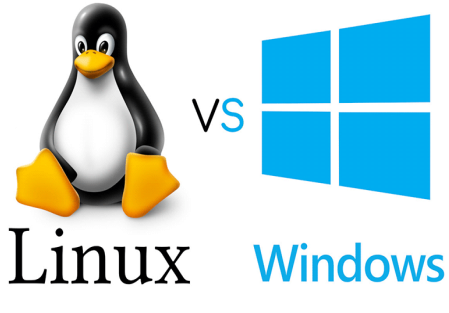
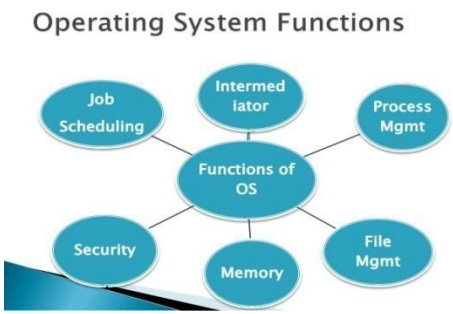
CIT210 OP. SYS. MANAG.

CSUN
COLLEGE OF ENGINEERING AND COMPUTER SCIENCE

Week13Day1 : OS Security - II: Linux Security, Boot Loader Security, User Account Policy, Using PAM, DNF vs Yum, Bastion Hardening, Isolate with chroot Jails





Securing Boot Loader (GRUB Configuration Options)

Configuration Options	Comments
default=0	This option is for default kernel to boot. When multiple kernels are listed, the first one in the list will start at zero.
timeout=0	This option sets the time out to zero.
color green/blue	This option specifies the color for the GRUB screen. In this case, green is the foreground color and blue is the background color.
password – md5 <encrypted password>	This option is for the encrypted password.
splashimage=(hd0,0)/grub/splash.xpm.gz	This option is for “splash” image that shows when you access the GRUB menu.

Kernel Space

- Kernel Space has access and can control all aspects of a Linux system.
- Loadable kernel modules (LKMs) are a common avenue for rootkits.

Importance of Securing Core Components

- Default settings, improper file permissions, and insecure user accounts are common methods used by black-hat hackers to gain unauthorized access.
- Best practices and compliance standards require basic security and can result in hefty fines, if not followed.

Managing Users and Groups

- One of the key administrative tasks with Linux is managing users and groups.
- The primary reason for user accounts is to verify the identity of each individual using a computer system.
- A secondary reason for user accounts is to permit the per-individual tailoring of resources and access privileges.
  - Resources can include
    - Files, directories, and devices.
    - Controlling access to these resources is a primary task of an administrator

Defining the User Account Policy

- Who needs access and why?
- How long does a user need access?
- Where will the user access the computer system from?
- What are the tasks the user needs to perform?

Determining Group Structure

- Some of the challenges facing system administrators when creating shared groups are:
  - What groups to create
  - Who to put in a given group
  - What type of permissions should these shared resources have

Determining Group Structure

- Each of the three permissions are assigned to three different categories of users.

The categories are:

- *owner* — The owner of the file or application.
- *group* — The group that owns the file or application.
- *everyone* — All users with access to the system.

Best Practices for Account Management

- Create a password policy in /etc/login.defs file.
- Lock user accounts that will not need access for a long period of time.
- Set account expiration for temporary accounts.
- Remove user and service accounts that are no longer being used.
- Monitor account usage and login attempts.

System, Service, and Regular User Accounts

System Account	Service Account	Regular Account
Created when the operating system is installed	Created automatically when installing a service using a package management program	Created by root or an account with privileged access
Users and groups < 100	Users and groups < 500	Users and groups > 500
Login directory typically set to /sbin/nologin or a system command, such as /sbin/shutdown	Login directory mostly set to /sbin/nologin but may also be set to a typical login shell, such as /bin/bash	Login directory set to /bin/bash

/etc/passwd

Several files are used when creating users in Linux. The following are a few most commonly used.

- /etc/passwd
- /etc/shadow
- /etc/group

TABLE 4-1 Data in `/etc/passwd`, by column.

COLUMN	DESCRIPTION
Username	Login name
Password	May be set to x or *. An x in a standard password column refers to `/etc/shadow` for the actual password. An * is shown if the account is disabled.
User ID	A numeric identifier for the user
Group ID	A numeric identifier for the primary group of the user
User information	Comments for the user; sometimes known as the GECOS field, based on its development as the General Electric Comprehensive Operating System
Home directory	The directory accessed when logging into the given account
Login shell	The start shell for the user

/etc/passwd

- **hdhillon:x:537:100:Harjit Dhillon:/home/hdhillon:/bin/bash**
- This line says:
  - account name is ‘hdhillon'
  - password is required ('x' represents the encrypted password)
  - numerical user ID is 537
  - default group is a group with group ID 100
  - the comments are ‘Harjit Dhillon'
  - the default home directory is '/home/hdhillon'
  - the default login shell is '/bin/bash'

/etc/passwd

Here is an another example of a /etc/passwd entry:

root:x:0:0:root:/root:/bin/bash

- This line shows that the root user has a shadow password, as well as a UID and GID of 0.
- The root user has /root/ as a home directory, and uses /bin/bash for a shell.

