



Open Source Security Tool Turbo Talks Wireshark Sharkfest 2011



Gordon “Fyodor” Lyon
Nmap Security Scanner Project



Tod Beardsley
Metasploit Project (Rapid7)



Thomas D'Otreppe
Aircrack-ng



Nmap Security Scanner

Zenmap

Scan Tools Profile Help

Target: Profile:

Command:

Hosts Services

OS	Host
	scanme.nmap
	facebook.com
	google.com (7
	nmap.org (74.
	microsoft.com

Nmap Output Ports / Hosts **Topology** Host Details Scans

Hosts Viewer Fisheye Controls

Filter Hosts



Outline

- Nmap Scripting Engine
- IPv6
- Zenmap GUI
- Nmap Suite
- Final Notes & Q&A

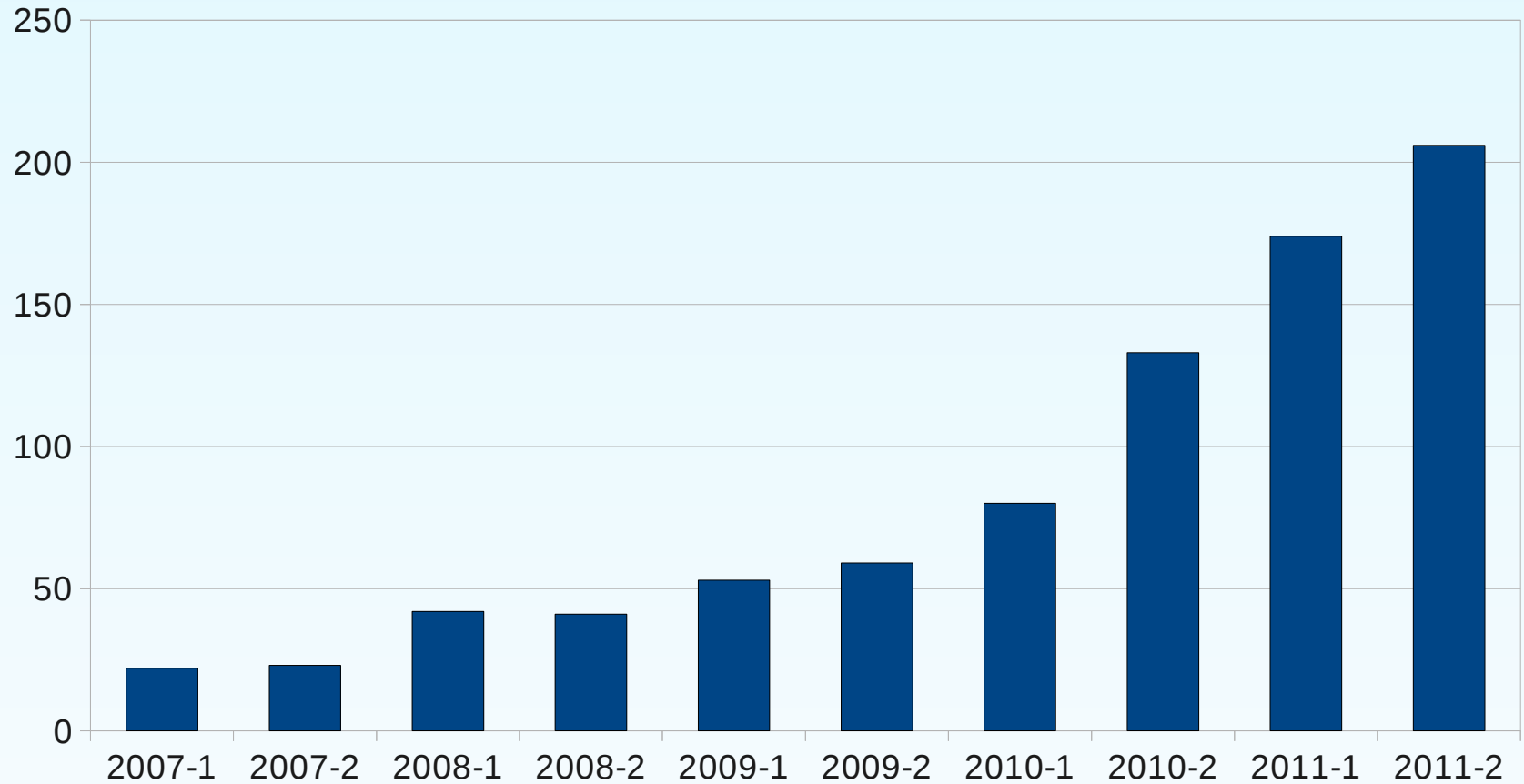


Nmap Scripting Engine

```
# nmap -A -T4 www.wireshark.org
[...]
21/tcp open  ftp          vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| drwxrwxr-x   3 ftp          ftp          4096 Jun 07 17:37 osx
| drwxrwxr-x   2 ftp          ftp          36864 Jun 13 10:01
prerelease
| drwxrwxr-x   3 ftp          ftp          4096 Jun 07 17:35 src
22/tcp open  ssh          OpenSSH 5.3p1 Debian 3ubuntu6
(protocol 2.0)
| ssh-hostkey: 1024
79:d7:cc:0c:8f:03:20:0d:75:39:09:7f:09:42:9c:25 (DSA)
|_2048 1c:6a:6d:94:5e:9b:60:ac:7e:15:f9:c7:24:85:4b:42 (RSA)
80/tcp open  http         Apache httpd 2.2.14 ((Ubuntu))
| http-robots.txt: 3 disallowed entries
|_/_awstats/ /cgi-bin/ /mailman/
|_http-title: Wireshark & middot; Go deep.
443/tcp open  ssl/http Apache httpd 2.2.14 ((Ubuntu))
|_http-title: Wireshark & middot; Go deep.
| http-robots.txt: 3 disallowed entries
