Mastering the Nmap Scripting Engine

by Fyodor and David Fifield

http://insecure.org/presentations/BHDC10/

Black Hat Briefings Las Vegas
July 28; 4:45 PM; Augustus 5+6

Defcon 18
July 30; 5:00 PM; Track One

Outline

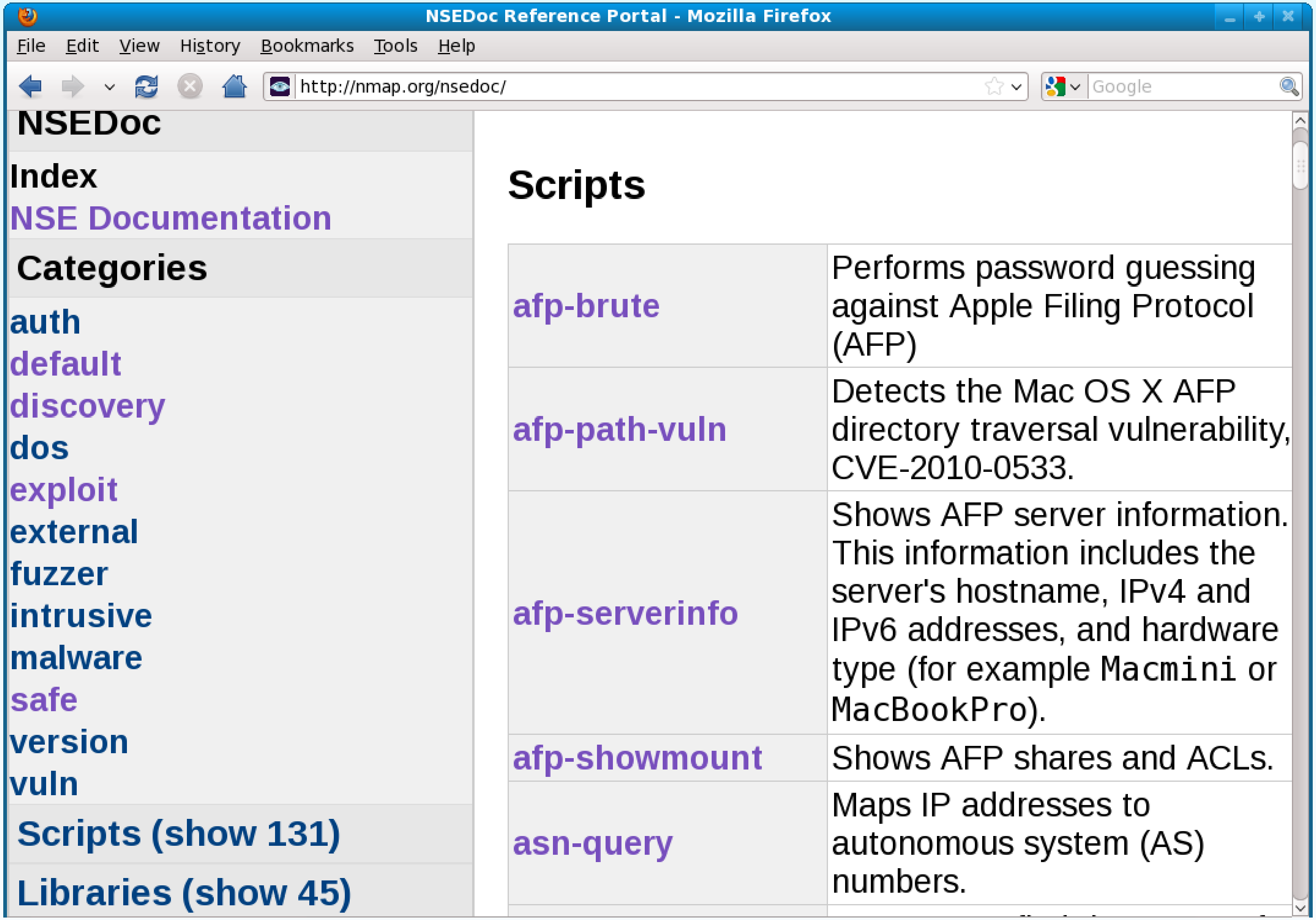
- NSE Intro & Usage
- Large-scale Scan #1: SMB/MSRPC
- Large-scale Scan #2: Favicon
- Writing NSE Scripts
- Live Script Writing Demo
- Nmap News
- Final Notes & Q/A

