KURUKULASOORIYA KVR **200332X**

CS 3400 CYBER SECURITY PROJECT WEEK 02

DISTURBING DISCOVERY

The Disturbing Discovery in Pandora Company LTD was carried out to analyze server configurations of Rocky Linux 9 Server and Windows Server 2019 R2 in order to identify the current security position of the company's 3 servers and harden them to enhance the protection while reducing the impact from possible vulnerabilities.

This report consists of 2 parts, Part I is an analysis of existing and recommended configurations with their implementation and their security implications for the 2 servers & Part II is about proposals for the implementation of Future Server Installation

Part I

1. For Rocky Linux Server 9

Identification of a Reputed Framework

The analysis was done based on the CIS Rocky Linux 9 Benchmark v1.0.0, a security configuration guide that provides best practices for hardening Rocky Linux 9 systems. Center for Internet Security (CIS), is a non-profit organization that provides security best practices for IT systems and they regularly update their benchmarks to reflect the changes in the threat landscape.

This very first and latest set of guidelines was released on December 13, 2022, and is inclusive of a number of new security controls that are more timely and system-centric. In contrast with Windows Servers, Linux Servers often come with less secure default configurations and it is a must to harden the Server to obtain a high level of security.

Identification of Key Hardening Framework

The hardening process is supposed to be done based on the following sections addressed by the CIS Rocky Linux 9 Benchmark v1.0.0 ;

- Initial Configurations
  - File System Configuration
  - Software Updates Configuration
  - File System Integrity Checking
  - Secure Boot Settings
  - Additional Process Hardening
  - Mandatory Access Control

CMD Warning Banners
GNOME Display Manager

- Services Settings
- Network Configuration
- Logging and Auditing
- Access, Authentication and Authorization
- System Maintenance

Analysis & Document Improvements over Default Settings

1. Initial Configuration

a)Default Settings:

- ✓ At the installation root filesystem will be stored into a single partition.
- ✓ By default, it supports a range of filetypes.

b) Recommended Settings:

- File System Configuration
  - Disable unused filesystems like mounting of squashfs and udf

Please refer to the bash scripts in Page 24 and 27 in references[1].

  - Ensure /tmp is a separate partition and nodev, noexec and nosuid options are set on

First **ensure that systemd is correctly configured** to ensure that /tmp will be mounted at boot time.

```
# systemctl unmask tmp.mount
```

For specific configuration requirements of the /tmp mount for your environment**, modify /etc/fstab.**
Edit the /etc/fstab file and add nodev to the fourth field (mounting options) for the /tmp partition.
Edit the /etc/fstab file and add noexec to the fourth field (mounting options) for the /tmp partition.
Edit the /etc/fstab file and add nosuid to the fourth field (mounting options) for the /tmp partition.

  - Ensure /var is a separate partition and nodev and nosuid options are set on

For new installations, during installation **create a custom partition setup and specify a separate partition for /var.**

Edit the /etc/fstab file and add nodev to the fourth field (mounting options) for the /var partition.

Edit the /etc/fstab file and add nosuid to the fourth field (mounting options) for the /var partition.

- Ensure /var/tmp is a separate partition and nodev, noexec and nosuid options are set on

For new installations, during installation **create a custom partition setup and specify a separate partition for /var/tmp.**

Edit the /etc/fstab file and add noexec to the fourth field (mounting options) for the /var/tmp partition.

Edit the /etc/fstab file and add nosuid to the fourth field (mounting options) for the /var/tmp partition.

Edit the /etc/fstab file and add nodev to the fourth field (mounting options) for the /var/tmp partition.

- Ensure var/log/ is a separate partition and nodev, noexec and nosuid options are set on

For new installations, **during installation create a custom partition setup and specify a separate partition for /var/log .**

Edit the /etc/fstab file and add nodev to the fourth field (mounting options) for the /var/log partition.

Edit the /etc/fstab file and add noexec to the fourth field (mounting options) for the /var/log partition.

Edit the /etc/fstab file and add nosuid to the fourth field (mounting options) for the /var/log partition.

- Ensure var/log/audit/ is a separate partition and nodev, noexec and nosuid options are set on.

For new installations, **during installation create a custom partition setup and specify a separate partition for /var/log/audit .**

Edit the /etc/fstab file and add nodev to the fourth field (mounting options) for the /var/log/audit partition.

Edit the /etc/fstab file and add noexec to the fourth field (mounting options) for the /var/log/audit partition.

Edit the /etc/fstab file and add nosuid to the fourth field (mounting options) for the /var/log/audit partition.

- Ensure /home is a separate partition and nodev and nosuid options are set on

For new installations, **during installation create a custom partition setup and specify a separate partition for /home.**

Edit the /etc/fstab file and add nodev to the fourth field (mounting options) for the /home partition.

Edit the /etc/fstab file and add nosuid to the fourth field (mounting options) for the /home partition.

- Ensure /dev/shm is a separate partition and nodev, nosuid and noexec options are set on

For specific configuration requirements of the /dev/shm mount for your environment**, modify /etc/fstab.**

Edit the /etc/fstab file and add nodev to the fourth field (mounting options) for the /dev/shm partition
Edit the /etc/fstab file and add nosuid to the fourth field (mounting options) for the /dev/shm partition.
Edit the /etc/fstab file and add noexec to the fourth field (mounting options) for the /dev/shm partition

- Disable USB storage

Please refer to the bash script in page 95 references[1].

- Software Updates Configuration

- Ensure GPG keys are configured

Update your package manager GPG keys in accordance with site policy.

- Ensure gpgcheck and repo_gpgcheck is globally activated.

Edit /etc/dnf/dnf.conf and set gpgcheck=1 in the [main] section.

Edit any failing files in /etc/yum.repos.d/* and **set all instances starting with gpgcheck to 1.**

Edit /etc/dnf/dnf.conf and set repo_gpgcheck=1 in the [main] section.

Edit any failing files in /etc/yum.repos.d/* and **set all instances starting with repo_gpgcheck to 1.**

- Ensure package manager repositories are configured

Configure your package manager repositories according to site policy

- File System Integrity Checking

- Ensure AIDE is installed

Run the following command to install AIDE:
 # dnf install aide

Configure AIDE as appropriate for your environment

- Ensure file system integrity is regularly checked while using cryptographic mechanisms to ensure integrity

Please refer to the page 112 for checking system-wide integrity.

Add or update the following selection lines for to a file ending in .conf in the /etc/aide.conf.d/ directory or to /etc/aide.conf to protect the integrity of the audit tools:

```
# Audit Tools

/sbin/auditctl p+i+n+u+g+s+b+acl+xattrs+sha512

/sbin/auditd p+i+n+u+g+s+b+acl+xattrs+sha512

/sbin/ausearch p+i+n+u+g+s+b+acl+xattrs+sha512

/sbin/aureport p+i+n+u+g+s+b+acl+xattrs+sha512

/sbin/autrace p+i+n+u+g+s+b+acl+xattrs+sha512

/sbin/augenrules p+i+n+u+g+s+b+acl+xattrs+sha512
```

- Secure Boot Settings

- Ensure bootloader password is set and permissions on bootloader config are configured.

