Server Hardening For Web Applications

Server Hardening is the process of enhancing server security through a variety of means which results in a much more secure server operating environment. This is due to the advanced security measures that are put in place during the server hardening process.

Server Hardening, probably one of the most important tasks to be handled on your servers, becomes more understandable when you realize all the risks involved. The default config of most operating systems are not designed with security as the primary focus. Instead, default setups focus more on usability, communications and functionality. To protect your servers you must establish solid and sophisticated server hardening policies for all servers in your organization. Developing a server hardening checklist would likely be a great first step in increasing your server and network security. Make sure that your checklist includes minimum security practices that you expect of your staff. If you go with a consultant you can provide them with your server hardening checklist to use as a baseline.

Server Hardening Tips & Tricks:

Every server security conscious organization will have their own methods for maintaining adequate system and network security. Often you will find that server hardening consultants can bring your security efforts up a notch with their specialized expertise.

Some common server hardening tips & tricks include:

- Use Data Encryption for your Communications
- Avoid using insecure protocols that send your information or passwords in plain text.
- Minimize unnecessary software on your servers.
- Disable Unwanted SUID and SGID Binaries
- Keep your operating system up to date, especially security patches.
- Using security extensions is a plus.

- When using Linux, SELinux should be considered. Linux server hardening is a primary focus for the web hosting industry, however in web hosting SELinux is probably not a good option as it often causes issues when the server is used for web hosting purposes.
- User Accounts should have very strong passwords
- Change passwords on a regular basis and do not reuse them
- Lock accounts after too many login failures. Often these login failures are illegitimate attempts to gain access to your system.
- Do not permit empty passwords.
- SSH Hardening
--- Change the port from default to a non standard one
--- Disable direct root logins. Switch to root from a lower level account only when necessary.
- Unnecessary services should be disabled. Disable all instances of IRC - BitchX, bnc, eggdrop, generic-sniffers, guardservices, ircd, psyBNC, ptlink.
- Securing /tmp /var/tmp /dev/shm
- Hide BIND DNS Sever Version and Apache version
- Hardening sysctl.conf
- Server hardenining by installing Root Kit Hunter and ChrootKit hunter.
- Minimize open network ports to be only what is needed for your specific circumstances.
- Configure the system firewall (Iptables) or get a software installed like CSF or APF. Proper setup of a firewall itself can prevent many attacks.
- Consider also using a hardware firewall
- Separate partitions in ways that make your system more secure.
- Disable unwanted binaries
- Maintain server logs; mirror logs to a separate log server
- Install Logwatch and review logwatch emails daily. Investigate any suspicious activity on your server.
- Use brute force and intrusion detection systems
- Install Linux Socket Monitor - Detects/alerts when new sockets are created on your system, often revealing hacker activity

- Install Mod_security as Webserver Hardening
- Hardening the Php installation
- Limit user accounts to accessing only what they need. Increased access should only be on an as-needed basis.
- Maintain proper backups
- Don't forget about physical server security

WhatsApp end-to-end Encryption

WhatsApp is now end-to-end encrypted at all times. This will ensure that users' messages, videos, photos sent over WhatsApp can't be read by anyone else — not WhatsApp, not cyber-criminals, not law-enforcement agencies. Even calls and group chats will be encrypted. WhatsApp is using **"The Signal Protocol"**, designed by Open Whisper Systems, for its encryption.

In its White Paper, explaining the technical details of the end-to-end encryption, WhatsApp says that "once the session is established, clients do not need to rebuild a new session with each other until the existing session state is lost through an external event such as an app reinstall or device change."

It reads, "Clients exchange messages that are protected with a Message Key using AES256 in CBC mode for encryption and HMAC-SHA256 for authentication. The Message Key changes for each message transmitted, and is ephemeral, such that the Message Key used to encrypt a message cannot be reconstructed from the session." It also says that calls, large file attachments are end-to-end encrypted as well.

It should be noted that **feature is enabled by default in WhatsApp,** which means that if you and your friends are on the latest version of the app, all chats will be end-to-end encrypted. Unlike say Telegram where users have to start a secret chat to enable the feature, WhatsApp has the feature on at all times. Users **don't have the option of switching off** end-to-end encryption.

Basic Input/output System (BIOS)

A basic input/output system (BIOS) is a preinstalled program used during startup on Windows-based computers. The CPU initially accesses the BIOS, after which the operating system is loaded.

A basic input/output system is also known as system BIOS or ROM BIOS.

