**Section 1, Step 19** – Take a Screenshot of the Terminal windows showing the number of packets captured by the *tcpdump* utility.

A screenshot of a computer

Description automatically generated**Section 2, Step 6** – Take a Screenshot of the Wireshark window with the filtered view for SMB network traffic.

A screenshot of a computer

Description automatically generated**Section 2, Step 7** – Take a Screenshot of the Wireshark window with the filtered view for HTTP network traffic.

A screenshot of a computer

Description automatically generated

**Questions**

1. How could an attacker utilize this captured traffic to prepare for and instigate an attack on the network (or the devices on the network)? The attacker could use the SMB traffic for file server traffic and credentials. Windows File Servers will use SMB traffic, an attacker could take advantage of that. With the HTTP traffic, this can include domain names, logins, or cookies/sessions that attacker could hijack.
2. *tcpdump* was run on and captured traffic generated by the Kali machine on that local network – Could the Kali machine have “sniffed” traffic generated by the OWASP BWA machine to another server also in the DMZ network? Why or why not? (Hint: it may help to look back at the pod topology at the beginning of the lab document) The answer depends on if traffic between devices is allowed to be seen by default. Similar to how a public Wi-Fi network will use protocols to restrict devices from talking to each other on that network.
3. Provide two distinct defenses that can be used to defeat “sniffing” – AND indicate at least one technique for each you may use as an attacker to sidestep or defeat those protections. Encrypting traffic between endpoints would be a good defense against “sniffing” techniques. However, a man in the middle attack, where the attacker is sniffing the packets before it is encrypted, could be a way around this. Another technique for stopping “sniffing” attacks would be to implement proper network segmentation using VLANs. An attacker could try to use a form of spoofing to jump across VLANs, but this is difficult.