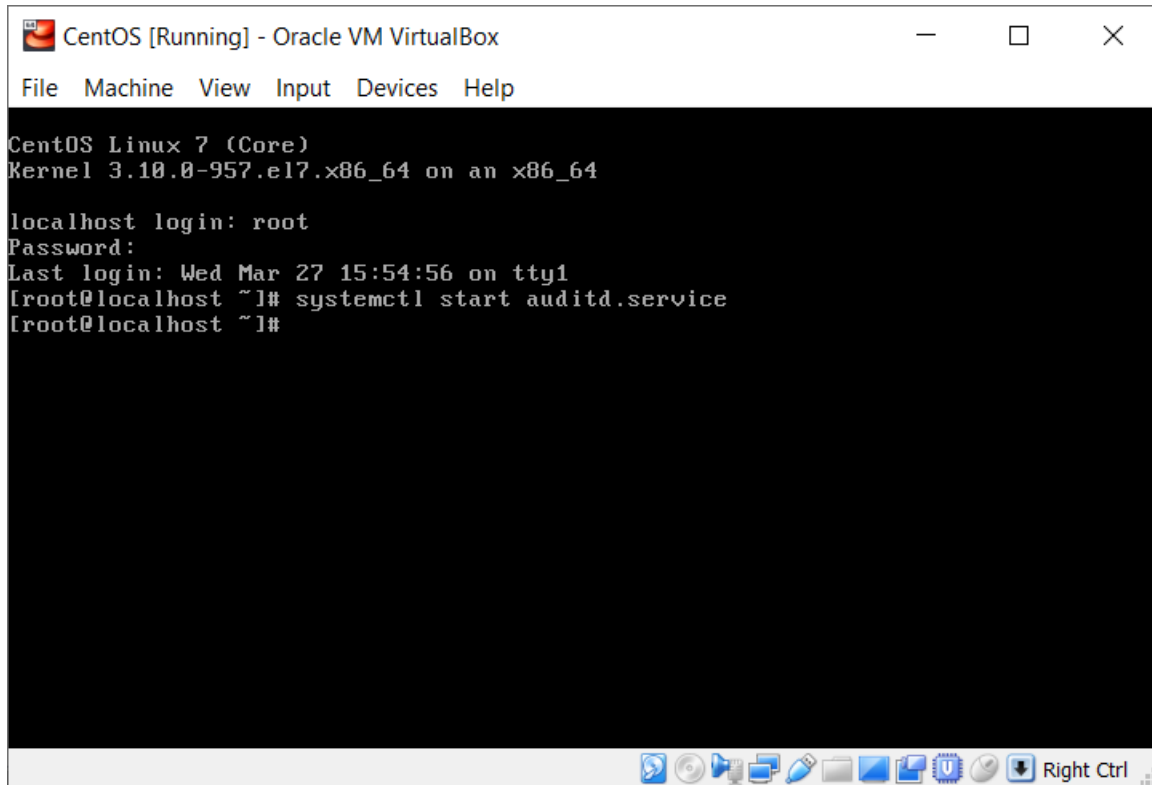


LAB 6 – Risk Management and Intrusion Detection Systems Folder

Name: Zamir Lalji
Professor: Khalil Abuosba
Due date: April 2nd, 2019
Student Number: 212779997

(Note: all screenshots for each question that required it)
Part 1: Introduction to Linux Operating Systems Auditing

Q4:

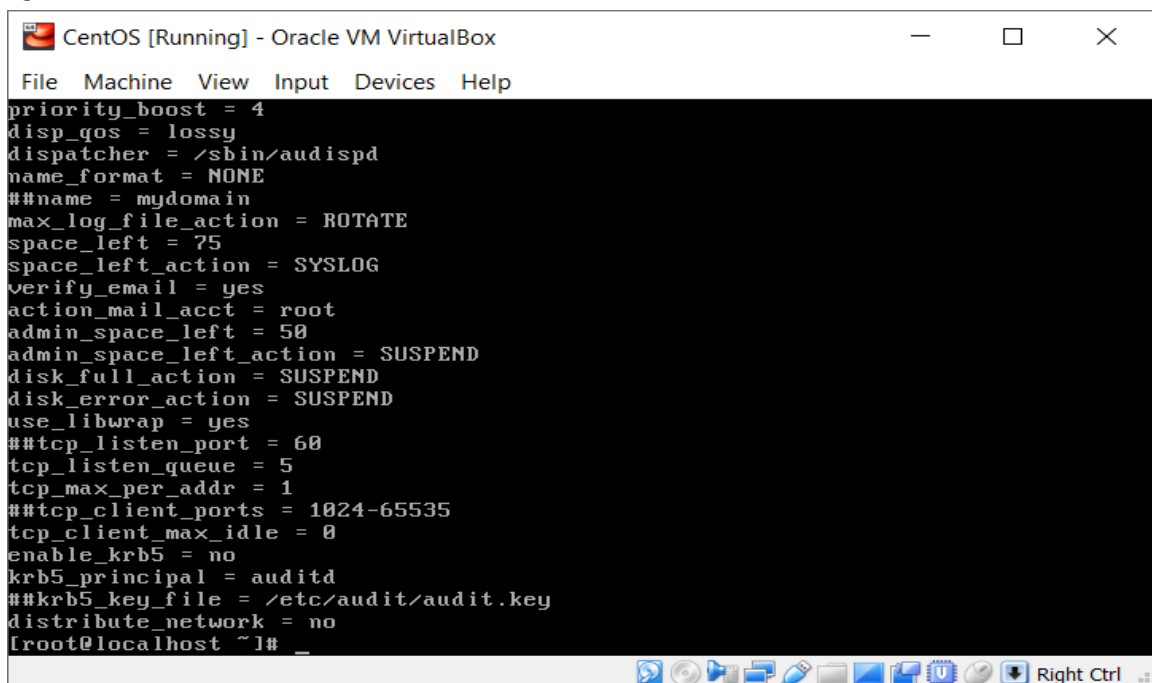


The screenshot shows a terminal window titled "CentOS [Running] - Oracle VM VirtualBox". The terminal output displays the CentOS Linux 7 (Core) kernel version 3.10.0-957.el7.x86_64. The user logs in as root and runs the command `systemctl start auditd.service`. The prompt returns to `[root@localhost ~]#`. The window includes a menu bar with "File", "Machine", "View", "Input", "Devices", and "Help", and a taskbar at the bottom with various icons and a "Right Ctrl" button.

```
CentOS Linux 7 (Core)
Kernel 3.10.0-957.el7.x86_64 on an x86_64

localhost login: root
Password:
Last login: Wed Mar 27 15:54:56 on tty1
[root@localhost ~]# systemctl start auditd.service
[root@localhost ~]#
```

