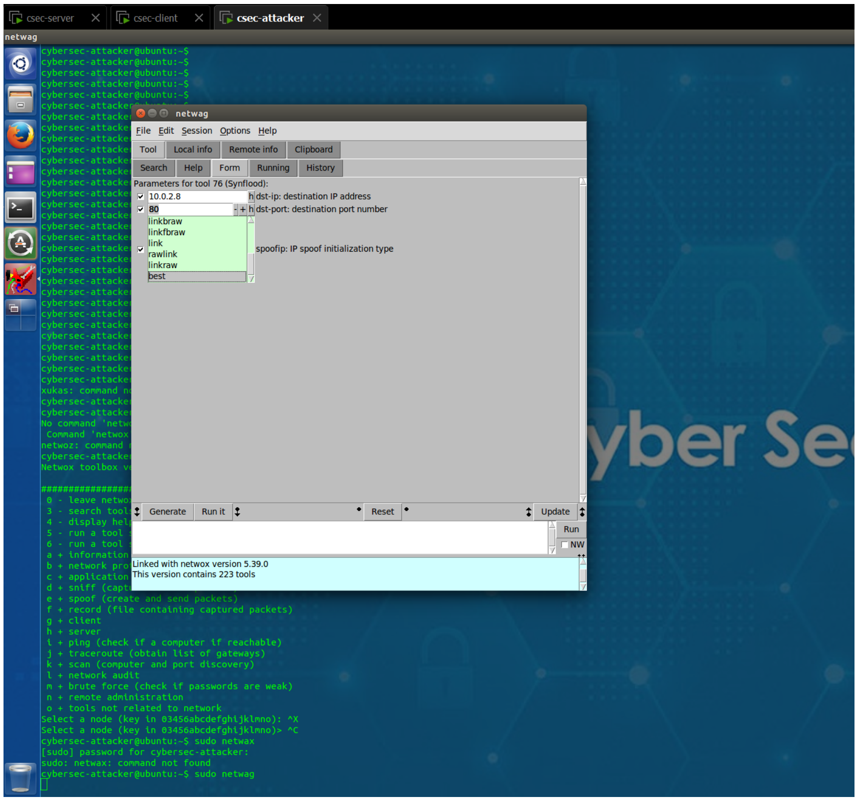
CSEC Week 05 Lab 04

Task 1 - SYN Flooding Attack

1. 

Parameters for tool 76 (Synflood):

☑ 10.0.2.8 h dst-ip: destination IP address

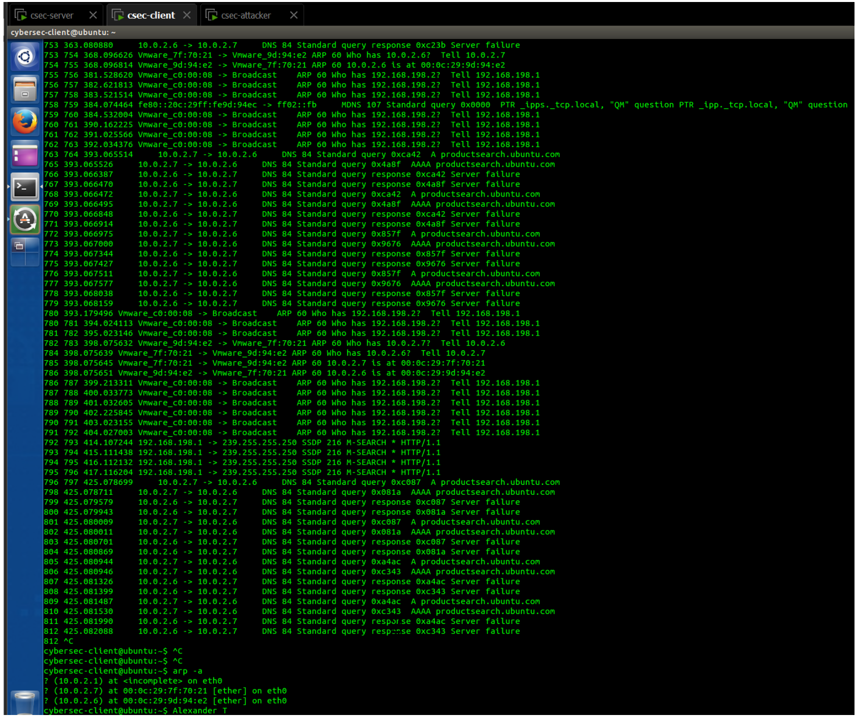
☑ 80 - + h dst-port: destination port number

☑ linkbraw / linkfbraw / link / rawlink / linkraw / best spoofip: IP spoof initialization type

