[ashleyk@awbs01 ~]$ sudo ./redhat7-security-baseline.sh check

Enter your <Password><GA Token>:

############################################################################################################

########################## **RedHat 7 Enterprise Linux Security Baseline** **###############################**

**############################################################################################################**

**################################# 3.1 PATCH MANAGEMENT ###################################**

**#-------------------------------------- 3.1 PATCH CURRENCY ------------------------------------------------#**

**#-- "Ensure all critical security related patches are applied within 30 days." : Mandatory**

#-- Checking/Fixing is out of scope of this script.

**#--** **"Ensure all non-critical security related patches are applied within 60 days." : Mandatory**

#-- Checking/Fixing is out of scope of this script.

#----------------------------------- **3.1.2 PATCH REPOSITORIES** **---------------------------------------------#**

**#-- "Ensure Telstra internal repositories are configured as the preferred source of operating system updates." : Mandatory**

#-- Checking/Fixing is out of scope of this script.

**#--** **"Verify the signature of any vendor hosted repositories prior to configuration as a software repository." : Mandatory**

#-- Checking/Fixing is out of scope of this script.

**#--** **"Verify the signature of all packages not installed using certified repositories." : Mandatory**

#-- Checking/Fixing is out of scope of this script.

**#--** **"Verify correct Red Hat GPG key is installed" : Mandatory** : ~~Not compliant : Manual fix is required~~

**COMPLIANT: SCRIPT IS NOT USING RED HAT KEY**

gpg --quiet --with-fingerprint /etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release

pub 4096R/FD431D51 2009-10-22 Red Hat, Inc. (release key 2) <security@redhat.com>

Key fingerprint = **567E 347A D004 4ADE 55BA 8A5F 199E 2F91 FD43 1D51**

pub 1024D/2FA658E0 2006-12-01 Red Hat, Inc. (auxiliary key) <security@redhat.com>

Key fingerprint = 43A6 E49C 4A38 F4BE 9ABF 2A53 4568 9C88 2FA6 58E0

<https://access.redhat.com/security/team/key> **Fingerprint:** 567E 347A D004 4ADE 55BA 8A5F 199E 2F91 FD43 1D

**#--** **"Activate gpgcheck in /etc/yum.conf" : Mandatory** : Compliant : No fix required

####################################### **3.2 BOOT** **#########################################**

**#-- "Bootloader configuration files must be owned by root" : Mandatory** : ~~Not compliant~~ **Compliant** : File /boot/grub2/grub.cfg does not exist.

**Script appears to only handle tradional BIOS configurations**

root@awbs01:/#ls -l /boot/grub2/grubenv

lrwxrwxrwx. 1 root root 25 Apr 8 15:49 /boot/grub2/grubenv -> ../efi/EFI/redhat/grubenv

**#--** **"Bootloader configuration files must be readable and writeable by root only" : Mandatory**: ~~Not compliant~~ **Compliant** : File /boot/grub2/grub.cfg does not exist.

**Script appears to only handle tradional BIOS configurations**

root@awbs01:/#ls -lL /boot/grub2/grubenv

-rwx------. 1 root root 1024 Apr 8 15:51 /boot/grub2/grubenv

**#--** **"Interactive boot (PROMPT) must be disabled" : Mandatory** : Not compliant : Fix is required

################################### **3.3 SERVICE RESTRICTION** **########################################**

**#----------------------------------- 3.3.1 SECURE BASELINE ------------------------------------------------#**

**#-- "Only necessary services are allowed at the default runlevel. All other services must be disabled."**

**: #-- Checking/Fixing is out of scope of this script.**

#---------------------------------- **3.3.2. APPLICATION STARTUP** **--------------------------------------------#**

**#-- "All third party applications must include init scripts to automate application startup and shutdown." : Mandatory**

: #-- Checking/Fixing is out of scope of this script.

**#--** **"Web based management services must be run on demand only and not enabled by default." : Mandatory**

: #-- Checking/Fixing is out of scope of this script.

#------------------------------- **3.3.3. EXPLICITLY DENIED SERVICES**  **---------------------------------------#**

**#-- "The following services must not be enabled on any RHEL host: Rsyncd (daemon mode), Automounting (autofs),**

**#-- "Telnet, FTP, TFTP, NIS/NIS+, r-services (rshd, rlogind, etc)**

**#-- "Historical services: echo, chargen, pcnfsd, finger, discard, daytime, rexecd, rstatd, rusersd, rwalld,**

**#-- "sprayd, uucp, comstat, talk, systat, netstat, time, tcpmux "# : Mandatory** : Compliant - No fix required

#------------------------------------------- **3.3.4. SNMP**  **-------------------------------------------------#**

**#-- "Where SNMP is required by management applications then it should be configured as follows:**

**#-- Community Name: "Must follow the Telstra Non-Personal Account Password Standard: Mandatory**

**#-- Access Level:**  **"Read-only access (no R/W): Mandatory**

**#-- Trap destinations:**  **"Two trap servers should be defined at a minimum: Optional**

**#-- Security:**  **"Access control should only allow SNMP access from Management host(s): Mandatory**

**#-- Security:**  **"Ensure permissions on the file /etc/snmp/snmpd.conf have a minimum of mode 640: Mandatory**

**#-- Security:**  **"Ensure permissions on all Management Information Base (MIB) files have a minimum of mode 640: Mandatory**

**#-- SNMP version:**  **"SNMPv3 should be used with both authentication and encryption options enabled: Mandatory\***

**#--** **"\* Where supported by the application "**

**\*\*\*\*\* File /etc/snmp/snmpd.conf does not exist. Verify that SNMP is installed \*\*\*\*\***

**SNMP is not installed**

#----------------------------------------- **3.3.5. SMTP**  **---------------------------------------------------#**

**#-- "Configure Mail Transfer Agent for local-only mode (inet\_interfaces = localhost in /etc/postfix/main.cf): Mandatory\***" : Not Compliant : Manual fix is required

**#--** **"\* Unless the hosts specific function is to act as a mail server "**

**SMTP is not installed**

**######################################### 3.4 SYSTEM #############################################**

**#------------------------------- 3.4.1 EXPLICITLY DENIED APPLICATIONS -------------------------------------#**

**#-- "Avahi must be disabled." : Mandatory : Not compliant** :

\*\*\*\*\* File /etc/systemctl-avahi does not exist. Verify that Avahi is installed \*\*\*\*\*

**Avahi is not installed**

**#--** **"X-Window server must not be installed." : Mandatory**

**#-- Checking/Fixing is out of scope of this script.**

**Systems configure with iptables/firewalld**

######################################### **3.5. NETWORK** **#############################################**

**#---------------------------------- 3.5.1 INSTALLED PROTOCOLS ---------------------------------------------#**

**#-- "Internet Protocol (IP) is the only installed network protocol" : Mandatory**

#-- Checking/Fixing is out of scope of this script.

