Basic Linux Hardening Checklist

DRAFT VERSION

07-JUL-2019

Hardening refers to providing various means of protection in a computer system. Protection is provided in various layers and is often referred to as defense in depth. Protecting in layers means to protect at the host level, the application level, the operating system level, the user level, the physical level and all the sublevels in between. Each level requires a unique method of security. A hardened computer system is a more secure computer system. Techopedia explains that Hardening's goal is to eliminate as many risks and threats to a computer system as necessary.

The following table lists the basic hardening requirements for a Linux system. Care should be taken to ensure that proper testing of the controls is done before deploying in production system(s).

ID	**UBU-0001**
Title	The system must require authentication upon booting into single-user and maintenance modes.
Description	If the system does not require valid root authentication before it boots into single-user or maintenance mode, anyone who invokes single-user or maintenance mode is granted privileged access to all files on the system.
Check(s)	Check if the system requires a password for entering single-user mode.# grep ':S:' /etc/inittabIf /sbin/sulogin is not listed, this is a finding.
ID	**UBU-0002**
Title	The root accounts executable search path must be the vendor default and must contain only absolute paths.
Description	The executable search path (typically the PATH environment variable) contains a list of directories for the shell to search to find executables. If this path includes the current working directory or other relative paths, executables in these directories may be executed instead of system commands. This variable is formatted as a colon-separated list of directories. If there is an empty entry, such as a leading or trailing colon or two consecutive colons, this is interpreted as the current working directory. Entries starting with a slash (/) are absolute paths.
Check(s)	To view the root user's PATH, log in as the root user, and execute:# env | grep PATHThis variable is formatted as a colon-separated list of directories. If there is an empty entry, such as a leading or trailing colon, or two consecutive colons, this is a finding. If an entry starts with a character other than a slash (/), this is a finding. If directories beyond those in the vendor's default root path are present. This is a finding.
ID	**UBU-0003**
Title	All skeleton files (typically those in /etc/skel) must have mode 0644 or less permissive.
Description	If the skeleton files are not protected, unauthorized personnel could change user startup parameters and possibly jeopardize user files.
Check(s)	Check skeleton files permissions.# ls -alL /etc/skelIf a skeleton file has a mode more permissive than 0644, this is a finding.
ID	**UBU-0004**
Title	NIS/NIS+/yp files must be owned by root, sys, or bin.

Description	NIS/NIS+/yp files are part of the system's identification and authentication processes and are critical to system security. Failure to give ownership of sensitive files or utilities to root or bin provides the designated owner and unauthorized users with the potential to access sensitive information or change the system configuration which could weaken the system's security posture.
Check(s)	Perform the following to check NIS file ownership:# ls -la /var/yp/*;If the file ownership is not root, sys, or bin, this is a finding.
ID	**UBU-0005**
Title	NIS/NIS+/yp files must be group-owned by root, sys, or bin.
Description	NIS/NIS+/yp files are part of the system's identification and authentication processes and are, therefore, critical to system security. Failure to give ownership of sensitive files or utilities to root or bin provides the designated owner and unauthorized users with the potential to access sensitive information or change the system configuration which could weaken the system's security posture.
Check(s)	Perform the following to check NIS file group ownership:# ls -la /var/yp/*If the file group ownership is not root, sys, or bin, this is a finding.
ID	**UBU-0006**
Title	Library files must have mode 0755 or less permissive.
Description	Unauthorized access could destroy the integrity of the library files.
Check(s)	Check the mode of library files.Procedure:# DIRS='/usr/lib /lib';for DIR in $DIRS;do find $DIR -type f -perm +022 -exec stat -c %a:%n {} \;;doneThis will return the octal permissions and name of all group or world writable files.If any file listed is world or group writable (either or both of the 2 lowest order digits contain a 2, 3 or 6), this is a finding.
ID	**UBU-0007**
Title	All system command files must have mode 0755 or less permissive.
Description	Restricting permissions will protect system command files from unauthorized modification. System command files include files present in directories used by the operating system for storing default system executables and files present in directories included in the system's default executable search paths.
Check(s)	Check the permissions for files in /etc, /bin, /usr/bin, /usr/lbin, /usr/usb, /sbin, and /usr/sbin. Procedure:# DIRS='/etc /bin /usr/bin /usr/lbin /usr/usb /sbin /usr/sbin';for DIR in $DIRS;do find $DIR -type f -perm +022 -exec stat -c %a:%n {} \;;doneThis will return the octal permissions and name of all group or world writable files. If any file listed is world or group writable (either or both of the 2 lowest order digits contain a 2, 3 or 6), this is a finding.Note: Elevate to Severity Code I if any file listed is world-writable.
ID	**UBU-0008**
Title	The /etc/shadow (or equivalent) file must be owned by root.
Description	The /etc/shadow file contains the list of local system accounts. It is vital to system security and must be protected from unauthorized modification. Failure to give ownership of sensitive files or utilities to root or bin provides the designated owner and unauthorized users with the potential to access sensitive information or change the system configuration which could weaken the system's security posture.

