Privilege Escalation

sleepunderflow
Grzegorz Zielinski

Link to last week box and writeups

- https://www.vulnhub.com/entry/mr-robot-1,151/

Why

- Simple, to get access to a higher privileged user

How

- Services running as more privileged user that you can control somehow
  - User input
    - Command injection
    - Binary exploitation
  - Exposed interfaces/APIs
  - External files
  - Environment variables
    - Path poisoning

How

- Automated processes periodically running as a more privileged user
  - cron
    - /etc/crontab
    - /etc/cron.daily
    - etc.
- SUID bit
- Groups!
- File and process capabilities

Tools

- Built-in commands:
  - Find, man, etc.
- Documentations
- LinEnum.sh
  - https://raw.githubusercontent.com/rebootuser/LinEnum/master/LinEnum.sh
- Linux smart enumeration
  - https://raw.githubusercontent.com/diego-treitos/linux-smart-enumeration/master/lse.sh
- pspy
  - https://github.com/DominicBreuker/pspy
- GTFOBins
  - https://gtfobins.github.io/

Challenge for today

docker run -it --rm -p22:22 sleepunderflow/privesc-trainer

Challenge for today

```
docker run -it --rm -p22:22 sleepunderflow/privesc-trainer
```