/etc/passwd

- Many accounts in the user-authentication database include a standard login shell in the last column, such as /bin/bash or /bin/sh.
- Changing the default shell for these nonstandard users can enhance security.
- Two fake shells available for this purpose are /bin/false and /sbin/nologin.
- In some distributions, the nologin shell is found in the /usr/sbin/ directory.

/etc/shadow

- This file is very similar to /etc/passwd, but encrypted passwords are no longer placed in /etc/passwd
- The /etc/shadow file contains the encrypted passwords and other password information.
- This file is viewable by the root user only.
- To view the /etc/shadow file use the following commands:

  su – root

  tail /etc/shadow

TABLE 4-3 Data in /etc/shadow, by column.

COLUMN	DESCRIPTION
Username	Login name
Password	A password that has normally been changed to a salted hash; if it starts with 1, it's been modified with the MD5 algorithm
Date of last password change	Date of last password change, in number of days after January 1, 1970
Minimum password life	Number of days a password must be retained
Maximum password life	Number of days the same password can be retained
Password warning period	Number of days before password expiration when a warning is given
Inactive period	Number of days after password expiration when an account is made inactive
Disabled period	Number of days after password expiration when an account is disabled

/etc/shadow

hdhillon:E^K2n5ho>Y8nUtQ:11235:0:99999:14:-1:-1:

1. User name : the login name
2. Password: It your encrypted password. The password should be minimum 6-8 characters long including special characters/digits
3. Last password change (lastchanged): Days since Jan 1, 2018 that password was last changed
4. Minimum: The minimum number of days required between password changes i.e. the number of days left before the user is allowed to change his/her password
5. Maximum: The maximum number of days the password is valid (after that user is forced to change his/her password). 99999 means never.
6. Warn : The number of days before password is to expire that user is warned that his/her password must be changed
7. Inactive : The number of days after password expires that account is disabled
8. Expire : days since Jan 1,2018 that account is disabled i.e. an absolute date specifying when the login may no longer be used

/etc/shadow

- User access to the /etc/shadow file is limited to the root administrative user
- Password is modified by a hash, normally using the Message Digest 5 (MD5) algorithm (default).

/etc/group

- The /etc/group file is world-readable and contains a list of groups, each on a separate line. Each line is a four field, colon delimited list including the following information:
  - *Group name* — The name of the group. Used by various utility programs as a human-readable identifier for the group.
  - *Group password* — If set, this allows users that are not part of the group to join the group by using the newgrp command and typing the password stored here. If a lower case x is in this field, then shadow group passwords are being used.
  - *Group ID* (*GID*) — The numerical equivalent of the group name. It is used by the operating system and applications when determining access privileges.
  - *Member list* — A comma delimited list of the users belonging to the group.

/etc/group

- Here is an example line from /etc/group:

general:x:502:juan,shelley,bob

- This line shows that the general group is using shadow passwords, has a GID of 502, and that juan, shelley, and bob are members.

TABLE 4-7 Groups with special permissions for users.

DESCRIPTION	GROUP NAME
Access external storage devices automatically	`plugdev`
Administer the system	`admin`
Configure printers	`lpadmin`
Connect to the Internet using a modem	`dip`
Connect to wireless and ethernet networks	`netdev`
Monitor system logs	`adm`
Mount user-space filesystems (FUSE)*	`fuse`
Send and receive faxes	`fax`
Share files with the local network	`sambashare`
Use audio devices	`audio`
Use CD-ROM drives	`cdrom`
Use floppy drives	`floppy`
Use modems	`dialout`
Use tape drives	`tape`
Use video devices	`video`

* FUSE is an acronym for Filesystems in USErspace.

/etc/gshadow

- The /etc/gshadow file is readable only by the root user and contains an encrypted password for each group, as well as group membership and administrator information.
- Just as in the /etc/group file, each group's information is on a separate line.
- Each of these lines is a colon delimited list including the following information:
  - *Group name*
  - *Encrypted password*
  - *Group administrators*
  - *Group members*

Establishing a User Account Policy

1. Open the /etc/login.defs file.
2. Set the Password Change directive.
3. Set the Warn directive.
4. Set the password minimum length.
5. Enable login failure logging.
6. Enable successful login logging.
7. Enable the su command.
8. Save and exit.

TABLE 4-6 Standard user- and group-management commands.

COMMAND	DESCRIPTION
`useradd`	Adds users to the shadow password suite based on defaults in `/etc/login.defs`, except when modified by `useradd` command options
`usermod`	Modifies user settings in the shadow password suite
`userdel`	Deletes users; by itself, the command retains the user home directory
`groupadd`	Creates a new group
`groupmod`	Modifies group information
`groupdel`	Deletes an existing group
`groups`	Lists group membership of the current user
`chage`	Revises aging information for a user's password

TABLE 4-5 `/etc/login.defs` security-related directives for new users and groups.

