Week 4 - Linux Systems Administration Homework

Ensure permissions on sensitive files

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

- **Command to inspect permissions**: ls -l | grep shadow
- **Command to Set Permissions (if needed)**: sudo chmod 600 shadow

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

- **Command to inspect permissions**: ls -l | grep gshadow
- **Command to Set Permissions (if needed)**: sudo chmod 600 gshadow

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

- **Command to inspect permissions**: ls -l | grep group
- **Command to Set Permissions (if needed)**: sudo chmod 644 group

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

- **Command to inspect permissions**:ls -l | grep passwd
- **Command to set permissions (if needed)**: sudo chmod 644 passwd

Create user accounts

Add user accounts `sam` , `joe` , `amy` , `sara` , and `admin`

- **Command to add each user account (please include all 5)**:
  - sudo adduser sam
  - sudo adduser joe
  - sudo adduser amy
  - sudo adduser sara
  - sudo adduser admin

Force users to create 16 character passwords incorporating numbers and symbols

- **Command to edit `pwquality.conf` file**: sudo nano security/pwquality.conf

- **Updates to configuration file**:
  - minlen = 16
  - dcredit = 1
  - ocredit = 1

Force passwords to expire every 90 days:

- **Command to to set each new user's password to expire in 90 days (please include all 5)**:
  - sudo chage -M 90 sam
  - sudo chage -M 90 joe
  - sudo chage -M 90 amy
  - sudo chage -M 90 sara
  - sudo chage -M 90 admin

Ensure that only the `admin` has general sudo access:

- **Command to add `admin` to the `sudo` group**: sudo usermod -aG sudo admin
  - verify with: groups admin

Create user group and collaborative folder

Add a `engineers` group to the system.

- **Command**: sudo addgroup engineers

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

- **Command to add users to `engineers` group (please include all 4)**:
  - sudo usermod -aG engineers sam
  - sudo usermod -aG engineers joe
  - sudo usermod -aG engineers amy
  - sudo usermod -aG engineers sara

- Verify with: tail group

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

- **Command to create the shared folder**: sudo mkdir /home/engineers

Change the group on the engineers directory to the `engineers` group

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

Add the `SGID` bit and the `sticky` bit to allow collaboration between engineers in this directory

- **Command to set SGID and sticky bit to shared folder**: sudo chmod o+t,g+s /home/engineers

Lynis auditing

Install and run `lynis`

- **Command to install `lynis` :** sudo apt install lynis

- **Command to see options:** man lynis

- **Command to run an audit:** sudo lynis audit system

Provide a report from `lynis` output on what more could be done to harden the system.

- **Screenshot of report output**:

```
-[ Lynis 2.6.2 Results ]-

Warnings (6):
----------------------------
! 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/

! Found one or more vulnerable packages. [PKGS-7392]
    https://cisofy.com/controls/PKGS-7392/

! Nameserver 127.0.0.53 does not respond [NETW-2704]
    https://cisofy.com/controls/NETW-2704/

! Couldn't find 2 responsive nameservers [NETW-2705]
    https://cisofy.com/controls/NETW-2705/

! Found some information disclosure in SMTP banner (OS or software name) [MAIL-8818]
    https://cisofy.com/controls/MAIL-8818/

Suggestions (53):
----------------------------
* 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 usi
ng 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/
```

```
    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/

* Delete accounts which are no longer used [AUTH-9288]
    https://cisofy.com/controls/AUTH-9288/

* 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/

* Install debsums utility for the verification of packages with known good database. [PKGS-7370]
    https://cisofy.com/controls/PKGS-7370/

* Update your system with apt-get update, apt-get upgrade, apt-get dist-upgrade and/or unattended-upgrades [PKGS-7392]
    https://cisofy.com/controls/PKGS-7392/

* Install package apt-show-versions for patch management purposes [PKGS-7394]
    https://cisofy.com/controls/PKGS-7394/

* Check connection to this nameserver and make sure no outbound DNS queries are blocked (port 53 UDP and TCP). [NETW-2704]
    https://cisofy.com/controls/NETW-2704/
```

```
      https://cisofy.com/controls/NETW-2705/

  * 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/

  * You are advised to hide the mail_name (option: smtpd_banner) from your postfix configuration. Use postconf -e or change your main.cf fi
le (/etc/postfix/main.cf) [MAIL-8818]
      https://cisofy.com/controls/MAIL-8818/

  * Disable the 'VRFY' command [MAIL-8820:disable_vrfy_command]
    - Details  : disable_vrfy_command=no
    - Solution : run postconf -e disable_vrfy_command=yes to change the value
      https://cisofy.com/controls/MAIL-8820/

  * 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/

  * 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/

  * Enable auditd to collect audit information [ACCT-9628]
      https://cisofy.com/controls/ACCT-9628/

  * Run 'docker info' to see warnings applicable to Docker daemon [CONT-8104]
      https://cisofy.com/controls/CONT-8104/

  * 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 : 53 [##########          ]
  Tests performed : 233
  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

================================================================================
  Notice: Lynis update available
  Current version : 262    Latest version : 275
================================================================================

  Lynis 2.6.2

  Auditing, system hardening, and compliance for UNIX-based systems
  (Linux, macOS, BSD, and others)

  2007-2018, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)

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

  [TIP]: Enhance Lynis audits by adding your settings to custom.prf (see /etc/lynis/default.prf for all settings)
```

Bonus: Check for Root Kits

Install and run `chkrootkit` .

Command to install `chkrootkit` : sudo apt install chkrootkit

- **Command to see options:** man chkrootkit

- **Command to run expert mode:** sudo chkrootkit -x

- **Screenshot of End of Sample Output:**