**Week 4 Homework – Linux Systems Administration**

**Step 1: Ensure/Double Check Permissions on Sensitive Files**

Note – My word processor libreoffice won’t allow me to put a forward slash (/) before etc in the content below.

1) *etc*/shadow file

ls -l shadow

-rw-r----- 1 root shadow 3269 Nov 26 06:14 shadow

sudo chmod 600 *etc*/shadow (if needed)

2) etc/gshadow file

ls -l gshadow

-rw-r----- 1 root shadow 1122 Nov 26 06:14 gshadow

sudo chmod 600 *etc*/gshadow (if needed)

3) etc/group file

ls -l group

-rw-r--r-- 1 root root 1361 Nov 26 06:14 group

sudo chmod 644 *etc*/group (if needed)

4) etc/passwd file

ls -l passwd

-rw-r--r-- 1 root root 3359 Nov 26 06:14 passwd

sudo chmod 644 *etc*/passwd (if needed)

### Step 2: Create User Accounts

sudo adduser sam

sudo adduser joe

sudo adduser amy

sudo adduser sara

sudo adduser admin

sudo visudo

sudo usermod -aG sudo admin

**Step 3: Create User Group and Collaborative Folder**

sudo groupadd engineers

sudo usermod -a -G engineers sam

sudo usermod -a -G engineers joe

sudo usermod -a -G engineers amy

sudo usermod -a -G engineers sara

mkdir *home/*engineers  
sudo chgrp engineers /home/engineers or sudo chown :engineers /*home/*engineers

**Step 4: Lynis Auditing**

sudo apt update && sudo apt install lynis

man lynis

sudo lynis audit system --log-file /home/sysadmin/lynis.log --report-file /home/sysadmin/lynis.report

sudo lynis audit system

Output on what more could be done to harden the system -

-[ Lynis 2.6.2 Results ]-

Warnings (2):

----------------------------

! Version of Lynis is very old and should be updated [LYNIS]

https://cisofy.com/controls/LYNIS/

! No password set for single mode [AUTH-9308]

https://cisofy.com/controls/AUTH-9308/

Suggestions (50):

----------------------------

\* Install libpam-tmpdir to set $TMP and $TMPDIR for PAM sessions [CUST-0280]

https://your-domain.example.org/controls/CUST-0280/

\* Install libpam-usb to enable multi-factor authentication for PAM sessions [CUST-0285]

https://your-domain.example.org/controls/CUST-0285/

\* Install apt-listbugs to display a list of critical bugs prior to each APT installation. [CUST-0810]

https://your-domain.example.org/controls/CUST-0810/

\* Install apt-listchanges to display any significant changes prior to any upgrade via APT. [CUST-0811]

https://your-domain.example.org/controls/CUST-0811/

\* Install debian-goodies so that you can run checkrestart after upgrades to determine which services are using old versions of libraries and need restarting. [CUST-0830]

https://your-domain.example.org/controls/CUST-0830/

\* Install needrestart, alternatively to debian-goodies, so that you can run needrestart after upgrades to determine which daemons are using old versions of libraries and need restarting. [CUST-0831]

https://your-domain.example.org/controls/CUST-0831/

\* Install debsecan to generate lists of vulnerabilities which affect this installation. [CUST-0870]

https://your-domain.example.org/controls/CUST-0870/

\* Install debsums for the verification of installed package files against MD5 checksums. [CUST-0875]

https://your-domain.example.org/controls/CUST-0875/

\* Install fail2ban to automatically ban hosts that commit multiple authentication errors. [DEB-0880]

https://cisofy.com/controls/DEB-0880/

\* Set a password on GRUB bootloader to prevent altering boot configuration (e.g. boot in single user mode without password) [BOOT-5122]

https://cisofy.com/controls/BOOT-5122/

\* Install a PAM module for password strength testing like pam\_cracklib or pam\_passwdqc [AUTH-9262]

https://cisofy.com/controls/AUTH-9262/

\* Configure minimum password age in /etc/login.defs [AUTH-9286]

https://cisofy.com/controls/AUTH-9286/

\* Configure maximum password age in /etc/login.defs [AUTH-9286]

https://cisofy.com/controls/AUTH-9286/

\* Set password for single user mode to minimize physical access attack surface [AUTH-9308]

https://cisofy.com/controls/AUTH-9308/

\* Default umask in /etc/login.defs could be more strict like 027 [AUTH-9328]

https://cisofy.com/controls/AUTH-9328/

\* To decrease the impact of a full /home file system, place /home on a separated partition [FILE-6310]

