8/31/2023

System Hardening

Pandora Company Limited

M.N.M Muaadh
200401J

What is Hardening?

Security hardening refers to the practice of enhancing security measures on an operating system (OS) to protect against potential vulnerabilities. It is a continuous process that involves a range of activities including software updates, configurations, and monitoring to limit the potential attack vectors. In the context of Pandora Company Limited, a hypothetical organization that could be involved in any sector from technology to healthcare, the implications of OS security hardening are critical for various reasons.

Importance of System Hardening for Pandora Company Limited

- Data Protection

Pandora Company likely handles a significant amount of sensitive data, be it customer information, intellectual property, or internal communications. Any security lapse in the OS could mean unauthorized access to this data.

- Business Continuity

The inability to access resources due to an attack could cause severe disruptions to the daily operations, leading to financial loss and damage to reputation.

- Legal and Compliance Risks

Non-compliance with data protection laws could lead to hefty fines and legal issues. Ensuring the OS is secure can be a cornerstone in an overall compliance strategy.

- Customer Trust

Customers and clients entrust their data to Pandora. A security breach could quickly erode that trust, making it difficult to retain clients or attract new ones.

How Security Hardening Helps ?

- Reducing Attack Surface:

Through practices such as disabling unnecessary services, ports, and protocols, OS hardening narrows the number of ways attackers can gain unauthorized access.

- Data Encryption:

Hardening often involves the encryption of data at rest and in transit, making it more difficult for unauthorized parties to make sense of it even if accessed.

- Multi-Factor Authentication (MFA):

Implementing MFA at the OS level adds an extra layer of security, making it harder for attackers to breach the system using stolen or brute-forced credentials.

- Regular Updates and Patches:

Keeping the OS updated ensures that it is armed against known vulnerabilities, which is crucial for maintaining a secure environment.

- Audit Trails:

A hardened OS often includes improved logging and monitoring capabilities, allowing Pandora to track all system access and changes, which could be crucial for forensic analysis following any security incidents.

- Access Control:

Proper hardening includes fine-tuning user permissions to adhere to the principle of least privilege, meaning each user has only the permissions necessary to perform their job and nothing more.

- Resource Isolation:

Security hardening can ensure that if one part of the system is compromised, the attacker cannot easily move laterally through the network, protecting other critical business assets.

Identification of Hardening Frameworks

The decision has been made to adopt the Center for Internet Security (CIS) as the framework for establishing security benchmarks for Rocky Linux 9 Server and Windows Server 2019 R2 systems within the organization. CIS offers comprehensive, consensus-driven guidelines that are highly regarded for their effectiveness in fortifying operating systems against vulnerabilities. This choice serves as a strategic move to secure the servers, providing robust protection against potential security threats and aligning with industry best practices.

CIS Rocky Linux 9 Benchmark

Key Hardening Sections

1. Initial Setup

Items in this section are advised for all systems, but may be difficult or require extensive preparation after the initial setup of the system.

Default Settings

- A number of uncommon filesystem types are supported under Linux.
- The default installation of Rocky Linux 9 creates a single partition for the root filesystem

I. File System Configuration

Directories that are used for system-wide functions can be further protected by placing them on separate partitions. This provides protection for resource exhaustion and enables the use of mounting options that are applicable to the directory's intended use. Users' data can be stored on separate partitions and have stricter mount options. A user partition is a filesystem that has been established for use by the users and does not contain software for system operations. The recommendations in this section are easier to perform during initial system installation. If the system is already installed, it is recommended that a full backup be performed before repartitioning the system.

i. Disable Unused File Systems

A number of uncommon filesystem types are supported under Linux. Removing support for unneeded filesystem types reduces the local attack surface of the system. If a filesystem type is not needed it should be disabled. Native Linux file systems are designed to ensure that built-in security controls function as expected. Non-native filesystems can lead to unexpected consequences to both the security and functionality of the system and should be used with caution. Many filesystems are created for niche use cases and are not maintained and supported as the operating systems are updated and patched. Users of non-native filesystems should ensure that there is attention and ongoing support for them, especially in light of frequent operating system changes.

II. Configure Software Updates

Fedora 34/CentOS 9 stream derived Linux distributions use dnf (previously yum) to install and update software packages. Patch management procedures may vary widely between enterprises. Large enterprises may choose to install a local updates server that can be used in place of their distributions servers, whereas a single deployment of a system may prefer to get updates directly. Updates can be performed automatically or manually, depending on the site's policy for patch management. Organizations may prefer to test patches against their environment on a non-production system before rolling out to production. For the purpose of this benchmark, the requirement is to ensure that a patch management process is defined and maintained, the specifics of which are left to the organization.

III. Filesystem Integrity Checking

AIDE is a file integrity checking tool, similar in nature to Tripwire. While it cannot prevent intrusions, it can detect unauthorized changes to configuration files by alerting when the files are changed. When setting up AIDE, decide internally what the site policy will be concerning integrity checking. Review the AIDE quick start guide and AIDE documentation before proceeding.

