PORT SCANNING TECHNIQUES

By Kris Katterjohn

03/08/07

CONTENTS

0.0 THIS PAPER

I wrote this to explain, and to be a general reference for, many popular port scanning techniques.

I put in small diagrams to help show what's going on in most sections. I have also put in examples using the Nmap Security Scanner and Hping3. They are both extremely powerful tools, and have taught me so much.

Nmap: http://insecure.org/nmap
Hping: http://hping.org

This paper assumes you have basic knowledge of the TCP/IP suite (how TCP and UDP are related, how they use IP, what IP addresses and port numbers are, and the some knowledge of the different TCP flags).

If you want a very in-depth, well written read on the TCP/IP protocol suite, I suggest the TCP/IP Illustrated volumes by W. Richard Stevens.

1.0 PORT SCAN TYPES

1.1 TCP CONNECT() SCAN

This uses the connect() system call to let the operating system establish a TCP connection. This is usually slower than scans using raw packets because it has to go through the full three-way handshake for open ports. This means

more time and more packets are used to get the same information as, say, the TCP SYN scan. This scan is also much more likely to get logged by the remote host.

```
$ nmap -sT 192.168.10.1

Starting Nmap 4.21ALPHA2 ( http://insecure.org ) at 2007-03-07 08:49 CST
Interesting ports on 192.168.10.1 (192.168.10.1):
Not shown: 1702 closed ports
PORT     STATE SERVICE
80/tcp   open  http
5190/tcp open  aol

Nmap finished: 1 IP address (1 host up) scanned in 1.459 seconds
```

1.2 TCP SYN SCAN

This scan sends raw SYN packets to a remote host and waits for a response. An open port will respond with a SYN/ACK packet, while a closed port will respond with a RST. If no response comes back, it's most likely filtered (there's probably a firewall somewhere along the way).

Open:

```
192.168.10.5  ->  192.168.10.1   SYN
192.168.10.5  <-  192.168.10.1   SYN/ACK
```

Closed:

```
192.168.10.5  ->  192.168.10.1   SYN
192.168.10.5  <-  192.168.10.1   RST/ACK
```

Filtered:

```
192.168.10.5  ->  192.168.10.1   SYN
         <no response>
```

```
# nmap -sS 192.168.10.1

Starting Nmap 4.21ALPHA2 ( http://insecure.org ) at 2007-03-07 08:50 CST
Interesting ports on 192.168.10.1 (192.168.10.1):
Not shown: 1702 closed ports
PORT     STATE SERVICE
80/tcp   open  http
5190/tcp open  aol
MAC Address: 00:0C:E5:4F:0F:AF (Motorola BCS)

Nmap finished: 1 IP address (1 host up) scanned in 1.616 seconds
```

```
# hping3 -c 1 --syn -p 80 192.168.10.1

HPING 192.168.10.1 (eth0 192.168.10.1): S set, 40 headers + 0 data bytes
len=46 ip=192.168.10.1 ttl=64 DF id=0 sport=80 flags=SA seq=0 win=5840 rtt=1.8 ms

--- 192.168.10.1 hping statistic ---
1 packets tramitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 1.7/1.7/1.7 ms



# hping3 -c 1 --syn -p 81 192.168.10.1

HPING 192.168.10.1 (eth0 192.168.10.1): S set, 40 headers + 0 data bytes
len=46 ip=192.168.10.1 ttl=64 DF id=0 sport=81 flags=RA seq=0 win=0 rtt=1.8 ms

--- 192.168.10.1 hping statistic ---
1 packets tramitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 1.7/1.7/1.7 ms
```

1.3 TCP FIN SCAN

This scan can tell us if a port is closed, but cannot distinguish between open and filtered because it shouldn't get back a response either way.

The idea is to send a FIN packet and if we get a RST, we know the port is closed. If it's not closed, the remote host shouldn't respond so it's either open or filtered.

This scan can slip past some non-stateful firewalls. One problem is that some systems don't follow the RFC and send RSTs even if it's open.

