Cyber Security Week-3 - DNS Pharming

Task 1

Screenshots required: (3)

1. Dig command before the change of ‘dns-nameservers’ in the ‘interfaces’ file.

```
cybersec-client@Benjamin:/etc/network$ 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: 28999
;; 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: 6 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Sat Aug 24 18:45:49 PDT 2024
;; MSG SIZE  rcvd: 98

cybersec-client@Benjamin:/etc/network$
```

2. The ‘interfaces’ file after the change of ‘dns-nameservers’.

```
CyberSecClient - VMware Workstation 17 Player (Non-commercial use only)
Player
cybersec-client@Benjamin: /etc/network
  GNU nano 2.2.6                                File: 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@Benjamin: /etc/network
  GNU nano 2.2.6                                File: ./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 10.0.2.7
```

3. Dig command after the change of ‘dns-nameservers’

```
cybersec-client@Benjamin:~$ 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: 31316
;; 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: 11 msec
;; SERVER: 10.0.2.7#53(10.0.2.7)
;; WHEN: Sat Aug 24 18:51:28 PDT 2024
;; MSG SIZE  rcvd: 98

cybersec-client@Benjamin:~$
```

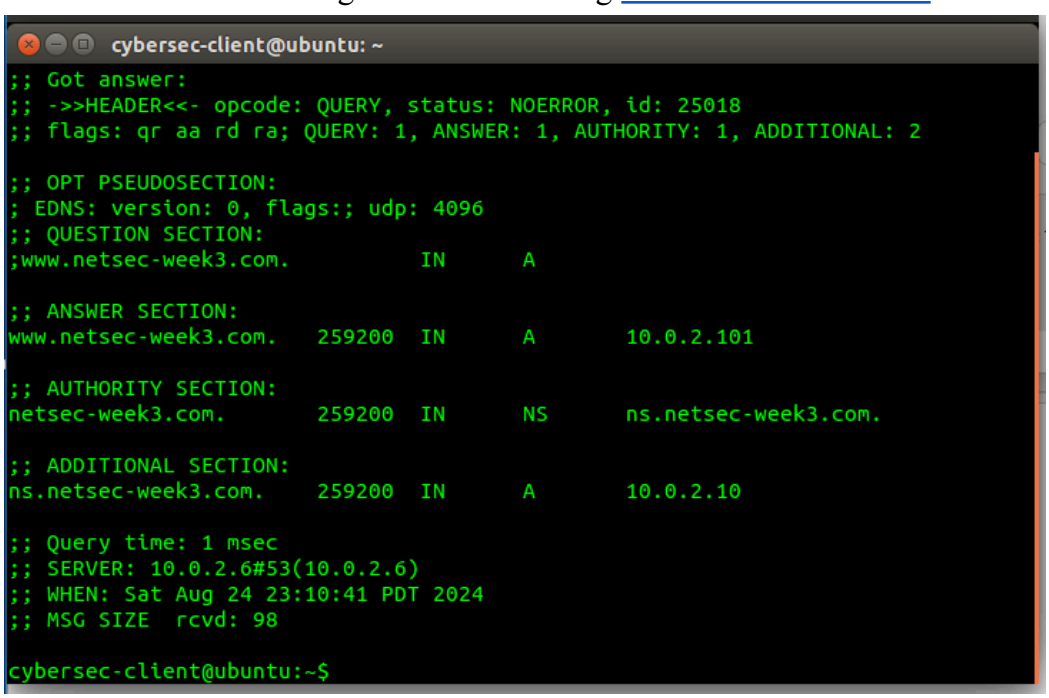
Task 2:

Steps:
1. Open Wireshark on Client VM by entering ‘sudo wireshark’ in the terminal window. Select ‘eth0’ as the
interface.
2. Run the dig command in the terminal of the Client VM.
3. Look for DNS Packets in the Wireshark Capture.
4. Open Netwag on Attacker VM by entering ‘sudo netwag’ in the terminal.
5. Search and open ‘105 Sniff and Send DNS answers’ .
6. Use the information gathered from Step 2 (Dig command) to create a fake response.
7. AŌer running the aΣack, repeat Step 2.
8. Look at DNS packets captured on Wireshark.
9. Check the info section of the Packet.
10. Stop the attack from Attacker VM.