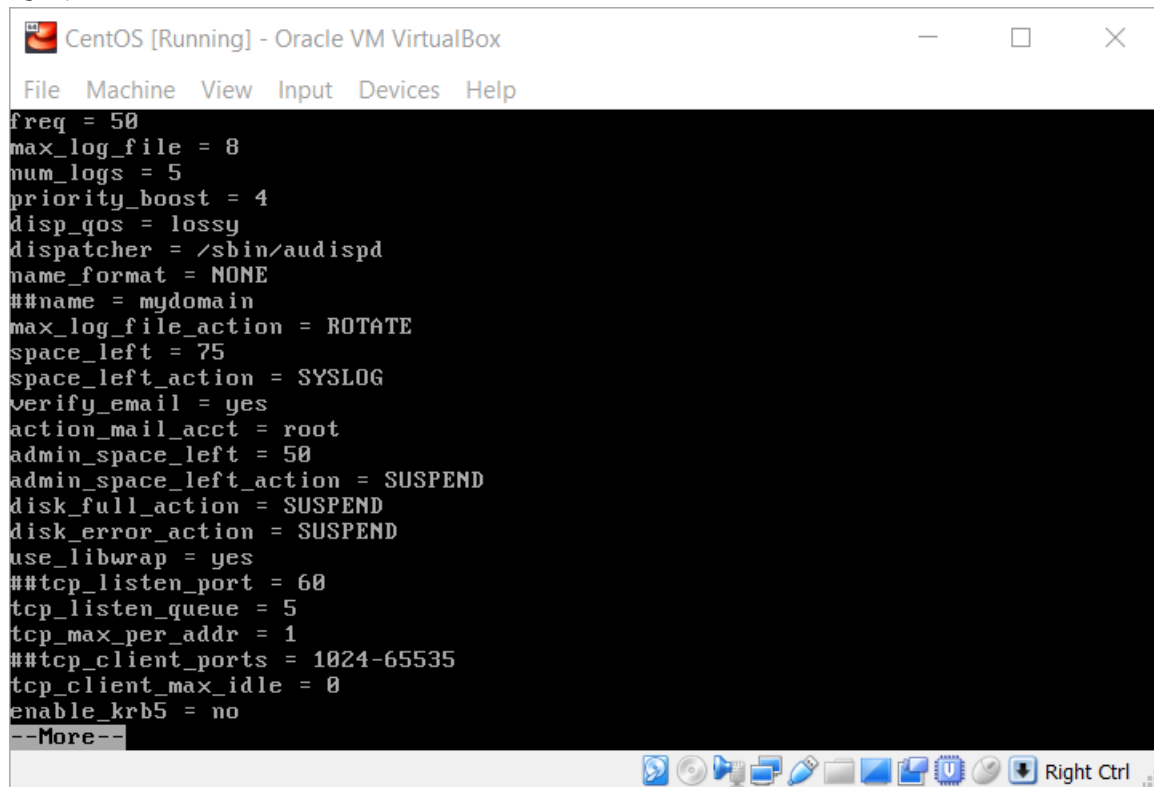
Q5i:



The screenshot shows a terminal window titled "CentOS [Running] - Oracle VM VirtualBox". The terminal output displays the contents of the `/etc/audit/auditd.conf` file. The configuration includes settings for log rotation, space management, email notifications, and network connections. The prompt returns to `[root@localhost ~]#`. The window includes a menu bar with "File", "Machine", "View", "Input", "Devices", and "Help", and a taskbar at the bottom with various icons and a "Right Ctrl" button.

```
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 ~]#
```

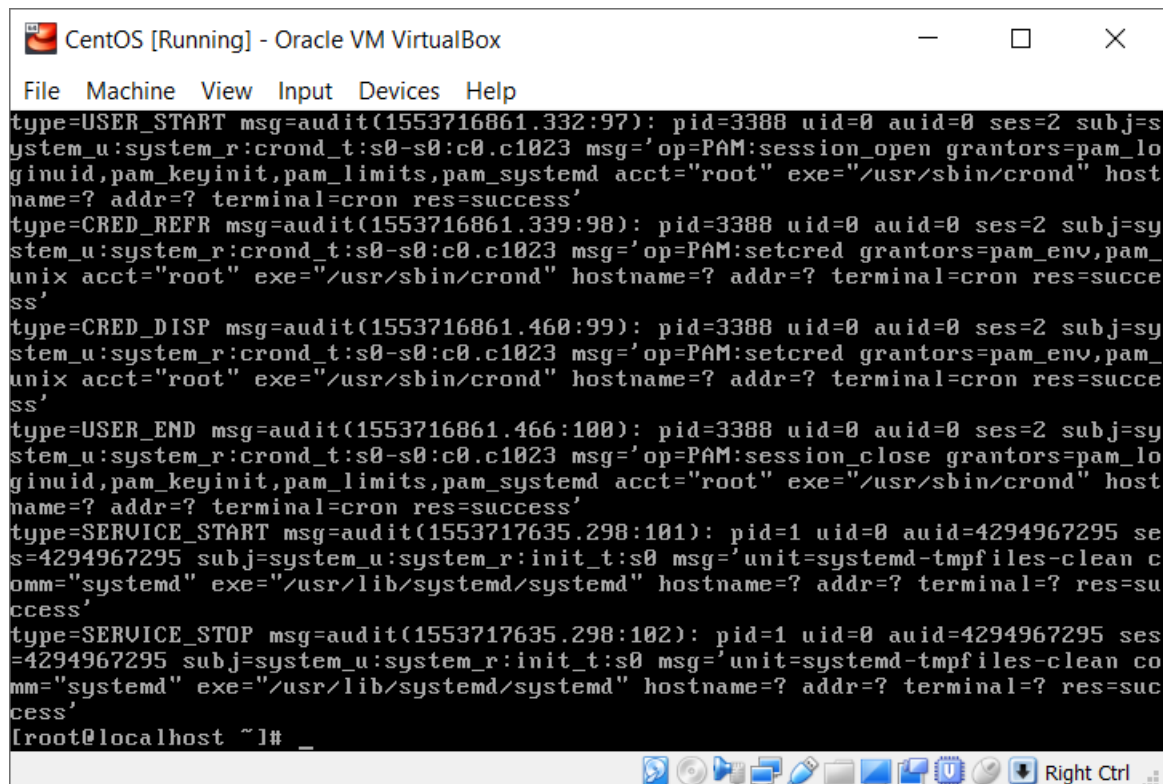
Q5ii)



The screenshot shows a terminal window titled "CentOS [Running] - Oracle VM VirtualBox". The terminal displays a list of system configuration parameters for a service, likely rsyslog, including log file settings, space management, email verification, and network ports. The parameters are listed in a key-value format. At the bottom of the terminal, there is a prompt "--More--" and a status bar with icons and the text "Right Ctrl".

```
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
--More--
```

