Humanidades, Tecnología y Ciencia, del Instituto Politécnico Nacional
Certificado de Reserva de Derechos al Uso Exclusivo del Título: 04-2010-0326124-14000-203 ISSN: 2007-1957

FEASIBILITY STUDY FOR THE IMPLEMENTATION OF AN INTRUSION PREVENTION SYSTEM

Kevin Enrique Ortiz Díaz
ESIME Zacatenco. Instituto Politécnico Nacional
kevo.diaz95@gmail.com

José Félix Serrano Talamamtes
CIDETEC Instituto Politécnico Nacional
jfserrano@ipn.mx

Mauricio Olguín Carbajal
CIDETEC Instituto Politécnico Nacional
molguinc@ipn.mx

Abstract

This study examines the technical and operational feasibility of implementing Snort as an Intrusion Prevention System (IPS) in ESIME Zacatenco's "Internet of Things" laboratory. The objective is to design and evaluate the effectiveness of Snort as a software-based IPS for protecting the laboratory's network against specific cyberattacks. The study also assesses the overall viability of Snort implementation in terms of resources, time, and benefits for security and data protection. By enhancing IoT system security and providing practical recommendations for IPS implementation in similar environments, this study contributes to cybersecurity knowledge and ensures data integrity in a rapidly growing connectivity environment.

Keywords: Snort, Intrusion Prevention System, IPS, Internet of Things laboratory, ESIME Zacatenco, technical feasibility, operational feasibility, cybersecurity, data protection, cyberattacks, IoT networks.

I. INTRODUCTION

Currently, the Internet of Things (IoT) is pivotal for its device connectivity, driving diverse applications across sectors. While its potential to revolutionize lives is undeniable, it poses security and data protection challenges. In this context, effective Intrusion Prevention Systems (IPS) are imperative to ensure data integrity and confidentiality in IoT environments. IPS serves as a key solution for detecting and preventing cyberattacks, adding an extra layer of security to connected systems.

This study focuses on assessing the feasibility of implementing Snort, a recognized IPS tool, in a specific setting: a networked laboratory with 24 powerful computers, used for IoT-related research at ESIME Zacatenco. Our primary objective is to analyze Snort's

Humanidades, Tecnología y Ciencia, del Instituto Politécnico Nacional
Certificado de Reserva de Derechos al Uso Exclusivo del Título: 04-2010-0326124-14000-203 ISSN: 2007-1957

technical, economic, and operational viability as an IPS in this laboratory, evaluating its detection and prevention capabilities, infrastructure compatibility, resource requirements, and its impact on IoT security.

Our research aims to contribute practical insights, assessing the technical, economic, and operational aspects of Snort's implementation in a specific laboratory setting, enhancing IoT system security and ensuring data integrity in this evolving connected environment.

II. DESIGN

An IPS based on software was implemented to protect the laboratory against three possible cyberattacks, which were:

a) Port scanning
b) Denial of Service (DDoS)
c) Man-in-the-middle"

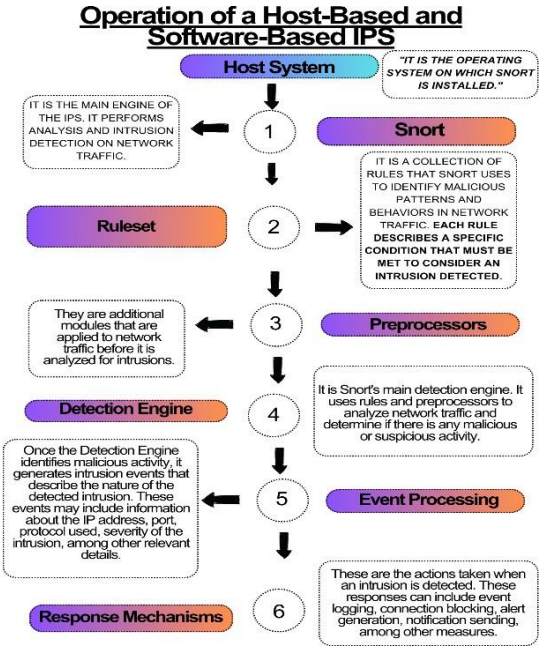

Figure 1. Software-Based IPS Diagram for the Laboratory.