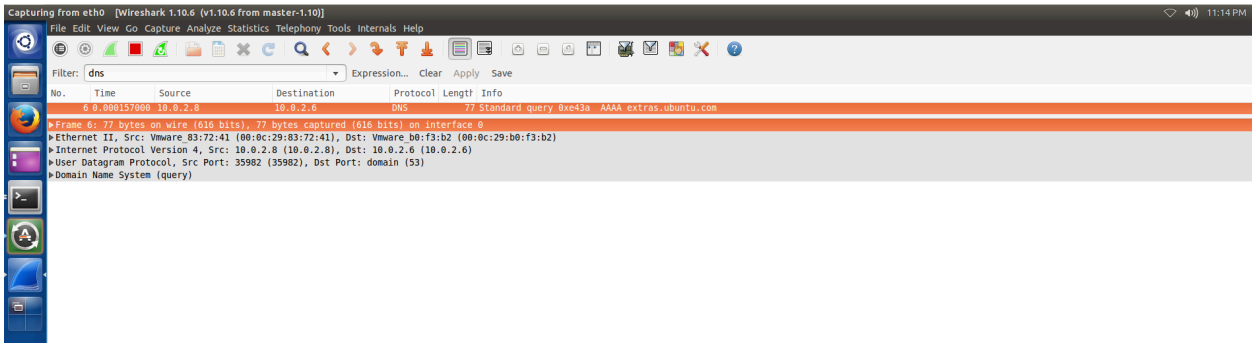
Screenshots Required: (6)

Step 2, Step 3, Step 6 (Netwag Configuraϴonϴonϴ), Step 7, Step 8 and Step 9

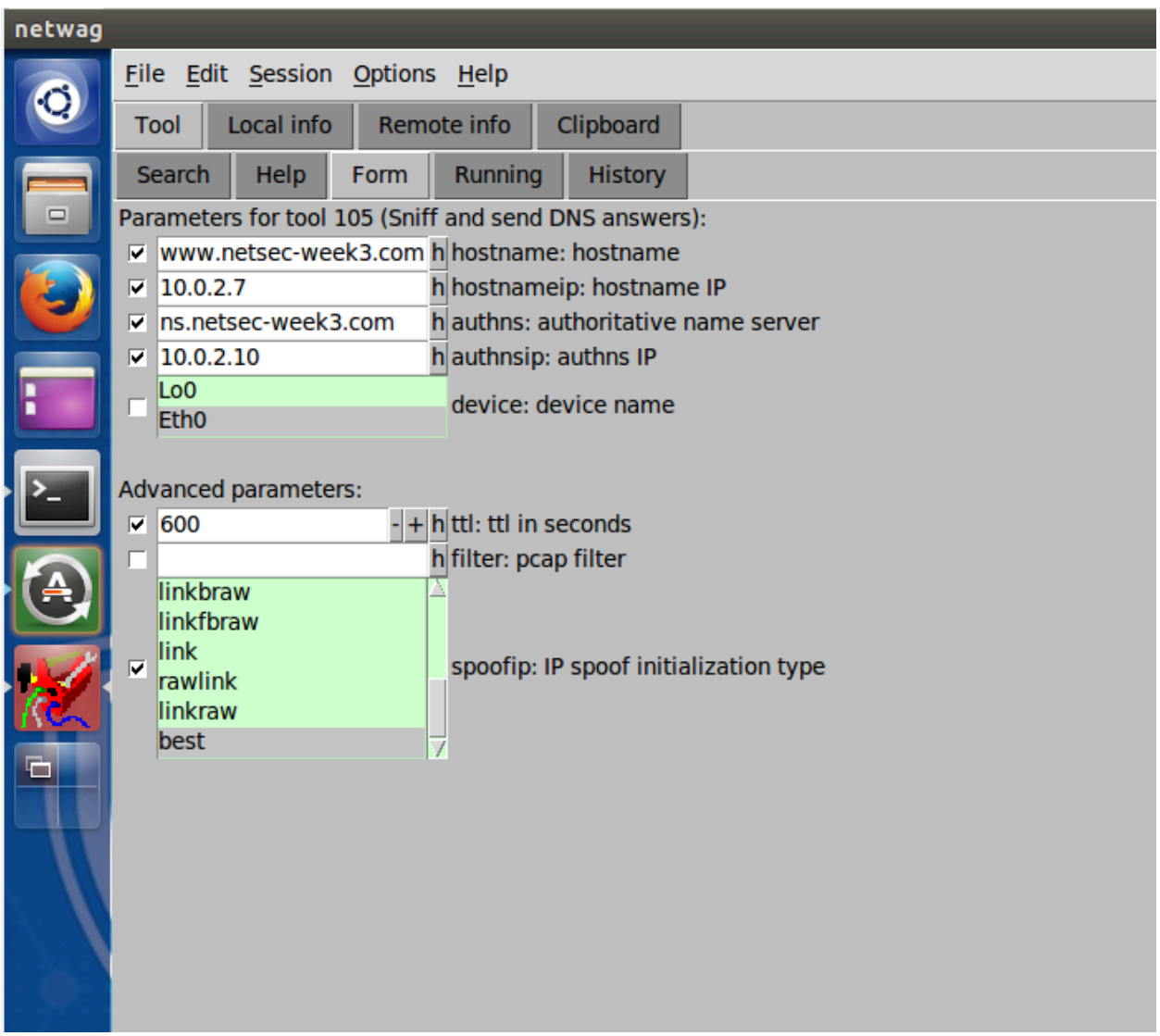
Initial result when running the command ‘Dig www.netsec-week.com’ in terminal



