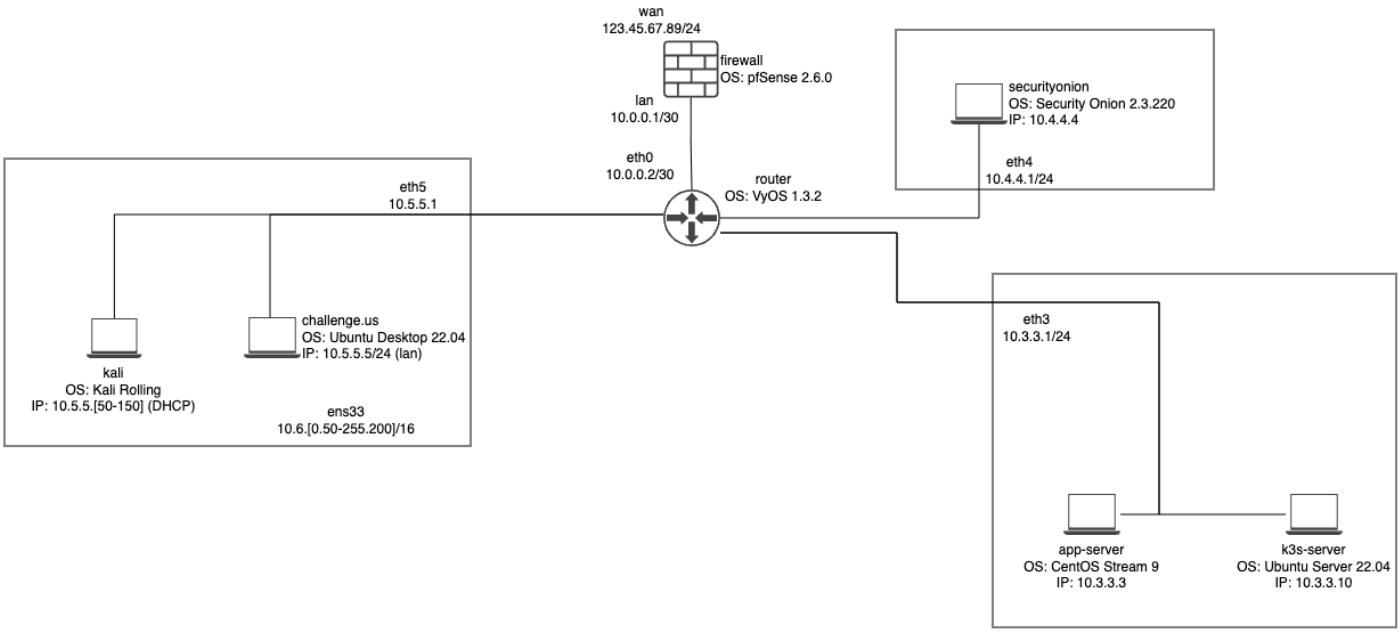
The *DAUNTED* – Security Controls Document

1. Introduction

This Security Controls Document applies to the *Daunted* network infrastructure. It is the responsibility of all employees, contractors, consultants, temporary, and other workers on board the *Daunted* of making sure controls below are enforced.

ATTENTION: All VM login passwords **should** remain the provided default password (***tartans***). Changing so goes against the Vulnerability Assessments conducted within the *Daunted* and will cause the provided "Compliance Assistant" to fail.



2. Scope

This document covers the following aspects of the *Daunted* security controls:

- Password management
- Secret management
- Network security
- Configuration Security
- Environment verification

3. Security Controls

3.1 Password management

- Passwords must meet uniqueness and complexity requirements as mentioned below:
    - Minimum length: 12 characters
    - At least one uppercase letter
    - At least one lowercase letter
    - At least one number
    - At least one special character
- In applications that allow users to create their own account, you must enforce password complexity by correctly configuring the necessary options.

3.2 Secret management

- Sensitive information, such as passwords, should not be included in Kubernetes deployment manifests. Instead, they should be stored in separate secrets and accessed through environment variables.

- Unused secrets should be removed from the cluster to reduce the risk of unauthorized access.

3.3 Network security

- Only required ports should be open, and unnecessary firewall rules should be removed. This helps reduce the attack surface of the Kubernetes cluster and prevent unauthorized access.

  IMPORTANT: Due to time constraints, you will only need to UDP scan the pfSense router. Scanning other hosts and networks will delay completion of the challenge.

Table 1: List of Authorized Open Ports

Port	Server	Justification
TCP 22	All Linux hosts	Remote management
TCP 5000	App Server	Docker Registry Instance
TCP 80,443	Kubernetes Server	Roundcube Mail Keycloak PGAdmin
TCP 8065	Kubernetes Server	Mattermost Chat
TCP 80,443	SecOnion Server	SecOnion webapp
TCP 514	SecOnion Server	Syslog server
TCP 8090	SecOnion Server	Osquery endpoint
TCP 9200	SecOnion Server	Elasticsearch REST API
TCP/UDP 53	pfSense	DNS resolver
TCP 80,443	pfSense	Firewall webapp
UDP 123	pfSense	NTP server

Table 2: List of Authorized Firewall Rules

Protocol	Source	Destination	Action	Interface
*	RFC 1918	Any	Block	WAN
*	Reserved/Not Assigned by IANA	Any	Block	WAN
TCP 443	ANY	10.7.7.7	Allow	WAN
TCP 80	ANY	10.7.7.7	Allow	WAN
TCP 80/443	ANY	LAN IP	Allow	LAN
IPv4	LAN	ANY	Allow	LAN
IPv6	LAN	ANY	Allow	LAN

3.4 Configuration security

- SSH access should not be allowed as the root user. This is a common security vulnerability that can be exploited by attackers.

3.5 Environment verification

- After redeploying the cluster, each deployment should have come back up to its normal state and allow login with no problems or errors. This makes sure modifications to the environment did not affect its Availability.