Nmap Scripting Engine

```
# nmap -A -T4 scanme.nmap.org

Starting Nmap 5.35DC18 ( http://nmap.org )
Nmap scan report for scanme.nmap.org (64.13.134.52)
Host is up (0.0018s latency).
Not shown: 995 filtered ports
PORT      STATE  SERVICE VERSION
22/tcp    open   ssh     OpenSSH 4.3 (protocol 2.0)
| ssh-hostkey: 1024
60:ac:4d:51:b1:cd:85:09:12:16:92:76:1d:5d:27:6e (DSA)
|_2048 2c:22:75:60:4b:c3:3b:18:a2:97:2c:96:7e:28:dc:dd (RSA)
53/tcp    open   domain
80/tcp    open   http    Apache httpd 2.2.3 ((CentOS))
|_html-title: Go ahead and ScanMe!
| http-methods: Potentially risky methods: TRACE
|_See http://nmap.org/nsedoc/scripts/http-methods.html
113/tcp   closed auth
31337/tcp closed Elite
OS details: Linux 2.6.13 - 2.6.31, Linux 2.6.18
Nmap done: 1 IP address (1 host up) scanned in 23.32 seconds
```

Pre-written Scripts and the NSEDoc Portal
http://nmap.org/nsedoc/


NSEDoc Reference Portal - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://nmap.org/nsedoc/
Google

NSEDoc

Index

NSE Documentation

Categories

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

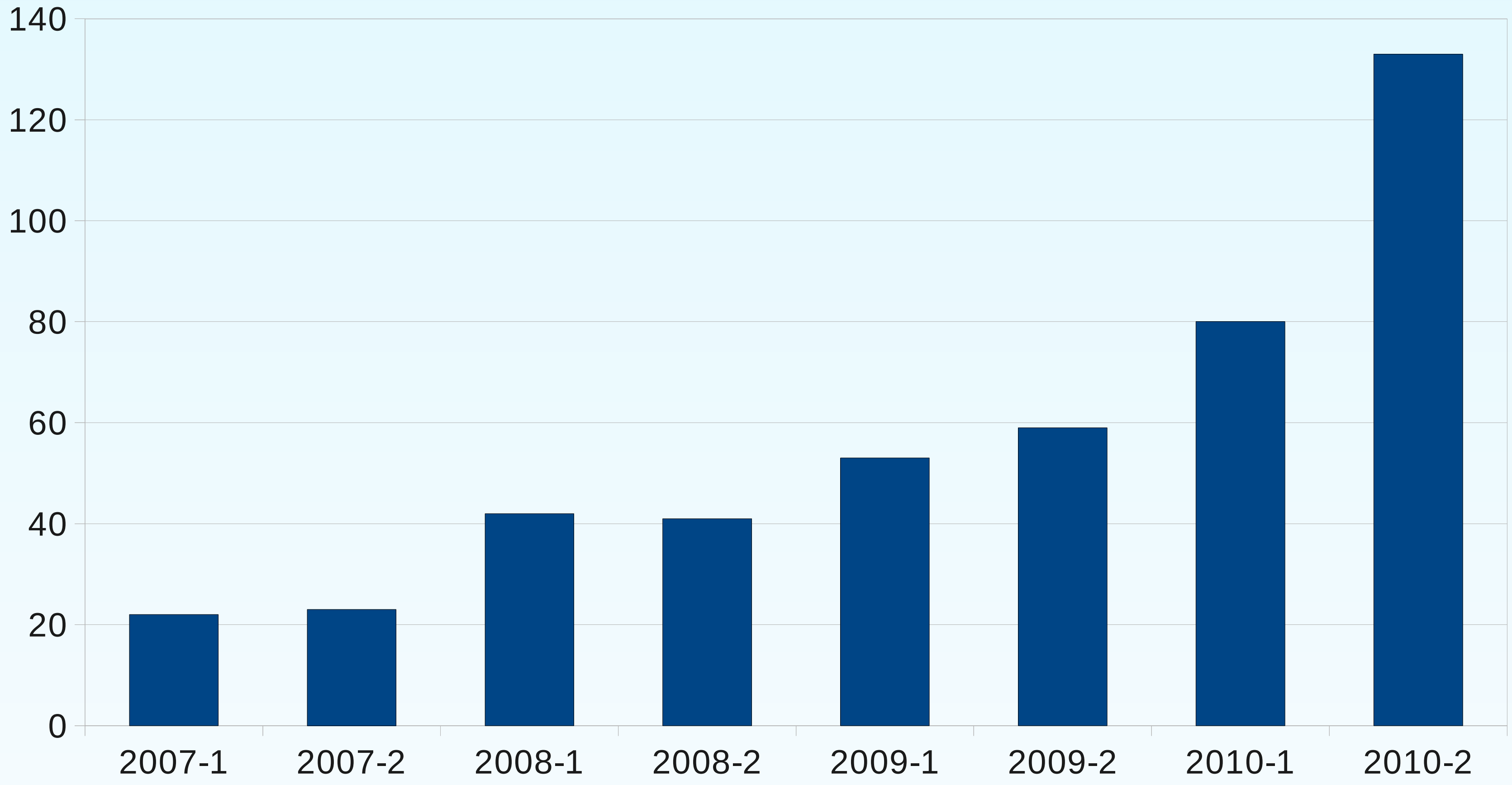
Scripts (show 131)