Linked with netwox version 5.39.0
This version contains 223 tools

```
cybersec-attacker@ubuntu:~$
cybersec-attacker@ubuntu:~$
cybersec-attacker@ubuntu:~$
cybersec-attacker@ubuntu:~$
cybersec-attacker@ubuntu:~$
cybersec-attacker
cybersec-attacker
cybersec-attacker
cybersec-attacker
cybersec-attacker
cybersec-attacker
cybersec-attacker
cybersec-attacker
cybersec-attacker
cybersec-attacker
cybersec-attacker
cybersec-attacker
cybersec-attacker
cybersec-attacker
cybersec-attacker
cybersec-attacker
cybersec-attacker
cybersec-attacker
cybersec-attacker
cybersec-attacker
cybersec-attacker
cybersec-attacker
cybersec-attacker
cybersec-attacker
cybersec-attacker
cybersec-attacker
xukas: command nc
cybersec-attacker
cybersec-attacker
No command 'netwc
 Command 'netwox
netwoz: command n
cybersec-attacker
Netwox toolbox ve

#################
 0 - leave netwox
 3 - search tools
 4 - display help
 5 - run a tool
 6 - run a tool
 a + information
 b + network pro
 c + application
 d + sniff (captu
 e + spoof (create and send packets)
 f + record (file containing captured packets)
 g + client
 h + server
 i + ping (check if a computer if reachable)
 j + traceroute (obtain list of gateways)
 k + scan (computer and port discovery)
 l + network audit
 m + brute force (check if passwords are weak)
 n + remote administration
 o + tools not related to network
Select a node (key in 03456abcdefghijklmno): ^X
Select a node (key in 03456abcdefghijklmno)> ^C
cybersec-attacker@ubuntu:~$ sudo netwax
[sudo] password for cybersec-attacker:
sudo: netwax: command not found
cybersec-attacker@ubuntu:~$ sudo netwag
```