Check(s)	Check the ownership of the /etc/shadow file.# ls -lL /etc/shadowIf the /etc/shadow file is not owned by root, this is a finding.
ID	**UBU-0009**
Title	The /etc/passwd file must have mode 0644 or less permissive.
Description	If the passwd file is writable by a group-owner or the world, the risk of passwd file compromise is increased. The passwd file contains the list of accounts on the system and associated information.
Check(s)	Check the mode of the /etc/passwd file.Procedure:# ls -lL /etc/passwdIf /etc/passwd has a mode more permissive than 0644, this is a finding.
ID	**UBU-0010**
Title	The /etc/shadow (or equivalent) file must have mode 0400.
Description	The /etc/shadow file contains the list of local system accounts. It is vital to system security and must be protected from unauthorized modification. The file also contains password hashes which must not be accessible to users other than root.
Check(s)	Check the mode of the /etc/shadow file.# ls -lL /etc/shadowIf the /etc/shadow file has a mode more permissive than 0400, this is a finding.
ID	**UBU-0011**
Title	The system and user default umask must be 077.
Description	The umask controls the default access mode assigned to newly created files. An umask of 077 limits new files to mode 700 or less permissive. Although umask can be represented as a 4-digit number, the first digit representing special access modes is typically ignored or required to be 0. This requirement applies to the globally configured system defaults and the user defaults for each account on the system.
Check(s)	NOTE: The following commands must be run in the BASH shell.Check global initialization files for the configured umask value.Procedure:# grep umask /etc/* Check local initialization files for the configured umask value.Procedure: # cut -d: -f6 /etc/passwd |xargs -n1 -IDIR find DIR -name '.*' -type f -maxdepth 1 -exec grep umask {} \;If the system and user default umask is not 077, this a finding. Note: If the default umask is 000 or allows for the creation of world-writable files this becomes a Severity Code I finding.
ID	**UBU-0012**
Title	Auditing must be implemented.
Description	Without auditing, individual system accesses cannot be tracked and malicious activity cannot be detected and traced back to an individual account.
Check(s)	Determine if auditing is enabled.# ps -ef |grep auditd If the auditd process is not found, this is a finding.
ID	**UBU-0013**
Title	System audit logs must be owned by root.
Description	Failure to give ownership of system audit log files to root provides the designated owner and unauthorized users with the potential to access sensitive information.
Check(s)	Perform the following to determine the location of audit logs and then check the ownership.Procedure:# grep '^log_file' /etc/audit/auditd.conf|sed s/^[^\/]*//|xargs stat -c %U:%nIf any audit log file is not owned by root, this is a finding.
ID	**UBU-0014**

