Angelo Salazar

University of Denver Cybersecurity Bootcamp

July 22nd, 2021

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 -la /etc/shadow shows root has read and write access to the shadow file.
   - Command to set permissions (if needed): chmod 600 /etc/shadow
2. Permissions on /etc/gshadow should allow only root read and write access.
   - Command to inspect permissions: ls -ls /etc/gshadow shows only read and write access to the gshadow file.
   - Command to set permissions (if needed): chmod 600 /etc/gshadow
3. Permissions on /etc/group should allow root read and write access, and allow everyone else read access only.
   - Command to inspect permissions: ls -la /etc/group shows root has read and write, and groups and others have only read.
   - Command to set permissions (if needed): chmod 644 /etc/group
4. Permissions on /etc/passwd should allow root read and write access, and allow everyone else read access only.
   - Command to inspect permissions: ls -la /etc/passwd shows root has read and write access, and groups and others have only read.
   - Command to set permissions (if needed): chmod 644 /etc/passwd

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):
     i. sudo adduser sam
     ii. sudo adduser joe
     iii. sudo adduser amy
     iv. sudo adduser sara
     v. sudo adduser admin
2. Ensure that only the admin has general sudo access.

- Command to add admin to the sudo group: sudo usermod -aG sudo admin
    - i. Ran command “groups admin” and got “admin : admin sudo” as my output.

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):
        - i. usermod -aG engineers sam
            1. Ran command “groups sam” and got “sam : sam engineers” as my output.
        - ii. usermod -aG engineers joe
            1. Ran command “groups sam” and got “joe : joe engineers” as my output.
        - iii. usermod -aG engineers amy
            1. Ran command “groups sam” and got “amy : amy engineers” as my output.
        - iv. usermod -aG engineers sara
            1. Ran command “groups sam” and got “sara : sara engineers” as my output.
3. Create a shared folder for this group at /home/engineers.
    - Command to create the shared folder: sudo mkdir /home/engineers
        - i. Ran ls /home and the engineers directory was present.
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

Step 4: Lynis Auditing

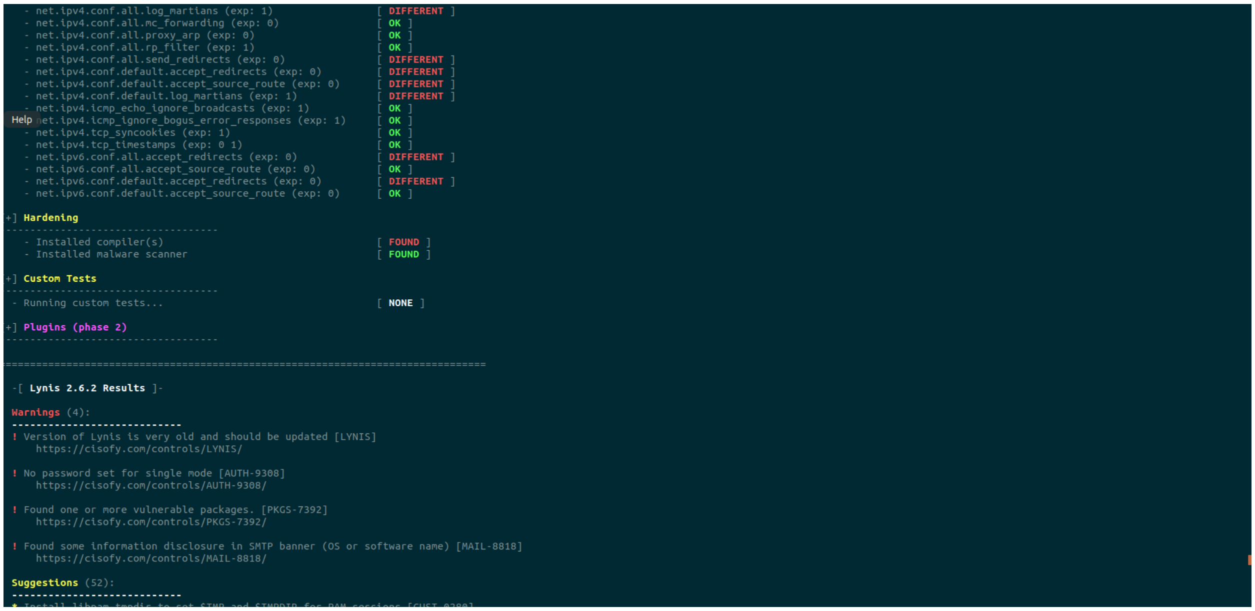
1. Command to install Lynis: sudo apt install lynis
2. Command to see documentation and instructions: man lynis or sudo lynis show help

