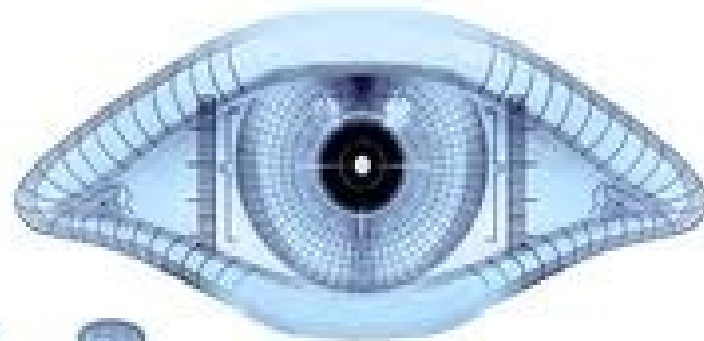


TCP Foo

NetCat and NMAP too

Nmap too.

Sorry, wrong nmap.



Nmap

A how-to on some scan foo...
To make the most doesn't require verbose.

Don't miss, make a list. -sL

```
acml77@thinktank:~/nmap$ ping scanme.nmap.org
PING scanme.nmap.org (64.13.134.52) 56(84) bytes of data.
64 bytes from scanme.nmap.org (64.13.134.52): icmp_seq=1 ttl=47 time=105 ms
```

```
acml77@thinktank:~/nmap$ nmap -sL 64.13.134.52
```

```
Starting Nmap 5.21 ( http://nmap.org ) at 2010-09-09 09:20 EDT
Nmap scan report for scanme.nmap.org (64.13.134.52)
Nmap done: 1 IP address (0 hosts up) scanned in 0.01 seconds
acml77@thinktank:~/nmap$ nmap -sL 64.13.134.*
```

```
Starting Nmap 5.21 ( http://nmap.org ) at 2010-09-09 09:21 EDT
Nmap scan report for 64.13.134.0
Nmap scan report for gw.titan.net (64.13.134.1)
Nmap scan report for mail.titan.net (64.13.134.2)
Nmap scan report for cust-134-3.titan.net (64.13.134.3)
Nmap scan report for syn.titan.net (64.13.134.4)
...
Nmap scan report for cust-134-47.titan.net (64.13.134.47)
Nmap scan report for nmap.org (64.13.134.48)
Nmap scan report for insecure.org (64.13.134.49)
Nmap scan report for seclists.org (64.13.134.50)
Nmap scan report for sectools.org (64.13.134.51)
Nmap scan report for scanme.nmap.org (64.13.134.52)
Nmap scan report for research.nmap.org (64.13.134.53)
Nmap scan report for cust-134-54.titan.net (64.13.134.54)
Nmap scan report for ns1.titan.net (64.13.134.58)
Nmap scan report for ns2.titan.net (64.13.134.59)
Nmap scan report for wwyr.titan.net (64.13.134.60)
Nmap scan report for nswc1.titan.net (64.13.134.61)
Nmap scan report for nswc2.titan.net (64.13.134.62)
...
Nmap done: 256 IP addresses (0 hosts up) scanned in 7.62 seconds
```

64.13.134.48-53

Enter the scanman

Nmap 64.13.134.48-53

Nmap 10.116.0-255.1-127

Nmap 192.168.1.1/24

Nmap *41.24-33.*.1-254


```
Starting Nmap 5.21 ( http://nmap.org ) at 2010-09-09 09:49 EDT
Nmap scan report for nmap.org (64.13.134.48)
Host is up (0.11s latency).
PORT      STATE  SERVICE
21/tcp    filtered ftp
22/tcp    filtered ssh
23/tcp    filtered telnet
80/tcp    open   http
443/tcp   filtered https

Nmap scan report for insecure.org (64.13.134.49)
Host is up (0.10s latency).
PORT      STATE  SERVICE
21/tcp    filtered ftp
22/tcp    filtered ssh
23/tcp    filtered telnet
80/tcp    open   http
443/tcp   filtered https

Nmap scan report for seclists.org (64.13.134.50)
Host is up (0.10s latency).
PORT      STATE  SERVICE
21/tcp    filtered ftp
22/tcp    filtered ssh
23/tcp    filtered telnet
80/tcp    open   http
443/tcp   filtered https

Nmap scan report for sectools.org (64.13.134.51)
Host is up (0.10s latency).
PORT      STATE  SERVICE
21/tcp    filtered ftp
22/tcp    filtered ssh
23/tcp    filtered telnet
80/tcp    open   http
443/tcp   filtered https

Nmap scan report for scanme.nmap.org (64.13.134.52)
Host is up (0.11s latency).
PORT      STATE  SERVICE
21/tcp    filtered ftp
22/tcp    open   ssh
23/tcp    filtered telnet
80/tcp    open   http
443/tcp   filtered https

Nmap scan report for research.nmap.org (64.13.134.53)
Host is up (0.11s latency).
PORT      STATE  SERVICE
21/tcp    filtered ftp
22/tcp    filtered ssh
23/tcp    filtered telnet
80/tcp    open   http
443/tcp   filtered https

Nmap done: 6 IP addresses (6 hosts up) scanned in 4.71 seconds
```