Create an encrypted password with grub2-setpassword:

 # grub2-setpassword Enter password: <password> Confirm password: <password>

Run the following commands to set ownership and permissions on your grub configuration files:

Run the following command to set ownership and permissions on grub.cfg:
 # chown root:root /boot/grub2/grub.cfg # chmod og-rwx /boot/grub2/grub.cfg
Run the following command to set ownership and permissions on grubenv:
 # chown root:root /boot/grub2/grubenv # chmod u-x,og-rwx /boot/grub2/grubenv
Run the following command to set ownership and permissions on user.cfg:
 # chown root:root /boot/grub2/user.cfg # chmod u-x,og-rwx /boot/grub2/user.cfg

- Additional Process Hardening

- Ensure coredump storages and backtraces are disabled

Edit **/etc/systemd/coredump.conf** and **edit or add the following line:**
Storage=none
Edit or add the following line in /etc/systemd/coredump.conf:
ProcessSizeMax=0

- Ensure ASLR is enabled

Please refer to the bash script in page 128 references[1].

- Mandatory Access Control

- Ensure SELinux is installed, configured and enforcing.

Run the following command to install SELinux:

```
# dnf install libselinux
```

Edit the /etc/selinux/config file to set the SELINUXTYPE parameter:

```
SELINUXTYPE=targeted
```

Edit the /etc/selinux/config file to set the SELINUX parameter: For Enforcing mode:

```
SELINUX=enforcing
```

Run the following command to set SELinux's running mode:

```
# setenforce 1
```

- Ensure no unconfined Services exist

Run the following command and verify not output is produced:

```
# ps -eZ | grep unconfined_service_t
```

- Ensure SETroubleshoot and mctrans are not installed

Run the following command to uninstall setroubleshoot:

```
# dnf remove setroubleshoot
```

Run the following command to uninstall mcstrans:

```
# dnf remove mcstrans
```

- CMD Warning Banners

- Ensure message of the day is configured

Edit the /etc/motd file with the appropriate contents according to your site policy, remove any instances of \m , \r , \s , \v or references to the OS platform

- Ensure both local login warning and remote logon warning are configured

Edit the /etc/issue file with the appropriate contents according to your site policy, remove any instances of \m , \r , \s , \v or references to the OS platform

 # echo "Authorized uses only. All activity may be monitored and reported." > /etc/issue

Edit the /etc/issue.net file with the appropriate contents according to your site policy, remove any instances of \m , \r , \s , \v or references to the OS platform

 # echo "Authorized uses only. All activity may be monitored and reported." > /etc/issue.net

- Ensure permissions on /etc/motd , /etc/issue, /etc/issue.net are configured

Run the following commands to set permissions on /etc/motd :

 # chown root:root /etc/motd # chmod u-x,go-wx /etc/motd

Run the following commands to set permissions on /etc/issue :

 # chown root:root /etc/issue # chmod u-x,go-wx /etc/issue

Run the following commands to set permissions on /etc/issue.net :

 # chown root:root /etc/issue.net # chmod u-x,go-wx /etc/issue.net

  - GNOME Display Manager
- Ensure GNOME Display Manager is removed

Run the following command to remove the gdm package

 # dnf remove gdm

- Ensure GDM is enabled and properly configured

Please refer to the bash scripts in page 170, 174, 179, 183, 188, 194, 198 & 202 references[1]..

- Ensure XDCMP is not enabled

Edit the file /etc/gdm/custom.conf and remove the line:

Enable=true

- Ensure updates, patches, and additional security software are installed and system-wide crypto policy is not legacy.

The following command will install all available updates:
 # dnf update
Once the update process is complete, verify if reboot is required to load changes.
dnf needs-restarting -r

Run the following command to change the system-wide crypto policy
 # update-crypto-policies --set <CRYPTO POLICY>

Run the following to make the updated system-wide crypto policy active
 # update-crypto-policies

c) Security Implications:

- ***File System Configuration*** help to prevent unauthorized access to files by restricting who has read, write, and execute permissions to different files and folders.
- ***Software Updates Configuration*** keeps the system safe by ontime running updates as software updates often include security patches that fix vulnerabilities that could be exploited by attackers.
- ***File System Integrity Checking*** help to detect unauthorized changes to files, which could be a sign of a security breach.
- ***Secure Boot Settings*** prevent malware from taking control of the boot process by only allowing trusted software to be loaded.
- ***Additional Process Hardening*** make it more difficult for malware to exploit vulnerabilities in running processes.
- ***Mandatory Access Control*** restricts access to resources based on the user's identity and privileges.
- ***CMD Warning Banners*** deter unauthorized access to the command prompt by displaying a message that warns users that unauthorized access is prohibited.
- ***GNOME Display Manager*** help to prevent unauthorized access to the graphical user interface by requiring users to enter a password before they can log in.

2. Services Settings

a)Default Configurations:

The security level of services settings in linux environment is relatively high, but there are still some unnecessary services might have installed and enabled that may probably increase the attack surface.

b)Recommended Configurations:

- Ensure time synchronization is in use and chrony is configured

Run the following command to install chrony:

 # dnf install chrony

Add or edit server or pool lines to /etc/chrony.conf as appropriate:
server <remote-server>
Add or edit the OPTIONS in /etc/sysconfig/chronyd to include '-u chrony':
OPTIONS="-u chrony"

- Ensure some special purpose services like xorg-x11, Avahi Server, CUPS, DHCP, DNS, VSFTP, TFTP, web server, IMAP & POP 3, Samba, HTTP Proxy Server, net-snmp, telnet server, dnsmasq, **nfs-utils, rpcbind rsync-daemon are not installed.**

Run the following command to remove the X Windows Server packages:

```
# dnf remove xorg-x11-server-common
Run the following commands to stop, mask and remove avahi:
# systemctl stop avahi-daemon.socket avahi-daemon.service
# dnf remove avahi
Run the following command to remove cups:
# dnf remove cups
Run the following command to remove dhcp:
# dnf remove dhcp-server
Run the following command to remove bind:
# dnf remove bind
Run the following command to remove vsftpd:
# dnf remove vsftpd
Run the following command to remove tftp-server:
# dnf remove tftp-server
Run the following command to remove httpd and nginx:
# dnf remove httpd nginx
Run the following command to remove dovecot and cyrus-imapd:
# dnf remove dovecot cyrus-imapd
Run the following command to remove samba:
# dnf remove samba
Run the following command to remove the squid package:
# dnf remove squid
Run the following command to remove net-snmpd:
# dnf remove net-snmp
Run the following command to remove the telnet-server package:
# dnf remove telnet-server
Run the following command to remove dnsmasq:
# dnf remove dnsmasq
```

- Ensure mail transfer agent is configured to local mode

```
Edit /etc/postfix/main.cf and add the following line to the RECEIVING MAIL
section. If the line already exists, change it to look like the line
below:
inet_interfaces = loopback-only
Run the following command to restart postfix:
# systemctl restart postfix
```

- Ensure service clients like telnet, LDAP, TFTP, FTP and any other non essential services listing on the system are not installed.

```
Check for the existence using rpm -q command and if exists , remove using
dnf remove command
```

c)Security Implications:

- ***Time synchronization*** ensures that all systems on a network have the same time. This is important for a variety of security-related tasks, such as logging, auditing, and intrusion detection.
- ***By uninstalling special purposes and unnecessary services and other server clients***, the attack surface could be reduced in the system and it makes it more difficult for attackers to gain access.

