**SCADA-Map: SMART INDIA HACKATHON 2024**

The SCADA-Map project addresses the need for a secure tool to automatically create network topology, especially for SCADA (Supervisory Control and Data Acquisition) systems. These systems are crucial in industries such as power, water supply, and manufacturing. As cyber threats evolve, securing such networks becomes critical. The proposed tool integrates security measures, real-time discovery, AI-based anomaly detection, and blockchain-based authentication, offering a solution that is robust, scalable, and suitable for protecting large SCADA infrastructures.

**Detailed Explanation**

**1. Secure Topology Discovery**

The project employs a combination of advanced technologies for secure network mapping:

**SNMPv3**: Provides secure device management through encryption and authentication, protecting sensitive data while allowing network administrators to monitor and control devices.

**ARP/MAC Tables**: Used to map the connections between devices, facilitating a real-time view of how devices are connected across the network.

**NetFlow**: Monitors and analyzes network traffic, offering insight into IP traffic flows. This helps identify anomalies and provides valuable data for network optimization.

**EIGRP (Enhanced Interior Gateway Routing Protocol)**: A dynamic routing protocol used for sharing routing information efficiently and securely across the network.

By utilizing these tools, the solution eliminates security vulnerabilities associated with older protocols like CDP (Cisco Discovery Protocol) and LLDP (Link Layer Discovery Protocol). This focus on secure data exchange and real-time updates allows for a constantly accurate and up-to-date network topology without compromising the system’s security.

**2. AI-Powered Anomaly Detection**

The solution incorporates artificial intelligence to monitor network activity and detect unusual behaviors that may indicate potential security breaches. Key features of the AI-based anomaly detection include:

**Continuous Traffic Analysis**: AI models analyze traffic patterns to detect outliers and deviations from normal network behavior.

**Device Behavior Monitoring**: The system monitors each device’s activity to identify suspicious behavior that could indicate unauthorized access or compromised devices.

**Proactive Alerts**: When anomalies are detected, the system generates alerts, allowing network administrators to take immediate action before any serious threats arise.

The AI-driven component uses machine learning models, particularly those built on frameworks like **TensorFlow** and **Scikit-learn**, to evolve and improve detection accuracy over time, making the system more robust as more data is processed.

**3. Blockchain-Based Device Authentication**

To ensure that only authorized devices access the network, the tool incorporates blockchain technology for device authentication. Blockchain provides a tamper-resistant method for verifying device identities, ensuring a high level of security. Features include:

**Decentralized Authentication**: Device identities are recorded on a blockchain ledger, ensuring transparency and security. Each device must be authenticated through the blockchain before it can access the network.

**Immutable Logs**: Every authentication event is recorded in the blockchain, providing a transparent and secure record of device interactions within the network.

**Prevention of Unauthorized Access**: By employing blockchain, the tool ensures that unauthorized devices are blocked from accessing sensitive parts of the network, significantly reducing the risk of cyber-attacks.

**4. Scalability for Large Networks**

The tool is designed to scale seamlessly across large and distributed networks. Many SCADA systems operate across vast geographical regions, sometimes spanning thousands of kilometers. To address this, the tool offers:

**Distributed Architecture**: It supports local enforcement of security policies at different nodes across the network, while maintaining centralized control and monitoring capabilities.

**Efficient Data Handling**: Even with a large number of devices and complex routing, the system ensures real-time updates and consistent performance.

The tool’s architecture is adaptable to the needs of vast networks, making it highly suitable for large industries that rely on SCADA systems for controlling critical infrastructure.

**5. Real-Time Visualization and Alerts**

A major advantage of the SCADA-Map is its real-time visualization feature. Network administrators can monitor the network topology and device status through a web-based interface. Key components include:

**Interactive Web-Based Interface**: The interface provides a visual representation of the network topology, allowing administrators to see the structure and status of devices at a glance.

**Real-Time Monitoring**: The system continuously updates the network map and device statuses, providing administrators with the latest information on device connectivity and health.

* **Instant Alerts**: If any anomalies or unauthorized access attempts are detected, the system generates real-time alerts, helping administrators react quickly to potential threats.

This feature is crucial for maintaining the health of the network and ensuring any issues are addressed before they lead to serious downtime or breaches.

**How the Solution Addresses the Problem**

The SCADA-Map solution provides a multi-faceted approach to securing large-scale networks. By integrating secure discovery protocols, AI-based monitoring, and blockchain authentication, it effectively addresses several key issues:

**Accurate Device Identification**: Instead of relying on insecure protocols like CDP/LLDP, which are prone to attacks, the system uses SNMPv3, ARP/MAC tables, NetFlow, and EIGRP to collect accurate and secure device and connection data.

