Name: __Madina Martazanova_____

Computer and Network Security

Lab 4 Networking

For this lab, you need to use a computer. I assume you have access to a Microsoft Windows based personal computer. You also need to install software on C drive under Program Files and hence you need access to a computer with **administrative privileges**.

In this lab, you will try to compromise **BadStore.net**, a vulnerable web application. The purpose is to understand vulnerabilities in web applications and learn how to develop software that will not exhibit such vulnerabilities. A **white hat hacker** is a computer security specialist who breaks into protected systems and networks to test and asses their security. In order to be successful as a white hat hacker, you need to be knowledgeable about technology and be extremely creative. Please do not apply the techniques you learn in this lab on systems for which you are not responsible and you do not have explicit permission.

1. Set up Virtual Box and Explore NAT Networking

Oracle VM VirtualBox is a hypervisor (virtualization software) for x86 computers from Oracle Corporation. VirtualBox may be installed on a number of **host** operating systems, including: Windows, OS X, and Linux. It supports the creation and management of **guest** virtual machines running versions and derivations of Windows and Linux.

a. We have already set up Oracle VM VirtualBox in Lab 1. You must have also set up Kali Linux and Metasploitable in Lab 1. If not, follow the instructions in that Lab and set up VirtualBox, Kali Linux, and Metasploitable.

b. By default, both Kali and Metasploitable would have been set up in way that their network adapters are attached to NAT (network address translation). That means, VirtualBox assigns a private IP address for your Kali or Metasploitable and maps the private address to the public address of your physical computer. You should be able to access the Internet.

c. Start Metasploitable. Login with username and password as msfadmin and msfadmin, respectively. In the terminal window, type: **`ifconfig eth0`**

   Private IP address associated with Metasploitable is: **_10.0.2.15____**

d. To check network connectivity, type: **`ping 8.8.8.8`**
   After a few lines of output, type **`Control-C`** to stop the pinging. Report the **`ping`** statistics.

   __9 packets transmitted, 9 received, 0% packet loss, time 8021ms
   Rtt min/avg/max/mdev = 14.242/32.773/143.733/39.473 ms___

Name: __Madina Martazanova_____

e. Determine the domain name of the address we just pinged. Type: **`nslookup 8.8.8.8`**

Domain name associated with 8.8.8.8: **__name = google-public-dns-a.google.com_**

f. Keeping Metasploitable running, we now want to start Kali. When you select Kali, properties of the machine should appear in the right column. Be sure that the network adapter is attached to NAT.

g. Login as root (password: toor). Type an appropriate command to determine the IP address.

Private IP address associated with Kali is: _ **10.0.2.15** _

You should find that the address is the same as we determined for Metasploitable.

h. Is Kali able to communicate with the outside world? **`ping 8.8.8.8`** and check.

Were you successful? ___**Yes__**

How can Kali and Metasploitable both have the same private IP address and yet communicate with the outside world? By default, VirtualBox isolates each virtual machine and places a separate "virtual router" between each virtual machine and the outside world. This separation maximizes security and with this kind of NAT the **virtual machines cannot talk to each other**, but each one can access the Internet. We will next explore how Kali and Metasploitable can communicate with each other.

i. **Shut down both machines**.

2. Virtual Box and Host-only Networking

a. In order for Kali and Metasploitable to communicate with each other, we will set up Host-only networking. For this, on VirtualBox, access **`File -> Preferences -> Network`**. You will be shown a list of possible networks, including NAT networks and Host-only Networks. Select Host-only networks. You should see **`VirtualBox Host-only Ethernet Adapter`**. If not, click the icon on the right to add one. (You need administrative privileges for this step.) It will add an entry with a name.

b. Select **`VirtualBox Host-only Ethernet Adapter`** entry and edit it by clicking the appropriate icon to the right. There are two tabs, one for the adapter, and the other for the DHCP server. The Adapter tab will give the IP address for the network, etc. It should read something like **`192.168.56.1`** with a subnet mask of **`255.255.255.0`**. The DHCP Server pane will show the DHCP server information. If it is not already enabled with the information filled in, then enable it and fill it in as follows:

