

إدارة المستخدمين و المجموعات في لينوكس

أولاً: المستخدمين

مقدمة:

أنظمة اليونكس دائماً دعمت منذ بدايتها المستخدمين المتعددين من حيث العمل إما بشكل مستقل أو عدة مستخدمين بنفس الوقت على نفس الكمبيوتر، في بداية نشوء النظام في الستينات كان المستخدمين الذين لديهم صلاحيات الوصول للجهاز يقومون بالدخول عبر إدخال اسم مستخدم وكلمة المرور الصحيحة و في حال تم التأكد منها يقوم النظام بالسماح للمستخدم بالدخول للجهاز و تشغيل تطبيقاته، طبعاً كان الدخول يتم عبر وحدات طرفية مؤلفة من شاشة و لوحة مفاتيح (بدون فارة في تلك الأيام D:)، الشبكات لم تكن جزءاً من تصميم اليونكس Unix الأساسي، و لكنها تطورت فيه بشكل سريع و مبكر مما أعطى المستخدمين إمكانية التعامل مع النظام من أي مكان...

اللينوكس Linux عندما بدأ أخذ هذه الميزة (تعدد المستخدمين) من اليونكس، كما ورث أيضاً العديد من المميزات الكبيرة و الرائعة منه أيضاً، و أيضاً لم تتغير كثيراً عبر الوقت الذي تغير في الواقع هي مجموعة الأدوات المستخدمة في إدارة هذه المميزات، كانت في السابق عملية إضافة اسم مستخدم جديد تتم إما عبر سطر الأوامر (التي لا تزال مستخدمة للآن) أو عن طريق ملف نصي يتم كتابة المتغيرات التي نريد تعيينها فيه و إلحاقها (يدوياً) ببرنامج يقوم بعمل الباقي، أما الآن فقد أصبحت العملية أسهل بسبب وجود العديد من البرامج التي تقوم بنفس العمل و لكن توفر الوقت و تسهل الجهد علينا للإدارة...

إجادة التعامل مع المستخدمين و التمكن جيداً من إدارتهم في النظام سيعطيك ميزة كبيرة في التعامل مع النظام و إدارته بكل سهولة، حيث ستستفيد أنت منه أولاً عبر نظامك الخاص بك ثم ستستطيع التعامل مع أي نظام مهما كان نوعه أو البيئة التي يعمل بها...

الكلام السابق هو الآن من الأساسيات أو البديهيات لكثير منكم، أي شخص يريد تشغيل الجهاز و الوصول للمعلومات التي فيه يجب أن تكون له الصلاحيات لفعل ذلك، حتى في جهازك الخاص في البيت...

التوزيعة التي استخدمتها في هذا الدرس هي fedora 11

المستخدمين العاديين و المستخدمين الأعلى:

أصبحت أغلب الأنظمة الآن إن لم تكن كلها تقسم المستخدمين إلى نوعين:

1. مستخدم عادي

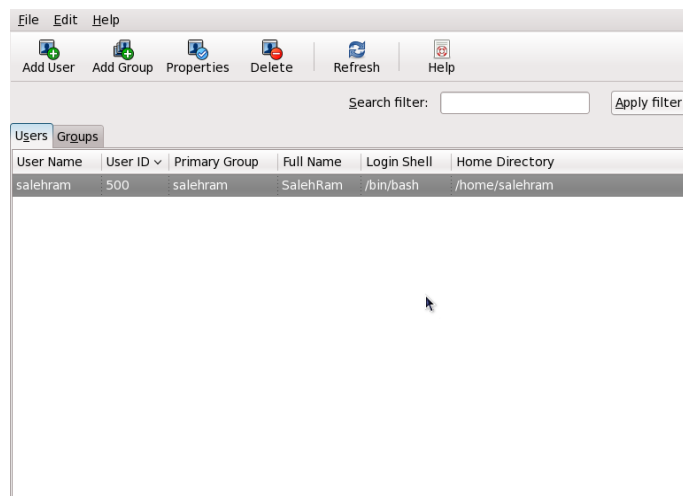
2. مستخدم أعلى أو مسئول أو Superuser

هذا التقسيم يساعد على جعل النظام أكثر أمان و قوة، فالمستخدم العادي ممنوع من تنفيذ مهام خاصة أو ضارة بالنظام إذا تم تنفيذها بصورة خاطئة، و في حال رغبته بتنفيذ أي منها سيحتاج إلى تصريح المستخدم المسئول لتنفيذ هذه المهام، لن أتطرق لهذه المهام لأنها معروفة جدا لديكم...

من أهم النقاط التي دائما يتم لفت النظر لها هي عدم تنفيذ أي مهمة يومية بصلاحيات المستخدم المسئول أو الـ root في الـ لينوكس و اليونكس و باقي الأنظمة المشابهة لها، و ذلك لأن مستخدم الـ root له الصلاحية المطلقة في عمل أي شيء بأي صورة في النظام (حتى حذف ملفات النظام) و لن يسأله النظام عن تصريح أو كلمة مرور أو أي شيء، لذا لا تستخدم صلاحيات الـ root إلا إذا احتجت لها...

