Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Essential Eight in Linux Environments

APRIL 2019

Introduction

This document has been developed to assist organisations understand how the Essential Eight from the ***Strategies to Mitigate Cyber Security Incidents*** can be implemented in Linux environments. While this document refers specifically to Linux environments, the guidance presented is equally applicable to all Unix-style environments.

This document is intended for cyber security professionals as well as information technology architects and support staff responsible for Linux assets on corporate networks.

Implementing the Essential Eight

The mitigation strategy that poses the most challenge in Linux environments is application whitelisting, while the remaining mitigation strategies are either not applicable or can be implemented in a similar manner to Microsoft Windows environments.

Application whitelisting

While Linux doesn't natively offer application whitelisting functionality, and the choices for application whitelisting in Linux environments are sparse compared to in Microsoft Windows environments, a small number of vendors do offer third party application whitelisting solutions. However, organisations need to consider the specific Linux distributions they are using and how application whitelisting solutions may impact other security controls. For example, deploying the latest kernel updates may be problematic on certain Linux distributions if the application whitelisting solutions don't support the latest kernel version and may be especially problematic in environments where custom kernels are in use.

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 machines 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.

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 ***Microsoft Office Macro Security*** publication[1], 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 machines 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 on each Linux machine 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[2] if required. Vendors that support Linux environments should also provide guidance on how to configure their solutions[3] once any pre-requisite drivers and Pluggable Authentication Modules have been installed[4].

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.

[1] https://www.acsc.gov.au/publications/protect/Microsoft_Office_Macro_Security.pdf
[2] https://mirrors.edge.kernel.org/pub/linux/libs/pam/FAQ
[3] https://support.yubico.com/support/solutions/articles/15000006449
[4] https://developers.yubico.com/pam-u2f/

General hardening of Linux

Given the difficulty in implementing application whitelisting in Linux environments, the following mitigation strategies can be implemented to assist with reducing the residual risk of the exploitation of Linux machines. 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).
- 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.
- Implement software-based firewalls for both internal and external network interfaces.
- Perform tasks with least privileges.
- Centralise auditing and analysis of system and application logs.
- Disable unrequired operating system functionality.
- Implement specific configurations based on server roles (e.g. running Apache webserver, harden as per Apache hardening guide).
- 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/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/publications/strategies-to-mitigate-cyber-security-incidents.

Additional guidance on hardening Red Hat Enterprise Linux 7.6 is available from Red Hat in their ***Security Guide*** and ***SELinux User's and Administrator's Guide*** publications. These publications can be found at https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/.

Additional guidance on hardening SUSE Linux Enterprise Server 12 SP4 is available from SUSE in their ***Security Guide*** publication. This publication can be found at https://www.suse.com/documentation/sles-12/book_security/data/book_security.html.

Additional guidance on hardening Ubuntu 18.04 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://help.ubuntu.com/lts/serverguide/index.html.

Contact details

Organisations or individuals with questions regarding this advice can email asd.assist@defence.gov.au or call 1300 CYBER1 (1300 292 371).