Nmap: Scanning the Internet

by Fyodor

Black Hat Briefings USA – August 6, 2008; 10AM
Defcon 16 – August 8, 2008; 4PM

Scan Goals

- Collect empirical data and use it to enhance Nmap functionality.
- Use the data to help knowlededeable people make your scans more effective.
- Detect and resolve Nmap bugs and performance issues through the large-scale scanning.
- Demonstrate techniques useful for routine scans as well as wide-scale Internet scanning.

Scan Challenges: Determining the IP addresses to Scan

- Dozens of large but targeted scans rather than one giant scan.
- Many options: BGP routing tables, DNS zone files, registry allocation, etc.
- Nmap's own random IP generation:

  -
    ```
    nmap -iR 25200000 -sL -n | grep "not scanned" | awk '{print $2}' | sort -n | uniq >! tp; head -25000000 tp >! 25M-IPs; rm tp
    ```

Scan Challenges:
Scan Source

- P2P scanning?
- Legal issues
- ISP response
- US Department of Defense response
  - DoD JTF-GNO: Joint Task Force for Global Network Operations

Scan Challenges: Firewalls

- Network conditions often differ significantly behind firewalls vs. Internet scanning
- Contributed data

Scan Challenges: Performance and Accuracy

- Internet scanning is long, hard work. Can be disheartening:

  -
    ```
    Stats: 93:57:40 elapsed; 254868 hosts completed (2048 up), 2048 undergoing UDP Scan
    UDP Scan Timing: About 11.34% done; ETC: 03:21 (-688:-41:-48 remaining)
    ```
- Finding and resolving performance and accuracy problems is a key goal.

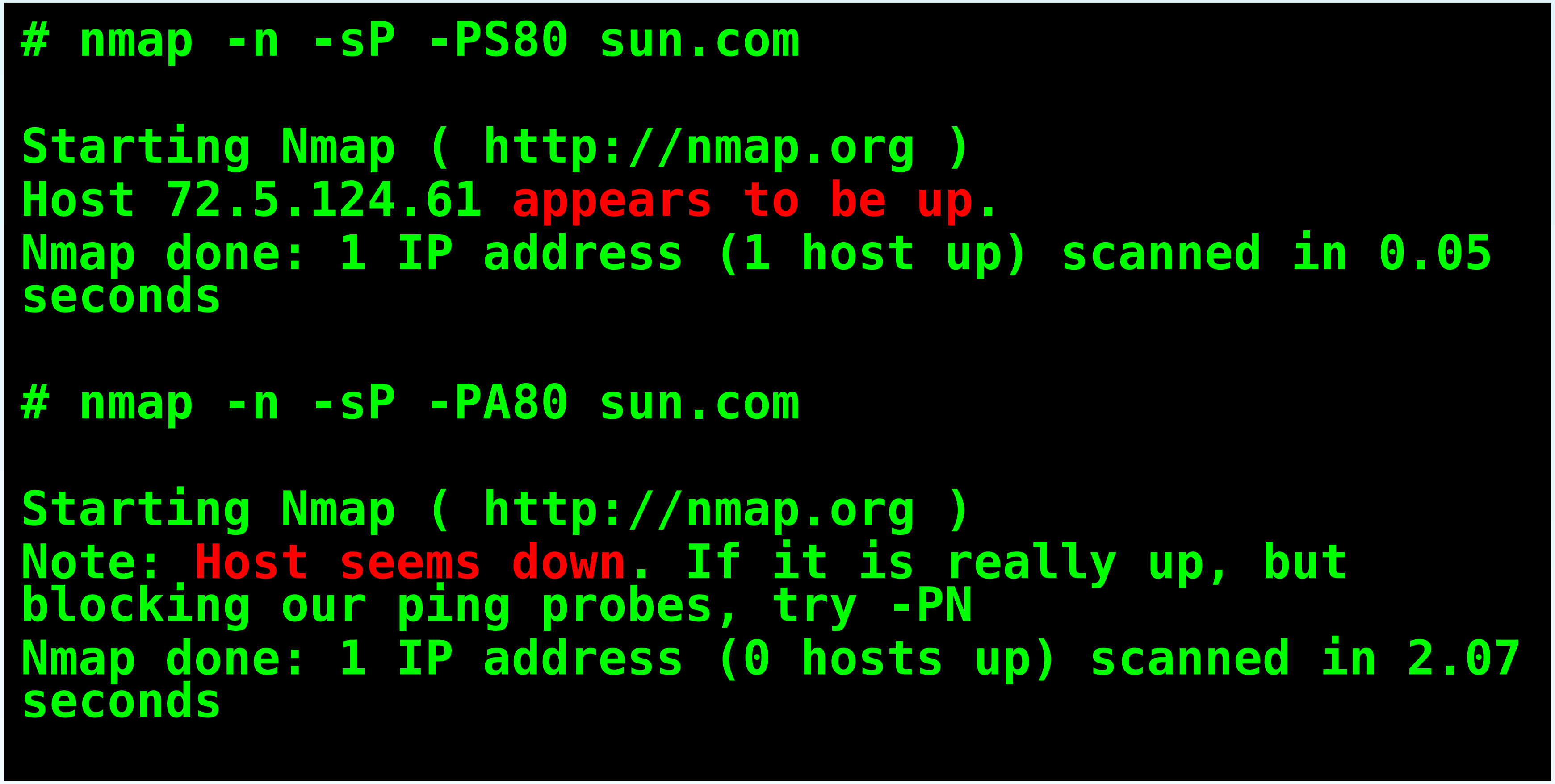
Optimizing Host Discovery

- Goals
- Big challenge: Deciding on discovery methods
- Echo requests and even Nmap default discovery (TCP ACK to port 80 & echo request) are often insufficient for Internet scanning.

TCP Host Discovery Methods (-PS, -PA)

- SYN packet discovery (-PS)
  - Best against stateful filrewalls
- ACK packet discovery (-PA)
  - Best against stateless firewalls

TCP Host Discovery Example



```
# nmap -n -sP -PS80 sun.com

Starting Nmap ( http://nmap.org )
Host 72.5.124.61 appears to be up.
Nmap done: 1 IP address (1 host up) scanned in 0.05
seconds

# nmap -n -sP -PA80 sun.com

Starting Nmap ( http://nmap.org )
Note: Host seems down. If it is really up, but
blocking our ping probes, try -PN
Nmap done: 1 IP address (0 hosts up) scanned in 2.07
seconds
```

TCP Host Discovery Methods: Top Ports

- Adding more TCP SYN and ACK probes can help, but which ports work the best?

Top 10 TCP Host Discovery Ports

- 80/http
- 25/smtp
- 22/ssh
- 443/https
- 21/ftp
- 113/auth
- 23/telnet
- 53/domain
- 554/rtsp
- 3389/ms-term-server

UDP Host Discovery (-PU)

- Closed ports better than open one because they are more likely to respond.
- Port 53 often worthwhile due to firewall exceptions for DNS.