كيف يقوم Linux بنخزين معلومات المستخدمين:

عند استخدام أدوات إدارة المستخدمين في الـ لينوكس تتعامل هذه الأدوات مع ملفات نصية معينة في النظام تحوي بيانات المستخدمين...



The screenshot shows a graphical user interface for managing system users. At the top, there is a menu bar with 'File', 'Edit', and 'Help'. Below the menu bar is a toolbar with icons for 'Add User', 'Add Group', 'Properties', 'Delete', 'Refresh', and 'Help'. A search filter input field with an 'Apply filter' button is located below the toolbar. The main content area has two tabs: 'Users' (selected) and 'Groups'. Below the tabs is a table with the following columns: 'User Name', 'User ID', 'Primary Group', 'Full Name', 'Login Shell', and 'Home Directory'. The table contains one entry for the user 'salehram'.

User Name	User ID	Primary Group	Full Name	Login Shell	Home Directory
salehram	500	salehram	SalehRam	/bin/bash	/home/salehram

هذه الملفات موجودة في الجدول التالي:

اسم الملف	الوظيفة
/etc/passwd	هذا الملف يحوي قائمة المستخدمين المحليين و بياناتهم
/etc/shadow	يحوي هذا الملف كلمات المرور مشفرة الخاصة بالمستخدمين و معلومات انتهاء الحساب
/etc/group	يتضح من اسم الملف أنه يحوي أسماء المجموعات في النظام و أيضا يحوي أسماء الحسابات المرتبطة بالمجموعات

إذا قمنا بفتح الملف passwd سنجد فيه المعلومات التالية:

```
# cat passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
avahi-autoipd:x:499:499:avahi-autoipd:/var/lib/avahi-autoipd:/sbin/nologin
ntp:x:38:38:/:etc/ntp:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkituser:x:87:87:PolicyKit:/:/sbin/nologin
avahi:x:498:497:avahi-daemon:/var/run/avahi-daemon:/sbin/nologin
mailnull:x:47:47:/:var/spool/mqueue:/sbin/nologin
smmsp:x:51:51:/:var/spool/mqueue:/sbin/nologin
openvpn:x:497:496:OpenVPN:/etc/openvpn:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:4294967294:495:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
pulse:x:496:494:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin
apache:x:48:48:Apache:/var/www:/sbin/nologin
nsd:x:28:28:NSCD Daemon:/:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
tcpdump:x:72:72:/:/sbin/nologin
smolt:x:495:490:Smolt:/usr/share/smolt:/sbin/nologin
torrent:x:494:489:BitTorrent Seed/Tracker:/var/lib/bittorrent:/sbin/nologin
haldaemon:x:68:68:HAL daemon:/:/sbin/nologin
mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash
nm-openconnect:x:493:488:NetworkManager user for OpenConnect:/:/sbin/nologin
backuppc:x:492:487:/:var/lib/BackupPC:/sbin/nologin
gdm:x:42:42:/:var/lib/gdm:/sbin/nologin
salehram:x:500:500:SalehRam:/home/salehram:/bin/bash
```

كل سطر في الإخراج السابق (البداية من السطر الثاني) الذي هو محتويات الملف passwd يمثل سجل لحساب مستخدم مسجل في النظام، مستخدم الـ root يكون في البداية دائماً، ثم يأتي بعده حسابات النظام، ثم في النهاية تجد المستخدمين العاديين، المعلومات التي تم عرضها بالأعلى (أو كل سطر منها) هو سجل لمستخدم كما اسلفت، و هذا السجل يحوي حقول أو معلومات مفصولة بنقطتين (:). هذا شرحها:

سأستخدم السجل الخاص باسم حسابي على النظام للتوضيح:

salehram:x:500:500:SalehRam:/home/salehram:/bin/bash

الثل الخاص بتسجيل الدخول	دليل مجلد البداية للحساب	وصف الحساب	GID	UID	كلمة المرور أو حافظ مكان كلمة المرور	اسم الحساب
/bin/bash	/home/salehram	SalehRam	500	500	x	salehram

و للتوضيح أكثر حول الحقول:

- اسم الحساب: و يحوي اسم تسجيل الدخول الخاص بالمستخدم الذي يقوم بإدخاله عند تسجيل الدخول للنظام (يفضل أن يكون طول هذا الحقل لا يتعدى ثمانية خانات)
- كلمة المرور: في السابق كان هذا الحقل يستخدم لتخزين كلمة المرور نفسها بصورة مشفرة، و لكن الآن بسبب الأخطار الأمنية التي يمكن أن يستغلها أي طرف تم وضع كلمة المرور المشفرة في ملف الـ shadow و بقي هذا الحقل لحجز مكان لكلمة المرور فقط
- UID: و هو اختصار لـ user identification number و هو يعرف حساب المستخدم، حيث ان كل رقم في هذا الحقل فريد و يجب ألا يتكرر، في حساب الـ root مثلا الرقم الخاص به هو 0 و في حال حدوث تكرار للرقم في حساب آخر الذي سيحدث هو أن الحساب الآخر سيحصل على صلاحيات الـ root كلها بسبب أن رقم التعريف هو 0، و طبعاً هذا خطير لأبعد حد...
- GID: اختصار لـ group identification number، هذا الرقم يقوم بتعريف المجموع الأساسية للمستخدم، هذا الرقم خاص بالمجموعة و يجب أن يكون فريداً على مستوى المجموعات، فلا يجب أن يتكرر مع أي مجموعة أخرى، الرقم الموجود هنا هو الرقم الذي يحدد المجموعة الأساسية للحساب، حيث يمكن أن ينتمي الحساب لمجموعة واحدة الموجودة رقمها بالفعل، و يمكن أن ينتمي لأكثر من مجموعة و لكن فقط المجموعة الأساسية يتم وضع رقمها هنا، المجموعة التي رقمها 0 يجب أن تكون دائماً للمستخدم الـ root و لكن ليست كخطورة الـ UID
- وصف الحساب: بشكل عام هذا الحقل لوصف الحساب، و يمكن أن يكون أي عبارة معبرة عن اسم الحساب و وظيفته، و هي ليست إلزامية إنما للمعلومات و التسهيل على من يريد التعامل

