

# Hackathon Soal 2 - Linux Server Hardening

Muhammad Rafif Tri Risqullah

ID: 06

Degree: S2

## Soal 2

### Creating users with sudo access (sudo group)

Implement a bash script for looping purposes creating new users from(range 1 - 100) with password and given pubkey in the /home/semesta/adm.pub

```
sevima@semesta-lab-06:~$ cat createusers.sh
#!/bin/bash

counter=1
placeholderName=sevima-adm
password=S3m3st4#2025
pubkey="/home/semesta/adm.pub"
while [ $counter -le 100 ]
do
    username="${placeholderName}${counter}"
    userhome="/home/$username"
    sudo useradd -m "$username"
    sudo usermod -aG sudo "$username"
    sudo mkdir -p "$userhome/.ssh"
    sudo chmod 700 "$userhome/.ssh"
    sudo cp /home/semesta/adm.pub $userhome/.ssh/authorized_keys
    echo "$username:$password" | sudo chpasswd
    echo "success $counter"
```

```
((counter++))  
done  
  
echo all done
```

Steps done consists of below

```
nano createusers.sh  
--coded the file + save--  
chmod +x createusers.sh  
bash createusers.sh
```

Output results

```
sevima@seimesta-lab-06:~$ bash createusers.sh  
[sudo] password for sevima:  
useradd: user 'sevima-adm1' already exists  
success 1  
useradd: user 'sevima-adm2' already exists  
success 2  
useradd: user 'sevima-adm3' already exists  
success 3  
useradd: user 'sevima-adm4' already exists  
success 4  
useradd: user 'sevima-adm5' already exists  
success 5  
useradd: user 'sevima-adm6' already exists  
success 6  
useradd: user 'sevima-adm7' already exists
```

```

sevima@seimesta-lab-06:~$ sudo ls /home
alice          sevima-adm18 sevima-adm3  sevima-adm41 sevima-adm53 sevima-adm65 sevima-adm77 sevima-adm89
seimesta      sevima-adm19 sevima-adm30 sevima-adm42 sevima-adm54 sevima-adm66 sevima-adm78 sevima-adm9
sevima        sevima-adm2  sevima-adm31 sevima-adm43 sevima-adm55 sevima-adm67 sevima-adm79 sevima-adm90
sevima-adm1   sevima-adm20 sevima-adm32 sevima-adm44 sevima-adm56 sevima-adm68 sevima-adm8  sevima-adm91
sevima-adm10  sevima-adm21 sevima-adm33 sevima-adm45 sevima-adm57 sevima-adm69 sevima-adm80 sevima-adm92
sevima-adm100 sevima-adm22 sevima-adm34 sevima-adm46 sevima-adm58 sevima-adm7  sevima-adm81 sevima-adm93
sevima-adm11  sevima-adm23 sevima-adm35 sevima-adm47 sevima-adm59 sevima-adm70 sevima-adm82 sevima-adm94
sevima-adm12  sevima-adm24 sevima-adm36 sevima-adm48 sevima-adm6  sevima-adm71 sevima-adm83 sevima-adm95
sevima-adm13  sevima-adm25 sevima-adm37 sevima-adm49 sevima-adm60 sevima-adm72 sevima-adm84 sevima-adm96
sevima-adm14  sevima-adm26 sevima-adm38 sevima-adm5  sevima-adm61 sevima-adm73 sevima-adm85 sevima-adm97
sevima-adm15  sevima-adm27 sevima-adm39 sevima-adm50 sevima-adm62 sevima-adm74 sevima-adm86 sevima-adm98
sevima-adm16  sevima-adm28 sevima-adm4  sevima-adm51 sevima-adm63 sevima-adm75 sevima-adm87 sevima-adm99
sevima-adm17  sevima-adm29 sevima-adm40 sevima-adm52 sevima-adm64 sevima-adm76 sevima-adm88

```

## Disabling password access for Root Login

Implementing PermitRootLogin prohibit-password in the /etc/ssh/sshd\_config file. In this case the sshd\_config is inheriting some values within sshd\_config.d/50-cloud-init.conf, so we need to implement some match case for root user

```
#updated sections
```

```
# Authentication:
```

```
#LoginGraceTime 2m
```

```
PermitRootLogin prohibit-password ←---
```

```
#StrictModes yes
```

```
MaxAuthTries 6
```

```
#MaxSessions 10
```

```
Match User root
```

```
    PasswordAuthentication no
```

### Steps

```
cd /etc/ssh
```

```
nano sshd_config
```

```
-- coded some stuff and save --
```

```
sudo systemctl restart ssh.service && sudo systemctl restart ssh.socket
```

### Output

```
C:\Users\zeonk>ssh root@192.168.99.16
root@192.168.99.16: Permission denied (publickey).
```

## Limiting Login Attempts (max-retry)

### A.2 Length

Password length has been found to be a primary factor in characterizing password strength [Strength] [Composition]. Passwords that are too short yield to brute force attacks as well as to dictionary attacks using words and commonly chosen passwords.

