

PSEC CA1-2 Comprehensive Tests & Reflection

Swaathi Lakshmanan | P2227171 | DISM/FT/1B/05

Main menu	2
Nmap	2
FTP	2
Custom Packet sender	3
Screenshots	5
Reflection	22
Checklist	22

Main menu

Test data	Expected result	Screenshot
Type letters, special characters and numbers not within 1 and 4	Should prompt for another input.	Figure 1
Type a number between 1 to 4.	Should perform relevant service.	Figure 2

Nmap

Test data	Expected result	Screenshot
Type 1 in main menu	Service should run and a table should be printed.	Figure 2

FTP

Test data		Expected result	Screenshot
Sub menu			
Type letters, special characters and numbers not within 1 and 2		Should prompt for another input.	Figure 3
Type 1 or 2		Should perform relevant service.	Figure 4
Service itself			
File type	Upload to ftpServerData	File should upload	Figure 5, 6, 7, 8, 9. 10, 11, 12
excel			
text			

json			
csv			
File type	Download to ftpClientData	File should download	Figure 13, 14, 15, 16, 17, 18, 19, 20
excel			
text			
json			
csv			
Enter a file number that is not within the range of files displayed for upload.		There should be a prompt for another number.	Figure 22
Enter a file number that is within the range of files displayed for upload.		The correct file should be uploaded.	Figure 5, 6, 7, 8, 9. 10, 11, 12
Enter a file number that is not within the range of files displayed for download.		There should be a prompt for another number.	Figure 21
Enter a file number that is within the range of files displayed for download.		The correct file should be downloaded.	Figure 13, 14, 15, 16, 17, 18, 19, 20

Custom Packet sender

Test data	Expected result	Screenshot
Source address		
Enter invalid host address to test regex.	There should be a prompt for another input.	Figure 23
Enter invalid host address to check if code is checking for associated ip address	There should be a prompt for another input.	Figure 24
Enter valid host address	The next prompt should be printed.	Figure 23
Port number		

Enter a port number bigger than the port range.	There should be a prompt for another input.	Figure 25
Enter a port number smaller than the port range.	There should be a prompt for another input.	Figure 25
Enter letters or special characters	There should be a prompt for another input.	Figure 25
Enter a valid port	The next prompt should be printed.	Figure 25
Packet type		
Enter a invalid packet type.	There should be a prompt for another input.	Figure 26
Enter a valid packet type.	The next prompt should be asked	Figure 26
RAW data		
Enter nothing	DISM-DISM-DISM-DISM should be displayed	Figure 27, 29
Enter some raw data	That raw data should be displayed	Figure 30
Number of packets		
Enter a packet number bigger than allowed range.	There should be a prompt for another input.	Figure 28
Enter a invalid packet number (letter, special characters)	There should be a prompt for another input.	Figure 28
Enter a packet number smaller than allowed range.	There should be a prompt for another input.	Figure 28
Enter a valid packet number.	The next prompt should be asked	Figure 28
Starting		
Enter a letter that is not y or just press enter	Packets should not be sent	Figure 32, 33
Enter 'y'	Packets should be sent.	Figure 31

Screenshots

```
** PSEC Info Security Apps **
1) Scan network
2) Upload/download file using FTP
3) Send custom packet
4) Quit

Your input: 5
Invalid input. Enter an integer within given range.
** PSEC Info Security Apps **
1) Scan network
2) Upload/download file using FTP
3) Send custom packet
4) Quit

Your input: -1
Invalid input. Enter an integer within given range.
** PSEC Info Security Apps **
1) Scan network
2) Upload/download file using FTP
3) Send custom packet
4) Quit

Your input: a
Invalid input. Enter an integer within given range.
** PSEC Info Security Apps **
1) Scan network
2) Upload/download file using FTP
3) Send custom packet
4) Quit

Your input: $
Invalid input. Enter an integer within given range.
** PSEC Info Security Apps **
```

Figure 1

```
Type of nmapScan : <class 'nmap.nmap.PortScanner'>
Scanning ports: localhost scanme.nmap.org
type of results: <class 'dict'>
```

