Nmap: Scanning the Internet
by Fyodor
Black Hat Inaugural Webcast; June 26, 2008
Planning the Big Scan

• Determining IP addresses to scan
• P2P Scanning?
• Legal Issues
• Firewalls
• Performance
Scan Results

- Scans are still running
- Some tentative results already available, and can improve scan performance.
Best TCP Ports for Host Discovery

- Echo request, and even Nmap default discovery scans are insufficient for Internet scanning.
- Adding more TCP SYN and ACK probes can help, but which ports work the best?
<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>http</td>
</tr>
<tr>
<td>25</td>
<td>smtp</td>
</tr>
<tr>
<td>22</td>
<td>ssh</td>
</tr>
<tr>
<td>443</td>
<td>https</td>
</tr>
<tr>
<td>21</td>
<td>ftp</td>
</tr>
<tr>
<td>113</td>
<td>auth</td>
</tr>
<tr>
<td>23</td>
<td>telnet</td>
</tr>
<tr>
<td>53</td>
<td>domain</td>
</tr>
<tr>
<td>554</td>
<td>rtsp</td>
</tr>
<tr>
<td>3389</td>
<td>ms-term-server</td>
</tr>
</tbody>
</table>
Default Host Discovery Effectiveness

```bash
# 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%)
Top Open TCP & UDP Ports

- Will be available by Black Hat USA
- Substantial reduction of current default 1703 TCP ports, 1480 UDP
- --top-ports feature available now, but no data to use it.
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)
```
Fixed-rate packet sending

nmap -min-rate 500 scanme.nmap.org
Zenmap GUI

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

Target: 10.0.0.10 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.net

Ports / Hosts Nmap Output Host Details Scan Details

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

Host Status
State: up
Open ports: 3
Filtered ports: 0
Closed ports: 2
Scanned ports: 5
Up time: 3916956

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%

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

Help Cancel OK
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)

# 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
<table>
<thead>
<tr>
<th>PORT</th>
<th>STATE</th>
<th>SERVICE</th>
<th>VERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>22/tcp</td>
<td>open</td>
<td>ssh</td>
<td>OpenSSH 4.3 (protocol 2.0)</td>
</tr>
<tr>
<td>25/tcp</td>
<td>closed</td>
<td>smtp</td>
<td></td>
</tr>
<tr>
<td>53/tcp</td>
<td>open</td>
<td>domain</td>
<td>ISC BIND 9.3.4</td>
</tr>
<tr>
<td>70/tcp</td>
<td>closed</td>
<td>gopher</td>
<td></td>
</tr>
<tr>
<td>80/tcp</td>
<td>open</td>
<td>http</td>
<td>Apache httpd 2.2.2 ((Fedora))</td>
</tr>
<tr>
<td>113/tcp</td>
<td>closed</td>
<td>auth</td>
<td></td>
</tr>
</tbody>
</table>

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 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>
Advanced Traceroute

```bash
# 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

```bash
# 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
Learn More

- Download Nmap from http://nmap.org
- Download these slides from: http://insecure.org/presentations/BHDC08/