Jake Wheeler
CS445
02/24/2017
HW2

1) tcpConnect.py

```
#!/usr/bin/env python
import sys
import random
from scapy.all import *
conf.verb=0

source=sys.argv[1]
target=sys.argv[2]

ports =[20, 21, 22, 23, 25, 80, 43, 53, 69, 443]
for port in ports:
  sourceport = random.randrange(1,65535)
  outString = "Scanning " + target + ":" + str(port) + " from " + source + ":" + str(sourceport)
  print outString
  p1=IP(dst=target,src=source)/TCP(dport=port,sport=sourceport,flags='S')
  r1=sr1(p1)
  if r1[TCP].flags == 18:
    print " Port " + str(port) +  " open."
  if r1[TCP].flags == 20:
    print " Port " + str(port) + " closed."
sys.exit(0)
```

OUTPUT:

```
Scanning 192.168.100.196:20 from 192.168.100.220:28326
 Port 20 closed.
Scanning 192.168.100.196:21 from 192.168.100.220:23740
 Port 21 closed.
Scanning 192.168.100.196:22 from 192.168.100.220:41453
 Port 22 closed.
Scanning 192.168.100.196:23 from 192.168.100.220:374
 Port 23 closed.
Scanning 192.168.100.196:25 from 192.168.100.220:23817
 Port 25 closed.
Scanning 192.168.100.196:80 from 192.168.100.220:32324
 Port 80 open.
Scanning 192.168.100.196:43 from 192.168.100.220:12624
 Port 43 closed.
Scanning 192.168.100.196:53 from 192.168.100.220:45976
 Port 53 closed.
Scanning 192.168.100.196:69 from 192.168.100.220:64348
 Port 69 closed.
Scanning 192.168.100.196:443 from 192.168.100.220:64173
 Port 443 closed.
```

2) xmasScan.py

```
#!/usr/bin/env python
import sys
import random
from scapy.all import *
conf.verb=0

source=sys.argv[1]
target=sys.argv[2]

ports =[20, 21, 22, 23, 25, 80, 43, 53, 69, 443]
for port in ports:
	sourceport = random.randrange(1,65535)
	outString = "Scanning " + target + ":" + str(port) + " from " + source + ":" +
str(sourceport)
	print outString
	p1=IP(dst=target,src=source)/TCP(dport=port,sport=sourceport,flags=41)
	r1=sr1(p1, timeout=2)
	if r1 is None:
		print " Port " + str(port) +  " open/filtered."
	elif r1[TCP].flags == 20:
		print " Port " + str(port) + " closed."
sys.exit(0)
```

OUTPUT:

```
Scanning 192.168.100.196:20 from 192.168.100.220:51110
 Port 20 closed.
Scanning 192.168.100.196:21 from 192.168.100.220:59425
 Port 21 closed.
Scanning 192.168.100.196:22 from 192.168.100.220:35340
 Port 22 closed.
Scanning 192.168.100.196:23 from 192.168.100.220:6254
 Port 23 closed.
Scanning 192.168.100.196:25 from 192.168.100.220:53340
 Port 25 closed.
Scanning 192.168.100.196:80 from 192.168.100.220:37597
 Port 80 open/filtered.
Scanning 192.168.100.196:43 from 192.168.100.220:24571
 Port 43 closed.
Scanning 192.168.100.196:53 from 192.168.100.220:61359
 Port 53 closed.
Scanning 192.168.100.196:69 from 192.168.100.220:12156
 Port 69 closed.
Scanning 192.168.100.196:443 from 192.168.100.220:19085
 Port 443 closed.
```

nmap -sT:

```
Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2017-02-23 17:23 PST
Nmap scan report for kali-linux-0.isolated (192.168.100.196)
Host is up (0.00069s latency).
PORT    STATE  SERVICE
20/tcp  closed ftp-data
21/tcp  closed ftp
22/tcp  closed ssh
23/tcp  closed telnet
25/tcp  closed smtp
43/tcp  closed whois
53/tcp  closed domain
69/tcp  closed tftp
80/tcp  open   http
443/tcp closed https
MAC Address: 52:54:00:03:5E:00 (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
```

nmap -sX:

```
Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2017-02-23 17:23 PST
Nmap scan report for kali-linux-0.isolated (192.168.100.196)
Host is up (0.00031s latency).
PORT    STATE         SERVICE
20/tcp  closed        ftp-data
21/tcp  closed        ftp
22/tcp  closed        ssh
23/tcp  closed        telnet
25/tcp  closed        smtp
43/tcp  closed        whois
53/tcp  closed        domain
69/tcp  closed        tftp
80/tcp  open|filtered http
443/tcp closed        https
MAC Address: 52:54:00:03:5E:00 (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.35 seconds
```

3. Performance was pretty similar between my scripts and nmap, with the exception of the xmas scan. The nmap -sX was slightly faster at producing results than my xmasScan.py, but I believe that is simply due to the timeout value that I provided when sending the packet. The status of each of the ports on each script/nmap call showed to be consistent. Port 80 showed as open with the tcp connect scan method, but open/filtered with the xmas scan method. This is due to the fact that the sent packet was not responded to because of a firewall filter or an open port, there is no way to differentiate the two with this scanning method.