COMP 7005
Assignment 3

Testing

Daryush Balsara
A01265967
Nov, 1 2024

Testing 1
Purpose 3
Tests 3
Test 1 4
Test 2 5
Test 3 7
Test 4 8
Test 5 (output is too long so i cut it off) 9
Test 6 10
Test 7 11
Test 8 12
Test 9 12
Test 10 13
Test 11 13

Purpose

- Build a basic port scanner that mimics the behavior of hping3 using scapy. This scanning technique is known as a TCP SYN scan and is commonly used because it provides basic information about the target's services without fully opening a TCP connection.

Tests

Test	Expected	Actual	Screenshot
-h	pass	pass	Test 1
Test on localhost	pass	pass	Test 2
Test scanning on a different device on the network	pass	pass	Test 3
Test with a delay of 100 between tests	pass	pass	Test 4
Test with default start and end ports	pass	pass	Test 5
Test with no start port and the end port at 50	pass	pass	Test 6
Test with start port at 65495 and no end port	pass	pass	Test 7
Test with start port end port and delay	pass	pass	Test 8
Test with invalid IP	fail	fail	Test 9
Test with invalid delay	fail	fail	Test 10
Test with wrong ports	fail	fail	Test 11

Test 1

```
…/7005_scapy_crafting/source on ᚠ main via 🐍 pyenv
→ python port_scanner.py -h
usage: port_scanner.py [-h] [-s START] [-e END] [-d DELAY] ip

Basic port scanner that mimics the behaviour of hping3. If no start and end port is specified then it defaults the scan from port 1-65535

positional arguments:
  ip                    Target IP address to capture on

options:
  -h, --help            show this help message and exit
  -s START, --start START
                        Start port number (default is 1)
  -e END, --end END     End port number (default is 65535)
  -d DELAY, --delay DELAY
                        Delay in milliseconds between each scan
```

Test 2

```
→ doas python port_scanner.py 127.0.0.1 -e 50 -d 100
doas (daryush@JetFire) password:
Port 1 on 127.0.0.1 is closed
Port 2 on 127.0.0.1 is closed
Port 3 on 127.0.0.1 is closed
Port 4 on 127.0.0.1 is closed
Port 5 on 127.0.0.1 is closed
Port 6 on 127.0.0.1 is closed
Port 7 on 127.0.0.1 is closed
Port 8 on 127.0.0.1 is closed
Port 9 on 127.0.0.1 is closed
Port 10 on 127.0.0.1 is closed
Port 11 on 127.0.0.1 is closed
Port 12 on 127.0.0.1 is closed
Port 13 on 127.0.0.1 is closed
Port 14 on 127.0.0.1 is closed
Port 15 on 127.0.0.1 is closed
Port 16 on 127.0.0.1 is closed
Port 17 on 127.0.0.1 is closed
Port 18 on 127.0.0.1 is closed
Port 19 on 127.0.0.1 is closed
Port 20 on 127.0.0.1 is closed
Port 21 on 127.0.0.1 is closed
Port 22 on 127.0.0.1 is open
Port 23 on 127.0.0.1 is closed
Port 24 on 127.0.0.1 is closed
Port 25 on 127.0.0.1 is closed
Port 26 on 127.0.0.1 is closed
Port 27 on 127.0.0.1 is closed
Port 28 on 127.0.0.1 is closed
Port 29 on 127.0.0.1 is closed
Port 30 on 127.0.0.1 is closed
Port 31 on 127.0.0.1 is closed
Port 32 on 127.0.0.1 is closed
Port 33 on 127.0.0.1 is closed
Port 34 on 127.0.0.1 is closed
Port 35 on 127.0.0.1 is closed
Port 36 on 127.0.0.1 is closed
Port 37 on 127.0.0.1 is closed
Port 38 on 127.0.0.1 is closed
Port 39 on 127.0.0.1 is closed
Port 40 on 127.0.0.1 is closed
Port 41 on 127.0.0.1 is closed
Port 42 on 127.0.0.1 is closed
Port 43 on 127.0.0.1 is closed
Port 44 on 127.0.0.1 is closed
Port 45 on 127.0.0.1 is closed
Port 46 on 127.0.0.1 is closed
Port 47 on 127.0.0.1 is closed
Port 48 on 127.0.0.1 is closed
Port 49 on 127.0.0.1 is closed
Port 50 on 127.0.0.1 is closed
```

