
Assignment #1

Simple Personal Linux Firewall

Steffen L. Norgren
A00683006

COMP 8006 - Network Administration & Security II • BCIT • January 28, 2010

TABLE OF CONTENTS

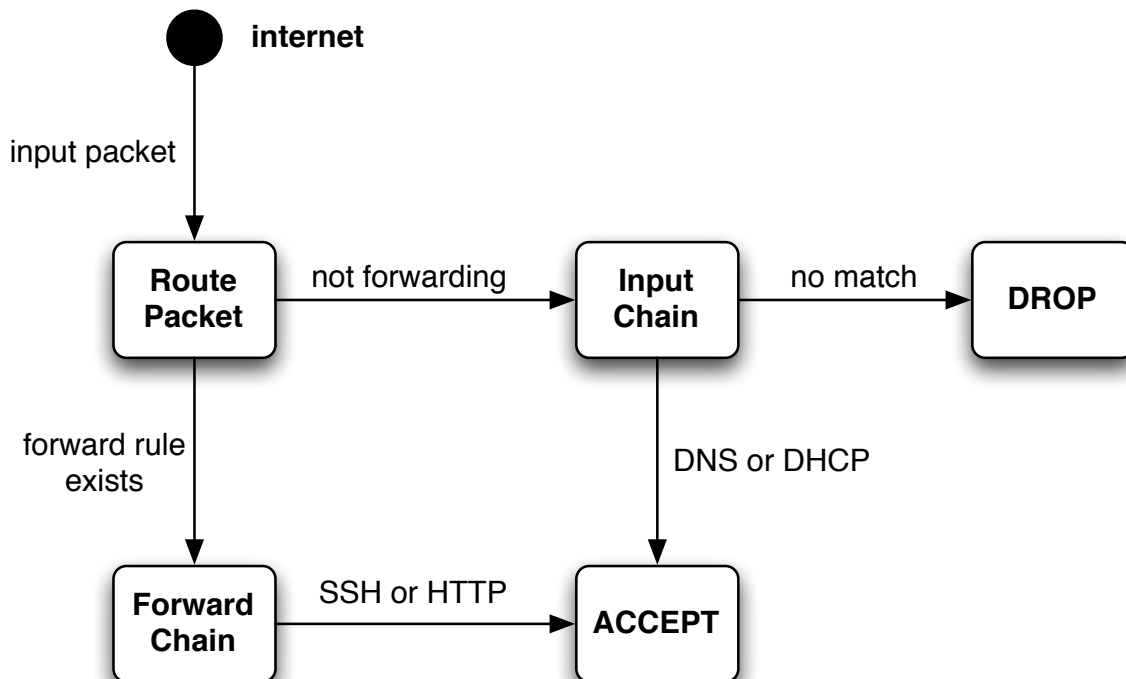
Overview	3
Design Work	3
Inbound Traffic	3
Outbound Traffic	4
Testing	5
Test Case #1	6
Test Case #2	6
Test Case #3	7
Test Case #4	8
Test Case #5	9
Test Case #6	10
Test Case #7	11

OVERVIEW

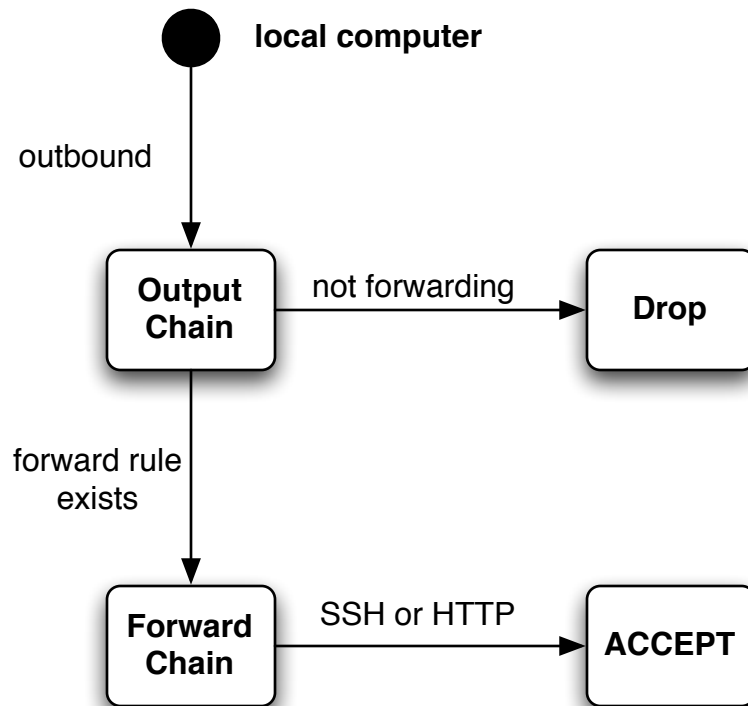
This assignment was for the purpose of creating a simple Linux firewall where everything would be blocked with the exception of SSH and HTTP traffic. To do this, I had to first create a default DROP policy and then selectively open the needed ports, which also included DHCP and DNS. Additionally, I needed make sure that the firewall allowed communication via established connections.

