# Hardening for Server/OS.

**Note: In this document you will see both theoretical knowledge and hands on also. So stay tuned.**

## What is OS Hardening?

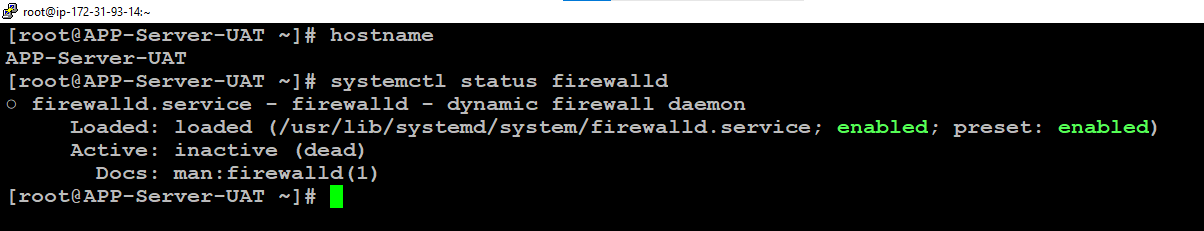
Operating system (OS) hardening, a type of [system hardening](https://perception-point.io/blog/system-hardening-guidelines-for-2022-critical-best-practices/), is the process of implementing security measures and patching for operating systems, such as Windows, Linux, or Apple OS X, to strengthen them against cyberattacks. The goal is to protect sensitive computing systems, reducing the system’s attack surface, in order to lower the risk of data breaches, unauthorized access, systems hacking, or malware.

OS hardening can include practices such as:

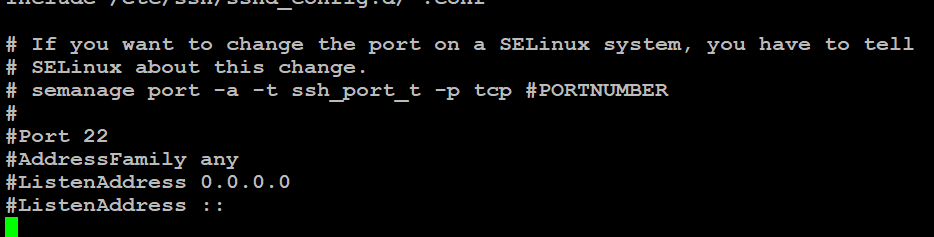
* Following security best practices and ensuring secure configuration.
* Updating the operating system, and automatically applying patches and service packs. This is typically done via software applications that MSPs or IT admins run on the system to install updates.
* Establishing strict access rules, limiting and authenticating system access permissions, and limiting creation of user accounts.
* Deploying additional security measures such as firewalls and endpoint protection systems.
* Using operating system security extensions such as AppArmor for Linux.
* Removing unnecessary applications and services and uninstalling unnecessary device drivers.
* Turning on only the ports and services required
* Encrypting the HDD or SSD that stores and hosts the OS

**Lab:**

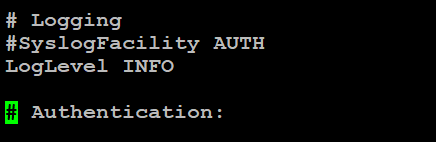
1. Check whether your machine has a hostname or not
2. Verify about the status of os-firewall: It may vary from server to server or based on the app requirement or lastly on the client/organization. For example is we have a slave caching server in in DR/HA then, firewall status could be just for formality.



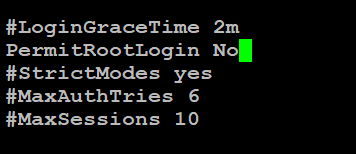
1. SSh—it has multiple parameters to check
   * Port 22 should be disabled in critical data servers and it is dependent on the domain you are hosting for.



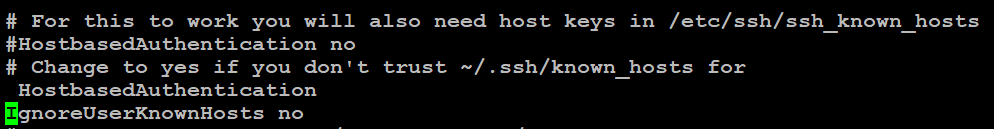
* + Logging info should be enabled to capture the logs of OS computing:



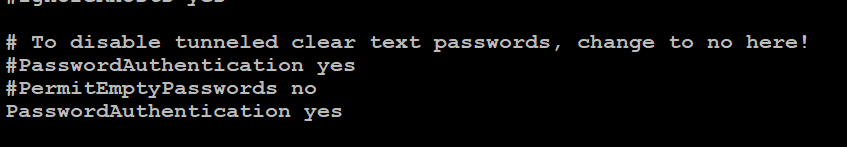
* + Root login should be disabled :



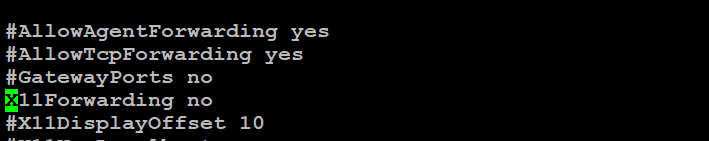
* + Host based authentication should be NO:



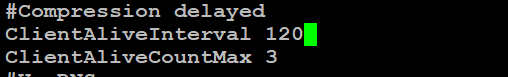
* + Password Authentication should be yes and permit empty password should be either commented or no

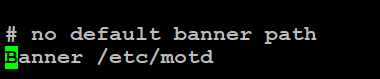
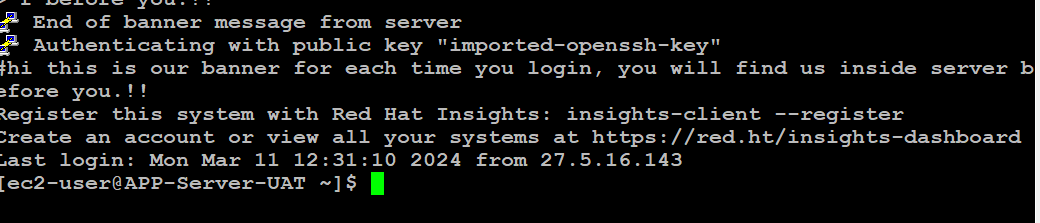


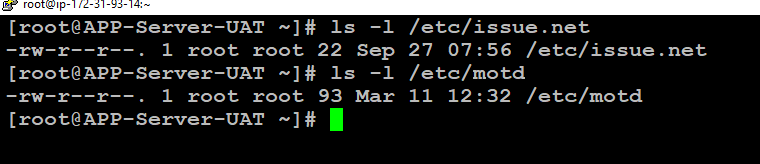
* + X11Forwarding should be no. X11Forwarding is a parameter which is useful when we try to install a package such as oracle or another db, it allows us to use a gui for those applicaitions.



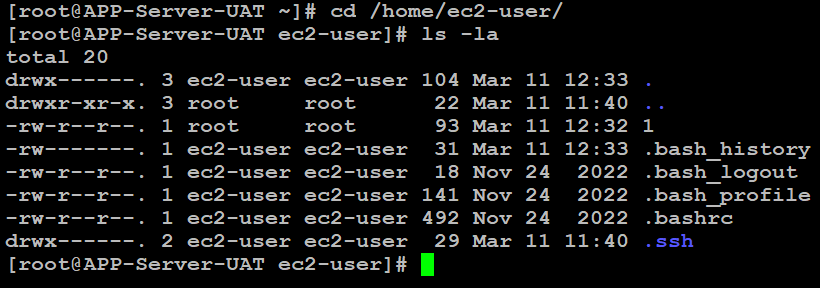
* + Most important is : ClientAliveInterval (Validates session for 120X3 = 360 sec’s i.e. 6mins)

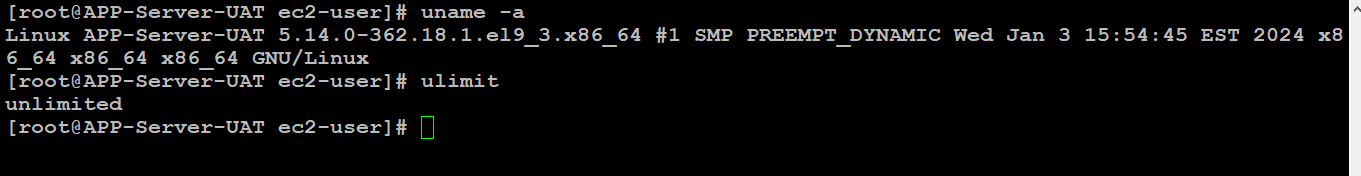
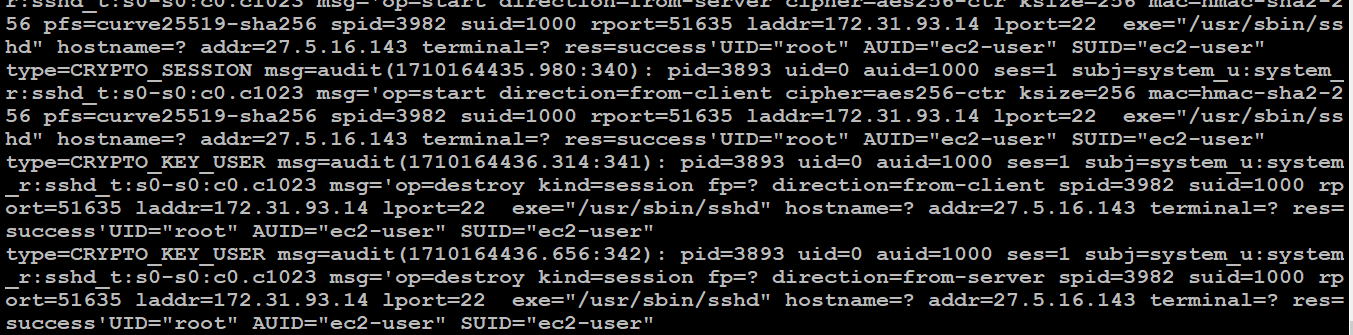


