HIDS FOR SMALL NETWORKS

SYED SOHAIB SHAH
HAMID REZA
SHAYAN AHMAD

INSTITUTE OF SPACE TECHNOLOGY

ABSTRACT

This paper provides an extensive explanation of the development and implementation of a Host-Based Intrusion Detection System (HIDS) which focuses on enhancing system security via different steps and measures. It includes manual and automatic port filtering, packet sniffing, comparing against YARA rules, and using machine learning for the detection of malicious executable (EXE) files. The main purpose of the system is to block unnecessary ports, monitor network traffic, and use machine learning algorithms to detect malicious files, thereby improving the overall security of the host system.

OBJECTIVE

- Develop a Host-Based Intrusion Detection System (HIDS) to enhance the security of individual systems
- Implement automatic port filtering to block unnecessary ports, thereby reducing the risk of security threats.
- Monitor network traffic in real-time to detect suspicious activities and potential threats.
- Utilize YARA rules to identify and mitigate malicious activities based on pattern matching. Apply machine learning techniques to detect and classify potentially malicious executable files.

RESULTS

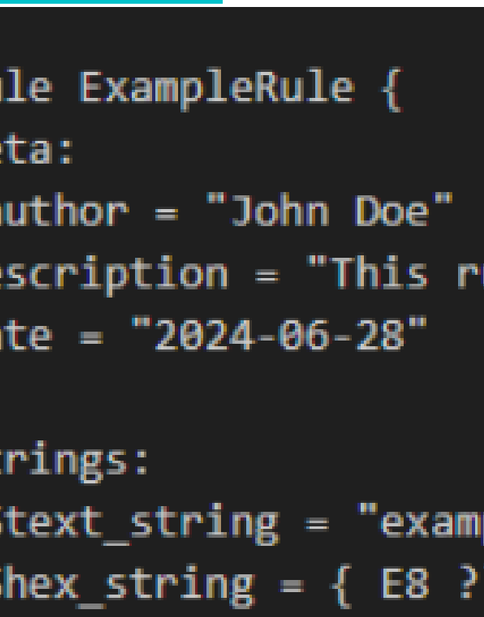
- Provide security through blocking ports.
- Analysis and monitoring of host's traffic for suspicious activities.
- Detection and alert the user about potential security threats.
- Machine learning will identify and inform users about malicious executable files, enhancing protection against advanced threats.

```
rule ExampleRule {
meta:
 author = "John Doe"
description = "This rule detects Example Malware"
date = "2024-06-28"

strings:
 $text_string = "example malware"
 $hex_string = { E8 ?? ?? ?? ?? 83 C4 04 }
 $regex_string = /malware[0-9]+/
condition:
 $text_string or $hex_string or $regex_string }
```

ACKNOWLEDGMENT

We are thankful to our Supervisor Sir Faran Mehmood for his invaluable guidance and support. Their expertise and mentorship has been crucial for our success.



METHODOLOGY

We will use C# and its libraries for HIDS.
We used Port Filtering to block the ports.
Using .Net (Packet Sniffing) will monitor and intercept packets for analysis purposes.
YARA Rule Comparison will help us detect the malicious data packet.
Machine Learning will be trained to detect and classify malicious .exe files.