Q6



The screenshot shows a terminal window titled "CentOS [Running] - Oracle VM VirtualBox". The terminal displays a series of audit logs. The first part shows a cron job execution for 'crond' with various attributes like pid, uid, auid, ses, subj, and exe. The second part shows a systemd service start and stop for 'systemd-tmpfiles-clean'. The logs are formatted as key-value pairs. At the bottom of the terminal, there is a prompt "[root@localhost ~]#" and a status bar with icons and the text "Right Ctrl".

```
type=USER_START msg=audit(1553716861.332:97): pid=3388 uid=0 auid=0 ses=2 subj=s
stem_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:session_open grantors=pam_lo
ginuid,pam_keyinit,pam_limits,pam_systemd acct="root" exe="/usr/sbin/crond" host
name=? addr=? terminal=cron res=success'
type=CRED_REFR msg=audit(1553716861.339:98): pid=3388 uid=0 auid=0 ses=2 subj=sy
stem_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=succ
ess'
type=CRED_DISP msg=audit(1553716861.460:99): pid=3388 uid=0 auid=0 ses=2 subj=sy
stem_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=succ
ess'
type=USER_END msg=audit(1553716861.466:100): pid=3388 uid=0 auid=0 ses=2 subj=sy
stem_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:session_close grantors=pam_lo
ginuid,pam_keyinit,pam_limits,pam_systemd acct="root" exe="/usr/sbin/crond" host
name=? addr=? terminal=cron res=success'
type=SERVICE_START msg=audit(1553717635.298:101): pid=1 uid=0 auid=4294967295 se
s=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=systemd-tmpfiles-clean c
omm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=su
ccess'
type=SERVICE_STOP msg=audit(1553717635.298:102): pid=1 uid=0 auid=4294967295 ses
=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=systemd-tmpfiles-clean co
mm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=suc
cess'
[root@localhost ~]#
```

Q7:

```
CentOS [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
-c 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
--More--
[2]+ Stopped auditctl : more
[root@localhost ~]#
```

Q8:

```
CentOS [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
-d <l,a> Field name, operator(=,!=), field name
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
--More--
[2]+ Stopped auditctl : more
[root@localhost ~]# auditctl -l
No rules
[root@localhost ~]#
```

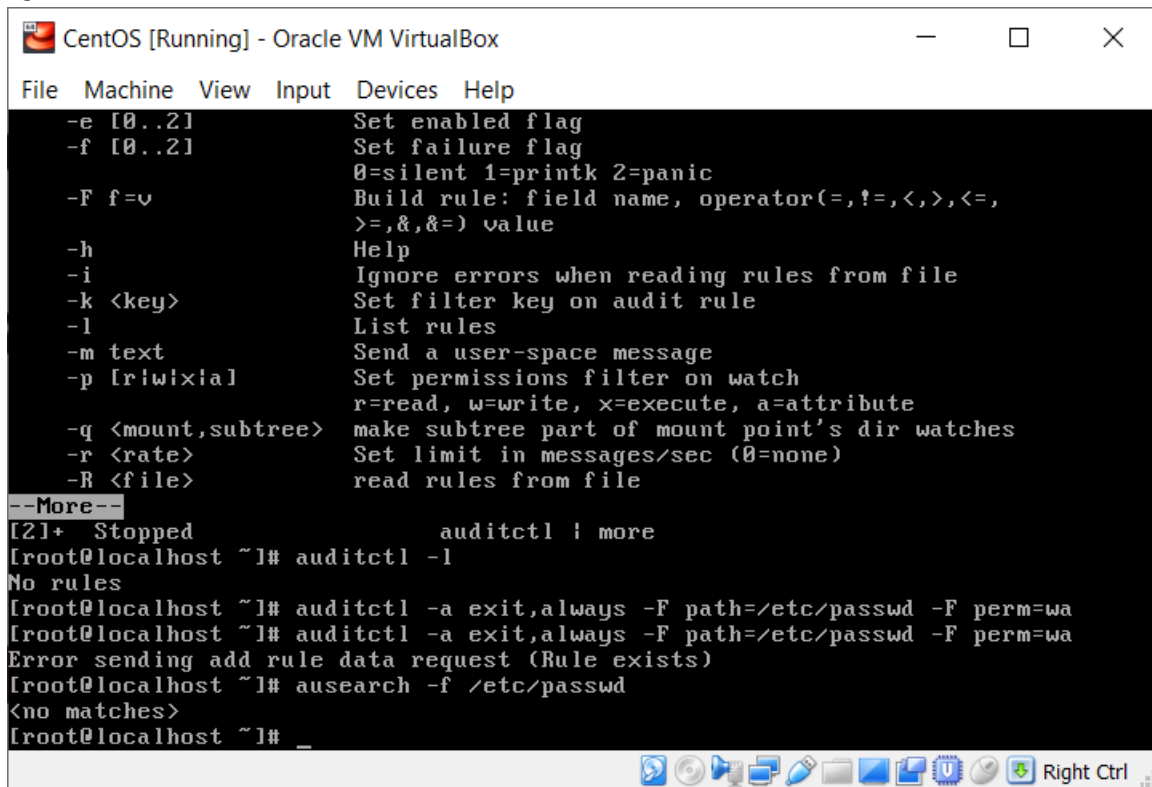
Q9:

```
CentOS [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
-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 [riwixal] 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
--More--
[2]+ Stopped auditctl : more
[root@localhost ~]# auditctl -l
No rules
[root@localhost ~]# auditctl -a exit,always -F path=/etc/passwd -F perm=wa
[root@localhost ~]
```

Q10:

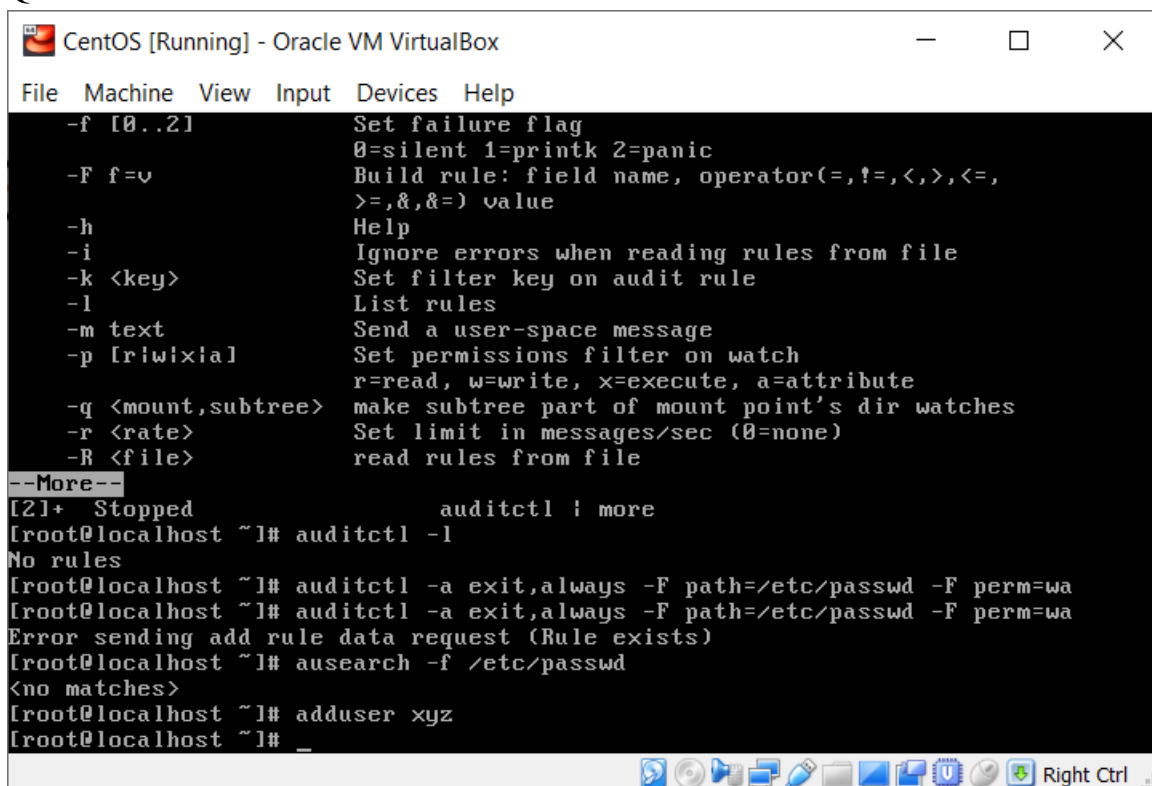
```
CentOS [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
a=never,always
-D Delete all rules and watches
-e [0..2] Set enabled flag
-f [0..2] Set failure flag
0=silent 1=printk 2=panic
-F f=v Build rule: field name, operator(=,!=,<,>,<=,
>=,&,&=) value
-h Help
-i Ignore errors when reading rules from file
-k <key> Set filter key on audit rule
-l List rules
-m text Send a user-space message
-p [riwixal] 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
--More--
[2]+ Stopped auditctl : more
[root@localhost ~]# auditctl -l
No rules
[root@localhost ~]# auditctl -a exit,always -F path=/etc/passwd -F perm=wa
[root@localhost ~]# auditctl -a exit,always -F path=/etc/passwd -F perm=wa
Error sending add rule data request (Rule exists)
[root@localhost ~]# _
```

