Local DNS Attack Project

A. Introduction:

DNS (domain name system) is a naming system for devices which connected to the internet. DNS has a hierarchical structure. For clarifying definition of DNS fallowing scenario can be considered [1].

Computer “A” request to visit http://www.webpage.com. This request goes to nearest DNS server, if it is not available, then it asks another DNS server to find IP address of the given link. If last server has IP address. Requested web pages ip address reversely fallow the path and goes to computer which request web pages ip address. DNS basically can be defined as text to IP and IP to text translator [1].

DNS has actually has gaps which should be considered network security gap. Such as DNS spoofing (DNS cache poisoning attack). DNS spoofing is important point for the recent network security issues [1, 2].

Project aims are understanding of DNS attacks and implementing DNS attacks in virtual machines. For this statement, first initial configuration established after several steps DNS attacks will be implemented on live action.

B. Configuration:

Before Start [3]:

You need to install virtual-box before starting. After installing virtual-box you need to download seedUbuntu which is necessary experimental OS for this project. You can download seedUbuntu from fallowing link “http://www.cis.syr.edu/~wedu/seed/lab_env.html". After downloading seedUbuntu. Extract it to fallowing named directory “ServerUbuntu”. Then copy ServerUbuntu folder twice and rename than with “AttackerUbuntu” and “UserUbuntu” [3].

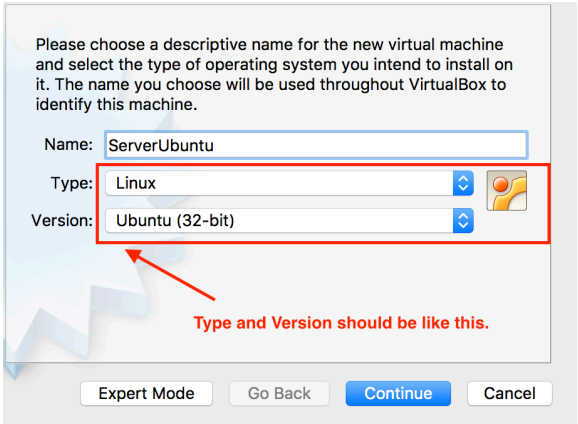
In this project you are using 3 different operating system at the same time. Reason of that, you need to change path during to creating each virtual operating systems.

Before the creating new operating system you should call following command from command-line or terminal.

```
VBoxManage internalcommands sethduuid yourVMDKpath
```

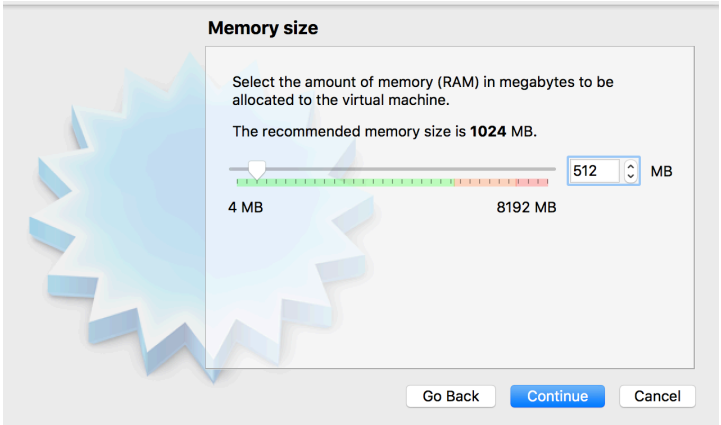
path example: yourVMDKpath = “/Volumes/CAN/server/SEEDUbuntu12.04.vmdk”

Open virtual-box. Then create new VM from virtual box manager.

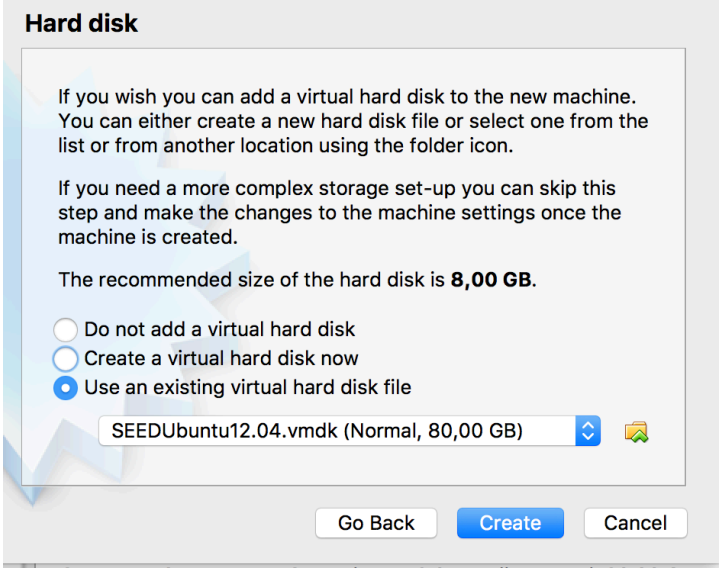


After clicking new fallow below figure. Your OS type and version should be selected according to figure.

Name the operating system ServerUbuntu, UserUbuntu, AttackerUbuntu. We are first continue with ServerUbuntu.