DESIGN WORK

Inbound Traffic



Outbound Traffic



TESTING

Rule #	Test Description	Tool Used	Expected Results	Pass/Fail
1	Permit inbound/outbound SSH packets.	Remotely access the SSH server	The iptables -L -n -v -x audit should show the traffic.	Pass. Detailed results are attached.
2	Permit inbound/outbound HTTP packets.	hping3 & opening a browser session.	hping2 should show a response on port 80 and the iptables -L -n -v -x audit should show the traffic.	Pass. Detailed results are attached.
3	Drop traffic to port 80 from source port < 1024	hping3	hping2 should not show any response and the iptables -L -n -v -x audit should NOT show the traffic.	Pass. Detailed results are attached.
4	Drop all incoming packets from/to port 0.	hping3	hping2 should not show any response and the iptables -L -n -v -x audit should show the dropped traffic.	Pass. Detailed results are attached.
5	Drop all incoming packets that have both the SYN and FIN bits set together.	hping3	hping2 should not show any response and the iptables -L -n -v -x audit should show the dropped traffic.	Pass. Detailed results are attached.
6	Allow outbound DNS & DHCP packets	nslookup	Should return results for any particular domain and the iptables -L -n -v -x audit should show the traffic.	Pass. Detailed results are attached.
7	Drop all inbound traffic except for SSH and HTTP traffic.	zenmap	Through scanning all 65535 ports, we should only see the SSH and HTTP services open. Additionally, the iptables -L -n -v -x audit should show dropped traffic.	Pass. Detailed results are attached.

Test Case #1

Before the test:

Chain inbound-acct (5 references)									
pkts	bytes	target	prot	opt	in	out	source	destination	
0	0	ACCEPT	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp spts:1024:65535 dpt:80
6	456	ACCEPT	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:22
15 600 DROP tcp -- * 0.0.0.0/0 0.0.0.0/0 tcp flags:0x3F/0x03									
Chain outbound-acct (5 references)									
pkts	bytes	target	prot	opt	in	out	source	destination	
0	0	ACCEPT	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp spt:80
0	0	ACCEPT	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:80
3	380	ACCEPT	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp spt:22
0	0	ACCEPT	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:22

After the test:

Chain inbound-acct (5 references)									
pkts	bytes	target	prot	opt	in	out	source	destination	
0	0	ACCEPT	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp spts:1024:65535 dpt:80
42	2904	ACCEPT	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:22
Chain outbound-acct (5 references)									
pkts	bytes	target	prot	opt	in	out	source	destination	
0	0	ACCEPT	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp spt:80
0	0	ACCEPT	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:80
29	30804	ACCEPT	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp spt:22
0	0	ACCEPT	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:22

Test Case #2

```
strumpet ~ # hping2 192.168.1.185 -p 80 -s 1241 -S
HPING 192.168.1.185 (eth0 192.168.1.185): S set, 40 headers + 0 data bytes
len=46 ip=192.168.1.185 ttl=64 DF id=0 sport=80 flags=RA seq=0 win=0 rtt=2.1 ms
len=46 ip=192.168.1.185 ttl=64 DF id=0 sport=80 flags=RA seq=1 win=0 rtt=242.0 ms
len=46 ip=192.168.1.185 ttl=64 DF id=0 sport=80 flags=RA seq=2 win=0 rtt=163.8 ms
len=46 ip=192.168.1.185 ttl=64 DF id=0 sport=80 flags=RA seq=3 win=0 rtt=85.4 ms
^C
--- 192.168.1.185 hping statistic ---
4 packets tramitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 2.1/123.3/242.0 ms
strumpet ~ #
```