Open or filtered:

```
192.168.10.5  ->  192.168.10.1   FIN
         <no response>
```

Closed:

```
192.168.10.5  ->  192.168.10.1   FIN
192.168.10.5  <-  192.168.10.1   RST/ACK



# nmap -sF 192.168.10.1

Starting Nmap 4.21ALPHA2 ( http://insecure.org ) at 2007-03-07 08:51 CST
Interesting ports on 192.168.10.1 (192.168.10.1):
Not shown: 1702 closed ports
PORT     STATE         SERVICE
80/tcp   open|filtered http
5190/tcp open|filtered aol
MAC Address: 00:0C:E5:4F:0F:AF (Motorola BCS)

Nmap finished: 1 IP address (1 host up) scanned in 2.812 seconds
```

```
# hping3 -c 1 --fin -p 80 192.168.10.1

HPING 192.168.10.1 (eth0 192.168.10.1): F set, 40 headers + 0 data bytes

--- 192.168.10.1 hping statistic ---
1 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms



# hping3 -c 1 --fin -p 81 192.168.10.1

HPING 192.168.10.1 (eth0 192.168.10.1): F set, 40 headers + 0 data bytes
len=46 ip=192.168.10.1 ttl=64 DF id=0 sport=81 flags=RA seq=0 win=0 rtt=1.6 ms

--- 192.168.10.1 hping statistic ---
1 packets tramitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 1.6/1.6/1.6 ms
```

1.4 TCP XMAS SCAN

This is the same as the FIN Scan, with the exception of using FIN, URG, and PSH instead of just FIN.

Open or filtered:

```
192.168.10.5  ->  192.168.10.1   FIN/URG/PSH
         <no response>
```

Closed:

```
192.168.10.5  ->  192.168.10.1   FIN/URG/PSH
192.168.10.5  <-  192.168.10.1   RST/ACK



# nmap -sX 192.168.10.1

Starting Nmap 4.21ALPHA2 ( http://insecure.org ) at 2007-03-07 08:54 CST
Interesting ports on 192.168.10.1 (192.168.10.1):
Not shown: 1702 closed ports
PORT     STATE         SERVICE
80/tcp   open|filtered http
5190/tcp open|filtered aol
MAC Address: 00:0C:E5:4F:0F:AF (Motorola BCS)

Nmap finished: 1 IP address (1 host up) scanned in 2.491 seconds



# hping3 -c 1 --fin --push --urg -p 80 192.168.10.1

HPING 192.168.10.1 (eth0 192.168.10.1): FPU set, 40 headers + 0 data bytes
```

```
--- 192.168.10.1 hping statistic ---
1 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms



# hping3 -c 1 --fin --push --urg -p 81 192.168.10.1

HPING 192.168.10.1 (eth0 192.168.10.1): FPU set, 40 headers + 0 data bytes
len=46 ip=192.168.10.1 ttl=64 DF id=0 sport=81 flags=RA seq=0 win=0 rtt=2.2 ms

--- 192.168.10.1 hping statistic ---
1 packets tramitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 1.7/1.7/1.7 ms



1.5 TCP NULL SCAN

This is just like the FIN and XMAS scans, except it doesn't turn on any flags
at all.


Open or filtered:

192.168.10.5  ->  192.168.10.1   (NONE)
         <no response>


Closed:

192.168.10.5  ->  192.168.10.1   (NONE)
192.168.10.5  <-  192.168.10.1   RST/ACK



# nmap -sN 192.168.10.1

Starting Nmap 4.21ALPHA2 ( http://insecure.org ) at 2007-03-07 08:57 CST
Interesting ports on 192.168.10.1 (192.168.10.1):
Not shown: 1702 closed ports
PORT     STATE         SERVICE
80/tcp   open|filtered http
5190/tcp open|filtered aol
MAC Address: 00:0C:E5:4F:0F:AF (Motorola BCS)

Nmap finished: 1 IP address (1 host up) scanned in 2.673 seconds



# hping3 -c 1 -p 80 192.168.10.1

HPING 192.168.10.1 (eth0 192.168.10.1): NO FLAGS are set, 40 headers + 0 data bytes

--- 192.168.10.1 hping statistic ---
1 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

```
# hping3 -c 1 -p 81 192.168.10.1

HPING 192.168.10.1 (eth0 192.168.10.1): NO FLAGS are set, 40 headers + 0 data bytes
len=40 ip=192.168.10.1 ttl=64 DF id=0 sport=80 flags=RA seq=0 win=0 rtt=0.1 ms

