Intrusion Detection System (IDS) Report

Hagay Cohen, Imri Shai

September 26, 2024

1 Conclusions from the R&D

The research we conducted on data leak attacks provided valuable insights into the types of attacks, methods of exfiltration, and detection mechanisms. We found that data leak attacks can be detected through packet inspection, user behavior analytics, and packet header analysis. These detection methods are implemented in our Intrusion Detection System (IDS) as discribed below.

2 System Architecture

Our IDS is designed to monitor network traffic and detect suspicious activities that may indicate data leaks. The system architecture is shown in Figure 1. The IDS consists of three main components: flow classifier, detection engine, and statistical analysis module.

Figure 1: System Architecture

2.1 Flow Classifier

For each packet, the flow classifier extracts a 5-tuple key (source IP, destination IP, source port, destination port, protocol) and assigns it to a flow. The flow classifier then updates the flow's statistics, such as packet count and byte count, and forwards the flow to the detection engine.

2.2 Detection Engine

The detection engine analyzes the flows received from the flow classifier to identify potential data leak attacks. It uses a set of rules and traffic patterns to detect suspicious activities, such as tunneling, social engineering, and backdoors misuse. When a potential attack is detected, the detection engine generates an alert, prints it to the console, saves it to a log file.

2.3 Statistical Analysis Module

When the IDS is ordered to stop, by gracefully shutting down or an end of a simulation, the statistical analysis module saves the statistics of the flows to a file. And then, it activates the UI module to display the statistics in a user-friendly way. All the alerts, flow data, and statistics imgaes are saved to further analysis. UI example is shown in Appendix A.

3   Detections Explanations

Our IDS is capable of detecting various types of intrusions. The detection mechanisms include...

4   Docker Network Simulation

We used Docker to simulate a network environment for testing our IDS. The setup includes containers for an internal server, a database, user machines, an external server, and the IDS itself.

4.1   Network Setup

The network is defined using a Docker Compose file with the following components:

- **Internal Server:** Nginx web server.

- **Database:** MySQL database.

- **User Machines:** Simulate normal and malicious activities.

- **External Server:** Simulates external threats.

- **IDS:** Monitors and detects suspicious activities.

4.2   Traffic Generation

Scripts in user containers generate normal and malicious traffic, including web browsing, and data exfiltration.

4.3   IDS Monitoring and Detection

The IDS inspects packets, analyzes user behavior, and examines packet headers to detect data leaks. Alerts and logs are generated for suspicious activities.

4.4 Results and Analysis

The IDS's effectiveness is evaluated by reviewing alerts and analyzing traffic patterns to identify vulnerabilities. As we assumed, the IDS detected the data leak attacks and generated alerts successfully.

5 Future Extensions

In the future, the IDS can be extended to include more sophisticated detection mechanisms.....

6 Conclusions and Notes

The IDS is a powerful tool for detecting data leak attacks ......

A User Interface Example