Auditing Linux

Prepared by: Krishni Naidu

References

The Process of hardening Linux, Chris Koutras, January 2001
Understanding the attackers toolkit, Sunnie Hawkins, January 2001
LIDS – Deploying enhanced kernel security in Linux, Thayne Allen, February 2001

Introduction

This checklist is to be used to audit a Linux environment. This checklist attempts to provide a generic set of controls to consider when auditing a Linux environment. It does not account for the differences between the different Linux distributions on the market e.g. Red Hat, Caldera, Mandrake, etc.

A listing of how to audit technical security controls is provided and no consideration is given to other control elements like physical access, security policy, etc. The omission of other controls does not mean that they lack importance. They are of equal importance however, they are deemed to be outside the scope of this checklist.

Some of the elements to consider prior to using the this checklist:

- Utilities: While every attempt has been made to include the security implications of using various utilities, it is not possible to list all of them and their security implications in this checklist. Thus, the auditor should ascertain what utilities are being used on the intended Linux server to be reviewed and determine their security implications. A good source to ascertain security implications of using certain utilities is to review the website of the vendor supplying the utility (whether it be freeware/shareware/commercial products). Another source is the supporting documentation that accompanies the utilities.
- Practicality of the checklist: This checklist lists controls to be checked for a very secure configuration. These may not be appropriate for all Linux servers in an organisation due to the risk assigned to particular data and applications. Also, some of the controls may be cost prohibitive to implement and management may have during the accreditation process decided to accept the risk of not being totally secure. The cost may relate to monetary and non-monetary elements. Non-monetary elements include items such as response times and availability.
- Interoperability with other products: This checklist does not provide the security issues to be considered when another system performs certain operations e.g. Windows NT providing the network authentication service. However, it is quite important that the auditor take this into consideration as certain systems coupled with a Linux server may introduce new vulnerabilities e.g. Netware is unsecure when mounting file systems. Also, this may aid the auditor in tailoring the checklist to suit the organisations environment e.g. more focus on the Samba server/SMB and less attention to Linux authentication if NT provides the network authentication service.
- Mitigating controls: The auditor needs to be aware of other controls provided by applications or databases. It may be that a weakness identified in the operating system is mitigated by a strong control found in the application or the database e.g. weak access control for the Linux operating system may be mitigated by very granular access control for the application.
- Significance of findings: To produce a good report that will receive management attention the auditor needs to perform a mini risk analysis. The risk analysis would ascertain if the finding is so significant as to affect the

organisation adversely. The first step in the risk analysis is to determine how sensitive the data stored on the server is and how critical the server is in the business operations. The second step is to determine how the finding would affect the organisation's ability to maintain confidentiality, integrity and availability. Once this has been done, a report indicating the priority and the potential effect on the organisation if the weakness is not corrected timeously needs to be issued to management.

- Applications and Database interfaces with Linux: A further consideration is the security provided for application and database files by the Linux server. The auditor needs to ascertain what applications and databases are loaded on the Linux server and ascertain the appropriateness of the permissions assigned to these files. This would also apply to sensitive data files.

An important consideration prior to auditing a Linux server is to determine the Linux server's function in the organisation. This is paramount to determining how the checklist below may be tailored. Since it is outside the scope of this checklist to list the security considerations in all the different functional instances that a Linux server may be used eg. as a HTTP server; it is important for the auditor to determine the security elements to be considered for a function as well as the associated applications that may be run for a specific function e.g. running Apache on a HTTP server.

Checklist

No	Control
1.	Installation: Ensure that the software is downloaded from secure sites. Ascertain if the PGP or MD- 5 signatures are verified. Ensure that a process exists to ascertain the function of the server and thus to install only those packages which are of relevance to the function. Ensure that the partition sizes are based on the function of the server e.g. A news server requires sufficient space on the /var/spool/news partition. Ensure that the partition scheme is documented to allow recovery later.
2.	Ensure that there is a process to update the system with the latest patches. If the patches are downloaded ensure that they are downloaded from secure sites. Ensure that the patches are tested in a test environment prior to being rolled out to the live environment. If RPM is being used to automatically download the related packages, ensure that the sites listed in /etc/autorpm.d/pools/redhat-updates are secure, trusted sites.
3.	Ensure that SSH is in use. Ensure that during the installation of SSH, the SSH daemon has been configured to support TCP Wrappers and disable support for rsh as a fallback option. Ensure that the SSH daemon is started at boot time by reviewing the /etc/rc.d/rc.local file for the following entry: • /usr/local/sbin/sshd. Ensure that the /etc/hosts.allow file is set up for SSh access. Ensure that the .ssh/identity file has 600 permissions and is owned by root. Ensure that the r programs are commented out of /etc/inetd.conf and have been removed.