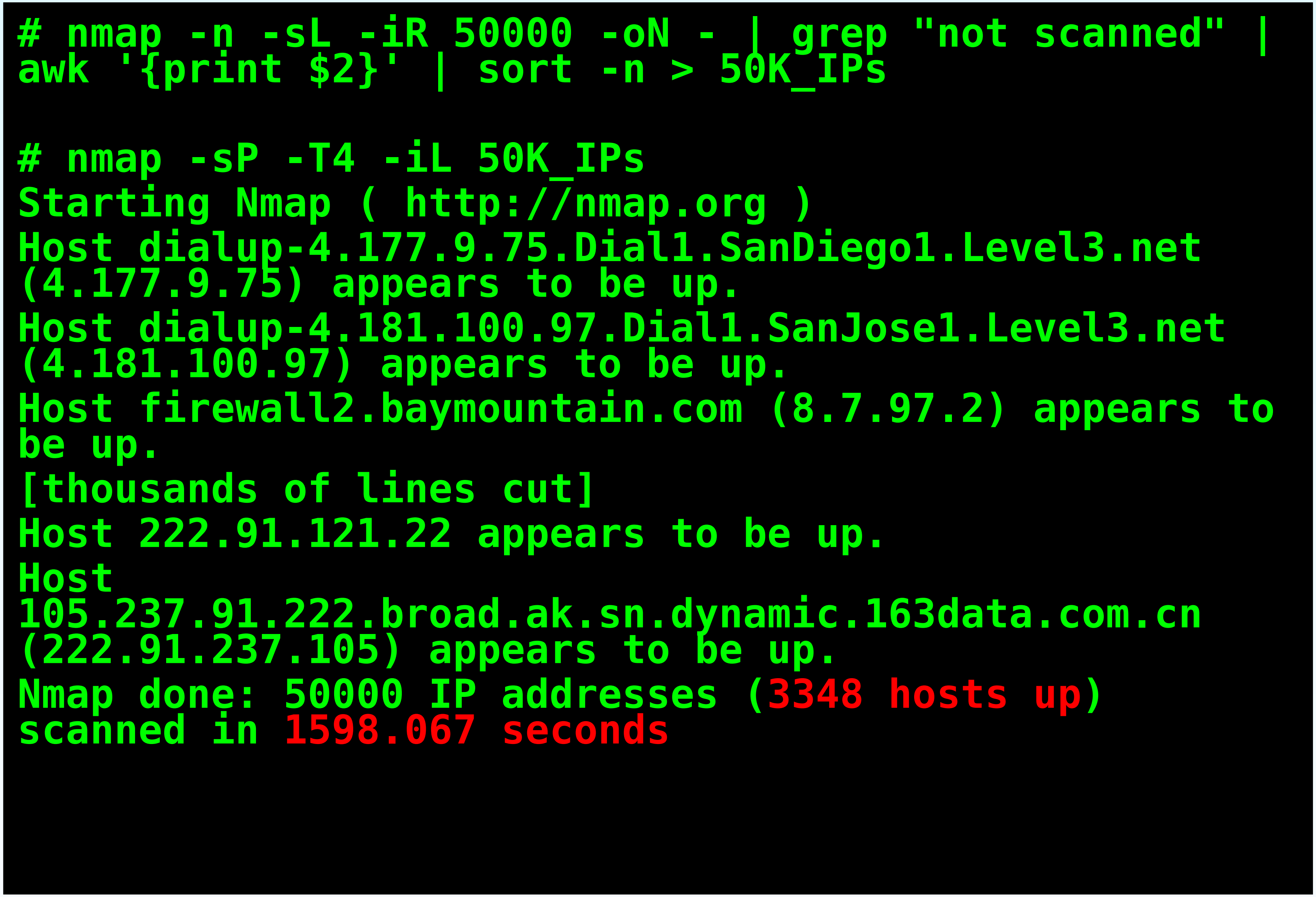
ICMP Host Discovery Methods (-PE, -PM, -PP)

- Some systems intentionally allow echo requests, but block the others.
- Others block echo requests explicitly, but forget about netmask/timestamp requests.
- Solution: Use both – echo request and one of the other two.

Protocol Ping (-PO)

- Default is to send 3 probes, for protocols 1 (ICMP), 2 (IGMP), and 4 (IP-in-IP)

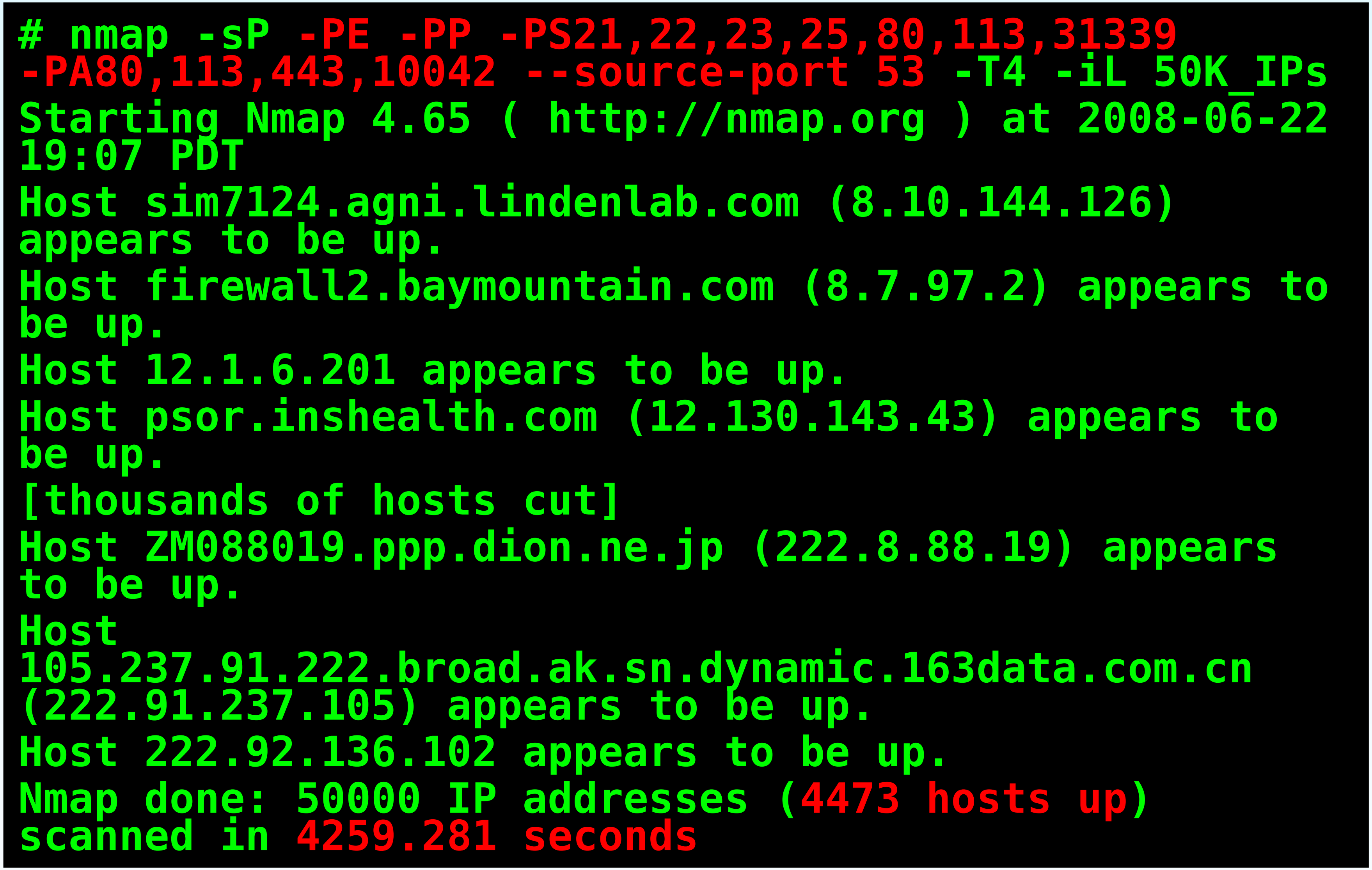
Default Host Discovery Effectiveness



```
# nmap -n -sL -iR 50000 -oN - | grep "not scanned" |
awk '{print $2}' | sort -n > 50K_IPs

# nmap -sP -T4 -iL 50K_IPs
Starting Nmap ( http://nmap.org )
Host dialup-4.177.9.75.Dial1.SanDiego1.Level3.net
(4.177.9.75) appears to be up.
Host dialup-4.181.100.97.Dial1.SanJose1.Level3.net
(4.181.100.97) appears to be up.
Host firewall2.baymountain.com (8.7.97.2) appears to
be up.
[thousands of lines cut]
Host 222.91.121.22 appears to be up.
Host
105.237.91.222.broad.ak.sn.dynamic.163data.com.cn
(222.91.237.105) appears to be up.
Nmap done: 50000 IP addresses (3348 hosts up)
scanned in 1598.067 seconds
```

