Understanding Linux Security

BENNETT UNIVERSITY
THE TIMES GROUP

Dr. Vimal Kr Baghel (Course Instructor), Assistant Professor
School of Computer Science Engineering & Technology (SCSET)
Bennett University Greater Noida

Outline

Linux Security

Password file

Shadow file

Q & A

Understanding Linux File Permissions

- We need mechanism to protect files against unauthorized access ?

- The Linux system follows the Unix method of file permissions, allowing individual users and groups access to files based on a set of security settings for each file and directory.

Linux Security

The core of the Linux security system is the ***user account***

The permissions are based on ***user account***, and are tracked with ***numeric UID***

Login name of ***8 characters*** or less

The Linux system uses special files and utilities to track and manage user accounts on the system to understand how to use them when working with file permissions.

How Linux handles user accounts?

The /etc/passwd file

To match the login name to a corresponding UID value.

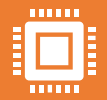
UID is 0 for root

System user account

Linux reserves UIDs below 500 for system accounts.

First UID starts from 501 usually

The /etc/passwd file



Every service that runs in background on a Linux server has its own user account to log in with. ***Why?***

The /etc/passwd file contains much more than just the login name and UID for the user.

The /etc/passwd file is a standard text file.

We can use any text editor to manually perform user management functions such as adding, modifying, or removing user accounts directly in the /etc/passwd file.

Field in /etc/passwd

- The fields of the /etc/passwd file contain the following information:
  - The login username
  - The password for the user
  - The numerical UID of the user account
  - The numerical group ID (GID) of the user account
  - A text description of the user account (called the comment field)
  - The location of the HOME directory for the user
  - The default shell for the user

The /etc/passwd file


```
$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/etc/news:
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
rpm:x:37:37::/var/lib/rpm:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
mailnull:x:47:47::/var/spool/mqueue:/sbin/nologin
smmsp:x:51:51::/var/spool/mqueue:/sbin/nologin
apache:x:48:48:Apache:/var/www:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
nscd:x:28:28:NSCD Daemon:/:/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
avahi:x:70:70:Avahi daemon:/:/sbin/nologin
hsqldb:x:96:96::/var/lib/hsqldb:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
haldaemon:x:68:68:HAL daemon:/:/sbin/nologin
xfs:x:43:43:X Font Server:/etc/X11/fs:/sbin/nologin
gdm:x:42:42::/var/gdm:/sbin/nologin
rich:x:500:500:Rich Blum:/home/rich:/bin/bash
mama:x:501:501:Mama:/home/mama:/bin/bash
katie:x:502:502:katie:/home/katie:/bin/bash
jessica:x:503:503:Jessica:/home/jessica:/bin/bash
mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash
$
```

/etc/shadow

- Most Linux systems hold user passwords in a separate file
- Only root can use it
- The /etc/shadow file contains one record for each user account on the system.
- A record looks like this:
  - `rich:$1$.FfcK0ns$f1UgiyHQ25wrB/hykCn020:11627:0:99999:7:::`

Fields in /etc/shadow file

- There are nine fields in each /etc/shadow fi le record:
  - The login name corresponding to the login name in the /etc/passwd fi le
  - The encrypted password
  - The number of days since January 1, 1970, that the password was last changed
  - The minimum number of days before the password can be changed
  - The number of days before the password must be changed
  - The number of days before password expiration that the user is warned to change the password
  - The number of days after a password expires before the account will be disabled
  - The date (stored as the number of days since January 1, 1970) since the user account was disabled
  - A field reserved for future use

Thanks

Q & A