Capabilitati in Linux

Pe una din masinile create, instalati urmatoarele pachete:

sudo apt-get install libattr1-dev
wget http://www.kernel.org/pub/linux/libs/security/linux-privs/libcap2/libcap-2.21.tar.gz
tar xvf libcap-2.21.tar.gz
cd libcap-2.21
sudo make
sudo make install

Verificati daca SELinux (Security Enhanced Linux) este instalat

ls /etc/selinux/config pentru a vedea daca fisierul exista.

In caz afirmativ, dezactivati temporar prin comanda:

sudo setenforce 0

Vizualizarea drepturilor de acces (***r,w,x***) asupra unui fisier:

ls -l fisier

Subcampurile de drepturi sunt asociate in aceasta ordine: proprietarului fisierului, grupului de care apartine acesta si restului utilizatorilor.
Modificarea drepturilor de acces:

chmod ... pentru detalii **man chmod**

Daca in locul dreptului '**x**', este setat '**s**', acesta indica faptul ca un fisier are setat un bit **SUID** (Set User ID). Mecanismul este utilizat pentru a permite altor utilizatori sa execute o comanda ce necesita drepturi de root: executabile ce au bitul SUID setat si proprietarul fisierului este root. Acest lucru poate conduce la vulnerabilitati de securitate. Daca un executabil care are bitul SUID are o vulnerabilitate de securitate, atunci sistemul poate fi compromis (un atacator poate obtine drepturi de root pe sistem).
Pentru a preveni acest lucru, a fost introdusa posibilitatea de a seta **capabilitati** asupra unui executabil. Acestea permit numai o multime particulara de operatii

privilegiate. In momentul in care un program este rulat, sistemul de operare verifica capabilitatile asociate cu respectivul executabil si permite executia strict in functie de acestea (de exemplu capabilitate de a deschide socketuri raw). Astfel este redus riscul ca un utilizator neautorizat sa obtina drepturi extinse in sistem.

Asignarea de capabilitati unui executabil:

setcap nume_capabilitati=flaguri_capabilitati program

- lista_capabilitati: lista de nume de capabilitati, separate prin virgula lista de capabilitati din Linux: **man capabilities**
- flaguri_capabilitati: p (permitted), e (effective), i (inheritable)

Eliminarea completa a capabilitatilor asociate unui program:

setcap -r program

Obtinerea capabilitatilor asociate unui program:

getcap program

Pentru a afla locatia pe disc a unei comenzi:

which comanda

Exercitii:

1. Eliminati bitul SUID din comanda **ping** si rulati comanda folosind capabilitati.
2. Afisati fisierul */etc/shadow* folosing comanda **less** si capabilitati.
3. Eliminati bitul SUID din comanda **passwd** si rulati comanda folosind capabilitati.
    - Comanda **passwd** folosita la schimbarea parolei creeaza un nou fisier */etc/nshadow*, modifica apoi proprietarul fisierului ca fiind root. Dupa aceasta este deschis fisierul */etc/shadow* si se copie tot continutul acestuia in */etc/nshadow* modificandu-se doar parola utilizatorului pentru care este executata comanda. In final, fisierul */etc/nshadow* este mutat in locul lui */etc/shadow*.