SCA Testing

1) CentOS 7

cis_rhel7_linux_rcl

Pass: 95 **Fail: 9** **Score: 91%**

6505:

```
condition: any
  rules:
    - 'f:/etc/fstab -> !r:^# && !r:/var/tmp;'
```

6506:

```
condition: any
  rules:
    - 'f:/etc/fstab -> !r:^# && !r:/var/log;'
```

6507:

```
condition: any
  rules:
    - 'f:/etc/fstab -> !r:^# && !r:/var/log/audit;'
```

They pass as being in a separate partition, even though /var itself does not exist as a separate partition, which doesn’t make sense as they are located in it.

*etc/*fstab:

```
#
# /etc/fstab
# Created by anaconda on Thu Feb 28 20:50:01 2019
#
```

```
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
UUID=f52f361a-da1a-4ea0-8c7f-ca2706e86b46 /                       xfs     defaults        0 0
/swapfile none swap defaults 0 0
```

6508:

```
condition: any
  rules:
    - 'f:/etc/fstab -> !r:^# && !r:/home;'
```

It passes even tough /home does not exist as a separate partition.

*etc/*fstab:

```
#
# /etc/fstab
# Created by anaconda on Thu Feb 28 20:50:01 2019
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
UUID=f52f361a-da1a-4ea0-8c7f-ca2706e86b46 /                       xfs     defaults        0 0
/swapfile none swap defaults 0 0
```

6560:

```
condition: any
  rules:
    - 'f:/etc/ssh/sshd_config -> !r:^# && !r:LogLevel\.+INFO;'
```

It passes the check because it is set to INFO, but it’s commented so it does not take effect.

/etc/ssh/sshd_config:

```
#	$OpenBSD: sshd_config,v 1.100 2016/08/15 12:32:04 naddy Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/usr/bin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

# If you want to change the port on a SELinux system, you have to tell
# SELinux about this change.
# semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
#
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
SyslogFacility AUTHPRIV
#LogLevel INFO
```

system_audit_ssh

Pass: 3 **Fail: 6** **Score: 33%**

1500:

```
condition: any
  rules:
    - 'f:$sshd_file -> !r:^# && r:Port\.+22;'
```

It passes the check even tough the port is never changed in the configuration file.

/etc/ssh/sshd_config:

```
#	$OpenBSD: sshd_config,v 1.100 2016/08/15 12:32:04 naddy Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/usr/bin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

# If you want to change the port on a SELinux system, you have to tell
# SELinux about this change.
# semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
#
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
```

system_audit_rcl

Pass: 76 **Fail: 0** **Score: 100%**

2) SUSE 11

cis_sles11_linux

Pass: 82 Fail: 9 Score: 90%

First of all there were a couple of issues in the requirements and variables sections of the policy file:

```
requirements:
  title: "Check Suse 11 version"
  description: "Requirements for running the SCA scan against SUSE Linux Enterprise Server 11"
  condition: "any required"
  rules:
    - 'f:/etc/os-release -> r:^PRETTY_NAME="SUSE Linux Enterprise Server 11";'
    - 'f:/etc/os-release -> r:^PRETTY_NAME="SUSE Linux Enterprise Server 11 SP1";'
    - 'f:/etc/os-release -> r:^PRETTY_NAME="SUSE Linux Enterprise Server 11 SP2";'
    - 'f:/etc/os-release -> r:^PRETTY_NAME="SUSE Linux Enterprise Server 11 SP3";'
    - 'f:/etc/os-release -> r:^PRETTY_NAME="SUSE Linux Enterprise Server 11 SP4";'

variables:
  $rc_dirs: /etc/rc.d/rc2.d,/etc/rc.d/rc3.d,/etc/rc.d/rc4.d,/etc/rc.d/rc5.d;
```

- The requirements are extracted from the /etc/os-release file, when that file does not exist. It should be extracted from /etc/issue.

- The variable “$sshd_file: /etc/ssh/sshd_config;” is missing, hindering the rules that depend on it.

