

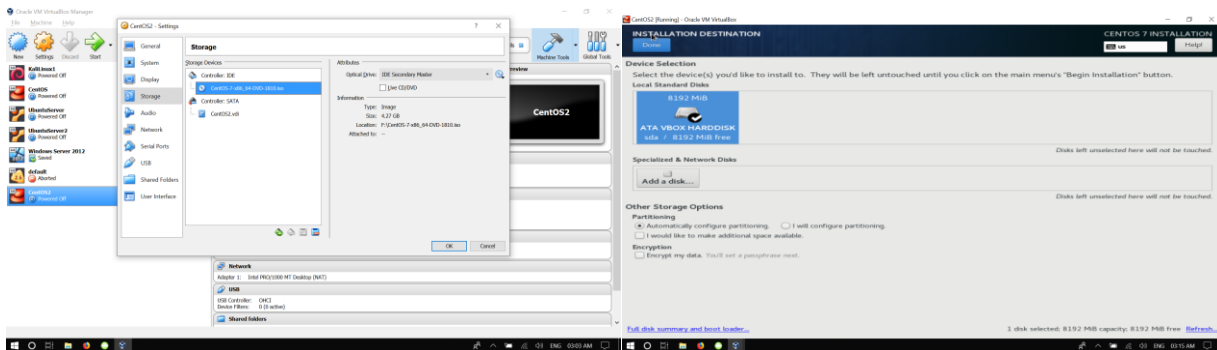
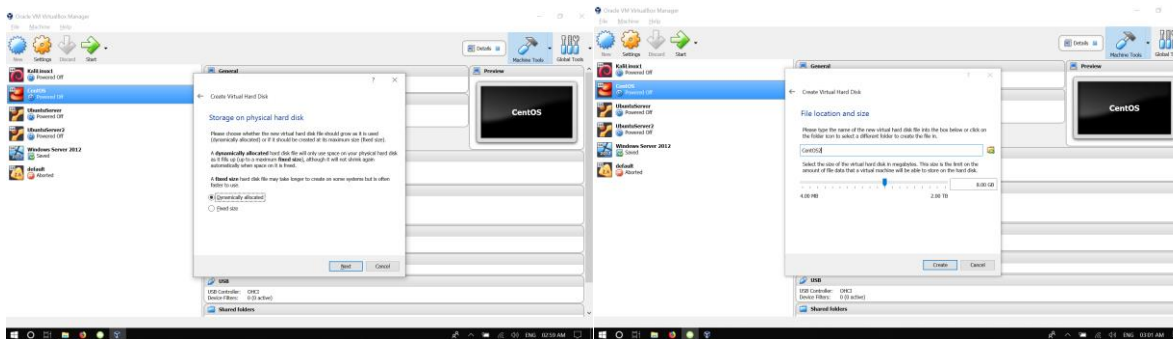
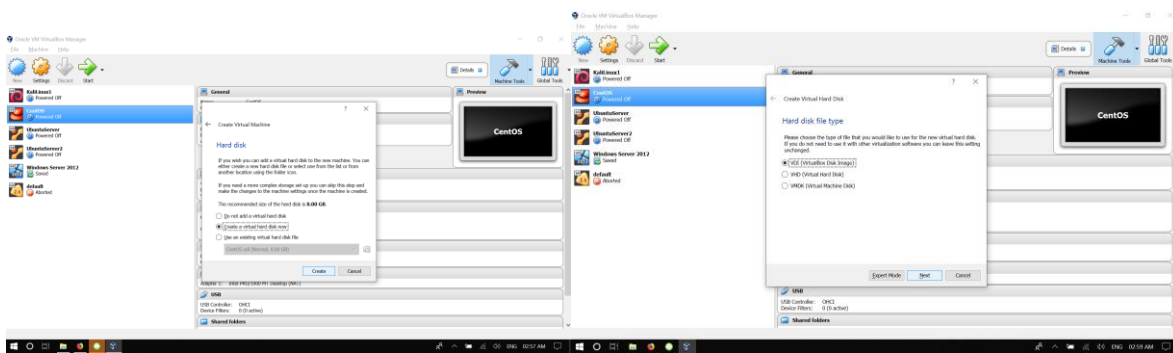
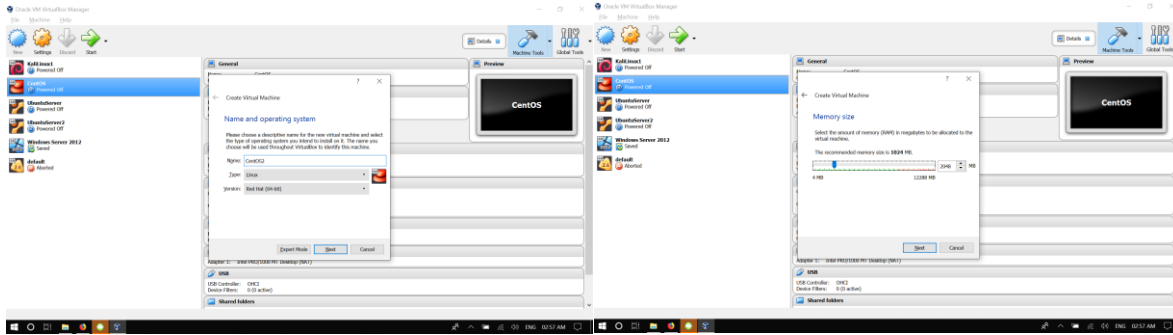
EECS 3482

