# Auditing Linux/Unix Server Operating Systems

**Muhammad Mushfiqur Rahman, CISA, CEH, CHFI, CCNA, ISO 27001 LA, ITIL V3, MCITP, MCP, MCSE, MCTS, OCP, SCSA,** has 12 years of IT operations, project management and custom business solutions, enterprise resource planning implementation, and information security analysis and management experience. Rahman is an information security analyst at Eastern Bank Limited, Bangladesh. He also has 12 years of experience teaching IT courses for end users and IT professionals. He can be reached at *mushfique98@gmail.com.*



Server auditing is an important task to ensure platform-level security in an IT infrastructure and to ensure the proper configuration of Linux server security. The Linux system has its own security configuration and management system to address the security requirements in an enterprise environment. The system administrator needs to configure the Linux system to get more security assurance from the system, and IS auditors need to check the Linux system configuration as per audit standards to ensure the secure system is in place in the enterprise.

It is an exigent task for a system administrator to secure the production system from malicious attacks.

## AUDITING PHYSICAL SYSTEM SECURITY

Physical security is the first and foremost task for any information system audit. Auditors must determine that the physical security of the systems configuration is standard, while also ensuring that the basic input-output system (BIOS) and the personal computer (PC) booting from CDs/DVDs, external devices and floppy drives in BIOS are rendered inoperative. Then, the auditor must ensure that the password is enabled in BIOS and that it also protects the GRand Unified Bootloader (GRUB) to ensure the restriction of physical access of the server.

In Linux or Unix-like systems, anyone can log in to the server in single-user mode using GRUB, as per the system configuration. Auditors must be certain that GRUB is protected with a strong password.

## PROTECT GRUB USING PASSWORDS

To protect GRUB, administrators must use the strongest possible password and issue a command using a message-digest 5 (MD5) hash password:

```
[root@host-1[1]~]# grub-md5-crypt
```

After issuing the command, the administrator should open the /boot/grub/menu.lst or /boot/grub/grub.conf file and add the MD5 password:

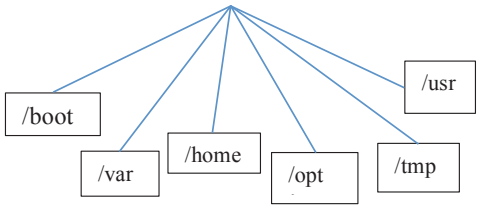
```
[root@ host-1  ~]# vi /boot/grub/menu.lst or
[root@ host-1  ~]# vi /boot/grub/grub.conf
```

The newly created MD5 password can then be added to the GRUB configuration file.

## AUDITING DISK PARTITIONING IN THE AUDITED SYSTEM

In the system configuration, hard disk partitioning is critical. If any flaw exists in the partitioning, it will lead to data loss and possibly to disclosure, which could threaten the confidentiality of the data. During the audit, the auditor needs to examine and evaluate the different partitions in the audited server to ensure data security in case of any disaster. An administrator can group and separate the data among different partitions. This configuration ensures that only the data of that particular partition are lost if any unexpected accident occurs, despite the fact that the data on other partitions continue to exist. Auditors need to check that systems are configured in a way that allows separate partitions and ensure that third-party applications are installed on separate file systems. A secure directory structure is illustrated in **figure 1**.

**Figure 1—Secure Directory Structure**




Source: Muhammad Mushfiqur Rahman. Reprinted with permission.

## AUDITING SERVERS FOR INSTALLED PACKAGES

It is recommended that when configuring the server, only the necessary packages should be installed. This ensures that the administrator may follow the standard configuration criteria of his/her organization and may scan the server using the Center for Internet Security Configuration Assessment Tool (CIS-CAT) and follow the recommendations of CIS-CAT. Unnecessary packages should not be installed into the system because such packages may create

a vulnerability in the system. During the audit program, the auditor must evaluate and check the installed packages of the audited server to minimize the risk that compromising one service may lead to compromising other services. To ensure vulnerability minimization in the audited server, installed packages must be examined and unwanted installed services identified. Services that are running on run level 3 can be identified using the "chkconfig" command:

```
# /sbin/chkconfig --list |grep '3:on'
```

