Network Security Automation Toolkit
User's guide V1.0

Published 25th January 2025

Developed By

Tejas Seruwam

Tharinsa Ambepitiya

Nathaniel Fernandez

Dinuka Liyanage

Contents

1.Introduction

Overview of ARTEMIS.

ARTEMIS is a Network Security Automation Toolkit which is built to automate security . This application is a CLI console-based application. Our application's focus is to improve the security of a network and its network devices in a Small to Medium Enterprise (SMEs) by streamlining compliance checks, device management, security control implementation, and reporting.

ARTEMIS is built using Python 3.13 and can be launched on any platform which is compatible with running python. Built with a modular, scalable architecture for easy integration and future developments, ARTEMIS is designed to adapt and grow with your security needs.

ARTEMIS is not just a tool to use. It's a strategic advantage. Designed with industry trends and efficiency in mind, It transforms manual error-prone security tasks into seamless, automated workflows. Whether you are a network administrator, security analyst, or SME business owner, ARTEMIS equips you with the tools and insights necessary to **stay ahead of evolving cyber threats**.

Aim & Vision

Our Aim: Automate networking and network security configurations by enforcing security compliance checks and reducing human error in network administration.

Our Vision: To develop an application which is capable of fully automating the security aspects of a Network within a Small to Medium Enterprise and safeguard network against network vulnerabilities.

What's in it for you?

Why ARTEMIS Stands Apart:

- **Intelligent Security Automation**: Apply custom most used security controls and framework-based security controls, **scan for vulnerabilities** using compliance checking, and patch them with minimal manual intervention.
- **Dynamic Device Management**: Securely store and manage network device credentials, **automatically strengthen weak passwords**, and streamline SSH connectivity — all using AES-256 encryption with CBC mode.
- **Attack-Specific Defense Deployment:** Quickly mitigate network threats by selecting controls based on specific attack types or security frameworks such as CIS and NIST 800-53.
- **Comprehensive Compliance Checks**: Generate **insightful compliance reports**, benchmark your network security posture, and ensure adherence to critical standards.
- **Simulation-Ready Architecture:** Developed using a virtualized network that mimics real-world SME infrastructures, ARTEMIS is built with robust testing and validation.

What ARTEMIS Can do:

- Check security controls implemented within network devices in your network.
- Automates apply security controls within network devices.
- Reduces the amount of workforce to configure and secure networks.
- Automates compliance reporting for audits and assessments.
- Provides insights into lacking security controls and to which attacks your network is vulnerable for.
- Custom security control benchmarking and compliance scores.
- Increases the networks resistance against attacks

What ARTEMIS Can't do:

- Check all network device related security controls and provide insights into lacking security measures.
- Provide full coverage on network security automation to all types of network devices including device vendor, model, and version. Please read the supported devices section for more information.

2. Installation and Setup

1) **Install Files**:

To install ARTEMIS, you can **download the zip file** or the files from ARTEMIS github repository. After downloading, extract the zip files and open a terminal within that directory.

URL-

https://github.com/Dinuka7L/Artemis-NSAT 

2) **Install Dependencies**:

ARTEMIS is built upon Python 3.13; therefore, your device must have python 3.13 installed for the application to be run(**download python** - https://www.python.org/downloads/). It also uses the following external python libraries for its functionality. It is essential to have them downloaded into your device for launching ARTEMIS Successfully.

Make sure to install through all required dependencies that are installed using the requirements.txt file.

Run the following command:
command terminal: pip install -r requirements.txt

Internal & External Python Libraries used by ARTEMIS

- Json
- Colorama
- Netmiko
- Subprocess
- Sys
- Os
- Datetime
- Reportlab
- Collections
- PyPDF2
- Io
- Pathlib

3. Getting Started

Launching the Application

1. Navigating the Directory:

The directory structure is composed of 6 subdirectories and 15 scripts. Each function or feature is categorized under the relevant subdirectory and for code efficiency. To better understand the structure please refer to the image below.

