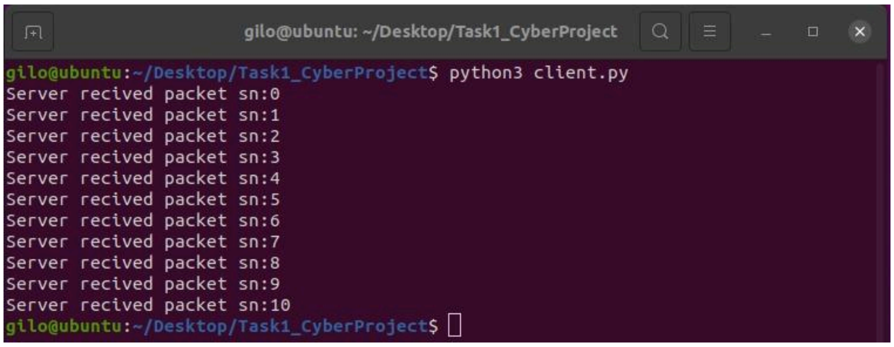
Cyber risk assessment project – Sniffer

Task 1:

The client sends messages to the server along with a serial number of the message.
In response, the server prints the message from the client and sends the client a notification that it has received message number X.

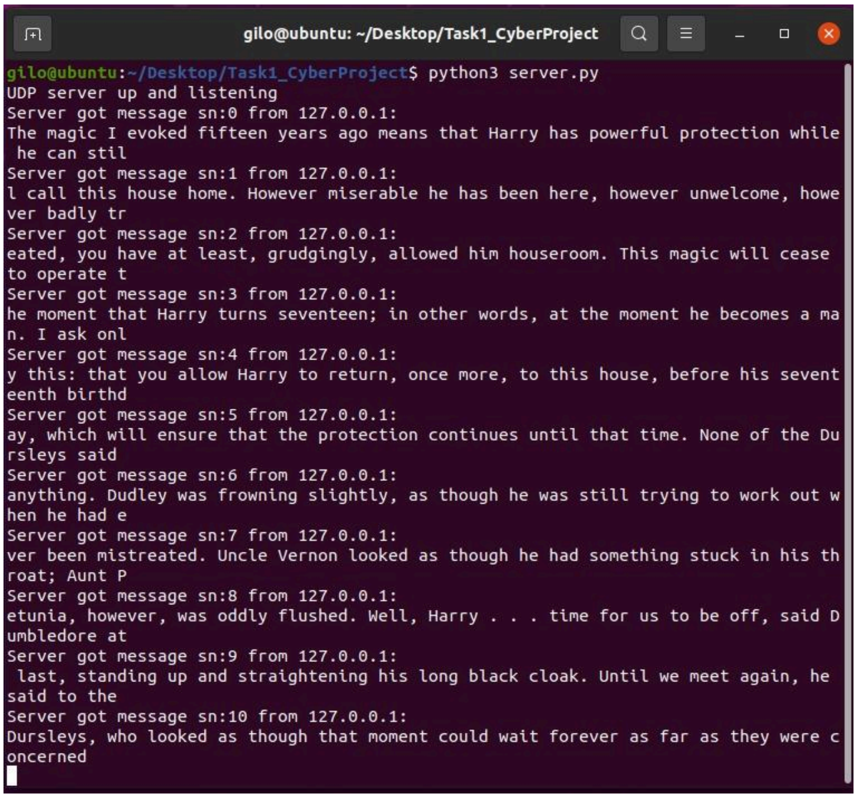
To implement the Sniffer we used scapy.
The attacker listens to the port and prints the payload of the messages.

Client:



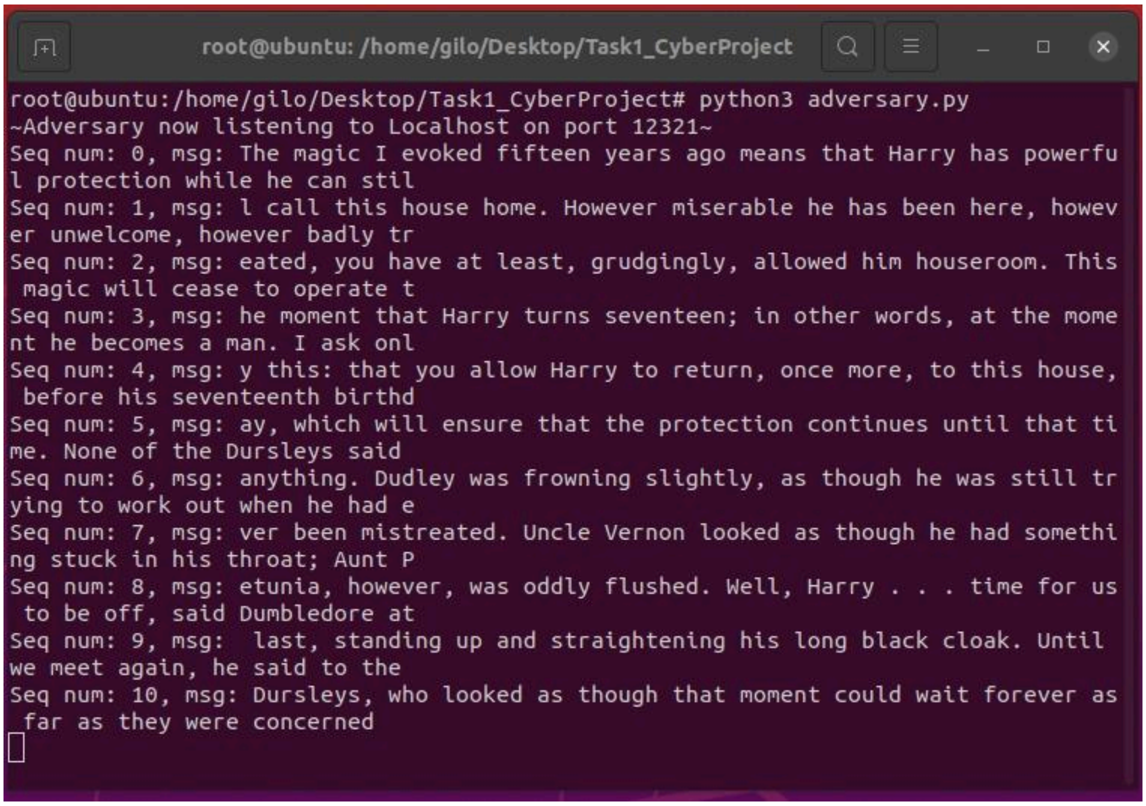
```
gilo@ubuntu:~/Desktop/Task1_CyberProject$ python3 client.py
Server recived packet sn:0
Server recived packet sn:1
Server recived packet sn:2
Server recived packet sn:3
Server recived packet sn:4
Server recived packet sn:5
Server recived packet sn:6
Server recived packet sn:7
Server recived packet sn:8
Server recived packet sn:9
Server recived packet sn:10
gilo@ubuntu:~/Desktop/Task1_CyberProject$ 
```

Server:



```
gilo@ubuntu:~/Desktop/Task1_CyberProject$ python3 server.py
UDP server up and listening
Server got message sn:0 from 127.0.0.1:
The magic I evoked fifteen years ago means that Harry has powerful protection while
 he can stil
Server got message sn:1 from 127.0.0.1:
l call this house home. However miserable he has been here, however unwelcome, howe
ver badly tr
Server got message sn:2 from 127.0.0.1:
eated, you have at least, grudgingly, allowed him houseroom. This magic will cease
to operate t
Server got message sn:3 from 127.0.0.1:
he moment that Harry turns seventeen; in other words, at the moment he becomes a ma
n. I ask onl
Server got message sn:4 from 127.0.0.1:
y this: that you allow Harry to return, once more, to this house, before his sevent
eenth birthd
Server got message sn:5 from 127.0.0.1:
ay, which will ensure that the protection continues until that time. None of the Du
rsleys said
Server got message sn:6 from 127.0.0.1:
anything. Dudley was frowning slightly, as though he was still trying to work out w
hen he had e
Server got message sn:7 from 127.0.0.1:
ver been mistreated. Uncle Vernon looked as though he had something stuck in his th
roat; Aunt P
Server got message sn:8 from 127.0.0.1:
etunia, however, was oddly flushed. Well, Harry . . . time for us to be off, said D
umbledore at
Server got message sn:9 from 127.0.0.1:
 last, standing up and straightening his long black cloak. Until we meet again, he
said to the
Server got message sn:10 from 127.0.0.1:
Dursleys, who looked as though that moment could wait forever as far as they were c
oncerned
```

Sniffer:



```
root@ubuntu:/home/gilo/Desktop/Task1_CyberProject# python3 adversary.py
~Adversary now listening to Localhost on port 12321~
Seq num: 0, msg: The magic I evoked fifteen years ago means that Harry has powerfu
l protection while he can stil
Seq num: 1, msg: l call this house home. However miserable he has been here, howev
er unwelcome, however badly tr
Seq num: 2, msg: eated, you have at least, grudgingly, allowed him houseroom. This
 magic will cease to operate t
Seq num: 3, msg: he moment that Harry turns seventeen; in other words, at the mome
nt he becomes a man. I ask onl
Seq num: 4, msg: y this: that you allow Harry to return, once more, to this house,
 before his seventeenth birthd
Seq num: 5, msg: ay, which will ensure that the protection continues until that ti
me. None of the Dursleys said
Seq num: 6, msg: anything. Dudley was frowning slightly, as though he was still tr
ying to work out when he had e
Seq num: 7, msg: ver been mistreated. Uncle Vernon looked as though he had somethi
ng stuck in his throat; Aunt P
Seq num: 8, msg: etunia, however, was oddly flushed. Well, Harry . . . time for us
 to be off, said Dumbledore at
Seq num: 9, msg:  last, standing up and straightening his long black cloak. Until
we meet again, he said to the
Seq num: 10, msg: Dursleys, who looked as though that moment could wait forever as
 far as they were concerned
```

Task 2:

Adversary:

Our attacker can insert a list of inputs that packets containing them will be dropped.
Since our protocol can handle the dropping of one packet, the attacker will drop at least 2 packets.