Libraries (show 45)

Scripts

afp-brute	Performs password guessing against Apple Filing Protocol (AFP)
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.
asn-query	Maps IP addresses to autonomous system (AS) numbers.

Script Collection Growth



Large Scale Scan #1: SMB/MSRPC Scripts

Ron Bowes spent months researching SMB/MSRPC protocols and wrote a suite of 13 scripts.

Informational: smb-os-discovery, smb-server-stats, smb-system-info, smb-security-mode

Detailed Enumeration: smb-enum-users, smb-enum-domains, smb-enum-groups, smb-enum-processes, smb-enum-sessions, smb-enum-shares

More intrusive: smb-brute, smb-check-vulns, smb-psexec

Who to test them out on?

MS Scan Details

- Step 1: Find target IP addresses. 1,004,632 located in ARIN DB.
- Step 2: Start broad version detection scan (nmap -T4 --top-ports 50 -sV -O --osscan-limit --osscan-guess --min-hostgroup 128 --host-timeout 10m -oA ms-vscan -iL ms.ips.lst)
  - – Found 74,293 hosts up out of 1M IPs in 26 hours
- Step 3: Examine results

MS SMB Scan Results

- Vast majority of MS networks block Windows ports such as 135 and 445 at their gateways.
- ... but not all!
- New scan: nmap -v -O -sV -T4 --osscan-guess -oA ms-smbscan --script=smb-enum-domains,smb-enum-processes,smb-enum-sessions,smb-enum-shares,smb-enum-users,smb-os-discovery,smb-security-mode,smb-system-info [Target Ips]
- Results

Humble Beginnings:
The Story of http-favicon.nse

A simple idea: fingerprint web applications by retrieving the favicon. Vlatko Kosturjak wrote a script to do it. (http://seclists.org/nmap-dev/2008/q4/397)

However, the database was small and of unknown quality. If only we had a tool to do large Internet scans... and a way to write scripts for it... (http://seclists.org/nmap-dev/2009/q3/462)

The favicon-survey.nse script (not part of the Nmap package) downloads favicons and stores them in the filesystem.

Results of the Favicon Survey

Scanned the external links of

- dmoz.org: 5,042,341
- en.wikipedia.org: 3,218,826
- de.wikipedia.org: 832,521
- fr.wikipedia.org: 652,040
- es.wikipedia.org: 532,951

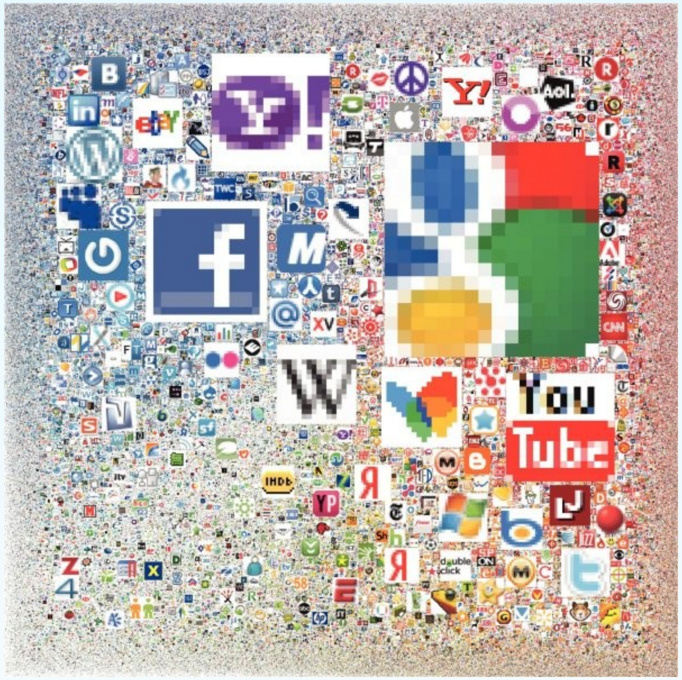
Omitting duplicates, around 8 million domains.