Q11:



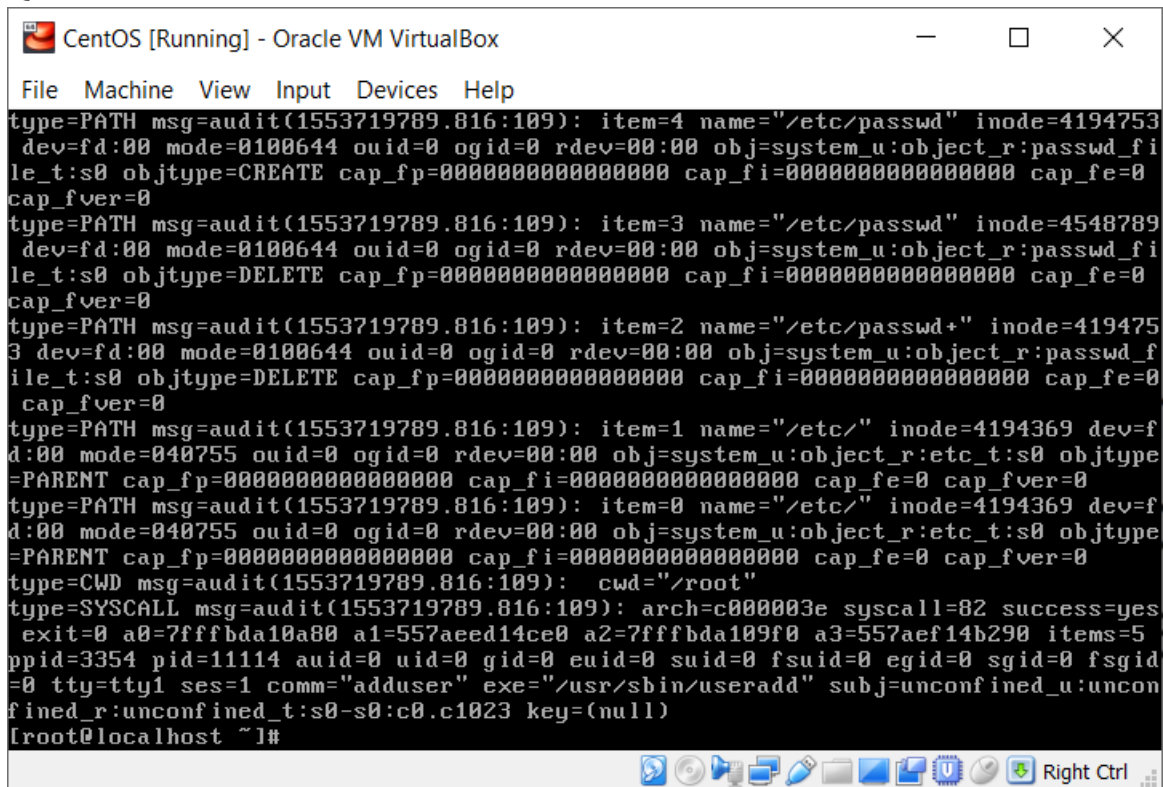
```
CentOS [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
-e [0..2] Set enabled flag
-f [0..2] Set failure flag
          0=silent 1=printk 2=panic
-F f=v Build rule: field name, operator(=,!=,<,>,<=,
          >=,&,&=) value
-h Help
-i Ignore errors when reading rules from file
-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
--More--
[2]+ Stopped auditctl i more
[root@localhost ~]# auditctl -l
No rules
[root@localhost ~]# auditctl -a exit,always -F path=/etc/passwd -F perm=wa
[root@localhost ~]# auditctl -a exit,always -F path=/etc/passwd -F perm=wa
Error sending add rule data request (Rule exists)
[root@localhost ~]# ausearch -f /etc/passwd
<no matches>
[root@localhost ~]# _
```

Q12:



```
CentOS [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
-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
--More--
[2]+ Stopped auditctl i more
[root@localhost ~]# auditctl -l
No rules
[root@localhost ~]# auditctl -a exit,always -F path=/etc/passwd -F perm=wa
[root@localhost ~]# auditctl -a exit,always -F path=/etc/passwd -F perm=wa
Error sending add rule data request (Rule exists)
[root@localhost ~]# ausearch -f /etc/passwd
<no matches>
[root@localhost ~]# adduser xyz
[root@localhost ~]# _
```

