Linux Systems Administration

Step 1: Ensure/Double Check Permissions on Sensitive Files

1. Permissions on `/etc/shadow` should allow only `root` read and write access.

   - Command to inspect permissions: ls -lt shadow

   - Command to set permissions (if needed):sudo chmod 600 /etc/shadow

```
sysadmin@UbuntuDesktop:/etc$ man lynis
sysadmin@UbuntuDesktop:/etc$ man chkrootkit
sysadmin@UbuntuDesktop:/etc$ ls -l shadow
-rw------- 1 root shadow 3247 Dec 12 19:05 shadow
sysadmin@UbuntuDesktop:/etc$ ls -l gshadow
-rw------- 1 root shadow 1180 Dec 15 13:55 gshadow
sysadmin@UbuntuDesktop:/etc$ ls -lt group
-rw----r-- 1 root root 1432 Dec 15 13:55 group
sysadmin@UbuntuDesktop:/etc$ ls -lt passwd
-rw----r-- 1 root root 3324 Dec 12 19:05 passwd
sysadmin@UbuntuDesktop:/etc$
```

2. Permissions on `/etc/gshadow` should allow only `root` read and write access.

   - Command to inspect permissions: ls -lt gshadow

   - Command to set permissions (if needed): sudo chmod 600 /etc/gshadow

```
sysadmin@UbuntuDesktop:/etc$ man lynis
sysadmin@UbuntuDesktop:/etc$ man chkrootkit
sysadmin@UbuntuDesktop:/etc$ ls -l shadow
-rw------- 1 root shadow 3247 Dec 12 19:05 shadow
sysadmin@UbuntuDesktop:/etc$ ls -l gshadow
-rw------- 1 root shadow 1180 Dec 15 13:55 gshadow
sysadmin@UbuntuDesktop:/etc$ ls -lt group
-rw----r-- 1 root root 1432 Dec 15 13:55 group
sysadmin@UbuntuDesktop:/etc$ ls -lt passwd
-rw----r-- 1 root root 3324 Dec 12 19:05 passwd
sysadmin@UbuntuDesktop:/etc$
```

3. Permissions on `/etc/group` should allow `root` read and write access, and allow everyone else read access only.

   - Command to inspect permissions: ls -lt group

   - Command to set permissions (if needed):sudo chmod 644 /etc/group

```
sysadmin@UbuntuDesktop:/etc$ man lynis
sysadmin@UbuntuDesktop:/etc$ man chkrootkit
sysadmin@UbuntuDesktop:/etc$ ls -l shadow
-rw------- 1 root shadow 3247 Dec 12 19:05 shadow
sysadmin@UbuntuDesktop:/etc$ ls -l gshadow
-rw------- 1 root shadow 1180 Dec 15 13:55 gshadow
sysadmin@UbuntuDesktop:/etc$ ls -lt group
-rw----r-- 1 root root 1432 Dec 15 13:55 group
sysadmin@UbuntuDesktop:/etc$ ls -lt passwd
-rw----r-- 1 root root 3324 Dec 12 19:05 passwd
sysadmin@UbuntuDesktop:/etc$
```

4. Permissions on `/etc/passwd` should allow `root` read and write access, and allow everyone else read access only.

- Command to inspect permissions: ls -lt passwd ls -lt passwd

- Command to set permissions (if needed): sudo chmod 644 /etc/passwd


```
sysadmin@UbuntuDesktop:/etc$ man lynis
sysadmin@UbuntuDesktop:/etc$ man chkrootkit
sysadmin@UbuntuDesktop:/etc$ ls -l shadow
-rw------- 1 root shadow 3247 Dec 12 19:05 shadow
sysadmin@UbuntuDesktop:/etc$ ls -l gshadow
-rw------- 1 root shadow 1180 Dec 15 13:55 gshadow
sysadmin@UbuntuDesktop:/etc$ ls -lt group
-rw----r-- 1 root root 1432 Dec 15 13:55 group
sysadmin@UbuntuDesktop:/etc$ ls -lt passwd
-rw----r-- 1 root root 3324 Dec 12 19:05 passwd
sysadmin@UbuntuDesktop:/etc$
```

Step 2: Create User Accounts

1. Add user accounts for `sam`, `joe`, `amy`, `sara`, and `admin`.

   - Command to add each user account (include all five users):
     sudo adduser sam
     sudo adduser joe
     sudo adduser amy
     sudo adduser sara
     sudo adduser admin

```
jane:$6$5352819218ac27c8$DnFioOsc0fYoC58e8
ltY4mfIfsdVPnedHt/:18562:0:99999:7:::
postfix:*:18562:0:99999:7:::
tripwire:*:18607:0:99999:7:::
joe:$6$ZWAYHAU1$rnQLEtgxRAEJWjMqxmLjMONYjz
x/dtGw6v0:18609:0:99999:7:::
sam:$6$OVPBbaWs$SRfU7HO40pZ8051hjSWgqnEF5v
4vTzYryy1:18609:0:99999:7:::
sara:$6$XOlU9PtW$anqnZabDHhl.oS8UdERlmmNdA
wLvmxYnMZ1:18609:0:99999:7:::
amy:$6$0RW.fq93$XGq.8gfJKNi772nGe.f151gFsp
p58nXR5Z.:18609:0:99999:7:::
admin:$6$SSt4l4BQ$MRJonCjJdLYl38Vpyhh1lKkT
mhluT3hO1l1:18613:0:99999:7:::
sysadmin@UbuntuDesktop:/etc$
```