- ***Mail transfer agent configured to local mode*** ensures the prevention from unauthorized users from accessing email messages.

3. Network Configuration

a)Default Configuration:

The level of security of default configuration on network related activities in Rockey Linux is relatively low because it enable a range of network protocol and in contrast with Windows Server, it does not use a separate and stand alone security management tool. Thus, every network security measures should have to be implemented through Network Manager as separate actions.

b) Recommended Configurations:

- Disable unused network protocols and devices

Enable or disable IPv6 in accordance with system requirements and local site policy. (By default, it is activated)

To disable any wireless interfaces, please refer to the bash script in page 271.

To disable TPIC, please refer to the bash script in page 275 references[1].

- Ensure unwanted activities like IP forwarding, packet redirect sending, ICMP & secure ICMP redirects are disabled or not accepted. And any suspicious activities are logged.

Set the following parameter in /etc/sysctl.conf or a /etc/sysctl.d/* file:

```
# printf "
net.ipv4.ip_forward = 0 " >> /etc/sysctl.d/60-netipv4_sysctl.conf
Run the following command to set the active kernel parameters:
# { sysctl -w net.ipv4.ip_forward=0 sysctl -w net.ipv4.route.flush=1 }
```

Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file: *Example:*

```
# printf " net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.send_redirects = 0 " >> /etc/sysctl.d/60-
netipv4_sysctl.conf
Run the following command to set the active kernel parameters:
# { sysctl -w net.ipv4.conf.all.send_redirects=0 sysctl -w
net.ipv4.conf.default.send_redirects=0 sysctl -w net.ipv4.route.flush=1 }
```

Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file: *Example:*

```
# printf " net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.default.accept_redirects = 0 " >> /etc/sysctl.d/60-
netipv4_sysctl.conf
Run the following command to set the active kernel parameters:
```

```
# { sysctl -w net.ipv4.conf.all.accept_redirects=0 sysctl -w
net.ipv4.conf.default.accept_redirects=0 sysctl -w net.ipv4.route.flush=1
}
```

Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file: *Example:*

```
# printf " net.ipv4.conf.all.secure_redirects = 0
net.ipv4.conf.default.secure_redirects = 0 " >> /etc/sysctl.d/60-
netipv4_sysctl.conf
```

Run the following commands to set the active kernel parameters:

```
# { sysctl -w net.ipv4.conf.all.secure_redirects=0 sysctl -w
net.ipv4.conf.default.secure_redirects=0 sysctl -w net.ipv4.route.flush=1
}
```

Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file: *Example:*

```
# printf " net.ipv4.conf.all.log_martians = 1
net.ipv4.conf.default.log_martians = 1 " >> /etc/sysctl.d/60-
netipv4_sysctl.conf
```

Run the following command to set the active kernel parameters:

```
# { sysctl -w net.ipv4.conf.all.log_martians=1 sysctl -w
net.ipv4.conf.default.log_martians=1 sysctl -w net.ipv4.route.flush=1 }
```

- Ensure TCP SYN Cookies, Reverse Path Filtering are enabled.

Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file: *Example:*

```
# printf " net.ipv4.tcp_syncookies = 1 " >> /etc/sysctl.d/60-
netipv4_sysctl.conf
```

Run the following command to set the active kernel parameters:

```
# { sysctl -w net.ipv4.tcp_syncookies=1 sysctl -w net.ipv4.route.flush=1 }
```

Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file: *Example:*

```
# printf " net.ipv4.conf.all.rp_filter = 1 net.ipv4.conf.default.rp_filter
= 1 " >> /etc/sysctl.d/60-netipv4_sysctl.conf
```

Run the following commands to set the active kernel parameters:

```
# { sysctl -w net.ipv4.conf.all.rp_filter=1 sysctl -w
net.ipv4.conf.default.rp_filter=1 sysctl -w net.ipv4.route.flush=1 }
```

- Configure nfttables are installed and a single firewall configuration utility is in use.

Run the following command to install nftables

```
# dnf install nftables
```

To ensure that a single firewall utility is in use, Please refer to the bash script in page 330.

- Configure firewall rules properly and have a host based firewall with nfttables default deny policy.

c)Security Implications:

- ***Disabling unused network devices and protocols*** reduce the attack surface of the system and make it more difficult for attackers to gain access.
- ***Ensuring unwanted network activities*** prevent attackers from using the system to attack other systems.
- ***Ensuring TCP SYN cookies and reverse path filterin****g* prevent attackers from launching denial-of-service attacks.
- ***Configuring firewall rules*** control which traffic is allowed to enter and exit the system.
- ***Having a host-based firewall with NFT tables default deny policy*** help to prevent unauthorized traffic from reaching your system

4. Logging and Auditing

a) Default Settings:

By default, Rockey Linux enables logging and auditing, but the level of scope and the security of log files, it is considered is moderate. Thus, in order to result in a good quality service and not to miss out on any evidence during an investigation, some additional configurations are yet to be enabled.

b) Recommended Configurations:

- Ensure auditing is enabled

```
Run the following command and verify auditd is installed:
# rpm -q audit
Run the following command to Install auditd
# dnf install audit
```

- Configure the settings on audit data retention by setting a sufficient audit log size, setting logs are not automatically deleted but the system to be disabled when the logs are full

```
Run the following command to add audit_backlog_limit=<BACKLOG SIZE> to
GRUB_CMDLINE_LINUX:
# grubby --update-kernel ALL --args 'audit_backlog_limit=<BACKLOG SIZE>'

Set the following parameter in /etc/audit/auditd.conf in accordance with
site policy:
max_log_file = <MB>

Set the following parameter in /etc/audit/auditd.conf:
max_log_file_action = keep_logs

Set the following parameters in /etc/audit/auditd.conf:
space_left_action = email action_mail_acct = root
set admin_space_left_action to either halt or single in
/etc/audit/auditd.conf.
```

- Ensure audit rules are formed to collect information on events and activities:
  - Changes to system admin scope

```
Edit or create a file in the /etc/audit/rules.d/ directory, ending in
.rules extension, with the relevant rules to monitor scope changes for
system administrators. Example:
# printf "
-w /etc/sudoers -p wa -k scope -w /etc/sudoers.d -p wa -k scope " >>
/etc/audit/rules.d/50-scope.rules
Merge and load the rules into active configuration:
# augenrules --load
```

  - Actions by the admin or any other users

```
Edit or create a file in the /etc/audit/rules.d/ directory, ending in
.rules extension, with the relevant rules to monitor elevated privileges.
# printf "
-a always,exit -F arch=b64 -C euid!=uid -F auid!=unset -S execve -k
user_emulation
-a always,exit -F arch=b32 -C euid!=uid -F auid!=unset -S execve -k
user_emulation
" >> /etc/audit/rules.d/50-user_emulation.rules

   Load audit rules
Merge and load the rules into active configuration:
# augenrules --load
```