**#--**  **"IP addresses statically assigned to host" : Mandatory** : Not compliant : Manual fix is required

sysctl: cannot stat /proc/sys/net/ipv6/conf/all/disable\_ipv6: No such file or directory

**ipv6 is disabled, static ipv4**

**#--**  **"IPv6 disabled": Mandatory\*** : Compliant : No fix required

**#--**  **"\* Unless the host explicitly requires IPv6 for its function, and has been included in the relevant**

**firewalls and consciously setup, all IPv6 service bindings and logical interfaces should be shut down"**

**#---------------------------------------- 3.5.2 IPTABLES --------------------------------------------------#**

**#-- "Enable and configure IPTABLES" : Optional**

#-- Checking/Fixing is out of scope of this script.

#-------------------------------- **3.5.3 /ETC/SYSCTL.CONF SETTINGS** **-----------------------------------------#**

**#-- "net.ipv4.conf.all.accept\_redirects = 0" : Mandatory** : Not compliant : Fix is required

**#-- "net.ipv4.conf.all.accept\_source\_route = 0" : Mandatory** : Not compliant : Fix is required

**#-- "net.ipv4.conf.all.secure\_redirects = 0" : Mandatory** : Not compliant : Fix is required

**#-- "net.ipv4.conf.all.send\_redirects = 0" : Mandatory** : Not compliant : Fix is required

**#-- "net.ipv4.conf.default.accept\_redirects = 0" : Mandatory** : Not compliant : Fix is required

**#-- "net.ipv4.conf.default.accept\_source\_route = 0" : Mandatory** : Not compliant : Fix is required

**#-- "net.ipv4.conf.default.secure\_redirects = 0" : Mandatory** : Not compliant : Fix is required

**#-- "net.ipv4.ip\_forward = 0" : Mandatory** : Compliant : Not fix required

**#-- "net.ipv4.conf.all.rp\_filter = 1" : Mandatory** : Not compliant : Fix is required

**#-- "net.ipv4.conf.default.rp\_filter = 1" : Mandatory** : Not compliant : Fix is required

**#-- "net.ipv4.icmp\_echo\_ignore\_broadcasts = 1" : Mandatory** : Not compliant : Fix is required

**#-- "net.ipv4.icmp\_ignore\_bogus\_error\_responses = 1" : Mandatory** : Not compliant : Fix is required

**#-- "net.ipv4.tcp\_syncookies = 1" : Mandatory** : Not compliant : Fix is required

**#-- "net.ipv4.conf.all.log\_martians = 1" : Optional** : Not compliant : Not fix required

**#-- "net.ipv4.conf.default.log\_martians = 1" : Optional** : Not compliant : Not fix required

**#-- "net.ipv4.conf.default.send\_redirects = 0" : Optional** : Not compliant : Not fix required

**#-- "net.ipv4.tcp\_max\_syn\_backlog = 4096" : Optional** : Not compliant : Not fix required

################################### **3.6. LOGGING** **########################################**

**#---------------------------------------- 3.6.1. STORAGE --------------------------------------------------#**

**#-- "Critical system logs stored securely off-host" : Optional**

#-- Checking/Fixing is out of scope of this script.

**Critical logs sent by rsyslog to offhost server**

#-------------------------------------- **3.6.2. TCP WRAPPERS** **-----------------------------------------------#**

**#-- "User TCP Wrapper connection logging" : Mandatory**

#-- Checking/Fixing is out of scope of this script.

#---------------------------------- **3.6.3. SYSLOG AUTH MESSAGES** **-------------------------------------------#**

**#-- "Configure syslog to capture logging information sent to the AUTHPRIV facility" : Mandatory** : Not compliant : Fix is required

#------------------------------------- **3.6.4. RECORD LOGINS** **-----------------------------------------------#**

**#-- "Files /var/run/utmp and /var/log/wtmp must exist" : Mandatory**

**#-- "File /var/run/utmp" : Compliant** : No fix required

**#-- "File /var/log/wtmp" : Compliant** : No fix required

#------------------------------ **3.6.5. CAPTURE ALL FAILED LOGIN ATTEMPTS** **----------------------------------#**

**#-- "/var/log/faillog must exist with permission 0600 \*" : Mandatory** : Not compliant : Fix is required

**File does notexist. Details logged to /var/log/Secure,/var/log/Messages and to of host server**

**#-- "/var/log/btmp must exist with permission 0600 \*" : Mandatory** : Compliant : No fix required

**#-- "\* for systems, not using pam\_tally2"**

**#------------------------------------- 3.6.6. CRON LOGGING ------------------------------------------------#**

**#-- "Cron must log all jobs run" : Mandatory** : Not compliant : Fix is required

No cronjobs. Systemd timers are used. Details logged in /var/log/messages

#----------------------------------- **3.6.7. SYSTEM ACCOUNTING** **---------------------------------------------#**

**#-- "Enable system accounting (auditd)" : Mandatory** : Compliant : No fix required

**#-- "Audit max log file = 10Mb or more" : Mandatory** : Not compliant : Fix required

**#-- "Configure auditd to record time modification" : Mandatory** : Not Compliant : Fix required

**#-- "Configure auditd to record user/group modification" : Mandatory** : Not Compliant : Fix required

**#-- "Configure auditd to record MAC modification" : Mandatory** : Not Compliant : Fix required

**#-- "Configure auditd to record logins/logouts" : Mandatory** : Not Compliant : Fix required

**#-- "Configure auditd to record session events" : Mandatory** : Not Compliant : Fix required

**#-- "Configure auditd to record DAC events" : Mandatory** : Not Compliant : Fix required

**#-- "Configure auditd to record unauthorized access" : Optional** : Not Compliant : No Fix required

**#-- "Configure auditd to record privileged commands events" : Mandatory** :

#-- Checking/Fixing is out of scope of this script.

