University of Pittsburgh
School of Information Science

IS2820/TEL 2813 - Security Management

Lab Assignment # 3
Intrusion Detection/Prevention Operation and Analysis

Lab GSA: Carlos Caicedo

I. Lab resources for this assignment

Network Sensor – CISCO IPS 4240 Series (IPS 1)
2 Windows 2000 PCs (PC 1 and PC 2)
1 Linux PC (PC 8)

II. Preliminary questions

1. What is the difference between intrusion detection and intrusion prevention?

2. While a packet filter typically looks at packets one at a time, an IDS/IPS is capable of looking at an entire stream of packets. What advantages does this present?

III. Lab objective

The network structure of this lab appears in figure 1 below. All computers shown have the IP addresses displayed. PC 2 is configured as an FTP server.

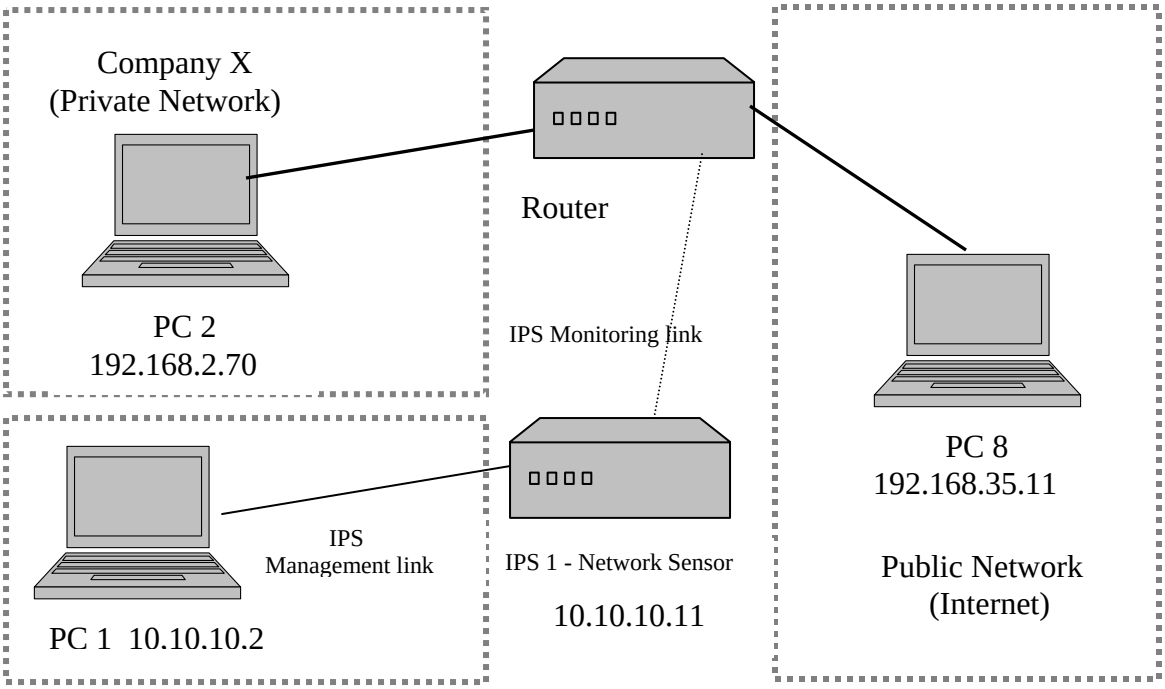

Figure 1

You must detect and/or log network traffic coming from the public (outside) network to the private (inside network) according to the requirements below:

Part A:

1. Run Snort (PC 2) so that it displays incoming packets to the screen and send four pings from PC 8 to PC 2. Take note of the packet statistics recorded by Snort.
2. Run Snort so that it logs packets to a file and records only incoming FTP traffic. You must start the FTP server (see previous lab) before starting Snort. You will need to create a Snort rule and reference it within your Snort configuration file (more on this later). Attempt FTP session from PC 8 to PC 2 using the anonymous account.
3. Repeat the above procedure only change your rule to record nmap X-mas scan activity. Scan PC 2 from PC 8 using an nmap X-mas scan (you will need to determine what flags to use for an X-mas scan).
4. Run Snort so that is detects and logs incoming FTP traffic that is fragmented. You will repeat procedure 2 above, however, you must fragment all outgoing traffic from PC 8. You can do this using a tool called fragroute (installed on PC 8). You will need to read the man page for fragroute or research how to use this tool in order to learn how to fragment outgoing traffic.

Part B:

- Configure the network sensor so that it records ICMP traffic only from PC 8. You will need to use the Cisco IDM software and the Cisco IDS Event Monitor. Send several pings from PC 8 to the network sensor IP address.

Satisfaction of these requirements can be approved by satisfying the following criteria:

Compliance Criteria for Part A:

1. Pings from PC 8 should register on PC 2's display while Snort is running.
2. The log file for this step should only show FTP packets that were captured.
3. The log file for this step should only show packets that were generated by the nmap X-mas scan.
4. The log file should still record the FTP traffic only even though the packets were fragmented.

Compliance Criteria for Part B:

1. The network sensor should only record ICMP traffic generated from PC 8. No other alerts should be generated.

IV. Technical details

Address pools:

Company's X public address pool for its network is 192.168.2.0 with a netmask of 255.255.255.0
The public address pool for the linux network is 192.168.35.0 with a netmask of 255.255.255.0

Running Snort

Snort is run from the command line (it is located on the D: drive on PC 2) by typing *snort* followed by the appropriate flags (you must run it from the bin directory). Whenever you want to stop Snort just type *CTRL-C*. When you begin logging packets, you must specify the path of where you want the log file saved. You must also reference a snort configuration file (one that you create, not the default one). Your configuration file must reference any rules that you create. Your rules should be saved in the *rules* directory and your configuration file should be saved in the *etc* directory. Make sure you define the variables for your local network and the external network in your configuration file. Below are some links where you can find more information about Snort. The second link has an example of a configuration file. Please note, the file you create will only contain about five lines (however, you can get some ideas from this example file).

http://www.freeos.com/articles/3496/
http://www.bleedingsnort.com/snort.conf/snort.conf-small.txt
http://www.snort.org

Cisco Network Sensor

You must connect the blue serial cable from PC 1 to the network sensor appliance (IPS 1)

In order to connect to the network sensor from PC 1, open up Internet Explorer on PC 1 and type in the following URL: https://10.10.10.11 (username is **cisco** and password is

seclab1). Click "OK" to all pop-up messages that pertain to accepting certificates. Most of the configuration of the sensor will be accomplished through the **Configuration** tab (then select Sensing Engine).

Login for Windows machines:
The username for both PC 1 and PC 2 is **seclab** and the password is **seclab1**.

Login for Linux machine:
The username is root and the password is seclab1.

V. Lab Report:

The lab report for this assignment should include:

1. Answers to the questions posted in the *Preliminary Questions* section of this assignment.
2. Screenshots or copies of any configuration files and rules that you create for Snort.
3. Screenshot or copy of a log file from step two and three for the Snort portion of the lab.
4. Evidence that the fragmented traffic was still recorded (step 4 of Snort lab). This might include a copy/screenshot of your log file and from this step as well as some proof the packets were fragmented (you could use ethereal on PC 2 to capture incoming fragmented packets and then take a screenshot of the packet details of a single fragmented packet).
5. A screenshot of the ICMP alerts that are displayed in the IDM software (the only alerts that should appear are the ones that you have configured the network sensor to detect- i.e. no random alerts should be displayed).