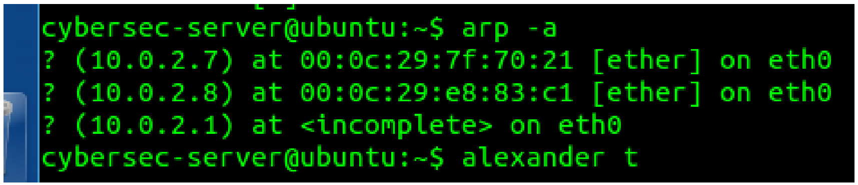


```
753 363.080880     10.0.2.6 -> 10.0.2.7     DNS 84 Standard query response 0xc23b Server failure
753 754 368.096626 Vmware_7f:70:21 -> Vmware_9d:94:e2 ARP 60 Who has 10.0.2.6?  Tell 10.0.2.7
754 755 368.096814 Vmware_9d:94:e2 -> Vmware_7f:70:21 ARP 60 10.0.2.6 is at 00:0c:29:9d:94:e2
755 756 381.528620 Vmware_c0:00:08 -> Broadcast    ARP 60 Who has 192.168.198.2?  Tell 192.168.198.1
756 757 382.621813 Vmware_c0:00:08 -> Broadcast    ARP 60 Who has 192.168.198.2?  Tell 192.168.198.1
757 758 383.521514 Vmware_c0:00:08 -> Broadcast    ARP 60 Who has 192.168.198.2?  Tell 192.168.198.1
758 759 384.074464 fe80::20c:29ff:fe9d:94ec -> ff02::fb     MDNS 107 Standard query 0x0000  PTR _ipps._tcp.local, "QM" question PTR _ipp._tcp.local, "QM" question
759 760 384.532004 Vmware_c0:00:08 -> Broadcast    ARP 60 Who has 192.168.198.2?  Tell 192.168.198.1
760 761 390.162225 Vmware_c0:00:08 -> Broadcast    ARP 60 Who has 192.168.198.2?  Tell 192.168.198.1
761 762 391.025566 Vmware_c0:00:08 -> Broadcast    ARP 60 Who has 192.168.198.2?  Tell 192.168.198.1
762 763 392.034376 Vmware_c0:00:08 -> Broadcast    ARP 60 Who has 192.168.198.2?  Tell 192.168.198.1
763 764 393.065514     10.0.2.7 -> 10.0.2.6     DNS 84 Standard query 0xca42  A productsearch.ubuntu.com
765 393.065526     10.0.2.7 -> 10.0.2.6     DNS 84 Standard query 0x4a8f  AAAA productsearch.ubuntu.com
766 393.066387     10.0.2.6 -> 10.0.2.7     DNS 84 Standard query response 0xca42 Server failure
767 393.066470     10.0.2.6 -> 10.0.2.7     DNS 84 Standard query response 0x4a8f Server failure
768 393.066472     10.0.2.7 -> 10.0.2.6     DNS 84 Standard query 0xca42  A productsearch.ubuntu.com
769 393.066495     10.0.2.7 -> 10.0.2.6     DNS 84 Standard query 0x4a8f  AAAA productsearch.ubuntu.com
770 393.066848     10.0.2.6 -> 10.0.2.7     DNS 84 Standard query response 0xca42 Server failure
771 393.066914     10.0.2.6 -> 10.0.2.7     DNS 84 Standard query response 0x4a8f Server failure
772 393.066975     10.0.2.7 -> 10.0.2.6     DNS 84 Standard query 0x857f  A productsearch.ubuntu.com
773 393.067000     10.0.2.7 -> 10.0.2.6     DNS 84 Standard query 0x9676  AAAA productsearch.ubuntu.com
774 393.067344     10.0.2.6 -> 10.0.2.7     DNS 84 Standard query response 0x857f Server failure
775 393.067427     10.0.2.6 -> 10.0.2.7     DNS 84 Standard query response 0x9676 Server failure
776 393.067511     10.0.2.7 -> 10.0.2.6     DNS 84 Standard query 0x857f  A productsearch.ubuntu.com
777 393.067577     10.0.2.7 -> 10.0.2.6     DNS 84 Standard query 0x9676  AAAA productsearch.ubuntu.com
778 393.068038     10.0.2.6 -> 10.0.2.7     DNS 84 Standard query response 0x857f Server failure
779 393.068159     10.0.2.6 -> 10.0.2.7     DNS 84 Standard query response 0x9676 Server failure
780 393.179496 Vmware_c0:00:08 -> Broadcast    ARP 60 Who has 192.168.198.2?  Tell 192.168.198.1
780 781 394.024113 Vmware_c0:00:08 -> Broadcast    ARP 60 Who has 192.168.198.2?  Tell 192.168.198.1
781 782 395.023146 Vmware_c0:00:08 -> Broadcast    ARP 60 Who has 192.168.198.2?  Tell 192.168.198.1
782 783 398.075632 Vmware_9d:94:e2 -> Vmware_7f:70:21 ARP 60 Who has 10.0.2.7?  Tell 10.0.2.6
