Setup Notes

systemctl - manage services (start/stop Wazuh manager)
tail -f - to view the logs in real time
ping - to verify connection between the two VM's
curl - to install my packages needed

11/08:
Setup Kali Linux VM and Ubuntu VM
Bridged a connection between the two VM's

Installed Wazuh on my Ubuntu by doing:

```
curl -s0 https://packages.wazuh.com/4.9/wazuh-install.sh
sudo bash wazuh-install.sh -a
```

Dashboard URL: https://wazuh-dashboard-ip:443
User: admin
Password: P9x?N[REDACTED]
Ubuntu IP: 192.168.[REDACTED]

11/09:
Installed Wazuh agent on my Kali-endpoint VM by doin:

```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.9.1-1_amd64.deb
sudo dpkg -i wazuh-agent_4.9.1-1_amd64.deb
```

Opened the config file to add my Ubuntu manager IP by doing:

```
sudo nano /var/ossec/etc/ossec.conf
```

updated the IP
then started the agent by doing:

```
sudo systemctl enable wazuh-agent
sudo systemctl start wazuh-agent
```

To generate brute force attempts I did:

```
sudo su -
for i in {1..5}; do su testuser; done
```

To port scan I did:

```
nmap -sS 127.0.0.1
```

To Modify protected file (FIM event) I did:

```
sudo touch /etc/fimtest_file
sudo echo “changed” | sudo tee -a /etc/fimtest_file
```