Then pressing continue previous step. You define memory to your operating system. Minimum you should select 512 MB for your virtual device. then continue.



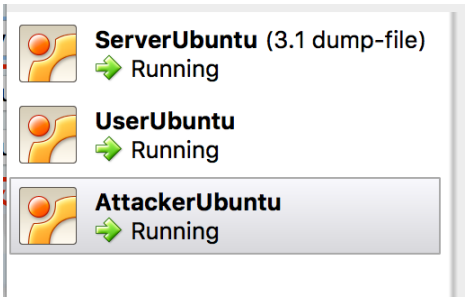
Continue with selecting “Use an existing virtual hard disk file”

Then select .VMDK extension file from your extracted directory.

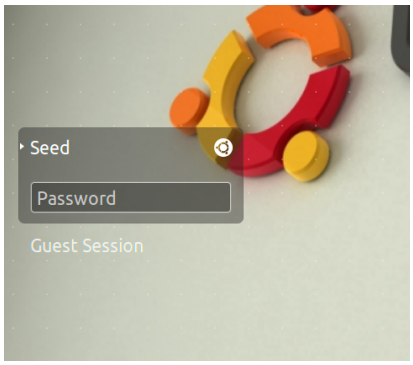
Then create your virtual OS and virtual machine.

Repeat this steps for attacker machine and user machine.

Do not forget to call command line command given above.

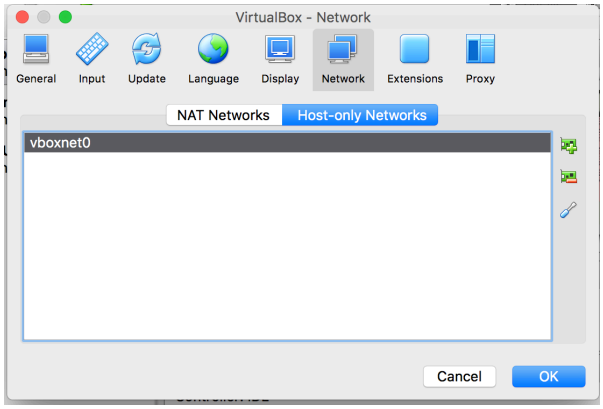


After creating all virtual machines. Run all of them from virtual-box. After running all virtual machines you should see all virtual machines like below..

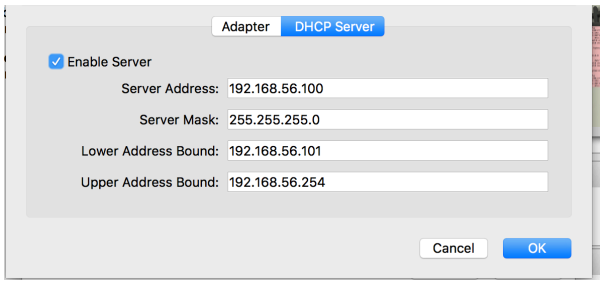


Enter password to all virtual operating systems which is “dees”.

User is Seed
Password is dees
Use sudo for the root access.

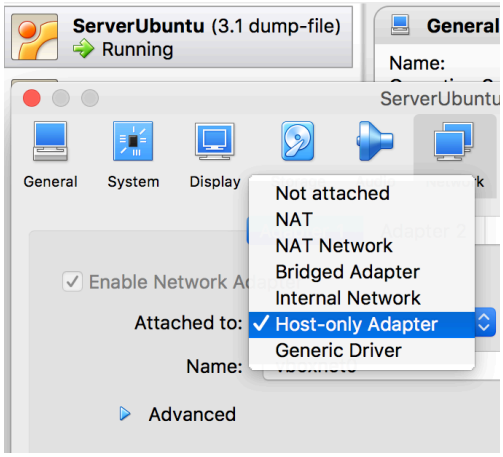


Before to go environment setup for project. Some changes should be applied to Virtual Box. Then go settings of the virtual box. Then select Network -> Host-only-networks.



Then double click vboxnet0. Then select DHCP server. Make sure fields filled with like figure.

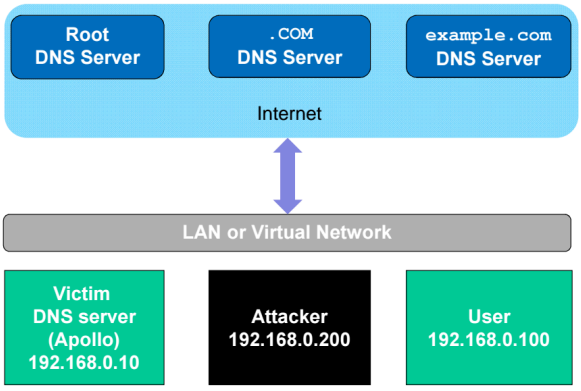
Then select host-only-network from network settings for each virtual machine.



Select Host-only adapter from all virtual-machines.

In advanced settings. Allow All should be selected from promiscuous mode.

Project Setup:



Given figure represents the project setup and how created machines will communicate each other. In that case we create virtual network. First lets continue with DNS server configuration for our test environment.

Figure [4]: Project Setup

DNS Server

For server side start server machine. And make sure above configurations were done. Open terminal with ctrl + alt + t/T.

