

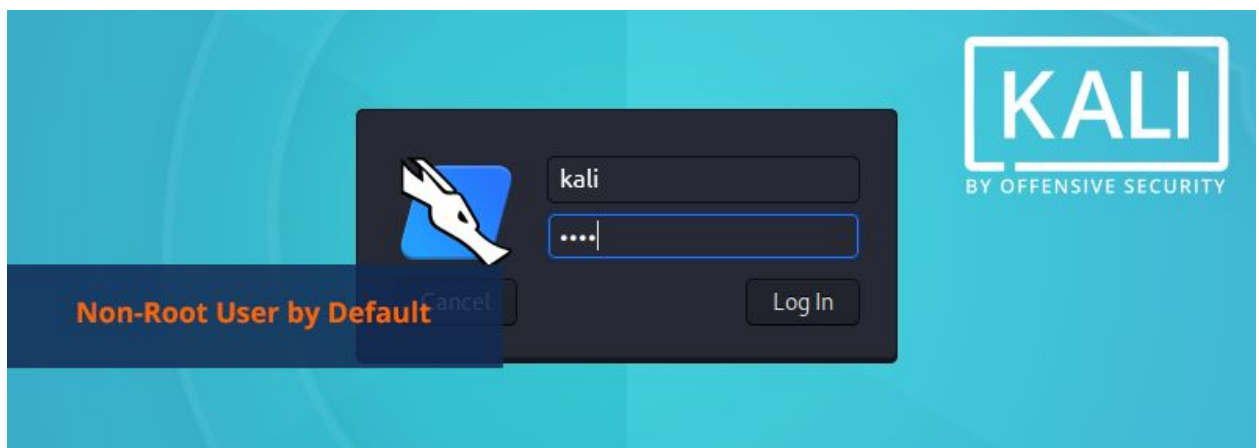
## User Managements And Groups in Linux

Linux OS သည် multi user system ဖြစ်ပါတယ်။ user များကို သက်ဆိုင်ရာ လိုအပ်ချက်အလိုက် user တွေခွဲပေးလို့ရသလို၊ ခွဲပေးလိုက်တဲ့ user ကို Permissions တွေနဲ့ တိတိကျကျ ကန့်သတ်အသုံးပြုလို့ရပါတယ်။

Linux System မှာ user အမျိုးအစား (၃) မျိုးနဲ့အလုပ်လုပ်ပါတယ်။

- Root user (Special user (or) super user)
- Normal user
- System user

Root User ကတော့ Linux System ကြီးတစ်ခုလုံးမှာ အကြီးဆုံးဖြစ်ပါတယ်။ သူ့ကို super user လို့တောင်တင်စားပြီးခေါ်ဝေါ်ကြပါတယ်။ဘာလို့လဲဆိုတဲ့ root user သည် system တစ်ခုလုံးကို ကိုင်တွယ်ပြီး ကြိုက်သလို စီမံနိုင်လို့ပဲဖြစ်ပါတယ်။ ဒါကြောင့် root user ကို ဘယ်သူမှ access (ဝင်ခွင့်) မပေးသင့်ပါဘူး။ System Admin တစ်ယောက်ပဲ Access လုပ်နိုင်မယ့် အခြေအနေကို maintain လုပ်ပေးထားမှာဖြစ်ပါတယ်။ Root user သည် linux system မှာ တစ်ယောက်ပဲရှိပါတယ်။