Title	System audit logs must have mode 0640 or less permissive.
Description	If a user can write to the audit logs, audit trails can be modified or destroyed and system intrusion may not be detected. System audit logs are those files generated from the audit system and do not include activity, error, or other log files created by application software.
Check(s)	Perform the following to determine the location of audit logs and then check the mode of the files.Procedure:# grep '^log_file' /etc/audit/auditd.conf|sed s/^[^\/]*//|xargs stat -c %a:%nIf any audit log file has a mode more permissive than 0640, this is a finding.
ID	**UBU-0015**
Title	The inetd.conf file, xinetd.conf file, and the xinetd.d directory must be owned by root or bin.
Description	Failure to give ownership of sensitive files or utilities to root provides the designated owner and unauthorized users with the potential to access sensitive information or change the system configuration possibly weakening the system's security posture.
Check(s)	Check the owner of the xinetd configuration files.Procedure:# ls -lL /etc/xinetd.conf # ls -laL /etc/xinetd.dThis is a finding if any of the above files or directories are not owned by root or bin.
ID	**UBU-0016**
Title	The services file must be owned by root or bin.
Description	Failure to give ownership of sensitive files or utilities to root or bin provides the designated owner and unauthorized users with the potential to access sensitive information or change the system configuration possibly weakening the system's security posture.
Check(s)	Check the ownership of the services file.Procedure:# ls -lL /etc/servicesIf the services file is not owned by root or bin, this is a finding.
ID	**UBU-0017**
Title	The ftpusers file must exist.
Description	The ftpusers file contains a list of accounts not allowed to use FTP to transfer files. If this file does not exist, then unauthorized accounts can utilize FTP.
Check(s)	Check for the existence of the ftpusers file.Procedure:For gssftp:# ls -l /etc/ftpusersFor vsftp:# ls -l /etc/vsftpd.ftpusersor# ls -l /etc/vsftpd/ftpusersIf the appropriate ftpusers file for the running FTP service does not exist, this is a finding.
ID	**UBU-0018**
Title	The Network Information System (NIS) protocol must not be used.
Description	Due to numerous security vulnerabilities existing within NIS, it must not be used. Possible alternative directory services are NIS+ and LDAP.
Check(s)	Perform the following to determine if NIS is active on the system:# ps -ef | grep ypbindIf NIS is found active on the system, this is a finding.
ID	**UBU-0019**
Title	The nosuid option must be enabled on all Network File System (NFS) client mounts.

Description	Enabling the nosuid mount option prevents the system from granting owner or group-owner privileges to programs with the suid or sgid bit set. If the system does not restrict this access, users with unprivileged access to the local system may be able to acquire privileged access by executing suid or sgid files located on the mounted NFS file system.
Check(s)	Check the system for NFS mounts not using the 'nosuid' option.Procedure:# mount -v | grep ' type nfs ' | egrep -v 'nosuid'If the mounted file systems do not have the 'nosuid' option, this is a finding.
ID	**UBU-0020**
Title	Access to the cron utility must be controlled using the cron.allow and/or cron.deny file(s).
Description	The cron facility allows users to execute recurring jobs on a regular and unattended basis. The cron.allow file designates accounts allowed to enter and execute jobs using the cron facility. If neither cron.allow nor cron.deny exists, then any account may use the cron facility. This may open the facility up for abuse by system intruders and malicious users.
Check(s)	Check for the existence of the cron.allow and cron.deny files.# ls -lL /etc/cron.allow# ls -lL /etc/cron.denyIf neither file exists, this is a finding.
ID	**UBU-0021**
Title	The cron.allow file must have mode 0600 or less permissive.
Description	A readable and/or writable cron.allow file by users other than root could allow potential intruders and malicious users to use the file contents to help discern information, such as who is allowed to execute cron programs, which could be harmful to overall system and network security.
Check(s)	Check mode of the cron.allow file.Procedure:# ls -lL /etc/cron.allowIf the file has a mode more permissive than 0600, this is a finding.
ID	**UBU-0022**
Title	Cron and crontab directories must be owned by root or bin.
Description	Incorrect ownership of the cron or crontab directories could permit unauthorized users the ability to alter cron jobs and run automated jobs as privileged users. Failure to give ownership of cron or crontab directories to root or to bin provides the designated owner and unauthorized users with the potential to access sensitive information or change the system configuration which could weaken the system's security posture.
Check(s)	Check the owner of the crontab directories.Procedure:# ls -ld /var/spool/cron# ls -ld /etc/cron.d /etc/crontab /etc/cron.daily /etc/cron.hourly /etc/cron.monthly /etc/cron.weeklyor # ls -ld /etc/cron*|grep -v denyIf the owner of any of the crontab directories is not root or bin, this is a finding.
ID	**UBU-0023**
Title	Cron and crontab directories must be group-owned by root, sys, bin or cron.
Description	To protect the integrity of scheduled system jobs and to prevent malicious modification to these jobs, crontab files must be secured. Failure to give group-ownership of cron or crontab directories to a system group provides the designated group and unauthorized users with the potential to access sensitive information or change the system configuration which could weaken the system's security posture.