Host	Hostname	Protocol	port ID	State	Product	Extrainfo	Reason	CPE
127.0.0.1	localhost	tcp	21	filtered			no-response	
127.0.0.1	localhost	tcp	22	filtered			no-response	
127.0.0.1	localhost	tcp	23	filtered			no-response	
127.0.0.1	localhost	tcp	25	filtered			no-response	
127.0.0.1	localhost	tcp	80	filtered			no-response	
127.0.0.1	localhost	tcp	110	filtered			no-response	
127.0.0.1	localhost	tcp	139	filtered			no-response	
127.0.0.1	localhost	tcp	443	filtered			no-response	
127.0.0.1	localhost	tcp	445	open			syn-ack	
127.0.0.1	localhost	tcp	3389	filtered			no-response	
127.0.0.1	localhost	udp	53	closed			port-unreach	
127.0.0.1	localhost	udp	67	closed			port-unreach	
127.0.0.1	localhost	udp	123	open filtered			no-response	
127.0.0.1	localhost	udp	135	closed			port-unreach	
127.0.0.1	localhost	udp	137	open filtered			no-response	
127.0.0.1	localhost	udp	138	closed			port-unreach	
127.0.0.1	localhost	udp	161	closed			port-unreach	
127.0.0.1	localhost	udp	445	closed			port-unreach	
45.33.32.156	scanme.nmap.org	tcp	110	filtered			no-response	
45.33.32.156	scanme.nmap.org	tcp	139	filtered			no-response	
45.33.32.156	scanme.nmap.org	tcp	443	filtered			no-response	
45.33.32.156	scanme.nmap.org	tcp	445	filtered			no-response	
45.33.32.156	scanme.nmap.org	tcp	3389	filtered			no-response	

Figure 2

```
** PSEC Info Security Apps **
1) Scan network
2) Upload/download file using FTP
3) Send custom packet
4) Quit

Your input: 2
Would you like to
1) upload
2) download
>>3
Please enter a valid input.
Would you like to
1) upload
2) download
>>@
Please enter a valid input.
Would you like to
1) upload
2) download
>>a
Please enter a valid input.
Would you like to
1) upload
2) download
>>0
Please enter a valid input.
Would you like to
1) upload
2) download
>>□
```

Figure 3

```
Would you like to
1) upload
2) download
>>1
1)      hello.csv
2)      hello.json
3)      hello.xls
4)      teststststst.txt
Enter the num of the file to upload? 
```

Figure 4

```
1)      hello.csv
2)      hello.json
3)      hello.xls
4)      teststststst.txt
Enter the num of the file to upload? 1
hello.csv
```

Figure 5

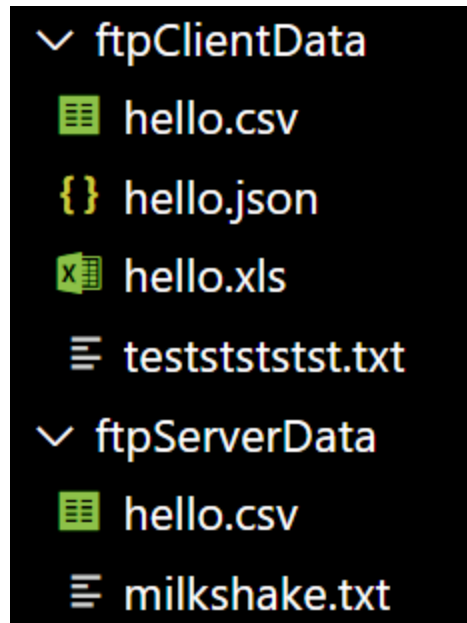


Figure 6

```
1)      hello.csv
2)      hello.json
3)      hello.xls
4)      teststststst.txt
Enter the num of the file to upload? 2
hello.json
```

