# CYB 400 Module Two Lab Worksheet

Complete this worksheet by replacing the bracketed phrases in the Response column with the relevant information.

| **Lab: Examining Wireless Networks** | |
| --- | --- |
| **Prompt** | **Response** |
| In the lab “Parsing Object From Traffic,” **Steps 4 and 5**, add your initials at the beginning of the filename (for example, KSMsteph.jpg and KSMcurry.jpg). After closing the Wireshark HTTP object list window, minimize Wireshark and take a screenshot of the two files (\*\*\*steph.jpg and \*\*\*curry.jpg) saved to the desktop. |  |
| In the lab “Parsing Object from Traffic,” **Step 10,** name the file using your initials followed by the number 1.pdf (for example, KSM1.pdf) and save it to the desktop. Take a screenshot of the desktop in Step 14 showing the PDF file. |  |
| What is the significance of being able to parse information from the HTTP stream? | Being able to parse information from a HTTP stream is it can let you know more information about the host. Such as what websites they are visiting. |
| What is the significance of being able to parse information from the FTP stream? | Being able to parse information from an FTP stream can allow you to find information easier and organize your information better on your desktop. You can see what files have been made and can save them to whatever part of your hard drive you want for later use. |

| **Lab: Deep Dive in Packet Analysis – Using Wireshark and Network Miner** | |
| --- | --- |
| **Prompt** | **Response** |
| What is the significance of understanding how to decipher different protocol traffic? | The significance of being able to decipher different protocol traffic is it makes you more efficient at finding what you need from the resource. Also, it allows you to filter to a specific message. |
| What is the significance of understanding the function of specific protocol port numbers? | The significance of understanding the function of specific port numbers is helping you to know which port number you need to filter through a list of results from a flow of TCP stream. |

| **Lab: Vulnerability Scanning of a Linux Target** | |
| --- | --- |
| **Prompt** | **Response** |
| In the lab “Scanning the Network for Vulnerable Systems – Scanning the network using Nmap,” **Step 23**,take a screenshot of the output after scanning the IP protocols. |  |
| In the lab “Scanning the Network for Vulnerable Systems – Scanning the Network Using Zenmap,” **Step 5**,take a screenshot of the output after running a ping scan on the 192.168.1.0/24 network. |  |
| In the lab “Scanning the Network for Vulnerable Systems – Scanning the Network Using Zenmap,” **Step 16**,take a screenshot of the output of the differences between the two scans. |  |
| In the lab “Scanning the Network Using OpenVAS – Scanning with OpenVAS,” **Step 15**,take a screenshot of the results after opening the SecInfo Management menu and opening the CVE’s window. |  |
| In the lab “Scanning the Network Using OpenVAS – Create New Target,” **Step 8**,take a screenshot of the results showing the newly created Ubuntu target. |  |
| In the lab “Scanning the Network Using OpenVAS – Create New User,” **Step 10**,take a screenshot of the window showing the new user, Analyst1. |  |
| In the lab “Scanning the Network Using OpenVAS – Create New Schedule,” **Step 9**,take a screenshot of the window showing the new scan scheduled for Ubuntu discovery. |  |
| In the lab “Scanning the Network Using OpenVAS – Analyzing the Scan Report,” **Step 5**,take a screenshot of the scan results for 10.1.1.10 showing the vulnerabilities. |  |
| Several different switches were used when running the nmap command in the lab. Pick three different switches and explain the functionality of each one. | **Nmap –sP IP address**. This will allow you to see live hosts on a network.  **Nmap –v –sP –spoof-mac 0 IP address**. This does a ping scan while spoofing your mac address at the same time.  **Nmap –sO IP address**. This allows you to see what protocols are supported by the host in the scanning process. |
| What is the difference in functionality between the use of nmap and the use of OpenVAS? | According to (Ask Ubuntu, 2023) OpenVAS looks for unknown vulnerabilities by using different sources with numerous attacks. As for Nmap you need to know what you're looking for and where to look in order for the tool to be used effectively.  Reference  Ask Ubuntu. (2023). *Vulnerability Scanner, nmap vs Nessus*. Ask Ubuntu. <https://askubuntu.com/questions/12434/vulnerability-scanner-nmap-vs-nessus> |