Linux Server Baseline

Created by Borgelt, Grant, last modified by Gong, Jian on Jan 06, 2021

Baseline Configuration

The following configurations are required for all Linux servers (new and existing) before they are deployed into a production environment unless an exception is required, in which case, the exception must be documented and both the business and technical owners must sign-off and accept the risk. These configurations include but are not limited to changes, updates or patches.

Category	Action
Filesystem Hardening	Set Sticky Bit on All World-Writable Directories
	Disable Mounting of cramfs Filesystems
	Disable Mounting of freevxfs Filesystems
	Disable Mounting of jffs2 Filesystems
	Disable Mounting of hfs Filesystems
	Disable Mounting of hfsplus Filesystems
	Disable Mounting of squashfs Filesystems
	Disable Mounting of udf Filesystems
Configure Software Updates	Verify CentOS GPG Key is Installed
	Verify that gpgcheck is Globally Activated
	Verify Package Integrity Using RPM
	Use DJ-approved service to manage software updates
Configure DJ Services	Use CyberArk to store & rotate Admin Account credentials
	Install Tanium Service
	Install DJ PKI Suite
Configure Secure Boot	Set User/Group Owner on /etc/grub.conf to root
	Set Permissions on /etc/grub.conf to 700
Configure Process Hardening	Restrict Core Dumps
	Enable ExecShield
	Enable Randomized Virtual Memory Region Placement
Remove Legacy Services	Remove telnet-server
	Remove rsh-server

Category	Action
	Remove rsh
	Remove NIS Client
	Remove NIS Server
	Remove tftp
	Remove tftp-server
	Remove talk
	Remove talk-server
	Remove xinetd
	Disable chargen-dgram
	Disable chargen-stream
	Disable daytime-dgram
	Disable daytime-stream
	Disable echo-dgram
	Disable echo-stream
	Disable tcpmux-server
Configure Special Purpose Services	Ensure the Default umask of 022 is set in /etc/init.d/functions (Set Daemon umask)
	Disable Avahi Server
	Disable Print Server - CUPS
	Remove DHCP Server
	Configure Network Time Protocol (NTP) to Dow Jones NTP Servers
	Remove LDAP
	Disable NFS and RPC
	Remove FTP Server
	Remove HTTP Server
	Remove Dovecot (IMAP and POP3 services)
	Remove Samba
	Remove HTTP Proxy Server
	Remove SNMP Server
	Configure Mail Transfer Agent for Local-Only Mode

Category	Action
Configure Network Configuration and Firewalls	Disable IP Forwarding
Modify Network Parameters (Host Only)	Disable Send Packet Redirects
Modify Network Parameters (Host and Router)	Disable Source Routed Packet Acceptance
	Disable ICMP Redirect Acceptance
	Disable Secure ICMP Redirect Acceptance
	Log Suspicious Packets (log packets with un-routable source addresses to the kernel log)
	Enable Ignore Broadcast Requests
	Enable Bad Error Message Protection
	Enable TCP SYN Cookies
Wireless Networking	Deactivate Wireless Interfaces
	Disable IPv6
	Install TCP Wrappers
	Set Permissions on /etc/hosts.allow to 700
	Set Permissions on /etc/hosts.deny to 700
Remove unneeded protocols	Disable DCCP
	Disable SCTP
	Disable RDS
	Disable TIPC
Configure Logging and Auditing	Install the rsyslog package
	Activate the rsyslog Service
	Configure /etc/rsyslog.conf (Defaults are OK)
	Set Permissions on rsyslog Log Files: 0600 (if no admin group) or 0640 (if there is a admin group)
	Set Ownership for rsyslog Log Files to root:root or root:<admin group>
	Accept Remote rsyslog Messages Only on Designated Log Hosts
auditd Configuration	Set Audit Log Storage Size to 100MB per file
	Disable System on Audit Log Full

