CSC427 Tutorial

Submission

Requirements

A single `wireshark.zip` file.
`answers.txt` — written answers.
`q1.pcap` — pcap file that can be opened by Wireshark.
`*q2_[domain name].[jpg|png]` — image of insecure data going to `[domain name]` (VM).
`*q3_[domain name].[jpg|png]` — image of insecure data going to `[domain name]` (real).
`q4.[jpg|png]` — image of plaintext credentials.
`q5b.[jpg|png]` — image of plaintext credentials.

* = multiple files of this form expected (for questions 2 and 3).

Structure

```
wireshark.zip
├─── answers.txt
├─── q1.pcap
├─── q2_[domain name].[jpg|png]
├─── q3_[domain name].[jpg|png]
├─── q4.[jpg|png]
└─── q5b.[jpg|png]
```

Example

```
wireshark.zip
├─── answers.txt
├─── q1.pcap
├─── q2_am-i-secure.com.png
├─── q2_most-secure.com.png
├─── q2_really-secure.com.png
├─── q2_super-secure.com.png
├─── q3_techpanda.org.png
├─── q3_notsecure.com.png
├─── q3_sendpasswords.com.png
├─── q4.png
└─── q5b.png
```

Tasks

Copy the VM to your virtual folder:

scp -r UTORID@dh2020pc02:/virtual/wireshark /virtual/UTORID

To set up the servers: **(after questions 1, 5, 6, 7)**

- Do “ip address” in the server VM’s terminal (has .pcap on desktop)
- Do “vi /etc/hosts” in the client VM’s terminal (doesn’t have .pcap on desktop)
- Replace all 172 ips with the ip from the server VM in the hosts file

START WITH QUESTIONS 1, 5, 6, 7. Pcap file available on the server desktop.

Note: Linux provides a screenshot application. Wireshark should only be running on the client vm.

Online Traffic

1. Start a capture and browse some sites.
   Submit a pcap file containing only GET requests on tcp port 80.

Website Security

2. On the client, open the websites hosted on the server VMs by going to csc427-tutorial.com.
   Are the sites secure? Write your answer in `answers.txt` and provide screenshots of plaintext traffic as seen by Wireshark, if it is available.
3. Find two sites that are insecure and provide fake credentials. You may use techpanda.org as one of them. Submit screenshots of plaintext credentials captured by Wireshark.

Wireshark SSL Decryption

4. `key.key` contains the private key to the vm websites. Give the to Wireshark to decrypt HTTPS traffic. Submit a screenshot of plaintext credentials sent to one of these sites.

Open the premade capture and provide answers to questions 5-7 in `answers.txt`.

Display Filters

5. Select an HTTP packet and isolate all packets that are associated with it (right click the packet and set the conversation filter to tcp)
   a. Describe the TCP handshake that takes place in the first few packets that occur between the client and host.
   b. Screenshot a Flow Graph (in the Statistics Tab) for just the tcp connection observed. The graph shows the exchange in a more visual way.
   c. Describe how the connection is terminated

6. Filter for all reset packets (packets colored red in the list).
    a. What is common between all reset packets received?
    b. When is a reset packet sent in a normal exchange?
    c. Search the term “TCP reset attack” and describe it in your own words.
    d. Does it appear that this type of attack has been observed in our file?

Statistics

7. Go to the statistics tab and select I/O graph.
    a. Observe the largest peak on the graph.
    b. Find the data in wireshark by determining at what time the packets were sent based on the graph.
    c. What protocol is used by the packets in this big spike?
    d. What is the likely cause of this increase in traffic.