



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)
PORT      STATE  SERVICE
80/tcp    open   http
113/tcp   closed auth
507/tcp   open   crs

Nmap finished: 1 IP address (1 host up) scanned in 24.490
seconds
```



FIN Scan against DocSRV

```
# 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)
PORT      STATE      SERVICE
7/tcp    open|filtered echo
9/tcp    open|filtered discard
11/tcp   open|filtered systat
13/tcp   open|filtered daytime
15/tcp   open|filtered netstat
19/tcp   open|filtered chargen
21/tcp   open|filtered ftp
22/tcp   open|filtered ssh
23/tcp   open|filtered telnet
25/tcp   open|filtered smtp
37/tcp   open|filtered time
79/tcp   open|filtered finger
80/tcp   open|filtered http
[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

```
# 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)
PORT      STATE      SERVICE
7/tcp    open      echo
9/tcp    open      discard
11/tcp   open      systat
13/tcp   open      daytime
15/tcp   open      netstat
19/tcp   open      chargen
21/tcp   open      ftp
22/tcp   open      ssh
23/tcp   open      telnet
25/tcp   open      smtp
37/tcp   open      time
79/tcp   open      finger
80/tcp   open      http
110/tcp  open      pop3
111/tcp  open      rpcbind
135/tcp  filtered  msrpc
143/tcp  open      imap
```



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";
nocase; 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:SFP;
flow:stateless; reference:arachnids,05;
classtype: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

```
# foreach target (205.217.153.53  
205.217.153.54 205.217.153.55)  
foreach? nmap --scan_delay 1075 --  
max_retries 0 -max_hostgroup 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 \  
# scanner-sliding-window 20 \  
# scanner-sliding-scale-factor 0.50 \  

```



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)

The screenshot shows the BlackICE Defender application window. The title bar reads "BlackICE Defender". The menu bar includes "File", "View", "Tools", and "Help". Below the menu bar are tabs for "Attacks", "Intruders", "History", and "Information". The main area contains a table with the following columns: "Time", "Attack", "Intruder", and "Count". The table lists various attacks such as "TCP ACK ping" and "NMAP OS fingerprint" from different intruder IP addresses. A status bar at the bottom contains a message: "[Scan] Attacker sends unusual combination of TCP flags to see how the system responds. This may assist further attacks." and a "advICE" button. At the very bottom are "Close" and "Help" buttons.

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

[Scan] Attacker sends unusual combination of TCP flags to see how the system responds. This may assist further attacks. [advICE](#)

Close Help



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

The screenshot shows the BlackICE Defender application window. The title bar reads "BlackICE Defender". The menu bar includes "File", "View", "Tools", and "Help". Below the menu bar are four tabs: "Attacks", "Intruders", "History", and "Information". The main area contains a table with the following data:

	Time	Attack	Intruder	Count
	05/16/01 06:09:11	SNMP backdoor	Your Mother	1

Below the table, a text box displays the message: "[Intrusion attempt] Intruder attempts to exploit a default backdoor in the network equipment." To the right of this message is a button labeled "advICE". At the bottom of the window are two buttons: "Close" and "Help".



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

```
# 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

```
# 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!

```
> 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|  
p/mydoom/ v/v012604/
```



Nmap 3.97 Shmoo

- 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 (--version_light, --version_all, --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

Adam Kerrison, Adam Morgan, Adriano Monteiro Marques, Alan Bishoff, Alan William Somers, Albert Chin, Alok Tangoankar, Amy Hennings, Anders Thulin, Andreia Gaita, Andy Lutomirski, Annalee Newitz, Arturo Buanzo Busleiman, Bart Dopheide, Beirne Konarski, Ben Harris, Bill Dale, Bill Petersen, Bill Pollock, Bo Jiang, Brian Hatch, Chad Loder, Chris Gibson, Christophe, Craig Humphrey, Curtis Doty, Dana Epp, Dirk Mueller, Doug Hoyte, Dragos Ruiu, Dug Song, Duilio J. Protti, Eric S. Raymond, Felix Gröbert, Florian Ebner, Fyodor Yarochkin, Ganga Bhavani, Gisle Vanem, Glyn Geoghegan, Greg A. Woods, Greg Darke, Greg Taleck, Gwenole Beauchesne, HD Moore, Jedi/Sector One, Jeff Nathan, Jesse Burns, Jim Carras, Jim Harrison, Jonathan Dieter, José Domingos, Justin Cranford, Justin M Cacak, Krok, KX, Lamont Jones, Lance Spitzner, Laurent Estieux, Lionel Cons, Lucien Raven, MadHat, Marius Strobl, Mark-David McLaughlin, Mark Ruef, Martin Macok, Matthieu Verbert, Matt Selsky, Max Schubert, Meethune Bhowmick, Mephisto, Mike Basinger, Mike Hatz, Murphy, Netris, Okan Demirmen, Ole Morten Grodaas, Oliver Eikemeier, Pascal Trouvin, Paul Tarjan, Petr Salinger, Petter Reinholdtsen, pijn trein, Ping Huang, Piotr Sobolewski, Priit Laes, Princess Nadia, Raven Alder, Richard Birkett, Richard Moore, Robert E. Lee, Rob Foehl, Ronak Sutaria, Royce Williams, Ruediger Rissmann, Saint Xavier, Saravanan, Scott Mansfield, Sebastian Wolfgarten, Seth Master, Shahid Khan, Simon Burr, Simple Nomad, Sina Bahram, Solar Designer, Srivatsan, Stephane Loeuillet, Stephen Bishop, Steve Christensen, Steve Martin, Thorsten Holz, Tom Duffy, Tom Rune Flo, Tom Sellers, Tony Golding, van Hauser, vlad902, William McVey, Zhao Lei



Questions?

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