Check(s)	Check the group owner of cron and crontab directories.Procedure:# ls -ld /var/spool/cron# ls -ld /etc/cron.d /etc/crontab /etc/cron.daily /etc/cron.hourly /etc/cron.monthly /etc/cron.weeklyor # ls -ld /etc/cron*|grep -v denyIf a directory is not group-owned by root, sys, bin, or cron, this is a finding.
ID	**UBU-0024**
Title	Access to the at utility must be controlled via the at.allow and/or at.deny file(s).
Description	The 'at' facility selectively allows users to execute jobs at deferred times. It is usually used for one-time jobs. The at.allow file selectively allows access to the 'at' facility. If there is no at.allow file, there is no ready documentation of who is allowed to submit 'at' jobs.
Check(s)	If the 'at' package is not installed, this is not applicable.Check for the existence of at.allow and at.deny files.# ls -lL /etc/at.allow# ls -lL /etc/at.denyIf neither file exists, this is a finding.
ID	**UBU-0025**
Title	The snmpd.conf file must have mode 0600 or less permissive.
Description	The snmpd.conf file contains authenticators and must be protected from unauthorized access and modification.
Check(s)	Check the mode of the SNMP daemon configuration file.Procedure:Examine the default install location /etc/snmp/snmpd.confor:# find / -name snmpd.conf# ls -lL <snmpd.conf file>If the snmpd.conf file has a mode more permissive than 0600, this is a finding.
ID	**UBU-0026**
Title	The Samba Web Administration Tool (SWAT) must be restricted to the local host or require SSL.
Description	SWAT is a tool used to configure Samba. It modifies Samba configuration, which can impact system security, and must be protected from unauthorized access. SWAT authentication may involve the root password, which must be protected by encryption when traversing the network.Restricting access to the local host allows for the use of SSH TCP forwarding, if configured, or administration by a web browser on the local system.
Check(s)	SWAT is a tool for configuring Samba and should only be found on a system with a requirement for Samba. If SWAT is used, it must be utilized with SSL to ensure a secure connection between the client and the server.Procedure:# grep -H 'bin/swat' /etc/xinetd.d/*|cut -d: -f1 |xargs grep 'only_from'If the value of the 'only_from' line in the 'xinetd.d' file which starts '/usr/sbin/swat' is not 'localhost' or the equivalent, this is a finding.
ID	**UBU-0027**
Title	The system must not have special privilege accounts, such as shutdown and halt.
Description	If special privilege accounts are compromised, the accounts could provide privileges to execute malicious commands on a system.
Check(s)	Perform the following to check for unnecessary privileged accounts:# grep '^shutdown' /etc/passwd# grep '^halt' /etc/passwd# grep '^reboot' /etc/passwdIf any unnecessary privileged accounts exist this is a finding.
ID	**UBU-0028**
Title	The SSH daemon must be configured to only use the SSHv2 protocol.

Description	SSHv1 is not a DoD-approved protocol and has many well-known vulnerability exploits. Exploits of the SSH daemon could provide immediate root access to the system.
Check(s)	Locate the sshd_config file: # more /etc/ssh/sshd_configExamine the file. If the variables 'Protocol 2,1' or 'Protocol 1' are defined on a line without a leading comment, this is a finding.If the SSH server is F-Secure, the variable name for SSH 1 compatibility is 'Ssh1Compatibility', not 'protocol'. If the variable 'Ssh1Compatiblity' is set to 'yes', then this is a finding.
ID	**UBU-0029**
Title	The system must not run Samba unless needed.
Description	Samba is a tool used for the sharing of files and printers between Windows and UNIX operating systems. It provides access to sensitive files and, therefore, poses a security risk if compromised.
Check(s)	Check the system for a running Samba server.Procedure:# ps -ef |grep smbdIf the Samba server is running, ask the SA if the Samba server is operationally required. If it is not, this is a finding.
ID	**UBU-0030**
Title	The at directory must be owned by root, bin, sys, daemon, or cron.
Description	If the owner of the 'at' directory is not root, bin, or sys, unauthorized users could be allowed to view or edit files containing sensitive information within the directory.
Check(s)	Check the ownership of the 'at' directory:Procedure:# ls -ld /var/spool/atIf the directory is not owned by root, sys, bin, daemon, or cron, this is a finding.
ID	**UBU-0031**
Title	The at.allow file must be owned by root, bin, or sys.
Description	If the owner of the at.allow file is not set to root, bin, or sys, unauthorized users could be allowed to view or edit sensitive information contained within the file.
Check(s)	# ls -lL /etc/at.allowIf the at.allow file is not owned by root, sys, or bin, this is a finding.
Fix(s)	Change the owner of the at.allow file.# chown root /etc/at.allow
ID	UBU-0032
Title	The at.deny file must be owned by root, bin, or sys.
Description	If the owner of the at.deny file is not set to root, bin, or sys, unauthorized users could be allowed to view or edit sensitive information contained within the file.
Check(s)	# ls -lL /etc/at.denyIf the at.deny file is not owned by root, sys, or bin, this is a finding.
ID	**UBU-0033**
Title	The rexec daemon must not be running.
Description	The rexecd process provides a typically unencrypted, host-authenticated remote access service. SSH should be used in place of this service.
Check(s)	# grep disable /etc/xinetd.d/rexecIf the service file exists and is not disabled, this is a finding.
ID	**UBU-0034**
Title	The system must log successful and unsuccessful access to the root account.
Description	If successful and unsuccessful logins and logouts are not monitored or recorded, access attempts cannot be tracked. Without this logging, it may be impossible to track unauthorized access to the system.