Test 3

```
../7005_scapy_crafting/source on  main via  pyenv took 6s
❯ doas python port_scanner.py 192.168.50.98 -s 22 -e 50 -d 100
doas (daryush@JetFire) password:
Port 22 on 192.168.50.98 is open
Port 23 on 192.168.50.98 is closed
Port 24 on 192.168.50.98 is closed
Port 25 on 192.168.50.98 is closed
Port 26 on 192.168.50.98 is closed
Port 27 on 192.168.50.98 is closed
Port 28 on 192.168.50.98 is closed
Port 29 on 192.168.50.98 is closed
Port 30 on 192.168.50.98 is closed
Port 31 on 192.168.50.98 is closed
Port 32 on 192.168.50.98 is closed
Port 33 on 192.168.50.98 is closed
Port 34 on 192.168.50.98 is closed
Port 35 on 192.168.50.98 is closed
Port 36 on 192.168.50.98 is closed
Port 37 on 192.168.50.98 is closed
Port 38 on 192.168.50.98 is closed
Port 39 on 192.168.50.98 is closed
Port 40 on 192.168.50.98 is closed
Port 41 on 192.168.50.98 is closed
Port 42 on 192.168.50.98 is closed
Port 43 on 192.168.50.98 is closed
Port 44 on 192.168.50.98 is closed
Port 45 on 192.168.50.98 is closed
Port 46 on 192.168.50.98 is closed
Port 47 on 192.168.50.98 is closed
Port 48 on 192.168.50.98 is closed
Port 49 on 192.168.50.98 is closed
Port 50 on 192.168.50.98 is closed
```

Test 4

```
…/7005_scapy_crafting/source on ᚠ main via 🐍 pyenv took 2s
❯ doas python port_scanner.py 192.168.50.98 -s 50 -e 80 -d 100
doas (daryush@JetFire) password:
Port 50 on 192.168.50.98 is closed
Port 51 on 192.168.50.98 is closed
Port 52 on 192.168.50.98 is closed
Port 53 on 192.168.50.98 is closed
Port 54 on 192.168.50.98 is closed
Port 55 on 192.168.50.98 is closed
Port 56 on 192.168.50.98 is closed
Port 57 on 192.168.50.98 is closed
Port 58 on 192.168.50.98 is closed
Port 59 on 192.168.50.98 is closed
Port 60 on 192.168.50.98 is closed
Port 61 on 192.168.50.98 is closed
Port 62 on 192.168.50.98 is closed
Port 63 on 192.168.50.98 is closed
Port 64 on 192.168.50.98 is closed
Port 65 on 192.168.50.98 is closed
Port 66 on 192.168.50.98 is closed
Port 67 on 192.168.50.98 is closed
Port 68 on 192.168.50.98 is closed
Port 69 on 192.168.50.98 is closed
Port 70 on 192.168.50.98 is closed
Port 71 on 192.168.50.98 is closed
Port 72 on 192.168.50.98 is closed
Port 73 on 192.168.50.98 is closed
Port 74 on 192.168.50.98 is closed
Port 75 on 192.168.50.98 is closed
Port 76 on 192.168.50.98 is closed
Port 77 on 192.168.50.98 is closed
Port 78 on 192.168.50.98 is closed
Port 79 on 192.168.50.98 is closed
Port 80 on 192.168.50.98 is closed
```

