Table Of Contents

nixCraft: Linux Tips, Hacks, Tutorials, And Ideas In Blog Format
http://www.cyberciti.biz/

Linux Disable Shell / FTP Access For a User Account

Posted by Vivek Gite <vivek@nixcraft.com>


[1]

My users will only be checking mail, and I want to disable FTP access as well as shell access under CentOS Linux. How do I disable shell (SSH) and FTP access to a new or old user under Linux without deleting user account?

You can easily disable shell, ssh and FTP access to a user using following commands:

1. **chsh command** : It used to change your login shell.
2. **/sbin/nologin**: Displays a message that an account is not available and exits non-zero. It is intended as a replacement shell field for accounts that have been disabled.

Task: Disable Linux User Shell Account

Type the following command to disable shell access for tom:

```
# chsh -s /sbin/nologin {username}
# chsh -s /sbin/nologin tom
```

Sample Outputs:

```
Changing shell for tom
Shell changed.
```

Where,

1. **-s /sbin/nologin**: Politely refuse a login
2. **tom** : The user name you wish to deny shell access to.

Task: Disable Linux FTP User Account

If you have VSFTPD [2] ftp server or other FTP server add user to /etc/ftpusers or /etc/vsftpd/ftpusers (VSFTPD) file.

```
# echo tom >> /etc/ftpuser
```

OR

```
# echo tom >> /etc/vsftpd/ftpusers
```

Any user name added to /etc/ftpusers or /etc/vsftpd/ftpusers will prevent them from logging into FTP. However, this will still allow user to login via email (webmail or pop3 / IMAP) and download emails without shell access.

A Note About PAM and access.conf

Apart from above two method Linux supports pam and access.conf login tables.

Pam modules can be used to enable or disable access to certain services such as vsftpd, ssh, and so on. /etc/security/access.conf act as login access control table, which is useful to deny or login access based upon ip address, network location or tty name. When someone logs in, the file is scanned for the first entry that matches the (user, host) combination, or, in case of non-networked logins, the first entry that matches the (user, tty) combination. The permissions field of that table entry determines whether the login will be accepted or refused. See how to use pam modules to enable [3] or disable login access. For e.g. deny access to tom, enter the following in /etc/security/access.conf

```
- : tom : ALL
```

Where,

- **- : Deny access. a "+" character (plus) for access granted or a "-" character (minus) for access denied.**
- **tom: Username. It should be a list of one or more login names, group names, or ALL (which always matches).**
- **ALL : Deny access from all ip address.**

Further readings:

- man pages access.conf, nologin, pam, chsh, vsftpd.conf