Figure 7

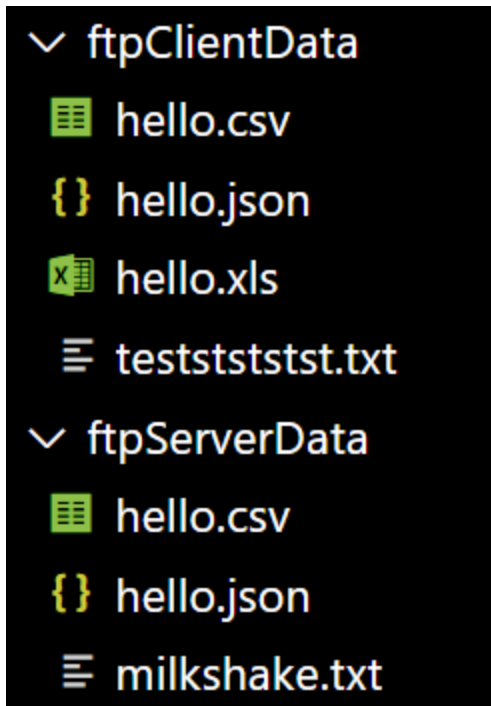


Figure 8

```
1)      hello.csv
2)      hello.json
3)      hello.xls
4)      teststststst.txt
Enter the num of the file to upload? 3
hello.xls
```

Figure 9



Figure 10

```
1)      hello.csv
2)      hello.json
3)      hello.xls
4)      teststststst.txt
Enter the num of the file to upload? 4
teststststst.txt
```

Figure 11

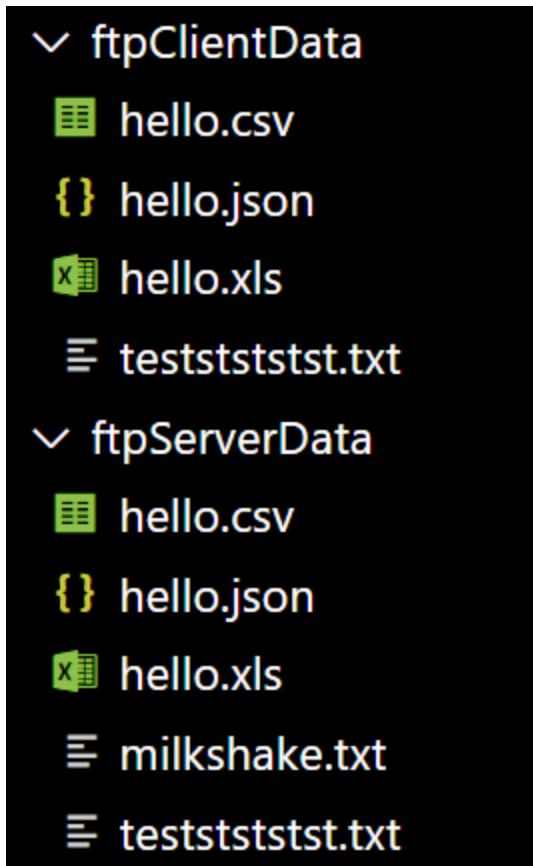


Figure 12

```
1)      -rw-rw-rw-   1 owner   group        5 Jan
30 06:19 goodbye.csv
2)      -rw-rw-rw-   1 owner   group       12 Jan
30 06:20 goodbye.json
3)      -rw-rw-rw-   1 owner   group       10 Jan
16 03:25 goodbye.txt
4)      -rw-rw-rw-   1 owner   group        5 Jan
30 06:21 goodbye.xls
5)      -rw-rw-rw-   1 owner   group        6 Jan
30 06:22 teststststst.txt
Enter the num of the file to download? 1
```

Figure 13



Figure 14

```
1)      -rw-rw-rw-   1 owner   group           5 Jan
30 06:19 goodbye.csv
2)      -rw-rw-rw-   1 owner   group          12 Jan
30 06:20 goodbye.json
3)      -rw-rw-rw-   1 owner   group          10 Jan
16 03:25 goodbye.txt
4)      -rw-rw-rw-   1 owner   group           5 Jan
30 06:21 goodbye.xls
5)      -rw-rw-rw-   1 owner   group           6 Jan
30 06:22 teststststst.txt
Enter the num of the file to download? 2
```

