Network Analysis for Malicious Sites

PROJECT REPORT

Submitted in the partial fulfilment of the requirements
for the award of the
Six Months Online Certificate Course
in
Cyber Security
Course Duration: [22-01-2024 to 21-07-2024]

By
K B M Sushanth
(Ht. No. 2406CYS103)

Under the Esteemed Guidance of
Prof. Niladri Dey

DIRECTORATE OF INNOVATIVE LEARNING & TEACHING (DILT)
JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
(Formerly SCDE_SCHOOL OF CONTINUING AND DISTANCE EDUCATION)
Kukatpally, Hyderabad, Telangana State, INDIA- 500 085
JULY 2024

ABSTRACT

In this project report, we present a comprehensive analysis of network traffic to identify and block access to malicious websites using Wireshark. Our focus is on creating rule engines to detect and prevent connections to a hypothetical malicious site, malice.com. The methodology involves capturing network traffic, identifying malicious packets, and generating specific rules to block the site as soon as it is accessed. The implementation and analysis demonstrate the effectiveness of these rule engines in enhancing network security and preventing potential cyber threats.

TABLE OF CONTENTS

1. Introduction

The rise of cyber threats necessitates robust methods to detect and prevent access to malicious websites. This project explores the use of Wireshark, a powerful network protocol analyzer, to identify and block a specific malicious site, malice.com. By analyzing network packets and creating targeted rule engines, we aim to enhance network security and mitigate potential risks.

2. Literature Survey

This section reviews existing research and methodologies related to network analysis, packet inspection, and malicious site detection. Key studies and tools that have contributed to the field are discussed to provide a foundation for the current project.

3. Problem Statement

The primary challenge addressed in this project is the detection and blocking of malicious websites in real-time. Specifically, we focus on preventing access to malice.com, a hypothetical malicious site, by analyzing network traffic and creating rule engines using Wireshark.

4. Objectives

- To analyze network traffic for malicious activities.

- To identify packets related to malice.com.
- To create rule engines in Wireshark to block access to malice.com.
- To evaluate the effectiveness of the rule engines in real-time.

5. Methodology

The methodology involves several key steps:

1. Capturing network traffic using Wireshark.
2. Filtering packets to identify those associated with malice.com.
3. Creating rule engines to block identified packets.
4. Testing the rule engines to ensure immediate blocking of malice.com upon access.

6. Algorithms

The project employs specific algorithms for packet filtering and rule generation in Wireshark. Detailed descriptions of these algorithms and their implementation are provided.

7. Implementation

The implementation section covers the practical steps taken to capture and analyze network traffic, create and apply rule engines in Wireshark, and test the system for effectiveness.

8. Results & Analysis

This section presents the results of the implemented rule engines, including success rates, performance metrics, and any challenges encountered. Analysis of the data demonstrates the system's capability to block malice.com in real-time.

9. Conclusion

The project successfully demonstrates the use of Wireshark for real-time detection and blocking of malicious websites. The rule engines created effectively prevent access to malice.com, highlighting the potential for similar approaches to enhance network security.

10. Future Scope

Future work may involve extending the methodology to detect and block a wider range of malicious sites, integrating machine learning techniques for improved detection accuracy, and automating the rule generation process for scalability.