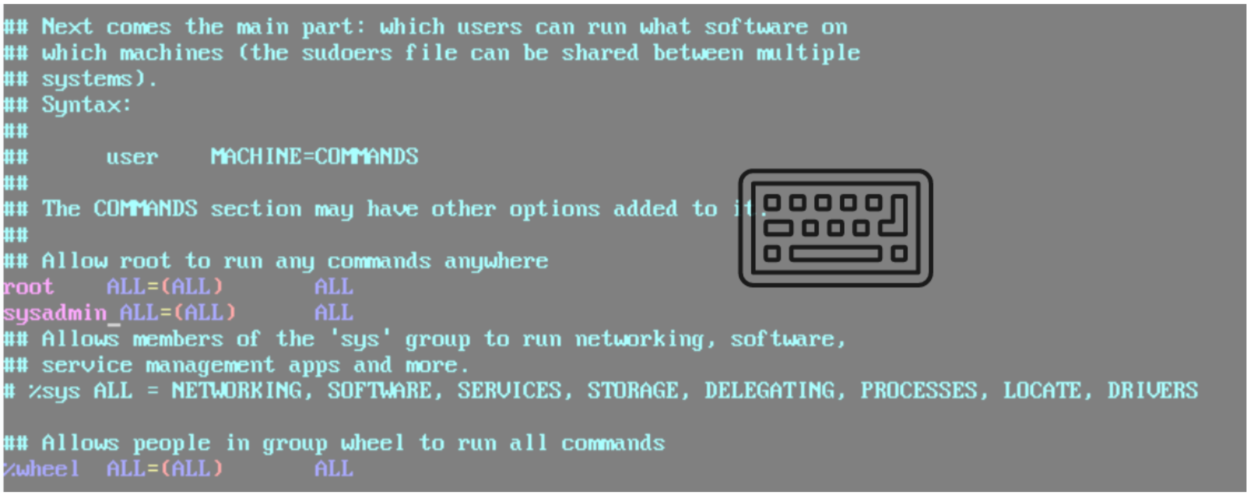
SPLUNK FIRST 15

1) Change password for sysadmin and root accounts

   Commands:
   passwd   (type pw twice)
   su sysadmin
   passwd   (type pw twice)

2) Switch back to root and run vi visudo. Add sysadmin to sudoers

   Commands:
   su root
   vi visudo



```
## Next comes the main part: which users can run what software on
## which machines (the sudoers file can be shared between multiple
## systems).
## Syntax:
##
##      user    MACHINE=COMMANDS
##
## The COMMANDS section may have other options added to it.
##
## Allow root to run any commands anywhere
root    ALL=(ALL)       ALL
sysadmin ALL=(ALL)      ALL
## Allows members of the 'sys' group to run networking, software,
## service management apps and more.
# %sys ALL = NETWORKING, SOFTWARE, SERVICES, STORAGE, DELEGATING, PROCESSES, LOCATE, DRIVERS

## Allows people in group wheel to run all commands
%wheel  ALL=(ALL)       ALL
```

3) Switch back to sysadmin and grab porygon.sh script, change permissions

   Commands:
   su sysadmin
   cd ~
   sudo curl https://raw.githubusercontent.com/Amberjar27/PoshFish-ForTheWin1/main/porygon.sh > porygon.sh
   chmod 755 porygon.sh

4) Run the firewall script using sudo

Commands:

```
sudo ./porygon.sh n
sudo firewall-cmd --zone=public --add-port=9998/tcp –permanent
```

5) Make splunk run as non-root user

Commands:

```
cd /opt
sudo /opt/splunk/bin/splunk stop
sudo chown -R splunk:splunk /opt/splunk
sudo /opt/splunk/bin/splunk enable boot-start -user splunk
sudo /opt/splunk/bin/splunk start
```

```
top       (TO TEST)
```

6) Change world writable files

Commands:

```
cd /opt/splunk/etc/apps/splunk_rapid_diag/bin/cli
chmod 754 __main__.py
cd /opt/splunk/etc/apps/splunk_rapid_diag/bin/splunklib/modularinput
chmod 754 event_writer.py
```

IF SPLUNK IS NOT GETTING SCORED ALLOW PING!!!
I don’t think there was an issue with this during competition.