Description of the diagram:

- **Network Traffic:** This is the communication network where the software-based IPS analyzes and protects network traffic.
- **IPS (Software):** The IPS software runs on a network host. It monitors and analyzes network traffic for potential threats and attacks.
- **Detection Rules (Ruleset):** The set of detection rules defines the patterns and malicious behaviors that the IPS searches for in network traffic. Each rule has a specific structure that includes conditions, options, and actions to take when the condition is met.
- **Rule 1, Rule 2, Rule 3:** These blocks represent individual rules within the ruleset. Each rule consists of conditions, options, and actions defined during the IPS configuration process. In this case, one rule is for port scanning, the second for denial of service, and the last for a man-in-the-middle attack, which are the attacks covered in this work.
- **Attack 1, Attack 2, Attack 3:** These blocks represent the specific attacks that have been mentioned. Each block indicates the type of attack and how it is detected and responded to by applying the corresponding detection rules. For these attacks, we will conduct penetration testing to execute exploits with the potential to compromise the network.
- **Generated Alerts:** When the IPS detects an attack or suspicious activity according to the configured rules, it generates alerts to notify administrators or security personnel.
- **IPS Responses:** Based on the configured rules, the IPS takes response measures to protect and

Humanidades, Tecnología y Ciencia, del Instituto Politécnico Nacional
Certificado de Reserva de Derechos al Uso Exclusivo del Título: 04-2010-0326124-14000-203 ISSN: 2007-1957

defend the network. These responses may include connection blocking, log generation, notification sending, and other actions defined in the rules.

The software based IPS analyzes network traffic using the defined detection rules. When an attack is detected according to the rules, alerts are generated, and responses are implemented to protect and defend the network against identified attacks.

Snort Rule Configuration Process

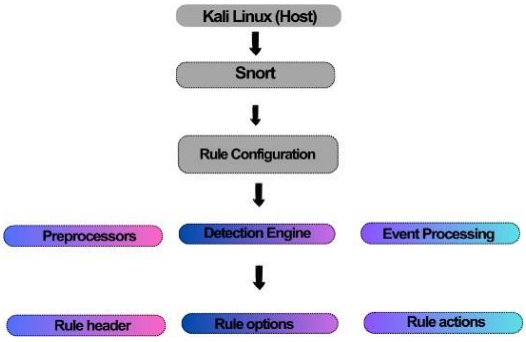

Figure 2. Snort Rule Configuration Process.

The process of installing Snort on Kali Linux involves using a package manager to download and install the Snort package on the Kali Linux operating system. Subsequently, the configuration of Snort is carried out, encompassing aspects such as defining network interfaces, setting up logs, output options, and other Snort-specific adjustments. Furthermore, the configuration and updating of intrusion detection rules in Snort are performed, which entails adding, modifying, or removing rules within the rule set used by Snort to detect malicious events. This process is tailored to specific security requirements; in our case, it addresses the three attacks covered in this thesis.

For beginners in Linux, it's important to understand the basics of networking and security (OccupyTheWeb, 2018).

III. PROTOTYPE

Rules

According to the procedures outlined in *Snort™ for Dummies®* (Wiley Publishing, Inc., 2004), it is important to configure Snort properly to enhance network security.

1.- alert udp any any -> any any (dsize: > 10000; sid:100001; rev:1; msg:"Posible ataque DDoS";)
2.- alert tcp any any -> $HOME_NET any (flags: S; msg:"Posible escaneo de puertos SYN"; sid:100002; rev:1;)
3.- alert tcp any any -> $HOME_NET any (content:"GET"; pcre:"/Host\x3a\s+[^.]+./H"; msg:"Posible ataque Man-in-the-Middle"; sid:100003; rev:1;)

Three specific rules have been developed to protect against the previously mentioned attacks. Below is a detailed explanation of how these rules work:

Rule 1, aimed at preventing DDoS attacks:

- **Code:** alert udp any any -> any any (dsize: > 10,000; sid:100001; rev:1; msg:"Possible DDoS Attack";)
- **Activation:** This rule is triggered when it detects UDP traffic with packet sizes greater than 10,000 bytes. Since Distributed Denial of Service (DDoS) attacks often involve a high volume of packets, this rule seeks to identify suspicious traffic of this nature and generates an alert for the security administrator to take action.

Rule 2, focused on port scanning detection:

- **Code:** alert tcp any any -> $HOME_NET any (flags: S; msg:"Possible SYN Port Scanning"; sid:100002; rev:1;)
- **Activation:** This rule activates when it detects TCP traffic with the SYN flag set that is directed toward your network ($HOME_NET). Port scans frequently start with TCP packets attempting to establish connections with multiple ports.

