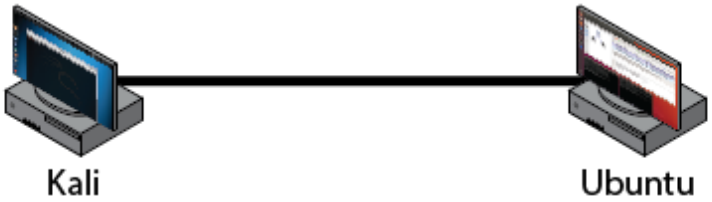
SIT716 Computer Networks and Security

Week 5: Web Vulnerabilities

Below you will find instructions for conducting an experiment designed to explore concepts of networking and/or security. Before referring to the instructions below, make sure you take the time to research and design your own experiment – even if you can't work out everything that is required. After completing your study of this unit, the skills you develop in designing your own experiments will be a critical skill for learning about new network protocols and security attacks, enabling you to work successfully as a valued professional in these fields.



Host	IP Address	Role
Ubuntu	192.168.1.1/24	Victim machine
Kali	192.168.1.2/24	Attacker that will perform a TCP SYN Flood

Outline:

In this lab we will be using Kali to attack an installation of Damn Vulnerable Web Application (DVWA) to highlight HTTP vulnerabilities. DVWA is an excellent web application designed for professionals and students alike to explore penetration tools, vulnerabilities, and varying network attack simulations. It is recommended to explore the DVWA website further at the end of this lab (http://www.dvwa.co.uk/).

There are several tools available that can allow us to expand our virtual test environments to explore varying HTTP vulnerabilities. We will be using Ubuntu to run an instance of DWVA, and executing attacks from Kali with 'httrack' and 'Skipfish'; both of which come pre-installed on Kali.

Instructions:

1. Load VirtualBox, Ubuntu, and Kali as required.
2. Ubuntu will need access to the Internet to install some tools (Docker and DVWA). If you have recently followed the screencast 'Connecting Ubuntu and Kali' then Ubuntu will no longer have access to the Internet. If that is the case, revert the network settings back to 'NAT' in VirtualBox, and 'Automatic' within Ubuntu network settings, to allow Internet connectivity (refer to the screencast for a reminder of what settings to change).
3. Once Internet access is re-acquired, proceed with the following steps to install Docker, and DVWA.

Installing Docker in Ubuntu

Our first task is the installation of Docker within Ubuntu. Docker (https://www.docker.com/) is an open-source technology that allows for applications to be created as a self-sufficient 'container' (similar to packages that you install on Ubuntu). This makes it very easy to deploy applications (especially for large enterprises who need to setup their workstations), and you can run more applications on the same amount of hardware (as containers use less resources than virtual machines hosting the applications), among other benefits. It is becoming widely popular.

We will use Docker to install DWVA (addressed below). The instructions below are derived from the official Docker installation instructions for Ubuntu (https://docs.docker.com/install/linux/docker-ce/ubuntu/#set-up-the-repository).

1. Open up VirtualBox, and run your instance of Ubuntu
2. Open a Terminal. Update the Ubuntu package manager before proceeding:

   ```
   sudo apt-get update
   ```

3. Run the following command to allow `apt` (the Ubuntu Advanced Packaging Tool) to use a repository over HTTPS:

   ```
   sudo apt-get install apt-transport-https ca-certificates curl software-properties-common
   ```

4. Add Docker's official GPG key:

   ```
   curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo apt-key add -
   ```

5. Verify that you now have the key with the fingerprint `9DC8 5822 9FC7 DD38 854A E2D8 8D81 803C 0EBF CD88`, by searching for the last 8 characters of the fingerprint:

   ```
   sudo apt-key fingerprint 0EBFCD88
   ```

6. From the above, you should receive the following output in the terminal. ***Do not type the below in***, just verify that the last 8 characters in the 'Key fingerprint' below match the one in the command above:

   ```
   pub   4096R/0EBFCD88 2017-02-22
         Key fingerprint = 9DC8 5822 9FC7 DD38 854A E2D8 8D81 803C 0EBF CD88
   uid                  Docker Release (CE deb) <docker@docker.com>
   sub   4096R/F273FCD8 2017-02-22
   ```

