Challenge #T0187

Engineer's Audit Advice

*Author: Bailey Kasin*  
**Framework Category:** Protect and Defend  
**Specialty Area:** Cybersecurity Defense Analysis  
**Work Role:** Cyber Defense Analyst  
**Task Description:** Plan and recommend modifications or adjustments based on exercise results or system environment.  
**Scenario**

Ashley Steele has run an auditing scan on our core Linux boxes and given recommendations on how to better secure them. We need you to implement the fixes.

**Additional Information**

More details and objectives about this challenge will be introduced during the challenge meeting, which will start once you begin deploying the challenge.  
  
You will be able to check your progress during this challenge using the check panel within the workspace once the challenge is deployed. The checks within the check panel report on the state of some or all of the required tasks within the challenge.  
  
Once you have completed the requested tasks, you will need to document the methodology you used with as much detail and professionalism as necessary. This should be done on the documentation tab within the workspace once the challenge is deployed. Below the main documentation section be sure to include a tagged list of applications you used to complete the challenge.  
  
Your username/password to access all virtual machines and services within the workspace will be the following...  
Username: playerone  
Password: password123  
  
The username/password used to access the Firewall's web interface within the workspace will be the following...  
Username: admin  
Password: password123

Links used:

**Prod-Joomla HTTP-6640:** <https://phoenixnap.com/kb/apache-mod-evasive>

**Prod-Joomla HTTP-6641:** [**https://ourcodeworld.com/articles/read/950/how-to-protect-your-apache-server-from-dos-attacks-denial-of-service-using-the-quality-of-service-qos-module-on-ubuntu-1604**](https://ourcodeworld.com/articles/read/950/how-to-protect-your-apache-server-from-dos-attacks-denial-of-service-using-the-quality-of-service-qos-module-on-ubuntu-1604)

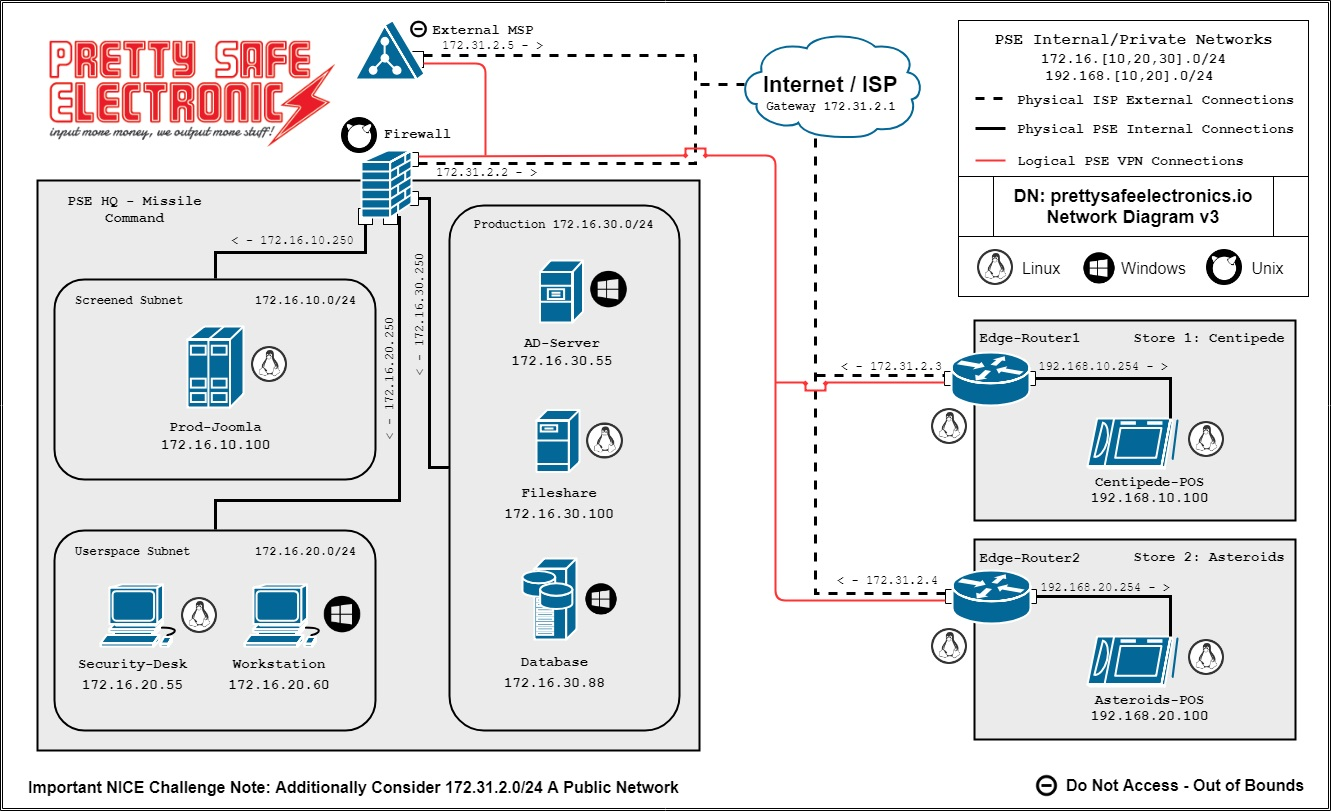
**Prod-Joomla AUTH-9262 and AUTH-9286 and Ashley Request:** [**https://www.cyberciti.biz/faq/securing-passwords-libpam-cracklib-on-debian-ubuntu-linux/**](https://www.cyberciti.biz/faq/securing-passwords-libpam-cracklib-on-debian-ubuntu-linux/)

**Prod-Joomla DEB-0880:** [**https://linuxize.com/post/install-configure-fail2ban-on-debian-10/**](https://linuxize.com/post/install-configure-fail2ban-on-debian-10/)

**Fileshare DEB-0880:** [**https://linuxize.com/post/install-configure-fail2ban-on-debian-10/**](https://linuxize.com/post/install-configure-fail2ban-on-debian-10/)

**Fileshare ACCT-9622:** [**https://linuxhint.com/enable-process-accounting-ubuntu/**](https://linuxhint.com/enable-process-accounting-ubuntu/)

**Fileshare AUTH-9262 and AUTH-9286 and Ashley Request:** [**https://www.cyberciti.biz/faq/securing-passwords-libpam-cracklib-on-debian-ubuntu-linux/**](https://www.cyberciti.biz/faq/securing-passwords-libpam-cracklib-on-debian-ubuntu-linux/)



NICE Framework KSA

* K0002. Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
* K0004. Knowledge of cybersecurity and privacy principles.
* K0005. Knowledge of cyber threats and vulnerabilities.
* K0007. Knowledge of authentication, authorization, and access control methods.
* K0075. Knowledge of security system design tools, methods, and techniques.
* K0167. Knowledge of system administration, network, and operating system hardening techniques.
* K0318. Knowledge of operating system command-line tools.
* S0167. Skill in recognizing vulnerabilities in security systems. (e.g., vulnerability and compliance scanning).

CAE Knowledge Units

* Basic Cyber Operations
* Cybersecurity Foundations
* Cybersecurity Principles
* Cyber Threats
* Linux System Administration
* Network Defense
* Operating Systems Hardening
* Security Program Management
* Web Application Security
  + - * QS\_ClientEntries 100000
      * QS\_SrvMaxConnPerIP 50
      * MaxClients 256
      * QS\_SrvMaxConnClose 180
      * QS\_SrvMinDataRate 150 1200