
State Bank of India

Linux - Secure Configuration Document

Version 7



Table of contents

1. Introduction	4
1.1. Purpose of this document	4
1.2. Instructions	4
1.2.1. How to use this document	4
1.2.2. Version Control	4
2. Configuration Document: Linux	5
2.1. Auditing, Logging and Monitoring	5
2.1.1. Auditing should be enabled	5
2.1.2. Security Configuration File changes should be monitored	6
2.1.3. System activities should be logged and reviewed	7
2.1.4. Privileged accounts should be reviewed	8
2.1.5. Trust relationships should be evaluated	8
2.2. File System Access and Management	9
2.2.1. Access to critical file, directories, data and programs should be restricted	9
2.2.2. Users must have an "Umask" value	10
2.2.3. Job entries submitted by deactivated users should be removed	10
2.2.4. Permissions to modify environmental control files should be restricted	11
2.2.5. Restrictions should be set on the public directories	11
2.2.6. User ID and Group IDs should be set	12
2.2.7. The Samba Guest account should be disabled	12
2.3. Password Management	13
2.3.1. User accounts should have passwords	13
2.3.2. Default passwords on software packages should be changed	13
2.3.3. MD5 and shadow passwords should be enabled	14
2.3.4. Strong password policy should be enabled	14
2.3.5. Passwords should be set for the boot loader	16
2.3.6. Single user mode should be password protected	17
2.4. System Configuration	18
2.4.1. Current Patches should be applied to the OS	18
2.4.2. Only authorized users should have access on the FTP and banners should be set	18
2.4.3. Telnet services should be disabled	19
2.4.4. Only essential services should be enabled on the system	20
2.4.5. Set login banners	23
2.4.6. Network settings should be configured appropriately	23
2.4.7. Disable Ctrl+Alt+Del functionality	24
2.4.8. Disable remote root login	25

.....	
2.5. User Management	26
2.5.1. Dormant accounts should be deleted and null shell should be set for default users	26
2.5.2. Accounts should have unique User Ids	26
2.5.3. System resource limit should be set for the users	27

1. Introduction

1.1. Purpose of this document

This document is intended to guide administrators to secure Operating Systems. All administrators should use this document for secure configuration.

1.2. Instructions

1.2.1. How to use this document

The security settings described in this document shall be configured on the Operating Systems by the administrators. All settings can only be done with administrative privileges. It is strongly recommended that all the settings be tested on the staging environment before applying on production environment. These settings should be applied on the Operating Systems after all applications have been installed. It is further recommended that the administrators of the Operating Systems make note of the original values while changing the settings. For each setting, a category is given, followed by control objective, control statement, risk rating, the risk/impact if the setting is not configured and the solution/implementation steps to fix it. Adequate backups should be taken before making any changes to the production system so that roll back is possible, in case system / application stop working.

1.2.2. Version Control

Version	Description of Change Request	Requested By	Approved By	Version Release Date
Version 6	<ul style="list-style-type: none"> Segregation of controls as per domains/category Changes made in File System Access and Management, Password Management and User Management Old SCD version 5 had 24 controls and New SCD version 6 has 29 controls 	SBI	SBI	01-04-2014
Version 7	<ul style="list-style-type: none"> No major changes 	SBI	SBI	15-06-2015

2. Configuration Document: Linux

2.1. Auditing, Logging and Monitoring

2.1.1. Auditing should be enabled

Control Statement

Auditing should be enabled for failed account logon events.

Risk/Impact

Multiple failed logons may indicate attempts to compromise the system. Auditing failed logons enhances the organization's ability to detect unauthorized access attempts on the system.

Risk Rating

High

Implementation Steps

Review the /var/log/messages file for failed login attempts with the following commands:

```
#/bin/grep "FAILED LOGIN" /var/log/messages
```

```
#/bin/grep "Failed password" /var/log/secure
```

Review the /etc/syslog.conf file and ensure that "authpriv.info" messages are being logged. This setting may be achieved in several different ways, e.g., *.* , authpriv.* , *.notice, or *.info.