Name: __Madina Martazanova_____

Server Address:	192.168.56.100
Server Mask:	255.255.255.0
Lower Address Bound:	192.168.56.101
Upper Address Bound:	192.168.56.254

Click **OK** twice to save the changes.

c. Now that we have created a host only network, we need to attach Metasploitable and Kali to the host-only network. To do so, select Metasploitable VM. Click the Network setting shown on the right. Select the **Host-only adapter** from the **Attached to** drop down list. The proper name of the adapter should appear in the Name box since there is only one. Click **OK** to save the setting.

d. For Kali, select the VM and the Network setting shown on the right. For Adpater1, uncheck the box that says Enable Network Adapter. Select **Adapter 2**. Enable this adapter. Select the **Host-only adapter** from the **Attached to** drop down list. The proper name of the adapter should appear in the Name box since there is only one. Click OK to save the setting.

e. Start Metasploitable and then Kali, in that specific order. Login on both machines and determine their IP addresses.

Private IP address of Metasploitable: **192.168.56.102**_

Private IP address of Kali: **_192.168.56.101**_

Ping Metasploitable from Kali. Where you successful? **_yes__**

Ping Kali from Metasploitable. Where you successful? **_No__**

Ping 8.8.8.8 from Metasploitable. Where you successful? **__No_**

Ping 8.8.8.8 from Kali. Where you successful? **__No_**

j. **Shut down both machines**.

3. Set up BadStore on VirtualBox

BadStore is a Linux-based server application. It is distributed as a bootable ISO and hence can be booted directly. But, we will set it up in VirtualBox.

a. Access **http://www.itss.brockport.edu/~nyu/security/** and download the BadStore ISO image.

b. You will download a file named **BadStore_212.iso**. Copy the file to **C:\Software**

Name: __Madina Martazanova_____

c. Determine its **SHA256** hash.

d. Ensure that it reads as below (where 8 hex digits have been deleted)

-- -- c6 df 91 39 d3 8e e0 a2 76 78 f1 fd 1e a0
21 58 f8 e8 18 81 46 44 c6 8a 0a 10 35 20 -- --

Provide the missing digits: **_65d4 / afcc __**

e. Start VirtualBox. Click the **New** icon to create a new VM. Give your new VM the name **BadStore**; specify the operating system type as **Linux**; and choose **32-bit Ubuntu**. You may allocate **1 GB** (1024 MB) RAM to your VM. Specify that it should create a virtual hard disk now, **8 GB**, **VDI**, **dynamically allocated**. (This way, VirtualBox will allocate space on the fly, and not reserve 8GB.)

f. To assign the BadStore ISO to the CD-ROM drive of the VM, select **Settings** for the VM you just created and then select the **Storage** tab. On the left you will see the VM's "Storage Tree" and you should see **Controller: IDE** as one listed. With this selected, add a new storage attachment to this tree by clicking the little icon at the bottom with the plus on it in the lower left. It will ask you to choose whether to add Optical drive or a Hard Disk; select **Optical drive**. Then it will ask you whether to "Choose Disk" or "Leave Empty"; select "Choose Disk". A file dialog will come up and you should choose the **BadStore_212.iso** file that you previously downloaded and saved in **C:\Software**. Once you do, you should see this image added below the IDE controller in the Storage Tree, and it should be the IDE Primary Master. You might also see an entry for "Empty" which was there at the start; if so, then remove it by selecting the Empty entry and clicking the icon with the minus sign on it. Click **OK** to save settings.

g. Assign the BadStore VM to the host-only network. To do so, select the Settings for the BadStore VM and then select the Network tab. Select the **Host-only adapter** from the **Attached to** drop down list. The proper name of the adapter should appear in the Name box since there is only one. Click **OK** to save the setting.

h. Now you are ready to boot the BadStore VM. Start Metasploitable, Kali and BadStore in that specific order, so that the same private IP addresses are assigned every time we work on these machines.

i. As you start BadStore, you will see a **text window** show up and a bunch of text fly by, while it is booting. When it is about to configure eth0 using DHCP, it appears to hang for a while. Wait patiently. Depending on your machine capability, it may take several minutes. Eventually, the message **Please press enter to activate this console** should appear.

