Lucrarea de laborator nr. 3

Configurarea și întărirea mediului securizat (hardening)

Scop

Scopul lucrării este configurarea și aplicarea măsurilor de bază pentru întărirea securității (hardening) unui sistem de operare client, precum și evaluarea impactului acestor măsuri asupra stării generale de securitate a sistemului.

Cerință generală

Configurați și aplicați măsuri de securitate pe un **sistem de operare client** (Windows, Linux sau macOS), fără a utiliza funcții specifice sistemelor server. Analizați starea de securitate a sistemului **înainte și după aplicarea măsurilor**.

Cerințe obligatorii

1. Alegerea și descrierea mediului de lucru

Indicați:

- sistemul de operare utilizat (versiunea inclusiv);
- tipul mediului (sistem fizic sau mașină virtuală);
- tipul de utilizator (standard / administrator).

2. Actualizări de securitate

Aplicați toate actualizările de securitate disponibile pentru sistemul de operare ales și descrieți:

- metoda utilizată pentru actualizare;
- starea sistemului înainte și după actualizare.

3. Gestionarea serviciilor și aplicațiilor neutilizate

Identificați și dezactivați **minimum 3 servicii sau aplicații neutilizate**, indicând:

- denumirea serviciului/aplicației;
- rolul acestuia;
- motivul dezactivării;
- impactul asupra securității.

4. Configurarea protecției antivirus / antimalware

Configurați mecanismul de protecție antimalware existent pe sistemul de operare și indicați:

- soluția utilizată;
- starea protecției în timp real;
- actualizarea bazelor de semnături;
- opțiuni suplimentare de protecție activate (dacă există).

5. Configurarea politicilor locale de securitate

Configurați cel puțin **3 politici locale de securitate**, de exemplu:

- politici de parole (complexitate, expirare);
- blocarea automată a sesiunii;
- auditarea autentificărilor;
- restricții pentru conturile standard.

6. Gestionarea conturilor de utilizator

Configurați și documentați:

- diferența dintre cont standard și cont de administrator;
- restricționarea utilizării contului de administrator;
- aplicarea principiului **privilegiului minim**.

7. Măsuri de securitate specifice versiunii sistemului de operare

Identificați și implementați cel puțin o măsură de securitate nou introdusă în versiunea sistemului de operare utilizat (de exemplu: izolare aplicații, protecție suplimentară a memoriei, control al aplicațiilor).

8. Compararea stării de securitate

Realizați o comparație între starea de securitate:

- înainte de aplicarea măsurilor;
- după aplicarea măsurilor.

Comparația va fi prezentată sub formă de **tabel** sau **checklist**.

Лабораторная работа №3

Настройка и усиление защищённой среды (hardening)

Цель работы

Целью данной лабораторной работы является настройка и применение базовых мер по усилению безопасности (hardening) клиентской операционной системы, а также оценка влияния этих мер на общее состояние безопасности системы.

Общее требование

Настройте и примените меры безопасности на **клиентской операционной системе** (Windows, Linux или macOS), без использования функций, специфичных для серверных систем. Проанализируйте состояние безопасности системы **до и после применения мер**.

Обязательные требования

1. Выбор и описание рабочей среды

Укажите:

- используемую операционную систему (включая версию);

- тип среды (физическая система или виртуальная машина);
- тип пользователя (стандартный / администратор).

2. Обновления безопасности

Примените все доступные обновления безопасности для выбранной операционной системы и опишите:

- используемый метод обновления;
- состояние системы до и после установки обновлений.

3. Управление неиспользуемыми службами и приложениями

Определите и отключите **не менее 3 неиспользуемых служб или приложений**, указав:

- наименование службы/приложения;
- её назначение;
- причину отключения;
- влияние на безопасность системы.

4. Настройка антивирусной / антималварной защиты

Настройте механизм антималварной защиты, встроенный в операционную систему, и укажите:

- используемое решение;
- состояние защиты в реальном времени;
- актуальность баз сигнатур;
- дополнительные включённые функции защиты (при наличии).

5. Настройка локальных политик безопасности

Настройте не менее **3 локальных политик безопасности**, например:

- политики паролей (сложность, срок действия);
- автоматическую блокировку сеанса;
- аудит аутентификаций;
- ограничения для стандартных учётных записей.

6. Управление учётными записями пользователей

Настройте и опишите:

- различия между стандартной учётной записью и учётной записью администратора;
- ограничение использования учётной записи администратора;
- применение принципа **минимальных привилегий**.

7. Меры безопасности, специфичные для версии операционной системы

Определите и реализуйте как минимум одну меру безопасности, недавно внедрённую в используемой версии операционной системы (например: изоляция приложений, дополнительная защита памяти, контроль приложений).

8. Сравнение состояния безопасности

Выполните сравнение состояния безопасности системы:

- до применения мер;
- после применения мер.

Сравнение должно быть представлено в виде **таблицы** или **контрольного списка (checklist)**.