To examine all installed packages in a system, the following command can be used:

```
# sudo apt-get remove package-name
```

A sample script1 can be used to check the services running in the system:

```
#!/bin/bash
if (( $(ps -ef | grep -v grep | grep $service | wc -l) > 0 ))
then
echo "$service is running!!!"
else
/etc/init.d/$service start
Fi
```

## AUDIT THE LISTENING PORTS

With the help of the Netstat networking command, all open ports and associated programs can be viewed. A sample script[2] is:

```
# netstat–tulpn
```

A script for port scanning is:

```
scan() {
  if [[ -z $1 || -z $2 ]]; then
    echo "Usage: $0 <host><port, ports, or port-range>"
    return
  fi

  local host=$1
  local ports=()
  case $2 in
    *-*)
      IFS=- read start end <<< "$2"
      for ((port=start; port <= end; port++)); do
        ports+=($port)
      done
      ;;
    *,*)
      IFS=, read -ra ports <<< "$2"
      ;;
    *)
      ports+=($2)
      ;;
  esac
  for port in "${ports[@]}"; do
    alarm 1 "echo >/dev/tcp/$host/$port" &&
      echo "port $port is open" ||
      echo "port $port is closed"
  done
}
```

## AUDIT REMOTE CONNECTIVITY OF THE AUDITED SERVER

Configuration of remote connectivity of the system in the network is penetrating and the remote protocol Telnet and rlogin is vulnerable because of the nonencrypted plaintext password and data transmission during the remote login. During the audit, the enabled remote connectivity services of the server should be checked, and the Secure Shell (SSH) protocol, which uses encryption technology during communication with the server should be examined. It is also necessary to check that the root login is disabled, the SSH port number is changed and the default port that is used by the audited server allows only specific authorized users access to the system. To do this, the auditor opens the main SSH configuration file and creates these parameters to restrict users' access:

```
# vi /etc/ssh/sshd_config
```

## DENYHOSTS AND FAIL2BAN

During the audit, the auditor should test the DenyHosts and Fail2ban feature. This is a log-based open-source intrusion prevention script used for SSH servers. This script is used by system administrators and users to monitor and analyze SSH server access logs for failed login attempts, known as dictionary-based attacks and brute-force attacks. In this script, the administrator can set the threshold for predefined failed logins from a specific Internet Protocol (IP) address and can ban the connection from specific IP addresses.

The features of DenyHosts include:

- Keeps and tracks logs from the /var/log/secure file, noting all successful and unsuccessful login attempts, and filters them.
- Regularly monitors the host as well as failed login attempts

- Sends email notification regarding blocked hosts and suspicious logins

The features of Fail2ban include:

- Keeps and tracks logs from /var/log/secure and /var/log/auth.log, /var/log/pwdfail
- Highly configurable and multithreaded
- Regularly monitors log files

### AUDITING THE ROOT LOGIN STATUS

During the audit, the auditor should check whether Linux systems allow remote login using SSH for everyone with root user status. This configuration allows users with root user credentials to directly log in to the system. To protect the server from remote login, the root user administrator must disable the root access remotely. Systems can be saved by using the strongest passwords, but it is also recommended that administrators disable the root login from the remote connection and have a separate login ID. Another recommendation is that users use sudo to gain root access in the server.

### AUDITING SSH PASSWORDLESS LOGIN

During the audit, the auditor should test the SSH passwordless login. Normally, system administrators use this feature for programmed backups, remotely executed required script, file transfers and remote script management, because it allows the administrator to perform these tasks without entering a password.

### AUDITING THE SYSTEM FOR UPDATED PATCHES

Systems must be updated with the latest releases' patches, security fixes and kernels when those become available:

```
# yum updates
# yum check-update
```

### AUDITING THE CRON JOBS STATUS

During audits, the auditor should check the built-in feature of cron jobs (cron) where it allows one to specify who may and who may not run jobs. This is controlled by the use of files called /etc/cron.allow and /etc/cron.deny. To lock a user using cron, usernames should be added to cron.deny. To allow a user to run cron, the user must be added to the cron.allow file. To disable all users from using cron, add the ALL line to the cron.deny file:

```
# echo ALL >>/etc/cron.deny[3]
```

### AUDITING THE STATUS OF USB DEVICES

During the audit, it is also important to examine and/or disable Universal Serial Bus (USB) devices. To mitigate data loss and control the spread of malware, users must be restricted from using USB devices in the systems.