Before the test:

Chain inbound-acct (5 references)									
pkts	bytes	target	prot	opt	in	out	source	destination	
0	0	ACCEPT	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp spts:1024:65535 dpt:80
6	456	ACCEPT	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:22
Chain outbound-acct (5 references)									
pkts	bytes	target	prot	opt	in	out	source	destination	
0	0	ACCEPT	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp spt:80
0	0	ACCEPT	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:80
3	380	ACCEPT	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp spt:22
0	0	ACCEPT	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:22

After the test:

Chain inbound-acct (5 references)									
pkts	bytes	target	prot	opt	in	out	source	destination	
4	160	ACCEPT	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp spts:1024:65535 dpt:80
12	864	ACCEPT	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:22
Chain outbound-acct (5 references)									
pkts	bytes	target	prot	opt	in	out	source	destination	
4	160	ACCEPT	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp spt:80
91	11386	ACCEPT	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:80
7	5420	ACCEPT	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp spt:22
0	0	ACCEPT	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:22

Test Case #3

```
strumpet ~ # hping2 192.168.1.185 -p 80 -s 1000 -S
HPING 192.168.1.185 (eth0 192.168.1.185): S set, 40 headers + 0 data bytes
--- 192.168.1.185 hping statistic ---
4 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Before the test:

Chain inbound-acct (5 references)									
pkts	bytes	target	prot	opt	in	out	source	destination	
0	0	ACCEPT	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp spts:1024:65535 dpt:80
6	456	ACCEPT	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:22
Chain outbound-acct (5 references)									
pkts	bytes	target	prot	opt	in	out	source	destination	
0	0	ACCEPT	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp spt:80
0	0	ACCEPT	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:80
3	380	ACCEPT	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp spt:22
0	0	ACCEPT	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:22

After the test:

Chain inbound-acct (5 references)									
pkts	bytes	target	prot	opt	in	out	source	destination	
0	0	ACCEPT	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp spts:1024:65535 dpt:80
12	864	ACCEPT	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:22
Chain outbound-acct (5 references)									
pkts	bytes	target	prot	opt	in	out	source	destination	
0	0	ACCEPT	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp spt:80
0	0	ACCEPT	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:80
7	5420	ACCEPT	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp spt:22
0	0	ACCEPT	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:22

Test Case #4

