https://42-cursus.gitbook.io/guide/rank-01/born2beroot/p2p-evaluation-questions

1. Configurazione del Server

- **Sistema Operativo**: Devi aver installato una distribuzione Linux (es. Debian o CentOS) su una macchina virtuale (es. VirtualBox, VMware).
- **Partizionamento del Disco**: Devi aver configurato il partizionamento del disco secondo le specifiche del progetto (es. partizione root, swap, home, ecc.).
- **Accesso SSH**: Devi aver configurato l'accesso SSH per connettersi al server in modo sicuro.

---

2. Politiche di Sicurezza

- **Password Policy**:
  - Configurare una politica di scadenza password (es. ogni 30 giorni).
  - Impostare una lunghezza minima per le password (es. 10 caratteri).
  - Richiedere che le password contengano almeno un carattere maiuscolo, uno minuscolo, un numero e un carattere speciale.
  - Impostare un numero massimo di tentativi di accesso falliti prima di bloccare l'account.
- **Sudoers**:
  - Configurare il file /etc/sudoers per limitare i comandi che gli utenti possono eseguire con sudo.
  - Creare un gruppo di utenti con privilegi sudo.

- **Firewall (UFW)**:
    - Configurare un firewall per permettere solo le connessioni necessarie (es. SSH, HTTP, HTTPS).
    - Bloccare tutte le altre porte.
- **Fail2Ban**:
    - Installare e configurare Fail2Ban per prevenire attacchi brute force (es. bloccare IP dopo un certo numero di tentativi falliti).

---

3. Gestione degli Utenti e dei Gruppi

- Creare utenti e gruppi specifici.
- Assegnare password sicure agli utenti.
- Configurare i permessi e le restrizioni per gli utenti.

---

4. Monitoraggio del Sistema

- **Cron Job**:
    - Configurare uno script che viene eseguito periodicamente (es. ogni 10 minuti) per monitorare lo stato del server.
    - Lo script deve mostrare informazioni come l'uso della RAM, della CPU, dello spazio su disco, ecc.
    - Lo script deve salvare il risultato in un file di log.
- **Gestione dei Log**:
    - Configurare il sistema per mantenere i log (es. /var/log/syslog).
    - Assicurarsi che i log vengano ruotati per evitare che occupino troppo spazio.

---

5. Conoscenze Tecniche Richieste

- **Comandi Linux**:
    - Devi essere in grado di usare comandi
      come ls, cd, chmod, chown, useradd, groupadd, crontab, ufw, s
      sh, sudo, fail2ban, ecc.
- **Scripting Bash**:
    - Devi saper scrivere script Bash per automatizzare compiti (es. monitoraggio del sistema).
- **Gestione dei Permessi**:
    - Devi comprendere i permessi dei file (es. chmod 755) e come gestirli.
- **Configurazione di Rete**:
    - Devi saper configurare indirizzi IP, DNS e altre impostazioni di rete.

---

6. Domande Frequenti durante la P2P Evaluation

Durante la correzione, ti verranno poste domande per verificare la tua comprensione del sistema. Ecco alcuni esempi:

- Come hai configurato la politica delle password?
- Come funziona il firewall che hai impostato?
- Cosa fa lo script di monitoraggio che hai creato?
- Come gestisci i log del sistema?
- Quali sono i vantaggi di usare Fail2Ban?

---

7. Errori Comuni da Evitare

- Non aver configurato correttamente la politica delle password.
- Non aver limitato l'accesso SSH solo agli utenti autorizzati.

- Non aver configurato correttamente il firewall.
- Non aver testato lo script di monitoraggio prima della correzione.

---

8. Preparazione per la Correzione

- **Testa tutto**: Assicurati che tutte le configurazioni funzionino correttamente prima della correzione.
- **Documenta**: Prendi appunti su come hai configurato il sistema, in modo da poter rispondere alle domande durante la correzione.
- **Simula una Correzione**: Fai pratica con un amico o un collega per simulare la P2P Evaluation.

Mandatory part

The project consists of creating and configuring a virtual machine following strict rules. The student being evaluated will have to help you during the defense. Make sure that all of the following points are observed.

Project overview

- The student being evaluated should explain to you simply:
  - How a virtual machine works.
  - Their choice of operating system.
  - The basic differences between Rocky and Debian.
  - The purpose of virtual machines.
  - If the evaluated student chose Rocky: what SELinux and DNF are.
  - If the evaluated student chose Debian: the difference between aptitude and apt, and what APPArmor is. During the defense, a script must display information all every 10 minutes. Its operation will be checked in detail later. If the explanations are not clear, the evaluation stops here.

Yes | No

Simple setup

Remember: Whenever you need help checking something, the student being evaluated should be able to help you.

- Ensure that the machine does not have a graphical environment at launch. A password will be requested before attempting to connect to this machine. Finally, connect with a user with the help of the student being evaluated. This user must not be root. Pay attention to the password chosen, it must follow the rules imposed in the subject.
- Check that the UFW service is started with the help of the student being evaluated.
- Check that the SSH service is started with the help of the student being evaluated.
- Check that the chosen operating system is Debian or Rocky with the help of the student being evaluated. If something does not work as expected or is not clearly explained, the evaluation stops here.

UFW / Firewalld

Remember: Whenever you need help checking something, the student being evaluated should be able to help you.

