In the name of God

Sharif University of Technology
Department of Computer Engineering

CE 817: Advanced Network Security

Mehdi Kharrazi *Day 1^{st}, 1394*

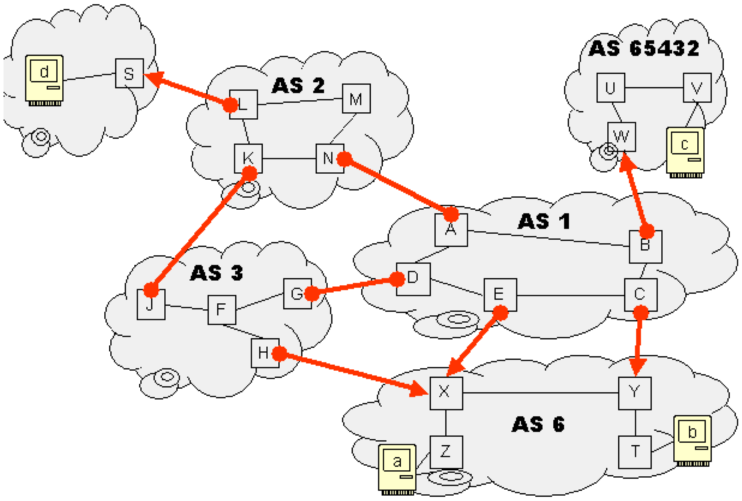
Homework 4

Please email your answers/report in **PDF format** TO “kharrazi@sharif.edu” and CC “masalehi@ce.sharif.edu” and “masoudian@ce.sharif.edu”. The HW file name should be **“Your Lastname-817- HW-4”**. Also the same title should be used as the subject of your email. Please follow the formatting. This homework is due by **Dey 12th, 11:59 PM**. Also, you will have a face-to- face delivery, the time of which will be announced later.

Report what you write down should be your own words, analysis, reasons and results in approximately 20 pages with maximum size of 2MB (Try to include text result or reduce screenshot size included in your report.). There will be a zero tolerance policy for cheating/copying HWs.

Part I: Theoretical

Consider the following network [1]:



- AS1, AS2, and AS3 are ISPs, peering with each other at the links between routers J-K, N-A, and D-G.
- AS6 is a customer of AS1 and AS3. Two more customer networks are shown.
- All routers are shown. All links between routers are shown. All networks are running OSPF as their IGP, and all link costs are equal.
- All providers are running I-BGP.

[1] This part of homework is retrieved from ”http://www1.cs.columbia.edu/ ji/F02”

- The prefix for AS6 is 12.2.0.0/16. The prefix for AS65432 is 135.207.16.0/20. The prefix for the nameless customer containing router S and host d is 192.20.225.0/24.
- AS1, AS2, and AS3 number their routers out of 1.0.0.0/8, 2.0.0.0/8, and 3.0.0.0/8, respectively. The loopback address of each router has the ascii value of the letter given in the figure as its last octet. For example, router G is 3.0.0.71.

1. What path (list of routers they go through) does traffic from host c to host d follow?
2. What path does traffic from host d to host c follow?
3. Suppose that AS6 announces its entire prefix out of both X and Y, and that it receives full BGP tables from its providers. What is the path from a to b? From a to c? From a to d? From c to a? From d to a?
4. Now suppose that AS6 announces the lower half of its address space (12.2.0.0/17) from the X-E link, and the upper half from the Y-C link. Let a's IP address be 12.2.33.65, and b's IP address be 12.2.192.66. What is the path from a to b? From a to c? From a to d? From c to a? From d to a?
5. What is undesirable about the flow of traffic in the previous question? Give two different ways to fix it.
6. How would AS6 tell the world that it prefers receiving traffic for the upper half of its address space only via the C-Y link, unless of course it is broken? List just the obvious way. For extra credit, define some communities, and make sure that traffic to the upper half only flows through the C-Y link.

Part II: Practical

Snort

Snort is one of the famous network based intrusion detection systems. In this section, you are supposed to get familiar with this tool and its capabilities. Therefore, you will be asked to write some rules and test them. Also, you are given a Virtual Machine image which you should analyze the services on it. Answer the following questions and prepare screenshots if necessary. Attach the rules and exploit code as a separate file to your homework too.

1. Get familiar with snort and its commands.
2. How many operation modes does Snort have? Explain each mode briefly.
3. Write Snort rules for the following requirement
   - Log all HTTP message containing the word sharif in it.
   - Log packets coming from outside Home Network.
   - Log all DNS packets.
   - Alert if any packet has size greater than 300 and destined to port 80.
   - Alert if any packet contains the string ”CE817”.
4. Now download and install the virtual machine image available at the course website. Install Snort on the machine and start it.
5. There is a vulnerable OpenSSL service in the virtual machine. Can you find the famous vulnerability of this version? Describe the vulnerability briefly and the possible ways to fix it.
6. Then, write a bash/python script or C/java program, exploit the vulnerability and extract memory contents(The output should be a hex dump of 64KB buffer).
7. Write a snort rule to detect if this vulnerability has been exploited. Test the accuracy of your rule.

Wireless Security

In this section of the homework, you are given a cap file that contains wireless traffics in a location. you should analyze the packets and answer the following questions:

1. Enumerate access points in that location and report SSIDs, MAC addresses and cryptography protocols of them.
2. Enumerate clients in that location and report MAC addresses of them.
3. Extract the relationships between clients and APs and report which clients connects to which APs.

Consider following criminal story:

Two guilty person want to meet each other in a location. So one of them sends other person the meeting location. Fortunately police could capture the network traffic of them for identifying meeting location.

Now:

1. What is the attack scenario used by police to capture this traffic. Describe that in details.
2. Crack this traffic and identify meeting location.