Advanced Network
Reconnaissance with Nmap

by Fyodor
fyodor@insecure.org
http://www.insecure.org/presentations/Shmoo06/
ShmooCon; Jan 14, 2006
Mission #1

Penetrate SCO's Firewall to discern all the open TCP ports on Docsrv.Caldera.Com
SYN Scan against DocSRV

# nmap -sS -T4 docsrv.caldera.com
Starting Nmap 3.97Shmoo ( http://www.insecure.org/nmap/ )
Interesting ports on docsrv.caldera.com (216.250.128.247):
(The 1669 ports scanned but not shown below are in state: filtered)

<table>
<thead>
<tr>
<th>PORT</th>
<th>STATE</th>
<th>SERVICE</th>
</tr>
</thead>
<tbody>
<tr>
<td>80/tcp</td>
<td>open</td>
<td>http</td>
</tr>
<tr>
<td>113/tcp</td>
<td>closed</td>
<td>auth</td>
</tr>
<tr>
<td>507/tcp</td>
<td>open</td>
<td>crs</td>
</tr>
</tbody>
</table>

Nmap finished: 1 IP address (1 host up) scanned in 24.490 seconds
# nmap -sF -T4 docsrv.caldera.com

Starting Nmap 3.97Shmoo ( http://www.insecure.org/nmap/ )

Interesting ports on docsrv.caldera.com (216.250.128.247):
(The 1632 ports scanned but not shown below are in state: closed)

<table>
<thead>
<tr>
<th>PORT</th>
<th>STATE</th>
<th>SERVICE</th>
</tr>
</thead>
<tbody>
<tr>
<td>7/tcp</td>
<td>open</td>
<td>filtered</td>
</tr>
<tr>
<td>9/tcp</td>
<td>open</td>
<td>filtered</td>
</tr>
<tr>
<td>11/tcp</td>
<td>open</td>
<td>filtered</td>
</tr>
<tr>
<td>13/tcp</td>
<td>open</td>
<td>filtered</td>
</tr>
<tr>
<td>15/tcp</td>
<td>open</td>
<td>filtered</td>
</tr>
<tr>
<td>19/tcp</td>
<td>open</td>
<td>filtered</td>
</tr>
<tr>
<td>21/tcp</td>
<td>open</td>
<td>filtered</td>
</tr>
<tr>
<td>22/tcp</td>
<td>open</td>
<td>filtered</td>
</tr>
<tr>
<td>23/tcp</td>
<td>open</td>
<td>filtered</td>
</tr>
<tr>
<td>25/tcp</td>
<td>open</td>
<td>filtered</td>
</tr>
<tr>
<td>37/tcp</td>
<td>open</td>
<td>filtered</td>
</tr>
<tr>
<td>79/tcp</td>
<td>open</td>
<td>filtered</td>
</tr>
<tr>
<td>80/tcp</td>
<td>open</td>
<td>filtered</td>
</tr>
</tbody>
</table>

[many ports cut]

| 135/tcp| open|filtered | auth |
ACK Scan against DocSRV

# nmap -sA -T4 docsrv.caldera.com
Starting Nmap 3.97Shmoo
Interesting ports on docsrv.caldera.com
(216.250.128.247):
(The 1669 ports scanned but not shown below are in state: UNfiltered)
PORT    STATE    SERVICE
135/tcp  filtered  msrpc
1434/tcp filtered  ms-sql-m
32777/tcp filtered  sometimes-rpc17

Nmap finished: 1 IP address (1 host up) scanned in 3.134 seconds
Window Scan against DocSRV

```bash
# nmap -sW -p- -T4 docsrv.caldera.com
Starting Nmap 3.97Shmoo ( http://www.insecure.org/nmap/ )
Interesting ports on docsrv.caldera.com (216.250.128.247):
(The 65479 ports scanned but not shown below are in state: closed)

<table>
<thead>
<tr>
<th>PORT</th>
<th>STATE</th>
<th>SERVICE</th>
</tr>
</thead>
<tbody>
<tr>
<td>7/tcp</td>
<td>open</td>
<td>echo</td>
</tr>
<tr>
<td>9/tcp</td>
<td>open</td>
<td>discard</td>
</tr>
<tr>
<td>11/tcp</td>
<td>open</td>
<td>systat</td>
</tr>
<tr>
<td>13/tcp</td>
<td>open</td>
<td>daytime</td>
</tr>
<tr>
<td>15/tcp</td>
<td>open</td>
<td>netstat</td>
</tr>
<tr>
<td>19/tcp</td>
<td>open</td>
<td>chargen</td>
</tr>
<tr>
<td>21/tcp</td>
<td>open</td>
<td>ftp</td>
</tr>
<tr>
<td>22/tcp</td>
<td>open</td>
<td>ssh</td>
</tr>
<tr>
<td>23/tcp</td>
<td>open</td>
<td>telnet</td>
</tr>
<tr>
<td>25/tcp</td>
<td>open</td>
<td>smtp</td>
</tr>
<tr>
<td>37/tcp</td>
<td>open</td>
<td>time</td>
</tr>
<tr>
<td>79/tcp</td>
<td>open</td>
<td>finger</td>
</tr>
<tr>
<td>80/tcp</td>
<td>open</td>
<td>http</td>
</tr>
<tr>
<td>110/tcp</td>
<td>open</td>
<td>pop3</td>
</tr>
<tr>
<td>111/tcp</td>
<td>open</td>
<td>rpcbind</td>
</tr>
<tr>
<td>135/tcp</td>
<td>filtered</td>
<td>msrpc</td>
</tr>
<tr>
<td>143/tcp</td>
<td>open</td>
<td>imap</td>
</tr>
</tbody>
</table>
```
Mission #2