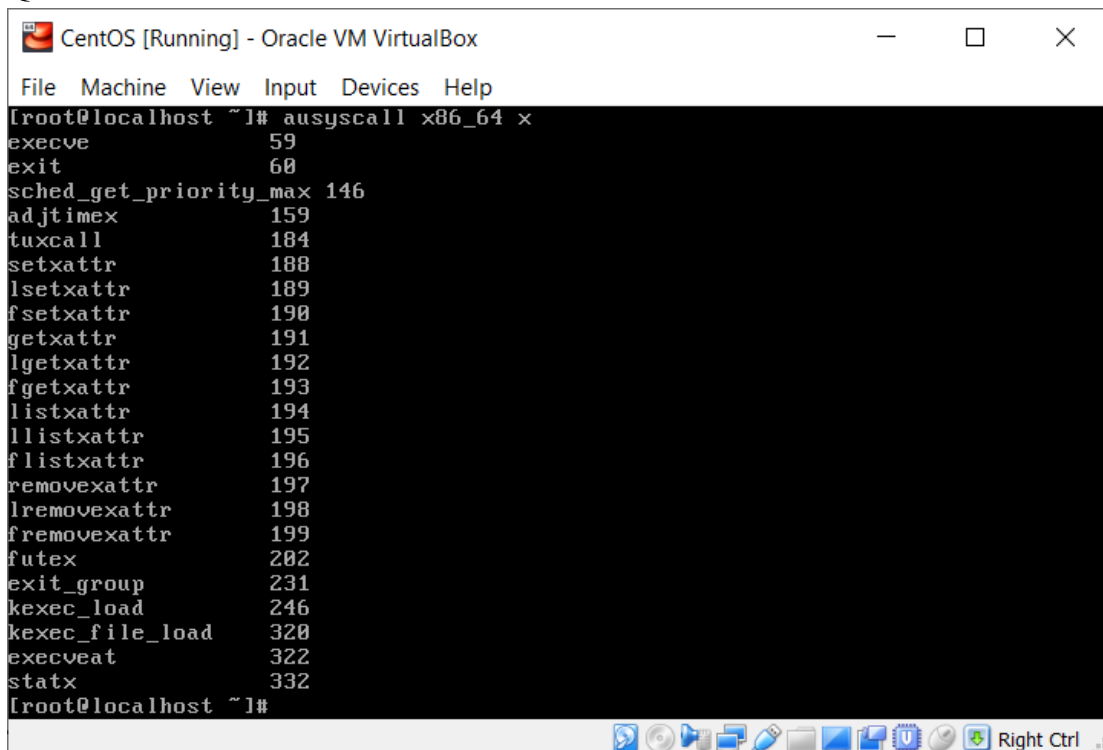
Q13:



The screenshot shows a terminal window titled "CentOS [Running] - Oracle VM VirtualBox". The terminal output displays a series of audit messages (msg=audit) for various system events. The messages include details such as item number, name, inode, device, mode, object ID, object type, and capabilities. The events shown are related to file operations on "/etc/passwd" and "/etc/". The terminal ends with the prompt "[root@localhost ~]#".

```
type=PATH msg=audit(1553719789.816:109): item=4 name="/etc/passwd" inode=4194753
dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:passwd_fi
le_t:s0 objtype=CREATE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0
cap_fver=0
type=PATH msg=audit(1553719789.816:109): item=3 name="/etc/passwd" inode=4548789
dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:passwd_fi
le_t:s0 objtype=DELETE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0
cap_fver=0
type=PATH msg=audit(1553719789.816:109): item=2 name="/etc/passwd+" inode=419475
3 dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:passwd_fi
le_t:s0 objtype=DELETE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0
cap_fver=0
type=PATH msg=audit(1553719789.816:109): item=1 name="/etc/" inode=4194369 dev=f
d: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(1553719789.816:109): item=0 name="/etc/" inode=4194369 dev=f
d: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(1553719789.816:109): cwd="/root"
type=SYSCALL msg=audit(1553719789.816:109): arch=c000003e syscall=82 success=yes
exit=0 a0=7ffffbda10a80 a1=557aeed14ce0 a2=7ffffbda109f0 a3=557aef14b290 items=5
ppid=3354 pid=1114 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid
=0 tty=tty1 ses=1 comm="adduser" exe="/usr/sbin/useradd" subj=unconfined_u:uncon
fined_r:unconfined_t:s0-s0:c0.c1023 key=(null)
[root@localhost ~]#
```

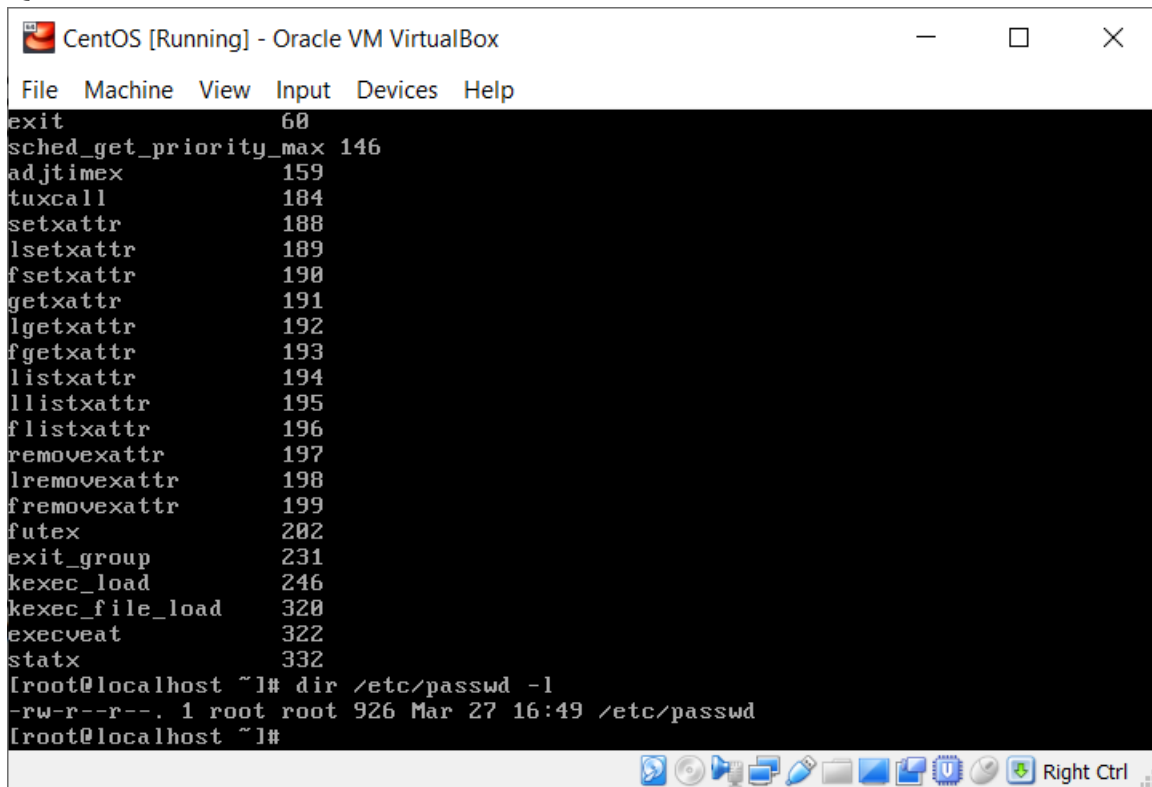
Q14:



The screenshot shows a terminal window titled "CentOS [Running] - Oracle VM VirtualBox". The terminal output displays the output of the command "ausyscall x86_64 x". The output is a list of system calls and their corresponding values. The terminal ends with the prompt "[root@localhost ~]#".

