Task 1.A

Codes:

文本

描述已自动生成

Before sending ARP request:

图形用户界面, 文本, 应用程序

描述已自动生成

After sending:

文本

描述已自动生成

Task 1.B

1. Scenario 1

Codes:

文本

描述已自动生成

Testing result:

图形用户界面, 文本

描述已自动生成

1. Scenario 2

The same code would not work in this case.

Testing result:

文本

描述已自动生成

One possible reason is that the OS would directly drop the ARP reply if target address not in ARP cache. One way to deal with is to spoof a ICMP echo to A to insert the IP address at A’s ARP cache table.

Task 1.C

1. Scenario 1:

文本

描述已自动生成

1. Scenario 2:

文本

描述已自动生成

Task 2:

Codes:

ARP poisoning:

文本

描述已自动生成

Spoofing:

文本

描述已自动生成

屏幕的截图

描述已自动生成

Running result:

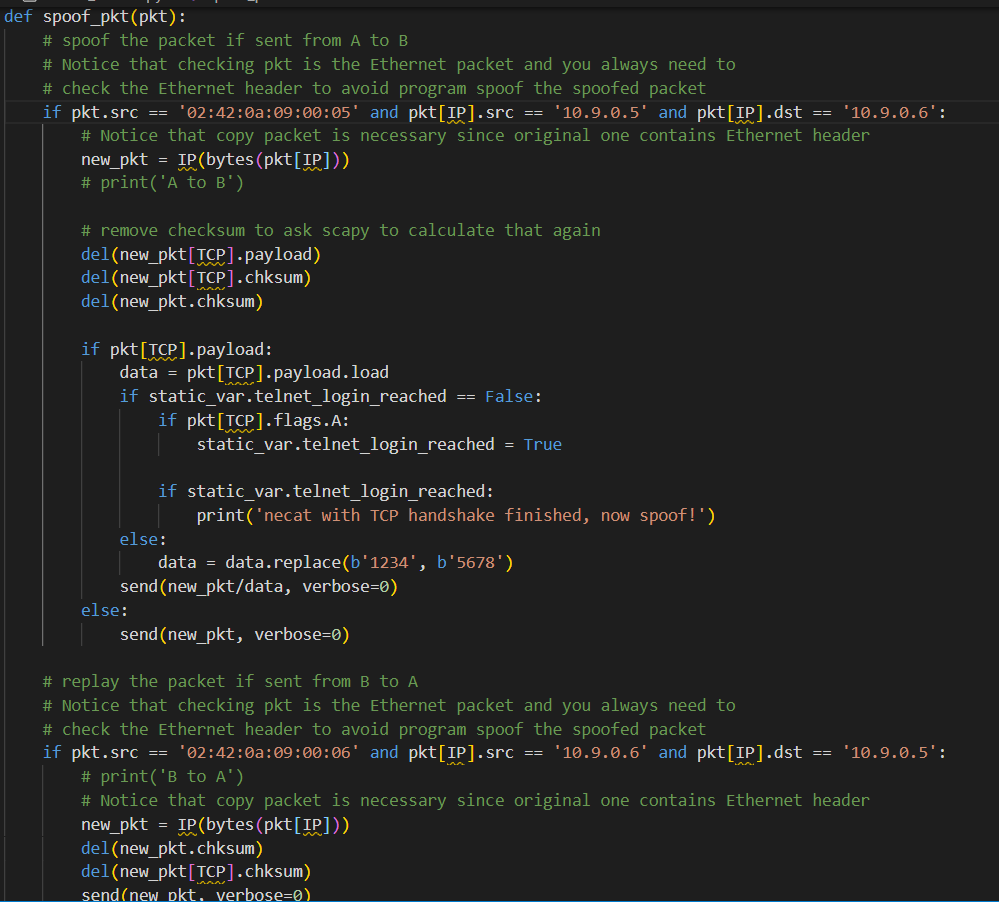
文本

描述已自动生成

Task 3

Basically, just modified the code in task 2 a little bit, then this task could be completed.

Codes:



Running result:

文本

描述已自动生成

Notice that sometimes, the packet from A is not successfully spoofed since some extra traffic may happened between A and B which may update A’s ARP cache.