CS 490 / ECE 492: Embedded Systems Security

Learning Linux Tools #01

Total Points: 100

Assigned Date : Wednesday, 13 January 2016
Due Date : Wednesday, January 20, 2016 @ 01:14:59 p.m.

1 Reading

Read Chapters 2 & 3 in the Molloy textbook.

2 Flashing Your BeagleBone

Flash your BeagleBone with the latest Debian image (Debian 7.9) from the BeagleBone website `http://beagleboard.org/latest-images`. There are a few SD cards available (just talk to one of us), but you will need a laptop (that has a SD card reader).

3 Learn Linux Command Line Tools

To Be Done Individually

To gain proficiency in using the Linux shell, develop 10 complex, custom shell commands on your BeagleBone Green. List each command, as well as a description of what the command does.

4 Get the BeagleBone on the Internet

When the BeagleBone is connected through USB, by default it only has a connection through USB, and by default this connection is only between itself and your desktop. Figure out how to configure the BeagleBone and your desktop so that the BeagleBone can access the Internet through the USB connection to your desktop. Successful completion of this portion will be a demonstration of Internet connectivity through the BB (ie. pinging Google).

5 Introduction to Security Tools

To Be Done Individually

5.1 Packet Sniffers

Packet sniffers are very commonly used to observe network traffic for a wide variety of reasons, some legitimate (like network debugging) and some nefarious (looking for unencrypted usernames/passwords). Use *tcpdump* to capture web traffic. With tcpdump running, browse to Dr. Gamage's or Dr. York's website. Output the capture to both the console and to a file (hint: *tee* command). Copy the dumped file over to your desktop. Open the dump in Wireshark and observe the traffic. As root, run Wireshark on your desktop and capture traffic to a website running https (Google, SIUE webmail, etc.). Observe the differences. Become comfortable with using both tcpdump (console) and Wireshark (GUI). A successful assignment/demo will show proficiency with both tools.

5.2 Port Scanners

One of the first steps in attempting to gain unauthorized access to systems is through the use of port scanning. *nmap* is a very well used tool for this purpose. For the assignment, check the nmap man page and figure out some of the capabilities of it. Using nmap, you should attempt to ping scan the entire lab to see if you can get a list of all present IP addresses. Once you have identified IP addresses within the lab space, you should attempt to port scan them to see which, if any services, the systems are running. You should also attempt to use some of the fingerprinting techniques within nmap to ID the operating system of your target.