1. Ensure AIDE is installed (Automated)

Advanced Intrusion Detection Environment (AIDE) is a intrusion detection tool that uses predefined rules to check the integrity of files and directories in the Linux operating system. AIDE has its own database to check the integrity of files and directories. AIDE takes a snapshot of files and directories including modification times, permissions, and file hashes which can then be used to compare against the current state of the filesystem to detect modifications to the system.

By monitoring the filesystem state compromised files can be detected to prevent or limit the exposure of accidental or malicious misconfigurations or modified binaries.

2. Ensure filesystem integrity is regularly checked (Automated)

Periodic checking of the filesystem integrity is needed to detect changes to the filesystem.

Periodic file checking allows the system administrator to determine on a regular basis if critical files have been changed in an unauthorized fashion.

3. Ensure cryptographic mechanisms are used to protect the integrity of audit tools (Automated)

Audit tools include, but are not limited to, vendor-provided and open source audit tools needed to successfully view and manipulate audit information system activity and records. Audit tools include custom queries and report generators.

Protecting the integrity of the tools used for auditing purposes is a critical step toward ensuring the integrity of audit information. Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity.

IV. Secure Boot Settings

The recommendations in this section focus on securing the bootloader and settings involved in the boot process directly.

i. Ensure bootloader password is set (Automated)

Setting the boot loader password will require that anyone rebooting the system must enter a password before being able to set command line boot parameters.

Requiring a boot password upon execution of the boot loader will prevent an unauthorized user from entering boot parameters or changing the boot partition. This prevents users from weakening security (e.g. turning off SELinux at boot time).

ii. Ensure permissions on bootloader config are configured (Automated)

The grub files contain information on boot settings and passwords for unlocking boot options.

Setting the permissions to read and write for root only prevents non-root users from seeing the boot parameters or changing them. Non-root users who read the boot parameters may be able to identify weaknesses in security upon boot and be able to exploit them.

V. Additional Process Hardening

i. Ensure core dump storage is disabled (Automated)

A core dump is the memory of an executable program. It is generally used to determine why a program aborted. It can also be used to glean confidential information from a core file.

A core dump includes a memory image taken at the time the operating system terminates an application. The memory image could contain sensitive data and is generally useful only for developers trying to debug problems.

ii. Ensure core dump backtraces are disabled (Automated)

A core dump is the memory of an executable program. It is generally used to determine why a program aborted. It can also be used to glean confidential information from a core file.

A core dump includes a memory image taken at the time the operating system terminates an application. **The memory image could contain sensitive data and is generally useful only for developers trying to debug problems, increasing the risk to the system.**

iii. Ensure address space layout randomization (ASLR) is enabled (Automated)

Address space layout randomization (ASLR) is an exploit mitigation technique which randomly arranges the address space of key data areas of a process.

Randomly placing virtual memory regions will make it difficult to write memory page exploits as the memory placement will be consistently shifting.

VI. Mandatory Access Control

Mandatory Access Control (MAC) provides an additional layer of access restrictions to processes on top of the base Discretionary Access Controls. By restricting how processes can access files and resources on a system the potential impact from vulnerabilities in the processes can be reduced.

Impact: Mandatory Access Control limits the capabilities of applications and daemons on a system, while this can prevent unauthorized access the configuration of MAC can be complex and difficult to implement correctly preventing legitimate access from occurring

i. Configure SELinux

SELinux implements Mandatory Access Control (MAC). Every process and system resource has a special security label called an SELinux context. A SELinux context, sometimes referred to as an SELinux label, is an identifier which abstracts away the system-level details and focuses on the security properties of the entity. Not only does this provide a consistent way of referencing objects in the SELinux policy, but it also removes any ambiguity that can be found in other identification methods. For example, a file can have multiple valid path names on a system that makes use of bind mounts.

The SELinux policy uses these contexts in a series of rules which define how processes can interact with each other and the various system resources. By default, the policy does not allow any interaction unless a rule explicitly grants access.

VII. Command Line Warning Banners

Presenting a warning message prior to the normal user login may assist in the prosecution of trespassers on the computer system. Changing some of these login banners also has the side effect of hiding OS version information and other detailed system information from attackers attempting to target specific exploits at a system. Guidelines published by the US Department of Defense require that warning messages include at least the name of the organization that owns the system, the fact that the system is subject to monitoring and that such monitoring is in compliance with local statutes, and that use of the system implies consent to such monitoring.

