Lab 5: Wireshark

In this lab, we are going to use a packet capture and analyzer program, called Wireshark. The following software are required:

- Metasploitable linux machine (Victim)
- Kali linux (attacker)
- Wireshark
- VBox
- A single virtual network that hosts both the victim and the attacker platforms

Lab requirements:

1. Both the victim and the kali linux must be connect to the internet
2. Start Wireshark on kali linux (attacker) to capture the victim machine packets. Select the tool from the “top Ten Security Tools” menu, or just type the following command in a terminal:
   
   ```
   root@kali:~#wireshark &
   ```
3. Login into the victim machine (Metasploitable), use a preinstalled web browser to access the Web.
4. Search for a three web site that enable unsecure user authentication based on http protocol.
5. Create a dummy account on the vulnerable website and try to login in with the security credentials you have enter during registration.
6. Capture all TCPs, UDPs, and http POSTs packets that are sent from the victim machine.
7. Capture all TCPs, UDPs, and http POSTs packets that are received by the victim machine.

Deliverables:

Submit a report describes each of the following:

- Analyze all TCPs, UDPs. Graph the percentages of TCPs and UDPs that are transmitted from the victim machine during a 3 minute duration.
- Locate any http packets that might contain authentication parameters (user name and password).
- What will be the content of the captured authentication parameters?