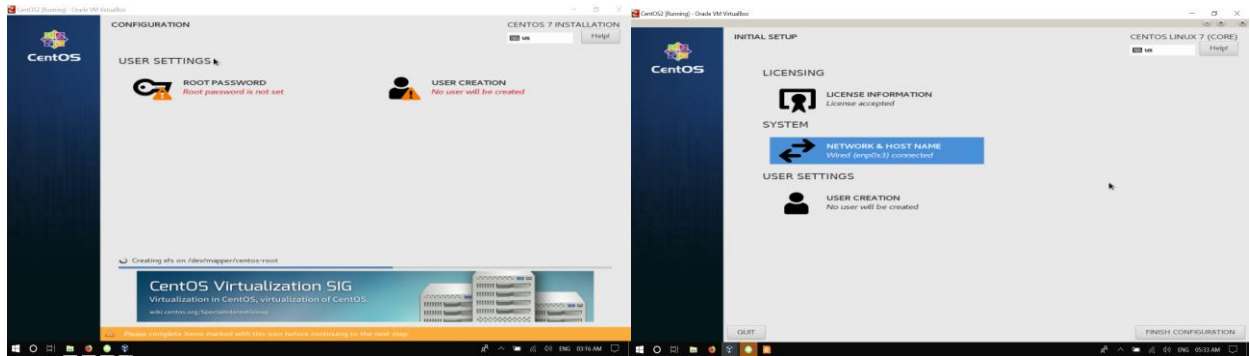
Lab 6

Name : AKALPIT SHARMA

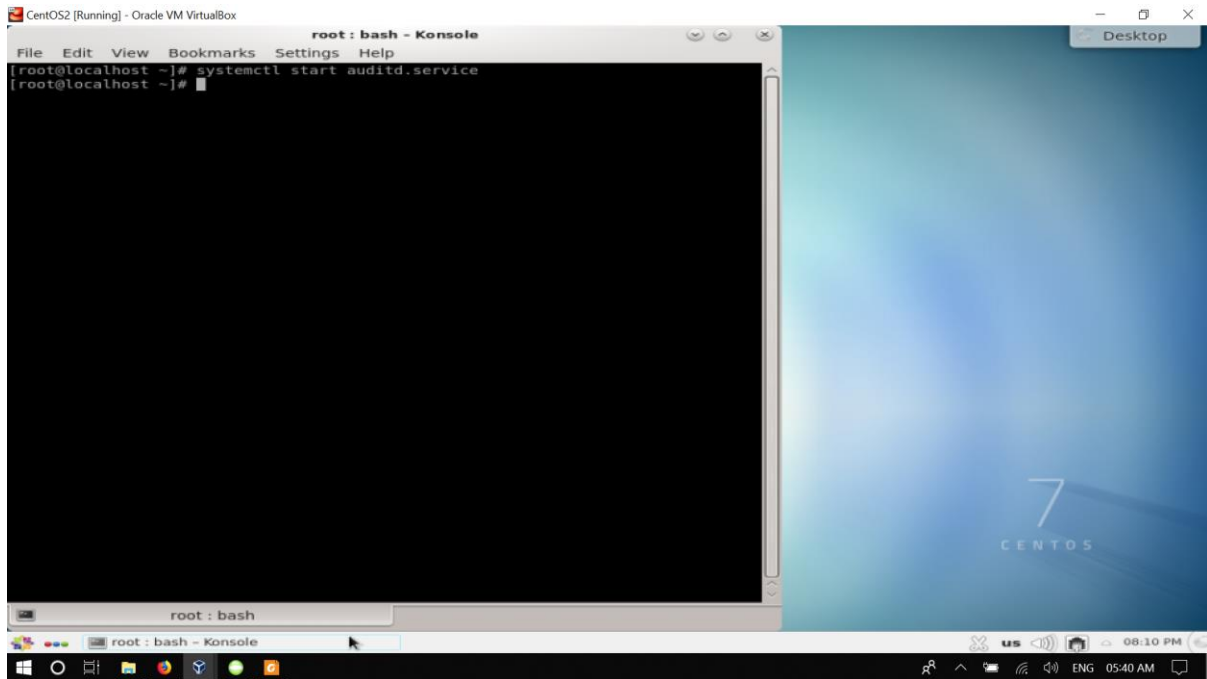
id : 212650628

Q1, Q2, Q3

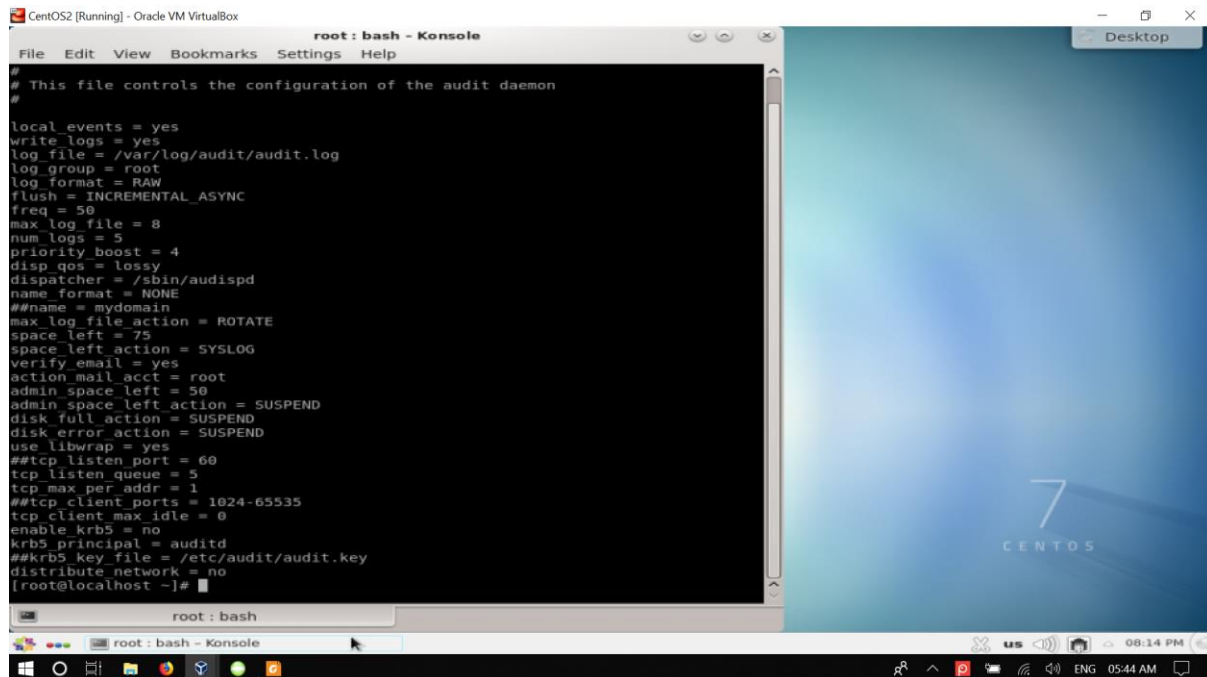




Q4



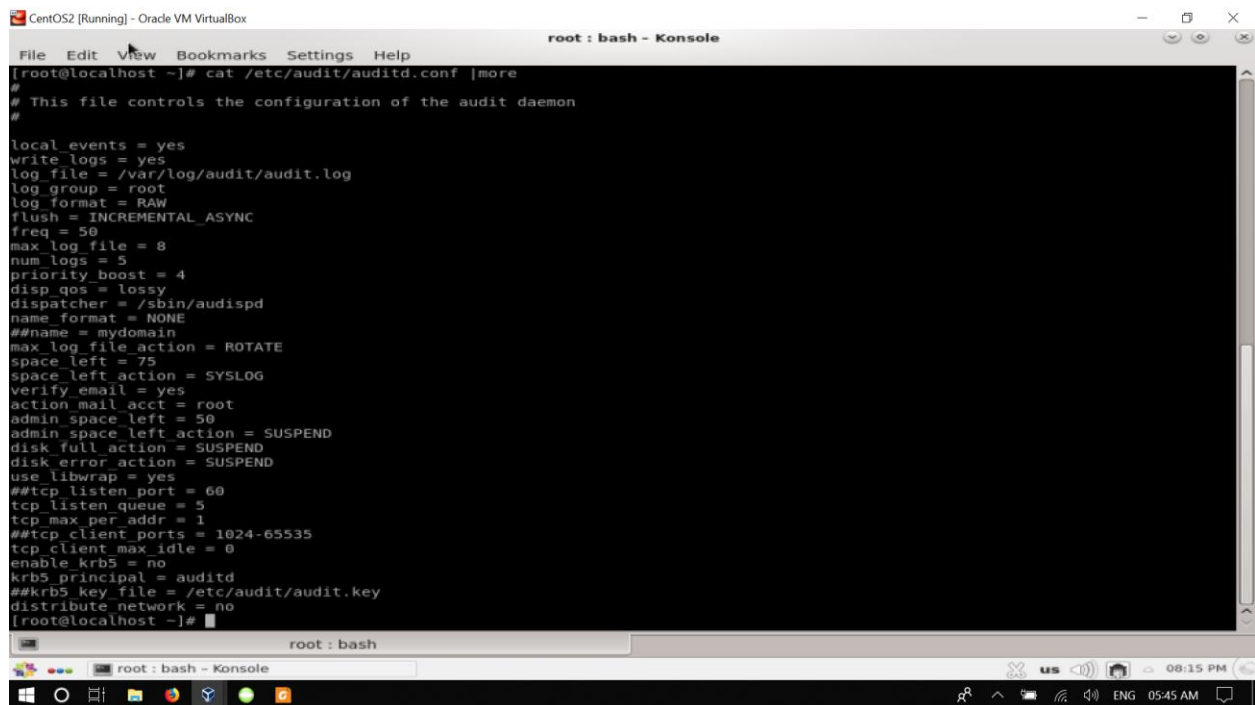
Q5 i



The screenshot shows a terminal window titled "root: bash - Konsole" within a "CentOS2 [Running] - Oracle VM VirtualBox" environment. The terminal displays the contents of the `/etc/audit/auditd.conf` file. The configuration includes settings for local events, logging, and network connections. The desktop background on the right shows the CentOS logo and the number 7.

```
# This file controls the configuration of the audit daemon
#
local_events = yes
write_logs = yes
log_file = /var/log/audit/audit.log
log_group = root
log_format = RAW
flush = INCREMENTAL_ASYNC
freq = 50
max_log_file = 8
num_logs = 5
priority_boost = 4
disp_qos = lossy
dispatcher = /sbin/audispd
name_format = NONE
##name = mydomain
max_log_file_action = ROTATE
space_left = 75
space_left_action = SYSLOG
verify_email = yes
action_mail_acct = root
admin_space_left = 50
admin_space_left_action = SUSPEND
disk_full_action = SUSPEND
disk_error_action = SUSPEND
use_libwrap = yes
##tcp_listen_port = 60
tcp_listen_queue = 5
tcp_max_per_addr = 1
##tcp_client_ports = 1024-65535
tcp_client_max_idle = 0
enable_krb5 = no
krb5_principal = auditd
##krb5_key_file = /etc/audit/audit.key
distribute_network = no
[root@localhost ~]#
```

