Linux Host Security

Monitoring Ports and services

Eghbal aminejad

LINUX AUTHOR AND TRAINER

github: @eqba1

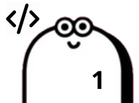
Monitoring Ports and services

Course Objectives

- **Using systemctl to list running services**
- **Disabling or removing unnecessary**
- **Implementing an NTP client without server on Linux with systemd**
- **Listing open ports and reducing interfaces used by services**

Weight

- After your server is installed, how many services are running that you do not need ?
- The systemd command set allows us to drill down to see running services
- systemctl list-units --type service --state running
- if a service dows not need to be running it can be disabled. Using the option --now will also stop the srevice as it is disabled

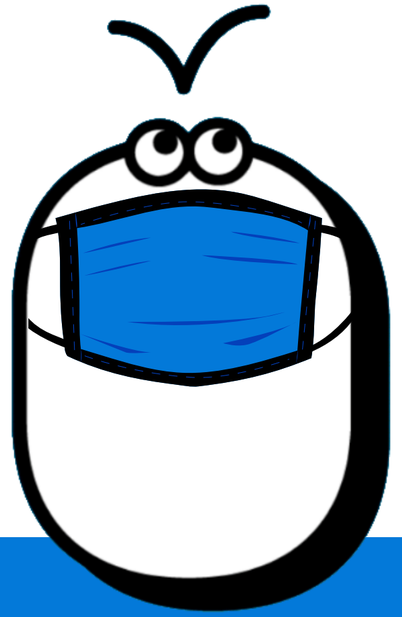


Removing Services

اگر از سرویسی هیچ وقت استفاده نمیکنید، حذفش کنید. برای مثال من هیچ وقت از سرویس atd استفاده نمی‌کنم. البته باید توجه داشته باشیم که سرویس مورد نظر به چه بخش های دیگر سیستم وابستگی دارد و مطمئن باشیم پکیج مهمی را همراهش حذف نکنیم.

```
$ dpkg -S $(which atd)
```

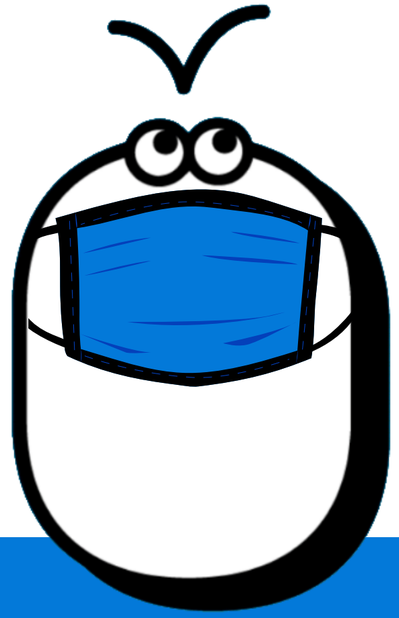
Using systemctl to
list running services



Demo

- Implementing time synchronization with NTP or Chrony you will have both a time server and time client
- Later versions of systemd include the timesyncd service. A client only NTP system
- if you need to set the tiem source to synchronize with use the /etc/systemd/timesyncd.conf

Implementing an NTP Client only on Ubuntu 20.04



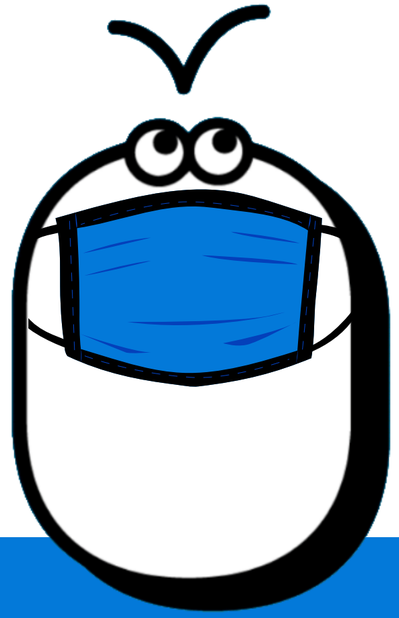
Demo

```
$ ss -ntl
$ ss -l '( sport = :ssh )'
$ grep -Fi listen /etc/ssh/sshd_config
```

Listing Ports

معمولا عادت داریم برای دیدن پورت های باز در سیستم از دستور netstat استفاده کنیم. البته این دستور منسوخ شده و حال دستور ss جایگزین آن است. سرویس SSHD بر روی همه رابط - interface - ها و پروتکل های ای پی ورژن ۴ و ۶ در حالت listen است. میدانیم هرچه رابط ها کمتری در حالت listen باشند احتمال حملات مخرب نیز کاهش می یابد.

Using filters with ss to list service ports and securing SSHD



Demo

summary

- Systemctl is a robgust tools to manage and list services
- systemctl list-units -- type service
- systemctl disable atd --now
- dpkg -S $(which atd)
- timedatectl
- /etc/systemd/timesyncd.conf
- ss -l '(sport = :ssh)'

Weight

Next up

Understanding Chroot Jails

Eghbal aminejad

LINUX AUTHOR AND TRAINER

github: @eqba1