Praktinė užduotis Nr. 1

Praktinės užduoties tikslas – susipažinti, kaip kuriami ir konfigūruojami (lokaliame kompiuteryje) vartotojai, jų teisės, prieigos prie failų, slaptažodžių politika. Pagal žemiau pateiktą scenarijų, darbas atliekamas Linux Ubuntu ir Windows 7 operacinėse sistemose atskirai, jei skliausteliuose nenurodyta kitaip. Užduoties atlikimo techniką ir būdus galima rinktis laisvai. Ties kiekvienu užduoties punktu pateiktas įrankis/būdas užduočiai atlikti yra laikytinas kaip pavyzdys. Paskutiniame užduoties punkte (Nr. 9) nurodytos komandos/įrankiai/būdai, kurie atliekant užduotį turi būti įtraukti į darbą, Jūsų pačių pasirinktose darbo vietose.

Scenarijus

Bendrovėje dirba aštuoni darbuotojai, suskirstyti į keturias grupes:

1. Sistemų administratorius (God),
2. Vadovas (Boss),
3. Administracija (Fin1 ir Fin2),
4. Vadybininkai (Man1, Man2, Man3, Man4),
5. Nežiniukas (Supreme).

Darbuotojų prieigos leidimai:

1. Vadovas turi visus leidimus.
2. Kiekvienas vartotojas turi visus leidimus savo kuriamiems objektams, o kitiems savo grupės objektams - tik skaitymo leidimą.
3. Yra bendras katalogas, kuriame visi darbuotojai turi visus leidimus.
4. Yra specialus katalogas, kuris prieinamas tik nurodytiems vartotojams.
5. Grupės vartotojas turi peržiūros leidimą žemesnių grupių objektams.
6. Nežiniukui parinkite sudėtingą leidimų schemą (su specialiais leidimais), pagal savo pageidavimą.

Užduotis

Reikia sukurti bent po vieną vartotoją iš kiekvienos scenarijuje nurodytos grupės ir:

1. Nustatyti jiems prieigos leidimus nurodytus scenarijuje (Windows: Computer management, icacls, Powershell; Linux: Users and groups, adduser).
2. Pasirinkti katalogą, priklausantį vadovui, ir suteikti įrašymo leidimą administracijos darbuotojui arba vadybininkui (Windows: object security tab, icacls, Powershell; Linux: chmod, setfacl).
3. Įgalinti slaptažodžių stiprumo ir ilgalaikiškumo politiką pagal šių dienų aktualijas IT srityje: minimum password length, maximum password age ir t.t. (Windows: local security policy, #net accounts; Linux: /etc/pam.d/common-password, chage username).

4. Darbuotojams uždrausti:
    a. Windows (gpedit.msc) - tinkinti monitoriaus nustatymus, keisti darbastalio fono paveikslėlį, skaityti išorines laikmenas, išjungti kompiuterį.
    b. Linux – pasiekti terminal (CLI), uždrausti panaudoti tam tikrą komandą, konfigūruoti tinklo adapterį (*angl.* interface).
5. Aktyvinti žurnalinių įvykių registravimą ir aktyvuoti Jums aktualių įvykių registravimą:
    a. Windows: audit logon events, audit system events (local security policy);
    b. Linux: rsyslog.
6. Perimti nuosavybės teisę (*angl.* ownership) pasirinktiems failams, kuriuos iš pradžių reikia sukurti prisijungus su darbuotojo ir administratoriaus vartotoju (Windows: object security tab; Linux: chown).
7. Pridėkite papildomų vartotojų ir įgalinkite jiems sudėtingas prieigos kontrolės schemas.
8. Įgyvendinkite visapusišką žurnalizavimą ir sesijų įrašymą privilegijuotiems vartotojams (angl. Logging and Sessions recording for Privileged users) (Windows ir Linux).
9. Taikyti nurodytas komandas/įrankius/būdus:
    a. Windows (icacls, takeown, inheritance, net accounts, LGP (local group policy), auditpol, NTRIGHTS);
    b. Linux (chmod, setfacl, getfacl, default ACL, SUID, GUID, sticky bit, chown, passwd, chattr).

Papildoma užduotis (neprivaloma)

1. Pagrindinę darbo dalį atlikite CLI aplinkoje, atitinkamai tiek, kiek leidžia naudojamos operacinės sistemos galimybės. Darbo rezultatas gali būti ir „skriptas“, be vartotojo įsikišimo sukonfigūruojantis sistemą pagal scenarijų.
2. Savarankiškai papildykite pagrindinėje užduotyje pateiktą scenarijų taip, kad prireiktų naudoti specialius leidimus (angl. special permissions) daugeliui vartotojų ir panaudokite bent tris skirtingus specialius leidimus pagal jūsų pačių papildytą scenarijų.
3. Taikydami savo pasirinktą metodą sulaužykite (angl. crash) pasirinktą aplikaciją ir peržvelkite įvykių registrą (angl. logs). Pateikite išvadas.