

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$ nano interfaces
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:

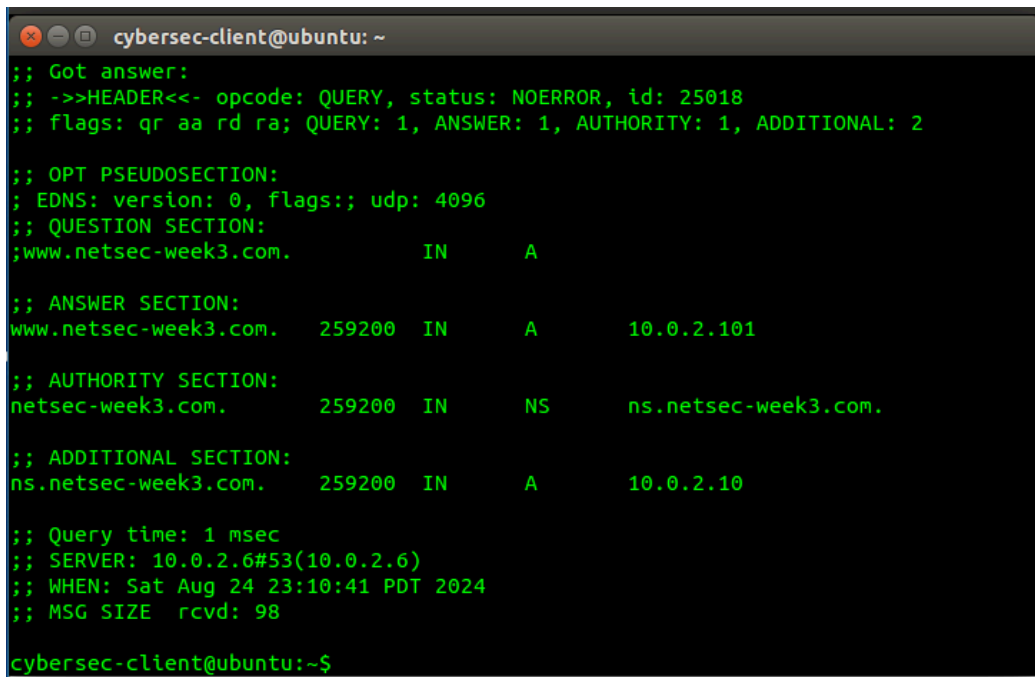
Steps:

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 Netmag on Attacker VM by entering 'sudo netmag' 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. After running the attack, 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)

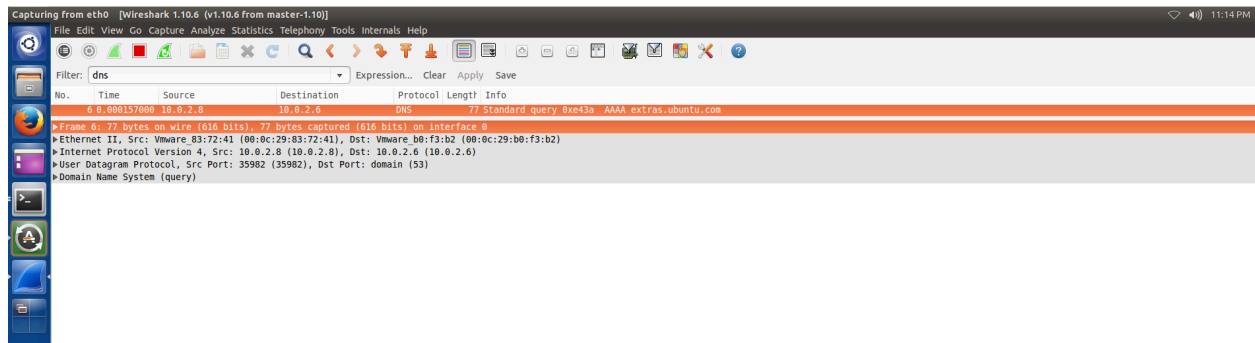
Step 2, Step 3, Step 6 (Netmag Configuration), Step 7, Step 8 and Step 9