linux က multi user ဖြစ်တဲ့အတွက် ဒီလို root user ကိုတော့ sharing လုပ်ပြီးမသုံးသင့်ပါဘူး။ Hacker တော်တော်များများက root user access ရဖို့အတွက် rootkits ဆိုတဲ့ malware အမျိုးအစားကို kernel ထဲကို ထည့်ပြီး Hack တက်ကြပါတယ်။ rootkits ကြီးရှိနေရင် ကျွန်တော်တို့ Linux System ရဲ့ process ထဲမှာ သူအလုပ်လုပ်နေကြောင်း မဖော်ပြပါဘူး။ ဒါကို ဘယ်လိုသိနိုင်သလဲဆိုရင် Chkrootkit , rkhunter စသဖြင့် rootkits malware ကို စစ်ဆေးပေးတဲ့ tools တွေနဲ့ စစ်ဆေးနိုင်ပါတယ်။ နောက်ထပ် စစ်ဆေးနိုင်တဲ့အရာတွေက စက်ရဲ့ performance ကြီး ရုတ်တရတ် လေးလာတာ memory usage ကြီးက ဘယ် process မှ မစားသုံးနေပဲ တိုးလာတာမျိုး၊ cpu core မလောက်တော့ဘဲ ကျွန်တော်တို့ရဲ့ project ကြီး လေးလာတာမျိုး၊ system admin တစ်ယောက်မပြောင်းလဲလိုက်ပဲနဲ့ permission တွေချိန်းသွားတဲ့အခါမျိုး တွေဆိုရင် rootkits ကြီးရှိနေမှန်းသိသာပါတယ်။

Normal User ကတော့ သာမန်ပါပဲ သူ့ကိုတော့ root user ကိုယ်တိုင်က manage လုပ်ပါတယ်။ အခြေနေ ပေါ်မူတည် normal user တွေကို permission တွေကန့်သန့်ပေးရပါတယ်။ အခြေအနေရ normal user တွေကို system user အနေနဲ့လည်းအသုံးပြုနိုင်ပါတယ်။ ဥပမာ- website တစ်ခု ပေါ်က mysql ကိုထိန်းချုပ်ပြီး manage လုပ်ဖို့အတွက် normal user လေးတစ်ခု တည်ဆောက်မယ်။ ပြီးရင် ဒီ user ကို mysql ကို manage လုပ်ဖို့အတွက်ပဲ permission ကန့်သတ် ပေးရပါတယ်။ ဒီ user သည် mysql database ကလွဲလို့ ဘာမှ ကို ထိတွေ့ကိုင်တွယ် ထိန်းချုပ်ခွင့်မရှိပါဘူး။

System User တွေက တော့ ကျွန်တော်တို့ အသုံးပြုတဲ့ system application တွေကနေထွက်ပေါ်လာတဲ့ user အမျိုးအစားဖြစ်ပါတယ်။ Login ဝင်သုံးလို့မရပါဘူး။ ကျွန်တော်တို့ Login ဝင်သုံးနိုင်တဲ့ User တွေက root user နဲ့ normal user ပဲဖြစ်ပါတယ်။

User အမျိုးအစားကိုဘယ်လိုသိနိုင်မလဲ

```
$ cat /etc/passwd
```

```

stu
stud
student@security:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin

```

ဒီ command လေးကတော့ cat ဆိုတာ output ထုတ်ကြည့်တဲ့ command ဖြစ်ပါတယ်။ cat အနောက်က ကောင်ကတော့ argument အမျိုးအစား ဖြစ်တဲ့ file path လမ်းကြောင်းဖြစ်ပါတယ်။ Linux ပေါ်မှာ User ဘယ်နှယောက်ရှိလဲ ဆိုတာသိချင်ရင် /etc/passwd ဆိုတဲ့ / (root) အောက်က etc directory ထဲက passwd ဆိုတဲ့ file လေးမှာသွားကြည့်နိုင်ပါတယ်။

ဒီ file ထဲက line တစ်လိုင်းချင်းစီ ဟာ user တစ်ယောက်စီပဲဖြစ်ပါတယ်။

ထိပ်ဆုံး Line မှာ root ဆိုတဲ့ user ကိုတွေ့မှာပါ။ အနောက်က ( : ) လေးခြားထားတာက ဒီ user ရဲ့ information တွေဖြစ်ပါတယ်။ x ဆိုတာ password သတ်မှတ်ထားတဲ့နေရာလေး ဖြစ်ပါတယ်။ နောက် colon တစ်ခုနဲ့ ထပ်ခြားထားတာက User ရဲ့ id ဖြစ်ပါတယ်။ root user ရဲ့ id သည် Linux System မှာ 0 ပဲဖြစ်ပါတယ်။ ကျွန်တော်တို့တွေဟာ user တွေခွဲခြားတဲ့အခါ Name နဲ့ ခွဲခြားပြီးသိကြပါတယ်။ Linux ကတော့ ID နဲ့ ပဲအလုပ်လုပ်ပါတယ်။

