**SQLMAP Ethical Attack**

**Colin Glory**

**Information Assurance and Security**

**Fall 2022**

**The scenario:** SQLmap is an open-source tool used in penetration testing to detect and exploit SQL injection flaws. SQLmap automates the process of detecting and exploiting SQL injection. SQL Injection attacks can take control of databases that utilize SQL. In this case, we will be using Kali to attack Metasploitable2. The easiest way to get a target machine is to use Metasploitable 2, which is an intentionally vulnerable Ubuntu Linux virtual machine that is designed for testing common vulnerabilities.

A scenario for this project can be a hacker wants to hack into an Amazon database and access user’s passwords.

**IT Assets:**

Kali: Kali Linux is a Debian-derived Linux distribution designed for digital forensics and penetration testing. It is maintained and funded by Offensive Security.

Download Link: <https://www.virtualbox.org/wiki/Downloads>

Requirements:

2 GB of RAM.

20 GB of disk space.

Broadband internet connection.

High-definition graphics card and monitor.

Broadband internet connection.

VirtualBox Settings: Use the Virtual Box “Internal Network / intnet” adapter setting for attacker/victim machines to communicate with each other.

Static IP: 192.168.106.25

Metasploitable2: The easiest way to get a target machine is to use Metasploitable 2, which is an intentionally vulnerable Ubuntu Linux virtual machine that is designed for testing common vulnerabilities.

Download Link: <https://sourceforge.net/projects/metasploitable/>

Requirements:

1 GB of RAM (2 GB is recommended)

VirtualBox Settings: Use the Virtual Box “Internal Network / intnet” adapter setting for attacker/victim machines to communicate with each other.

Static IP: 192.168.106.51

**Videos Used:**

[**https://www.youtube.com/watch?v=IGIA7eSMxs8&t=647s**](https://www.youtube.com/watch?v=IGIA7eSMxs8&t=647s)

**https://www.youtube.com/watch?v=-q8Jj4aAWYw&t=236s**

1. **VirtualBox Setup**
   1. Go to <https://www.virtualbox.org/wiki/Downloads>
   2. Select
   3. Let it download, then run the program when finished
   4. When VirtualBox opens, select next, next again, next, yes, then install
   5. If you get asked to download device software, press install.
   6. You may now run VirtualBox
2. **Kali Download**
   1. Go to <https://www.kali.org/get-kali/>
   2. Graphical user interface

      Description automatically generatedSelect the option:

* 1. Your system is either 32 bit or 64 bit, make your download decision based off of that
  2. A screenshot of a computer screen

     Description automatically generated with medium confidenceSelect the download button:
  3. Wait for it to install

1. **Kali Setup**
   1. Go to your downloads, then right click on the kali download zipped file, then extract to whatever folder you want.
   2. Load up Virtual Box, select tools, then New

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

Description automatically generated

* 1. Name: Kali | Type: Linux | Version: Debian 64 bit
  2. Next
  3. For the memory size, it depends on your system. For me I chose around 8gb due to having 32gb of RAM
  4. Graphical user interface, text, application, letter, email

     Description automatically generatedFor the hard disk, select use an existing virtual hard disk:
  5. Qr code

     Description automatically generated with medium confidenceSelect the folder icon at the bottom, then select Add at the top right
  6. Go to the unzipped folder of Kali that we previously unzipped
  7. Now select🡺
  8. After selecting the file, press open
  9. Now choose that file in the hard disk area and select create
  10. Graphical user interface, text, application, email

      Description automatically generatedFor Kali settings, make sure the network adapter 1 is enabled and select Internal Network ⇒
  11. You may now run Kali
  12. Let Kali run. It may run some installations, if it does then let it finish. Once you get to the login screen, the credentials are as follows:
      1. User: kali
      2. Password: kali

1. Metasploitable2 Setup/Download
   1. Graphical user interface

      Description automatically generated with low confidenceGo to https://sourceforge.net/projects/metasploitable/ then select download
   2. Let it download. Go to the zipped file when it is finished, then unzip it to your desired folder.
   3. Load up Virtual Box.
   4. Select Tools, then New
   5. Name: Metasploitable2
   6. Type: Linux
   7. Version Debian 64 bit, then select next

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

Description automatically generated

* 1. For the memory size, it depends on your system. For me i chose around 8gb due to having 32gb of RAM.
  2. Graphical user interface, text, application, letter, email

     Description automatically generatedFor the hard disk, select use an existing virtual hard disk ⇒
  3. Select the folder at the bottom of the screen then press add ⇒ Qr code

     Description automatically generated with medium confidence
  4. Go to the unzipped folder of Kali that we previously unzipped.
  5. Select🡺 
  6. Now you can hit create.
  7. For the network settings, make sure the network adapter 1 is enabled and select Internal Network ⇒Graphical user interface, text, application, email

     Description automatically generated
  8. You can run Metasploitable2 now.
  9. Let Metasploitable2 run. It may run some installations, if it does then let it finish. Once you get to the login screen, the credentials are as follows:
     1. Username: msfadmin
     2. Password: msfadmin
  10. This vm machine will look different than Kali.