Enhanced Host Discovery Effectiveness



```
# nmap -sP -PE -PP -PS21,22,23,25,80,113,31339
-PA80,113,443,10042 --source-port 53 -T4 -iL 50K_IPs
Starting Nmap 4.65 ( http://nmap.org ) at 2008-06-22
19:07 PDT
Host sim7124.agni.lindenlab.com (8.10.144.126)
appears to be up.
Host firewall2.baymountain.com (8.7.97.2) appears to
be up.
Host 12.1.6.201 appears to be up.
Host psor.inshealth.com (12.130.143.43) appears to
be up.
[thousands of hosts cut]
Host ZM088019.ppp.dion.ne.jp (222.8.88.19) appears
to be up.
Host
105.237.91.222.broad.ak.sn.dynamic.163data.com.cn
(222.91.237.105) appears to be up.
Host 222.92.136.102 appears to be up.
Nmap done: 50000 IP addresses (4473 hosts up)
scanned in 4259.281 seconds
```

Enhanced Discovery Results

- Enhanced discovery:
  - took 71 minutes vs. 27 (up 167%)
  - Found 1,125 more live hosts (up 34%)

Upgrade your Nmap

- Many bug fixes and performance improvements in version 4.68. See http://nmap.org/changelog.html
- For even newer, try the svn release. See http://nmap.org/book/install.html#inst-svn
- For all the goods in this presentation:

```
svn co –username guest –password “”
svn://svn.insecure.org/nmap-exp/bhdc08
```

Top Ports Project

- A massive scan of millions of Internet IPs to determine most commonly open TCP and UDP ports.
- Some large organizations also contributed scan data to give a behind-the-firewall perspective.
- nmap-services file augmented with frequency data for each port.

Default Scan Ports

- In Nmap 4.68: 1715 ports for TCP scans, plus 1488 for UDP scans. Ports 1-1024, plus all named ports above that.
- With augmented nmap-services: Top 1000 ports for each protocol. Finishes faster, and often finds more open ports.

Fast Scan (-F) Ports

- In Nmap 4.68: 1276 ports for TCP scans, plus 1017 for UDP scans. Includes all named ports.
- With augmented nmap-services: Top 100 ports for each protocol.

Fast Scan Example Times

- Nmap -sUV -F -T4 scanme.nmap.org
  - With 4.68: 1 hour, 2 minutes, 62 seconds
  - With bhdc08: 6 minutes, 29 seconds
  - With bhdc08 & “--version-intensity 0”: 13 sec
  - All three found the same open port (53)

New –top-ports and –port-ratio features

- --top-ports <n> scans the most commonly open <n> ports for each protocol requested.
- --port-ratio <n> (where <n> is between 0 and 1) scans all ports with a frequency of at least the given level.

Top 10 TCP ports

- 80 (http)
- 23 (telnet)
- 22 (ssh)
- 443 (https)
- 3389 (ms-term-serv)
- 445 (microsoft-ds)
- 139 (netbios-ssn)
- 21 (ftp)
- 135 (msrpc)
- 25 (smtp)

TCP effectiveness of –top-port values

- --top-ports 10: 48%
- --top-ports 50: 65%
- --top-ports 100: 73%
- --top-ports 250: 83%
- --top-ports 500: 89%
- --top-ports 1000: 93%
- --top-ports 2000: 96%
- --top-ports 3674: 100%

Top 10 UDP ports

- 137 (netbios-ns)
- 161 (snmp)
- 1434 (ms-sql-m)
- 123 (ntp)
- 138 (netbios-dgm)
- 445 (microsoft-ds)
- 135 (msrpc)
- 67 (dhcps)
- 139 (netbios-ssn)
- 53 (domain)

UDP effectiveness of –top-port values

- --top-ports 10: 50%
- --top-ports 50: 86%
- --top-ports 100: 90%
- --top-ports 250: 94%
- --top-ports 500: 97%
- --top-ports 1017: 100%
- Note: -p- UDP data not yet available