  - Modifications on the sudo log file, data and time information and the system's network environment is collected.

```
Edit or create a file in the /etc/audit/rules.d/ directory, ending in
.rules extension, with the relevant rules to monitor events that modify
the sudo log file. Example:
# { SUDO_LOG_FILE=$(grep -r logfile /etc/sudoers* | sed -e
's/.*logfile=//;s/,? .*//' -e 's/"//g') [ -n "${SUDO_LOG_FILE}" ] &&
printf " -w ${SUDO_LOG_FILE} -p wa -k sudo_log_file " >>
/etc/audit/rules.d/50-sudo.rules || printf "ERROR: Variable
'SUDO_LOG_FILE_ESCAPED' is unset.\n" }
Merge and load the rules into active configuration:
   # augenrules –load


Edit or create a file in the /etc/audit/rules.d/ directory, ending in
.rules extension, with the relevant rules to monitor events that modify
date and time information.
# printf " -a always,exit -F arch=b64 -S
adjtimex,settimeofday,clock_settime -k time-change -a always,exit -F
arch=b32 -S adjtimex,settimeofday,clock_settime -k time-change -w
/etc/localtime -p wa -k time-change " >> /etc/audit/rules.d/50-time-
change.rules
Merge and load the rules into active configuration:
# augenrules –load
```

Edit or create a file in the /etc/audit/rules.d/ directory, ending in .rules extension, with the relevant rules to monitor events that modify the system's network environment.

```
# printf " -a always,exit -F arch=b64 -S sethostname,setdomainname -k system-locale -a always,exit -F arch=b32 -S sethostname,setdomainname -k system-locale -w /etc/issue -p wa -k system-locale -w /etc/issue.net -p wa -k system-locale -w /etc/hosts -p wa -k system-locale -w /etc/sysconfig/network -p wa -k system-locale -w /etc/sysconfig/network-scripts/ -p wa -k system-locale " >> /etc/audit/rules.d/50-system_local.rules
```

Merge and load the rules into active configuration:

```
# augenrules --load
```

- Unsuccessful file attempts, use of privileged commands and events that modify user/ group privileges and discretionary access control permissions
  - Successful file mounts
  - Log in and out events
  - Session initiation information and file deletion by users
  - Every successful and unsuccessful attempts to use setfacl, chacl, and usermod command
  - Every actions on loading, unloading or modification on kernel

Edit or create a file in the /etc/audit/rules.d/ directory, ending in .rules extension, with the relevant rules to monitor above requirements.

Merge and load the rules into active configuration:

```
# augenrules --load
```

- Configure audited file access based on related numeric file access permissions:
  - Ensure audit log files are 0640 or less primitive

Run the following command to remove more permissive mode than 0640 from audit log files:

```
# [ -f /etc/audit/auditd.conf ] && find "$(dirname $(awk -F "=" '/^\s*log_file/ {print $2}' /etc/audit/auditd.conf | xargs))" -type f \( ! -perm 600 -a ! -perm 0400 -a ! -perm 0200 -a ! -perm 0000 -a ! -perm 0640 -a ! -perm 0440 -a ! -perm 0040 \) -exec chmod u-x,g-wx,o-rwx {} +
```

  - Ensure audit configuration files are 640 or more restrictive

Run the following command to remove more permissive mode than 0640 from the audit configuration files:

```
# find /etc/audit/ -type f \( -name '*.conf' -o -name '*.rules' \) -exec chmod u-x,g-wx,o-rwx {} +
```

  - Ensure audit log directory is 0750 or more restrictive

Run the following command to configure the audit log directory to have a mode of "0750" or less permissive:

```
# chmod g-w,o-rwx "$(dirname $( awk -F"=" '/^\s*log_file\s*=\s*/ {print $2}' /etc/audit/auditd.conf))"
```

- Ensure audit tools are *755* or more restrictive

Run the following command to remove more permissive mode from the audit tools:

```
# chmod go-w /sbin/auditctl /sbin/aureport /sbin/ausearch /sbin/autrace /sbin/auditd /sbin/augenrules
```

- Ensure only authorized users and groups own audit log files.

Run the following command to configure the audit log files to be owned by the root user:

```
# [ -f /etc/audit/auditd.conf ] && find "$(dirname $(awk -F "=" '/^\s*log_file/ {print $2}' /etc/audit/auditd.conf | xargs))" -type f ! -user root -exec chown root {} +
```

- Ensure audit configuration files, tools are owned by root and belongs to group root

Run the following command to change the owner of the audit tools to the root user:

```
# chown root /sbin/auditctl /sbin/aureport /sbin/ausearch /sbin/autrace /sbin/auditd /sbin/augenrules
```

Run the following command to change ownership to root user:

```
# find /etc/audit/ -type f \( -name '*.conf' -o -name '*.rules' \) ! -user root -exec chown root {} +
```

- Configure rsylog by ensuring it installed, enabled, configured, logged by enabling journald.

Verify the existence with rpm -q command and it not exists, install using dnf install command.

Run the following command to enable rsyslog:

```
# systemctl --now enable rsyslog
```

Edit the /etc/systemd/journald.conf file and add the following line:

```
ForwardToSyslog=yes
```

- Ensure journald is is configured to send logs to a remote log host.

Edit the /etc/rsyslog.conf and /etc/rsyslog.d/*.conf files and add the following line (where loghost.example.com is the name of your central log host). The target directive may either be a fully qualified domain name or an IP address.

```
*.* action(type="omfwd" target="192.168.2.100" port="514" protocol="tcp" action.resumeRetryCount="100" queue.type="LinkedList" queue.size="1000")
```

c)Security Implications:

- ***Enabling auditing*** tracks and records important events that occur on a system, such as user logins, file access, and system changes that could be used to investigate security incidents and to identify potential security vulnerabilities.

- ***Configuring audit log storage*** ensures there would be no failures in logging and reporting system while it ensures each and every piece of important information would not be missed out.
- ***Properly configuring audit rules*** ensure that only the important events are logged, and that the logs are not too large or too noisy.
- ***Setting numeric file access permissions to audit files*** ensures the authorized access by the owner, group, and others depending on the specific needs of the system.
- ***Logging all suspicious activities*** often is a piece of great evidence to identify potential security threats and to take steps to mitigate them.
- ***Configuring the ownership of audit files*** helps to prevent unauthorized users from tampering with the logs.
- ***Properly configuring rsyslog*** which is a popular logging daemon that can be used to collect and store audit logs, ensure that the logs are collected and stored in a secure and efficient manner.

5. Access, Authentication and Authorization

a) Default Settings:

The default access, authentication and authorization used in Rockey Linux is at a very basic level which is also very risky.

