KENNESAW STATE
UNIVERSITY
UNIVERSITY INFORMATION
TECHNOLOGY SERVICES

Linux Server Best Practices

Revised – 05/13/2021
Version 2.0.1

Table of Contents

1. Initial Document 9
2. Revision 9
3. Acknowledgments 9
4. Usage 9
5. Linux Best Practices 9
5.1 Installation 9
5.2 Authentication and Passwords 10
5.3 User Accounts 10
5.4 Disabling Unused Services 10
5.5 File Permissions and ACLs 11
5.6 Kernel Parameters 11
5.7 File Shares 11
5.8 Webservers 11
5.9 Update Practices 11
5.10 Security Related Software 12
5.10.1 Antivirus and Antispyware 12
5.10.2 Firewall 12
5.10.3 SELinux 12
5.10.4 Intrusion Detection System 12
5.11 Auditing Practices 12
5.11.1 Logging 12
5.11.2 Log Retention 13
5.11.3 Auditing Practices 13
5.11.4 NTP - Network Time Protocol 13
6. Exceptions 13
7. References and Resources 13
Appendix I: Examples 15

1. Initial Document

Creation Date: August 21, 2009

2. Revision

Revised By: 2019 Linux Server Security Best Practices

Committee Revision Date: 05/13/2021

Version Number: 2.0.1

3. Acknowledgments

The final release document is a collaborative work between the following committee members:

IE-Linux Team

4. Usage

This document contains a set of guidelines and best practices recommended by the Best Practices Committee at Kennesaw State University.

This document is intended to serve as a general guideline for how servers should be created and maintained. Furthermore, the ever-changing nature of information technology prevents this document from being entirely inclusive but should serve as a general baseline for server installation. Please feel free to query the System Administrators Group and ListServ for additional guidance.

KSU policy regarding server set up and maintenance can be found at university's policy repository, https://policy.kennesaw.edu. Other policies may be applicable to your server based on datausage, programs offered, or other criteria. Please regularly audit the available policies at the policy repository.

5. Linux Best Practices

5.1 Installation

RedHat and CentOS are the preferred versions of Linux. When installing packages should be kept to a minimum. Only packages those that are needed for the proper functioning of the server for its designed purpose should be installed as extraneous packages offer additional avenues of attack. No new server should be created using an operating system which has reached end-of-life. Whenever possible, the newest stable release of an operating system should be used.

Packages and protocols which are inherently insecure will not be installed. FTPD and TelnetD are examples of services which will not be used. Instead use their secured versions, SFTP and SSH.

All servers must have a DNS entry for both forward reverse lookup. The DNS name should be reflective of the function of the server. Alias may be added as CNAME entries. DNS entries can be requested by contacting the service desk.

Once installation is complete, it is the duty of the system administrator to ensure that the system is secure. The process of ensuring this will include a port scan to detect the presence of unnecessarily open ports or active services and a full update of the OS, including all available patches. The system administrator should then contact the service desk to request an audit scan from the UITS-Office of Cyber Security.

5.2 Authentication and Passwords

Configure all services that permit login access to the system to display a logon warning banner (find and example banner in Appendix I). Any time a password would be transmitted over the network, it must do so through an encrypted channel.

Command line access will be accomplished through secure protocols such as SSH with users logging into their own account. If root privileges are need, they may be established after authentication through the use of sudo.

Root will not be allowed direct access remotely and should only logged into directly via the console.

Passwords should never be stored in plain text and all user passwords must comply with the university's password policy. Passwords, including root's, should be changed at least once per year.

5.3 User Accounts

User accounts will only be created on an 'as-needed' basis. When no longer needed, accounts should be disabled and/or deleted. Permissions will be granted at a minimum level which allows a user to perform their job functions. If needed, "sudo" may be used to grant elevated permissions. The proper configuration of "sudo" is not a trivial matter and the Linux system administrator group should be consulted. In order to do so, please contact the service desk.

Contractors and consultants may be granted temporary accounts with pre-set expiration dates. The permissions on these accounts should be even more tightly controlled that normal user accounts. Sudo permissions should not be granted to these accounts.

5.4 Disabling Unused Services

Any service which is not needed for the proper functioning of the service will be disabled.

5.5 File Permissions and ACLs

File permissions and access control lists (ACLs) should be configured in such a way that neither data, scripts, nor executables are available to unauthorized users. Group ownership can be used to grant/restrict access to certain files for multiple users.

5.6 Kernel Parameters

Consider modifying kernel parameters to harden the system against certain types of attacks. Common parameters include enabling ExecShield, TCP SynCookies, source IP address verification, and suspicious packet logging. There are resources on the web which can expand on these options.

5.7 File Shares

File shares on Linux systems will be kept secure and up to date when used. In general, it will be discouraged and avoided if possible. Unsecured shares leave a system vulnerable both to direct attacks and use as an unauthorized share for copyrighted or sensitive data. Infected files may be stored on these shares which are harmless to the host system but have attack vectors on the client machines.

In order to prevent these issues, it is important to keep the packages and programs that provide file sharing stay up to date. The service will be configured such that “Anonymous” logins will not be permitted.

5.8 Webservers

Web servers can be particularly vulnerable to attacks and can serve as vectors to infect othermachines. As such, special care should be taken to secure and harden your webserver.

Web servers should use the HTTPS protocol. At this point the processing requirements of HTTPSare miniscule compared to the processing power available. As with all software, regular updates are a must and the webserver should be included in the monthly update process. The ability to retrieve the web server version, OS information, or directory listings should be disabled as well as any unnecessary modules. The service should be run as a dedicated user and not as root.

These should be considered minimum security requirements. The system administrator isencouraged to look into further ways to harden their webserver.

5.9 Update Practices

Updates and patches maintain the security and integrity of servers and the data which they host. Out of date operating systems allow for the exploitation of known vulnerabilities. Systems should be kept as up to date as possible given any constraints of the technology. Patches and updates should be tested for compatibility with the hardware and software of a given system before being widely distributed.

Normal updates and patches should be applied at least monthly. Critical security vulnerabilities should be patched as soon as possible, even though it may involve unscheduled

downtime. In situations where critical patches are needed, emergency downtime should be coordinated with the Universities' Service Desk and Change Management Committee.

RedHat and CentOS systems should make use of the university's RedHat Satellite server.

5.10 Security Related Software

Servers are vulnerable to many forms of attack. It's important that a server be equipped with safeguards to protect the information resident on the system and the system itself.

5.10.1 Antivirus and Antispyware

Every server will make use of anti-virus and anti-spyware systems. Viruses and spyware which target Linux are limited and less common than those for other operating systems. That does not alleviate the need for anti-virus or anti-spyware software. Files and data are frequently moved between Linux systems and systems with more vulnerable operating systems. Contact ocs@kennesaw.edu if there are specific questions on setting up a Linux AV client.

5.10.2 Firewall

Kennesaw State University employs a campus firewall that protects the campus environment from many threats which originate outside the university's network. This does nothing to protect the systems from all external attacks and offers no protection from on-campus attacks.

All Linux systems must have a local, active firewall. The firewall should be configured such that the default action is to deny, drop, or reject any packet. Ports should be opened only on an "as-needed" basis.

5.10.3 SELinux

SELinux is a suite of kernel modules which implement a high level of security through the use of access control security policies and mandatory access controls. SELinux will be enabled and set to "enforcing" on all Linux servers.

5.10.4 Intrusion Detection System

An additional consideration is that of an Intrusion Detection System. This can add another level of security by alerting you to attempts at unauthorized access. An IDS system should be strongly considered for systems with sensitive information.

5.11 Auditing Practices

5.11.1 Logging

Logging should be configured to assist in security investigations, problem tracking, and troubleshooting. At a minimum, logging should capture at least "critical", "alert" and "emergency" levels. When feasible, "warning" messages should also be logged. Levels above

this are unnecessary except in specific situations and consume large quantities of storage space.

5.11.2 Log Retention

Logs will be kept for a minimum of 30 days. This time frame may be extended in times when having historical logging can assist in trouble shooting long term problems. If you suspect you server may have been attacked, you should extend the log retention time frame to ensure evidence isn't erased.

There are time when logs may be needed for investigations of malfeasance, corruption, or criminal activities. In these cases logs will be kept until such time as the universities legal department give written clearance to destroy them.

5.11.3 Auditing Practices

Logs should be periodically reviewed to ensure proper functionality and that security has not been breached. The frequency of these audits is determined by the importance of the system and the amount of sensitive data stored on the server. Systems which provide infrastructure or are of a critical nature should employ an automated auditing and monitoring suite.

5.11.4 NTP - Network Time Protocol

All Linux servers will be configured to synchronize their time with the university's NTP servers. Primarily this ensures proper functioning of software which can rely on accurate time. Additionally, accurate time is critical in investigations of incidents of systems failure, criminal activities, or other malfeasance.

6. Exceptions

Any exceptions to these best practices will be reviewed and approves by the Office ofCybersecurity (ocs@kennesaw.edu).

7. References and Resources

Useful Links:

- HowToForge: http://www.howtoforge.com/ (good resource with tutorials on securing a variety of Linux distributions)
- Red Hat Enterprise Linux 7 Security Guide: https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Security_Guide/index.html

- Red Hat Enterprise Linux 8 Security Guide: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/pdf/security_hardening/Red_Hat_Enterprise_Linux-8-Security_hardening-en-US.pdf
- Common Vulnerabilities and Exposures (CVE) http://cve.mitre.org/
- Security Focus: http://www.securityfocus.com

Specific programs exist for securing your server:

- http://www.cisecurity.org/bench_linux.html ("benchmarking" your security level)
- http://www.chkrootkit.org/ (program that will check for rootkits on your Linux system)
- http://rkhunter.sourceforge.net/ (alternative to chkrootkit)
- http://www.la-samhna.de/samhain/ (host-based intrusion detection system for Linux, Unix, and Windows)

Appendix I: Examples

Sample Warning Banner (/etc/issue and /etc/issue.net)

***** NOTICE *****

Access to this system is for authorized users of Kennesaw State University only! Unauthorized access may be a violation of Federal and State of Georgia Law, including 18 U.S.C. S1030 and O.C.G.A. 16-9-90et seq. Use of this system constitutes consent to monitoring of such use. Violators will be prosecuted.

***** NOTICE *****