Australian Government
Department of Defence
Intelligence and Security

CYBER SECURITY OPERATIONS CENTRE

PROTECT

November 2013

(U) **LEGAL NOTICE:** THIS PUBLICATION HAS BEEN PRODUCED BY THE DEFENCE SIGNALS DIRECTORATE (DSD), ALSO KNOWN AS THE AUSTRALIAN SIGNALS DIRECTORATE (ASD). ALL REFERENCES TO ASD SHOULD BE TAKEN TO BE REFERENCES TO DSD.

The Top 4 in a Linux Environment

Introduction

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

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 ICT 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. This section contains technical guidance for implementing the Top 4 on Linux.

Application Whitelisting

5. Implementing application whitelisting on Linux is likely to be more resource intensive than implementing application whitelisting on Microsoft Windows as a mechanism to perform application whitelisting has not been implemented in either the core Linux kernel or popular Linux distributions. While implementing application whitelisting on Linux is still possible through a number of different approaches, it is generally advised against due to the high administrative overhead associated with it at this time. Possible application whitelisting approaches include:

   a. **Commercial solutions:** A small number of third party companies offer application whitelisting products for Linux. Deploying the latest kernel updates may be problematic as the application whitelisting solution must explicitly support the latest kernel in order for the solution to be

[1] http://www.asd.gov.au/infosec/top35mitigationstrategies.htm

reliable and supported by the product vendor. This can be especially difficult in environments where custom kernels are in use. Before implementing any commercial solution ensure the solution fully supports the kernel in use and satisfies all patching requirements.

b. **SELinux or AppArmor Policies:** While not designed specifically for this purpose, custom SELinux or AppArmor configurations can potentially provide similar functionality to application whitelisting. However, SELinux and AppArmor policies to enforce application whitelisting are likely to be resource intensive to develop and test thoroughly.

c. **Custom Linux Security Modules**: Custom Linux security modules may be developed to enforce application whitelisting, however, this would require a significant resource investment to both develop and maintain, and may introduce potential security vulnerabilities if developed insecurely.

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 the 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 their Linux environment.

Minimising the Number of Users with Administrative Privileges

7. 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 primary group ID of 0, which would grant that specific user root access on that machine.

8. 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 for Linux

9. As it is generally not practical to implement application whitelisting on Linux machines, the following basic strategies should be considered to ensure a comparable level of security to a “Top 4”

hardened Windows machine. Note, this list is not exhaustive and does not take into account specific use cases or differences between Linux distributions.

a. Use unique restricted user accounts for key at-risk services, especially internet accessible services (e.g. Apache software runs under a restricted 'apache' user context).

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

e. Perform tasks with least privilege.

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

g. Disable unrequired operating system functionality.

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

Summary

10. Given the challenges associated with implementing application whitelisting on Linux, and in light of the currently preferred methods of intrusions into an ICT environment, organisations may choose to address application and operating system patching, reducing the number of users with administrative privileges and general hardening as a higher priority.

Further Information

11. The Top 4 strategies are described in the document "Top 4 Strategies to Mitigate Targeted Cyber Intrusions – Mandatory Requirement Explained".

Contact Details

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

Australian businesses or other private sector organisations seeking further information should contact CERT Australia at info@cert.gov.au or by calling 1300 172 499.

(U) **LEGAL WARNING**: ALL DOCUMENTS ORIGINATING WITH OR RECEIVED FROM DSD, ALSO KNOWN AS ASD, ARE EXEMPT UNDER SECTION 7(2A) OF THE *FREEDOM OF INFORMATION (FOI) ACT 1982*. THIS EXEMPTION EXTENDS TO DOCUMENTS THAT CONTAIN SUMMARIES OF A DSD, ALSO KNOWN AS ASD, DOCUMENT OR EXTRACTS FROM SUCH A DOCUMENT. DSD, ALSO KNOWN AS ASD, MUST BE CONSULTED PRIOR TO THE RELEASE OF ANY SUCH INFORMATION UNDER AN FOI REQUEST.