COMP 3134

Introduction to Cyber Security

Objective:

Exemplify Passive sniffing techniques on both your droplet server and localhost machine.
All information does NOT need to come from one droplet and/or one local machine.

Task 1: 2 marks

Start a packet capture for 2 minutes while browsing a non-sensitive website. A non-sensitive website is a website where you do not log into.

Apply a filter to show only HTTP or DNS traffic. Submit a screenshot **(1 mark)**

Identify and extract the source IP, destination IP, and protocol from one captured packet. Submit a screenshot of the filtered capture with annotations. **(1 marks)**

Task 2: 5 marks

Use Wireshark to capture unencrypted traffic on your laptop/desktop localhost network. Submit a screenshot **(1 mark)**

Identify a plaintext credential or request (e.g., an HTTP login or an unencrypted message). Submit a screenshot of that captured data and describe what was exposed **(2 marks)**

Explain how encryption would prevent this exposure by writing a paragraph-long answer in a .txt file **(2 marks)**

Task 3: 3 marks

Navigate to your droplet and block all http traffic to your droplet. Submit the screenshot of the commands to execute to add and apply the firewall rule. **(2 marks)**

Open any navigator and confirm that no traffic is being allowed to your droplet. Submit a screenshot that shows both your IP address and the browser response. **(1 mark)**

Task 4: 5 marks

Using the command-line on your local machine's local host, run the command to show your ARP table. Submit a screenshot that shows the command and the output of the command. **(2 marks)**

Using Wireshark, show all ARP traffic of your local machine's localhost. Submit a screenshot. (**1 mark**)

Explain how you would mitigate ARP spoofing attacks by writing a paragraph-long answer in a .txt file **(2 marks)**

Submission Guideline:

- Submit all files individually.
- There should be 2 text files and 6 image files, totaling 8 files.
- Add one more .txt file that outlines all group members, including yourself (first name, last name & student ID).
    - Each member should be written on one line.
        - If there is 1 group member, the file should only contain one line.
        - If there are 5 group members, the file should contain five lines.
    - Add this .txt file even if you are working individually.
- Only 1 team member should submit.
- Do not submit a zip file.