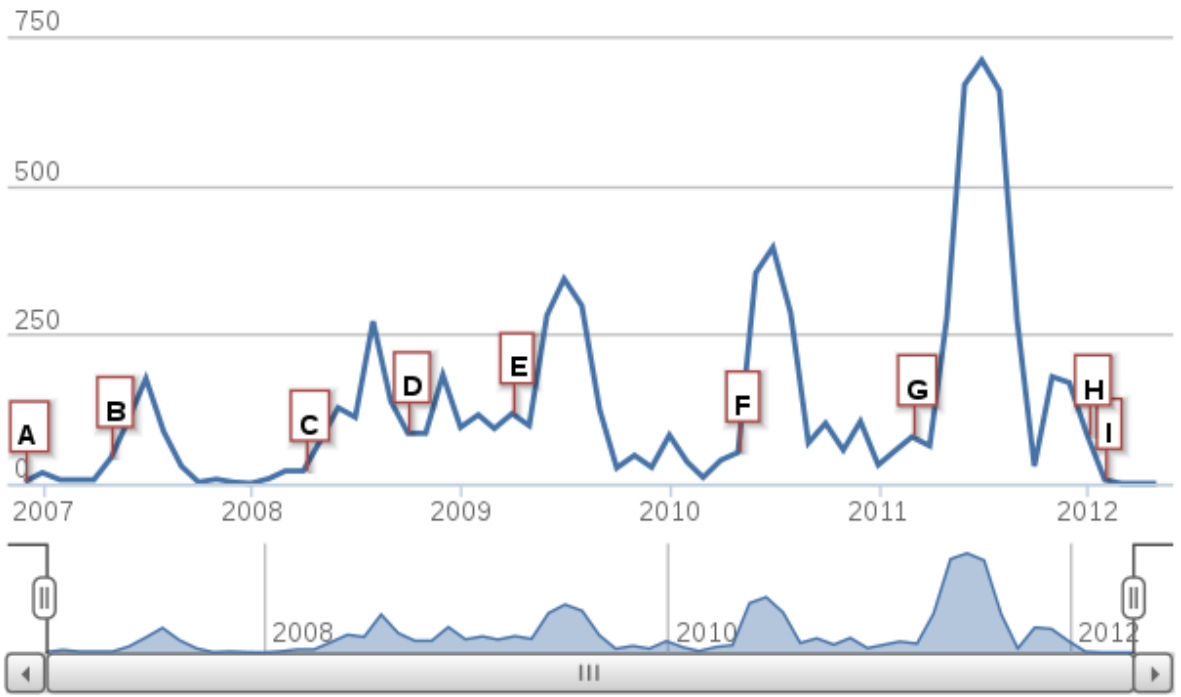
Your own awesome idea!

...and code? ;)

Development

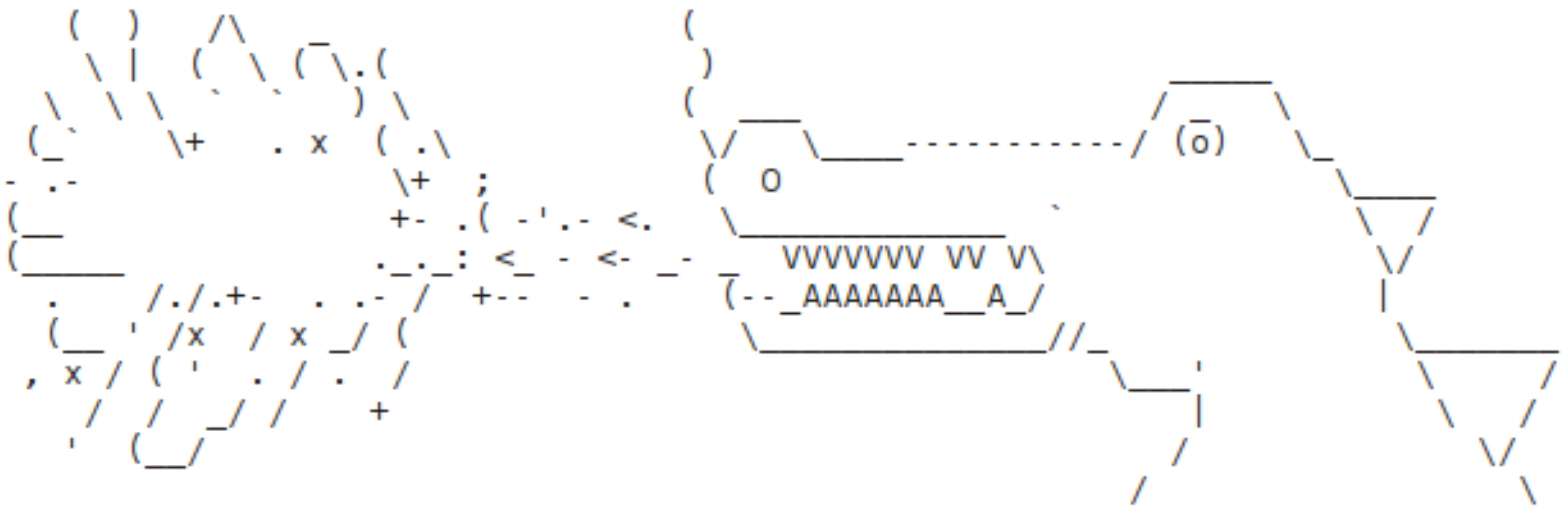
Increasing development pace

- 2011 was the most active year ever in the project history! (`ohloh.net`).
- 8^{th} consecutive Google Summer of Code



Happy birthday nmap!

15th birthday this year (Sept. 1st)



Questions?

`http://nmap.org`

`nmap-dev@insecure.org` (it's cool, join!)