Name: __Madina Martazanova_____

j. We need to get the IP address for the BadStore VM. Press enter to activate the VM's console. In the **bash** prompt, type the **UNIX** command

```
ifconfig eth0
```

IP address (**inet addr**) for BadStore: __**192.168.56.103**__

If you had followed all the instructions carefully, the IP addresses associated with **Metasploitable**, **Kali** and **BadStore** should be **192.168.56.101**, **192.168.56.102**, and **192.168.56.103**, respectively, since the address range for the DHCP server was set as 192.168.56.101-192.168.56.254. I will assume the same for the rest of the lab. If the IP addresses that you have are different, make suitable changes.

k. To make the access to Metasploitable and BadStore easy, let us add the IP addresses to your Kali machine's **/etc/hosts** file. Use an editor, such as **pico**, to edit **/etc/hosts** and add two lines as follows immediately after the line that reads: **127.0.1.1 kali**

```
192.168.56.101      www.metasploitable.com
192.168.56.103      www.badstore.net
```

Save the changes and quit.

l. Open a terminal window on Kali and type the command:

```
ping www.badstore.net
```

If you see a ping response, you have successfully set up the hosts file. Likewise, try

```
ping www.metasploitable.com
```

Where you successful in both? ___**Yes**___

m. Open Mozilla Firefox. I recommend Firefox because it has a nice set of developer tools that allow you to inspect, and modify, the contents of Web pages. Type the address **http://www.badstore.net** on the address bar. You should see the landing page for the BadStore, which displays a black-and-white picture of an old-west-style saloon. If you see it, you have successfully set up BadStore on VirtualBox.

Have you successfully set up BadStore? _____
If not, please see me in person and seek help.

If you want to shut down the VM, select in the console window showing BadStore running **File -> Close**, and **Save the state**. This way, you will be able to restart the VM in the same state later. If you have no desire to restart in the same state, you may power down the virtual machine rather than choosing to save the state.