7005:

```
condition: any
   rules:
     - 'f:/etc/fstab -> ^# && !r:/var/log;'
```

7006:

```
condition: any
   rules:
    - 'f:/etc/fstab -> ^# && !r:/var/log/audit;'
```

They pass as being in a separate partition, even though /var itself does not exist as a separate partition, which doesn’t make sense as they are located in it.

*etc/*fstab:

```
devpts  /dev/pts         devpts  mode=0620,gid=5 0 0
proc    /proc            proc    defaults       0 0
sysfs   /sys             sysfs   noauto         0 0
debugfs /sys/kernel/debug debugfs noauto         0 0
tmpfs   /run             tmpfs   noauto         0 0
/dev/sda1 / ext3 defaults 1 1
```

7007:

```
condition: any
  rules:
    - 'f:/etc/fstab -> ^# && !r:/home;'
```

It passes even tough /home does not exist as a separate partition.

*etc/*fstab:

```
devpts  /dev/pts         devpts  mode=0620,gid=5 0 0
proc    /proc            proc    defaults       0 0
sysfs   /sys             sysfs   noauto         0 0
debugfs /sys/kernel/debug debugfs noauto         0 0
tmpfs   /run             tmpfs   noauto         0 0
/dev/sda1 / ext3 defaults 1 1
```

7043:

```
condition: any
```

```
  rules:
    - 'f:/proc/sys/net/ipv4/conf/all/send_redirects -> 0;'
    - 'f:/proc/sys/net/ipv4/conf/default/send_redirects -> 0;'
```

Since we want it to be disabled, the rules should check if it has a value of 1, not 0.

7053:

```
condition: any
  rules:
    - 'f:/etc/ssh/sshd_config -> !r:^# && !r:LogLevel\.+INFO;'
```

It passes the check because it is set to INFO, but it’s commented so it does not take effect.

/etc/ssh/sshd_config:

```
# Logging
# obsoletes QuietMode and FascistLogging
#SyslogFacility AUTH
#LogLevel INFO
```

system_audit_ssh

Pass: 3   **Fail: 6**   **Score: 33%**

1500:

```
condition: any
  rules:
    - 'f:$sshd_file -> !r:^# && r:Port\.+22;'
```

It passes the check even tough the port is never changed in the configuration file.

/etc/ssh/sshd_config:

```
#	$OpenBSD: sshd_config,v 1.100 2016/08/15 12:32:04 naddy Exp $
```

```
# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/usr/bin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

# If you want to change the port on a SELinux system, you have to tell
# SELinux about this change.
# semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
#
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
```

system_audit_rcl

Pass: 76 **Fail: 0** **Score: 100%**

system_audit_pw

Pass: 0 **Fail: 4** **Score: 0%**

3) CentOS 5

cis_rhel5_linux_rcl

Pass: 97   **Fail: 14**   **Score: 87%**

5505:

```
condition: any
  rules:
    - 'f:/etc/fstab -> r:^# && !r:/var/tmp && !r:bind;'
```

It passes the check even tough the /var/tmp directory is not bound to /tmp.

/etc/fstab:

```
/dev/VolGroup00/LogVol00 /                       ext3    defaults        1 1
LABEL=/boot             /boot                   ext3    defaults        1 2
tmpfs                   /dev/shm                tmpfs   defaults        0 0
devpts                  /dev/pts                devpts  gid=5,mode=620  0 0
sysfs                   /sys                    sysfs   defaults        0 0
proc                    /proc                   proc    defaults        0 0
/dev/VolGroup00/LogVol01 swap                    swap    defaults        0 0
```

5506:

```
condition: any
  rules:
    - 'f:/etc/fstab -> ^# && !r:/var/log;'
```

5507:

```
condition: any
  rules:
    - 'f:/etc/fstab -> ^# && !r:/var/log/audit;'
```

They pass as being in a separate partition, even though /var itself does not exist as a separate partition, which doesn't make sense as they are located in it.