Go to this directory —> "/etc/bind/". You can use below command to go given directory.

```
cd /etc/bind/
```

Then select open given file with below command. File name is "named.conf.options"

```
sudo nano named.conf.options
```

You need to get root privileges so you need to add sudo at the beginning of the nano terminal editor to edit "named.conf.options" file.

Enter dees as a root password after entering above command. Then add fallowing lines to the "named.conf.options" file.

```
options {

dump-file "/var/cache/bind/dump.db";

};
```

After adding above code snippet in "named.conf.options" file. Press ctrl + x/X to save content. Then continue with opening "named.conf" file with below command from terminal.

```
sudo nano named.conf
```

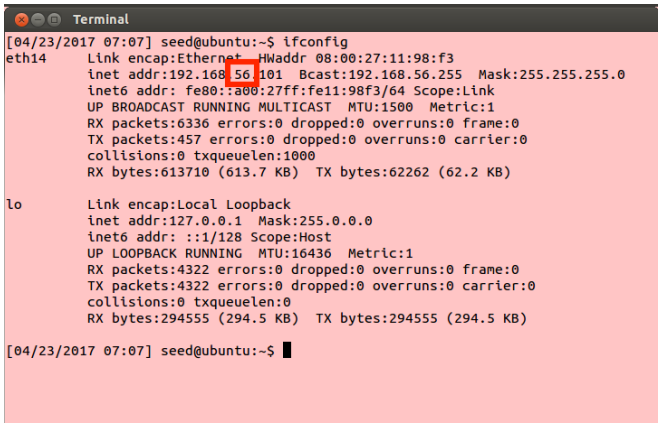
Then add fallowing code snippet.

```
zone "example.com" {
type master;
file "/var/cache/bind/example.com.db";
};
```

```
zone "X.168.192.in-addr.arpa" {
type master;
file "/var/cache/bind/192.168.X";
};
```

X should be related to your servers IP adress. Press ctrl + alt + t open new terminal and type ifconfig.

Your result should be like below.



Set to given X = 56. It can be different on your virtual machine. Again save it with ctrl + x/X and quit from nano.

Then go to next directory with below command.

```
cd /var/cache/bind/
```

Then create new file with “touch” command. Again in this directory we need root access to read and write. Reason of that use “sudo touch” instead of just “touch”. Enter below command to create new file which named “example.com.db”

```
sudo touch example.com.db
```

Open created file with below command from terminal.

```
sudo nano example.com.db
```

Then add fallowing lines into example.com.db

```
$TTL 3D

@ IN SOA ns.example.com. admin.example.com. (

2008111001 ;serial, today’s date + today’s serial number

8H ;refresh, seconds

2H ;retry, seconds

4W ;expire, seconds

1D) ;minimum, seconds
```

```
@ IN NS ns.example.com. ;Address of name server

@ IN MX 10 mail.example.com. ;Primary Mail Exchanger

www IN A 192.168.0.101 ;Address of www.example.com

mail IN A 192.168.0.102 ;Address of mail.example.com

ns IN A 192.168.0.10 ;Address of ns.example.com

*.example.com. IN A 192.168.0.100 ;Address for other URL in

;example.com. domain
```

You should do some changes above code snippet. Changes given above.

```
// ————————————————————————————————————————————————————————————

@ IN MX 10 mail.example.com. ;Primary Mail Exchanger

www IN A 192.168.56.151 ;Address of www.example.com —> example.com web address

mail IN A 192.168.56.152 ;Address of mail.example.com —> example.com mail address

ns IN A 192.168.56.101 ;Address of ns.example.com —> Server IP address

*.example.com. IN A 192.168.56.103 ;Address for other URL in —> User IP address

// ————————————————————————————————————————————————————————————
```

Example IP addresses are can be random values. You can add any IP address you want. Then save again with ctrl + x and quit.

We need last part to add to server side setup. Again go given below directory with “cd”.

```
cd /var/cache/bind/
```

Then add fallowing file with “sudo touch command”. Create “192.168.X” file. X related to your IP address (virtual DNS server). You can check your IP again with ifconfig. In that case x = 56.

```
sudo touch 192.168.X
```

Again with sudo nano 192.168.x open the text editor of the terminal and add below code snippet.

```
$TTL 3D

@ IN SOA ns.example.com. admin.example.com. (

2008111001

8H
```

```
2H

4W

1D)

@ IN NS ns.example.com.

101 IN PTR www.example.com.

102 IN PTR mail.example.com.

10 IN PTR ns.example.com.
```

In this code snippet some changes also required explanations given below.

```
2008111001
8H
2H
4W
1D)
@ IN NS ns.example.com.
151 IN PTR www.example.com.
152 IN PTR mail.example.com.
101 IN PTR ns.example.com.
```

www.example.com should match with previous file's IP address end. "151" In that case. mail.example.com also should match. In that case "152". For DNS, ns.example.com it should match with end of the DNS server IP address in that case it is 101. Again you can always check server IP address with ifconfig.

Before finalising server setup type fallowing command to terminal.

```
sudo /etc/init.d/bind9 restart
```

User

You should start user virtual machine.

Then we need to add our DNS server to user's machine for that purpose go to fallowing directory with fallowing command.

```
cd /etc/
```

Then type fallowing command to edit "resolv.conf" file.

```
sudo nano resolv.conf
```

Again we need to add sudo. You need to type password "seed" again.

