

Task 1: SYN Flooding Attack

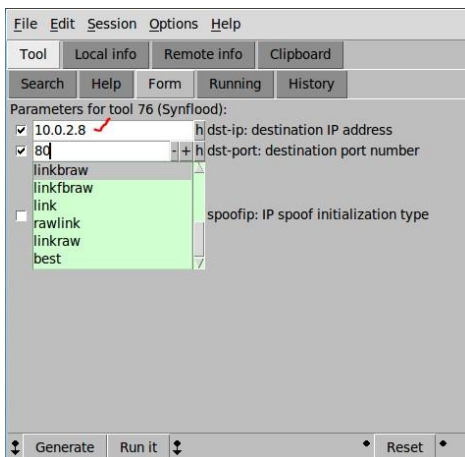
Turn off the connection first in the CyberSec-Server.



Type 'sudo tshark' on the CyberSec-Client

```
^Ccybersec-client@ubuntu:~$ sudo tshark ✓
tshark: Lua: Error during loading:
[string "/usr/share/wireshark/init.lua"]:46: dofile has been disabled due to ru
nning Wireshark as superuser. See http://wiki.wireshark.org/CaptureSetup/Capture
Privileges for help in running Wireshark as an unprivileged user.
Running as user "root" and group "root". This could be dangerous.
Capturing on 'eth0' ✓
1 0.000000 192.168.216.1 -> 192.168.216.255 UDP 305 Source port: 54915 Des
tination port: 54915
1 2 0.996211 192.168.216.1 -> 192.168.216.255 UDP 305 Source port: 54915 De
stination port: 54915
2 3 1.094215 192.168.216.1 -> 192.168.216.255 UDP 305 Source port: 54915 De
stination port: 54915
3 4 2.994303 192.168.216.1 -> 192.168.216.255 UDP 305 Source port: 54915 De
stination port: 54915
4 5 3.985883 192.168.216.1 -> 192.168.216.255 UDP 305 Source port: 54915 De
stination port: 54915
5 6 4.988888 192.168.216.1 -> 192.168.216.255 UDP 305 Source port: 54915 De
stination port: 54915
```

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]

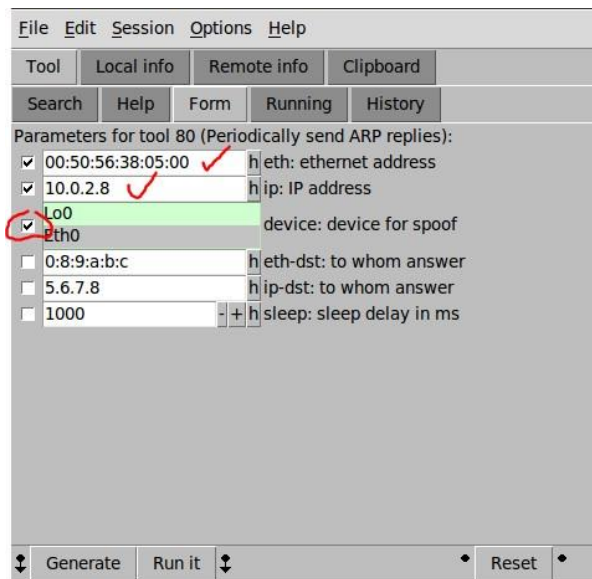
```
cybersec-client@ubuntu: ~
0
48800 28.683678 179.134.198.60 -> 10.0.2.8 TCP 60 35100 > http [SYN] Seq=0 Win=1500 Le
n=0
48801 28.683683 165.209.207.221 -> 10.0.2.8 TCP 60 11207 > http [SYN] Seq=0 Win=1500 L
en=0
48802 28.683702 205.87.113.231 -> 10.0.2.8 TCP 60 30653 > http [SYN] Seq=0 Win=1500 Le
n=0
48803 28.683705 228.252.93.254 -> 10.0.2.8 TCP 60 21676 > http [SYN] Seq=0 Win=1500 Le
n=0
48804 28.683709 71.39.166.56 -> 10.0.2.8 TCP 60 rmtserver > http [SYN] Seq=0 Win=1500
Len=0
48805 28.683794 178.197.228.181 -> 10.0.2.8 TCP 60 ansoft-lm-1 > http [SYN] Seq=0 Win=
1500 Len=0
48806 28.683831 286.177.83.13 -> 10.0.2.8 TCP 60 18579 > http [SYN] Seq=0 Win=1500 Len
=0
48807 28.683836 99.198.128.142 -> 10.0.2.8 TCP 60 12368 > http [SYN] Seq=0 Win=1500 Le
n=0
48808 28.683882 173.153.107.136 -> 10.0.2.8 TCP 60 60225 > http [SYN] Seq=0 Win=1500 L
en=0
48809 28.683893 247.236.138.245 -> 10.0.2.8 TCP 60 22984 > http [SYN] Seq=0 Win=1500 L
en=0
48810 28.683897 27.43.255.22 -> 10.0.2.8 TCP 60 47069 > http [SYN] Seq=0 Win=1500 Len=
```

