**ФИО:** Степанищева Анастасия Андреевна

**Группа:** 11–902

**Тема:** ЛАБОРАТОРНАЯ РАБОТА №7. ИСПОЛЬЗОВАНИЕ ЗАГРУЗЧИКА GRUB ДЛЯ ПОЛУЧЕНИЯ ПРИВЕЛЕГИЙ ROOT.

**Содержание:**

1. Получение доступа к загрузчику grub

2. Правка параметров

3. Установка нового пароля

4. Форензика

5. Результаты

**Отчет:**

**1. Получение доступа к загрузчику grub**

Переходим в меню загрузки grub. Для этого при загрузке системы переводим фокус в виртуальную машину и нажимаем esc при появлении меню VMWare

**2. Выполним правку параметров загрузки меню grub**

1. выбираем ядро восстановления (Ubuntu 8.04, kernel 2.6.24-16-server (recovery mode)) и нажимаем е(для правки параметров)

2. Выбираем ядро системы (kernel /vmlinuz-2.6.24-16-server) и нажимаем е для правки параметров

3. Удаляем все параметры до параметра ro(права доступа к системе)

4. Меняем права доступа на rw

5. Устанавливаем bash первым запускаемым в системе пользовательским процессом (добавить параметр init=/bin/bash)

6. Запускаем систему (b)

**3. Установим новый пароль для root** (passwd root) и протестируем его после перезапуска системы (/sbin/reboot -f)

**4. Форензика**

Для данной атаки необходим непосредственный доступ к машине. Проследить ее довольно сложно, т.к идет в обход всех средств защиты. Единственный способ – проследить по косвенным признакам (изменение параметров запуска ядра или смены пароля root)

**5. Результаты**

Вывести в консоль

1. grep "ROOT LOGIN" /var/log/auth.log | tail -1
2. ls -l /etc/shadow
3. date
4. echo "Ф.И.О. проделавшего работу";

Изображение выглядит как текст

Автоматически созданное описание