784 398.075639 Vmware_7f:70:21 -> Vmware_9d:94:e2 ARP 60 Who has 10.0.2.6?  Tell 10.0.2.7
785 398.075645 Vmware_7f:70:21 -> Vmware_9d:94:e2 ARP 60 10.0.2.7 is at 00:0c:29:7f:70:21
786 398.075651 Vmware_9d:94:e2 -> Vmware_7f:70:21 ARP 60 10.0.2.6 is at 00:0c:29:9d:94:e2
786 787 399.213311 Vmware_c0:00:08 -> Broadcast    ARP 60 Who has 192.168.198.2?  Tell 192.168.198.1
787 788 400.033773 Vmware_c0:00:08 -> Broadcast    ARP 60 Who has 192.168.198.2?  Tell 192.168.198.1
788 789 401.032605 Vmware_c0:00:08 -> Broadcast    ARP 60 Who has 192.168.198.2?  Tell 192.168.198.1
789 790 402.225845 Vmware_c0:00:08 -> Broadcast    ARP 60 Who has 192.168.198.2?  Tell 192.168.198.1
790 791 403.023155 Vmware_c0:00:08 -> Broadcast    ARP 60 Who has 192.168.198.2?  Tell 192.168.198.1
791 792 404.027003 Vmware_c0:00:08 -> Broadcast    ARP 60 Who has 192.168.198.2?  Tell 192.168.198.1
792 793 414.107244 192.168.198.1 -> 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
793 794 415.111438 192.168.198.1 -> 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
794 795 416.112132 192.168.198.1 -> 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
795 796 417.116204 192.168.198.1 -> 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
796 797 425.078699     10.0.2.7 -> 10.0.2.6     DNS 84 Standard query 0xc087  A productsearch.ubuntu.com
798 425.078711     10.0.2.7 -> 10.0.2.6     DNS 84 Standard query 0x081a  AAAA productsearch.ubuntu.com
799 425.079579     10.0.2.6 -> 10.0.2.7     DNS 84 Standard query response 0xc087 Server failure
800 425.079943     10.0.2.6 -> 10.0.2.7     DNS 84 Standard query response 0x081a Server failure
801 425.080009     10.0.2.7 -> 10.0.2.6     DNS 84 Standard query 0xc087  A productsearch.ubuntu.com
802 425.080011     10.0.2.7 -> 10.0.2.6     DNS 84 Standard query 0x081a  AAAA productsearch.ubuntu.com
803 425.080701     10.0.2.6 -> 10.0.2.7     DNS 84 Standard query response 0xc087 Server failure
804 425.080869     10.0.2.6 -> 10.0.2.7     DNS 84 Standard query response 0x081a Server failure
805 425.080944     10.0.2.7 -> 10.0.2.6     DNS 84 Standard query 0xa4ac  A productsearch.ubuntu.com
806 425.080946     10.0.2.7 -> 10.0.2.6     DNS 84 Standard query 0xc343  AAAA productsearch.ubuntu.com
807 425.081326     10.0.2.6 -> 10.0.2.7     DNS 84 Standard query response 0xa4ac Server failure
808 425.081399     10.0.2.6 -> 10.0.2.7     DNS 84 Standard query response 0xc343 Server failure
809 425.081487     10.0.2.7 -> 10.0.2.6     DNS 84 Standard query 0xa4ac  A productsearch.ubuntu.com
810 425.081530     10.0.2.7 -> 10.0.2.6     DNS 84 Standard query 0xc343  AAAA productsearch.ubuntu.com
811 425.081990     10.0.2.6 -> 10.0.2.7     DNS 84 Standard query response 0xa4ac Server failure
812 425.082088     10.0.2.6 -> 10.0.2.7     DNS 84 Standard query response 0xc343 Server failure
812 ^C
cybersec-client@ubuntu:~$ ^C
cybersec-client@ubuntu:~$ ^C
cybersec-client@ubuntu:~$ arp -a
? (10.0.2.1) at <incomplete> on eth0
? (10.0.2.7) at 00:0c:29:7f:70:21 [ether] on eth0
? (10.0.2.6) at 00:0c:29:9d:94:e2 [ether] on eth0
cybersec-client@ubuntu:~$ Alexander T
```

