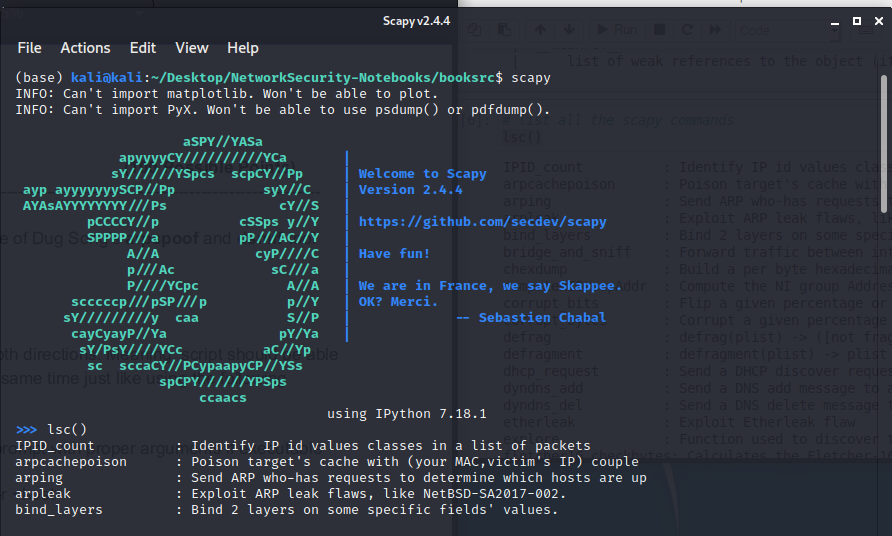
Kimlong Seng

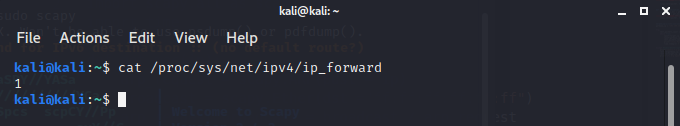
ARP Spoof

1. First, we need to install scapy (linux): pip3 install scapy

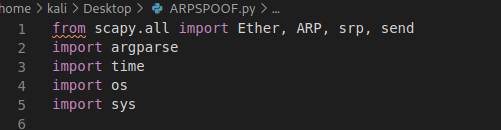


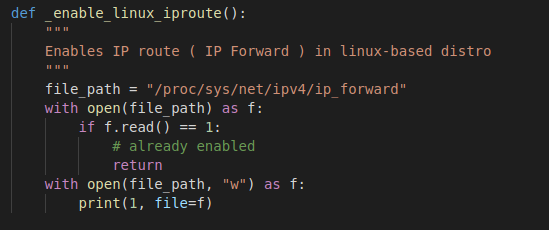
1. Make sure that the port forwarding is enable you can check it by using the command below.

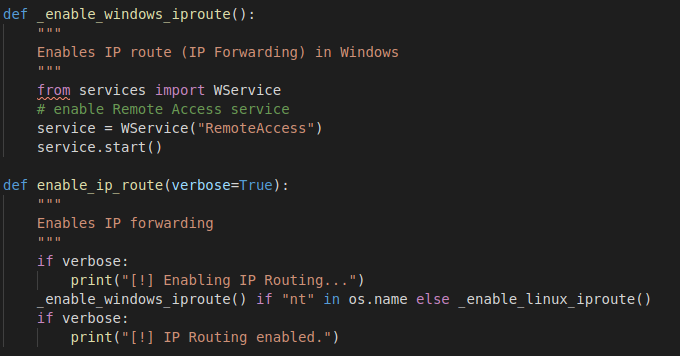
If it prints out 1 it means that port forwarding is enable. if it prints out 0 it means that port forwarding is disable, therefore you need to enable it by changing the number from 0 to 1.