مع المستخدم...

- دليل مجلد البداية للحساب: هذا الحقل يحدد مكان تخزين الملفات للمستخدم و هو ليس ضروريا تحديده في الاستخدامات الشخصية للنظام، و لكن يمكن الاستفادة منه في بيئة الشبكات لوضع ملفات المستخدمين في أي مكان على الشبكة.
- الشل الخاص بتسجيل الدخول: و يحوي هذا الحقل على الشل الخاص بالحساب، و هو المسئول عن تنفيذ أوامر المستخدم، و سأحدث عن موضوع الـ shell في موضوع منفصل إن شاء الله...

بالنسبة لملف الـ shadow في حال فتحه سنجد المحتويات التالية:

```
[root@salehram etc]# cat shadow
root:$1$eAũkæŮAE$Kv55YOaIHDCPlI7q6igoQO:11961:0:99999:7:::
bin:!:14344:0:99999:7:::
daemon:!:14344:0:99999:7:::
adm:!:14344:0:99999:7:::
lp:!:14344:0:99999:7:::
sync:!:14344:0:99999:7:::
shutdown:!:14344:0:99999:7:::
halt:!:14344:0:99999:7:::
mail:!:14344:0:99999:7:::
uucp:!:14344:0:99999:7:::
operator:!:14344:0:99999:7:::
games:!:14344:0:99999:7:::
gopher:!:14344:0:99999:7:::
ftp:!:14344:0:99999:7:::
nobody:!:14344:0:99999:7:::
vcsa:!!:14441:!:!:!:!:!:
avahi-autoipd:!!:14441:!:!:!:!:!:
ntp:!!:14441:!:!:!:!:!:
dbus:!!:14441:!:!:!:!:!:
polkituser:!!:14441:!:!:!:!:!:
avahi:!!:14441:!:!:!:!:!:
mailnull:!!:14441:!:!:!:!:!:
smmisp:!!:14441:!:!:!:!:!:
openvpn:!!:14441:!:!:!:!:!:
rpc:!!:14441:0:99999:7:::
rpcuser:!!:14441:!:!:!:!:!:
nfsnobody:!!:14441:!:!:!:!:!:
pulse:!!:14441:!:!:!:!:!:
apache:!!:14441:!:!:!:!:!:
nscd:!!:14441:!:!:!:!:!:
sshd:!!:14441:!:!:!:!:!:
tcpdump:!!:14441:!:!:!:!:!:
smolt:!!:14441:!:!:!:!:!:
torrent:!!:14441:!:!:!:!:!:
haldaemon:!!:14441:!:!:!:!:!:
mysql:!!:14441:!:!:!:!:!:
nm-openconnect:!!:14441:!:!:!:!:!:
backupper:!!:14441:!:!:!:!:!:
gdm:!!:14441:!:!:!:!:!:
salehram:$1$eAũkæŮAE$Kv55YOaIHDCPlI7q6igoQO:14441:0:99999:7:::
```

كما يتضح من الإخراج السابق فإن الملف يحوي أسماء الحسابات يقابلها كلمات المرور لكل حساب بصيغة مشفرة، و أيضا فإن مستخدم الـ root دائما في البداية ثم يليه حسابات النظام ثم في النهاية الحسابات العادية للمستخدمين....

لتجنب المخاطر الأمنية من تخزين كلمة المرور في ملف واحد و فك تشفيرها من أي شخص فقد تم تعيين كل صلاحيات الوصول لملف الـ shadow لحساب الـ root فقط و لن يستطيع أي مستخدم الوصول لهذا الملف عدا الـ root...

القوة او النقطة الأساسية هنا في موضوع تشفير كلمة المرور هي أنه بعد أن يقوم المستخدم بإدخال كلمة المرور و يقوم النظام بتشفيرها لن تكون هناك حاجة مرة أخرى لفك تشفيرها من جديد، و لكن عند الحاجة للتحقق من بيانات مستخدم ما فإن النظام يقوم بأخذ كلمة المرور المدخلة و يقوم بتشفيرها و مقارنتها مع المخزنة لديه، و بالتالي يكون هناك أمان أكثر في العملية...

يمكن اكتشاف كلمة المرور المشفرة و لكن ليس عبر فك تشفيرها و لكن عبر استخدام تقنيات الهجوم الأخرى المعروفة كهجوم القاموس و غيره لمعرفة كلمة المرور الأصلية...

