Wicked Quick Wazuh

Setup Wazuh central server and forwarding agents

Type of Systems: Debian, Ubuntu, CentOS, etc
Necessary Skills: Linux admin, basic understanding of ELK & SIEM usage
Complete Goal: Bootstrap Wazuh, Register forwarding agents

Wazuh Stack Install:

1. Pull down and run install script
   (can copy from wazuh.com -> Docs -> Install guide)

```
sudo curl -so ~/all-in-one-installation.sh
https://raw.githubusercontent.com/wazuh/wazuh-documentation/4.1/resources/open-distro/unattended-installation/all-in-one-installation.sh &&
sudo bash ~/all-in-one-installation.sh
```

2. Pull down password changing script:
   (can copy from wazuh.com -> Docs -> Install guide -> User Manual -> Elastic tuning)

```
curl -so wazuh-passwords-tool.sh
https://raw.githubusercontent.com/wazuh/wazuh-documentation/4.1/resources/open-distro/tools/wazuh-passwords-tool.sh
```

3. Get rid of default creds:
   a. Run password change script:
      `sudo bash wazuh-passwords-tool.sh -a > passwords`
   b. Copy these out to somewhere **safer** or **limit** permissions/ownership of this file
   c. Add usable password, remove password from history:
      `sudo bash wazuh-passwords-tool.sh -u admin -p <password> ; history -d $(history 1)`
4. Change permissions for kibana:
   a. `chmod 640 /etc/kibana/kibana.yml`
   b. sudo chown kibana:kibana /etc/kibana/kibana.yml
5. Edit `/etc/kibana/kibana.yml` and update kibanaserver password
6. Edit `/etc/filebeat/filebeat.yml` and update admin password
7. Restart both filebeat and kibana:
   a. `sudo systemctl restart kibana filebeat`
8. Minimal security on Wazuh-API(mitigate default creds):
   a. Edit `/var/ossec/api/configuration/api.yaml`, uncomment the host line and set host to 127.0.0.1

    b. Restart wazuh manager
    c. `sudo systemctl restart wazuh-manager`

9. Test out the kibana by going to https://<wazuh-ip>/ and logging in w/ admin creds
10. Set up groups if necessary, and under Settings->Configuration under General, set the Enrollment DNS to the Wazuh server IP or FQDN.

Wazuh Agent Install:

1. Get Wazuh Admin credentials and Wazuh IP/FQDN from whoever set up the Wazuh (a.k.a. the Wazuh wizard)
2. Log into Wazuh at https://<wazuh-ip>/
3. Installation:
    a. Navigate to Wazuh->Agents and select “Deploy new agent”
    b. Select your OS
    c. Select Architecture if prompted (hint: x86_64 == 64bit)
    d. Follow the steps, using the default group unless told otherwise by the Wazuh wizard.

Appendix:

Port usage:

- 1515 TCP for registration
- 1514 TCP for logs

Custom File monitoring:

https://documentation.wazuh.com/current/user-manual/capabilities/file-integrity/fim-configuration.html#configuring-syscheck-basic-usage