If the above mentioned files are not present, create the files by executing the following command:

```
touch /var/log/messages
```

```
touch /var/log/secure
```

```
chown root /var/log/messages
```

```
chown root /var/log/secure
```

```
chmod 600 /var/log/messages
```

```
chmod 600 /var/log/secure
```

2.1.2. *Security Configuration File changes should be monitored*

Control Statement

Security configuration file changes should be monitored in accordance with corporate standards. Unauthorized changes to security configuration files should be investigated.

Risk/Impact

Unauthorized changes to sensitive configuration files (e.g. the /etc/passwd, /etc/shadow, /etc/group, /etc/inet/inetd.conf) may compromise system integrity. Monitoring changes to key files can assist in identifying a compromise, or in determining the point of entry.

Risk Rating

High

Implementation Steps

Change the owner of these files to root and also change the permission using the following commands:

```
cd /etc
```

```
chown root:root passwd shadow group
```

```
chmod 644 passwd group
```

```
chmod 400 shadow
```

2.1.3. ***System activities should be logged and reviewed***

Control Statement

System activities should be adequately logged and reviewed in accordance with corporate standards. Strong permissions should be set on the log files.

Risk/Impact

Insufficient logging will result in a lack of an audit trail in the event of an unauthorized access. Logging and monitoring processes assist administrators in identifying events that indicate a problem is occurring.

Risk Rating

Medium

Implementation Steps

System activity log:

- 1) Open the /etc/syslog.conf configuration file in an editor. Enable proper logging in accordance with corporate policies.
- 2) At a minimum, authentications events should be logged with the syslog logging facility.

Add the following line to /etc/syslog.conf if not already present.

authpriv.* /var/log/secure

- 3) Activate the changes using the following command:

#pkill -HUP syslogd.

- 4) Review /var/log/messages and /var/log/secure in accordance with corporate policy with the following command to view system and security events:

more /var/log/messages.

Strong permissions setting:

Enable logging in the syslog.conf file. Secure the permission of the above files and give them permission as mentioned below. Use programs like logcheck and swatch to filter out the suspicious entries in the log files.

Check the permission on the following files:

- 1) ls -l /var/log/messages. The safe permission is 600.
- 2) ls -l /var/log/wtmp. The safe permission is 600.
- 3) ls -l /var/log/xferlog. The safe permission is 600.
- 4) ls -l /var/log/cron. The safe permission is 600.
- 5) ls -l /var/log/lastlog. The safe permission is 600

2.1.4. **Privileged accounts should be reviewed**

Control Statement

The use of privileged accounts (e.g. root) should be logged and reviewed regularly.

Risk/Impact

Monitoring the use of escalated privileges decreases the likelihood that escalated privilege abuse will go undetected.

Risk Rating

Medium

Implementation Steps

For baseline implementation:

- 1) Review the /var/log/messages file for privilege escalation attempts related to the su command.
- 2) Review /var/log/secure file for unauthorized privileged escalation related to the sudo command.
- 3) Investigate any unauthorized privilege escalation

2.1.5. **Trust relationships should be evaluated**

Control Statement

Trust relationships should be evaluated regularly. Any relationships that do not serve a business or operational purpose should be removed.

Risk/Impact

Trust relationships increase the risk of system compromise: if a trusted system is compromised, a malicious user may be able to directly access multiple trusted systems.

Risk Rating

Low

Implementation Steps

- 1) Find any .rhosts or .shosts files that have been created since the initial installation or the previous security check with the following command
`# find {home-directories} -name .rhosts -ls`
- 2) Also review the /etc/hosts.equiv and /etc/ssh/shosts.equiv files and investigate the purpose of these files and remove them if they are not necessary.
- 3) Review the contents of the /etc/hosts.equiv, /etc/ssh/shosts.equiv, .shosts and .rhosts files and ensure the users and machines listed have been approved. Ensure there is no "+" sign in any of the files as this grants access to all users.

