Chapter 5

Lab 5.5

Objective: Perform security testing on Dromedary using Gauntlt

Introduction

Security testing is an important process because it can reveal application vulnerabilities. To accomplish this, we can use a security testing framework called **Gauntlt**.

Install Gauntlt

1. Install Ruby 2.3.0 via the instructions provided at https://rvm.io/:

```
$ gpg --keyserver hkp://keys.gnupg.net --recv-keys
409B6B1796C275462A1703113804BB82D39DC0E3
$ curl -sSL https://get.rvm.io | bash -s stable --ruby=2.3.0
$ source /home/vagrant/.rvm/scripts/rvm
$ ruby -v
```

2. Clone the Gauntlt repository:

```
$ git clone https://github.com/gauntlt/gauntlt.git
```

3. Install Gauntlt via the instructions at https://github.com/gauntlt/gauntlt. However, also install `libcurl` as a dependency for **DIRB** and **nmap**:

```
$ sudo apt-get install libcurl4-gnutls-dev nmap
$ cd gauntlt/
$ source ./install_gauntlt_deps.sh
$ bash ./ready_to_rumble.sh
```

Start Dromedary

1. Refer to the instructions provided in Chapter 5, Lab 5.1 to install Dromedary.
2. Run Dromedary in the background:

```
$ cd dromedary
$ PORT=1337 nohup gulp &

# ctrl+C to return to the command prompt
```

Modify Attack Files

1. Some of Gauntlt's example **.attack** files are going to be utilized to test the security of the Dromedary application. Navigate to the **examples** directory and view Gauntlt's defined attacks using **--list**:

   ```
   $ cd gauntlt/examples
   $ gauntlt --list
   ```

2. **Arachni** is "*a feature-full, modular, high-performance Ruby framework aimed towards helping penetration testers and administrators evaluate the security of modern web applications*" (http://www.arachni-scanner.com/). Gauntlt can use Arachni to identify cross-site scripting. Edit **arachni/arachni-xss.attack** using a preferred text editor. Replace **http://scanme.nmap.org** with **http://10.0.2.2:1337** to point the attack at the running Dromedary application.

3. **SSLyze** is "*a Python tool that can analyze the SSL configuration of a server by connecting to it*" (https://github.com/iSECPartners/sslyze). Gauntlt can use SSLyze to prevent anonymous certificates. Edit **sslyze/sslyze.attack** using a preferred text editor. Replace **google.com** with **http://10.0.2.2:1337** to point the attack at the running Dromedary application.

4. **DIRB** aids in professional web auditing (http://dirb.sourceforge.net/about.html). Gauntlt can use DIRB to scan for basic security requirements. Edit **dirb/dirb.attack** using a preferred text editor. Replace **http://localhost:8008** with **http://10.0.2.2:1337** to point the attack at the running Dromedary application.

5. **Network Mapper** (**nmap**) is a security auditing utility tool (https://nmap.org/). Gauntlt can use **nmap** to confirm that an application is available on the correct ports. Edit **nmap/simple.attack** using a preferred text editor. Replace **scanme.nmap.org** with **10.0.2.2** to point the attack at the local network. Replace both instances of "**80**" with "**1337**", to specify "**1337**" as the port being checked.

Run the Four Security Tests and Examine the Output

Run all of the modified **.attack** files using Gauntlt. All four tests should pass with a green font:

```
$ gauntlt arachni/arachni-xss.attack sslyze/sslyze.attack dirb/dirb.attack
nmap/simple.attack
```

Further Reading

Refer to the Gauntlt's "Attack Adapters" section at https://github.com/gauntlt/gauntlt#attack-adapters to learn about further uses of Gauntlt.