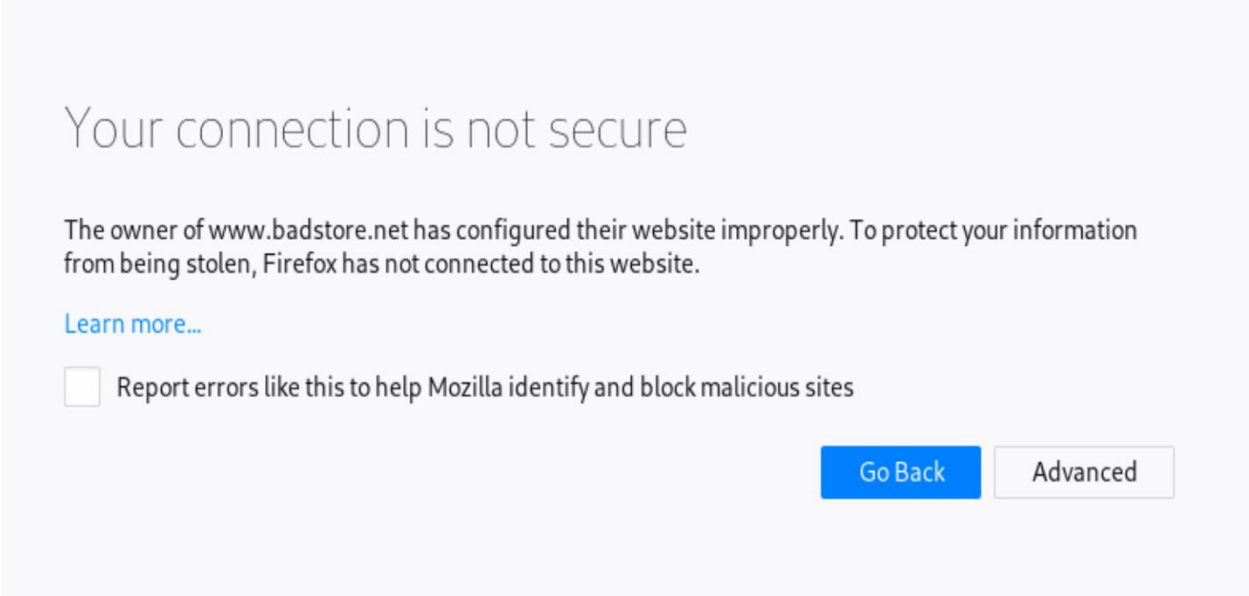
Name: __Madina Martazanova_____

Note that if you **reboot** the BadStore VM, its IP address may change, so you will have to edit the hosts file again. Hence, you should, close the running VM, **saving its state** rather than powering it off. When you restart it, it should restart the network and reconnect using the same address (which you can confirm using the ifconfig command). Also, BadStore is a database driven web application that maintains the changes made to the database only in RAM. Hence, rebooting BadStore will **reset** the database. If for some reason, you wish to reset the database without rebooting, you may do by using the URL **`http://www.badstore.net/cgi-bin/initdbs.cgi`**

4. Exploring BadStore SSL Certificate

a. Open **`Mozilla Firefox`** on **`Kali`**. Type the address **`https://www.badstore.net`** on the address bar. Note that I am explicitly using the **`https`** protocol and not **`http`**. You will receive an error message as the certificate is not trusted.

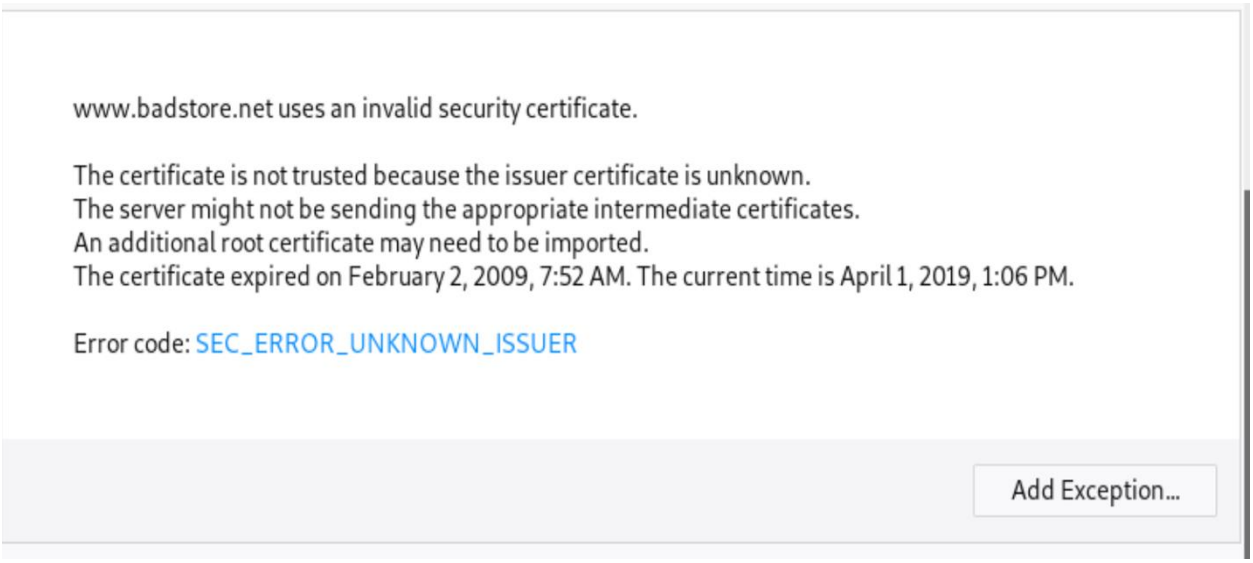
Error message:



b. Click on **`Advanced`**. More detail is revealed. What specifically is the reason given for stating that the server uses an invalid security certificate?

