

ЛАБОРАТОРНАЯ РАБОТА №7 .

ИСПОЛЬЗОВАНИЕ ЗАГРУЗЧИКА GRUB ДЛЯ ПОЛУЧЕНИЯ ПРИВИЛЕГИЙ ROOT

Выполнил Трофимов Даниил 11-902.

Ход работы:

- 1.Получение доступа к загрузчику grub.
GRUB — загрузчик операционной системы от проекта GNU. GRUB позволяет пользователю иметь несколько установленных операционных систем и при включении компьютера выбирать одну из них для загрузки. Был совершен переход в меню загрузки grub. 1.2. Правка параметров загрузки меню grub.
- 2.Выбрано ядро восстановления: Ubuntu 8.04, kernel 2.6.24-16-server (recovery mode);
3. Выбрано ядро системы: kernel /vmlinuz-2.6.24-16-server;
- 4.Удалены все параметры пока не встретится параметр: ro, отвечающий за права доступа к системе;
- 5.Изменены права доступа на rw и установлены bash первым пользовательским процессом запускаемым в системе, после добавления init=/bin/bash;
- 6.Совершен выход из меню правки и выполнен запуск системы
- 7.Установка нового пароля для root.
- 8.После загрузки ядра сменен пароль root командой passwd root;

9.Перезапущена система командой `/sbin/reboot -f`
Произведен обычный запуск системы и
протестируйте новый пароль.

Форензика

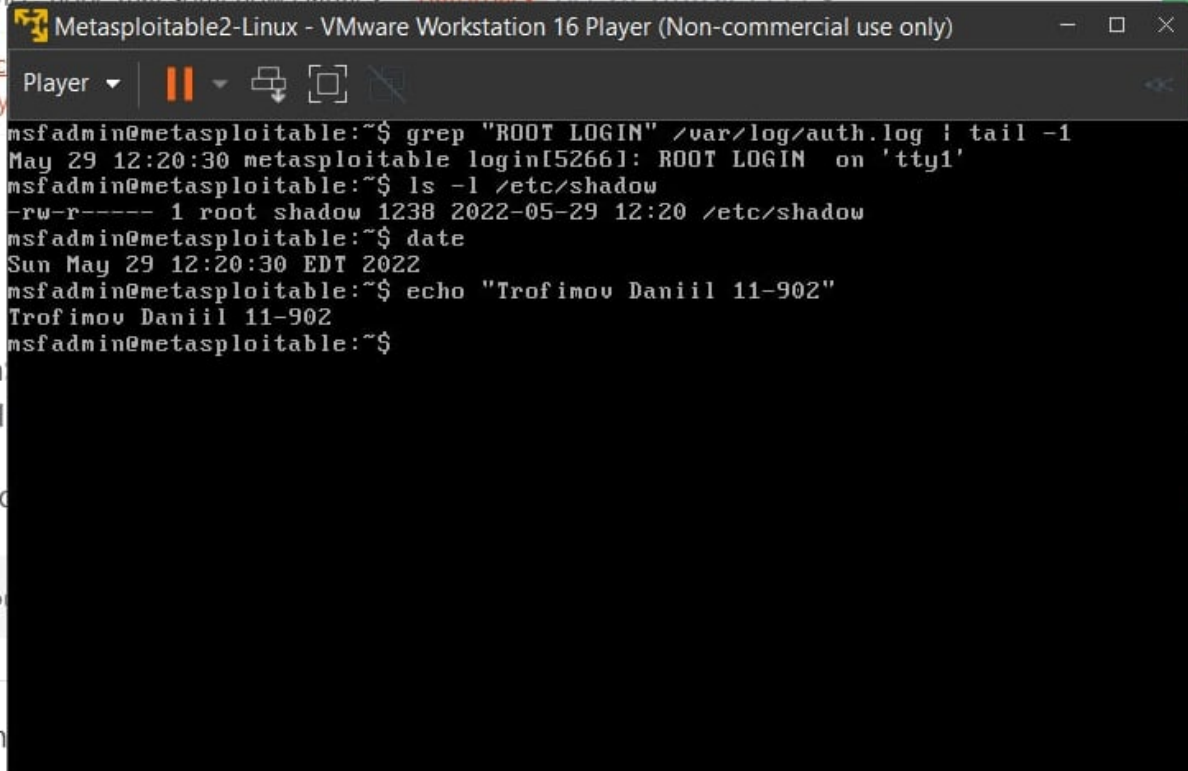
Данный вид НСД потребует от злоумышленника непосредственного доступа к машине, что само по себе является не простой задачей, но в тоже время является крайне опасным, так как идет в обход всех средств защиты. Проследить данную атаку можно лишь по косвенным признакам, таким как изменение параметров запуска 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 забудем 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:

vice: hope that somehow clarifies – [gatorback](#) Dec 28, 2016 at 19:19



```
msfadmin@metasploitable:~$ grep "ROOT LOGIN" /var/log/auth.log | tail -1
May 29 12:20:30 metasploitable login[5266]: ROOT LOGIN on 'tty1'
msfadmin@metasploitable:~$ ls -l /etc/shadow
-rw-r----- 1 root shadow 1238 2022-05-29 12:20 /etc/shadow
msfadmin@metasploitable:~$ date
Sun May 29 12:20:30 EDT 2022
msfadmin@metasploitable:~$ echo "Trofimov Daniil 11-902"
Trofimov Daniil 11-902
msfadmin@metasploitable:~$
```