- Check that the "UFW" (or "Firewalld" for rocky) program is properly installed on the virtual machine.
- Check that it is working properly.
- The student being evaluated should explain to you basically what UFW (or Firewalld) is and the value of using it.
- List the active rules in UFW (or Firewalld). A rule must exist for port 4242.
- Add a new rule to open port 8080. Check that this one has been added by listing the active rules.
- Finally, delete this new rule with the help of the student being evaluated. If something does not work as expected or is not clearly explained, the evaluation stops here.

Yes | No

SSH

Remember: Whenever you need help checking something, the student being evaluated should be able to help you.

- Check that the SSH service is properly installed on the virtual machine.
- Check that it is working properly.
- The student being evaluated must be able to explain to you basically what SSH is and the value of using it.
- Verify that the SSH service only uses port 4242 in the virtual machine.
- The student being evaluated should help you use SSH in order to log in with the newly created user. To do this, you can use a key or a simple password. It will depend on the student being evaluated. Of course, you have to make sure that you cannot use SSH with the "root" user as stated in the subject. If something does not work as expected or is not clearly explained, the evaluation stops here.

Yes | No

Script monitoring

Remember: Whenever you need help checking something, the student being evaluated should be able to help you.

The student being evaluated should explain to you simply:

- How their script works by showing you the code.
- What "cron" is.
- How the student being evaluated set up their script so that it runs every 10 minutes from when the server starts. Once the correct functioning of the script has been verified, the student being evaluated should ensure that this script runs every minute. You can run whatever you want to make sure the script runs with dynamic values correctly. Finally, the student being evaluated should make the script stop running when the server has started up, but without modifying the script itself. To check this point, you will have to restart the server one last time. At startup, it will be necessary to check that the script still exists in the same place, that its rights have remained unchanged, and that it has not been modified. If something does not work as expected or is not clearly explained, the evaluation stops here.

Yes | No

Bonus

Evaluate the bonus part if, and only if, the mandatory part has been entirely and perfectly done, and the error management handles unexpected or bad usage. In case all the mandatory points were not passed during the defense, bonus points must be totally ignored.

Bonus

Check, with the help of the subject and the student being evaluated, the bonus points authorized for this project:

- Setting up partitions is worth 2 points.
- Setting up WordPress, only with the services required by the subject, is worth 2 points.
- The free choice service is worth 1 point. Verify and test the proper functioning and implementation of each extra service. For the free choice service, the student being evaluated has to give you a simple explanation about how it works and why they think it is useful. Please note that NGINX and Apache2 are prohibited.

User

Remember: Whenever you need help checking something, the student being evaluated should be able to help you.

The subject requests that a user with the login of the student being evaluated is present on the virtual machine. Check that it has been added and that it belongs to the "sudo" and "user42" groups.

Make sure the rules imposed in the subject concerning the password policy have been put in place by following the following steps.

First, create a new user. Assign it a password of your choice, respecting the subject rules. The student being evaluated must now explain to you how they were able to set up the rules requested in the subject on their virtual machine.
Normally there should be one or two modified files. If there is any problem, the evaluation stops here.

- Now that you have a new user, ask the student being evaluated to create a group named "evaluating" in
  front of you and assign it to this user. Finally, check that this user belongs to the "evaluating" group.
- Finally, ask the student being evaluated to explain the advantages of this password policy, as well as the
  advantages and disadvantages of its implementation. Of course, answering that it is because the subject asks
  for it does not count.

If something does not work as expected or is not clearly explained, the evaluation stops here.

Yes | No

Hostname and partitions

Remember: Whenever you need help checking something, the student being evaluated should be able to help you.

- Check that the hostname of the machine is correctly formatted as follows: login42 (login of the student being evaluated).
- Modify this hostname by replacing the login with yours, then restart the machine. If on restart, the hostname has not been updated, the evaluation stops here.
- You can now restore the machine to the original hostname.
- Ask the student being evaluated how to view the partitions for this virtual machine.
- Compare the output with the example given in the subject. Please note: if the student evaluated makes the bonuses, it will be necessary to refer to the bonus example.

This part is an opportunity to discuss the scores! The student being evaluated should

Hostname and partitions

Remember: Whenever you need help checking something, the student being evaluated should be able to help you.

- Check that the hostname of the machine is correctly formatted as follows: login42 (login of the student being evaluated).
- Modify this hostname by replacing the login with yours, then restart the machine. If on restart, the hostname has not been updated, the evaluation stops here.
- You can now restore the machine to the original hostname.
- Ask the student being evaluated how to view the partitions for this virtual machine.
- Compare the output with the example given in the subject. Please note: if the student evaluated makes the bonuses, it will be necessary to refer to the bonus example.

This part is an opportunity to discuss the scores! The student being evaluated should give you a brief explanation of how LVM works and what it is all about.
If something does not work as expected or is not clearly explained, the evaluation stops here.

Yes | No

SUDO

Remember: Whenever you need help checking something, the student being evaluated should be able to help you.

- Check that the "sudo" program is properly installed on the virtual machine.
- The student being evaluated should now show assigning your new user to the "sudo" group.
- The subject imposes strict rules for sudo. The student being evaluated must first explain the value and operation of sudo using examples of their choice. In a second step, it must show you the implementation of the rules imposed by the subject.
- Verify that the "/var/log/sudo/" folder exists and has at least one file. Check the contents of the files in this folder, You should see a history of the commands used with sudo. Finally, try to run a command via sudo. See if the file (s) in the "/var/log/sudo/" folder have been updated. If something does not work as expected or is not clearly explained, the evaluation stops here.

Yes | No