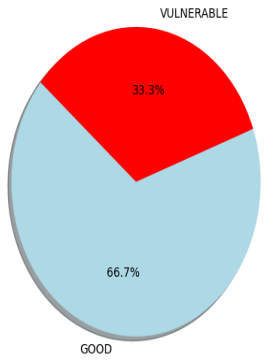
Result

OS info

- CentOS Linux 7 (Core)
- inet 192.168.13.129 netmask 255.255.255.0 broadcast 192.168.13.255

Summary Chart



Summary Table

No	Result
1.Default ID Check	BAD
2.Root MGM Check	GOOD
3.Passwd File Check	GOOD
4.Group File Check	GOOD
5.Password Rule Check	BAD
6.Default Shell Check	GOOD
7-1.SU Permission Check(pam.d)	BAD
7-2.SU Permission Check(wheel)	GOOD
8.Shadow File Check	GOOD

Detail

1.Default ID Check

- Result : BAD
- Detail

lp, uucp, nuucp founded!!

root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:999:998:User for polkitd:/:/sbin/nologin
libstoragemgmt:x:998:995:daemon account for libstoragemgmt:/var/run/lsm:/sbin/nologin

colord:x:997:994:User for colord:/var/lib/colord:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
saned:x:996:993:SANE scanner daemon user:/usr/share/sane:/sbin/nologin
gluster:x:995:992:GlusterFS daemons:/run/gluster:/sbin/nologin
saslauth:x:994:76:Saslauthd user:/run/saslauthd:/sbin/nologin
abrt:x:173:173::/etc/abrt:/sbin/nologin
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
pulse:x:171:171:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin
radvd:x:75:75:radvd user:/:/sbin/nologin
chrony:x:993:988::/var/lib/chrony:/sbin/nologin
unbound:x:992:987:Unbound DNS resolver:/etc/unbound:/sbin/nologin
qemu:x:107:107:qemu user:/:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
tss:x:59:59:Account used by the trousers package to sandbox the tcsd daemon:/dev/null:/sbin/nologin
usbmuxd:x:113:113:usbmuxd user:/:/sbin/nologin
geoclue:x:991:985:User for geoclue:/var/lib/geoclue:/sbin/nologin
sssd:x:990:984:User for sssd:/:/sbin/nologin
setroubleshoot:x:989:983::/var/lib/setroubleshoot:/sbin/nologin
gdm:x:42:42::/var/lib/gdm:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
gnome-initial-setup:x:988:982::/run/gnome-initial-setup/:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
kimg00n:x:1000:1000:kimg00n:/home/kimg00n:/bin/bash

2.Root MGM Check

- Result : GOOD
- Detail

only root have uid 0

root -> UID= 0

3.Passwd File Check

- Result : GOOD
- Detail

passwd file permission is 644

-rw-r--r--. 1 root root 2313 10ì›” 6 06:31 /etc/passwd

4.Group File Check

- Result : GOOD
- Detail

group file permission is 644

-rw-r--r--. 1 root root 983 10ì›” 7 22:45 /etc/group

5.Password Rule Check

- Result : BAD
- Detail

PASS_MIN_LEN   5
PASS_MAX_DAYS   99999
PASS_MIN_DAYS   0

6.Default Shell Check

- Result : GOOD
- Detail

nologin user doesn't have shell

bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin

7-1.SU Permission Check(pam.d)

- Result : BAD
- Detail

su command will execute with unauth user!!

```
#%PAM-1.0
auth        sufficient  pam_rootok.so
# Uncomment the following line to implicitly trust users in the "wheel" group.
#auth       sufficient  pam_wheel.so trust use_uid
# Uncomment the following line to require a user to be in the "wheel" group.
#auth       required    pam_wheel.so use_uid
auth        substack    system-auth
auth        include     postlogin
account     sufficient  pam_succeed_if.so uid = 0 use_uid quiet
account     include     system-auth
password    include     system-auth
session     include     system-auth
session     include     postlogin
session     optional    pam_xauth.so
```

7-2.SU Permission Check(wheel)

- Result : GOOD
- Detail

wheel group user doesn't exist

```
root:x:0:
bin:x:1:
daemon:x:2:
sys:x:3:
adm:x:4:
tty:x:5:
disk:x:6:
lp:x:7:
mem:x:8:
kmem:x:9:
wheel:x:10:
cdrom:x:11:
mail:x:12:postfix
man:x:15:
dialout:x:18:
floppy:x:19:
games:x:20:
tape:x:33:
video:x:39:
ftp:x:50:
lock:x:54:
audio:x:63:
nobody:x:99:
users:x:100:
utmp:x:22:
utempter:x:35:
stapusr:x:156:
stapsys:x:157:
stapdev:x:158:
input:x:999:
systemd-journal:x:190:
systemd-network:x:192:
dbus:x:81:
polkitd:x:998:
printadmin:x:997:
cgred:x:996:
libstoragemgmt:x:995:
colord:x:994:
rpc:x:32:
```

saned:x:993:
dip:x:40:
gluster:x:992:
ssh_keys:x:991:
saslauth:x:76:
abrt:x:173:
rtkit:x:172:
pulse-access:x:990:
pulse-rt:x:989:
pulse:x:171:
radvd:x:75:
chrony:x:988:
unbound:x:987:
kvm:x:36:qemu
qemu:x:107:
ntp:x:38:
tss:x:59:
libvirt:x:986:
usbmuxd:x:113:
geoclue:x:985:
sssd:x:984:
setroubleshoot:x:983:
gdm:x:42:
rpcuser:x:29:
nfsnobody:x:65534:
gnome-initial-setup:x:982:
sshd:x:74:
slocate:x:21:
avahi:x:70:
postdrop:x:90:
postfix:x:89:
tcpdump:x:72:
kimg00n:x:1000:kimg00n

8.Shadow File Check

- Result : GOOD
- Detail

shadow file permission is Good

----------. 1 root root 1266 10ì›” 6 06:31 /etc/shadow