### AUDITING THE STATUS OF SELINUX

During audit, it is important to observe the status of Security-enhanced Linux (SELinux). It is an essential security mechanism for logical access control, which is provided in the kernel. This feature must be enabled in the system. Disabled SELinux demonstrates that the security mechanism has been deleted from the system.

The operations modes of SELinux include:

- **Enforcing**—This is the default mode of SELinux; it enforces the SELinux security policy in the machine.
- **Permissive**—This mode is used to troubleshoot SELinux-related issues; it tracks the log for each activity.
- **Disabled**—This mode speaks for itself and is not recommended.

During the audit, the auditor should use the following script to check the status of SELinux or use the system-config-selinux, getenforce or sestatus commands:

```
ENABLED=`cat /selinux/enforce`
if [ "$ENABLED" == 1 ]; then
  echo "SELinux is enabled, disable? (yes/no):"
  read disable
  if [ $disable == "yes" ]; then
    echo "disabling selinux"
setenforce 0
fi
fi
```

### AUDITING THE IPV6 STATUS

During the audit, the auditor should check the activation and use of IPv6 in the system. If no one is using IPv6, it should be disabled in the system, because any unused service creates vulnerabilities for the system. During an audit, the auditor should check and confirm this. To do so, the auditor goes to the network configuration file and adds the following lines to disable IPv6:

```
# vi /etc/sysconfig/network

NETWORKING_IPV6=no
IPV6INIT=no
```

### AUDITING EXISTING USER LISTS

The /etc/passwdfile stores users in Linux-based systems. To check existing users, the auditor should run the following script:

```
#!/bin/bash
# userslistinthesystem.sh

# count and Lists existing "real" users in the system.

echo
echo "[*] Existing users (sorted alphabetically):"
echo
grep '/bin/bash' /etc/passwd | grep -v 'root' | cut -f1
-d':' | sort
echo

echo -n "[*] Number of real users found: "
grep '/bin/bash' /etc/passwd | grep -v 'root' | wc -l
echo
```

### AUDITING USER ACTIVITIES IN THE SYSTEM

During the audit, the auditor should check that audited systems are configured with psacct or acct. Both are open source applications for monitoring users' activities in the system. Both psacct or acct applications run in the background and keep track of each user's activity on the system, as well as what resources are being consumed. The auditor can use the following script[4] to audit user activities in the system:[5]

```
#!/usr/bin/envksh
last -Fa|awk '
   /wtmp begins/ { next; }
   /still logged in/ { next; }
   $0 == reboot { next; }

   NF > 0  {
      if( NR > 1 )
printf( "\n" );

printf( "       User:\t%s\n", $1 );     # user
printf( "      Start:\t%s %s %s %s\n", $3, $4, $5, $6 );
      if( $9 == "down" )
printf( "        End:\tshutdown\n" );
      else
printf( "        End:\t%s %s %s %s\n", $9, $10, $11, $12 );

      if( substr( $NF, 1, 1 ) == "(" )
      {
         t = $NF;
         h = "localhost";
      }
      else
      {
         t = $(NF-1);
         h = $NF;
      }

gsub( "[()]", "", t );
printf( "    Time On:\t%s\n", t );
printf( "Remote Host:\t%s\n", h );
} '
```

Furthermore, during the audit, the auditor examines the documentation for the log retention policy of the organization to ensure compliance with the law and regulations of the organization and its regulatory body.

