

Assessment Plan: Testing the Effectiveness of Micro Trend’s Host Intrusion Prevention System

24/08/2023

Table of Contents

[executive summary 2](#_Toc143717401)

[Standard Access Lists vs Extended Access Lists: 2](#_Toc143717402)

[Conclusion: 3](#_Toc143717403)

# Glossary

Table 1: Glossary

|  |  |
| --- | --- |
| Term | Definition |
| **HIPS** | Host Intrusion Prevention System |
| **IIS** |  |
| **TBA** |  |
|  |  |
|  |  |
|  |  |
|  |  |

# Executive summary

|  |  |
| --- | --- |
|  | In the evaluation of the Host Intrusion Prevention System’ (HIPS) effectiveness, it is recommended to employ a comprehensive approach that involves simulating both malicious and benign traffic scenarios to observe the system's behavior and whether rules are triggered, bypassed, or false alarms are issued.  This assessment plan proposes different testing approaches, such as:   * Creation of batch files or scripts that mimic the behavior of malware. * Visiting potentially malicious websites. * Externally performing cyber attacks such as directory traversal, URI double encoding, etc. * Intentionally introducing malicious files into the test environment to evaluate the HIPS's capability to promptly identify and prevent the exploitation of vulnerabilities.   Additionally, the HIPS’ performance is put into test to validate its effectiveness under normal host condition as well as under compromise. |

# Assessment plan

|  |  |
| --- | --- |
|  | Goals and Objectives:  * Evaluate the effectiveness of the HIPS in detecting and preventing unpermitted activities on an agent as per configured rules. * Measure the HIPS’ impact on system performance. * Evaluate the system's responsiveness to incidents and verify centralized real-time logging of events. |
|  | Assessment Scope: **The assessment scope is bounded by..** |

|  |  |
| --- | --- |
|  | Assessment Metrics:  * **Rule triggering rate.** * **False alarms rate.** * **Impact on system performance (CPU usage, memory consumption).** * **HIPS responsiveness in incident handling & reporting.** |

|  |  |
| --- | --- |
|  | Assessment Methodology: **Review corresponding policies.**  **Measure the system's baseline performance (CPU, memory, disk usage) without the HIPS enabled. (use nmon).**  **Testing Environment: Set up a controlled and segregated testing environment that closely resembles the production system's configuration.**  **Validate rules of the HIPS by attempting to bypass them through:**   * Simulation of various types of attacks, including malware execution, privilege escalation, and unauthorized access attempts. * Testing the HIPS’ **timely** response to both signature-based and behavior-based threats. |

# Assessing effectiveness of configured rules:

|  |  |
| --- | --- |
|  | In this section, we aim to validate the effectiveness of configured rules on the HIPS. Following table presents a summary of findings. |

Table 2: Validation of Configured Rules

|  |  |  |
| --- | --- | --- |
| Rule | Description | Validation |
| **TBA** | Host Intrusion Prevention System |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

|  |  |
| --- | --- |
|  | We will now take rules individually and cover: what they protect from, ways to validate their effectiveness, and recommendations. |

## Rule 1: ---

|  |  |
| --- | --- |
|  | **What it protects from:**  TBAA  **Affected Systems/ Components:**  TBAA  **Validation Method:**  TBAA  **Recommendations:**  TBAA |

## Rule 2: ---

|  |  |
| --- | --- |
|  | **What it protects from:**  TBAA  **Affected Systems/ Components:**  TBAA  **Validation Method:**  TBAA  **Recommendations:**  TBAA |

## Rule 3: ---

|  |  |
| --- | --- |
|  | **What it protects from:**  TBAA  **Affected Systems/ Components:**  TBAA  **Validation Method:**  TBAA  **Recommendations:**  TBAA |

## Rule 4: ---

|  |  |
| --- | --- |
|  | **What it protects from:**  TBAA  **Affected Systems/ Components:**  TBAA  **Validation Method:**  TBAA  **Recommendations:**  TBAA |

## Rule 5: ---

|  |  |
| --- | --- |
|  | **What it protects from:**  TBAA  **Affected Systems/ Components:**  TBAA  **Validation Method:**  TBAA  **Recommendations:**  TBAA |