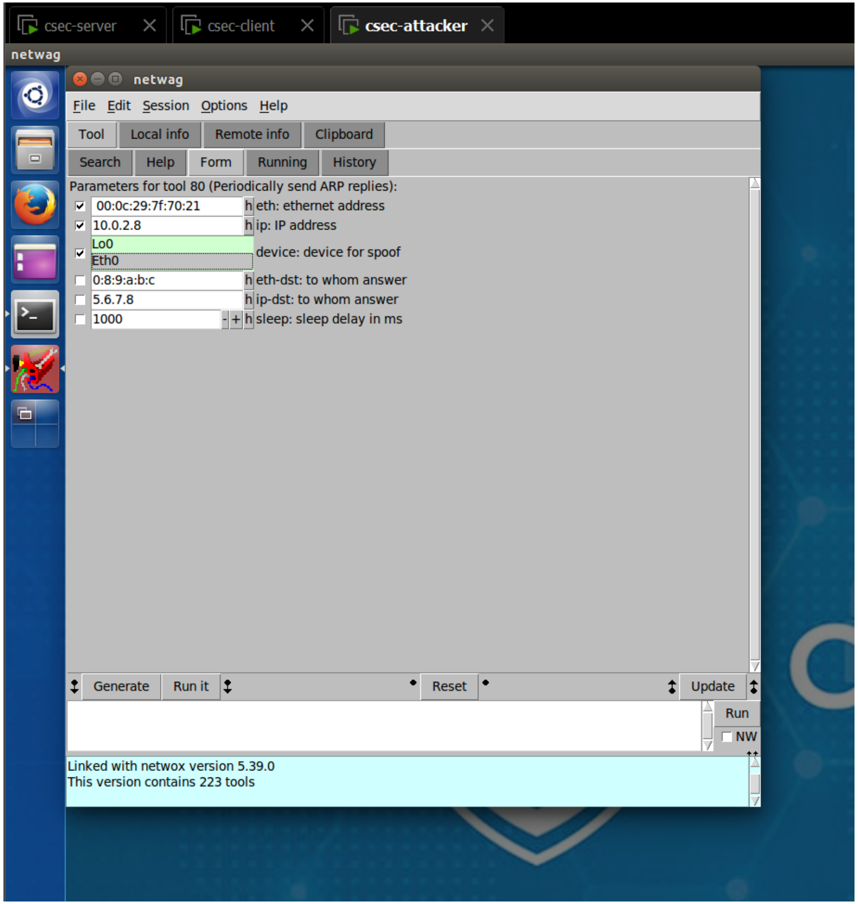
2. We can see from the screenshots that as soon as the SYN flooding attack is initiated from the attacker, the client gets flooded with ARP packets (there are also some DNS queries from the Ubuntu app store, but those are not part of the attack).

3. While a DOS attack attempts to overwhelm a server due to the sheer number of requests, this can be somewhat mitigated by simply improving the hardware. A SYN flood attack exploits the queue size of the target server, which means improving the hardware may not protect against SYN flood attacks - you also need to increase the queue size (or even better, use key hashes to prevent using the queue altogether for unfinished requests). This attack is easily mitigated now, but can be quite impactful to availability.