DIRECTIVE	DESCRIPTION
FAILLOG_ENAB	Failed login attempts are collected in the binary `/var/log/faillog` file, unless `pam_tally` is configured in PAM (described later in this chapter)
LOG_OK_LOGINS	Successful logins are collected in a log file defined by `/etc/syslog.conf`
SYSLOG_SU_ENAB	Uses of the su command are logged
SYSLOG_SG_ENAB	Uses of the sg command are logged
FTMP_FILE	Login failures collected in an associated file
PASS_MAX_DAYS	Maximum number of days a password can be used
PASS_MIN_DAYS	Minimum number of days a password must be retained
PASS_MIN_LENGTH	Minimum password length
LOGIN_TIMEOUT	Maximum time for a console login

Securing Groups of Users

- *User Private Group Scheme*
  - Linux users are typically assigned to at least one group, which is based on that user's account.
  - Every user has a primary group. To identify that group, review the third and fourth fields in the /etc/passwd file.
  - Linux distributions that don't implement the user private group scheme may assign all users to the same group. That group is typically named users, with a GID of 100.

A Hierarchy of Administrative Privileges

- Administrative Privileges in Services
  - Some services support the configuration of administrative privileges.
  - Example is the Common UNIX Printing System (CUPS).
  - In its main configuration file, /etc/cups/cupsd.conf, you may find a SystemGroup directive.
  - That directive can be configured to assign a group such as lpadmin or sys as a print administrator group.
  - Ubuntu systems authorize access to many log files for users who are members of the adm group.
- One way to verify the files owned by the adm group is with the following command:
- # find / -group adm

The su and sg Commands

- Use the su command by itself to log in from a regular account into the root administrative account.
- That action prompts for the root password.
- Since logging in as the root administrative user is dangerous, the right way to use the su command is with the -c switch.
- This applies administrative privileges for that one command.
- For example, the following command opens the noted /dev/sda drive in the fdisk utility.
- $ su -c '/sbin/fdisk /dev/sda'

The su and sg Commands

- Use the su command by itself to log in from a regular account into the root administrative account.
- That action prompts for the root password.
- Since logging in as the root administrative user is dangerous, the right way to use the su command is with the -c switch.
- This applies administrative privileges for that one command.
- For example, the following command opens the noted /dev/sda drive in the fdisk utility.
- $ su -c '/sbin/fdisk /dev/sda'

The su and sg Commands

- sg command allows a user to join a group on a temporary basis.
- It works only if there's a group password in the /etc/gshadow file.

Options with sudo and /etc/sudoers

- Limited administrative permissions is based on the sudo command, configured in the /etc/sudoers configuration file
- The sudo command is so important in the Ubuntu distribution that you won't even find a root administrative password on Ubuntu releases. Ubuntu disables logins to the root account.

Basic Options in /etc/sudoers

- The standard /etc/sudoers file contains the following entry, which gives the root administrative user full privileges through sudo:
- root ALL=(ALL) ALL

- Following entry configures full administrative privileges for members of the admin group:
- %admin ALL=(ALL) ALL

TABLE 4-8 Groups of commands in /etc/sudoers.

VARIABLE	COMMANDS
NETWORKING	route, ifconfig, ping, dhclient, net, iptables, rfcomm, wvdial, iwconfig, mii-tool
SOFTWARE	rpm, up2date, yum
SERVICES	service, chkconfig
LOCATE	updated
STORAGE	fdisk, sfdisk, parted, partprobe, mount, umount
DELEGATING	sudo, chown, chmod, chgrp
PROCESSES	nice, kill, killall
DRIVERS	modprobe