Sneak past all of the Nmap-related Snort IDS Rules
Nmap-Specific Snort Rules

~/snortrules-pr-2.4/rules>egrep -i 'alert.*nmap' *.rules

icmp.rules:alert icmp $EXTERNAL_NET any -> $HOME_NET any
(msg:"ICMP PING NMAP"; dsize:0; itype:8;
reference:arachnids,162; classtype:attempted-recon;
sid:469; rev:3;)

scan.rules:alert tcp $EXTERNAL_NET any -> $HOME_NET any
(msg:"SCAN nmap XMAS"; flow:stateless; flags:FPU,12;
reference:arachnids,30; classtype:attempted-recon;
sid:1228; rev:7;)

web-attacks.rules:alert tcp $EXTERNAL_NET any ->
$HTTP_SERVERS $HTTP_PORTS (msg:"WEB-ATTACKS nmap command attempt";
flow:to_server,established; content:"nmap%20";
ocase; classtype:web-application-attack; sid:1361; rev:5;)

deleted.rules:alert tcp $EXTERNAL_NET any -> $HOME_NET any
(msg:"SCAN nmap TCP"; ack:0; flags:A,12; flow:stateless;
reference:arachnids,28; classtype:attempted-recon; sid:628;
rev:7;)

deleted.rules:alert tcp $EXTERNAL_NET any -> $HOME_NET any
(msg:"SCAN nmap fingerprint attempt"; flags:SFPFU;
flow:stateless; reference:arachnids,05;
classstype:attempted-recon; sid:629; rev:6;)

Flow-portscan – Fixed Window

~/$snort-2.2.0/etc> grep 'scanner-fixed' snort.conf
#
# scanner-fixed-threshold 15 \ 
#
# scanner-fixed-window 15 \
Defeating Fixed Window Scan Detection

```bash
# foreach target (205.217.153.53 205.217.153.54 205.217.153.55)
foreach? nmap --scan_delay 1075 --max_retries 0 -max_hostrgroup 1 -P0 -p21,22,23,25,53 $target
foreach? usleep 1075000
foreach? end
```
Flow-portscan – Sliding Window

~/snort-2.2.0/etc> grep scanner-sliding snort.conf
# scanner-sliding-threshold 40 \n# scanner-sliding-window 20 \n# scanner-sliding-scale-factor 0.50 \n
Defeating Snort Sliding & Fixed Window Detection

felix~# foreach target (205.217.153.53 205.217.153.54 205.217.153.55) 
foreach? nmap -min_parallelism 15 -- 
max_retries 0 -P0 -p21,22,23,25,53 $target 
foreach? usleep 23000000 
foreach? end
Another Option: Just Exploit the Thing

Try the Snort Back Orifice Pre-processor
Exploit:
http://www.frsirt.com/exploits/20051025.THC
snortbo.c.php
Don't Forget Decoys (-D)