Task 2: ARP Cache Poisoning

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

```
cybersec-server@ubuntu:~$ arp -a
? (10.0.2.7) at 00:50:56:2d:b6:94 [ether] on eth0
? (10.0.2.1) at <incomplete> on eth0
? (10.0.2.8) at 00:50:56:3c:b0:17 [ether] on eth0
cybersec-server@ubuntu:~$
```

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.

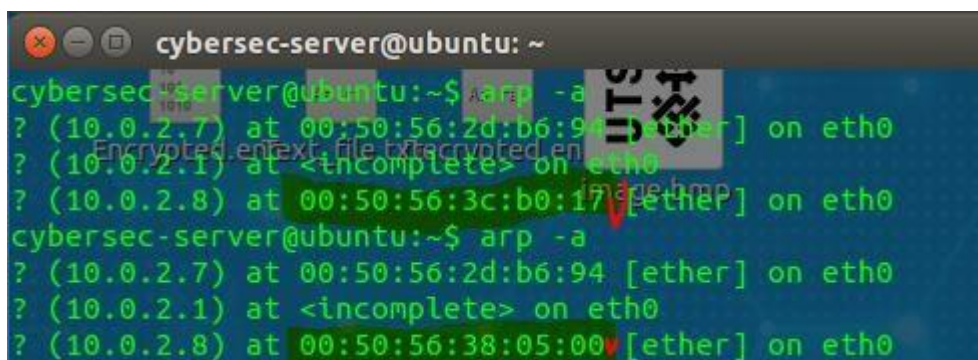


The screenshot shows the NetWag tool interface with the following parameters for tool 80 (Periodically send ARP replies):

Parameter	Value	Description
<input checked="" type="checkbox"/> 00:50:56:38:05:00	✓	h eth: ethernet address
<input checked="" type="checkbox"/> 10.0.2.8	✓	h ip: IP address
<input checked="" type="checkbox"/> Lo0		device: device for spoof
<input type="checkbox"/> 0:8:9:a:b:c		h eth-dst: to whom answer
<input type="checkbox"/> 5.6.7.8		h ip-dst: to whom answer
<input type="checkbox"/> 1000		h sleep: sleep delay in ms

Buttons at the bottom: Generate, Run it, Reset.

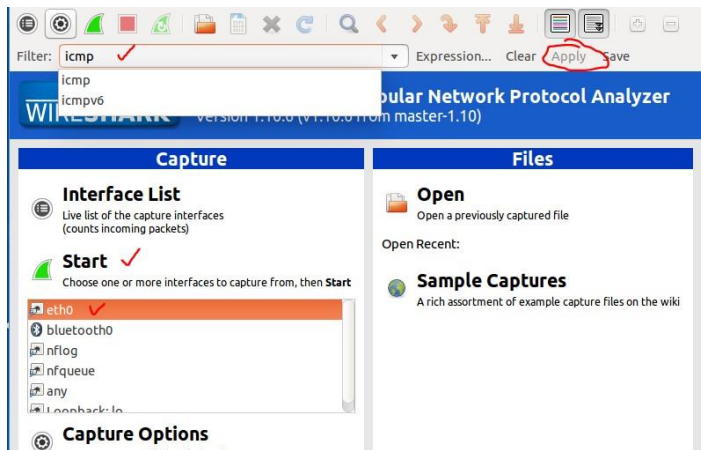
As can be seen the result has 'arp' on the filter.