Q5 ii



The screenshot shows a terminal window titled "root: bash - Konsole" within a "CentOS2 [Running] - Oracle VM VirtualBox" environment. The terminal shows the command `cat /etc/audit/auditd.conf | more` being executed, which displays the same configuration as in the previous screenshot. The desktop background on the right shows the CentOS logo and the number 7.

```
[root@localhost ~]# cat /etc/audit/auditd.conf | more
# This file controls the configuration of the audit daemon
#
local_events = yes
write_logs = yes
log_file = /var/log/audit/audit.log
log_group = root
log_format = RAW
flush = INCREMENTAL_ASYNC
freq = 50
max_log_file = 8
num_logs = 5
priority_boost = 4
disp_qos = lossy
dispatcher = /sbin/audispd
name_format = NONE
##name = mydomain
max_log_file_action = ROTATE
space_left = 75
space_left_action = SYSLOG
verify_email = yes
action_mail_acct = root
admin_space_left = 50
admin_space_left_action = SUSPEND
disk_full_action = SUSPEND
disk_error_action = SUSPEND
use_libwrap = yes
##tcp_listen_port = 60
tcp_listen_queue = 5
tcp_max_per_addr = 1
##tcp_client_ports = 1024-65535
tcp_client_max_idle = 0
enable_krb5 = no
krb5_principal = auditd
##krb5_key_file = /etc/audit/audit.key
distribute_network = no
[root@localhost ~]#
```

Q6

```

CentOS2 [Running] - Oracle VM VirtualBox
root : bash - Konsole

success'
type=USER_LOGIN msg=audit(1554163479.630:154): pid=13244 uid=0 auid=0 ses=3 subj=system u:system r:xdm t:s0-s0:c0.c1023 msg='
uid=0 exe="/usr/libexec/gdm-session-worker" hostname=? addr=? terminal=? res=success'
type=AVC msg=audit(1554163479.967:155): avc: denied { create } for pid=13262 comm="gdm-session-wor" name="gdm" scontext=system u:system r:xdm t:s0-s0:c0.c1023 tcontext=system u:object r:admin home t:s0 tclass=dir permissive=0
type=SYSCALL msg=audit(1554163479.967:155): arch=c000003e syscall=83 success=no exit=-13 a0=55f0a4980100 a1=1c0 a2=55f0a4980110 a3=b items=0 ppid=13244 pid=13262 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=3 comm="gdm-session-wor" exe="/usr/libexec/gdm-session-worker" subj=system u:system r:xdm t:s0-s0:c0.c1023 key=(null)
type=PROCTITLE msg=audit(1554163479.967:155): proctitle=67646D2D73657373696F6E2D776F72686572205B70616D2F67646D2D70617373776F72645D
type=SERVICE_STOP msg=audit(1554163480.135:156): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system u:system r:init t:s0 msg='unit=systemd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'
type=SERVICE_STOP msg=audit(1554163480.293:157): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system u:system r:init t:s0 msg='unit=systemd-hostnamed comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'
type=SERVICE_STOP msg=audit(1554163511.204:158): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system u:system r:init t:s0 msg='unit=realmd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'
type=USER ACCT msg=audit(1554163801.536:159): pid=3846 uid=0 auid=4294967295 ses=4294967295 subj=system u:system r:crond t:s0-s0:c0.c1023 msg='op=PAM:accounting grantors=pam_access,pam_unix,pam_localuser acct="root" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'
type=CRED ACQ msg=audit(1554163801.537:160): pid=3846 uid=0 auid=4294967295 ses=4294967295 subj=system u:system r:crond t:s0-s0:c0.c1023 msg='op=PAM:setcred grantors=pam_env,pam_unix acct="root" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'
type=LOGIN msg=audit(1554163801.538:161): pid=3846 uid=0 auid=4294967295 ses=4294967295 subj=system u:system r:crond t:s0-s0:c0.c1023 old-auid=4294967295 auid=0 tty=(none) old-ses=4294967295 ses=4 res=1
type=USER START msg=audit(1554163801.618:162): pid=3846 uid=0 auid=4294967295 ses=4294967295 subj=system u:system r:crond t:s0-s0:c0.c1023 msg='op=PAM:session open grantors=pam_loginuid,pam_keyinit,pam_limits,pam_systemd acct="root" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'
type=CRED REFR msg=audit(1554163801.621:163): pid=3846 uid=0 auid=4294967295 ses=4294967295 subj=system u:system r:crond t:s0-s0:c0.c1023 msg='op=PAM:setcred grantors=pam_env,pam_unix acct="root" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'
type=CRED DISP msg=audit(1554163801.746:164): pid=3846 uid=0 auid=4294967295 ses=4294967295 subj=system u:system r:crond t:s0-s0:c0.c1023 msg='op=PAM:setcred grantors=pam_env,pam_unix acct="root" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'
type=USER END msg=audit(1554163801.753:165): pid=3846 uid=0 auid=4294967295 ses=4294967295 subj=system u:system r:crond t:s0-s0:c0.c1023 msg='op=PAM:session close grantors=pam_loginuid,pam_keyinit,pam_limits,pam_systemd acct="root" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'
type=SERVICE_START msg=audit(1554164171.310:166): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system u:system r:init t:s0 msg='unit=systemd-tmpfiles-clean comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'
type=SERVICE_STOP msg=audit(1554164171.310:167): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system u:system r:init t:s0 msg='unit=systemd-tmpfiles-clean comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'
[root@localhost ~]#

```

Q7

```

CentOS2 [Running] - Oracle VM VirtualBox
root : bash - Konsole

type=SERVICE_STOP msg=audit(1554164171.310:167): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system u:system r:init t:s0 msg='unit=systemd-tmpfiles-clean comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'
[root@localhost ~]# auditctl | more
usage: auditctl [options]
  -a <L,A>          Append rule to end of <L>list with <A>action
  -A <L,A>          Add rule at beginning of <L>list with <A>action
  -b <backlog>       Set max number of outstanding audit buffers
                        allowed Default=64
  -C                Continue through errors in rules
  -C f=f            Compare collected fields if available:
                        Field name, operator(=,!=,<,>,<=,>=),
                        l=task,exit,user,exclude
                        a=never,always
  -D                Delete all rules and watches
  -e [0..2]         Set enabled flag
  -f [0..2]         Set failure flag
                        0=silent 1=printk 2=panic
  -F f=vv           Build rule: field name, operator(=,!=,<,>,<=,>=),
                        >=,<=,<=) value
  -h                Help
  -i                Ignore errors when reading rules from file
  -k <key>          Set filter key on audit rule
  -l               List rules
  -m text           Send a user-space message
  -p [r|w|x|a]      Set permissions filter on watch
                        r=read, w=write, x=execute, a=attribute
  -q <mount,subtree> make subtree part of mount point's dir watches
  -r <rate>         Set limit in messages/sec (0=none)
  -R <file>         read rules from file
  -s               Report status
  -S syscall        Build rule: syscall name or number
  -t               Trim directory watches
  -v               Version
  -W <path>         Insert watch at <path>
  -W <path>         Remove watch at <path>
  --loginuid-immutable Make loginuids unchangeable once set
  --reset-lost      Reset the lost record counter
[root@localhost ~]#

```

Q8

```
CentOS2 [Running] - Oracle VM VirtualBox
root : bash - Konsole

File Edit View Bookmarks Settings Help

-c          allowed Default=64
            Continue through errors in rules
-C f=f      Compare collected fields if available:
            Field name, operator(=,!=), field name
-d <l,a>     Delete rule from <l>ist with <a>ction
            l=task,exit,user,exclude
            a=never,always
-D          Delete all rules and watches
-e [0..2]   Set enabled flag
-f [0..2]   Set failure flag
            0=silent 1=printk 2=panic
-F f=v      Build rule: field name, operator(=,!=,<,>,<=,
            >=,&,&=) value
-h          Help
-i          Ignore errors when reading rules from file
-k <key>    Set filter key on audit rule
-l          List rules
-m text     Send a user-space message
-p [r|w|x|a] Set permissions filter on watch
            r=read, w=write, x=execute, a=attribute
-q <mount,subtree> make subtree part of mount point's dir watches
-r <rate>   Set limit in messages/sec (0=none)
-R <file>   read rules from file
-s          Report status
-S syscall  Build rule: syscall name or number
-t          Trim directory watches
-v          Version
-W <path>   Insert watch at <path>
-W <path>   Remove watch at <path>
--loginuid-immutable Make loginuids unchangeable once set
--reset-lost Reset the lost record counter

[root@localhost ~]# auditctl -l
No rules
[root@localhost ~]# auditctl -a exit,always -F path=/etc/passwd -F perm=wa
Append rule - bad keyword exit,always
[root@localhost ~]# auditctl -a exit,always -F path=/etc/passwd -F perm=wa
[root@localhost ~]# ausearch -f /etc/passwd
<no matches>
[root@localhost ~]#
```