--- 192.168.10.1 hping statistic ---
1 packets tramitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0.1/0.1/0.1 ms
```

1.6 TCP WINDOW SCAN

This is the same as the TCP ACK Scan (see Section 3.1), except it attempts to differentiate between open and closed ports. This is done by examining the Window field of the TCP header from the received RST packet. Some systems use a positive Window size for open ports, and zero for closed. Fewer systems do the exact opposite. If you scan and get tons of open ports and just a few closed ones, chances are it's the opposite. And some systems don't do either (like the one I'm scanning below), so you can't always trust it.

Open:

```
192.168.10.5  ->  192.168.10.1   ACK
192.168.10.5  <-  192.168.10.1   RST  [Window size > 0]
```

Closed:

```
192.168.10.5  ->  192.168.10.1   ACK
192.168.10.5  <-  192.168.10.1   RST  [Window size == 0]
```

Filtered:

```
192.168.10.5  ->  192.168.10.1   ACK
         <no response>
```

```
# nmap -sW 192.168.10.1

Starting Nmap 4.21ALPHA2 ( http://insecure.org ) at 2007-03-07 11:02 CST
All 1704 scanned ports on 192.168.10.1 (192.168.10.1) are closed
MAC Address: 00:0C:E5:4F:0F:AF (Motorola BCS)

Nmap finished: 1 IP address (1 host up) scanned in 1.500 seconds
```

```
# hping3 -c 1 --ack -p 80 192.168.10.1

HPING 192.168.10.1 (eth0 192.168.10.1): A set, 40 headers + 0 data bytes
len=46 ip=192.168.10.1 ttl=64 DF id=0 sport=80 flags=R seq=0 win=0 rtt=1.7 ms

--- 192.168.10.1 hping statistic ---
1 packets tramitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 5.2/5.2/5.2 ms
```

1.7 UDP SCAN

TCP may be an extremely popular protocol, but UDP gets it's share too. Services like DNS and DHCP use it. The idea is to send a UDP packet and wait for a response. If we get an ICMP Port Unreachable, that means the port is closed. If we get other ICMP unreachables, it's most likely filtered. If we actually get a UDP response back, it's open. Otherwise, it's either open (and not responding) or filtered.

Open:

```
192.168.10.5  ->  192.168.10.1   [UDP]
192.168.10.5  <-  192.168.10.1   [UDP]
```

Open or filtered:

```
192.168.10.5  ->  192.168.10.1   [UDP]
         <no response>
```

Closed:

```
192.168.10.5  ->  192.168.10.1   [UDP]
192.168.10.5  <-  192.168.10.1   [ICMP Port Unreachable]
```

Filtered:

```
192.168.10.5  ->  192.168.10.1   [UDP]
192.168.10.5  <-  192.168.10.1   [Misc. ICMP Unreachable]
```

```
# nmap -sU 192.168.10.1

Starting Nmap 4.21ALPHA2 ( http://insecure.org ) at 2007-03-07 09:18 CST
Interesting ports on 192.168.10.1 (192.168.10.1):
Not shown: 1485 closed ports
PORT     STATE         SERVICE
53/udp   open|filtered domain
67/udp   open|filtered dhcps
2049/udp open|filtered nfs
MAC Address: 00:0C:E5:4F:0F:AF (Motorola BCS)

Nmap finished: 1 IP address (1 host up) scanned in 1489.293 seconds
```

```
# hping3 -c 1 --udp -p 53 192.168.10.1

HPING 192.168.10.1 (eth0 192.168.10.1): udp mode set, 28 headers + 0 data bytes

--- 192.168.10.1 hping statistic ---
1 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

```
# hping3 -c 1 --udp -p 54 192.168.10.1

HPING 192.168.10.1 (eth0 192.168.10.1): udp mode set, 28 headers + 0 data bytes
ICMP Port Unreachable from ip=192.168.10.1 name=192.168.10.1

--- 192.168.10.1 hping statistic ---
1 packets tramitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

2.0 OTHER SCAN TYPES

This section is for scans that don't check for open or closed ports, but are similar and still very useful.

2.1 TCP ACK SCAN

Firewalls are a pain when trying to port scan. If we were using the SYN scan on a host that's firewalled, we probably wouldn't get back the SYN/ACK or RST, so we wouldn't know what's going on. This is where the ACK scan comes in. It doesn't tell us if a port is open or closed, but it does try to tell us if the firewall is stateful (keeps tracks of connections) or not (probably just denies incoming SYN packets).

If the firewall is non-stateful and just drops SYN packets, an ACK will get in because it looks like a reply to something from the other side.

If an open OR closed port receives an unexpected ACK, it should send a RST back. So if we get a RST back, then it means the firewall is non-stateful (or there's just not one in place). If we don't get a response, or some ICMP unreachable is sent, it's most likely filtered.

Unfiltered (got through firewall):