<table>
<thead>
<tr>
<th>Time</th>
<th>Attack</th>
<th>Intruder</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>05/16/01 06:00:39</td>
<td>TCP ACK ping</td>
<td>12.72.193.4</td>
<td>6</td>
</tr>
<tr>
<td>05/16/01 06:00:38</td>
<td>NMAP OS fingerprint</td>
<td>119.33.21.232</td>
<td>9</td>
</tr>
<tr>
<td>05/16/01 06:00:38</td>
<td>NMAP OS fingerprint</td>
<td>72.38.20.47</td>
<td>6</td>
</tr>
<tr>
<td>05/16/01 06:00:38</td>
<td>NMAP OS fingerprint</td>
<td>123.4.61.89</td>
<td>3</td>
</tr>
<tr>
<td>05/16/01 06:00:38</td>
<td>NMAP OS fingerprint</td>
<td>192.168.0.2</td>
<td>3</td>
</tr>
<tr>
<td>05/16/01 06:00:38</td>
<td>NMAP OS fingerprint</td>
<td>95.23.114.67</td>
<td>3</td>
</tr>
<tr>
<td>05/16/01 06:00:38</td>
<td>NMAP OS fingerprint</td>
<td>63.175.91.128</td>
<td>3</td>
</tr>
<tr>
<td>05/16/01 06:00:38</td>
<td>NMAP OS fingerprint</td>
<td>96.184.127.10</td>
<td>3</td>
</tr>
<tr>
<td>05/16/01 06:00:38</td>
<td>NMAP OS fingerprint</td>
<td>12.114.187.169</td>
<td>3</td>
</tr>
<tr>
<td>05/16/01 06:00:38</td>
<td>NMAP OS fingerprint</td>
<td>48.210.38.12</td>
<td>3</td>
</tr>
<tr>
<td>05/16/01 06:00:38</td>
<td>NMAP OS fingerprint</td>
<td>10.45.161.9</td>
<td>3</td>
</tr>
<tr>
<td>05/16/01 06:00:38</td>
<td>NMAP OS fingerprint</td>
<td>192.168.7.90</td>
<td>3</td>
</tr>
<tr>
<td>05/16/01 06:00:38</td>
<td>NMAP OS fingerprint</td>
<td>42.79.122.16</td>
<td>3</td>
</tr>
<tr>
<td>05/16/01 06:00:38</td>
<td>NMAP OS fingerprint</td>
<td>94.101.211.12</td>
<td>3</td>
</tr>
<tr>
<td>05/16/01 06:00:38</td>
<td>NMAP OS fingerprint</td>
<td>51.176.79.2</td>
<td>3</td>
</tr>
<tr>
<td>05/16/01 06:00:38</td>
<td>NMAP OS fingerprint</td>
<td>12.72.193.4</td>
<td>3</td>
</tr>
<tr>
<td>05/16/01 06:00:36</td>
<td>UDP port probe</td>
<td>119.22.21.232</td>
<td>6</td>
</tr>
<tr>
<td>05/16/01 06:00:36</td>
<td>UDP port probe</td>
<td>72.38.20.47</td>
<td>4</td>
</tr>
<tr>
<td>05/16/01 06:00:36</td>
<td>UDP port probe</td>
<td>123.4.61.89</td>
<td>2</td>
</tr>
<tr>
<td>05/16/01 06:00:36</td>
<td>UDP port probe</td>
<td>182.169.0.2</td>
<td>2</td>
</tr>
</tbody>
</table>

[Scan] Attacker sends unusual combination of TCP flags to see how the system responds. This may assist further attacks.
Also Don't Forget

- Exotic scan flags (--scanflags)
- Source port manipulation (-g)
- Ipv6 (-6)
- IPID Idle Scanning (-sl)
- Fragmentation (-f, --mtu)
- Proxies
- Source Routing
- Etc.
Finally, Have Some Fun With It

<table>
<thead>
<tr>
<th>Time</th>
<th>Attack</th>
<th>Intruder</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>05/16/01 06:09:11</td>
<td>SNMP backdoor</td>
<td>Your Mother</td>
<td>1</td>
</tr>
</tbody>
</table>

[Intrusion attempt] Intruder attempts to exploit a default backdoor in the network equipment.
Single Service Discovery
Mission #3

Locate webserver(s) on the Playboy.Com network offering free images
Step 1: Find Network to Scan

Step 1: Find the network to scan

core~> whois -h whois.arin.net n playboy

[...]
OrgName: Playboy
OrgID: PLAYBO
Address: 680 N. Lake Shore Drive
City: Chicago
StateProv: IL
PostalCode: 60611
Country: US

NetRange: 216.163.128.0 – 216.163.143.255
CIDR: 216.163.128.0/20 [...]

