Linux hardening:

**High priority:**

* SSH
* protocol v2 – report if other than v2 ( fix script yet to be done ) – TODO Kishore ( Murali )
* How do I find out the SSH V1/V2 from CMD and trim it
* SElinux status – report if it is disabled ( fix script yet to be done ) – (Murali)
  + Getenforce ( to know the status )
  + Setenforce ( in fix script ).
  + Config file : /etc/seclinux/config
* USB Storage enable/disable - (Rahul)

Disable:

* + If usb-storage module loaded run – “modprobe –r usb-storage”
  + If /etc/modprobe.d/usb-storage.conf found - updatefile /etc/modprobe.d/usb-storage.conf to have contents “install usb-storage /bin/true”
  + Enable:
    - Check the kernel module - ="/lib/modules/`uname –r`/kernel/drivers/usb/storage/usb-storage.ko
    - Can comment out (with #) the line “install usb-storage /bin/true” – once done as soon as someone plugs in usb device it will become active – no need to reboot
* SSH root login: ( Murali )
  + Change to PermitRootLogin without-password ( modify it )
  + PermitEmptyPasswords no (add it )
* Xinetd Services: ( Rahul )
  + Verify xinetd service RPM installed ( rpm –q xinetd > /dev/null ) report if found.
  + Also check the status of the xinetd service ( service xinetd status OR systemctl status xinetd )
  + To disable / remove : stop the service ( service xinetd stop OR systemctl stop xinetd and chkconfig off xinetd )
  + Also remove the RPM from server permanently: rpm –e –nodeps xinetd
* Account must be locked/inactive after 35 days ( password expire ) ( Murali )
  + Check the following to determine the account inactive parameter from the file.
  + grep INACTIVE /etc/default/useradd
  + If it finds “-1” ( like INACTIVE=-1 ), then say, users inactive/password expiry no set.
  + TO FIX: do following:
  + Replace “INACTIVE=-1” with “INACTIVE=35” in file /etc/default/useradd
* YPSERV Services: ( Rahul )
  + Verify ypserv service RPM installed ( rpm –q ypserv > /dev/null ) report if found.
  + Also check the status of the xinetd service ( service ypserv status OR systemctl status ypserv )
  + To disable / remove : stop the service ( service ypserv stop OR systemctl stop ypserv and chkconfig off ypserv )
  + Also remove the RPM from server permanently: rpm –e –nodeps ypserv
* TFTP Services: ( Rahul )
  + Verify tftp-server service RPM installed ( rpm –q tftp-server > /dev/null ) report if found.
  + To disable / remove :
  + remove the RPM from server permanently: rpm –e –nodeps tftp-server
* Telnet Services: ( Rahul )
  + Verify telnet-server service RPM installed ( rpm –q telnet-server > /dev/null )
  + Ps –ef |grep –i telnetd , report both if they find or report if any one find.
  + To disable / remove :

|  |
| --- |
| if [ -e /etc/xinetd.d/ ]; then |
| echo '===================================================' |
| echo ' Patching GEN003850: Disable Telnet Daemon' |
| echo '===================================================' |
| for TELNETCONF in `ls /etc/xinetd.d/ | grep telnet`; do |
| if [ -e $TELNETCONF ]; then |
| sed -i 's/[[:blank:]]\*disable[[:blank:]]\*=[[:blank:]]\*no/ disable = yes/g' $TELNETCONF |
| fi |
| done |
| fi |

* + remove the RPM from server permanently: rpm –e –nodeps telnet-server
* Open LDAP Services: ( Rahul )
  + Verify telnet-server service RPM installed ( rpm –q openldap-servers > /dev/null ) report if found.
  + To disable / remove :
  + remove the RPM from server permanently: rpm –e –nodeps openldap-servers
* Account not required ( Murali )
  + We need to check following accounts active in /etc/passwd file and mention they not need
  + grep news /etc/passwd ; ( like this there are other accounts – operator,games,gopher,nfsnobody,ftp)
  + To fix this

|  |
| --- |
| echo '===================================================' |
| echo ' Disable unnecessary accounts.' |
| echo '===================================================' |
| /usr/sbin/userdel news |
| /usr/sbin/userdel operator |
| /usr/sbin/userdel games |
| /usr/sbin/userdel gopher |
| /usr/sbin/userdel nfsnobody |
| /usr/sbin/userdel ftp |

* TCP Wrappers: ( Rahul )
  + Detect if TCP wrapper installed or not

|  |
| --- |
| TCPWAPPA=$( rpm -qa | grep tcp\_wrappers | wc -l ) |
| #Start-Lockdown |
| if [ $TCPWAPPA -eq 0 ]; then |
| echo " ERROR: TCP Wrappers not installed." |
| fi |

* NIS must not be used:
  + Check if NIS is active or not
  + ps –ef |grep –I ypbind check the output, if it is runining then report NIS service running.
  + To fix

|  |
| --- |
| chkconfig --list ypbind 2>/dev/null | egrep -e '[2345]:on' |
| if [ $? -eq 0 ]; then |
| echo '===================================================' |
| echo ' Patching GEN006400: Disable NIS' |
| echo '===================================================' |
| service ypbind stop > /dev/null |
| chkconfig --level 2345 ypbind off |
| fi |