```
192.168.10.5  ->  192.168.10.1   ACK
192.168.10.5  <-  192.168.10.1   RST
```

Filtered:

```
192.168.10.5  ->  192.168.10.1   ACK
192.168.10.5  <-  192.168.10.1   [Misc. ICMP Unreachable]
              OR
         <no response>
```

```
# nmap -sA 192.168.10.1

Starting Nmap 4.21ALPHA2 ( http://insecure.org ) at 2007-03-07 09:03 CST
All 1704 scanned ports on 192.168.10.1 (192.168.10.1) are UNfiltered
MAC Address: 00:0C:E5:4F:0F:AF (Motorola BCS)

Nmap finished: 1 IP address (1 host up) scanned in 2.468 seconds
```

```
# hping3 -c 1 --ack -p 80 192.168.10.1

HPING 192.168.10.1 (eth0 192.168.10.1): A set, 40 headers + 0 data bytes
len=46 ip=192.168.10.1 ttl=64 DF id=0 sport=80 flags=R seq=0 win=0 rtt=1.7 ms

--- 192.168.10.1 hping statistic ---
1 packets tramitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 5.2/5.2/5.2 ms
```

2.2 IP PROTOCOL SCAN

This is a cool scan that looks for supported IP protocols rather than open ports. It's very similar to the UDP Scan, but it sends raw IP packets with different values in the protocol field of the header. And instead of looking for ICMP Port Unreachables, it looks for ICMP Protocol Unreachables to tell if it's closed (or, rather, unsupported). If we get a response back in the same protocol, it's open (or supported). If we get some different ICMP unreachable, it's probably filtered. If we don't get anything back, it's either open (and didn't reply) or filtered.

Supported:

```
192.168.10.5  ->  192.168.10.1   [Some IP protocol]
192.168.10.5  <-  192.168.10.1   [Same IP protocol]
```

Supported or filtered:

```
192.168.10.5  ->  192.168.10.1   [Some IP protocol]
192.168.10.5  <-  192.168.10.1   [Misc. ICMP Unreachable]
              OR
         <no response>
```

Unsupported:

```
192.168.10.5  ->  192.168.10.1   [Some IP protocol]
192.168.10.5  <-  192.168.10.1   [ICMP Protocol Unreachable]
```

```
# nmap -sO 192.168.10.1

Starting Nmap 4.21ALPHA2 ( http://insecure.org ) at 2007-03-07 09:03 CST
Interesting protocols on 192.168.10.1 (192.168.10.1):
Not shown: 252 open|filtered protocols
PROTOCOL STATE  SERVICE
1        open   icmp
2        closed igmp
6        open   tcp
17       open   udp
MAC Address: 00:0C:E5:4F:0F:AF (Motorola BCS)

Nmap finished: 1 IP address (1 host up) scanned in 5.781 seconds
```

```
# hping3 -c 1 --rawip --ipproto 0 192.168.10.1

HPING 192.168.10.1 (eth0 192.168.10.1): raw IP mode set, 20 headers + 0 data bytes

--- 192.168.10.1 hping statistic ---
1 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms



# hping3 -c 1 --icmp 192.168.10.1

HPING 192.168.10.1 (eth0 192.168.10.1): icmp mode set, 28 headers + 0 data bytes
len=46 ip=192.168.10.1 ttl=64 id=40509 icmp_seq=0 rtt=1.6 ms

--- 192.168.10.1 hping statistic ---
1 packets tramitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 18.6/18.6/18.6 ms



# hping3 -c 1 --rawip --ipproto 2 192.168.10.1

HPING 192.168.10.1 (eth0 192.168.10.1): raw IP mode set, 20 headers + 0 data bytes
ICMP Protocol Unreachable from ip=192.168.10.1 name=192.168.10.1

--- 192.168.10.1 hping statistic ---
1 packets tramitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```