JOHNS HOPKINS

Linux Server Security Guidance
I. Table of Contents
II. Introduction ............................................................................................................. 3
   A. Background ............................................................................................................ 3
   B. Audience .............................................................................................................. 3
   C. Scope .................................................................................................................... 3
   D. Linux Server and Desktop .................................................................................. 4
III. Linux Security Checklist .......................................................................................... 4
    A. Set-up and Install ................................................................................................. 5
    B. Services .............................................................................................................. 6
    C. Accounts ............................................................................................................ 6
    D. Logging and Security Tools ................................................................................. 7
    E. Ongoing Administration ...................................................................................... 7
IV. References ............................................................................................................... 8
    Books ....................................................................................................................... 8
    Web Sites ................................................................................................................ 8
V. Appendix .................................................................................................................... 8
**Introduction**

This document is a collection of security practices to be used in the operation of Linux-based operating systems at Johns Hopkins institutions. The goal of this standard is to enhance the security of Linux computers, particularly servers, that are a part of the Hopkins network. All systems must be administered securely so as to not adversely affect other systems within the Hopkins environment.

Systems administration in Linux often requires a different approach than that used for Windows servers or even proprietary UNIX systems. Many of the virtues of Linux – cost, diversity of support and tools – are also its weaknesses. Secure and reliable Linux administration involves many options and decisions. It is therefore critical that systems administrators realistically assess their experience with administering systems and consider risks accordingly.

The diversity and complexity of the Linux environment also means that it is difficult to develop straightforward standards. We have therefore adopted an approach that offers guidelines and checklists for configuring machines. It is the responsibility of administrators to use these guidelines, as well as up to date technology-specific hardening guidelines available online, to ensure that appropriate practices and security controls are in place.

**A. Background**

Given the diversity of type and scope of Linux implementations, we highlight a concise set of security considerations and tools. Individual server configurations will differ.

**B. Audience**

The target audience for this document is anyone who is responsible for building, deploying, or administering Linux computers on the Johns Hopkins Network. This document is intended for administrators who have some level of Linux experience. Users new to Linux should consider consulting with an experienced administrator and working through this guidance.

**C. Scope**

This is a Linux security document. There may be some guidance that may provide some operational benefit beyond security, but that would be purely accidental. This guidance applies to both Restricted systems (i.e. those which store, process or transmit Restricted information or are otherwise business critical) and other networked Linux computers performing other services.

*Please note:* while we make some distinction between Restricted and non-Restricted servers, nearly all of the guidance herein is equally applicable to both. Compromised Linux servers, even those without critical functions, make excellent tools for compromise of other machines on the JH Network. Our guidance should be seen as a baseline that can and should be refined and exceeded.
**Please also note:** there is little consensus in the security community regarding “best” security. There are many different approaches to the use of, for example, *sudo*, PAM, anti-virus, integrity checking, patch management, xinetd, logging, back-up, remote access and logging. Approaches vary by distribution, use, applications and the predilections of administrators. This is a guidance document and, we hope, a jumping off point for more thorough discussions of security. It should not be considered the last word on security.

**D. Linux Server and Desktop**

This document focuses on Linux server installations and is not principally concerned with Linux desktop configurations. Most of these controls are appropriate to desktops also, though the more stringent security settings will be impractical for users’ personal machines. We recommend that Linux desktops use supported distributions (e.g. Ubuntu, Fedora, CentOS), install and open only necessary services, and patch routinely. Desktop Linux users should be aware that many distributions install network services commonly used on servers by default, and should be familiar with the issues that could arise from having these services running on their computers.

The term 'Linux server' refers to a computer on the JH Network that hosts or serves centralized data and resources that other clients access and rely upon for tasks pertaining to JH business purposes. The data and resources that such computers serve are generally time and security sensitive. Examples of such computers would be file servers, account information servers, web servers, compute clusters, etc. The data these computers serve should be information directly pertaining to the business of JH. A Linux server is also a computer that will serve this data out to a network of computers via any network protocol or other remote transmissions. It therefore requires secure or limited access.