**#-- Add the output of the command: df --local -P | awk {&apos;if (NR!=1) print $6&apos;} | xargs -I &apos;{}&apos; find &apos;{}&apos; -xdev \( -perm -4000 -o -perm -2000 \) -type f | awk &apos;{print "-a always,exit -F path="$1" -F perm=x -F auid>=500 -F auid!=4294967295 -k privileged" }&apos;**

**#-- to the file: /etc/audit/audit.rules**

**#-- "Configure auditd to record mount events" : Mandatory** : Not Compliant : Fix required

**#-- "Configure auditd to record sudo modifications" : Mandatory** : Not Compliant : Fix required

**#-- "Configure auditd to record kernel module loading" : Mandatory** : Not Compliant : Fix required

**#-- "Make audit.log immutable" : Mandatory** : Not Compliant : Fix required

#------------------------------------- **3.6.8. LOG RETENTION** **-----------------------------------------------#**

**#-- "Minimum period logs must be kept for production systems: 12 months" : Mandatory**

#-- Checking/Fixing is out of scope of this script.

**#-- "Minimum period logs must be kept for non-production systems: 2 months" : Mandatory**

#-- Checking/Fixing is out of scope of this script.

################################ **3.7. FILESYSTEMS AND PARTITIONS** **########################################**

**FileSystem layout preconfigured in Redhat VM template.**

**#-- "Create separate partition for /tmp" : Mandatory** : Compliant : No fix required

**#-- "Set nodev, nosuid, noexec options for /tmp" : Mandatory** : Compliant : No fix required

**#-- "Create separate partition for /var" : Mandatory** : Compliant : No fix required

**#-- "Bind mount the /var/tmp directory to /tmp" : Mandatory** : Not Compliant : Manual fix is required

**#-- "Create separate partition for /var/log" : Mandatory** : Not Compliant : Manual fix is required

**#-- "Create separate partition for audit (/var/audit)" : Optional** : Not Compliant : Manual fix might be needed

**#-- "Create separate partition for /home" : Mandatory** : Compliant : No fix required

**#-- "Set nodev option for /home" : Mandatory** : Not Compliant : Fix is required

**#-- "Add nodev, nosuid, noexec options to /dev/shm partition" : Mandatory** : Compliant : No fix is required

############################## **3.8. FILE AND DIRECTORY PROTECTIONS** **########################################**

**#------------------------------- 3.8.1. WORLD-WRITABLE DIRECTORIES ----------------------------------------#**

**#-- ""Sticky" permission bit set on /tmp and /var/tmp" : Mandatory** : Compliant : No fix is required

**#-- ""Sticky" permission bit set on all world-writable directories" : Optional\***

: #-- Checking/Fixing is out of scope of this script.

**#-- \* Consult appropriate vendor documentation before blindly applying the sticky bit to**

**#-- any world writable directories in order to avoid breaking any application dependencies on a given directory**

**#------------------------------------ 3.8.2. OSR PROTECTION -----------------------------------------------#**

**#-- "All operating system resources (OSR) must be protected from unauthorized changes." : Mandatory**

#-- Checking/Fixing is out of scope of this script.

#-------------------------------------- **3.8.3. DEVICE FILES** **-----------------------------------------------#**

**#-- "All device files must exist under /dev or /selinux" : Mandatory**

#-- Checking/Fixing is out of scope of this script.

#--------------------------------- **3.8.4. USER HOME DIRECTORIES** **-------------------------------------------#**

**#-- "The minimum permission on user home directories set to 0750" : Mandatory**

#-- Important: The accounts&apos; home directory might content documents/scripts/data that could compromise the security of the system

#-- For all directories found not to be compliant, make sure that sensitive data has not been exposed. Check the .dot files

#-- and change the passwords of the owner accounts of those directories. Please consult your Security SME for additionals steps to follow

**#--**  **root : /root : Compliant** : No fix required

**#--**  **sxcadmin : /home/sxcadmin : Compliant** : No fix required

**#--**  **opsmgrsvc : /home/opsmgrsvc : Compliant** : No fix required

**#--**  **ashleyk : /home/ashleyk : Compliant** : No fix required

**#--**  **peterb : /home/peterb : Compliant** : No fix required

**#--**  **pattik : /home/pattik : Compliant** : No fix required

**#--**  **carols : /home/carols : Compliant** : No fix required

**#-- "Users must own their own home directory" : Mandatory**

#-- Important: The accounts&apos; home directory might content documents/scripts/data that could compromise the security of the system

#-- For all directories found not to be compliant, make sure that sensitive data has not been exposed. Check the .dot files

#-- and change the passwords of the owner accounts of those directories. Please consult your Security SME for additionals steps to follow

**#--**  **root : /root : Compliant** : No fix required

**#--**  **sxcadmin : /home/sxcadmin : Compliant** : No fix required

**#--**  **opsmgrsvc : /home/opsmgrsvc : Compliant** : No fix required

**#--**  **ashleyk : /home/ashleyk : Compliant** : No fix required

**#--**  **peterb : /home/peterb : Compliant** : No fix required

**#--**  **pattik : /home/pattik : Compliant** : No fix required

**#--**  **carols : /home/carols : Compliant** : No fix required

#------------------------------------ **3.8.5. USER DOT FILES** **-----------------------------------------------#**

**#-- "The required permission on user dot files is 0700" : Mandatory**

#-- Important: The dot files in accounts&apos; home directory might content passwords and other data that could compromise the security of the system

#-- For all directories found not to be compliant, make sure that sensitive data has not been exposed. Check the .dot files

#-- and change the passwords of the owner accounts of those directories. Please consult your Security SME for additionals steps to follow