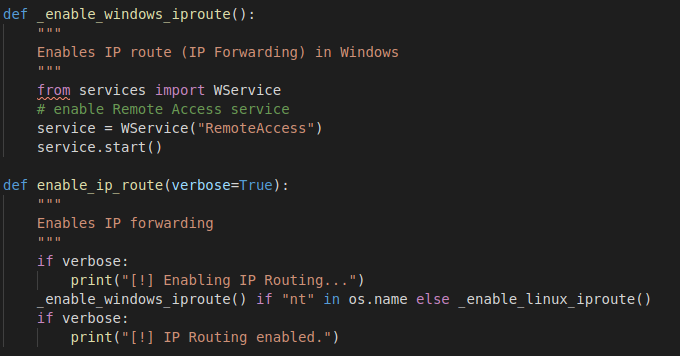
1. Writing the script:
2. First, we import all the necessary module to our script arpspoof.py

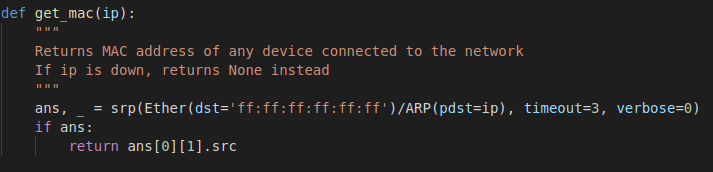


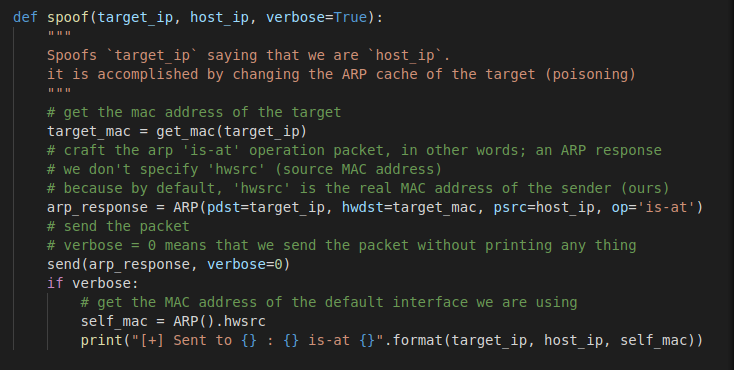
1. We check to see if port forwarding was enabled or not.
2. Port forwarding check function for window user.

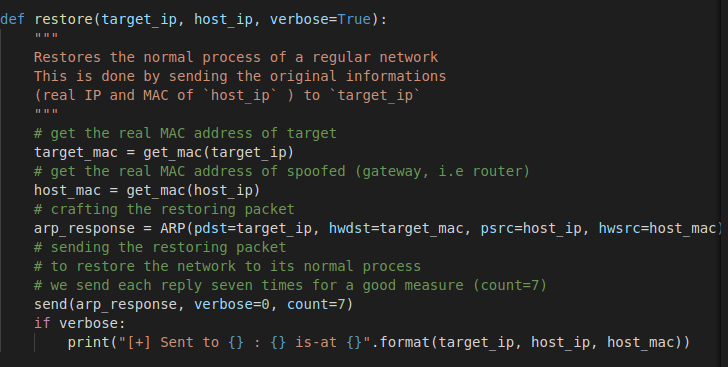


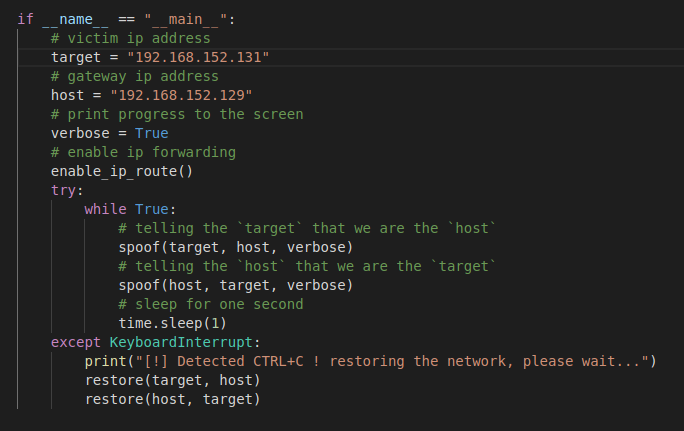
1. This function to enable the IP routing for all platforms



