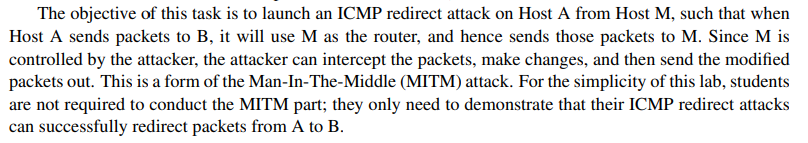
Task 02 – IP/ICMP Attacks

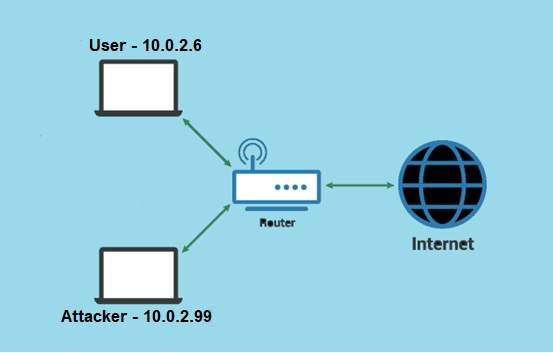
**3. Task 2 - ICMP redirect attack**

****

In this task we are going to use ICMP redirect attack on 'User', by changing its default gateway to the Attacker's IP address. That means every packet the User will send to a computer outside of his LAN will pass through the Attacker.

We will check our attack on the connection between User and the IP address of Google's DNS server – 8.8.8.8.

The network for this task:

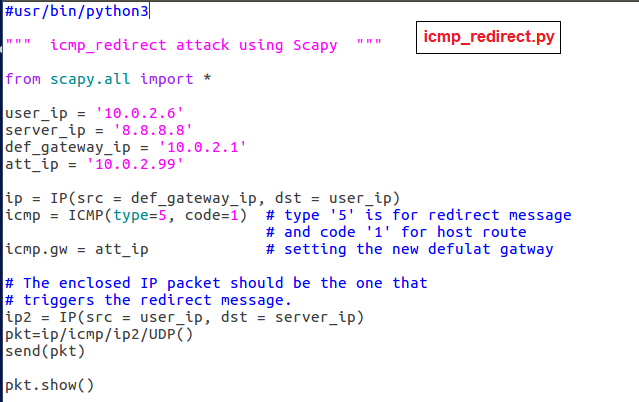


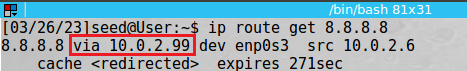
Let's see what's the current default gateway (before the attack) the User is using to access Google (using "ip route get" command):

Now we can see the User (10.0.2.6) is using 10.0.2.1 as default gateway. After launching the attack, it's expected that the default gateway will be our Attacker's IP.

In order to launch the attack, we need to send a message from User to Google, this message will go through the current default gateway. The next step is to build a packet, allegedly from the current default gateway address (router), that there is a faster way to access Google via a closer router – the Attacker's IP.

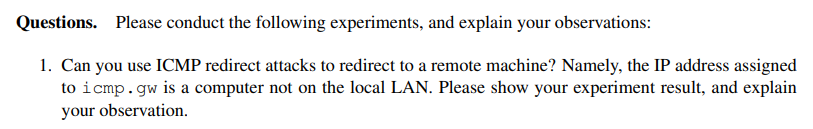
In the code below, the first section stands for the ICMP redirect message, the spoofed message from the Attacker to User that will make User change its default gateway. And the second section is for the message from User to Google that will "trigger" the ICMP redirect message from the router:

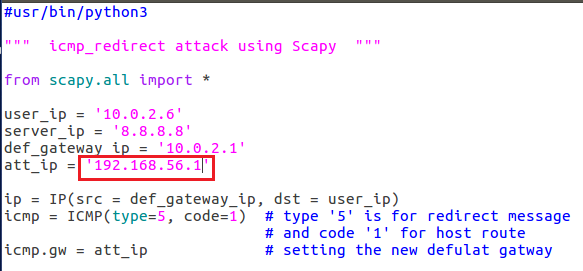


After executing "icmp\_redirect.py" in Attacker, this was the result in User:

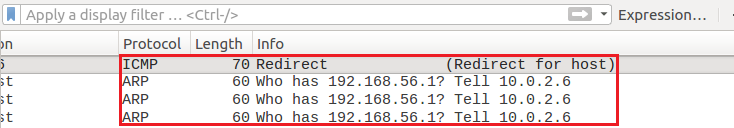
We can see our attack was successful, since now the default gateway User will use in order to access Google will be the Attacker (10.0.2.99)!