**#-- " Account: root : Compliant** : No fix required

**#-- " Account: sxcadmin : Compliant** : No fix required

**#-- " Account: opsmgrsvc : Compliant** : No fix required

**#-- " Account: ashleyk : Compliant** : No fix required

**#-- " Account: peterb : Compliant** : No fix required

**#-- " Account: pattik : Compliant** : No fix required

**#-- " Account: carols : Compliant** : No fix required

**#-- ".netrc and .rhosts files are expressly forbidden" : Mandatory**

**#-- " Account: root : Compliant** : No fix required

**#-- " Account: sxcadmin : Compliant** : No fix required

**#-- " Account: opsmgrsvc : Compliant** : No fix required

**#-- " Account: ashleyk : Compliant** : No fix required

**#-- " Account: peterb : Compliant** : No fix required

**#-- " Account: pattik : Compliant** : No fix required

**#-- " Account: carols : Compliant** : No fix required

**#-- ".forward file is forbidden" : Optional**

**#-- " Account: root : Compliant** : No fix required

**#-- " Account: sxcadmin : Compliant** : No fix required

**#-- " Account: opsmgrsvc : Compliant** : No fix required

**#-- " Account: ashleyk : Compliant** : No fix required

**#-- " Account: peterb : Compliant** : No fix required

**#-- " Account: pattik : Compliant** : No fix required

**#-- " Account: carols : Compliant** : No fix required

#------------------------------------- **3.8.6. MISCELLANEOUS** **-----------------------------------------------#**

**#-- "All files must be owned by a valid group and user" : Mandatory** : This checking is done in section 3.12.1 File integrity verification

##################################### **3.9. SYSTEM ACCESS** **###########################################**

**#---------------------------------- 3.9.1. DISABLE SERIAL LOGINS ------------------------------------------#**

**#-- "Disable logins enabled on serial ports except for system console." : Mandatory** : - Manual fix required

**Not explicitly disabled via grub (8250.nr\_uarts=0), Access is Administratively prohibited via /etc/securetty and PAM**

#--------------------------------- **3.9.2. SECURE CONSOLE ACCESS** **-------------------------------------------#**

**#-- "Ensure system console is physically secure" : Mandatory**

#-- Checking/Fixing is out of scope of this script.

**Access is Administratively prohibited via /etc/securetty and PAM**

**Root login via console is disabled. Only LT Admin can login on console using 2FA. LT Admin can sudo to root using 2FA**

#------------------------------------- **3.9.3. CONFIGURE SSH** **-----------------------------------------------#**

**##############################################################################################################**

**################################### OPENSSH SECURITY BASELINE ##########################################**

**##############################################################################################################**

**############################## 4. COMMON SECURITY REQUIREMENTS #######################################**

**#--------------------------------- 4.1. PROTOCOLS AND ALGORITHMS --------------------------------------------#**

**#-- "Use only SSH Protocol 2 (or newer). Disable SSH Protocol 1" : Mandatory** : Compliant : No fix required

#------------------------------------------ **4.1. FEATURES**  **--------------------------------------------------#**

**#------------------------------------- 4.2.1. SERVER FEATURES -----------------------------------------------#**

**#-- "Configure Idle Log Out Timeout Interval" : Mandatory** : ~~Not compliant : Fix is required~~

**LT Admin user Idle times are managed administratively outside of business hours.**

**#-- "Enable Maximum authentication attempts" : Mandatory** : Not compliant : Fix is required

**3 Attempts allowed before disconnection. Authentication requires KeyPair with mandatory passphrase(empty passphrases administratively dissallowed),Password+Google Authentication otp**

**#-- "Disable .rhosts Files. Don’t read the user’s ~/.rhosts and ~/.shosts ssh\_serv\_file" : Mandatory** : Compliant : No fix required

**#-- "Disable Host-Based Authentication" : Optional** : Compliant : No fix required

**#-- "Root login is not allowed for auditing reasons. Disable root Login via SSH" : Mandatory** : Compliant : No fix required

**#-- "Disable Use of X11Forwarding" : Optional** : Compliant : No fix required

**#-- "DNS hostname checking" : Optional** : Not compliant : No fix required

**Deliberately disabled. Use of internal N/W with managed IPs negates use of DNS.**

**#-- "Disable Empty passwords" : Mandatory** : Compliant : No fix required

**#-- "Enable Public key authentication. If all users are using PublicKey Auth disable Password" : Optional** : Not compliant : No fix required

**LT Admin : Multifactor authentication -**

**KeyPair with mandatory passphrase(empty passphrases administratively dissallowed),Password+Google Authentication otp**

**#-- "Enable Tesltra’s legal Warning Banner" : Mandatory** : Not compliant : Fix is required

**Banner is displayed on Bastion server only**

**#-- "Enable StrictMode" : Mandatory** : Not compliant : Fix is required

**File modes and ownership of the user's files and home directory are controlled at administrative level**

**#-- "LogLevel VERBOSE logs user&apos;s key fingerprint on login." : Optional** : Not compliant : No fix required

**#-- "Password based logins are disabled where possible" : Optional**: Not compliant : No fix required

**Incorrectly assessed by script. Password based logins are disabled. All IPND users accounts are password locked. TTY access is disabled**

**#-- "Log sftp level ssh\_serv\_file access" : Optional** : Not compliant : No fix required

**Incorrectly assessed by script. All SSH based access is logged vis systemd**

**#-- "Use kernel sandbox mechanisms where possible in unprivileged processes" : Mandatory** : Compliant : No fix required

**#-- "Use of AuthorizedKeysCommand requires AuthorizedKeysCommandUser to be set to a unprivileged user" : Mandatory** : Compliant : No fix required

#------------------------------------- **4.2.2. CLIENT FEATURES** **-----------------------------------------------#**

**#-- "Ensure KnownHosts are unreadable if leaked" : Optional** : Not compliant : No fix required

**#-- "Check the host IP address in the known\_hosts file" : Optional** : Not compliant : No fix required

**#-- "Disable UseRoaming" : Optional** : Not compliant : No fix required

**Incorrectly assessed by script. Roaming is disabled in ssh\_config: UseRoaming no**

**#-- "Do not use Agent Forwarding" : Mandatory** : Compliant : No fix required

#--------------------------------------- **4.4. KEYS MANAGEMENT** **-----------------------------------------------#**

**#-- "Remove old Host keys: "/etc/ssh/ssh\_host\_dsa\_key" and "/etc/ssh/ssh\_host\_key"" : Mandatory** : Compliant : No fix required