--top-ports 5

One of my favorite new switches. It saves you stitches when hiding from snitches, bitches.

I meant sneeches.

Technique and more switches.

--top-ports 5

--reason

--sA (Ack scan)

```
Starting Nmap 5.21 ( http://nmap.org ) at 2010-09-09 09:58 EDT
```

```
Nmap scan report for scanme.nmap.org (64.13.134.52)
```

```
Host is up, received syn-ack (0.10s latency).
```

PORT	STATE	SERVICE	REASON
21/tcp	filtered	ftp	no-response
22/tcp	open	ssh	syn-ack
23/tcp	filtered	telnet	no-response
80/tcp	open	http	syn-ack
443/tcp	filtered	https	no-response

```
Nmap done: 1 IP address (1 host up) scanned in 3.83 seconds
```

```
acml77@thinktank:~/nmap/hackpgh$ sudo nmap -sA --top-ports 5 64.13.134.52 --reason  
[sudo] password for acml77:
```

```
Starting Nmap 5.21 ( http://nmap.org ) at 2010-09-09 09:58 EDT
```

```
Nmap scan report for scanme.nmap.org (64.13.134.52)
```

```
Host is up, received echo-reply (0.10s latency).
```

PORT	STATE	SERVICE	REASON
21/tcp	filtered	ftp	no-response
22/tcp	unfiltered	ssh	reset
23/tcp	filtered	telnet	no-response
80/tcp	unfiltered	http	reset
443/tcp	filtered	https	no-response

```
Nmap done: 1 IP address (1 host up) scanned in 1.97 seconds
```

Here is your TCP foo.

Tcp full-connect*

No-response (The firewall disregards)

Syn-ack (The dude obliges)

Ack-scan

Reset (ZOMGWTF! RFC793)

```
acml77@thinktank:~/nmap/hackpgh$ sudo nmap -PN -sT --top-ports 5 ftp.xyz.com --reason
```

```
Starting Nmap 5.21 ( http://nmap.org ) at 2010-09-09 10:19 EDT
```

```
Nmap scan report for ftp.xyz.com
```

```
Host is up, received user-set (0.027s latency).
```

PORT	STATE	SERVICE	REASON
21/tcp	open	ftp	syn-ack
22/tcp	open	ssh	syn-ack
23/tcp	filtered	telnet	no-response
80/tcp	filtered	http	no-response
443/tcp	filtered	https	no-response

```
Nmap done: 1 IP address (1 host up) scanned in 1.32 seconds
```

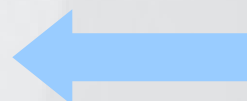
```
acml77@thinktank:~/nmap/hackpgh$ sudo nmap -PN -sA --top-ports 5 ftp.xyz.com --reason
```

```
Starting Nmap 5.21 ( http://nmap.org ) at 2010-09-09 10:19 EDT
```

```
Nmap scan report for ftp.xyz.com
```

```
Host is up, received user-set.
```

PORT	STATE	SERVICE	REASON
21/tcp	filtered	ftp	no-response
22/tcp	filtered	ssh	no-response
23/tcp	filtered	telnet	no-response
80/tcp	filtered	http	no-response
443/tcp	filtered	https	no-response



```
Nmap done: 1 IP address (1 host up) scanned in 3.16 seconds
```

No Response (This is a state-full firewall.)

acm177@thinktank: ~/nmap

```
acm177@thinktank:~/nmap$ sudo nmap -PN -sT 192.168.1.1 --reason
```

Starting Nmap 5.21 (<http://nmap.org>) at 2010-09-10 10:08 EDT

Nmap scan report for DD-WRT (192.168.1.1)

Host is up, received user-set (0.050s latency).

