

Хакимуллин Рустем Рафаилович, 11-901

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

Шаблон для упражнения:

- Цель
- Ситуация
- Алгоритм
- Результат

Содержание:

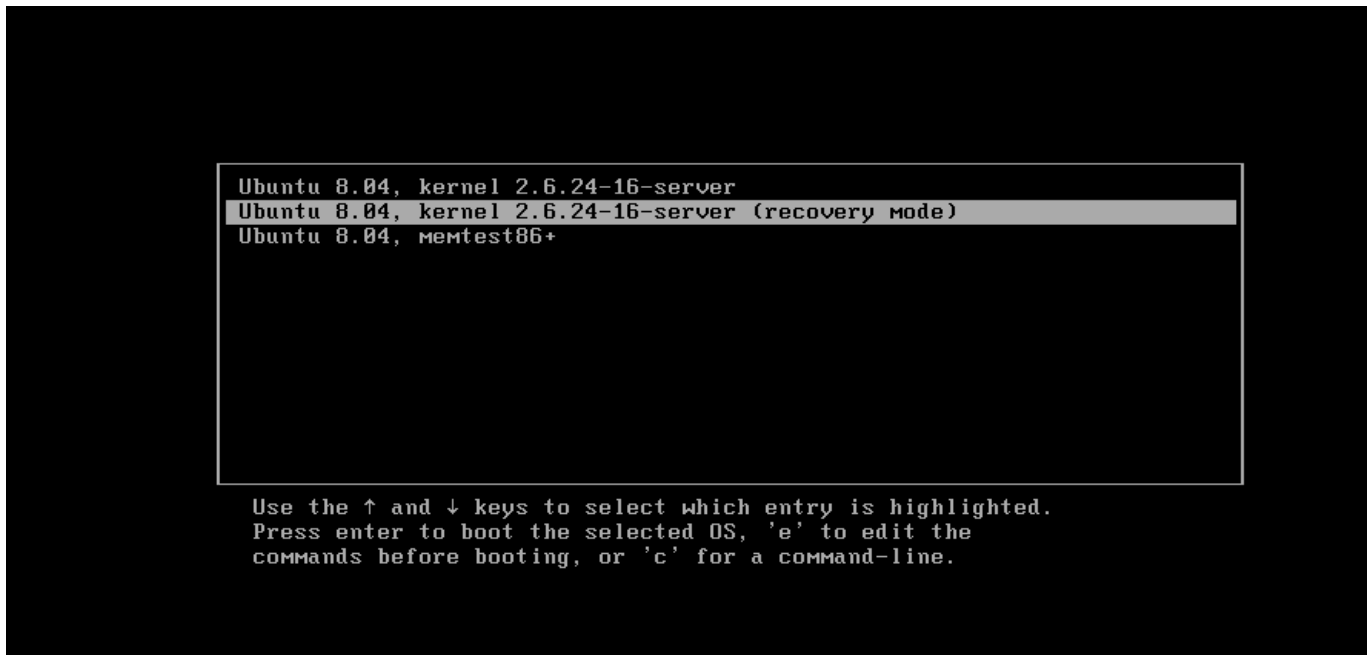
1. Получение доступа к загрузчику grub.
2. Правка параметров загрузки меню grub.
3. Установка нового пароля для root.
4. Форензика
5. Оформление результатов работы

Получение доступа к загрузчику grub.

- Цель: Получить доступ к загрузчику grub
- Ситуация: Доступ к загрузчику не получен
- Алгоритм:

1. При загрузке системы перевести фокус в виртуальную машину, кликнув мышкой в экран VMWare;

2. При появлении меню VMWare нажать клавишу для перехода в меню загрузки grub.