#--------------------------------------- **4.5. .SSH/CONFIG SERVER** **--------------------------------------------#**

**#---------------------------------- 4.5.1. MODERN (OPENSSH 6.7+) --------------------------------------------#**

**#-- "Supported HostKey algorithms by order of preference:**

**"HostKey /etc/ssh/ssh\_host\_ed25519\_key", "HostKey /etc/ssh/ssh\_host\_ecdsa\_key" and "HostKey /etc/ssh/ssh\_host\_rsa\_key"" : Mandatory** : Not compliant : Fix is required

**Incorrectly assessed by script. HostKey ordering is as listed**

**#-- "Specify the available Key Exchange algorithms:**

**curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-nistp256" : Mandatory** : Compliant : No fix required

**#-- "Specify the allowed ciphers: chacha20-poly1305@openssh.com,aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr" : Mandatory** : Compliant : No fix required

**#-- "Specify the available message authentication code algorithms:**

**MACs hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-512,hmac-sha2-256,umac-128@openssh.com" : Mandatory** : Compliant : No fix required

#-------------------------------- **4.5.2. INTERMEDIATE (OPENSSH 5.3)** **-----------------------------------------#**

**#-------------------------------- 4.5.2. Section not applicable to Red Hat 7 --------------------------------#**

**#---------------------------------------- 4.6. SSH/CONFIG CLIENT --------------------------------------------#**

**#---------------------------------- 4.6.1. MODERN (OPENSSH 6.7+) --------------------------------------------#**

**BUGGY SCRIPT. THIS IS A REPEAT OF PREVIOUS SECTION 4.5.1 with different results**

**#-- "Specify Host keys by order of preference: ssh-ed25519-cert-v01@openssh.com,ssh-rsa-cert-v01@openssh.com,ssh-ed25519,ssh-rsa,ecdsa-sha2-nistp521-cert-v01@openssh.com,ecdsa-sha2-nistp384-cert-v01@openssh.com,ecdsa-sha2-nistp256-cert-v01@openssh.com,ecdsa-sha2-nistp521,ecdsa-sha2-nistp384,ecdsa-sha2-nistp256" : Mandatory** : Not compliant : Fix is required

**Incorrectly assessed by script. HostKey ordering is as listed**

**#-- "Specify the available Key Exchange algorithms:**

**curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-nistp256" : Mandatory** : Not compliant : Fix is required

**Incorrectly assessed by script. Key Exchange algorithms as listed**

**#-- "Specify the allowed ciphers: chacha20-poly1305@openssh.com,aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr" : Mandatory** : Not compliant : Fix is required

**Incorrectly assessed by script. Ciphers as listed**

**#-- "Specify the available message authentication code algorithms:**

**MACs hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-512,hmac-sha2-256,umac-128@openssh.com" : Mandatory** : Not compliant : Fix is required

**Incorrectly assessed by script. MACs as listed**

#-------------------------------- **4.6.2. INTERMEDIATE (OPENSSH 5.3)** **-----------------------------------------#**

**#-------------------------------- 4.6.2. Section not applicable to Red Hat 7 --------------------------------#**

**#--------------------------------- 3.9.4. DISABLE RHOSTS SUPPORT ------------------------------------------#**

**#-- "Permanently disable .rhosts support (via PAM)" : Mandatory** : - Manual fix required

**rsh not installed, ALL allowed terminals disabled in securetty, No rlogon/rhosts entries in any pam files**

#-------------------------------- **3.9.5. DEFAULT LOGIN SETTINGS** **-------------------------------------------#**

**#-- "UMASK: 027" : Mandatory** : Not compliant : Fix is required

**UMASK is 027 for LT Admin Users**

**#-- "FAIL\_DELAY: 4" : Mandatory** : Not compliant : Fix is required

#------------------------------------- **3.9.6. SESSION TIMEOUTS** **--------------------------------------------#**

**#-- "For GUI sessions, the server should automatically lock after 10 minutes of no activity and require a password to unlock" : Mandatory**

#-- Checking/Fixing is out of scope of this script.

**#-- "Interactive logins to a shell must automatically log out after 10 minutes of inactivity" : Mandatory** : Not compliant : Fix is required

**LT Admin user Idle times are managed administratively outside of business hours.**

#-------------------------------------- **3.9.7. CRON/AT ACCESS** **---------------------------------------------#**

**#-- "Only authorized users have access to command scheduling" : Mandatory**

#-- Checking/Fixing is out of scope of this script.

**#-- "cron.allow and at.allow files exist" : Mandatory** : Compliant : No fix required

**#-- "cron.deny and at.deny files do not exist" : Mandatory** : Not compliant : Fix is required

**Incorrectly assessed by script. Files exist**

**#-- "set owner root:root, permission 0600 to /etc/at.allow" : Mandatory** : Compliant : No fix required

**#-- "Permissions on individual and system crontab files set to 0400" : Mandatory** : - Manual fix required

**#-- "set to owner root:root , permission 0700 to the following:" : Mandatory**

**#-- "/var/spool/cron" : Mandatory** : Compliant : No fix required

**#-- "/etc/cron.hourly" : Mandatory** : Compliant : No fix required

**#-- "/etc/cron.daily" : Mandatory** : Compliant : No fix required

**#-- "/etc/cron.weekly" : Mandatory** : Compliant : No fix required

**#-- "/etc/cron.monthly" : Mandatory** : Compliant : No fix required

**#-- "/etc/cron.d" : Mandatory** : Compliant : No fix required

**#**------------------------------ **3.9.8. SINGLE USER MODE ACCESS** **--------------------------------------------#**

**#-- "Booting the system to single user mode must require a password" : Mandatory** : Not compliant : Fix is required

#---------------------------------- **3.9.9. PRIVILEGE ESCALATION** **-------------------------------------------#**

**ALL sudo access is administratively configured to require 2FA**

**#-- "Account names created must adhere to the System Identifier Framework (001 785)" : Mandatory**

#-- Checking/Fixing is out of scope of this script.

**#-- "User passwords must follow the Telstra Personal Account Password Standard (013 582)" : Mandatory**

#-- Checking/Fixing is out of scope of this script.