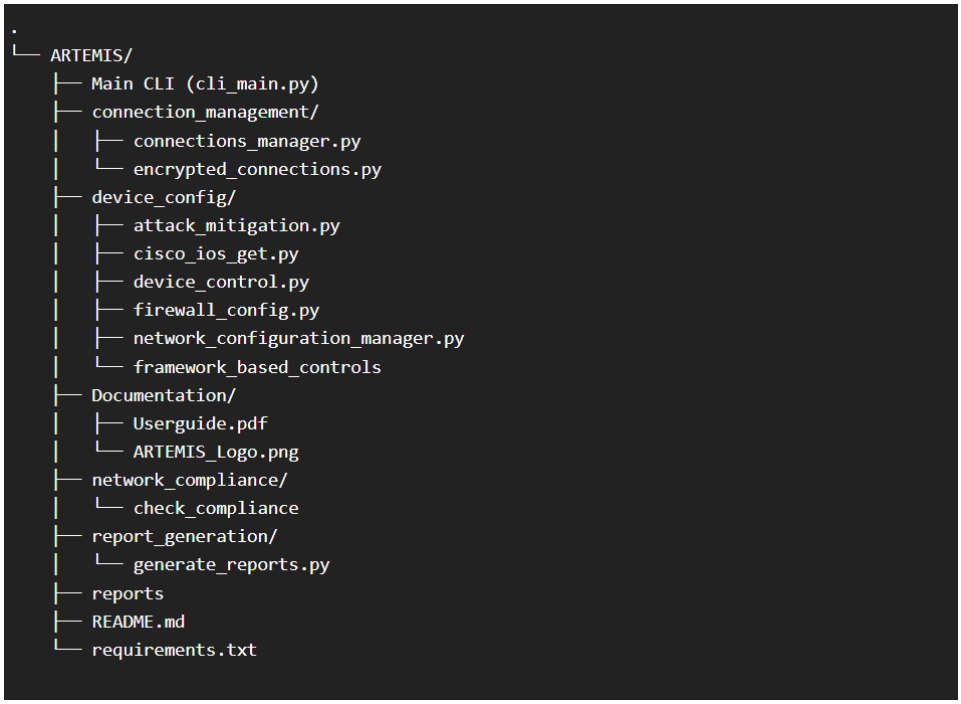


Figure1: Navigating ARTEMIS Directory

- **Main CLI (cli_main.py)** – To run ARTEMIS, launch this file using python 3.13
- **connection_management** - Includes modules for device SSH connection management
- **connections_manager.py** - User interface for management of devices securely
- **encrypted_connections.py** - For connecting with database and devices
- **device_config** - Includes device config retrieval and pushing modules
- **attack_mitigation.py** - Security controls to mitigate certain vulnerabilities
- **cisco_ios_get.py** - For retrieval of device configurations of CISCO IOS based devices
- **device_control.py** - For configuring security controls within CISCO IOS based devices
- **firewall_config.py** - For the configuration of firewall.
- **network_configuration_manager.py -** User interface of management of security controls in devices

- **Framework_based_controls –** To launch framework-based controls.
- **Documentation** - Includes Project Documentation
- **Userguide.pdf** - User's guide V1.0
- **ARTEMIS_Logo.png** – Logo of ARTEMIS
- **network_compliance** - Includes module for network compliance and benchmarking
- **check_compliance**
- **report_generation** - Includes module for generating report.
- **generate_reports.py**
- **reports** - Includes generated reports by generate reports
- **README.md** - Instructions
- **requirements.txt** - Download dependencies

2. Launch the Main Application:

Start the application by running the cli_main.py file:

```
python cli_main.py
```

4. Using ARTEMIS

Overview of the CLI Interface

The Command Line Interface of ARTMIS is composed of 3 main parts. 1. Information displayed. 2. User input. 3.Outputs. For ease of use, we have color coded different items displayed on the main user interface, and they are as follows:

- **White/Blue** – Options Displayed and Output results
- **Green** – Where user is prompted to input
- **Red** – Invalid inputs, errors.
- **Yellow** – Program termination

Command Prompt Area: The main section where you can type commands to interact with our application.

Feedback/Output Section: Displays the results, errors, or logs of the commands executed.

Figure2: ARTEMIS Main Menu

Main Menu

The Main Menu of ARTEMIS is composed of 6 options.

1. Device Management
2. Device Specific Configuration
3. Attack Mitigation
4. Enforce Framework based controls
5. Network Compliance and benchmarking
6. Exit

Upon selection of the option, you want to execute, the relevant sub module is executed using the subprocess function, opening the file related to the option you have chosen.

