**ITT-307 - Lab Assessment Report Template**

Professor: Ingrid Gaviria

Course: **ITT-307, Cybersecurity Foundations, Topic 8**

Student: James Darling

Date: 08/25/2024

Title: WIreshark

Directions:

# Overview: Perform a Wireshark scan on the network VM’s and compare and contrast with the vulnerability assessment

# Details: Open VM Open Wireshark Select Capture Select filters, Hit startA screenshot of a computer Description automatically generated

Hit the red square button on the top left to stop capturingA screenshot of a computer

Description automatically generated

Save ScanA screenshot of a computer

Description automatically generatedApply different filters such as DNSA screenshot of a computer

Description automatically generatedSelect Analyze to choose different filtersA screenshot of a computer

Description automatically generated

Summary: In addition to monitoring and reading data, Wireshark is a packet analyzer which will show most if not all network issues and analyze data coming into and leaving the device. IP addresses, ports, and other information found in the data are displayed by Wireshark, along with vulnerabilities that are scanned and presented in a readable format while the application is operating. In digital forensics, Wireshark is used to track and trace the origins of an attack. It will show the source and destination, read the IP address to determine the attack's location, and compare it to another. Wireshark has an additional capability that allows you to verify and justify the communications between sources and destinations. Along with disclosing the MAC address, it will provide all the data that was gathered and delivered. Below is a photo that you can view. The Flow graph is an additional Wireshark tool that users can utilize to determine the nature of a network problem such as dropped frames, timeouts, or lost connections. After choosing an IP address and extracting it using TCP packets, the device's send and receive packet flow will be seen. The hierarchy is a feature that allows the presentation of every layer that has been applied to the program. Wireshark offers a far more in depth look at an active network contrasting the vulnerability assessment of looking over general security concerns and constraints. I believe the use of both is of best practice. Assess the overall outlook find the problems and use Wireshark to dig deeper and find the specifics you may be looking for.