|_/_awstats/ /cgi-bin/ /mailman/
```



Script Collection Growth





IPv6

- Current status
- World IPv6 Day Commemorative Release:
<http://bit.ly/nmapv6>
- Future plans
- Demo



Zenmap GUI

The screenshot displays the Zenmap application window. At the top, the title bar reads "Zenmap". Below it is a menu bar with "Scan", "Tools", "Profile", and "Help". The main interface includes a "Target:" field with the value "scanme.nmap.org facebook.cor" and a "Profile:" dropdown set to "Intense scan". A "Command:" field contains the command: `nmap -T4 -A -v scanme.nmap.org facebook.com google.com microsoft.com nmap.org`. Below the command field are tabs for "Hosts" and "Services". On the left, a list of hosts is shown with columns for "OS" and "Host". The "Hosts" tab is active, showing a list of hosts including "scanme.nmap.org", "facebook.com", "google.com (7)", "nmap.org (74)", and "microsoft.com". The main area is divided into "Nmap Output", "Ports / Hosts", "Topology", "Host Details", and "Scans". The "Topology" tab is selected, showing a network diagram with nodes and connections. A "Save Graphic" button is visible in the top right of the topology view. The nodes in the topology include: "scanme.nmap.org (64.134.52)", "xe4-1.core1.svk.layer42.net", "Layer42.car2.SanJose1.Level3.net", "ae-42-90.car2.SanJose1.Level3.net", "pos-1-5-0-0-cr01.sanjose.ca.ibone.com", "te-1-11-0-3-ar01.sfsutro.ca.sfb.comcast.net", and "google.com".