Option 1

Device Management

Once option one is selected you will be directed to the Network Connection Manager where you will be presented with four options:

1. **Add Device – To add SSH Credentials of the devices within your network**
2. **Show Devices – To display the saved device information**
3. **Remove Devices – To remove device information**
4. **Go Back to the main menu – Go to Main Menu**

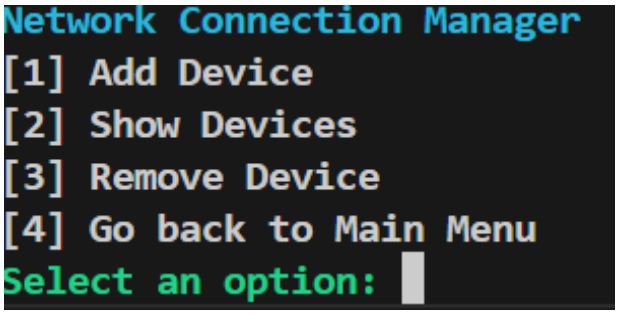


Figure 3: Network Configuration Manager Available Options

Adding Devices in the Network Connection Manager

ARTEMIS Soley **relies on Secure Shell(SSH)** to connect to devices in the network for the functionality of application. Therefore, before using ARTEMIS, it is required to implement SSH on network devices.

When selecting Option 1 (Add Device) from the Network Connection Manager menu, you can add a device by providing the required details. Below is a step-by-step breakdown of the process:

Device Category:
You will first be prompted to enter the type of device you wish to add. The available options are:
Router, Switch, Firewall, Server
Example: Enter router for a network router.

Device IP Address:
Enter the IP address of the device you want to add.
Example: 192.168.50.5.

Device Name:
Provide a unique and descriptive name for the device to identify it in the system.
Example: Border-Router-Test.

Username:
Enter the administrative username used to access the device.
Example: admin.

Current SSH Password:
Enter the current SSH password for the device to authenticate and establish a connection.
Example: admin123.

Current Enable Secret:
Enter the device's current enable secret. This is used to elevate privileges on the device.
Example: cisco.

Weak Secret Alert:
If the current enable secret is weak, the system will notify you. In this example, the secret “cisco” is deemed weak.

Updating the Enable Secret:

You will be prompted to update the enable secret if it is weak.

Enter a new, strong enable secret with at least 8 characters.
Example: thisisaverystrongpassword000.

Credential Update:
The system will update the credentials on the network device and notify you when the process is complete.

```
Network Connection Manager
[1] Add Device
[2] Show Devices
[3] Remove Device
[4] Go back to Main Menu
Select an option: 1
Enter device category (router, switch, firewall, server): router
Enter device IP: 192.168.86.1
Enter device name: router2
Enter username: admin2
Enter current SSH password: cisco
Enter current enable secret: cisco123
Your Current SSH Login Password is weak.
 Would you like to update the password?(y/n):y
Enter a new strong SSH password (at least 8 characters): ciscoadmin123
Updating credentials on the network device...
```

Figure 4: Setting up a router

Viewing Devices in the Network Connection Manager

When you select Option 2 (Show Devices) from the Network Connection Manager menu, the system will display a list of all the devices currently added. The output includes the following details for each device:

1. IP Address (IP): The IP address of the device.
2. Device Name (devicename): The name assigned to the device during the addition process.
3. Device Category (device_category): The type of device (e.g., router, switch, firewall).

How to Use:

- This feature helps you quickly view all connected devices, their categories, and IP addresses.
- It is useful for managing and verifying your network inventory.

```
Network Connection Manager
[1] Add Device
[2] Show Devices
[3] Remove Device
[4] Go back to Main Menu
Select an option: 2
Available devices:
{'ip': '192.168.86.4', 'devicename': 'DHCP-Router', 'device_category': 'router'}
{'ip': '192.168.90.1', 'devicename': 'PFSense', 'device_category': 'firewall'}
{'ip': '192.168.86.7', 'devicename': 'ENTERPRISE-L2', 'device_category': 'switch'}
```

Figure5: Displays available devices

Removing Devices

When you select Option 3 (Remove devices) from the Network Connection Manager menu, you will be presented with a prompt asking the IP address of the device you wish to remove. Upon correctly entering the IP address of the device, all records related to device will be removed from the application.

```
Network Connection Manager
[1] Add Device
[2] Show Devices
[3] Remove Device
[4] Go back to Main Menu
Select an option: 3
Enter the IP of the device to remove: 192.168.90.1

Network Connection Manager
[1] Add Device
[2] Show Devices
[3] Remove Device
[4] Go back to Main Menu
Select an option: 2
Available devices:
{'ip': '192.168.86.4', 'devicename': 'DHCP-Router', 'device_category': 'router'}
{'ip': '192.168.86.7', 'devicename': 'ENTERPRISE-L2', 'device_category': 'switch'}
```

