

IRIS BUSINESS SERVICES LIMITED

Document Control:

Document Name	Hardening
Version Number	V1.2
Prepared By	Akshay Rane
Reviewed By	Sabu O
Date of Review	10-08-2022
Approved By	PKX Thomas
Date of Release	18-08-2022

Version Control:--

Version No.	Date	Prepared by / Modified by	Overview of Changes
V1.0	20-08-2020	Vishal Vare	First Release
V1.1	0-08-2022	Akshay Rane	No Modifications

Table of Contents

1. Physical Protection----------Page| 3

2. User Separate Disk Partition----------Page| 3

3. Use LVM for Redundancy and File System Growth----------Page| 3

4. Install only Minimum Amount of Packages Required----------Page| 4

5. Update the System Frequently----------Page| 4

6. Disable Ctrl+Alt+Del----------Page| 4

7. Remove Uncessary Software Packages----------Page| 4

8. Restart Systemd Service after Daemon Updates----------Page| 4

9. Remove Unneeded Services----------Page| 5

10. Network Port Scanning----------Page| 5

11. Packet filtering Firewall----------Page| 5

12. Inspect Protocol Packets with TCP Dump----------Page| 5

1) Physical Protection

Lock down your server rooms access, use racks locking and video surveillance. Take into consideration that any physical access to server rooms can expose your machine to serious security issues.

Disable USB

lsmod

#vi /etc/modprob.d/no-usb

Install usb-storage /bin/true

2) Use Separate Disk Partitions.

/boot
/home
/tmp
/var
/opt
/var/audit (optional)
/usr

3) Use LVM and RAID for Redundancy and File System Growth

The task is to create LVM storage for virtual machine images. So LVM will be used in any case.

There are two ways LVM providing redundancy:

1. block mirroring

   lvcreate -m 1 --mirrorlog mirrored -n logical_volume -L 50G vg01
2. internal RAID mechanism

lvcreate --type=raid1 -n logical_volume -L 50G vg01

4) Install Only the Minimum Amount of Packages Required

Avoid installing unimportant or unnecessary programs, applications or services to avoid package vulnerabilities. This can decrease the risk that the compromise of a piece of software may lead to compromise other applications, parts of the system or even file systems, finally resulting in data corruption or data loss.

5) Update the system frequently

Update the system regularly. Keep Linux kernel in sync with the latest security patches and all the installed software up-to-date with the latest versions by issuing the below command:

```
# yum update
```

6) Disable Ctrl+Alt+Del

In order to prevent users to reboot the server once they have physical access to keyboard or via a Remote Console Application or a virtualized console (**KVM**, Virtualizing software interface) you should disable Ctrl+Alt+Del key sequence by executing the below command.

```
# systemctl mask ctrl-alt-del.target
```

7) Remove Unnecessary Software Packages

nstall minimal software required for your machine. Never install extra programs or services. Install packages only from trusted or official repositories. Use minimal installation of the system in case the machine is destined to run its entire live as a server.

Verify installed packages using one of the following commands:

```
# rpm -qa
```

Make a local list of all installed packages.

```
# yum list installed >> installed.txt
```

Consult the list for useless software and delete a package by issuing the below command:

```
# yum remove package_name
```

8) Restart systemd services after daemon updates

Use the below command example to restart a systemd service in order to apply new updates.

```
# systemctl restart httpd.service
```

9) Remove Unneeded Services

Identify the services that are listening on specific ports using the following command.

```
# ss -tulpn
```

To list all installed services with their output status issue the below command:

```
# systemctl list-units -t service
```

For instance, **CentOS 7** default minimal installation comes with Postfix daemon installed by default which runs by the name of master under port **25**. Remove Postfix network service in case your machine will not be used as a mail server.

```
# yum remove postfix
```

10) Network Port Scanning

Conduct external port checks using the nmap tool from a remote system over the LAN. This type of scanning can be used to verify network vulnerabilities or test the firewall rules.

```
# nmap -sT -O 192.168.1.10
```

11) Packet-filtering Firewall

Use **firewalld** utility to protect the system ports, open or close specific services ports, especially well-known ports (<1024).

Install, start, enable and list the firewall rules by issuing the below commands:

```
# yum install firewalld
# systemctl start firewalld.service
# systemctl enable firewalld.service
# firewall-cmd --list-all
```

12) Inspect Protocol Packets with tcpdump

Use **tcpdump** utility in order to sniff network packets locally and inspect their content for suspicious traffic (source-destination ports, tcp/ip protocols, layer two traffic, unusual ARP requests).

For a better analysis of the **tcpdump** captured file use a more advanced program such as **Wireshark**.

```
# tcpdump -i eno16777736 -w tcpdump.pcap
```