1.5 Este hardening-ul proceselor configurat corect?

Audit:

Nedefinit

Remediere:

Nedefinit

1.5.1 Sunt core dump-urile restrictionate?

Audit:

Run the following commands and verify output matches:

grep "hard core" /etc/security/limits.conf /etc/security/limits.d/*

* hard core 0

sysctl fs.suid_dumpable

fs.suid_dumpable = 0

grep "fs\.suid_dumpable" /etc/sysctl.conf /etc/sysctl.d/*

fs.suid_dumpable = 0

Remediere:

Add the following line to /etc/security/limits.conf or a /etc/security/limits.d/*

file:

* hard core 0

Set the following parameter in /etc/sysctl.conf or a /etc/sysctl.d/* file:

1.5.2 Este suportul XD/NX activat?

Audit:

Run the following command and verify output matches:

sysctl kernel.randomize_va_space

kernel.randomize_va_space = 2

grep "kernel\.randomize_va_space" /etc/sysctl.conf /etc/sysctl.d/*

kernel.randomize_va_space = 2

Remediere:

Set the following parameter in /etc/sysctl.conf or a /etc/sysctl.d/* file:

kernel.randomize_va_space = 2

Run the following command to set the active kernel parameter:

sysctl -w kernel.randomize_va_space=2

CIS Controls:

8.4 Enable Anti-exploitation Features (i.e. DEP, ASLR, EMET)

Enable anti-exploitation features such as Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualization/containerization, etc. For increased

1.5.3 Este randomizarea adreselor de memorie (ASLR) activata?

Audit:

Nedefinit

Remediere:

Nedefinit

1.5.4 Este prelink dezactivat?

Audit:

Run the following command and verify prelink is not installed:

dpkg -s prelink

Remediere:

Run the following command to restore binaries to normal:

prelink -ua

Run the following command to uninstall prelink:

apt-get remove prelink

CIS Controls:

3.5 Use File Integrity Tools For Critical System Files

Use file integrity checking tools to ensure that critical system files (including sensitive system and application executables, libraries, and configurations) have not been altered. The reporting system should: have the ability to account for routine and expected changes; highlight and alert on unusual or unexpected alterations; show the history of configuration

2.1 Sunt serviciile inetd configurate corect?

Audit:

Verify the daytime service is not enabled. Run the following command and verify results are as indicated:

grep -R "^daytime" /etc/inetd.*

No results should be returned

check /etc/xinetd.conf and /etc/xinetd.d/* and verify all daytime services have disable = yes set.

Remediere:

Comment out or remove any lines starting with daytime from /etc/inetd.conf and /etc/inetd.d/*.

Set disable = yes on all daytime services in /etc/xinetd.conf and /etc/xinetd.d/*.

CIS Controls:

9.1 Limit Open Ports, Protocols, and Services

Ensure that only ports, protocols, and services with validated business needs are running on each system.

2.1.1 Sunt serviciile chargen dezactivate?

Audit:

Verify the discard service is not enabled. Run the following command and verify results are as indicated:

grep -R "^discard" /etc/inetd.*

No results should be returned

check /etc/xinetd.conf and /etc/xinetd.d/* and verify all discard services have disable = yes set.

Remediere:

Comment out or remove any lines starting with discard from /etc/inetd.conf and /etc/inetd.d/*.

Set disable = yes on all discard services in /etc/xinetd.conf and /etc/xinetd.d/*.

CIS Controls:

9.1 Limit Open Ports, Protocols, and Services

Ensure that only ports, protocols, and services with validated business needs are running on each system.

2.1.2 Sunt serviciile daytime dezactivate?

Audit:

Verify the echo service is not enabled. Run the following command and verify results are as indicated:

grep -R "^echo" /etc/inetd.*

No results should be returned

check /etc/xinetd.conf and /etc/xinetd.d/* and verify all echo services have disable = yes set.

Remediere:

Comment out or remove any lines starting with echo from /etc/inetd.conf and /etc/inetd.d/*.

Set disable = yes on all echo services in /etc/xinetd.conf and /etc/xinetd.d/*.

CIS Controls:

9.1 Limit Open Ports, Protocols, and Services

Ensure that only ports, protocols, and services with validated business needs are running on each system.

