**Ernest Pobee - Unit 4 Homework**

**Week 4 Homework Submission File: 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:

Is -l shadow 
1 root shadow 2989 Oct 9 13:35 shadow 

* Command to set permissions (if needed):

No command required to set permissions

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

* Command to inspect permissions:

-rw-r-- 
Is -l gshadow 
1 root shadow 1094 Oct 9 13:34 gshadow 

* Command to set permissions (if needed):

Is -l gshadow 
1 root shadow 1094 Oct 9 13:34 gshadow 
-rw-r----- 
sudo chmod 600 gshadow 
sysadmin@UbuntuDesktop : /etcS 

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

* Command to inspect permissions:

Is 
-l 
I-rw-r--r-- 
1 root root 
sysadmin@UbuntuDesktop : /etcS 
1323 oct 
9 
group 
13:34 group 

* Command to set permissions (if needed):

No command required to set permissions

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

* Command to inspect permissions:

Is 
-l 
1 root root 
-rw-r--r-- 
sysadmin@UbuntuDesktop : /etcS 
3190 oct 
9 
/etc/passwd 
13:35 /etc/passwd 

* Command to set permissions (if needed):

No command required to set permissions

**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):











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

* Command to add admin to the sudo group:



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

1. Add an engineers group to the system.
   * Command to add group:



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

* Command to add users to engineers group (include all four users):









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

Command to create the shared folder:

sysadminßUbuntuDesktop: 'homes Is -al engineers/ 
total 8 
drwxr -xr-x 2 root engineers 4e96 Oct 12 17:47 

  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:



Or **sudo chgrp -R engineers /home/engineers**

**Step 4: Lynis Auditing**

1. Command to install Lynis:

**sudo apt install Lynis**

****

2. Command to see documentation and instructions:



**man <command>**

**<command> --ls help**

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.

* Screenshot of report output:

Text

Description automatically generated

[+] Kernet Hardening 
- Compartng sysctl key patrs With scan 
- fs.protected hardltnks (exp: 1) 
- fs.protected_symltnks (exp: 1) 
- fs.sutd_dumpable (exp: O) 
kernet. core uses_ptd (exp: 1) 
- kernet.ctrl-alt-del (exp: O) 
kernet .dmesg_restrtct (exp: 1) 
kernet.kptr_restrtct (exp: 2) 
kernet. randomtze_va space (exp: 2) 
kernet. sysrq (exp: O) 
kernet.yama.ptrace scope (exp: 1 2 
proftle 
3) 
(exp: O) 
net. tpv4. conf. 
net. tpv4. conf. 
net. tpv4. conf. 
net. tpv4. conf. 
net. tpv4. conf. 
net. tpv4. conf. 
net. tpv4. conf. 
net. tpv4. conf. 
net. tpv4. conf. 
net. tpv4. conf. 
net. tpv4. conf. 
net. tpv4. conf. 
net . tpv4. tcmp 
. accept_redt rects 
. accept_source route (exp. 
bootp_relay (exp: O) 
all. 
forwardtng (exp: O) 
all. 
log_marttans (exp: 1) 
all. 
.mc_forwardtng (exp: O) 
proxy_arp (exp: O) 
all. 
rp_ftlter (exp: 1) 
all. 
. send_redtrects (exp: O) 
default.accept_redtrects (exp: O) 
default. accept_source route (exp 
default. log_marttans (exp: 1) 
echo_tgnore_broadcasts (exp: 1) 
net. tpv4. tcmp_tgnore_bogus_error responses (exp: 
net. tpv4. tcp_syncooktes (exp: 1) 
net. tpv4. tcp_ttmestamps (exp: 0 1) 
net. tpv6.conf.all.accept_redtrects (exp: O) 
net. tpv6.conf.all.accept_source route (exp: O) 
net. tpv6.conf.default.accept_redtrects (exp: O) 
net. tpv6. conf.default.accept_source route (exp. 
1) 
OK ] 
OK ] 
DIFFERENT 
DIFFERENT 
OK ] 
DIFFERENT 
DIFFERENT 
OK ] 
DIFFERENT 
OK ] 
OK ] 
OK ] 
OK ] 
DIFFERENT 
DIFFERENT 
OK ] 
OK ] 
OK ] 
DIFFERENT 
DIFFERENT 
DIFFERENT 
DIFFERENT 
OK ] 
OK ] 
OK ] 
OK ] 
DIFFERENT 
OK ] 
DIFFERENT 
OK ] 