Add fallowing code snippet into resolv.conf.

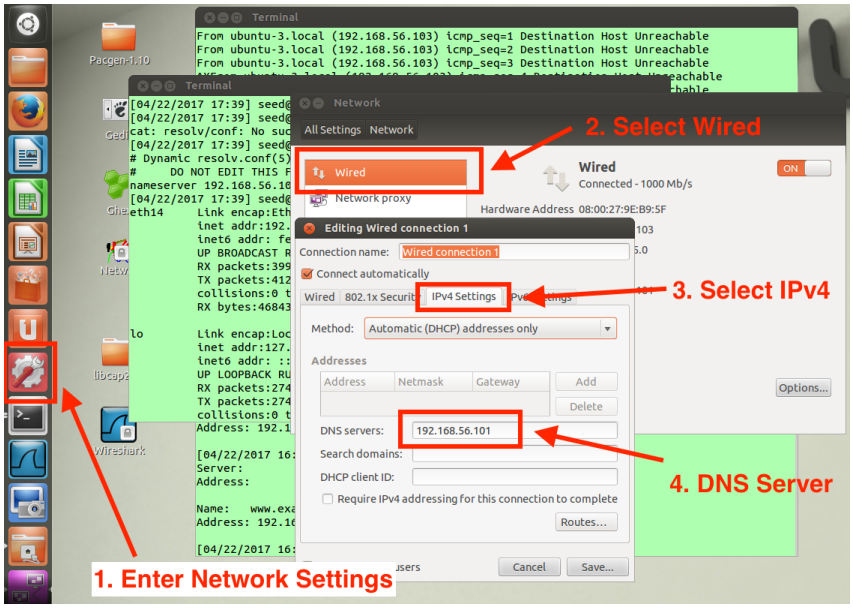
```
nameserver 192.168.Y.X # the ip of the DNS server you just setup
```

Y should be 56. I mentioned that why it is 56. X should be match the DNS servers IP address.

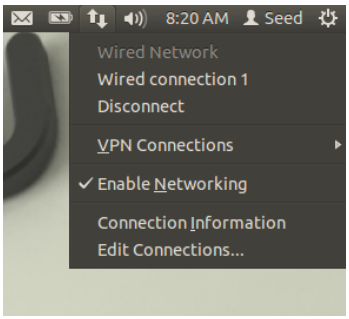
Go to DNS server machine and type ifconfig. And find IP address of the DNS server.

Quit from nano with ctrl + x and save with typing yes then press enter.

Go to settings and fallow below figure.



Enter settings from ubuntu side bar From figure step 1. And select Network from ubuntu settings. Then click wired. Then select IPv4 connection settings. Then select Automatic (DHCP) addresses only. We use this since it can be automatically added by ubuntu. We want to use our DNS server. So type our DNS server IP. You can use ifconfig from server machine terminal.



Than save it. And select wired connection 1 from ubuntu network bar. After selecting wired connection 1. Your user machines network refreshed according to your settings.

In terminal please type fallowing command to see your DNS server is working or not.

```
dig www.example.com
```

if you see DNS server ip address from result of the command you entered.

Project configuration is works properly.

Project configuration is over.

Some useful terminal commands.

cd —> change directory
cd .. —> previous directory
cd xx —> go xx directory

sudo —> root access —> password is “dees”
sudo nano xxx —> open text editor in terminal open xxxx file

sudo touch xxx —> create new file which named xxxx

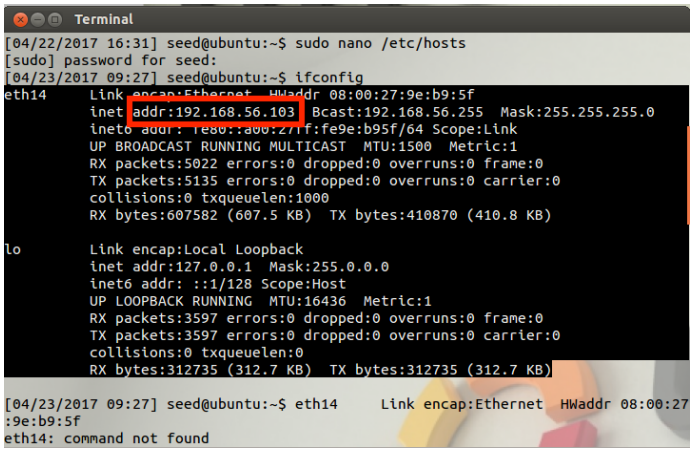
Project Task 1: Attackers have already compromised the victim’s machine:

In this part we assume that attacker has access to victims machine. We try to making some changes on this machine to forwarding our ip address (attacker IP address).

First we know our IP address as a attacker. Reason of that start attacker machine and open terminal witch ctrl + alt + t. And type ifconfig. As you can see in that case attacker IP address is 192.168.56.103

After taking this information we need to connect victim (user) machine.

```
ifconfig
```



Left figure demonstrates how to find attacker IP address. Red circled area shows IP address of the attacker.

We need this address since we need to change Host file from victim’s machine.

We need to connect victims machine with ssh (secure shell). For more information you can go fallowing link “https://www.ssh.com". SSH basically allows to remotely connect another computer.

