Universidad de Puerto Rico

Recinto de Bayamón

Departamento de Ciencias en Computadoras

Python Host-Based Intrusion Detection System

User Manual

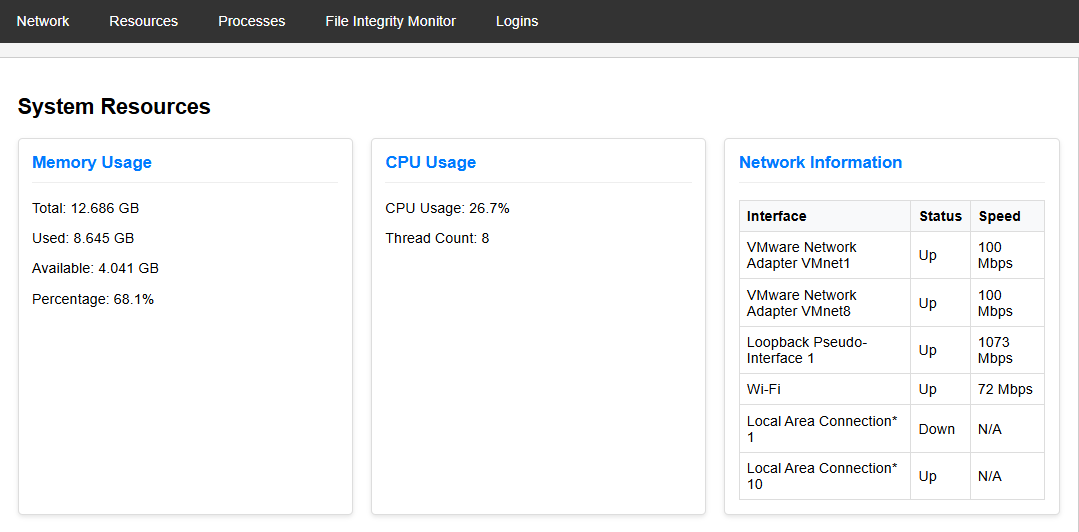
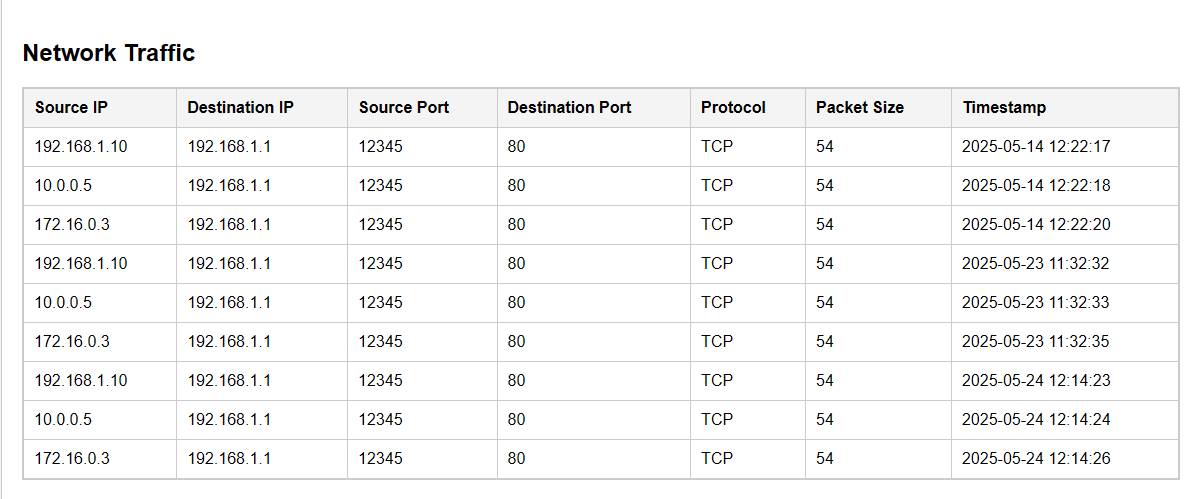
Jean L. González Milán