Q9

```
CentOS2 [Running] - Oracle VM VirtualBox
root : bash - Konsole

File Edit View Bookmarks Settings Help

No rules
[root@localhost ~]# auditctl -a exit,always -F path=/etc/passwd -F perm=wa
Append rule - bad keyword exit,always
[root@localhost ~]# auditctl -a exit,always -F path=/etc/passwd -F perm=wa
[root@localhost ~]# ausearch -f /etc/passwd
<no matches>
[root@localhost ~]# adduser xyz
[root@localhost ~]# ausearch -f /etc/passwd
----
time->Mon Apr 1 20:19:51 2019
type=CONFIG_CHANGE msg=audit(1554164391.154:172): auid=0 ses=3 op=updated_rules path="/etc/passwd" key=(null) list=4 res=1
----
time->Mon Apr 1 20:19:50 2019
type=PROCTITLE msg=audit(1554164390.778:169): proctitle=616464757365720078797A
type=PATH msg=audit(1554164390.778:169): item=0 name="/etc/passwd" inode=6246317 dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00
:00 obj=system u:object r:passwd file t:s0 objtype=NORMAL cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=CWD msg=audit(1554164390.778:169): cwd="/root"
type=SYSCALL msg=audit(1554164390.778:169): arch=c000003e syscall=2 success=yes exit=5 a0=56426b728ce0 a1=20902 a2=0 a3=8 ite
ms=1 ppid=17372 pid=28758 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts1 ses=3 comm="adduser" exe="/
usr/sbin/useradd" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=(null)
----
time->Mon Apr 1 20:19:51 2019
type=PROCTITLE msg=audit(1554164391.154:173): proctitle=616464757365720078797A
type=PATH msg=audit(1554164391.154:173): item=4 name="/etc/passwd" inode=4204141 dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00
:00 obj=system u:object r:passwd file t:s0 objtype=CREATE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=PATH msg=audit(1554164391.154:173): item=3 name="/etc/passwd" inode=6246317 dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00
:00 obj=system u:object r:passwd file t:s0 objtype=DELETE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=PATH msg=audit(1554164391.154:173): item=2 name="/etc/passwd" inode=4204141 dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00
:00 obj=system u:object r:passwd file t:s0 objtype=DELETE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=PATH msg=audit(1554164391.154:173): item=1 name="/etc/" inode=4194369 dev=fd:00 mode=040755 ouid=0 ogid=0 rdev=00:00 obj
=system u:object r:etc t:s0 objtype=PARENT cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=PATH msg=audit(1554164391.154:173): item=0 name="/etc/" inode=4194369 dev=fd:00 mode=040755 ouid=0 ogid=0 rdev=00:00 obj
=system u:object r:etc t:s0 objtype=PARENT cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=CWD msg=audit(1554164391.154:173): cwd="/root"
type=SYSCALL msg=audit(1554164391.154:173): arch=c000003e syscall=82 success=yes exit=0 a0=7fffd9d547070 a1=56426b728ce0 a2=7f
fd9d546fe0 a3=56426bc03db0 items=5 ppid=17372 pid=28758 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pt
s1 ses=3 comm="adduser" exe="/usr/sbin/useradd" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=(null)
[root@localhost ~]#
```


Q10

```
CentOS2 [Running] - Oracle VM VirtualBox
root : bash - Konsole

File Edit View Bookmarks Settings Help

No rules
[root@localhost ~]# auditctl -a exit,always -F path=/etc/passwd -F perm=wa
Append rule - bad keyword exit,always
[root@localhost ~]# auditctl -a exit,always -F path=/etc/passwd -F perm=wa
[root@localhost ~]# ausearch -f /etc/passwd
<no matches>
[root@localhost ~]# adduser xyz
[root@localhost ~]# ausearch -f /etc/passwd
----
time->Mon Apr 1 20:19:51 2019
type=CONFIG_CHANGE msg=audit(1554164391.154:172): auid=0 ses=3 op=updated_rules path="/etc/passwd" key=(null) list=4 res=1
----
time->Mon Apr 1 20:19:50 2019
type=PROCTITLE msg=audit(1554164390.778:169): proctitle=616464757365720078797A
type=PATH msg=audit(1554164390.778:169): item=0 name="/etc/passwd" inode=6246317 dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00
:00 obj=system u:object r:passwd file t:s0 objtype=NORMAL cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=CWD msg=audit(1554164390.778:169): cwd="/root"
type=SYSCALL msg=audit(1554164390.778:169): arch=c000003e syscall=2 success=yes exit=5 a0=56426b728ce0 a1=20902 a2=0 a3=8 ite
ms=1 ppid=17372 pid=28758 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts1 ses=3 comm="adduser" exe="/
usr/sbin/useradd" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=(null)
----
time->Mon Apr 1 20:19:51 2019
type=PROCTITLE msg=audit(1554164391.154:173): proctitle=616464757365720078797A
type=PATH msg=audit(1554164391.154:173): item=4 name="/etc/passwd" inode=4204141 dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00
:00 obj=system u:object r:passwd file t:s0 objtype=CREATE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=PATH msg=audit(1554164391.154:173): item=3 name="/etc/passwd" inode=6246317 dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00
:00 obj=system u:object r:passwd file t:s0 objtype=DELETE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=PATH msg=audit(1554164391.154:173): item=2 name="/etc/passwd+" inode=4204141 dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00
:00 obj=system u:object r:passwd file t:s0 objtype=DELETE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=PATH msg=audit(1554164391.154:173): item=1 name="/etc/" inode=4194369 dev=fd:00 mode=040755 ouid=0 ogid=0 rdev=00:00 obj
=system u:object r:etc t:s0 objtype=PARENT cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=PATH msg=audit(1554164391.154:173): item=0 name="/etc/" inode=4194369 dev=fd:00 mode=040755 ouid=0 ogid=0 rdev=00:00 obj
=system u:object r:etc t:s0 objtype=PARENT cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=CWD msg=audit(1554164391.154:173): cwd="/root"
type=SYSCALL msg=audit(1554164391.154:173): arch=c000003e syscall=82 success=yes exit=0 a0=7ffd9d547070 a1=56426b728ce0 a2=7f
fd9d546fe0 a3=56426bc03db0 items=5 ppid=17372 pid=28758 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pt
s1 ses=3 comm="adduser" exe="/usr/sbin/useradd" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=(null)
[root@localhost ~]#
```

Q11

```
CentOS2 [Running] - Oracle VM VirtualBox
root : bash - Konsole

File Edit View Bookmarks Settings Help

No rules
[root@localhost ~]# auditctl -a exit,always -F path=/etc/passwd -F perm=wa
Append rule - bad keyword exit,always
[root@localhost ~]# auditctl -a exit,always -F path=/etc/passwd -F perm=wa
[root@localhost ~]# ausearch -f /etc/passwd
<no matches>
[root@localhost ~]# adduser xyz
[root@localhost ~]# ausearch -f /etc/passwd
----
time->Mon Apr 1 20:19:51 2019
type=CONFIG_CHANGE msg=audit(1554164391.154:172): auid=0 ses=3 op=updated_rules path="/etc/passwd" key=(null) list=4 res=1
----
time->Mon Apr 1 20:19:50 2019
type=PROCTITLE msg=audit(1554164390.778:169): proctitle=616464757365720078797A
type=PATH msg=audit(1554164390.778:169): item=0 name="/etc/passwd" inode=6246317 dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00
:00 obj=system u:object r:passwd file t:s0 objtype=NORMAL cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=CWD msg=audit(1554164390.778:169): cwd="/root"
type=SYSCALL msg=audit(1554164390.778:169): arch=c000003e syscall=2 success=yes exit=5 a0=56426b728ce0 a1=20902 a2=0 a3=8 ite
ms=1 ppid=17372 pid=28758 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts1 ses=3 comm="adduser" exe="/
usr/sbin/useradd" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=(null)
----
time->Mon Apr 1 20:19:51 2019
type=PROCTITLE msg=audit(1554164391.154:173): proctitle=616464757365720078797A
type=PATH msg=audit(1554164391.154:173): item=4 name="/etc/passwd" inode=4204141 dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00
:00 obj=system u:object r:passwd file t:s0 objtype=CREATE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=PATH msg=audit(1554164391.154:173): item=3 name="/etc/passwd" inode=6246317 dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00
:00 obj=system u:object r:passwd file t:s0 objtype=DELETE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=PATH msg=audit(1554164391.154:173): item=2 name="/etc/passwd+" inode=4204141 dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00
:00 obj=system u:object r:passwd file t:s0 objtype=DELETE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=PATH msg=audit(1554164391.154:173): item=1 name="/etc/" inode=4194369 dev=fd:00 mode=040755 ouid=0 ogid=0 rdev=00:00 obj
=system u:object r:etc t:s0 objtype=PARENT cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=PATH msg=audit(1554164391.154:173): item=0 name="/etc/" inode=4194369 dev=fd:00 mode=040755 ouid=0 ogid=0 rdev=00:00 obj
=system u:object r:etc t:s0 objtype=PARENT cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=CWD msg=audit(1554164391.154:173): cwd="/root"
type=SYSCALL msg=audit(1554164391.154:173): arch=c000003e syscall=82 success=yes exit=0 a0=7ffd9d547070 a1=56426b728ce0 a2=7f
fd9d546fe0 a3=56426bc03db0 items=5 ppid=17372 pid=28758 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pt
s1 ses=3 comm="adduser" exe="/usr/sbin/useradd" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=(null)
[root@localhost ~]#
```