Not shown: 997 closed ports

Reason: 997 conn-refused

PORT	STATE	SERVICE	REASON
23/tcp	open	telnet	syn-ack
53/tcp	open	domain	syn-ack
80/tcp	open	http	syn-ack

Nmap done: 1 IP address (1 host up) scanned in 0.59 seconds

```
acm177@thinktank:~/nmap$ sudo nmap -PN -sF 192.168.1.1 --reason
```

Starting Nmap 5.21 (<http://nmap.org>) at 2010-09-10 10:08 EDT

Nmap scan report for DD-WRT (192.168.1.1)

Host is up, received arp-response (0.015s latency).

Not shown: 997 closed ports

Reason: 997 resets

PORT	STATE	SERVICE	REASON
23/tcp	open filtered	telnet	no-response
53/tcp	open filtered	domain	no-response
80/tcp	open filtered	http	no-response

MAC Address: 00:40:10:10:00:01 (Sonic Systems)

Nmap done: 1 IP address (1 host up) scanned in 1.69 seconds

```
acm177@thinktank:~/nmap$
```


Closed ports tend to reply to your FIN with a RST.
Open ports tend to ignore the packet in question.

Except for windows machines.
Open or closed, they RST.

acm177@thinktank: ~/nmap

```
acm177@thinktank:~/nmap$ sudo nmap -PN -sT 192.168.1.101 --reason
```

Starting Nmap 5.21 (<http://nmap.org>) at 2010-09-10 09:58 EDT

Nmap scan report for server-bf6087eb (192.168.1.101)

Host is up, received user-set (0.00058s latency).

Not shown: 994 closed ports

Reason: 994 conn-refused

PORT	STATE	SERVICE	REASON
80/tcp	open	http	syn-ack
135/tcp	open	msrpc	syn-ack
139/tcp	open	netbios-ssn	syn-ack
445/tcp	open	microsoft-ds	syn-ack
1025/tcp	open	NFS-or-IIS	syn-ack
3389/tcp	open	ms-term-serv	syn-ack

Nmap done: 1 IP address (1 host up) scanned in 1.24 seconds

```
acm177@thinktank:~/nmap$ sudo nmap -PN -sF 192.168.1.101 --reason
```

Starting Nmap 5.21 (<http://nmap.org>) at 2010-09-10 09:58 EDT

Nmap scan report for server-bf6087eb (192.168.1.101)

Host is up, received arp-response (0.00027s latency).

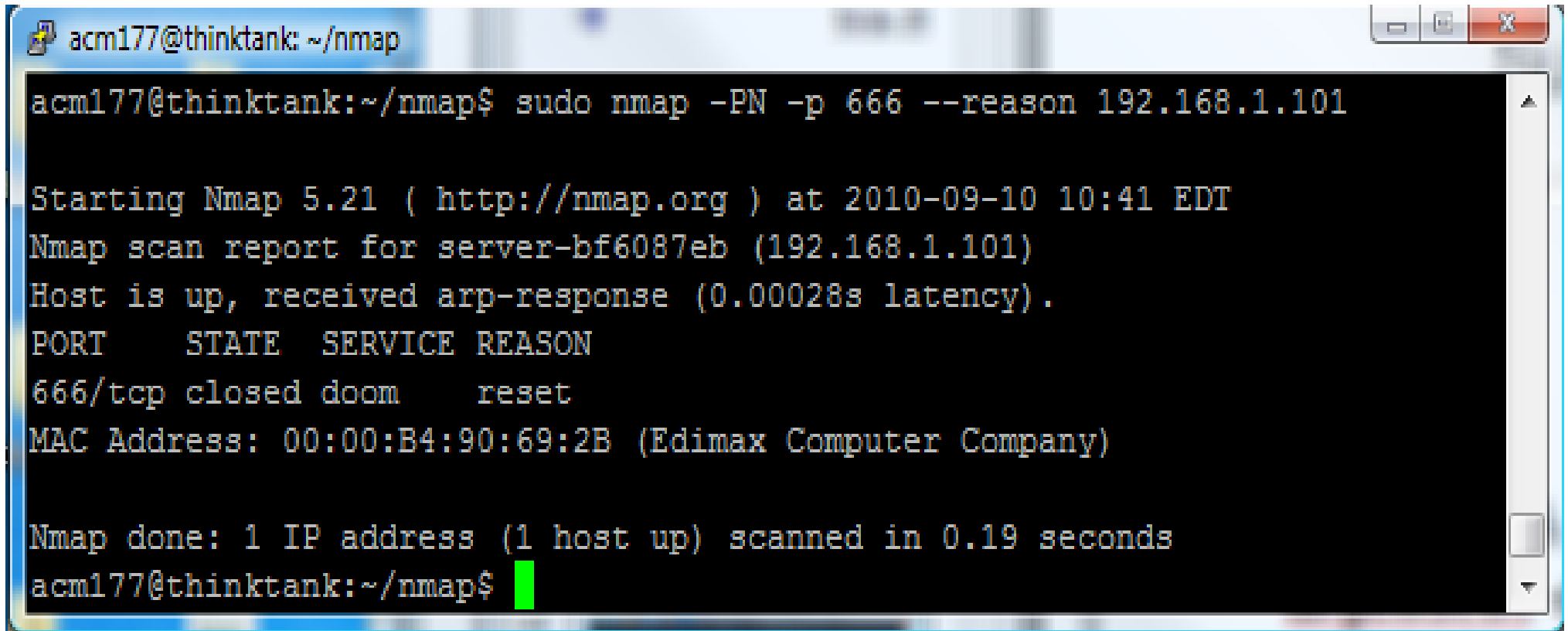
All 1000 scanned ports on server-bf6087eb (192.168.1.101) are closed because of 1000 resets

