Name: Hassan Alshehri.

Email: has1215@rit.edu.

Team: Blue Team.

Semester: Fall 2023

Ansible Script Usage Information:

In my Ansible scripts provided are aimed at automating the deployment and configuration of an Apache web server. The goal is to simplify and accelerate the process of setting up a web server, ultimately enhancing efficiency. I bilevel a standardized and secure Apache web server setup provides a strong foundation for security.

Target System Requirements:

I think you can run the tasks but maybe you need to try this command.

```
Sudo ansible-playbook apache_setup.yml -I hosts -Kk
```

Answers to Questions:

What is the goal of these Ansible scripts? What purpose does it bring to the Gray team effort (or possibly Red or Blue)?

The main purpose of these Ansible scripts is to automate the installation of an Apache web server. This simplifies and speeds up the process of setting up a web server, which is a critical activity for any Blue Team. This automation increases the efficiency of the Blue Team and allows them to devote more time to critical security components such as monitoring, incident response, and vulnerability assessments. The Blue Team may improve their security posture and respond effectively to any security attacks by swiftly deploying a standardized and safe Apache web server.

What was the most challenging aspect of working with Ansible?

The most challenging aspect of working with Ansible was maintaining the right balance between flexibility and simplicity. Creating a playbook that can be easily customized to suit various environments while ensuring it remains easy to read and understand was a delicate task. Striking this balance ensures that the playbook can adapt to different needs and configurations while remaining accessible to team members, even those with varying levels of experience with Ansible.

If you were to expand this Ansible script, what would you add?

If I were to expand this Ansible script for the Blue Team, I would incorporate additional security measures. This could involve tasks such as setting up a firewall to control traffic, enabling HTTPS with SSL certificates to enhance data security, and integrating intrusion detection systems like Snort or OSSEC for proactive monitoring. Additionally, tasks for regular security updates and patches to the Apache server would be included to ensure the server is up to date with the latest security enhancements. Integration of centralized logging and automated backup mechanisms would also be added to enhance overall security and resilience. These additions would contribute to a more comprehensive and secure web server setup for the Blue Team.