- 995,152 unique icons
- 799,924 image files
- 195,228 non-image files (HTML error pages)

> “Indeed, I have been scanning ;-)”
>
> —Brandon Enright (http:seclists.org/nmap-dev/2009/q3/487)

Favicon Visualization

A secondary survey: The Alexa top one million sites. Pack the icons tightly, with the size of each one proportional to its "reach."



http://nmap.org/favicon/

Writing NSE Scripts

Introduction to Lua & Why We Chose It

- Lightweight embeddable scripting language
  - Easy to learn
  - Tiny to embed: “Complete distribution (source code, manual, plus binaries for some platforms) fits comfortably on a floppy disk”.
- Widely used, known, and debugged
  - Created in Brazil in 1993, still actively developed
  - Best known for its use in the game industry: World of Warcraft, Crysis, etc.
  - Security tools: Nmap, Wireshark, Snort 3.0

Why We Chose Lua (Continued)

- Extensible
  - – Hooked to Nmap's fast parallel networking libraries
- Safe & Secure
  - – No buffer overflows, format string vulns, etc.
- Portable
  - – Windows, Linux, Mac, *BSD, etc.
- Interpreted

Capabilities Added by Nmap

- Protocol/helper libraries
  - 45, including DNS, HTTP, MSRPC, Packet, SNMP, unpwdb, etc.
- Protocol brute forcers
- Easy SSL
- Dependencies

Script Example #1: rpcinfo

Script Example #2: smb-enum-users

Live Script Demonstration

Problem: Find my webcam on a dynamic IP address.

The webcam uses thttpd to serve /cam.jpg, so use a script to check those two things.

Make it a Production Script

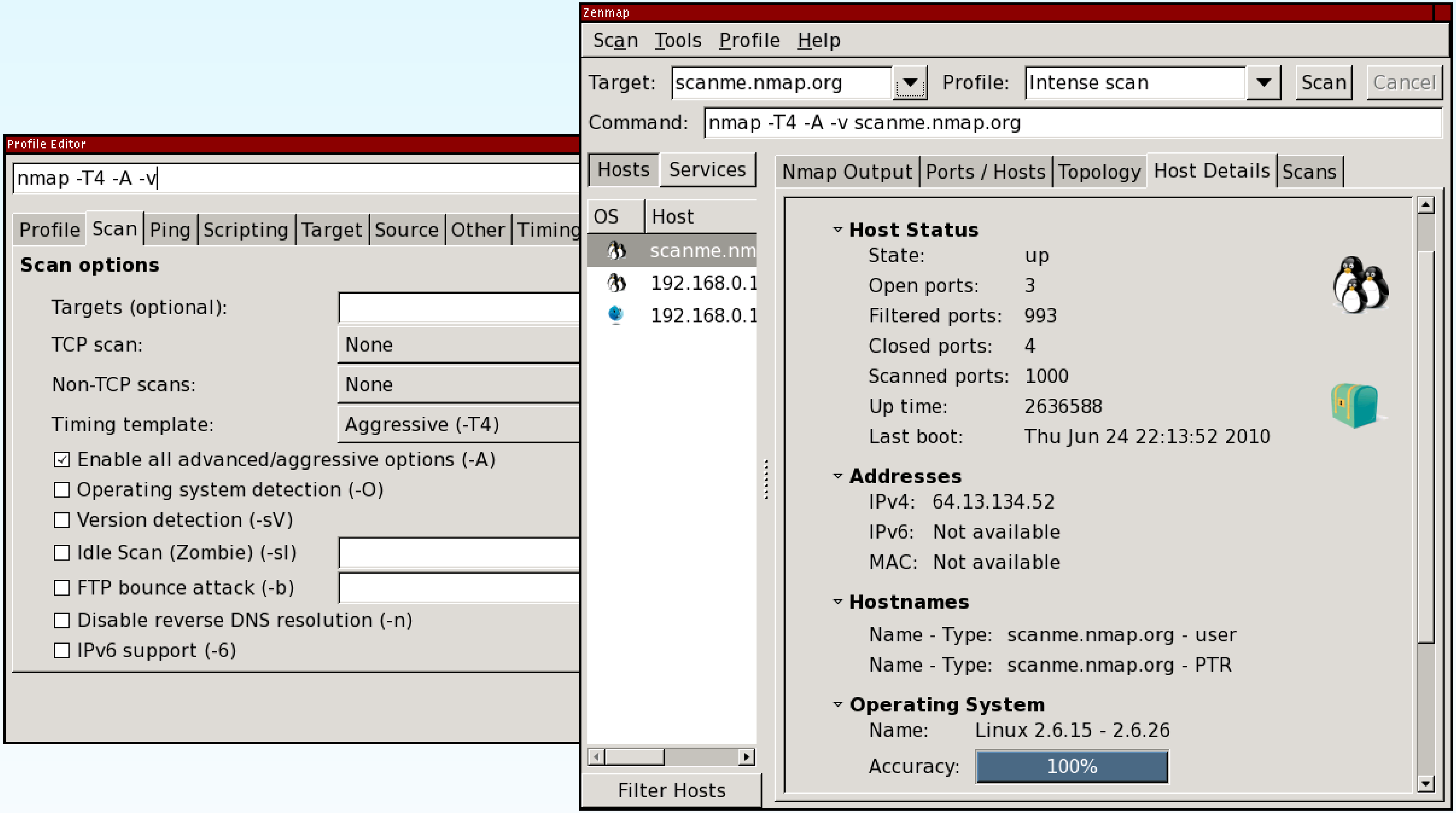
To turn http-brute into distribution-ready script, I would next