```
root@XenoTux:~$ hping3 192.168.227.130 -s 0 -d 22 -S
HPING 192.168.227.130 (eth1 192.168.227.130): S set, 40 headers + 22 data bytes
AC
--- 192.168.227.130 hping statistic ---
9 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@XenoTux:~$ hping3 192.168.227.130 -s 1234 -d 0 -S
HPING 192.168.227.130 (eth1 192.168.227.130): S set, 40 headers + 0 data bytes
AC
--- 192.168.227.130 hping statistic ---
5 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@XenoTux:~$
```

Before the test:

Chain INPUT (policy DROP 1 packets, 52 bytes)									
pkts	bytes	target	prot	opt	in	out	source	destination	
0	0	ACCEPT	all	--	lo	*	0.0.0.0/0	0.0.0.0/0	
0	0	DROP	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp spt:0
0	0	DROP	udp	--	*	*	0.0.0.0/0	0.0.0.0/0	udp spt:0
0	0	DROP	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:0
0	0	DROP	udp	--	*	*	0.0.0.0/0	0.0.0.0/0	udp dpt:0
0	0	DROP	all	--	*	*	0.0.0.0/0	0.0.0.0/0	state INVALID
0	0	DROP	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x17/0x02 state NEW
0	0	DROP	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x3F/0x00
0	0	DROP	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x3F/0x3F
0	0	DROP	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x3F/0x29
0	0	DROP	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x3F/0x37
0	0	DROP	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x06/0x06
0	0	DROP	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x03/0x03
0	0	ACCEPT	udp	--	*	*	0.0.0.0/0	0.0.0.0/0	udp spt:67 dpt:68
0	0	DROP	all	--	*	*	0.0.0.0/0	0.0.0.0/0	PKTTYPE = broadcast
40	3040	inbound-acct	tcp	--	eth0	*	0.0.0.0/0	0.0.0.0/0	
0	0	ACCEPT	all	--	eth0	*	0.0.0.0/0	0.0.0.0/0	state RELATED,ESTABLISHED

After the test:

Chain INPUT (policy DROP 1 packets, 52 bytes)									
pkts	bytes	target	prot	opt	in	out	source	destination	
0	0	ACCEPT	all	--	lo	*	0.0.0.0/0	0.0.0.0/0	
1	62	DROP	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp spt:0
0	0	DROP	udp	--	*	*	0.0.0.0/0	0.0.0.0/0	udp spt:0
13	696	DROP	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:0
0	0	DROP	udp	--	*	*	0.0.0.0/0	0.0.0.0/0	udp dpt:0
0	0	DROP	all	--	*	*	0.0.0.0/0	0.0.0.0/0	state INVALID
0	0	DROP	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x17/0x02 state NEW
0	0	DROP	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x3F/0x00
0	0	DROP	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x3F/0x3F
0	0	DROP	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x3F/0x29
0	0	DROP	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x3F/0x37
0	0	DROP	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x06/0x06
0	0	DROP	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x03/0x03
0	0	ACCEPT	udp	--	*	*	0.0.0.0/0	0.0.0.0/0	udp spt:67 dpt:68
2	274	DROP	all	--	*	*	0.0.0.0/0	0.0.0.0/0	PKTTYPE = broadcast
44	3344	inbound-acct	tcp	--	eth0	*	0.0.0.0/0	0.0.0.0/0	
0	0	ACCEPT	all	--	eth0	*	0.0.0.0/0	0.0.0.0/0	state RELATED,ESTABLISHED

Test Case #5

```
strumpet ~ # hping2 192.168.1.185 -p 22 -s 1274 -S -F
HPING 192.168.1.185 (eth0 192.168.1.185): SF set, 40 headers + 0 data bytes
--- 192.168.1.185 hping statistic ---
4 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Before the test:

Chain INPUT (policy DROP 0 packets, 0 bytes)									
pkts	bytes	target	prot	opt	in	out	source	destination	
0	0	ACCEPT	all	--	lo	*	0.0.0.0/0	0.0.0.0/0	
0	0	DROP	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp spt:0
0	0	DROP	udp	--	*	*	0.0.0.0/0	0.0.0.0/0	udp spt:0
0	0	DROP	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:0
0	0	DROP	udp	--	*	*	0.0.0.0/0	0.0.0.0/0	udp dpt:0
0	0	DROP	all	--	*	*	0.0.0.0/0	0.0.0.0/0	state INVALID
0	0	DROP	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x17/0x02 state NEW
0	0	DROP	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x3F/0x00
0	0	DROP	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x3F/0x3F
0	0	DROP	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x3F/0x29
0	0	DROP	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x3F/0x37
0	0	DROP	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x06/0x06
0	0	DROP	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x03/0x03
0	0	ACCEPT	udp	--	*	*	0.0.0.0/0	0.0.0.0/0	udp spt:67 dpt:68
0	0	DROP	all	--	*	*	0.0.0.0/0	0.0.0.0/0	PKTTYPE = broadcast
6	456	inbound-acct	tcp	--	eth0	*	0.0.0.0/0	0.0.0.0/0	
0	0	ACCEPT	all	--	eth0	*	0.0.0.0/0	0.0.0.0/0	state RELATED,ESTABLISHED

After the test:

Chain INPUT (policy DROP 0 packets, 0 bytes)									
pkts	bytes	target	prot	opt	in	out	source	destination	
0	0	ACCEPT	all	--	lo	*	0.0.0.0/0	0.0.0.0/0	
0	0	DROP	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp spt:0
0	0	DROP	udp	--	*	*	0.0.0.0/0	0.0.0.0/0	udp spt:0
0	0	DROP	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:0
0	0	DROP	udp	--	*	*	0.0.0.0/0	0.0.0.0/0	udp dpt:0
7	280	DROP	all	--	*	*	0.0.0.0/0	0.0.0.0/0	state INVALID
0	0	DROP	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x17/0x02 state NEW
0	0	DROP	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x3F/0x00
0	0	DROP	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x3F/0x3F
0	0	DROP	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x3F/0x29
0	0	DROP	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x3F/0x37
0	0	DROP	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x06/0x06
0	0	DROP	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x03/0x03
0	0	ACCEPT	udp	--	*	*	0.0.0.0/0	0.0.0.0/0	udp spt:67 dpt:68
5	823	DROP	all	--	*	*	0.0.0.0/0	0.0.0.0/0	PKTTYPE = broadcast
11	812	inbound-acct	tcp	--	eth0	*	0.0.0.0/0	0.0.0.0/0	
0	0	ACCEPT	all	--	eth0	*	0.0.0.0/0	0.0.0.0/0	state RELATED,ESTABLISHED

Test Case #6

```
root@XenoTux:/home/ironix/Assignment #1/Source$ nslookup yahoo.com
Server:                192.168.1.1
Address: 192.168.1.1#53

Non-authoritative answer:
Name:   yahoo.com
Address: 209.191.93.53
Name:   yahoo.com
Address: 69.147.114.224
Name:   yahoo.com
Address: 209.131.36.159
```

Before the test:

Chain OUTPUT (policy DROP 0 packets, 0 bytes)

pkts	bytes	target	prot	opt	in	out	source	destination	
0	0	ACCEPT	all	--	*	*	127.0.0.1	0.0.0.0/0	
0	0	ACCEPT	all	--	*	lo	0.0.0.0/0	0.0.0.0/0	
0	0	ACCEPT	udp	--	*	*	0.0.0.0/0	0.0.0.0/0	udp dpt:68 state NEW
0	0	ACCEPT	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:53 state NEW
0	0	ACCEPT	udp	--	*	*	0.0.0.0/0	0.0.0.0/0	udp dpt:53 state NEW
18	1880	outbound-acct	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	

After the test:

Chain OUTPUT (policy DROP 0 packets, 0 bytes)

pkts	bytes	target	prot	opt	in	out	source	destination	
0	0	ACCEPT	all	--	*	*	127.0.0.1	0.0.0.0/0	
0	0	ACCEPT	all	--	*	lo	0.0.0.0/0	0.0.0.0/0	
0	0	ACCEPT	udp	--	*	*	0.0.0.0/0	0.0.0.0/0	udp dpt:68 state NEW
0	0	ACCEPT	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:53 state NEW
1	55	ACCEPT	udp	--	*	*	0.0.0.0/0	0.0.0.0/0	udp dpt:53 state NEW
27	4028	outbound-acct	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	

Test Case #7

Only the SSH and HTTP ports were discovered during the scan.

```
Starting Nmap 5.00 ( http://nmap.org ) at 2010-01-28 10:17 PST
NSE: Loaded 30 scripts for scanning.
Initiating ARP Ping Scan at 10:17
Scanning 192.168.227.130 [1 port]
Completed ARP Ping Scan at 10:17, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:17
Completed Parallel DNS resolution of 1 host. at 10:17, 0.01s elapsed
Initiating SYN Stealth Scan at 10:17
Scanning 192.168.227.130 [65535 ports]
Discovered open port 22/tcp on 192.168.227.130
Discovered open port 80/tcp on 192.168.227.130
SYN Stealth Scan Timing: About 19.82% done; ETC: 10:19 (0:02:05 remaining)
SYN Stealth Scan Timing: About 47.97% done; ETC: 10:19 (0:01:06 remaining)
Completed SYN Stealth Scan at 10:19, 104.88s elapsed (65535 total ports)
Initiating Service scan at 10:19
Scanning 2 services on 192.168.227.130
Completed Service scan at 10:19, 6.01s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against 192.168.227.130
Retrying OS detection (try #2) against 192.168.227.130
NSE: Script scanning 192.168.227.130.
NSE: Starting runlevel 1 scan
Initiating NSE at 10:19
Completed NSE at 10:19, 0.10s elapsed
NSE: Script Scanning completed.
Host 192.168.227.130 is up (0.00049s latency).
Interesting ports on 192.168.227.130:
Not shown: 65533 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 5.1p1 Debian 6ubuntu2 (protocol 2.0)
|_ ssh-hostkey: 1024 d3:55:2c:2f:96:74:f3:d8:d1:37:86:7c:ce:82:31:33 (DSA)
|_ 2048 39:af:2d:6c:5a:80:89:99:ab:12:65:0c:e2:ca:eb:35 (RSA)
80/tcp    open  http     Apache httpd 2.2.12 ((Ubuntu))
|_ html-title: Site doesn't have a title (text/html).
MAC Address: 00:0C:29:25:96:01 (VMware)
```