Packet Rate Control

- --min-rate <packets per second>
- --max-rate <packets per second>

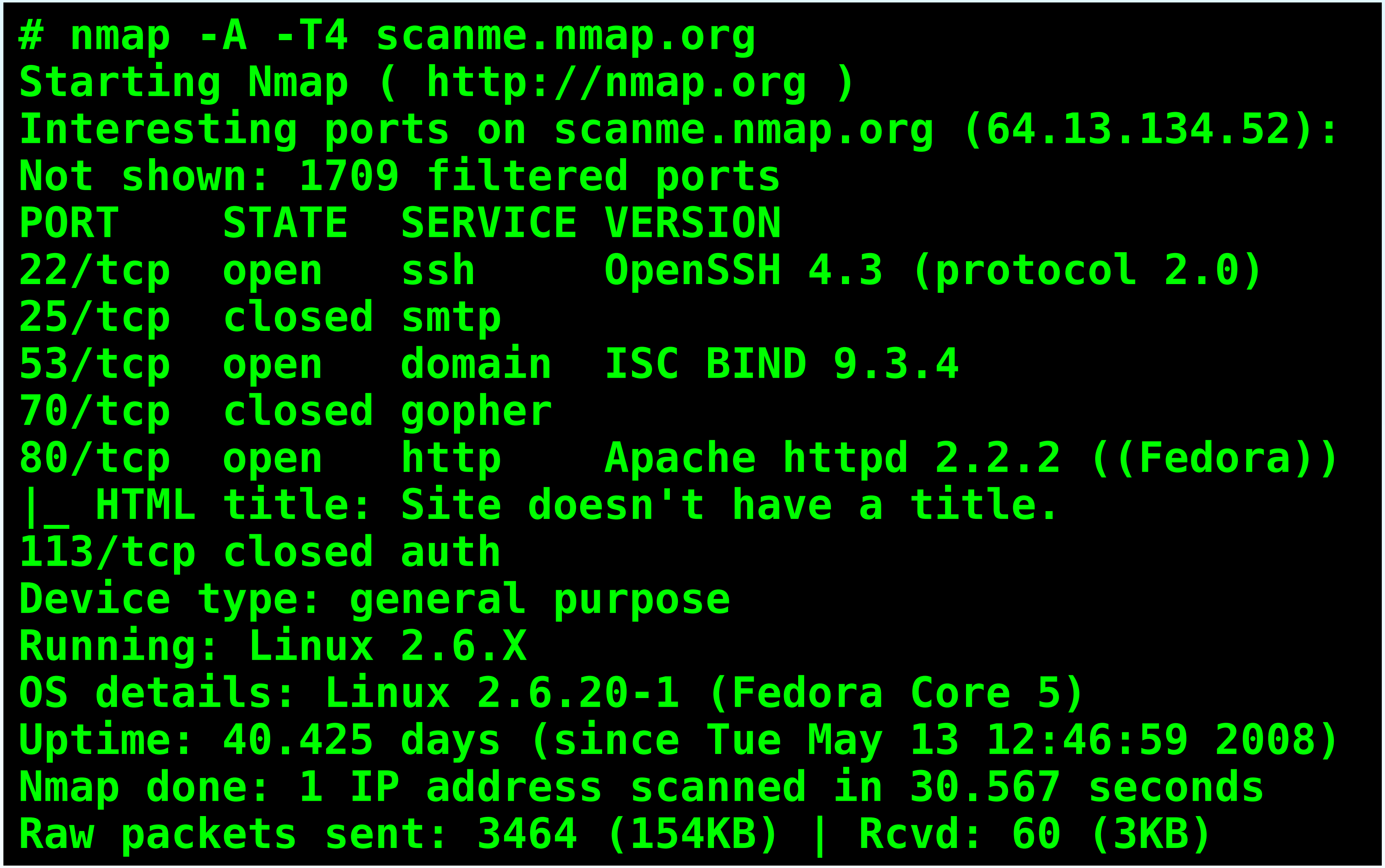
```
nmap –min-rate 500 scanme.nmap.org
```

Putting it all Together

```
nmap -S [srcip] -d --max-scan-delay 10
-oA logs/tcp-allports-%T-%D -iL tcp-
allports-1M-IPs --max-retries 1
--randomize-hosts -p-
-PS21,22,23,25,53,80,443 -T4 --min-
hostgroup 256 --min-rate 175 –max-rate
300
```

Nmap News!

Nmap Scripting Engine (NSE)



```
# nmap -A -T4 scanme.nmap.org
Starting Nmap ( http://nmap.org )
Interesting ports on scanme.nmap.org (64.13.134.52):
Not shown: 1709 filtered ports
PORT    STATE  SERVICE VERSION
22/tcp  open   ssh     OpenSSH 4.3 (protocol 2.0)
25/tcp  closed smtp
53/tcp  open   domain  ISC BIND 9.3.4
70/tcp  closed gopher
80/tcp  open   http    Apache httpd 2.2.2 ((Fedora))
|_ HTML title: Site doesn't have a title.
113/tcp closed auth
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.20-1 (Fedora Core 5)
Uptime: 40.425 days (since Tue May 13 12:46:59 2008)
Nmap done: 1 IP address scanned in 30.567 seconds
Raw packets sent: 3464 (154KB) | Rcvd: 60 (3KB)
```