Figure 15



Figure 16

```
1)      -rw-rw-rw-   1 owner   group        5 Jan
30 06:19 goodbye.csv
2)      -rw-rw-rw-   1 owner   group       12 Jan
30 06:20 goodbye.json
3)      -rw-rw-rw-   1 owner   group       10 Jan
16 03:25 goodbye.txt
4)      -rw-rw-rw-   1 owner   group        5 Jan
30 06:21 goodbye.xls
5)      -rw-rw-rw-   1 owner   group        6 Jan
30 06:22 teststststst.txt
Enter the num of the file to download? 3
```

Figure 17

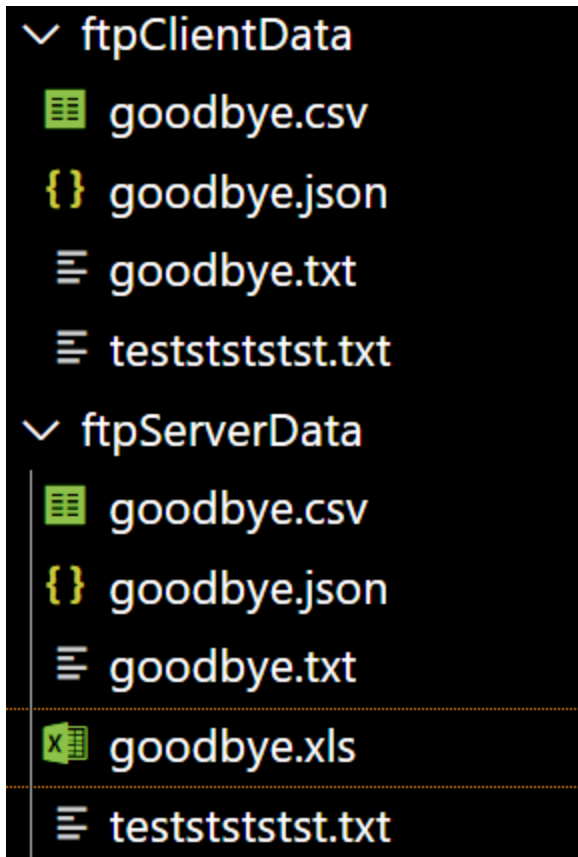


Figure 18

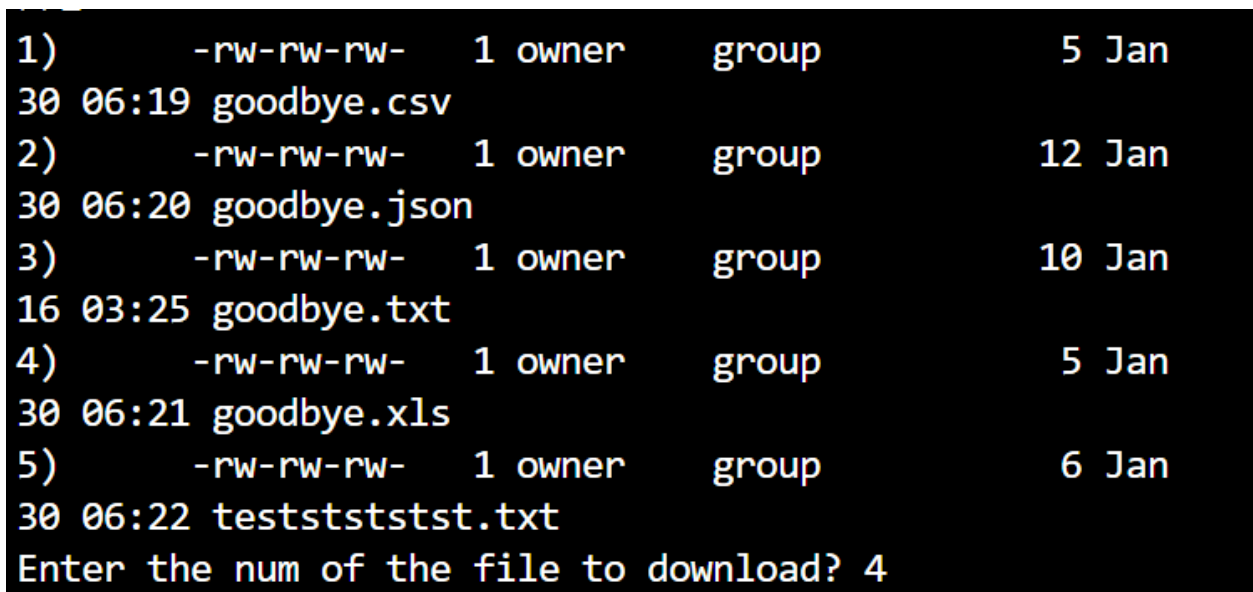


Figure 19



Figure 20


```
Enter the num of the file to upload?
Please enter a valid integer within given range.
Enter the num of the file to upload? q
Please enter a valid integer within given range.
Enter the num of the file to upload? w
Please enter a valid integer within given range.
Enter the num of the file to upload? #
Please enter a valid integer within given range.
Enter the num of the file to upload? 6
Please enter a valid integer within given range.
Enter the num of the file to upload? 0
Please enter a valid integer within given range.
Enter the num of the file to upload? 
```

Figure 21

```
Enter the num of the file to download? 0
Please enter a valid integer within given range.
Enter the num of the file to download?
Please enter a valid integer within given range.
Enter the num of the file to download? @
Please enter a valid integer within given range.
Enter the num of the file to download? e
Please enter a valid integer within given range.
Enter the num of the file to download? 7
Please enter a valid integer within given range.
Enter the num of the file to download? 
```

Figure 22

```
Enter source address of packet: wwwwww.hello.sp
