Lynis and Fail2ban

FreeBSD:

Lynis-

PREREQUISITE: install git

`git clone` https://github.com/CISOfy/lynis
To clone lynis from git

Make sure the following are run in the lynis file
`lynis audit system`
To run an audit on the system

`lynis audit dockerfile`
To run an audit on a dockerfile

`./lynis -c`
To run a check

`./lynis -c -Q`
To run a check without user input

`vim /var/log/lynis.log`
To see the full logs

Centos 7:

Lynis-

`yum install epel-release`
`yum install lynis`
To install lynis

Make sure the following are run in the lynis file
`lynis audit system`
To run an audit on the system

`lynis audit dockerfile`
To run an audit on a dockerfile

`./lynis -c`
To run a check

`./lynis -c -Q`
To run a check without user input

`vim /var/log/lynis.log`
To see the full logs

Fail2ban-

`yum install epel-release`
`yum install fail2ban fail2ban-systemd`
To install fail2ban

`systemctl enable fail2ban`
`systemctl start fail2ban`
To enable and start fail2ban

`cp -pf /etc/fail2ban/jail.conf /etc/fail2ban/jail.local`
To make a copy of the jail.conf file and save it with the name jail.local

`vim /etc/fail2ban/jail.local`
To configure the conf file

Ubuntu:

Lynis-

`apt install lynis`
To install lynis

Make sure the following are run in the lynis file
`lynis audit system`
To run an audit on the system

`lynis audit dockerfile`
To run an audit on a dockerfile

`./lynis -c`
To run a check

`./lynis -c -Q`
To run a check without user input

`vim /var/log/lynis.log`
To see the full logs

Fail2ban-

`apt-get fail2ban`
To install fail2ban

`systemctl enable fail2ban`
`systemctl start fail2ban`
To enable and start fail2ban

`cp -pf /etc/fail2ban/jail.conf /etc/fail2ban/jail.local`
To make a copy of the jail.conf file and save it with the name jail.local

`vim /etc/fail2ban/jail.local`
To configure the conf file