နောက် colon တစ်ခုနဲ့ id တစ်ခုကတော့ Root User ရဲ့ Primary Group id ဖြစ်ပါတယ်။ နောက်ထပ် root လို့ရေးထားတာက root user ဖြစ်ကြောင်း စာရေးထားတာဖြစ်ပါတယ်။ ကိုယ်ကြိုက်တဲ့ စာသားရေးနိုင်ပါတယ်။ ဒါကို comment လေးလုပ်ထားတာလို့ပြောတာဖြစ်ပါတယ်။ /root ဆိုတာကတော့ root ရဲ့ home directory

တည်နေရာကို ညွှန်းထားတာပါ။ နောက်ထပ် colon အနောက်ဆုံးမှာတော့ root user အသုံးပြုတဲ့ shell အမျိုးအစားပဲဖြစ်ပါတယ်။ /bin/bash ဆိုတဲ့ binary directory ထဲက bash shell အမျိုးအစားကိုအသုံးပြုတာဖြစ်ပါတယ်။

User တွေကို ID နဲ့ဘယ်လိုခွဲသလဲဆိုတော့။

**Root user** ဆိုရင် **ID = 0** ဖြစ်ပါတယ်

**System User** ဆိုရင် **ID = 1** ကနေ **999** ထိ ရှိတယ်လို့သတ်မှတ်ပါတယ်။

**Normal User** ဆိုရင် **ID = 1000** ကနေ **60000** ထိရှိပါတယ်။

ဒီ user အမျိုးအစားသုံးမျိုးထဲမှာ Root User နဲ့ Normal User ကိုဘဲ Login ဝင်သုံးပြုနိုင်ပြီး manage လုပ်ရမှာဖြစ်ပါတယ်။

```
gnome-initial-setup:x:124:65534:./run/gnome-initial-setup:/bin/false
gdm:x:125:130:Gnome Display Manager:/var/lib/gdm3:/bin/false
cops:x:1000:1000:Kyaw Swar Tun,,,:/home/cops:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:./usr/sbin/nologin
student:x:1001:1001:./home/student:/bin/bash
student@security:~$
```

အထက်ပါပုံမှာကြည့်မယ်ဆိုရင် User ID 1000 နဲ့ 1001 ကိုတွေ့ပါလိမ့်မယ်။ cops ဆိုတဲ့ user နဲ့ student user ပဲဖြစ်ပါတယ်။ ဒီ user တွေဟာ normal user တွေပါ။ gdm, systemd-coredump တို့ကတော့ system user အမျိုးအစားတွေဖြစ်ပါတယ်။ ID က 125 နဲ့ 999 တို့ဖြစ်နေလို့ဖြစ်ပါတယ်။ system user တွေအသုံးပြုတဲ့ shell အမျိုးအစားကို လေ့လာကြည့်ရင်လည်း /bin/false နဲ့ /usr/sbin/nologin စတဲ့ Login ဝင်သုံးလို့မရတဲ့ system နဲ့ပတ်သတ်တဲ့ shell အမျိုးအစားတွေဖြစ်ကြောင်း တွေ့နိုင်ပါတယ်။

Linux ပေါ်မှာ user အလိုက် ခွဲပြီးအသုံးပြုလို့ရသလို user တွေကို စုစည်း group ဖွဲ့ပြီး permission တွေကန့်သတ်ပေးလို့ရပါသေးတယ်။ အိုကေ။

Group အမျိုးအစား သုံးမျိုးရှိပါတယ်။

- System Group

- Primary Group

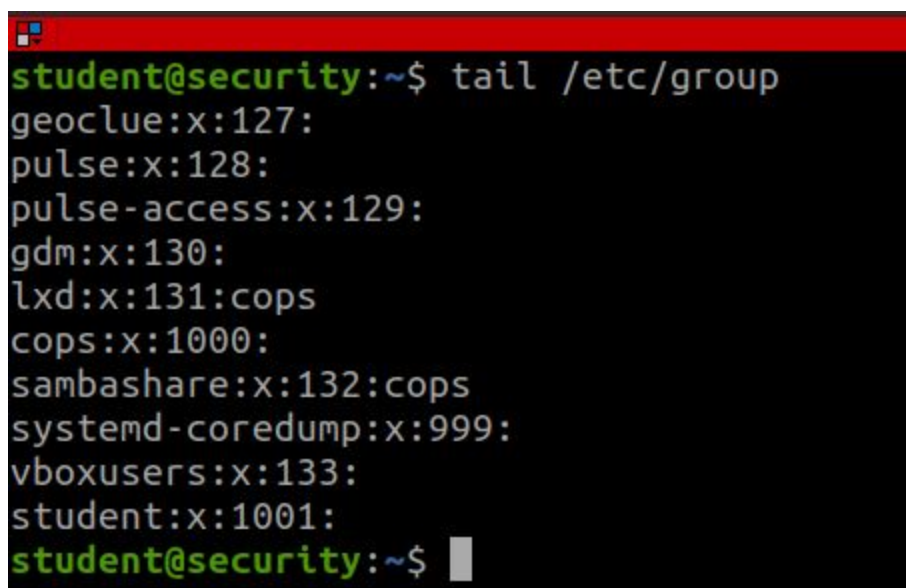
- Secondary Group (or) Supplementary Group

System Group ဆိုတာ system user တွေကထွက်ပေါ်လာတဲ့ group ဖြစ်ပြီး system အတွင်းမှာ ကျွန်တော်တို့ အများအားဖြင့် manage လုပ်ပေးစရာမလိုဘဲ auto အလုပ်လုပ်ပေးပါတယ်။

Primary Group ကတော့ Normal User တစ်ယောက် ထည့်လိုက်မယ်ဆိုရင် သူ့ရဲ့ primary group ပါပြီးသားဖြစ်ပါတယ်။ Root User မှာလည်း root ရဲ့ primary group ရှိပါတယ်။ normal user ထည့်လိုက်ရင် normal user ရဲ့ name တိုင်းပဲ သူ့ရဲ့ primary group ရဲ့ name ကို ထည့်ပေးပါတယ်။

**/etc/group**

( / ) root directory အောက်က etc directory ထဲမှာ group ဆိုတဲ့ နာမည်နဲ့ file လေးရှိပါတယ်။ ဒီ file လေးက Linux System ကြီးမှာ group ဘယ်နှခုရှိကြောင်း group ရဲ့ information အပြည့်အစုံ ဖော်ပြထားပါတယ်။



```
student@security:~$ tail /etc/group
geoclue:x:127:
pulse:x:128:
pulse-access:x:129:
gdm:x:130:
lxd:x:131:cops
cops:x:1000:
sambashare:x:132:cops
systemd-coredump:x:999:
vboxusers:x:133:
student:x:1001:
student@security:~$
```

**tail** ဆိုတဲ့ command က group ဆိုတဲ့ file တဲ့ အချက်အလက်တွေကို အောက်ဆုံး က စပြီး ၁၀ ကြောင်းထုတ်ကြည့်ပေးတာဖြစ်ပါတယ်။ cat နဲ့မတူတာက cat ဆိုတာ file တစ်ခုလုံးက data တွေကိုဖော်ပြပေးတဲ့အတွက် အများကြီးဖြစ်သွားပါတယ်။ ခုက အောက်ဆုံး ၁၀ ကြောင်းကို ပြပေးပါလို့ဆိုလိုတာဖြစ်ပါတယ်။