VIII. GNOME Display Manager

The GNOME Display Manager (GDM) is a program that manages graphical display servers and handles graphical user logins. Note: If GDM is not installed on the system, this section can be skipped

i. Ensure GNOME Display Manager is removed (Automated)
ii. Ensure GDM login banner is configured (Automated)
iii. Ensure GDM disable-user-list option is enabled (Automated)
iv. Ensure GDM screen locks when the user is idle (Automated)
v. Ensure GDM screen locks cannot be overridden (Automated)
vi. Ensure GDM automatic mounting of removable media is disabled (Automated)
vii. Ensure GDM disabling automatic mounting of removable media is not overridden (Automated)
viii. Ensure GDM autorun-never is enabled (Automated)
ix. Ensure GDM autorun-never is not overridden (Automated)
x. Ensure XDCMP is not enabled (Automated)

IX. Ensure updates, patches, and additional security software are installed (Manual)

Periodically patches are released for included software either due to security flaws or to include additional functionality.

Newer patches may contain security enhancements that would not be available through the latest full update. As a result, it is recommended that the latest software patches be used to take advantage of the latest functionality. As with any software installation, organizations need to determine if a given update meets their requirements and verify the compatibility and supportability of any additional software against the update revision that is selected

X. Ensure system-wide crypto policy is not legacy (Automated)

The system-wide crypto-policies followed by the crypto core components allow consistently deprecating and disabling algorithms system-wide.

If the Legacy system-wide crypto policy is selected, it includes support for TLS 1.0, TLS 1.1, and SSH2 protocols or later. The algorithms DSA, 3DES, and RC4 are allowed, while RSA and Diffie-Hellman parameters are accepted if larger than 1023-bits. **These legacy protocols and algorithms can make the system vulnerable to attacks, including those listed in RFC 7457**

Security Implications
The recommended settings for filesystem configurations can help to improve security by

- Reducing the attack surface by isolating different types of data.
- Preventing the execution of malicious code.
- Verifying the authenticity of packages before they are installed.
- Detecting unauthorized changes to the filesystem.
- Preventing unauthorized access to files and directories.

2. Services

While applying system updates and patches helps correct known vulnerabilities, one of the best ways to protect the system against as yet unreported vulnerabilities is to disable all services that are not required for normal system operation. This prevents the exploitation of vulnerabilities discovered at a later date. If a service is not enabled, it cannot be exploited. The actions in this section of the document provide guidance on some services which can be safely disabled and under which circumstances, greatly reducing the number of possible threats to the resulting system. **Additionally, some services which should remain enabled but with secure configuration are covered as well as insecure service clients.**

Default Settings

- The default service settings in Rocky Linux 9 are generally secure. However, some unnecessary installations have been enabled in rocky Linux.

I. Time Synchronization

It is recommended that physical systems and virtual guests lacking direct access to the physical host's clock be configured to synchronize their time using a service such as NTP or chrony.

i. Ensure time synchronization is in use (Automated)

System time should be synchronized between all systems in an environment. This is typically done by establishing an authoritative time server or set of servers and having all systems synchronize their clocks to them.

Note: If another method for time synchronization is being used, this section may be skipped

ii. Ensure chrony is configured (Automated)

If chrony is in use on the system proper configuration is vital to ensuring time synchronization is working properly.

II. Special Purpose Services

This section describes services that are installed on systems that specifically need to run these services. **If any of these services are not required, it is recommended that the package be removed, or the service be masked to reduce the potential attack surface**.

Note: This should not be considered a comprehensive list of services not required for normal system operation. You may wish to consider additions to those listed here for your environment.

i. Ensure xorg-x11-server-common is not installed (Automated)

The X Window System provides a Graphical User Interface (GUI) where users can have multiple windows in which to run programs and various add on. The X Windows system is typically used on workstations where users login, but not on servers where users typically do not login.

Unless your organization specifically requires graphical login access via X Windows, remove it to reduce the potential attack surface.

ii. Ensure Avahi Server is not installed (Automated)

Avahi is a free zeroconf implementation, including a system for multicast DNS/DNS-SD service discovery. Avahi allows programs to publish and discover services and hosts running on a local network with no specific configuration. For example, a user can plug a computer into a network and Avahi automatically finds printers to print to, files to look at and people to talk to, as well as network services running on the machine.

Automatic discovery of network services is not normally required for system functionality. It is recommended to remove this package to reduce the potential attack surface.

iii. Ensure CUPS is not installed (Automated)

The Common Unix Print System (CUPS) provides the ability to print to both local and network printers. A system running CUPS can also accept print jobs from remote systems and print them to local printers. It also provides a web based remote administration capability.

If the system does not need to print jobs or accept print jobs from other systems, it is recommended that CUPS be removed to reduce the potential attack surface.

Note: Removing CUPS will prevent printing from the system

iv. Ensure DHCP Server is not installed (Automated)

The Dynamic Host Configuration Protocol (DHCP) is a service that allows machines to be dynamically assigned IP addresses.

Unless a system is specifically set up to act as a DHCP server, it is recommended that the dhcp-server package be removed to reduce the potential attack surface.

v. Ensure DNS Server is not installed (Automated)

The Domain Name System (DNS) is a hierarchical naming system that maps names to IP addresses for computers, services and other resources connected to a network.