- expand the portrule to match more HTTP services,
- add script arguments to control the path retrieved and the method used,
- add NSEDoc @usage and @output examples, and
- let it cache credentials for other scripts to use.

What's Coming in NSE?

- Prerules & Postrules
- Target Acquisition Scripts
- Lots more scripts! Current queue:
  - Vnc-info (Patrik Karlsson)
  - Vnc-brute (Patrik Karlsson)
  - Svn-brute (Patrik Karlsson)
  - Hostmap (Ange Gutek)
  - Http-xst (Eduardo Garcia Melia)
  - Rmi-dumpregistry (Martin Swende)

Zenmap NSE Integration



```
nmap -T4 -A -v
```

Scan options

Targets (optional):

TCP scan: None

Non-TCP scans: None

Timing template: Aggressive (-T4)

- ☑ Enable all advanced/aggressive options (-A)
- ☐ Operating system detection (-O)
- ☐ Version detection (-sV)
- ☐ Idle Scan (Zombie) (-sI)
- ☐ FTP bounce attack (-b)
- ☐ Disable reverse DNS resolution (-n)
- ☐ IPv6 support (-6)

Target: scanme.nmap.org

Profile: Intense scan

Command:

```
nmap -T4 -A -v scanme.nmap.org
```

OS	Host
	scanme.nm
	192.168.0.1
	192.168.0.1

Host Status

State:	up
Open ports:	3
Filtered ports:	993
Closed ports:	4
Scanned ports:	1000
Up time:	2636588
Last boot:	Thu Jun 24 22:13:52 2010