Test 5 (output is too long so i cut it off)

```
…/7005_scapy_crafting/source on ᚠ main via pyenv took 10s
→ doas python port_scanner.py 192.168.50.98
doas (daryush@JetFire) password:
Port 1 on 192.168.50.98 is closed
Port 2 on 192.168.50.98 is closed
Port 3 on 192.168.50.98 is closed
Port 4 on 192.168.50.98 is closed
Port 5 on 192.168.50.98 is closed
Port 6 on 192.168.50.98 is closed
Port 7 on 192.168.50.98 is closed
Port 8 on 192.168.50.98 is closed
Port 9 on 192.168.50.98 is closed
Port 10 on 192.168.50.98 is closed
Port 11 on 192.168.50.98 is closed
Port 12 on 192.168.50.98 is closed
Port 13 on 192.168.50.98 is closed
Port 14 on 192.168.50.98 is closed
Port 15 on 192.168.50.98 is closed
Port 16 on 192.168.50.98 is closed
Port 17 on 192.168.50.98 is closed
Port 18 on 192.168.50.98 is closed
Port 19 on 192.168.50.98 is closed
Port 20 on 192.168.50.98 is closed
Port 21 on 192.168.50.98 is closed
Port 22 on 192.168.50.98 is open
Port 23 on 192.168.50.98 is closed
Port 24 on 192.168.50.98 is closed
Port 25 on 192.168.50.98 is closed
Port 26 on 192.168.50.98 is closed
Port 27 on 192.168.50.98 is closed
Port 28 on 192.168.50.98 is closed
Port 29 on 192.168.50.98 is closed
Port 30 on 192.168.50.98 is closed
Port 31 on 192.168.50.98 is closed
Port 32 on 192.168.50.98 is closed
Port 33 on 192.168.50.98 is closed
Port 34 on 192.168.50.98 is closed
Port 35 on 192.168.50.98 is closed
Port 36 on 192.168.50.98 is closed
Port 37 on 192.168.50.98 is closed
Port 38 on 192.168.50.98 is closed
Port 39 on 192.168.50.98 is closed
Port 40 on 192.168.50.98 is closed
Port 41 on 192.168.50.98 is closed
Port 42 on 192.168.50.98 is closed
```

Test 6

```
❯ doas python port_scanner.py 192.168.50.98 -e 50
doas (daryush@JetFire) password:
Port 1 on 192.168.50.98 is closed
Port 2 on 192.168.50.98 is closed
Port 3 on 192.168.50.98 is closed
Port 4 on 192.168.50.98 is closed
Port 5 on 192.168.50.98 is closed
Port 6 on 192.168.50.98 is closed
Port 7 on 192.168.50.98 is closed
Port 8 on 192.168.50.98 is closed
Port 9 on 192.168.50.98 is closed
Port 10 on 192.168.50.98 is closed
Port 11 on 192.168.50.98 is closed
Port 12 on 192.168.50.98 is closed
Port 13 on 192.168.50.98 is closed
Port 14 on 192.168.50.98 is closed
Port 15 on 192.168.50.98 is closed
Port 16 on 192.168.50.98 is closed
Port 17 on 192.168.50.98 is closed
Port 18 on 192.168.50.98 is closed
Port 19 on 192.168.50.98 is closed
Port 20 on 192.168.50.98 is closed
Port 21 on 192.168.50.98 is closed
Port 22 on 192.168.50.98 is open
Port 23 on 192.168.50.98 is closed
Port 24 on 192.168.50.98 is closed
Port 25 on 192.168.50.98 is closed
Port 26 on 192.168.50.98 is closed
Port 27 on 192.168.50.98 is closed
Port 28 on 192.168.50.98 is closed
Port 29 on 192.168.50.98 is closed
Port 30 on 192.168.50.98 is closed
Port 31 on 192.168.50.98 is closed
Port 32 on 192.168.50.98 is closed
Port 33 on 192.168.50.98 is closed
Port 34 on 192.168.50.98 is closed
Port 35 on 192.168.50.98 is closed
Port 36 on 192.168.50.98 is closed
Port 37 on 192.168.50.98 is closed
Port 38 on 192.168.50.98 is closed
Port 39 on 192.168.50.98 is closed
Port 40 on 192.168.50.98 is closed
Port 41 on 192.168.50.98 is closed
Port 42 on 192.168.50.98 is closed
Port 43 on 192.168.50.98 is closed
Port 44 on 192.168.50.98 is closed
Port 45 on 192.168.50.98 is closed
Port 46 on 192.168.50.98 is closed
Port 47 on 192.168.50.98 is closed
Port 48 on 192.168.50.98 is closed
Port 49 on 192.168.50.98 is closed
Port 50 on 192.168.50.98 is closed
```

