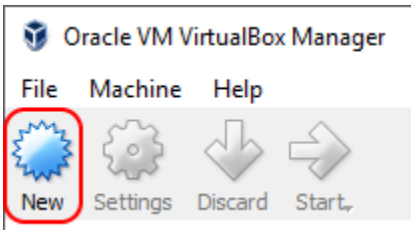
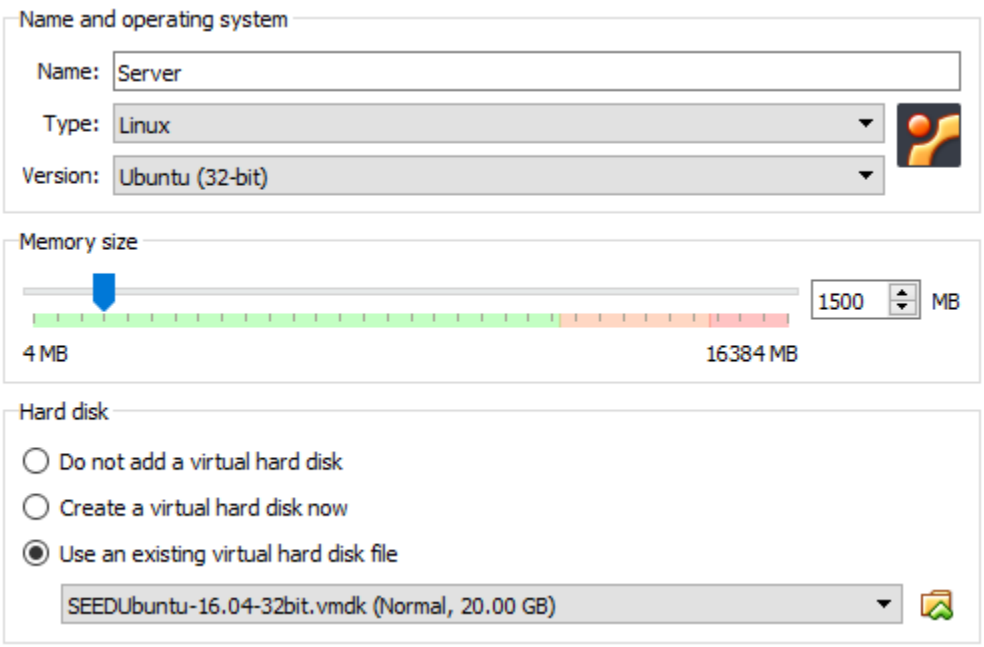
Create and Configure the Virtual Machines:

1. Download and extract the "SEEDUbuntu-16.04-32bit" virtual machine from http://www.cis.syr.edu/~wedu/seed/lab_env.html.

2. Open VirtualBox and create a new virtual machine.



3. Enter Expert Mode. Configure the settings as shown below and select the virtual machine hard disk that you downloaded and extracted in step 1. When finished, press Create.



4. Open the settings for the Server virtual machine.
   a. In the *General* → *Advanced* tab, set Shared Clipboard and Drag'n'Drop to Bidirectional.
   b. In the *Network* → *Adapter 1* tab, set the "Attached to" field to Bridged Adapter. Click the arrow to show advanced settings and change "Promiscuous Mode" to Allow VMs.

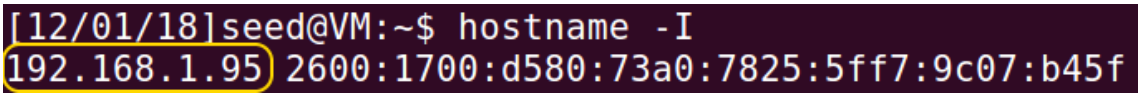
5. Right click on the Server VM and select Clone. (Note: the VM must be Powered Off). Name the new virtual machine "User", select "Reinitialize the MAC address", and create a Full Clone.

6. Repeat step 5 once more to create another virtual machine named "Attacker".

7. You should now have three virtual machines (Server, User, and Attacker). Start all three of them.

8. Identify the IPv4 address of each of your virtual machines. To do this, right click the desktop and select Open Terminal. Run the following command to get the IPv4 address of the current VM:

```
hostname -I
```



We are only interested in the first listed address. Repeat this command for all three virtual machines and record the IPv4 address of each machine for future use.

Task 1: Configure the User Machine

1. On the User virtual machine, run the following command to open the head file for editing:

```
sudo gedit /etc/resolvconf/resolv.conf.d/head
```

If prompted, the password for seed is “dees”.

2. Add the entry “nameserver <IP>” to this file, replacing <IP> with the IPv4 address of your Server VM. Ignore the warning about editing the file by hand. Save the file and exit.