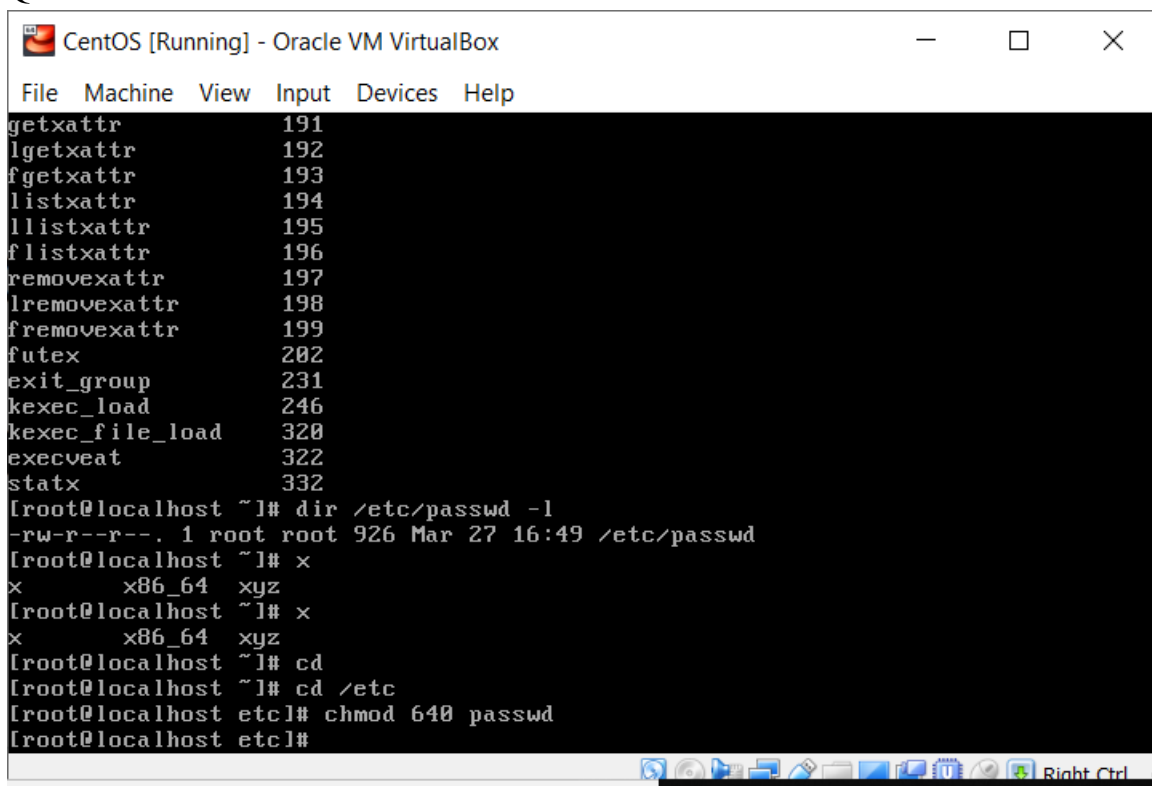
```
[root@localhost ~]# ausyscall x86_64 x
execve 59
exit 60
sched_get_priority_max 146
adjtimex 159
tuxcall 184
setxattr 188
lsetxattr 189
fsetxattr 190
getxattr 191
lgetxattr 192
fgetxattr 193
listxattr 194
llistxattr 195
flistxattr 196
removexattr 197
lremovexattr 198
fremovexattr 199
futex 202
exit_group 231
kexec_load 246
kexec_file_load 320
execveat 322
statx 332
[root@localhost ~]#
```

Q15:



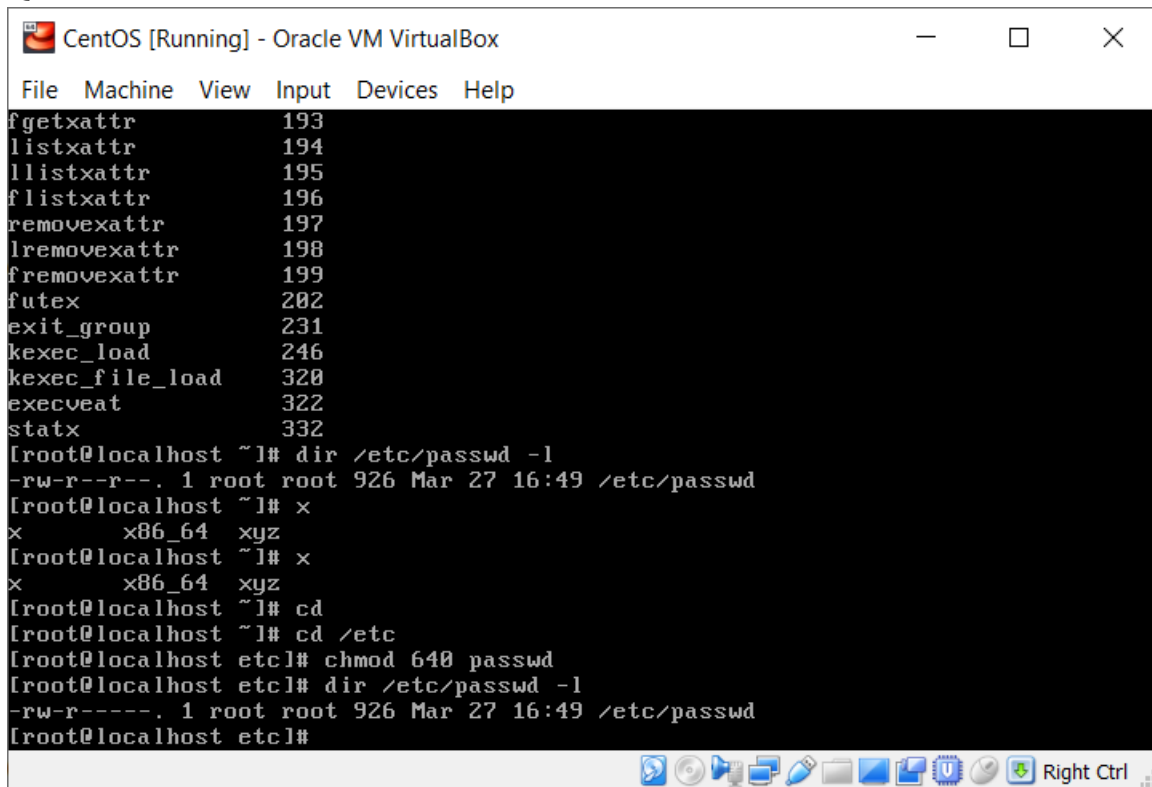
```
CentOS [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
exit 60
sched_get_priority_max 146
adjtimex 159
tuxcall 184
setxattr 188
lsetxattr 189
fsetxattr 190
getxattr 191
lgetxattr 192
fgetxattr 193
listxattr 194
llistxattr 195
flistxattr 196
removexattr 197
lremovexattr 198
fremovexattr 199
futex 202
exit_group 231
kexec_load 246
kexec_file_load 320
execveat 322
statx 332
[root@localhost ~]# dir /etc/passwd -l
-rw-r--r--. 1 root root 926 Mar 27 16:49 /etc/passwd
[root@localhost ~]#
```