2.2. File System Access and Management

2.2.1. Access to critical file, directories, data and programs should be restricted

Control Statement

Access to critical file, directories data and programs should be restricted based on the user's business requirements. Role-based access control should be used, granting access based on the principle of least-privilege.

Risk/Impact

If access to application programs and data is not restricted to appropriate individuals, sensitive data could be viewed, modified or deleted by a malicious user.

Risk Rating

High

Implementation Steps

Determine the critical data and program files, and identify the permissions on them by running the command
`$ls -la filename`

If the last character in the permissions string is a +, execute

`$ getfacl filename` to view the extended ACLs

Access should be granted on a least-privilege basis. Use the following commands to set secure permissions:

`# chown owner filename`

to set the file's owner

`# chgrp group filename`

to change a files' group

`# chmod permissions filename`

to change a file's Basic Permissions

If there are extended ACLs on files, use the command

`# setfacl command to change a file's Extended Permissions.`

Consult the man page for "setfacl" for detailed instructions on assigning extended permissions.

Critical Files/directories such as:

/	/etc/security	/usr/bin	/usr/local/bin	/var/log
/bin	/home	/usr/sbin/	/usr/local/sbin/	/var/www/
/dev	/opt	/usr/etc	/usr/local/lib	/var/nis/
/etc	/sbin	/usr/lib	/usr/spool	/var/spool
/etc/*.*d	/usr	/usr/local	/var	/var/spool/cron/crontabs

2.2.2. Users must have an "Umask" value

Control Statement

All users should have a "umask" value, which defines the permissions to newly created files, of 027.

Risk/Impact

The "umask" variable is used for default file-creation permissions. Permissive "umask" settings allow users other than the owner of the file read or write permissions to files. This increases the risk that file permissions will be unintentionally weak, allowing unauthorized users to view, delete, or modify sensitive information.

Risk Rating

Low

Implementation Steps

Edit existing users, including root's, .profile and .cshrc files with the following parameter:

umask=027

Modify the default /etc/profile file with the umask=027.

2.2.3. Job entries submitted by deactivated users should be removed

Control Statement

Entries submitted to the system job scheduling programs by deactivated users should be removed.

Risk/Impact

Permitting scheduled jobs to run under the context of a user account no longer on the system increases the risk that a new user will be created with the same user ID and gain control over the job. This could lead to unauthorized access to data.

Risk Rating

Medium

Implementation Steps

Remove all cron files for non-existent users from the /var/spool/cron directory. If these jobs are essential to system operation, they should be scheduled to run using a valid user identification code. Remove all jobs in third party scheduling software for non-existent users.

2.2.4. Permissions to modify environmental control files should be restricted

Control Statement

Permission to modify environmental control files in user home directories should be restricted to the owner of the file.

Risk/Impact

Environmental control files are used to create the control and operating environment for users. Parameters set in this file override global control settings. If an unauthorized user is able to modify these files, that user could escalate their privileges, or cause commands to be executed as the target user when that user next logs in.

Risk Rating

Medium

Implementation Steps

- 1) Protect files, such as .profile, .kshrc, .cshrc and .login from write access by anyone other than the file owner and/or system administrator.
- 2) If users are given the ability to modify the contents of these files or their permissions, periodic checks of these files to ensure compliance with minimal controls requirements is recommended.
- 3) If the system administrator (owner=root) controls access then the security administrator should monitor and reconcile changes to ensure they are appropriate and authorized.
- 4) The security administrator should verify that the file permissions are set at 700 on these files.

2.2.5. Restrictions should be set on the public directories

Control Statement

Public directories, such as /tmp/, should have restrictions to protect files located within those directories from deletion by users other than their owners.

Risk/Impact

Public directories allow any user to read, write, and delete any file located within the directory. This increases the risk that users could inadvertently delete files of which they are not the owner. Allowing a user write permission to a directory when they have not been authorized write access to all of the files contained in that directory increases the risk of unauthorized modifications.