Q12

```
CentOS [Running] - Oracle VM VirtualBox
root : bash - Konsole

File Edit View Bookmarks Settings Help

[root@localhost ~]# adduser xyz
[root@localhost ~]# ausearch -f /etc/passwd
----
time->Mon Apr 1 20:19:51 2019
type=CONFIG_CHANGE msg=audit(1554164391.154:172): auid=0 ses=3 op=updated_rules path="/etc/passwd" key=(null) list=4 res=1
----
time->Mon Apr 1 20:19:50 2019
type=PROCTITLE msg=audit(1554164390.778:169): proctitle=616464757365720078797A
type=PATH msg=audit(1554164391.154:173): item=4 name="/etc/passwd" inode=6246317 dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00
:00 obj=system_u:object_r:passwd_file_t:s0 objtype=CREATE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=CWD msg=audit(1554164390.778:169): cwd="/root"
type=SYSCALL msg=audit(1554164390.778:169): arch=c000003e syscall=2 success=yes exit=5 a0=56426b728ce0 a1=20902 a2=0 a3=8 ite
ms=1 ppid=17372 pid=28758 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts1 ses=3 comm="adduser" exe="/
usr/sbin/useradd" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=(null)
----
time->Mon Apr 1 20:19:51 2019
type=PROCTITLE msg=audit(1554164391.154:173): proctitle=616464757365720078797A
type=PATH msg=audit(1554164391.154:173): item=4 name="/etc/passwd" inode=4204141 dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00
:00 obj=system_u:object_r:passwd_file_t:s0 objtype=CREATE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=PATH msg=audit(1554164391.154:173): item=3 name="/etc/passwd" inode=6246317 dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00
:00 obj=system_u:object_r:passwd_file_t:s0 objtype=DELETE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=PATH msg=audit(1554164391.154:173): item=2 name="/etc/passwd" inode=4204141 dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00
:00 obj=system_u:object_r:passwd_file_t:s0 objtype=DELETE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=PATH msg=audit(1554164391.154:173): item=1 name="/etc/" inode=4194369 dev=fd:00 mode=040755 ouid=0 ogid=0 rdev=00:00 obj
=system_u:object_r:etc_t:s0 objtype=PARENT cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=PATH msg=audit(1554164391.154:173): item=0 name="/etc/" inode=4194369 dev=fd:00 mode=040755 ouid=0 ogid=0 rdev=00:00 obj
=system_u:object_r:etc_t:s0 objtype=PARENT cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=CWD msg=audit(1554164391.154:173): cwd="/root"
type=SYSCALL msg=audit(1554164391.154:173): arch=c000003e syscall=82 success=yes exit=0 a0=7ffd9d547070 a1=56426b728ce0 a2=7f
fd9d546fe0 a3=56426bc03db0 items=5 ppid=17372 pid=28758 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pt
s1 ses=3 comm="adduser" exe="/usr/sbin/useradd" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=(null)
[root@localhost ~]# auscaall x86_64 x
bash: auscaall: command not found
[root@localhost ~]# auscall x86_64 x
bash: auscall: command not found
[root@localhost ~]# dir /etc/passwd -l
-rw-r--r--. 1 root root 1883 Apr 1 20:19 /etc/passwd
[root@localhost ~]#
```

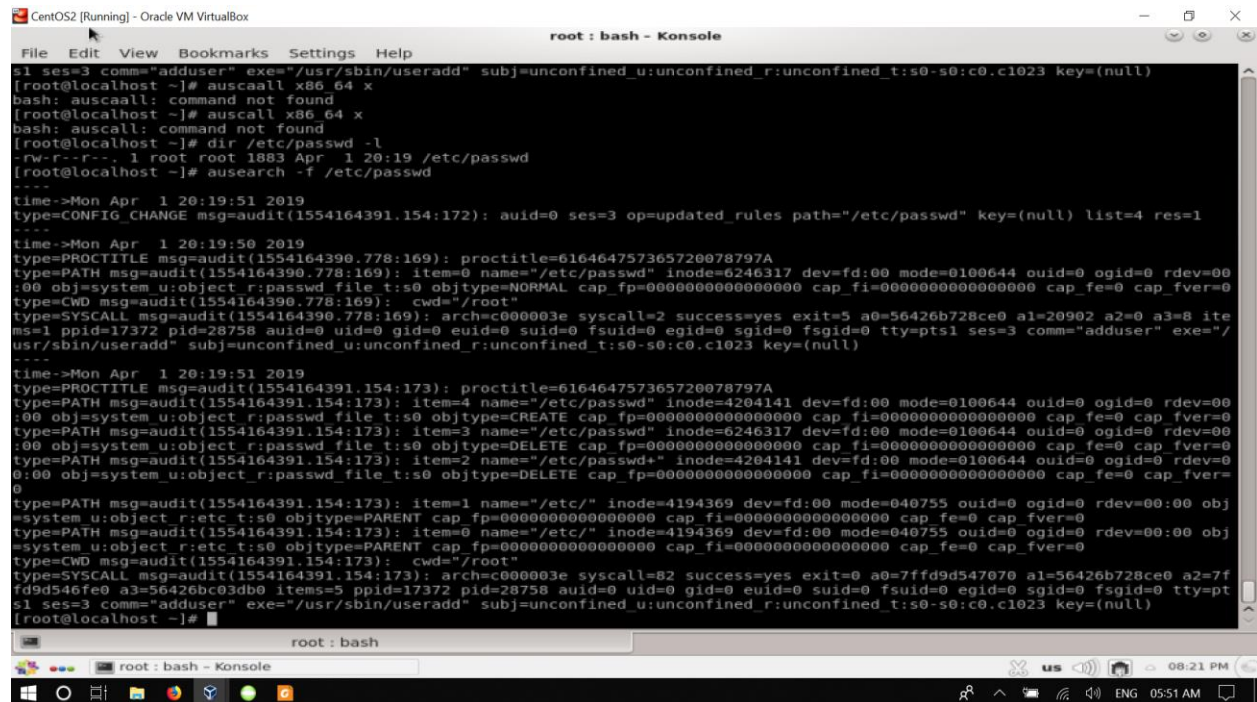
Q13

```
CentOS [Running] - Oracle VM VirtualBox
root : bash - Konsole

File Edit View Bookmarks Settings Help

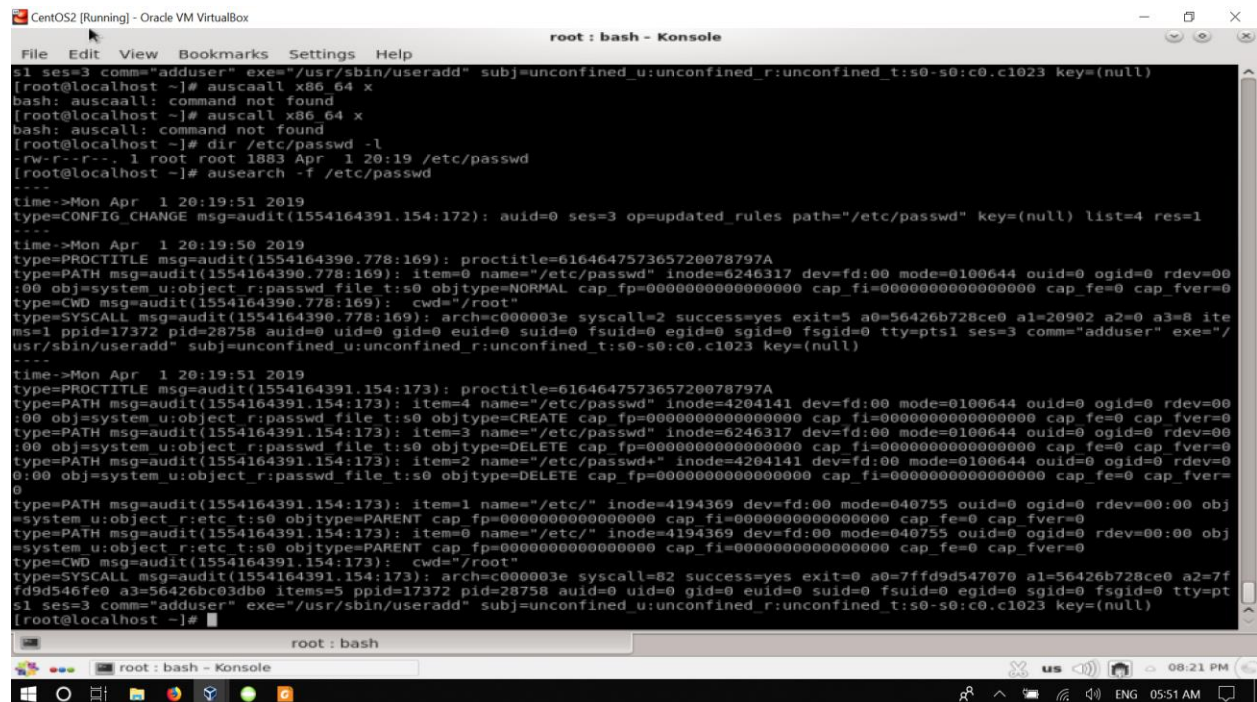
[root@localhost ~]# adduser xyz
[root@localhost ~]# ausearch -f /etc/passwd
----
time->Mon Apr 1 20:19:51 2019
type=CONFIG_CHANGE msg=audit(1554164391.154:172): auid=0 ses=3 op=updated_rules path="/etc/passwd" key=(null) list=4 res=1
----
time->Mon Apr 1 20:19:50 2019
type=PROCTITLE msg=audit(1554164390.778:169): proctitle=616464757365720078797A
type=PATH msg=audit(1554164391.154:173): item=4 name="/etc/passwd" inode=6246317 dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00
:00 obj=system_u:object_r:passwd_file_t:s0 objtype=CREATE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=CWD msg=audit(1554164390.778:169): cwd="/root"
type=SYSCALL msg=audit(1554164390.778:169): arch=c000003e syscall=2 success=yes exit=5 a0=56426b728ce0 a1=20902 a2=0 a3=8 ite
ms=1 ppid=17372 pid=28758 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts1 ses=3 comm="adduser" exe="/
usr/sbin/useradd" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=(null)
----
time->Mon Apr 1 20:19:51 2019
type=PROCTITLE msg=audit(1554164391.154:173): proctitle=616464757365720078797A
type=PATH msg=audit(1554164391.154:173): item=4 name="/etc/passwd" inode=4204141 dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00
:00 obj=system_u:object_r:passwd_file_t:s0 objtype=CREATE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=PATH msg=audit(1554164391.154:173): item=3 name="/etc/passwd" inode=6246317 dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00
:00 obj=system_u:object_r:passwd_file_t:s0 objtype=DELETE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=PATH msg=audit(1554164391.154:173): item=2 name="/etc/passwd" inode=4204141 dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00
:00 obj=system_u:object_r:passwd_file_t:s0 objtype=DELETE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=PATH msg=audit(1554164391.154:173): item=1 name="/etc/" inode=4194369 dev=fd:00 mode=040755 ouid=0 ogid=0 rdev=00:00 obj
=system_u:object_r:etc_t:s0 objtype=PARENT cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=PATH msg=audit(1554164391.154:173): item=0 name="/etc/" inode=4194369 dev=fd:00 mode=040755 ouid=0 ogid=0 rdev=00:00 obj
=system_u:object_r:etc_t:s0 objtype=PARENT cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=CWD msg=audit(1554164391.154:173): cwd="/root"
type=SYSCALL msg=audit(1554164391.154:173): arch=c000003e syscall=82 success=yes exit=0 a0=7ffd9d547070 a1=56426b728ce0 a2=7f
fd9d546fe0 a3=56426bc03db0 items=5 ppid=17372 pid=28758 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pt
s1 ses=3 comm="adduser" exe="/usr/sbin/useradd" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=(null)
[root@localhost ~]# auscaall x86_64 x
bash: auscaall: command not found
[root@localhost ~]# auscall x86_64 x
bash: auscall: command not found
[root@localhost ~]# dir /etc/passwd -l
-rw-r--r--. 1 root root 1883 Apr 1 20:19 /etc/passwd
[root@localhost ~]#
```