Addresses

IPv4:	64.13.134.52
IPv6:	Not available
MAC:	Not available

Hostnames

Name - Type:	scanme.nmap.org - user
Name - Type:	scanme.nmap.org - PTR

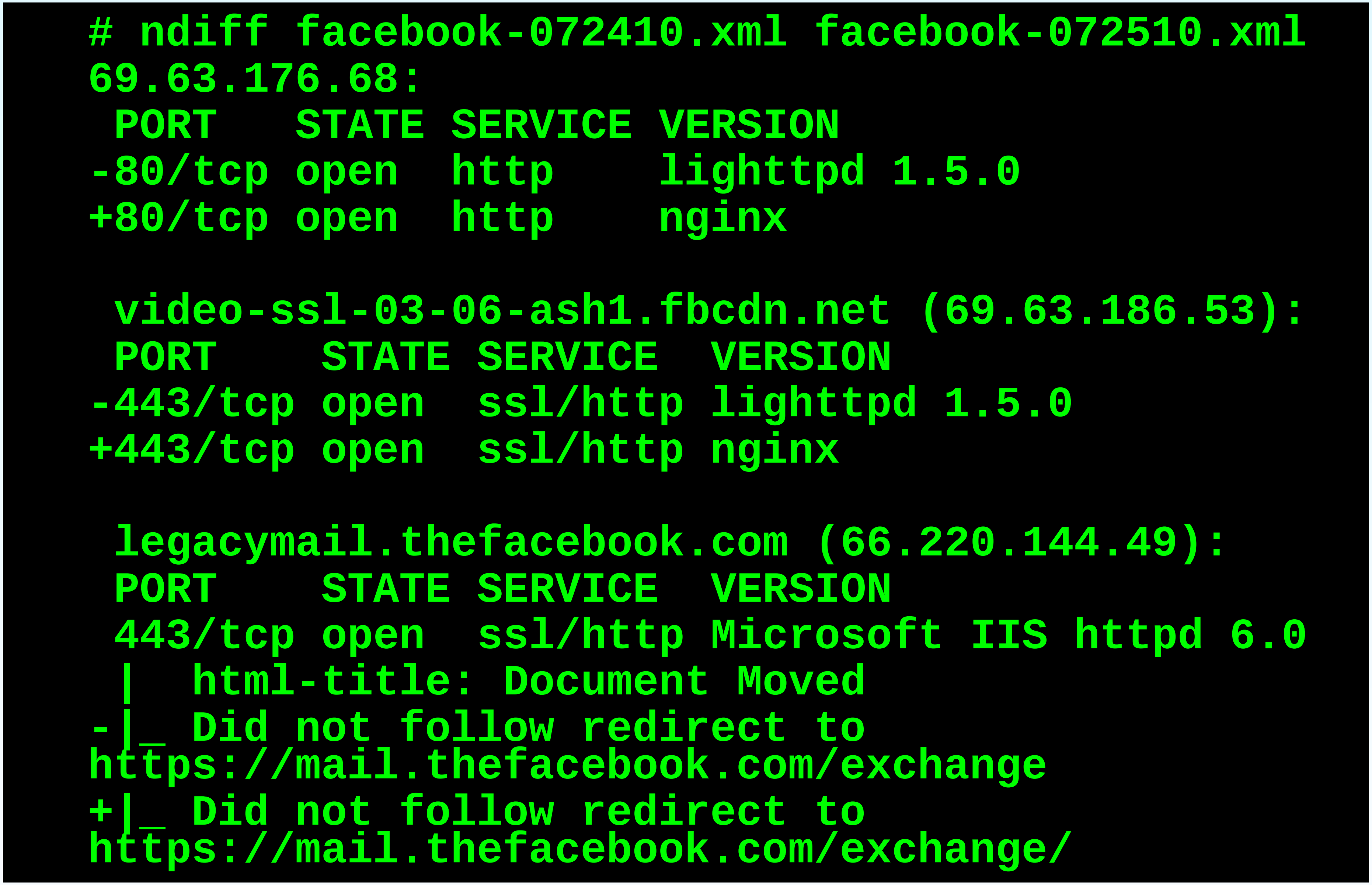
Operating System

Name:	Linux 2.6.15 - 2.6.26
Accuracy:	100%

NMAP NEWS!

A bridge declarer can be
like that, except the puddles
In a maximum of
his opening bid. South
hand with a diamond
the club queen on
conditions found
had as many
the SEC

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/
```

Simple Ndiff Cron Script

```
#!/bin/sh
date=`date "+%s"`
cd /hack/facebook/scripts/
nmap -T4 -F -sV -O --osscan-limit --osscan-guess -oA facebook-${date} [netblocks]  > /dev/null
ndiff facebook-old.xml facebook-${date}.xml > facebook-diff-${date}
cp facebook-${date}.xml facebook-old.xml
printf "\n*********** NDIFF RESULTS ***********\n"
cat facebook-vscan-diff-${date}
printf "\n*********** SCAN RESULTS ***********\n"
cat facebook-vscan-${date}.nmap
```

Ncat

http://nmap.org/ncat/