Using PAM

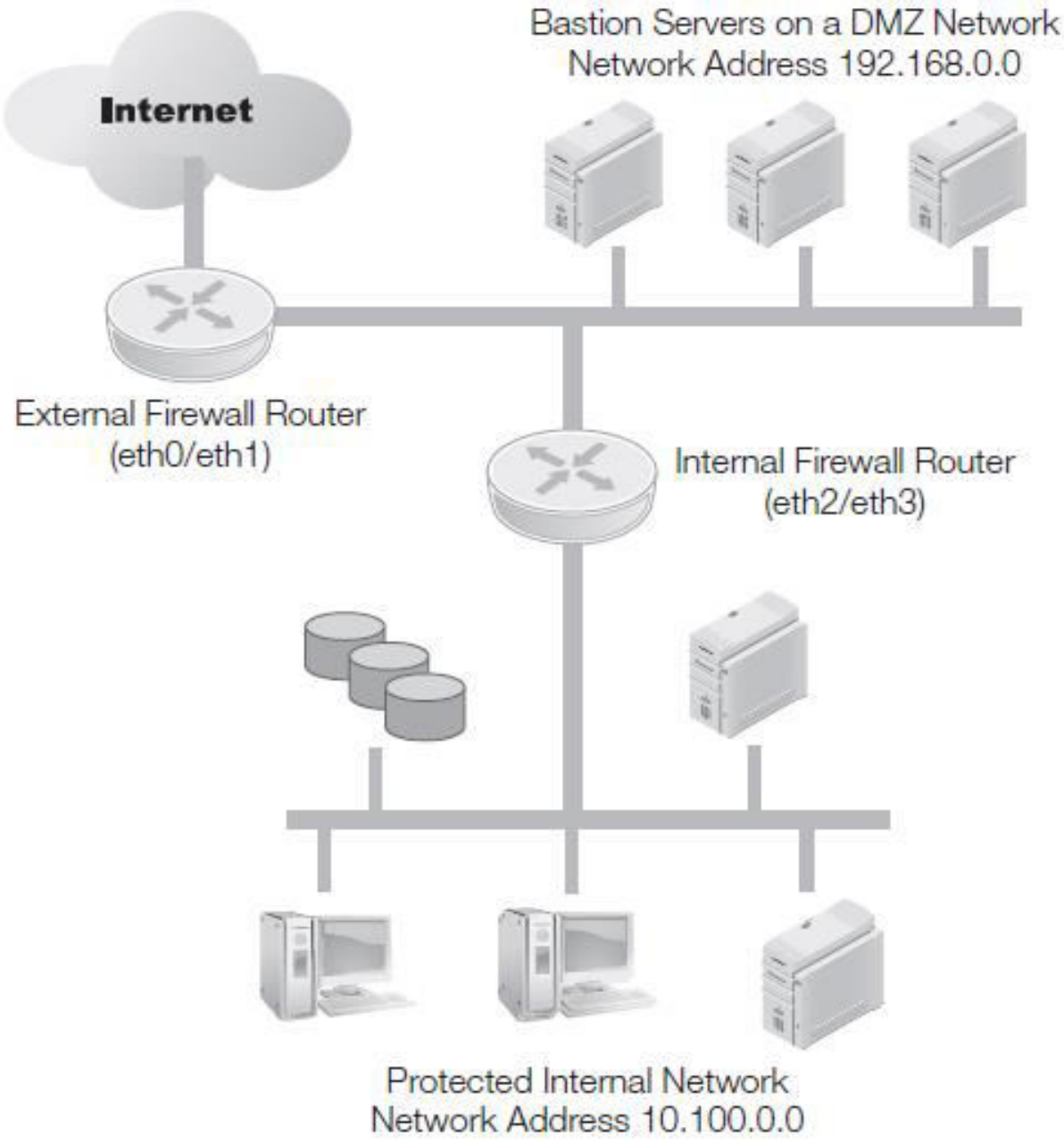
- **An application can use its own authentication file in the /etc/pam.d directory.**
- **PAM can be used to:**
  - Allow access to specific application only during certain times of the day
  - Deny user logins based on files and restrict the user of the su command to only certain groups or users
  - Disconnect a user after ‘x’ number of login attempts

Basic Bastion Hardening

- A bastion server is configured to minimize the risk
- Ideal bastion server is used for a single purpose
- Advantages
  - Minimal additional software—The server has just the software required for the service, and nothing else that could present a security risk.
  - Closed ports—The only open ports are for the service and a remote administrative tool.

FIGURE 6-1

Bastions belong in the DMZ network.



Service Reviews

- Check currently active and installed services.
- Active services can typically be found in one of two locations:
  - scripts in the /etc/init.d/ directory or
  - files in the /etc/xinetd.d/ directory

```
[root@RHEL5-Bastion ~]# \ls /etc/rc3.d/
K01dnsmasq            K89dund                S12restorecond  S28autofs
K02avahi-dnsconfd     K89netplugd            S12syslog       S55sshd
K02NetworkManager     K89pand                S13irqbalance   S56cups
K05conman             K89rdisc               S13portmap      S56rawdevices
K05saslauthd          K91capi                S14nfslock      S56xinetd
K10psacct             K99readahead_later     S15mdmonitor    S80sendmail
K20nfs                S02lvm2-monitor        S18rpcidmapd    S85gpm
K24irda               S04readahead_early     S19rpcgssd      S90crond
K50netconsole         S05kudzu               S22messagebus   S95anacron
K69rpcsvcgssd         S06cpuspeed            S25bluetooth    S95atd
K73ypbind             S08ip6tables           S25netfs        S97rhnsd
K74ipmi               S08iptables            S25pcscd        S97yum-updatesd
K74nscd               S08mcstrans            S26acpid        S98avahi-daemon
K85mdmpd              S09isdn                S26apmd         S99firstboot
K87multipathd         S10network             S26haldaemon    S99local
K88wpa_supplicant     S11auditd              S26hidd         S99smartd
[root@RHEL5-Bastion ~]#
```

DHCP SERVER INFO

- Avoid dynamic DNS—
  - Use the ddns-update-style none; directive in the DHCP configuration file.
- Deny client decline messages—
  - The deny declines; directive can resist attempts by black-hat hackers to exhaust a pool of IP addresses.
- Avoid serving remote networks—
  - If you can avoid the use of the Bootstrap Protocol (BOOTP) with the deny bootp; directive, you'll remove one more possible attack mode.
- Minimize provided information—
  - Don't let the DHCP server provide domain names, DNS servers, NIS servers, NTP servers, or gateway information unless necessary

