ServerOS Essentials

*Week 01 - Oefeningen*

Oefening 1-10: herhaling Desktop OS

1. Elk linux (UNIX) systeem is een multi-user systeem. De verschillende gebruikers zijn onderverdeeld in groepen.

In welk bestand worden deze groepen gedefinieerd ? Geef het id van de volgende groepen :

Group Group-ID

root 0………..

daemon 1………..

bin 2………..

mail 8…………

users 100……

2. De definitie van de gebruikers zelf wordt bijgehouden in het bestand

/etc/passwd. Dit bestand bevat voor elke gebruiker 1 lijn. Elke lijn is ingedeeld in 7 velden, gescheiden door een “:”.

Geef de beschrijving van de verschillende velden :

Veld1: username…………………………………………..

Veld2: password…………………………………………..

Veld3: userid……………………………………..

Veld4: groupid………………………………………..

Veld5: useridinfo…………………………………..

Veld6: home-directory…………………………..

Veld7: shell…………………………………………..

3. Vroeger, in the early days of Unix, bevatte het bestand /etc/passwd behalve user-informatie, ook de gecodeerde versie van het paswoord. Dat was natuurlijk een zwak punt in de beveiliging van het Unix

systeem, aangezien iedereen het /etc/passwd bestand kan lezen en dus van alle gebruikers de gecodeerde paswoorden kon zien. Voor hackers was de volgende stap het ontwikkelen van tools om die gecodeerde paswoorden te decoderen, bijvoorbeeld: cracker. Nadat men dit probleem had erkend als een serieus beveiligingsprobleem, heeft men besloten de paswoorden van de gebruikers in een apart bestand te bewaren. Dit bestand is alleen toegankelijk door de gebruiker root, onder wiens ID het passwd en login programma wordt uitgevoerd.

Wat is de naam van dat bestand met de gecodeerde paswoorden ?

/etc/shadow

4. Maak een groep aan met de naam “testgroep” en groep-ID 200.

Gebruikt commando :

***student@studentvm:~$ sudo groupadd -g 200 testgroep***

Wijzig de naam van de groep “testgroep” in “pcaktief”. Gebruikt commando :

***student@studentvm:~$ sudo groupmod -n pcaktief testgroep***

Verwijder de groep “pcaktief”. Gebruikt commando :

***student@studentvm:~$ sudo groupdel pcaktief***

5. Maak een gebruiker aan met volgende kenmerken : User-name: jan

User-ID: 201

Group-ID: 100 (=users)

Omschrijving: Testuser Jan

Home-dir: /home/jan

Shell: /bin/bash

Gebruikt commando :

***student@studentvm:~$ sudo useradd -n jan -u 201 -g 100 -c Testuser Jan -d /home/jan -s /bin/bash***

Nadat een gebruiker aangemaakt werd, wordt zijn paswoord ingesteld op “!”, wat betekent dat die naam nog niet kan gebruikt worden om u aan te melden. Om dat wel mogelijk te maken, moet je jan een paswoord geven. Stel het paswoord van jan in op “januari”.

Gebruikt commando :

***student@studentvm:~$ sudo passwd jan januari***

6. De gebruiker jan is nu aangemaakt op uw systeem. Nu kan jan informatie opvragen over zichzelf. Log aan als jan en voer volgende commando’s uit:

id

output :

uid=201(Jan) gid=100(users) groups=100(users)

finger jan *(nog te installeren)*

output :

***student@studentvm:~$ finger jan***

**login: jan name: Testuser Jan**

**Directory: /home/jan shell: /bin/bash**

**on since ...**

**no mail.**

**no plan.**

7. Log aan als jan en voer volgend commando uit ls /root.

Output :

ls: cannot open directory “/root” permission denied

Die output komt er omdat de directory /root eigendom is van de gebruiker ‘root’ en omdat de beveiliging ervan zo is ingesteld dat niemand behalve de ‘root’ en users die lid zijn van de group ‘root’ er toegang toe heeft.

Laten we nu stellen dat jan ook een systeembeheerder is en toegang

moet krijgen tot de directories van de group ‘root’. In dat geval moeten we jan ook lid maken van de ‘root’-group.

Log aan als root, met welk commando doe je bovenstaande?

