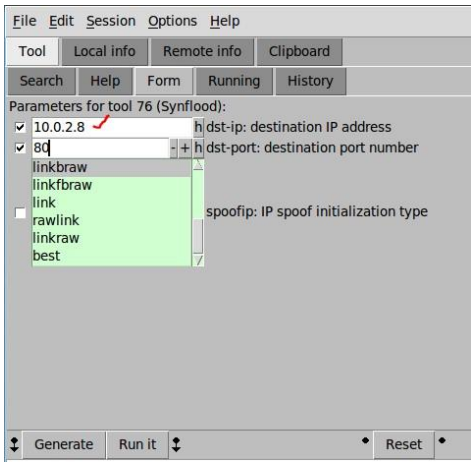
Task 1: SYN Flooding Attack

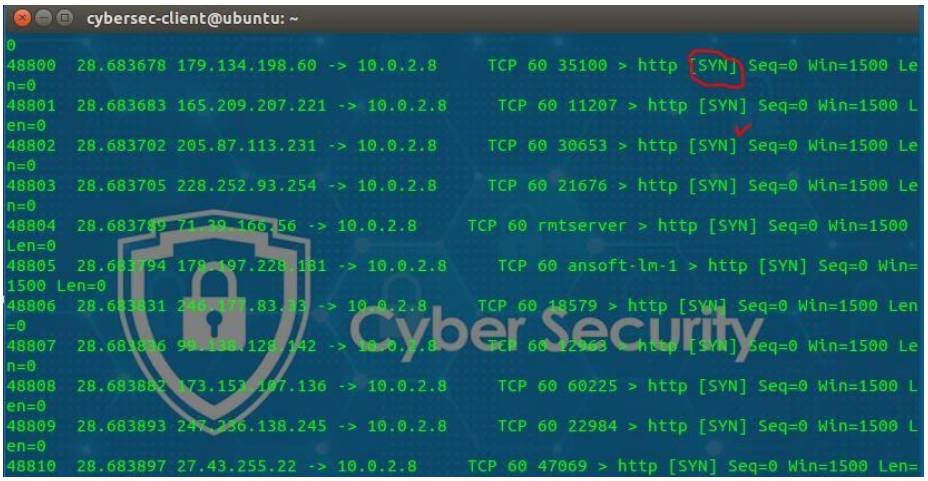
Turn off the connection first in the CyberSec-Server.

Type ‘sudo tshark’ on the CyberSec-Client

Type ‘sudo netwag’ and run it. Once the interface shows up, use the search box and type syn (tool 76).

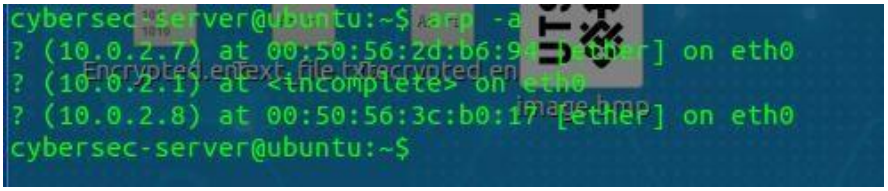


Enter all the required details then run it, and press ‘interrupt’ after few seconds. The result can be seen in Cyber-Sec Client where it shows [SYN-ACK]

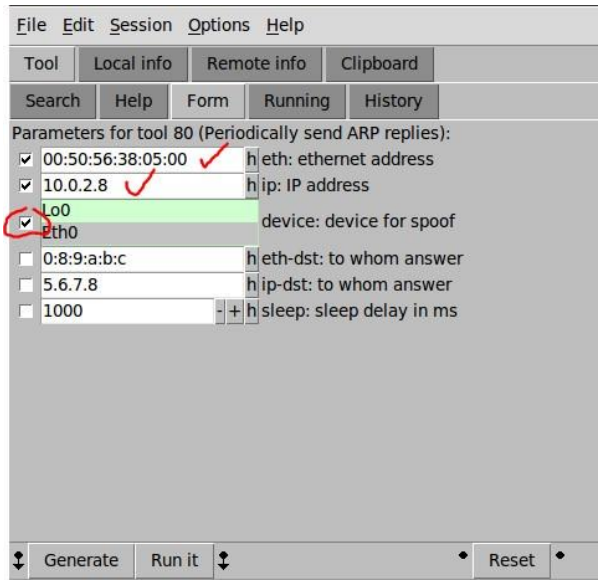


Task 2: ARP Cache Poisoning

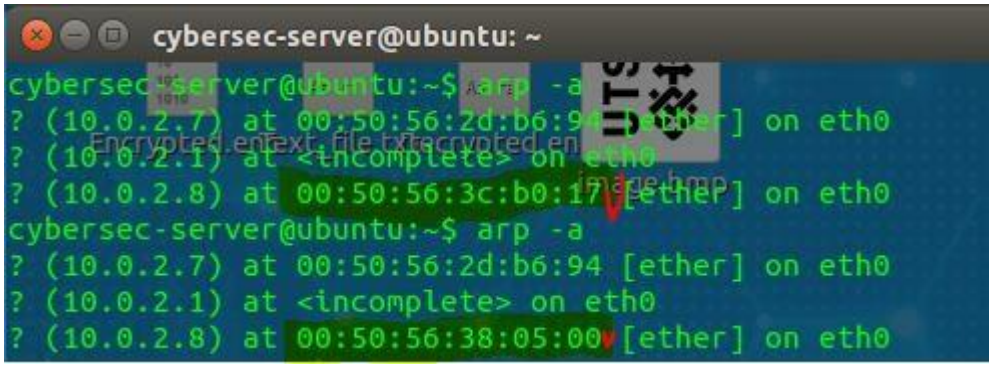
Open CyberSec-Server, get the arp information by entering arp-a and open Wireshark inside the CyberSec-Client.



