Documentație proiect ASO

Faza 3

Student Ban Bogdan

Grupa 30643

Contents

Descriere

Faza 3 a proiectului presupune securizarea sistemului. Sursele de cod C încărcate de concurenți pot să exploateze sistemul pe care sunt rulate (mașina virtuală). Pentru a remedia această problemă, s-a creat un utilizator cu privilegii limitate *„aso_user”.* Restricțiile sunt

- imposibilitatea intra în alte directoare (nu poate să execute comanda *cd*)
- imposibilitatea de a vizualiza conținutul fișierelor de test

Acestă modalitate de securizare nu este foarte sigură și, în cazul unui atac mai puternic, unele date de pe sistem ar putea fi compromise (furate, criptate etc). Se vor prezenta metode de securitate mai avansate în capitolul „Alte modalități de securizare”.

Detalii de implementare

S-a adăugat un utilizator nou în sistem („aso_user”) și s-a setat directorul „home” în „/aso_dirs”

>sudo useradd aso_user –d /aso_dirs/

Pentru a interzice deplasarea între directoarele sistemului, i s-a atribuit un „restricted shell” (rbash) folosind comanda

>sudo usermod –shell /bin/rbash aso_user

Deoarece fișierele de test sunt stocate în directorul în care este blocat „aso_user”, li s-au eliminat anumite permisiuni (citirea) pentru „others” folosind comanda

>sudo chmod o-r inputX.txt

>sudo chmod o-r outputX.txt

Unde X va fi pe rând 1, 2, 3.

După compilarea surselor C, executabilele vor fi rulate în numele utilizatorului „aso_user”. Pentru a realiza acest lucru, s-au facut 3 modificări identice în scriptul de evaluare. S-a înlocuit linia

os.system(path + programName[:-2])

cu linia

os.system(”sudo –H –u aso_user bash -c” + ”`” + path + programName[:-2] + “`”)

Funcția os.system efectuază un apel de sistem, în acest caz o comandă linux. Astfel, se rulează programul în numele utilizatorului „aso_user”.

Posibilități de dezvolare ulterioară

După cum s-a specificat și mai sus, acestă metodă oferă o securitate redusă și poate fi exploatată. Pentru a îmbunătăți securitatea sistemului se poate crea un „ chroot jail”, adică un nou arbore de directoare conenctat la resursele necesare pentru rularea unui proces. În acest caz, procesul este rularea programului C al unui concurent. Acest mod de securizare este mai eficient deoarece împiedică comunicarea cu orice alt director sau fișier din afara arborelui asociat procesului. Totuși, și acestă securitate poate fi exploatată. Ultima variantă și cea mai eficientă devine crearea unei mașini virtuale Docker în care se va rula fiecare program.