Introduction to SELinux

SELinux ဆိုတာသည် Linux ကိုလေ့လာမည့်သူတိုင်း ကြားဖူးကြမယ်ထင်ပါတယ်။ SELinux (Security-Enhanced Linux) ဆိုတာ Security အတွက်ထပ်မံပြုလုပ်ထားတဲ့ အလွှာလေး တစ်ခုဖြစ် ပါ တယ်။ ကျွန်တော်တို့ရဲ့ Security ကျိုးပေါက်သွားခဲ့ရင် impact ဖြစ်မယ့် Scope တွေကိုလဲသူက လျော့ချပေးပါတယ်။ SELinux ဆိုတာ Antivirus လိုလဲမဟုတ်ပါဘူး။ Password , Firewall လိုတခြား Security System တွေကိုလဲ အစားထိုးဖို့ မဟုတ်ပါဘူး။ SELinux သည် Linux Distro တွေဖြစ်တဲ့ Red Hat , CentOs , Fedora linux အစ ရှိတဲ့ Distro တွေမှာ Default အနေနဲ့ပါဝင်ပါတယ်။ Kali , Ubuntu တို့မှာတော့ ထည့်သွင်း အသုံးပြုနိုင်ပါတယ်။

SELinux ဟာ အမေရိကန်နိုင်ငံ (NSA:National Security Agency) ကနေ စတင်ခဲ့တာဘဲ ဖြစ်ပါတယ်။ နောက်ပိုင်းမှာတော့ Linus Torvalds ရဲ့ အကြံပေးမှုနဲ့အတူ NSA ဟာ LSM(Linux Security Modules) ဆိုတဲ့ Framwork ကိုအသုံးပြုကာ SELinux ကို Linux Kernal ဆီ ပေါင်းစပ်ခဲ့ပါတယ်။ နောက်ပိုင်းမှာ RedHat နဲ့ NSA တို့ပူးပေါင်းကာ SELinux ကို ကောင်းသတဲ့ ကောင်းအောင်ကြိုးပန်းလာကြပါတယ်။ သူတို့ရဲ့ကြိုးပန်းမှုကြောင့် Initial relase အနေဖြင့် 2000 ခုနှစ် Dec 22 မှာ စတင်ခဲ့ပြီး Stable Release အနေဖြင့် 2018 ခုနှစ် May 24 မှာ စတင်ခဲ့ပါ တယ်။ SELinux အကြောင်းကိုလေ့လာမည်ဆိုလျှင် ပထမဦးဆုံး DAC နဲ့ MAC ဆိုတာကို သိဖို့လိုအပ် ပါတယ်။

DAC (Discrertionary Access Control)

Lower Level Access Control လို့လဲပြောနိုင်ပါတယ်။ User အနေနဲ့ ကိုယ့်ဘာသာကိုယ် သတ်မှတ်တဲ့ Security Access Control ကိုဆိုလိုပါတယ်။
chmod (Change Mode) ဆိုတဲ့ Command ကိုသုံးပြီး file တွေ Folder တွေရဲ့ User တွေ group တွေနဲ့ other user တွေအလိုက် read (r),write(w),execute(x) အစရှိသဖြင့် သတ်မှတ်ခြင်း Special Parmission သတ်မှတ်ခြင်းတွေကို DAC လို့ခေါ်တာဖြစ်ပါတယ်။

setfacl , getfacl အစရှိသဖြင့် ACL နဲ့ Permission ကန့်သတ်တာတွေသည်လည်း DAC ဖြစ်ပါတယ်။ ဆိုရရင် DAC မှာ owner ဖြစ်တဲ့ user အနေဖြင့် object တွေအပေါ် access control ကိုစိတ်ကြိုက်ဖန်တီးနိုင်သလို တခြား user တွေကိုလဲ လွှဲပြောင်းပေးနိုင်ပါတယ်။ အချုပ်အားဖြင့် DAC ဟာ file , folder တွေရဲ့ Owner ရဲ့ ဆုံးဖြတ်ချက်နဲ့ သတ်မှတ်တဲ့ Object Access Privileges တွေဘဲလို့ဆိုနိုင်ပါတယ်။

MAC (Mandatory Access Control)

MAC ဆိုတာ စည်းမျဉ်းစည်းကမ်း တရပ်နဲ့ထိန်းချုပ်တဲ့ Security Strategy လုံခြုံရေး မဟာဗျူဟာတရပ်ပါ။
အပေါ်မှာပြောခဲ့တဲ့ Lower Level Access Control လို့ခေါ်တဲ့ DAC အပေါ်ကို ထပ်မံအထူးပြုထားတာလည်းဖြစ်ပါတယ်။
MAC အတွက် criteria တွေကို system administrator တွေက သတ်မှတ်ပေးပါတယ်။ Operating System နဲ့ Kernal က ထိုသတ်မှတ်ချက်ကို လိုက်နာဆောင်ရွက်ပေးပါတယ်။ တခြား User တွေအနေနဲ့ ထိုသတ်မှတ်ချက်ကို ပြောင်းလို့မရပါဘူး။ MAC ဟာ user,file,folder,service တွေအပေါ်မှာ Label တွေ Role တွေနဲ့ စီမံခန့်ခွဲပါတယ် ဆိုရရင် User , Subject နဲ့ Object ကြားမှာ label တခုသတ်မှတ်လိုက်ပြီး အပြန်အလှန် Control လုပ်သွားတာဘဲဖြစ်တယ်။ အချုပ်ဆိုရရင် DAC ဟာ user based ဖြစ်ပြီး MAC ဟာ policy based လို့သတ်မှတ်နိုင်ပါတယ်။Linux Kernal မှာ အလုပ်လုပ်တဲ့ အရာသည် policy based ဖြစ်တဲ့ MAC ဘဲဖြစ်ပါတယ်။

#Networking & Information Technology