**Taiwo John**

**Step 1**

tar xvf TarDocs.tar

tar -czvf Javaless\_Docs.tar --exclude=\*Java\* ~/Projects/TarDocs/Documents

tar -tvf Javaless\_Docs.tar | grep -i java | less

sudo tar cvvWf logs\_backup\_tar.gz --listed-incremental=snapshot.file --level=0 /var/log

-c is used to create tar file

-x is used to extract from a tar file

**Step 2**

0 6 \* \* 3 tar czvf /auth\_backup.tgz /var/log/auth.log

**Step 3**

sudo mkdir -p ~/backups/{freemem,diskuse,openlist,freedisk}

**Step 4**

sudo nano system.sh

################

#!/bin/bash

**Step 5**

free -h > ~/backups/freemen/free\_mem.txt

du -h > ~/backups/diskuse/disk\_usage.txt

ls -l > ~/backups/openlist/open\_list.txt

df -h > ~/backups/freedisk/free\_disk

########################

sudo chmod +x system.sh

@weekly /home/sysadmin/system.sh

sudo journalctl -n 10 -o verbose

sudo journalctl -u systemd-journald | less

sudo journalctl --vacuum-files=2

sudo journalctl -p 0..2 > /home/sysadmin/Priority\_High\_txt

@daily sudo journalctl -p 0..2 > /home/sysadmin/Priority\_High\_txt

-Command to record all mail log

/var/log/auth.log {

rotate 180

daily

notifempty

compress

delay compression

endscript

}

**Bonus**

Command to verify auditd is active:

systemctl status auditd

Command to set number of retained logs and maximum log file size:

sudo nano /etc/audit/auditd.conf

num\_logs = 5

logs-/etc/audit/auditd/auditd.conf

Command using auditd to set rules for /etc/shadow, /etc/passwd and /var/log/auth.log:

-w /etc/shadow -p wa -k shadow

-w /etc/shadow -p wa -k passwd

-w /var/log/auth.log -p wa -k auth.log

-restart:

sudo systemctl restart auditd

-list all:

sudo auditctl -l

-audit report

sudo aureport -au

Authentication Report

============================================

# date time acct host term exe success event

============================================

1. 09/07/2020 23:52:20 sysadmin ? /dev/pts/1 /usr/bin/sudo yes 345

-create user

sudo useradd attacker

sudo aureport -m

Account Modifications Report

=================================================

# date time auid addr term exe acct success event

=================================================

1. 09/07/2020 23:52:20 1000 UbuntuDesktop pts/1 /usr/sbin/useradd attacker yes 350

2. 09/07/2020 23:52:20 1000 UbuntuDesktop pts/1 /usr/sbin/useradd ? yes 351

command to use auditd-

sudo nano /etc/audit/rules.d/audit.rules