LINUX RENDSZERFEJLESZTÉS ÉS ÜZEMELTETÉS

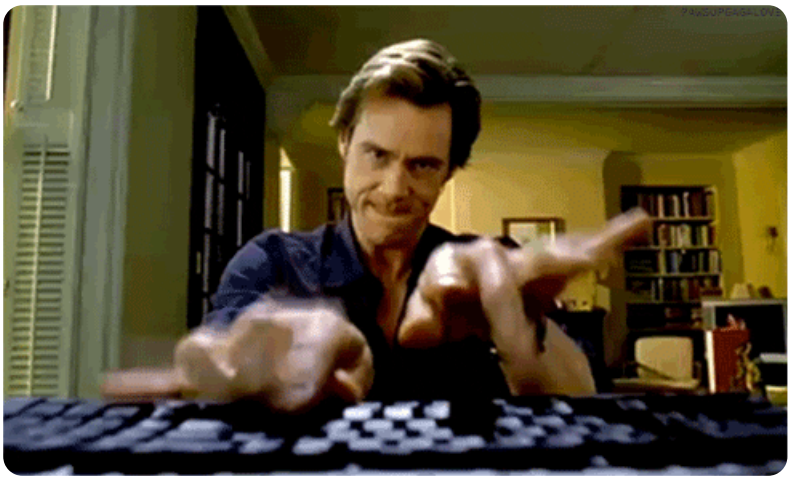
6. forduló

A kategória támogatója: One Identity - Quest Hungary

Ismertető a feladatlaphoz

> Kezdj neki minél hamarabb, mert a feladatot a forduló záró időpontjáig lehet beküldeni, nem addig lehet elkezdeni!

Sok sikert!



1. feladat 1 pont

Egy Linux operációs rendszeren az alábbi PAM konfiguráció van.

```
auth    [success=2 default=ignore]                                  pam_unix.s
auth    [success=ok new_authtok_reqd=ok ignore=ignore default=die]  pam_deny.s
auth    [success=ok new_authtok_reqd=ok ignore=ignore default=bad]  pam_permit
auth    optional                        pam_cap.so
```

Sikeres lesz-e az auth szekció, ha a pam_unix.so sikeres, a pam_deny.so visszerérése "abort" és a pam_permit.so visszatérési értéke "perm_denied"

Válasz

- [ ] igen
- [ ] nem
- [ ] igen, de csak akkor, ha a pam_cap.so modul visszatérése "success"

2. feladat 1 pont

Az alábbi formátumú Apache access naplókból szeretnénk összeszámolni a HTTP kéréseket státusz kódok alapján csoportosítva.

```
5.2.202.156 - - [04/Oct/2023:11:34:14 +0200] "POST /wp-admin/admin-ajax.php HTTP/1
188.173.150.28 - - [04/Oct/2023:11:34:14 +0200] "POST /wp-admin/admin-ajax.php HTT
86.120.101.142 - - [04/Oct/2023:11:34:14 +0200] "POST /wp-admin/admin-ajax.php HTT
```

Melyik a helyes parancssor?

Válaszok

- [ ] `cat /var/log/httpd/access_log | perl -lne 'print $1 if /^.*"\s([0-9]{3}).*$/'`
- [ ] `cat /var/log/httpd/access_log | perl -lne 'print $1 if /^(?:[0-9]{1,3}\.){3}[0`
- [ ] `cat /var/log/httpd/access_log | perl -lne 'print if /^.*"\s([0-9]{3}).*$/' | s`
- [ ] `cat /var/log/httpd/access_log | perl -lne 'print $1 if /^(?:[0-9]{1,3}\.){3}[0`

3. feladat 1 pont

Melyik audit rule rögzíti a /srv/app/etc/config fájl nem jogosult olvasási hozzáférés próbálkozását?

Válaszok

- [ ] auditctl -a always,exit -F arch=b64 -S open -S openat -F path=/srv/app/etc/config -F exit=-EACCES -k file-open
- [ ] auditctl -a always,exit -F arch=b64 -S open -S openat -F path=/srv/app/etc/config -F exit=-EPERM -k file-open
- [ ] auditctl -w /srv/app/etc/config

4. feladat 1 pont

Hogyan lehet beállítani az SPF (Sender Policy Framework) rekordot egy domainhez, hogy megakadályozzuk az email hamisítást?

Válasz

- ( ) Az SPF rekordot a DNS TXT rekordjaként kell létrehozni, amely tartalmazza azokat az IP címeket vagy domaineket, amelyekről engedélyezett az email küldése az adott domain nevében, valamint az erre vonatkozó policy-t
- ( ) Az SPF rekordot a DNS MX rekordjaként kell létrehozni, amely tartalmazza azokat az IP címeket vagy domaineket, amelyekről engedélyezett az email küldése az adott domain nevében.
- ( ) Az SPF rekordot a DNS SRV rekordjaként kell létrehozni, amely tartalmazza azokat az IP címeket vagy domaineket, amelyekről engedélyezett az email küldése az adott domain nevében.

Megoldások beküldése