بالنسبة للبيانات المخزنة في ملف الـ shadow فهي كتالي (و أيضا مفصولة بنقطتين ":" - سأستخدم مثال من الملف الخاص بنظامي)

salehram:\$1\$eAúkáÚAÈ\$kv55YOaIHdCPlI1q6igoQ0:14441:0:99999:7:::

اسم الحساب	كلمة المرور المشفرة	تاريخ آخر تغيير في كلمة المرور	الأيام التي لا يمكن تغيير كلمة المرور قبلها	الأيام التي يجب تغيير كلمة المرور بعدها	فترة التنبيه لتغيير كلمة المرور قبل انتهائها	الأيام التي سيتم بعدها تعطيل الحساب بعد انتهاء صلاحية كلمة المرور	تاريخ انتهاء صلاحية الحساب	هذه الخانة محجوزة للاستخدام المستقبلي
salehram	\$1\$eAúkáÚAÈ\$kv55YOaIHdCPlI1q6igoQ0	14441	0	99999	7	:	:	:

بالنسبة لتفاصيل الحقول فهي كالتالي:

- اسم الحساب: و هو يحوي اسم الحساب، و هو يجب أن يكون مطابقا تماما للاسم الموجود في ملف الـ passwd...
- كلمة المرور المشفرة: و يحوي النص المشفر لكلمة المرور، في حال وجود علامة النجمة "*" يعني أن الحساب معطل، و وجود علامتي تعجب "!!" قبل كلمة المرور يعني أن الحساب مقفل مؤقتا.

- تاريخ آخر تغيير في كلمة المرور: و هذا الرقم هو مجموع الأيام من تاريخ 1-1-1970 حتى هذه اللحظة، في مثالي السابق يعني أن كلمة المرور تم تغييرها بعد مرور 14441 يوم من 1-1-1970
- الأيام التي لا يمكن تغيير كلمة المرور بعدها: هذا الحقل يحوي عدد الأيام التي لا يمكن تغيير كلمة المرور قبل مرورها، في حال كان الرقم 0 يعني أن كلمة المرور يمكن تغييرها في اي وقت.
- الأيام التي يجب تغيير كلمة المرور بعدها: و هذا العدد يحدد المدة التي يجب تغيير كلمة المرور بعد انقضائها، القيمة الافتراضية لهذا الحقل (99999) تعني أن كلمة المرور يمكنها البقاء كما هي لمدة 274 سنة تقريبا (D: احسبها بالآلة الحاسبة 99999/365)...
- فترة التنبيه لتغيير كلمة المرور قبل انتهائها: و هذا الرقم يحدد الفترة التي سيتلقى فيها المستخدم تنبيه بأن كلمة المرور الخاصة به ستنتهي...
- الأيام التي سيتم بعدها تعطيل الحساب بعد انتهاء صلاحية كلمة المرور: يتم تحديد في هذا الحقل عدد الأيام التي سيتم بعد انقضائها تعطيل الحساب نهائيا إذا لم يقم صاحب الحساب بتغيير كلمة المرور بعد انتهاء صلاحيتها.
- تاريخ انتهاء صلاحية الحساب: يحوي هذا الحقل التاريخ الذي سوف يتم انتهاء صلاحية الحساب فيه معبرا عنه بعدد الأيام منذ التاريخ: 1-1-1970
- الخانة الأخيرة فارغة و محجوزة لاستخدامات أخرى

كما هو معروف فالحساب يمكن أن ينتمي لعدة مجموعات في النظام، و لكن ملف الـ passwd يسمح فقط بعرض مجموعة واحدة و هي المجموعة الرئيسية، و باقي المجموعات التي ينتمي لها تكون موجودة في هذا الدليل بالإضافة إلى أسماء الحسابات الأعضاء بها أمامها... فلو عرضنا محتويات الملف group سنجد فيه المعلومات التالية:

```
root@salehram etc]# cat group
root:x:0:root
bin:x:1:root,bin,daemon
daemon:x:2:root,bin,daemon
sys:x:3:root,bin,adm
adm:x:4:root,adm,daemon
:dip:x:40
:ftp:x:50
:sshd:x:74
:screen:x:84
:tcpdump:x:72
:wbpriv:x:88
:haldaemon:x:68
:mysql:x:27
:nm-openconnect:x:488
backuppc:x:487:apache
salehram:x:500
test:x:501:salehram
```

كما تلاحظون الإخراج بنفس الأسلوب السابق، و لتوضيحه أكثر سأشرح هذا المثال على المجموعة الأخيرة test التي تحوي اسم الحساب الخاص بي...

test:x:501:salehram

الحسابات الأعضاء في المجموعة	رقم تعريف المجموعة GID	كلمة مرور المجموعة أو حاجز مكان كلمة المرور	اسم المجموعة
salehram	501	x	test

لن أتحدث عن تفصيل الجدول السابق كله و لكن سأكتفي بالحقل الأخير منه لأنه هو الذي يهمني توضيحه هنا...