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

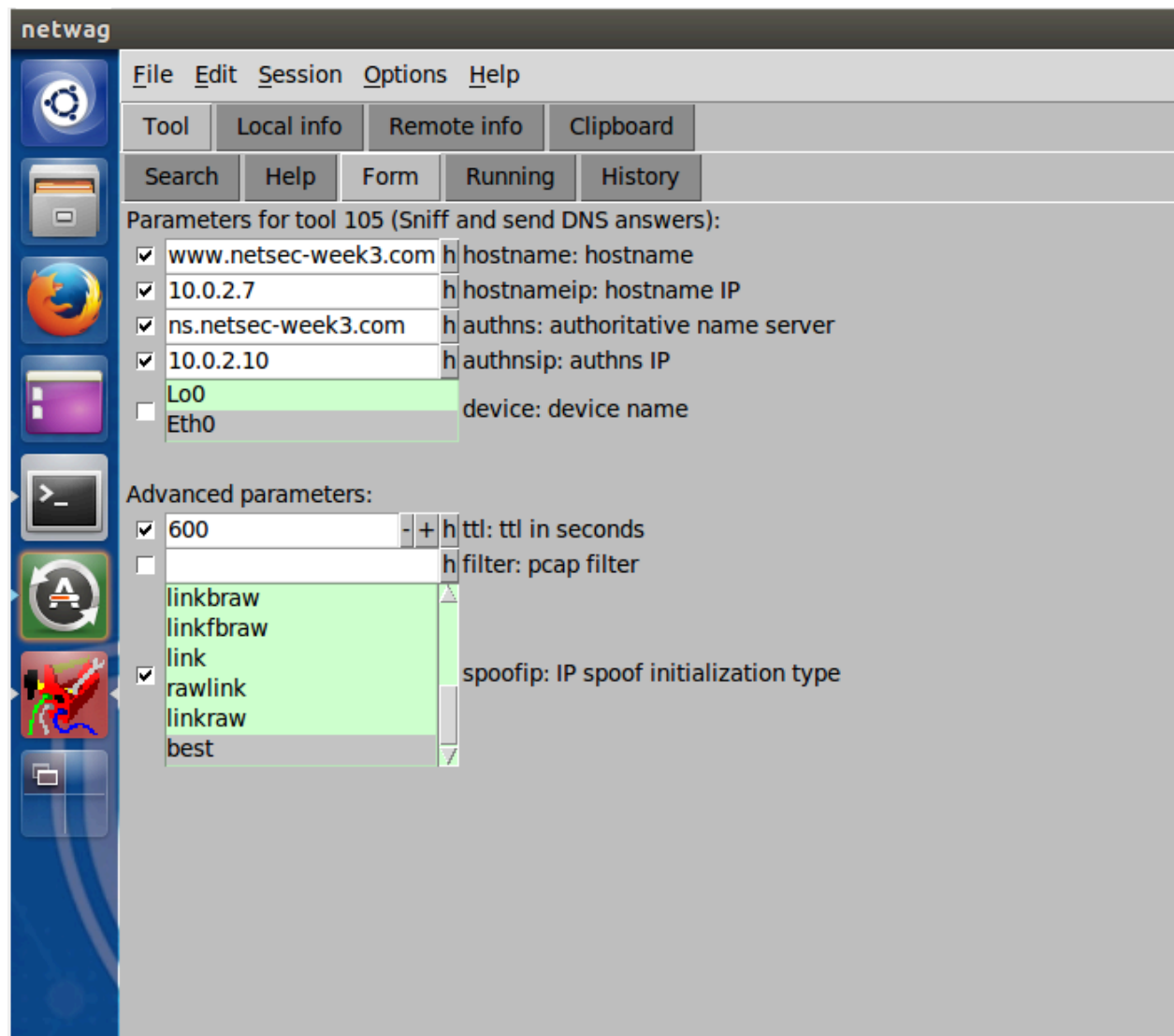


```
cybersec-client@ubuntu: ~  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25018  
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags:; udp: 4096  
;; QUESTION SECTION:  
;www.netsec-week3.com.      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 23:10:41 PDT 2024  
;; MSG SIZE rcvd: 98  
  
cybersec-client@ubuntu:~$
```