Risk Rating

Medium

Implementation Steps

Use the following command to identify directories with world writeable permissions

```
# find / -perm -2 -type d -ls
```

Verify the sticky bit is set appropriately from the above output. The last character will be a t or T. If the sticky bit is not set, issue the following command to activate the sticky bit:

```
# chmod u+t
```

State Bank of India - Linux - Secure Configuration Document

PwC

2.2.6. **User ID and Group IDs should be set**

Control Statement

Set user ID (setUID) and set group ID (setGID) files should only exist if they are needed for the proper functioning of the system, and they should only be writeable by the owner of the file.

Risk/Impact

Poorly designed setUID/setGID programs could be abused by malicious users, allowing them to execute a shell with privileged access. Once at the shell prompt, the user would retain the same access as the actual owner of the setUID/setGID file. This is especially dangerous when the file is owned by root. Each setUID/setGID file on the system has the potential of containing a buffer overflow vulnerability that is not yet publicly known.

Risk Rating

High

Implementation Steps

Run the following command to locate all SUID files:

```
# find / -type f -perm -04000 -exec ls -l {} \; | tee /tmp/suidfiles
```

Review the output and determine if the listed files need to be run as root. Remove the SUID bit on files that do not need to be run as root by running the following command:

```
# chmod o-s filename
```

Run the following command to locate all SGID files:

```
# find / -type f -perm -02000 -exec ls -l {} \; | tee /tmp/sgidfiles
```

Review the output and determine if the listed files need to be run as a privileged group. Remove the SGID bit on files that do not need to be run as root by running the following command:

```
# chmod g-s filename
```

2.2.7. **The Samba Guest account should be disabled**

Control Statement

The Samba guest account should not be enabled.

Risk/Impact

The Samba guest account provides anonymous access to file shares on the system and may lead to the disclosure of sensitive data.

Risk Rating

Low

Implementation Steps

Review the /etc/samba/smb.conf file and verify that the line containing "guest account" is commented.

2.3. Password Management

2.3.1. User accounts should have passwords

Control Statement

All user accounts should have passwords.

Risk/Impact

User accounts without passwords increase the risk that unauthorized users will gain access to the system. Once a malicious user has obtained a list of system users, a common next step in attempting to compromise the system is to try logging into each account with a blank password.

Risk Rating

High

Implementation Steps

- 1) Identify any accounts without passwords using the following command:
`# cat /etc/passwd | cut -d':' -f1 | xargs -i passwd -S {}`
- 2) Accounts without passwords will not have any characters between the second and third set of colons; and
- 3) Set passwords on any accounts found without passwords using the following command:
`# passwd username`

2.3.2. Default passwords on software packages should be changed

Control Statement

Default passwords supplied with software packages should be changed upon installation. In addition, these passwords should be complex and conform to corporate security standards and guidelines.

Risk/Impact

Application default passwords are widely known and are often initial targets for attacks. The risk that unauthorized access will be obtained by malicious users increases if these passwords are not changed.

Risk Rating

Medium

Implementation Steps

- 1) Identify the default accounts in /etc/passwd using the following command:
`# cat /etc/passwd`
- 2) Use the following command to change the passwords supplied with software packages:
`# passwd username`

2.3.3. MD5 and shadow passwords should be enabled

Control Statement

Passwords are very sensitive information which needs to be protected. Passwords can be secured against unauthorized access by implementing MD5 and shadow passwords features.

Risk/Impact

The /etc/passwd file must be readable by any user on the system for programs to function properly. If password hashes are stored in this file then any user can retrieve the hashes and attempt to crack them using "brute force" techniques. If permissions on password files are weak then any user could change other passwords or retrieve password hashes.

