

LinkedIn respects your privacy

LinkedIn and 3rd parties use essential and non-essential cookies to provide, secure, analyze and improve our Services, and to show you relevant ads (including professional and job ads) on and off LinkedIn. Learn more in our [Cookie Policy](#).

Select **Accept** to consent or **Reject** to decline. You can update your choices at any time in your account settings.

Accept

Reject



Top Content

```

1/bin/sh
# atrun uid=0 gid=0
# mail root 0
umask 22
LS_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=
01;32;4*:tar=01;31;4*:tgz=01;31;4*:arc=01
=01;31;4*:zip=01;31;4*:z=01;31;4*:Z=01;3
1;4*:tbz=01;31;4*:tbz2=01;31;4*:tz=01;31;4
*:cpio=01;31;4*:7z=01;31;4*:rz=01;31;4*:
35;4*:bmp=01;35;4*:pbm=01;35;4*:pgm=01;35
;35;4*:pcx=01;35;4*:mov=01;35;4*:mpg=01;
01;35;4*:nuv=01;35;4*:wmv=01;35;4*:asf=01
;35;4*:yuv=01;35;4*:cgm=01;35;4*:emf=01;
0;36;4*:mpc=00;36;4*:ogg=00;36;4*:ra=00;
SSH_CONNECTION=192.168.1.1 49945 192.168.1.1
LESSCLOSE=/usr/bin/lesspipe %s %s; export
LANG=C.UTF-8; export LANG
OLDPWD=/var/spool/cron; export OLDPWD
XDG_SESSION_ID=3359; export XDG_SESSION_ID
USER=root; export USER
PWD=/var/spool/cron/atjobs; export PWD
HOME=/root; export HOME
SSH_CLIENT=192.168.1.1 49945 22; export
XDG_DATA_DIRS=/usr/local/share:/usr/share:/v
SSH_TTY=/dev/pts/4; export SSH_TTY
MAIL=/var/mail/root; export MAIL
SHLVL=1; export SHLVL
LOGNAME=root; export LOGNAME
XDG_RUNTIME_DIR=/run/user/0; export XDG_RUIN
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbi
PS1=sandflysecurity#\ ; export PS1
LESSOPEN=|\ /usr/bin/lesspipe %s; export L
cd /var/spool/cron/atjobs | {
  echo 'Execution directory inaccessible'
  exit 1
}
https://pastebin.com/4154
sandflysecurity#

```

Agree & Join LinkedIn

By clicking Continue to join or sign in, you agree to LinkedIn's [User Agreement](#), [Privacy Policy](#), and [Cookie Policy](#).

Sign in with Google

Use your Google Account to sign in to LinkedIn

No more passwords to remember. Signing in is fast, simple and secure.

Continue

Continue with Google

Join with email

Already on LinkedIn? [Sign in](#)

By clicking Continue to join or sign in, you agree to LinkedIn's [User Agreement](#), [Privacy Policy](#), and [Cookie Policy](#).

Getting an Attacker IP Address from a Malicious Linux At Job



Craig Rowland

Published Jul 25, 2019

+ Follow

1 LinkedIn respects your privacy

LinkedIn and 3rd parties use essential and non-essential cookies to provide, secure, analyze and improve our Services, and to show you relevant ads (including professional and job ads) on and off LinkedIn. Learn more in our [Cookie Policy](#).

Select **Accept** to consent or **Reject** to decline. You can update your choices at any time in your account settings.

Agree & Join LinkedIn

By clicking Continue to join or sign in, you agree to LinkedIn's [User Agreement](#), [Privacy Policy](#), and [Cookie Policy](#).



Join now to view more content

Create your free account or sign in to continue your search

 Join with email

or

Already on LinkedIn? [Sign in](#)

By clicking Continue to join or sign in, you agree to LinkedIn's [User Agreement](#), [Privacy Policy](#), and [Cookie Policy](#).

```
root@ubuntu-18-10:~# cat /etc/passwd | grep root
root:x:0:0:root:/:/bin/bash
root:x:1:1:root:/:/bin/bash
root:x:2:2:root:/:/bin/bash
root:x:3:3:root:/:/bin/bash
root:x:4:4:root:/:/bin/bash
root:x:1:1:root:/:/bin/bash
root@ubuntu-18-10:~#
```

The above we see four jobs for the root user. The first column is the *at* job number which we can list individually with the *at -c <jobnum>* command:


1 LinkedIn respects your privacy

LinkedIn and 3rd parties use essential and non-essential cookies to provide, secure, analyze and improve our Services, and to show you relevant ads (including professional and job ads) on and off LinkedIn. Learn more in our [Cookie Policy](#).

Select Accept to consent or Reject to decline. You can also manage your preferences and update your choices at any time in your account settings.