Initial Wireshark results before any sniff, Filtered to show only DNS results.



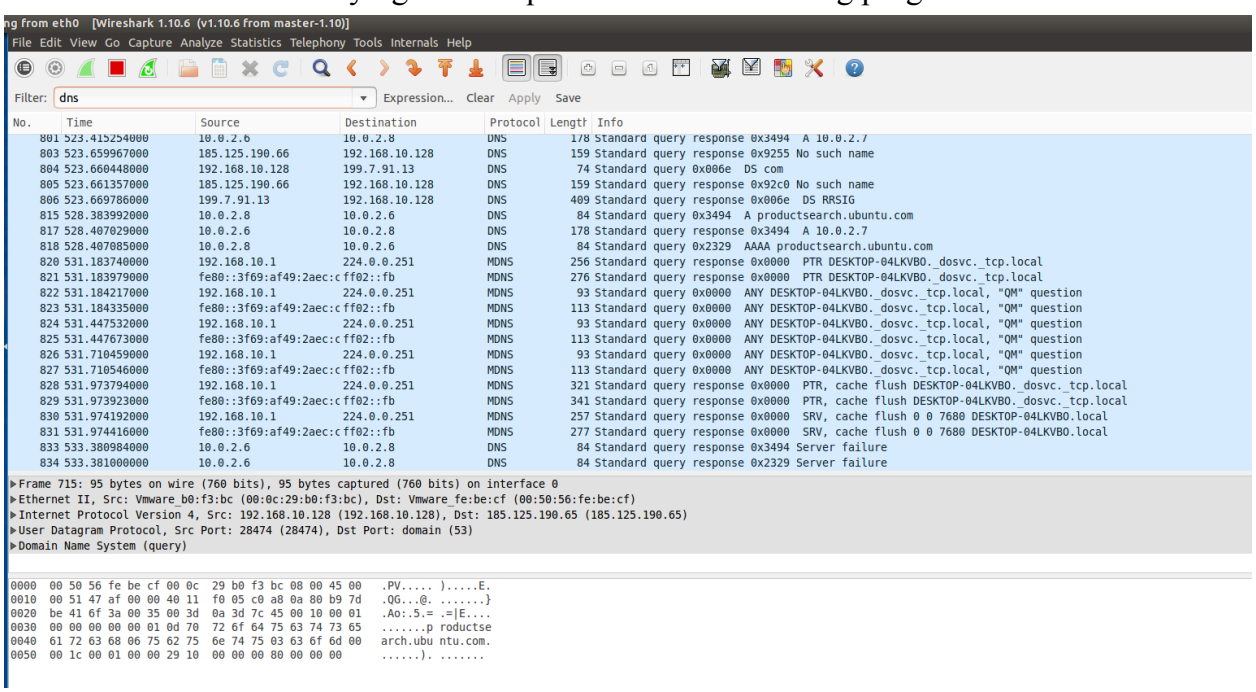
Setting used on the attacking VM- Utilizing tool 105



