Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Hardening Linux Workstations and Servers

JANUARY 2021

Introduction

This document has been developed to assist organisations understand how to harden Linux workstations and servers, including by applying the Essential Eight from the Australian Cyber Security Centre (ACSC)'s ***Strategies to Mitigate Cyber Security Incidents***.

While this document refers specifically to Linux environments, the guidance presented is equally applicable to all Unix-style environments.

Implementing the Essential Eight

Application control

Implementing application control within Linux environments can be achieved using the File Access Policy daemon (fapolicyd)[1] [2]. The fapolicyd framework allows Linux system administrators to control which applications are allowed (or denied) execution based on either path, hash, MIME type or if they are trusted (i.e. properly installed by the system package manager and registered in the RPM database). The Red Hat ***Security Hardening*** publication[3] provides advice on how to configure and manage the use of the fapolicyd framework within Red Hat Enterprise Linux 8.

Application and operating system patching

Patching Linux is easy to achieve when combined with locally hosted repositories and scheduled scripts. Some Linux distributions now provide administrative servers that allow control of workstations and servers from a centralised location to approve updates as required. This can enhance the ability of an organisation to efficiently and effectively manage their change management process while ensuring timely patching occurs. Linux system administrators should check with their vendor if they are unsure how to best handle application and operating system patching in Linux environments.

[1] https://github.com/linux-application-whitelisting/fapolicyd

[2] https://www.redhat.com/en/blog/stop-unauthorized-applications-rhel-8s-file-access-policy-daemon

[3] https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/security_hardening/assembly_blocking-and-allowing-applications-using-fapolicyd_security-hardening

Configure Microsoft Office macro settings

As Microsoft Office desktop applications are not supported natively in Linux environments, this mitigation strategy is typically not applicable. However, if emulation software is used to enable Linux environments to run Microsoft Office, macro settings should be configured as per the ACSC's ***Microsoft Office Macro Security*** publication, albeit likely without the use of Microsoft's Group Policy functionality to distribute and enforce configuration settings.

User application hardening

As typically targeted business applications such as web browsers and PDF viewers are equally used in Linux and Microsoft Windows environments, and are largely independent of the underlying operating system, this mitigation strategy can be implemented in Linux environments in a similar manner to Microsoft Windows environments.

Restricting administrative privileges

Restricting administrative privileges in Linux environments can be achieved by controlling the number of users with administrative privileges, as well as controlling the access of those accounts.

The number of users with administrative privileges on Linux workstations and servers can be determined by auditing the number of users with privileged accounts or the ability to elevate permissions. This can be achieved by listing groups and group memberships of users to check which users belong to each group. The 'sudoers' group, and any other specific admin groups for a given distribution, must be considered when conducting this audit. Additionally, organisations should ensure users do not have a user ID (UID) or group ID (GID) of 0 which would grant root access.

In addition to minimising the number of users with administrative privileges, organisations should ensure they enforce a policy of using the sudo command when administering Linux servers as opposed to logging in locally or remotely with an administrative account. This will not only prevent the use of shared accounts, but also enhance the ability of an organisation to audit administrative access and encourage system administrator accountability.

Multi-factor authentication

While the choice of where and how to enforce the use of multi-factor authentication is largely independent of the operating system used by users, the support for specific multi-factor solutions may not be. For example, when implementing multi-factor authentication for Linux environments care should be taken to select a vendor that provides Linux drivers and Pluggable Authentication Modules[4] if required. Vendors that support Linux environments should also provide guidance on how to configure their solutions[5] once any pre-requisite drivers and Pluggable Authentication Modules have been installed[6].

Daily backups

As conducting daily backups is largely independent of the underlying operating system, this mitigation strategy can be implemented in Linux environments in a similar manner to Microsoft Windows environments.

[4] https://mirrors.edge.kernel.org/pub/linux/libs/pam/FAQ

[5] https://support.yubico.com/support/solutions/articles/15000006449

[6] https://developers.yubico.com/pam-u2f/

General hardening of Linux environments

Given the difficulty in implementing application control in Linux environments, the following mitigation strategies can be implemented to assist with reducing the residual risk of the exploitation of Linux workstations and servers. Note, this list is not exhaustive and does not take into account specific use cases or differences between Linux distributions:

- Use unique restricted users for key at-risk services (e.g. Apache software runs under a restricted 'apache' user role).
- Disable unrequired operating system functionality, including disabling unrequired network services.
- Apply additional forms of security policy enforcement such as SELinux or AppArmor.
- Implement appropriately hardened security configurations and permissions of key configuration files (e.g. /etc/security/access.conf, /etc/hosts, /etc/nsswitch.conf).
- Use the 'noexec' parameter to mount partitions which users have write access to.
- Perform an inventory of binaries, determine which ones users need to run, and for all others either uninstall them or remove the setuid permission.
- Implement software-based firewalls for both internal and external network interfaces, for IPv4 and IPv6 (or disable IPv6 support).
- Perform tasks with least privileges.
- Centralise auditing and analysis of system and application logs.
- Implement specific configurations based on server roles (e.g. if running Apache HTTP Server, harden as per Apache hardening guidance).
- As far as practical, implement vendor security guidance for specific Linux distributions.

Further information

The ***Australian Government Information Security Manual*** (ISM) assists in the protection of information that is processed, stored or communicated by organisations' systems. It can be found at https://www.cyber.gov.au/acsc/view-all-content/ism.

The ***Strategies to Mitigate Cyber Security Incidents*** complements the advice in the ISM. The complete list of strategies can be found at https://www.cyber.gov.au/acsc/view-all-content/publications/strategies-mitigate-cyber-security-incidents.

Additional guidance on hardening Red Hat Enterprise Linux 8.3 is available from Red Hat in their ***Security Hardening*** publication. This publications can be found at https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/security_hardening/index.

Additional guidance on hardening SUSE Linux Enterprise Server 15 SP2 is available from SUSE in their ***Security Guide*** publication. This publication can be found at https://documentation.suse.com/sles/15-SP2/html/SLES-all/book-security.html.

Additional guidance on hardening Ubuntu 20.04 LTS is available from Canonical in their ***Basic Ubuntu Security Guide*** and ***Ubuntu Server Guide***. These publications can be found at https://wiki.ubuntu.com/BasicSecurity and https://ubuntu.com/server/docs.

Contact details

If you have any questions regarding this guidance you can contact us via 1300 CYBER1 (1300 292 371) or https://www.cyber.gov.au/acsc/contact.