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 knowledgeable 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 firewalls
- 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

```bash
# 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 -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)

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

PORT   STATE SERVICE
53/udp open  domain
__ Nameserver open recursive queries (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 172.17.22.3 10.0.0.10 wap.yuma.net zardozyuma.net

Target: wap.yuma.net zardozyuma.net
Profile: Intense Scan

Scan options:
- TCP scan:
- Special scans:
- Timing:
- FTP bounce attack
- Idle Scan (Zombie)
- Services version detection
- Operating system detection
- Disable reverse DNS resolution
- IPv6 support
- Maximum Retries: 1

Command:
nmap -SF -SV -T Sneaky -6 -O <target>
2\textsuperscript{nd} Generation OS Detection

```bash
# 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:
Version Detection

```bash
# 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)
```
# 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

<table>
<thead>
<tr>
<th>PORT</th>
<th>STATE</th>
<th>SERVICE</th>
<th>REASON</th>
</tr>
</thead>
<tbody>
<tr>
<td>22/tcp</td>
<td>open</td>
<td>ssh</td>
<td>syn-ack</td>
</tr>
<tr>
<td>25/tcp</td>
<td>closed</td>
<td>smtp</td>
<td>reset</td>
</tr>
<tr>
<td>53/tcp</td>
<td>open</td>
<td>domain</td>
<td>syn-ack</td>
</tr>
<tr>
<td>70/tcp</td>
<td>closed</td>
<td>gopher</td>
<td>reset</td>
</tr>
<tr>
<td>80/tcp</td>
<td>open</td>
<td>http</td>
<td>syn-ack</td>
</tr>
<tr>
<td>113/tcp</td>
<td>closed</td>
<td>auth</td>
<td>reset</td>
</tr>
</tbody>
</table>
# 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  metro00.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/
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