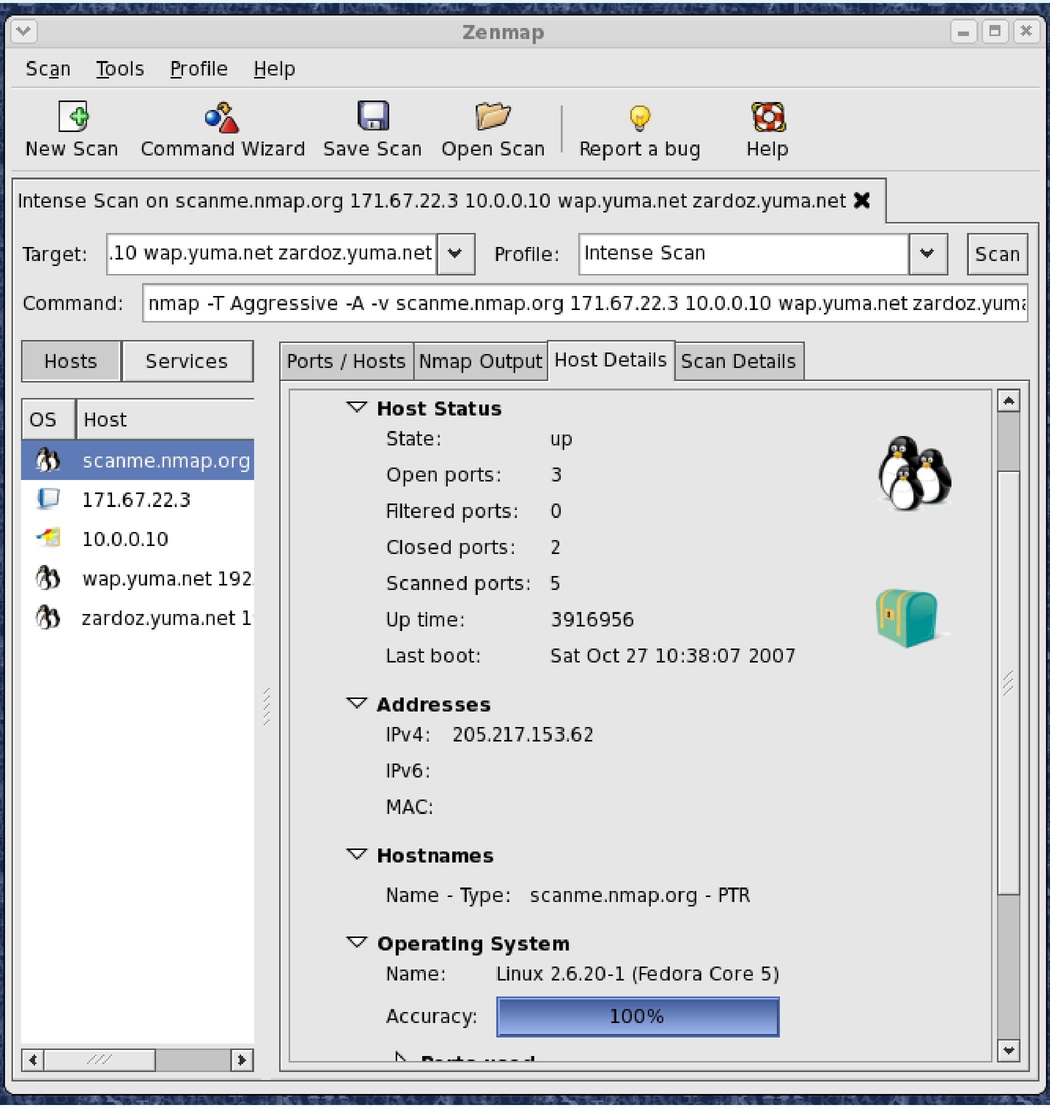
NSE Demo

```
# ./nmap -PN -v -sU -p53 -T4 --script=dns-test-open-
recursion,dns-safe-recursion-port.nse,dns-safe-recursion-
txid.nse dns-1.blackhat.com archimedes.shmoo.com

Interesting ports on dns-1.blackhat.com (216.231.63.55):
PORT   STATE SERVICE
53/udp open  domain
|_ DNS source port randomness: ERROR: Server refused
recursion
|_ DNS TXID randomness: ERROR: Server refused recursion

Interesting ports on archimedes.shmoo.com (12.21.210.234):
PORT   STATE SERVICE
53/udp open  domain
|_ Nameserver open recursive querys (CVE-1999-0024) (BID
136, 678): Recursion seems enabled
|_ DNS source port randomness: 12.21.210.234 is GREAT: 51
queries in 3.2 seconds from 51 ports with std dev 16099
|_ DNS TXID randomness: 12.21.210.234 is GREAT: 52 queries
in 3.3 seconds from 52 txids with std dev 20996
```

Zenmap GUI



Intense Scan on scanme.nmap.org 171.67.22.3 10.0.0.10 wap.yuma.net zardoz.yuma.net

Target: .10 wap.yuma.net zardoz.yuma.net

Profile: Intense Scan

Command: nmap -T Aggressive -A -v scanme.nmap.org 171.67.22.3 10.0.0.10 wap.yuma.net zardoz.yuma

OS	Host
	scanme.nmap.org
	171.67.22.3
	10.0.0.10
	wap.yuma.net 192
	zardoz.yuma.net 1

Host Status

State: up
Open ports: 3
Filtered ports: 0
Closed ports: 2
Scanned ports: 5
Up time: 3916956
Last boot: Sat Oct 27 10:38:07 2007

Addresses

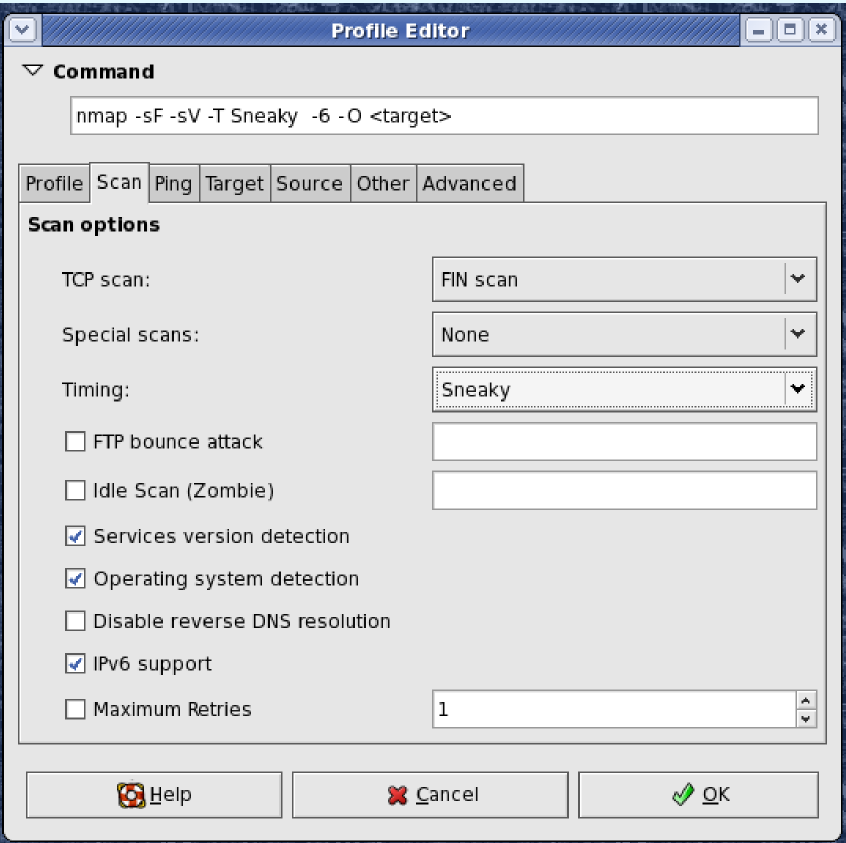
IPv4: 205.217.153.62
IPv6:
MAC:

Hostnames

Name - Type: scanme.nmap.org - PTR

Operating System

Name: Linux 2.6.20-1 (Fedora Core 5)
Accuracy: 100%



Command

nmap -sF -sV -T Sneaky -6 -O <target>

Scan options

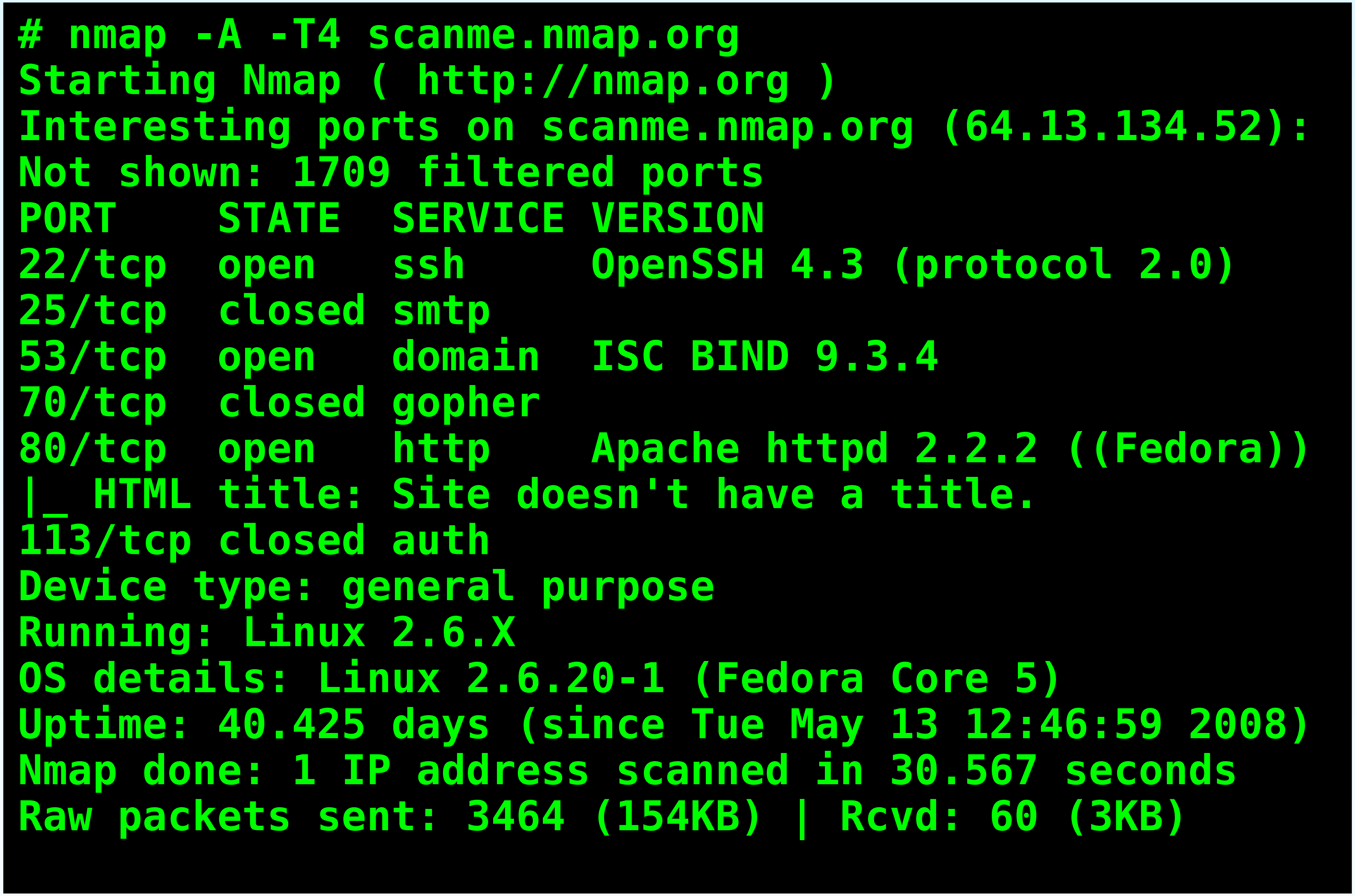
TCP scan: FIN scan
Special scans: None
Timing: Sneaky
☐ FTP bounce attack
☐ Idle Scan (Zombie)
☑ Services version detection
☑ Operating system detection
☐ Disable reverse DNS resolution
☑ IPv6 support
☐ Maximum Retries 1

2nd Generation OS Detection

```
# nmap -A -T4 scanme.nmap.org
[...]
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.20-1 (Fedora Core 5)
```

More info:
http://nmap.org/book/osdetect.html

Version Detection



```
# nmap -A -T4 scanme.nmap.org
Starting Nmap ( http://nmap.org )
Interesting ports on scanme.nmap.org (64.13.134.52):
Not shown: 1709 filtered ports
PORT    STATE  SERVICE VERSION
22/tcp  open   ssh     OpenSSH 4.3 (protocol 2.0)
25/tcp  closed smtp
53/tcp  open   domain  ISC BIND 9.3.4
70/tcp  closed gopher
80/tcp  open   http    Apache httpd 2.2.2 ((Fedora))
|_ HTML title: Site doesn't have a title.
113/tcp closed auth
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.20-1 (Fedora Core 5)
Uptime: 40.425 days (since Tue May 13 12:46:59 2008)
Nmap done: 1 IP address scanned in 30.567 seconds
Raw packets sent: 3464 (154KB) | Rcvd: 60 (3KB)
```

--reason

```
# nmap --reason -T4 scanme.nmap.org
[...]
Interesting ports on scanme.nmap.org
(205.217.153.62):
Not shown: 1709 filtered ports
Reason: 1709 no-responses
PORT    STATE  SERVICE REASON
22/tcp  open   ssh     syn-ack
25/tcp  closed smtp    reset
53/tcp  open   domain  syn-ack
70/tcp  closed gopher  reset
80/tcp  open   http    syn-ack
113/tcp closed auth    reset
```

--packet-trace

```
# nmap --packet-trace -p 25,113
scanme.nmap.org

Starting Nmap ( http://nmap.org )
[...]
RCVD (0.1430s) TCP 64.13.134.52:25 >
192.168.0.8:46736 RA ttl=55 id=0
iplen=40  seq=0 win=0 ack=2914477947
RCVD (0.1440s) TCP 64.13.134.52:113 >
192.168.0.8:46736 RA ttl=55 id=0
iplen=40  seq=0 win=0 ack=2914477947
[...]

Nmap done: 1 IP address (1 host up)
scanned in 0.15 seconds
```

Advanced Traceroute

```
# nmap —traceroute scanme.nmap.org
[...]
TRACEROUTE (using port 22/tcp)
HOP RTT   ADDRESS
1   0.60  wap.nmap-int.org (192.168.0.6)
[...]
6   9.74  151.164.251.42
7   10.89 so-1-0-0.mpr1.sjc2.us.above.net
(64.125.30.174)
8   10.52 so-4-2-0.mpr3.pao1.us.above.net
(64.125.28.142)
9   14.25 metro0.sv.svcolo.com
(208.185.168.173)
10  12.80 scanme.nmap.org (64.13.134.52)
```

Performance and Accuracy

```
# nmap -T4 --max_rtt_timeout 200
--initial_rtt_timeout 150
--min_hostgroup 512 –max_retries
0 -n -P0 -p80 -oG pb3.gnmap
216.163.128.0/20
Starting Nmap
[...]
Nmap run completed -- 4096 IP
addresses (4096 hosts up) scanned
in 46.052 seconds
```

TCP and IP Header Options

```
# nmap  -vv -n -sS -P0 -p 445
--ip-options "L 10.4.2.1"
10.5.2.1
```