Risk Rating

High

Implementation Steps

- 1) Identify user accounts that have password hashes stored in the passwd file by issuing the following command to examine the passwd file:

```
#more /etc/passwd
```

- 2) Run the following command to merge the password hashes remaining in /etc/passwd into the /etc/shadow file:

```
#pwconv
```

- 3) Verify the permissions of the /etc/passwd and /etc/shadow files by issuing the following commands:

```
#ls -l /etc/passwd
```

```
#ls -l /etc/shadow
```

The recommended permissions are:

permissions for /etc/passwd - 644

permissions for /etc/shadow - 400

2.3.4. Strong password policy should be enabled

Control Statement

Password policy is required to control user passwords including password minimum length, password aging and other critical parameters.

Risk/Impact

Users may use weak passwords or same password for long time. The accounts with such passwords can get compromised.

Risk Rating

High

Implementation Steps

To configure password policy, edit /etc/login.defs file and set the following password configuration:

```
vi /etc/login.defs
```

```
PASS_MIN_LEN=8
```

```
PASS_MAX_DAYS=45
```

```
PASS_MIN_DAYS=7
```

```
PASS_WARN=14
```

Configure the Pluggable Authentication Modules (PAM) sub-system to utilize the below library on the "password required" line in the /etc/pam.d/system-auth file:

```
/lib/security/$ISA/pam_cracklib.so
```

This will ensure that it uses the password dictionaries /usr/lib/cracklib_dict.* for newly created passwords.

Configure PAM to require the use of "credits" which will enforce the user of numbers, special characters, and mixed cases in passwords. Ensure the following parameters are present in the line where "pam_cracklib.so" is referenced:

```
dcredit=-1 ucredit=-1 lcredit=-1
```

This will require the use of 1 uppercase alphabet character, 1 numeric digit, and 1 lowercase alphabet character.

For enhanced implementation:

Configure PAM password "credits" to require multiple numeric digits and special characters. Ensure the following parameters are present in the line where "pam_cracklib.so" is referenced:

```
dcredit=-2 ucredit=-1 lcredit=-1 ocredit=-2
```

This will require the use of 1 uppercase alphabet character, 2 numeric digits, 1 lowercase alphabet character, and 2 special characters.

Ensure PAM is configured to lock accounts after a predetermined number of authentication failures. Verify the following parameters exist in the pam_tally declaration in /etc/pam.d/system-auth:

```
onerr=fail no_magic_root deny=5 reset
```

2.3.5. **Passwords should be set for the boot loader**

Control Statement

Set passwords for Grub or LILO.

Risk/Impact

An unprotected GRUB/LILO boot loader prompt allows an attacker with physical access to subvert the normal boot process very easily. The action below will allow the system to boot normally, only requiring a password when anyone attempts to modify the boot process by passing commands to GRUB/LILO.

Risk Rating

Medium

Implementation Steps

Securing LILO:

- 1) Edit the /etc/lilo.conf file using your favourite editor.
- 2) Add the following lines under the label=linux line. [root@localhost root]# less /etc/lilo.conf prompt

```
timeout=50 default=linux boot=/dev/sda
```

```
map=/boot/map
```

```
install=/boot/boot.b
```

```
message=/boot/message
```

```
linear
```

```
image=/boot/vmlinuz-2.4.18-14
```

```
label=linux password=yourpassword
```

```
restricted initrd=/boot/initrd-2.4.18-14.img
```

```
read-only
```

```
append="root=LABEL=/"
```

After adding these two lines, save the lilo.conf file and quit your editor. Change the permissions of that file to 0600 and run the lilo program once using lilo command.

```
#chmod 0600 /etc/lilo.conf
```

```
#lilo
```

Securing GRUB:

- 1) As a root user type the following command,

```
#/sbin/grub-md5-crypt
```

```
password: <your password>
```

2) #<MD5 hash of your password>

Copy the MD5 hash of the password for later use.

3) Open /etc/grub.conf and add the password parameter below the splashimage parameter line.
Splashimage=(hd0,1)/grub/splash.xpm.gz

password -md5 <MD5 hash of password>

4) Change the permissions of the file to 0600 and run the grub program once using grub-install
/dev/hda command.

```
#chmod 0600 /etc/grub.conf #grub-install /dev/hda
```

2.3.6. Single user mode should be password protected

Control Statement

Linux provides a mechanism for system maintenance via “Single user mode” which is typically started when the system is booting.

