

Check Your Server Security

Sometimes it is possible that your server is compromised, but the actions made by attacker do not affect your server functionality, so you may never find that your machine was compromised.

So, is good from time to time to check your server security, to see if any strange activities/processes are in your system.

Check if your server resources are affected. You could check CPU usage by issuing top command. Look for applications/scripts that consume your CPU.

Check for strange processes with ps -awux command.

Check your /tmp directory and also your /var/tmp directory for scripts/binaries copied there.

When a server is compromised sometimes the attacker use it to host a IRC bot (like psybnc or eggdrop) that connects to port 6667. You could check if any of your applications connect to that port with sockstat:

```
#sockstat | grep 6667
```

If there's not much traffic on your server you could use netstat command to see if suspect connections are made.

```
#netstat -a
```

Install and run at regular period of times an rootkit finder application (for example /usr/ports/security/rkhunter).

Check your open ports with nmap. See if you have other open ports than the ones you use for your running services.