ХОД РАБОТЫ

1.1. Получение доступа к загрузчику grub.

1. Был совершен переход в меню загрузки grub.

1.2. Правка параметров загрузки меню grub.

1. Выбрано ядро восстановления: Ubuntu 8.04, kernel 2.6.24-16-server (recovery mode);

2. Выбрано ядро системы: kernel /vmlinuz-2.6.24-16-server;

3. Удалены все параметры пока не встретится параметр: ro, отвечающий за права доступа к системе;

4. Изменены права доступа на rw и установлены bash первым пользовательским процессом запускаемым в системе, после добавления init=/bin/bash;

5. Совершен выход из меню правки и выполнен запуск системы

1.3. Установка нового пароля для root.

1) после загрузки ядра сменен пароль root командой passwd root;

2) перезапущена система командой /sbin/reboot –f;

3) произведен обычный запуск системы и протестируйте новый пароль.

1.4. Форензика.

Данный вид НСД потребует от злоумышленника непосредственного доступа к машине, что само по себе является не простой задачей, но в тоже время является крайне опасным, так как идет в обход всех средств защиты. Проследить данную атаку можно лишь по косвенным признакам, таким как изменение параметров запуска ядра или смены пароля root, что тоже не всегда заметно. В первом случае требуется постоянный контроль загрузчика grub, а второй выявляется только при попытке входа под root (если в системе присутствуют sudoers пользователи, то данный факт может вообще не вскрыться). Проследить изменения вносимые в grub нельзя, так как логирование специально не было добавлено разработчиками. При загрузке никакие сервисы по очистке логов не работают (они запускаются позже) и, если, в процессе загрузки система свалится и начнет перезагружаться, то лог будет только расти, что может привести к скорому исчерпанию места на жестком диске. В случае kernel panic мы и вовсе забьем все свободное пространство диска, система наглухо зависнет и даже в режиме восстановления её не возможно будет загрузить. Добавление очистки логов в grub противоречит идеологии ‘nix систем. Превентивной мерой в данном случае будет установка grub2. В ней

возможно настроить доступ по паролю как к отдельным пунктам меню, так и к опциям на их редактирование и запуск.

РЕЗУЛЬТАТ РАБОТЫ