### AUDITING USERS' ABILITY TO USE OLD PASSWORDS

During the audit, it is important to check the configuration of password history in the system. It is recommended that administrators configure the system in a way so users are not able to revert to using old passwords when the password must be changed. The old password file is located at /etc/security/opasswd. This can be achieved through the following steps:[6]

- Open '/etc/pam.d/system-auth' file under RHEL:
  ```
  # vi /etc/pam.d/system-auth
  ```
- Open '/etc/pam.d/common-password' file under Ubuntu/Debian/Linux Mint:
  ```
  # vi /etc/pam.d/common-password
  ```
- Add the following line to 'auth' section:
  ```
  auth    sufficient    pam_unix.so likeauthnullok
  ```
- To disallow a user from reusing the last six passwords of his/hers, include the following line:
  ```
  Password    sufficient    pam_unix.so nullokuse_authtok md5
  shadow remember=6
  ```

After executing the command, the server stores the users' previous six passwords, so if any user tries to update his/her password using any of his/her last six passwords, he/she will get an error message.

### AUDITING THE STATUS OF USER PASSWORD EXPIRATION

During the audit, the auditor should check the configuration of the password expiration of users. In Linux systems, the /etc/shadow file stores users' passwords in an encrypted format. To check a user's password expiration, one can use the change command. This command results in detailed information regarding the password expiration date, as well as the date of change of the last password. Based on these details, the system will decide when a user must change his/her password.

The following command can be used to view existing users' information regarding the age of a password:

```
#chage -l username
```

Changes to password-aging of any user can be made with the following command:

```
#chage -M 60 username
#chage -M 60 -m 7 -W 7 userName
```

**Parameters**

The following parameters are used to set the password age in the system:

- Parameter -M is used to set password maximum age in days.
- Parameter -m is used to set password minimum age in days.
- Parameter -W is used to set the number of warnings in days.

### AUDITING THE LOCK AND UNLOCK STATUS OF USER ACCOUNTS

During the audit, the auditor should check the list of locked and unlocked users. To examine this status, the following command can be used:

```
# passwd –s accountName
```

### AUDITING PASSWORD STRENGTH IN THE SYSTEM

During the audit, the auditor should check the configuration of password strength to mitigate the risk from dictionary or brute-force attacks. System administrators must use pluggable authentication modules (PAM) to ensure that users set strong passwords.

The auditor can open the following file with an editor:

```
# vi /etc/pam.d/system-auth
```

### AUDITING THE IPTABLES (FIREWALL) STATUS

During the audit, the auditor can check the configuration of the Linux firewall to prevent unauthorized access of the audited servers. To control the traffic, rules can be applied in iptables, which will filter incoming, outgoing and forwarding packets. Iptables can also allow and deny specific User Datagram Protocol/Transmission Control Protocol (UDP/TCP) port numbers.

### AUDITING THE ACCOUNT FOR EMPTY PASSWORDS

During the audit, the auditor should check to identify any account having an empty password, which is prohibited and would allow anyone to access the system without entering a password. The auditor must check accounts for strong passwords and be certain that no one has any unauthorized access. Empty password accounts are a security risk and can be easily exploited by an attacker. Using the following command, one can determine the existence of accounts with empty passwords:

```
# cat /etc/shadow | awk -F: '($2==""){print $1}'
```

### AUDITING TIME STATISTICS OF USERS

Since organizations have a large number of users, they need to monitor the activities of users in the system, and, to do so, the auditor needs to ensure that the ac command is enabled in the system to review the activities of the users:

```
# ac
```

The command "ac -d" prints out the total login time in hours and by day:

```
# ac -d
```

The command to get the total login statistics time of user "isas" in hours is:

```
# ac isas
```

### AUDITING THE LOG REVIEW STATUS

During the audit, check the logs and the frequency of the log review should also checked. As per the sensitivity of the data or based on business impact analysis (BIA), it is recommended that logs move in a dedicated log server. This may prevent intruders from easily modifying local logs. The common Linux default log file names and their usage, /var/log/message, include:[7]

1. /var/log/auth.log – Authentication logs.
2. /var/log/kern.log – Kernel logs.
3. /var/log/cron.log – Crond logs (cron job).
4. /var/log/maillog – Mail server logs.
5. /var/log/boot.log – System boot log.
6. /var/log/mysqld.log – MySQL database server log file.

