Lab Report

1. Your name

   劉品枘

2. Lab Log:

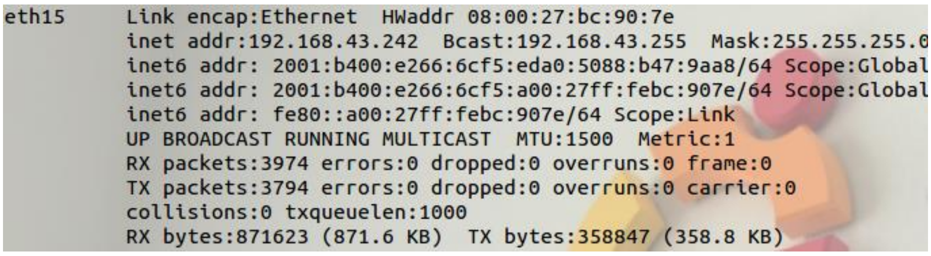
   - How long did you work on this lab? 1:30
   - Any problems?　How did you resolve the problem? No

3. VM Host information

	Physical Interface	MAC Address	IP Address
VM host1 (client)		08:00:27:bc:90:7e	192.168.43.242
VM host2 (hacker)		08:00:27:1c:70:0c	192.168.43.59
VM host3 (server)		08:00:27:f7:f3:0c	192.168.43.55

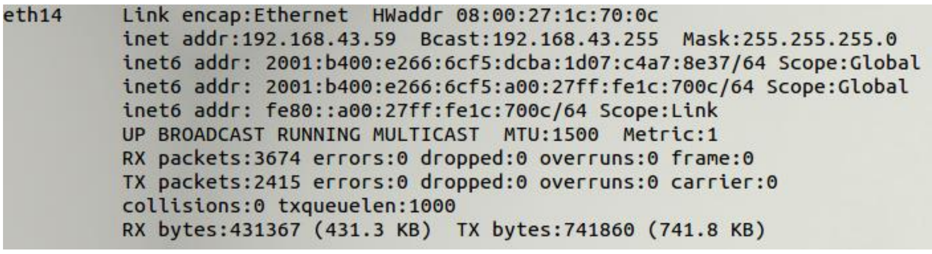
Physical Interface:

VM1:



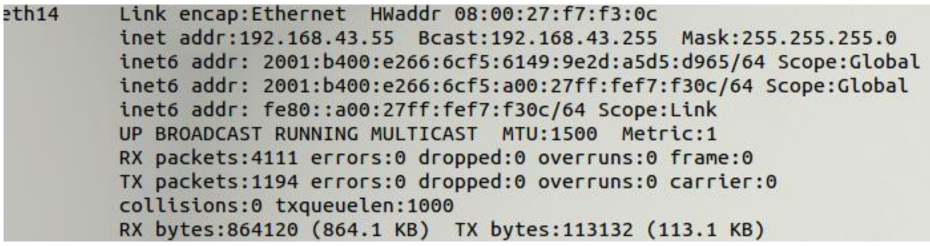
```
eth15     Link encap:Ethernet  HWaddr 08:00:27:bc:90:7e
          inet addr:192.168.43.242  Bcast:192.168.43.255  Mask:255.255.255.0
          inet6 addr: 2001:b400:e266:6cf5:eda0:5088:b47:9aa8/64 Scope:Global
          inet6 addr: 2001:b400:e266:6cf5:a00:27ff:febc:907e/64 Scope:Global
          inet6 addr: fe80::a00:27ff:febc:907e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3974 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3794 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:871623 (871.6 KB)  TX bytes:358847 (358.8 KB)
```

VM2:



```
eth14     Link encap:Ethernet  HWaddr 08:00:27:1c:70:0c
          inet addr:192.168.43.59  Bcast:192.168.43.255  Mask:255.255.255.0
          inet6 addr: 2001:b400:e266:6cf5:dcba:1d07:c4a7:8e37/64 Scope:Global
          inet6 addr: 2001:b400:e266:6cf5:a00:27ff:fe1c:700c/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fe1c:700c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3674 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2415 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:431367 (431.3 KB)  TX bytes:741860 (741.8 KB)
```