Check(s)	Check the log files to determine if access to the root account is being logged.Procedure:Examine /etc/syslog.conf to confirm the location to which 'authpriv' messages will be directed. The default syslog.conf uses /var/log/messages and /var/log/secure but this needs to be confirmed.# grep @ /etc/syslog.confIf a line starting with '*.*' is returned then all syslog messages will be sent to system whose address appears after the '@'. In this case syslog may or may not be configured to also log 'authpriv' messages locally.# grep authpriv /etc/syslog.confIf any lines are returned which do not start with '#' the 'authpriv' messages will be sent to the indicated files or remote systems.Try to 'su -' and enter an incorrect password.If there are no records indicating the authentication failure, this is a finding.
ID	**UBU-0035**
Title	All skeleton files and directories (typically in /etc/skel) must be owned by root or bin.
Description	If the skeleton files are not protected, unauthorized personnel could change user startup parameters and possibly jeopardize user files. Failure to give ownership of sensitive files or utilities to root or bin provides the designated owner and unauthorized users with the potential to access sensitive information or change the system configuration which could weaken the system's security posture.
Check(s)	Check skeleton files ownership.# ls -alL /etc/skelIf a skeleton file is not owned by root or bin, this is a finding.
ID	**UBU-0036**
Title	The system must implement non-executable program stacks.
Description	A common type of exploit is the stack buffer overflow. An application receives, from an attacker, more data than it is prepared for and stores this information on its stack, writing beyond the space reserved for it. This can be designed to cause execution of the data written on the stack. One mechanism to mitigate this vulnerability is for the system to not allow the execution of instructions in sections of memory identified as part of the stack.
Check(s)	If the system being evaluated is running a Red Hat compatible operating system kernel, check that the 'kernel.exec-shield' kernel parameter is set to '1' in /etc/sysctl.conf. If the system is running an Oracle Unbreakable Enterprise kernel, verify that Oracle's Data Execution Prevention is enabled.First, determine if the system is operating an Oracle Unbreakable Enterprise Kernel (UEK):# uname -r | grep uekIf no value is returned, the system is running a Red Hat compatible kernel. Verify the 'kernel.exec-shield' kernel parameter is set to '1' in /etc/sysctl.conf:# grep ^kernel\.exec-shield /etc/sysctl.conf | awk -F= '{ print $2 }'kernel.exec-shield = 1If there is no value returned or if a value is returned that is not '2', this is a finding.If the system was found to be running an Unbreakable Enterprise Kernel, verify DEP is enabled:# dmesg | grep 'NX.*protection:If there is no value returned or if a value is returned that is not 'NX (Execute Disable) protection: active', this is a finding.Note that this is not a finding when the underlying processor architecture does not support the 'Execute Disable' (NX) capability. To determine if the processor supports this capability, run the command:# cat /proc/cpuinfo | grep flags | xargs -n 1 echo | grep -w 'nx' | sort -uIf a system's underlying processor supports this functionality, a single entry containing the keyword 'nx' will be returned.