7. /var/log/secure – Authentication log.
8. /var/log/utmp or /var/log/wtmp : Login records file.
9. /var/log/yum.log: Yum log files

### AUDITING THE /BOOT DIRECTORY

During the audit, the auditor should check the status of the /boot directory. In Linux, kernel and its related files are placed in the /boot directory and auditors need to ensure that this folder is configured as read-only, which prevents unauthorized modification of the critical files in the Linux system. To ensure this configuration, the /etc/fstab file should be opened and the configuration checked:

```
# vi /etc/fstab
```

Then, the auditor should add the following line at the bottom, and save and close the file:

```
LABEL=/boot     /boot     ext2     defaults,ro     1 2
```

### AUDITING INTERNET CONTROL MESSAGE PROTOCOL OR BROADCAST REQUEST

During the audit, the auditor should check that systems are configured in a way that ensures that the system ignores ping or broadcast requests, because excessive ping requests or broadcast echo replies slowdown the network and furthermore attackers may generate the denial-of-service (DoS)/distributed denial-of-service (DDoS) attack using the ICMP echo. To deny the ping or broadcast request, the following line should be added in the "/etc/sysctl.conf" file:[8]

```
Ignore ICMP request:
net.ipv4.icmp_echo_ignore_all = 1

Ignore Broadcast request:
net.ipv4.icmp_echo_ignore_broadcasts = 1
```

New settings can be loaded by running following command:

```
#sysctl–p
```

### AUDITING THE CONFIGURATION OF THE NTP SERVER

During the audit, it is important to check the status of the Network Time Protocol (NTP) because NTP is a client-server protocol and it uses the UDP 123. Time is critical in networked systems, and the system needs to identify and track each transaction and activity of users centrally to make them accountable for their activities with the data/information of the organization. To achieve this, the auditor must examine the enablement of NTP in the server and its configuration status. To check if NTP is configured to run at system start, the following command can be issued:

```
~]$ chkconfig --list ntpd
```

By default, when NTP is installed, it is configured to start at every system start.

To check if NTP is running, the following command can be issued:

```
~]$ ntpq -p
```

To obtain a brief status report from NTP, the following command can be issued:

```
~]$ ntpstat
```

### VERIFY THE EXISTING STATUS OF NTP SERVER

The auditor should use the exit status of the NTP server to verify its operations:[9]

- Exit status 0 shows that the clock is synchronized.
- Exit status 1 shows that the clock is not synchronized.
- Exit status 2 shows that the clock state is indeterminant, e.g., if NTP cannot be contacted.

### CONCLUSION

Assurance and auditing are the obligatory activities to secure the information of any organization. Auditing must be a continuous and ongoing process, no matter what system or provider is being used. The audit and assurance program needs to examine the system configuration and the status of information security on a periodic basis to avoid cyberattack. Because the operating system is a penetrating component in business, it is important to make sure that it is configured properly to ensure the security of business information.

A comprehensive, all-encompassing auditing solution that can easily accomplish each of the following at the operating system level must be implemented:

- Access and authentication auditing
- User and administrator auditing

- Suspicious activity auditing
- Vulnerability and threat auditing
- Change auditing

Without a sweeping auditing solution, organizations put critical information at risk. Corrupt, inaccurate or compromised data equal lost revenue, lost time, and compromised customer and employee relationships.

**ENDNOTES**

[1] Akamaras blog, *www.akamaras.com*
[2] Krumins, P.: *catonmat.com*
[3] Saive, R.; "25 Hardening Security Tips for Linux Servers," Techmint.com, 24 June 2013, *http://www.tecmint.com/linux-server-hardening-security-tips/*
[4] SK, "Monitoring Users Activity Using psacct or acct Tools in Linus," Unixmen, 11 May 2013, *www.unixmen.com/monitoring-users-activitiy-using-psacct-or-acct-tools-in-linux*
[5] Argoat.net, *http://argoat.net/Blog/?paged=20*
[6] *Op cit*, Saive
[7] *Ibid*.
[8] *Ibid*.
[9] Gile, Vivek; "How to: Verify My NTP Working or Not," nixCraft, 25 March 2010, *www.cyberciti.biz/faq/linus-unix-bsd-is-ntp-client-working.com*