ဒီထဲမှာ id 1001 နဲ့ပြထားတဲ့ group name သည် စောစော ကပါလာတဲ့ student user ရဲ့ primary group ဖြစ်ပါတယ်။

Secondary Group (or) Supplementary Group ကတော့ ကျွန်တော်တို့ စနစ်တစ်ခုရဲ့လိုအပ်ချက်အရ သက်သက်ဖွဲ့ စည်းပေးရတဲ့ Group အမျိုးအစားကို ဆိုလိုတာဖြစ်ပါတယ်။ ဥပမာ - Company တစ်ခုမှာ AdminTeam ရှိတယ်ဆိုပါစို့ ဒီ adminteam အတွက် Data တွေပေးနိုင်မယ် နေရာတစ်ခု ဖန်တီးလိုက်မယ်။ ပြီးရင် adminteam ထဲမှာ ပါဝင်တဲ့ user တွေကို adminteam group ထဲကိုထည့်ပေးရပါတယ်။ အိုကေ ခုန က ဖန်တီးထားတဲ့ data တွေကို adminteam group ကို access လုပ်ခွင့် permission ပေးလိုက်တာနဲ့ group ထဲက user members တွေအကုန်လုံး ဒီ data ကို access လုပ်ခွင့်ရှိသွားမှာဖြစ်ပါတယ်။ ဒီလိုခြေနေ တွေရောက်ရှိလာတဲ့ အခါမှာ secondary group (supplementary group) ကို ဖွဲ့စည်းပေး ပြုလုပ်ပေးလို့ ရပါတယ်။

```
cops:x:1000:
sambashare:x:132:cops
systemd-coredump:x:999:
vboxusers:x:133:
student:x:1001:
adminteam:x:1002:student,cops
student@security:~$
```

အထက်ပါပုံအရ ဆိုလျှင် adminteam group ထဲကို student user နဲ့ cops ဆိုတဲ့ user နှစ်ယောက်က ဝင်ရောက်ထားတာကို တွေ့မြင်ရမှာဖြစ်ပါတယ်။

**/etc/shadow**

( / ) root directory အောက်က etc directory အောက်မှာ ရှိနေတဲ့ shadow ဆိုတဲ့ file လေးက user တွေရဲ့ information အပြည့်အစုံကို ထပ်မံဖော်ပြပေးထားပါတယ်။

```
root@security:~# head /etc/shadow
root:!:18581:0:99999:7:::
daemon*:18474:0:99999:7:::
bin*:18474:0:99999:7:::
sys*:18474:0:99999:7:::
sync*:18474:0:99999:7:::
games*:18474:0:99999:7:::
man*:18474:0:99999:7:::
lp*:18474:0:99999:7:::
mail*:18474:0:99999:7:::
news*:18474:0:99999:7:::
```

**head** ဆိုတဲ့ command ကတော့ file ထဲက စာတွေရဲ့ ထိပ်ဆုံး စာကြောင်း ၁၀ ကြောင်းကို defaults အနေနဲ့ ပြပေးပါတယ်။

အပေါ်ဆုံးက root user ရဲ့ information ကိုကြည့်လိုက်မယ်ဆိုရင် သူ့ရဲ့ information အပြည့်အစုံကို colon လေးနဲ့ ဖော်ပြပေးထားပါတယ်။

❶name: ❷password: ❸lastchange: ❹minage: ❺maxage: ❻warning: ❼inactive: Ⓣexpire: Ⓣblank

1. Username ,
2. Password ကို မသတ်မှတ်ရသေးတဲ့အတွက် ! လေးနဲ့ ဖော်ပြပါတယ်။
3. Lastchange ဆိုတာ Linux စတင်အသုံးပြုခဲ့တဲ့ 1970.01.01 နေ့ကနေ ခုလက်ရှိ root user password change ခဲ့တဲ့ နေ့ရက်ထိ ရေတွက်ထားတဲ့ ရက်ပေါင်းဖြစ်ပါတယ်။



