Assignment 3:  
IPA Server Hardening

*Kyle Walker*

*NETW2500*

*10/21/2024*

Table of Contents

[Glossary: 2](#_Toc180409050)

[Task 2: Setup Logging and Security 2](#_Toc180409051)

[Server Hardening Methods: 3](#_Toc180409052)

[Task 3: 3](#_Toc180409053)

# Glossary:

1. **ElasticSearch:** Like a search engine, but for JSON requests. Works as a large database with searching and analytic abilities. (Knowi)
2. **Rsyslog:** Rsyslog stands for “Rocket-Fast System for Log processing”. It allows users to accept a variety of inputs, transform them and output them to many different places for logging purposes. It also works with ElasticSearch. (Rsyslog)
3. **REK/ELK:** The ELK Stack refers to **E**lasticSearch, **L**ogstash, **K**ibana. This stack allows users to gather logs, analyze them and create graphs and charts for fast troubleshooting, security, etc. (Amazon, n.d.)
4. **Logstash:** Logstash allows administrators to gather data and transform it and send it to another location for logging. (Amazon, n.d.)
5. **Kibana:** FreeIPA uses Kibana for data display and dashboards alongside ElasticSearch and rsyslog for a Centralized Logging Server. Kibana is commonly referred to as REK, ELK servers. (FreeIPA)

# Task 2: Setup Logging and Security

I was unable to get the Kibana dashboard operational, but I did try a few troubleshooting steps to try and resolve my issue.

First, I tried double-checking my Docker install to ensure that Kibana was installed correctly by pulling the “hello-world” from Docker itself, thus updating my Docker installation. After that didn’t work, I tried reloading from my PostA2 snapshot, assuming there was an issue with either my Docker or Kibana installation.

Secondly, after some research I discovered the script is only working on older versions of Python, so I tried using a shebang command alongside sudo to launch the script with an older version. No errors appeared after the command, but the Kibana dashboard was still not available.

“#! /usr/bin/env python2.7 ipa\_log\_config.py -target 192.168.203.30”

I also tried to rewrite the script from Python 2 to Python 3 using an automated client <https://python2to3.com/> but after running the new script, nothing happened.

## Server Hardening Methods:

1. I began my server hardening by forcing strong passwords by editing my /etc/pam.d/system-auth file and adding a line to require a minimum length and only permit 3 retries to prevent brute force attacks.
2. I also disabled SSH to prevent any unauthorized access without my knowledge or permission. I made sure to write down my commands in case SSH is required for future assignments or troubleshooting.
3. I also blocked USB Storage to prevent any physical attacks on the system itself by adding some lines to /etc/modprobe.d/blacklist.conf and /etc/rc.local

# Documentation and Backups:

# A screenshot of a computer Description automatically generated

*CentOS Gold Copy Properties*