**WSL Config**

**Create Sudo Users Group:**

# sudo visudo

# %<group name> ALL=(ALL) ALL

Add user to Sudo group:

# usermod -aG <Group Name> <Username>

Disbale Root:

#vim /etc/profile.d/restrict\_root.sh

# Add following content:

If [ “$(id -u)” –eq 0 ]; then

Echo “Root access is restricted. Exiting….”

Exit 1

Fi

# chmod +x /etc/profile.d/restrict\_root.sh

**Change default wsl user:**

# vim /etc/wsl.conf

#Add content:

[user]

Default = <username>

**Set default directory for user:**

# vim ./.bashrc

# Add content:

-Cd ~ (This will put the user in /home/<username>)

-WIN\_USER=$(cmd.exe /c “echo %USERNAME%” | tr –d ‘r’)

Cd /mnt/c/users/”$WIN\_USER” || exit (sets the default directory to the window user that is signed in to WSL)

OSCAP:

#sudo dnf install openscap-scanner scap-security-guide

#sudo oscap xccdf list –profiles /usr/share/xml/scap/content/ssg-rhel8-ds.xml

#sudo oscap xccdf eval –profile stig –results results.xml –report report.html /usr/share/xml/scap/content/ssg-rhel8-ds.xml

Remediate with

# sudo oscap xccdf eval –profile stig –remediate –results results.xml –report report.html /usr/share/xml/scap/content/ssg-rhel8-ds.xml

**Add yum server for dnf:**

#sudo vim /etc/hosts

Add content:

10.3.18.18 mdc-yum.mnet.local mdc-yum

Minimal Groupinstall:

#dnf grouplist

#dnf groupinstall “Minimal Install” –allowerasing

**Elastic Agent:**

**Install:**

Move the .tar from /mnt/c/Users/<Where ever the file is> do this in the /opt

# tar xvf elastic-agent-8.5.2-linux-x86\_64.tar

# cd elastic-agent-8.5.2-linux-x86\_64

# sudo ./elastic-agent install --url=https://mdc-fleet.mnet.local:8220 --enrollment-token=UV9kRXhZUUJiYmpxYXpVME9KRHc6d21zVkN5a3hUa2FWQzRhN1N3TWJXZw== --insecure

**Create elasticagent group and give sudo:**

# groupadd elasticagent

# usermod –aG elasticagent <user>

# visudo

-Add: %elasticagent ALL=(ALL) NOPASSWD: /opt/Elastic/Agent/elastic-agent run

**Give file permissions to group:**

# Chown –R :elasticagent /opt/elastic-agent-<version>-linux-x86\_64

# Chmod –R 750 /opt/elastic-agent-<version>-linux-x86\_64

# Chown –R /opt/Elastic

# Chmod 750 –R/opt/Elastic

# Chmod 770 /opt/Elastic/Agent/elastic-agent.log

**Script to run on login:**

**#** vim /etc/bashrc

-Add content at end of file:

If ! pgrep –f elastic-agent > dev/null; then

Sudo /opt/Elastic/Agent/elastic-agent run > /opt/Elastic/Agent/elastic-agent.log 2>&1 &

Fi

# ps aux (see if agent is running) or # jobs

# tail –f /opt/Elastic/Agent/elastic-agent.log (see if logs are working)