4. Root user ရဲ့ password အနိမ့်ဆုံးသတ်တမ်းကုန်ဆုံးရက်ဖြစ်ပါတယ်။
5. Root user ရဲ့ password အများဆုံးသတ်တမ်းကုန်ဆုံးရက်ဖြစ်ပါတယ်။
6. Root user ရဲ့ password သတ်တမ်းမကုန်ခင် Warning ပြမယ့် ရက်ပေါင်းဖြစ်ပါတယ်။
7. Root User password သတ်တမ်းကုန်ဆုံးသွားပြီး password ကို ပြန်change ပြီး သုံးလို့ရသေးတဲ့ Account inactive ရက်ပေါင်းဖြစ်ပါတယ်။
8. Root User ရဲ့ password ကို ပြန်ပြီး မချိန်းဘဲ နေတဲ့ အတွက် password သတ်တမ်းကုန်ဆုံးသွားပြီး Account ပါ expire ဖြစ်သွားမယ့် နေ့ရက်ဖြစ်ပါတယ်။ ဒီလိုနေ့ရက်ကို ရောက်ရှိသွားရင် User Account ကိုသုံးလို့လုံးဝမရတော့ပါဘူး။
9. နောက်ဆုံး colon ကတော့ လာမယ့် future မှာလိုအပ်မယ့် service ထပ်ထည့်မှာဖြစ်တဲ့အတွက် ဒီတိုင်း blank ပဲဖြစ်ပါတယ်။

```
root@security:~# tail -n 5 /etc/shadow
gnome-initial-setup:*:18474:0:99999:7:::
gdm:*:18474:0:99999:7:::
cops:$6$2jNoPCmaKzj1lAJ0$gK5T5KHkZ0F/IMckc8vSpcUvRXGT/ZnCW7I7Y34sNZ4wI
RvppJA/:18581:0:99999:7:::
systemd-coredump:!!:18581:::::
student:$6$htFYJHLOWB7/AXam$neqrD1SdNxiPGRY4iqRG8WRZoKnnwySdQwu68rvNp
LH00ZxfPR/:18585:0:99999:7:::
root@security:~#
```

**tail** command အကြောင်းကို သိပီးပီဆိုတော့ အထက်ပါ ပုံမှာသုံးထားတဲ့ option လေးကတော့ -n 5 ဖြစ်ပါတယ်။ argument အနေနဲ့ /etc/shadow ဆိုတဲ့ file ကို ထုတ်ကြည့်ထားတာဖြစ်ပါတယ်။ -n 5 ဆိုတာကတော့ လိုင်း ၅ ကြောင်းကို ကြည့်ချင်လို့ဖြစ်ပါတယ်။ tail command ရဲ့ default output ထုတ်ပေးတဲ့ line ဟာ ၁၀ ကြောင်းဖြစ်ပါတယ်။ ၅ ကြောင်းပဲ ကြည့်ချင်တဲ့အတွက် -n 5 ဆိုပြီး -n option ကို ထည့်ပေးရတာပါ။

အိုကေဒီထဲမှာ student ဆိုတဲ့ line ကို လေ့လာကြည့်မယ်ဆိုရင် student ဆိုတဲ့ username ပါမယ်။ colon ခြားပြီး ပြထားတဲ့ ရှုပ်နေတဲ့ စာတစ်ချို့တွေ့ရပါလိမ့်မယ်။ ဒါက password



သတ်မှတ်ထားတဲ့အတွက် password encrypt လုပ်ထားတဲ့ ဖိုင်ဖြစ်ပါတယ်။ ဒီစာကြောင်းကို သေချာကြည့်မယ်ဆိုရင် \$ နဲ့ password ကို သုံးပိုင်းပိုင်းထားတာကို တွေ့ရပါလိမ့်မယ်။