**Real-Time Network Topology**: The tool provides up-to-the-minute network maps, helping administrators keep track of the constantly changing landscape of device connectivity, which is especially useful for troubleshooting.

**Network Security Across Large Areas**: The combination of AI for anomaly detection and blockchain for device authentication ensures that even expansive networks remain secure and segmented in the event of a security threat, helping to isolate issues before they escalate.

**Technical Approach**

**1. Front-End Technology Stack**

**HTML, CSS, JavaScript**: These standard web technologies are used to build the user interface, ensuring that the system is accessible via a web browser.

**D3.js**: A JavaScript library for creating dynamic, interactive data visualizations, used here to visualize the network topology in real time.

**2. Back-End Technology Stack**

**Python**: The back-end of the system is built with Python, which is widely used for network automation and security projects due to its simplicity and compatibility with many libraries.

**3. Libraries & Tools**

**PySNMP**: This Python library is used for interacting with SNMP devices, gathering essential data for network monitoring and topology creation.

**Scapy**: A powerful Python-based network packet manipulation tool, used for network discovery and security assessments.

**NetFlow**: A tool for monitoring network traffic and analyzing flow data.

**Netmiko**: A library for automating tasks across network devices from different vendors.

**4. Security Technologies**

**Blockchain**: Used for secure device authentication, ensuring that only authorized devices can interact with the network.

**OAuth 2.0 / JWT (JSON Web Tokens)**: Provides secure user authentication and session management, protecting the interface from unauthorized access.

**SSL/HTTPS**: Ensures that all data exchanged between the web interface and the system is encrypted, preventing eavesdropping or tampering.

**5. AI/ML/DL Technologies**

The system uses artificial intelligence and machine learning to monitor traffic and detect anomalies:

**TensorFlow**: A popular open-source framework for building machine learning models, used for the AI-powered anomaly detection.

**Scikit-learn**: A machine learning library used to implement predictive analytics and identify network behavior patterns.

**Keras**: A high-level neural networks API, used for building deep learning models to analyze network traffic data.

**Feasibility and Viability**

The solution is technically feasible due to the use of proven, widely available tools and technologies. Potential challenges include the complexity of scaling the system to handle large networks and ensuring that the blockchain-based authentication remains efficient.

**Challenges**:

**Data Handling**: Real-time monitoring of large amounts of network traffic can be resource-intensive. The system needs to process this data efficiently to avoid bottlenecks.

**Blockchain Scalability**: As the number of devices grows, the blockchain-based authentication system must remain fast and lightweight.

**AI Model Tuning**: Fine-tuning the AI models to minimize false positives or negatives in detecting threats could be challenging, particularly when deploying the system in new environments.

**Solutions**:

**Data Optimization**: Distributed data handling and processing techniques can be used to manage traffic efficiently.

**Customized Blockchain Protocols**: Optimization of the blockchain processes will ensure quick device authentication.

**Continuous Model Training**: AI models can be regularly updated and refined using real-world network data, improving their accuracy over time.

**Impact and Benefits**

The SCADA-Map tool has numerous benefits for organizations managing large SCADA networks. These benefits include:

**Enhanced Security**: The system prevents unauthorized devices from accessing the network while continuously monitoring for potential security threats.

**Increased Efficiency**: Automatic topology creation and anomaly detection reduce the need for manual monitoring, allowing network administrators to focus on more critical tasks.

**Real-Time Monitoring**: The real-time visualization feature helps administrators keep the network running smoothly, reducing downtime and improving response times to potential issues.

**Cost-Effective Solution**: By using open-source tools and requiring no additional hardware, the solution offers a budget-friendly option for securing large networks.

**Scalability**: Designed to handle even the largest networks, this system is suitable for industries that operate over vast geographical areas.

**Proactive Threat Detection**: The AI-driven anomaly detection identifies threats early, allowing for quick responses to minimize the risk of security breaches.

**User-Friendly Interface**: The web-based user interface simplifies network management, providing intuitive controls and real-time data for administrators.

**Conclusion:**

The SCADA-Map solution proposed by Team DenQueue is an innovative tool that addresses the need for secure and efficient automatic network topology discovery for SCADA systems. By combining modern technologies like blockchain, AI, and secure networking protocols, the system provides a robust solution for monitoring, managing, and protecting critical network infrastructure. Its scalability, cost-effectiveness, and focus on real-time security make it an invaluable asset for industries managing large and complex networks, ensuring continuous, secure operations.