ID	**UBU-0037**
Title	Unencrypted FTP must not be used on the system.
Description	FTP is typically unencrypted and presents confidentiality and integrity risks. FTP may be protected by encryption in certain cases, such as when used in a Kerberos environment. SFTP and FTPS are encrypted alternatives to FTP.
Check(s)	Perform the following to determine if unencrypted FTP is enabled:# chkconfig --list gssftp# chkconfig --list vsftpdIf any of these services are found, ask the SA if these services are encrypted. If they are not, this is a finding.
ID	UBU-0038
Title	All FTP users must have a default umask of 077.
Description	The umask controls the default access mode assigned to newly created files. An umask of 077 limits new files to mode 700 or less permissive. Although umask is stored as a 4-digit number, the first digit representing special access modes is typically ignored or required to be zero (0).
Check(s)	Check the umask setting for FTP users.Procedure:For gssftp:Assuming an anonymous ftp user has been defined with no user initialization script invoked to change the umask# ftp localhostName: (localhost:root): anonymousPassword: anythingftp>umaskIf the umask value returned is not 077, this is a finding.or:# grep 'server_args' /etc/xinetd.d/gssftpThe default umask for FTP is '023' if the server _args entry does not contain '-u 077' this is a finding.For vsftp:# grep '_mask' /etc/vsftpd/vsftpd.confThe default 'local_umask' setting is 077. If this has been changed, or the 'anon_umask' setting is not 077, this is a finding.
ID	**UBU-0039**
Title	X Window System connections not required must be disabled.
Description	If unauthorized clients are permitted access to the X server, a user's X session may be compromised.
Check(s)	Determine if the X window system is running.Procedure:# ps -ef |grep XorgAsk the SA if the X window system is an operational requirement. If it is not, this is a finding.
ID	**UBU-0040**
Title	The systems access control program must be configured to grant or deny system access to specific hosts.
Description	If the system's access control program is not configured with appropriate rules for allowing and denying access to system network resources, services may be accessible to unauthorized hosts.
Check(s)	Check for the existence of the '/etc/hosts.allow' and '/etc/hosts.deny' files.Procedure:# ls -la /etc/hosts.allow# ls -la /etc/hosts.denyIf either file does not exist, this is a finding.Check for the presence of a 'default deny' entry.Procedure:# grep 'ALL: ALL' /etc/hosts.denyIf the 'ALL: ALL' entry is not present the '/etc/hosts.deny' file, any TCP service from a host or network not matching other rules will be allowed access. If the entry is not in '/etc/hosts.deny', this is a finding.
ID	**UBU-0041**
Title	The /etc/securetty file must be group-owned by root, sys, or bin.
Description	The securetty file contains the list of terminals permitting direct root logins. It must be protected from unauthorized modification.

Check(s)	Check /etc/securetty group ownership:# ls -lL /etc/securettyIf /etc/securetty is not group owned by root, sys, or bin, then this is a finding.
ID	**UBU-0042**
Title	The /etc/securetty file must be owned by root.
Description	The securetty file contains the list of terminals permitting direct root logins. It must be protected from unauthorized modification.
Check(s)	Check /etc/securetty ownership.Procedure:# ls -lL /etc/securettyIf /etc/securetty is not owned by root, this is a finding.
ID	**UBU-0043**
Title	The system must use a FIPS 140-2 approved cryptographic hashing algorithm for generating account password hashes.
Description	Systems must employ cryptographic hashes for passwords using the SHA-2 family of algorithms or FIPS 140-2 approved successors. The use of unapproved algorithms may result in weak password hashes more vulnerable to compromise.
Check(s)	Verify the algorithm used for password hashing is of the SHA-2 family.# egrep 'password .* pam_unix.so' /etc/pam.d/system-auth-acIf the line indicates the hash algorithm is not set to sha256 or sha512, this is a finding.
ID	**UBU-0044**
Title	The at directory must be group-owned by root, bin, sys, or cron.
Description	If the group of the 'at' directory is not root, bin, sys, or cron, unauthorized users could be allowed to view or edit files containing sensitive information within the directory.
Check(s)	Check the group ownership of the file.Procedure:# ls -lL /var/spool/atIf the file is not group-owned by root, bin, sys, daemon or cron, this is a finding.
ID	**UBU-0045**
Title	Kernel core dumps must be disabled unless needed.
Description	Kernel core dumps may contain the full contents of system memory at the time of the crash. Kernel core dumps may consume a considerable amount of disk space and may result in Denial of Service by exhausting the available space on the target file system. The kernel core dump process may increase the amount of time a system is unavailable due to a crash. Kernel core dumps can be useful for kernel debugging.
Check(s)	Verify the kdump service is not running.Procedure:# service kdump statusIf 'Kdump is operational' is returned, this is a finding.
ID	**UBU-0046**
Title	The system must not respond to Internet Control Message Protocol v4 (ICMPv4) echoes sent to a broadcast address.
Description	Responding to broadcast (ICMP) echoes facilitates network mapping and provides a vector for amplification attacks.
Check(s)	Verify the system does not respond to ICMP ECHO_REQUESTs set to broadcast addresses.Procedure:# cat /proc/sys/net/ipv4/icmp_echo_ignore_broadcastsIf the result is not 1, this is a finding.
ID	**UBU-0047**
Title	The system must ignore IPv4 Internet Control Message Protocol (ICMP) redirect messages.