Q14



```
CentOS2 [Running] - Oracle VM VirtualBox
root : bash - Konsole
File Edit View Bookmarks Settings Help
s1 ses=3 comm='adduser' exe='/usr/sbin/useradd' subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=(null)
[root@localhost ~]# auscaall x86 64 x
bash: auscaall: command not found
[root@localhost ~]# auscall x86 64 x
bash: auscall: command not found
[root@localhost ~]# dir /etc/passwd -l
-rw-r--r-- 1 root root 1883 Apr 1 20:19 /etc/passwd
[root@localhost ~]# ausearch -f /etc/passwd
----
time->Mon Apr 1 20:19:51 2019
type=CONFIG_CHANGE msg=audit(1554164391.154:172): auid=0 ses=3 op=updated_rules path="/etc/passwd" key=(null) list=4 res=1
----
time->Mon Apr 1 20:19:50 2019
type=PROCTITLE msg=audit(1554164390.778:169): proctitle=616464757365720078797A
type=PATH msg=audit(1554164390.778:169): item=0 name="/etc/passwd" inode=6246317 dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00
:00 obj=system u:object r:passwd file t:s0 objtype=NORMAL cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=CWD msg=audit(1554164390.778:169): cwd="/root"
type=SYSCALL msg=audit(1554164390.778:169): arch=c000003e syscall=2 success=yes exit=5 a0=56426b728ce0 a1=20902 a2=0 a3=8 ite
ms=1 ppid=17372 pid=28758 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts1 ses=3 comm="adduser" exe="/
usr/sbin/useradd" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=(null)
----
time->Mon Apr 1 20:19:51 2019
type=PROCTITLE msg=audit(1554164391.154:173): proctitle=616464757365720078797A
type=PATH msg=audit(1554164391.154:173): item=4 name="/etc/passwd" inode=4204141 dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00
:00 obj=system u:object r:passwd file t:s0 objtype=CREATE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=PATH msg=audit(1554164391.154:173): item=3 name="/etc/passwd" inode=6246317 dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00
:00 obj=system u:object r:passwd file t:s0 objtype=DELETE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=PATH msg=audit(1554164391.154:173): item=2 name="/etc/passwd+" inode=4204141 dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00
:00 obj=system u:object r:passwd file t:s0 objtype=DELETE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=PATH msg=audit(1554164391.154:173): item=1 name="/etc/" inode=4194369 dev=fd:00 mode=040755 ouid=0 ogid=0 rdev=00:00 obj
=system u:object r:etc t:s0 objtype=PARENT cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=PATH msg=audit(1554164391.154:173): item=0 name="/etc/" inode=4194369 dev=fd:00 mode=040755 ouid=0 ogid=0 rdev=00:00 obj
=system u:object r:etc t:s0 objtype=PARENT cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=CWD msg=audit(1554164391.154:173): cwd="/root"
type=SYSCALL msg=audit(1554164391.154:173): arch=c000003e syscall=82 success=yes exit=0 a0=7ffd9d547070 a1=56426b728ce0 a2=7f
fd9d546fe0 a3=56426bc03db0 items=5 ppid=17372 pid=28758 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pt
s1 ses=3 comm="adduser" exe="/usr/sbin/useradd" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=(null)
[root@localhost ~]#
```

