1.1.1.1 Este montarea sistemelor de fisiere cramfs dezactivata?

Audit:

Run the following commands and verify the output is as indicated:

```
# modprobe -n -v freevxfs

install /bin/true

# lsmod | grep freevxfs

<No output>
```

Remediere:

Edit or create the file /etc/modprobe.d/CIS.conf and add the following line:

```
install freevxfs /bin/true
```

Run the following command to unload the freevxfs module:

```
# rmmod freevxfs
```

CIS Controls:

13 Data Protection

Data Protection

1.2.1 Sunt repository-rile pentru managerul de pachete configurate?

Audit:

Run the following command and verify package repositories are configured correctly:

```
# apt-cache policy
```

Remediere:

Configure your package manager repositories according to site policy.

CIS Controls:

1.2.2 Sunt cheile GPG configurate corect?

Audit:

Run the following command and verify GPG keys are configured correctly for your package manager:

```
# apt-key list
```

Remediere:

Update your package manager GPG keys in accordance with site policy.

CIS Controls:

4.5 Use Automated Patch Management And Software Update Tools

Deploy automated patch management tools and software update tools for operating system and software/applications on all systems for which such tools are available and safe.

Patches should be applied to all systems, even systems that are properly air gapped.

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
```