Installation and Removal on Red Hat Systems

- If you know the names of both packages, the following command could work:

rpm -e samba system-config-samba

- uninstall the open source sendmail e-mail server:

yum remove sendmail

Installation and Removal on Ubuntu Systems

- Uninstall the Samba Web Administration tool (SWAT).

dpkg -r samba swat

- You can use the apt-get and apt-cache automatically find dependencies when you as an administrator want to install and remove packages from a system.
- uninstall filesystem infrastructure associated with the X Window system:

apt-get remove x11-common

Virtual Machine Networks

- The three options are:
- Bridged network—
  - bridged network card directly accesses the same network services as the host system.
  - It gets its IP address information from the same DHCP servers.
  - It connects to the network as if it were just another client.

Virtual Machine Networks

- Network address translation (NAT)—
  - When configured with NAT, virtual clients on a system are configured on their own private network.
  - The host system functions as a gateway between the NAT private network and outside networks.
  - The normal way for external systems to connect to virtual clients on the NAT is with port forwarding.

Virtual Machine Networks

- Host-only network—
  - Similar to a NAT, except communication through the host is disabled.
  - Virtual machines on a host-only network can communicate with the virtual host and with other virtual guests on the same private network.

TABLE 6-2 Service scripts in Red Hat's `/etc/init.d/` directory.

SERVICE SCRIPT	DESCRIPTION	ACTION
`acpid`	Advanced configuration and power interface (ACPI) daemon; should remain enabled unless you don't care about power management.	Enable
`anacron`	Service that runs `cron` scripts if the system is down when jobs are scheduled; disable if the server is powered up 24/7.	Disable
`apmd`	Advanced power-management (APM) daemon; if ACPI is enabled, APM isn't necessary and can be disabled.	Disable
`atd`	The AT daemon runs one-time jobs that are queued, and can be regulated by user as described in Chapter 7.	Maybe
`auditd`	The audit daemon is important for security-related events, including those highlighted by SELinux.	Enable
`autofs`	The automounter mounts removable and network directories on demand.	Disable
`avahi-daemon`	The Avahi daemon is the Linux implementation of the Microsoft zeroconf technology and the Apple Bonjour service discovery protocol. It uses port 5353 to discover printers and shared directories on a local network. Sometimes used for sharing music via Rhythmbox.	Disable
`avahi-dnsconfd`	For discovery of local Domain Name Service (DNS) servers.	Disable
`bluetooth`	For Bluetooth hardware support.	Disable
`bootlogd`	For logging boot messages.	Enable
`capi`	For Integrated Services Digital Network (ISDN) cards.	Disable
`conman`	Service for console management, including SSH and Telnet connections.	Enable
`console-setup`	For text console configuration.	Enable
`cpuspeed`	Service for CPU power management. On later Ubuntu systems, controlled by the `ondemand` script.	Enable
`crond`	Cron daemon for regular administrative jobs; can be regulated by user, as described in Chapter 7.	Enable
`cryptdisks-*`	Encryption service for disks.	Enable
`cups`	Common UNIX Printing System; can disable unless a printer is installed locally or if you need to print from the local system.	Disable
`dnsmasq`	For small-scale DNS and DHCP servers.	Disable

TABLE 6-2 *continued*

SERVICE SCRIPT	DESCRIPTION	ACTION
dund	For Bluetooth-based dial-up networking.	Disable
firstboot	A service that is run once after the operating system is installed.	Disable
functions	For functions used by other /etc/init.d/ scripts.	Enable
gpm	For the console-based mouse pointer; can be useful to copy text.	Depends
grub-common	For GRUB 2.0 boot logging.	Enable
haldaemon	Red Hat suggests you keep this active for the applications that depend on it; the NSA suggests that this daemon is vulnerable in multiple ways.	Depends
hidd	For Bluetooth input devices.	Disable
ip6tables	Firewall for IPv6 networking.	Disable
ipmi	A service for the Intelligent Platform Management Interface (IPMI) to monitor system health.	Enable
iptables	Firewall for IPv4 networking.	Enable
irda	For communication with infrared devices.	Disable
irqbalance	To balance hardware interrupts over multiple processors; disable if only one CPU is on the local system.	Enable
isdn	For support of an ISDN modem.	Disable
keyboard-setup	Initiates keyboard detection during the boot process.	Enable
krb524	For converting Kerberos 5 credentials to Kerberos 4.	Disable
kudzu	Red Hat suggests enabling kudzu for hardware probing; the NSA suggests that it should be disabled.	Depends
lvm2-monitor	For monitoring logical volumes; not necessary unless logical volumes are configured locally.	Depends
mcstrans	For translating category labels in SELinux; required by a few services.	Depends
mdmonitor	For watching over software RAID arrays.	Depends
mdmpd	For watching software RAID multiple path devices.	Depends
messagebus	To listen for real-time changes in hardware.	Depends
microcode_ctl	Standard for Intel 32-bit CPUs.	Depends
multipathd	For configuring multiple devices to storage.	Depends