For this connection we need user IP address, User name and Password. In this part we assume that attacker own all of these information. So lets continue with how to connect user address.

We know attacker IP address but we don’t know user IP address. Fallow above steps for attacker IP investigation which is ifconfig.

Above figure shows ifconfig result of user.

```
[04/23/2017 09:38] seed@ubuntu:~$ ifconfig
eth14     Link encap:Ethernet  HWaddr 08:00:27:9e:b9:5f
          inet addr:192.168.56.102  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe9e:b95f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5554 errors:0 dropped:0 overruns:0 frame:0
          TX packets:5955 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:645686 (645.6 KB)  TX bytes:505566 (505.5 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:3657 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3657 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:318015 (318.0 KB)  TX bytes:318015 (318.0 KB)

[04/23/2017 09:38] seed@ubuntu:~$
```

We used seed ubuntu in this project and user name is seed and password is “dees”.

So we will connect with ssh to user machine.

Fallowing command line command allows us to connect victims machine which is ssh command. Sample ssh connection terminal command given below.

Warning: You should come back to attacker virtual machine.

```
ssh username@IP_ADDRESS_of_USER
```

After typing above command you need to enter password please type “dees” and enter. After entering password you can almost fully access to victims computer.

After taking control of the computer. We need to edit host file of the computer. Host files explanation comes fallowing. Host files works like an telephone books. In host file each domains have its confronting IP address in this file. So this file is obviously is the best place to attack and direct the domain address to our vulnerable web pages IP address [5].

You can access host file with below command.

Example host file from user(victim) without any attack given below.

```
cat /etc/hosts
```

“cat” command allows to display content of the file.

```
[04/23/2017 09:58] seed@ubuntu://etc$ cat hosts
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
```

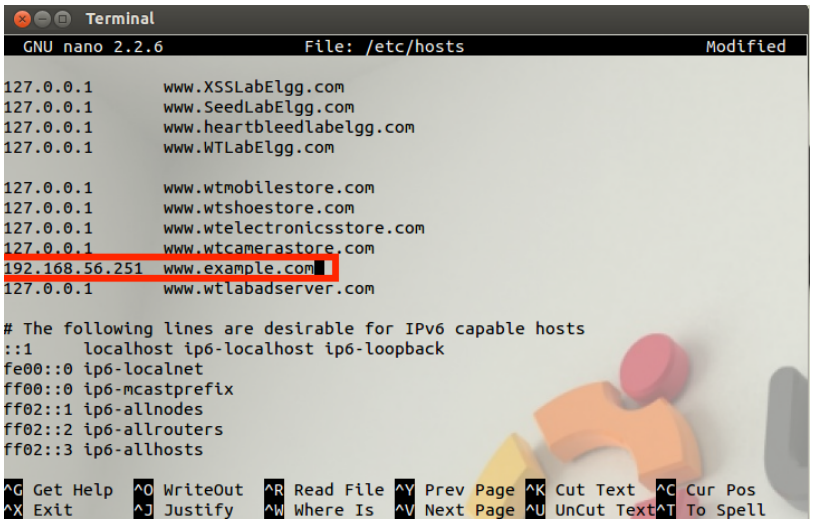
As you can see from figure it is really looks like an phone address book. There is IP address and they have domains. If you change any IP from these domains. When you type from browser you directed to changed IP address.

So we will use this gap to attack our user.

Lets go back to attacker side. Open attacker virtual machine and repeat ssh connection step. After ssh connection is successfully established. You should type fallowing command to open hosts file with fallowing command. And add fallowing line by-pass www.example.com IP address to attacker address which is 192.168.56.103 But below example we direct it to 192.168.56.251

Below code allows to edit hosts file. We need a privilege of the root so we need to add sudo to nano part. And type seed as password.

```
sudo nano /etc/hosts
```



With that technique attacker IP address may hided and untraceable.

When we come back to user machine and try to ping www.example.com we can see given IP address. Below command shows to how ping given domain.

```
ping www.example.com
```

Below figure shows result of the ping.

```
[04/22/2017 16:28] seed@ubuntu:~$ ping www.example.com
PING www.example.com (192.168.56.251) 56(84) bytes of data.
From ubuntu-3.local (192.168.56.103) icmp_seq=1 Destination Host Unreachable
From ubuntu-3.local (192.168.56.103) icmp_seq=2 Destination Host Unreachable
From ubuntu-3.local (192.168.56.103) icmp_seq=3 Destination Host Unreachable
^XFrom ubuntu-3.local (192.168.56.103) icmp_seq=4 Destination Host Unreachable
```

As you can see from above figure IP address of the www.example.com is changed. We assigned it from dis server is 192.168.56.151 But ping result shows attacker desired IP address.

NSLookUp ignores hosts file so it did not show 192.168.56.251 it shows 192.168.56.151. Reason of this is NSLookUp ignores hosts file.

But this obviously ping and browser tricked with this method. Again this method is too risky also impossible some cases. We need ssh connection informations of the victim.

Such as IP address, Password, Username. This informations only taken from social attacks.

Let’s continue with task 2…

Project Task 2: Directly Spoof Response to User:

This attack type did not require any direct access to user such as SSH. You directly attack between DNS server and user (victim). For that purpose we need to use some program seed-ubuntu provide which is NetWag.