The minimum password length that should be required depends to a large extent on the threat model being addressed. Online attacks where the attacker attempts to log in by guessing the password can be mitigated by limiting the rate of **login attempts** permitted. In order to prevent an attacker (or a persistent claimant with poor typing skills) from easily inflicting a denial-of-service attack on the subscriber by making many incorrect guesses, passwords need to be complex enough that rate limiting does not occur after a modest number of erroneous attempts, but does occur before there is a significant chance of a successful guess.

Offline attacks are sometimes possible when one or more hashed passwords is obtained by the attacker through a database breach. The ability of the attacker to determine one or more users' passwords depends on the way in which the password is stored. Commonly, passwords are salted with a random value and hashed, preferably using a computationally expensive algorithm. Even with such measures, the current ability of attackers to compute many billions of hashes per second with no rate limiting requires passwords intended to resist such attacks to be orders of magnitude more complex than those that are expected to resist only online attacks.

Users should be encouraged to make their passwords as lengthy as they want, within reason. Since the size of a hashed password is independent of its length, there is no reason not to permit the use of lengthy passwords (or pass phrases) if the user wishes. Extremely long passwords (perhaps megabytes in length) could conceivably require excessive processing time to hash, so it is reasonable to have some limit.

cited from <https://pages.nist.gov/800-63-3/sp800-63b.html>

In this case I am implementing 6 attempts max in the sshd\_config file (default from the config file)

#updated sections

# Authentication:

#LoginGraceTime 2m

PermitRootLogin prohibit-password

#StrictModes yes

MaxAuthTries 6 ← ----

#MaxSessions 10

```
Match User root
    PasswordAuthentication no
```

## Steps

```
cd /etc/ssh
nano sshd_config
-- coded some stuff and save --
sudo systemctl restart ssh.service && sudo systemctl restart ssh.socket
```

## Output

```
C:\Users\zeonk>ssh sevima-adm1@192.168.99.16
sevima-adm1@192.168.99.16's password:
Permission denied, please try again.
sevima-adm1@192.168.99.16's password:
Permission denied, please try again.
sevima-adm1@192.168.99.16's password:
sevima-adm1@192.168.99.16: Permission denied (publickey,password).
```

## /var/log/auth.log

```
2025-07-19T06:36:11.228582+00:00 hachathon-lab-main sudo: pam_unix(sudo:
2025-07-19T06:36:18.544013+00:00 hachathon-lab-main sshd[18703]: Failed p
2025-07-19T06:36:20.347378+00:00 hachathon-lab-main sshd[18703]: messag
2025-07-19T06:36:20.372880+00:00 hachathon-lab-main sshd[18703]: Connec
```

## Enabling firewall

### Step

```
sudo ufw status
sudo ufw enable
sudo ufw allow 22/tcp ← current server purpose only for SSH. Not needed for
```

Output

```
sevima@semesta-lab-06:~$ sudo ufw status
Status: active

To Action From
--
22/tcp ALLOW Anywhere
22/tcp (v6) ALLOW Anywhere (v6)
```

## LVM setup from block storage sdb with encryption enabled

using LUKS - Linux Unified Key Setup for disk encryption.

Step

```
lsblk
sudo cryptsetup luksFormat /dev/sdb
sudo cryptsetup luksDump /dev/sdb
sudo cryptsetup luksOpen /dev/sdb encrypted
sudo dmsetup info encrypted # info for the encrypted LUKS part
sudo pvcreate /dev/mapper/encrypted # physical volume creation
sudo vgcreate hackathon-syadm7 /dev/mapper/encrypted # volume group creat
sudo lvcreate -L 1.5G -n nfs-hackathon-syadm7 hackathon-syadm7 # logical vol
sudo mkfs.ext4 /dev/hackathon-syadm7/nfs-hackathon-syadm7 # format to ext4
sudo lvdisplay /dev/hackathon-syadm7/nfs-hackathon-syadm7 # lv info
cd /mnt && sudo mkdir nfs-hackathon
sudo apt update && sudo apt install nfs-common -y
sudo mount -t nfs 192.168.99.3:nfs-semesta7 /mnt/nfs-hackathon # mount the nf
df -h /mnt/nfs-hackathon
```