Angelo Salazar

University of Denver Cybersecurity Bootcamp

July 22nd, 2021

3. Command to run an audit: lynis audit system
4. Provide a report from the Lynis output on what can be done to harden the system.
    - After running sudo lynis audit system, I was provided 2 suggestions for system hardening.



```
    - net.ipv4.conf.all.log_martians (exp: 1)                 [ DIFFERENT ]
    - net.ipv4.conf.all.mc_forwarding (exp: 0)                [ OK ]
    - net.ipv4.conf.all.proxy_arp (exp: 0)                    [ OK ]
    - net.ipv4.conf.all.rp_filter (exp: 1)                    [ OK ]
    - net.ipv4.conf.all.send_redirects (exp: 0)               [ DIFFERENT ]
    - net.ipv4.conf.default.accept_redirects (exp: 0)         [ DIFFERENT ]
    - net.ipv4.conf.default.accept_source_route (exp: 0)      [ DIFFERENT ]
    - net.ipv4.conf.default.log_martians (exp: 1)             [ DIFFERENT ]
    - net.ipv4.icmp_echo_ignore_broadcasts (exp: 1)           [ OK ]
      net.ipv4.icmp_ignore_bogus_error_responses (exp: 1)     [ OK ]
    - net.ipv4.tcp_syncookies (exp: 1)                        [ OK ]
    - net.ipv4.tcp_timestamps (exp: 0 1)                      [ OK ]
    - net.ipv6.conf.all.accept_redirects (exp: 0)             [ DIFFERENT ]
    - net.ipv6.conf.all.accept_source_route (exp: 0)          [ OK ]
    - net.ipv6.conf.default.accept_redirects (exp: 0)         [ DIFFERENT ]
    - net.ipv6.conf.default.accept_source_route (exp: 0)      [ OK ]

[+] Hardening
------------------------------------
    - Installed compiler(s)                                   [ FOUND ]
    - Installed malware scanner                               [ FOUND ]

[+] Custom Tests
------------------------------------
  - Running custom tests...                                   [ NONE ]

[+] Plugins (phase 2)
------------------------------------

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

  -[ Lynis 2.6.2 Results ]-

  Warnings (4):
  ----------------------------
  ! 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/

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

  Suggestions (52):
  ----------------------------
  * Install libpam-tmpdir to set $TMP and $TMPDIR for PAM sessions [CUST-0280]
```

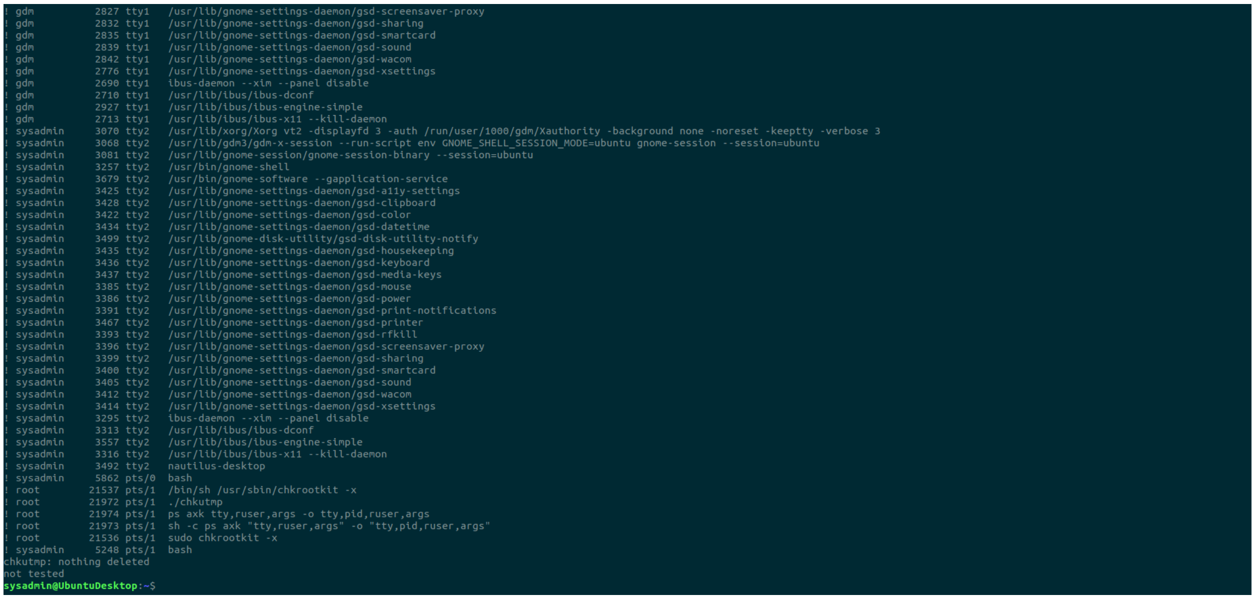
Bonus

1. Command to install chkrootkit: sudo apt install chkrootkit
2. Command to see documentation and instructions: man chkrootkit or chkrootkit --help
3. Command to run expert mode: sudo chkrootkit -x
4. Provide a report from the chrootkit output on what can be done to harden the system.
    - Screenshot of end of sample output