https://cisofy.com/controls/FILE-6310/

\* To decrease the impact of a full /tmp file system, place /tmp on a separated partition [FILE-6310]

https://cisofy.com/controls/FILE-6310/

\* To decrease the impact of a full /var file system, place /var on a separated partition [FILE-6310]

https://cisofy.com/controls/FILE-6310/

\* Disable drivers like USB storage when not used, to prevent unauthorized storage or data theft [STRG-1840]

https://cisofy.com/controls/STRG-1840/

\* Check DNS configuration for the dns domain name [NAME-4028]

https://cisofy.com/controls/NAME-4028/

\* Check RPM database as RPM binary available but does not reveal any packages [PKGS-7308]

https://cisofy.com/controls/PKGS-7308/

\* Purge old/removed packages (5 found) with aptitude purge or dpkg --purge command. This will cleanup old configuration files, cron jobs and startup scripts. [PKGS-7346]

https://cisofy.com/controls/PKGS-7346/

\* Install debsums utility for the verification of packages with known good database. [PKGS-7370]

https://cisofy.com/controls/PKGS-7370/

\* Install package apt-show-versions for patch management purposes [PKGS-7394]

https://cisofy.com/controls/PKGS-7394/

\* Consider running ARP monitoring software (arpwatch,arpon) [NETW-3032]

https://cisofy.com/controls/NETW-3032/

\* Access to CUPS configuration could be more strict. [PRNT-2307]

https://cisofy.com/controls/PRNT-2307/

\* Check iptables rules to see which rules are currently not used [FIRE-4513]

https://cisofy.com/controls/FIRE-4513/

\* Install Apache mod\_evasive to guard webserver against DoS/brute force attempts [HTTP-6640]

https://cisofy.com/controls/HTTP-6640/

\* Install Apache modsecurity to guard webserver against web application attacks [HTTP-6643]

https://cisofy.com/controls/HTTP-6643/

\* Add HTTPS to nginx virtual hosts for enhanced protection of sensitive data and privacy [HTTP-6710]

https://cisofy.com/controls/HTTP-6710/

\* Consider hardening SSH configuration [SSH-7408]

- Details : AllowTcpForwarding (YES --> NO)

https://cisofy.com/controls/SSH-7408/

\* Consider hardening SSH configuration [SSH-7408]

- Details : ClientAliveCountMax (3 --> 2)

https://cisofy.com/controls/SSH-7408/

\* Consider hardening SSH configuration [SSH-7408]

- Details : Compression (YES --> (DELAYED|NO))

https://cisofy.com/controls/SSH-7408/

\* Consider hardening SSH configuration [SSH-7408]

- Details : LogLevel (INFO --> VERBOSE)

https://cisofy.com/controls/SSH-7408/

\* Consider hardening SSH configuration [SSH-7408]

- Details : MaxAuthTries (6 --> 2)

https://cisofy.com/controls/SSH-7408/

\* Consider hardening SSH configuration [SSH-7408]

- Details : MaxSessions (10 --> 2)

https://cisofy.com/controls/SSH-7408/

\* Consider hardening SSH configuration [SSH-7408]

- Details : PermitRootLogin (WITHOUT-PASSWORD --> NO)

https://cisofy.com/controls/SSH-7408/

\* Consider hardening SSH configuration [SSH-7408]

- Details : Port (22 --> )

https://cisofy.com/controls/SSH-7408/

\* Consider hardening SSH configuration [SSH-7408]

- Details : TCPKeepAlive (YES --> NO)

https://cisofy.com/controls/SSH-7408/

\* Consider hardening SSH configuration [SSH-7408]

- Details : X11Forwarding (YES --> NO)

https://cisofy.com/controls/SSH-7408/

\* Consider hardening SSH configuration [SSH-7408]

- Details : AllowAgentForwarding (YES --> NO)

https://cisofy.com/controls/SSH-7408/

\* Check what deleted files are still in use and why. [LOGG-2190]

https://cisofy.com/controls/LOGG-2190/

\* Add a legal banner to /etc/issue, to warn unauthorized users [BANN-7126]

https://cisofy.com/controls/BANN-7126/

\* Add legal banner to /etc/issue.net, to warn unauthorized users [BANN-7130]

https://cisofy.com/controls/BANN-7130/

\* Enable process accounting [ACCT-9622]

https://cisofy.com/controls/ACCT-9622/

\* Enable sysstat to collect accounting (no results) [ACCT-9626]

https://cisofy.com/controls/ACCT-9626/

\* Run 'docker info' to see warnings applicable to Docker daemon [CONT-8104]

https://cisofy.com/controls/CONT-8104/

\* Install a file integrity tool to monitor changes to critical and sensitive files [FINT-4350]

https://cisofy.com/controls/FINT-4350/

\* One or more sysctl values differ from the scan profile and could be tweaked [KRNL-6000]