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

Wireshark 1.10.6 (v1.10.6 from master-1.10)

Filter: dns

No.	Time	Source	Destination	Protocol	Length	Info
801	523.415254000	10.0.2.6	10.0.2.8	DNS	178	Standard query response 0x3494 A 10.0.2.7
803	523.659967000	185.125.190.66	192.168.10.128	DNS	159	Standard query response 0x9255 No such name
804	523.660448000	192.168.10.128	199.7.91.13	DNS	74	Standard query 0x006e DS com
805	523.661357000	185.125.190.66	192.168.10.128	DNS	159	Standard query response 0x92c0 No such name
806	523.669786000	199.7.91.13	192.168.10.128	DNS	409	Standard query response 0x006e DS RRSIG
815	528.383929000	10.0.2.8	10.0.2.6	DNS	84	Standard query 0x3494 A productsearch.ubuntu.com
817	528.407029000	10.0.2.6	10.0.2.8	DNS	178	Standard query response 0x3494 A 10.0.2.7
818	528.407085000	10.0.2.8	10.0.2.6	DNS	84	Standard query 0x2329 AAAA productsearch.ubuntu.com
820	531.183740000	192.168.10.1	224.0.0.251	MDNS	256	Standard query response 0x0000 PTR DESKTOP-04LKVB0.dosvc_tcp.local
821	531.183979000	fe80::3f69:af49:2aec::ff02::fb	224.0.0.251	MDNS	276	Standard query response 0x0000 PTR DESKTOP-04LKVB0.dosvc_tcp.local
822	531.184217000	192.168.10.1	224.0.0.251	MDNS	93	Standard query 0x0000 ANY DESKTOP-04LKVB0.dosvc_tcp.local, "QM" question
823	531.184335000	fe80::3f69:af49:2aec::ff02::fb	224.0.0.251	MDNS	113	Standard query 0x0000 ANY DESKTOP-04LKVB0.dosvc_tcp.local, "QM" question
824	531.447532000	192.168.10.1	224.0.0.251	MDNS	93	Standard query 0x0000 ANY DESKTOP-04LKVB0.dosvc_tcp.local, "QM" question
825	531.447673000	fe80::3f69:af49:2aec::ff02::fb	224.0.0.251	MDNS	113	Standard query 0x0000 ANY DESKTOP-04LKVB0.dosvc_tcp.local, "QM" question
826	531.710459000	192.168.10.1	224.0.0.251	MDNS	93	Standard query 0x0000 ANY DESKTOP-04LKVB0.dosvc_tcp.local, "QM" question
827	531.710546000	fe80::3f69:af49:2aec::ff02::fb	224.0.0.251	MDNS	113	Standard query 0x0000 ANY DESKTOP-04LKVB0.dosvc_tcp.local, "QM" question
828	531.973794000	192.168.10.1	224.0.0.251	MDNS	321	Standard query response 0x0000 PTR, cache flush DESKTOP-04LKVB0.dosvc_tcp.local
829	531.973923000	fe80::3f69:af49:2aec::ff02::fb	224.0.0.251	MDNS	341	Standard query response 0x0000 PTR, cache flush DESKTOP-04LKVB0.dosvc_tcp.local
830	531.974192000	192.168.10.1	224.0.0.251	MDNS	257	Standard query response 0x0000 SRV, cache flush 0 0 7680 DESKTOP-04LKVB0.local
831	531.974416000	fe80::3f69:af49:2aec::ff02::fb	224.0.0.251	MDNS	277	Standard query response 0x0000 SRV, cache flush 0 0 7680 DESKTOP-04LKVB0.local
833	533.380984000	10.0.2.6	10.0.2.8	DNS	84	Standard query response 0x3494 Server failure
834	533.381000000	10.0.2.6	10.0.2.8	DNS	84	Standard query response 0x2329 Server failure

Frame 715: 95 bytes on wire (760 bits), 95 bytes captured (760 bits) on interface 0