Angelo Salazar

University of Denver Cybersecurity Bootcamp

July 22nd, 2021



```
! gdm          2827 tty1   /usr/lib/gnome-settings-daemon/gsd-screensaver-proxy
! gdm          2832 tty1   /usr/lib/gnome-settings-daemon/gsd-sharing
! gdm          2835 tty1   /usr/lib/gnome-settings-daemon/gsd-smartcard
! gdm          2839 tty1   /usr/lib/gnome-settings-daemon/gsd-sound
! gdm          2842 tty1   /usr/lib/gnome-settings-daemon/gsd-wacom
! gdm          2776 tty1   /usr/lib/gnome-settings-daemon/gsd-xsettings
! gdm          2690 tty1   ibus-daemon --xim --panel disable
! gdm          2710 tty1   /usr/lib/ibus/ibus-dconf
! gdm          2927 tty1   /usr/lib/ibus/ibus-engine-simple
! gdm          2713 tty1   /usr/lib/ibus/ibus-x11 --kill-daemon
! sysadmin     3070 tty2   /usr/lib/xorg/Xorg vt2 -displayfd 3 -auth /run/user/1000/gdm/Xauthority -background none -noreset -keeptty -verbose 3
! sysadmin     3068 tty2   /usr/lib/gdm3/gdm-x-session --run-script env GNOME_SHELL_SESSION_MODE=ubuntu gnome-session --session=ubuntu
! sysadmin     3081 tty2   /usr/lib/gnome-session/gnome-session-binary --session=ubuntu
! sysadmin     3257 tty2   /usr/bin/gnome-shell
! sysadmin     3679 tty2   /usr/bin/gnome-software --gapplication-service
! sysadmin     3425 tty2   /usr/lib/gnome-settings-daemon/gsd-a11y-settings
! sysadmin     3428 tty2   /usr/lib/gnome-settings-daemon/gsd-clipboard
! sysadmin     3422 tty2   /usr/lib/gnome-settings-daemon/gsd-color
! sysadmin     3434 tty2   /usr/lib/gnome-settings-daemon/gsd-datetime
! sysadmin     3499 tty2   /usr/lib/gnome-disk-utility/gsd-disk-utility-notify
! sysadmin     3435 tty2   /usr/lib/gnome-settings-daemon/gsd-housekeeping
! sysadmin     3436 tty2   /usr/lib/gnome-settings-daemon/gsd-keyboard
! sysadmin     3437 tty2   /usr/lib/gnome-settings-daemon/gsd-media-keys
! sysadmin     3385 tty2   /usr/lib/gnome-settings-daemon/gsd-mouse
! sysadmin     3386 tty2   /usr/lib/gnome-settings-daemon/gsd-power
! sysadmin     3391 tty2   /usr/lib/gnome-settings-daemon/gsd-print-notifications
! sysadmin     3467 tty2   /usr/lib/gnome-settings-daemon/gsd-printer
! sysadmin     3393 tty2   /usr/lib/gnome-settings-daemon/gsd-rfkill
! sysadmin     3396 tty2   /usr/lib/gnome-settings-daemon/gsd-screensaver-proxy
! sysadmin     3399 tty2   /usr/lib/gnome-settings-daemon/gsd-sharing
! sysadmin     3400 tty2   /usr/lib/gnome-settings-daemon/gsd-smartcard
! sysadmin     3405 tty2   /usr/lib/gnome-settings-daemon/gsd-sound
! sysadmin     3412 tty2   /usr/lib/gnome-settings-daemon/gsd-wacom
! sysadmin     3414 tty2   /usr/lib/gnome-settings-daemon/gsd-xsettings
! sysadmin     3295 tty2   ibus-daemon --xim --panel disable
! sysadmin     3313 tty2   /usr/lib/ibus/ibus-dconf
! sysadmin     3557 tty2   /usr/lib/ibus/ibus-engine-simple
! sysadmin     3316 tty2   /usr/lib/ibus/ibus-x11 --kill-daemon
! sysadmin     3492 tty2   nautilus-desktop
! sysadmin     5862 pts/0  bash
! root        21537 pts/1  /bin/sh /usr/sbin/chkrootkit -x
! root        21972 pts/1  ./chkutmp
! root        21974 pts/1  ps axk tty,ruser,args -o tty,pid,ruser,args
! root        21973 pts/1  sh -c ps axk "tty,ruser,args" -o "tty,pid,ruser,args"
! root        21536 pts/1  sudo chkrootkit -x
! sysadmin     5248 pts/1  bash
chkutmp: nothing deleted
not tested
sysadmin@UbuntuDesktop:~$
```