The BIOS is built-in software that contains generic code required to control the keyboard, display screens, disk drives and other functions. The primary purpose of the BIOS is to set up hardware and further load and start an operating system. BIOS is placed in a non-volatile ROM chip inside the computer, ensuring the availability of BIOS at all times and preventing accidental disk failure. The BIOS checks every hardware connection and locates the devices, after which the operating system is loaded into computer memory.

BIOS software is designed to work with the various devices that make up a complimentary system chipset. The BIOS library has certain functions used to operate and control system peripherals, which can be initiated by external software.

Users using the BIOS user interface can perform functions such as:

- Setting the system clock
- Enabling and disabling certain system components
- Hardware configuration
- Selecting boot drives
- Set password prompts for secured access to BIOS user interface function

Modern PCs have BIOS stored in rewritable memory, permitting contents to be rewritten or replaced. Such content rewriting is called flashing and is executed through a special program provided by system manufacturers.

Booting Process

Booting is a process or set of operations that loads and hence starts the operating system, starting from the point when user switches on the power button.

Basically documents related to booting are generally confusing as they are often related to some specific operating system that is Linux machine or Windows machine. But I will keep it as general as possible. ***General Booting sequence*** comprises of the following steps:

· Turn on the Power button.

· CPU pins are reset and registers are set to specific value.

· CPU jump to address of BIOS (0xFFFF0).

· BIOS run POST (Power-On Self-Test) and other necessary checks.

· BIOS jumps to MBR(Master Boot Record).

· Primary Bootloader runs from MBR and jumps to Secondary Bootloader.

· Secondary Bootloaders loads Operating System.

These are the tasks that are carried during booting process. Now let us discuss them in detail.

As soon as we turn the power button, the reset signal is sent and the registers in the CPU are set to their pre-defined value. The first and foremost is the reset vector as shown in the figure (example is taken of 4GB RAM). It should be noted that RAM contains the garbage value at this time, and the instructions/data stored at any memory location is due to the memory map of the chipset. Memory map maps the location (address) to flash memory containing values or instructions. It is ensured that the instruction stored at this reset vector location is jump to system BIOS, as BIOS takes up further process of powering up the system.

POST

Power on Self-Test is the foremost routine which checks and tests the basic hardware. If it fails then it displays error.

· Initialization of the hardware devices by letting them run their individual BIOS (e.g. video card have their own inbuilt BIOS code).

· Searching for the Master Boot Record and reading it.

· Copying the boot sector code to RAM and then switching the control to it.

UEFI

Unified Extensible Firmware Interface (UEFI) is a specification for a software program that connects a computer's firmware to its operating system (OS).UEFI is expected to eventually replace BIOS. Like BIOS, UEFI is installed at the time of manufacturing and is the first program that runs when a computer is turned on.

Unified Extensible Firmware Interface (**UEFI**) is a specification for a software program that connects a computer's firmware to its operating system (OS).**UEFI** is expected to eventually replace BIOS. Like BIOS, **UEFI** is installed at the time of manufacturing and is the first program that runs when a computer is turned on.

Difference between RAID and LVM

S.No.	RAID	LVM
1.	RAID is used for redundancy.	LVM is a way in which you partition the hard disk logically and it contains its own advantages.
2.	A RAID device is a physical grouping of disk devices in order to create a logical presentation of one device to an Operating System for redundancy or performance or a combination of the two.	LVM is a logical layer that that can be manipulated in order to create and, or expand a logical presentation of a disk device to an Operating System.
3.	RAID is a way to create a redundant or striped block device with redundancy using other physical block devices.	LVM usually sits on top of RAID blocks or even standard block devices to accomplish the same result as a partitioning, however it is much more flexible than partitions. You can create multiple volumes crossing multiple physical devices, remove physical devices without loosing data, resize the volumes, create snapshots, etc
4.	RAID is either software or a hardware technique to create data storage redundancy across multiple block devices based on required RAID levels.	LVM is a software tool to manage large pool of storage devices making them appear as a single manageable pool of storage resource. LVM can be used to manage a large pool of what we call Just-a-bunch-of-Disk (JBOD) presenting them as a single logical volume and thereby create various partitions for software RAID.

5.	RAID is NOT any kind of Data backup solution. It's a solution to prevent one of the SPOFs (Single Point of Failure) i.e. DISK failure. By configuring RAID you are just providing an emergency substitute for the Primary disk. It NEVER means that you have configured DATA backup.	LVM is a disk management approach that allows us to create, extend, reduce, delete or resize the volume groups or logical volumes.