* Samba status:
  + Check if Samba is active or not
  + Rpm –qa |grep samba and ps –ef |grep –I smbd check the output, if it is runining then report Samba service running.
  + To fix

|  |
| --- |
|  |
| rpm -q samba > /dev/null |
| if [ $? -eq 0 ]; then |
| echo '===================================================' |
| echo ' Remove Samba Unless Needed' |
| echo '===================================================' |
| rpm -e --nodeps samba > /dev/null |
| fi |

* IP Forwarding:
  + Grep for following to check IP forwarding enabled or not
    - net.ipv4.ip\_forward = 0” in /etc/sysctl.conf file
    - if it find above then its disabled, don’t report
    - if it wont find that then report
    - TO FIX
    - Do following.

|  |  |
| --- | --- |
|  | sed -i "/net\.ipv4\.ip\_forward/ c\ |
|  | net.ipv4.ip\_forward = 0" /etc/sysctl.conf |

* SNMP Version checker:
  + SNMP should not use version v1,v2 and other unsecure paremters, check with below command
  + grep -E '(v1|v2c|community|com2sec)' <snmp.conf file> | grep -v '^#'
  + if it found, then report
  + TO FIX, use following logic

|  |  |
| --- | --- |
|  | SNMPCONF=/etc/snmp/snmpd.conf |
|  |  |
|  | if [ -e $SNMPCONF ]; then |
|  | echo '===================================================' |
|  | echo ' Patching GEN005305: Only SNMPv3 Allowed' |
|  | echo '===================================================' |
|  |  |
|  | V1VAR=$( cat $SNMPCONF | grep -i v1 | grep -v '^#' | wc -l ) |
|  | V2CVAR=$( cat $SNMPCONF | grep -i v2c | grep -v '^#' | wc -l ) |
|  | COMMVAR=$( cat $SNMPCONF | grep -i community | grep -v '^#' | wc -l ) |
|  | COM2VAR=$( cat $SNMPCONF | grep -i com2sec | grep -v '^#' | wc -l ) |
|  |  |
|  | #Check if the v1 SNMPCONF is in the config file |
|  | if [ $V1VAR -ne 0 ]; then |
|  | #Comment out any SNMPCONF that has v1 in it. |
|  | sed -i 's/.\*v1/#&/g' /etc/snmp/snmpd.conf |
|  | fi |
|  |  |
|  | #Check if the v2 SNMPCONF is in the config file |
|  | if [ $V2CVAR -ne 0 ]; then |
|  | sed -i 's/.\*v2c/#&/g' /etc/snmp/snmpd.conf |
|  | fi |
|  |  |
|  | #Check if the community SNMPCONF is in the config file |
|  | if [ $COMMVAR -ne 0 ]; then |
|  | sed -i 's/.\*community/#&/g' /etc/snmp/snmpd.conf |
|  | fi |
|  |  |
|  | if [ $COM2VAR -ne 0 ]; then |
|  | sed -i 's/.\*com2sec/#&/g' /etc/snmp/snmpd.conf |
|  | fi |
|  | fi |

* + Restart the snmp service using “service snmpd restart OR systemctl restart snmpd”
* Network Analysis tools disable:
  + Find following packages/rpms are installed.
  + wireshark wireshark-gnome nc tcpdump nmap
  + command : rpm –qa { wireshark wireshark-gnome nc tcpdump nmap}
  + if it find then report
  + to fix

|  |
| --- |
| for NETPKG in wireshark wireshark-gnome nc tcpdump nmap; do |
| rpm -q $NETPKG |
| if [ $? -eq 0 ]; then |
| rpm -e --nodeps $NETPKG |
| fi |
| done |
|  |
| find / -name wireshark -o -name wireshark -o -name wireshark-gnome -o -name nc -o -name tcpdump -o -name snoop -o -name tshark -o -name nmap -exec rm -f {} \; |

* RSHD Services: ( Rahul )
  + Verify rsh-server service RPM installed ( rpm –qa rsh-server > /dev/null ) report if found.
  + To disable / remove :
  + remove the RPM from server permanently: rpm –e –nodeps rsh-server
* RLOGIN Services:
  + Verify rlogin running/configured
  + Cat /etc/xinetd.d/rlogin 🡪 if this file exists and does not contain “disable = yes” then report.
  + To fix

|  |
| --- |
| RLOGIN='/etc/xinetd.d/rlogin' |
| if [ -a $RLOGIN ]; then |
| echo '===================================================' |
| echo ' Patching GEN003830: Disable rlogin Service' |
| echo '===================================================' |
| rm -f /etc/xinetd.d/rlogin |
| service xinetd restart |
| fi |

* Services:
  + IPV6 ( not enabled – report ) – Completed.

**Low Priority:**

* SSH port : report if we are using port 22 as default, suggest customer to change the defaults.
* Network run level – always ON for Runlevel 3 ( completed )