Hardening guide

For systems Windows 2019, Windows 10, and Oracle Linux

Windows 2019

Domain controllers

-2.3.5.2 (L1) Ensure 'Domain controller: Allow vulnerable Netlogon secure channel connections' is set to 'Not Configured' (DC Only) (Automated)

-2.3.5.3 (L1) Ensure 'Domain controller: LDAP server channel binding token requirements' is set to 'Always' (DC Only) (Automated)

-2.3.5.4 (L1) Ensure 'Domain controller: LDAP server signing requirements' is set to 'Require signing' (DC only) (Automated)

-2.3.5.5 (L1) Ensure 'Domain controller: Refuse machine account password changes' is set to 'Disabled' (DC only) (Automated)

Web servers

-18.5.10.2 (L2) Ensure 'Turn off Microsoft Peer-to-Peer Networking Services is set to 'Enabled' (Automated)

-18.5.19.2.1 (L2) Disable IPv6 (Ensure TCPIP6 Parameter Disabled Components' is set to 'Oxff (255)) (Automated)

-18.8.22.1.6 (L2) Ensure 'Turn off printing over HTTP' is set to 'Enabled" (Automated)

-18.9.4.1 (L2) Ensure 'Allow a Windows app to share application data between users' is set to Disabled' (Automated)

-18.9.47.6.1 (L2) Ensure Enable file hash computation feature' is set to Enabled' (Automated)

Oracle

POS servers

-Dramatically simplify implementation, monitoring, patching, and upgrades
-Speed deployment and time to value
-Ensure Payment Card Industry Data Security Standard (PCI DSS) compliance
-Quickly identify suspicious trends, transactions, and other anomalies
-Respond instantly via automated alerts

1.2.1 Ensure GPG keys are configured (Manual)

1.2.2 Ensure gpgcheck is globally activated (Automated)

1.1.5.2 Ensure nodev option set on /var/log partition (Automated)

1.1.5.3 Ensure noexec option set on /var/log partition (Automated).

-Improve service levels and save sales

Windows 10

Users running the POS software

-adaptability friendliness

-can be easily tweaked to adapt to industry trends

-guest expectations

-new ideas specific to a business

-The software boasts strong reporting features and supports multiple locations.

-Updates can be made on the system from anywhere, from any mobile device connected to the internet.

Users not running the POS software

-2.3.17.6 (1.1) Ensure User Account Control: Run all administrators in Admin Approval Mode is set to 'Enabled' (Automated).

-2.3.17.4 (L1) Ensure 'User Account Control: Detect application installations and prompt for elevation is set to 'Enabled' (Automated).

-2.3.11.1 (L1) Ensure 'Network security: Allow Local System to use computer identity for NTLM' is set to 'Enabled' (Automated).

-2.3.11.5 (11) Ensure "Network security: Do not store LAN Manager hash value on next password change' is set to 'Enabled' (Automated).