Table Of Contents

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

Help: Old Employees Accessing The Linux Server

Posted by Vivek Gite <vivek@nixcraft.com>

I've recently noticed that two of my former employees are still accessing one of our Linux box. Old user account wasn't deleted because it has some important files. How do I make sure account get deleted without losing files and email stored in the account? Can you describe a terminations clearance policy for an employee account including email accounts, forwarding aliases, ssh / ftp, and access to vpn dialup services under Red Hat Enterprise Linux server?

Laid-off employee may seek revenge so delete and disable all unwanted account. When an employee leaves you can immediately lock down shell access by typing the following command: [1]

```
# passwd -l username
```

The -l option disables an account by changing the password to a value which matches no possible encrypted value, and by setting the account expiry field to 1. This make sure he / she cannot get into server. You can delete a user account without removing any files as follows:

```
# userdel username
```

You can also tell userdel to remove the user's home directory and all of its contents:

```
# userdel -r username
```

Files in the user' s home directory will be removed along with the home directory itself and the user´s mail spool. Files located in other file systems will have to be searched for and deleted manually. Additional cleanup work is is left to the administrator.

Recommend Procedure To Delete User Account

The following is recommend procedure. Linux / UNIX server accounts are maintained as long as the owner is affiliated with you or your business. Generally, users or employees who leave for one reason or another will eventually lose their accounts and data. However, please consult your legal or HR department regarding local laws and privacy policy laws.

#1: Deactivate the account

First, local down user account and disable login to shell, ftp and ssh services:

```
passwd -l username
```

#2: Scan For rootkits

Scan file for virus, bad stuff and rootkits. Try chkrootkit and rkhunter [2] software for scanning rootkits. If user accessing Linux file server via Windows or Mac operating system, use Microsoft / Mac os tools and anti-virus software to scan files. The ClamAV virus scanner is available and may be used to scan Linux / Unix file systems for viruses which infect other operating systems. Some employees leave rootkits and virus for backdoor entry. This is critical before you make a backup of existing data.

#3: Backup Data

Usually, you need to backup:

- Home directory
- Email box
- FTP directory
- Cron jobs

- Webserver files
- CVS files
- MySQL / PGSQL database etc

Just create a tarball of home directory, cron jobs, and mailbox at safe location in another directory:

```
# DEST=/path/to/safe/delete_accounts/user/data_$(date +"%d-%m-%Y_%H_%M_%P").tar.gz
# SHOME=/home/$user
# SMAILBOX=/usr/local/mailboxes/domain.com/$user
# SCRON=/var/spool/cron/crontabs/$user
# SFTP=/var/spool/ftp/$user
# tar -zcvf $DEST $SHOME $SMAILBOX $SCRON $SFTP
```

Replace $user and other paths with actual values.

#4: List Files In Other Directories

User may have left files in other directories. Type the following command to get a complete list of files owned by user vivek:

```
# find / -user vivek -print0 > /root/viveksfiles.txt 2>/root/error.log &
```

You can backup those files or simply change their ownership using find command itself. Removes all files owned by the user from /tmp, /var/tmp, and other tmp locations.

Delete User Account

Finally, you can delete the user account and all files:

```
# userdel -r $user
```

Make sure you removed the username from all groups to which it belongs in /etc/group [3].

#5: Removes The User's Crontab

Type the following command to backup and delete cronjobs:

```
# crontab -u username -l > /path/to/safe/delete_accounts/user/crontab.bak
# crontab -u username -r
```

#6: Removes The User's at Jobs

Type atq command to lists the user's pending jobs, unless the user is the superuser; in that case, everybody's jobs are listed. The format of the output lines:

```
# atq | less
# atq > /path/to/safe/delete_accounts/user/at.bak
# atrm jobid
```

#7: Delete All Process

You need to send a SIGKILL (-9) signal to all processes owned by the user. For example, send -KILL single to all process [4] owned by vivek use the following commands. Get detailed inforation about running process:

```
# ps -fp $(pgrep -u vivek)
```

Get all PIDS:

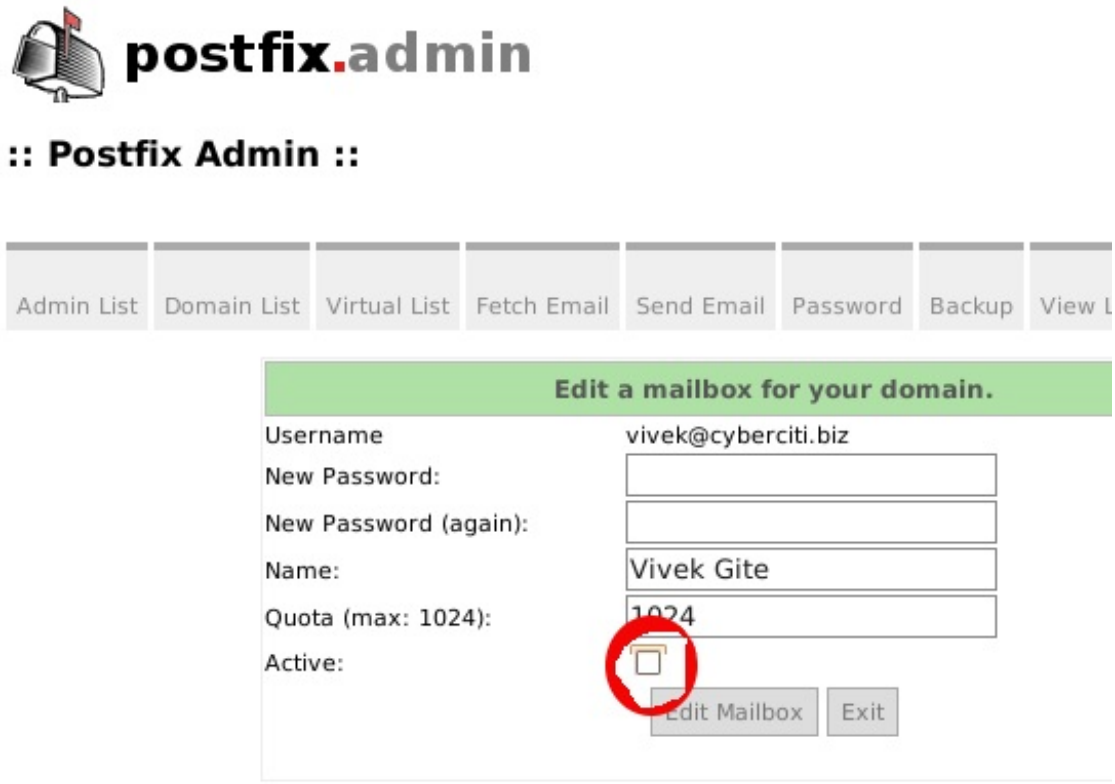
```
# pgrep -u vivek
# pkill -9 -u vivek pid1 pid2
```

OR

```
# killall -KILL -u vivek
```

#8: Disable Email Login

Configure your email server to forward or deny access to email box. Usually, this is done by editing mysql or LDAP database files. Removes the incoming mail (postfix or sendmail) and POP / IMAP daemon mail files belonging to the user from /var/mail or /var/spool/mail.



[5]

Fig.01: Postfix - Disable Email Box Using Postfixadmin

You can also forward incoming email or simply delete mailbox with Postfixadmin.

#9: Disable Proxy Server and VPN Remote Login

Again update your central login database (such as LDAP) and disable all login access.

#10: Files and Emails

Generally, any files or email left on a system can be turned over to employees supervisor if necessary.

#11: Dealing With Root Level Access

If former employee had root access you may need to look out for following additional things:

1. Trojans.
2. Hidden kernel backdoor modules.
3. Rootkits.
4. Cron and at jobs can be to run arbitrary shell scripts or give back root level access again.
5. .forward file can be to run arbitrary shell scripts.
6. Unwanted and hidden network services.
7. SSH password less remote login keys etc.
8. Unwanted SUID/SGID binaries.
9. Iptables firewalls settings.
10. Removes all message queues, shared memory segments and semaphores owned by the user.

Use Identity Manager Software

Third party identity manager software can easily enable and disable access to many services. You can configure various policies based on users employment status or weekend login policy etc using an automated provisioning software.

Automation

You can write a perl or shell script to automate the entire procedure to disable access to user account and backup files / emails in other safe location.

URLs in this post:

[1] Image: **http://www.cyberciti.biz/faq/category/linux/**
[2] chkrootkit and rkhunter: **http://www.cyberciti.biz/faq/howto-check-linux-rootkist-with-detectors-software/**
[3] /etc/group: **http://www.cyberciti.biz/faq/understanding-etcgroup-file/**
[4] send -KILL single to all process: **http://bash.cyberciti.biz/guide/Sending_signal_to_Processes**
[5] Image: **http://www.cyberciti.biz/faq/former-employees-keep-accessing-linux-unix-server/postfix-admin-mail-nixcraft-net/**