In this attack we mimic the DNS responses and forward to our attacker server. But it is not always successful since our attack should capture and forward to attacker machine.

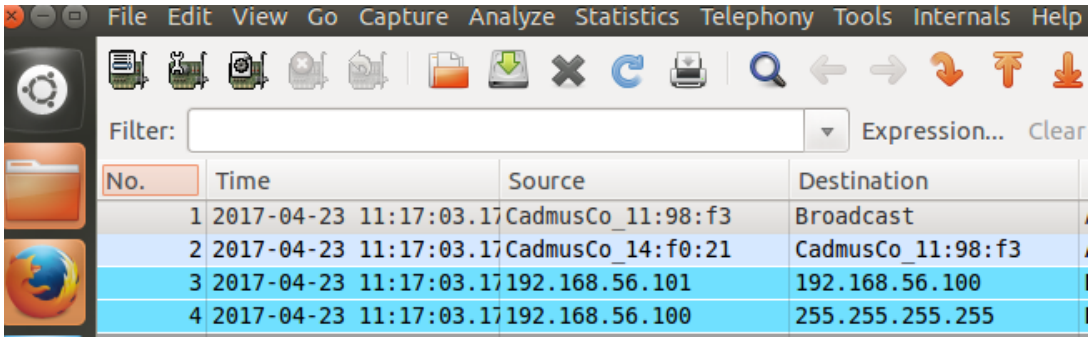
For this attack we need users and DNS server IP address. We can find DNS server IP address via wire-shark. Assume that we know user IP address in this part.

So first obtain user IP address with “ifconfig” command from user (victim) machine.

Attacker found its own ip address with “ipconfig” in this scenario attacker ip address is 192.168.56.102.

In this part this is 192.168.56.103 (previously it is end with 102 be careful)

We obtain that from wire-shark sending ping to any domain. So our DNS server ip address is 192.168.56.101 from wire-shark.



For wire star start capturing. Then ping to www.example.com with below code. Wireshark result is shown above.

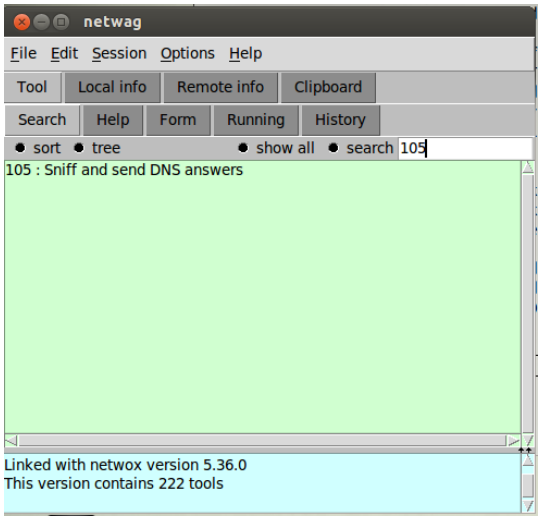
```
ping www.example.com
```

With identifying DNS ip address we are ready to use our tool which is NetWag.

NetWag gives us a interface to forward DNS responses to attacker machine. NetWag configurations given next page.

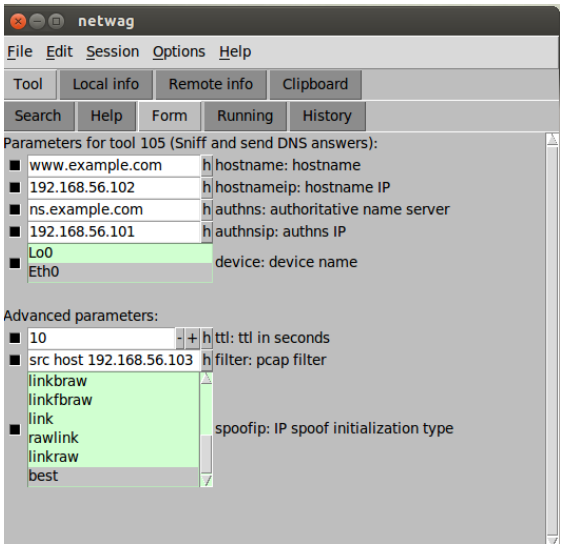
NetWag Configuration.

When you open NetWag type 105 to search and double click it. (It shown in below figure)



NetWag 105 tool allow to attacker sniff DNS answers and mimic that according to future configurations.

Double clicking NetWag we need to complete below form.



Hostname you need to type domain address to desired webpage.

Second add attacker ip address which is 192.168.56.102 which is forwarded ip address.

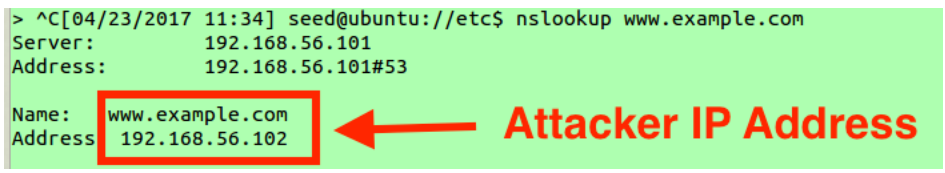
ns.exaple.com is refers to authenticated server name.

Next one is our DNS server ip address which we found with wire-shark.