Task 2 - ARP cache poisoning

1. 

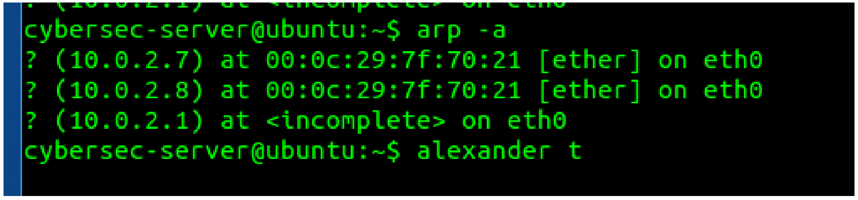
```
cybersec-server@ubuntu:~$ arp -a
? (10.0.2.7) at 00:0c:29:7f:70:21 [ether] on eth0
? (10.0.2.8) at 00:0c:29:e8:83:c1 [ether] on eth0
? (10.0.2.1) at <incomplete> on eth0
cybersec-server@ubuntu:~$ alexander t
```



Parameters for tool 80 (Periodically send ARP replies):

```
☑ 00:0c:29:7f:70:21   h eth: ethernet address
☑ 10.0.2.8            h ip: IP address
☑ Lo0
  Eth0                  device: device for spoof
□ 0:8:9:a:b:c         h eth-dst: to whom answer
□ 5.6.7.8             h ip-dst: to whom answer
□ 1000            - + h sleep: sleep delay in ms
```

```
Linked with netwox version 5.39.0
This version contains 223 tools
```



```
cybersec-server@ubuntu:~$ arp -a
? (10.0.2.7) at 00:0c:29:7f:70:21 [ether] on eth0
? (10.0.2.8) at 00:0c:29:7f:70:21 [ether] on eth0
? (10.0.2.1) at <incomplete> on eth0
cybersec-server@ubuntu:~$ alexander t
```

2. We can see that after running the attack, the server's ARP cache points the Clients IP address to the Attackers MAC address, effectively spoofing the client.

3. To mitigate this attack we can:

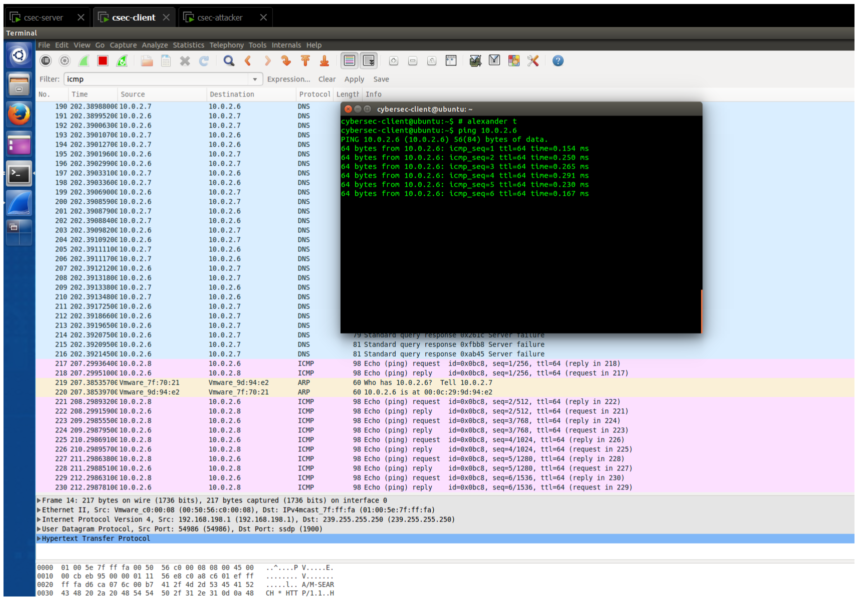
    1. Prevent the Attacker from entering the network - this is usually standard practice, but passwords on your networks!

    2. Checking for duplicate MAC addresses - this can help detect an ARP spoofing attempt, but can be circumvented by the Attacker.