############################# **3.10. USER ACCOUNTS AND ENVIRONMENT** **##################################**

**#---------------------------------- 3.10.1. ACCOUNT REGISTRATION ------------------------------------------#**

**#-- "Account names created must adhere to the System Identifier Framework (001 785)" : Mandatory**

#-- Checking/Fixing is out of scope of this script.

**#-- "User passwords must follow the Telstra Personal Account Password Standard (013 582)" : Mandatory**

#-- Checking/Fixing is out of scope of this script.

#------------------------------- **3.10.2. DISABLE SYSTEM ACCOUNTS** **------------------------------------------#**

**#-- "The following standard system accounts should be locked to ensure they cannot login or run an interactive shell:**

**bin daemon adm lp mail uucp operator games gopher ftp nobody nscd vcsa pcap ntp dbus avahi rpc mailnull smmsp sshd xfs**

**rpcuser haldaemon avahi-autoipd gdm sabayon man news postfix " : Mandatory** : Compliant : No fix required

#---------------------------- **3.10.3. DEFAULT PASSWORD SETTINGS** **-------------------------------------------#**

**#-- "PASS\_MAX\_DAYS (/etc/login.defs): 90" : Mandatory** : Compliant : No fix required

**#-- "PASS\_WARN\_AGE (/etc/login.defs): 14" : Mandatory** : Compliant : No fix required

**#-- "Password hashing: SHA512" : Mandatory** : Compliant : No fix required

**#-- "Password history: 10" : Mandatory** : Compliant : No fix required

**#-- "Minimum password length: 12 (it also checks/applies password complexity)" : Mandatory** : Compliant : No fix required

**#-- "Dictionary check: On" : Mandatory** : ~~Not compliant : Fix is required~~

**Pointless given the complexity rules. Passwords required as part of MFA: KeyPair passphrase(empty passphrases administratively disallowed), Password+Google Authentication otp**

**#-- "pam\_pwcheck or pam\_cracklib modules must be used to check password strength: Required" : Mandatory** :

#-- Not applicable : pam\_pwquality module is used to check password strength.

**#-- "Ensure all users last password change date is in the past" : Mandatory** : Manual fix might be required

#------------------------------- **3.10.4. ROOT ACCOUNT PROTECTIONS** **------------------------------------------#**

**#-- Important: The root account is of utmost importance in the system. If found that the following setting is not compliant,**

#-- it is possible that this host might have been compromised. Please contact your Security SME immediately to notify of

#-- this issue. This script will not fix this issue.

**#-- "Root’s default group must be group “root” (GID 0)" : Mandatory** : Compliant : No fix required

#-- Important: The root account is of utmost importance in the system. If found that the following setting is not compliant,

#-- it is possible that this host might have been compromised. Please contact your Security SME immediately to notify of

#-- this issue.

**#-- "Root’s home directory must be /root, root-owned, mode 0700" : Mandatory** : Compliant : No fix required

#-- Important: The root account is of utmost importance in the system. If found that the following setting is not compliant,

#-- it is possible that this host might have been compromised. Please contact your Security SME immediately to notify of

#-- this issue.

**#-- "Root’s PATH must not contain the current working directory (.)" : Mandatory** : Compliant - No fix required

#-- Important: The root account is of utmost importance in the system. If found that the following setting is not compliant,

#-- it is possible that this host might have been compromised. Please contact your Security SME immediately to notify of

#-- this issue.

**#-- "Root’s PATH must not contain directories writable by other than root" : Mandatory** : Compliant - No fix required

#-- Important: The root account is of utmost importance in the system. If found that the following setting is not compliant,

#-- it is possible that this host might have been compromised. Please contact your Security SME immediately to notify of

#-- this issue. This script will not fix this issue.

**#-- "No other accounts except root have UID 0" : Mandatory** : Compliant - No fix required

**#-- "Root account password known only to a minimal group of operationally responsible system administrators" : Mandatory**

#-- Checking/Fixing is out of scope of this script.

**#-- "Direct login as root is not permitted except on the system console" : Mandatory** : Compliant : No fix required

#---------------------------------- **3.10.5. LOGIN ENVIRONMENT** **----------------------------------------------#**

**#-- "Set “mesg n” in system-wide login scripts" : Mandatory** : Not compliant - Fix is required

**#-- "Set traps on signals 1,2, & 3 in system-wide login scripts" : Mandatory** : Not implemented yet

**#-- "Date and time of last successful login displayed" : Mandatory** : Not compliant - Fix is required

**Incorrectly assessed by script. Date, Time and IP of last login details displayed**

#-------------------------------- **3.10.6.LOCK INACTIVE USER ACCOUNTS** **----------------------------------------#**

**#-- "Accounts should be locked after 90 days of inactivity" : Optional**

**#-- root**  : Not compliant : No fix required

**#-- sxcadmin**  : Not compliant : No fix required

**#-- opsmgrsvc**  : Not compliant : No fix required

**#-- ashleyk**  : Not compliant : No fix required

**#-- peterb**  : Not compliant : No fix required

**#-- pattik**  : Not compliant : No fix required

**#-- carols**  : Not compliant : No fix required

#-------------------------------------- **3.10.7. ACCOUNT LOCKING** **---------------------------------------------#**

**#-- "Lock out users after 5 unsuccessful consecutive login attempts" : Mandatory** : Not compliant : Fix is required

**3 Attempts allowed before disconnection. Passwords required as part of MFA: KeyPair passphrase(empty passphrases administratively disallowed), Password+Google Authentication otp.**

**Setting this could be problematic if there are temporary drifts with realtime clocks on client and server.**

#--------------------------- **3.10.8. CENTRALIZED AUTHENTICATION AND AUTHORIZATION** **---------------------------#**

**#-- "Centralize user authentication using LDAPS or Kerberos" : Optional** : #-- Checking/Fixing is out of scope of this script.

**#-- "Centralize user authorization using LDAPS" : Optional** : #-- Checking/Fixing is out of scope of this script.

#------------------------------------- **3.11. WARNING BANNERS** **------------------------------------------------#**

**#-- This script checks against an example of a warning banner provided in the RedHat 7 Linux Security Baseline**

#-- to be written in /etc/issue. However, it is not required to have exactly the same banner. Use the file

#-- /etc/issue to comply with the following settings.