Unless a system is specifically designated to act as a DNS server, it is recommended that the package be removed to reduce the potential attack surface.

vi. Ensure VSFTP Server is not installed (Automated)

FTP (File Transfer Protocol) is a traditional and widely used standard tool for transferring files between a server and clients over a network, especially where no authentication is necessary (permits anonymous users to connect to a server).

Unless there is a need to run the system as a FTP server, it is recommended that the package be removed to reduce the potential attack surface.

vii. Ensure TFTP Server is not installed (Automated)

Trivial File Transfer Protocol (TFTP) is a simple protocol for exchanging files between two TCP/IP machines. TFTP servers allow connections from a TFTP Client for sending and receiving files.

Unless there is a need to run the system as a TFTP server, it is recommended that the package be removed to reduce the potential attack surface. TFTP does not have built-in encryption, access control or authentication. This makes it very easy for an attacker to exploit TFTP to gain access to files

viii. Ensure a web server is not installed (Automated)

Web servers provide the ability to host web site content.

Unless there is a need to run the system as a web server, it is recommended that the packages be removed to reduce the potential attack surface.

Note: Several http servers exist. They should also be audited, and removed, if not required

ix. Ensure IMAP and POP3 server is not installed (Automated)

dovecot is an open source IMAP and POP3 server for Linux based systems.

Unless POP3 and/or IMAP servers are to be provided by this system, it is recommended that the package be removed to reduce the potential attack surface.

Note: Several IMAP/POP3 servers exist and can use other service names. These should also be audited and the packages removed if not required.

x. Ensure Samba is not installed (Automated)

The Samba daemon allows system administrators to configure their Linux systems to share file systems and directories with Windows desktops. Samba will advertise the file systems and directories via the Server Message Block (SMB) protocol. Windows desktop users will be able to mount these directories and file systems as letter drives on their systems.

If there is no need to mount directories and file systems to Windows systems, then this package can be removed to reduce the potential attack surface.

xi. Ensure HTTP Proxy Server is not installed (Automated)

Squid is a standard proxy server used in many distributions and environments.

Unless a system is specifically set up to act as a proxy server, it is recommended that the squid package be removed to reduce the potential attack surface.

Note: Several HTTP proxy servers exist. These should be checked and removed unless required.

xii. Ensure net-snmp is not installed (Automated)

The Simple Network Management Protocol (SNMP) server is used to listen for SNMP commands from an SNMP management system, execute the commands or collect the information and then send results back to the requesting system.

The SNMP server can communicate using SNMPv1, which transmits data in the clear and does not require authentication to execute commands. SNMPv3 replaces the simple/clear text password sharing used in SNMPv2 with more securely encoded parameters. **If the the SNMP service is not required, the net-snmp package should be removed to reduce the attack surface of the system**

xiii. Ensure telnet-server is not installed (Automated)

The telnet-server package contains the telnet daemon, which accepts connections from users from other systems via the telnet protocol.

The telnet protocol is insecure and unencrypted**. The use of an unencrypted transmission medium could allow a user with access to sniff network traffic the ability to steal credentials. The ssh package provides an encrypted session and stronger security.**

III. Service Clients

A number of insecure services exist. **While disabling the servers prevents a local attack against these services, it is advised to remove their clients unless they are required.**

Note: This should not be considered a comprehensive list of insecure service clients. You may wish to consider additions to those listed here for your environment.

Security Implications

- Reducing the attack surface by disabling unused services.
- Preventing unauthorized access by using strong authentication methods.
- Hardening the configuration of enabled services to prevent unauthorized access and malicious activity.
- Tracking suspicious activity and identifying security incidents by configuring logging for all services.
- Detecting and responding to security incidents quickly by monitoring all services for unauthorized activity.

3. Network Configuration

This section provides guidance on for securing the network configuration of the system through kernel parameters, access list control, and firewall settings.

Default Settings

- The default network configuration settings in Rocky Linux 9 are generally not very secure. The default installation of Rocky Linux 9 uses the NetworkManager service to manage network interfaces.

I. Disable unused network protocols and devices

To reduce the attack surface of a system, unused network protocols and devices should be disabled. The Linux kernel modules support several network protocols that are not commonly used. If these protocols are not needed, it is recommended that they be disabled in the kernel

II. Network Parameters (Host Only)

The following network parameters are intended for use if the system is to act as a host only. A system is considered host only if the system has a single interface, or has multiple interfaces but will not be configured as a router.

III. Network Parameters (Host and Router)

The following network parameters are intended for use on both host only and router systems. A system acts as a router if it has at least two interfaces and is configured to perform routing functions.'

IV. Configure Host Based Firewall

A Host Based Firewall, on a Linux system, is a set of rules. When a data packet moves into or out of a protected network space, its contents (in particular, information about its origin, target, and the protocol it plans to use) are tested against the firewall rules to see if it should be allowed through To provide a Host Based Firewall, the Linux kernel includes support for nftables.

i. Configure a firewall utility
ii. Configure firewall rules

Security Implications

- Reducing the attack surface by configuring static IP addresses.
- Preventing unauthorized access by enabling firewall rules.
- Protecting passwords by using strong passwords and SSH keys.
- Deterring unauthorized access by disabling remote root login.
- Detecting suspicious activity by monitoring network traffic.