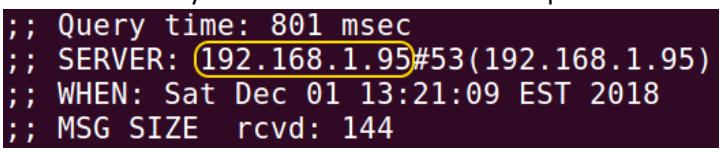
3. Run the provided command:

```
sudo resolvconf -u
```

4. Run a dig command on any hostname to test your DNS server setup. For example:

```
dig www.uhcl.edu
```

You should see your server IP listed in the output:



Task 2: Set Up a Local DNS Server

Steps 1 and 2 have already been completed on the provided virtual machine.

In step 4, you can ping a hostname (such as www.google.com) with the following command:

```
ping www.google.com
```

Press Ctrl-C to stop pinging. Alternatively, you can ping a fixed number of times (10 in this case):

```
ping -c 10 www.google.com
```

Task 3: Host a Zone in the Local DNS Server

In step 2, if you choose to copy and paste the provided zone file, be aware that the second line mistakenly contains a colon (:) that should be a semicolon (;).

In step 4, when you issue the dig command, you should see the correct IP addresses:

```
;; ANSWER SECTION:
www.example.com.        259200  IN      A       192.168.0.101

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

;; ADDITIONAL SECTION:
ns.example.com.         259200  IN      A       192.168.0.10
```

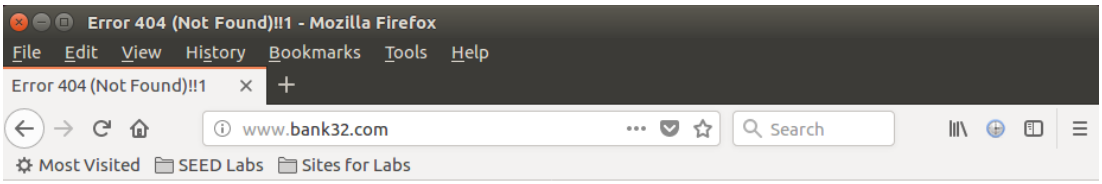
Task 4: Modifying the Host File

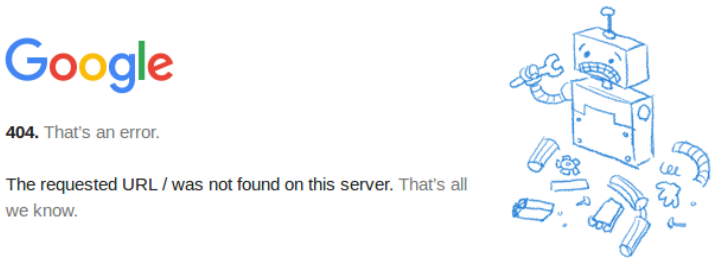
To remotely connect to the User's machine from the Attacker's machine, run the following command, where <IP> is replaced with the IPv4 address of your User VM:

```
ssh <IP>
```

When asked if you are sure you want to continue, enter "yes". When prompted for a password, enter "dees". You can now modify the User's hosts file from the Attacker's machine.

Try making www.bank32.com resolve to the IP address of www.google.com (172.217.1.132) and observe the results in Firefox (on the User's machine.) You should see something like this:





If Firefox doesn't show the expected result, there may be something wrong with how it handles the hosts file. Instead, simply ping www.bank32.com to verify that the domain name resolves to the IP you entered.

When you have finished, you can exit the SSH session by running the following command:

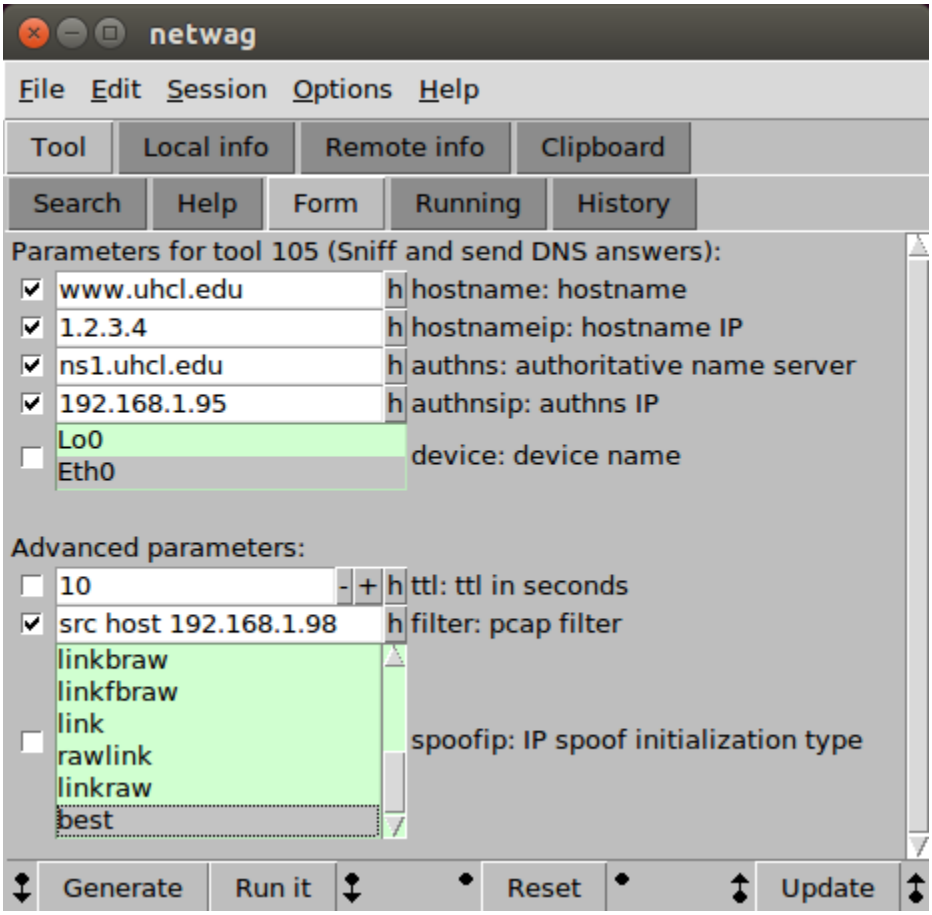
```
exit
```

Task 5: Directly Spoofing Response to User

Use of the Netwox tool is easier with the provided GUI. To access the GUI, run this command from the Attacker's machine:

```
sudo netwag
```

In the Netwag window, navigate to and click on command 105: "Sniff and send DNS answers." You will see an interface like this:



The *hostname* field should contain the domain name of the DNS query you want to target. Note that it cannot be "www.example.com", as we have previously hosted this domain on our local DNS server, so no DNS query will be sent out for hostnames in that domain.

The *hostnameip* field should contain the fake IP address you want to send to the user in response to the DNS query you are targeting.

The *authns* field should contain the name server of the targeted domain. You can find the nameservers of a domain by issuing a dig command.

The *authnsip* field should contain the IPv4 address of your Server VM.

The *filter* field should contain the command "src host <IP>", where <IP> is replaced with the IPv4 address of your User VM.

The other, unchecked fields are not used. In the example above, the Attacker will sniff packets sent from the User. When the User sends a DNS request for the targeted domain, the Attacker will send a spoofed response containing the address in the *hostnameip* field.

When you have finished filling out the parameters, click "Run it" and leave the Netwag program running. Open the User VM and issue a DNS query with the following command:

```
nslookup www.uhcl.edu
```

Of course, replace "www.uhcl.edu" with the domain name that you chose to target.

The response should contain the spoofed IP sent by the Attacker:

```
[12/01/18]seed@VM:~$ nslookup www.uhcl.edu
Server:         192.168.1.95
Address:        192.168.1.95#53

Name:   www.uhcl.edu
Address: 1.2.3.4
```

Note that this will only work for the first query you issue, since your local DNS Server will cache the correct address for future requests. To send a spoofed result to the same domain again, you must clear the local DNS Server's cache by running the following command on the Server VM:

```
sudo rndc flush
```

Task 6: DNS Cache Poisoning Attack

Adjust the Attacker's Netwag configuration according to the instructions and have the User get the IP of the targeted domain once again. This time, you will notice that the spoofed IP is persistent – the Server will continue to give out the fake IP address for as long as you specify in the ttl (time to live) field in Netwag.

Task 7: DNS Cache Poisoning: Targeting the Authority Section

To create and run the Python script:

1. Right click on the desktop on the Attacker machine and select New Document → Empty Document. Rename the document to "attack.py" and open it for editing.

2. Copy the sample code provided in the *Guideline* section towards the end of the instructions and paste it in your empty Python file.

3. Indent the code to match the sample code. Replace all of the curly single quotes (‘) with manually-entered straight single quotes ('). Remove the ① symbol in the code.

4. Modify the Authority section according to the instructions.

5. In the DNS packet construction section, modify "nscount", "arcount", "ns", and "ar" to match what is required in the instructions (there should be one entry in the Authority section and no entries in the Additional section.) Save the file when you are finished.

6. Open the terminal and run the Python script with the following command:

```
sudo python Desktop/attack.py
```

7. On the User machine, issue a dig command on the domain www.example.net. If you notice an error on the Attacker's terminal ("IndexError: Layer [IP] not found"), flush the Server's cache, re-run the Attacker's Python script, and issue the User's dig command again.

8. When you are finished, press Ctrl-C on the Attacker terminal to terminate the Python script.

Task 8: Targeting Another Domain

In attack.py, modify the Authority section according to the instructions. Be sure to also modify the corresponding variables in the DNS packet construction section. Flush the server's cache and re-run the Python script.

Task 9: Targeting the Additional Section

In attack.py, modify the Authority and Additional sections according to the instructions. Be sure to also modify the corresponding variables in the DNS packet construction section. Flush the server's cache and re-run the Python script.