No	Control
4.	Ensure that the inetd.conf file has been secured with the removal of unnecessary services. This is dependant on the function of the Linux server in the environment. The following should be commented out: • ftp • tftp ftp • tftp • systat • rexd • ypupdated • netstat • rstatd • rusersd • sprayd • walld • exec • talk • comsat • rquotad • name • uucp • sadmind • login • finger • chargen • echo • time • daytime • discard • sadmind • login • finger • chargen • echo • time • daytime • discard Ensure that the r programs have been commented out from the inetd.conf file due to the numerous vulnerabilities in these programs. Ensure that there are no /etc/hosts.equiv file and that no user account has a .rhosts file in its home directory.
5.	Ensure that Tripwire is in use. Ensure that one copy of the Tripwire database is copied onto a write protected floppy or CD. Ascertain how often a Tripwire compare is done. Determine what corrective actions are taken if there are variances i.e. changed files. Ensure that Tripwire sends alerts to the appropriate system administrator if a modification has occurred. If selective monitoring is enabled ascertain that the files being monitored are those that maintain sensitive information.
6.	Vulnerability scans Ascertain how often vulnerability scans are run and what corrective action is taken if security weaknesses are detected. If using Tiger, review /usr/local/tiger/systems/Linux/2 to ascertain whether the base information used for comparison is plausible. If using TARA, review the tigerrc file to ensure that suitable system checks are enabled. Other tools that can be used for vulnerability scans are SATAN, SARA, SAINT. Ensure that the latest versions of these scanners are being used. Commercial products like ISS system scanner or internet scanner as well as Cybercop may be used as vulnerability scanners.
7.	Ensure that Shadow passwords with MD5 hashing are enabled.
8.	Ensure that a boot disk has been created to recover from emergencies. Ensure that appropriate baselines are created for directory structures, file permissions, filenames and sizes. These files should be stored on CD’s.
9.	Review the /etc/lilo.conf file to ensure that the LILO prompt has been password protected and that permissions have been changed to 600.

No	Control
10.	Logging Review the /etc/syslog.comf file to ascertain if warnings and errors on all facilities are being logged and that all priorities on the kernel facility is being logged. Ensure that the permissions on the syslog files are 700. Review the /etc/logrotate.conf file to ascertain if the logs are rotated in compliance with security policy. Review the crontab file to ascertain if the logrotate is scheduled daily. If remote logging is enabled ensure that the correct host is included in the /etc/syslog.conf file and that the system clock is synchronised with the logserver. To check the synchronisation of the system clock review the /etc/cron.hourly/set-ntp file and ensure that the hardware clock CMOS value is set to the current system time. Ensure that the log entries are reviewed regularly either manually or using tools like Swatch or Logcheck. If Swatch is used, review the /urs/doc/swatch-2.2/config_files/swatchrc.personal control file to ensure that all different log files are being monitored (mail logs, samba logs, etc) and that the expressions to ignore are plausible. If using Logcheck, review the logcheck.ignore files to ensure that the patterns to ignore are plausible.
11.	Review /etc/inittab file to ascertain if: • Rebooting from the console with Ctrl+Alt+Del key sequence is disabled • Root password is required to enter single user mode
12.	Review the /etc/ftpusers file to ensure that root and system accounts are included.
13.	Review the /etc/security/access.conf file to ensure that all console logins except for root and administrator are disabled.
14.	TCP Wrappers Ensure that the default access rule is set to deny all in the /etc/hosts.allow file. Determine if a procedure exists to run tcpdchk after rule changes. Run tcpdchk to ensure that the syntax of /etc/inetd.conf file are consistent and that there are no errors. Review the /etc/banners file to ensure that the appropriate legal notice has been included in the banner. Review the /etc/hosts.allow file to ensure that the banners have been activated.
15.	Startup/shutdown scripts Ascertain if there is a process to ascertain which process is listening on which port (either lsof or nertstat command) and whether any unnecessary services are eliminated. Review the /etc/rc.d/init.d file to ensure that only the necessary services based on the function of the server are being run. The services to be stopped are as follows (this is dependant on the server function): • automounter /etc/rc2.d/S74autofs • Sendmail /etc/rc2.d/S88sendmail and /etc/rc1.d/K57sendamil • RPC /etc/rc2.d/ S71rpc • SNMP /etc/rc2.d/S76snmpdx • NFS server /etc/rc3.d/S15nfs.server • NFS client /etc/rc2/S73nfs.client