Risk/Impact

This allows an attacker at the console to bypass any system protection and move into run level 1 as root and change system settings.

Risk Rating

Medium

Implementation Steps

To password protect single user mode, edit /etc/inittab file to have entry as shown below.

```
vi /etc/inittab
```

```
id:5:initdefault:
```

```
~~:S:wait:/sbin/sulogin
```

Save the changes and restart the service: [/sbin/init q]

2.4. System Configuration

2.4.1. Current Patches should be applied to the OS

Control Statement

Current patches should be applied to the operating system.

Risk/Impact

Current versions of the operating system contain processing and security enhancements. A system that is not updated with the latest security patches is vulnerable to well-known, published exploits. Such exploits may allow remote or local users to obtain privileged access and the ability to modify or delete data. Vendors release security patches and fixes to address these vulnerabilities.

Risk Rating

Medium

Implementation Steps

- 1) Determine the kernel version by examining the output of the \$uname -r command
- 2) ensure the kernel is up-to-date by comparing the output to the latest version from kernel.org or the vendors website.
- 3) Use the "yum" utility to patch non-kernel components.

Up2date is deprecated in RHEL v5 and has been replaced with "yum". "up2date" is still used in RHEL v4.s

2.4.2. Only authorized users should have access on the FTP and banners should be set

Control Statement

FTP access should be restricted only to users who require it and if FTP is used set appropriate banners.

Risk/Impact

Without the existence of the /etc/vsftpd.ftpusers or the /etc/vsftpd.user_list files, any user listed in the /etc/passwd file can transfer files across the network. This increases the risk that unauthorized files are transferred across the network.

Risk Rating

Medium

Implementation Steps

For baseline implementation: Restricted Access

- 1) Review the /etc/pam.d/vsftpd file. Ensure the following line exists and is un-commented: "auth required pam_listfile.so item=user sense=deny file=/etc/vsftpd.ftpusers onerr=succeed" ;
- 2) Review the /etc/vsftpd.ftpusers or ftpusers file. Ensure at a minimum the following accounts are listed:
- root - bin - sys - uucp - sync - any guest accounts - accounts with restricted shell - privileged application accounts such as "oracle" - any other account that should not be copying files across the network

For enhanced implementations:

- 1) Review the /etc/vsftpd.user_list or ftpusers file. Verify with the system administrator that users listed require ftp access; and
- 2) Open the /etc/vsftpd/vsftpd.conf or /etc/vsftpd.conf file using an editor. Verify the userlist_enable variable is set to YES. Verify the userlist_deny variable is set to NO.
- 3) Create the file if it does not exist and set appropriate file permissions and ownership with the following commands:

```
# chmod 600 /etc/ftpusers or /etc/vsftpd.ftpusers  
# chown root /etc/ftpusers or /etc/vsftpd.ftpusers
```

FTP banners:

- 1) The FTP banner should be set in the ftpd_banner parameter in the /etc/vsftpd/vsftpd.conf or /etc/vsftpd.conf file using following commands.

vi /etc/issue.net

vi /etc/vsftpd/vsftpd.conf

2.4.3. **Telnet services should be disabled**

Control Statement

The Telnet service should be disabled.

Risk/Impact

The Telnet protocol does not encrypt credentials or data, increasing the risk that a malicious user will obtain sensitive information through network sniffing.

Risk Rating

Low

Implementation Steps

Disable the Telnet service in the xinetd services daemon and implement an encrypted remote access method such as SSH.

1. Open the /etc/xinetd.d/ or /etc/init.d/ folder and search for telnet file.
2. Add the line "disable = yes".
3. Restart the xinetd process by performing the following commands: # pkill -HUP xinetd.