Once again open netwag on the CyberSec-Attacker and search for tool 80 and enter all details inside the form section. After running the attack for a few seconds, press 'interrupt' button.

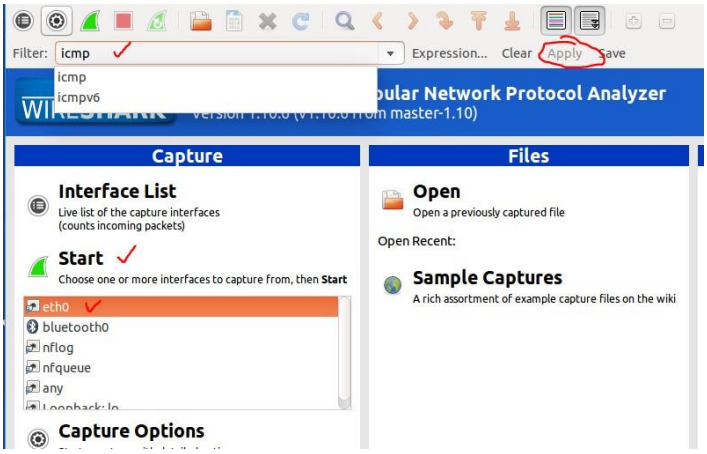


As can be seen the result has 'arp' on the filter.

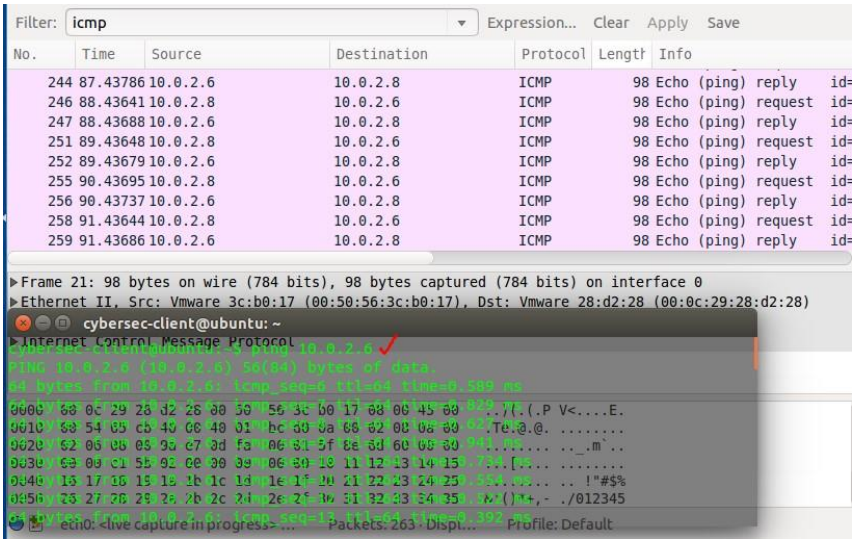


Task 3: ICMP Redirect Attack

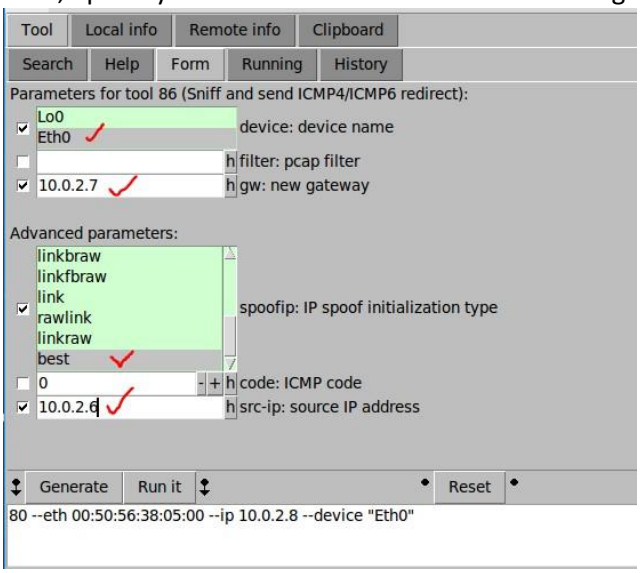
Go to CyberSec-Client and enter 'sudo wireshark'. Fill in 'icmp' in the filter then press apply. Then press start.