TABLE 6-2 *continued*

SERVICE SCRIPT	DESCRIPTION	ACTION
`netconsole`	For remote recording of kernel panic messages; may disable until kernel panic issue becomes difficult.	Disable
`netfs`	For system mounting of remotely shared directories from NFS and Samba servers.	Depends
`netplugd`	A daemon that monitors connections to LANs.	Depends
`network`	For basic networking.	Enable
`NetworkManager`	Automates switching between network connections; useful for systems with wired and wireless connections.	Disable
`nfs`	Required for shared Network File System (NFS) connections.	Disable
`nfslock`	For the NFS file-locking service.	Disable
`nscd`	Name service caching daemon (NCSD) for networked authentication services.	Enable
`pand`	For Bluetooth connections to Ethernet networks.	Disable
`pcscd`	Smartcard support.	Depends
`portmap`	To convert remote procedure call (RPC) numbers to TCP/IP ports; used by NFS and the Network Information Service (NIS).	Disable
`psacct`	For kernel process accounting log files.	Enable
`rawdevices`	For connections to Oracle databases.	Disable
`rc.local`	Runs commands in `/etc/rc.local`; avoid if possible.	Depends
`rdisc`	For router discovery.	Depends
`readahead_early`	Loads programs during the boot process; the NSA recommends disabling.	Disable
`readahead_late`	Loads programs during the boot process; the NSA recommends disabling.	Disable
`restorecond`	SELinux monitor for files.	Enable
`rhnsd`	Red Hat Network (RHN) action monitor, needed if you administer this system from RHN.	Enable
`rpcgssd`	Supports credential searches for NFS.	Disable
`rpcidmapd`	The NFS name-mapping daemon.	Disable
`rpcsvcgssd`	Server-side credential searches for NFS.	Disable

TABLE 6-2 *continued*

SERVICE SCRIPT	DESCRIPTION	ACTION
saslauthd	Simple authentication and security layer service, used for some services such as sendmail.	Depends
sendmail	An open source Simple Mail Transfer Protocol (SMTP) e-mail service.	Depends
smartd	Monitor for modern hard drives.	Enable
sshd	SSH server.	Enable
syslog	Log service.	Enable
wpa_supplicant	Wireless network access.	Disable
x11-common	Filesystem infrastructure for additional GUI software.	Disable
xinetd	Extended internet super server.	Disable
ypbind	Binding for NIS clients and servers.	Disable
yum-updatesd	Automatic updates.	Depends

Isolate with chroot Jails

- Without a chroot jail, a user with limited file permissions would still be able to navigate to top-level directories.
- As an example, suppose the user's directory is /home/user.
- Without chroot, nothing would prevent the user from navigating up to /home to see other users' directories or even navigating up to / where they can see /etc, /usr, /var, /lib, and other system-critical directories.

Background on chroot

- The chroot system call changes the root directory of the current and all child processes to the given path,
- The new path is seen entirely as "/" by the process, and we refer to this restricted environment as the "jail".
- It's not possible to escape this jail except in very limited circumstances.
- The chroot system call is found in all versions of UNIX
- it serves to create a temporary root directory for a running process,
- it's a way of taking a limited hierarchy of a filesystem (say, /chroot/named) and making this the top of the directory tree as seen by the application.

Isolate with chroot Jails

- A properly configured chroot jail does not allow privilege escalation of any sort, whether through SUID- or SGID-bit modified executable files or other means of gaining administrative access.
- If a black-hat hacker is able to break into a service, his actions should be confined to the files and subdirectories in the chroot jail.
- Significant services that have been configured with chroot jails include the
  - Berkeley Internet Name Daemon (BIND) software for DNS,
  - Very secure FTP daemon (vsFTPd),
  - Postfix e-mail service.

DNF vs Yum

- The DNF package manager offers robust features for installing, updating, and removing packages.
- Dandified yum, better known as DNF, is a software package manager for RPM-based Linux distributions that installs, updates, and removes packages.
- It was first introduced in Fedora 18 in a testable state (i.e., tech preview), but it's been Fedora's default package manager since Fedora 22.

DNF vs Yum

- **Some of the features that distinguish DNF from yum are:**
  - **Dependency calculation based on modern dependency-solving technology**
  - **Optimized memory-intensive operations**
  - **The ability to run in Python 2 and Python 3**
  - **Complete documentation available for Python APIs**

Avoid X Servers and X Clients

- GUI should be protected carefully.
- Disable any sort of access through the X Display Manager Control Protocol (XDMCP).
- If active, users who browse your networks can see that system as a login option.
- XDMCP works through port 177.
- X clients can still be run remotely even if port 177 is closed.
- The primary means is through an SSH server.
- When a user runs the ssh -X remotehost command, that user is given access to remote GUI clients
- ADD following directive to the SSH server configuration file (sshd_config in the /etc/ssh/ directory):

  X11forwarding no

One System, One Shared Network Service

- Use Kerberos for network authentication
- Install authentication service as well as the Network Time Protocol (NTP) service to keep those systems in sync.
- The default versions of NTP installed for both Red Hat and Ubuntu systems

server 0.rhel.pool.ntp.org

server ntp.ubuntu.com

Install and Configure a Kerberos Server

- Kerberos use key distribution center (KDC) to verify the credentials of a user before allowing access to various network services.
- When verified, the KDC issues a ticket-granting ticket (TGT), a sort of time-limited super-ticket that supports access to other systems without additional authentication.
- The Kerberos server that grants TGTs is known as a ticket-granting server (TGS), which works hand in hand with the KDC.