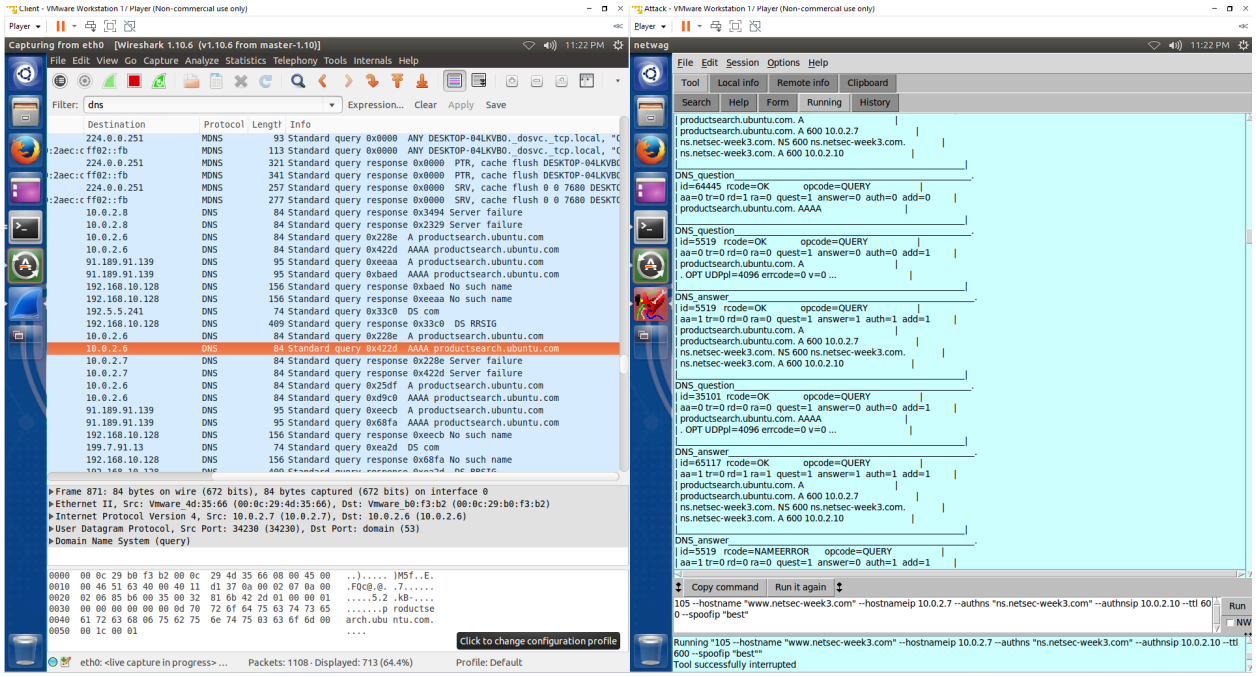
Results of the same ‘Dig’ Command after starting up the 105 attack.

```
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: 51645
;; 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: Sat Aug 24 23:19:30 PDT 2024
;; MSG SIZE  rcvd: 98

cybersec-client@ubuntu:~$
```

Wireshark results - Identifying DNS requests from the attacking program

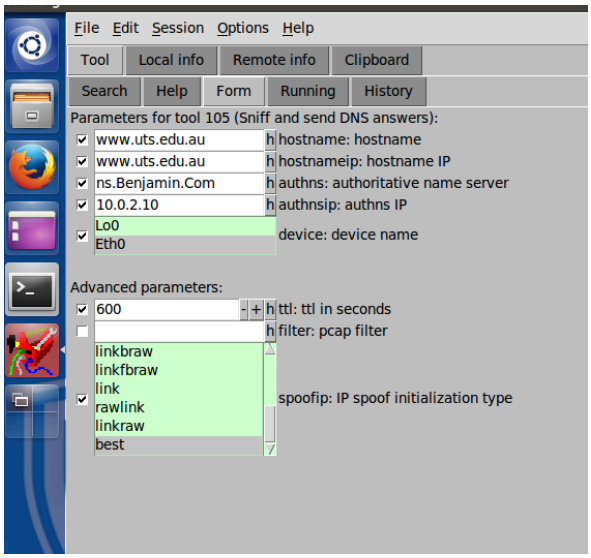


Comparing the results information from wireshark shows the same queries from the attacking machine.