Ethernet II, Src: Vmware_b0:f3:bc (00:0c:29:b0:f3:bc), Dst: Vmware_fe:be:cf (00:50:56:fe:be:cf)

Internet Protocol Version 4, Src: 192.168.10.128 (192.168.10.128), Dst: 185.125.190.65 (185.125.190.65)

User Datagram Protocol, Src Port: 28474 (28474), Dst Port: domain (53)

Domain Name System (query)

0000 00 50 56 fe be cf 00 0c 29 b0 f3 bc 00 00 45 00 .PV....E.
0010 00 51 47 af 00 00 40 11 f0 05 c0 a8 0a 80 b9 7d .Q0...@.....
0020 be 41 6f 3a 00 35 00 3d 0a 3d 7c 45 00 10 00 01 .Ao:5.=.|E....
0030 00 00 00 00 01 0d 70 72 6f 64 75 63 74 73 65p rductse
0040 61 72 63 68 06 75 62 75 6e 74 75 03 63 6f 64 00 arch.ubu ntun.com.
0050 00 1c 00 01 00 00 29 10 00 00 00 00 00 00 00).

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

The image displays two side-by-side screenshots of the Wireshark network traffic analysis tool, showing DNS traffic captured on an interface.

Left Screenshot (Wireshark 1.10.6):

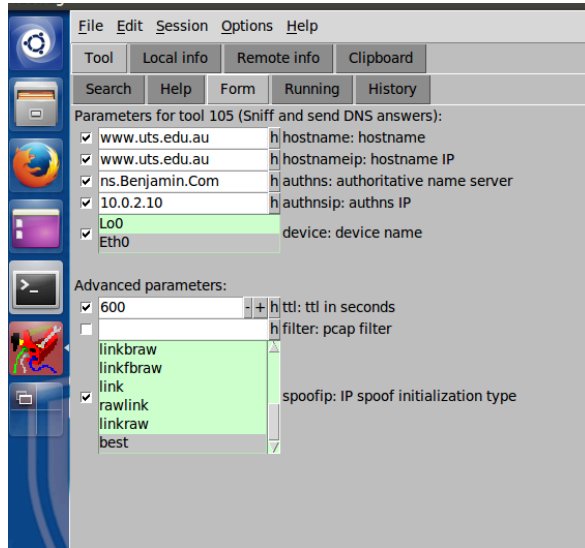
- Filter:** dns
- Packet List:** Shows a list of captured packets. The selected packet is 100, which is a DNS query from 10.0.2.7 to 10.0.2.6.
- Packet Details:** Shows the structure of the selected packet:
 - Frame 871: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface 0
 - Ethernet II, Src: Vmware 44:35:66 (00:0c:29:4d:35:66), Dst: Vmware b0:f3:b2 (00:0c:29:b0:f3:b2)
 - Internet Protocol Version 4, Src: 10.0.2.7 (10.0.2.7), Dst: 10.0.2.6 (10.0.2.6)
 - User Datagram Protocol, Src Port: 34230 (34230), Dst Port: domain (53)
 - Domain Name System (query)
- Packet Bytes:** Shows the raw data of the packet in hexadecimal and ASCII format.

Right Screenshot (Wireshark 1.10.6):

- Filter:** dns
- Packet List:** Shows a list of captured packets. The selected packet is 100, which is a DNS query from 10.0.2.7 to 10.0.2.6.
- Packet Details:** Shows the structure of the selected packet:
 - Frame 871: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface 0
 - Ethernet II, Src: Vmware 44:35:66 (00:0c:29:4d:35:66), Dst: Vmware b0:f3:b2 (00:0c:29:b0:f3:b2)
 - Internet Protocol Version 4, Src: 10.0.2.7 (10.0.2.7), Dst: 10.0.2.6 (10.0.2.6)
 - User Datagram Protocol, Src Port: 34230 (34230), Dst Port: domain (53)
 - Domain Name System (query)
- Packet Bytes:** Shows the raw data of the packet in hexadecimal and ASCII format.

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 enquiry

```
;; 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:~$
```