Initial Try

```
nmap -P0 -p80 -oG pb.gnmap
216.163.128.0/20
Starting nmap 3.81
[...]
Nmap run completed -- 4096 IP addresses (4096 hosts up) scanned in 1236.309 seconds
```
Help Nmap Out with Timing Information

> host www.playboy.com
www.playboy.com has address 209.247.228.201

Mail servers (host -t mx playboy.com):
  mx.la.playboy.com. 10 216.163.128.15
  mx.chi.playboy.com. 5 216.163.143.4
Ping Known Hosts for RTT Estimates

> ping -c5 mx.chi.playboy.com
PING mx.chi.playboy.com (216.163.143.4) 56(84) bytes of data.
--- mx.chi.playboy.com ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4000ms

> ping -c5 mx.la.playboy.com
PING mx.la.playboy.com (216.163.128.15) 56(84) bytes of data.
--- mx.la.playboy.com ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4011ms
Perhaps TCP Ping Will Work Better

```bash
# hping2 --syn -p 25 -c 5 mx.chi.playboy.com
HPING mx.chi.playboy.com (eth0 216.163.143.4)
46 bytes from 216.163.143.4: flags=SA
46 bytes from 216.163.143.4: flags=SA
[cut]
--- mx.chi.playboy.com hping statistic ---
5 packets transmitted, 5 packets received
round-trip min/avg/max = 56.8/58.0/61.8 ms

# hping2 --syn -p 25 -c 5 mx.la.playboy.com
HPING mx.la.playboy.com (eth0 216.163.128.15)
46 bytes from 216.163.128.15: flags=SA
46 bytes from 216.163.128.15: flags=SA
[cut]
--- mx.la.playboy.com hping statistic ---
5 packets transmitted, 5 packets received
round-trip min/avg/max = 15.4/15.8/16.4 ms
```
Designing a Faster Scan

nmap -T4 --max_rtt_timeout 200 --initial_rtt_timeout 150 --min_hostgroup 512 -P0 -p80 -oG pb2.gnmap 216.163.128.0/20
Re-Launch the Scan

```bash
# nmap -T4 --max_rtt_timeout 200 --initial_rtt_timeout 150 --min_hostgroup 512 -P0 -p80 -oG pb2.gnmap 216.163.128.0/20
Starting nmap 3.81
[...] 
Nmap run completed -- 4096 IP addresses (4096 hosts up) scanned in 868.714 seconds
```
Upgrade to 3.97Shmoo + --max_retries

# nmap -T4 --max_rtt_timeout 200 --initial_rtt_timeout 150 --min_hostgroup 512 --max_retries 0 -P0 -p80 -oG pb3.gnmap
216.163.128.0/20
Starting nmap 3.97Shmoo
[...]
Nmap run completed -- 4096 IP addresses (4096 hosts up) scanned in 289.579 seconds

Under 5 Minutes!
Skip DNS

# 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 3.97Shmoo
[...]
Nmap run completed -- 4096 IP addresses (4096 hosts up) scanned in 46.052 seconds
Time for the Results!

```bash
> grep 80/open pb3.gnmap | awk '{print $2}'
216.163.129.20 216.163.136.21 216.163.136.22
216.163.136.27 216.163.136.29 216.163.136.30
216.163.136.31 216.163.137.3  216.163.137.4
216.163.137.5  216.163.137.6  216.163.137.7
216.163.137.8  216.163.137.9  216.163.137.10
216.163.137.11 216.163.137.12 216.163.137.13
216.163.137.14 216.163.137.15 216.163.137.16
216.163.137.17 216.163.137.18 216.163.137.19
216.163.137.20 216.163.137.21 216.163.137.22
216.163.137.23 216.163.137.25 216.163.137.26
216.163.137.27 216.163.140.20 216.163.143.11
```
Add Version Detection (-sV)

####### mydoom backdoor PROBE #######
Probe TCP mydoom q|\x0d\x0d|
ports 3127-3198
match mydoom m|\x04\x5b\0\0\0\0\0\0\0|p/mydoom/ v/v012604/
Nmap 3.97Shmoo

• Download the goods from http://www.insecure.org/presentations/Shmoo06/

• Features Since 3.95:
  – Runtime Interaction
  – Parallel reverse DNS
  – Corrupt TCP/UDP checksum option (--badsum)
  – --max_retries
Features Since 3.50

- ARP Scanning and Spoofing
- Rewrote core port scanning engine
- Diet Nmap
- Brand new man page/reference guide, in 7 languages so far
- Huge version detection DB update (from 1,000 to 3,000 signatures)
- Version detection now gathers OS, device type, and hostname
Features Since 3.50 (Cont'd)

- Version detection rarity (\texttt{--version\_light}, \texttt{--version\_all}, \texttt{--version\_intensity})
- Massive OS detection update (grew more than 50\% to 1,684 fingerprints)
- Dramatic Windows performance improvements – now sends via NDIS driver.
- MAC Address Printing
- 'l33t ASCII art in configurator
- XSL stylesheet for HTML output
Features Since 3.50 (Cont'd)

• open|filtered and closed|filtered states
• Completion time estimates
• NmapFE ported to GTK2
Top Nmap Contributors Since 3.50

Questions?

Any questions about Nmap, Network Reconnaissance, or anything else?