Q15



```
CentOS2 [Running] - Oracle VM VirtualBox
root : bash - Konsole
File Edit View Bookmarks Settings Help
s1 ses=3 comm='adduser' exe='/usr/sbin/useradd' subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=(null)
[root@localhost ~]# auscaall x86 64 x
bash: auscaall: command not found
[root@localhost ~]# auscall x86 64 x
bash: auscall: command not found
[root@localhost ~]# dir /etc/passwd -l
-rw-r--r-- 1 root root 1883 Apr 1 20:19 /etc/passwd
[root@localhost ~]# ausearch -f /etc/passwd
----
time->Mon Apr 1 20:19:51 2019
type=CONFIG_CHANGE msg=audit(1554164391.154:172): auid=0 ses=3 op=updated_rules path="/etc/passwd" key=(null) list=4 res=1
----
time->Mon Apr 1 20:19:50 2019
type=PROCTITLE msg=audit(1554164390.778:169): proctitle=616464757365720078797A
type=PATH msg=audit(1554164390.778:169): item=0 name="/etc/passwd" inode=6246317 dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00
:00 obj=system u:object r:passwd file t:s0 objtype=NORMAL cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=CWD msg=audit(1554164390.778:169): cwd="/root"
type=SYSCALL msg=audit(1554164390.778:169): arch=c000003e syscall=2 success=yes exit=5 a0=56426b728ce0 a1=20902 a2=0 a3=8 ite
ms=1 ppid=17372 pid=28758 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts1 ses=3 comm="adduser" exe="/
usr/sbin/useradd" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=(null)
----
time->Mon Apr 1 20:19:51 2019
type=PROCTITLE msg=audit(1554164391.154:173): proctitle=616464757365720078797A
type=PATH msg=audit(1554164391.154:173): item=4 name="/etc/passwd" inode=4204141 dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00
:00 obj=system u:object r:passwd file t:s0 objtype=CREATE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=PATH msg=audit(1554164391.154:173): item=3 name="/etc/passwd" inode=6246317 dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00
:00 obj=system u:object r:passwd file t:s0 objtype=DELETE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=PATH msg=audit(1554164391.154:173): item=2 name="/etc/passwd+" inode=4204141 dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00
:00 obj=system u:object r:passwd file t:s0 objtype=DELETE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=PATH msg=audit(1554164391.154:173): item=1 name="/etc/" inode=4194369 dev=fd:00 mode=040755 ouid=0 ogid=0 rdev=00:00 obj
=system u:object r:etc t:s0 objtype=PARENT cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=PATH msg=audit(1554164391.154:173): item=0 name="/etc/" inode=4194369 dev=fd:00 mode=040755 ouid=0 ogid=0 rdev=00:00 obj
=system u:object r:etc t:s0 objtype=PARENT cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=CWD msg=audit(1554164391.154:173): cwd="/root"
type=SYSCALL msg=audit(1554164391.154:173): arch=c000003e syscall=82 success=yes exit=0 a0=7ffd9d547070 a1=56426b728ce0 a2=7f
fd9d546fe0 a3=56426bc03db0 items=5 ppid=17372 pid=28758 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pt
s1 ses=3 comm="adduser" exe="/usr/sbin/useradd" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=(null)
[root@localhost ~]#
```

Q16 AND Q 17

```
root@localhost ~]# cd /etc
root@localhost etc]# chmod 640 passwd
root@localhost etc]# dir /etc/passwd -l
-rw-r-----. 1 root root 926 Mar 27 16:49 /etc/passwd
root@localhost etc]#
```

Q18

```
root@localhost ~]# ausearch -f /etc/passwd
----
time->Mon Apr 1 20:19:51 2019
type=CONFIG_CHANGE msg=audit(1554164391.154:172): auid=0 ses=3 op=updated_rules path="/etc/passwd" key=(null) list=4 res=1
----
time->Mon Apr 1 20:19:50 2019
type=PROCTITLE msg=audit(1554164390.778:169): proctitle=616464757365720078797A
type=PATH msg=audit(1554164390.778:169): item=0 name="/etc/passwd" inode=6246317 dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00
:00 obj=system_u:object_r:passwd_file_t:s0 objtype=NORMAL cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=CWD msg=audit(1554164390.778:169): cwd="/root"
type=SYSCALL msg=audit(1554164390.778:169): arch=c000003e syscall=2 success=yes exit=5 a0=56426b728ce0 a1=20902 a2=0 a3=8 ite
ms=1 ppid=17372 pid=28758 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts1 ses=3 comm="adduser" exe="/
usr/sbin/useradd" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=(null)
----
time->Mon Apr 1 20:19:51 2019
type=PROCTITLE msg=audit(1554164391.154:173): proctitle=616464757365720078797A
type=PATH msg=audit(1554164391.154:173): item=4 name="/etc/passwd" inode=4204141 dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00
:00 obj=system_u:object_r:passwd_file_t:s0 objtype=CREATE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=PATH msg=audit(1554164391.154:173): item=3 name="/etc/passwd" inode=6246317 dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00
:00 obj=system_u:object_r:passwd_file_t:s0 objtype=DELETE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=PATH msg=audit(1554164391.154:173): item=2 name="/etc/passwd" inode=4204141 dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00
:00 obj=system_u:object_r:passwd_file_t:s0 objtype=DELETE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=PATH msg=audit(1554164391.154:173): item=1 name="/etc/" inode=4194369 dev=fd:00 mode=040755 ouid=0 ogid=0 rdev=00:00 obj
=system_u:object_r:etc_t:s0 objtype=PARENT cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=PATH msg=audit(1554164391.154:173): item=0 name="/etc/" inode=4194369 dev=fd:00 mode=040755 ouid=0 ogid=0 rdev=00:00 obj
=system_u:object_r:etc_t:s0 objtype=PARENT cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=CWD msg=audit(1554164391.154:173): cwd="/root"
type=SYSCALL msg=audit(1554164391.154:173): arch=c000003e syscall=82 success=yes exit=0 a0=7fffd9d547070 a1=56426b728ce0 a2=7f
fd9d546fe0 a3=56426bc03d00 items=5 ppid=17372 pid=28758 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pt
s1 ses=3 comm="adduser" exe="/usr/sbin/useradd" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=(null)
root@localhost ~]#
```

Q19 VALUE IS IN THE SNAP SHOT "adduser" exe="/usr/sbin/useradd"

```
CentOS7 [Running] - Oracle VM VirtualBox
root : bash - Konsole

File Edit View Bookmarks Settings Help
s1 ses=3 comm="adduser" exe="/usr/sbin/useradd" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=(null)
[root@localhost ~]# auscaall x86_64 x
bash: auscaall: command not found
[root@localhost ~]# auscall x86_64 x
bash: auscall: command not found
[root@localhost ~]# dir /etc/passwd -l
-rw-r-----. 1 root root 1883 Apr 1 20:19 /etc/passwd
[root@localhost ~]# ausearch -f /etc/passwd
----
time->Mon Apr 1 20:19:51 2019
type=CONFIG_CHANGE msg=audit(1554164391.154:172): auid=0 ses=3 op=updated_rules path="/etc/passwd" key=(null) list=4 res=1
----
time->Mon Apr 1 20:19:50 2019
type=PROCTITLE msg=audit(1554164390.778:169): proctitle=616464757365720078797A
type=PATH msg=audit(1554164390.778:169): item=0 name="/etc/passwd" inode=6246317 dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00
:00 obj=system_u:object_r:passwd_file_t:s0 objtype=NORMAL cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=CWD msg=audit(1554164390.778:169): cwd="/root"
type=SYSCALL msg=audit(1554164390.778:169): arch=c000003e syscall=2 success=yes exit=5 a0=56426b728ce0 a1=20902 a2=0 a3=8 ite
ms=1 ppid=17372 pid=28758 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts1 ses=3 comm="adduser" exe="/
usr/sbin/useradd" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=(null)
----
time->Mon Apr 1 20:19:51 2019
type=PROCTITLE msg=audit(1554164391.154:173): proctitle=616464757365720078797A
type=PATH msg=audit(1554164391.154:173): item=4 name="/etc/passwd" inode=4204141 dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00
:00 obj=system_u:object_r:passwd_file_t:s0 objtype=CREATE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=PATH msg=audit(1554164391.154:173): item=3 name="/etc/passwd" inode=6246317 dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00
:00 obj=system_u:object_r:passwd_file_t:s0 objtype=DELETE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=PATH msg=audit(1554164391.154:173): item=2 name="/etc/passwd" inode=4204141 dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00
:00 obj=system_u:object_r:passwd_file_t:s0 objtype=DELETE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=PATH msg=audit(1554164391.154:173): item=1 name="/etc/" inode=4194369 dev=fd:00 mode=040755 ouid=0 ogid=0 rdev=00:00 obj
=system_u:object_r:etc_t:s0 objtype=PARENT cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=PATH msg=audit(1554164391.154:173): item=0 name="/etc/" inode=4194369 dev=fd:00 mode=040755 ouid=0 ogid=0 rdev=00:00 obj
=system_u:object_r:etc_t:s0 objtype=PARENT cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=CWD msg=audit(1554164391.154:173): cwd="/root"
type=SYSCALL msg=audit(1554164391.154:173): arch=c000003e syscall=82 success=yes exit=0 a0=7fffd9d547070 a1=56426b728ce0 a2=7f
fd9d546fe0 a3=56426bc03d00 items=5 ppid=17372 pid=28758 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pt
s1 ses=3 comm="adduser" exe="/usr/sbin/useradd" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=(null)
root@localhost ~]#
```