**Bonus**

1. Command to install chkrootkit:



2. Command to see documentation and instructions:



3. Command to run expert mode:



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

* Screenshot of end of sample output:

1. **Ensure the Linux/Ebury file is tested**
2. **Investigate, isolate and remove possible Malicious Linux.Xor.Ddos installed**

**Searching 
Searching 
Searching 
Searching 
Searching 
Searching 
Searching 
Searching 
Searching 
Searchin 
Searchin 
Searching 
Searching 
Searching 
Searching 
Searching 
Searching 
3.sh 
fo r 
for 
for 
for 
for 
for 
for 
for 
for 
for 
for 
for 
for 
for 
for 
for 
for 
/ tmp/burpsut 
ZK rootktt default files and dirs. 
ShKtt rootktt default files and dirs. 
AjaKtt rootktt default files and dirs. .. 
zaRwT rootktt default files and dirs. .. 
Madaltn rootktt default files. 
Fu rootktt default files. 
ESRK rootktt default files. 
rootedoor... 
ENYELKM rootktt default files. 
common ssh-scanners default files... 
Linux Ebur 
O eratton kitndt o ssh... 
64-btt Linux Rootktt 
64-btt Linux Rootktt modules. 
Mumblehard Linux . 
Backdoor.Ltnux .Mokes.a 
Malicious TtnyDNS . 
Linux.Xor.DDoS 
11 
nothing 
nothing 
nothing 
nothing 
nothing 
nothing 
nothing 
nothing 
nothing 
nothin 
found 
found 
found 
found 
found 
found 
found 
found 
found 
found 
/tmp/vagrant-shell 
/tmp/ response . varftle 
/tmp/str . sh 
Searching for Linux.Proxy.1.e . 
Searching for suspect PHP files. 
Searching for anomalies tn shell 
Checking •asp' 
Checking 'bindshell' 
Checking 'lkm' 
chkdtrs: nothing detected 
Checking rexedcs' . 
Checking •sniffer' 
history 
files... 
not tested 
nothing found 
nothing found 
nothing found 
nothing found 
nothing found 
INFECTED: possible Malicious Linux .Xor . DDoS installed 
nothing found 
nothing found 
nothing found 
not infected 
not infected 
chkproc: nothing detected 
not found 
to: not promisc and no packet sniffer sockets 
enpos3: PACKET 
dockere: not promisc and no packet sniffer sockets 
Checking 'w55808' 
Checking 'wted' 
1 deletion(s) between Mon Oct 11 11:19:23 2021 and 
Checking •scalper' 
Checking 'slapper' 
Checking • z2' 
Checking •chkutmp' 
tn /var/run/utmp ! 
Mon 
oct 
not infected 
1 deletion(s) between Frt Oct 
11 17:19:17 2021 
not infected 
not infected 
chklastlog: nothing deleted 
8 2021 and sat oct 
9 2021 
! RUID 
! gdm 
! gdm 
! gdm 
! gdm 
! gdm 
! gdm 
! gdm 
! gdm 
PID 
2024 
1976 
1981 
1988 
2110 
2112 
2116 
2120 
TTY 
ttyl 
ttyl 
ttyl 
ttyl 
ttyl 
ttyl 
ttyl 
ttyl 
CMD 
/usr/btn/xwayland : 1024 
The tty of the following user process(es) were not found 
-rootless -terminate -accessx -core -Itsten 4 -Itsten 5 -displayfd 6 
/usr/ltb/gdm3/gdm-wayland-sesston gnome-session 
-autostart /usr/share/gdm/greeter/autostart 
/usr/ltb/gnome-sesston/gnome-sesston-btnary --autostart /usr/share/gdm/greeter/autostart 
/usr/btn/gnome-shell 
/usr/ltb/gnome-setttngs -daemon/gsd-ally -settings 
/usr/ltb/gnome-setttngs -daemon/gsd-cltpboard 
/usr/ltb/gnome-setttngs-daemon/gsd 
- co lor 
/usr/ltb/gnome-setttngs-daemon/gsd-datettme **