**#-- "Appropriate warning banners exist for standard login services" : Mandatory** : It requires manual checking/fixing

**#-- "Appropriate warning banners exist for GUI login services" : Mandatory** : It requires manual checking/fixing

**#-- "Appropriate warning banners exist for application login services" : Mandatory** : It requires manual checking/fixing

#-- The file /etc/issue does not contain the warning banner example. : Not compliant

################################## **3.12. SYSTEM MAINTENANCE** **########################################**

**#------------------------------------ 3.12.1. FILE INTEGRITY VERIFICATION -----------------------------------#**

**#-- "Integrity of installed files must be regularly verified against RPM database" : Optional**

#-- Checking/Fixing is out of scope of this script.

#-- Important: The /etc/passwd file contains important settings about user accounts in the host.

#-- If found that the following setting is not compliant, it is possible that this host might have been compromised.

#-- Please contact your Security SME immediately to notify ofthis issue.

**#-- "/etc/passwd permissions = 644, owned by root:root" : Mandatory** : Compliant - No fix required

#-- Important: The /etc/shadow file contains sensitive data about user accounts in the host.

#-- If found that the following setting is not compliant, it is highly likely that this host has been compromised.

#-- Please contact your Security SME immediately to notify ofthis issue.

**#-- "/etc/shadow permissions = 000, owned by root:root" : Mandatory** : Compliant - No fix required

#-- Important: The /etc/gshadow file contains sensitive data about group accounts in the host.

#-- If found that the following setting is not compliant, it is highly likely that this host has been compromised.

#-- Please contact your Security SME immediately to notify ofthis issue.

**#-- "/etc/gshadow permissions = 000, owned by root:root" : Mandatory** : Compliant - No fix required

#-- Important: The /etc/group file contains important settings about group accounts in the host.

#-- If found that the following setting is not compliant, it is possible that this host might have been compromised.

#-- Please contact your Security SME immediately to notify ofthis issue.

**#-- "/etc/group permissions = 644, owned by root:root" : Mandatory** : Compliant - No fix required

#-- The checking of the following setting might take a few minutes.

**#-- "All files must be owned by a valid group and user" : Mandatory** :

Compliant: No fix required

#---------------------------- **3.12.2. RESTRICT CORE DUMPS TO PROTECTED DIRECTORY** **----------------------------#**

**#-- "If enabled, core dumps must dump to a restricted directory with mode 0700" : Mandatory** : -

**#-- "If enabled, core dump size limitations must not exceed available disk space on target partition - hard limit must be set" : Mandatory** : Not compliant - Manual fix is required

#------------------------------------- **3.12.3. RESTRICT SETUID EXECUTION** **------------------------------------#**

**#-- "Mount appropriate non-root filesystems with “nosuid” option" : Mandatory**

#-- Checking/Fixing is out of scope of this script.

#-- The checking of the following setting might take a few minutes.

#-- If any SUID and SGID file(s) is found to have writable permissions, make sure to investigate further.

#-- the higuer the privilege of the owner(s) of such files, the higher is the risk of being compromised.

#-- Please contact your Security SME immediately to notify ofthis issue.

**#-- "All SUID and SGID files must not be world writable" : Mandatory**

**#--** **SUID files: Compliant**: No fix required

**#--** **SGID files: Compliant**: No fix required

**#-- "Directories containing SUID or SGID files must be owned by root or system groups and must not be world writable" : Mandatory** : - Manual fix required

#-------------------------------- **3.12.4. RESTRICT DEVICE SPECIAL FILE ACCESS** **-------------------------------#**

**#-- "Mount appropriate non-root filesystems with “nodev” option" : Mandatory**

**#--**  **/boot : Not compliant** : Fix is required

**#--**  **/boot/efi : Not compliant** : Fix is required

**#--**  **/data : Not compliant** : Fix is required

**#--**  **/var : Not compliant** : Fix is required

**#--**  **/apps : Not compliant** : Fix is required

**#--**  **/home : Not compliant** : Fix is required

#---------------------------------- **3.12.5. RESTRICT PROGRAM EXECUTION** **--------------------------------------#**

**#-- "Mount appropriate non-root filesystems with “noexec” option" : Mandatory**

#-- Checking/Fixing is out of scope of this script.

#---------------------------- **3.12.6. DISABLE USER-MOUNTED REMOVABLE FILESYSTEMS** **----------------------------#**

**#-- "Disable user mountable removable filesystems" : Mandatory** - : - Manual fix required

#--------------------------------- **3.12.7. GROUP AND PASSWD FILE CONSISTENCY** **--------------------------------#**

**#-- Important: The /etc/passwd and /etc/group files contain important settings about user and group accounts in the host.**

#-- If found that the following setting is not compliant, it is possible that this host might have been compromised.

#-- This script will not solve this issue. Please contact your Security SME immediately to notify ofthis issue.

**#-- "Ensure groups used in /etc/passwd exist in /etc/group" : Mandatory**: Compliant : No fix required

**#-- "Ensure currency of administrative group membership" : Mandatory** : - Manual fix required

#-- Important: The /etc/passwd file contains important settings about accounts in the host.

#-- If found that the following setting is not compliant, it is possible that this host might have been compromised.

#-- This script will not solve this issue. Please contact your Security SME immediately to notify ofthis issue.

**#-- "Ensure home directories used in /etc/passwd exist." : Mandatory**

#-- The directory **/var/ftp** **defined as the home directory of the account ftp does not exist**

**#-- The directory /var/lib/insights defined as the home directory of the account insights does not exist**

**#-- Important: The /etc/passwd file contains important settings about user accounts in the host.**

#-- If found that the following setting is not compliant, it is possible that this host might have been compromised.

#-- This script will not solve this issue. Please contact your Security SME immediately to notify ofthis issue.

**#-- "Users must be assigned unique UIDs" : Mandatory**: Compliant : No fix required

#-- Important: The /etc/passwd file contains important settings about user accounts in the host.

#-- If found that the following setting is not compliant, it is possible that this host might have been compromised.

#-- This script will not solve this issue. Please contact your Security SME immediately to notify ofthis issue.