Certificate expired on:

Name: __Madina Martazanova_____



c. Click on **`Add Exception`** button. Let us view the certificate. Click on View.

Domain for which the certificate is issued: _ **www.badstore.net** __

Issued by (certification authority): **Snake Oil CA**

Period of validity: **_Begins On May 10,2016 Expires On February 2,2009**

Certificate signature algorithm: _____

Observe that the certificate hierarchy shows no other higher level certificate. That is, while we have a certificate for www.badstore.net, we do not have the certificate of its certification authority (Snake Oil) to verify the signature on the certificate presented by www.badstore.net.

d. We will now add this certificate to our certificate store so the error message does not appear again. Close the certificate and the click **`Confirm Security Exception`**. You will now be allowed to view the site.

e. What exactly happened? Select Firefox **`Preference`** (The three horizontal lines icon on the right.). Select **`Advanced -> Certificates -> View Certificates -> Server`**. Scroll down and see that the certificate sent by **`www.badstore.net`** is stored in the certificate store.

What is the name of the company under which it is listed? __ **Snake Oil, Ltd** __

Select the certificate for www.badstore.net itself.

What actions are possible on the certificate? __ **SHA256 or SHA1**
___

Note that we may delete this certificate from the browser's certificate store at any time we wish.

f. Select **`Preferences -> Privacy -> Clear your recent history`**. Select **`Details`** and make sure all boxes are checked. Then, in the time range to clear, select **`Everything`** and clear the cache completely. Close Firefox.

5. Explore http headers and BadStore

Now that we have successfully set up BadStore and cleared the cache, let us explore the store and understand what it has to offer.

a. Use Mozilla Firefox and access **`http://www.badstore.net`**. Note that the URL displayed in the address bar changes right away:

Redirected URL: __ **http://www.badstore.net/cgi-bin/badstore.cgi** _

b. This page has very little text. It has several images on the other hand. To see the http requests made to get all the files needed, open the **`developer tool`** as follows: click on the three horizontal lines icon (Open Menu) on the tool bar at the right next to home page icon. Choose developer tools and Network. In the small window that opens up at the bottom, click on **`Show in separate Window`** (near close button). Click reload to see the http requests and responses.

You should see a listing of the requests sent, giving method, file, domain, type, etc.

How many requests were made in total? __17_

What method was used for all of them? __GET_____

Select the first GET request. You should now see more detail, specifically the headers sent and received, cookies involved, the response file, etc. Explore each one of tabs, one by one.

What web server software is powering this application? (Write in full detail, because version numbers are very important for a hacker, black hat or white hat.)

Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c

Select the **`Cookies`** tab.

Cookies placed by the server at this stage: **None__**

Name: __Madina Martazanova_____

Note that there is a button that allows us to edit and resend the request. This will be very helpful later to modify and resend form data.

Hide request detail by clicking the little icon to the left of the panel that opened up. Explore other requests one by one.

What is status code 404? **_404_Not Found** _

Three files that resulted in status code 404: **shapeimage_1.png, shapeimage_3.png, shapeimage_4.jpg**

Name of the JavaScript file received: _ **BadStore_page.js**_

File type of the shopping cart image? **__jpg**_

There are three **`jpg`** images that were successfully obtained. What are their names?

shapeimage_4.jpg, store1.jpg, BadStore.jpg

c. Return to the Firefox display Window and explore the store systematically, one link at a time on the left column.

Click on Home. There should be no change.

Click on What's New.

