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 11

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. -

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

5.5 File Permissions and

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

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)
-

Appendix