

Administrarea sigură a unui mediu Linux

Fișă publică de proiect · exerciții și criterii de acceptare

Înveți inspectia utilizatorilor, permisiunilor și serviciilor înainte de modificare. Exercițiile care schimbă sistemul se fac într-o mașină de test.

Livrabile

- Fișă de comenzi
- Hartă de permisiuni
- Diagnostic serviciu
- Plan SSH

Criterii de acceptare

- Ținta și utilizatorul sunt confirmați
- Secretele au acces restrictiv
- Există o cale de administrare funcțională

Terminal de laborator cu observarea directorului curent

O comandă se execută într-un context: utilizator, director și variabile de mediu. Începe prin a le observa înainte de modificări. Lucrează într-un director creat pentru exercițiu și nu folosi sudo când nu este necesar. Ieșirea unei comenzi și codul ei de terminare sunt indicii distincte. Un mesaj afișat nu dovedește succesul dacă operația a întors un cod de eroare. Comenzile sunt pentru un shell Linux.

Exemplu de lucru

```
whoami
pwd
mkdir -p ~/laborator-linux
cd ~/laborator-linux
printf 'linie demo
' > nota.txt
cat nota.txt
ls -l nota.txt
# După o comandă, verifică imediat codul cu: echo $?
```

Interpretarea rezultatului

Directorul de lucru trebuie să fie laborator-linux. Redirecționarea > suprascrie fișierul dacă există, de aceea nu o folosi pe o cale necunoscută. Exercițiul nu cere ștergeri sau acces de administrator. Pe PowerShell, sintaxa și cmdleturile pot fi diferite.

Exercițiu de consolidare

Rulează o comandă de citire pe un fișier inexistent și compară mesajul cu codul de ieșire.

1. Terminalul, fără frică

Rulează o comandă de citire pe un fișier inexistent și compară mesajul cu codul de ieșire.

Verificare orientativă

Directorul de lucru trebuie să fie `laborator-linux`. Redirecționarea `>` suprascrie fișierul dacă există, de aceea nu o folosi pe o cale necunoscută. Exercițiul nu cere ștergeri sau acces de administrator. Pe PowerShell, sintaxa și cmdleturile pot fi diferite.

De evitat

O comandă copiată nu trebuie executată fără înțelegerea țintei.

Căi relative, absolute și fișiere ascunse

Calea relativă depinde de directorul curent, iar cea absolută pornește de la rădăcină. Numele care încep cu punct sunt ascunse de afișarea obișnuită, dar nu sunt protejate prin acest fapt. Înainte de copiere, verifică sursa și destinația. Ghilimelele păstrează un nume cu spații ca un singur argument. Nu construi operații recursive pe căi calculate fără a confirma domeniul laboratorului.

Exemplu de lucru

```
cd ~/laborator-linux
mkdir -p documente copii
printf 'demo
' > 'documente/nota de lucru.txt'
cp -- 'documente/nota de lucru.txt' 'copii/nota de lucru.txt'
ls -la documente copii
realpath 'copii/nota de lucru.txt'
# Citește ambele fișiere și compară înainte de alte operații.
```

Interpretarea rezultatului

`cp` creează o copie, iar schimbarea ei nu ar trebui să modifice originalul obișnuit. Linkurile simbolice au alt comportament și trebuie identificate separat. Nu presupune că un fișier `.env` este sigur doar fiindcă nu apare la `ls` fără `-a`.

Exercițiu de consolidare

Creează un nume cu spații și diacritice și verifică citirea lui folosind ghilimele.

2. Fișiere și directoare

Creează un nume cu spații și diacritice și verifică citirea lui folosind ghilimele.

Verificare orientativă

`cp` creează o copie, iar schimbarea ei nu ar trebui să modifice originalul obișnuit. Linkurile simbolice au alt comportament și trebuie identificate separat. Nu presupune că un fișier `.env` este sigur doar fiindcă nu apare la `ls` fără `-a`.

De evitat

O cale relativă depinde de directorul curent.

Permisiuni interpretate pentru proprietar, grup și ceilalți

Permisiunile rwx au sens diferit pentru fișiere și directoare: execuția pe director permite traversarea. Nu folosi `chmod 777` ca remediu general pentru o eroare. Identifică utilizatorul procesului și accesul minim necesar. Pentru un fișier privat de laborator, 600 permite citire și scriere proprietarului. Grupurile pot fi folosite pentru acces controlat, dar trebuie verificate și directoarele părinte.