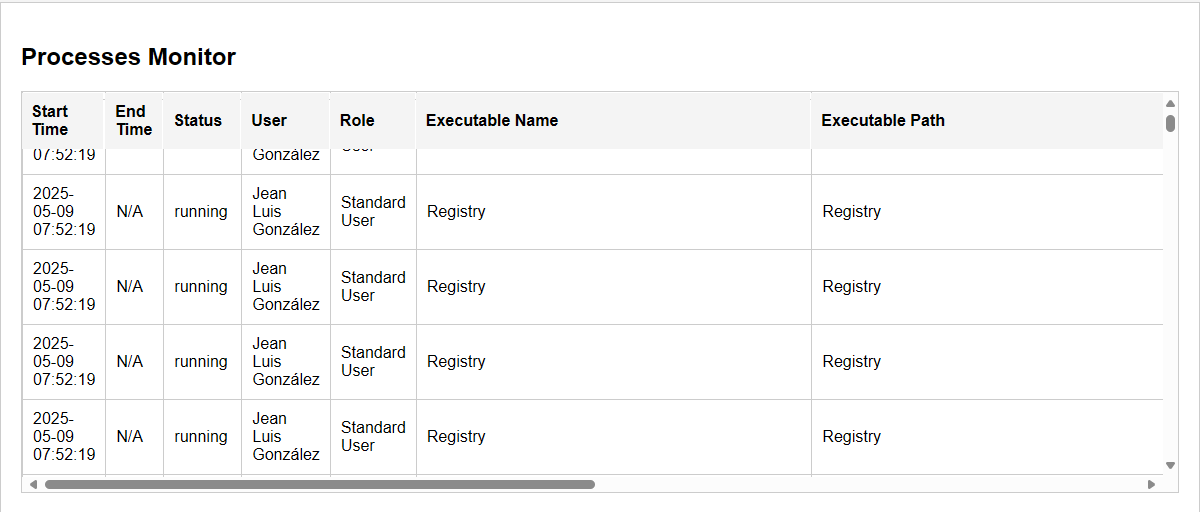
SICI-4038

Dr. Nelliud Torres Batista

**Table of Contents**

1. **Introduction………………………………………………………………..Page 3**
   1. Getting Started
2. **System Access**
   1. Navigate to the main page
   2. System Requirements
3. **Login………………………………………………………………………….Page 3**
   1. Default Credentials
   2. Accessing panel
4. **Dashboard Navigation…………………………………………………..Page 4**
   1. Description of the Dashboard
   2. Monitoring Tabs
5. **Network Monitoring……………………………………………………..Page 5**
   1. Traffic Visualization
   2. Blacklist Configuration
6. **System Resources……………………………………………………….Page 6**
   1. Performance Metrics
   2. CPU & Memory Usage
7. **Active Processes…………………………………………………………Page 7**
   1. Process Listing
   2. Resource Alerts
8. **File Integrity Monitoring………………………………………………..Page 8**
   1. Change Detection
   2. Directory Configuration
9. **Logout………………………………………………………………………..Page 9**
10. **Troubleshooting……………………………………………………….Page 9**
    1. Connection Issues
    2. Data Not Updating
11. **Contact Information……………………………………………….Page 10**
12. **Introduction**
    * **Welcome to the *Host Intrusion Detection System* (HIDS), a comprehensive security monitoring solution designed to:**
      + Supervise suspicious network traffic
      + Monitor real-time system performance
      + Detect unauthorized changes in critical files
      + Identify malicious processes or resource-heavy processes
13. **Access to the System**
    * **Navigate to the main page**
      1. Open your web browser
      2. Access the URL: [**http://localhost:500**](http://localhost:500)(Could subjected to changes based on your network configuration)
    * **System requirements**
      + Web browser
      + Administrator privileges for complete system access.
      + Python 3.12+ or higher version.
14. **Login**
    * **Default credentials** (Could subjected to changes based on your organization)
      + **User:** admin
      + **Password:** password
    * **Accessing panel**
      1. Complete the user and password fields
      2. A screenshot of a computer

         AI-generated content may be incorrect.Click the ***“Login”*** button  
           
         ***Figure 1:*** *Login Screen*
15. **Dashboard Navigation**
    * **Description of the Dashboard:**
      + **Top Bar:** System title
      + **Horizontal menu:** Monitor tabs
      + **Central area:** Visualization of data
    * **Monitoring tabs:**
      + **Network:** Displays suspicious traffic from blacklisted IPs
      + **Resources:** Shows CPU, memory, and network stats
      + **Processes:** Lists running processes with resource usage
      + **Files:** Tracks file changes (creation/modification/deletion)
      + **Logins:** Monitoring system logins  
          
        ***Figure 2:*** *View of system menu tabs*
16. **Network Monitoring**
    * **Traffic Visualization**
      + Displays:
        - Source/Destination IPs and ports
        - Protocol (TCP/UPD)
        - Packet size and timestamp
    * **Blacklist Configuration**
17. Edit ***blacklist.txt***in the root directory
18. Add one IP per line (e.g., 192.168.1.100).
19. Restart the service to apply changes  
      
    ***Figure 3:*** *Network traffic panel*
20. **System Resources**
    * **Performance Metrics**
      + CPU usage
      + Memory (Total / Used / Available in GB)
      + A screenshot of a computer

        AI-generated content may be incorrect.Network interfaces status  
         ***Figure 4:*** *System resources panel*
21. **Active Processes**
    * **Process Listing**  
      Display all running processes with:
      + Start/End times
      + User & Rol
      + Executable name & path
      + CPU & memory usage
      + Thread count
      + Usage Level  
        ***Figure 5:*** *Process Monitoring Table*
    * **Resource Alerts**
      + Normal <20%
      + Moderate 20-50%
      + Critical >50%
22. **File Integrity Monitoring**
    * **Change Detection**Tracks file events with:
      + Creation/Modification/Deletion Timestamps
      + CRC32 Checksums (for integrity verification)
      + A screenshot of a computer

        AI-generated content may be incorrect.User responsible  
        ***Figure 6:*** *File Integrity Alerts Table*
    * **Directory Configuration**  
      To modify monitored directories:
23. Edit ***main.py***
24. Update ***directories\_to\_monitor*** list to add the directories that should be monitored.
25. **Logout  
    Process of logging out of the dashboard**
26. Click the logout button on the bottom left corner
27. System redirects to login page

A screenshot of a computer dashboard

AI-generated content may be incorrect.

***Figure 7:*** *Logging out of panel*

1. **Troubleshooting**
   * **Connection Issues**
     + **Problem:** Dashboard won’t load
     + **Solution:** 
       - Ensure python ***main.py*** is running
       - Check if port 5000 is available (or the port that the network administrator configured)
   * **Data Not Updating**
     + **Problem:** Metrics are outdated
     + **Solutions:**
       - Verify all monitoring services are active
       - Check database connection(hids\_database.db)
2. **Contact Information**  
   For technical support:
   * **Email**: [support@hids.com](mailto:support@hids.com)
   * **Phone**: +1(787) 902-2942
   * **Hours**: Mon-Fri, 8am-5pm