- Solution : Change sysctl value or disable test (skip-test=KRNL-6000:<sysctl-key>)

https://cisofy.com/controls/KRNL-6000/

\* Harden compilers like restricting access to root user only [HRDN-7222]

https://cisofy.com/controls/HRDN-7222/

Follow-up:

----------------------------

- Show details of a test (lynis show details TEST-ID)

- Check the logfile for all details (less /var/log/lynis.log)

- Read security controls texts (https://cisofy.com)

- Use --upload to upload data to central system (Lynis Enterprise users)

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

Lynis security scan details:

Hardening index : 60 [############ ]

Tests performed : 242

Plugins enabled : 1

Components:

- Firewall [V]

- Malware scanner [V]

Lynis Modules:

- Compliance Status [?]

- Security Audit [V]

- Vulnerability Scan [V]

Files:

- Test and debug information : /var/log/lynis.log

- Report data : /var/log/lynis-report.dat

**Bonus**

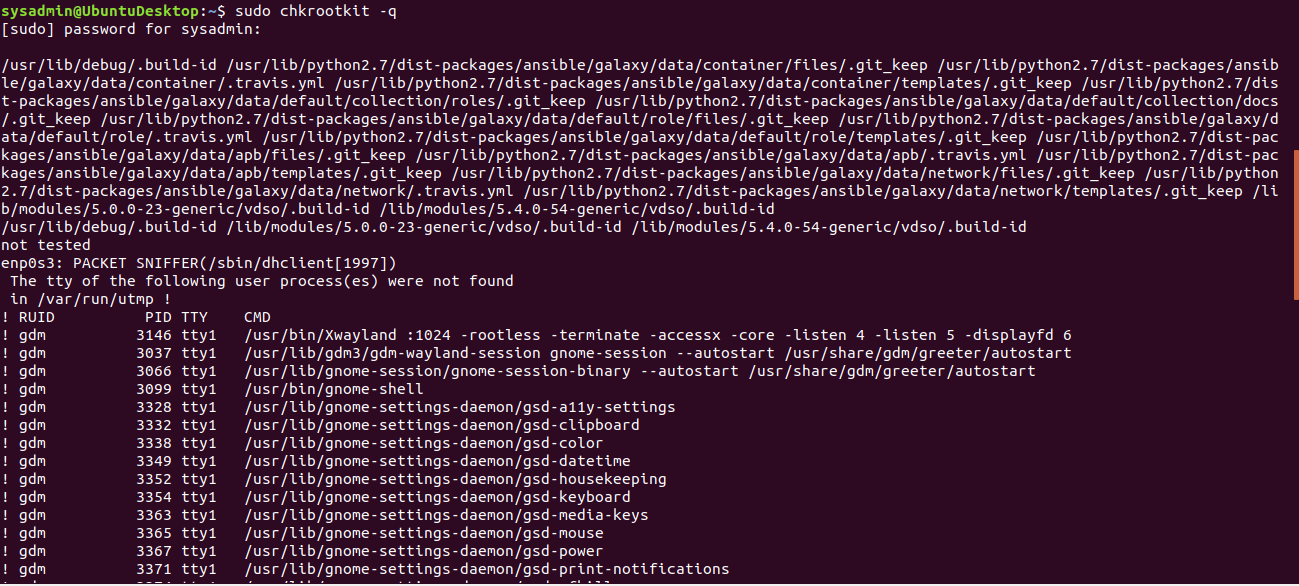
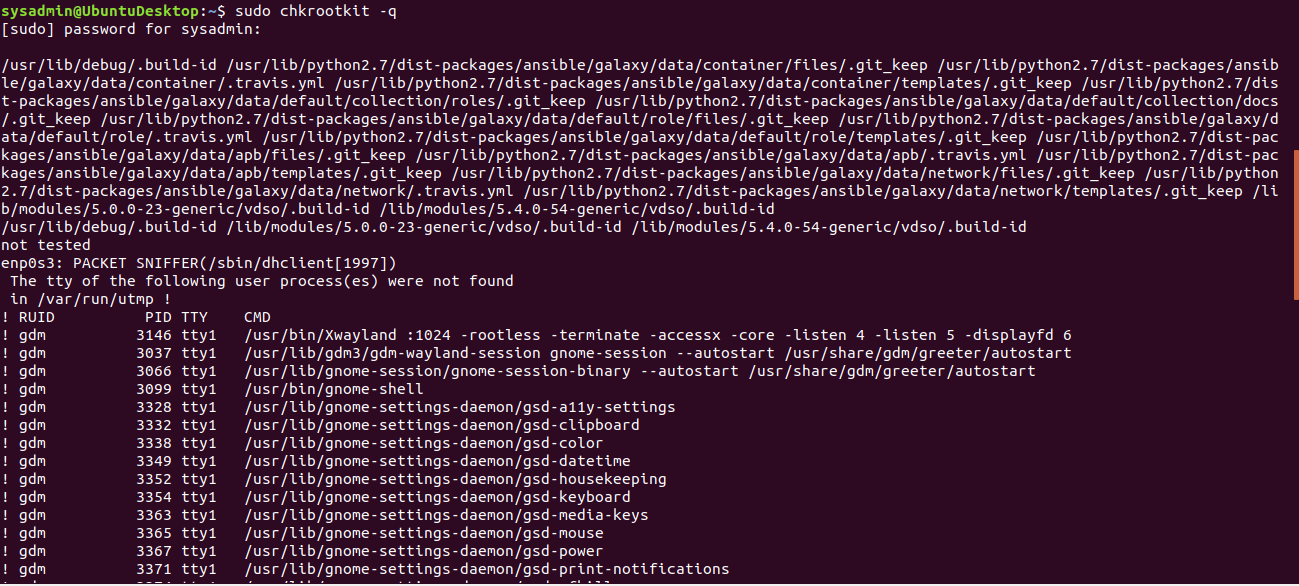
sudo apt update && sudo apt install chkrootkit