Note: We can see that the change of the default gateway is temporary – for 5 minutes, and afterwards the situation turned back to what it was before. This is a security measure activated by the OS.

2. Question 1 – External machine

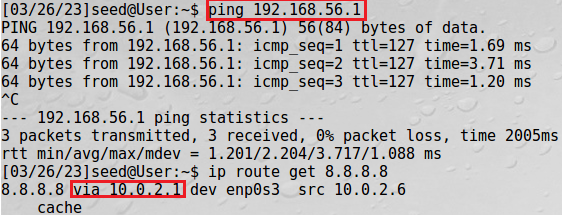
We changed the Attacker's IP in the code of "icmp\_redirect.py" to a machine that's outside of the User's LAN:

Again, we executed the code on Attacker and sent it to User, but now we couldn't take over the default gateway address, and it remained the same as before the attack:

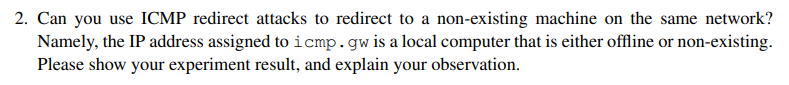
This is a screenshot from Wireshark:

We can see that the message was indeed sent, and then an ARP broadcast from the User was sent asking who has this address that the ICMP redirect message told it's a better touter for him.

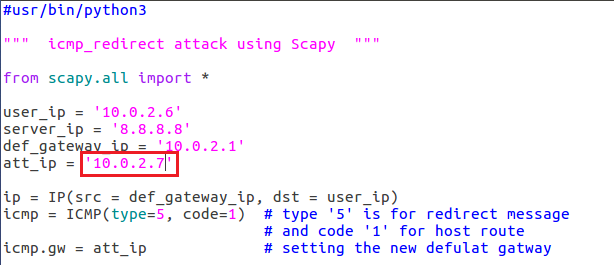
But we wanted to check it more deeply, so we sent a ping message from User to this IP address, so that User will have the IP address stored. Then, we sent the spoofed packet all over again. There wasn't any change in the results, the default gateway steel didn't change.



**To conclude**, it seems that it’s not possible to use external machine as the default gateway. This fact makes sense, since an ICMP redirect message should offer a better and closer way to a destination, and it's not likely that an external machine is a better way from the router of the LAN.

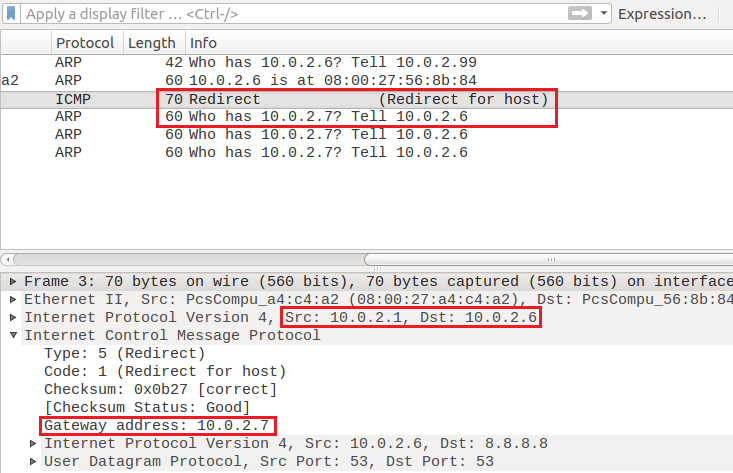
2. Question 2 – Offline machine (inside LAN)

Again, we changed the Attacker's IP in the code of "icmp\_redirect.py" to a machine that's inside the User's LAN but is currently offline:



The result was identical to the previous task – the default gateway wasn't changed:

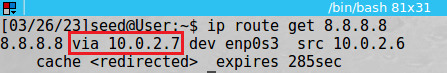


On Wireshark:

Again, we can see that the message was sent, and that the User sent immediately an ARP request who has this IP address.