Exemplu de lucru

```
cd ~/laborator-linux
printf 'configurație fictivă
' > privat.txt
chmod 600 privat.txt
ls -l privat.txt
stat privat.txt
id
# Pentru directoare private, evaluează traversarea și accesul pe întregul traseu.
```

Interpretarea rezultatului

Un fișier 600 într-un director public nu devine automat accesibil procesului web; contează identitatea procesului. Invers, un server poate expune date dacă rulează cu un utilizator prea privilegiat. Nu modifica proprietari pe directoare de sistem pentru a rezolva un laborator.

Exercițiu de consolidare

Explică diferența dintre 640 pe fișier și 750 pe director și în ce situație un grup controlat poate citi fișierul.

3. Permisiuni și utilizatori

Explică diferența dintre 640 pe fișier și 750 pe director și în ce situație un grup controlat poate citi fișierul.

Verificare orientativă

Un fișier 600 într-un director public nu devine automat accesibil procesului web; contează identitatea procesului. Invers, un server poate expune date dacă rulează cu un utilizator prea privilegiat. Nu modifica proprietari pe directoare de sistem pentru a rezolva un laborator.

De evitat

`chmod 777` nu este o soluție pentru erori de acces.

Proces și serviciu observate înainte de restart

Un proces este o execuție, iar un serviciu este gestionat de un mecanism precum `systemd`. Înainte de restart, citește statusul și logurile pentru a înțelege cauza. Un restart poate ascunde temporar un defect și poate întrerupe utilizatori. Pentru laborator, folosește întâi comenzi de observare. Numele serviciilor diferă după distribuție și instalare; nu presupune că `php-fpm` are aceeași unitate peste tot.

Exemplu de lucru

```
ps -ef
systemctl status nginx --no-pager
journalctl -u nginx -n 50 --no-pager
ss -lnt
# Verifică utilizatorul, PID-ul, portul și mesajul de eroare.
# Unitatea poate lipsi dacă nginx nu este instalat în laborator.
```

Interpretarea rezultatului

Un serviciu active nu dovedește că aplicația răspunde corect; trebuie verificată și o cerere HTTP. Un port ascultat nu spune singur ce aplicație livrează conținutul. Nu publica loguri care conțin tokenuri sau date private când ceri ajutor.

Exercițiu de consolidare

Describe două cauze pentru un serviciu activ care răspunde cu 502 și ce informație ai verifica înainte de restart.

4. Procese și servicii

Describe două cauze pentru un serviciu activ care răspunde cu 502 și ce informație ai verifica înainte de restart.

Verificare orientativă

Un serviciu active nu dovedește că aplicația răspunde corect; trebuie verificată și o cerere HTTP. Un port ascultat nu spune singur ce aplicație livrează conținutul. Nu publica loguri care conțin tokenuri sau date private când ceri ajutor.

De evitat

Restart-ul fără diagnostic poate ascunde cauza.

Actualizări cu inventar și plan de compatibilitate

Managerul de pachete gestionează software-ul distribuției, dar un update poate schimba comportamentul serviciilor. Înainte de actualizare, verifică versiunea curentă, pachetele disponibile și necesitatea unui backup sau a unei ferestre de mentenanță. Nu rula upgrade-uri majore direct pe un server critic fără test. Dependențele aplicației instalate cu Composer sau npm au un ciclu separat și nu sunt toate rezolvate prin apt.

Exemplu de lucru

Ubuntu/Debian, observare:

```
apt list --upgradable  
apt-cache policy nginx  
php --version  
nginx -v
```

Plan: inventar → backup → test pe copie → actualizare → verificare funcțională → monitorizare.

Nu combina: upgrade de OS, PHP și aplicație într-o singură schimbare fără diagnostic separat.

Interpretarea rezultatului

Lista de actualizări nu autorizează automat aplicarea lor într-un laborator partajat. Verifică documentația distribuției și changelogul pentru schimbări relevante. După actualizare, testează traseele importante ale aplicației, nu doar versiunea afișată.

Exercițiu de consolidare

Construiește o listă de verificare pentru un update PHP care include extensiile și compatibilitatea Composer.

5. Pachete și update-uri

Construiește o listă de verificare pentru un update PHP care include extensiile și compatibilitatea Composer.

