# CYB 310 Module Four Lab Worksheet

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

**Lab: Identifying & Analyzing Network Host Intrusion Detection System Alerts**

| **Prompt** | **Response** |
| --- | --- |
| In the lab, “Analyzing Network Events Using Snorby,” **Step 18,** take a screenshot of the alert window showing signature information and TCP header information. | A screenshot of a computer  Description automatically generated |
| In the lab section, “Network Security Monitoring with Squert,” in the lab, “Analyzing Network Events Using Squert,” **Step 11,** take a screenshot of the Squert window displaying filtered scans for ip 203.0.113.2. | A screenshot of a computer  Description automatically generated |
| In the lab section, “Network Security Monitoring with Squert,” in the lab, “Analyzing Network Events Using Squert,” **Step 17,** take a screenshot of the Squert window displaying no results when filtering events for ip 10.1.1.10. | A screenshot of a computer  Description automatically generated |
| There are a variety of network analyzers. Which tool did you feel was the most powerful and easiest to use? | Snorby stands out as the most powerful and easiest to use among the network analyzers I used. Its user interface is straightforward, making tracking and analyzing network events simpler. This ease of use, combined with its comprehensive data visualization capabilities, allows for quicker analysis of complex network data, enhancing my ability to swiftly identify and respond to network anomalies. |
| Why is it important to add network analyzer tools to your cybersecurity analyst skill set? | Network analyzer tools are crucial in cybersecurity. They help with monitoring and analysis of network traffic to detect and respond to potential threats and intrusions. By understanding the data flow through a network, I can identify unusual patterns that may indicate a security breach, ensuring proactive threat management. These tools are valuable for maintaining network integrity and security. |
| How will you use network analyzer tools in a professional manner? | In my professional role, I plan to utilize network analyzer tools to continuously monitor network traffic, ensuring all communications are secure and free from unauthorized intrusions. By regularly analyzing network data, I can help maintain a secure environment, contribute to the organization’s cybersecurity policies, and assist in forensic analysis during and after an incident. |

**Lab: Intrusion Detection Using Snort**

| **Prompt** | **Response** |
| --- | --- |
| In the lab section, “Setting up the Sniffer,”**Step 19,** type your name after the command prompt and take a screenshot of the output after running the *tcpdump -i eth1* command. |  |
| In the lab section, “Detecting Unwanted Incoming Attacks,” **Step 9,** take a screenshot of the results in the Bruter window after it has cycled through the dictionary words. |  |
| In the lab, “Detecting Unwanted Outgoing Traffic,”**Step 6,** type your name at the command prompt and take a screenshot of the output of the payload generated. | A screenshot of a computer  Description automatically generated |
| How can you see what options are available for the *tcpdump* command? How can this tool be used by a security analyst? | To see the available options for the tcpdump command, you can use the `tcpdump --help` or `man tcpdump` command. This tool is invaluable for security analysts as it allows for the capture and detailed inspection of network packets. Analyzing these packets helps understand network traffic flow and spot suspicious activities, forming the basis for security monitoring and threat detection. |
| What command will display all of the Ethernet interfaces within Linux? How can this be valuable to a security analyst? | The command `ifconfig -a` or `ip link show` can display all Ethernet interfaces on a Linux system. This information is valuable to a security analyst for configuring network monitoring tools, ensuring proper network interface management, and troubleshooting connectivity issues. |

**Detecting Malware and Unauthorized Devices**

| **Prompt** | **Response** |
| --- | --- |
| In the lab, “Keyloggers,” **Step 6**, scroll up to the prompt where you typed the *nmap* command and take a screenshot of the output from the scan. Be sure to include the timestamp at the top (date and time). |  |
| In the lab, “Keyloggers,” **Step 21**, take a screenshot of the successful migration after running the *migrate* command. **Note: The number you use will be different from the one in the example.** | A computer screen with white text  Description automatically generated |
| In the lab, “Keyloggers,” **Step 30**, take a screenshot of the output after running the *kerberos* command. Scroll up to the prompt where you typed the command and include the administrator password in your screenshot to show the success of the keylogger dump. | A screenshot of a computer screen  Description automatically generated |
| In the lab, “Examining Malware**,” Step 32,** take a screenshot of the History tab in Windows Defender showing the quarantined file that was detected. | A screenshot of a computer error  Description automatically generated |
| Explain the difference between **active and passive scanning tools and techniques**. | **Active vs. Passive Scanning Tools:** Active scanning tools interact with the network to generate traffic and analyze the response, thus detecting active devices and vulnerabilities. In contrast, passive scanning involves listening to the network without sending probes or altering the traffic, allowing the detection of ongoing traffic and activities without the network being aware of the scan. Both techniques are essential for a comprehensive security posture, balancing proactive engagement and discreet monitoring. |
| Explain the significance of the **kerberos** output. | **Significance of the Kerberos Output:** The Kerberos output is significant as it demonstrates the successful authentication and ticket-granting process used within secure network environments. By analyzing this output, I can verify that authentication protocols are functioning correctly and ensure that security measures are in place to effectively manage and protect user credentials and access within the network. |