A logo on a black background

Description automatically generated

***Exploring and Using Network Sniffers Report***

***Purpose***

*This report explores the functionality, benefits, and potential risks of using network sniffers in cybersecurity. This report will provide a detailed analysis of how network sniffers capture, analyze, and monitor network traffic to aid in network management and threat detection. Additionally, it will examine both ethical and unethical uses of network sniffers, helping cybersecurity professionals understand best practices for their implementation.*

***Scope***

*This report focuses on the practical application of network sniffers within a corporate or enterprise network environment. It will cover different types of sniffing tools, such as Wireshark and Tcpdump, and explore their use cases in areas like network performance monitoring, troubleshooting, and security analysis. The report will also discuss legal and ethical considerations for using these tools, including the risks of unauthorized packet capturing and data breaches.*

***Overview***

*Network sniffers, or packet analyzers, capture and examine data traveling across a network in real time. They play a critical role in network troubleshooting and cybersecurity incident response, allowing network administrators to monitor data flow, detect vulnerabilities, and respond to threats. By analyzing packet-level data, sniffers provide deep insights into network performance, potential security risks, and possible misconfigurations. This report will investigate their architecture, operational functionality, and common use cases in everyday network management and specialized cybersecurity applications.*

***Results***

*This section presents the findings derived from network traffic captures using Wireshark and tcpdump alongside Snort's detection capabilities with custom rules. The results include a detailed analysis of captured network traffic, detection of specific network behaviors, and an overview of the security measures implemented to safeguard against sniffing. These results provide insights into network performance, potential security threats, and the effectiveness of protective measures in place.*

**Part 1: Wireshark**

**1.**

A screenshot of a computer

Description automatically generated

**Part 2: Tcpdump**

A screenshot of a computer

Description automatically generated

B

A computer screen shot of white text

Description automatically generated

A screenshot of a computer

Description automatically generated

c.

A computer screen with white text

Description automatically generated

d.

A computer screen with white text

Description automatically generated

***Part 3: Detecting Sniffers with Snorts***

a.

A screenshot of a computer

Description automatically generated

b.

A screen shot of a computer

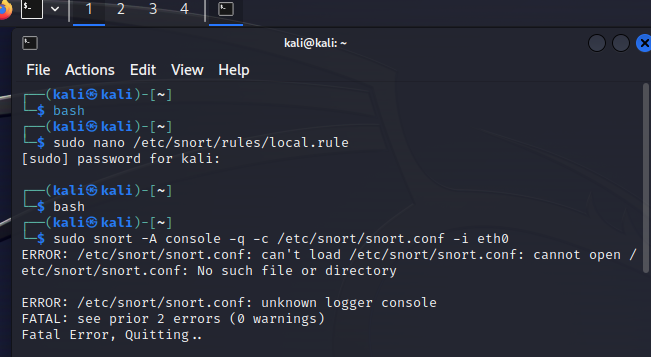
Description automatically generated

c.

A screenshot of a computer

Description automatically generated

d.



Part 4: Protecting Against Sniffers

A close up of a black background

Description automatically generated

A computer screen shot of a program

Description automatically generated

A screen shot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