Basic Kerberos Configuration

- Install of Kerberos software on both the client and the server.
- modify the /etc/krb5.conf file
- matched with changes either
- changes made to /etc/krb5.conf should be matched to the Domain Name System (DNS) database or the /etc/hosts files for each applicable system.
- Note the port numbers associated with the Kerberos key distribution center (kdc) and the administrative server (admin_server), as associated with the noted directives.

```
[libdefaults]
      default_realm = EXAMPLE.ORG
[realms]
      EXAMPLE.ORG = {
            kdc = RHELserver.example.org:88
            admin_server = RHELserver.example.org:749
            default_domain = example.org }
[domain_realm]
      .example.org = EXAMPLE.ORG
      example.org = EXAMPLE.ORG
```

Configuration Options for vsFTP

- The following directive sets up a specific directory for anonymous access to the vsFTP server:

  anon_root = /secure

- logging information about uploads and downloads may be useful. It's activated with the xferlog_enable directive

  xferlog_enable = yes

- One option for uploads is to change the ownership of such files to a specific user, such as nobody or another user configured with minimal privileges.
- chown_uploads = yes
- chown_username = nobody
- Reduce the value of the idle_session_timeout directive.

  idle_session_timeout = 600

  data_connection_timeout = 120

Configuration Options for vsFTP

- Two other confi guration files are directly used for the vsFTP service: ftpusers and user_list.
- includes users with user IDs (UIDs) below 100, 500, or 1000, depending on the distribution.
- If a black-hat hacker breaks into one of these accounts, he or she may be able to obtain limited administrative privileges (or more) through these accounts.
- Red Hat systems specifically cite /etc/vsftpd/ftpusers in the associated pluggable authentication module (PAM) confi guration fi le, /etc/pam.d/vsftpd.

Samba Global Options

- Network-Related Options

  workgroup = bigdomain

  server string = Samba Server Version %v

  netbios name = trivialinfo

- hosts allow directive can be revised to limit access to a domain or even individual host names.

  interfaces = lo eth0 192.168.12.2/24 192.168.13.2/24

  hosts allow = 127. 192.168.12. 192.168.13.

Make Sure SSH Stays Secure

- Directives listed here are based on the default versions of sshd_config installed for Red Hat and Ubuntu systems.
- First, the standard SSH port number is 22, as confirmed here:

  Port 22
- The ListenAddress directive can limit the networks configured for SSH.

  ListenAddress 192.168.10.1
- HostKey directives specify Digital Signature Algorithm (DSA) and Rivest Shamir Adelman (RSA) host key files that can be used to help verify the integrity of the host server.

  HostKey /etc/ssh/ssh_host_dsa_key

  HostKey /etc/ssh/ssh_host_rsa_key

Make Sure SSH Stays Secure

- MaxAuthTries limits the number of login attempts per connection.

  LoginGraceTime 2m

  PermitRootLogin no

  StrictModes yes

  MaxAuthTries 6

- The AuthorizedKeysFile specifies the location of authorized SSH keys in each user's home directory:

  PubkeyAuthentication yes

  AuthorizedKeysFile .ssh/authorized_keys

- Once you've set up passphrases, you can revise this to no to disable clear-text tunneled passwords:

  PasswordAuthentication yes

- Of course, when passwords are used, they should not be empty:

  PermitEmptyPasswords no

Networks and Encryption

- Encapsulating Security Payload (ESP) protocol—Uses protocol number 50. ESP traffic can be allowed through an iptables firewall with a
- -p 50 -j ACCEPT switch.
- • Authentication Header (AH) protocol—Uses protocol number 51. AH traffic can be allowed through an iptables firewall with a

  -p 51 -j ACCEPT switch.
- • Internet Key Exchange (IKE) protocol—Uses the User Datagram Protocol (UDP) over port 500. IKE traffi c can be allowed through an iptables firewall with

  a -p udp --dport 500 -j ACCEPT switch.
- • Network Address Translation (NAT) traversal protocol—Uses the Transmission Control Protocol (TCP) and UDP over port 4500.
- NAT traffic can be allowed through an iptables firewall with
- -p tcp --dport 4500 -j ACCEPT and
- -p tcp --dport 4500 -j ACCEPT switches.

Web Services: Apache

- Apache does not work alone.
- It can be integrated with a variety of database and scripting languages.
- One popular combination is known as the Linux/Apache/MySQL/P (LAMP) stack,

  where the “P” can stand for Perl, Python, or PHP: Hypertext Preprocessor (PHP).

TABLE 9-1 Default security-related MySQL directives in my.cnf.