- AAA is only based on assigning a password for every user for the authentication purposes.
- The level of default password strength is very low.
- Root user has broad access privileges and control over the whole system.
- Commands of su and sudo allows any user to run commands as a root user.
- Enables a broad SSH access.

b) Recommended Configurations:

- Ensure time-based job schedulers are enabled and configured.
  - Enable cron daemon is enabled and restricted to authorized users.

```
Run the following command to enable cron:
# systemctl --now enable crond
```

  - Ensure permissions on /etc/crontab, /etc/cron.hourly, /etc/cron.daily, /etc/cron.weekly, /etc/cron.monthly, /etc/cron.d is configured.

```
Run the following commands to set ownership and permissions on
/etc/crontab :
# chown root:root /etc/crontab # chmod og-rwx /etc/crontab

Likewise, replace the /etc/crontab to other options to set all the
permissions required.
```

- Configure SSH Server by setting,

- Permissions on /etc/ssh/sshd_config, SSH private and public host key files are configured.
- SSH PAM, SSH IgnoreRhosts is enabled.
- SSH root login, SSH host based authentication, Permit Empty passwords, Permit user environment, X11 forwarding, Allow TCP forwarding is disabled.
- SSH access is limited and Log level is appropriate.
- SSH warning banner and Max Startups are configured.
- SSH MaxAuth Tries is set to 4 or less , SSH MaxSessions is set to 10 or less, and SSH LoginGrace Time is set I minute or less.
- SSH idle timeout interval is configured.
- System wide crypto policy is not over-ridden

Please refer to the scripts from page 546 to 601 references[1] for the above SSH related security implementations.

- Configure Privilege escalation by sudo is installed, sudo command use pty , sudo log files **exists and sudo authentication timeout is configured correctly.**

Run the following command to install sudo
 # dnf install sudo

Edit the file /etc/sudoers with visudo or a file in /etc/sudoers.d/ with visudo -f <*PATH_TO_FILE*> and add the following line:
Defaults use_pty

Edit the file /etc/sudoers or a file in /etc/sudoers.d/ with visudo or visudo -f <PATH TO FILE> and add the following line:
Defaults logfile="<PATH TO CUSTOM LOG FILE>"

- Ensure users must provide password for escalation and re-authentication is not disabled globally.
- Ensure Access to su command is restricted.

Create an empty group that will be specified for use of the su command. The group should be named according to site policy. *Example:*
 # groupadd sugroup
Add the following line to the /etc/pam.d/su file, specifying the empty group:
auth required pam_wheel.so use_uid group=sugroup

- Configure authselect by using a custom authselect file including with-faillock
- Ensure PAM by setting password creation requirements, lockout for failed passwords attempts are configured.

Please refer to the page 623 to 625 references[1].

- Ensure password reuse is limited

Please refer to the bash script in page 632 references[1].

- Ensure password hashing algorithm is SHA-512 or yescrypt.

Please refer to the bash script in page 636 references[1].

- Ensure password usage and lifetime settings as,

  - Password expiration 365 days or less

```
Set the PASS_MAX_DAYS parameter to conform to site policy in
/etc/login.defs :
PASS_MAX_DAYS 365
Modify user parameters for all users with a password set to match:
# chage --maxdays 365 <user>
```

  - Minimum days between password changes are properly configured

```
Set the PASS_MIN_DAYS parameter to 1 in /etc/login.defs:
PASS_MIN_DAYS 1
Modify user parameters for all users with a password set to match:
# chage --mindays 1 <user>
```

  - Minimum expiration warning is 7 days or more

```
Set the PASS_WARN_AGE parameter to 7 in /etc/login.defs :
PASS_WARN_AGE 7
Modify user parameters for all users with a password set to match:
# chage --warndays 7 <user>
```

  - Inactive password lock is 30 days or less

```
Run the following command to set the default password inactivity period to
30 days:
# useradd -D -f 30
Modify user parameters for all users with a password set to match:
# chage --inactive 30 <user>
```

- Ensure default user shell timeout is 900 seconds or less, default group for root account is GID 0 and default user unmask is 027 or more restrictive.

Investigate any users with a password change date in the future and correct them. Locking the account, expiring the password, or resetting the password manually may be appropriate.

- Ensure root password is set and all system accounts are secured.

```
Set the root password with:
# passwd root
```

c)Security Implications:

- ***Enabling and configuring cron daemon*** which is a system service that can be used to run tasks at scheduled intervals, helps to prevent unauthorized users from running malicious commands.
- ***Configuring the SSH server securely*** can help to prevent unauthorized users from gaining access to the system.

- ***Restricting the use of sudo*** helps to prevent unauthorized users from gaining root privileges and logging all sudo attempts can help to track down unauthorized activity.
- ***Restricting the su command*** prevents unauthorized users from gaining access to other user accounts.
- ***Configuring authselect*** which is a tool that can be used to configure authentication methods for users, prevent unauthorized users from gaining access to the system.
- ***Password security measures*** enhances the security of the password and reduce the probability of some malicious attacker to crack or steal and enter the system unauthorizedly.
- ***Setting root password*** prevents unauthorized users from gaining root privileges.

6. System Maintenance

a) Default Settings:

By default Rockey Linux 9 has **no system maintenance configurations have enabled**. It only **provides configurable options for the system admin to enable at his consent.** It implies that in a system wide corruption, it would be very difficult to recover it back, if proper backups have not kept regularly.

b) Recommended Configurations:

- Ensure the system file permissions are set and configured such as /etc/passwd, /etc/passwd-, /etc/group, /etc/group-, /etc/shadow, /etc/shadow-, /etc/gshadow and /etc/gshadow-

```
Run the following commands to remove excess permissions, set owner, and
set group on /etc/passwd:
# chmod u-x,go-wx /etc/passwd # chown root:root /etc/passwd

Change the relevant parameters (/etc/passwd) and continue for others
```

- Ensure no word writable, no unowned files and no ungrouped files are exist and sticky bit is set on all world writable files.

```
Removing write access for the "other" category ( chmod o-w <filename> ) is
advisable, but always consult relevant vendor documentation to avoid
breaking any application dependencies on a given file.

Locate files that are owned by users or groups not listed in the system
configuration files, and reset the ownership of these files to some active
user on the system as appropriate.
```

- Audit SUID, SGID and system file permissions.

```
Ensure that no rogue SUID, SGID programs have been introduced into the
system. Review the files returned by the action in the Audit section and
confirm the integrity of these binaries.
```

- Ensure accounts in /etc/passwd use shadowed passwords and /etc/shadow password fields are not empty

- Ensure all groups in /etc/passwd exist in /etc/group
- Ensure no duplicate UID / GID, usernames and group names are exist.

Run and Audit and Based on the results of the audit script, establish unique UIDs or GIDs and review all files owned by the shared UIDs to determine which UID they are supposed to belong to.

- Ensure rootpath integrity and root is only set to UID 0 account.

Run and audit and correct any mismatches discovered

- Ensure local interactive user home directories exists, owned and mode 750 or more restrictive
- Ensure no local interactive user has .netrc, .forward, .rhosts files
- Ensure local interactive user dot files are not group or worldwide.

c)Security Implications:

- ***Setting file system permissions*** prevent unauthorized access to files by restricting who has read, write, and execute permissions to different files and folders while adhering data security with CIA policy.
- ***Removal of unowned files and directories*** which could be accessed by any user reduces the possible attack surface of the system.
- ***Sticky bit set on all writable files*** helps to prevent unauthorized users from deleting or modifying important files.
- ***Auditing SUID, SGID*** identifies any files that have these permissions set incorrectly since this can be a security risk if these permissions are set on files that should not be executable by all users.
- ***Removal of duplicates*** enhances both the security and performance of the system.
- ***Configuring local interactive users*** help to prevent unauthorized users from gaining access to the system.