Figure6: Removing a device

Option 2

Device-Specific Configuration

Once option two is selected, you will be presented with the following options:

1. Configuration Retrieve
2. Configuration Set

Configuration Retrieve

Once option one is selected you will be presented with the existing security controls

Retrieving Configuration of Routers

When selecting Option 1 (Retrieve Configuration of Routers) from the Network Configuration Manager menu, the system will:

- Select the routers you want to retrieve configurations currently managed by the system
- You are prompted to select a specific router from the list

Configuration Checks

After selecting a specific router, you will be presented with the following configuration checks that you can implement on your router:

Check if telnet is enabled: This security control checks if insecure Telnet protocol is enabled on the switch.

Check if ssh v2 is enabled: This security control checks if the secure SSH protocol (version 2) is enabled for remote access.

Check if password encryption is enabled: This security control checks if the passwords stored in the switch configuration are encrypted.

Check if privilege exec mode password is set: This security control makes sure that a password is required to access administrative functions.

Check if Cisco IOS version is up to date: This security control checks the current version of cisco that's running on the router and may compare it against known vulnerabilities or recommendations.

Check Message of the Day Warning: This security control verifies if a warning banner is displayed to users when they log in.

Check if Syslog is configured: This security control checks if the router is configured to send system logs to a logging server for monitoring and auditing.

Check Exec timeout settings: This security control checks if an inactivity timeout is set for remote sessions to prevent unauthorized access if a session is left open.

Selecting Checks:

You will be able to prompt the numbers of the specific checks you want to implement on the available interfaces.

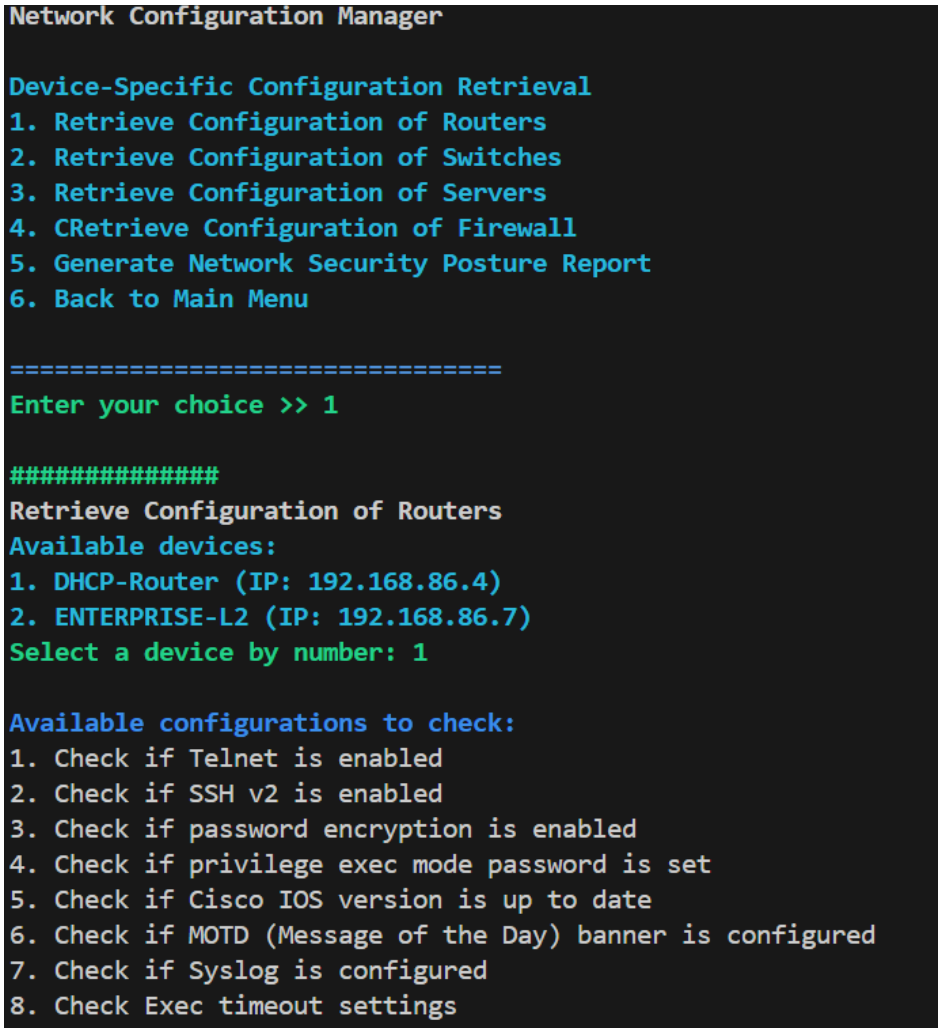


Figure 7: Retrieving configurations of routers

Retrieving Configuration of Switches

When selecting Option 2 (Retrieve Configuration of Switches) from the Network Configuration Manager menu, the system will display the available devices: Ex:

1. DHCP-Router
2. Border-Router
3. PfSense
4. ENTERPRISE-L2

Once you have selected an option, you will be presented with the following configuration checks which are available to implement on the Enterprise-L2 Switch.

Configuration Checks

1. **Check if telnet is enabled: This** security control checks if insecure Telnet protocol is enabled on the switch.

2. **Check if ssh v2 is enabled:** This security control checks if the secure SSH protocol (version 2) is enabled for remote access.

3. **Check if password encryption is enabled:** This security control checks if the passwords stored in the switch configuration are encrypted.

4. **Check if privilege exec mode password is set:** This security control makes sure that a password is required to access administrative functions.

5. **Check IOS Version:** This security control checks the version of the Cisco IOS running on the switch.

6. **Check Message of the Day Warning:** This security control verifies if a warning banner is displayed to users when they log in.

7. **Check logging status:** This security control checks if logging is enabled to record important events.

8. **Check Remote Login Execution Timeout:** This security control verifies if a timeout is set for remote login sessions.

9. **Check Port Security status in switch:** This security control checks if port security is enabled to limit the number of devices connected to a port.

10. **Check BPDU Guard:** This security control checks if BPDU Guard is enabled to prevent spanning-tree attacks.

11. **Check Root Guard:** This security control checks if root guard is enabled to prevent unauthorized switches from becoming the root bridge.

12. **Check Administratively Shutdown Ports:** This security control checks if unused ports are administratively shut down.

13. **Check Administratively Active Ports:** This security control checks which ports are actively enabled for communication.

14. **Check DTP Nonegotiate Ports:** This security control checks if DTP negotiation is disabled on access ports to prevent VLAN hopping or setting port to trunk by unauthorized users.

15. **Check CDP Disabled Ports:** This security control checks if CDP is disabled on access ports to reduce information leakage.

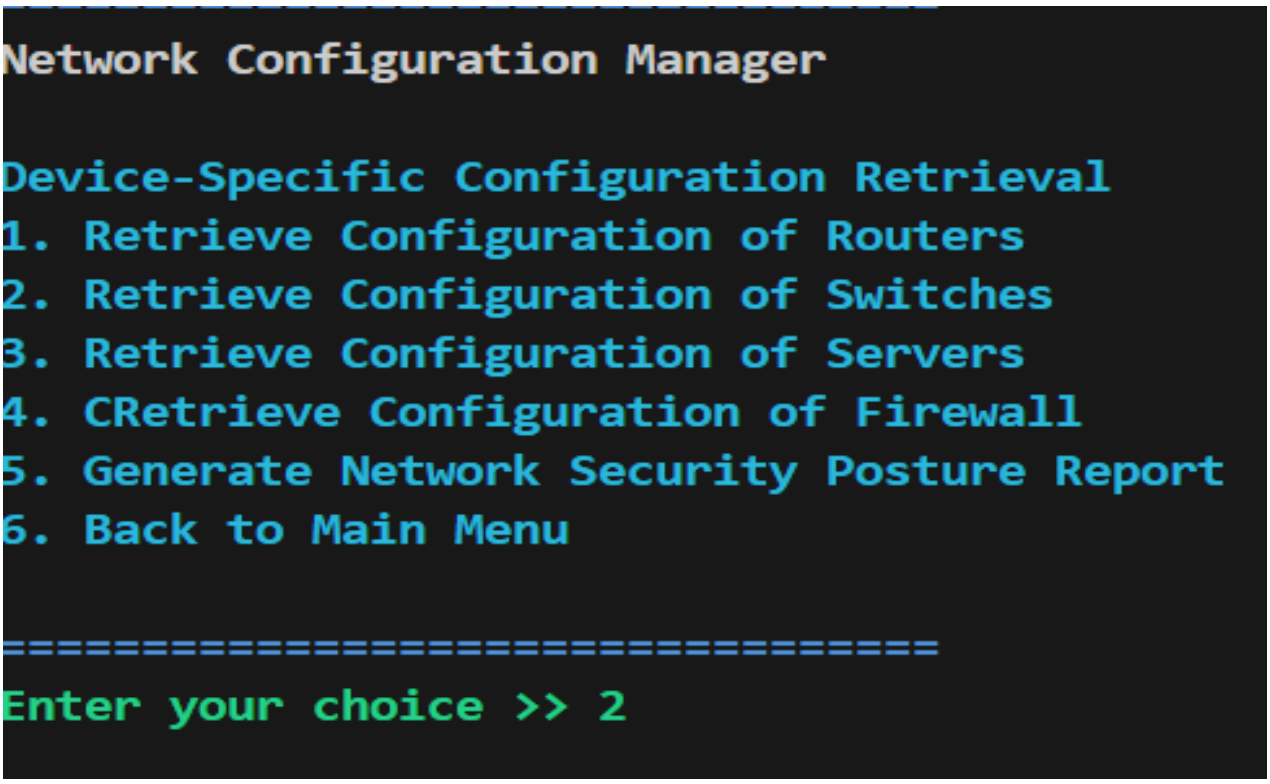
16. **Check IP DHCP Snooping Status:** This security control checks if DHCP snooping is enabled to prevent rogue DHCP servers.