MAC Address: 00:00:B4:90:69:2B (Edimax Computer Company)

Nmap done: 1 IP address (1 host up) scanned in 1.34 seconds

```
acm177@thinktank:~/nmap$
```

A normal, actual closed port.



```
acm177@thinktank: ~/nmap
acm177@thinktank:~/nmap$ sudo nmap -PN -p 666 --reason 192.168.1.101

Starting Nmap 5.21 ( http://nmap.org ) at 2010-09-10 10:41 EDT
Nmap scan report for server-bf6087eb (192.168.1.101)
Host is up, received arp-response (0.00028s latency).
PORT      STATE  SERVICE REASON
666/tcp   closed doom      reset
MAC Address: 00:00:B4:90:69:2B (Edimax Computer Company)

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
acm177@thinktank:~/nmap$
```

SCAN TECHNIQUES:

- sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
- sU: UDP Scan
- sN/sF/sX: TCP Null, FIN, and Xmas scans

More (built in) Fingerprinting

-sV -O -sC

Or simply...



acm177@thinktank: ~/nmap

```
acm177@thinktank:~/nmap$ sudo nmap -PN -A 192.168.1.1
```

Starting Nmap 5.21 (<http://nmap.org>) at 2010-09-10 10:24 EDT

Nmap scan report for DD-WRT (192.168.1.1)

Host is up (0.0021s latency).

Not shown: 997 closed ports

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

23/tcp	open	telnet	DD-WRT telnetd (DD-WRT v24 micro (c) 2008 NewMedia-NET GmbH)
--------	------	--------	--

53/tcp	open	domain	dnsmasq 2.45
--------	------	--------	--------------

80/tcp	open	http	DD-WRT milli_httpd
--------	------	------	--------------------

|_html-title: DD-WRT - Info

|_http-favicon:

MAC Address: 00:40:10:10:00:01 (Sonic Systems)

Device type: WAP

Running: Linux 2.4.X

OS details: DD-WRT v23 - v24 (Linux 2.4.20 - 2.4.37)

Network Distance: 1 hop

Service Info: OS: Linux; Device: WAP

HOP	RTT	ADDRESS
-----	-----	---------

1	2.10 ms	DD-WRT (192.168.1.1)
---	---------	----------------------

OS and Service detection performed. Please report any incorrect results at <http://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 14.03 seconds

```
acm177@thinktank:~/nmap$
```



```
acm177@thinktank:~/nmap$ sudo nmap -PN -A 192.168.1.101
```

```
Starting Nmap 5.21 ( http://nmap.org ) at 2010-09-10 10:28 EDT
```

```
Nmap scan report for server-bf6087eb (192.168.1.101)
```

```
Host is up (0.00040s latency).
```

```
Not shown: 994 closed ports
```

PORT	STATE	SERVICE	VERSION
80/tcp	open	http	Microsoft IIS webserver 6.0
_html-title: Under Construction			
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	
445/tcp	open	microsoft-ds	Microsoft Windows 2003 or 2008 microsoft-ds
1025/tcp	open	msrpc	Microsoft Windows RPC
3389/tcp	open	microsoft-rdp	Microsoft Terminal Service

MAC Address: 00:00:B4:90:69:2B (Edimax Computer Company)

```
Device type: general purpose
```

```
Running: Microsoft Windows 2003
```

```
OS details: Microsoft Windows Server 2003 SP1 or SP2
```

```
Network Distance: 1 hop
```

```
Service Info: OS: Windows
```

```
Host script results:
```

```
|_nbstat: NetBIOS name: SERVER-BF6087EB, NetBIOS user: <unknown>, NetBIOS  
MAC: 00:00:b4:90:69:2b
```

```
| smb-os-discovery:
```

```
| OS: Windows Server 2003 3790 Service Pack 2 (Windows Server 2003 5.2)
```

```
| Name: WORKGROUP\SERVER-BF6087EB
```

```
|_ System time: 2010-09-10 10:30:20 UTC-4
```

```
|_ smbv2-enabled: Server doesn't support SMBv2 protocol
```

HOP	RTT	ADDRESS
1	0.40 ms	server-bf6087eb (192.168.1.101)

```
OS and Service detection performed. Please report any incorrect results a  
t http://nmap.org/submit/ .
```

```
Nmap done: 1 IP address (1 host up) scanned in 23.96 seconds
```

```
acm177@thinktank:~/nmap$
```

Not often remembered.

- - interactive

```
acm177@thinktank:~/nmap$ nmap --interactive
```

```
Starting Nmap V. 5.21 ( http://nmap.org )
```

```
Welcome to Interactive Mode -- press h <enter> for help
```

```
nmap> h
```

```
Nmap Interactive Commands:
```

```
n <nmap args> -- executes an nmap scan using the arguments given and  
waits for nmap to finish. Results are printed to the  
screen (of course you can still use file output commands).
```

```
! <command> -- runs shell command given in the foreground
```

```
x -- Exit Nmap
```

```
f [--spooft <fakeargs>] [--nmap-path <path>] <nmap args>
```

```
-- Executes nmap in the background (results are NOT  
printed to the screen). You should generally specify a  
file for results (with -oX, -oG, or -oN). If you specify  
fakeargs with --spooft, Nmap will try to make those  
appear in ps listings. If you wish to execute a special  
version of Nmap, specify --nmap-path.
```

```
n -h -- Obtain help with Nmap syntax
```

```
h -- Prints this help screen.
```

```
Examples:
```

```
n -sS -O -v example.com/24
```

```
f --spooft "/usr/local/bin/pico -z hello.c" -sS -oN e.log example.com/24
```

```
nmap> 
```

Summary:

```
nmap -sT
```

```
-A --osscan-limit
```

```
-T5 --min-hostgroup 100 --max-retries 2
```

```
--top-ports 10 --reason
```

```
-vv -iL DailyScan.txt -oA $(DATE)scan
```

This page intentionally blank

NetCat

the TCP/IP swiss army knife

- A Unix utility which reads and writes data across network connections, using TCP or UDP
- It is designed to be a reliable "back-end" tool that can be used directly or easily driven by other programs and scripts.

Caveat

netcat-openbsd

is not

netcat-traditional

So boring, I'm snoring

- Direct connect
 - `nc -nvlp 8080` (*server*)
 - `nc <server> 8080` (*client*)
- Stupid Chat

- Getting Shell

- -e
- AV and Me

- File Transfer

- `nc -nvlp 8080 > poopypants.txt` (server)
- `nc <server> 8080 < poopypants.txt` (client)

Don't be at a loss, NetCat really is pure awesome sauce

- Reverse Connect – The Firewall Killer
 - `nc -nvlp 8080` (client)
 - `nc <server> 8080` (server)
- Port Scanning with NetCat
(okay, it's no nmap)
 - `nc -v -n -w 2 -z <target>`

- Banner grabbing
 - `nc -v <target host> <target port>`
- PHUKD + Netcat



Still more you can do, once you master NCat too.

- Ncat is NetCat for the 21st century
 - -k keep the connection open for more than one client
 - --broker allow mutiple connections and allow communication between the clients
 - -ssl encrypt your foo
 - --telnet accept telnet negotiations

