Лабораторна робота №1 "Механізми захисту ОС Linux".

Дана лабораторна робота узагальнює матріал відповідних робіт з курсів «Операційні системи» та «Основи технологій захисту інформації».

Попередньо необхідно знати формат і параметри наступних утиліт:
pwd, whoami, cd, ls, touch, mkdir, rmdir, rm, cp, mv,
cat, grep, wc, head, tail, sort, od, dd, xargs, cut, awk.

Для зазначених в завданні утиліт і конфігураційних файлів необхідно знати відповідний формат та параметри.

Для автоматизація рутинних операцій необхідно вміти використовувати можливості скриптових мов програмування.

Завдання роботи:

1. Ідентіфкація суб'єктів ОС. Атрибути суб'єктів (утиліта id). Облікові записи користувачів системи (файли /etc/passwd, /etc/shadow, /etc/group). Створення та управління обліковими записами (утиліти useradd, groupadd, passwd, userdel).

2. Процедура автентифікації суб'єктів.
Чи можливий вхід користувача в систему без пароля? Які користувачі не зможуть увійти в систему через стандартну процедуру автентифікації?

Перевірка стійкості паролів за допомогою утиліти John the Ripper.

Налаштування системи автентіфкації Linux за допомогою PAM-модулів (файл /etc/pam.conf та файли в каталозі /etc/pam.d/). Які параметри автентифікації можливо налаштувати у вашій системі за допомогою PAM?

3. Обліковий запис суперкористувача. Права суперкористувача в системі.
Чи можливе існування в системі декількох облікових записів суперкористувача?
Виконання програм з правами суперкористувача або іншого користувача (утиліти su, sudo, файл /etc/sudoers).

4. Різновиди файлових об'єктів. Права доступу на файлові об'єкти системи (утиліти chmod, chown, chgrp, umask). Відмінність прав доступу на каталоги і файли. Біти SUID, SGID і StickyBit - їх зміна та вплив на поведінку файлових об'єктів.

Жорсткі і символічні посилання на файлові об'екти (утиліта ln).

Атрибути файлів (утиліти lsattr, chattr). На що впливають атрибути файлів?

Можливості Linux Capabilities (утиліти getcap, setcap, getpcaps, capsh).

Можливості Linux ACL (утиліти getfacl, setfacl).

Пошук об'єктів в файлової системі за деякими параметрами (наприклад, із заданими правами доступу). Утиліта find.

5. Управління процесами в системі (утиліти ps, top, kill, renice).

6. Управління ресурсами системи (утиліти ulimit, cpulimit, nice, ionice, quota, trickle, cgroups).

7. Створення замкнутої файлової системи для деякого процесу за допомогою chroot.

8. Перевірка мережного підключення (утиліти ifconfig, ping, traceroute) і контроль мережної активності в системі (утиліти netstat і fuser).

9. Використовуючи утиліти автоматичної перевірки захищеності системи (наприклад, LinPeas, Lynis, OpenSCAP ...) дізнайтеся про можливі вразливості у встановлених програмних продуктах, налаштуваннях, правах доступу тощо. Опишіть методику перевірки захищеності системи, яку вони використовують.