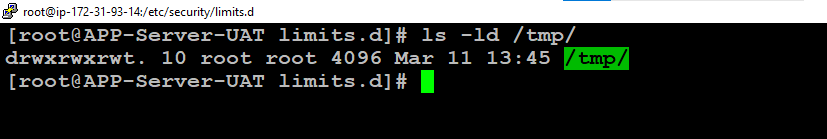
* + Banner should be enabled as when a new user logins any pre-requisites you want to mention you can also mention here. 
  + Reload ssh service: systemctl reload sshd and then duplicate the session. 
  + Only owner should have access to these following files:

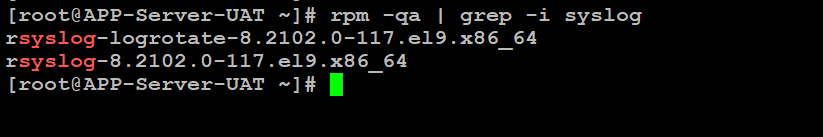


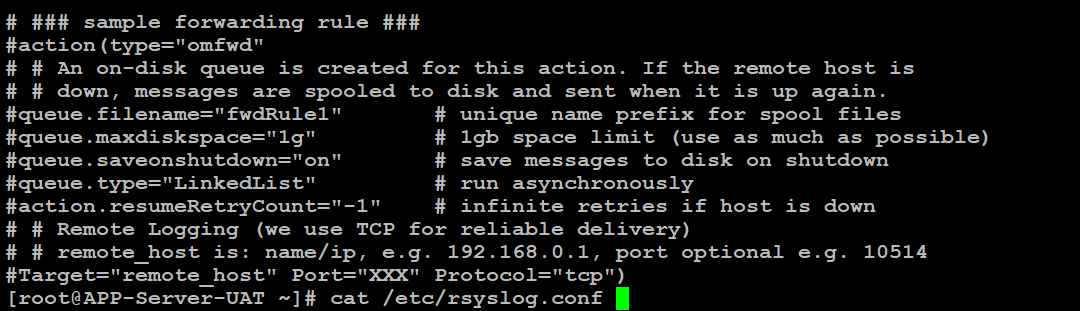
1. Only users should have read write and execute permissions in their user directories. So that if they generate any data during the middle ware dependency, rest of the linux world should not celebrate.



1. Latest kernel version should be installed and ulimit should not be unlimited unless root user:: to edit it vi this file: [root@APP-Server-UAT limits.d]# vi/etc/security/limits.d/2-0-proc.conf
2. Set audit =1 in this file: [root@APP-Server-UAT limits.d]# **cat /etc/grub2.cfg**
3. Audit logs will be reflected here afterwards**: cat /var/log/audit/audit.log**
4. Sticky bit should be enabled for /tmp: As any user should have access to create files in the tmp directory and only that user should be allowed to delete them.



1. Rsyslog packages should be present: rpm –qa| grep –I rsyslog
2. You can check cat /etc/rsyslog.conf and if you have a central logging server you can mention here by uncommenting the respective modules. Replace (remote\_host) with server ip and its port (XXX):



1. Ntpq should be installed inside your vm as it is network time protocol
2. Telnet packages should not be present if you are creating an important database server: 
3. Final take will be no other user shoud=ld have root permissions or 0 uid in /etc/passwd
4. Don’t forget to terminate/ shutdown your test servers.

# The End