But we wanted to check it more deeply, so we sent a ping message from this 3rd machine address (10.0.2.7) to User, so that User will have the 3rd machine's IP address stored. Then, we turned this computer off and sent the spoofed packet all over again.

Surprisingly, we managed to set the User's default gateway to the 3rd machine's address even though it was closed!

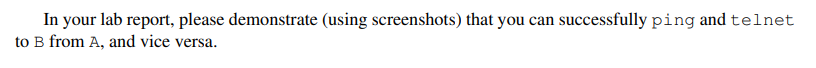


To conclude, it's possible to set a machine that's inside the User's LAN, but only if its IP address is familiar to user and stored on his computer.

**4. Task 3 – Routing and Reverse Path Filtering**

The network for this task:תמונה שמכילה תרשים

התיאור נוצר באופן אוטומטי

Task 3.b – Routing Setup

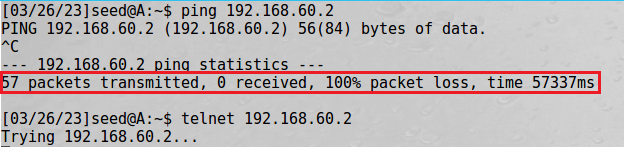
In the first phase we'll show that a connection cannot be established between A and B.

Then, in order to accomplish this objective, we first turned on "IP forwarding" in computer R, as instructed, so it can be used as a router (using the command: "*sudo sysctl net.ipv4.ip\_forward=1*"). Afterwards we added on A and B the other interface's details to the route table (as R is used as the router).

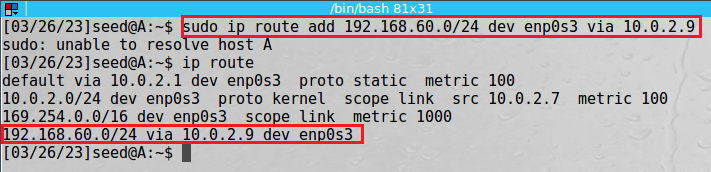
Let’s show that there isn't a way to connect between A and B:

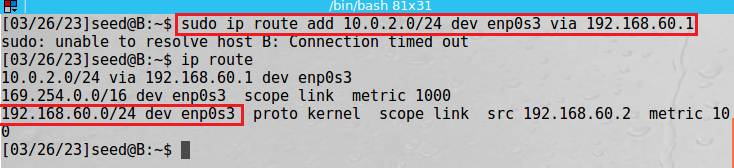
תמונה שמכילה טקסט

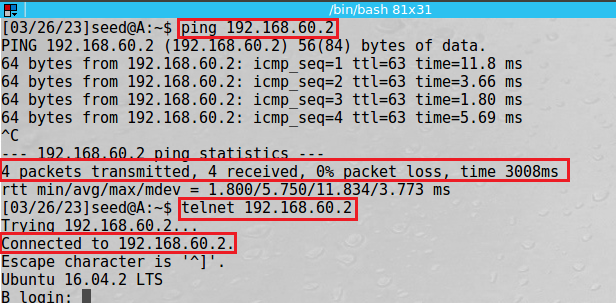
התיאור נוצר באופן אוטומטיTries to ping and establish telnet connection from B to A:

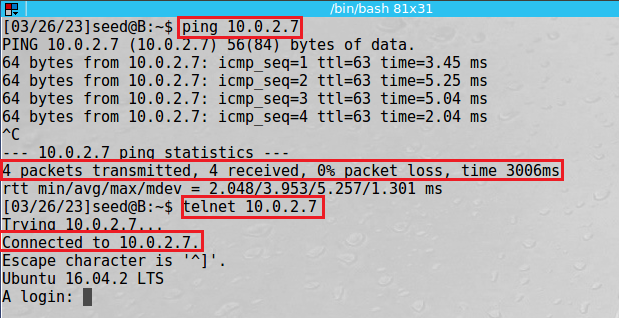
The situation is the same from A to B:

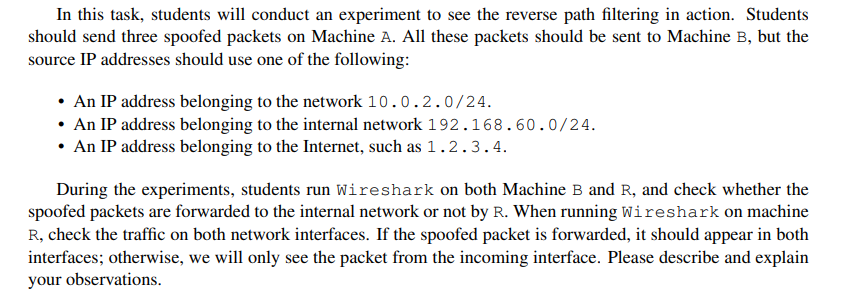
Then, we added the networks details in the machines, so they can communicate:



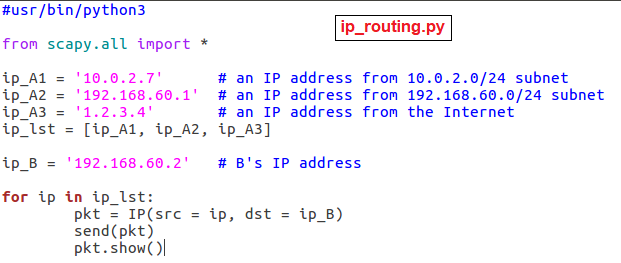


Now, we can see that we are able to ping and telnet from A to B:



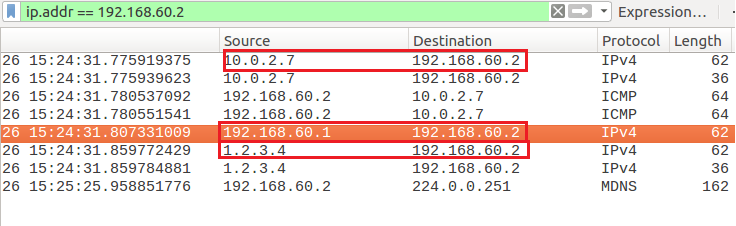
Task 3.c – Reverse Path Filtering

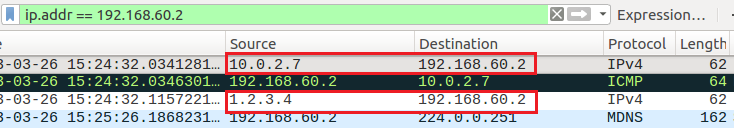
We activated Wireshark both B and R machines, and wrote the following Scapy code to send the 3 packets (from A to B) as instructed:



We executed this code ("ip\_routing.py") in machine A, and now we'll see which packets actually passed through R to B:

Screenshot of Wireshark from R:



Screenshot from Wireshark from B:

We can see that despite all 3 messages arrived machine R, only the 1st and 3rd messages (the messages from the "not-spoofed" nets) passed through to B.

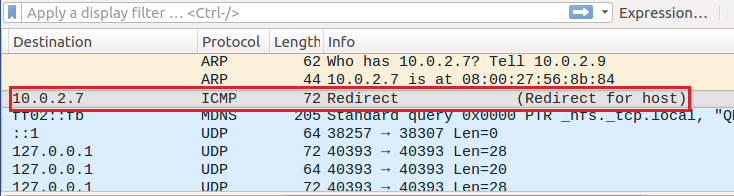
To conclude, as expected, the message from A to B that came through the interface of 192.168.60.0 with the IP from interface 10.0.2.0 was discarded by R, because of the RPF. But the other messages in which the IP address was compatible to the interface it should return to (1.2.3.4 came from "the internet" and should return that way, and 10.0.2.7 from interface 10.0.2.0 should also return that way) – were passed over to B.

**Netwox 86 – Automatic ICMP redirect**

In addition to Scapy we used it task 3, there is an automatic tool in netwox that generates ICMP redirect attacks easily – **netwox 86**.

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטיUsing netwox 86 in Attacker:

The result in User:

The big advantage of this tool is that it can be used for a wider range of victims.