In advanced we need to select time to leave parameter. Which can be 10 - 60 is enough for our attack.

For filter: pcap filter we need to set our user IP address (we assume that attacker know that)

Then run NetWag with selected configuration. After run state we need to check it is work or not. We can check that with going user machine and open terminal and type nslookup.



DNS look up shows that (above figure) we successfully directly spoof DNS with this method.

Check the address 192.168.56.102.

Again we attack user machine and we need to know user's ip address and it makes harder to spoof.

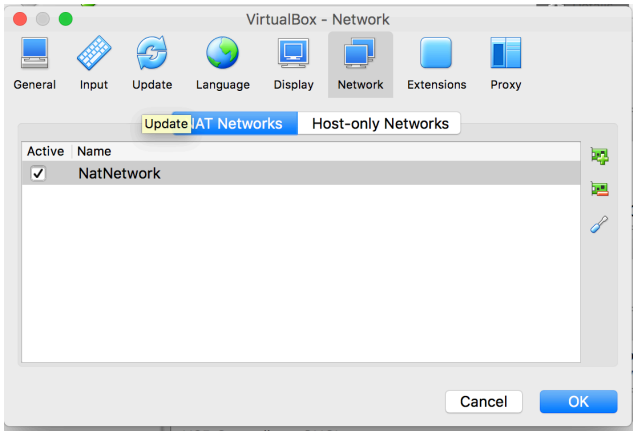
Again social attacks necessary for this attack.

For the next task we try to spoof directly DNS server.

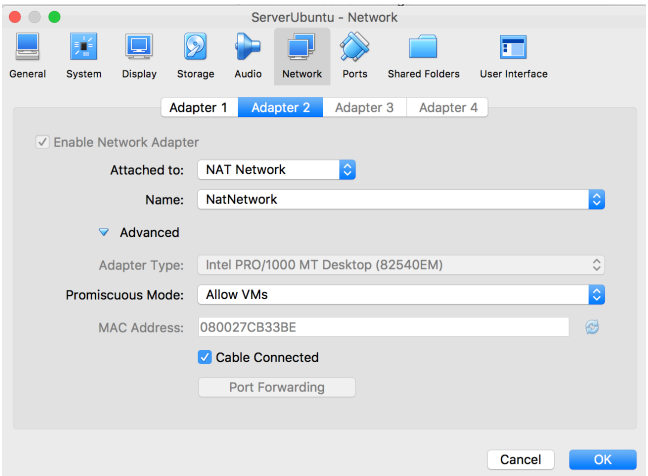
Project Task 3: DNS Server Cache Poisoning:

This time we directly attack the DNS server for cache poisoning. In that case we need to create virtual internet connection. In that purpose we create internet connection for attacker and DNS server.

First close all virtual machines.



Go to preferences of VirtualBox. Create NAT network from network preferences. Press "+" button and create it.



Then add this created network to attacker and server virtual machines as adapter 2.

Promiscuous mode should be Allow VMs.

Lets look IP addresses of the virtual machines again. You can check ip address with ifconfig.

```
          collisions:0 txqueuelen:1000
          RX bytes:24646 (24.6 KB)  TX bytes:14637 (14.6 KB)

eth15     Link encap:Ethernet  HWaddr 08:00:27:cb:33:be
          inet addr:10.0.2.4  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fecb:33be/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:142 errors:0 dropped:0 overruns:0 frame:0
          TX packets:171 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:51603 (51.6 KB)  TX bytes:22531 (22.5 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:54 errors:0 dropped:0 overruns:0 frame:0
          TX packets:54 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:4352 (4.3 KB)  TX bytes:4352 (4.3 KB)
```

Left figure illustrates ip addresses of the server.

```
[04/23/2017 12:38] seed@ubuntu:~$ ifconfig
eth14     Link encap:Ethernet  HWaddr 08:00:27:9e:b9:5f
          inet addr:192.168.56.103  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe9e:b95f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:79 errors:0 dropped:0 overruns:0 frame:0
          TX packets:75 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:16128 (16.1 KB)  TX bytes:13619 (13.6 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:2072 (2.0 KB)  TX bytes:2072 (2.0 KB)
```

Left figure illustrates ip addresses of the user.

```
[04/23/2017 12:38] seed@ubuntu:~$ ifconfig
eth14     Link encap:Ethernet  HWaddr 08:00:27:04:7c:9d
          inet addr:192.168.56.102  Bcast:192.168.56.255  Mask:255.2
          inet6 addr: fe80::a00:27ff:fe04:7c9d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:57 errors:0 dropped:0 overruns:0 frame:0
          TX packets:73 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:13083 (13.0 KB)  TX bytes:13001 (13.0 KB)

eth15     Link encap:Ethernet  HWaddr 08:00:27:a6:d4:98
          inet addr:10.0.2.5  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fea6:d498/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:97 errors:0 dropped:0 overruns:0 frame:0
          TX packets:159 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:40806 (40.8 KB)  TX bytes:21372 (21.3 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:67 errors:0 dropped:0 overruns:0 frame:0
```

