1. Disable the SSH protocol version 1 from the ssh configuration.

# The default requires explicit activation of protocol 1

Protocol 2 (Uncomment Protocol 2 /etc/sshd/ssh\_config)

* 1. service sshd restart
  2. service sshd status

1. Uninstall the unused/unnecessary services if any.

[ec2-user@ip-10-158-39-154 ~]$ rpm -qa | grep auth

authconfig-6.2.8-30.el7.x86\_64

[ec2-user@ip-10-158-39-154 ~]$ rpm -qa | grep nis

libunistring-0.9.3-9.el7.x86\_64

[ec2-user@ip-10-158-39-154 ~]$ rpm -qa | grep nfs

[ec2-user@ip-10-158-39-154 ~]$ rpm -qa | grep postgres

[ec2-user@ip-10-158-39-154 ~]$ rpm -qa | grep sendmail

[ec2-user@ip-10-158-39-154 ~]$ rpm -qa | grep firewalled

1. Install and Enable the sysstat package for System Activity Report

(https://www.itadminstrator.com/2016/12/how-to-install-and-configure-sysstat.html)

* 1. yum list installed sysstat
  2. yum install sysstat -y -q && yum list installed sysstat -q
  3. systemctl enable sysstat
  4. systemctl start sysstat && systemctl status sysstat -l

1. Install and Enable the psacct which will help us monitoring the user activities reports

Enable/disable/start/stop process accounting (psacct)

* 1. yum install psacct -y
  2. service psacct start
  3. systemctl enable on
  4. service psacct status
  5. ac -d (Display the statistics for total login time)

1. Use netstat -tunlp command to check what network services are running/listening, stop the unused services using service and chkconfig commands.

Run the following to check what service are running/listening “netstat -tunlp”

1. Display SSH D2A Security Warning Banner before login: write the banner to the following file: /etc/motd

Logout and login again to see the message

core@ip-10-158-35-146 ~ $ ssh -i att\_staging.pem ec2-user@10.158.39.154

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* SSH D2A Security \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. Change ssh log level to INFO by uncomment the following line in sshd\_config:

LogLevel INFO

1. Install and configure rsyslog
2. Change the parameters in /etc/sysctl.conf for kernel hardening.
   1. Enable TCP SYN Cookie Protection - net.ipv4.tcp\_syncookies = 1
   2. Disable IP Source Routing - net.ipv4.conf.all.accept\_source\_route = 0
   3. Disable **ICMP Redirect** Acceptance - net.ipv4.conf.all.accept\_redirects = 0
   4. Enable IP Spoofing Protection - net.ipv4.conf.all.rp\_filter = 1
   5. Enable Ignoring Broadcasts Request - net.ipv4.icmp\_echo\_ignore\_broadcasts = 1
   6. Enable Logging of Spoofed **Packets, Source** Routed Packets, Redirect Packets - net.ipv4.conf.all.log\_martians = 1
   7. Disable IP forwarding- net.ipv4.ip\_forward = 1
   8. Disable source routing- net.ipv4.conf.all.accept\_source\_route = 0

To reload the vaules run below command

sysctl –system

and cross verify using below commands

[root@ip-10-158-39-154 ec2-user]# sysctl -a | grep net.ipv4.tcp\_syncookies

net.ipv4.tcp\_syncookies = 1

check with sysctl -a all the added configuration above.

1. Make sure /var/log/wtmp file exists to record the login/logout of the users and server reboots, if not create one with the touch command : touch /var/log/wtmp

ls /var/log/wtmp

/var/log/wtmp

1. (done automaticly on first install of server) Clean up all the SSH Access Keys from the system
2. Remove any custom users that are not needed
3. Allow only relevant port on /etc/sysconfig/iptables and restart iptables service after change.
4. Clean up the bash history(before creating image clean bash history) by running the following command: cat /dev/null > ~/.bash\_history