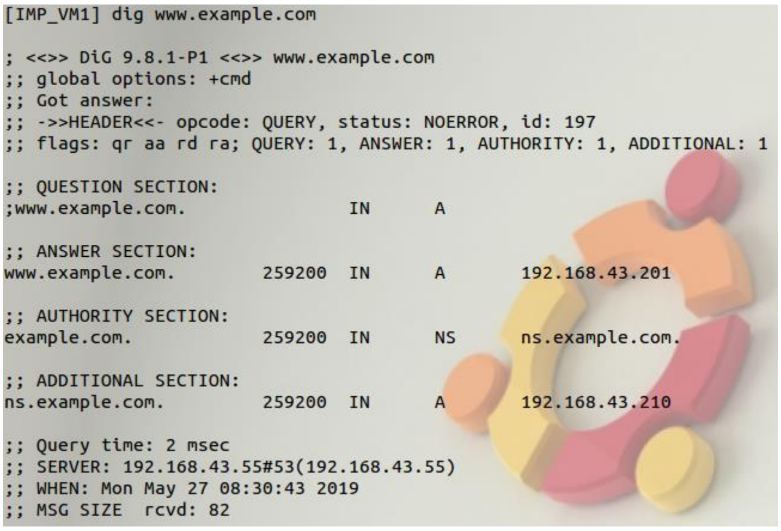
VM3:



```
eth14     Link encap:Ethernet  HWaddr 08:00:27:f7:f3:0c
          inet addr:192.168.43.55  Bcast:192.168.43.255  Mask:255.255.255.0
          inet6 addr: 2001:b400:e266:6cf5:6149:9e2d:a5d5:d965/64 Scope:Global
          inet6 addr: 2001:b400:e266:6cf5:a00:27ff:fef7:f30c/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fef7:f30c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4111 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1194 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:864120 (864.1 KB)  TX bytes:113132 (113.1 KB)
```

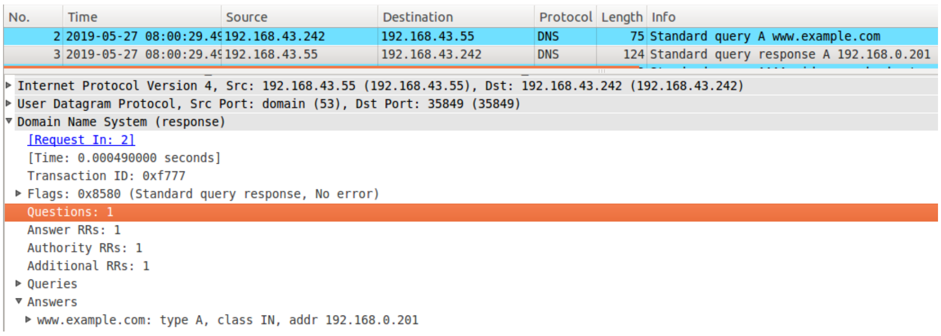
4. Proof of your lab work

   a. Screenshot-1: DNS query of www.example.com (before hacking)



```
[IMP_VM1] dig www.example.com

; <<>> DiG 9.8.1-P1 <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 197
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        259200  IN      A       192.168.43.201

;; AUTHORITY SECTION:
example.com.            259200  IN      NS      ns.example.com.

;; ADDITIONAL SECTION:
ns.example.com.         259200  IN      A       192.168.43.210

;; Query time: 2 msec
;; SERVER: 192.168.43.55#53(192.168.43.55)
;; WHEN: Mon May 27 08:30:43 2019
;; MSG SIZE  rcvd: 82
```

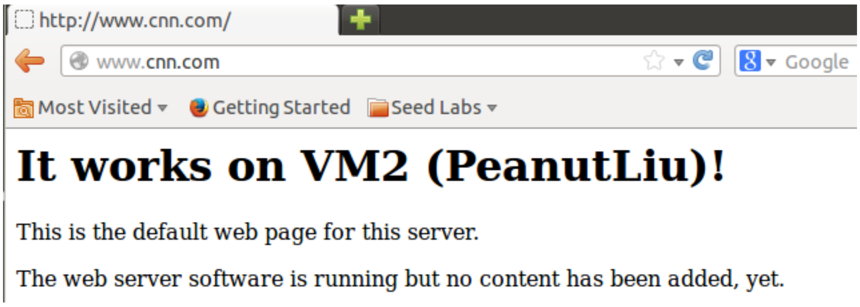
b. Screenshot-2: wireshark of DNS query for www.example.com (before hacking)