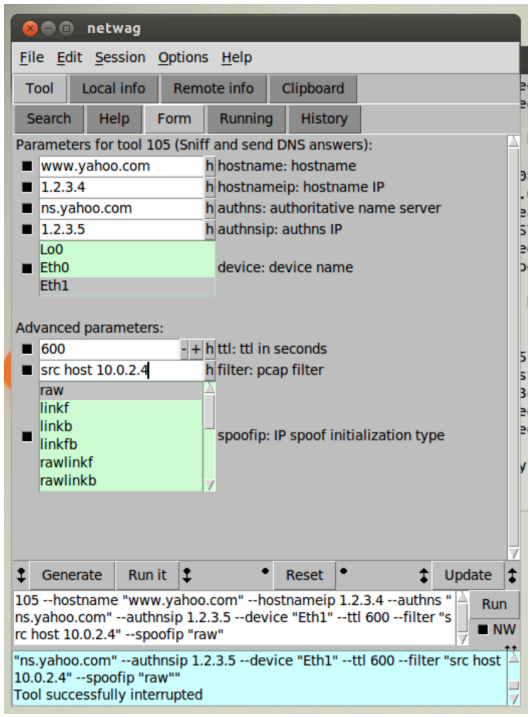
Left figure illustrates ip addresses of the attacker.

Two different IP address present.

You can see different ip dresses present for server and attacker. So we created a NAT network between attacker and server. In NAT network can machines can see their packages. Reason of that host-only adapter fail in this attack type.

So lets continue with how to achieve this attack.

In this attack first we go to attacker machine and open preinstalled program in seed ubuntu which is NetWag program. Again in task 2. Search 105 and double click it. But in this time we fill form differently



Lets assume our user enters www.yahoo.com. In this scenario our hacker or attacker want to direct IP address to 1.2.3.4. According to that we will fill form like below. First is designate to our target domain.

Second one is our directed IP address. Third one is authoritative name server. You need to remove wwww from address and add ns on start of it.

4. one is desired authors IP you can type anything you want.

Than select our NAT network to attack. For that purpose Eth1 is selected since eth1 is NAT network. You can see that from ifconfig.

TTL is lets say 10 minutes 10 x 60 second = 600 this is enough time for checksum.

Select raw mode since NetWag tries to spoof MAC address. Reason of that ARP requests to yahoo. Since yahoo and our virtual server is not on same network.

In pcap filter select DNS servers NAT network IP address. In that case 10.0.2.4.

We make cache empty before starting attack.

Go to server machine and type fallowing command.

```
sudo rndc flush
```

Reason of flushing is some cache data make fail our attack since my yahoo DNS informations set in cache so just flush it.

After flushing that click generate and run it from attacker's machine (use netwag with filled form)

Lets go to the user machine and open terminal and type

```
nslookup www.yahoo.com
```

results shown in next page.

```
[04/23/2017 12:38] seed@ubuntu:~$ nslookup www.yahoo.com
Server:         192.168.56.101
Address:        192.168.56.101#53

Non-authoritative answer:
Name:   www.yahoo.com
Address: 1.2.3.4

[04/23/2017 12:40] seed@ubuntu:~$ nslookup www.yahoo.com
Server:         192.168.56.101
Address:        192.168.56.101#53

Non-authoritative answer:
Name:   www.yahoo.com
Address: 1.2.3.4

[04/23/2017 12:41] seed@ubuntu:~$ nslookup www.yahoo.com
Server:         192.168.56.101
Address:        192.168.56.101#53

Non-authoritative answer:
Name:   www.yahoo.com
Address: 1.2.3.4
```

As you can see address is as we given address which is entered to netwag. After that you can interrupt running NetWag and you can see it is present on the DNS's servers cache.

sudo cat /var/cache/bind/dump.db allows to you see cached DNS entities you can find our poisoning from there.

As we can see finally we don't need user information and DNS poisoning is successfully achieved with final task.

You can also track from wireshark.

EXTRA

Each extra network level makes more harder since finding DNS server IP address is harder this scenario also same for the finding user IP address.

Conclusion:

In conclusion we tried to poison two ways and directly add DNS information with user privileges. In third task we can see not the only target is user. We can also attack directly to DNS server. It is obviously that we don't need to know user account information or user ip address. As you can see we can obtain DNS server ip address it is much more easy if we are same lan with the DNS server. This attack types are still dangerous for networks [1].

References:

[1] Turgut A. C. DKIM Modification for DNS Based Attacks. Retrieved from https://github.com/acanturgut/Network_Security/blob/master Access Date: 22 April 2017

[2] Son, S., & Shmatikov, V. (n.d.). The Hitchhiker's Guide to DNS Cache Poisoning. Retrieved from https://www.cs.cornell.edu/~shmat/shmat_securecomm10.pdf

[3] How to use VirtualBox to Run Our Pre-built VM Image? Step 1: Create a New VM in VirtualBox Step 2: Provide a Name and Select the OS Type and Version. (n.d.). Retrieved from http://www.cis.syr.edu/~wedu/seed/Documentation/VirtualBox/UseVirtualBox.pdf

[4] Project3 - Local DNS Attack.pdf. Koç University, COMP 434 Project #3 Description (n.d.). Retrieved April 23, 2017, from https://docs.google.com/a/ku.edu.tr/viewer Access Date

[5] Hosts File. (n.d.). Retrieved April 23, 2017, from http://support.isoc.net/Page.aspx/117/hosts.html

Setup is combination of [3] and [4]