No	Control
16.	Domain Name Service For the master server ensure that zone transfers are restricted by reviewing the /etc/named.conf file. The IP address of the masters should appear next to the allow-transfer option. For slave/secondary servers ensure that the no zone information is transferred to any other server – review the /etc/named.conf file for the slaves. None should appear next to the allow-transfer option. Ensure that named is run in chroot jail. Ensure that syslogd is set to listen to named logging by reviewing the /etc/rc.d/init.d/syslog to ensure that the line referring to the syslog daemon has been edited to read as follows: • daemon syslog –a /home/dns/dev/log.
17.	E-Mail Ensure that the SMTP vrfy and expn have been turned off by reviewing the /etc/sendmail.cf file. (PrivacyOptions = goaway). Review the /etc/mail/access file to ensure that it includes only the fully qualified hostname, subdomain, domain or network names/addresses that are authorised to relay mail. Ensure that domain name masquerading has been set by reviewing the /etc/sendmail.cf file. The masquerade name should be appended to the DM line. Ensure that the latest patches of POP/IMAP are installed on the mail server. Review the /etc/hosts.allow file to ensure that mail is only delivered to the authorised network and domain. The network and domain name should appear after the ipop3d and imapd lines. Ensure that SSL wrapper has been installed for secure POP/IMAP connections.
18.	Printing Services Review the /etc/hosts.lpd file to ensure that only authorised hosts are allowed to use the print server. If LPRng is used, review the /etc/lpd.perms file to ensure that only authorised hosts or networks are allowed access to the print server and to perform specific operations.
19.	NFS Ensure that only authorised hosts are allowed access to RPC services by reviewing the /etc/hosts.allow file for entries after portmap. Review the /etc/exports file and ascertain that directories are only exported to authorised hosts with read only option.
20.	Server Message Block SMB/SAMBA server Ensure that the latest version of SAMBA is being run. Review the /etc/smb.conf file to ensure that only authorised hosts are allowed SAMBA server access. Ensure that encrypted passwords are used. Ensure that the permissions on the /etc/smbpasswd file is 600. Review the /etc/smbpasswd file to ensure that system accounts have been removed (bin, daemon, ftp). Review the /etc/smb.conf file to ensure that unnecessary shares are disabled. Review the /etc/smb.conf file to ensure that write permissions have been restricted to authorised users. Review the /etc/smb.conf file to ensure that the files are not created world readable. The create mask should have a permission bit of 770 and the directory mask should have a permission bit of 750.
21.	Review the /etc/securetty file to ensure that remote users are not included i.e. the file only contains tty1 to tty8, inclusive.

No	Control
22.	FTP Review /home/ftp, to ensure that the bin, etc and pub directories are owned by root. Review the /etc/hosts.allow file to ensure that only authorised hosts are allowed access to the ftp server. Authorised hosts and networks should be found after the in.ftpd. Review the /etc/ftpaccess file to ensure that anonymous users are prevented from modifying writable directories. The entries should be as follows: • chmod no guest,anonymous • delete no guest,anonymous • overwrite no guest,anonymous • rename no guest,anonymous Review the /etc/ftpaccess file to ensure that files uploaded to the incoming directory has root as owner and the user is not allowed to create subdirectories. Ensure that downloads are denied from the incoming directory. The lines should read as follows: • upload /home/ftp /incoming yes root nodirs • noretrieve /home/ftp/incoming/ Ensure that the incoming directory is reviewed daily and the files moved out of the anonymous directory tree.
23.	Intrusion Detection Ensure that PortSentry is in use. Review the portsentry.conf file and ensure that the KILL_ROUTE option is configured to either: • add an entry to in the routing table to send responses to the attacking host to a fictitious destination • add firewall filter rules to drop all packets from the attacking host. Ensure that LIDS (Linux Intrusion Detection/Defense System) is in use. Review lidsadm to ascertain what directories are being protected and the other security options that are enabled.
24.	Ensure PAM is enabled.
25.	HTTP Server Ensure that the basic access is set to default deny by reviewing access.conf. The options should be set as follows: • <Directory /> • Options None • AllowOverride None • Order deny,allow • Deny from all • </ Directory> Ensure that further entries to access.conf only allow access and specific options to authorised hosts based on their function. Ensure that directories don't have any of the following options set: • ExecCGI • FollowSymlINKS • Includes • Indexes Ensure that password protection is used for sensitive data. However, the auditor must be aware that this security control is inadequate on it's own since the userid and password are passed over the network in the clear. Ensure that SSL is used for secure HTTP communications.