***student@studentvm:~$ sudo su root***

***student@studentvm:~$ usermod -aG root jan***

Wat is er veranderd in het bestand /etc/group ?

***jan is toegevoegd aan root.***

Kan je nu als user jan een ls doen van de dir /root ? JA / NEE

***Nee.***

8. Verwijder de gebruiker jan van het systeem m.b.v. het commando:

userdel –r jan

Wat is er veranderd in het bestand /etc/group?

**jan is uit de groep van root gehaald en user jan is volledig verwijderd.**

Bestaat de dir /home/jan nog ? JA / NEE

***Nee.***

9. Stel dat je in een bedrijf werkt waar men toestellen ontwerpt,maakt, herstelt en verkoopt. Voor het ontwerpen van toestellen zijn er ingenieurs aangesteld. Voor het maken en herstellen van die toestellen zijn er techniekers aangesteld en voor het verkopen verkopers. Alle medewerkers van uw bedrijf werken op een centraal Linux-systeem. De gebruikers van het Linux-systeem moeten zo gedefinieerd zijn dat de ingenieurs elk hun eigen home-dir hebben,

maar samen een directory /home/shared/ontwerpen kunnen delen (waarop ze alle rechten hebben). Alle techniekers delen dezelfde home-dir /home/techniekers en alle verkopers hebben een eigen home-dir, maar delen een gezamelijke directory /home/shared/info (waarop ze alle rechten hebben) waarin er technische/marketing gegevens staan over de toestellen. De ingenieurs moeten ook toegang hebben tot de directory /home/shared/info (alle rechten).

De ingenieurs zijn: (usernaam/paswoord)

peter/zomer1 patrick/zomer2

De techniekers zijn: wim/winter1 ward/winter2

De verkopers zijn: bert/budget1 ilse/budget2

De groepen voor de verschillende diensten zijn: Dienst Linux-groep ingenieurs ingenieur techniekers techniek

verkopers verkoop

Speciale groepen voor de shared-directories: Directory Linux-groep

/home/shared/ontwerpen ontwerpen

/home/shared/info info

De eigenaar van de shared-directories is de ‘root’

Maak de groepen en users en directories aan, conform aan de situatie zoals hierboven beschreven.

**\*alle commando's voor alles in orde te krijgen\***

**sudo su**

**adduser --home /home/peter --shell /bin/bash peter**

**passwd peter \*zomer1\* -> dit voor alle andere gebruikers doen met hun eigen passwd**

**adduser --home /home/patrick --shell /bin/bash patrick**

**groupadd ingenieur**

**groupadd ontwerpen**

**mkdir /home/shared**

**ls -ld /home/shared**

**chown root /home/shared**

**usermod -a -G ingenieur peter**

**usermod -a -G ingenieur patrick**

**mkdir /home/shared/ontwerpen**

**usermod -a -G ontwerpen peter**

**usermod -a -G ontwerpen patrick**

**adduser --home /home/techniekers --shell /bin/bash wim**

**adduser --home /home/techniekers --shell /bin/bash ward**

**groupadd techniek**

**usermod -a -G techniek wim**

**usermod -a -G techniek ward**

**groupadd verkoop**

**groupadd info**

**adduser --home /home/bert --shell /bin/bash bert**

**adduser --home /home/ilse --shell /bin/bash ilse**

**mkdir /home/shared/info**

**usermod -a -G verkoop bert**

**usermod -a -G verkoop ilse**

**usermod -a -G info bert**

**usermod -a -G info ilse**

**setfacl -m g:ontwerpen:7 ontwerpen/**

**getfacl ontwerpen/ -> testen of alles in orde is**

**setfacl -m g:info:7 info/**

**setfacl -m g:ingenieur:7 info/**

**getfacl info/ -> checken of beide groepen zijn toegevoegd en of ze allebei volledige toegang hebben**

**#setfacl -x group:verkoop \* -> in het geval er een group verwijderd dient te worden (als deze perongeluk aangemaakt was)**

**ls -ld (van iedere map) -> checken of alles in orde is**

**\*Met adduser wordt de home dir automatisch aangemaakt\***

10. Maak 7 gebruikers aan :

Walter, Karel,Dirk, Evert, Ine, Els en Tina

Els, Tina en Ine zijn als hoofgroep lid van users, als bijkomende groep lid van verkoop.