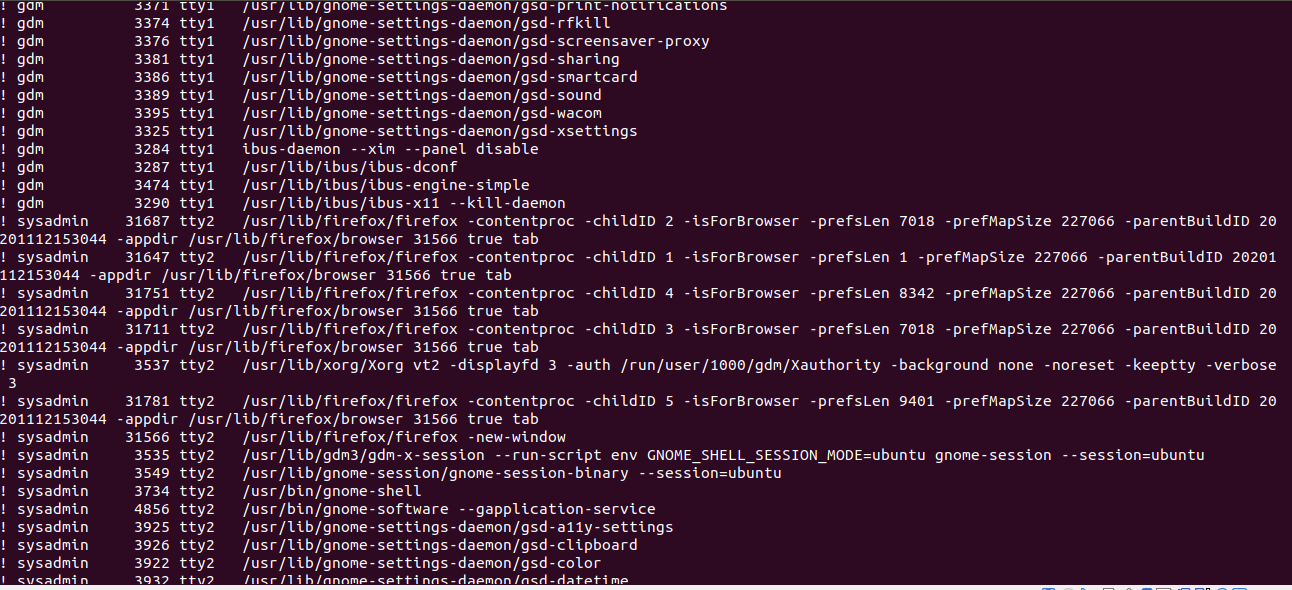
man chkrootkit

sudo chkrootkit -x > /home/sysadmin/chkrootkit.log

sudo chkrootkit -q

Screemshots below -

|

|