كما لاحظتم فإن الحقل يحوي الحسابات الأعضاء بها، و لو رجعتم إلى الجدول الأول (ملف الـ passwd) لوجدتم الحساب الخاص بي مرتبط بمجموعة بالفعل و هي salehram و هذه المجموعة هي المجموعة الأساسية بالنسبة لحسابي، أما test التي أنتمي لها أيضا ليست مجموعتي الأساسية، و بالتالي لم يتم وضع رقمها في ذلك الملف، و لذا لا بد من ذكر أو ربط حسابي معها، و لذلك يتم استخدام هذا الملف و وضع اسمي أمام المجموعات الأخرى التي أنتمي لها مقابل معلوماتها، و في حال كان هناك أكثر من حساب مرتبط مع هذه المجموعة تكتب جميعها و يفصلها فاصلة (,) مثل:

test:x:501:salehram,account1,account2...

إدارة المستخدمين المتقدمة:

- هدف من هذا الدرس هو شرح و توضيح عملية إدارة المستخدمين من خلال الواجهة الخطية للنظام (التي يشعر الكثير منا عند رؤيتها بالملل و الانزعاج)، و ذلك لعدة أسباب:
- عند استخدامك للبرامج الرسومية فأنت تكون قد حققت الهدف الذي تريده و هو عمل شيء ما لحساب مستخدم، و لكن في نفس الوقت لم تتعرف على ما يحدث في الخلف و ما يمكنك عمله بنفسك بدون استخدام أي برامج مساعدة...
 - افرض مثلا أن نظامك لم يعد يعمل بالواجهة الرسومية لأي سبب و أنك محتاج بشدة للدخول للنظام و عمل تغييرات به و من ضمنها عمليات على حسابات المستخدمين... ماذا ستفعل عندها؟
 - باعتبارك مستخدما لنظام لينوكس فإنه يجب عليك على الأقل معرفة الأوامر الضرورية لإدارة جهازك بشكل صحيح و سليم، و إدارة المستخدمين واحدة من أهم النقاط التي يجب عليك معرفتها...

- أن موضوع المستخدمين موضوع كبير و سهل في نفس الوقت و يمكن فهمه بسهولة، و هو يمثل جزءا كبيرا من النظام أيضا، فلو تم إتقان الموضوع بشكل جيد فلن تكون هناك مشكلة في إدارة النظام في بيئة أكبر من بيئة جهازك الشخصي في البيت...
- الفائدة من استخدام الأدوات المعتمدة على الواجهة الخطية هي إمكانية وضعها في سكربتات يتم تنفيذها تلقائيا لتوفير الوقت و الجهد في بيئة تتطلب عمليات كثيرة على المستخدمين أو إضافة عدد كبير من المستخدمين أو حذفه...

بعد أن رأينا بنية الملفات التي تستخدم لتخزين معلومات المستخدمين، و حيث أنها ملفات نصية عادية، يمكن أن نقوم بتعديلها يدويا لنتمكن من إدارة المستخدمين على النظام، و لكن هذه الطريقة ليست مستحسنة لعدة أسباب أهمها أن هذه الملفات هي ملفات نظام و بقاؤها في حالة سليمة أمر ضروري جدا لبقاء نظامك يعمل بشكل جيد، و لذلك في حال رغبتك بالتعديل عليها يدويا و مباشرة فأنت على مسؤوليتك في ذلك...

ما أريد أن أتكلم عنه هنا هو الأوامر المستخدمة في الواجهة النصية لإدارة المستخدمين، و سأبدأ بهذا الأمر البسيط الذي وظيفته هو عرض هويتك أثناء العمل:

```
$ id
uid=500(salehram) gid=500(salehram) groups=500(salehram)
context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

كما هو الإخراج السابق، فالأمر `id` يظهر لك بيانات الحساب الخاص بك أثناء الجلسة التي أنت بها...

بالنسبة لإضافة المستخدمين فالأمر المستخدم هو `useradd` و يمكن استخدامه كالتالي:

```
[root@salehram salehram]# useradd -c 'Test User' -s /bin/bash testu
```

الأمر السابق يقوم بعمل مستخدم بالقيم الافتراضية له، و يجب تنفيذه كـ `root` عبر `su` ثم كتابة كلمة المرور الخاصة بالحساب، هذا الأمر بسيط جدا، و كما ذكرت يقوم بعمل الحساب على القيم الافتراضية التي يضعها النظام، أو لا نقوم بتعيين الوصف للمستخدم عبر الخيار `C` ثم نكتب الوصف بين علامتي اقتباس، و نحدد الشيل الذي سيستخدمه الحساب للدخول عبر الخيار `S` و أخيرا نحدد اسم المستخدم أو اسم تسجيل الدخول للحساب و هو هنا `testu`، لو قمنا الآن بمحاولة لتسجيل الدخول باستخدام هذا الحساب فإنها لن تنجح و ذلك لأن الحساب معطل، و لتمكينه يجب علينا تعيين كلمة مرور للحساب الجديد عبر هذه الأمر:

```
[root@salehram salehram]# passwd testu
Changing password for user testu.
New password: [set the new value,password is not visible]
Retype new password: [retype the new value,password is not visible]
passwd: all authentication tokens updated successfully.
```

نستطيع عرض محتويات الملفات passwd, shadow, group الجديدة التي تمت عليها بعد هذه العملية، و يمكن الآن تسجيل الدخول بهذا الحساب الجديد:

```
[salehram@salehram ~]$ su - testu
Password:
[testu@salehram ~]$ pwd
/home/testu
[testu@salehram ~]$
```

معلومات انتهاء كلمة المرور و الحساب يتم أخذها من الملفين login.defs في الدليل etc و الملف الآخر هو useradd في الدليل default داخل etc، لو قمنا بتنفيذ الأمر ls -a داخل المجلد home للحساب الذي قمنا بإنشائه الآن ستجده غير فارغ، الملفات التي يحويها يتم نسخها من الدليل skeleton داخل etc، و هذا الدليل يحوي الملفات التي يجب إضافتها إلى دليل الـ home الجديد لأي حساب جديد يتم إنشاؤه...

الجدول التالي يوضح كل الأوامر و الخيارات التي يمكن استخدامها مع الأمر useradd:

الخيار	الوصف
-d	يمكن من تغيير الموقع الافتراضي لمجلد الـ home للحساب الجديد
-e	يمكنك من تحديد تاريخ الانتهاء للحساب الجديد بالتنسيق dd-mm-yyyy
-f	يمكنك من تحديد عدد الأيام التي ينتظر فيها النظام بعد انتهاء صلاحية كلمة المرور لتعطيل الحساب نهائيا
-g	يمكنك من تحديد رقم الـ GID الخاص بالحساب الجديد
-G	يمكنك من تحديد قائمة مفصولة بفواصل بأسماء المجموعات الأخرى التي ينتمي لها الحساب
-M	يمكنك من إلغاء إنشاء دليل الـ home
-u	يمكنك من تعيين رقم تعريف المستخدم UID للحساب الذي سيتم إنشاؤه

بالنسبة لتعديل كلمة المرور، كل مستخدم يمكنه تعديل كلمة المرور الخاصة به فقط عبر كتابة الأمر passwd، أما الـ root يمكنه تعديل كلمة المرور لأي شخص بكتابة passwd ثم اسم الحساب المراد تغيير كلمة المرور له...

لتغيير معلومات الحساب الخاص بك من سطر الأوامر يمكنك استخدام الطريقة التالية:
(سأقوم بتغيير المعلومات للمستخدم الذي قمنا بإنشائه مسبقاً)

```
[testu@salehram ~]$ chfn
Changing finger information for testu.
Password:
Name [Test User]:
Office []:
Office Phone []:
Home Phone []:
Finger information not changed.
```

كما لاحظتم ستعرض مجموعة من المعلومات الخاصة بالمستخدم، عند ملء حقل معين يتم الضغط على زر Enter للانتقال للحقل الذي يليه، طبعاً كل ما سأذكره الآن يمكن القيام به عبر الواجهة الرسومية للنظام و لكن قد لا أتطرق لها حالياً لأن اهتمامي الآن على سطر الأوامر...

بالنسبة لتغيير الشل الخاص بالحساب يمكن استخدام الأمر chsh كالتالي:

```
[testu@salehram ~]$ chsh
Changing shell for testu.
Password:
New shell [/bin/bash]:
```

النقطة المهمة و القوية هنا كما أسلفت أنه يمكن وضع هذه الأوامر في سكريبتات ذاتية التنفيذ للاستفادة منها في البيئات الضخمة لتوفير الوقت على مدراء النظام؛ عند كتابة الأمر السابق سيطلب منك النظام كلمة المرور الخاصة بك للتحقق من هويتك، ثم سيطلب منك تحديد مسار الشل الجديد (المجلد bin يحتوي على عدة أنواع منها، يمكنك اختيار أحدها)، تستطيع استخدام الأمر man لمعرفة المزيد عن chfn و chsh و أيضاً useradd

المستخدم root و كيف يمكن استخدامه في إدارة حسابات مستخدمين آخرين:

هذا القسم مهم جداً، حيث أنه سيوضح طرق التعامل مع المستخدمين الآخرين عبر المستخدم المسؤول root و ذلك لتغيير كلمات المرور الخاصة بهم و تغيير تفاصيل الحساب الأخرى مثل الوصف، دليل مجلد الـ home و غيرها من التفاصيل الخاصة بالمستخدم...

الإجراءات التي سأحدث عنها هنا هي تغيير كلمة المرور و تغيير اسم تسجيل الدخول و تغيير الوصف للحساب، و تغيير مجلد الـ home للحساب، أما بالنسبة لباقي التفاصيل و الخيارات التي يمكن تغييرها يمكنك استخدام usermod man لمعرفة كل التفاصيل عن الأمر usermod المستخدم في هذه الحالة...

قبل البداية سأذكر الصيغة العامة لأمر `usermod` و هي كالتالي:
`usermod [option] [new value] [user name]`

- سأبدأ بتغيير كلمة المرور لحساب:

و ليكن الحساب هو حساب تجاربنا `testu`، و صيغة الأمر هي كالتالي:

```
[root@salehram etc]# passwd testu
Changing password for user testu.
New password: [type the new password then press Enter]
Retype new password: [retype the password and press Enter]
passwd: all authentication tokens updated successfully.
```

الصيغة المستخدمة هنا هي `passwd` ثم اسم المستخدم الذي نريد تغيير كلمة المرور له، نقوم بإدخال كلمة المرور مرتين للتأكيد ثم `Enter` لتغييرها...

- و لتغيير اسم تسجيل الدخول للمستخدم:

و سأستخدم المستخدم الذي قمنا بعمله مسبقا و هو `testu` و سأقوم بتغيير اسم تسجيل الدخول الخاص به إلى `testuser`