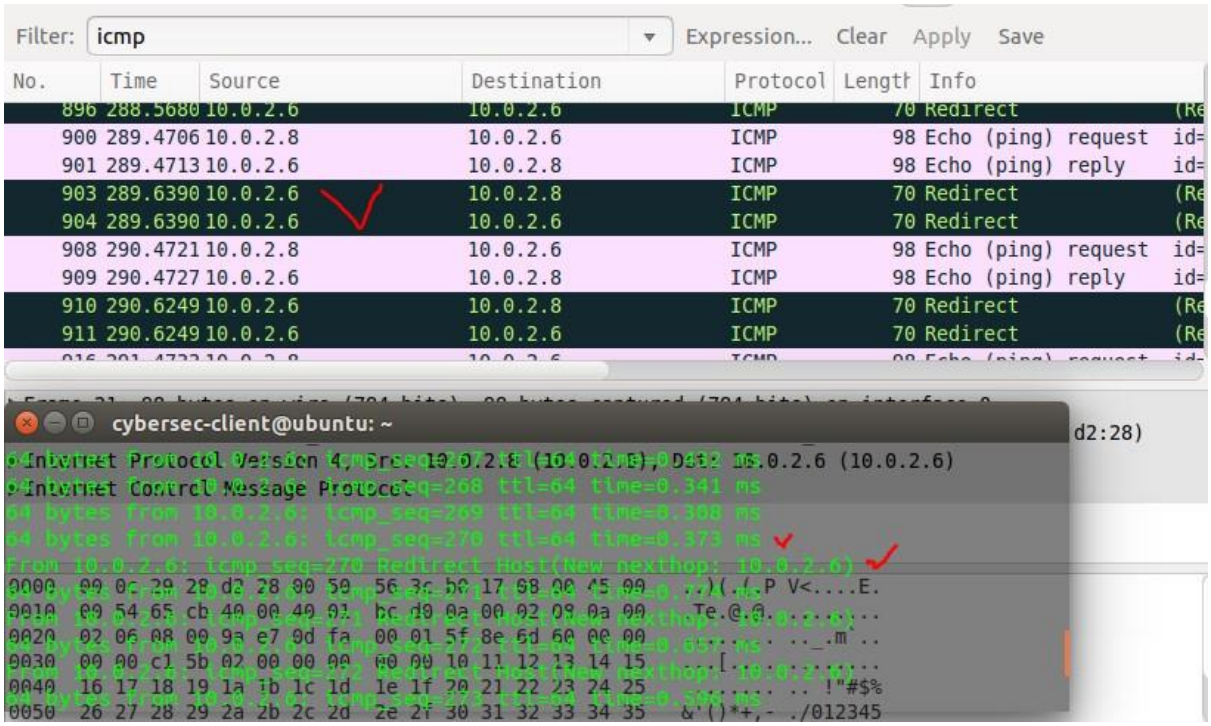
Open another terminal in the ClientSec-Client and type 'ping 10.0.2.6'. Here's the result.



Then, open CyberSec-Attacker and run 'sudo netwag' on the terminal.



Last thing is to verify the result on CyberSec-Server by pinging 10.0.2.6


Filter: icmp
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
896 288.5680 10.0.2.6 10.0.2.6 ICMP 70 Redirect
900 289.4706 10.0.2.8 10.0.2.6 ICMP 98 Echo (ping) request
901 289.4713 10.0.2.6 10.0.2.8 ICMP 98 Echo (ping) reply
903 289.6390 10.0.2.6 10.0.2.8 ICMP 70 Redirect
904 289.6390 10.0.2.6 10.0.2.6 ICMP 70 Redirect
908 290.4721 10.0.2.8 10.0.2.6 ICMP 98 Echo (ping) request
909 290.4727 10.0.2.6 10.0.2.8 ICMP 98 Echo (ping) reply
910 290.6249 10.0.2.6 10.0.2.8 ICMP 70 Redirect
911 290.6249 10.0.2.6 10.0.2.6 ICMP 70 Redirect
cybersec-client@ubuntu: ~
Internet Protocol Version 4, Src: 10.0.2.8 (10.0.2.8), Dst: 10.0.2.6 (10.0.2.6)
Internet Control Message Protocol
64 bytes from 10.0.2.6: icmp_seq=268 ttl=64 time=0.341 ms
64 bytes from 10.0.2.6: icmp_seq=269 ttl=64 time=0.308 ms
64 bytes from 10.0.2.6: icmp_seq=270 ttl=64 time=0.373 ms
From 10.0.2.6: icmp_seq=270 Redirect Host(New nexthop: 10.0.2.6)
0000 00 0c 29 28 d2 28 00 50 56 3c bc 17 08 00 45 00 ..)(.(.P V<....E.
0010 00 54 65 cb 40 00 40 01 bc d0 0a 00 02 08 0a 00 .Te.@.@. ....
0020 02 06 08 00 9a e7 0d fa 00 01 5f 8e 6d 60 00 00 .... .._.m`..
0030 00 00 c1 5b 02 00 00 00 00 00 10 11 12 13 14 15 ...[.... ....
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 .... .. !"#$%
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 &'()*+,- ./012345