

ЛАБОРАТОРНАЯ РАБОТА №7.

Свидиров Кирилл, 11-902

04.05.2022

Содержание

1	Общая информация	3
2	Постановка задачи	4
2.1	Суть задания	4
2.2	Цель упражнения	4
2.3	Используемые средства	4
3	Исходное состояние	5
4	Выполнение задания	6
4.1	Получение доступа к загрузчику grub	6
4.2	Правка параметров загрузки меню grub	6
4.3	Установка нового пароля для root	6
4.4	Оформление результатов работы	7

1 Общая информация

- ✦ Работу выполнил Свидиров Кирилл Андреевич, 11-902 группа.
- ✦ Название лабораторной работы – “ЛАБОРАТОРНАЯ РАБОТА №7. ИСПОЛЬЗОВАНИЕ ЗАГРУЗЧИКА GRUB ДЛЯ ПОЛУЧЕНИЯ ПРИВИЛЕГИЙ ROOT”.

2 Постановка задачи

2.1 Суть задания

С помощью grub запустить систему в обход аутентификации, изменить пароль для root пользователя и после в обычном режиме войти под нужным логином.

2.2 Цель упражнения

На практике попробовать подменить пароль через grub.

2.3 Используемые средства

- ✈ VMware Workstation 16 Player - для запуска виртуальной машины с уязвимым образом Linux – Metasploitable.
- ✈ Metasploitable – устаревший и уязвимый образ Linux. Используется, чтобы свободно изучать существующие уязвимости операционной системы.
- ✈ grub - загрузчик операционной системы.

3 Исходное состояние

Образ Metasploitable с изменёнными репозиториями. В процессе выполнения лабораторной работы будет:

- ✎ Изменён пароль root пользователя

4 Выполнение задания

4.1 Получение доступа к загрузчику grub

- ✓ С помощью клавиши `<esc>` в момент загрузки виртуальной машины был совершён переход в grub.

4.2 Правка параметров загрузки меню grub

- ✓ Перемещением курсора стрелками была выбрана строка "Ubuntu 8.04, kernel 2.6.24-16-server (recovery mode)"
- ✓ С помощью клавиши "e" была выбрана правка параметров
- ✓ Перемещением курсора стрелками было выбрано ядро системы "kernel /vmlinuz-2.6.24-16-server"
- ✓ С помощью клавиши "e" была выбрана правка параметров
- ✓ В выведенном файле были удалены все файлы до "ro", а "ro" было заменено на "rw"-возможность записи. Также было добавлено "init=/bin/bash"-при инициализации теперь запускается bash.
- ✓ После чего были нажаты клавиши "Enter" и "b", чтобы сохранить изменения и запустить систему.

4.3 Установка нового пароля для root

- ✓ В запущенной системе пароль root был заменён командой `[passwd root]` на `new_password`.
- ✓ С помощью команды `[/sbin/reboot -f]` система была перезагружена
- ✓ В запущенной нормальным образом системе был получен доступ через изменённый пароль.

4.4 Оформление результатов работы

7