```
  .       .
  \`_"'"_'/
   } 6 6 {
  ==. Y ,==
    /^^^\  .
   /     \  )
  (  )-(  )/     _
  _""___""___   /
 /   Ncat    \_/
(     ____
 \_.=|____E
```

Modern Networking Features

- SSL encryption support (client or server)
- Proxy (act as proxy server, or client chaining through multiple proxies)
- Portability
- TCP/UDP port redirection
- IPv6
- Fine-grained access control
- Connection brokering
- Missing feature

Ncat Chat

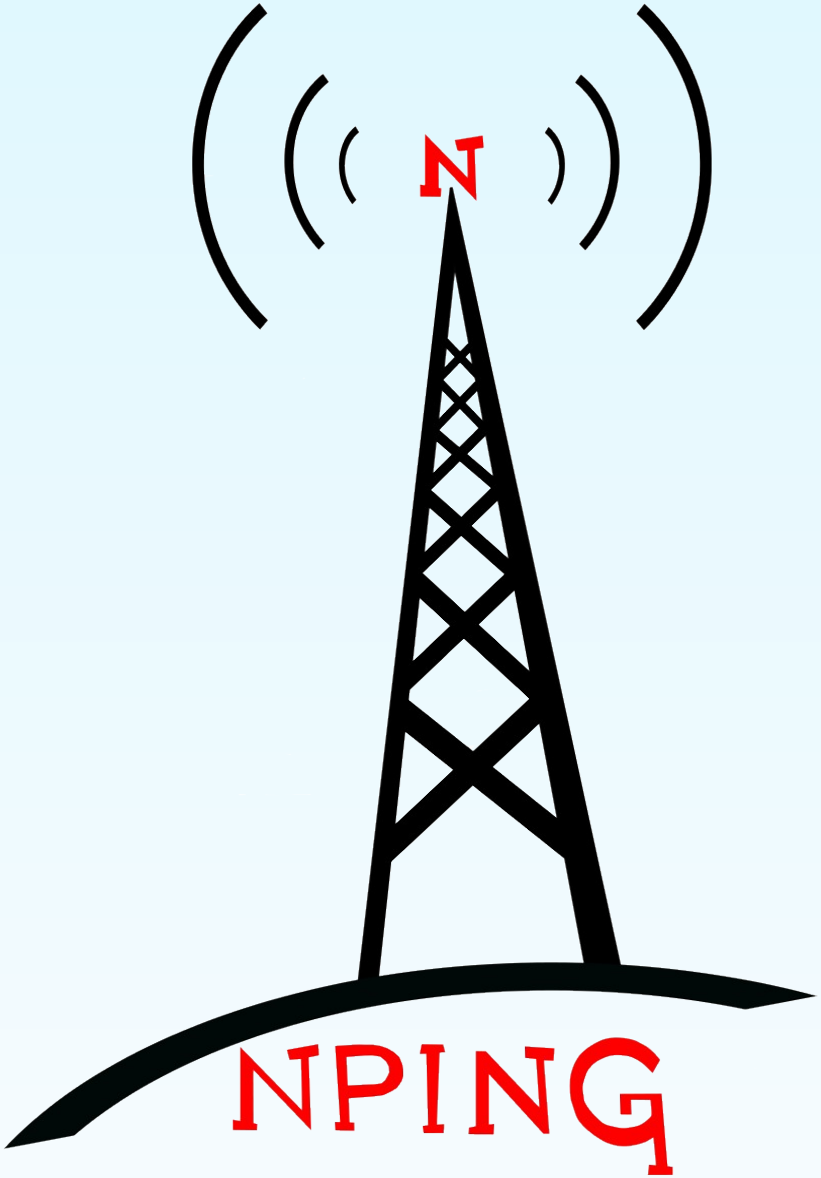
A slight hack to broker mode enables a very rudimentary chat server.

Official chat server for this presentation:

```
ncat --ssl -v chat.nmap.org
```

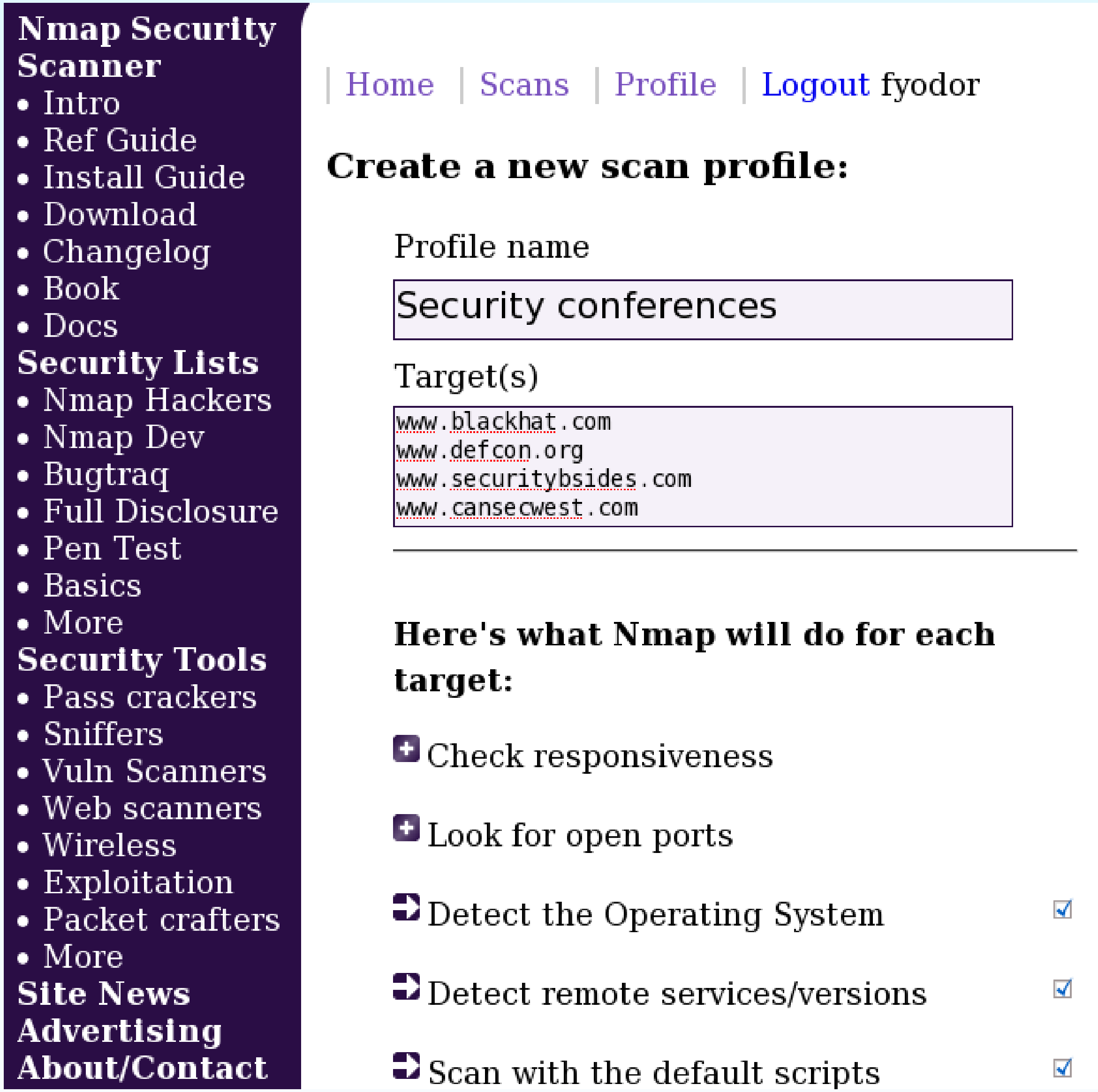
Server was started with command:

```
ncat -l --ssl --chat chat.nmap.org
```


N
NPING

Ncrack

Rainmap: An Online Scanning Service



Nmap Security Scanner
- Intro
- Ref Guide
- Install Guide
- Download
- Changelog
- Book
- Docs

Security Lists
- Nmap Hackers
- Nmap Dev
- Bugtraq
- Full Disclosure
- Pen Test
- Basics
- More

Security Tools
- Pass crackers
- Sniffers
- Vuln Scanners
- Web scanners
- Wireless
- Exploitation
- Packet crafters
- More

Site News
Advertising
About/Contact

| Home | Scans | Profile | Logout fyodor

Create a new scan profile:

Profile name

Security conferences

Target(s)

```
www.blackhat.com
www.defcon.org
www.securitybsides.com
www.cansecwest.com
```

Here's what Nmap will do for each target:

⊞ Check responsiveness

⊞ Look for open ports

➲ Detect the Operating System ☑

➲ Detect remote services/versions ☑

➲ Scan with the default scripts ☑

Nmap Script Authors

Aaron Leininger
Andrew Orr
Ange Gutek
Arturo Busleiman
Bernd Stroessenreuther
Brandon Enright
David Fifield
Diman Todorov
Djalal Harouni
Doug Hoyte
Duarte Silva
Eddie Bell
Eugene V. Alexeev
Felix Groebert
Ferdy Riphagen
Jah
Jason DePriest
Joao Correa
Kris Katterjohn
Mak Kolybabi
Marek Majkowski
Martin Swende
Matthew Boyle
Michael Pattrick
Michael Schierl
Patrik Karlsson
Philip Pickering
Richard Sammet
Rob Nicholls
Ron Bowes
Sven Klemm
Thomas Buchanan
Tom Sellers
Vladz
Vlatko Kosturjak

Final Notes

- Ron Bowes at Black Hat Arsenal
  - Thursday, Station 5, 8:00 AM – 12:30 PM
- Slides to be posted Friday (and video as soon as we get it) to: http://insecure.org/presentations/
- Download Nmap from: http://nmap.org
- NSEDoc portal: http://nmap.org/nsedoc/
- NSE system docs: http://nmap.org/book/nse.html

Questions?