4. Logging and Auditing

The items in this section describe how to configure logging, log monitoring, and auditing, using tools included in most distributions. It is recommended that rsyslog be used for logging (with logwatch providing summarization) and auditd be used for auditing (with aureport providing summarization) to automatically monitor logs for intrusion attempts and other suspicious system behavior.

Default Settings

- Rockey Linux default enables the logging and auditing but in default configuration difficult to track the logging and auditing.

I. Configure System Accounting (auditd)

The Linux Auditing System operates on a set of rules that collects certain types of system activity to facilitate incident investigation, detect unauthorized access or modification of data. By default events will be logged to /var/log/audit/audit.log, which can be configured in /etc/audit/auditd.conf.

i. Ensure Auditing is Enabled
ii. Configure Data Retention
iii. Configure auditd Rules
iv. Configure auditd file access

II. Configure Logging Logging

Services should be configured to prevent information leaks and to aggregate logs on a remote server so that they can be reviewed in the event of a system compromise. A centralized log server provides a single point of entry for further analysis, monitoring and filtering.

Security principals for logging

- Ensure transport layer security is implemented between the client and the log server.
- Ensure that logs are rotated as per the environment requirements.
- Ensure all locally generated logs have the appropriate permissions.
- Ensure all security logs are sent to a remote log server.
- Ensure the required events are logged.

Security Implications

The recommended settings for logging and auditing can help to improve security by:

- Detecting suspicious activity early.
- Investigating security incidents quickly.
- Identifying unauthorized access to the system.
- Tracking changes to system configuration files.
- Deterring attackers by making it more difficult to hide their activities.

5. Access, Authentication and Authorization

Default Settings

- By default, Rocky Linux 9 uses a default AAA configuration that is not very secure. This configuration can be easily exploited by attackers.
- The following are some recommended settings for AAA.

I. Configure time-based job schedulers

cron is a time-based job scheduler used to schedule jobs, commands or shell scripts, to run periodically at fixed times, dates, or intervals. at provides the ability to execute a command or shell script at a specified date and hour, or after a given interval of time.

II. Configure SSH Server

SSH is a secure, encrypted replacement for common login services such as telnet, ftp, rlogin, rsh, and rcp. It is strongly recommended that sites abandon older cleartext login protocols and use SSH to prevent session hijacking and sniffing of sensitive data off the network.

III. Configure privilege escalation

There are various tools which allows a permitted user to execute a command as the superuser or another user, as specified by the security polic

IV. Configure authselect

Authselect is a utility that simplifies the configuration of user authentication. Authselect offers two ready-made profiles that can be universally used with all modern identity management systems Authselect makes testing and troubleshooting easy because it only modifies files in these directories:

- /etc/nsswitch.conf
- /etc/pam.d/* files
- /etc/dconf/db/distro.d/* files

V. Configure PAM

PAM (Pluggable Authentication Modules) is a service that implements modular authentication modules on UNIX systems. PAM is implemented as a set of shared objects that are loaded and executed when a program needs to authenticate a user. Files for PAM are typically located in the /etc/pam.d directory. PAM must be carefully configured to secure system authentication. While this section covers some of PAM, please consult other PAM resources to fully understand the configuration capabilities.

VI. User Accounts and Environment

This section provides guidance on setting up secure defaults for system and user accounts and their environment.

Default Settings

- By default, Rocky Linux 9 uses a default AAA configuration that is not very secure. This configuration can be easily exploited by attackers.
- The following are some recommended settings for AAA.

6. System Maintenance

Recommendations in this section are intended as maintenance and are intended to be checked on a frequent basis to ensure system stability. Many recommendations do not have quick remediations and require investigation into the cause and best fix available and may indicate an attempted breach of system security.

Default Settings

- Rocky Linux 9 does not have any system maintenance tasks enabled. This means that the system is not protected from known vulnerabilities and that data loss can occur if the system is not backed up regularly.

I. System File Permissions

This section provides guidance on securing aspects of system files and directories.

II. Local User and Group Settings

This section provides guidance on securing aspects of the local users and groups.

Security Implications

The recommended settings for system maintenance can help to improve security by

- Reducing the attack surface by keeping software up to date and applying security patches promptly.
- Detecting and fixing vulnerabilities early by enabling logging and auditing.
- Identifying and mitigating risks by using a security scanner.
- Recovering from data loss or system failure by creating regular backups and testing them regularly.
- Implementing a disaster recovery plan to minimize the impact of a security incident

CIS Windows Server 2019 R2 Benchmarks

CIS Microsoft Windows Server 2019 Benchmark

v2.0.0 - 04-14-2023

Key Hardening Sections

1. Account Policies

This section contains recommendations for account policies.