17. **Check IP ARP Inspection Status:** This security control checks if ARP inspection is enabled to prevent ARP poisoning attacks.

18. **Check Login Fail Lock Status:** This security control checks if login fail lock is enabled to prevent brute-force attacks.

Selecting Checks:

You will be able to prompt the numbers of the specific checks you want to implement on the available interfaces.



```
Enter your choice >> 2

###############
Retrieve Configuration of Switches
Available devices:
1. DHCP-Router (IP: 192.168.86.4)
2. ENTERPRISE-L2 (IP: 192.168.86.7)
Select a device by number: 2

Switch Configuration Checks:
1. Check if telnet is enabled
2. Check if ssh v2 is enabled
3. Check if password encryption is enabled
4. Check if privilege exec mode password is set
5. Check IOS Version
6. Check Message Of the Day Warning
7. Check logging status
8. Check Remote Login Execution Timeout
9. Check Port Security status in switch
10. Check BPDU Guard
11. Check Root Guard
12. Check Administratively Shutdown Ports
13. Check Administratively Active Ports
14. Check DTP Nonegotiate Ports
15. Check CDP Disabled Ports
16. Check IP DHCP Snooping Status
17. Check IP ARP Inspection Status
18. Check Login Fail Lock Status
19. Back to Main Menu
Enter the numbers of the checks to perform (e.g., 1,3,5): 1,4,5,7,11,15,17
```

Figure8: Retrieving configurations of switches

Retrieving Configuration of Servers

When selecting Option 3 (Retrieve Configuration of Servers) from the Network Configuratin Manager menu, the system will open retrieval of firewall rules.

Option – 3

Attack Mitigation

Once option three is selected (Attack Mitigation) under the main menu you will be presented with the following attacks you can mitigate to reduce the risk to network users.

1. Disable Telnet (Unauthorized Access)
2. Password Encryption (Password Attacks)
3. Enable Secret (Password Attacks)
4. Port Security (MAC Address Overflow)
5. MOTD Banner (Unauthorized Access)
6. Exec Timeout (Unauthorized Access)
7. Syslog Configuration (Logging)
8. BPDU Guard (STP Attack)
9. Root Guard (STP Attack)
10. Shutdown Ports (Network Misconfigurations)
11. Activate Ports (Network Misconfigurations)
12. Disable DTP (Network Misconfigurations)
13. Disable CDP (Network Misconfigurations)
14. DHCP Snooping (DHCP Starvation)
15. Dynamic ARP Inspection (Data Integrity)
16. Login Block (Brute-force Prevention)

Using the Attack Mitigation Menu

1. **Select Mitigations:** Enter the numbers corresponding to the mitigations you wish to apply, separated by commas (e.g., "1,2,5" to disable Telnet, enable password encryption, and configure the MOTD banner).
2. **Select Device:** After selecting the mitigations, the system will display a list of available devices (routers and switches). Select the device you want to configure by entering its corresponding number.
3. **Configuration Application:** The system will then connect to the chosen device and apply the selected mitigations.