2. For Windows Server 2019 R2

Identification of a Reputed Framework

The analysis was done based on the CIS Microsoft Windows Server 2019 Benchmark v2.0.0, a security configuration guide that provides best practices for hardening Microsoft Windows Server 2019 R2 systems. Center for Internet Security (CIS), is a non-profit organization that provides security best practices for IT systems and they regularly update their benchmarks to reflect the changes in the threat landscape.

The latest set of guidelines was released on April 14, 2023, and is inclusive of a number of new security controls that are more timely and system-centric.

Identification of Key Hardening Framework

The hardening process is supposed to be done based on the following sections addressed by the CIS Microsoft Windows Server 2019 Benchmark v2.0.0 ;

- Account management
- Authentication and authorization
- Network security
- Data security
- Logging and auditing
- Device Security

Analysis & Document Improvements over Default Settings

1. Account management

a) **Default Settings:**
   - ✓ All users have broad access to system files including read and execution permissions.
   - ✓ The Administrator account has broad access plus full control over system files.

b) **Recommended Settings:**

The CSI Benchmark guidelines specify to,

- leave that only for the Administrator account to have broad access and full control over the system while restricting other unnecessary access by other accounts and giving only the relevant and minimum access permissions to do their task.
  - Ensure 'Access this computer from the network is set to 'Administrators, Authenticated Users, ENTERPRISE DOMAIN CONTROLLERS' only

To establish the recommended configuration via GP, configure the following UI path: **Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Access this computer from the network**

  - Ensure 'Access this computer from the network is set to 'Administrators, Authenticated Users' only

To establish the recommended configuration via GP, configure the following UI path: **Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Access this computer from the network**

  - Ensure 'Add workstations to domain' is set to 'Administrators only

To establish the recommended configuration via GP, set the following UI path to Administrators: **Computer Configuration\Policies\Windows**

Settings\Security Settings\Local Policies\User Rights Assignment\Add workstations to domain

- Ensure 'Deny access to this computer from the network' to include 'Guests, Local account and members of Administrators group too.

To establish the recommended configuration via GP, configure the following UI path: **Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny access to this computer from the network**

- Ensure 'Deny log on as a batch job' to include 'Guests' too

To establish the recommended configuration via GP, set the following UI path to include Guests: **Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny log on as a batch job**

- Ensure 'Deny log on as a service to include 'Guests' too

To establish the recommended configuration via GP, set the following UI path to include Guests: **Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny log on as a service**

- Ensure 'Deny log on locally' to include 'Guests' too

To establish the recommended configuration via GP, set the following UI path to include Guests: **Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny log on locally**

- Ensure 'Deny log on through Remote Desktop Services' to include 'Guests' too

To establish the recommended configuration via GP, configure the following UI path: **Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny log on through Remote Desktop Services**

- Ensure a proper account lockout policy.
  - Ensure 'Account lockout duration' is set to '15 or more minute(s)

To establish the recommended configuration via GP, set the following UI path to 15 or more minute(s): **Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Account lockout duration**

- Ensure 'Account lockout threshold' is set to '5 or fewer invalid logon attempt(s), but not 0'

To establish the recommended configuration via GP, set the following UI path to 5 or fewer invalid login attempt(s), but not 0:

Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Account lockout threshold

- Ensure 'Allow Administrator account lockout' is set to 'Enabled'

To establish the recommended configuration via GP, set the following UI path to Enabled: **Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policies\Allow Administrator account lockout**

- Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)'

To establish the recommended configuration via GP, set the following UI path to 15 or more minute(s): **Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Reset account lockout counter after**

From Additional Resources:

- Use strong passwords and enforce password complexity requirements while allowing to rotate passwords regularly.
- Implement multifactor authentication for better security.
- Monitor and audit account activities for suspicious behavior and disable unused accounts.

c) **Security Implications:**

- ***Access Restrictions*** eliminate any type of unauthorized access and modification of system files done by the user accounts. Also, it reduces the risk of malware and other unauthorized activities from compromising the system integrity.
- ***Proper account lockout policy ensures that*** accounts are not easily compromised by brute-force attacks and unauthorized users are prevented from accessing systems and data.
- ***Continuous monitoring and logging for account activities*** enable the identification of suspicious activity as soon as possible to mitigate possible attacks or system compromises.

2. Authentication and authorization

a) **Default Settings:**

- ✓ Every user needs to have a local username and a password for authentication.
- ✓ Maximum Password age is set to 42 days in password rotating.
- ✓ The minimum Password age is 0 for stand-alone servers.

- ✓ The minimum password length is 0 for stand-alone servers.
- ✓ Password history is set to remember 0 for stand-alone servers.
- ✓ Password meets complexity requirements and is disabled for stand-alone servers.
- ✓ Based on the permission assigned by the administrator to each user, access requests will be authorized

b) Recommended Settings:

- Rotate passwords regularly and adhere to complex requirements for setting passwords.
  - Ensure 'Enforce password history is set to '24 or more password(s)'

To establish the recommended configuration via GP, set the following UI path to 24 or more password(s): **Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Enforce password history**

  - Ensure 'Maximum password age is set to '365 or fewer days, but not 0'

To establish the recommended configuration via GP, set the following UI path to 365 or fewer days, but not 0: **Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Maximum password age**

  - Ensure 'Minimum password age is set to '1 or more day(s)

To establish the recommended configuration via GP, set the following UI path to 1 or more day(s): **Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Minimum password age**

  - Ensure 'Minimum password length is set to '14 or more character(s)'

To establish the recommended configuration via GP, set the following UI path to 14 or more character(s): **Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Minimum password length**

  - Ensure 'Password must meet complexity requirements' is set to 'Enabled'

To establish the recommended configuration via GP, set the following UI path to Enabled: **Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Password must meet complexity requirements**

From Additional Resources:

- A group policy should be used to enforce password complexity requirements and expiration policies.
- Multi-factor authentication is implemented for all users who have administrative privileges.
- Implement Role-Based Access Control (RBAC) when granting permissions.
- Keep every authentication and authorization event monitored for any suspicious behavior.

c) Security Implications:

- ***MFA*** ensures that it is more difficult for attackers to gain access to systems, even if they have stolen passwords.
- ***Rotating passwords regularly*** ensures less risk from compromised passwords.
- ***Password complexity requirements and password expiration policies*** prevent attackers from guessing and cracking passwords or make it difficult to brute force.
- ***A strong access control method like RBAC*** helps to prevent unauthorized access to systems and data and it is very easy for the admin to grant/ revoke or modify users' access privileges.
- ***Monitoring authentication and authorization events for suspicious behavior*** helps to identify and take actions to mitigate it quickly

3. Network Security

a) Default Settings:

In the default domain, the Network Security on Windows Server 2019 is considerably advanced compared to older versions, with the implementation of Windows Defender with Advanced Security. It's basic functionalities include;

- ✓ A host-based firewall is on by default
- ✓ Most incoming ports that contain some kind of security risk are blocked but still not for 22 (SSH), 3389 (Remote Desktop Protocol), 80 (HTTP), and 443 (HTTPS) that could be used by attackers to enter the system.
- ✓ All outgoing traffic is allowed.
- ✓ Display a notification when a program is blocked from receiving inbound connections.
- ✓ The traffic will be logged and stored within the system files and the records exceeding the default limit (4096 KB) will overwrite the existing content.

b) Recommended Settings:

- Ensure the log files will be stored in the specified file.

