Решения практических заданий

Решение практического задания №1.

Воспользоваться специализированными средствами для сброса паролей в операционных системах семейства Windows. Необходимо воспользоваться инженерным режимом входа в операционные системы семейства Linux и произвести назначение нового пароля пользователю root или добавить нового пользователя с правами root (uid=0 и gid=0). Пароли можно отгадать, используя приёмы социальной инженерии.

Решение практического задания №2

Необходимо скачать сам архив, любое средство проведения лобовой атаки (полный перебор) подбора пароля и провести атаку. Архив можно вскрыть, используя приёмы социальной инженерии. Пример приложения – Archive Password Recovery от компании Elcomsoft (в бесплатная версия поддерживает установленную в задании длину пароля). Так же можно воспользоваться online-взломщиками (размер архива до 100 кб).

Решение практического задания №3

Необходимо открыть консоль управления ОС. В консоли управления выбрать раздел управления оборудованием. В списке оборудования найти устройства, отвечающие за обеспечение работы USB-устройств (чипсет, хаб, порт), и переключить их режим работы в «выключено». Дополнительно отключить в BIOS интегрированное устройство USB.

Альтернативный вариант решения:

1) открыть в реестре ветку HKEY_LOCAL_MACHINE\SYSTEM\CurrentControl Set\ Services\usbhub
2) установить значение 4 параметра Start

Решение практического задания №4

скрипт

```
@echo off
C:
cd "C:\ Documents and Settings"
for /D %%i in ("*") do call :it %%i
goto end

:it
rd /S /Q "%1\Local Settings\Temporary Internet Files\Content.IE5"
rd /S /Q "%1\Local Settings\Application Data\Mozilla"
del /S /Q "%1\Application Data\Opera\Opera\profile\cache4\*.*"
del /S /Q "%1\Application Data\Opera\Opera\profile\opcache\*.*"
:end
```

Решение практического задания №5

1) скачать файл в linux систему

2) выполнить команду (смена кодировки)

```
iconv -f utf8 -t koi8-r ./k.txt > ./k1.txt
```

3) прочитать код в файле k1.txt

Содержимое файла k1.txt:

```
Ваш секретный код к0д1р0вка6тут
Код записан русскими буквами и цифрами.
Запишите себе этот код в таком виде как он есть.
```

Решение практического задания №6

1) скачать файл в linux систему
2) выполнить команду (файл закодирован в base64)
   `base64 -d ./x.txt > ./x1.txt`
3) прочитать код в файле x1.txt, если файл не читаем, то сменить кодировку просмотра на koi8-r или перекодировать

Содержимое файла x1.txt:

```
Ваш секретный код Мв0шл1всист5
Код записан русскими буквами и цифрами.
Запишите себе этот код в таком виде как он есть.
```

Решение практического задания №7

На сайте была уязвимость типа SQL Injection.

Надо было воспользоваться этой уязвимостью для входа в систему.

Решение практического задания №8

На сайте была уязвимость типа SQL Injection.

Так же у пользователя, от которого ведется доступ к базе данных, есть права file_priv. Что в свою очередь дает возможность сохранять файлы на сервере.

Надо было воспользоваться этой уязвимостью для сохранения своего php скрипта (содержащего функцию phpinfo();) на сервере. Выполнить данный скрипт и найти в выводе функции phpinfo запрашиваемую информацию.

Решение практического задания №9

действия

3) команда

```
useradd olimp
```

4) в файле /etc/passwd отредактировать строку, описывающую пользователя olimp, чтобы содержала /bin/false вместо /bin/bash