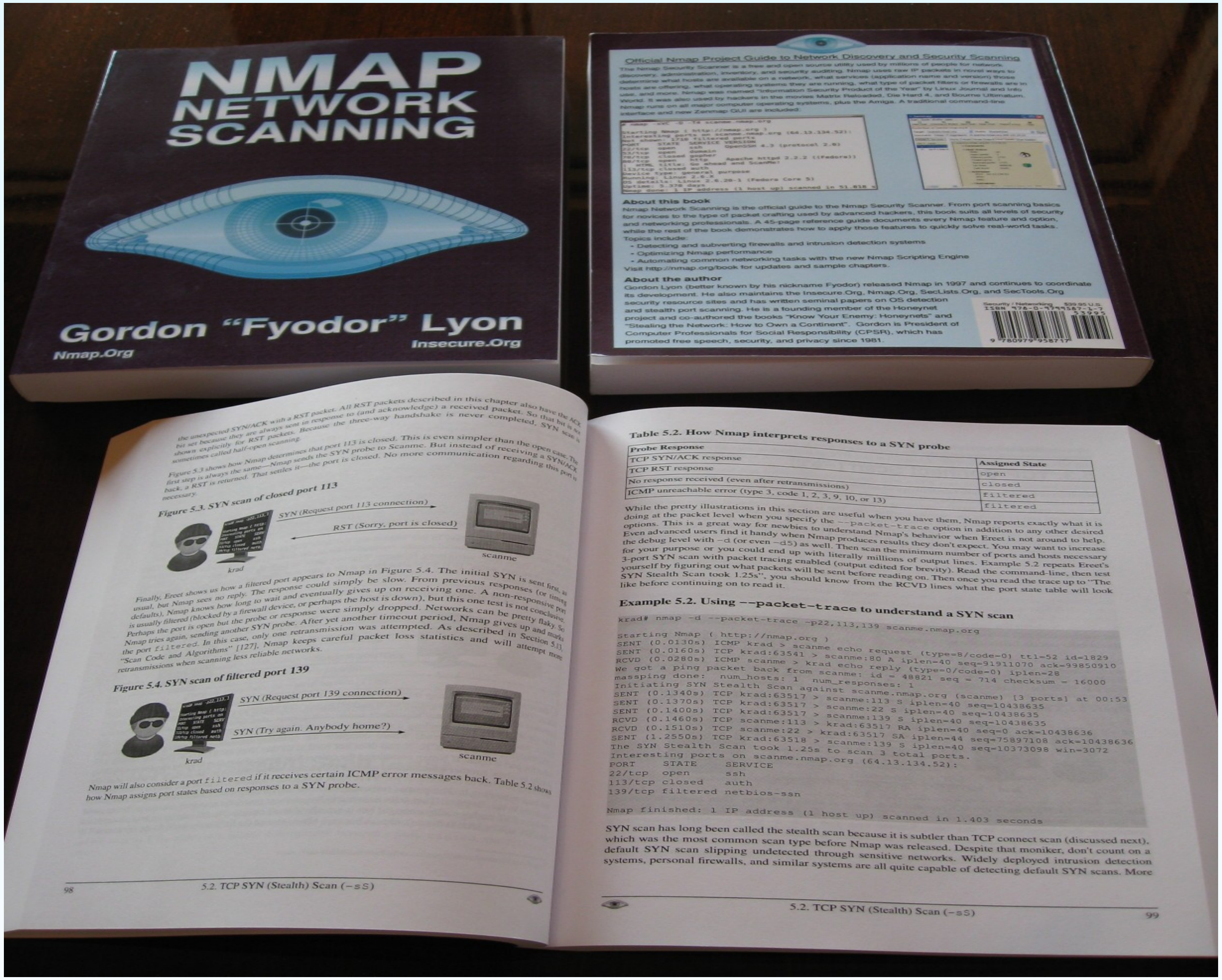
Ncat

- A modern interpretation of Hobbit's venerable Netcat
- Supports virtually all of the Netcat 1.10 features, except the basic portscanner.
- Also supports SSL, IPv6, multiple platforms, connection brokering, port redirection, proxies (client, server, chaining), shell execution, access control, and more.
- In development since 2005, nearly ready for release. Current dev lead is Kris Katterjohn.
- Available from svn://svn.insecure.org/ncat (login: guest/guest)

Ndiff

- Compares two (or more) scans, displays changes (new/removed hosts, ports, changed services, etc.)
- Great for quick change detection with recurring scans.
- Perl version available from: svn://svn.insecure.org/nmap-exp/ndiff

Nmap Network Scanning
http://nmap.org/book/



NMAP NETWORK SCANNING

Gordon "Fyodor" Lyon

Nmap.Org

Insecure.Org

Official Nmap Project Guide to Network Discovery and Security Scanning

The Nmap Security Scanner is a free and open source utility used by millions of people for network discovery, administration, inventory, and security auditing. Nmap uses raw IP packets in novel ways to determine what hosts are available on a network, what services (application name and version) those hosts are offering, what operating systems they are running, what type of packet filters or firewalls are in use, and more. Nmap was named "Information Security Product of the Year" by Linux Journal and Info World. It was also used by hackers in the movies Matrix Reloaded, Die Hard 4, and Bourne Ultimatum. Nmap runs on all major computer operating systems, plus the Amiga. A traditional command-line interface and new Zenmap GUI are included:

```
# nmap -sVC -O -T4 scanme.nmap.org
Starting Nmap ( http://nmap.org )
Interesting ports on scanme.nmap.org (64.13.134.52):
Not shown: 1710 filtered ports
PORT     STATE  SERVICE VERSION
22/tcp   open   ssh     OpenSSH 4.3 (protocol 2.0)
53/tcp   open   domain
70/tcp   closed gopher
80/tcp   open   http    Apache httpd 2.2.2 ((Fedora))
|_ HTML title: Go ahead and ScanMe!
113/tcp  closed auth
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.20-1 (Fedora Core 5)
Uptime: 5.378 days
Nmap done: 1 IP address (1 host up) scanned in 51.818 s
```

About this book

Nmap Network Scanning is the official guide to the Nmap Security Scanner. From port scanning basics for novices to the type of packet crafting used by advanced hackers, this book suits all levels of security and networking professionals. A 45-page reference guide documents every Nmap feature and option, while the rest of the book demonstrates how to apply those features to quickly solve real-world tasks. Topics include:

- Detecting and subverting firewalls and intrusion detection systems
- Optimizing Nmap performance
- Automating common networking tasks with the new Nmap Scripting Engine

Visit http://nmap.org/book for updates and sample chapters.

About the author

Gordon Lyon (better known by his nickname Fyodor) released Nmap in 1997 and continues to coordinate its development. He also maintains the Insecure.Org, Nmap.Org, SecLists.Org, and SecTools.Org security resource sites and has written seminal papers on OS detection and stealth port scanning. He is a founding member of the Honeynet project and co-authored the books "Know Your Enemy: Honeynets" and "Stealing the Network: How to Own a Continent". Gordon is President of Computer Professionals for Social Responsibility (CPSR), which has promoted free speech, security, and privacy since 1981.