Default Settings

- 24 passwords remembered on domain members. 0 passwords remembered on standalone servers.
- Maximum password age is 42 days and minimum password age is 1 day for domain members and 0 days for stand-alone members.
- Minimum password length is 7 characters on domain members, and 0 characters on stand-alone servers.
- Password complexity enable on domain members, disable on stand-alone servers.
- In default server has 0 failed logon attempts.

I. Password Policy

i. Ensure 'Enforce password history' is set to '24 or more password(s)' (Automated)

ii. Ensure 'Maximum password age' is set to '365 or fewer days, but not 0' (Automated)

iii. Ensure 'Minimum password age' is set to '1 or more day(s)' (Automated)

iv. Ensure 'Minimum password age' is set to '1 or more day(s)' (Automated)

v. Ensure 'Password must meet complexity requirements' is set to 'Enabled' (Automated)
vi. Ensure 'Store passwords using reversible encryption' is set to 'Disabled' (Automated)

II. Account Lockout Policy

i. Ensure 'Account lockout duration' is set to '15 or more minute(s)' (Automated
ii. Ensure 'Account lockout threshold' is set to '5 or fewer invalid logon attempt(s), but not 0' (Automated)
iii. Ensure 'Allow Administrator account lockout' is set to 'Enabled' (Manual)
iv. Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)' (Automated)

Security Implications

- Default and recommended settings for password and account policies impact system security.
- Default settings prioritize user convenience but expose the system to password guessing attacks.
- Recommended settings enhance security by enforcing strong passwords, regular updates, and preventing repeated login attempts.
- Choice between default and recommended settings involves balancing user convenience and system safety.
- Recommended settings offer improved protection against cyber threats, making data safer and the system more secure.

2. Local Policies

This section contains recommendations for local policies

Default Settings

- Administrators, Authenticated Users, Enterprise Domain Controllers, Everyone, Pre-Windows 2000 Compatible Access.
- Default this computer access from the network is set to Administrators, Backup Operators, Users, and Everyone.
- Default backup and files directories are Administrators, Backup operators, and server operators.
- Default force shutdown from a remote system is set to Administrators and server operators.
- Default increase scheduling priority is set to Administrators, Window Manager\Window Manager Group.
- Default load and unload device drivers are set to Administrators and print operators.

- Default restore files and directories are set to administrators, backup operators, and server operators.
- Default shutdown of the system is set to Administrators, Backup Operators, Server Operators, Print Operators.
- Users are able to use Microsoft accounts with Windows.
- Domain controller LDAP server channel binding token requirements are set to Never.
- Default interactive logon: Do not display the last user name set to Disabled.
- Default interactive logon: Require Domain Controller Authentication to unlock workstation is set to Disabled.
- Default Microsoft network client: Digitally sign communications (always) is set to 'Disabled'.
- Default network security: Allow Local System to use computer identity for NTLM is set to 'Disabled'
- Default network security: Configure encryption types allowed for Kerberos is set to RC4_HMAC_MD5, AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types.
- Default User Account Control: Admin Approval Mode for the Built-in Administrator account is set to Disabled.
- Disable User Account Control: Detect application installations and prompt for elevation is set to Disabled.

I. Audit Policies

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

II. User Rights Assignments

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

i. Ensure 'Access Credential Manager as a trusted caller' is set to 'No One' (Automated)

ii. Ensure 'Access this computer from the network' is set to 'Administrators, Authenticated Users, ENTERPRISE DOMAIN CONTROLLERS' (DC only) (Automated)

iii. Ensure 'Access this computer from the network' is set to 'Administrators, Authenticated Users' (MS only) (Automated)

iv. Ensure 'Act as part of the operating system' is set to 'No One' (Automated)

v. Ensure 'Add workstations to domain' is set to 'Administrators' (DC only) (Automated)

vi. Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE' (Automated)
vii. Ensure 'Allow log on locally' is set to 'Administrators' (Automated)
viii. Ensure 'Allow log on through Remote Desktop Services' is set to 'Administrators' (DC only) (Automated)
ix. Ensure 'Allow log on through Remote Desktop Services' is set to 'Administrators, Remote Desktop Users' (MS only) (Automated)
x. Ensure 'Back up files and directories' is set to 'Administrators' (Automated)
xi. Ensure 'Change the system time' is set to 'Administrators, LOCAL SERVICE' (Automated)

III. Security Options

This section contains recommendations for security options.

Security Implications

- Strengthened authentication and encryption for data protection.
- Admin Approval Mode and elevation prompts ensure controlled admin actions.
- Adoption of recommended settings bolsters system defense.
- Elevates data safeguarding measures.
- Encourages a forward-thinking cybersecurity approach.

3. Event Log

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

4. Restricted Groups

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

5. System Services

This section contains recommendations for system services.

Default Settings

- ‘Print Spooler (Spooler)’ is set in automatic ' (DC only).
- ‘Print Spooler (Spooler)’ is set in automatic ' (MS only).