    3. Static ARP table - impossible to scale and maintain.

    4. Detecting and preventing with automated tools - probably best bet.

Task 3 - ICMP Redirect Attack

1. 

csec-server
csec-client
csec-attacker
Terminal
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: icmp

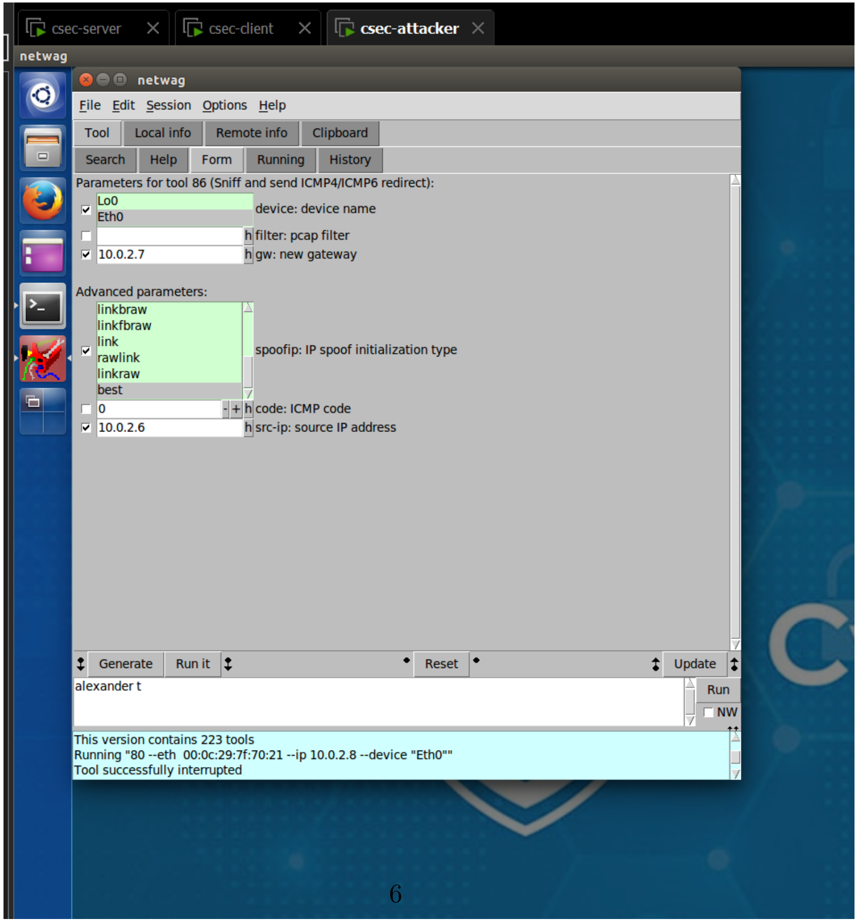
```
No.   Time        Source            Destination       Protocol Length Info
  190 202.3898000 10.0.2.7          10.0.2.6          DNS
  191 202.3899520 10.0.2.6          10.0.2.7          DNS
  192 202.3900630 10.0.2.6          10.0.2.7          DNS
  193 202.3901070 10.0.2.7          10.0.2.6          DNS
  194 202.3901270 10.0.2.7          10.0.2.6          DNS
  195 202.3901960 10.0.2.6          10.0.2.7          DNS
  196 202.3902990 10.0.2.6          10.0.2.7          DNS
  197 202.3903310 10.0.2.7          10.0.2.6          DNS
  198 202.3903360 10.0.2.7          10.0.2.6          DNS
  199 202.3906900 10.0.2.6          10.0.2.7          DNS
  200 202.3908590 10.0.2.6          10.0.2.7          DNS
  201 202.3908790 10.0.2.7          10.0.2.6          DNS
  202 202.3908840 10.0.2.7          10.0.2.6          DNS
  203 202.3909820 10.0.2.6          10.0.2.7          DNS
  204 202.3910920 10.0.2.6          10.0.2.7          DNS
  205 202.3911110 10.0.2.7          10.0.2.6          DNS
  206 202.3911170 10.0.2.7          10.0.2.6          DNS
  207 202.3912120 10.0.2.6          10.0.2.7          DNS
  208 202.3913180 10.0.2.6          10.0.2.7          DNS
  209 202.3913380 10.0.2.7          10.0.2.6          DNS
  210 202.3913480 10.0.2.7          10.0.2.6          DNS
  211 202.3917250 10.0.2.6          10.0.2.7          DNS
  212 202.3918660 10.0.2.6          10.0.2.7          DNS
  213 202.3919650 10.0.2.6          10.0.2.7          DNS
  214 202.3920750 10.0.2.6          10.0.2.7          DNS          79 Standard query response 0x261c Server failure
  215 202.3920950 10.0.2.6          10.0.2.7          DNS          81 Standard query response 0xfbb8 Server failure
  216 202.3921450 10.0.2.6          10.0.2.7          DNS          81 Standard query response 0xab45 Server failure
  217 207.2993640 10.0.2.8          10.0.2.6          ICMP         98 Echo (ping) request  id=0x0bc8, seq=1/256, ttl=64 (reply in 218)
  218 207.2995100 10.0.2.6          10.0.2.8          ICMP         98 Echo (ping) reply    id=0x0bc8, seq=1/256, ttl=64 (request in 217)
  219 207.3853570 Vmware_7f:70:21   Vmware_9d:94:e2   ARP          60 Who has 10.0.2.6?  Tell 10.0.2.7
  220 207.3853970 Vmware_9d:94:e2   Vmware_7f:70:21   ARP          60 10.0.2.6 is at 00:0c:29:9d:94:e2
  221 208.2989320 10.0.2.8          10.0.2.6          ICMP         98 Echo (ping) request  id=0x0bc8, seq=2/512, ttl=64 (reply in 222)
  222 208.2991590 10.0.2.6          10.0.2.8          ICMP         98 Echo (ping) reply    id=0x0bc8, seq=2/512, ttl=64 (request in 221)
  223 209.2985550 10.0.2.8          10.0.2.6          ICMP         98 Echo (ping) request  id=0x0bc8, seq=3/768, ttl=64 (reply in 224)
  224 209.2987950 10.0.2.6          10.0.2.8          ICMP         98 Echo (ping) reply    id=0x0bc8, seq=3/768, ttl=64 (request in 223)
  225 210.2986910 10.0.2.8          10.0.2.6          ICMP         98 Echo (ping) request  id=0x0bc8, seq=4/1024, ttl=64 (reply in 226)
  226 210.2989570 10.0.2.6          10.0.2.8          ICMP         98 Echo (ping) reply    id=0x0bc8, seq=4/1024, ttl=64 (request in 225)
  227 211.2986380 10.0.2.8          10.0.2.6          ICMP         98 Echo (ping) request  id=0x0bc8, seq=5/1280, ttl=64 (reply in 228)
  228 211.2988510 10.0.2.6          10.0.2.8          ICMP         98 Echo (ping) reply    id=0x0bc8, seq=5/1280, ttl=64 (request in 227)
  229 212.2986310 10.0.2.8          10.0.2.6          ICMP         98 Echo (ping) request  id=0x0bc8, seq=6/1536, ttl=64 (reply in 230)
  230 212.2987810 10.0.2.6          10.0.2.8          ICMP         98 Echo (ping) reply    id=0x0bc8, seq=6/1536, ttl=64 (request in 229)
```

```
▶Frame 14: 217 bytes on wire (1736 bits), 217 bytes captured (1736 bits) on interface 0
▶Ethernet II, Src: Vmware_c0:00:08 (00:50:56:c0:00:08), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
▶Internet Protocol Version 4, Src: 192.168.198.1 (192.168.198.1), Dst: 239.255.255.250 (239.255.255.250)
▶User Datagram Protocol, Src Port: 54986 (54986), Dst Port: ssdp (1900)
▶Hypertext Transfer Protocol

0000  01 00 5e 7f ff fa 00 50  56 c0 00 08 08 00 45 00   ..^....P V.....E.
0010  00 cb eb 95 00 00 01 11  56 e8 c0 a8 c6 01 ef ff   ........ V.......
0020  ff fa d6 ca 07 6c 00 b7  41 2f 4d 2d 53 45 41 52   .....l.. A/M-SEAR
0030  43 48 20 2a 20 48 54 54  50 2f 31 2e 31 0d 0a 48   CH * HTT P/1.1..H
```

