
**April 2016**

# The Top 4 in a Linux Environment

## Introduction

1. This document has been developed by the Australian Signals Directorate (ASD) to assist organisations understand how the top four strategies ('Top 4') of ASD's *Strategies to Mitigate Targeted Cyber Intrusions* can be implemented in a Linux environment.

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

## Intended audience

3. This document is intended for cyber security professionals as well as information technology decision makers, architects, designers and support staff responsible for Linux assets on their corporate network.

## Implementing the Top 4 on Linux

4. The Top 4 strategy that poses the most challenge on Linux is application whitelisting, while the remaining three strategies can be implemented in a similar manner to Microsoft Windows.

### Application whitelisting

5. Whilst Linux doesn't natively offer application whitelisting functionality, and the choices for application whitelisting on Linux are sparse compared to Microsoft Windows, a small number of vendors do offer 3rd 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

6. 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 push updates as necessary. 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 a Linux environment.

**Restricting administrative privileges**

7. Restricting administrative privileges in a Linux environment can be achieved through a combination of controlling the number of users with administrative privileges, controlling the access that those users have and auditing the actions of those users.

8. Determining the number of users with administrative privileges on Linux machines is relatively simple. Auditing the number of users with the ability to elevate permissions, or having privileged accounts, 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 that specific user root access on that machine.

9. 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.

## General hardening of Linux

10. Given the difficulty in implementing application whitelisting on Linux, the following 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.

    a. Use unique restricted users for key at-risk services (e.g. Apache software runs under a restricted ‘apache’ user role).

    b. Apply additional forms of security policy enforcement such as SELinux or AppArmour.

    c. Implement appropriately hardened security configurations, and permissions of key configuration files (e.g. /etc/security/access.conf, /etc/hosts, /etc/nsswitch.conf).

    d. Use the ‘noexec’ parameter to mount partitions which users have write access to.

    e. Implement software-based firewalls for both internal and external network interfaces.

    f. Perform tasks with least privileges.

    g. Centralise auditing and analysis of system and application logs.

    h. Disable unrequired operating system functionality.

    i. Implement specific configurations based on server role (e.g. running Apache webserver, harden as per Apache hardening guide)

    j. As far as practical, implement vendor security guidance for specific Linux distributions.

## Summary

11. Given the difficulty in implementing application whitelisting on Linux, organisations may choose to address as a higher priority application and operating system patching, restricting administrative privileges and implementing general system hardening measures.

## Further information

12. The *Australian Government Information Security Manual* (ISM) assists in the protection of official government information that is processed, stored or communicated by Australian Government systems. It can be found at: http://www.asd.gov.au/infosec/ism/.

13. ASD's *Strategies to Mitigate Targeted Cyber Intrusions* complements the advice in the ISM. The complete list of mitigation strategies and supporting publications can be found at: http://www.asd.gov.au/infosec/mitigationstrategies.htm.

14. Additional guidance on hardening Red Hat Enterprise Linux 7 is available from redhat in their *A Guide to Securing Red Hat Enterprise Linux 7* 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/index.html.

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

16. Additional guidance on hardening Ubuntu is available from Canonical. Canonical's security documentation can be found at: https://wiki.ubuntu.com/BasicSecurity and https://help.ubuntu.com/lts/serverguide/security.html.

## Contact details

17. Australian government customers with questions regarding this advice should contact ASD Advice and Assistance by emailing asd.assist@defence.gov.au or by calling 1300 CYBER1 (1300 292 371).

18. Australian businesses or other private sector organisations with questions regarding this advice should contact CERT Australia by emailing info@cert.gov.au or by calling 1300 172 499.