`To establish the recommended configuration via GP, set the following UI path to %SystemRoot%\System32\logfiles\firewall\domainfw.log:` **`Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall`**

with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Logging Customize\Name

- Set an unlimited or considerably high file size for the file.

To establish the recommended configuration via GP, set the following UI path to 16,384 KB or greater: **Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Logging Customize\Size limit (KB)**

- Ensure the Information about dropped packets will be recorded in the firewall log file

To establish the recommended configuration via GP, set the following UI path to Yes: **Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Logging Customize\Log dropped packets**

- Ensure the Information about successful connections will be recorded in the firewall log file.

To establish the recommended configuration via GP, set the following UI path to Yes: **Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Logging Customize\Log successful connections**

c) Security Implications:

- ***Logging the events related to network traffic and events*** ensure that organizations can track and monitor all activity on their networks and it makes them to identify and investigate security incidents very keenly.
- **Logging of almost all events inclusive dropped packets and successful connections** ensure that the organization have not missed any important information in a case of emergency / any other security investigation.

4. Data security

a) Default Settings:

The default data security settings on Windows Server 2019 are relatively weak.

- ✓ data is not encrypted by default
- ✓ It does include a feature called BitLocker Drive encryption for the purpose of full drive encryption including OS driver and other drivers but it is not even enabled by default. (need to run the wizard)

b) Recommended Settings:

From Additional Resources:

- ➢ Use strong passwords and enforce password complexity requirements
- ➢ Rotate passwords regularly.
- ➢ Use multi-factor authentication (MFA)
- ➢ Monitor file access for suspicious activity.

*****Encrypt all sensitive data at rest and in transit.**

***** This is not suggested by CIS benchmarks but is the best solution that is generally recommended to ensure data confidentiality and integrity**

c) Security Implications:

- ***Strong passwords and password complexity requirements*** help to prevent attackers from guessing or cracking passwords.
- ***Rotating passwords regularly*** helps to mitigate the risk of compromised passwords.
- ***Multi-factor authentication*** provides an additional layer of security by requiring users to provide something they know (password) and something they have (token or biometrics) in order to authenticate.
- ***Monitoring data access for suspicious activity*** can help to identify and respond to attacks quickly.
- ***By encrypting all sensitive data,*** organizations can make it much more difficult for attackers to access it even if they have gained physical access to systems.

CIS Benchmark Guidelines suggest that the security of the data must be provided solely by the advancements and correct configurations done on authentication/ authorization and access controls settings but not by the encryption of data.

5. Logging and auditing

a) Default Settings: Windows server 2019 provides a comprehensive set of options to be followed in Logging and maintaining an audit policy. By default,

- ✓ 'Audit Credential Validation' is set to 'Success
- ✓ Audit Kerberos Authentication Service' is set to 'Success
- ✓ 'Audit Kerberos Service Ticket Operations' is set to 'Success
- ✓ 'Audit Directory Service Access' is set to Success

Not audited sections:

- ✓ 'Audit Application Group Management' is not audited
- ✓ Audit Distribution Group Management' is not audited
- ✓ Audit Other Account Management Events' is not audited
- ✓ 'Audit Process Creation' is not audited.
- ✓ 'Audit Directory Service Changes' are not audited

Successfully audited Sections as same as recommendations:

- ✓ 'Audit Security Group Management' is set to Success
- ✓ 'Audit User Account Management' is set to Success
- ✓ 'Audit Computer Account Management' is set to include 'Success'

b) Recommended Settings:

- o Ensure the Audit on Credential Validation / Kerberos Authentication Service / Kerberos Service Ticket Operations' is set to 'Success and Failure'

To establish the recommended configuration via GP, set the following UI path to Success and Failure: **Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Logon\Audit Credential Validation**

To establish the recommended configuration via GP, set the following UI path to Success and Failure: **Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Logon\Audit Kerberos Authentication Service**

To establish the recommended configuration via GP, set the following UI path to Success and Failure: **Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Logon\Audit Kerberos Service Ticket Operations**

- Ensure Audits on application group mgt and distribution grp mgt and other account management events are set to Success

To establish the recommended configuration via GP, set the following UI path to Success: **Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Application Group Management**

To establish the recommended configuration via GP, set the following UI path to include Success: **Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Distribution Group Management**

To establish the recommended configuration via GP, set the following UI path to include Success: **Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Other Account Management Events**

- Ensure process creation audit is set to success

To establish the recommended configuration via GP, set the following UI path to include Success: **Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Detailed Tracking\Audit Process Creation**

- Ensure 'Audit Directory Service Access' and 'Audit Directory Service Changes' are set to include 'Failure'

To establish the recommended configuration via GP, set the following UI path to include Failure: **Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\DS Access\Audit Directory Service Access**

- Ensure 'Audit Directory Service Changes' are set to Success

To establish the recommended configuration via GP, set the following UI path to include Success: **Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\DS Access\Audit Directory Service Changes**

- Ensure 'Audit Group Membership' is set to include 'Success

To establish the recommended configuration via GP, set the following UI path to include Success: **Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Group Membership**

- Ensure 'Audit PNP Activity' is set to include 'Success

To establish the recommended configuration via GP, set the following UI path to include Success: **Computer Configuration\Policies\Windows**

Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Detailed Tracking\Audit PNP Activity

c) Security Implications:

All the above recommendations ensure that **detailed audit logs** on authentication/authorization/execution and modification/data and settings data manipulation are enabled and collected for use in future investigations if a case arises.

CSI Benchmarks rationale that,

" **If no audit settings are configured, or if audit settings are too lax** on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur.

However, **if audit settings are too severe**, critically important entries in the Security log may be obscured by all of the meaningless entries, and computer performance and the available amount of data storage may be seriously affected. "

6. Device security

a) Default Settings:

Device security in Windows Server 2019 is a set of features that help to protect your servers from malware, attacks, unauthorized access and even system crashes. In this case, there is a few number of default configurations set but present themselves as options to be configured manually. The best option provided is Virtualization that enables through a feature called Device Guard that helps to prevent malware from running on your server by isolating trusted applications from untrusted code.