cybersec-client@ubuntu: ~

```
cybersec-client@ubuntu:~$ # alexander t
cybersec-client@ubuntu:~$ ping 10.0.2.6
PING 10.0.2.6 (10.0.2.6) 56(84) bytes of data.
64 bytes from 10.0.2.6: icmp_seq=1 ttl=64 time=0.154 ms
64 bytes from 10.0.2.6: icmp_seq=2 ttl=64 time=0.250 ms
64 bytes from 10.0.2.6: icmp_seq=3 ttl=64 time=0.265 ms
64 bytes from 10.0.2.6: icmp_seq=4 ttl=64 time=0.291 ms
64 bytes from 10.0.2.6: icmp_seq=5 ttl=64 time=0.230 ms
64 bytes from 10.0.2.6: icmp_seq=6 ttl=64 time=0.167 ms
```



csec-server
csec-client
csec-attacker
netwag
netwag
File Edit Session Options Help
Tool Local info Remote info Clipboard
Search Help Form Running History
Generate Run it Reset Update
Run

Parameters for tool 86 (Sniff and send ICMP4/ICMP6 redirect):

☑ Lo0 / Eth0 device: device name
□ h filter: pcap filter
☑ 10.0.2.7 h gw: new gateway

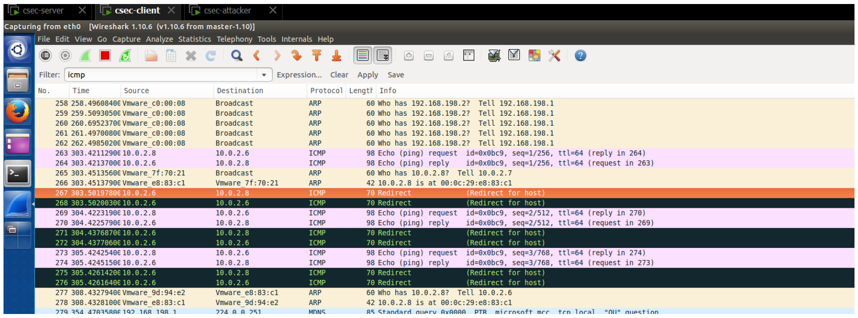
Advanced parameters:

☑ linkbraw / linkfbraw / link / rawlink / linkraw / best spoofip: IP spoof initialization type
□ 0 - + h code: ICMP code
☑ 10.0.2.6 h src-ip: source IP address

alexander t

□ NW

```
This version contains 223 tools
Running "80 --eth  00:0c:29:7f:70:21 --ip 10.0.2.8 --device "Eth0""
Tool successfully interrupted
```


csec-server
csec-client
csec-attacker
Capturing from eth0 [Wireshark 1.10.6 (v1.10.6 from master-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: icmp

```
No.   Time         Source             Destination        Protocol Length Info
  258 258.4960840  Vmware_c0:00:08    Broadcast          ARP       60 Who has 192.168.198.2?  Tell 192.168.198.1
  259 259.5093050  Vmware_c0:00:08    Broadcast          ARP       60 Who has 192.168.198.2?  Tell 192.168.198.1
  260 260.6952370  Vmware_c0:00:08    Broadcast          ARP       60 Who has 192.168.198.2?  Tell 192.168.198.1
  261 261.4970080  Vmware_c0:00:08    Broadcast          ARP       60 Who has 192.168.198.2?  Tell 192.168.198.1
  262 262.4985020  Vmware_c0:00:08    Broadcast          ARP       60 Who has 192.168.198.2?  Tell 192.168.198.1
  263 303.4211290  10.0.2.8           10.0.2.6           ICMP      98 Echo (ping) request  id=0x0bc9, seq=1/256, ttl=64 (reply in 264)
  264 303.4213700  10.0.2.6           10.0.2.8           ICMP      98 Echo (ping) reply    id=0x0bc9, seq=1/256, ttl=64 (request in 263)
  265 303.4513560  Vmware_7f:70:21    Broadcast          ARP       60 Who has 10.0.2.8?  Tell 10.0.2.7
  266 303.4513790  Vmware_e8:83:c1    Vmware_7f:70:21    ARP       42 10.0.2.8 is at 00:0c:29:e8:83:c1
  267 303.5019780  10.0.2.6           10.0.2.8           ICMP      70 Redirect             (Redirect for host)
  268 303.5020030  10.0.2.6           10.0.2.6           ICMP      70 Redirect             (Redirect for host)
  269 304.4223190  10.0.2.8           10.0.2.6           ICMP      98 Echo (ping) request  id=0x0bc9, seq=2/512, ttl=64 (reply in 270)
  270 304.4225790  10.0.2.6           10.0.2.8           ICMP      98 Echo (ping) reply    id=0x0bc9, seq=2/512, ttl=64 (request in 269)
  271 304.4376870  10.0.2.6           10.0.2.8           ICMP      70 Redirect             (Redirect for host)
  272 304.4377060  10.0.2.6           10.0.2.6           ICMP      70 Redirect             (Redirect for host)
  273 305.4242540  10.0.2.8           10.0.2.6           ICMP      98 Echo (ping) request  id=0x0bc9, seq=3/768, ttl=64 (reply in 274)
  274 305.4245150  10.0.2.6           10.0.2.8           ICMP      98 Echo (ping) reply    id=0x0bc9, seq=3/768, ttl=64 (request in 273)
  275 305.4261420  10.0.2.6           10.0.2.8           ICMP      70 Redirect             (Redirect for host)
  276 305.4261640  10.0.2.6           10.0.2.6           ICMP      70 Redirect             (Redirect for host)
  277 308.4327940  Vmware_9d:94:e2    Vmware_e8:83:c1    ARP       60 Who has 10.0.2.8?  Tell 10.0.2.6
  278 308.4328100  Vmware_e8:83:c1    Vmware_9d:94:e2    ARP       42 10.0.2.8 is at 00:0c:29:e8:83:c1
  279 354.4703580  192.168.198.1      224.0.0.251        MDNS      85 Standard query 0x0000  PTR _microsoft_mcc._tcp.local, "QU" question
```

2. After launching the attack, the client starts receiving redirects, prompting an updato to its routing.

3. Biggest mitigation seems to just be not using ICMP at all.