2. Ensure that only the `admin` has general sudo access.

```
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/u

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL
vagrant ALL=(ALL:ALL) NOPASSWD:ALL
sysadmin ALL=(ALL:ALL) NOPASSWD:ALL
# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL
```

   - Command to add `admin` to the `sudo` group: sudo useradd -aG sudo admin

Step 3: Create User Group and Collaborative Folder

1. Add an `engineers` group to the system.

   - Command to add group: sudo addgroup engineers

2. Add users `sam`, `joe`, `amy`, and `sara` to the managed group.

   - Command to add users to `engineers` group (include all four users):
     sudo usermod -aG engineers sam
     sudo usermod -aG engineers joe
     sudo usermod -aG engineers amy
     sudo usermod -aG engineers sara

```
sysadmin@UbuntuDesktop:/etc$ cat group | grep engineer
engineers:x:1005:amy,sam,joe,sara
sysadmin@UbuntuDesktop:/etc$
```

3. Create a shared folder for this group at `/home/engineers`.

   - Command to create the shared folder:
     sudo mkdir -p engineers

4. Change ownership on the new engineers' shared folder to the `engineers` group.

   - Command to change ownership of engineer's shared folder to engineer group:
     sudo chown :engineers /home/engineers/

```
drwxr-xr-x  8 sam        adam       4096 Oct 27 16:32 adam
drwxr-xr-x  8 amy        amy        4096 Dec 12 19:05 amy
drwxr-xr-x  8 billy      billy      4096 Oct 27 16:32 billy
drwxrwxr--  2 root       engineers  4096 Dec 12 19:36 engineers
drwxr-xr-x  8 http       http       4096 Oct 27 16:32 http
drwxr-xr-x  8 instructor instructor 4096 Oct 27 16:24 instructor
drwxr-xr-x  9 jane       jane       4096 Dec 17 09:03 jane
drwxr-xr-x  8 joe        joe        4096 Dec 12 19:03 joe
```

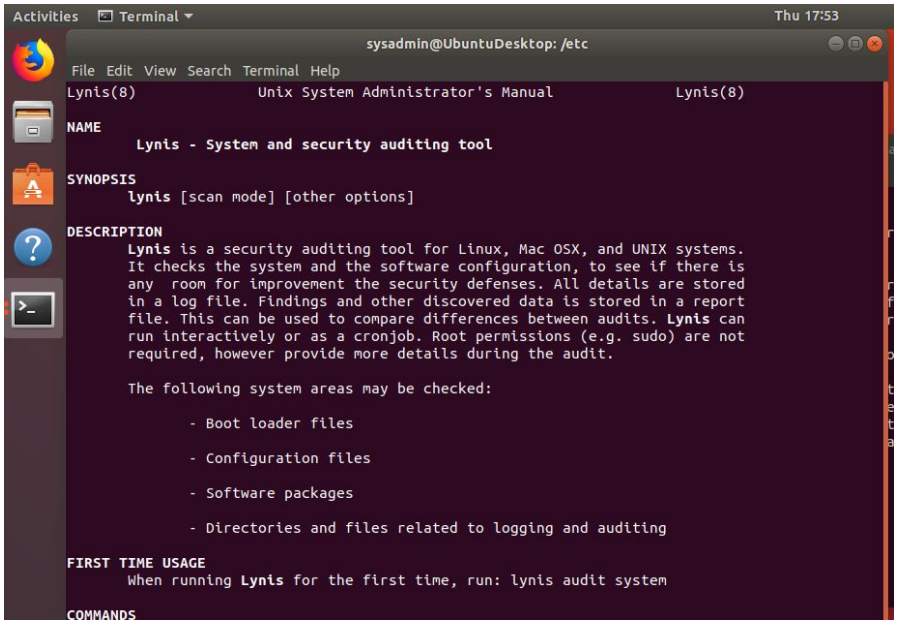
Step 4: Lynis Auditing

1. Command to install Lynis:

   sudo apt install lynis

2. Command to see documentation and instructions:

   man lynis or lynis --help



3. Command to run an audit:

   sudo lynis audit system

4. Provide a report from the Lynis output on what can be done to harden the system.

- Screenshot of report output:

sudo cat lynis-report.dat | grep suggestion

```
suggestion[]=SSH-7408|Consider hardening SSH configuration|AllowTcpForwarding (YES --> NO)|-|
suggestion[]=SSH-7408|Consider hardening SSH configuration|ClientAliveCountMax (3 --> 2)|-|
suggestion[]=SSH-7408|Consider hardening SSH configuration|Compression (YES --> (DELAYED|NO))|-|
suggestion[]=SSH-7408|Consider hardening SSH configuration|LogLevel (INFO --> VERBOSE)|-|
suggestion[]=SSH-7408|Consider hardening SSH configuration|MaxAuthTries (6 --> 2)|-|
suggestion[]=SSH-7408|Consider hardening SSH configuration|MaxSessions (10 --> 2)|-|
suggestion[]=SSH-7408|Consider hardening SSH configuration|PermitRootLogin (WITHOUT-PASSWORD --> NO)|-|
suggestion[]=SSH-7408|Consider hardening SSH configuration|Port (22 --> )|-|
suggestion[]=SSH-7408|Consider hardening SSH configuration|TCPKeepAlive (YES --> NO)|-|
suggestion[]=SSH-7408|Consider hardening SSH configuration|X11Forwarding (YES --> NO)|-|
suggestion[]=SSH-7408|Consider hardening SSH configuration|AllowAgentForwarding (YES --> NO)|-|
suggestion[]=LOGG-2190|Check what deleted files are still in use and why.|-|-|
suggestion[]=BANN-7126|Add a legal banner to /etc/issue, to warn unauthorized users|-|-|
suggestion[]=BANN-7130|Add legal banner to /etc/issue.net, to warn unauthorized users|-|-|
suggestion[]=ACCT-9622|Enable process accounting|-|-|
suggestion[]=ACCT-9626|Enable sysstat to collect accounting (no results)|-|-|
suggestion[]=ACCT-9628|Enable auditd to collect audit information|-|-|
suggestion[]=CONT-8104|Run 'docker info' to see warnings applicable to Docker daemon|-|-|
suggestion[]=FINT-4350|Install a file integrity tool to monitor changes to critical and sensitive files|-|
suggestion[]=KRNL-6000|One or more sysctl values differ from the scan profile and could be tweaked||Change
suggestion[]=HRDN-7222|Harden compilers like restricting access to root user only|-|-|
suggestion[]=HRDN-7230|Harden the system by installing at least one malware scanner, to perform periodic f
```

Bonus

1. Command to install chkrootkit:

   sudo apt install chkrootkit

2. Command to see documentation and instructions:

   man chkrootkit or chkrootkit --help

```
chkrootkit(1)                    General Commands Manual                    chkrootkit(1)

NAME
       chkrootkit - Determine whether the system is infected with a rootkit

SYNOPSIS
       chkrootkit [OPTION]... [TESTNAME]...

DESCRIPTION
       chkrootkit  examines  certain  elements of the target system and determines whether
       they have been tampered with. Some tools which chkrootkit applies  while  analyzing
       binaries and log files can be found at /usr/lib/chkrootkit.

OPTIONS
       -h     Print a short help message and exit.

       -V     Print version information and exit.

       -l     Print available tests.

       -d     Enter debug mode.

       -x     Enter expert mode.

       -e     Exclude known false positive files/dirs, quoted, space separated.

       -q     Enter quiet mode.

       -r dir Use dir as the root directory.

       -p dir1:dir2:dirN
              Specify the path for the external commands used by chkrootkit.
```

3. Command to run expert mode:

   sudo apt install `chkrootkit -x`

In this mode the user can examine suspicious strings in the binary programs that may indicate a trojan.

4. Provide a report from the chrootkit output on what can be done to harden the system.
   - Screenshot of end of sample output:

```
root@UbuntuDesktop:/# clear

root@UbuntuDesktop:/# chkrootkit
ROOTDIR is `/'
Checking `amd'...                                           not found
Checking `basename'...                                      not infected
Checking `biff'...                                          not found
Checking `chfn'...                                          not infected
Checking `chsh'...                                          not infected
Checking `cron'...                                          not infected
Checking `crontab'...                                       not infected
Checking `date'...                                          not infected
Checking `du'...                                            not infected
Checking `dirname'...                                       not infected
Checking `echo'...                                          not infected
Checking `egrep'...                                         not infected
Checking `env'...                                           not infected
Checking `find'...                                          not infected
Checking `fingerd'...                                       not found
Checking `gpm'...                                           not found
Checking `grep'...                                          not infected
Checking `hdparm'...                                        not infected
Checking `su'...                                            not infected
```

```
sysadmin@UbuntuDesktop:~$ sudo chkrootkit | grep Vulnerable
! sysadmin     4128 pts/0  grep --color=auto Vulnerable
sysadmin@UbuntuDesktop:~$ sudo chkrootkit | grep INFECTED
Searching for Linux.Xor.DDoS ...                    INFECTED: Possible Malicious Linux.Xor.DDoS installed
! sysadmin     4859 pts/0  grep --color=auto INFECTED
sysadmin@UbuntuDesktop:~$ sudo chkrootkit | grep "Vulnerable"
! sysadmin     5642 pts/0  grep --color=auto Vulnerable
sysadmin@UbuntuDesktop:~$
```

Ways to harden:

- Identify your enterprise's needs for protection, access, and performance
- Define "mission critical" for your specific environment
- Take advantage of next-generation firewall capabilities for DDoS mitigation
- Ensure that enterprise systems are not running on manufacturers' default configurations