What is the URL on the address bar?_
http://www.badstore.net/cgi-bin/badstore.cgi?action=whatsnew

How many items are on store display? **__8 Items** _____

Add **Snake Oil** to the Cart. Perhaps this will create a cookie. Use the developer tool to determine the cookie. (**`CartID`**)

Cookie: ___

As you can see, the cookie consists of several values separated by colon (**:**) symbol. Add one more item to the cart, say the **Perfect Code**. Determine the cookie.

Request cookie: **__1553878598:1:11.5:1000_____**

Note that the request cookie is the same as above.

Name: __Madina Martazanova_____

Response cookie: **__1553878598:1:11.5:1000_**

Now guess the **format** of the cookie. That is, identify what the values in the cookie represent. The first field is Cart ID.

Format of the cookie: **`Cart ID`**: _____

CartID : Request number : Size (kb) : max number of requests

d. Choose Sign our Guestbook.

URL on the address bar: __
http://www.badstore.net/cgi-bin/badstore.cgi?action=guestbook____

Add a comment to their Guestbook, saying: **I love the current offerings. I look forward to your Memorial Day Sales.** Use any fictitious name and email address.

Some users have previously signed up the Guestbook. Some are likely to be registered users. Noting down their names and email addresses is a good idea for later exploit.

Other signers: **Evil Hacker s8n@haxor.com**

e. What information/services are provided under the following links?

View Previous Orders: **You have no previous orders!_**

About Us: _ **summary of the site's purpose, has a picture of a Seal balancing a ball on its nose.**

My Account: __ **A link to the login/registration page.**
A text field for a user to enter their e-mail address.
A security question asking for the user to select their favorite color from a drop-down list.
A button to reset a password.
_

f. Register a new account as a User. You may use fictitious name, email address, etc. But, you need to keep track of them as you will need them later. On successful registration, the visible effect is that your name appears to the left of the shopping cart.

Explore the form submission and response in developer tool.

Look at the **`Params`** of the **`Post`** method. Most of the fields are obvious. But there is a field named **`Role`** that you did not fill out.

Name: __Madina Martazanova_____

Value associated with Role: _____

Also see the cookies now. There is a new cookie **SSOid**.

Length of the **SSOid** string (should be a multiple of 4):

bWFkbzA2eWFob28uY29tOjg0NGMxNTM5ZTQ3YWE2NTAzNWVlYTAyOTY4NGViZDU2Ok1hZG8gTWFydDpV

This seems to be a long string of meaningless characters. But considering that it consists mostly of upper case and lower case characters a-z and digits 0-9, and that its length is a multiple of 4, there is a strong possibility that it is a Base-64 encoded string.

Use an online Base-64 decoder at **https://www.base64decode.org/** and see if it can be decoded. It will result in a meaningful string only if it is indeed Base64 encoded.

Decoded **SSOid** Cookie:

mado06yahoo.com:844c1539e47aa65035eea029684ebd56:Mado Mart:U

Indeed, this cookie keeps the session going once you have logged in. The presence of **U** in the session cookie, which we had previously identified as **Role**, suggests the possibility that perhaps this character in the session cookie establishes the privilege level. Clearly one of the privilege level is as a registered user, indicated by a **U**. What else is possible – perhaps **Supplier** or **Administrator**.

g. Click on the link View Cart to the right of the Cart. Place the Order. You need to enter country to ship and a credit card number. Enter 1234567890123456 as a 16-digit credit card number and 03/20 as the expiry date. Since it is not a valid credit card number that meets the check digit property, you will receive an error message.

Error message printed: _____

Use the first valid VISA number from the site below and place the order:
http://www.freeformatter.com/credit-card-number-generator-validator.html

Credit card number used: _: **Bad Card Number: Invalid Luhn Checksum**

Name: __Madina Martazanova_____

h. Select the link My Account. It has changed. What information/services are provided?

The text fields for "New Full Name", "New Email Address" and "Change Password"/"Verify" have been added to edit the details of my account.

Now that you have familiarized yourself with the BadStore application, in next lab, you will continue the exploits. Be sure to save the state of the BadStore rather than powering it off.

Comment Summary