2.1.3 Sunt serviciile discard dezactivate?

Audit:

Verify the rsh services are not enabled. Run the following commands and verify results are as indicated:

grep -R "^shell" /etc/inetd.*

grep -R "^login" /etc/inetd.*

grep -R "^exec" /etc/inetd.*

No results should be returned

check /etc/xinetd.conf and /etc/xinetd.d/* and verify all rsh, rlogin, and rexec services have disable = yes set.

Remediere:

Comment out or remove any lines starting with shell, login, or exec from /etc/inetd.conf and /etc/inetd.d/*.

Set disable = yes on all rsh, rlogin, and rexec services in /etc/xinetd.conf and /etc/xinetd.d/*.

CIS Controls:

3.4 Use Only Secure Channels For Remote System Administration

Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that do not

2.1.4 Sunt serviciile echo dezactivate?

Audit:

Verify the talk service is not enabled. Run the following commands and verify results are as indicated:

grep -R "^talk" /etc/inetd.*

grep -R "^ntalk" /etc/inetd.*

No results should be returned

check /etc/xinetd.conf and /etc/xinetd.d/* and verify all talk services have disable = yes set.

Remediere:

Comment out or remove any lines starting with talk or ntalk from /etc/inetd.conf and /etc/inetd.d/*.

Set disable = yes on all talk services in /etc/xinetd.conf and /etc/xinetd.d/*.

CIS Controls:

9.1 Limit Open Ports, Protocols, and Services

Ensure that only ports, protocols, and services with validated business needs are running on each system.

2.1.5 Sunt serviciile time dezactivate?

Audit:

Verify the telnet service is not enabled. Run the following command and verify results are as indicated:

grep -R "^telnet" /etc/inetd.*

No results should be returned

check /etc/xinetd.conf and /etc/xinetd.d/* and verify all telnet services have disable = yes set.

Remediere:

Comment out or remove any lines starting with telnet from /etc/inetd.conf and /etc/inetd.d/*.

Set disable = yes on all telnet services in /etc/xinetd.conf and /etc/xinetd.d/*.

CIS Controls:

3.4 Use Only Secure Channels For Remote System Administration

Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as SSL, TLS or IPSEC.

2.1.7 Este serverul talk dezactivat?

Audit:

Verify the tftp service is not enabled. Run the following command and verify results are as indicated:

grep -R "^tftp" /etc/inetd.*

No results should be returned

check /etc/xinetd.conf and /etc/xinetd.d/* and verify all tftp services have disable = yes set.

Remediere:

Comment out or remove any lines starting with tftp from /etc/inetd.conf and /etc/inetd.d/*.

Set disable = yes on all tftp services in /etc/xinetd.conf and /etc/xinetd.d/*.

CIS Controls:

9.1 Limit Open Ports, Protocols, and Services

Ensure that only ports, protocols, and services with validated business needs are running on each system.

2.1.8 Este serverul telnet dezactivat?

Audit:

Run the following commands to verify no start conditions listed for xinetd:

initctl show-config xinetd

xinetd

Remediere:

Remove or comment out start lines in /etc/init/xinetd.conf:

#start on runlevel [2345]

CIS Controls:

9.1 Limit Open Ports, Protocols, and Services

Ensure that only ports, protocols, and services with validated business needs are running

on each system.

2.1.9 Este serverul tftp dezactivat?

Audit:

Run the following command and verify openbsd-inetd is not installed:

dpkg -s openbsd-inetd

Remediere:

Run the following command to uninstall openbsd-inetd:

apt-get remove openbsd-inetd

CIS Controls:

9.1 Limit Open Ports, Protocols, and Services

Ensure that only ports, protocols, and services with validated business needs are running on each system.

2.2 Special Purpose Services

This section describes services that are installed on systems that specifically need to run these services. If any of these services are not required, it is recommended that they be disabled or deleted from the system to reduce the potential attack surface.

2.1.10 Este xinetd dezactivat?

Audit:

Nedefinit

Remediere:

Nedefinit

2.1.11 Este openbsd-inetd dezinstalat?

Audit:

On physical systems or virtual systems where host based time synchronization is not available run the following commands and verify either NTP or chrony is installed:

dpkg -s ntp

dpkg -s chrony

On virtual systems where host based time synchronization is available consult your virtualization software documentation and verify that host based synchronization is in use.