Invalid host
Enter source address of packet: 123.goof.com
Invalid host
Enter source address of packet: www.1234.co
Invalid host
Enter source address of packet: www.sp.com
Enter source port of packet: 
```

Figure 23

```
Enter source address of packet: www.hiplsworkthisshoul
dnot.com
Invalid host
Enter source address of packet: www.sp.com
Enter source port of packet: 
```

Figure 24

```
Enter source port of packet: 700000
Port is invalid.
Enter source port of packet: -2
Port is invalid.
Enter source port of packet: www
Port is invalid.
Enter source port of packet: $$
Port is invalid.
Enter source port of packet: 3000
Enter destination address of packet: 
```

Figure 25

```

Enter Type (T) TCP, (U) UDP, (I) ICMP echo request (T/
U/I): 4
enter a valid protocol
Enter Type (T) TCP, (U) UDP, (I) ICMP echo request (T/
U/I): @
enter a valid protocol
Enter Type (T) TCP, (U) UDP, (I) ICMP echo request (T/
U/I): a
enter a valid protocol
Enter Type (T) TCP, (U) UDP, (I) ICMP echo request (T/
U/I): t

```

Figure 26

```

Packet RAW Data (optional, DISM-DISM-DISM-DISM left blank):

```

Figure 27

```

No of Packet to send (1-65535): 777777
Number is invalid.
No of Packet to send (1-65535): -20
Number is invalid.
No of Packet to send (1-65535): f
Number is invalid.
No of Packet to send (1-65535): @
Number is invalid.
No of Packet to send (1-65535): 30
Enter Y to Start, Any other return to main menu: 

```

Figure 28

58 11 22 04 42 50 10 6f	d9 f6 ea f7 08 00 45 00	X·"·BP·o ·····E·
00 2f 00 01 00 00 40 11	e1 e8 a5 a0 0d 14 0d f8	·/····@· ······
d8 28 0b b8 16 a8 00 1b	8d f9 44 49 53 4d 2d 44	·(····· ··DISM-D
49 53 4d 2d 44 49 53 4d	2d 44 49 53 4d	ISM-DISM -DISM