Q16:



```
CentOS [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
getxattr 191
lgetxattr 192
fgetxattr 193
listxattr 194
llistxattr 195
flistxattr 196
removexattr 197
lremovexattr 198
fremovexattr 199
futex 202
exit_group 231
kexec_load 246
kexec_file_load 320
execveat 322
statx 332
[root@localhost ~]# dir /etc/passwd -l
-rw-r--r--. 1 root root 926 Mar 27 16:49 /etc/passwd
[root@localhost ~]# x
x      x86_64 xyz
[root@localhost ~]# x
x      x86_64 xyz
[root@localhost ~]# cd
[root@localhost ~]# cd /etc
[root@localhost etc]# chmod 640 passwd
[root@localhost etc]#
```


Q17:



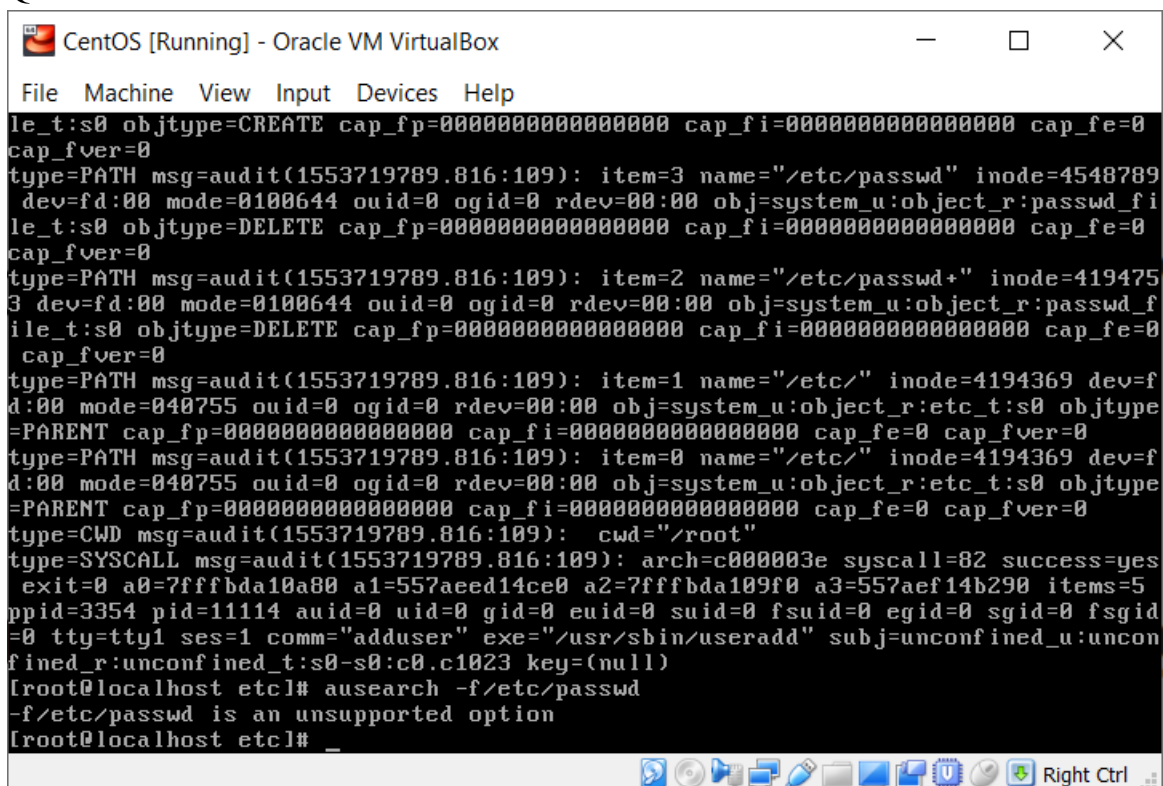
CentOS [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
fgetxattr      193
listxattr      194
llistxattr     195
flistxattr     196
removexattr    197
lremovexattr   198
fremovexattr   199
futex          202
exit_group     231
kexec_load     246
kexec_file_load 320
execveat       322
statx          332
[root@localhost ~]# dir /etc/passwd -l
-rw-r--r--. 1 root root 926 Mar 27 16:49 /etc/passwd
[root@localhost ~]# x
x      x86_64 xyz
[root@localhost ~]# x
x      x86_64 xyz
[root@localhost ~]# cd
[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]#
```

Right Ctrl

Q18:



CentOS [Running] - Oracle VM VirtualBox

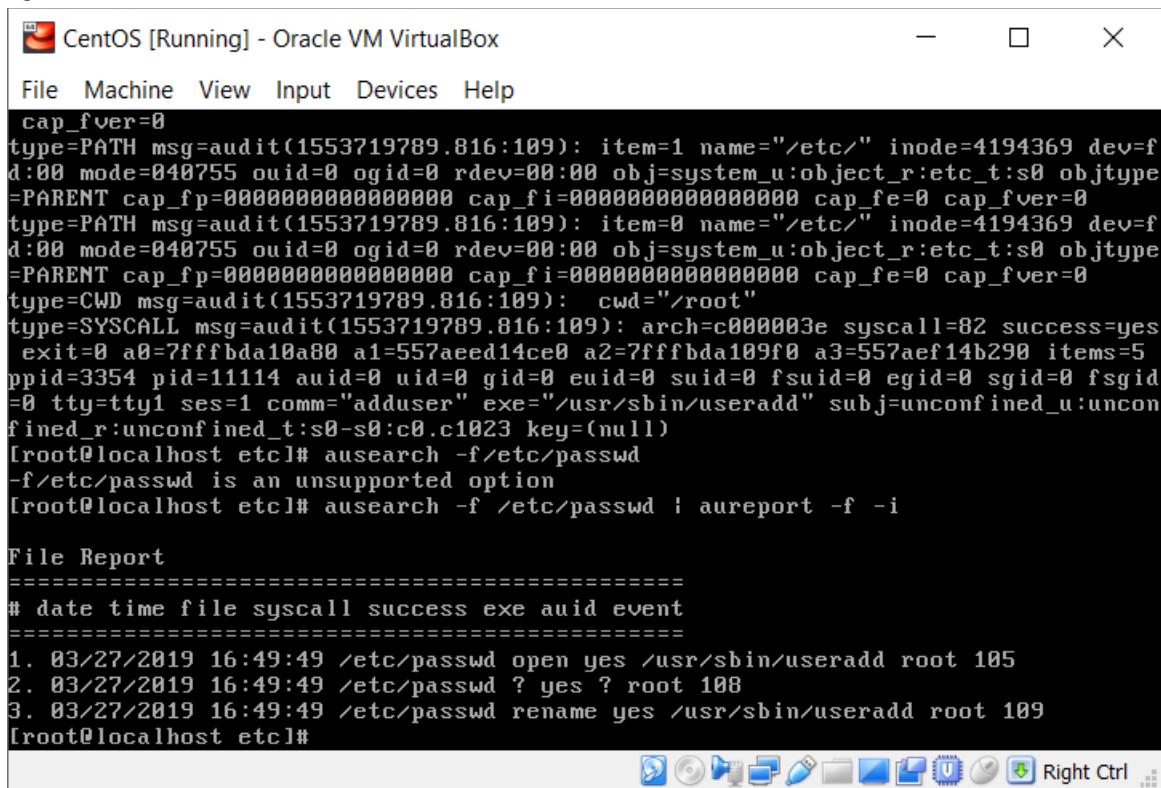
File Machine View Input Devices Help

