CSC4222/6222: HW2

Programming Part

Due at 23:50 pm, Oct. 1st

I. Symmetric Cryptosystem

In this programming Assignment, students are asked to implement a toy symmetric cryptosystem based on the following method.

a. Keys are 16-bit randomly generated values
b. Messages are randomly generated strings with an even number of characters (Valid characters are upper and lower-case letters)
c. The encryption of a message M of length n (in bytes) is given by

$$\mathrm{E_k}(M) = M \oplus (K||K||K \dots),$$

Where the key K is represented n/2 times and "||" means String Concatenation Operator.

d. The decryption algorithm for a ciphertext C is the same as the encryption algorithm:

$$\mathrm{D_k}(C) = C \oplus (K||K||K \dots).$$

Students need to implement a brutal force decryption attack for this cryptosystem and test it on randomly generated English character message.

Requirement:

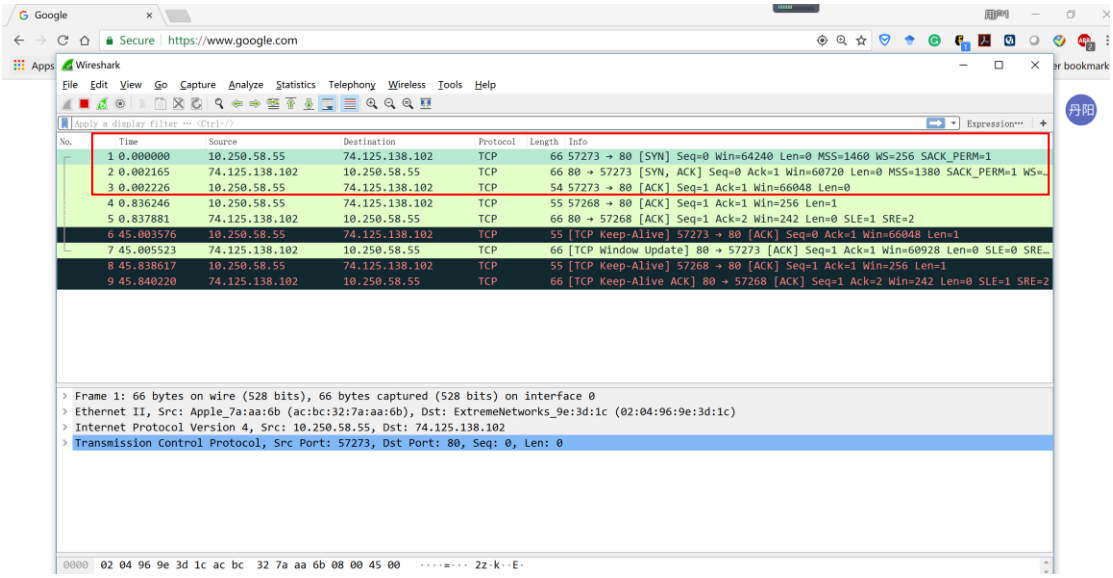
1. You can use Java or Python programming language to finish this assignment and follow the given Structure.
2. Your work is expected to be runnable. Any program has error or exception will receive 0 as grade.
3. A copied program will receive 0 as grade.

II. Wireshark

1. Use Wireshark to monitor the TCP to capture packets showing the TCP shaking hands process.

Step1: Download wireshark at https://www.wireshark.org/.

Step2: For example, use capture function to capture packets that specify the hand shaking process.



Requirement:

a. Student firstly needs to figure out the IP address of the cs.gsu.edu.

   Then, students are required to use wireshark to capture the TCP shake hands process packets as aforementioned.

b. Instead of the screenshot, student needs to upload xxxx.pcapng file (.pcapng file can be acquired from wireshark).

c. Specifically, students with same IP address will be regarded as copied work and get 0 as grade.

III. Intrusion Detection

In this problem, you will write a simple intrusion detection system to detect potential attacks or dangerous behavior in network activity. Attached includes two pcaps with example attacks:

1. arpspoofing.pcap includes an ARP spoof attack. IP address 192.168.0.100 advertises the wrong MAC address for 192.168.0.1.

2. portscan.pcap includes a TCP SYN port scan (**This is for CSc 6222 only**).

Your job is to write a software IDS executable (in Java) or script (in Python) that takes as input a pcap trace and looks for such malicious behavior. The local network you are protecting is configured with two machines (192.168.0.100 with MAC address 7c:d1:c3:94:9e:b8 and 192.168.0.103 with MAC address d8:96:95:01:a5:c9) and a router (192.168.0.1 with MAC address f8:1a:67:cd:57:6e).

Your scanner should:

1. Detect ARP spoofing attempts. Output a warning including the offending MAC address and the packet number of the offending packet.

2. Detect port scans. A port scan is defined to occur whenever TCP SYNs or UDP packets are sent to a 100 or more different ports on a target system. The scanner should output a warning including the offending source IP address, the victim destination IP address, and the offending packet numbers.

Your program should take as input the filename of a pcap file that contains captured network packets. The output of your program will be the warning messages as described above. The format of your result is free but it should be

clear to the user. You should use either Java or Python. Check that your scanner runs properly on the mumble machines before turning it in. The sample pcap files can be used to test your scanner. We will also test your scanner on fresh pcaps we generate that include other non-malicious behaviors, as well as boundary conditions.

.