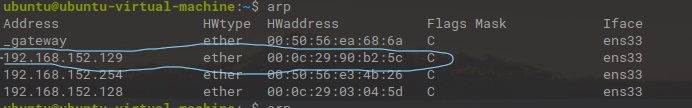
1. Before getting into the interesting part of the code we use a this function to get the all the MAC address in the network. We use srp() to send request and keep listening for any Arp response.
2. Second, we create a function that change the ARP cache of the target ip address and say that we have the host ip address. This will allow us to get the mac address of the target and reply with our ARP packet.



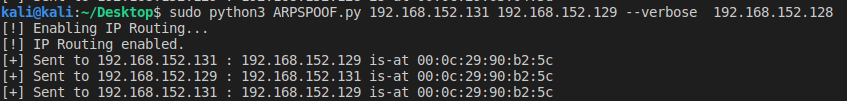
1. When we stop the attack, we want to restore and reassign the real addresses to the target device and leave the crime scene if we were never there in the first place. If we do not restore the addresses the target will lose internet connection and will notice that something has gone wrong.
2. Lastly, we need to write the main code, which spoof the target continuously until CTRL+C is detected then we will restore the original addresses.

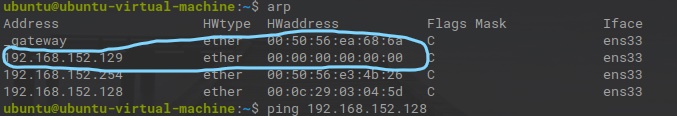
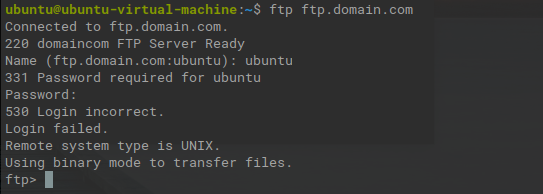


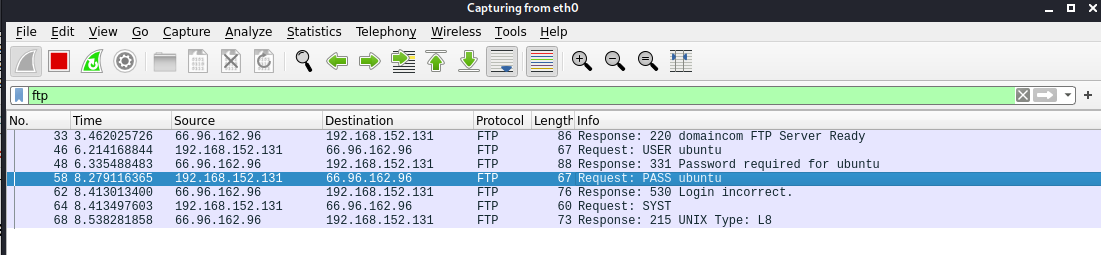
1. Running the script
2. Before we run the script, on the target machine, we use arp command to see the list of address on the server. Notice that Attacker HWaddress is normal.

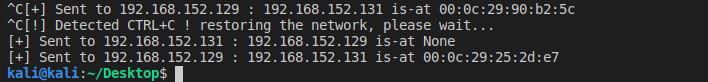


1. Now, we run the script using python3 ARPSOOF.py <target ip> <host-ip> --verbose



1. After we start the script, if we go to the target machine and run arp again, we can see that the HWaddress of the attacker change. That tell us that the script work.
2. At this point we can use any dsniff tool to sniff the net work in this case I use Wireshark to sniff and FTP package from the target machine. We can see that wiredshark was able to capter the username and password that the target sent using FTP.



1. After we finish sniffing. We will use CTRL+C to restore and assign the address back to the target.

This program has been taken from: https://www.thepythoncode.com/article/building-arp-spoofer-using-scapy