Implementation:

- In order for the attacker to be able to listen to the port and print the packets, we used scapy.
- In order for the attacker to be able to drop packages, we used iptables commands.

Our protocol takes into account the loss of packets by a communication problem or attack:

Client :

In this task, before sending the messages containing the text, the following steps were performed:

1. The client will choose a random number d which will be the number of messages the client will send.
2. The client will compile a list of messages to send and calculate e in the following way: e = m_1 XOR m_2 XOR m_3 … XOR m_d
3. The client will send the server a message containing e and d.
   If the client does not receive a confirmation message about the handshake from the server, it will return to the first section.
4. The client will send the d messages to the server.
5. The client will wait for a message from the server, if the message is :
   - FIN : The client will close the connection.
   - Retransmission: The client will send the d messages again.

Server - In each transmission of d packets:

1. If only one package is missing from the d packages, then the server knows how to recover it by doing XOR of all the packets that came and with e.
   for example: if d=3 and packet2 is missing then: e = m1 XOR m2 XOR m3 .
   The server has m1, m3 and e and can therefore calculate m2 by:
   m2 = e XOR m1 XOR m3
2. If more than one packet is missing, the server notifies the client that a retransmission is needed .
3. If the server received all d packets then check if server_e = client_e . if not the server ask for retransmission , else the server send to the client a FIN message.

Defenses against attack:

we would like a mechanism to identify an attacker that will work during the entire connection. In each transmission of d packets the server will check :

1. If at least 80% of the messages (0.8*d) didn't arrive at least 2 times .
2. If a specific packet does not arrive at least 5 times.
3. If all d packets were retransmitted at least max(8,0.5*d) times.

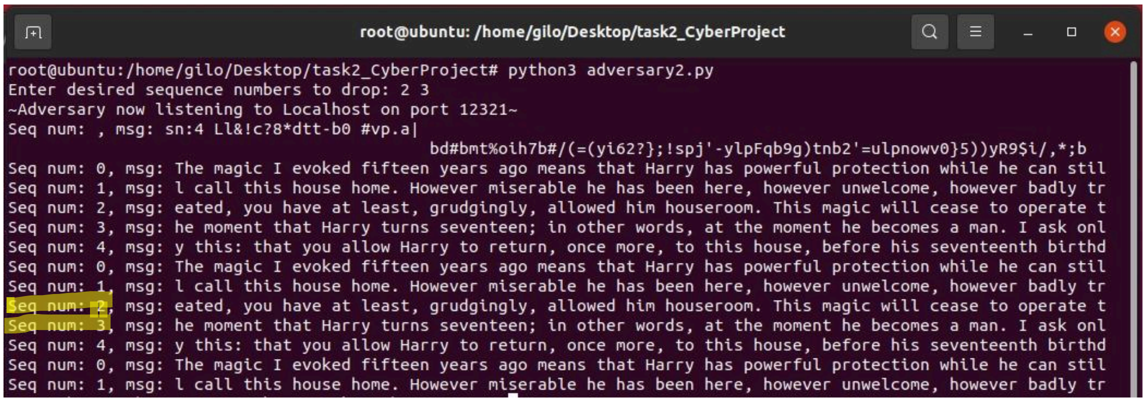
If one of the conditions is met, the server sends the client a warning message about a high probability of an attack. The client will close the connection.

In addition**,** assume the attacker tries to prevent the connection by dropping the handshake packet (which contains e and d). Our protocol makes the attack more difficult by having the number d be randomly rechosen, so the packet of the handshake is dynamic.

Example 1 : two packets drops

Adversary:

The attacker chooses to drop the packages with serial numbers 2 and 3:

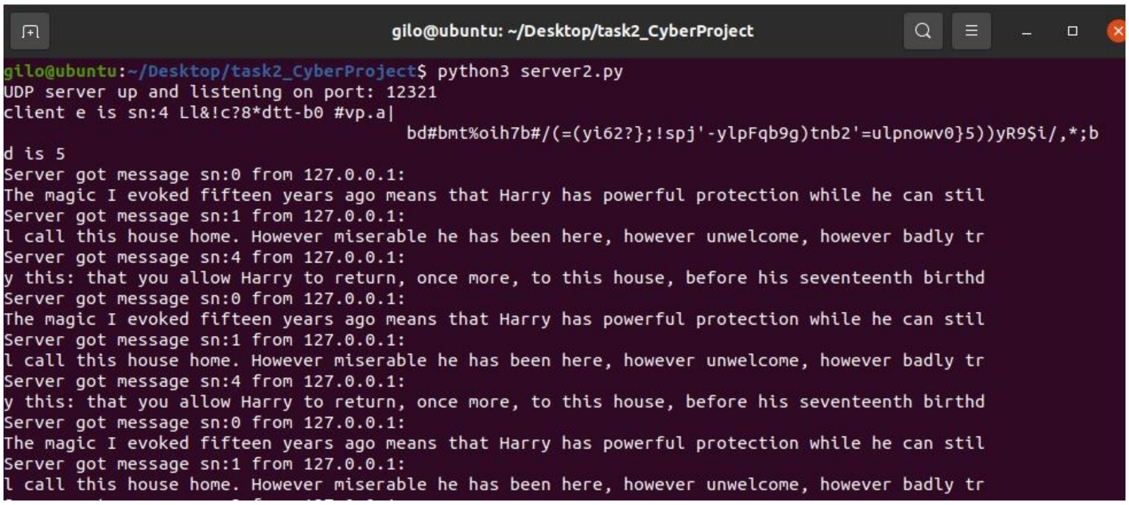


root@ubuntu: /home/gilo/Desktop/task2_CyberProject

```
root@ubuntu:/home/gilo/Desktop/task2_CyberProject# python3 adversary2.py
Enter desired sequence numbers to drop: 2 3
~Adversary now listening to Localhost on port 12321~
Seq num: , msg: sn:4 Ll&!c?8*dtt-b0 #vp.a|
                                              bd#bmt%oih7b#/(=(yi62?};!spj'-ylpFqb9g)tnb2'=ulpnowv0}5))yR9$i/,*;b
Seq num: 0, msg: The magic I evoked fifteen years ago means that Harry has powerful protection while he can stil
Seq num: 1, msg: l call this house home. However miserable he has been here, however unwelcome, however badly tr
Seq num: 2, msg: eated, you have at least, grudgingly, allowed him houseroom. This magic will cease to operate t
Seq num: 3, msg: he moment that Harry turns seventeen; in other words, at the moment he becomes a man. I ask onl
Seq num: 4, msg: y this: that you allow Harry to return, once more, to this house, before his seventeenth birthd
Seq num: 0, msg: The magic I evoked fifteen years ago means that Harry has powerful protection while he can stil
Seq num: 1, msg: l call this house home. However miserable he has been here, however unwelcome, however badly tr
Seq num: 2, msg: eated, you have at least, grudgingly, allowed him houseroom. This magic will cease to operate t
Seq num: 3, msg: he moment that Harry turns seventeen; in other words, at the moment he becomes a man. I ask onl
Seq num: 4, msg: y this: that you allow Harry to return, once more, to this house, before his seventeenth birthd
Seq num: 0, msg: The magic I evoked fifteen years ago means that Harry has powerful protection while he can stil
Seq num: 1, msg: l call this house home. However miserable he has been here, however unwelcome, however badly tr
```

Server:

It can be seen that packets number 2 and 3 do not reach the server But they do reach the adversary.