DIRECTIVE	DESCRIPTION
bind-address	IP address of associated network card to which MySQL listens
datadir	Directory with MySQL data; may require special protection
port	Port number
ssl-ca	SSL certificate authority file
ssl-cert	SSL certificate file
ssl-key	SSL certificate key file

MySQL and Apache

- If you use MySQL, be sure to open port 3306 on any applicable firewall between the Web server and MySQL database server.
- Don’t open that port on an external firewall
- If you prefer a different port, that’s easy to configure
- in the main MySQL configuration file with the port directive.

Security-Related Apache Directives

- One of the strengths of the Apache Web server is its modularity
- Port 443 is the standard for the secure Hypertext Transfer Protocol (HTTPS).

  Listen 443
- directive would listen for requests through port 443 on the noted IP address:

  Listen 192.168.100.10:443

TABLE 9-2 Standard Multi-Processing Module directives.

DIRECTIVE	DESCRIPTION
`StartServers`	Child server processes created during the Apache start process
`MinSpareServers`	Minimum idle child server processes
`MaxSpareServers`	Maximum idle child server processes
`ServerLimit`	Maximum number of clients; also see `ThreadLimit` in the Apache documentation
`MaxClients`	Maximum number of client connections processed simultaneously
`MaxRequestsPerChild`	Maximum number of requests per child server process
`MinSpareThreads`	Minimum number of idle threads to handle additional requests
`MaxSpareThreads`	Maximum number of idle threads to handle additional requests
`ThreadsPerChild`	Number of threads created per child process
`MaxRequestsPerChild`	Maximum number of requests in the life of a child process

An Apache User and Group

- Such ownership can be configured with the User and Group directives:

  User apache

  Group apache

- make sure anyone who logs into that account doesn't get a shell.
- That can be configured in the /etc/passwd file.
- If a black-hat hacker is able to add an .htaccess file to a Web server directory, that user can override anything you've configured with directives in that file.
- To disable the use of the .htaccess file, add the following directive in any stanza with the Directory tag:

  AllowOverride None

Configure Protection on a Web Site

- Configure Protection on a Web Site
- Deny access from all systems except those that send requests from addresses with the noted IP network address and network mask:

```
Order deny,allow
 Deny from all
 Allow from 192.168.0.0/255.255.255.0
```

Configure Protection on a Web Site

- Configure a Secure Web site
  - By default, Web sites that use the HTTPS protocol use port 443.
  - But enabling the appropriate SSL module requires different commands on different systems.
  - On Red Hat systems, when the mod_ssl package is installed,
  - On Ubuntu systems, when the a2enmod command described earlier is applied to the ssl module,
  - directives can also be found in an ssl.conf file, this time in the /etc/apache2/mods-enabled/ directory.

Configure a Certificate Authority

- A certificate authority (CA) is an entity that issues digital certificates.
- The actual certificates are based on a private/public key pair.
- To create a self-signed certificate, you can use the openssl command

```
# openssl genrsa -aes256 -out server.key 1024
```

What is Squid?

- A caching proxy for
  - HTTP, HTTPS (tunnel only)
  - FTP
  - Gopher
  - WAIS (requires additional software)
  - WHOIS (Squid version 2 only)
- Supports transparent proxying
- Supports proxy hierarchies
- Squid is not an origin server!

What is a caching proxy?

- Stores a local copy of objects fetched
  - Subsequent accesses by other users in the organization are served from the local cache, rather than the origin server
  - Reduces network bandwidth
  - Users experience faster web access

Working with Squid

- Any Web proxy server can be configured for two basic purposes.
  - It can cache frequently accessed information,
  - it can regulate user access to remote Web sites.

Working with Squid

- Squid uses the Inter-Cache Protocol (ICP) for transfers between peer and parent/child caching servers.
- It can be used in two directions.
  - As a traditional proxy server, it caches data on behalf of other systems on the local network.
  - As a front-end accelerator, it caches on behalf of clients on remote networks.
- *Squid can block access to certain domains.*
- *If you want to keep users from navigating to certain domains, Squid can access lists of such domains.*

Working with Squid

- The standard port number associated with Squid communication is 3128, which is documented in th following directive:

  http_port 3128.

- The simplest use of Squid ACLs limits access by IP address.

  acl localhost src 127.0.0.1/32

  acl some_net src 192.168.0.0/24

- Allows access from all systems:

  acl all src 0.0.0.0/0.0.0.0

DNS: BIND and More

- Four different types of DNS servers available:
  - • Master—A master DNS server is the authoritative server for a domain.
  - • Slave—A slave DNS server relies on a master DNS server for data.
  - • Caching-only—A caching-only DNS server refers requests to other DNS servers. It also stores recent requests in a local cache.
  - • Forwarding-only—A forwarding-only DNS server refers all requests to other DNS servers.

Secure BIND Configuration

- An authoritative-only name server should not search other DNS servers for additional information. The following directive disables such recursive searches:

  recursion no;

- Any secure DNS server should not allow transfers of zone databases to minimize the risk of cache poisoning. The following directive allows transfers to no other DNS servers:
- allow-transfer{none;};