**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, ssh, 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.