7. Setup the Docker repository below to the latest stable release by entering the below command in the terminal. Type this on the one line in the terminal (don't purposefully try to add new lines):

```
sudo add-apt-repository "deb [arch=amd64]
https://download.docker.com/linux/ubuntu $(lsb_release -cs) stable"
```

8. With the Docker repository correctly configured with `apt`, prepare for installation with:

```
sudo apt-get update
```

9. Install Docker:

```
sudo apt-get install docker-ce
```

10. Verify installation was complete by running a simple Docker container called "Hello World":

```
sudo docker run hello-world
```

Installing DVWA in Ubuntu

With Docker installed, we can install the Damn Vulnerable Web Application (via a Docker container) quite easily, as it will take care of all the dependencies required (e.g. mySQL).

1. Open a terminal within your Ubuntu instance.
2. Install DVWA with the following command:

```
sudo docker run --rm -it -p 80:80 vulnerables/web-dvwa
```

DVWA should now be installed and running. To access it, open up Firefox and browse to your localhost address. In other words, in the URL toolbar (where you type in URLs), enter in "localhost".

3. Login to DVWA with username ‘admin’ and password ‘password
4. Once logged in, select the ‘Create/Reset Database’

Note: If you reboot your Ubuntu instance, you will need to re-run the above commands to start DVWA again. Also once logged in, don’t forget to click the create/reset database button.

Attacking DVWA with httrack and Skipfish from Kali

Return Ubuntu back to an Internal network (so that Ubuntu and Kali and communicate with each other; refer to the ‘Connect Ubuntu and Kali’ screencast for a reminder if needed). Ensure that they are connected by pinging each other. With DVWA running on Ubuntu, we can now attack it from our Kali instance. Within Kali we will focus on two tools; httrack, and Skipfish.

Httrack allows you to download an entire website onto your local machine, including its HTML pages, images, recursive directories, and so on. Interestingly this is not necessarily considered a ‘hack’, as it is only accessing data and files that are already publicly available (e.g. you are already free to browse the website at will).

Skipfish is a security reconnaissance tool that recursively searches a website to create an interactive map. Also aims to generate a report that assesses and summarises any discovered or suspected web vulnerabilities that the website may have.

We will use both of these tools against our DVWA.

Attacking DVWA with Skipfish

Within Kali, browse to Applications (top left of desktop UI) -> Web Application Analysis-> Skipfish. A terminal will open detailing the range of parameters that can be set. We will keep it basic in this document, however it is strongly recommended that you perform additional research and explore what else Skipfish allows you to do.

1. Within the Skipfish terminal, attack the DVWA with:

```
skipfish -o dvwa -A admin:password http://192.168.1.1
```

the range of the command uses the following parameters:

```
-o: Set the directory where the output will go (in our case, a folder named 'dvwa' in the Home directory)

-A: provide HTTP authentication credentials (allows us to login into DVWA to do a deeper search)
```

2. Browse to the Home directory and open the newly created dvwa folder.
3. Inside will be an index.html file, open it. This contains the Skipfish report. What can you learn from this report?
4. Do some additional research online to learn more about the Skipfish report.

Currently the DVWA's security level is set to 'impossible', meaning that it should be secure against all known vulnerabilities. Let's change it to low and re-run Skipfish to do a comparison.

5. Return to Ubuntu and the running DVWA. Login into DVWA if needed, and browse to 'DVWA Security' in the navigation list. Set the security level in the dropdown list to 'Low'.
6. Re-run Skipfish. You will need to set the directory to a new folder so as to not overwrite the folder you created last time (e.g. -o dvwa_low)
7. Browse to Home -> dvwa_low -> index.html. How does this report compare to the last one you created when the DVWA Security setting was set at Impossible?

Attacking DVWA with httrack

Within Kali, browse to Applications (top left of desktop UI) -> Web Application Analysis-> httrack. A terminal will open detailing the range of parameters that can be set. We will keep it basic in this document, however it is strongly recommended that you perform additional research and explore what else httrack allows you to do.