

Forum:[Hack Forums](#)

Thread: [How to confirm how/who is hacking a linux server?](#)

virtualpaul - June 29, 2018, 9:25 am

I am getting very large GB consumption on my server so I am guessing it has been hacked.
I am following a small tutorial on how to check if your linux server has been hacked.

It says to use 'netstat' as follows: "check both carefully because if you got a malicious script is trying to sending spam mail or try to attach other server you can easily find here"

I see many entries but I have no clue on how to determine the above. Here is a filtered list:

netstat

Active Internet connections (w/o servers)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	<number>	<number>	<address>	<address>	TIME_WAIT
tcp	<number>	<number>	<address>	<address>	ESTABLISHED
tcp	<number>	<number>	<address>	<address>	CLOSING
udp6	<number>	<number>	localhost:<number>	localhost:<number>	ESTABLISHED
...					

Active UNIX domain sockets (w/o servers)

Proto	RefCnt	Flags	Type	State	I-Node	Path
unix	2	[]	DGRAM		<number>	<path>
unix	3	[]	STREAM	CONNECTED	<number>	<path>
...						

Some of the <path> are as follows:

- /run/systemd/notify
- /run/systemd/cgroups-agent
- /run/systemd/journal/dev-log
- /var/spool/postfix/dev/log
- /run/systemd/journal/socket
- /run/systemd/journal/syslog
- private/anvil
- /run/systemd/journal/stdout
- /var/run/dbus/system_bus_socket
- /var/run/dovecot/anvil-auth-penalty
- private/rewrite
- public/cleanup
- /var/run/dovecot/auth-worker

Anybody can help?

dmzero_ - July 1, 2018, 8:26 am

Some things you can have a look at are the following:

top - this will show the process from the ones utilizing the most bandwidth to the lowest. If you setup different user accounts the process user might give you indication as to what rights the process is

running on.

You can use the following to have a look at incoming/outgoing packets:

```
tcpflow -i eth0 -c port 7891
```

Also if you have some funny ports listening that you know you haven't configured it might be worth blocking access to those using ufw.

You could also try to view the last modified files for an indication on whether a shell was dropped or other software is being installed using:

```
ls -lt | head -5
```

or

```
ls -t | tail -n 5
```

And obviously things like spikes in disk usage and memory or CPU could also leave some clues.

This is off the top of my head, hope it helps!

lurking - July 3, 2018, 3:00 am

First and foremost, I would start by looking at your `/var/log/auth.log`. See if any rouge users have successfully accepted connections to the box. Given that there aren't many public ways known to get root on a system (if any since dirty cow), cleaning these logs would essentially be impossible if you've properly prevented users from escalating to root.

As for actually looking at the inbound/outbound you can use iftop. That can be found here:

<http://www.ex-parrot.com/pdw/iftop/>

Most linux distributions/package managers will have the ability to simply install iftop. For example debian/ubuntu: `sudo apt-get install iftop`. Here you can see the traffic going in and out, and to what IP Addresses.

In addition, we can look at `/etc/passwd` to see the users on the system. If you see new users you didn't create, you're probably compromised... or a package created a user. You can hop around and look at the history of each user, though this can be easily cleared (unlike auth log, which I mentioned above).

In the meantime, ensure that you are only accepting ssh-keys via your `/etc/ssh/sshd_config`, and specify `AllowUsers` for your username. This will ensure only you can log into your box (via ssh assuming another backdoor has not been introduced) and that you're only accepting your ssh-key. You can read further here: https://www.ssh.com/ssh/sshd_config/

If you would like help in seeing if your system is compromised, feel free to send me a private message. If you are unclear on any section of this, especially messing with ssh-keys and `AllowUsers` just contact me first. You can lock yourself out, which isn't so helpful. I would be happy to assist further.