```
[root@salehram etc]# usermod -l testuser testu
```

الخيار المستخدم هنا هو `l` و يعني أننا نريد تغيير اسم تسجيل الدخول للمستخدم المحدد في الأمر، و تكون طريقة كتابة الأمر كالتالي:

```
usermod [option (-l here)] [new login name] [user name]
```

- لتغيير الوصف الخاص بالحساب نستخدم الطريقة التالية:

أصبح اسم المستخدم الخاص بنا الآن بعد التغيير السابق هو `testuser` و ستكون صيغة الأمر كالتالي:

```
[root@salehram etc]# usermod -c 'this is a testing user' testuser
```

استخدمنا الخيار `C` و يعني `comment` لتغيير التعليق أو الوصف الخاص بذلك الحساب، و الصيغة مثل الصيغة السابقة:

```
usermod [option (-c here)] [new comment] [user name]
```

- لتغيير دليل المجلد `home` نستخدم الأمر التالي:

سنستخدم في هذا الأمر الخيار `d` من `directory`:

```
[root@salehram etc]# usermod -d /home/users/testuser testuser
```

الصيغة العامة للأمر أصبحت معروفة، و لا داعي لكتابتها...

و لكن يوجد إضافة هي لو أننا نريد نقل المجلد و نقل محتوياته أيضا فإننا سنضع الخيار `m` بعد الدليل، لتصبح الصيغة كالتالي:

```
[root@salehram etc]# usermod -d /home/users/testuser -m testuser
```

• أريد أيضا إضافة أمرين إضافيين و هي تغيير UID و GID:

سأغير الـ UID للحساب testuser (المسمى testu سابقا) بالأمر التالي:

```
[root@salehram etc]# usermod -u 510 testuser
```

و هنا قمت بتغيير الـ UID إلى القيمة 510

و بالنسبة لتغيير الـ GID فنستخدم هذا الأمر:

```
[root@salehram etc]# usermod -g 510 testuser
```

و هنا قمت بتغيير الـ GID إلى القيمة 510

لن أتحدث عن تفاصيل هذين الأمرين لأن التغيير في أرقام UID و GID يؤدي أحيانا إلى نتائج جانبية غير جيدة، فمثلا لو كان للمستخدم ملفات خارج مجلد الـ home الخاص به فإنه لن يصبح مالك ملفاتة بعد التغيير السابق، لأن هذا الأمر لا يغير الملكية للملفات و لكن يجب تغييرها يدويا بطرق أخرى؛ يمكنك معرفة المزيد من التفاصيل عن هذه الأوامر عبر صفحة الـ man للأمر usermod

حذف المستخدمين:

دائما كان تدمير الشيء اسهل من عمله، و كذلك هنا في حذف المستخدمين عملية حذف المستخدم تتم بأمر واحد فقط مع خيار واحد غير إلزامي...

الصيغة العامة لأمر الحذف:

userdel [user name] يحذف حساب المستخدم فقط

userdel -r [username] يحذف حساب المستخدم و ملفاتة كلها

و كمثال عليه:

```
[root@salehram etc]# userdel test2
```

أو

```
[root@salehram etc]# userdel -r test2
```

لدي إضافة أخيرة تتعلق بالأمر SU و من الأفضل مراجعة صفحة الـ man الخاصة به و قراءة بعض التفاصيل عن الخيار C الذي يمكن من تشغيل مهام بصلاحيات مستخدم آخر، و أيضا عن الأمر - SU الذي يختلف قليلا عن ...SU

إنهئى الحديث عن المستخدمين و سابدأ بالمجموعات التي لا نقل أهميتها عن أهمية المستخدمين و لأنها مرتبطة جدا بموضوع المستخدمين

ثانيا: المجموعات

مقدمة:

أرجو أن أكون قد وفقت في توضيح موضوع المستخدمين في القسم السابق، و الآن سأدخل في موضوع المجموعات، المهم هو أيضا، حيث أن للمجموعات دور كبير في التحكم بالمستخدمين في النظام...

النقاط التي سوف أتكلم عنها في هذا القسم هي كالتالي:

- إضافة المجموعات عبر سطر الأوامر
- إدارة عضويات المجموعات عبر سطر الأوامر
- إلغاء صلاحيات مستخدم في مجموعة
- حذف المجموعات

سأقوم هنا بإعطاء فكرة عن كيفية إنشاء مجموعة عبر سطر الأوامر باستخدام الأوامر الأساسية لهذا الغرض، و يمكنك معرفة المزيد عبر تنفيذ الأمر `man groupadd`؛ الأمر المستخدم هنا لتنفيذ العملية هو كما لاحظتم `groupadd` الذي يمكن استخدامه لوحده بدون أي إضافات أخرى معه ليقوم بأخذ اسم المجموعة المعطى و تعيين رقمها تلقائيا، و في حال أردنا تعيين معرفها بأنفسنا سنستخدم الخيار `-g` مع الأمر، و هذا المثال للتوضيح:

```
[root@salehram ~]# groupadd testgroup1
```

في المثال السابق قمنا بإضافة المجموعة المسماة `testgroup1` و لم نستخدم أي خيار مع الأمر و بالتالي سيقوم النظام بتعيين رقم المعرف تلقائيا، و لو رجعنا إلى ملف الـ `group` السابق سنجد فيه التالي:

```
...
testgroup1:x:503:
...
```

كما هو واضح، قام النظام بتعيين أول رقم حر بعد 500 و حجزه لهذه المجموعة...

و في حال كنا نريد تعيين المعرف يدويا كل ما علينا هو استخدام الخيار `-g` مع الأمر السابق و نقوم بإدخال رقم معرف المجموعة بالإضافة إلى اسمها و تنفيذ الأمر كالتالي:

```
[root@salehram etc]# groupadd -g 1001 testgroup2
```

و هذه محتويات الملف group بعد الإضافة:

```
...
testgroup1:x:503:
testgroup2:x:1001:
...
```

كما تلاحظون فقد قام النظام بتعيين رقم المعرف الذي قمنا نحن بتعيينه للمجموعة و لم يقم بتعيين القيمة الافتراضية التي يقوم بتعيينها عند إنشاء مجموعات جديدة...

بقي ملاحظة بسيطة و هي أنه يمكن إضافة مجموعة كمجموعة نظام و ذلك باستخدام الخيار `-r` بعد الأمر `groupadd` و سيقوم النظام بإنشاء مجموعة و إعطائها رقم تعريف يكون أقل من 500 التي تكون هذه الأرقام محجوزة لمجموعات النظام، ما لم يتم استخدام الخيار `-g` مع الأمر فيقوم النظام بتعيين المعرف الذي قمنا بإعطائه...

بالنسبة للنقطة الثانية و هي إدارة المجموعات، ما أريد توضيحه هو إمكانية إعطاء المستخدمين صلاحيات لإدارة مجموعة ما هم أعضاء فيها عن طريق مستخدم الـ `root`، حيث يمكن تنفيذ ذلك عبر استخدام الأمر `gpasswd` الذي يقوم بإضافة المستخدمين للمجموعات و تغيير صلاحياتهم فيها، و يكون تنفيذ الأمر كالتالي:

أولا نقوم بإضافة المستخدم الذي نريد تعيين صلاحيات إدارية له إلى المجموعة إن لم يكن عضوا فيها في السطر الأول، ثم في السطر الذي يليه نقوم بتعيين الصلاحيات الإدارية له على المجموعة:

```
[root@salehram etc]# gpasswd -a testuser testgroup1
Adding user testuser to group testgroup1
[root@salehram etc]# gpasswd -A testuser testgroup1
```

لاحظ أننا استخدمنا في السطر الأول `a` صغير لإضافة المستخدم للمجموعة، و `A` كبير لتعيين الصلاحيات له...

لو قمنا بالدخول باسم `testuser` و قمنا بمحاولة إضافة أو حذف مستخدمين للمجموعة سنجد أنه يوجد صلاحيات لدينا لعمل ذلك...

في حال أردنا إزالة هذه الصلاحيات من المستخدم في المجموعة فنقوم بذلك عبر نفس الأمر السابق لكن مع تنفيذ حيلة صغيرة و هي تمرير قائمة المستخدمين الذين لديهم صلاحيات في المجموعة و لكن هذه المرة قائمة فارغة، كالتالي:

```
[root@salehram etc]# gpasswd -A '' testgroup1
```

بالأمر السابق ما قمنا به هو إخبار المجموعة بأنه لا يوجد مستخدمين لديهم صلاحيات الإضافة أو الحذف فيها إلا مستخدم الـ root و بالتالي لن تقبل أي عملية عليها من أي حساب آخر غير الـ ...root

لحذف المستخدمين من المجموعة نستخدم الخيار -d مع الأمر gpasswd و نقوم بتحديد اسم المستخدم الذي نريد حذفه من المجموعة كالتالي:

```
[root@salehram etc]# gpasswd -d testuser testgroup1
Removing user testuser from group testgroup1
```

بالنسبة للنقطة الأخيرة و هي حذف المجموعات فتتم عبر الأمر groupdel و إلحاق اسم المجموعة به ثم تنفيذ الأمر، و لكن دائما من الأفضل عدم حذف أي مجموعة طالما أنها تحوي حسابات مستخدمين كمجموعة أساسية لهم، و يمكن حذف المجموعات الثانوية بدون أي مشاكل...

في حال حذف مجموعة سيتم ترك ملفات بمجموعات لم تعد موجودة، و لمعرفة هذه الملفات و إعادة تعيينها نقوم بتنفيذ الأمر التالي:

```
[root@salehram etc]# find / -nouser -o -nogroup
```

و أيضا لابد من مراجعة صفحة الـ man الخاصة بالأوامر: groupadd groupdel لمعرفة المزيد عنها...

أرجو أن أكون قد وفقن في إيصال المعلومة الجيدة
و ما كان من صواب فبنوفيق الله
و ما كان من خطأ فمن نفسي و الشيطان
و باننظار أي ملاحظة أو إضافة على هذا العمل

SalehRam

<http://www.arabteam2000-forum.com>
<http://salehram.wordpress.com>

salehram@gmail.com