Remediere:

On physical systems or virtual systems where host based time synchronization is not available install NTP or chrony using one of the following commands:

apt-get install ntp

apt-get install chrony

2.2 Sunt serviciile speciale configurate corect?

Audit:

Run the following command and verify output matches:

grep "^restrict" /etc/ntp.conf

restrict -4 default kod nomodify notrap nopeer noquery

restrict -6 default kod nomodify notrap nopeer noquery

The -4 in the first line is optional and options after default can appear in any order.

Additional restriction lines may exist.

Run the following command and verify remote server is configured properly:

grep "^(server|pool)" /etc/ntp.conf

server <remote-server>

Multiple servers may be configured.

Verify that ntp is configured to run as the ntp user by running the following command:

grep "RUNASUSER=ntp" /etc/init.d/ntp

RUNASUSER=ntp

Remediere:

Nedefinit

2.2.1.1 Este sincronizarea orei activata?

Audit:

Run the following command and verify remote server is configured properly:

grep "^(server|pool)" /etc/chrony/chrony.conf

server <remote-server>

Multiple servers may be configured.

Remediere:

Add or edit server or pool lines to /etc/chrony/chrony.conf as appropriate:

server <remote-server>

CIS Controls:

6.1 Use At Least Two Synchronized Time Sources For All Servers And Network Equipment

Include at least two synchronized time sources from which all servers and network equipment retrieve time information on a regular basis so that timestamps in logs are consistent.

2.2.1.2 Este NTP configurat corect?

Audit:

Run the following command and verify X Windows System is not installed:

dpkg -l xserver-xorg*

Remediere:

Run the following command to remove the X Windows System packages:

apt-get remove xserver-xorg*

CIS Controls:

2 Inventory of Authorized and Unauthorized Software

Inventory of Authorized and Unauthorized Software

2.2.1.3 Este chrony configurat corect?

Audit:

Run the following commands to verify no start conditions listed for avahi-daemon:

initctl show-config avahi-daemon

avahi-daemon

Remediere:

Remove or comment out start lines in /etc/init/avahi-daemon.conf:

#start on runlevel [2345]

CIS Controls:

9.1 Limit Open Ports, Protocols, and Services

Ensure that only ports, protocols, and services with validated business needs are running

on each system.

2.2.2 Este X Window System dezinstalat?

Audit:

Run the following commands to verify no start conditions listed for cups:

initctl show-config cups

cups

Remediere:

Remove or comment out start lines in /etc/init/cups.conf:

#start on runlevel [2345]

2.2.3 Este serverul Avahi dezactivat?

Audit:

Ensure no start conditions listed for isc-dhcp-serveror isc-dhcp-server6:

initctl show-config isc-dhcp-server

isc-dhcp-server

initctl show-config isc-dhcp-server6

isc-dhcp-server6

Remediere:

Remove or comment out start lines in /etc/init/isc-dhcp-server.confand

/etc/init/isc-dhcp-server6.conf:

#start on runlevel [2345]

2.2.4 Este CUPS dezactivat?

Audit:

Run the following to ensure no start links for slapd exist in /etc/rc*.d:

ls /etc/rc*.d/S*slapd

No results should be returned.

Remediere:

Run the following command to disable slapd:

update-rc.d slapd disable

2.2.5 Este serverul DHCP dezactivat?

Audit:

Run the following to ensure no start links for nfs-kernel-server exist in /etc/rc*.d:

ls /etc/rc*.d/S*nfs-kernel-server

No results should be returned.

Run the following commands to verify no start conditions listed for rpcbind:

initctl show-config rpcbind

rpcbind

Remediere:

Remove or comment out start lines in /etc/init/rpcbind.conf:

#start on start-rpcbind

Run the following command to disable nfs-kernel-server:

update-rc.d nfs-kernel-server disable

CIS Controls:

2.2.6 Este serverul LDAP dezactivat?

Audit:

Run the following to ensure no start links for bind9 exist in /etc/rc*.d:

ls /etc/rc*.d/S*bind9

No results should be returned.

Remediere:

Run the following command to disable bind9:

update-rc.d bind9 disable

CIS Controls:

9.1 Limit Open Ports, Protocols, and Services

Ensure that only ports, protocols, and services with validated business needs are running on each system.

2.2.7 Sunt NFS si RPC dezactivate?

Audit:

Run the following commands to verify no start conditions listed for vsftpd:

initctl show-config vsftpd

vsftpd

Remediere:

Remove or comment out start lines in /etc/init/vsftpd.conf:

#start on runlevel [2345] or net-device-up IFACE!=lo

2.2.8 Este serverul DNS dezactivat?

Audit:

Run the following to ensure no start links for apache2 exist in /etc/rc*.d:

ls /etc/rc*.d/S*apache2

No results should be returned.