Figure 29

```

58 11 22 04 42 50 10 6f d9 f6 ea f7 08 00 45 00 X."BP.o .....E.
00 31 00 01 00 00 40 06 e1 f1 0d f8 d8 28 a5 a0 .1....@. ....(..
0d 14 0b b8 16 a8 00 00 00 00 00 00 00 00 50 02 .....P.
20 00 2c 80 00 00 68 65 6c 6c 6f 20 31 32 33 .,...he llo 123

```

Figure 30

434	50.748710	165.160.13.20	13.248.216.40	ICMP	45 Echo (pi
435	50.752263	165.160.13.20	13.248.216.40	ICMP	45 Echo (pi
436	50.756052	165.160.13.20	13.248.216.40	ICMP	45 Echo (pi
437	50.759610	165.160.13.20	13.248.216.40	ICMP	45 Echo (pi
438	50.763856	165.160.13.20	13.248.216.40	ICMP	45 Echo (pi
439	50.767410	165.160.13.20	13.248.216.40	ICMP	45 Echo (pi
440	50.771658	165.160.13.20	13.248.216.40	ICMP	45 Echo (pi
441	50.775564	165.160.13.20	13.248.216.40	ICMP	45 Echo (pi
442	50.779440	165.160.13.20	13.248.216.40	ICMP	45 Echo (pi
443	50.782982	165.160.13.20	13.248.216.40	ICMP	45 Echo (pi
444	50.786979	165.160.13.20	13.248.216.40	ICMP	45 Echo (pi
445	50.791099	165.160.13.20	13.248.216.40	ICMP	45 Echo (pi
446	50.794994	165.160.13.20	13.248.216.40	ICMP	45 Echo (pi
447	50.799011	165.160.13.20	13.248.216.40	ICMP	45 Echo (pi

Figure 31

```

Enter source address of packet: www.sp.com
Enter source port of packet: 3000
Enter destination address of packet: www.pp.com
Enter destination port of packet: 5800
Enter Type (T) TCP, (U) UDP, (I) ICMP echo request (T/
U/I): T
Packet RAW Data (optional, DISM-DISM-DISM-DISM left bl
ank):
No of Packet to send (1-65535): 80
Enter Y to Start, Any other return to main menu: n

```

Figure 32

3023	200.663535	172.217.194.138	192.168.50.176	UDP	74 443 → 61
3024	200.672187	192.168.50.176	172.217.194.138	UDP	76 61952 →
3025	200.698281	192.168.50.176	52.114.44.81	TLSv1.2	112 Applicat
3026	200.773066	52.114.44.81	192.168.50.176	TLSv1.2	101 Applicat
3027	200.823832	192.168.50.176	52.114.44.81	TCP	54 1133 → 4
3028	200.895545	ASUSTekC_04:42:50	Spanning-tree-(for-... 0x2e00	60 Ethernet	
3029	200.895576	ASUSTekC_04:42:54	Spanning-tree-(for-... 0x2e00	60 Ethernet	
3030	200.914472	172.217.194.138	192.168.50.176	UDP	578 443 → 61

Figure 33

Reflection

I found this assignment challenging because I was forced to come out of my comfort zone and use multiple Python modules that I was not comfortable with. This assignment also made me learn how to be versatile and navigate uncharted waters when it comes to using Python modules that I do not know.

I am thankful to have done this assignment because I was put in a similar situation for another module, Applied Cryptography. But having done this assignment I was able to apply my newly learnt skills to also traverse that assignment. Learning these modules are also really important because I can see myself using nmap, ftp, regex and scapy in DISM in the future. Though it was not intended, I also learnt how to use modules such as os, socket, importlib, subprocess and more. Though I do not know the entirety of Python, I do feel like I understand the language better after this assignment. This assignment has also given me the confidence that I can progressively learn new aspects of a (programming) language as I am doing the coding.

Checklist

No	Description	Remarks*
1	Main menu to select apps	100%
1.1	Scan Network	100%
1.2	Upload/download file using FTP	100%
1.3	Send Custom packet	100%
2	User testing a) Description of test data and the test b) Screen shots	100%
3	Documentation for each script	100%