Threat Intelligence Implementation Report

1. Introduction

This report details the implementation of threat intelligence principles through the analysis of Indicators of Compromise (IoCs) and the setup of the OpenCTI Threat Intelligence Platform. The project includes the detection methods for two IoCs, the configuration of the OpenCTI platform, and the integration of connectors to enhance threat intelligence capabilities.

2. Analysis of Indicators of Compromise (IoCs)

IoC 1: Broadcast-avahi-dos (CVE-2011-1002)

Description:

The Broadcast-avahi-dos vulnerability is associated with the Avahi service, commonly used for local network service discovery. This vulnerability can be exploited for a Denial of Service (DoS) attack via NULL UDP packets.

Detection Method:

- **Tool Used:** Nmap
- **Command:** `nmap -sV --script vuln <target-IP>`
- **Detection:** The Nmap script detects the presence of the Avahi service and checks for vulnerability to the NULL UDP packet attack.

Threat Indication:

The presence of this vulnerability indicates a potential risk of service disruption through a DoS attack, which could impact network availability and service reliability.

IoC 2: Unauthorized Network Access

Description:

Unauthorized network access attempts, particularly those targeting SSH services, are indicative of potential brute force attacks or unauthorized entry attempts.

Detection Method:

- **Tool Used:** Suricata/Snort
- **Rule Example:**
- `alert tcp any any -> $HOME_NET 22 (msg:"Possible SSH Brute Force Attack"; flags:S; threshold: type both, track by_src, count 5, seconds 300; sid:1000001;)`
- **Log Source:** System logs (e.g., `/var/log/auth.log` for Linux) and firewall logs.

Threat Indication:

Multiple failed login attempts from a single IP address within a short period indicate a potential brute force attack, which could lead to unauthorized access and system compromise.

3. OpenCTI Threat Intelligence Platform Implementation

Platform Setup

Installation Method:

The OpenCTI platform was installed using Docker for ease of deployment and management.

Configuration:

- **Docker Command:**
- `docker run -d -p 8080:8080 opencti/platform`
- **Initial Setup:** Accessed the platform via `http://localhost:8080` and completed the initial configuration, including setting up the admin account and basic platform settings.

Connector Integration

Connector 1: OpenCTI Datasets Connector

- **Purpose:** This connector collects data from the OpenCTI datasets repository to pre-populate the OpenCTI instance with essential information such as companies, industry sectors, and geographical locations.
- **Configuration:** Configured to import identity and location objects, providing a foundational dataset for threat intelligence analysis.

Connector 2: OpenCTI CISA Connector

- **Purpose:** This connector integrates with the CISA Known Exploited Vulnerability (KEV) catalog, which is a critical resource for identifying and mitigating vulnerabilities actively exploited in the wild.
- **Configuration:** Set up to download and parse the KEV catalog, importing Identity, Infrastructure, and Vulnerability STIX Objects into the OpenCTI platform. This helps prioritize remediation efforts based on active threats.

Documentation and Usage Demonstration

- **Platform Setup Documentation:** Detailed steps for Docker installation and initial configuration were documented, including screenshots and command examples.
- **Connector Integration Documentation:** Provided step-by-step guides for configuring the OpenCTI Datasets and CISA connectors, along with explanations of their functionality and importance.
- **Basic Usage Demonstration:** Demonstrated how to navigate the platform, create entities, and use connectors for data import and export.

4. Conclusion

The implementation of threat intelligence principles through the analysis of IoCs and the setup of the OpenCTI platform has enhanced the organization's ability to detect and respond to potential threats. The detection methods for the IoCs provide a clear indication of threats, while the OpenCTI platform, with its configured connectors, facilitates efficient threat intelligence management and analysis.

5. Next Steps

- **Regular Testing:** Conduct regular tests of the detection methods and platform functionality to ensure ongoing effectiveness.
- **Improved Alerting:** Enhance alerting mechanisms by integrating logs with SIEM tools like Splunk for real-time monitoring.
- **Continuous Monitoring:** Maintain continuous monitoring and regular updates to the threat intelligence database to stay ahead of evolving threats.

This report provides a comprehensive overview of the threat intelligence implementation, ensuring that the organization is well-prepared to identify and mitigate potential security threats.