**ပထမ \$** နောက်က တော့ md5 algorithm ကို အသုံးပြုထားတဲ့ encrypted password ဖြစ်ပါတယ်။

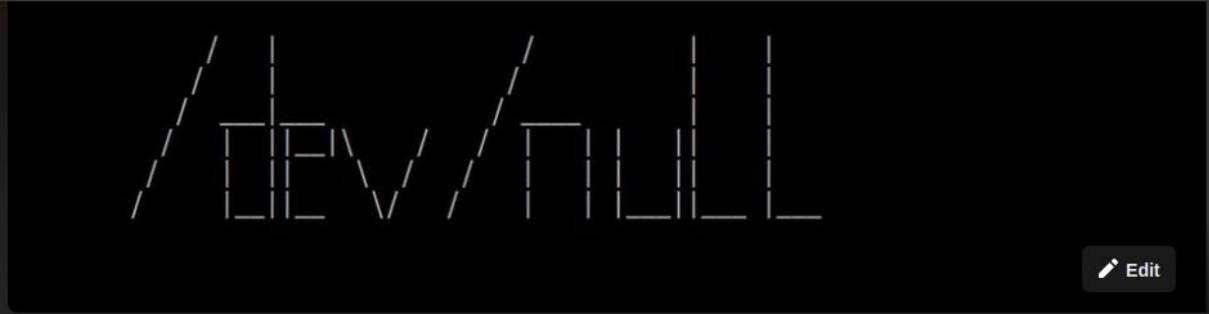
**ဒုတိယ \$** နောက်ကတော့ sha256 algorithm နဲ့ အသုံးပြုပြီး encrypted password ဖြစ်ပါတယ်။

**တတိယ \$** အနောက်ကတော့ SHA512 algorithm ကို အသုံးပြုထားတဲ့ encrypted password ဖြစ်ပါတယ်။

ကျွန်တော်တို့ သတ်မှတ်လိုက်တဲ့ password တွေကို password သတ်မှတ်လိုက်တဲ့အချိန်နဲ့ ဒီလို algorithm တွေကို အသုံးပြုပြီး encrypted လုပ်ထားတာဖြစ်ပါတယ်။ User တွေဟာ အချင်းချင်း password တူညီစွာသတ်မှတ်ထားရင်တောင် encrypted လုပ်ထားတဲ့ format ကတော့မတူညီပါဘူး။ ဒီ code တွေကို decrypt လုပ်ဖို့အတွက် ကျွန်တော်တို့ အသက်ရဲ့ သက်တမ်းတစ်ဝက်လောက်ကြာနိုင်ပါတယ်။ အနောက်က colon တွေကတော့ အပေါ်မှာ ပြောထားတဲ့အတိုင်း user account ရဲ့ သက်တမ်းတွေနဲ့ account expire, password expire ဖြစ်မယ့် အချိန်တွေပဲဖြစ်ပါတယ်။

### Account Age


















အကောင့်တစ်ခုရဲ့ သက်တမ်းတွေကို Defaults အရ သတ်မှတ်ပေးထားတဲ့ file လေးကတော့ **/etc/login.defs** ပဲဖြစ်ပါတယ်။ ဒီ file ထဲမှာ သွားရောက်ပြင်ဆင်ပြီး လိုအပ်သလို သက်တမ်းသတ်မှတ်နိုင်သလို ရှိပြီး သားအကောင့်တွေရဲ့ သက်တမ်းတွေကိုလည်းလိုအပ်သလို ပြင်ဆင်ပြောင်းလဲ သတ်မှတ်နိုင်ပါတယ်။



[Edit](#)



## Linux Digger


Public group · 175 members






[+ Invite](#)

[About](#) [Discussion](#) [Rooms](#) [Members](#) [Events](#) [Media](#)







 Room  Request Shift Cover  Photo/Video

From Notifications

### About

Deep And Dive to the Linux Black Hole

-  **Public**  
Anyone can see who's in the group and what they post.
-  **Visible**  
Anyone can find this group.

