Q.1 What are some ways to prevent unauthorized access to your Linux machine?

1. Only install required packages

You should only install the packages that your business needs to run in order to protect the functionality of your server.

Linux server distributions come with a variety of common packages already installed, such as adduser and base-passwd. During installation, users can opt to install additional packages, including an Open SSH server, a DNS server, a LAMP stack, and a print server.

2. Disable the root login

Linux distributions include a superuser called ‘root’ that contains elevated administrative permissions. Keeping root login enabled can present a security risk and diminish the safety of small business cloud resources hosted on the server, as hackers can exploit this credential to access the server. To strengthen your server security, you must disable this login.

3. Configure 2FA

Two-factor authentication (2FA) greatly improves the security of user access by requiring a password and second token before users can log on to the server.

4. Enforce good password hygiene

Good password hygiene isn’t only relevant to users logging into their personal computers or SaaS applications. For servers, administrators also need to ensure that users are utilizing sufficiently rigorous passwords. This practice makes them much more resistant to attacks.

5. Server-side antivirus software

While Linux computers are considered relatively resistant to viruses, malware, and other forms of cyberattack, all Linux endpoints – including desktops – should run antivirus protection. Antivirus products will enhance the defensive capabilities of any server it runs.

6. Enable a firewall

Every Linux server should be running a firewall as an initial line of defence against unauthorized or malicious connection requests.

2. Name some advantages of using an open-source operating system like Linux over more closed-source alternatives like Windows or Mac OS X.

**1. Reliable and efficient**

The open-source operating systems are most reliable and efficient. Thousands of eyes monitor these because the source code is public. As a result, if there are any bugs or errors, they are fixed by the best developers worldwide.

**2. Cost-efficient**

Most of the open-source operating systems are free. And some of them are far less expensive than commercially closed products.

**3. Flexibility**

The great advantage is you may customize it as per your requirement. And there is creative freedom.

Q.3 How to Terminate (Kill) Running Processes? List all the ways.

Q.4 How To Check The Running Network Services in the Linux?

Q.5 How to Setup Password Aging in Linux?

Password aging **requires users to change their password if the password has existed on the system for a defined time period**

To enable and configure password aging, logon to your server and open, with root privileges, **/etc/login.defs**. I've used nano as my editor for this but you can swap out nano for your preferred editor.

The config file provides a handy explanation for what each of the config values mean and do.

Once you've set your desired values simply save and close the file **CTRL + X**, press **Y** to confirm you want to save and then hit **Enter** to confirm the file to write **/etc/login.defs**.

Q.6 Hot to Lock the boot directory?

The boot directory contains important files related to the Linux kernel, so you need to make sure that this directory is locked down to read-only permissions by following the next simple steps. First, open the “fstab” file.

root@kali:~ #nano /etc/fstab

When you finish editing the file, you need to set the owner by executing the following command:

#chown root:root /etc/fstab

Q.7 What are different ways to disable the USB drive in windows and linux?

For Linux

1. Removing USB Driver - # mv /lib/modules/$(uname -r)/kernel/drivers/usb/storage/usb-storage.ko /home/centlinux
2. Backlist USB- Storage - # echo 'blacklist usb-storage' >> /etc/modprobe.d/blacklist.conf

This method has one downside i.e. any privileged user can load the usb-storage module by executing the following command.

$ sudo modprobe usb-storage

For Windows

1. Manually Edit the Registry

Begin by pressing Win + R, then enter "regedit".

Agree to the User Account Control message, then browse to HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\USBSTOR. Here, double-click Start (or right-click > Modify) and edit the value to 4.

**Q.8 How can we identify that some port are open ?**

### **Testing ports with the command prompt**

If you would like to test ports on your computer, use the Windows command prompt and the [**CMD command**](https://www.ionos.com/digitalguide/server/know-how/windows-cmd-commands/)**netstat -ano**. Windows will show you all currently existing network connections via open ports or open, listening ports that are currently not establishing a connection.

### **Testing ports with port-scanner software**

**Port scanners** work in a similar way to the command prompt. This is software that examines open ports and authorized services. In addition, port scanners are able to examine **network security and structure**. Port scanners send data packets to a destination address for analysis and evaluate the resulting responses in order to check ports.

### **Testing ports with online tools**

A third alternative for a port check are **free online tools** that detect open ports on your computer and thus, potential security gaps.

**Q.9 How to harden the network in the Windows and Linux operating system?**

**Q.10 What is registry file? Explain with respect to both Windows and Linux.**

For windows

The Windows registry is **a centralized, hierarchical database that manages resources and stores configuration settings for applications on the Windows operating system**. Security account services, user interfaces, and device drivers can all use the Windows registry

For linux