NETWORK MONITORING IN DATA LINK

Umika Saroha, Anchal Kumari,
Department of Computer Science and Engineering
National Institute of Technology Karnataka
Surathkal, Mangalore, India
7678416475, 6299349700
umikasaroha.211cs161@nitk.edu.in, anchalkumari.211cs105@nitk.edu.in

March 13, 2023

Abstract

A. Background of the problem statement

The fast expansion of the Internet has prompted widespread worry about network privacy, integrity and confidentiality. Administrators have to deal with not only high speed wired network but also wireless networks. It is important for network to be monitored properly.Network monitoring in the data link layer involves analyzing and capturing network traffic at the link layer of the OSI model. The data link layer is responsible for framing packet providing error detectio and ensuring reliable transmission of data over the physical network.

B. Challenges and issues of the problem statement

To help ensure network quality, network administrators should analyze, monitor and secure network traffic. Network monitoring enables the oversight of a computer network for failures and deficiencies to ensure continued network performance.

Tools made to aid network monitoring also commonly notify users if there are any significant or troublesome changes to network performance. Network monitoring enables administrators and IT teams to react quickly to any network issues.

C. Existing approaches or methods and their issues

Port Mirrorin available in switches TA[redacted] at high speeds Packet Capturttere[redacted] access to full network data during analysis Pattern Matching DPI detection rule development Event Based DPI:requires more complicated implementation that pattern matching DPI Flow Observation:privacy packet payload data not used

D. Your problem statement

Several authors have proposed solutions to mitigate data link layer attacks. Each mitigation technique were entirely different from others.

E. Objectives of the proposed work

Prime focus of the project is to identify the attack at data link layer and checking its possibility to merge together all attack at one place using [redacted] Snort generally works at network layer or above the network layer. Not all the data link layer attack can be identified by ID For the current work a various solution already researched are put together to analyse attack at data link layer. Further customized code can be written to detect data link layer attack is possible.

References

[1] Mitigation Technique, https://www.hypr.com/security-encyclopedia/mitigation#:~:text=Mitigation%2C%20or%20Attack%20Mitigation%2C%20is,activism%2C%20retribution%2C%20or%20mischief.

[2] Framing Packets, https://www.baeldung.com/cs/networking-packet-fragment-frame-datagram-segment#:~:text=While%20a%20packet%20is%20the,length%20and%20variable%2Dlength%20frames.

[3] Port Mirroring, https://www.techopedia.com/definition/16134/port-mirroring.

[4] IDS, https://www.geeksforgeeks.org/intrusion-detection-system-ids/amp/.

[5] Packet Capture, https://www.varonis.com/blog/packet-capture.

[6] Pattern matching DPI, https://ieeexplore.ieee.org/document/4545432.

[7] Error detection, https://www.geeksforgeeks.org/error-detection-in-computer-networks/amp/.

[8] R. Shanker, A. Singh, Analysis of network attacks at data link layer and its mitigation (2021). doi:10.1109/ICCS54944.2021.00061.

[9] J. Svoboda, I. Ghafir, V. Prenosil, Network monitoring approaches: An overview, International Journal of Advances in Computer Networks and Its Security– IJCNS 5 (2015) 88–93.

[10] Snort, https://en.wikipedia.org/wiki/Snort_(software).

[11] Snort, https://www.geeksforgeeks.org/what-is-snort/.

[12] Snort, https://www.snort.org/.

[13] Tap, https://insights.profitap.com/what-are-network-taps.

[14] Protocol Analyzer, https://www.geeksforgeeks.org/what-is-protocol-analyzer/.

[15] Packet Sniffers, https://www.kaspersky.com/resource-center/definitions/what-is-a-packet-sniffer.

[16] J. Conard, Services and protocols of the data link layer (1983). doi:10.1109/PROC.1983.12781.

****** END ******

Note:

- Include your reference details in ref.bib file of the shared project
- References to be referred to within the content as [1–16]