Linux Security Audit Report

OS Version:

{'result': 'Description:\tParrot OS 5.3 (Electro Ara)', 'passed': True}

Kernel Version:

{'result': '6.1.0-1parrot1-amd64', 'passed': True}

Firewall Status:

{'result': '', 'passed': False}

Running Services:

{'result': ['UNIT   LOAD   ACTIVE SUB   DESCRIPTION', ' accounts-daemon.service   loaded active running Accounts Service', ' cron.service   loaded active running Regular background program processing daemon', ' dbus.service   loaded active running D-Bus System Message Bus', ' getty@tty1.service   loaded active running Getty on tty1', ' haveged.service   loaded active running Entropy Daemon based on the HAVEGE algorithm', ' lightdm.service   loaded active running Light Display Manager', ' ModemManager.service   loaded active running Modem Manager', ' NetworkManager.service   loaded active running Network Manager', ' polkit.service   loaded active running Authorization Manager'], 'passed': True}

Listening Ports:

{'result': ['tcp   LISTEN 0   128   0.0.0.0:22   0.0.0.0:*   ', 'tcp   LISTEN 0   128   [::]:22   [::]:*'], 'passed': True}

Users:

{'result': ['root', 'daemon', 'bin', 'sys', 'sync', 'games', 'man', 'lp', 'mail', 'news', 'uucp', 'proxy', 'www-data', 'backup', 'list', 'irc', 'gnats', 'nobody', '_apt', 'systemd-network', 'systemd-resolve', 'tss', 'strongswan', 'messagebus', 'systemd-timesync', 'Debian-exim', 'uuidd', 'debian-tor', 'usbmux', 'rtkit',

'dnsmasq', 'avahi', 'nm-openvpn', 'nm-openconnect', 'speech-dispatcher', 'pulse', 'geoclue', 'lightdm', 'mysql', 'tcpdump', 'stunnel4', 'sshd', 'sslh', 'ntp', 'postgres', 'arpwatch', 'miredo-server', 'iodine', 'miredo', 'redis', 'inetsim', '_gvm', 'beef-xss', 'parrot', 'ftp'], 'passed': True}

Groups:

{'result': ['root', 'daemon', 'bin', 'sys', 'adm', 'tty', 'disk', 'lp', 'mail', 'news', 'uucp', 'man', 'proxy', 'kmem', 'dialout', 'fax', 'voice', 'cdrom', 'floppy', 'tape', 'sudo', 'audio', 'dip', 'www-data', 'backup', 'operator', 'list', 'irc', 'src', 'gnats', 'shadow', 'utmp', 'video', 'sasl', 'plugdev', 'staff', 'games', 'users', 'nogroup', 'systemd-journal', 'systemd-network', 'systemd-resolve', 'input', 'kvm', 'render', 'crontab', 'netdev', 'tss', 'messagebus', 'systemd-timesync', 'Debian-exim', 'uuidd', 'debian-tor', 'ssh', 'bluetooth', 'rtkit', 'vboxsf', 'avahi', 'nm-openvpn', 'nm-openconnect', 'pulse', 'pulse-access', 'geoclue', 'lightdm', 'sgx', 'pipewire', 'mysql', 'tcpdump', 'rdma', 'stunnel4', 'sslh', 'ssl-cert', 'ntp', 'postgres', 'arpwatch', 'sambashare', 'redis', 'inetsim', 'wireshark', '_gvm', 'beef-xss', 'lpadmin', 'scanner', 'docker', 'autologin', 'parrot', 'ftp'], 'passed': True}

Installed Packages:

{'result': ['0trace', 'accountsservice', 'adduser', 'adwaita-icon-theme', 'afflib-tools', 'afl', 'afl++', 'afl++-clang', 'afl++-doc', 'aircrack-ng'], 'passed': True}

Scheduled Cron Jobs:

{'result': [''], 'passed': True}

Disk Usage:

{'result': ['total   131G 15G 115G 12% -'], 'passed': True}

Memory Usage:

{'result': ['Mem: 2741   622   1383   6   735   1965'], 'passed': True}

CPU Usage:

{'result': ['%Cpu(s): 0.0 us, 1.6 sy, 0.0 ni, 98.4 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st'], 'passed': True}

Log Files:

{'result': [''], 'passed': True}

Failed Login Attempts:

{'result': [''], 'passed': True}

System Log Errors:

{'result': [''], 'passed': True}

Auth Log Failures:

{'result': [''], 'passed': True}

Kernel Segfaults:

{'result': [''], 'passed': True}

Journal Errors:

{'result': ['Apr 08 07:42:15 parrot sudo[1337]: pam_unix(sudo:auth): conversation failed', 'Apr 08 07:42:15 parrot sudo[1337]: pam_unix(sudo:auth): auth could not identify password for [parrot]', 'Apr 08 07:42:15 parrot sudo[1353]: pam_unix(sudo:auth): conversation failed', 'Apr 08 07:42:15 parrot sudo[1353]: pam_unix(sudo:auth): auth could not identify password for [parrot]', 'Apr 08 07:44:01 parrot sudo[1530]: pam_unix(sudo:auth): conversation failed', 'Apr 08 07:44:01 parrot sudo[1530]: pam_unix(sudo:auth): auth could not identify password for [parrot]', 'Apr 08 07:44:01 parrot sudo[1546]: pam_unix(sudo:auth): conversation failed', 'Apr 08 07:44:01 parrot sudo[1546]: pam_unix(sudo:auth): auth could not identify password for [parrot]'], 'passed': True}