Lucrarea de laborator nr. 4

Controlul accesului și AAA (Autentificare, Autorizare, Contabilizare)

Scop

Scopul lucrării este configurarea și analiza mecanismelor de **autentificare, autorizare și contabilizare (AAA)** și aplicarea principiilor de control al accesului pe sisteme de operare client Windows și/sau Linux.

Cerință generală

Configurați mecanismele de **autentificare, autorizare și contabilizare (AAA)** pe un sistem de operare client (Windows, Linux sau ambele), utilizând conturi de utilizator diferite și aplicând principiul **privilegiului minim**. Verificați funcționalitatea politicilor configurate.

Cerințe obligatorii

1. Descrierea mediului de lucru

Indicați:

- sistemul de operare utilizat (versiunea inclusiv);
- mediul de lucru (sistem fizic sau mașină virtuală);
- numărul de conturi de utilizator utilizate.

2. Configurarea autentificării

Configurați și documentați:

- metodele de autentificare utilizate (parolă, PIN, autentificare locală);
- cerințele de autentificare pentru utilizatori diferiți;
- politici de autentificare (complexitatea parolei, blocarea contului după încercări eșuate).

3. Configurarea autorizării (controlul accesului)

Configurați mecanismele de autorizare prin:

- crearea a cel puțin **două conturi de utilizator** cu roluri diferite;
- atribuirea drepturilor și permisiunilor pentru fișiere, directoare sau aplicații;
- restricționarea accesului la resurse pentru utilizatorii neautorizați.

4. Aplicarea principiului privilegiului minim

Demonstrați aplicarea principiului privilegiului minim prin:

- utilizarea conturilor standard pentru activități zilnice;
- limitarea utilizării contului de administrator;
- justificarea drepturilor acordate fiecărui cont.

5. Configurarea contabilizării (Accounting)

Configurați mecanisme de contabilizare și monitorizare a accesului, indicând:

- tipurile de evenimente înregistrate (autentificări reușite/eșuate, acces la resurse);

- locația jurnalelor de securitate;
- exemple de evenimente înregistrate.

6. Verificarea funcționalității politicilor

Testați și documentați:

- accesul permis și interzis pentru diferite conturi;
- comportamentul sistemului în cazul autentificărilor nereușite;
- evidențierea funcționării corecte a politicilor configurate.

Лабораторная работа №4

Контроль доступа и AAA (Аутентификация, Авторизация, Учёт)

Цель работы

Целью данной лабораторной работы является настройка и анализ механизмов **аутентификации, авторизации и учёта (AAA)**, а также применение принципов контроля доступа на клиентских операционных системах Windows и/или Linux.

Общее требование

Настройте механизмы **аутентификации, авторизации и учёта (AAA)** на клиентской операционной системе (Windows, Linux или обеих), используя различные учётные записи пользователей и применяя принцип **минимальных привилегий**. Проверьте работоспособность настроенных политик.

Обязательные требования

1. Описание рабочей среды

Укажите:

- используемую операционную систему (включая версию);
- рабочую среду (физическая система или виртуальная машина);
- количество используемых учётных записей пользователей.

2. Настройка аутентификации

Настройте и документируйте:

- используемые методы аутентификации (пароль, PIN, локальная аутентификация);
- требования аутентификации для различных пользователей;
- политики аутентификации (сложность пароля, блокировка учётной записи после неудачных попыток входа).

3. Настройка авторизации (контроль доступа)

Настройте механизмы авторизации путём:

- создания как минимум **двух учётных записей пользователей** с различными ролями;
- назначения прав и разрешений для файлов, каталогов или приложений;
- ограничения доступа к ресурсам для неавторизованных пользователей.

4. Применение принципа минимальных привилегий

Продемонстрируйте применение принципа минимальных привилегий посредством:

- использования стандартных учётных записей для повседневной работы;
- ограничения использования учётной записи администратора;
- обоснования прав, предоставленных каждой учётной записи.

5. Настройка учёта (Accounting)

Настройте механизмы учёта и мониторинга доступа, указав:

- типы регистрируемых событий (успешные/неудачные аутентификации, доступ к ресурсам);
- расположение журналов безопасности;
- примеры зарегистрированных событий.

6. Проверка работоспособности политик

Проверьте и задокументируйте:

- разрешённый и запрещённый доступ для различных учётных записей;
- поведение системы при неудачных попытках аутентификации;
- подтверждение корректной работы настроенных политик.