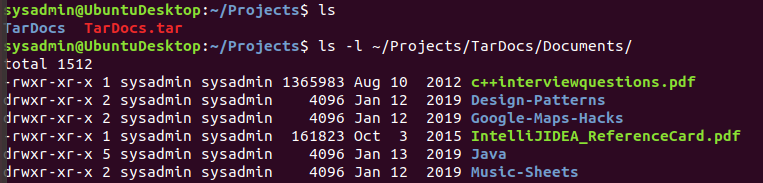
**Week 5 Homework Submission File: Archiving and Logging Data**

Please edit this file by adding the solution commands on the line below the prompt.

Save and submit the completed file for your homework submission.

Step 1: Create, Extract, Compress, and Manage tar Backup Archives

Command to extract the TarDocs.tar archive to the current directory: tar -xvf TarDocs.tar to extract the file to the current directory.



Command to create the Javaless\_Doc.tar archive from the TarDocs/ directory, while excluding the TarDocs/Documents/Java directory: tar –cvf javaless\_doc.tar --remove ~/Projects/TarDocs/Documents/Java TarDocs

Command to ensure Java/ is not in the new Javaless\_Docs.tar archive: tar –xf javaless\_doc.tar | grep java. Nothing comes up cause no java.

Bonus

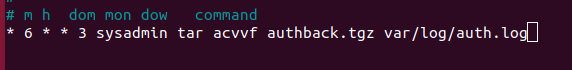
Command to create an incremental archive called logs\_backup\_tar.gz with only changed files to snapshot.file for the /var/log directory: tar cvvWf logs.backup.tar.gz –listed-incremental=snapshot.file.snar

Critical Analysis Question

Why wouldn't you use the options -x and -c at the same with tar? Options "-x" and "-c" are operations. Only one operation argument can be given at a time, so you wouldnt run more than one per command.

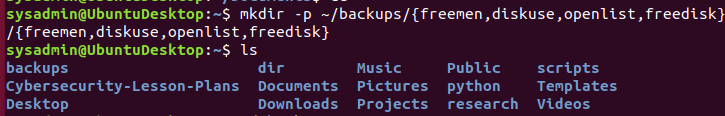
Step 2: Create, Manage, and Automate Cron Jobs

Cron job for backing up the /var/log/auth.log file:



Step 3: Write Basic Bash Scripts

Brace expansion command to create the four subdirectories: :~$ mkdir -p ~/backups/{freemen,diskuse,openlist,freedisk}/{freemen,diskuse,openlist,freedisk}



Paste your system.sh script edits below:

#!/bin/bash

#!/bin/bash  
echo "Memory Info:" > ~/backups/freemen/freemen.txt  
free > ~/backups/freemen/freemen.txt  
echo -e "\nDisk Usage:" > ~/backups/diskuse/disk\_usage.txt  
du -H | head -2 >> ~/backups/diskuse/disk\_usage.txt  
lsof > ~/backups/openlist/open\_list.txt  
df -h > ~/backups/freedisk/free\_disk.txt



Command to make the system.sh script executable: CTRL+X + CTRL+Y.

Optional

Commands to test the script and confirm its execution: sudo bash system.sh

Bonus

Command to copy system to system-wide cron directory:

Step 4. Manage Log File Sizes

Run sudo nano /etc/logrotate.conf to edit the logrotate configuration file.

Configure a log rotation scheme that backs up authentication messages to the /var/log/auth.log.

Add your config file edits below:

# see "man logrotate" for details  
# rotate log files weekly  
weekly  
  
# use the syslog group by default, since this is the owning group  
# of /var/log/syslog.  
su root syslog  
  
# keep 4 weeks worth of backlogs  
rotate 7  
notifempty  
  
# create new (empty) log files after rotating old ones  
create  
  
# uncomment this if you want your log files compressed  
delaycompress  
  
# packages drop log rotation information into this directory  
include /etc/logrotate.d  
  
# no packages own wtmp, or btmp -- we'll rotate them here  
/var/log/wtmp {  
    missingok  
    monthly  
    create 0664 root utmp  
    rotate 1  
}

Bonus: Check for Policy and File Violations

Command to verify auditd is active:

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

Add the edits made to the configuration file below:

[Your solution edits here]

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

Add the edits made to the rules file below:

[Your solution edits here]

Command to restart auditd:

Command to list all auditd rules:

Command to produce an audit report:

Create a user with sudo useradd attacker and produce an audit report that lists account modifications:

Command to use auditd to watch /var/log/cron:

Command to verify auditd rules:

Bonus (Research Activity): Perform Various Log Filtering Techniques

Command to return journalctl messages with priorities from emergency to error:

Command to check the disk usage of the system journal unit since the most recent boot:

Command to remove all archived journal files except the most recent two:

Command to filter all log messages with priority levels between zero and two, and save output to /home/sysadmin/Priority\_High.txt:

Command to automate the last command in a daily cronjob. Add the edits made to the crontab file below:

[Your solution cron edits here]

© 2020 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.