Snort-EagleX Laboratory – Module 13 Intrusion Detection Systems (IDS)

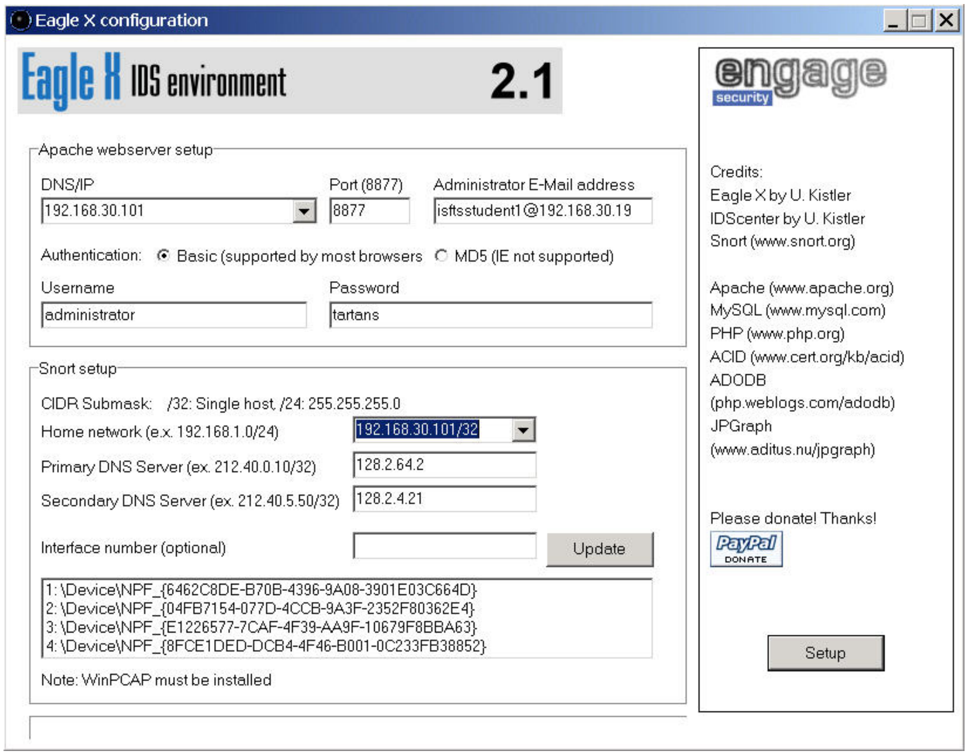
Background: This Lab reinforces the concepts of network-based IDS by requiring the student to complete the configuration of a snort-based freeware IDS called EagleX.

Requirements/assumptions:

- Windows 2000 Professional
- Local administrative privileges
- EagleX application (http://www.engagesecurity.com/downloads/#eaglex)

Install EagleX

1. Open the **InfoSec Course Share\Tools\EagleX** folder located on your Desktop (note: it is also available for download in the apps share of the 192.168.30.250 class server)
2. Double Click the EagleX Setup file: [Setup.exe]
3. Click Yes at the prompt to start the Setup Wizard
4. Accept all of the defaults in the Wizard and then click the Install button
5. When prompted to install WinPcap, cancel out of its install routine (it's already loaded on your system)
6. Review the Setup-EagleX Information dialogue and then click Next.
7. At the next dialogue box, click Finish
8. The will appear along with the EagleX readme file
9. Review the Readme.txt file and then close it
10. At the EagleX Configuration Screen, Apache webserver setup…
11. Click the drop down menu next to DNS/IP and select your system's IP address



Eagle X configuration

Eagle X IDS environment 2.1

Apache webserver setup

DNS/IP: 192.168.30.101

Port (8877): 8877

Administrator E-Mail address: isftsstudent1@192.168.30.19

Authentication: ● Basic (supported by most browsers ○ MD5 (IE not supported)

Username: administrator

Password: tartans

Snort setup

CIDR Submask: /32: Single host, /24: 255.255.255.0

Home network (e.x. 192.168.1.0/24): 192.168.30.101/32

Primary DNS Server (ex. 212.40.0.10/32): 128.2.64.2

Secondary DNS Server (ex. 212.40.5.50/32): 128.2.4.21

Interface number (optional):

```
1: \Device\NPF_{6462C8DE-B70B-4396-9A08-3901E03C664D}
2: \Device\NPF_{04FB7154-077D-4CCB-9A3F-2352F80362E4}
3: \Device\NPF_{E1226577-7CAF-4F39-AA9F-10679F8BBA63}
4: \Device\NPF_{8FCE1DED-DCB4-4F46-B001-0C233FB38852}
```

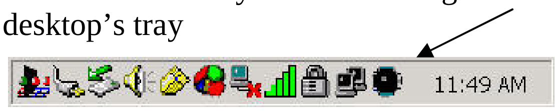
Note: WinPCAP must be installed

Credits:
Eagle X by U. Kistler
IDScenter by U. Kistler
Snort (www.snort.org)

Apache (www.apache.org)
MySQL (www.mysql.com)
PHP (www.php.org)
ACID (www.cert.org/kb/acid)
ADODB
(php.weblogs.com/adodb)
JPGraph
(www.aditus.nu/jpgraph)

Please donate! Thanks!

12. Type port 8877 in the Port box
13. Type your ISFTS class email address (i.e. isftsstudent1@192.168.30.19)
14. Insert administrator and tartans in the Username and Password boxes
15. Under Snort Setup, type your IP address with a 32 bit prefix in the Home Network Box (i.e. 192.168.30.101/32
16. Type in your primary and secondary DNS Server's IP address in the appropriate boxes
17. If you have more than 1 network interface card, select it from the list of devices at the bottom of the screen and click update (this is optional)
18. Now click the Setup button
19. After EagleX is installed, you can Launch it by double clicking the black circular IDSCenter icon in the your desktop's tray



20. You can interface with the EagleX tool via the IDSCenter GUI.
21. Now, click the View Alerts button at the top of screen
22. Login with administrator and tartans
23. This brings up the Analysis Console for Intrusion Databases (ACID) web interface
24. Now open your Languard Network Scanner and run a scan against your partner's IP address and vice versa
25. Take a look at your ACID display. You should see some alerts as a result of your scanning activity.
26. Feel free to explore some of the capabilities of ACID and IDSCenter on your own