**#-- "User names must be unique" : Mandatory**: Compliant : No fix required

#-- Important: The /etc/group file contains important settings about group accounts in the host.

#-- If found that the following setting is not compliant, it is possible that this host might have been compromised.

#-- This script will not solve this issue. Please contact your Security SME immediately to notify ofthis issue.

**#-- "Groups must be assigned unique GIDs" : Mandatory**: Compliant : No fix required

#-- Important: The /etc/group file contains important settings about group accounts in the host.

#-- If found that the following setting is not compliant, it is possible that this host might have been compromised.

#-- This script will not solve this issue. Please contact your Security SME immediately to notify ofthis issue.

**#-- "Group names must be unique" : Mandatory**: Compliant : No fix required

**#-- "Reserved UIDs (0-99) are assigned to system accounts only" : Mandatory** : Unkown compliant:

Revise the following accounts: root bin daemon adm lp sync shutdown halt mail operator games ftp nobody systemd-network dbus abrt rpc tss postfix sshd ntp tcpdump

**#-- "Every account must have a password, \*, or !" : Mandatory** : Compliant : No fix required

**#-- "Personal usernames must not belong to system groups" : Mandatory**

#-- Checking/Fixing is out of scope of this script.

#------------------------------------------ **3.12.8. EXECSHIELD** **----------------------------------------------#**

**#-- "Enable ExecShield" : Mandatory**

#-- Checking/Fixing is out of scope of this script.

#------------------------------------ **3.12.9. RANDOMIZED VIRTUAL MEMORY REGION** **------------------------------#**

**#-- "Set the system flag to force randomized virtual memory region placement (kernel.randomize\_va\_space = 2)" : Mandatory** : Not compliant : Fix is required

################################## **3.13. APPLICATION SECURITY** **######################################**

**#-- "Application resources must not be world-writable" : Mandatory**

#-- Checking/Fixing is out of scope of this script.

**#-- "Application resource controls must be applied where available" : Mandatory**

#-- Checking/Fixing is out of scope of this script.

**#-- "Applications must not run as root" : Mandatory**

#-- Checking/Fixing is out of scope of this script.

**#-- "Direct remote logins to application accounts (i.e. oracle) are not permitted" : Mandatory**

#-- Checking/Fixing is out of scope of this script.

**#-- "Data transfer or robot accounts must not have a valid login shell" : Mandatory**

#-- Checking/Fixing is out of scope of this script.

**#-- "Where possible, robot accounts should be chrooted to restrict access to their home directory only" : Mandatory**

#-- Checking/Fixing is out of scope of this script.

**#-- "SFTP/SCP accounts must use public key authentication for non-interactive logins" : Mandatory**

#-- Checking/Fixing is out of scope of this script.

###################################### **ADDITIONAL ITEMS** **############################################**

**#-- Last time the host has been updated: 1617861023 (Thu 08 Apr 2021 15:50:23 AEST) zlib**

**#-- The following accounts have high privilegues through sudo: root sxcadmin opsmgrsvc ashleyk peterb pattik carols**

#------------------------------------ **USER ACCOUNTS INFORMATION**  **----------------------------------------#**

**#-- Accounts with non-compliant password expiration time: root ashleyk peterb pattik carols**

**#-- Accounts with non-compliant warning password expiration time: root sxcadmin opsmgrsvc ashleyk peterb pattik carols**

**#--** Password information:

**#--** To fix hashed-stored password issues, just changed the password of those affected accounts,

**#--** once the host password settings has been configured.

#------------------------------------ **SYSTEM ACCOUNTS INFORMATION**  **--------------------------------------#**

**#-- Accounts with non-compliant password expiration time: systemd-bus-proxy polkitd libstoragemgmt chrony xymon insights nginx**

**#-- Accounts with non-compliant warning password expiration time: systemd-bus-proxy polkitd libstoragemgmt chrony xymon insights nginx**

**#--** Password information:

**#-- systemd-bus-proxy: Locked and password not set**

**#-- polkitd: Locked and password not set**

**#-- libstoragemgmt: Locked and password not set**

**#-- chrony: Locked and password not set**

**#-- xymon: Locked and password not set**

**#-- insights: Locked and password not set**

**#-- nginx: Locked and password not set**

**#--** To fix hashed-stored password issues, just changed the password of those affected accounts,

**#--** once the host password settings has been configured.

#------------------------------------ **RESERVED ACCOUNTS INFORMATION**  **------------------------------------#**

**#-- Accounts with non-compliant password expiration time: bin daemon adm lp sync shutdown halt mail operator games ftp nobody systemd-network dbus abrt rpc tss postfix sshd ntp tcpdump**

**#-- Accounts with non-compliant warning password expiration time: bin daemon adm lp sync shutdown halt mail operator games ftp nobody systemd-network dbus abrt rpc tss postfix sshd ntp tcpdump**

**#--** Password information:

**#-- bin: "\*" on the password field**

**#-- daemon: "\*" on the password field**

**#-- adm: "\*" on the password field**

**#-- lp: "\*" on the password field**

**#-- sync: "\*" on the password field**

**#-- shutdown: "\*" on the password field**

**#-- halt: "\*" on the password field**

**#-- mail: "\*" on the password field**

**#-- operator: "\*" on the password field**

**#-- games: "\*" on the password field**

**#-- ftp: "\*" on the password field**

**#-- nobody: "\*" on the password field**

**#-- systemd-network: Locked and password not set**

**#-- dbus: Locked and password not set**

**#-- abrt: Locked and password not set**

**#-- rpc: Locked and password not set**

**#-- tss: Locked and password not set**

**#-- postfix: Locked and password not set**

**#-- sshd: Locked and password not set**

**#-- ntp: Locked and password not set**

**#-- tcpdump: Locked and password not set**

**#--** To fix hashed-stored password issues, just changed the password of those affected accounts,

**#--** once the host password settings has been configured.

#------------------------------------ **SUSPICIOUS ACCOUNTS INFORMATION** **-----------------------------------#**

**#-- Accounts with non-compliant password expiration time:**

**#-- Accounts with non-compliant warning password expiration time:**

**#--** Password information:

**#--** To fix hashed-stored password issues, just changed the password of those affected accounts,

**#--** once the host password settings has been configured.