4.1 Generating legitimate traﬃc

Created a file **using sudo nano bashscript.sh**

#!/bin/bash

COUNTER=0

while [ $COUNTER -lt 180 do

sleep 1

curl 5.6.7.8

let COUNTER=COUNTER+1

done

Used command **sudo chmod gou+x bashscript.sh**

Used command **./bashscript.sh** to execute it

4.4 Collecting traﬃc statistics

SYN Cookies off on server node

SSH into attacker node, and client node.

Started tcpdump with command **sudo tcpdump -nn -i eth1 -w tcpdumpfile.txt**

started legit traffic on client node with command **./bashscript.sh**

After 30seconds , start attack with command **sudo flooder --dst 5.6.7.8 --src 1.1.2.5 --srcmask 255.255.255.0 --proto TCP --tcpflags SYN --sportmin 80 --sportmax 80**

After 120 seconds, stopped the attack

After 30 seconds, legit traffic stopped

Result is saved in file **tcpdumpfile.txt**

Viewed the results with command **sudo tcpdump -q -r tcpdump.txt**