CSCI 530 Lab 7

Intrusion Detection Systems
Date Assigned: 3/5
Date Due: 3/19

Overview:

In this lab, students begin to understand the uses of intrusion detection systems and there uses in the protection of a network. They will install an open source IDS and understand the make up of the system and the different features it can provide.

Instructions:

1. Download EagleX at http://www.engagesecurity.com/downloads/#eaglex
    a. Select Eagle X version 2.1
    b. Select Save executable to desktop.
    c. Double Click on zip file that you downloaded called eablexv21.zip
    d. Launch setup.exe

2. In the Configuration Wizard:
    a. Click yes to install Eagle X.
    b. Click Next in wizard setup.
    c. Click Next in selecting destination directory.
    d. Click Next in selecting start menu folder.
    e. Click Next in selecting additional tasks.
    f. Click Next in Ready to install.

3. Next you will install WinPcap 3.0
    a. Click Next
    b. Agree to liscence agreement and then click next.
    c. If you are prompted with a version conflict menu, just click yes to all.
    d. Click Next on the Readme Information window.
    e. Click Ok.
4. Click Next and then Finish to finish out the instillation of Eagle X.

5. Configuring Eagle X
    a. In DNS/IP enter your ip. You can find your ip by going to start→run, and entering cmd. At the command prompt, enter the command *ipconfig*. Your ip will start with 192.168.0.x, where x will be different for every machine.
    b. In Port enter 8877
    c. Administrator email, enter your email.

   d. In username and password, enter in anything but **remember** the information.
   e. For Home Network, enter your ip/32, so if your ip is 192.168.0.169, enter 192.168.0.169/32
   f. Primary and Secondary DNS Servers are 192.168.0.1
   g. Click on update button.
   h. Click Setup
6. If install was successful you should be notified. The program will launch in the tool bar in the bottom right as a black orb.
7. Double click on the orb.
8. Next in the tabs on the right click on wizard.
   a. Click on Rules/ Signatures and mark the check boxes for all rules
   b. Click on Preprocessors and check Keep session statistics and detect state problems.
   c. Still in Preprocessors, uncheck disable evasion alerts.
   d. Still in Preprocessors, click on the tab protscan detection
      i. Check the Portscan Detection box'
      ii. In the drop down menu Monitored host/networks select $HOME_NET.
9. Get into partners and one of you download NMAP.
   a. http://insecure.org/nmap/download.html
   b. The link is farther down the page. You want to download the Latest Stable version labeled nmap-4.11-setup.exe.
   c. Save NMap to disk
   d. Launch a cmd window and get to the NMap program
   e. One partner run the command nmap –sS –v <ip address>
10. The partner being port scanned; turn off windows firewall and Symantec Antivirus.
11. Also the partner being port scanned, turn off snort. There is a button in the top left corner of the IDScenter window to stop and start snort.
12. Once snort is stopped. the partner with NMap ping your partner and run a port scan in the command window with this command: nmap –sS –v <ip address>. View the results.
13. Now turn on snort.
14. In the IDScenter window, click on view alters and input the username and password that you set earlier.
15. As your partner port scans and pings, keep clicking go at the top of the window in view alerts. You will see the IDS recognize it being port scanned.

Assignment:

Perform the lab and answer any questions asked in the lab and include them with these questions below:

1. Give one example where you would not want an IDS running within your network?

2. Go back to wizard -> Rules/Signatures and select one of the rule-paths by double clicking on them. Select 4 rules under one rule path and explain the information given about them and why they are necessary?