No.	Time	Source	Destination	Protocol	Length	Info
2	2019-05-27 08:00:29.49	192.168.43.242	192.168.43.55	DNS	75	Standard query A www.example.com
3	2019-05-27 08:00:29.49	192.168.43.55	192.168.43.242	DNS	124	Standard query response A 192.168.0.201

```
▶ Internet Protocol Version 4, Src: 192.168.43.55 (192.168.43.55), Dst: 192.168.43.242 (192.168.43.242)
▶ User Datagram Protocol, Src Port: domain (53), Dst Port: 35849 (35849)
▼ Domain Name System (response)
    [Request In: 2]
    [Time: 0.000490000 seconds]
    Transaction ID: 0xf777
  ▶ Flags: 0x8580 (Standard query response, No error)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 1
    Additional RRs: 1
  ▶ Queries
  ▼ Answers
    ▶ www.example.com: type A, class IN, addr 192.168.0.201
```

c. Screenshot-3: www.cnn.com of local DNS attack (pharmed IP addresses in /etc/hosts)

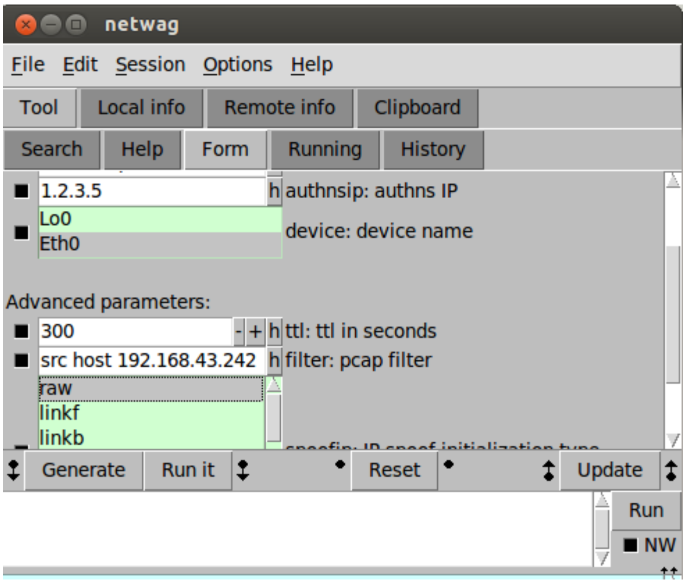


It works on VM2 (PeanutLiu)!

This is the default web page for this server.

The web server software is running but no content has been added, yet.

d. Screenshot-4: netwag configuration for DNS Spoofing (client side)


netwag
File Edit Session Options Help
Tool Local info Remote info Clipboard
Search Help Form Running History
Generate Run it Reset Update
Run
NW

■ 1.2.3.5 authnsip: authns IP

■ Lo0
Eth0 device: device name

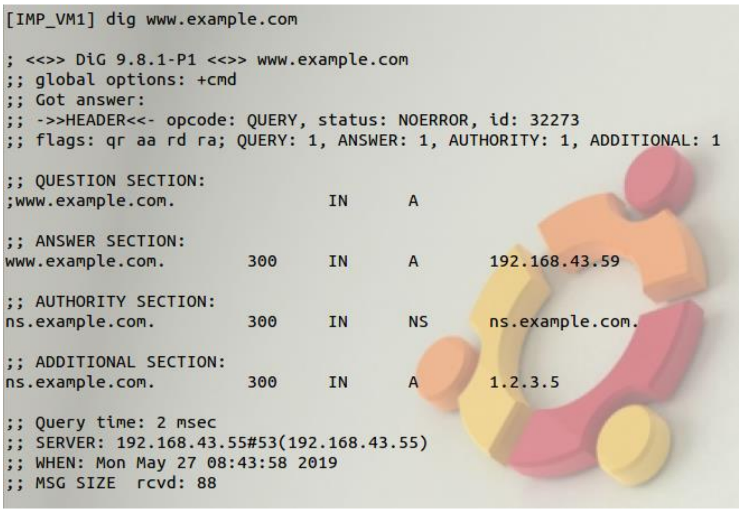
Advanced parameters:

■ 300 ttl: ttl in seconds

■ src host 192.168.43.242 filter: pcap filter

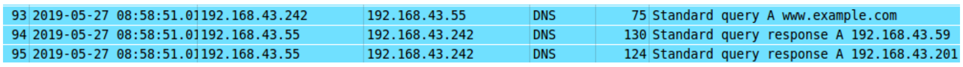
raw
linkf
linkb spoofip: IP spoof initialization type

e. Screenshot-5: Proof of DNS hacking (www.exammple.com, client side)