Description	ICMP redirect messages are used by routers to inform hosts that a more direct route exists for a particular destination. These messages modify the host's route table and are unauthenticated. An illicit ICMP redirect message could result in a man-in-the-middle attack.
Check(s)	Verify the system does not accept IPv4 ICMP redirect messages.# grep [01] /proc/sys/net/ipv4/conf/*/accept_redirects|egrep 'default|all'If all of the resulting lines do not end with '0', this is a finding.
ID	**UBU-0048**
Title	The system must not send IPv4 Internet Control Message Protocol (ICMP) redirects.
Description	ICMP redirect messages are used by routers to inform hosts that a more direct route exists for a particular destination. These messages contain information from the system's route table possibly revealing portions of the network topology.
Check(s)	Verify the system does not send IPv4 ICMP redirect messages.# grep [01] /proc/sys/net/ipv4/conf/*/send_redirects|egrep 'default|all'If all of the resulting lines do not end with '0', this is a finding.
ID	**UBU-0049**
Title	The system must be configured to use TCP syncookies when experiencing a TCP SYN flood.
Description	A TCP SYN flood attack can cause Denial of Service by filling a system's TCP connection table with connections in the SYN_RCVD state. Syncookies are a mechanism used to only track a connection when a subsequent ACK is received, verifying the initiator is attempting a valid connection and is not a flood source. This technique does not operate in a fully standards-compliant manner, but is only activated when a flood condition is detected, and allows defense of the system while continuing to service valid requests.
Check(s)	Verify the system configured to use TCP syncookies when experiencing a TCP SYN flood.# cat /proc/sys/net/ipv4/tcp_syncookiesIf the result is not '1', this is a finding.
ID	**UBU-0050**
Title	The inetd.conf file, xinetd.conf file, and the xinetd.d directory must be group-owned by root, bin, sys, or system.
Description	Failure to give ownership of sensitive files or utilities to system groups may provide unauthorized users with the potential to access sensitive information or change the system configuration possibly weakening the system's security posture.
Check(s)	Check the group ownership of the xinetd configuration files and directories.Procedure:# ls -alL /etc/xinetd.conf /etc/xinetd.dIf a file or directory is not group-owned by root, bin, sys, or system, this is a finding.
ID	**UBU-0051**
Title	The xinetd.d directory must have mode 0755 or less permissive.
Description	The Internet service daemon configuration files must be protected as malicious modification could cause Denial of Service or increase the attack surface of the system.
Check(s)	Check the permissions of the xinetd configuration directories.# ls -dlL /etc/xinetd.dIf the mode of the directory is more permissive than 0755, this is a finding.
ID	**UBU-0052**
Title	The portmap or rpcbind service must not be installed unless needed.

Description	The portmap and rpcbind services increase the attack surface of the system and should only be used when needed. The portmap or rpcbind services are used by a variety of services using Remote Procedure Calls (RPCs).
Check(s)	Check if the portmap package is installed.# rpm -qa | grep portmapIf a package is found, this is a finding.
ID	**UBU-0053**
Title	The rshd service must not be installed.
Description	The rshd process provides a typically unencrypted, host-authenticated remote access service. SSH should be used in place of this service.
Check(s)	Check if the rsh-server package is installed.Procedure:# rpm -qa | grep rsh-serverIf a package is found, this is a finding.
ID	**UBU-0054**
Title	The rlogind service must not be installed.
Description	The rlogind process provides a typically unencrypted, host-authenticated remote access service. SSH should be used in place of this service.
Check(s)	Check if the rsh-server package is installed.Procedure:# rpm -qa | grep rsh-serverIf a package is found, this is a finding.
ID	**UBU-0055**
Title	The rexecd service must not be installed.
Description	The rexecd process provides a typically unencrypted, host-authenticated remote access service. SSH should be used in place of this service.
Check(s)	Check if the rsh-server package is installed.Procedure:# rpm -qa | grep rsh-serverIf a package is found, this is a finding.
Fix(s)	Remove the rsh-server package.Procedure:# rpm -e rsh-server
ID	**UBU-0056**
Title	All Network File System (NFS) exported system files and system directories must be group-owned by root, bin, sys, or system.
Description	Failure to give group-ownership of sensitive files or directories to root provides the members of the owning group with the potential to access sensitive information or change system configuration which could weaken the system's security posture.
Check(s)	List the exports.# cat /etc/exportsFor each file system displayed, check the ownership.# ls -ldL <exported file system path>If the directory is not group-owned by root, bin, sys, or system, this is a finding.
ID	**UBU-0057**
Title	Samba must be configured to use an authentication mechanism other than share.
Description	Samba share authentication does not provide for individual user identification and must not be used.
Check(s)	Check the security mode of the Samba configuration.# grep -i security /etc/samba/smb.conf If the security mode is 'share', this is a finding.
ID	**UBU-0058**
Title	Samba must be configured to not allow guest access to shares.
Description	Guest access to shares permits anonymous access and is not permitted.