Remediere:

Run the following command to disable apache2:

update-rc.d apache2 disable

CIS Controls:

9.1 Limit Open Ports, Protocols, and Services

Ensure that only ports, protocols, and services with validated business needs are running on each system.

2.2.9 Este serverul FTP dezactivat?

Audit:

Run the following commands to verify no start conditions listed for dovecot:

initctl show-config dovecot

dovecot

Remediere:

Remove or comment out start lines in /etc/init/dovecot.conf:

#start on runlevel [2345]

2.2.10 Este serverul HTTP dezactivat?

Audit:

Ensure no start conditions listed for smbd:

initctl show-config smbd

smbd

Remediere:

Remove or comment out start lines in /etc/init/smbd.conf:

#start on (local-filesystems and net-device-up)

CIS Controls:

9.1 Limit Open Ports, Protocols, and Services

Ensure that only ports, protocols, and services with validated business needs are running on each system.

2.2.11 Sunt serverele IMAP si POP3 dezactivate?

Audit:

Ensure no start conditions listed for squid3:

initctl show-config squid3

squid3

Remediere:

Remove or comment out start lines in /etc/init/squid3.conf:

#start on runlevel [2345]

CIS Controls:

9.1 Limit Open Ports, Protocols, and Services

Ensure that only ports, protocols, and services with validated business needs are running

on each system.

2.2.12 Este Samba dezactivata?

Audit:

Run the following command and verify that the MTA is not listening on any non-loopback address (127.0.0.1 or ::1):

```
# netstat -an | grep LIST | grep ":25[[:space:]]"
tcp 0 0 127.0.0.1:25 0.0.0.0:* LISTEN
```

Remediere:

Edit /etc/postfix/main.cf and add the following line to the RECEIVING MAIL section. If the line already exists, change it to look like the line below:

```
inet_interfaces = loopback-only
```

Restart postfix:

```
# service postfix restart
```

2.2.13 Este serverul proxy HTTP dezactivat?

Audit:

Run the following command to verify that the rsync service is not enabled:

grep ^RSYNC_ENABLE /etc/default/rsync

RSYNC_ENABLE=false

Remediere:

Edit the /etc/default/rsync file and set RSYNC_ENABLE to false:

RSYNC_ENABLE=false

CIS Controls:

9.1 Limit Open Ports, Protocols, and Services

Ensure that only ports, protocols, and services with validated business needs are running

on each system.

2.2.14 Este serverul SNMP dezactivat?

Audit:

Run the following commands to verify no start conditions listed for ypserv:

initctl show-config ypserv

ypserv

Remediere:

Remove or comment out start lines in /etc/init/ypserv.conf:

#start on (started portmap ON_BOOT=

or (started portmap ON_BOOT=y

and ((filesystem and static-network-up) or failsafe-boot)))

CIS Controls:

9.1 Limit Open Ports, Protocols, and Services

Ensure that only ports, protocols, and services with validated business needs are running

on each system.

2.2.16 Este serviciul rsync dezactivat?

Audit:

Nedefinit

Remediere:

Nedefinit

2.2.17 Este serverul NIS dezactivat?

Audit:

Run the following command and verify nis is not installed:

dpkg -s nis

Remediere:

Run the following command to uninstall nis:

apt-get remove nis

2.3 Sunt clientii de servicii configurati corect?

Audit:

Run the following commands and verify rsh is not installed:

dpkg -s rsh-client

dpkg -s rsh-redone-client

Remediere:

Run the following command to uninstall rsh:

apt-get remove rsh-client rsh-redone-client

2.3.1 Este clientul NIS dezinstalat?

Audit:

Run the following command and verify talk is not installed:

dpkg -s talk

Remediere:

Run the following command to uninstall talk:

apt-get remove talk

2.3.2 Este clientul rsh dezinstalat?

Audit:

Run the following command and verify telnet is not installed:

dpkg -s telnet

Remediere:

Run the following command to uninstall telnet:

apt-get remove telnet

2.3.3 Este clientul talk dezinstalat?

Audit:

Run the following command and verify ldap-utils is not installed:

dpkg -s ldap-utils

Remediere:

Uninstall ldap-utils using the appropriate package manager or manual installation:

apt-get remove ldap-utils

2.3.4 Este clientul telnet dezinstalat?

Audit:

Nedefinit

Remediere:

Nedefinit

2.3.5 Este clientul LDAP dezinstalat?

Audit:

Run the following command and verify output matches:

sysctl net.ipv4.ip_forward

net.ipv4.ip_forward = 0

grep "net\.ipv4\.ip_forward" /etc/sysctl.conf /etc/sysctl.d/*

net.ipv4.ip_forward = 0

Remediere:

Set the following parameter in /etc/sysctl.conf or a /etc/sysctl.d/* file:

net.ipv4.ip_forward = 0

Run the following commands to set the active kernel parameters:

sysctl -w net.ipv4.ip_forward=0

sysctl -w net.ipv4.route.flush=1

3.1 Sunt parametrii de retea (doar host) configurati corect?

Audit:

Run the following commands and verify output matches:

sysctl net.ipv4.conf.all.send_redirects

net.ipv4.conf.all.send_redirects = 0

sysctl net.ipv4.conf.default.send_redirects

net.ipv4.conf.default.send_redirects = 0

grep "net\.ipv4\.conf\.all\.send_redirects" /etc/sysctl.conf

/etc/sysctl.d/*

net.ipv4.conf.all.send_redirects = 0

grep "net\.ipv4\.conf\.default\.send_redirects" /etc/sysctl.conf

/etc/sysctl.d/*

net.ipv4.conf.default.send_redirects= 0

Remediere:

Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file:

net.ipv4.conf.all.send_redirects = 0

net.ipv4.conf.default.send_redirects = 0

Run the following commands to set the active kernel parameters:

sysctl -w net.ipv4.conf.all.send_redirects=0

sysctl -w net.ipv4.conf.default.send_redirects=0

sysctl -w net.ipv4.route.flush=1

3.1.1 Este forwarding-ul IP dezactivat?

Audit:

Nedefinit

Remediere:

Nedefinit

3.1.2 Este trimiterea de redirectari de pachete dezactivata?

Audit:

Run the following commands and verify output matches:

sysctl net.ipv4.conf.all.accept_source_route

net.ipv4.conf.all.accept_source_route = 0

sysctl net.ipv4.conf.default.accept_source_route

net.ipv4.conf.default.accept_source_route = 0

grep "net\.ipv4\.conf\.all\.accept_source_route" /etc/sysctl.conf

Remediere:

Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file:

net.ipv4.conf.all.accept_source_route = 0

net.ipv4.conf.default.accept_source_route = 0

Run the following commands to set the active kernel parameters:

sysctl -w net.ipv4.conf.all.accept_source_route=0

sysctl -w net.ipv4.conf.default.accept_source_route=0

sysctl -w net.ipv4.route.flush=1

CIS Controls:

3 Secure Configurations for Hardware and Software on Mobile Devices, Laptops,

Workstations, and Servers

Secure Configurations for Hardware and Software on Mobile Devices, Laptops,

Workstations, and Servers

11 Secure Configurations for Network Devices such as Firewalls, Routers and switches

Secure Configurations for Network Devices such as Firewalls, Routers and switches

6.1 Sunt permisiunile fisierelor de sistem configurate corect?

Audit:

Run the following command and verify Uid and Gid are both 0/root and Access is 644:

stat /etc/passwd

Access: (0644/-rw-r--r--) Uid: (0/   root)   Gid: (0/   root)

Remediere:

Run the following command to set permissions on /etc/passwd:

chown root:root /etc/passwd

chmod 644 /etc/passwd

CIS Controls:

16.14 Encrypt/Hash All Authentication Files And Monitor Their Access

Verify that all authentication files are encrypted or hashed and that these files cannot be accessed without root or administrator privileges. Audit all access to password files in the system.

6.1.1 Au fost auditate permisiunile fisierelor de sistem?

Audit:

Run the following command and verify Uid is 0/root, Gid is <gid>/shadow, and Access is 640 or more restrictive:

stat /etc/shadow

Access: (0640/-rw-r-----) Uid: (0/   root)   Gid: (42/ shadow)

Remediere:

Run the one following commands to set permissions on /etc/shadow:

chown root:shadow /etc/shadow

chmod o-rwx,g-wx /etc/shadow

CIS Controls:

16.14 Encrypt/Hash All Authentication Files And Monitor Their Access

Verify that all authentication files are encrypted or hashed and that these files cannot be accessed without root or administrator privileges. Audit all access to password files in the system.

