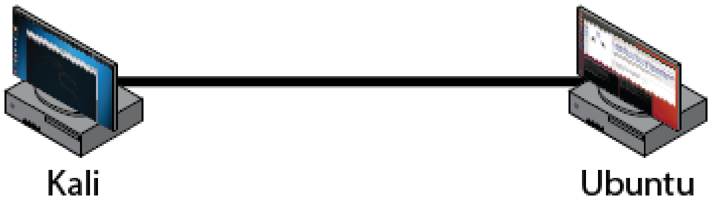
SIT716 Computer Networks and Security

Week 6: User Credentials

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	Passive reconnaissance attacker

Outline:

In this lab we will be using Kali to capture user credentials when logging in to a telnet server and a web application (Damn Vulnerable Web Application/DVWA). If you haven't installed DVWA previously, make sure to refer back to Week 5 for instructions on getting DVWA installed.

There are several tools available in Kali for capturing user credentials. We will be using the Ettercap tool for this purpose, however there are other tools available in Kali that you can substitute for Ettercap and repeat the experiment to learn more. Make sure you take the time to explore and learn what you can!

Instructions:

1. Load VirtualBox, Ubuntu, and Kali as required.
2. Confirm that they Ubuntu and Kali are isolated to the internal network and are connected together correctly by performing a simple `ping` against each other. If this does not work, go back to the Connecting Ubuntu and Kali screencast before continuing.

Using Ettercap to capture passwords

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.

Ettercap is a free and open-source tool to perform man-in-the-middle attacks. We will be using it to sniff the packets being sent as we connect to the DVWA.

1. Within Ubuntu, open a Terminal and startup net utilities:

   ```
   inetutils-inetd
   ```

2. Within the same terminal, start DVWA via Docker:

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

3. Switch over to Kali. Open up a Terminal, and we will open up Ettercap (can also be done from the GUI under the Applications menu):

   ```
   ettercap -G
   ```

4. We need to setup Ettercap for it to sniff the traffic on a particular network interface. In Ettercap, open the Sniff menu, then select the Unified sniffing option
5. In the next dialog, select network interface 'eth0', and click OK.
6. We will establish a Telnet connection into our Ubuntu instance. Open up a new terminal window, and enter in:

   ```
   telnet 192.168.1.1
   ```

7. When prompted, enter in your *Ubuntu* username and password. We are logging in just to verify the connection.
8. Once successfully connected, we have verified the connection, so let's logout again:

   ```
   logout
   ```

9. Within Kali, open Firefox, and browse to your Ubuntu connection (type in 192.168.1.1 in the address bar). When we browse to 192.168.1.1 we are greeted with DVWA, which is being hosted on your Ubuntu's localhost via Apache web server.
10. Login to DVWA (default username is admin, password is password)
11. Bring up Ettercap. Note the output received. You should see the captured username and password that was entered into DVWA.