Humanidades, Tecnología y Ciencia, del Instituto Politécnico Nacional
Certificado de Reserva de Derechos al Uso Exclusivo del Título: 04-2010-0326124-14000-203 ISSN: 2007-1957

The rule identifies such traffic and triggers an alert when the condition is met.

Rule 3, designed to prevent Man-in-the-Middle attacks:

- **Code:** alert tcp any any -> $HOME_NET any (content:"GET"; pcre:"/Host\x3a\s+[^.]+./H"; msg:"Possible Man-in-the-Middle Attack"; sid:100003; rev:1;)
- **Activation:** This rule triggers when it detects an HTTP GET request in which the "Host" field contains a domain different from that of your network ($HOME_NET). A Man-in-the-Middle attack involves an attacker intercepting communication between two parties and impersonating one of them. The rule seeks to identify HTTP requests that may indicate such an attack and generates an alert when the condition is met.

It is important to note that in addition to these custom rules, Snort includes a set of pre-existing rules that contribute to a more comprehensive and secure environment.

Laboratory tests

The procedures for using Kali Linux are well-documented (Hertzog, O'Gorman, & Aharoni, 2017).

1. **Port Scanning:**

According to Terán Pérez (2018), "It involves checking which ports are available to be explored within one or more computers on a network" (p. 223).

Objective: Send port scan requests from a testing machine to the lab, analyzing how the IPS responds to and detects this suspicious activity.

Tool: Kali Linux tool: Nmap (Network Mapper)

Steps:

Configure a Kali Linux machine with Nmap installed.

Execute the command "nmap -p <ports> <lab IP>" to scan specific ports in the lab.

Analyze the logs and alerts generated by Snort to determine if the IPS has correctly detected and blocked the port scanning attempts.

Results: Detailed report including scanned ports, IPS alerts, and whether port scanning attempts were detected and blocked.

2. **DDoS Attack:**

Objective: Simulate a DDoS attack from multiple sources to the lab to evaluate how the IPS identifies and mitigates such attacks.

Tool: Kali Linux tool: Hping3

Steps:

Configure a Kali Linux machine with Hping3 installed.

Use Hping3 to send a large number of ICMP or TCP SYN packets to the lab from multiple simulated IP addresses.

Monitor the IPS response and verify if it identifies and blocks the suspicious traffic associated with the DDoS attack.

Results: Report including the type of DDoS attack simulated, source IP addresses used, Snort alerts, and whether the IPS successfully mitigated the DDoS attack.

3. **Man-in-the-Middle (MitM) Attack:**

Objective: Perform a MitM attack to intercept and modify traffic between two systems in the lab, assessing if the IPS can detect and prevent such malicious activity.

Tool: Kali Linux tool: Ettercap

Steps:

Configure a Kali Linux machine with Ettercap installed.

Execute a MitM attack using Ettercap to intercept and redirect traffic between two target systems in the lab.

Monitor the IPS response and check if it detects and blocks the MitM attack, generating the corresponding alerts.

Humanidades, Tecnología y Ciencia, del Instituto Politécnico Nacional
Certificado de Reserva de Derechos al Uso Exclusivo del Título: 04-2010-0326124-14000-203 ISSN: 2007-1957

Results: Presentation of a report detailing the MitM attack performed, affected target systems, IPS alerts, and if the malicious activity was successfully blocked.

Conclusions:

Implementing an IPS based on software, such as Snort, for the "Internet of Things" laboratory at ESIME Zacatenco, proves to be a strategic decision in enhancing network security. This approach aligns with the project's objectives of designing, developing, implementing, and evaluating the IPS prototype. By combining the IPS with antivirus and firewall technologies, the laboratory can establish a robust defense against various cyber threats, ensuring the integrity and confidentiality of its network. Regular testing and updates will be essential to maintain a strong security posture and protect against evolving cyber threats in the future.

References

Terán Pérez, D. M. (2018). *Administración y seguridad en redes de computadoras*. México: Alfaomega Grupo Editor, S.A. de C.V.

Hertzog, R., O'Gorman, J., & Aharoni, M. (2017). *Kali Linux revealed*. Cornelius, NC: Offsec Press.

OccupyTheWeb. (2018). *Linux basics for hackers: Getting started with networking, scripting, and security in Kali*. San Francisco, CA: No Starch Press, Inc.

Wiley Publishing, Inc. (2004). *Snort™ for dummies®*. Indianapolis, IN: Wiley Publishing, Inc.