Agree & Join LinkedIn
By clicking Continue to join or sign in, you agree to LinkedIn's [User Agreement](#), [Privacy Policy](#), and [Cookie Policy](#).

```
LANG=C.UTF-8; export LANG
OLDPWD=/var/spool/cron/crontabs/
XDG_SESSION_ID=3
USER=root; export USER
PWD=/var/spool/cron/crontabs/
HOME=/root; export HOME
SSH_CLIENT=192.168.1.100 22 0
XDG_DATA_DIRS=/usr/share/termin
SSH_TTY=/dev/pts/0
MAIL=/var/mail/root
SHLVL=1; export SHLVL
LOGNAME=root; export LOGNAME
XDG_RUNTIME_DIR=/run/user/0
PATH=/usr/local/sbin:/usr/local
PS1=sandflysecure@kali:~$
LESSOPEN=|| /usr/bin/lesspipe
cd /var/spool/cron/crontabs/
echo '
exit 1
}
hxxps://pastebin.com/
```



Join now to view more content

Create your free account or sign in to continue your search

or

Already on LinkedIn? [Sign in](#)

By clicking Continue to join or sign in, you agree to LinkedIn's [User Agreement](#), [Privacy Policy](#), and [Cookie Policy](#).

This dumps each job number and you can see some interesting things. The most important part is the SSH_CONNECTION and SSH_CLIENT variables. These contain the IP addresses of the machine that created the jobs!

If you want to see all the `at` jobs at once quickly, you can simply use the `cat` command to dump them like this:

LinkedIn respects your privacy

LinkedIn and 3rd parties use essential and non-essential cookies to provide, secure, analyze and improve our Services, and to show you relevant ads (including professional and job ads) on and off LinkedIn. Learn more in our [Cookie Policy](#).

Select **Accept** to consent or **Reject** to decline. You can update your choices at any time in your account settings.

Agree & Join LinkedIn

By clicking Continue to join or sign in, you agree to LinkedIn's [User Agreement](#), [Privacy Policy](#), and [Cookie Policy](#).

Always Check At J

In general, *at* jobs are a good idea and you did not do anything wrong. If you're investigating a job, you can give you valuable clues. Information from other sources can help you get a better idea of what is going on.

Have Sandfly Check

Even better than watching a video, our agentless security tool can detect attacks on Linux 24/7. It is in plain details.



Join now to view more content

Create your free account or sign in to continue your search



Join with email

or

Already on LinkedIn? [Sign in](#)

By clicking Continue to join or sign in, you agree to LinkedIn's [User Agreement](#), [Privacy Policy](#), and [Cookie Policy](#).

Linux hosts. If you see no did and why. If you have a good idea and can help with their connection

Jobs, you can have the persistence we'll show you what



Like



Comment



Share



9 · 2 Comments

James King

6y

Love these blog posts, keep up the good work!

Like · Reply | 1 Reaction



LinkedIn respects your privacy

LinkedIn and 3rd parties use essential and non-essential cookies to provide, secure, analyze and improve our Services, and to show you relevant ads (including professional and job ads) on and off LinkedIn. Learn more in our [Cookie Policy](#).

Select **Accept** to consent or **Reject** to decline. You can update your choices at any time in your settings.

Agree & Join LinkedIn
By clicking Continue to join or sign in, you agree to LinkedIn's [User Agreement](#), [Privacy Policy](#), and [Cookie Policy](#).


Linux Medusa Rootkit Detect

I was some

Jun 23, SCTP The S telecc

Jun 16, Detect Packe some

Mar 27, Detect A new to hid



Join now to view more content

Create your free account or sign in to continue your search

 [Join with email](#)

or

Already on LinkedIn? [Sign in](#)

By clicking Continue to join or sign in, you agree to LinkedIn's [User Agreement](#), [Privacy Policy](#), and [Cookie Policy](#).

[Show more](#)

Others also viewed



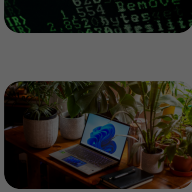
Security hysteria in an example: SMBv1 vs the world.
Konrads Klints · 7y



ASLR: The Linux Ninja That Guards Your System
Tushar Vyavahare · 2y

LinkedIn respects your privacy
LinkedIn and 3rd parties use essential and non-essential cookies to provide, secure, analyze and improve our Services, and to show you relevant ads (including professional and job ads) on and off LinkedIn. Learn more in our [Cookie Policy](#).
Select **Accept** to consent or **Reject** to decline. You can update your choices at any time in your settings.


Agree & Join LinkedIn
By clicking Continue to join or sign in, you agree to LinkedIn's [User Agreement](#), [Privacy Policy](#), and [Cookie Policy](#).

 **In-Depth Stack**
Hanuman

Show more ▾

Explore content

- Career
- Productivity
- Project Management
- Show more



Join now to view more content

Create your free account or sign in to continue your search

or

Already on LinkedIn? [Sign in](#)

By clicking Continue to join or sign in, you agree to LinkedIn's [User Agreement](#), [Privacy Policy](#), and [Cookie Policy](#).

© 2026

- Accessibility
- Privacy Policy
- Copyright Policy
- Guest Controls
- Language

- Brand Policy
- Community Guidelines