Q20

```
CentOS2 [Running] - Oracle VM VirtualBox
root : bash - Konsole

File Edit View Bookmarks Settings Help

time->Mon Apr 1 20:19:51 2019
type=CONFIG_CHANGE msg=audit(1554164391.154:172): auid=0 ses=3 op=updated_rules path="/etc/passwd" key=(null) list=4 res=1
----
time->Mon Apr 1 20:19:50 2019
type=PROCTITLE msg=audit(1554164390.778:169): proctitle=616464757365720078797A
type=PATH msg=audit(1554164390.778:169): item=0 name="/etc/passwd" inode=6246317 dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00
:00 obj=system_u:object_r:passwd_file_t:s0 objtype=NORMAL cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=CWD msg=audit(1554164390.778:169): : cwd="/root"
type=SYSCALL msg=audit(1554164390.778:169): arch=c000003e syscall=2 success=yes exit=5 a0=56426b728ce0 a1=20902 a2=0 a3=8 ite
ms=1 ppid=17372 pid=28758 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts1 ses=3 comm="adduser" exe="/
usr/sbin/useradd" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=(null)
----
time->Mon Apr 1 20:19:51 2019
type=PROCTITLE msg=audit(1554164391.154:173): proctitle=616464757365720078797A
type=PATH msg=audit(1554164391.154:173): item=4 name="/etc/passwd" inode=4204141 dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00
:00 obj=system_u:object_r:passwd_file_t:s0 objtype=CREATE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=PATH msg=audit(1554164391.154:173): item=3 name="/etc/passwd" inode=6246317 dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00
:00 obj=system_u:object_r:passwd_file_t:s0 objtype=DELETE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=PATH msg=audit(1554164391.154:173): item=2 name="/etc/passwd" inode=4204141 dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=0
0:00 obj=system_u:object_r:passwd_file_t:s0 objtype=DELETE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=
0
type=PATH msg=audit(1554164391.154:173): item=1 name="/etc/" inode=4194369 dev=fd:00 mode=040755 ouid=0 ogid=0 rdev=00:00 obj
=system_u:object_r:etc_t:s0 objtype=PARENT cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=PATH msg=audit(1554164391.154:173): item=0 name="/etc/" inode=4194369 dev=fd:00 mode=040755 ouid=0 ogid=0 rdev=00:00 obj
=system_u:object_r:etc_t:s0 objtype=PARENT cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=CWD msg=audit(1554164391.154:173): : cwd="/root"
type=SYSCALL msg=audit(1554164391.154:173): arch=c000003e syscall=82 success=yes exit=0 a0=7ffd9d547070 a1=56426b728ce0 a2=7f
fd9d546fe0 a3=56426bc03db0 items=5 ppid=17372 pid=28758 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pt
s1 ses=3 comm="adduser" exe="/usr/sbin/useradd" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=(null)
[root@localhost ~]# ausearch -f /etc/passwd | aureport -f -i

File Report
# date time file syscall success exe auid event
1. 04/01/2019 20:19:51 /etc/passwd ? yes ? root 172
2. 04/01/2019 20:19:50 /etc/passwd open yes /usr/sbin/useradd root 169
3. 04/01/2019 20:19:51 /etc/passwd rename yes /usr/sbin/useradd root 173
[root@localhost ~]#
```

Q21

```
CentOS2 [Running] - Oracle VM VirtualBox
root : bash - Konsole

File Edit View Bookmarks Settings Help

type=PATH msg=audit(1554164391.154:173): item=3 name="/etc/passwd" inode=6246317 dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00
:00 obj=system_u:object_r:passwd_file_t:s0 objtype=DELETE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=PATH msg=audit(1554164391.154:173): item=2 name="/etc/passwd" inode=4204141 dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=0
0:00 obj=system_u:object_r:passwd_file_t:s0 objtype=DELETE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=
0
type=PATH msg=audit(1554164391.154:173): item=1 name="/etc/" inode=4194369 dev=fd:00 mode=040755 ouid=0 ogid=0 rdev=00:00 obj
=system_u:object_r:etc_t:s0 objtype=PARENT cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=PATH msg=audit(1554164391.154:173): item=0 name="/etc/" inode=4194369 dev=fd:00 mode=040755 ouid=0 ogid=0 rdev=00:00 obj
=system_u:object_r:etc_t:s0 objtype=PARENT cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=CWD msg=audit(1554164391.154:173): : cwd="/root"
type=SYSCALL msg=audit(1554164391.154:173): arch=c000003e syscall=82 success=yes exit=0 a0=7ffd9d547070 a1=56426b728ce0 a2=7f
fd9d546fe0 a3=56426bc03db0 items=5 ppid=17372 pid=28758 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pt
s1 ses=3 comm="adduser" exe="/usr/sbin/useradd" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=(null)
[root@localhost ~]# ausearch -f /etc/passwd | aureport -f -i

File Report
# date time file syscall success exe auid event
1. 04/01/2019 20:19:51 /etc/passwd ? yes ? root 172
2. 04/01/2019 20:19:50 /etc/passwd open yes /usr/sbin/useradd root 169
3. 04/01/2019 20:19:51 /etc/passwd rename yes /usr/sbin/useradd root 173
[root@localhost ~]# ausearch -m LOGIN --start today -i
----
type=LOGIN msg=audit(04/01/2019 20:00:02.575:101): pid=9928 uid=root subj=system_u:system_r:crond_t:s0-s0:c0.c1023 old-auid=
unset auid=root tty=(none) old-ses=4294967295 ses=1 res=yes
----
type=LOGIN msg=audit(04/01/2019 20:03:24.157:119): pid=12916 uid=root subj=system_u:system_r:crond_t:s0-s0:c0.c1023 old-auid
=unset auid=root tty=(none) old-ses=4294967295 ses=2 res=yes
----
type=LOGIN msg=audit(04/01/2019 20:04:39.028:151): pid=13244 uid=root subj=system_u:system_r:xdm_t:s0-s0:c0.c1023 old-auid=u
nset auid=root tty=(none) old-ses=4294967295 ses=3 res=yes
----
type=LOGIN msg=audit(04/01/2019 20:10:01.538:161): pid=3846 uid=root subj=system_u:system_r:crond_t:s0-s0:c0.c1023 old-auid=
unset auid=root tty=(none) old-ses=4294967295 ses=4 res=yes
----
type=LOGIN msg=audit(04/01/2019 20:20:01.833:177): pid=29864 uid=root subj=system_u:system_r:crond_t:s0-s0:c0.c1023 old-auid
=unset auid=root tty=(none) old-ses=4294967295 ses=5 res=yes
[root@localhost ~]#
```

Part 2: Introduction to Snort IDSs Rules:

Q1.1: The “→” symbol is used to indicate traffic from internal network to external network.

Q1.2: The “<- ->” symbol is used to indicate bidirectional traffic between internal and external networks.

Q1.3: The “<-” symbol is used to indicate traffic from external to internal networks.

Q2.1: All hosts in the internal network are: `Ipvar HOME_NET`

Q2.2: All hosts in the external network are: `Ipvar EXTERNAL_NET`

Q2.3: `Ipvar net100 [192.168.1.0/24, 10.1.1.0]` is the variable `net100` for the 192.168.1.0

Q2.4: `Ipvar clientA[192.168.0.1, 10.0.1.1]` is declared as `clientA` which has IP as 192.168.0.1 and 10.0.1.1

Q3.1: `Ipvar HTTP_SERVERS $HOME_NET` declares all web servers

Q3.2: `Ipvar SMTP_SERVERS $HOME_NET` declares all E-mail servers

Q3.3: `Ipvar DNS_SERVERS $HOME_NET` declares all DNS servers

Q3.4: `Ipvar SSH_SERVERS $HOME_NET` declares all secure shell servers

Q3.5: `Ipvar FTS_SERVERS $HOME_NET` declares all file servers

Q3.6: `Ipvar TELNET_SERVERS $HOME_NET` declares all IP telephony servers

Q4.1: `portvar HTTP_PORTS [80, 8080]` are port number web servers run on

Q4.2: `portvar SHELLCODE_PORTS !80` represents ports of SHELLCODE type

Q4.3: The lists of ports that you need to look for SSH connections are port 22 and 26

Q4.4: `portvar REGISTRATION_PORTS[0:1024]`

Q5.1: `alert tcp any any -> any 80 (content: !"GET";)`

Q5.2: `alert tcp EXTERNAL_NET any -> EXTERNAL_NET any (msg: "Backdoor signature was detected Subseven Trojan";content:`

`"0d0a5b52504c5d3030320d0a";reference:arachnids,485;)`

Q5.3: `log tcp !192.168.1.0/24 any → 192.168.1.0/24 23`