I. (L1) Ensure 'Print Spooler (Spooler)' is set to 'Disabled' (DC only) (Automated)
II. (L2) Ensure 'Print Spooler (Spooler)' is set to 'Disabled' (MS only) (Automated)

Security Implications

- Reduces vulnerabilities and potential remote attacks.
- Minimizes risks from malware and unauthorized access.
- Boosts system resilience against breaches and threats.

6. Registry

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

7. File System

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

8. Wired Network (IEEE 802.3) Policies

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

9. Windows Defender Firewall with Advanced Security (formerly Windows Firewall with Advanced Security)

Default Settings

- Default 'Windows Firewall: Domain: Settings: Display a notification' is set to Yes.
- Default 'Windows Firewall: Domain: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\pfirewall.log'.
- Default 'Windows Firewall: Domain: Logging: Log dropped packets' is set to No.
- Default 'Windows Firewall: Domain: Logging: Log successful connections' is set to No.
- Default 'Windows Firewall: Private: Settings: Display a notification' is set to Yes.
- Default 'Windows Firewall: Private: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\pfirewall.log '.
- Default 'Windows Firewall: Private: Logging: Log dropped packets' is set to No.
- Default 'Windows Firewall: Private: Logging: Log successful connections' is set to No.
- Default 'Windows Firewall: Public: Settings: Display a notification' is set to Yes.
- Default 'Windows Firewall: Public: Settings: Apply local firewall rules' is set to Yes.
- Default 'Windows Firewall: Public: Settings: Apply local connection security rules' is set to Yes.
- Default 'Windows Firewall: Public: Logging: Log dropped packets' is set to No.
- Default 'Windows Firewall: Public: Logging: Log successful connections' is set to No.

I. Domain Profile

This section contains recommendations for the Domain Profile of the Windows Firewall.

- Ensure 'Windows Firewall: Domain: Settings: Display a notification' is set to 'No'.
- Ensure 'Windows Firewall: Domain: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\domainfw.log'.
- Ensure 'Windows Firewall: Domain: Logging: Log dropped packets' is set to 'Yes'.
- Ensure 'Windows Firewall: Domain: Logging: Log successful connections' is set to 'Yes'.

II. Private Profile

This section contains recommendations for the Private Profile of the Windows Firewall.

- Ensure 'Windows Firewall: Private: Settings: Display a notification' is set to 'No'.
- Ensure 'Windows Firewall: Private: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\privatefw.log'.
- Ensure 'Windows Firewall: Private: Logging: Log dropped packets' is set to 'Yes'.
- Ensure 'Windows Firewall: Private: Logging: Log successful connections' is set to 'Yes'.

III. Public Profile

This section contains recommendations for the Private Profile of the Windows Firewall.

- Ensure 'Windows Firewall: Public: Settings: Display a notification' is set to 'No'.
- Ensure 'Windows Firewall: Public: Settings: Apply local firewall rules' is set to 'No'.
- Ensure 'Windows Firewall: Public: Settings: Apply local connection security rules' is set to 'No'.
- Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set to 'Yes'.
- Ensure 'Windows Firewall: Public: Logging: Log successful connections' is set to 'Yes'.

Security Implications

- Recommended settings significantly enhance system security compared to defaults.
- Settings balance robust protection and streamlined operation.
- Disabling notifications minimizes distractions during critical tasks.
- Comprehensive tracking of dropped packets and successful connections increases threat visibility.
- Certain rule applications are disabled for a more secure network environment.
- Logged data aids compliance efforts and tracking authorized access.
- The deliberate approach strengthens defenses and promotes operational excellence.

10. Network List Manager Policies

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

11. Wireless Network (IEEE 802.11) Policies

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

12. Public Key Policies

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent

13. Software Restriction Policies

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent

14. Network Access Protection NAP Client Configuration

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

15. Application Control Policies

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

16. IP Security Policies

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

17. Advanced Audit Policy Configuration

This section contains recommendations for configuring the Windows audit facilities.

Default Settings

- Default 'Audit Credential Validation' is set to ‘Success’.
- Default 'Audit Kerberos Authentication Service' is set to ‘Success’.
- Default 'Audit Application Group Management' is No Auditing.
- Default ‘Audit Distribution Group Management' is No Auditing.
- Default ‘Audit User Account Management’ is set to ‘Success’.
- Default 'Audit Process Creation' is No Auditing.
- Default 'Audit Directory Service Access' is set to include Success.
- Default 'Audit Directory Service Changes' is No Auditing.
- Default 'Audit Account Lockout' is set to include Success.
- Default 'Audit Other Logon/Logoff Events' is No Auditing.

- Default 'Audit Detailed File Share' is No Auditing.
- Default 'Audit File Share' is No Auditing.
- Default 'Audit MPSSVC Rule-Level Policy Change' is No Auditing.
- Default 'Audit Sensitive Privilege Use' is No Auditing.
- Default 'Audit IPsec Driver' is No Auditing.
- Default 'Audit Security System Extension' is No Auditing.