Check(s)	Check the access to shares for Samba.# grep -i 'guest ok' /etc/samba/smb.conf If the setting exists and is set to 'yes', this is a finding.
ID	**UBU-0059**
Title	The system must ignore IPv6 ICMP redirect messages.
Description	ICMP redirect messages are used by routers to inform hosts that a more direct route exists for a particular destination. These messages modify the host's route table and are unauthenticated. An illicit ICMP redirect message could result in a man-in-the-middle attack.
Check(s)	Verify the system is configured to ignore IPv6 ICMP redirect messages.# cat /proc/sys/net/ipv6/conf/all/accept_redirectsIf the /proc/sys/net/ipv6/conf/all/accept_redirects entry does not exist because of compliance with GEN007720, this is not a finding.If the returned value is not '0', this is a finding.
ID	**UBU-0060**
Title	System audit logs must be group-owned by root, bin, sys, or system.
Description	Sensitive system and user information could provide a malicious user with enough information to penetrate further into the system.
Check(s)	Check the group ownership of the audit logs.Procedure:# grep '^log_file' /etc/audit/auditd.conf|sed s/^[^\/]*//|xargs stat -c %G:%nIf any audit log file is not group-owned by root, bin, sys, or system, this is a finding.
ID	**UBU-0061**
Title	Mail relaying must be restricted.
Description	If unrestricted mail relaying is permitted, unauthorized senders could use this host as a mail relay for the purpose of sending SPAM or other unauthorized activity.
Check(s)	If the system uses sendmail examine the configuration files. Determine if sendmail only binds to loopback addresses by examining the 'DaemonPortOptions' configuration options.Procedure: # grep -i 'O DaemonPortOptions' /etc/mail/sendmail.cfIf there are uncommented DaemonPortOptions lines, and all such lines specify system loopback addresses, this is not a finding.Otherwise, determine if sendmail is configured to allow open relay operation.Procedure: # grep -i promiscuous_relay /etc/mail/sendmail.mcIf the promiscuous relay feature is enabled, this is a finding.If the system uses Postfix, locate the main.cf file.Procedure: # find / -name main.cfDetermine if Postfix only binds to loopback addresses by examining the 'inet_interfaces' line.Procedure: # grep inet_interfaces </path/to/main.cf>If 'inet_interfaces' is set to 'loopback-only' or contains only loopback addresses such as 127.0.0.1 and [::1], Postfix is not listening on external network interfaces, and this is not a finding.Otherwise, determine if Postfix is configured to restrict clients permitted to relay mail by examining the 'smtpd_client_restrictions' line.Procedure: # grep smtpd_client_restrictions </path/to/main.cf>If the 'smtpd_client_restrictions' line is missing, or does not contain 'reject', this is a finding. If the line contains 'permit' before 'reject', this is a finding.If the system is using other SMTP software, consult the software's documentation for procedures to verify mail relaying is restricted.
ID	**UBU-0062**
Title	The telnet daemon must not be running.

Description	The telnet daemon provides a typically unencrypted remote access service which does not provide for the confidentiality and integrity of user passwords or the remote session. If a privileged user were to log on using this service, the privileged user password could be compromised.
Check(s)	The telnet service included in the operating system is a part of krb5-workstation. There are two versions of telnetd server provided. The xinetd.d file ekrb5-telnet allows only connections authenticated through Kerberos. The xinetd.d krb5-telnet allows normal telnet connections as well as kerberized connections. Both are set to 'disable = yes' by default. Ensure that neither is running.Procedure:Check if telnetd is running:# ps -ef |grep telnetdIf the telnet daemon is running, this is a finding.Check if telnetd is enabled on startup:# chkconfig --list|grep telnetIf an entry with 'on' is found, this is a finding.