Test 7

```
…/7005_scapy_crafting/source on main via pyenv took 11s
→ doas python port_scanner.py 192.168.50.98 -s 65495
doas (daryush@JetFire) password:
Port 65495 on 192.168.50.98 is closed
Port 65496 on 192.168.50.98 is closed
Port 65497 on 192.168.50.98 is closed
Port 65498 on 192.168.50.98 is closed
Port 65499 on 192.168.50.98 is closed
Port 65500 on 192.168.50.98 is closed
Port 65501 on 192.168.50.98 is closed
Port 65502 on 192.168.50.98 is closed
Port 65503 on 192.168.50.98 is closed
Port 65504 on 192.168.50.98 is closed
Port 65505 on 192.168.50.98 is closed
Port 65506 on 192.168.50.98 is closed
Port 65507 on 192.168.50.98 is closed
Port 65508 on 192.168.50.98 is closed
Port 65509 on 192.168.50.98 is closed
Port 65510 on 192.168.50.98 is closed
Port 65511 on 192.168.50.98 is closed
Port 65512 on 192.168.50.98 is closed
Port 65513 on 192.168.50.98 is closed
Port 65514 on 192.168.50.98 is closed
Port 65515 on 192.168.50.98 is closed
Port 65516 on 192.168.50.98 is closed
Port 65517 on 192.168.50.98 is closed
Port 65518 on 192.168.50.98 is closed
Port 65519 on 192.168.50.98 is closed
Port 65520 on 192.168.50.98 is closed
Port 65521 on 192.168.50.98 is closed
Port 65522 on 192.168.50.98 is closed
Port 65523 on 192.168.50.98 is closed
Port 65524 on 192.168.50.98 is closed
Port 65525 on 192.168.50.98 is closed
Port 65526 on 192.168.50.98 is closed
Port 65527 on 192.168.50.98 is closed
Port 65528 on 192.168.50.98 is closed
Port 65529 on 192.168.50.98 is closed
Port 65530 on 192.168.50.98 is closed
Port 65531 on 192.168.50.98 is closed
Port 65532 on 192.168.50.98 is closed
Port 65533 on 192.168.50.98 is closed
Port 65534 on 192.168.50.98 is closed
Port 65535 on 192.168.50.98 is closed
```

Test 8

```
…/7005_scapy_crafting/source on main via pyenv took 5s
→ doas python port_scanner.py 192.168.50.98 -s 65495 -e 65535 -d 10
doas (daryush@JetFire) password:
Port 65495 on 192.168.50.98 is closed
Port 65496 on 192.168.50.98 is closed
Port 65497 on 192.168.50.98 is closed
Port 65498 on 192.168.50.98 is closed
Port 65499 on 192.168.50.98 is closed
Port 65500 on 192.168.50.98 is closed
Port 65501 on 192.168.50.98 is closed
Port 65502 on 192.168.50.98 is closed
Port 65503 on 192.168.50.98 is closed
Port 65504 on 192.168.50.98 is closed
Port 65505 on 192.168.50.98 is closed
Port 65506 on 192.168.50.98 is closed
Port 65507 on 192.168.50.98 is closed
Port 65508 on 192.168.50.98 is closed
Port 65509 on 192.168.50.98 is closed
Port 65510 on 192.168.50.98 is closed
Port 65511 on 192.168.50.98 is closed
Port 65512 on 192.168.50.98 is closed
Port 65513 on 192.168.50.98 is closed
Port 65514 on 192.168.50.98 is closed
Port 65515 on 192.168.50.98 is closed
Port 65516 on 192.168.50.98 is closed
Port 65517 on 192.168.50.98 is closed
Port 65518 on 192.168.50.98 is closed
Port 65519 on 192.168.50.98 is closed
Port 65520 on 192.168.50.98 is closed
Port 65521 on 192.168.50.98 is closed
Port 65522 on 192.168.50.98 is closed
Port 65523 on 192.168.50.98 is closed
Port 65524 on 192.168.50.98 is closed
Port 65525 on 192.168.50.98 is closed
Port 65526 on 192.168.50.98 is closed
Port 65527 on 192.168.50.98 is closed
Port 65528 on 192.168.50.98 is closed
Port 65529 on 192.168.50.98 is closed
Port 65530 on 192.168.50.98 is closed
Port 65531 on 192.168.50.98 is closed
Port 65532 on 192.168.50.98 is closed
Port 65533 on 192.168.50.98 is closed
Port 65534 on 192.168.50.98 is closed
Port 65535 on 192.168.50.98 is closed
```

