Born2beRoot - Complete Defense Guide

# Tips

✦ Tips by Mohammad Alhendi (malhendi @ 42)  
  
- Focus on understanding, not just memorizing.  
- During the defense, explain concepts in your own words.  
- Practice the commands regularly so you don't freeze.  
- Always verify your setup before evaluation (firewall, SSH, users, partitions).  
- Remember: the goal is learning system administration basics, not only passing.

# Introduction

Born2beRoot is a system administration project designed to introduce virtualization, basic Linux server configuration, and security practices. You will create and configure a VM (Debian or Rocky), implement strict rules, and defend your work during evaluation.

# Subject Requirements

## System Choice

You must install either Debian (recommended) or Rocky Linux (more complex). AppArmor must run on Debian, SELinux must run on Rocky.

## Partitioning & LVM

You must create at least 2 encrypted partitions using LVM during installation. Commands to inspect:  
lsblk  
sudo pvs  
sudo vgs  
sudo lvs

## SSH Setup

SSH must be running on port 4242. Root login must be disabled.  
Config file: /etc/ssh/sshd\_config  
→ Port 4242  
→ PermitRootLogin no  
  
Check: sudo systemctl status ssh  
Connect: ssh user@127.0.0.1 -p 4242

## Firewall

Debian: use ufw. Rocky: use firewalld.  
Commands:  
sudo ufw enable  
sudo ufw allow 4242/tcp  
sudo ufw status

## Users & Groups

Create a user with your login, assign to sudo and user42 groups.  
sudo adduser <username>  
sudo usermod -aG sudo,user42 <username>  
groups <username>  
  
During evaluation: create a group 'evaluating' and add a user to it.

## Password Policy

/etc/login.defs:  
PASS\_MAX\_DAYS 30  
PASS\_MIN\_DAYS 2  
PASS\_WARN\_AGE 7  
  
/etc/pam.d/common-password:  
password requisite pam\_pwquality.so retry=3 minlen=10 ucredit=-1 dcredit=-1 maxrepeat=3 reject\_username difok=7  
  
Test: chage -l <username>

## Sudo Rules

In /etc/sudoers (visudo):  
Defaults passwd\_tries=3  
Defaults badpass\_message="Custom Message"  
Defaults logfile="/var/log/sudo/sudo.log"  
Defaults requiretty  
Defaults secure\_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"  
  
Check logs in /var/log/sudo/ after running sudo commands.

## Monitoring Script

File: /usr/local/bin/monitoring.sh  
Must display every 10 minutes via wall or cron.  
  
Info required:  
- Architecture & kernel  
- CPU (physical & virtual)  
- RAM usage  
- Disk usage  
- CPU load  
- Last boot  
- LVM active?  
- Active connections  
- Logged users  
- IPv4 & MAC  
- Number of sudo commands  
  
Use crontab:  
\*/10 \* \* \* \* /usr/local/bin/monitoring.sh

# Evaluation Questions & Answers

## How does a VM work?

A VM is a software-based emulation of a computer. The hypervisor allocates CPU, RAM, and disk from the host machine. This allows multiple isolated OS instances to run on one hardware.

## Why Debian or Rocky?

Debian: stable, easier, AppArmor.  
Rocky: RHEL clone, enterprise, SELinux, more complex.

## Differences between Debian and Rocky?

Debian uses apt, AppArmor, large community.  
Rocky uses dnf, SELinux, enterprise support.

## Purpose of VMs

Isolation, testing, multiple OS on one hardware, efficient resource usage.

## SELinux & DNF (Rocky)

SELinux: Mandatory Access Control framework.  
DNF: package manager (successor of YUM).

## Aptitude vs APT & AppArmor (Debian)

APT: normal package manager.  
Aptitude: interactive with better dependency resolution.  
AppArmor: security profiles restricting apps (Mandatory Access Control).

## Hostname & Partitions

hostnamectl set-hostname login42  
lsblk to view partitions.  
LVM explained as: PV (disk), VG (group of PVs), LV (logical partition).

## Sudo Value & Rules

Sudo allows executing commands with root privileges securely. Rules: attempts, logs, tty, path.

## Firewall Value & Commands

Firewall controls access to ports/services. Use ufw (Debian) or firewalld (Rocky).

## SSH Value & Config

SSH provides secure remote login. Configured on port 4242, root login disabled.

## Monitoring Script & Cron

Script gathers system info. Cron schedules it every 10 min.  
Explain cron syntax: \*/10 \* \* \* \*

## Password Policy Pros/Cons

Pros: strong security, prevents weak/reused passwords.  
Cons: users may forget passwords, slight inconvenience.

# Essential Commands Reference

## Update package list

sudo apt-get update -y

## Install sudo

sudo apt install sudo

## Edit sudoers file

visudo

## Add user

sudo adduser <username>

## Add user to groups

sudo usermod -aG sudo,user42 <username>

## Check groups

groups <username>

## Check password aging

chage -l <username>

## Enable firewall

sudo ufw enable

## Allow port 4242

sudo ufw allow 4242/tcp

## Check firewall status

sudo ufw status

## Check SSH service

sudo systemctl status ssh

## Restart SSH

sudo service ssh restart

## Connect via SSH

ssh user@127.0.0.1 -p 4242

## Change hostname

sudo hostnamectl set-hostname login42

## Show partitions

lsblk

## Show sudo logs

cat /var/log/sudo/sudo.log

# Extra Notes

File Systems: ext4 (default), btrfs (snapshots), XFS (large files).  
RAID: RAID0 (performance), RAID1 (redundancy), RAID5 (balanced), RAID10 (perf + redundancy).  
LVM: PV = disk, VG = group, LV = logical volume.  
Security: SELinux (labels), AppArmor (profiles).  
Networking: Host vs Guest ports, NAT, SSH encryption.