Verificare orientativă

Lista de actualizări nu autorizează automat aplicarea lor într-un laborator partajat. Verifică documentația distribuției și changelogul pentru schimbări relevante. După actualizare, testează traseele importante ale aplicației, nu doar versiunea afișată.

De evitat

Actualizarea poate modifica servicii folosite de aplicație.

Chei SSH și verificarea gazdei

Cheia privată rămâne pe client, iar cheia publică poate fi adăugată contului autorizat de pe server. Verificarea cheii gazdei previne conectarea neobservată la alt server. Nu dezactivează StrictHostKeyChecking ca soluție de rutină și nu copia cheia privată într-un chat. Pentru laborator, generează o cheie dedicată și protejează-o cu parolă când fluxul permite. Accesul serverului trebuie limitat la utilizatorul și scopul necesar.

Exemplu de lucru

```
ssh-keygen -t ed25519 -f ~/.ssh/laborator_ed25519
ssh -i ~/.ssh/laborator_ed25519 utilizator@server-autorizat
Pe server: verifică whoami și hostname.
Fișier public: laborator_ed25519.pub.
Fișier privat: laborator_ed25519, nu se distribuie.
Fingerprint gazdă: confirmare pe un canal de încredere înainte de acceptare.
```

Interpretarea rezultatului

Un whoami corect confirmă utilizatorul sesiunii, nu faptul că toate permisiunile sunt potrivite. Verifică și identitatea gazdei. Pentru automatizări, folosește o cheie și un cont cu drepturi limitate, nu acces general root dacă nu este necesar.

Exercițiu de consolidare

Describe ce faci când fingerprintul gazdei se schimbă și de ce nu ștergi automat avertizarea.

6. SSH și chei

Describe ce faci când fingerprintul gazdei se schimbă și de ce nu ștergi automat avertizarea.

Verificare orientativă

Un whoami corect confirmă utilizatorul sesiunii, nu faptul că toate permisiunile sunt potrivite. Verifică și identitatea gazdei. Pentru automatizări, folosește o cheie și un cont cu drepturi limitate, nu acces general root dacă nu este necesar.

De evitat

Nu copia cheia privată pe server sau în chat.

Atelier final: Diagnostic Linux înainte de schimbare

Timp de lucru estimat: 40 de minute. Folosește datele de laborator de mai jos și salvează rezultatul separat de orice proiect real.

Date de pornire

Mașină virtuală de test: un serviciu nu poate citi configul, iar portul așteptat nu răspunde. Ai utilizator administrativ autorizat și o copie a configurației.

1. Pregătire — 5 minute

Extrage intrările și condițiile din enunț. Notează ce rezultat trebuie produs și ce informații nu sunt confirmate. Pregătește fișierele sau tabelul în care vei păstra dovada lucrului.

2. Construire — 15 minute

Notează identitatea, permisiunile, starea serviciului și jurnalul relevant. Formulează o ipoteză, apoi schimbă numai permisiunea sau configurația justificată de dovezi.

3. Variație și verificare — 15 minute

Simulează separat un port greșit în configurație. Explică de ce aceeași simptomatologie nu justifică aceeași remediare.

4. Autoevaluare — 5 minute

Compară rezultatul cu reperele de mai jos. Înregistrează cel puțin o eroare identificată sau un caz-limită verificat, plus corectura ori explicația comportamentului observat.

Repere de rezolvare

Raportul identifică proprietarul și drepturile necesare. Soluția nu este `chmod 777` și nu dezactivează protecții globale. După schimbare se verifică serviciul și accesul la fișier.

Ce predai

- Fișă de comenzi
- Hartă de permisiuni
- Diagnostic serviciu
- Plan SSH

Criterii de acceptare

- Ținta și utilizatorul sunt confirmați
- Secretele au acces restrictiv
- Există o cale de administrare funcțională

Păstrează o versiune inițială și una revizuită, cu explicația diferențelor. Dacă un criteriu nu este îndeplinit, revino la lecția relevantă și repetă verificarea. Durata este orientativă; instalarea mediului și aprofundarea pot necesita timp suplimentar.

Registrul de lucru

Pentru fiecare etapă notează intrarea, rezultatul, dovada verificării, eroarea găsită și corectura. Nu introduce date personale sau secrete în fișa partajată.

Documentație și surse

- Ubuntu Server documentation — Canonical

<https://documentation.ubuntu.com/server/>