6.1.2 Sunt permisiunile pe /etc/passwd configurate corect?

Audit:

Run the following command and verify Uid and Gid are both 0/root and Access is 644:

stat /etc/group

Access: (0644/-rw-r--r--) Uid: (0/   root)   Gid: (0/   root)

Remediere:

Run the following command to set permissions on /etc/group:

chown root:root /etc/group

chmod 644 /etc/group

CIS Controls:

16.14 Encrypt/Hash All Authentication Files And Monitor Their Access

Verify that all authentication files are encrypted or hashed and that these files cannot be accessed without root or administrator privileges. Audit all access to password files in the system.

6.1.3 Sunt permisiunile pe /etc/shadow configurate corect?

Audit:

Run the following command and verify verify Uid is 0/root, Gid is <gid>/shadow, and

Access is 640 or more restrictive:

stat /etc/gshadow

Access: (0640/-rw-r-----) Uid: (0/   root)   Gid: (42/ shadow)

Remediere:

Run the following commands to set permissions on /etc/gshadow:

chown root:shadow /etc/gshadow

chmod o-rwx,g-rw /etc/gshadow

CIS Controls:

16.14 Encrypt/Hash All Authentication Files And Monitor Their Access

Verify that all authentication files are encrypted or hashed and that these files cannot be accessed without root or administrator privileges. Audit all access to password files in the system.

6.1.4 Sunt permisiunile pe /etc/group configurate corect?

Audit:

Run the following command and verify Uid and Gid are both 0/root and Access is 644 or more restrictive:

```
# stat /etc/passwd-
Access: (0644/-rw-------)  Uid: (    0/    root)   Gid: (    0/    root)
```

Remediere:

Run the following command to set permissions on /etc/passwd- :

```
# chown root:root /etc/passwd-
# chmod u-x,go-wx /etc/passwd-
```

CIS Controls:

16.14 Encrypt/Hash All Authentication Files And Monitor Their Access

Verify that all authentication files are encrypted or hashed and that these files cannot be accessed without root or administrator privileges. Audit all access to password files in the system.

6.1.5 Sunt permisiunile pe /etc/gshadow configurate corect?

Audit:

Run the following command and verify verify Uid is 0/root, Gid is 0/root or

<gid>/shadow, and Access is 640 or more restrictive:

stat /etc/shadow-

Access: (0640/-rw-r-----) Uid: (0/   root)   Gid: (42/ shadow)

Remediere:

Run the one of the following chown commands as appropriate and the chmod to set

permissions on /etc/shadow- :

chown root:root /etc/shadow-

chown root:shadow /etc/shadow-

chmod o-rwx,g-rw /etc/shadow-

CIS Controls:

16.14 Encrypt/Hash All Authentication Files And Monitor Their Access

Verify that all authentication files are encrypted or hashed and that these files cannot be

accessed without root or administrator privileges. Audit all access to password files in the

system.

6.1.6 Sunt permisiunile pe /etc/passwd- configurate corect?

Audit:

Run the following command and verify Uid and Gid are both 0/root and Access is 644 or more restrictive:

stat /etc/group-

Access: (0644/-rw-------) Uid: (0/   root)   Gid: (0/   root)

Remediere:

Run the following command to set permissions on /etc/group- :

chown root:root /etc/group-

chmod u-x,go-wx /etc/group-

CIS Controls:

16.14 Encrypt/Hash All Authentication Files And Monitor Their Access

Verify that all authentication files are encrypted or hashed and that these files cannot be accessed without root or administrator privileges. Audit all access to password files in the system.

6.1.7 Sunt permisiunile pe /etc/shadow- configurate corect?

Audit:

Run the following command and verify verify Uid is 0/root, Gid is 0/root or

<gid>/shadow, and Access is 640 or more restrictive:

stat /etc/gshadow-

Access: (0640/-rw-r-----) Uid: (0/   root)   Gid: (42/ shadow)

Remediere:

Run the one of the following chown commands as appropriate and the chmod to set

permissions on /etc/gshadow- :

chown root:root /etc/gshadow-

chown root:shadow /etc/gshadow-

chmod o-rwx,g-rw /etc/gshadow-

CIS Controls:

16.14 Encrypt/Hash All Authentication Files And Monitor Their Access

Verify that all authentication files are encrypted or hashed and that these files cannot be

accessed without root or administrator privileges. Audit all access to password files in the

system.