Linux desktop distribution suites (e.g. Mint, Ubuntu, Fedora) are geared toward end user applications and are generally not appropriate for server configurations. Server administrators should use server alternatives (e.g. Red Hat, CentOS). Linux desktop security should follow the principles discussed below, but the number and style of desktop configurations are beyond the scope of this document.

**II. Linux Security Checklist**

The following checklist identifies a high-level list of suggested to-do(s) prior to, during and post-install of the Linux server OS, e.g. RedHat 7. It is recommended that Linux administrators use this checklist, when planning, building, and or updating, include notes if appropriate.

In addition to the checklist below there are specific “must do” requirements for the creation and administration of Linux servers and they have been listed here. These
same requirements can be found in the list below and may contain additional information.

- Deploy a host firewall (e.g. firewalld or iptables)
- Configure SSH with secure settings
- Replace clear text services, i.e. Telnet and FTP, with encrypted alternatives
- Regular backups are required for systems that store Restricted Information
- Systems that store Restricted Information are required to have regular Tenable vulnerability scans
- Install a monitoring application tool to monitor the server
- IT administrators and other staff with administrative rights must use Multi-Factor authentication (MFA)

A. Initial Setup and Pre-Install

1. Use SE Linux as a first option for server deployments
2. Prior to setting up a server, document the purpose, access controls and life cycle of the server. There is a template that is available for use by IT staff to document servers/applications available on the IT Policy Standards and Guidelines site. The template, Project Application System Planning Template, covers the majority of information critical to supporting a server.
3. Create a server name based upon sensible server naming conventions, either from a Hopkins document or department internal naming policy.
4. If your department uses a Server Asset Inventory Data Base ensure that it is updated. This inventory should include both static information (location, server administrator), along with dynamic information. IT @ JH provides access to a CMDB for static and dynamic server asset information.
5. For physical servers ensure that the location has appropriate physical security controls. The ICSC has approved standards for physical security of servers (Data Center Security Standards and Guidance, http://www.it.johnshopkins.edu/policies/standards.html).
6. When doing the initial distribution download, check to determine whether the download is the latest package. It would also be recommended to check the hash algorithm to ensure the integrity of the download if appropriate. Pick either the minimal server or default install options whenever available and then add required tools to that if necessary, rather than picking a pre-configured option that might install services you don’t require.

B. Post-Install and Services

7. The following Linux Security options are suggested:
   - Install and enable local Linux security package, e.g. Red Hat SElinux
   - Deploy a host firewall (e.g. firewalld or iptables)
   - It is highly recommended that an Intrusion Prevention tool be installed, e.g. Fail2ban.
8. Servers should be left in the logged-off or locked state when not in use.
9. Confirm the system clock configuration with the Hopkins NTP (Network Time Protocol) to ensure consistent time stamps across logged systems.
10. Configure primary and secondary DNS.
11. Configure SSH with secure settings – this is still one of the most commonly exploited attacks.
12. Move SSH to a non-standard port (above 1024) if it requires internet accessibility – contact network.security@jhmi.edu to adjust external firewall policy.
13. Review and disable any services and/or applications started by a network super-service that are not being utilized, e.g. `xinetd` or `inetd`. Ideally, do not just disable unused services but actually completely remove the package. Attackers can often activate disabled software.
14. Disable and remove if possible unused standard boot services.
15. Replace clear text services, such as Telnet and FTP, with encrypted alternatives.
16. Regular backups are required for systems that store Restricted information or serve/support another critical business purpose – i.e. configuration settings. Ensure that all backups to removable media solutions are encrypted.
17. Use `chroot` where applicable – ideal for web servers. A properly configured chrooted web server will not allow the underlying server to be compromised via a web server.
18. Consider configuring the local firewall to restrict (or at least monitor) outgoing connections. Generally the first thing an attacker does, no matter method of attack, is to download software to the compromised server. This software will often attempt to call out to malicious sites.

C. Accounts and Security

19. Consider using an encrypted file system. Encryption remains to be one of the most important tools for securing data, whether that data is in transit or at rest on the server. It helps to protect confidentially as well as it will help authenticate the actual data. (refer to the Hopkins Encryption Standards for details):
20. Ensure that the terminal security file is configured to deny direct remote root logins. Limit direct root logins to the console and disable GUI root logins.
21. Consider disabling or randomizing root if your application allows.
22. Review configuration files for PAM, `/etc/pam.d/*` to default to deny and warn for each PAM-enabled process.
23. Once the server has been built consider downloading and installing an open source security auditing tool called Lynis from “CISOFY – Auditing-Hardening-Compliance”. [https://cisofy.com/lynis/] Lynis performs hundreds of individual tests to determine the security state of the system. Results will be grouped at the bottom of the screen output and they can be viewed for suggestions and possible actions.
24. For user authentication, consider using the Johns Hopkins Active Directory tree to ensure account security and password quality standards are met.
25. It is required that IT Administrators and other staff with administrative rights use Multi-Factor Authentication (MFA). Therefore Restricted systems must include MFA for all admin access.
26. All Web-based applications and systems/applications authenticating JHED users against AD/LDAP must be secured with an SSL Certification and use an enterprise WebSSO solution through the Enterprise Authentication team (mailto:enterpriseauth@jhmi.edu). Trusted certification can be SSL/TLS certificates requested through the Johns Hopkins’ Comodo SSL/TLS certificate request site. For more information please go to the SSL Certificate Services site.

D. Logging and Security Tools

27. Activate logwatch for simple monitoring of basic elements – ensure notices are sent to a valid and monitored email address.
28. Additional tools should be installed to monitor the server for environmental health and to track service-level performance (e.g. Up.time, Big Brother, Cacti, Nagios, Splunk, sysstat).
29. Automate log reviews (refer to JH Log Management Guidance) and tune messaging alerts to ensure prompt response.
   The Guidance document can be found at: http://www.it.johnshopkins.edu/restricted/standards/StandardLogManAPPROVED0612.pdf
30. It is suggested that a process accounting package be installed and enabled (e.g. psacct).
31. It is recommended to deploy an integrity checking tool (e.g. Tripwire, AIDE, SamHain, OSSEC).
32. Systems that store Restricted information are required to have regular Tenable vulnerability scans. It is recommended that all Linux servers have regular vulnerability scans. Tenable (NESSUS) can be accessed after registration in the CMDB and by contacting network.security@jhu.edu for account setup.
   Consider allowing NESSUS scans to run authenticated, and publickey auth is appropriate for this.

E. Ongoing Administration

33. Use SUDO for elevated privileges. SUDO should not be used to become root.
   Specific authorized commands should be listed in sudoers file. SUDO – su rights should be limited. Subscribe to the automated Linux update services.
34. Periodically check for weak administrative passwords.
35. For systems with multiple users and administrators, determine whether a login warning banner can be implemented (i.e. specifically for GUI login).
36. Routinely check system and log backups as part of system management.
III. References

Books

Web Sites
- [www.sans.edu](http://www.sans.edu)
- [http://www.redhat.com/](http://www.redhat.com/)
- [http://www.debian.org/](http://www.debian.org/)
- [http://kernel.org/](http://kernel.org/)
- [http://www.cisecurity.org/](http://www.cisecurity.org/)
- [http://tldp.org](http://tldp.org)
- [http://www.amanda.org](http://www.amanda.org)
- [http://www.it.jhu.edu/infosec/tips/index.html](http://www.it.jhu.edu/infosec/tips/index.html)
- [https://lightning.nts.jhu.edu](https://lightning.nts.jhu.edu)
- [https://registration.nts.jhu.edu/tripwire/signup.php](https://registration.nts.jhu.edu/tripwire/signup.php)
- [http://www.uptimesoftware.com/](http://www.uptimesoftware.com/)
- [http://www.it.johnshopkins.edu/restricted/security/jhsc.html](http://www.it.johnshopkins.edu/restricted/security/jhsc.html)

IV. Appendix

The CIS Red Hat Enterprise Linux 7 Benchmark will provide specific guidance for establishing a secure configuration for version 7 running x86 and or x64 platforms. The latest version of the guide can be found at [http://benchmarks.cisecurity.org](http://benchmarks.cisecurity.org)