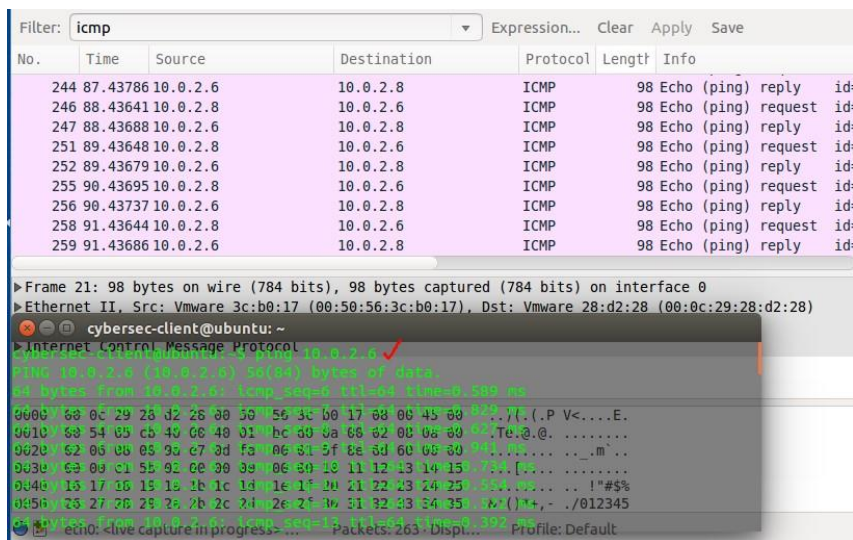
```
cybersec-server@ubuntu: ~
cybersec-server@ubuntu:~$ arp -a
? (10.0.2.7) at 00:50:56:2d:b6:94 [ether] on eth0
? (10.0.2.1) at <incomplete> on eth0
? (10.0.2.8) at 00:50:56:3c:b0:17 [ether] on eth0
cybersec-server@ubuntu:~$ arp -a
? (10.0.2.7) at 00:50:56:2d:b6:94 [ether] on eth0
? (10.0.2.1) at <incomplete> on eth0
? (10.0.2.8) at 00:50:56:38:05:00 [ether] on eth0
```

Task 3: ICMP Redirect Attack

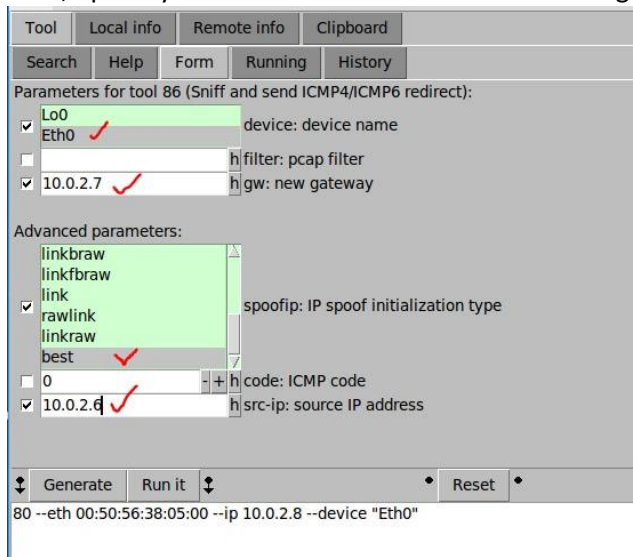
Go to CyberSec-Client and enter 'sudo wireshark'. Fill in 'icmp' in the filter then press apply. Then press start.



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 ping 10.0.2.6