*etc/*fstab:

```
/dev/VolGroup00/LogVol00 /                      ext3    defaults        1 1
LABEL=/boot             /boot                   ext3    defaults        1 2
tmpfs                   /dev/shm                tmpfs   defaults        0 0
devpts                  /dev/pts                devpts  gid=5,mode=620  0 0
sysfs                   /sys                    sysfs   defaults        0 0
proc                    /proc                   proc    defaults        0 0
/dev/VolGroup00/LogVol01 swap                   swap    defaults        0 0
```

5508:

```
condition: any
   rules:
     - 'f:/etc/fstab -> ^# && !r:/home;'
```

It passes even tough /home does not exist as a separate partition.

*etc/*fstab:

```
/dev/VolGroup00/LogVol00 /                      ext3    defaults        1 1
LABEL=/boot             /boot                   ext3    defaults        1 2
tmpfs                   /dev/shm                tmpfs   defaults        0 0
devpts                  /dev/pts                devpts  gid=5,mode=620  0 0
sysfs                   /sys                    sysfs   defaults        0 0
proc                    /proc                   proc    defaults        0 0
/dev/VolGroup00/LogVol01 swap                   swap    defaults        0 0
```

5516:

```
condition: any
   rules:
     - 'f:/etc/fstab -> !r:^# && r:/dev/shm && !r:noexec;'
     - 'p:yum-updatesd;'
```

This rule fails, but looking at the corresponding rules section, I think this has a copypasting issue. This doesn’t have anything to do with fstab.

5518:

```
condition: any
  rules:
    - 'f:/etc/selinux/config -> r:SELINUX=enforcing;'
```

This rule passes but it should not. If we want to have selinux=enforcing, we should make the rule trigger when it is NOT set to enforcing.

/etc/selinux/config:

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#       enforcing - SELinux security policy is enforced.
#       permissive - SELinux prints warnings instead of enforcing.
#       disabled - SELinux is fully disabled.
SELINUX=disabled
# SELINUXTYPE= type of policy in use. Possible values are:
#       targeted - Only targeted network daemons are protected.
#       strict - Full SELinux protection.
SELINUXTYPE=targeted

# SETLOCALDEFS= Check local definition changes
SETLOCALDEFS=0
```

5519:

```
condition: any
  rules:
    - 'f:/etc/selinux/config -> r:SELINUX=enforcing;'
```

Same reasoning as above, this fails when it IS set to targeted.

/etc/selinux/config:

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#       enforcing - SELinux security policy is enforced.
#       permissive - SELinux prints warnings instead of enforcing.
#       disabled - SELinux is fully disabled.
SELINUX=disabled
# SELINUXTYPE= type of policy in use. Possible values are:
#       targeted - Only targeted network daemons are protected.
#       strict - Full SELinux protection.
SELINUXTYPE=targeted

# SETLOCALDEFS= Check local definition changes
SETLOCALDEFS=0
```

5536:

```
condition: all
  rules:
    - 'f:/etc/init.d/functions -> !r:^# && r:^umask && <:umask 027;'
```

It passes the check when umask is not set to 027

/etc/init.d/functions:

```
# Make sure umask is sane
umask 022
```

5547:

```
condition: any
  rules:
    - 'f:/proc/sys/net/ipv4/conf/all/send_redirects -> 0;'
    - 'f:/proc/sys/net/ipv4/conf/default/send_redirects -> 0;'
```

Since we want it to be disabled, the rules should check if it has a value of 1, not 0.

system_audit_ssh

Pass: 2   Fail: 7   Score: 22%

1500:

```
condition: any
  rules:
    - 'f:$sshd_file -> !r:^# && r:Port\.+22;'
```

It passes the check even tough the port is never changed in the configuration file.

/etc/ssh/sshd_config:

```
#	$OpenBSD: sshd_config,v 1.100 2016/08/15 12:32:04 naddy Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/usr/bin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

# If you want to change the port on a SELinux system, you have to tell
# SELinux about this change.
# semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
#
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
```

system_audit_rcl

Pass: 76 Fail: 0 Score: 100%

system_audit_pw

Pass: 0 Fail: 4 Score: 0%