Ndiff

```
# ndiff facebook-072410.xml facebook-072510.xml
69.63.176.68:
  PORT      STATE SERVICE  VERSION
-80/tcp    open  http     lighttpd 1.5.0
+80/tcp    open  http     nginx

video-ssl-03-06-ash1.fbcdn.net (69.63.186.53):
  PORT      STATE SERVICE  VERSION
-443/tcp   open  ssl/http lighttpd 1.5.0
+443/tcp   open  ssl/http nginx

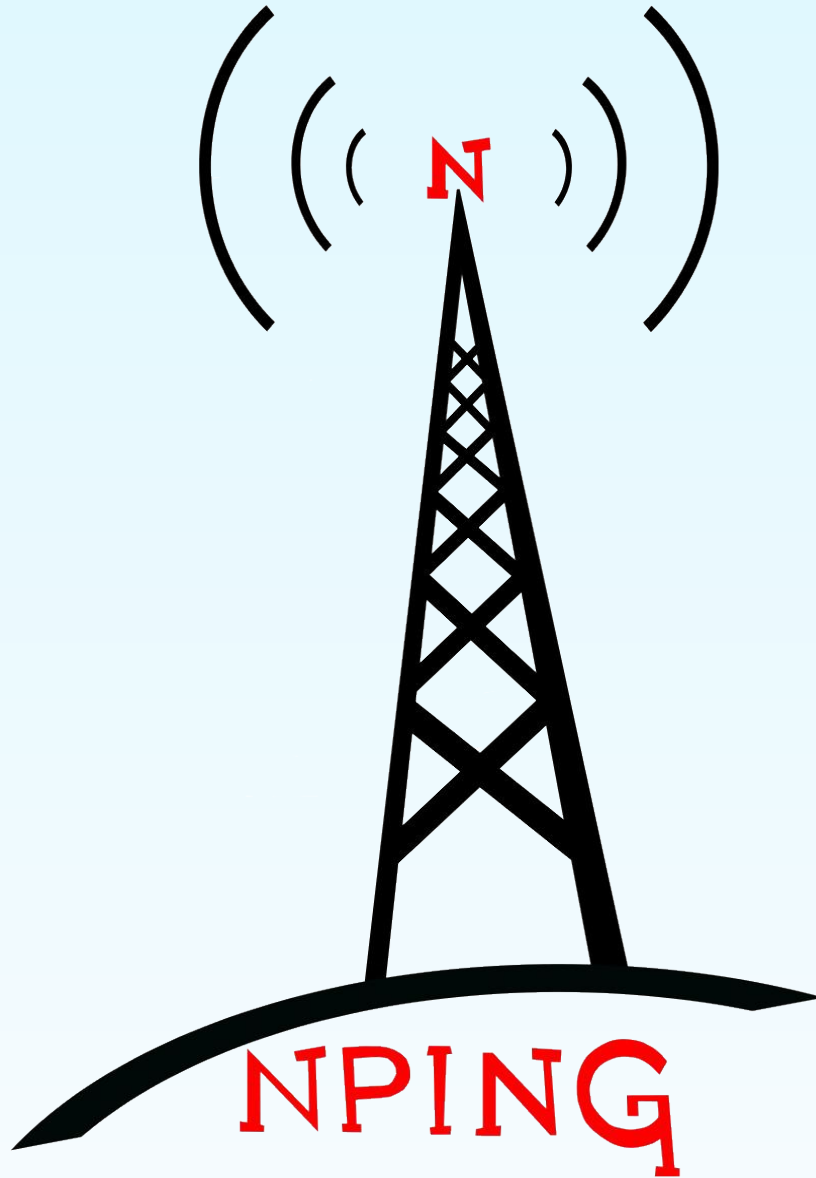
legacymail.thefacebook.com (66.220.144.49):
  PORT      STATE SERVICE  VERSION
443/tcp    open  ssl/http Microsoft IIS httpd 6.0
|_ html-title: Document Moved
-|_ Did not follow redirect to
https://mail.thefacebook.com/exchange
+|_ Did not follow redirect to
https://mail.thefacebook.com/exchange/
```




Ncat

<http://nmap.org/ncat/>







Resources:

Download Nmap for free: <http://nmap.org>

Contact me: fyodor@insecure.org

Slides for this talk: <http://nmap.org/presentations>

Questions?