Category	Action
	Delete Local Logs Older Than 6 Months
	Enable auditd Service
	Enable Auditing for Processes That Start Prior to auditd
	Record Events That Modify Date and Time Information
	Record Events That Modify User/Group Information
	Record Events That Modify the System's Network Environment
	Record Events That Modify the System's Mandatory Access Controls
	Collect Login and Logout Events
	Collect Session Initiation Information
	Collect Discretionary Access Control Permission Modification Events
	Collect Unsuccessful Unauthorized Access Attempts to Files
	Collect Use of Privileged Commands
	Collect Successful File System Mounts
	Collect File Deletion Events by User
	Collect Changes to System Administration Scope (sudoers)
	Collect System Administrator Actions (sudolog)
	Collect Kernel Module Loading and Unloading
	Make the Audit Configuration Immutable
	Ensure /etc/logrotate.d/syslog rotates: /var/log/messages /var/log/secure /var/log/maillog /var/log/spooler /var/log/boot.log /var/log/cron (i.e. Configure logrotate)
cron and anacron	Enable crond Daemon
	Set User/Group Owner to Root and Permissions on /etc/anacrontab to 770
	Set User/Group Owner to Root and Permissions on /etc/crontab to 770
	Set User/Group Owner to Root and Permissions on /etc/cron.hourly to 770
	Set User/Group Owner to Root and Permissions on /etc/cron.daily to 770
	Set User/Group Owner to Root and Permissions on /etc/cron.weekly to 770
	Set User/Group Owner to Root and Permissions on /etc/cron.monthly to 770

Category	Action
	Set User/Group Owner to Root and Permissions on /etc/cron.d to 770
	Remove /etc/at.deny file & Create An Empty /etc/at.allow File with 770 Permissions for User/Group root (Restrict at Daemon)
	Restrict at/cron to Authorized Users
	Set LogLevel to INFO
SSH	Set SSH Protocol to 2
	Set User/Group, Permissions on /etc/ssh/sshd_config to root:root, 600
	Set SSH MaxAuthTries to 4 or Less
	Set SSH IgnoreRhosts to Yes
	Set SSH HostbasedAuthentication to No
	Disable SSH Root Login
	Set SSH PermitEmptyPasswords to No
	Do Not Allow Users to Set Environment Options
	Ensure /etc/ssh/sshd_config contains: KexAlgorithms diffie-hellman-group-exchange-sha256 MACs hmac-sha2-512,hmac-sha2-256 Ciphers aes256-ctr,aes192-ctr,aes128-ctr
	Set Idle Timeout Interval to 15 min for User Login
	Set SSH Banner to DJ Legal-approved warning
Password / Account Policies	Upgrade Password Hashing Algorithm to SHA-512
	Set Password Creation Requirement Parameters Using pam_cracklib to DJ Password Standard
	Set Lockout for Failed Password Attempts (5 Invalid)
	Limit Password Reuse (to the last 15 passwords)
	Restrict Access to the su Command to the 'wheel' group
	Set Shadow Password Suite Parameters (/etc/login.defs)
	Set Password Expiration Days (90)
	Set Password Change Minimum Number of Days (1)
	Set Password Expiration Warning Days (30)
	Disable System Accounts by setting shell to /sbin/nologin
	Set Default Group for root Account
	Set Default umask for Users
	Lock Inactive User Accounts after 90 days

Category	Action
Configure Warning Banners	Set Warning Banner for Standard Login Services to DJ Legal-approved warning
	Remove OS Information from Login Warning Banners
	Set GNOME Warning Banner to DJ Legal-approved warning

Questions & Guidance

If you have questions or require further guidance regarding this Configuration Baseline or its subject matter, please contact the Cybersecurity Office at cso@dowjones.com or the DJ Service Desk at servicedesk@dowjones.com.

Document Control

Version	Date	Person	Action/Comments
0.01	7/26/17	S. Riggs and J. Kelath	Reviewed & Drafted
0.02	8/29/17	G. Borgelt	Converted Google Doc to Conflucne page
1.0	12/8/20	J. Gong and A. Venkataraman	Updated to reflect client requirements
1.1	12/22/20	J. Gong	Clarified client requirement

No labels