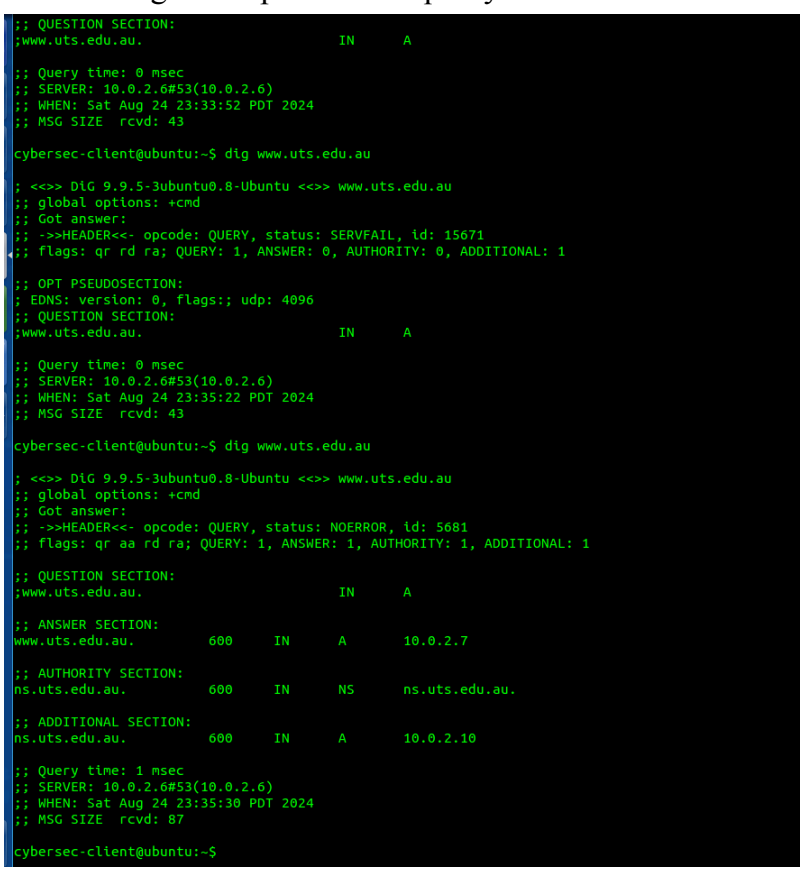


Task 3

Steps used in this task was similar to the one above. This time we targeted a domain url (www.uts.edu.au) to spoof a response allowing us to get information. In the first screenshot you can see the settings used to trigger the enquiries.



The screenshot belows shows both the failed attempt followed by the successful one due to the cacheing of the previous enquirey



```
;; QUESTION SECTION:
;www.uts.edu.au.                        IN      A

;; Query time: 0 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Sat Aug 24 23:33:52 PDT 2024
;; MSG SIZE  rcvd: 43

cybersec-client@ubuntu:~$ dig www.uts.edu.au

; <<>> DiG 9.9.5-3ubuntu0.8-Ubuntu <<>> www.uts.edu.au
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 15671
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.uts.edu.au.                        IN      A

;; Query time: 0 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Sat Aug 24 23:35:22 PDT 2024
;; MSG SIZE  rcvd: 43

cybersec-client@ubuntu:~$ dig www.uts.edu.au

; <<>> DiG 9.9.5-3ubuntu0.8-Ubuntu <<>> www.uts.edu.au
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5681
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; QUESTION SECTION:
;www.uts.edu.au.                        IN      A

;; ANSWER SECTION:
www.uts.edu.au.         600     IN      A       10.0.2.7

;; AUTHORITY SECTION:
ns.uts.edu.au.          600     IN      NS      ns.uts.edu.au.

;; ADDITIONAL SECTION:
ns.uts.edu.au.          600     IN      A       10.0.2.10

;; Query time: 1 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Sat Aug 24 23:35:30 PDT 2024
;; MSG SIZE  rcvd: 87

cybersec-client@ubuntu:~$
```