Before the test:

```
Chain INPUT (policy DROP 15 packets, 1140 bytes)
 0 0 ACCEPT all -- lo * 0.0.0.0/0 0.0.0.0/0
Target 0 192.168.0.0 DROP tcp -- * 0.0.0.0/0 0.0.0.0/0 profile: int tcp spt:0 all TCP ports
0 0 DROP udp -- * 0.0.0.0/0 0.0.0.0/0 udp spt:0
Command: nm 0 65535 tcp -- * 0.0.0.0/0 0.0.0.0/0 tcp dpt:0
0 0 DROP udp -- * 0.0.0.0/0 0.0.0.0/0 udp dpt:0
0 0 DROP all -- * 0.0.0.0/0 0.0.0.0/0 state INVALID
0 0 DROP tcp -- * 0.0.0.0/0 0.0.0.0/0 tcp flags:0x17/0x02 state NEW
0 0 DROP tcp -- * 0.0.0.0/0 0.0.0.0/0 tcp flags:0x3F/0x00
OS host 0 0 DROP tcp -- * 0.0.0.0/0 0.0.0.0/0 tcp flags:0x3F/0x3F
0 0 DROP tcp -- * 0.0.0.0/0 0.0.0.0/0 tcp flags:0x3F/0x29
0 0 DROP tcp -- * 0.0.0.0/0 0.0.0.0/0 tcp flags:0x3F/0x37
0 0 DROP tcp -- * 0.0.0.0/0 0.0.0.0/0 tcp flags:0x06/0x06
0 0 DROP tcp -- * 0.0.0.0/0 0.0.0.0/0 tcp flags:0x03/0x03
0 0 ACCEPT udp -- * 0.0.0.0/0 0.0.0.0/0 udp spt:67 dpt:68
0 0 DROP all -- * 0.0.0.0/0 0.0.0.0/0 PKTTYPE = broadcast
6 456 inbound-acct tcp -- eth0 * 0.0.0.0/0 0.0.0.0/0 Comp 0.0.0.0/0 Ping Scan 0.0.0.0/0
0 0 ACCEPT all -- eth0 * 0.0.0.0/0 0.0.0.0/0 Int 0.0.0.0/0 Parallel D 0.0.0.0/0 state RELATED, ESTABLISHED
```

After the test:

```
Chain INPUT (policy DROP 131698 packets, 5808751 bytes)
  pkts bytes target prot opt in out source destination
  0 0 ACCEPT all -- lo * * 0.0.0.0/0 0.0.0.0/0
  0 0 DROP tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp spt:0
  0 0 DROP udp -- * * 0.0.0.0/0 0.0.0.0/0 udp spt:0
  0 0 DROP tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:0
  0 0 DROP udp -- * * 0.0.0.0/0 0.0.0.0/0 udp dpt:0
  24 1440 DROP all -- * * 0.0.0.0/0 0.0.0.0/0 state INVALID
  16 960 DROP tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp flags:0x17/0x02 state NEW
  0 0 DROP tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp flags:0x3F/0x00
  0 0 DROP tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp flags:0x3F/0x3F
  0 0 DROP tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp flags:0x3F/0x29
  0 0 DROP tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp flags:0x3F/0x37
  0 0 DROP tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp flags:0x06/0x06
  0 0 DROP tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp flags:0x03/0x03
  0 0 ACCEPT udp -- * * 0.0.0.0/0 0.0.0.0/0 udp spt:67 dpt:68
  7 959 DROP all -- * * 0.0.0.0/0 0.0.0.0/0 PKTTYPE = broadcast
  131333 5781033 inbound-acct tcp -- eth0 * 0.0.0.0/0 0.0.0.0/0
  0 0 ACCEPT all -- eth0 * 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED
```