State Bank of India - Linux - Secure Configuration Document

PwC

19

2.4.4. ***Only essential services should be enabled on the system***

Control Statement

Only services that serve a documented operational or business need should be listening for network connections.

Risk/Impact

Each listening service is an avenue of communication with the network and presents risk to the system. The service may be accessed repeatedly, denying legitimate users access to the system and degrading performance. A buffer overflow vulnerability may exist which could allow a remote attacker to obtain privileged access to the system.

Risk Rating

High

Implementation Steps

Identify all the running services using the following command:

```
# netstat -tupan
```

Open the /etc/xinetd.conf or inetc.conf file in an editor and disable any unneeded services listed in this file by adding a # to the beginning of their configuration line. Disable any unneeded services by adding a "disable = yes" line to the appropriate /etc/xinetd.d/ file and restart the inetc process by performing the following command:

```
# pkill -HUP xinetd
```

or

```
# pkill -HUP inetc
```

SERVICE	COMMENT
Anacron	(Turn on if you schedule jobs using cron on this server)
Apmd	(If ACPI is ON this can be turned off)
atd	(Turn on if you schedule jobs using at on this server)
Avahi-daemon	
Bluetooth/hidd/pand	
Capi	
Crond	(Turn on if you schedule jobs using cron on this server)
CUPS/cups-config-daemon	
Dhcdbd	(Can keep this ON if IP Addressing is controlled using DHCP)
Httpd	(Retain if this is a web-server and you are using Apache to host the website)
Iptables/ip6tables	(If you're using the fire-walling services on this box keep it running)
Irda	
Irqbalance	(Useful only in multi-processor systems; turn it ON if the server is a multi-processor system)
Kudzu	
Lisa	
Mdmonitor	(Retain if Hard disks configured with RAID support)
NetworkManager/ NetworkManagerDispatcher	
Named	(Turn this ON if this is a DNS server)
Nfsd	(Turn this ON if you use NFS for file sharing across networks)
Nscd	(Retain only if you are running NIS or LDAP)
Ntpd	(Retain only if you are hosting an NTP server on this)
Portmap	(Retain if you are using RPC services)
Rpcgssd/rpcidmapd/rpcsvcgs sd	
Sendmail	(Turn on if you hosting an Email server)
Smartd	
Winbind	(Keep this ON if SAMBA is used for accessing shares over the network)
Ypbind	(Retain if you are using NIS/NIS+)
finger	
netstat	
rstatd	
systat	

2.4.5. Set login banners

Control Statement

A legal warning should be implemented to provide notice to users that activity is monitored.

Risk/Impact

Displaying a legal warning ensures that users are aware of the consequences of unauthorized access and assists in conveying the protection of corporate assets should an incident ever result in litigation.

Risk Rating

Low

Implementation Steps

For baseline implementation:

- 1) Obtain a legal warning message from a legal authority or corporate standards body.
- 2) Edit the pre-login message file, /etc/issue to include the legal warning message and for post log on message edit /etc/motd
- 3) Edit the Secure Shell Daemon configuration file, /etc/ssh/sshd_config.
- 4) Add the following line to the file

Banner=/etc/issue

2.4.6. Network settings should be configured appropriately

Control Statement

There are several kernel options in Red Hat Linux that can be configured to increase the overall network security. The kernel can be modified by editing /etc/sysctl.conf file. The file is loaded whenever the server reboots or an administrator manually restarts the network services.

Risk/Impact

Weak network settings can be used to launch DOS attacks on the server or use the machine as an intermediary in attacks.