```
le_t:s0 objtype=CREATE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0
cap_fver=0
type=PATH msg=audit(1553719789.816:109): item=3 name="/etc/passwd" inode=4548789
dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:passwd_fi
le_t:s0 objtype=DELETE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0
cap_fver=0
type=PATH msg=audit(1553719789.816:109): item=2 name="/etc/passwd+" inode=419475
3 dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:passwd_f
ile_t:s0 objtype=DELETE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0
cap_fver=0
type=PATH msg=audit(1553719789.816:109): item=1 name="/etc/" inode=4194369 dev=f
d: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(1553719789.816:109): item=0 name="/etc/" inode=4194369 dev=f
d: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(1553719789.816:109): cwd="/root"
type=SYSCALL msg=audit(1553719789.816:109): arch=c000003e syscall=82 success=yes
exit=0 a0=7ffffbda10a80 a1=557aeced14ce0 a2=7ffffbda109f0 a3=557aef14b290 items=5
ppid=3354 pid=11114 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid
=0 tty=tty1 ses=1 comm="adduser" exe="/usr/sbin/useradd" subj=unconfined_u:uncon
fined_r:unconfined_t:s0-s0:c0.c1023 key=(null)
[root@localhost etc]# ausearch -f /etc/passwd
-f /etc/passwd is an unsupported option
[root@localhost etc]#
```

Right Ctrl

Q19: the value of COMM in the log is as follows: "adduser" exe="/usr/sbin/useradd"

Q20:

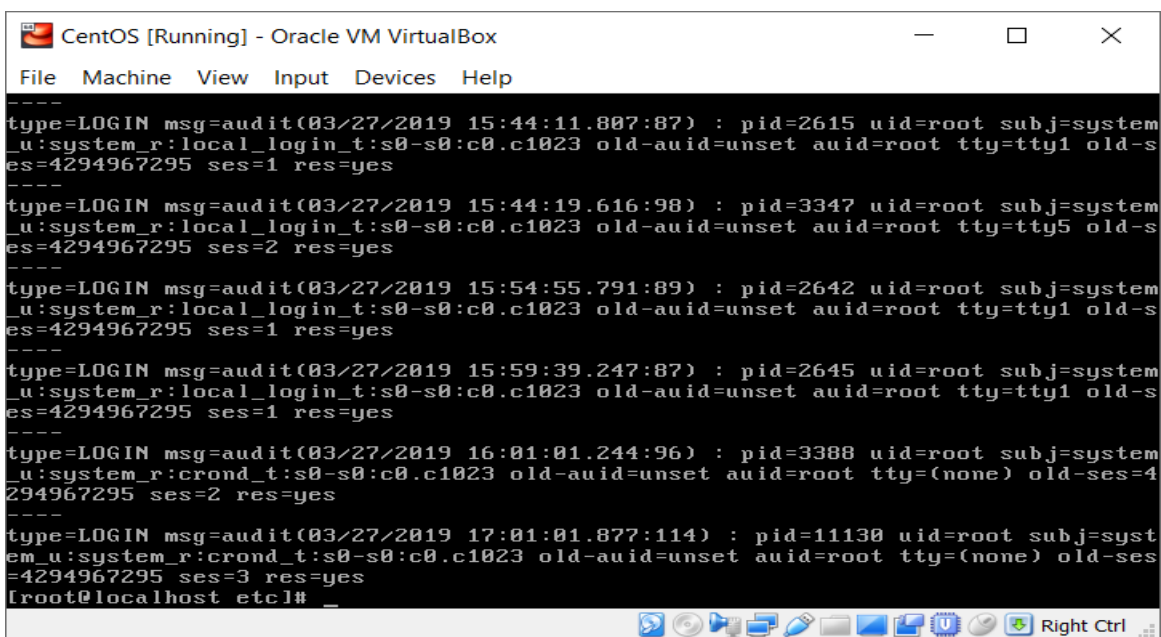


```
CentOS [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

cap_fver=0
type=PATH msg=audit(1553719789.816:109): item=1 name="/etc/" inode=4194369 dev=f
d: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(1553719789.816:109): item=0 name="/etc/" inode=4194369 dev=f
d: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(1553719789.816:109): cwd="/root"
type=SYSCALL msg=audit(1553719789.816:109): arch=c000003e syscall=82 success=yes
exit=0 a0=7ffffbda10a80 a1=557aeed14ce0 a2=7ffffbda109f0 a3=557aef14b290 items=5
ppid=3354 pid=11114 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid
=0 tty=tty1 ses=1 comm="adduser" exe="/usr/sbin/useradd" subj=unconfined_u:uncon
fined_r:unconfined_t:s0-s0:c0.c1023 key=(null)
[root@localhost etc]# ausearch -f /etc/passwd
-f /etc/passwd is an unsupported option
[root@localhost etc]# ausearch -f /etc/passwd | aureport -f -i

File Report
=====
# date time file syscall success exe auid event
=====
1. 03/27/2019 16:49:49 /etc/passwd open yes /usr/sbin/useradd root 105
2. 03/27/2019 16:49:49 /etc/passwd ? yes ? root 108
3. 03/27/2019 16:49:49 /etc/passwd rename yes /usr/sbin/useradd root 109
[root@localhost etc]#
```

Q21:



```
CentOS [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

type=LOGIN msg=audit(03/27/2019 15:44:11.807:87) : pid=2615 uid=root subj=system
_u:system_r:local_login_t:s0-s0:c0.c1023 old-auid=unset auid=root tty=tty1 old-s
es=4294967295 ses=1 res=yes
type=LOGIN msg=audit(03/27/2019 15:44:19.616:98) : pid=3347 uid=root subj=system
_u:system_r:local_login_t:s0-s0:c0.c1023 old-auid=unset auid=root tty=tty5 old-s
es=4294967295 ses=2 res=yes
type=LOGIN msg=audit(03/27/2019 15:54:55.791:89) : pid=2642 uid=root subj=system
_u:system_r:local_login_t:s0-s0:c0.c1023 old-auid=unset auid=root tty=tty1 old-s
es=4294967295 ses=1 res=yes
type=LOGIN msg=audit(03/27/2019 15:59:39.247:87) : pid=2645 uid=root subj=system
_u:system_r:local_login_t:s0-s0:c0.c1023 old-auid=unset auid=root tty=tty1 old-s
es=4294967295 ses=1 res=yes
type=LOGIN msg=audit(03/27/2019 16:01:01.244:96) : pid=3388 uid=root subj=system
_u:system_r:cron_t:s0-s0:c0.c1023 old-auid=unset auid=root tty=(none) old-ses=4
294967295 ses=2 res=yes
type=LOGIN msg=audit(03/27/2019 17:01:01.877:114) : pid=11130 uid=root subj=syst
em_u:system_r:cron_t:s0-s0:c0.c1023 old-auid=unset auid=root tty=(none) old-ses
=4294967295 ses=3 res=yes
[root@localhost etc]#
```

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`