# Configuration

## Enable SSH

1. ssh localhost
2. sudo apt-get update
3. sudo apt-get install openssh-server
4. sudo service ssh status
5. sudo apt-get install nano

## Login as root

1. su
2. Password: a\*\*

# 1. Ensure SSH PermitEmptyPasswords is disabled

1. cd /etc/ssh
2. dir
3. nano sshd\_config **OR**
4. **nano /etc/ssh/sshd\_config**
5. **uncomment/EDIT**: SSH PermitEmptyPasswords no

# 2. Ensure SSH root login is disabled

1. cd /etc/ssh
2. dir
3. nano sshd\_config
4. **uncomment/EDIT**: PermitRootLogin no

# 3. Ensure SSH Protocol is set to 2

1. cd /etc/ssh
2. dir
3. nano sshd\_config
4. **uncomment/EDIT**: Protocol 2

# 4. Ensure password expiration is 90 days or less

1. cd /etc
2. dir
3. nano login.defs
4. **uncomment/EDIT**: PASS\_MAX\_DAYS 90

# 5. Ensure system accounts are non-login

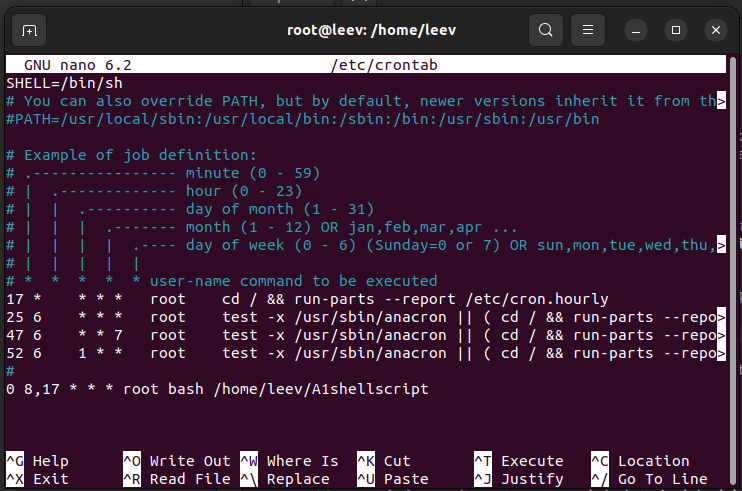
1. [](https://secscan.acron.pl/centos7/5/4/2)

## Check cron is running

1. systemctl status cron

## Bash script executed every 8am and 5pm on a daily basis

1. nano /etc/crontab



0 8,17 \* \* \* refers to the cron expression (8am and 5pm)

bash /home/leev/A1shellscript executes shellscript file in root folder

SCRIPT

**// SLIDE ONE**

* Good morning —-- and colleagues. I am —-- and I will be presenting my product today that will ensure essential basic security requirements can be configured on any system and enhance security of servers easily.
* Cloud-computing services like CloudFlare, allow firms to avoid the cost and complexity of owning and maintaining their own IT infrastructure, and instead simply pay for what they use.

**// SLIDE TWO**

* Several large firms like Udemy and Discord rely on CloudFlare for hosting its services.
* If there is a data breach from CloudFlare, what is the resulting impact of the many firms that rely on CloudFlare's cloud services?
* So point 3, cybersecurity is important -- It is pertinent to ensure that data in the cloud is secured
* Security starts at the server configuration.
* To harden system security, the Center for Internet Security, CIS has devised a standard for cybersecurity, aka the CIS Benchmarks.
* CIS Benchmarks offer guidance on how to establish a secure baseline configuration. To list a few, it checks for:
  + 1) secure configuration for hardware and software on mobile devices, workstations & servers; &
  + 2) limitation and control of network ports, protocols & services
* My bash script today will monitor the server's compliance for a small sample of the CIS requirements

**// SLIDE THREE**

So before I move on, take a second to take in this slide on examples of cybersecurity standards.

**// SLIDE FOUR**

* Moving on, I shall elaborate on the importance of CIS Benchmarks.
* CIS Benchmarks are as the name says, a set of cybersecurity benchmarks for defending IT systems and data against cyberattacks.
* CIS is referenced and recognised by compliance standards such as the Payment Card Industry Data Security Standard (PCI DSS), Federal Information Security Management Act (FISMA), and more.
* When deploying a product to a live environment, product vendors must certify that their products are secured by relevant guidelines.
* The "CIS Benchmarks Configuration Certification" is awarded to denote conformance with the CIS Benchmark.

**// SLIDE TEN**

* System accounts like syslog exist to perform system functions like logging of events.
* System accounts have an ID below 1000 and are in-built in Ubuntu systems
* System accounts have a definite level of privilege to execute commands to perform these system functions
* Ensuring system accounts are non-login makes sure that they are not being used to open shell and execute malicious commands.