Walter en Karel zijn lid van planning.

Dirk en Evert springen in allebei de departementen in en zijn dan ook lid van allebei de groepen.

Alle gebruikers hebben hun homedir in /home/gebruikersnaam. Er zijn 3 extra directories in home te vinden:

/home/planning bevat de planning, aanpasbaar door leden van de groep planning

/home/verkoop bevat informatie over verkoop, aanpasbaar door leden van de groep verkoop

/home/algemeen bevat algemene informatie voor iedereen. (Evert is hiervoor verantwoordelijk en dus alleen Evert heeft schrijfrechten op deze dir en de inhoud).

Alle gebruikers (lid van groep users) hebben leesrechten op deze directories.

*Test ook deze instellingen !*

11. Maak een group pxl aan en een user itstudent. Deze user heeft als primaire group de group pxl. Password voor deze user is test123.

De home directory is /home/itstudent en als shell gebruik je /bin/bash. Doe alles rechtstreeks in de configuratiebestanden.

**a. sudo su -**

**b. vim /etc/passwd**

**-> itstudent:x:1008:1013::/home/itstudent:/bin/bash**

**c. vim /etc/group**

**-> pxl:x:1013:itstudent**

**d. ecrypteer het paswoord**

**-> openssl passwd**

**e. vim /etc/shadow**

**-> itstudent:LdHG7SuH9Jwp6:17737:0:99999:7:::**

**f. Maak een homedirectory aan met de inhoud van /etc/skel en stel de juiste ownership en permissies in.**

**-> cp -r /etc/skel /home/itstudent**

**-> chown -R itstudent:pxl /home/itstudent**

**g. Test de net aangemaakte user (en het paswoord)**

**->su – itstudent**

12. Zorg ervoor dat de user itstudent een sudoer wordt.

***student@studentvm:~$ sudo* gpasswd -a itstudent sudo**

13. Verander je umask naar 0037.

***student@studentvm:~$* umask 0037**

14. Als je nu een bestand aanmaakt, welke permissies heeft dit dan ?

**-rw-r-----**

Als je nu een directory aanmaakt, welke permissies heeft deze dan ? (Vul eerst in en controleer daarna pas door het uit te voeren.)

**-rwxr-----**

15. Test op uw systeem of de volgende bewering waar is: ‘Als iemand op een directory de permissie write heeft, geldt dat automatisch ook voor alle bestanden die in die directory voorkomen en betekent dat dus dat de persoon in kwestie al deze bestanden mag lezen ?’

16. Kopieer het bestand /etc/hosts naar uw homedirectory (niet als root doen!!!).

***student@studentvm:~$* cp /etc/hosts /home/student**

Zorg er via de opdracht chmod voor dat de permissies als volgt zijn ingesteld: xr voor others, wr voor group en geen permissies voor de eigenaar.

***student@studentvm:~$* chmod u-x, u-w, u-r, g=wr, o=xr hosts**

Controleer met ls –l of dit goed is gegaan.

***student@studentvm:~$* ls -l**

Mag de eigenaar nu het bestand bekijken? Waarom wel/niet?

**Je mag enkel het bestand bekijken als je root bent of met een sudo.**

Mag hij andere permissies instellen?

**Hij mag nog altijd permissies instellen.**

Mag hij het bestand verwijderen?

**Ja, hosts mag verwijdert worden.**

17. Met chsh kan een gebruiker zijn login-shell aanpassen, hetwelk gespecificeerd wordt in /etc/passwd. Het bestand /etc/passwd is niet beschrijfbaar door een gewone gebruiker. Waarom kan een gewone gebruiker dan toch zijn login-shell aanpassen?

18. Zoek alle bestanden op de harddisk die de setuid-bit gezet hebben.

***student@studentvm:~$* find / -perm /4000**

19. Maak twee gebruikers aan (elk in zijn eigen group). Maak ook een group ICT. Plaats de twee gebruikers ook in de group ICT. Maak een map /ICTfiles. Zorg er voor dat de ICT-gebruikers bestanden kunnen plaatsen en dat iedereen van ICT deze bestanden kan aanpassen. Zorg er wel voor dat een ICT-gebruiker enkel zijn EIGEN bestanden mag verwijderen.

***student@studentvm:~$* sudo find -user student -perm -u+s**