7) GET GUI

Commands:

```
sudo dnf group install “Server with GUI” -y
sudo systemctl set-default graphical
reboot
```

Login as sysadmin in the GUI
Firefox version should work but if not update it

8) Log into the Splunk WebUI with admin:changeme

9) Go to settings < users
Click on Admin
Change password to Orange44$yellow
Set timezone as central
Accept the terms and save

10) FIX THE CVE!

Commands:

```
sudo vi /opt/splunk/etc/system/default/web.conf
/Xslt

enableSearchJobXslt = false
```

NEXT STEPS:

At this point the only main things left to do are set up Splunk data inputs and update Oracle Linux to 9.3

SPLUNK DATA INPUTS

UDP:1514 Palo Logs (Context Palo Networks App)

UDP:1515 Syslog (Context Search and Reporting)

TCP:1516 Syslog (Context Search and Reporting)

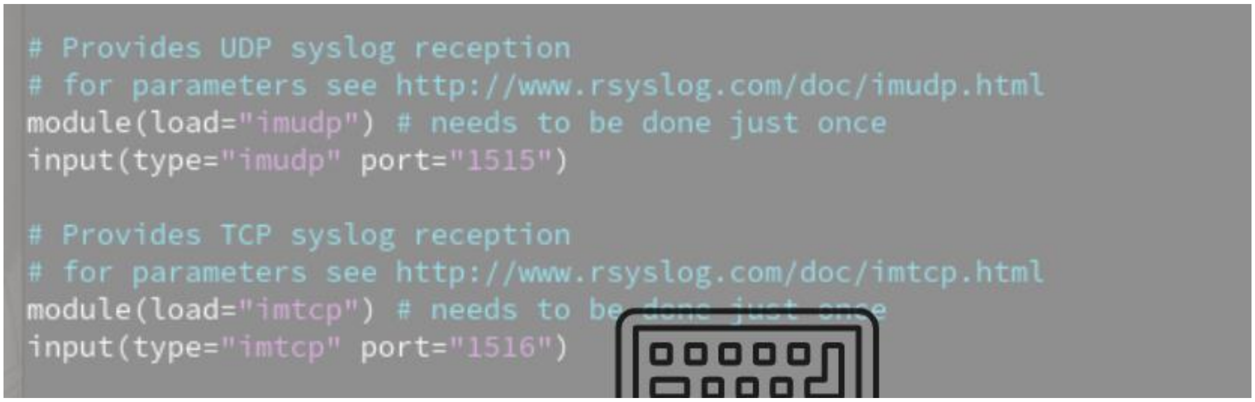
Configure a receiver on port 9998 for Windows Logs

UPDATE TO 9.3

```
sudo dnf update -y
```

RSYSLOG

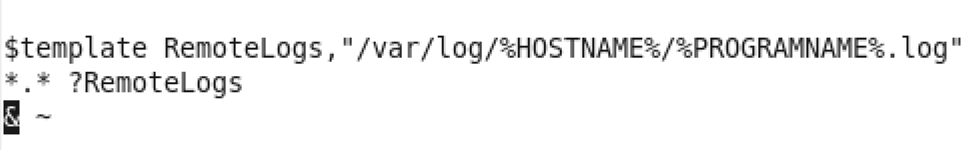
Edit /etc/rsyslog.conf to match the following



```
# Provides UDP syslog reception
# for parameters see http://www.rsyslog.com/doc/imudp.html
module(load="imudp") # needs to be done just once
input(type="imudp" port="1515")

# Provides TCP syslog reception
# for parameters see http://www.rsyslog.com/doc/imtcp.html
module(load="imtcp") # needs to be done just once
input(type="imtcp" port="1516")
```

Optional:



```
$template RemoteLogs,"/var/log/%HOSTNAME%/%PROGRAMNAME%.log"
*.* ?RemoteLogs
& ~
```

```
sudo systemctl restart rsyslog
```

CLIENT

Add the following to the bottom of the /etc/rsyslog.conf file

```
*.*@172.20.241.20:1515

*.*@@172.20.241.20:1516
```

The first line *.*@[ip]:[port] is for udp traffic
The second line *.*@@[ip]:[port] is for tcp traffic

Restart rsyslog on the client and send a test using logger if applicable

```
service rsyslog restart OR systemctl restart rsyslog

logger -t test “TEST MESSAGE”
```

THIS HAS BEEN TESTED AND WORKS FOR ALL LINUX MACHINES