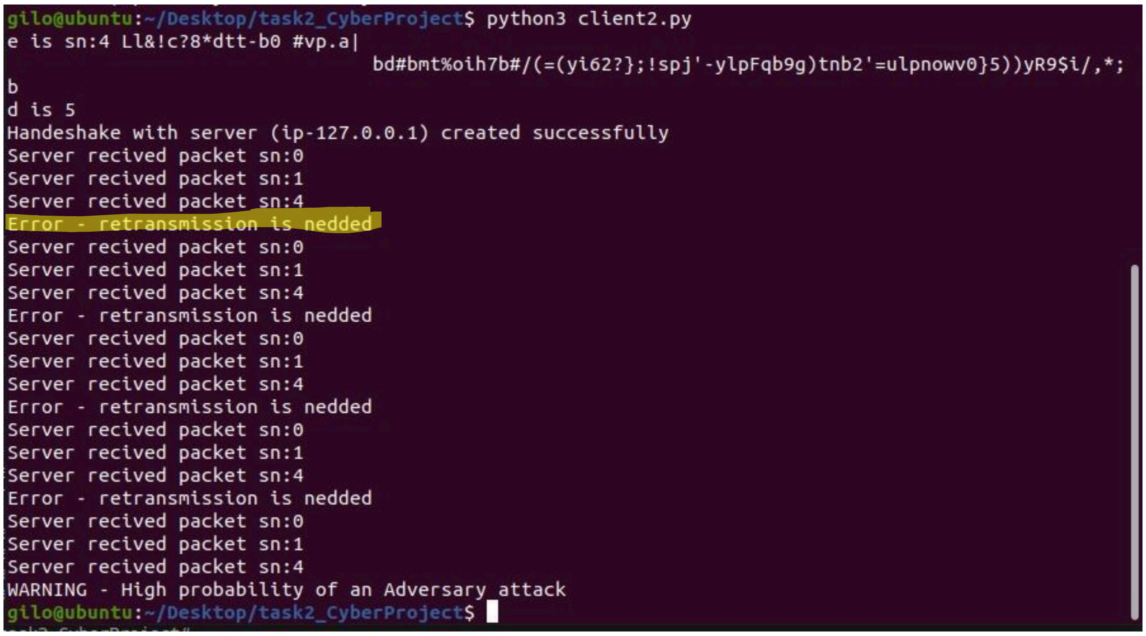


gilo@ubuntu: ~/Desktop/task2_CyberProject

```
gilo@ubuntu:~/Desktop/task2_CyberProject$ python3 server2.py
UDP server up and listening on port: 12321
client e is sn:4 Ll&!c?8*dtt-b0 #vp.a|
                                       bd#bmt%oih7b#/(=(yi62?};!spj'-ylpFqb9g)tnb2'=ulpnowv0}5))yR9$i/,*;b
d is 5
Server got message sn:0 from 127.0.0.1:
The magic I evoked fifteen years ago means that Harry has powerful protection while he can stil
Server got message sn:1 from 127.0.0.1:
l call this house home. However miserable he has been here, however unwelcome, however badly tr
Server got message sn:4 from 127.0.0.1:
y this: that you allow Harry to return, once more, to this house, before his seventeenth birthd
Server got message sn:0 from 127.0.0.1:
The magic I evoked fifteen years ago means that Harry has powerful protection while he can stil
Server got message sn:1 from 127.0.0.1:
l call this house home. However miserable he has been here, however unwelcome, however badly tr
Server got message sn:4 from 127.0.0.1:
y this: that you allow Harry to return, once more, to this house, before his seventeenth birthd
Server got message sn:0 from 127.0.0.1:
The magic I evoked fifteen years ago means that Harry has powerful protection while he can stil
Server got message sn:1 from 127.0.0.1:
l call this house home. However miserable he has been here, however unwelcome, however badly tr
```

Client:

- The client receives confirmation messages from the server. Therefore, it can be seen that packages number 2 and 3 fall in every transmission. The server informs the client that retransmission is necessary, in response the client retransmits all d packets.
- The server detected that the **same** packages were dropped 5 times and therefore sends a warning to the client. In response, the client closes the connection.

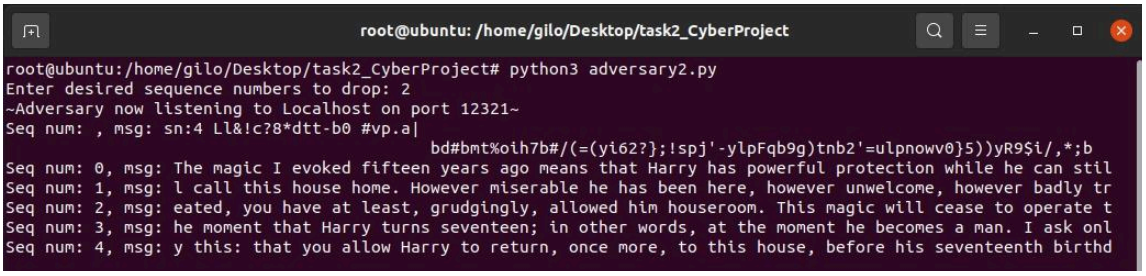


```
gilo@ubuntu:~/Desktop/task2_CyberProject$ python3 client2.py
e is sn:4 Ll&!c?8*dtt-b0 #vp.a|
                                         bd#bmt%oih7b#/(=(yi62?};!spj'-ylpFqb9g)tnb2'=ulpnowv0}5))yR9$i/,*;
b
d is 5
Handeshake with server (ip-127.0.0.1) created successfully
Server recived packet sn:0
Server recived packet sn:1
Server recived packet sn:4
Error - retransmission is nedded
Server recived packet sn:0
Server recived packet sn:1
Server recived packet sn:4
Error - retransmission is nedded
Server recived packet sn:0
Server recived packet sn:1
Server recived packet sn:4
Error - retransmission is nedded
Server recived packet sn:0
Server recived packet sn:1
Server recived packet sn:4
Error - retransmission is nedded
Server recived packet sn:0
Server recived packet sn:1
Server recived packet sn:4
WARNING - High probability of an Adversary attack
gilo@ubuntu:~/Desktop/task2_CyberProject$ 
```

Example 2 : one packet are drops

Adversary:

The attacker chooses to drop the package with serial number 2:

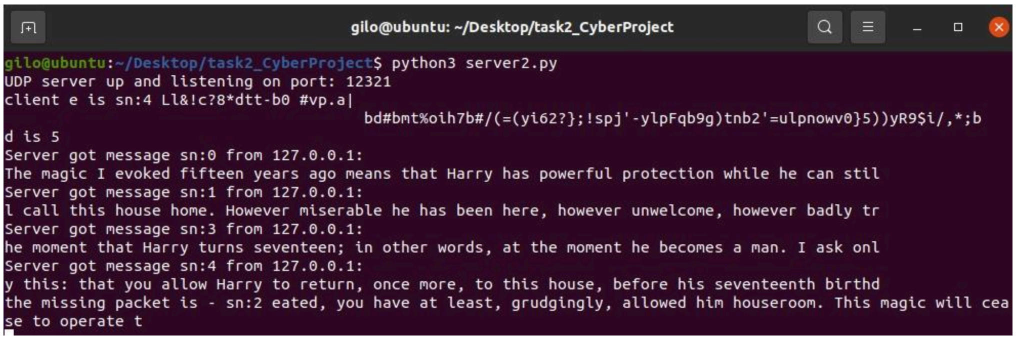


```
root@ubuntu:/home/gilo/Desktop/task2_CyberProject# python3 adversary2.py
Enter desired sequence numbers to drop: 2
~Adversary now listening to Localhost on port 12321~
Seq num: , msg: sn:4 Ll&!c?8*dtt-b0 #vp.a|
                                           bd#bmt%oih7b#/(=(yi62?};!spj'-ylpFqb9g)tnb2'=ulpnowv0}5))yR9$i/,*;b
Seq num: 0, msg: The magic I evoked fifteen years ago means that Harry has powerful protection while he can stil
Seq num: 1, msg: l call this house home. However miserable he has been here, however unwelcome, however badly tr
Seq num: 2, msg: eated, you have at least, grudgingly, allowed him houseroom. This magic will cease to operate t
Seq num: 3, msg: he moment that Harry turns seventeen; in other words, at the moment he becomes a man. I ask onl
Seq num: 4, msg: y this: that you allow Harry to return, once more, to this house, before his seventeenth birthd
```

Server:

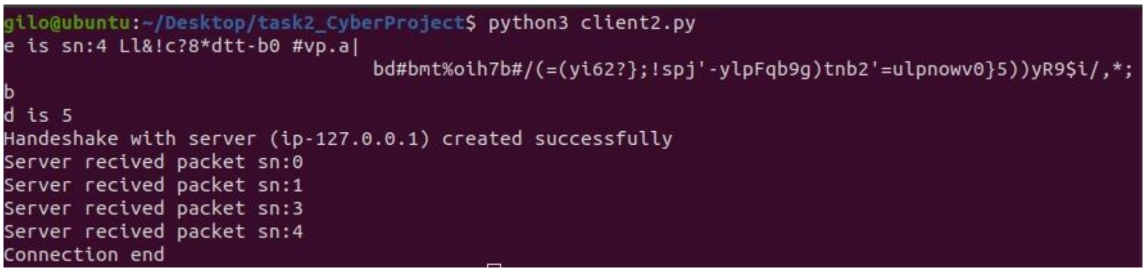
Package number 2 does not reach the server but the server does not request retransmission. In our protocol, the server can restore it as we explained above.

It can be seen that the package that the server restored is the same as package number 2 that appears with the attacker.



```
gilo@ubuntu:~/Desktop/task2_CyberProject$ python3 server2.py
UDP server up and listening on port: 12321
client e is sn:4 Ll&!c?8*dtt-b0 #vp.a|
                                       bd#bmt%oih7b#/(=(yi62?};!spj'-ylpFqb9g)tnb2'=ulpnowv0}5))yR9$i/,*;b
d is 5
Server got message sn:0 from 127.0.0.1:
The magic I evoked fifteen years ago means that Harry has powerful protection while he can stil
Server got message sn:1 from 127.0.0.1:
l call this house home. However miserable he has been here, however unwelcome, however badly tr
Server got message sn:3 from 127.0.0.1:
he moment that Harry turns seventeen; in other words, at the moment he becomes a man. I ask onl
Server got message sn:4 from 127.0.0.1:
y this: that you allow Harry to return, once more, to this house, before his seventeenth birthd
the missing packet is - sn:2 eated, you have at least, grudgingly, allowed him houseroom. This magic will cea
se to operate t
```

Client:

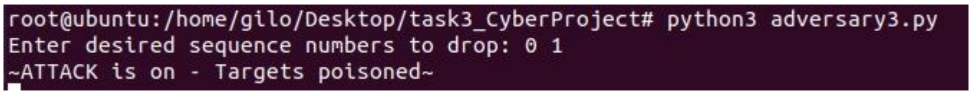


```
gilo@ubuntu:~/Desktop/task2_CyberProject$ python3 client2.py
e is sn:4 Ll&!c?8*dtt-b0 #vp.a|
                                bd#bmt%oih7b#/(=(yi62?};!spj'-ylpFqb9g)tnb2'=ulpnowv0}5))yR9$i/,*;
b
d is 5
Handeshake with server (ip-127.0.0.1) created successfully
Server recived packet sn:0
Server recived packet sn:1
Server recived packet sn:3
Server recived packet sn:4
Connection end
```

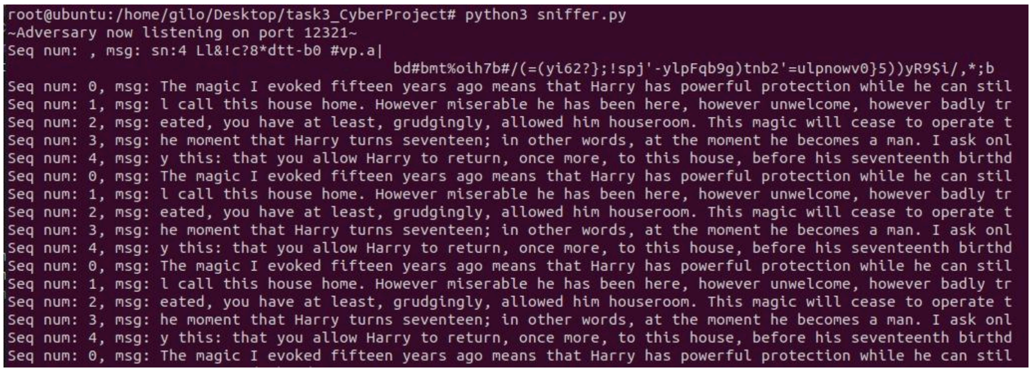
Task 3:

Adversary – runs on Ubuntu: IP = 192.168.112.129

The attack works with the same principles as task 2, and In order for the attack to work on different IPs we used arp spoofing.

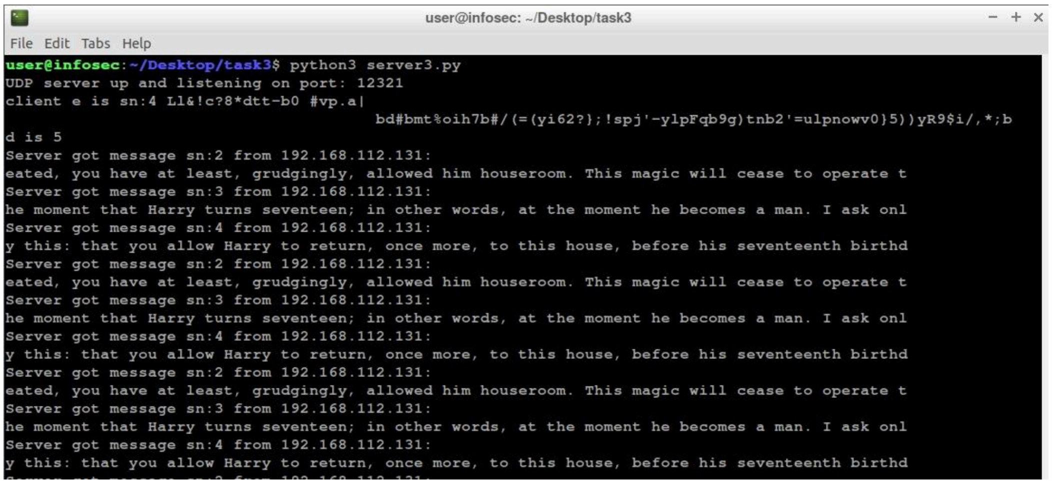


```
root@ubuntu:/home/gilo/Desktop/task3_CyberProject# python3 adversary3.py
Enter desired sequence numbers to drop: 0 1
~ATTACK is on - Targets poisoned~
```



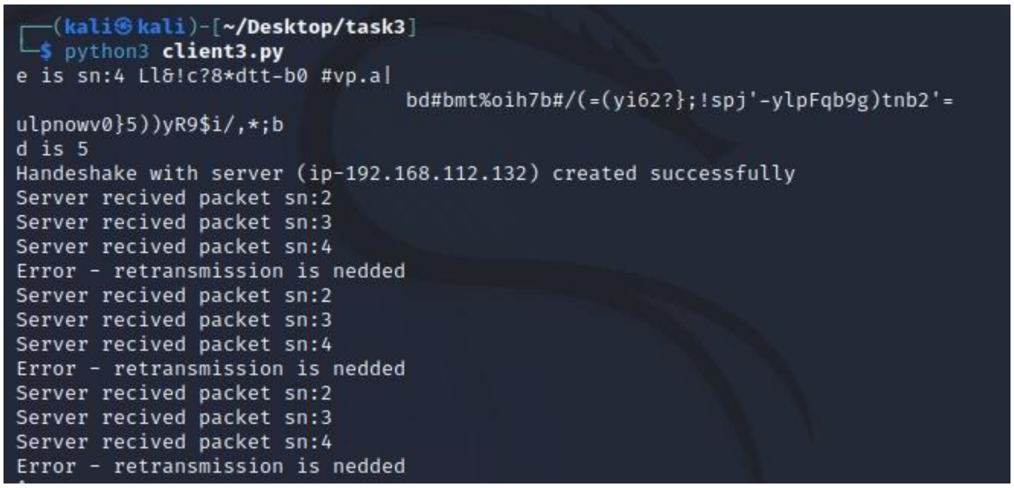
```
root@ubuntu:/home/gilo/Desktop/task3_CyberProject# python3 sniffer.py
~Adversary now listening on port 12321~
Seq num: , msg: sn:4 Ll&!c?8*dtt-b0 #vp.a|
                                         bd#bmt%oih7b#/(=(yi62?};!spj'-ylpFqb9g)tnb2'=ulpnowv0}5))yR9$i/,*;b
Seq num: 0, msg: The magic I evoked fifteen years ago means that Harry has powerful protection while he can stil
Seq num: 1, msg: l call this house home. However miserable he has been here, however unwelcome, however badly tr
Seq num: 2, msg: eated, you have at least, grudgingly, allowed him houseroom. This magic will cease to operate t
Seq num: 3, msg: he moment that Harry turns seventeen; in other words, at the moment he becomes a man. I ask onl
Seq num: 4, msg: y this: that you allow Harry to return, once more, to this house, before his seventeenth birthd
Seq num: 0, msg: The magic I evoked fifteen years ago means that Harry has powerful protection while he can stil
Seq num: 1, msg: l call this house home. However miserable he has been here, however unwelcome, however badly tr
Seq num: 2, msg: eated, you have at least, grudgingly, allowed him houseroom. This magic will cease to operate t
Seq num: 3, msg: he moment that Harry turns seventeen; in other words, at the moment he becomes a man. I ask onl
Seq num: 4, msg: y this: that you allow Harry to return, once more, to this house, before his seventeenth birthd
Seq num: 0, msg: The magic I evoked fifteen years ago means that Harry has powerful protection while he can stil
Seq num: 1, msg: l call this house home. However miserable he has been here, however unwelcome, however badly tr
Seq num: 2, msg: eated, you have at least, grudgingly, allowed him houseroom. This magic will cease to operate t
Seq num: 3, msg: he moment that Harry turns seventeen; in other words, at the moment he becomes a man. I ask onl
Seq num: 4, msg: y this: that you allow Harry to return, once more, to this house, before his seventeenth birthd
Seq num: 0, msg: The magic I evoked fifteen years ago means that Harry has powerful protection while he can stil
```

Server – runs on InfoSec: IP = 192.168.112.132



```
user@infosec:~/Desktop/task3$ python3 server3.py
UDP server up and listening on port: 12321
client e is sn:4 Ll&!c?8*dtt-b0 #vp.a|
                                        bd#bmt%oih7b#/(=(yi62?};!spj'-ylpFqb9g)tnb2'=ulpnowv0}5))yR9$i/,*;b
d is 5
Server got message sn:2 from 192.168.112.131:
eated, you have at least, grudgingly, allowed him houseroom. This magic will cease to operate t
Server got message sn:3 from 192.168.112.131:
he moment that Harry turns seventeen; in other words, at the moment he becomes a man. I ask onl
Server got message sn:4 from 192.168.112.131:
y this: that you allow Harry to return, once more, to this house, before his seventeenth birthd
Server got message sn:2 from 192.168.112.131:
eated, you have at least, grudgingly, allowed him houseroom. This magic will cease to operate t
Server got message sn:3 from 192.168.112.131:
he moment that Harry turns seventeen; in other words, at the moment he becomes a man. I ask onl
Server got message sn:4 from 192.168.112.131:
y this: that you allow Harry to return, once more, to this house, before his seventeenth birthd
Server got message sn:2 from 192.168.112.131:
eated, you have at least, grudgingly, allowed him houseroom. This magic will cease to operate t
Server got message sn:3 from 192.168.112.131:
he moment that Harry turns seventeen; in other words, at the moment he becomes a man. I ask onl
Server got message sn:4 from 192.168.112.131:
y this: that you allow Harry to return, once more, to this house, before his seventeenth birthd
```

Client – run on Kali: IP = 192.168.112.131



```
┌──(kali㉿kali)-[~/Desktop/task3]
└─$ python3 client3.py
e is sn:4 Ll&!c?8*dtt-b0 #vp.a|
                                  bd#bmt%oih7b#/(=(yi62?};!spj'-ylpFqb9g)tnb2'=
ulpnowv0}5))yR9$i/,*;b
d is 5
Handeshake with server (ip-192.168.112.132) created successfully
Server recived packet sn:2
Server recived packet sn:3
Server recived packet sn:4
Error - retransmission is nedded
Server recived packet sn:2
Server recived packet sn:3
Server recived packet sn:4
Error - retransmission is nedded
Server recived packet sn:2
Server recived packet sn:3
Server recived packet sn:4
Error - retransmission is nedded
```

Requirements:

python==3.8.10

scapy==2.4.5

** To run the adversary scripts in task 3, you must use the terminal as ROOT.
(e.g. sudo python3 adversary3.py)