Risk Rating

Medium

Implementation Steps

Set the value of the parameters as following in /etc/sysctl.conf file

```
net.ipv4.conf.default.secure_redirects = 0  
net.ipv4.conf.all.secure_redirects = 0  
net.ipv4.icmp_echo_ignore_broadcasts = 1  
net.ipv4.conf.all.accept_redirects = 0  
net.ipv4.conf.default.accept_redirects = 0  
net.ipv4.tcp_syncookies = 1  
net.ipv4.tcp_max_syn_backlog = 4096  
net.ipv4.conf.all.rp_filter = 1  
net.ipv4.conf.default.rp_filter = 1  
net.ipv4.conf.all.accept_source_route = 0  
net.ipv4.conf.default.accept_source_route = 0  
net.ipv4.ip_forward = 0  
net.ipv4.conf.all.send_redirects = 0  
net.ipv4.conf.default.send_redirects = 0  
net.ipv4.icmp_ignore_bogus_error_responses = 1
```

2.4.7. Disable Ctrl+Alt+Del functionality

Control Statement

By default CTRL-ATL-DEL to reboot the machine functionality is enabled in the system. This allows any user to reboot the machine.

Risk/Impact

This function allows an attacker to reboot the server.

Risk Rating

Medium

Implementation Steps

To disable CTRL-ATL-DEL functionality:

- 1) Edit /etc/inittab file comment the following line:

```
vi /etc/inittab  
ca::ctrlaltdel:/sbin/shutdown -t3 -r -now
```

- 2) Save the change and restart init service for the change to take effect: /sbin/init q

2.4.8. ***Disable remote root login***

Control Statement

Root user must not be able to login from a remote console. The login command is part of the authentication process to access a local Linux Operating Environment account. Any action requiring direct login to the system using "root" should be restricted to the local console.

Risk/Impact

Login to the system through telnet session can reveal the clear text password of root user. Allowing remote login for root also enables a malicious user to attempt access to the system leading to system compromise.

Risk Rating

High

Implementation Steps

- 1) View the /etc/securetty file to verify that the "console" and "tty#" entries are the only entries in the file.
- 2) View the /etc/security/access.conf file. Ensure the following line is present: -:root:ALL EXCEPT LOCAL

2.5. User Management

2.5.1. **Dormant accounts should be deleted and null shell should be set for default users**

Control Statement

Accounts of users who are no longer employed, or no longer need their accounts, should be deleted or disabled and null shell should be set for the default users.

Risk/Impact

Non-essential user accounts increase the likelihood of compromise by providing attackers with more user accounts to check for security holes.

Risk Rating

Medium

Implementation Steps

For baseline implementation to disable unwanted accounts:

- 1) Disable un-necessary user accounts using the following command: # passwd -l
- 2) Delete un-necessary user accounts using the following command: # userdel

Set the null shell (/sbin/nologin **or** /bin/false **or** /sbin/false **or** /usr/bin/false **or** /sbin/noshell **or** /bin/noshell **or** /usr/bin/noshell **or** /dev/null **or** /bin/nologin **or** /usr/bin/nologin) for all the non essential users account given below:

Lp, Sync, Shutdown, Halt , News, uucp, operator, games, gopher, adm, ftp, nobody, nsqd

2.5.2. **Accounts should have unique User Ids**

Control Statement

Each account should have a unique user ID (UID).

Risk/Impact

Duplicate UIDs increase the risk that unauthorized users will modify or delete files created by another user, decreasing individual accountability. Duplicate root-equivalent accounts (UID=0) increase the risk that users have system access privileges that are not required for their job functions. In addition, unauthorized users who target root-equivalent accounts will have multiple opportunities to gain root access.

Risk Rating

Medium

Implementation Steps

Ensure that accounts with same UID as that of root are authorized system administrators. In the /etc/passwd file change the UID of such accounts.

```
usermod -u <changed UID> username
```

2.5.3. *System resource limit should be set for the users*

Control Statement

By default no restriction is specified for the system users regarding consumption of system resources.

Risk/Impact

If users consume too many system resources, then denial of service can happen.

Risk Rating

Low

Implementation Steps

/etc/security/limits.conf file so that core files will not be created, individual file sizes are limited to 100 MB, and a user can only have 150 concurrent process running. Note however that these requirements can change based on organizational requirements.

```
vi /etc/security/limits.conf (Add these lines)
```

```
* hard core 0
```

```
* hard fsiz 102400
```

```
* hard nproc 150
```