Test 9

```
…/7005_scapy_crafting/source on main [!] via pyenv took 12s
→ doas python port_scanner.py 192.168.2
doas (daryush@JetFire) password:
usage: port_scanner.py [-h] [-s START] [-e END] [-d DELAY] ip
port_scanner.py: error: argument ip: invalid ip_address value: '192.168.2'
```

Test 10

```
…/7005_scapy_crafting/source on main [!] via pyenv took 5s
→ doas python port_scanner.py 192.168.50.98 -d test
doas (daryush@JetFire) password:
usage: port_scanner.py [-h] [-s START] [-e END] [-d DELAY] ip
port_scanner.py: error: argument -d/--delay: invalid int value: 'test'
```

Test 11

```
…/7005_scapy_crafting/source on main [!] via pyenv took 19s
→ doas python port_scanner.py 192.168.50.98 -s 68970 -e 69000
doas (daryush@JetFire) password:
ERROR: --- Error sending packets
Traceback (most recent call last):
  File "/usr/lib/python3.12/site-packages/scapy/sendrecv.py", line 273, in _sndrcv_snd
    self.hsent.setdefault(p.hashret(), []).append(p)
                          ^^^^^^^^^^^
  File "/usr/lib/python3.12/site-packages/scapy/layers/inet.py", line 594, in hashret
    struct.pack("B", self.proto) + self.payload.hashret())
                                   ^^^^^^^^^^^^^^^^^^^^^^
  File "/usr/lib/python3.12/site-packages/scapy/layers/inet.py", line 774, in hashret
    return struct.pack("H", self.sport ^ self.dport) + self.payload.hashret()  # noqa: E501
           ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
struct.error: 'H' format requires 0 <= number <= 65535
Port 68970 on 192.168.50.98 is filtered
ERROR: --- Error sending packets
Traceback (most recent call last):
  File "/usr/lib/python3.12/site-packages/scapy/sendrecv.py", line 273, in _sndrcv_snd
    self.hsent.setdefault(p.hashret(), []).append(p)
                          ^^^^^^^^^^^
  File "/usr/lib/python3.12/site-packages/scapy/layers/inet.py", line 594, in hashret
    struct.pack("B", self.proto) + self.payload.hashret())
                                   ^^^^^^^^^^^^^^^^^^^^^^
  File "/usr/lib/python3.12/site-packages/scapy/layers/inet.py", line 774, in hashret
    return struct.pack("H", self.sport ^ self.dport) + self.payload.hashret()  # noqa: E501
           ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
struct.error: 'H' format requires 0 <= number <= 65535
Port 68971 on 192.168.50.98 is filtered
ERROR: more --- Error sending packets
Traceback (most recent call last):
  File "/usr/lib/python3.12/site-packages/scapy/sendrecv.py", line 273, in _sndrcv_snd
    self.hsent.setdefault(p.hashret(), []).append(p)
                          ^^^^^^^^^^^
  File "/usr/lib/python3.12/site-packages/scapy/layers/inet.py", line 594, in hashret
    struct.pack("B", self.proto) + self.payload.hashret())
                                   ^^^^^^^^^^^^^^^^^^^^^^
  File "/usr/lib/python3.12/site-packages/scapy/layers/inet.py", line 774, in hashret
    return struct.pack("H", self.sport ^ self.dport) + self.payload.hashret()  # noqa: E501
           ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
struct.error: 'H' format requires 0 <= number <= 65535
```