I. Account Logon

- Ensure 'Audit Credential Validation' is set to 'Success and Failure'.
- Ensure 'Audit Kerberos Authentication Service' is set to 'Success and Failure'.

II. Account Management

- Ensure 'Audit Application Group Management' is set to 'Success and Failure'.
- Ensure 'Audit Distribution Group Management' is set to include 'Success'.
- Ensure 'Audit User Account Management' is set to 'Success and Failure'.

III. Detailed Tracking

- Ensure 'Audit Process Creation' is set to include 'Success'.

IV. DS Access

- Ensure 'Audit Directory Service Access' is set to include 'Failure'.
- Ensure 'Audit Directory Service Changes' is set to include 'Success'.

V. Logon / Logoff

- Ensure 'Audit Directory Service Access' is set to include 'Failure'.
- Ensure 'Audit Directory Service Changes' is set to include 'Success'.

VI. Object Access

- Ensure 'Audit Detailed File Share' is set to include 'Failure'.
- Ensure 'Audit File Share' is set to 'Success and Failure'

VII. Policy Change

- Ensure 'Audit MPSSVC Rule-Level Policy Change' is set to 'Success and Failure'.

VIII. Privilege Use

- Ensure 'Audit Sensitive Privilege Use' is set to 'Success and Failure'.

IX. System

- Ensure 'Audit IPsec Driver' is set to 'Success and Failure'.
- Ensure 'Audit Security System Extension' is set to include 'Success'.

Security Implications

- auditing of security events, e.g., successful credential validation and Kerberos authentication.
- Enhance security by auditing a broader range of events.
- Include both successful and failed actions for better insight.
- Improved visibility into potential security threats.
- Enhanced monitoring of system activities.

Better detection and response to security incidents

Proposal for Implementation of OS Security Hardening Measures for Future Server Installations

Executive Summary

To mitigate risks associated with cyber threats and vulnerabilities, Pandora Company Limited must implement OS security hardening measures for all future server installations. This proposal outlines a structured plan based on the Center for Internet Security (CIS) framework to secure Rocky Linux 9 Server and Windows Server 2019 R2 systems.

Objectives

- Protect sensitive data
- Ensure business continuity
- Comply with legal and regulatory requirements
- Maintain customer trust
- Gain a competitive edge in the market

Scope

This proposal covers all future installations of Rocky Linux 9 Server and Windows Server 2019 R2 within Pandora Company Limited.

Implementation Plan

Phase 1: Planning and Assessment

1.1 Identify Stakeholders

- IT Team
- Compliance Officers
- Business Heads

1.2 Resource Allocation

Allocate necessary resources including manpower, time, and budget for the security hardening process.

1.3 Risk Assessment

Conduct an initial risk assessment to identify vulnerabilities that are specific to Pandora's business operations.

1.4 Documentation

Prepare initial documentation outlining server configurations, user roles, and permissions.

Phase 2: Configuration and Hardening

2.1 Baseline Configuration

Establish a baseline configuration based on CIS guidelines for both Rocky Linux 9 and Windows Server 2019 R2.

2.2 Implement Security Measures

- Disable unnecessary services and ports
- Configure firewalls
- Implement Multi-Factor Authentication (MFA)
- Set up data encryption

2.3 User Access Control

Set permissions based on the principle of least privilege.

2.4 Test Environment

Before deploying, test the hardening measures in a sandboxed environment to ensure they work as expected without affecting other systems.

Phase 3: Monitoring and Maintenance

3.1 Continuous Monitoring

Deploy monitoring tools to identify and alert on unauthorized access or anomalies.

3.2 Regular Updates and Patches

Ensure that all servers are updated regularly with the latest patches.

3.3 Audit and Compliance

Perform regular audits to ensure compliance with CIS and other regulatory frameworks.

3.4 Documentation Update

Keep all system configurations and security measures up-to-date in documentation.

Phase 4: Review and Feedback

Conduct a review meeting with stakeholders to assess the effectiveness of the hardening measures. Update the strategy based on feedback and identified gaps.

Timeline

- Phase 1: 1-2 weeks
- Phase 2: 3-4 weeks
- Phase 3: Ongoing
- Phase 4: After 6 months and then annually

Budget

A detailed budget breakdown will be prepared upon approval of this proposal.

Conclusion

Implementing this plan will significantly enhance the security posture of Pandora Company Limited, aligning it with industry best practices and ensuring robust protection against a myriad of cyber threats.

Recommendations

Approval of this proposal at the earliest convenience.

Allocation of necessary resources for immediate implementation.

By embracing a proactive approach to server security, Pandora Company Limited can safeguard its assets, ensure business continuity, and maintain the trust of clients and stakeholders.

References

- CIS_Enterprise_Linux_9_Benchmark_v1.0.0.pdf
- CIS_Microsoft_Windows_Server_2019_Benchmark_v2.0.0.pdf