- ✓ Virtualization based security is disabled and it's settings are not set.
- ✓ Ensure 'Turn On Virtualization Based Security: Credential Guard Configuration' is set to 'Disabled'
- ✓ Device installations are widely open with broad access

b) Recommended Settings:

- Enable and configure Virtualization
  - Ensure 'Turn On Virtualization Based Security' is set to 'Enabled

To establish the recommended configuration via GP, set the following UI path to Enabled: **Computer Configuration\Policies\Administrative Templates\System\Device Guard\Turn On Virtualization Based Security**

- Ensure 'Turn On Virtualization Based Security: Select Platform Security Level' is set to 'Secure Boot' or higher

To establish the recommended configuration via GP, set the following UI path to Secure Boot or Secure Boot and DMA Protection: **Computer Configuration\Policies\Administrative Templates\System\Device Guard\Turn On Virtualization Based Security: Select Platform Security Level**

- Ensure 'Turn On Virtualization Based Security: Virtualization Based Protection of Code Integrity' is set to 'Enabled with UEFI lock

To establish the recommended configuration via GP, set the following UI path to Enabled with UEFI lock: **Computer Configuration\Policies\Administrative Templates\System\Device Guard\Turn On Virtualization Based Security: Virtualization Based Protection of Code Integrity**

- Ensure 'Turn On Virtualization Based Security: Require UEFI Memory Attributes Table' is set to 'True

To establish the recommended configuration via GP, set the following UI path to TRUE: **Computer Configuration\Policies\Administrative Templates\System\Device Guard\Turn On Virtualization Based Security: Require UEFI Memory Attributes Table**

- Ensure 'Turn On Virtualization Based Security: Credential Guard Configuration' is set to 'Enabled with UEFI lock

To establish the recommended configuration via GP, set the following UI path to Enabled with UEFI lock (on Member Servers only): **Computer Configuration\Policies\Administrative Templates\System\Device Guard\Turn On Virtualization Based Security: Credential Guard Configuration**

- Ensure 'Turn On Virtualization Based Security: Secure Launch Configuration' is set to 'Enabled'

To establish the recommended configuration via GP, set the following UI path to Enabled: **Computer Configuration\Policies\Administrative Templates\System\Device Guard\Turn On Virtualization Based Security: Secure Launch Configuration**

- Enable and configure device installation restrictions
  - Ensure 'Prevent device metadata retrieval from the Internet' is set to 'Enabled

To establish the recommended configuration via GP, set the following UI path to Enabled: **Computer Configuration\Policies\Administrative Templates\System\Device Installation\Prevent device metadata retrieval from the Internet**

c)Security Implications:

- ***Virtualization*** enables the creation of multiple isolated operating systems or applications on a single physical machine while improving efficiency and security, as each virtual machine can be configured and managed independently. It prevents any harm from misconfigurations or malicious act in a installed OS to be result in a system wide corruption.
- ***Device installation restrictions*** ensures that only authorized devices can be installed on a system. This can help to prevent malware and other security threats from being introduced to the system.

Part II

Proposals for Implementation of Future Server Installation

Based on the analysis, Pandora Company Limited to implement the following plan for hardening measures in upcoming server installations.

1. Physical Level Security:

The servers should be placed in a safe location with some security measures enabled such as **a locked room with limited physical access, real-time monitoring with CCTV cameras and using some authenticator to access the server room**. This will help to prevent unauthorized access to the servers. In addition to that, **setting up intrusion alarms, Fire suppression systems, environmental controls to regulate temperature, humidity etc and placing some security guards** may add another layer of security.

2. Device Level Security

Only authorized Access to the systems should be considered and the **authentication process may be based on any of something you have/know/ are but with a strong policy**. **Multi factor authentication** is also preferred since it provides an extra layer of security.

All installed applications must be configured securely and kept up to date with the latest security patches. It is much better to have secure and well-recognized tools to automatically download and install security updates and always need to keep in mind that patching can never win the “patch rat race”.

A hardware-level firewall could be added to the network to block unauthorized traffic from reaching the server. But Firewalls should be configured and maintained regularly to ensure that they are effective.

Antivirus software can be used to scan the servers for malware. It will help to remove any malware except Zero Day that may have infected the server. **Removing unnecessary software** will help to reduce the attack surface of the server which would be possible malware and vectors that could be compromised by the attackers with time.

3. OS Level Security

The first step would be to **use a secure operating system**. Operating systems usually come with some default configurations which would be less secure, thus it is **a must to harden** them and ensure security. **By keeping the OS up to date by installing OS security updates** often including security patches that can help to protect your server from vulnerabilities, a level of security of the OS can be confirmed.

Some OSes come with **inbuilt encryption, firewall, and logging features.** Thus, it would be very efficient and cost-effective if the full benefit of them could be taken by configuring them properly.

Always keep the **access privileges over the system/ files and directories/application properly configured and granted based on the principle of least privilege**. This will ensure that only authorized users have access to the resources they need, and that users cannot access data or systems that they are not authorized to access.

Authentication and authorization of the access is also mandatory since it governs the policy on only authorized users have access to the system/files and directories/applications. It is suggested **to use some next-level AAA mechanisms to be implemented such as Multi factor Authentication, Role Based access Controls, Access Control Lists etc.**

Logging and auditing would also helps to track user activity and identify any suspicious behavior. **A properly configured logging system may ensure that any useful information of evidence is not missed out for the investigation in case.**

4. Information Security

By enabling **only authorized users to enter the files and directories**, would be the best and the first countermeasure to enhance the information level security. Strong authentication measures prevent unauthorized access to data and any possible compromises while protecting CIA properties.

It is a must to **have a plan to back up the server's data regularly.** This will help to protect the data in case of a security breach or system corruption. Backups should be stored off-site in a secure location should also need to be properly secured.

Encryption can be used to secure the data stored on the server, by protecting it from unauthorized access to read/ write or manipulate data. This is a very good practice because the information will be still secure even if the server is physically compromised or completely under the control of an attacker.

Summary

The evaluation of Pandora Company Limited's IT infrastructure revealed a significant vulnerability: the servers were operating with default configurations, leaving the company open to potential cyber threats. This prompted a thorough security analysis and the implementation of essential hardening measures. The current system comprised an Apache web server on Rocky Linux 9, internal web applications on Windows Server 2019 R2, and a MySQL/MariaDB database server on Rocky Linux 9.
The chosen approach involved adopting the Center for Internet Security (CIS) benchmarks as a recognized framework for security hardening. The report emphasizes the importance of modifying default settings in key sections to enhance security, covering areas like Filesystem Configurations, Service Settings, User and Account Management, and Logging and Monitoring. This proactive strategy aims to fortify Pandora Company Limited's cybersecurity posture against potential future threats.

References

[1] Center for Information Security, " CIS Benchmarks: CIS Rocky Linux 9 Benchmark v1.0.0, [2022 December 13] Available at: https://downloads.cisecurity.org/ , To Download: https://drive.google.com/file/d/1N0iYf4c0O4Lu7QN3VeeLS5u9j8L4U5r-/view?usp=sharing

[2] Center for Information Security, " CIS Benchmarks: CIS Microsoft Windows Server 2019 Benchmark v2.0.0, [2023 April 14] ,Available at: https://downloads.cisecurity.org/, To Download: https://drive.google.com/file/d/1KTjFImESNyxdRvk6AshaTr03KNufbsWH/view?usp=sharing

[3]Robinharwood, ManikaDhiman,DhuratJ,v-alje,dknappetmsft and JohCobb on learn.microsost.com, " What is new in Windows Server 2019" [2022 December 15], Available at: https://learn.microsoft.com/en-us/windows-server/get-started/whats-new-in-windows-server-2019

[4] Thomas Jung, "Windows Server 2019 OS Hardening" on AT&T Business, [2020 March 23], Available At :https://cybersecurity.att.com/blogs/security-essentials/windows-server-2019-os-hardening