6.1.8 Sunt permisiunile pe /etc/group- configurate corect?

Audit:

Run the following command and verify no files are returned:

df --local -P | awk {'if (NR!=1) print $6'} | xargs -I

'{}' find '{}' -xdev -type f -perm -0002

The command above only searches local filesystems, there may still be compromised items on network mounted partitions. Additionally the --local option to df is not universal to all versions, it can be omitted to search all filesystems on a system including network mounted filesystems or the following command can be run manually for each partition:

find <partition> -xdev -type f -perm -0002

Remediere:

Removing write access for the "other" category (chmod o-w <filename>) is advisable, but always consult relevant vendor documentation to avoid breaking any application dependencies on a given file.

CIS Controls:

14 Controlled Access Based on the Need to Know

Controlled Access Based on the Need to Know

6.1.9 Sunt permisiunile pe /etc/gshadow- configurate corect?

Audit:

Run the following command and verify no files are returned:

df --local -P | awk {'if (NR!=1) print $6'} | xargs -I '{}' find '{}' -xdev

-nouser

The command above only searches local filesystems, there may still be compromised items on network mounted partitions. Additionally the --local option to df is not universal to all versions, it can be omitted to search all filesystems on a system including network mounted filesystems or the following command can be run manually for each partition:

find <partition> -xdev -nouser

Remediere:

Locate files that are owned by users or groups not listed in the system configuration files, and reset the ownership of these files to some active user on the system as appropriate.

CIS Controls:

14 Controlled Access Based on the Need to Know

Controlled Access Based on the Need to Know

6.1.10 Exista fisiere world-writable?

Audit:

Run the following command and verify no files are returned:

df --local -P | awk {'if (NR!=1) print $6'} | xargs -I '{}' find '{}' -xdev

-nogroup

The command above only searches local filesystems, there may still be compromised items on network mounted partitions. Additionally the --local option to df is not universal to all versions, it can be omitted to search all filesystems on a system including network mounted filesystems or the following command can be run manually for each partition:

find <partition> -xdev -nogroup

Remediere:

Locate files that are owned by users or groups not listed in the system configuration files, and reset the ownership of these files to some active user on the system as appropriate.

CIS Controls:

14 Controlled Access Based on the Need to Know

Controlled Access Based on the Need to Know

6.1.11 Exista fisiere sau directoare fara proprietar?

Audit:

Run the following command to list SUID files:

df --local -P | awk {'if (NR!=1) print $6'} | xargs -I '{}' find '{}' -xdev

-type f -perm -4000

The command above only searches local filesystems, there may still be compromised items on network mounted partitions. Additionally the --local option to df is not universal to all versions, it can be omitted to search all filesystems on a system including network mounted filesystems or the following command can be run manually for each partition:

find <partition> -xdev -type f -perm -4000

Remediere:

Ensure that no rogue SUID programs have been introduced into the system. Review the files returned by the action in the Audit section and confirm the integrity of these binaries.

CIS Controls:

5.1 Minimize And Sparingly Use Administrative Privileges

Minimize administrative privileges and only use administrative accounts when they are

6.1.12 Exista fisiere sau directoare fara grup?

Audit:

Run the following command to list SGID files:

df --local -P | awk {'if (NR!=1) print $6'} | xargs -I '{}' find '{}' -xdev

-type f -perm -2000

The command above only searches local filesystems, there may still be compromised items on network mounted partitions. Additionally the --local option to df is not universal to all versions, it can be omitted to search all filesystems on a system including network mounted filesystems or the following command can be run manually for each partition:

find <partition> -xdev -type f -perm -2000

Remediere:

Ensure that no rogue SGID programs have been introduced into the system. Review the files returned by the action in the Audit section and confirm the integrity of these binaries.

CIS Controls:

6.1.13 Au fost auditate executabilele SUID?

Audit:

Nedefinit

Remediere:

Nedefinit

6.1.14 Au fost auditate executabilele SGID?

Audit:

Run the following command and verify that no output is returned:

cat /etc/shadow | awk -F: '($2 == "") { print $1 " does not have a

password "}'

Remediere:

If any accounts in the /etc/shadow file do not have a password, run the following command

to lock the account until it can be determined why it does not have a password:

passwd -l <username>

Also, check to see if the account is logged in and investigate what it is being used for to

determine if it needs to be forced off.

CIS Controls: