

# Nmap Scanning Techniques

Maniac



# Nmap Scanning

- Before we dive in...
  - Port states that Nmap Identifies.
  - Types of port scanning.



# Nmap Scanning

[open]	[closed]
[filtered]	[unfiltered]
[open filtered]	[closed filtered]



# Nmap Scanning

- Syn Scans

- PRO: Very fast, most common scan used.

- CON: Funky stuff happens when a firewall, packet filter, or packet shaper is in-between you and the target.



# Nmap Scanning

- FIN Scans

- PRO: FIN Scans can sneak around non-stateful firewalls and packet filters.
- CON: Because of the way the scan is conducted, ports respond as either closed, or open/filtered. Many major OS' sent a RST regardless of open or closed.
- NOTE: Variations of this are NULL and Xmas Scans



# Nmap Scanning

- ACK Scan

- PRO: Determines filtered from unfiltered ports.
- CON: Won't tell if the port is open or closed.



# Nmap Scanning

- Window Scan

- PRO: Can tell if a port is open or closed, whereas the ACK scan cannot.
- CON: Works on only a few OS's, and sometimes acts flaky.



# Nmap Scanning

- Ok, so this is all fine and dandy, but what do I do with this?



# Scanning Techniques

- Mission

- Penetrate SCO's Firewall to discern all the open TCP ports on Docsrv.Caldera.Com.



# Hitting SCO

- Performing the initial SYN Scan.

```
# 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
```



# Hitting SCO

## 👁 FIN Scan

```
# 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
```



# Hitting SCO

## 👁 ACK Scan

```
# 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
```



# Hitting SCO

## 👁 Window Scan

```
# 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
```



# Scanning Techniques

## 👁 Mission 2

- 👁 Locate webserver(s) on the Playboy.Com network offering free images



# Hitting Playboy

- Step one, finding the network.

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 [...]
```



# Hitting Playboy

- Running the initial scan.

```
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
```



# Hitting Playboy

- Now wait a second! That took just under 21 minutes! Is there a way to cut that time down?



# Hitting Playboy

- First we need to get hosts to figure out the timing.

```
> 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
```



# Hitting Playboy

- Now we need to ping them to get a round trip time.

```
# 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
```



# Hitting Playboy

- Ok, I think we can write a better scan now.

```
nmap -T4 --max_rtt_timeout  
200 --initial_rtt_timeout 150  
--min_hostgroup 512 -P0 -p80  
-oG pb2.gnmap  
216.163.128.0/20
```



# Hitting Playboy

- OMGWTFLOL! That scanned a lot faster!

```
# 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
```



# Hitting Playboy

- 5 minutes. Thats pretty good! Can we cut it down more though?



# Hitting Playboy

- Turning off DNS (-n) in the scan...

```
# 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
```

- 46 seconds!



# Hitting Playboy

- Mmmm...pretty webserver!

```
> 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
```



# Hitting Playboy

- Well what does that first IP hand out?



- Interesting...but not what we are looking for.



# Hitting Playboy

- Well what about the 3rd entry?

Index of /

http://216.163.136.31/

Software mirrored here:

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>	27-Oct-2005 13:39	-	
<a href="#">Blastwave/</a>	25-Jan-2006 16:24	-	
<a href="#">CPAN/</a>	02-Feb-2006 04:23	-	
<a href="#">FreeBSD/</a>	12-Aug-2004 12:44	-	
<a href="#">TIME</a>	28-Oct-2005 09:00	1k	
<a href="#">apache/</a>	02-Feb-2006 11:48	-	
<a href="#">eclipse/</a>	02-Feb-2006 07:00	-	
<a href="#">fedora/</a>	09-Jun-2005 11:40	-	
<a href="#">jsan/</a>	29-Jan-2006 18:31	-	

- Eureka! We have images!



# Scanning Techniques

• Questions?



# Scanning Techniques

- The vast majority of mission data was provided by Fyodor. Thank him fellas!