## Auto Mounting on Boot

Step

```
# auto change to encrypted (/dev/sdb) on boot
echo "encrypted /dev/sdb none luks,discard" | sudo tee -a /etc/crypttab

# auto add nfs to lvm after the crypttab action
# -- use netdev flag to wait for network conn
echo "192.168.99.3:nfs-semesta7 /mnt/nfs-hackathon nfs defaults,_netdev 0 0" \
| sudo tee -a /etc/fstab
```

## Create Folder with name-IP on the mnt/nfs

```
cd /mnt/nfs-hackathon
mkdir MuhammadRafifTriRisqullah-192.168.99.16
```

### Output

```
sevima@semesta-lab-06:/mnt$ sudo mount -t nfs 192.168.99.3:nfs-semesta7 /mnt/nfs-hackathon
sevima@semesta-lab-06:/mnt$ cd nfs-hackathon/
sevima@semesta-lab-06:/mnt/nfs-hackathon$ df -h
Filesystem                Size      Used Avail Use% Mounted on
tmpfs                    392M    1.1M   391M   1% /run
/dev/mapper/ubuntu--vg-ubuntu--lv  24G    7.0G    16G  32% /
tmpfs                    2.0G         0  2.0G   0% /dev/shm
tmpfs                    5.0M         0  5.0M   0% /run/lock
/dev/sda2                 2.0G   100M    1.7G   6% /boot
tmpfs                    392M    12K   392M   1% /run/user/1000
192.168.99.3:/nfs-semesta7  24G    6.4G    16G  29% /mnt/nfs-hackathon
sevima@semesta-lab-06:/mnt/nfs-hackathon$ df -h /mnt/nfs-hackathon
Filesystem                Size      Used Avail Use% Mounted on
192.168.99.3:/nfs-semesta7  24G    6.4G    16G  29% /mnt/nfs-hackathon
sevima@semesta-lab-06:/mnt/nfs-hackathon$ ls
achmadalifnasrulloh-192.168.99.11 test1
sevima@semesta-lab-06:/mnt/nfs-hackathon$ cd achmadalifnasrulloh-192.168.99.11/
sevima@semesta-lab-06:/mnt/nfs-hackathon/achmadalifnasrulloh-192.168.99.11$ ls
sevima@semesta-lab-06:/mnt/nfs-hackathon/achmadalifnasrulloh-192.168.99.11$ cd ..
sevima@semesta-lab-06:/mnt/nfs-hackathon$ cat test1
sevima@semesta-lab-06:/mnt/nfs-hackathon$
```

### LV info

```

sevima@semesta-lab-06:~$ sudo lvdisplay /dev/hackathon-syadm7/nfs-hackathon-syadm7
--- Logical volume ---
LV Path                /dev/hackathon-syadm7/nfs-hackathon-syadm7
LV Name                 nfs-hackathon-syadm7
VG Name                 hackathon-syadm7
LV UUID                 S7l070-VnEG-5s2e-mNSF-uLrN-6Sgq-1lrseN
LV Write Access         read/write
LV Creation host, time  semesta-lab-06, 2025-07-19 07:23:35 +0000
LV Status                available
# open                  0
LV Size                 1.50 GiB
Current LE              384
Segments                1
Allocation               inherit
Read ahead sectors      auto
 - currently set to     256
Block device            252:2

```

## lsblk result

NAME	MAJ:MIN	RM	SIZE	RO	TYPE	MOUNTPOINTS
sda	8:0	0	50G	0	disk	
└sda1	8:1	0	1M	0	part	
└sda2	8:2	0	2G	0	part	/boot
└sda3	8:3	0	48G	0	part	
└└ubuntu--vg-ubuntu--lv	252:0	0	24G	0	lvm	/
sdb	8:16	0	2G	0	disk	
└encrypted	252:1	0	2G	0	crypt	
└└hackathon--syadm7-nfs--hackathon--syadm7	252:2	0	1.5G	0	lvm	
sdc	8:32	0	2G	0	disk	
sr0	11:0	1	3G	0	rom	