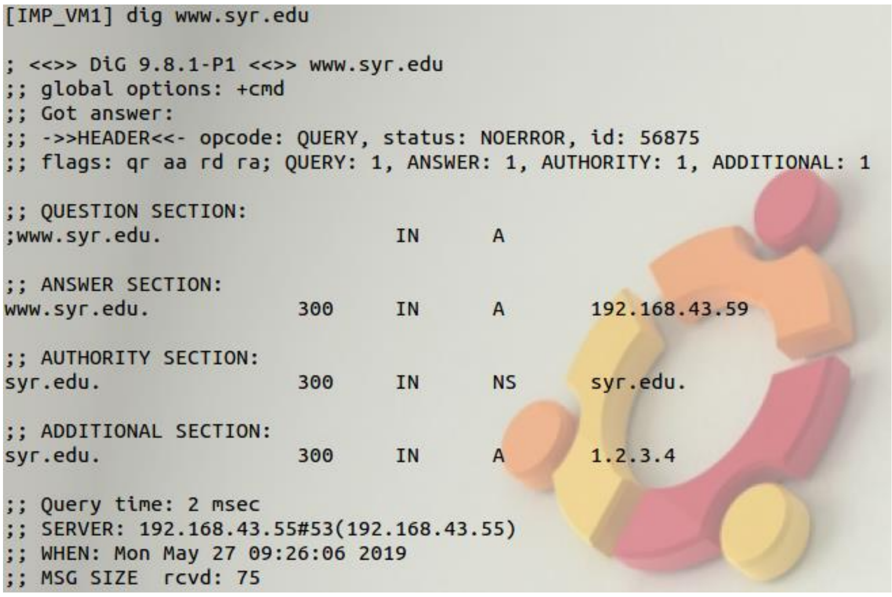
```
[IMP_VM1] dig www.example.com

; <<>> DiG 9.8.1-P1 <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32273
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        300     IN      A       192.168.43.59

;; AUTHORITY SECTION:
ns.example.com.         300     IN      NS      ns.example.com.

;; ADDITIONAL SECTION:
ns.example.com.         300     IN      A       1.2.3.5

;; Query time: 2 msec
;; SERVER: 192.168.43.55#53(192.168.43.55)
;; WHEN: Mon May 27 08:43:58 2019
;; MSG SIZE  rcvd: 88
```

f. Screenshot-6: Wireshark of Hacked DNS Response (client side)



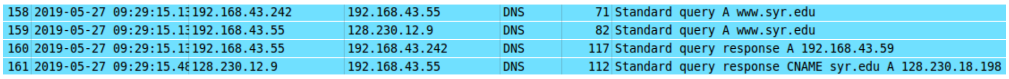
93	2019-05-27 08:58:51.01	192.168.43.242	192.168.43.55	DNS	75	Standard query A www.example.com
94	2019-05-27 08:58:51.01	192.168.43.55	192.168.43.242	DNS	130	Standard query response A 192.168.43.59
95	2019-05-27 08:58:51.01	192.168.43.55	192.168.43.242	DNS	124	Standard query response A 192.168.43.201

g. Screenshot-7: Proof of DNS hacking (www.syr.edu, server side)



```
[IMP_VM1] dig www.syr.edu

; <<>> DiG 9.8.1-P1 <<>> www.syr.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56875
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; QUESTION SECTION:
;www.syr.edu.                   IN      A

;; ANSWER SECTION:
www.syr.edu.            300     IN      A       192.168.43.59

;; AUTHORITY SECTION:
syr.edu.                300     IN      NS      syr.edu.

;; ADDITIONAL SECTION:
syr.edu.                300     IN      A       1.2.3.4

;; Query time: 2 msec
;; SERVER: 192.168.43.55#53(192.168.43.55)
;; WHEN: Mon May 27 09:26:06 2019
;; MSG SIZE  rcvd: 75
```

h. Screenshot-8: Wireshark of Hacked DNS Response (server side)



```
158 2019-05-27 09:29:15.1 192.168.43.242   192.168.43.55    DNS    71 Standard query A www.syr.edu
159 2019-05-27 09:29:15.1 192.168.43.55    128.230.12.9     DNS    82 Standard query A www.syr.edu
160 2019-05-27 09:29:15.1 192.168.43.55    192.168.43.242   DNS   117 Standard query response A 192.168.43.59
161 2019-05-27 09:29:15.4 128.230.12.9     192.168.43.55    DNS   112 Standard query response CNAME syr.edu A 128.230.18.198
```

5. Question:

   Comparing Task-3 and Task-4, which DNS attack is more effective?   Why?

   Effectiveness is defined as the percentage of successful attacks.

6. Lab reflection

   Describe if the lab learning goals are met and also any interesting observation from this lab exercise.

   It’s interesting to finish DNS cache poisoning. But use tool to complete the task can’t let me fully understand.