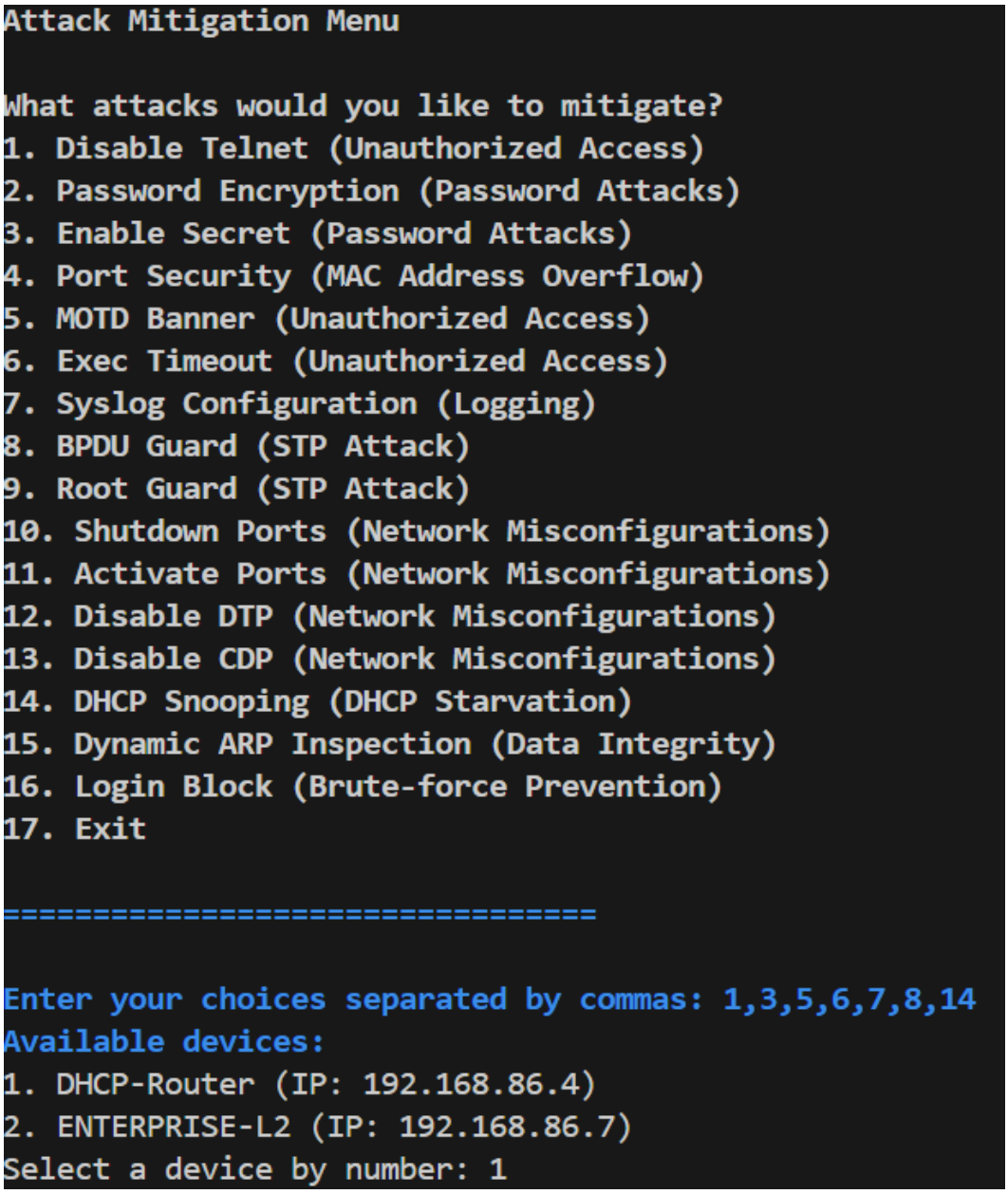


Figure 9: Navigating attack mitigation menu

Framework based controls – Option 4

Once option four is selected (Framework based controls based on the main menu you will be able to enforce the following security controls based on your security framework:

NIST Controls SP 800-53

AC-6-3: Network Access to Privileged Commands

Applicable device/s: Network Devices (e.g., routers, switches)

Description: Ensures that privileged commands can only be carried out via secure connections over the network.

Why do you need it?

Improves security for key system functions by preventing unauthorized execution of elevated commands.

Categories/ Key words: Privilege Escalation, Network Security

CP-9: Information System Backup

Applicable device/s: Servers, Administrative Systems

Description: Restricts the use of privileged accounts to authorized purposes only

Why do you need it?