Security / Networking $39.95 U.S.
ISBN 978-0-9799587-1-7
53995
9 780979 958717

the unexpected SYN/ACK with a RST packet. All RST packets described in this chapter also have the ACK bit set because they are always sent in response to (and acknowledge) a received packet. So that bit is not shown explicitly for RST packets. Because the three-way handshake is never completed, SYN scan is sometimes called half-open scanning.

Figure 5.3 shows how Nmap determines that port 113 is closed. This is even simpler than the open case. The first step is always the same—Nmap sends the SYN probe to Scanme. But instead of receiving a SYN/ACK back, a RST is returned. That settles it—the port is closed. No more communication regarding this port is necessary.

Figure 5.3. SYN scan of closed port 113

SYN (Request port 113 connection)
RST (Sorry, port is closed)
krad
scanme

Finally, Ereet shows us how a filtered port appears to Nmap in Figure 5.4. The initial SYN is sent first, as usual, but Nmap sees no reply. The response could simply be slow. From previous responses (or timing defaults), Nmap knows how long to wait and eventually gives up on receiving one. A non-responsive port is usually filtered (blocked by a firewall device, or perhaps the host is down), but this one test is not conclusive. Perhaps the port is open but the probe or response were simply dropped. Networks can be pretty flaky. So Nmap tries again, sending another SYN probe. After yet another timeout period, Nmap gives up and marks the port filtered. In this case, only one retransmission was attempted. As described in Section 5.13, "Scan Code and Algorithms" [127], Nmap keeps careful packet loss statistics and will attempt more retransmissions when scanning less reliable networks.

Figure 5.4. SYN scan of filtered port 139

SYN (Request port 139 connection)
SYN (Try again. Anybody home?)
krad
scanme

Nmap will also consider a port filtered if it receives certain ICMP error messages back. Table 5.2 shows how Nmap assigns port states based on responses to a SYN probe.

98 5.2. TCP SYN (Stealth) Scan (-sS)

Table 5.2. How Nmap interprets responses to a SYN probe

Probe Response	Assigned State
TCP SYN/ACK response	open
TCP RST response	closed
No response received (even after retransmissions)	filtered
ICMP unreachable error (type 3, code 1, 2, 3, 9, 10, or 13)	filtered

While the pretty illustrations in this section are useful when you have them, Nmap reports exactly what it is doing at the packet level when you specify the --packet-trace option in addition to any other desired options. This is a great way for newbies to understand Nmap's behavior when Ereet is not around to help. Even advanced users find it handy when Nmap produces results they don't expect. You may want to increase the debug level with -d (or even -d5) as well. Then scan the minimum number of ports and hosts necessary for your purpose or you could end up with literally millions of output lines. Example 5.2 repeats Ereet's 3-port SYN scan with packet tracing enabled (output edited for brevity). Read the command-line, then test yourself by figuring out what packets will be sent before reading on. Then once you read the trace up to "The SYN Stealth Scan took 1.25s", you should know from the RCVD lines what the port state table will look like before continuing on to read it.

Example 5.2. Using --packet-trace to understand a SYN scan

```
krad# nmap -d --packet-trace -p22,113,139 scanme.nmap.org

Starting Nmap ( http://nmap.org )
SENT (0.0130s) ICMP krad > scanme echo request (type=8/code=0) ttl=52 id=1829
SENT (0.0160s) TCP krad:63541 > scanme:80 A iplen=40 seq=91911070 ack=99850910
RCVD (0.0280s) ICMP scanme > krad echo reply (type=0/code=0) iplen=28
We got a ping packet back from scanme: id = 48821 seq = 714 checksum = 16000
massping done:  num_hosts: 1  num_responses: 1
Initiating SYN Stealth Scan against scanme.nmap.org (scanme) [3 ports] at 00:53
SENT (0.1340s) TCP krad:63517 > scanme:113 S iplen=40 seq=10438635
SENT (0.1370s) TCP krad:63517 > scanme:22 S iplen=40 seq=10438635
SENT (0.1400s) TCP krad:63517 > scanme:139 S iplen=40 seq=10438635
RCVD (0.1460s) TCP scanme:113 > krad:63517 RA iplen=40 seq=0 ack=10438636
RCVD (0.1510s) TCP scanme:22 > krad:63517 SA iplen=44 seq=75897108 ack=10438636
SENT (1.2550s) TCP krad:63518 > scanme:139 S iplen=40 seq=10373098 win=3072
The SYN Stealth Scan took 1.25s to scan 3 total ports.
Interesting ports on scanme.nmap.org (64.13.134.52):
PORT     STATE    SERVICE
22/tcp   open     ssh
113/tcp  closed   auth
139/tcp  filtered netbios-ssn

Nmap finished: 1 IP address (1 host up) scanned in 1.403 seconds
```

SYN scan has long been called the stealth scan because it is subtler than TCP connect scan (discussed next), which was the most common scan type before Nmap was released. Despite that moniker, don't count on a default SYN scan slipping undetected through sensitive networks. Widely deployed intrusion detection systems, personal firewalls, and similar systems are all quite capable of detecting default SYN scans. More

5.2. TCP SYN (Stealth) Scan (-sS) 99

Top Nmap Contributors since 4.50

Aaron Leininger, Adriano Monteiro Marques, Allison Randal, Andrew J. Bennieston, Andy Lutomirski, Arturo Buanzo Busleiman, Benson Kalahar, Bill Pollock, Brandon Enright, Brian Hatch, Chad Loder, Chris Gibson, Daniel Roethlisberger, David Fifield, David Moore, Diman Todorov, Doug Hoyte, Dragos Ruiu, Dudi Itzhakov, Eddie Bell, Emma Jane Hogbin, Gisle Vanem, Guilherme Polo, HD Moore, Ithilgore, Jabra, Jah, James Messer, Jason DePriest, Jeff Nathan, Jesse Burns, Joao Medeiros, Jurand Nogiec, Kris Katterjohn, Lamont Jones, Lance Spitzner, Leigh Honeywell, Lionel Cons, Martin Macok, Max Schubert, Michael Pattrick, Mixter, Nathan Bills, Patrick Donnelly, Philip Pickering, Rainer Müller, Raven Alder, Rob Nicholls, Sebastián García, Simple Nomad, Solar Designer, Stephan Fijneman, Steve Christensen, Sven Klemm, Thomas Buchanan, Thorsten Holz, Tim Adam, Tom Duffy, Tom Sellers, Tyler Reguly, van Hauser, Vlad Alexa, Vladimir Mitrovic, William McVey, Zhao Lei

Questions and Resources

- Download Nmap from http://nmap.org
- Download these slides from: http://insecure.org/presentations/BHDC08/
- Nmap Network Scanning pre-release is available at:
  - Black Hat Bookstore – Sold out!
  - No Starch booth at Defcon starting at 10AM Friday.
- Newest Nmap: svn://svn.insecure.org/nmap-exp/bhdc08