1. Static IP Address Setup
   1. On Kali, right click the icon to the left of the volume button, then select edit connections ⇒ Graphical user interface, text, application, chat or text message

      Description automatically generated
   2. Now select Wired Connection 1 then press the settings button at the bottom. Go to IPV4 settings  and press the add button. Enter as follows:

Graphical user interface, application

Description automatically generated

* 1. Once the information is entered in, press save at the bottom and load a new terminal window. In the window type *ifconfig* to see if your address has changed. 
  2. Now for Metasploitable2. You may type ifconfig to view your current network settings and IP. To change the address, you must type sudo nano /etc/network/interfaces
  3. Once you have entered the file, you will see information. You will change the section that starts with  to:

Text

Description automatically generated

* 1. Cntrl + O then cntrl X to save and exit
  2. Now type ifconfig in a terminal. You will now see the updated ip address

1. **Pinging Machines**
   1. Now you should be able to ping each machine.
   2. To ping kali from Meta type *Ping 192.168.106.25 -c4*
   3. To ping from Kali to Meta would be *ping 192.168.106.51 -c4*
2. **Apache2 Server Setup**
   1. You will need to set up a web server on the Metasploitable machine.
   2. You can type clear in the terminal to clean up the screen. To install apache2, type in the terminal *sudo apt-get install apache2*
   3. This will install the webserver. To start the web server type in the command *sudo /etc/init.d/apache2 restart*
   4. Now on the Kali machine. Go to Firefox, then type *192.168.106.51* in the search bar.
   5. Graphical user interface

      Description automatically generatedYou are now ready to start the attack.
3. SQLMAP Attack
   1. On the Metasploitable2 machine type the following:
   2. 
   3. Change dbname to owasp10, then CRTL O to write out and CTRL X to exit

Text

Description automatically generated

* 1. Finally it is time to attack our victim machine, Metasploitable2. On firefox in Kali, type in Metasploitable 2’s IP Address, *192.168.106.51*.
  2. Select the Mutillidae tab: Text, letter

     Description automatically generated
  3. Select OWASP Top 10 , ⇒A1 Injection⇒ SQli Extract Data⇒user info
  4. To make sure the database is working properly, choose *Please register here* and fill in random information. If you get no errors, the database is set up properly. If you have an error, please check the previous slide.
  5. Go back to the login page and enter in admin for username and something random for the password. You may now hit View Account Details
  6. You will get an error, which is what we want.
  7. Now copy your URL bar: 
  8. And now paste it in a notepad on Kali. You will put double quotes around the pasted text: 
  9. Copy the updated text and open a new Kali terminal window. In the terminal window type *sqlmap -u “paste the new url here”*
  10. SQLMAP will now start to run and you will be prompted with Y/n questions. Type Y. SQLMAP will begin tests. A picture containing text

      Description automatically generated
  11. You will be prompted with this statement:
  12. 
  13. The username is enough to get us access into the database, so you can press N.
  14. We can now view the databases of Mutillidae. In the terminal type *sqlmap -u “paste the new url here” –dbs*
  15. Press Y when you get promoted with a question. You will now see the databases. Text

      Description automatically generated
  16. We can go a step further and view the tables of each database. Let's choose owasp10.
  17. In the terminal type *sqlmap -u “paste the new url here” –tables -D owasp10*
  18. Once again it will ask you a question, type Y
  19. Here are the tables: Text

      Description automatically generated
  20. We can go another step forward and view the contents of the tables
  21. In the terminal type *sqlmap -u “paste the new url here” -T accounts –dump*
  22. Press Y when the question gets asked
  23. We have accessed their tables! We breached heir system and can now see all of the login Information. The attack is done, but you can explore this tool to go even further. You can try to change table information!

1. Appendix
   1. The first problem I ran into was not knowing how to how the attacker access the victim’s localhost web page. To fix this, you need to follow the apache2 web server steps.
   2. The last problem I have dealt with had to do with setting up static ip addresses. I was able to configure Kali’s ip address to my liking, but couldn’t figure out how to do it for Metasploitable’s machine. You must edit the file in /etc/network/interfaces. All steps are provided above.