Ensures security of privileged accounts and reduces risk of misuse or overuse

Categories/ Key words:

Privileged Accounts, Role-Based Access Control (RBAC)

CIS V7 Controls

1.3 - Use of System Logging

Applicable device/s: DHCP Server, Firewall, Routers, switches

Description: enable and utilize logging to maintain a record system logs, monitor network devices, detect unauthorized access, and support troubleshooting.

Why do you need it?

Tracks network activity, aids in identifying unauthorized access, and simplifies troubleshooting processes.

Categories/ Key words: Logging, IP Management, Troubleshooting

4.3 - Configure automatic session lock

Applicable device/s: Workstation, laptops, VM, routers, switches

Description: Set up automatic session locks to protect devices when left unattended.

Why do you need it?

Prevents unauthorized access during idle periods.

Categories/ Key words: Security, Session Management

11.2 - Perform Automated Backups

Applicable device/s: Servers, VM, Router, switch

Description: Schedule regular automated backups to secure critical data

Why do you need it?

Protects data from loss due to hardware failure or cyberattacks.

Categories/ Key words: Backup, Data Protection

12.3 - Securely manage network infrastructure

Applicable device/s: Routers, Switches, Firewalls

Description: Implement secure protocols and configurations for managing network devices. This includes disabling older versions of SSH and Telnet.

Why do you need it?

Mitigates risks of unauthorized access to critical infrastructure.

Categories/ Key words: Network Security, Protocol Management

13.9 - Deploy port level access control

Applicable device/s: Switches, router, server, Firewall, VM

Description: Enforce access control policies at the port level to limit unauthorized device connections.

Why do you need it?

Enables real-time monitoring and quicker threat detection

Categories/ Key words:

Event Monitoring, Threat Detection, Access Control, Port Security

(Option – 5)

Network Compliance and Benchmarking

Once option one is selected you will be directed to the Network Connection Manager where you will be presented with four options:

1. Apply CIS Controls
2. Apply NIST Controls
3. Apply Selective Controls
4. Back to Main Menu

Apply CIS Controls (Option 1)

This option would apply a set of security controls based on the CIS (Center for Internet Security) Benchmarks.

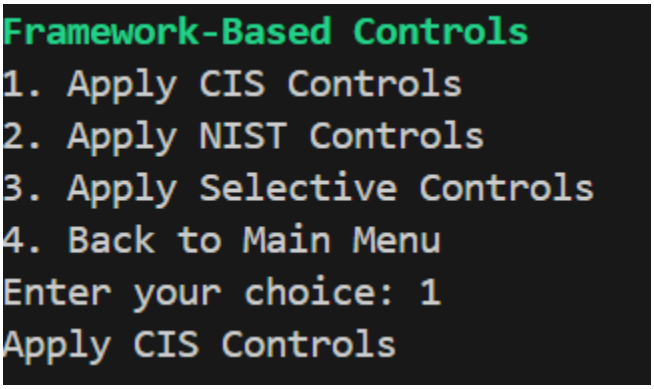


Figure10: Applying CIS controls

Apply NIST Controls (Option 2)

This option would apply a set of security controls based on NIST (National Institute of Standards and Technology) guidelines.

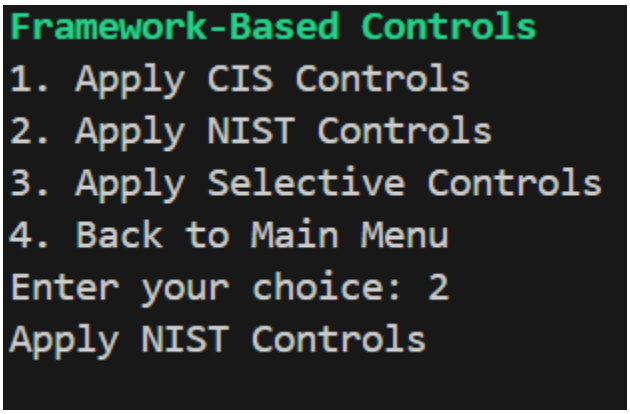


Figure11: Applying NIST controls

Contact and Support

Dinuka Liyange - 10601996 dhikkadu@our.ecu.edu.au

Tharinsa Ambepitiya-10658677 tambepit@our.ecu.edu.au

Tejas Seruwam – 10623733 tseruwam@our.ecu.edu.au

Nathaniel Fernandez –10676219 ndfernan@our.ecu.edu.au