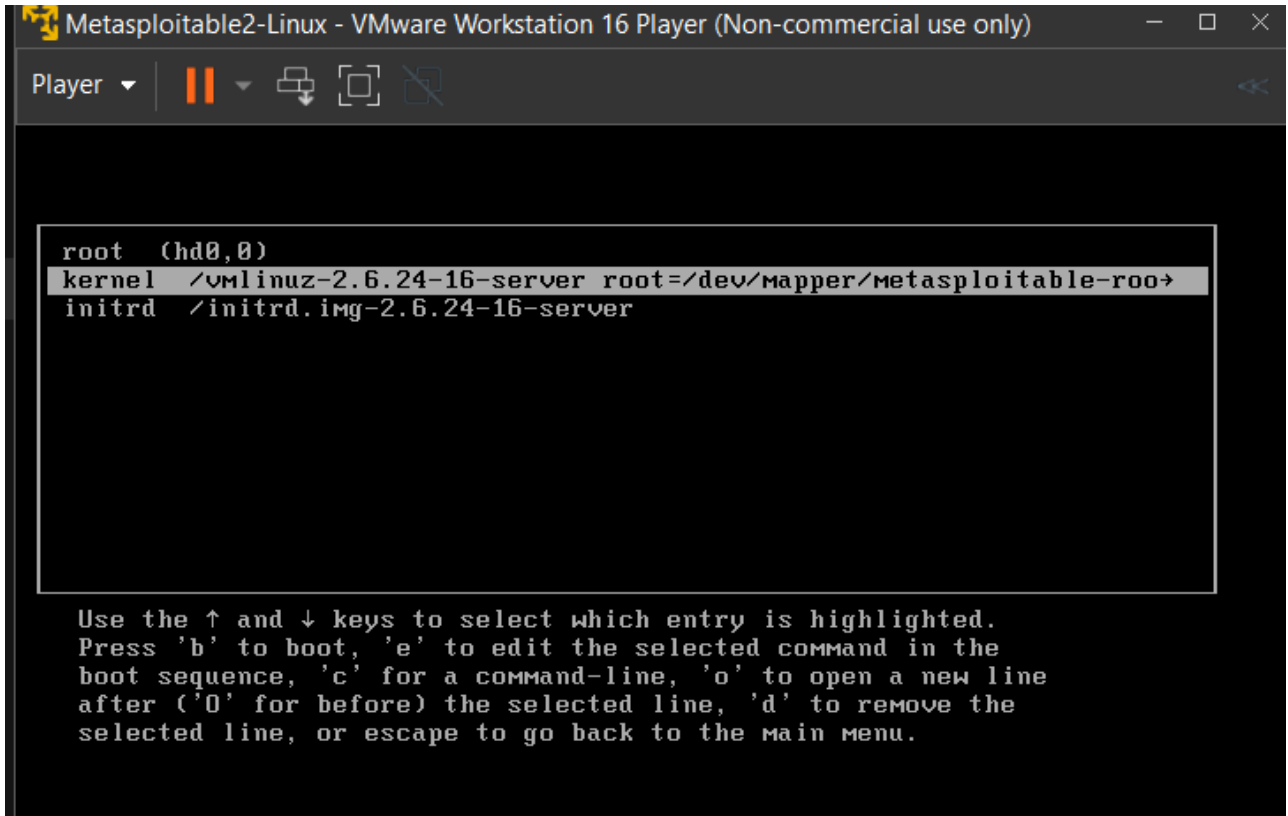


- Результат: зашли в реCOVERи мод

Правка параметров загрузки меню grub.

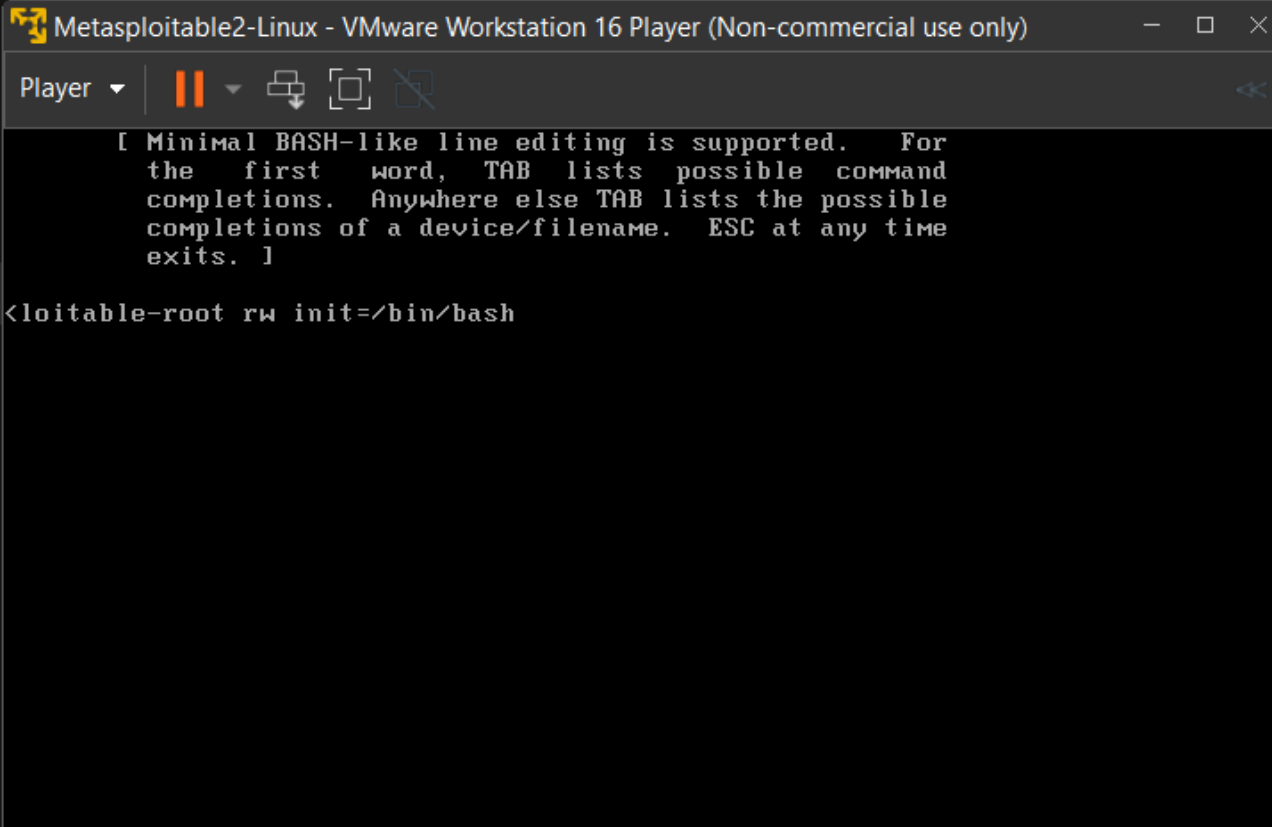
- Цель: научиться править параметры grub
- Ситуация: стоят параметры по умолчанию
- Алгоритм:
 1. Выбираем ядро восстановления: Ubuntu 8.04, kernel 2.6.24-16-server (recovery mode);
 2. Нажимаем “e” для правки параметров;

3. Выбираем ядро системы: kernel /vmlinuz-2.6.24-16-server;



4. Нажимаем “e” для правки параметров ядра системы восстановления;
5. Удаляем все параметры пока не встретится параметр: ro, отвечающий за права доступа к системе;
6. Изменяем права доступа на rw и установить bash первым пользовательским процессом запускаемым в системе, добавив

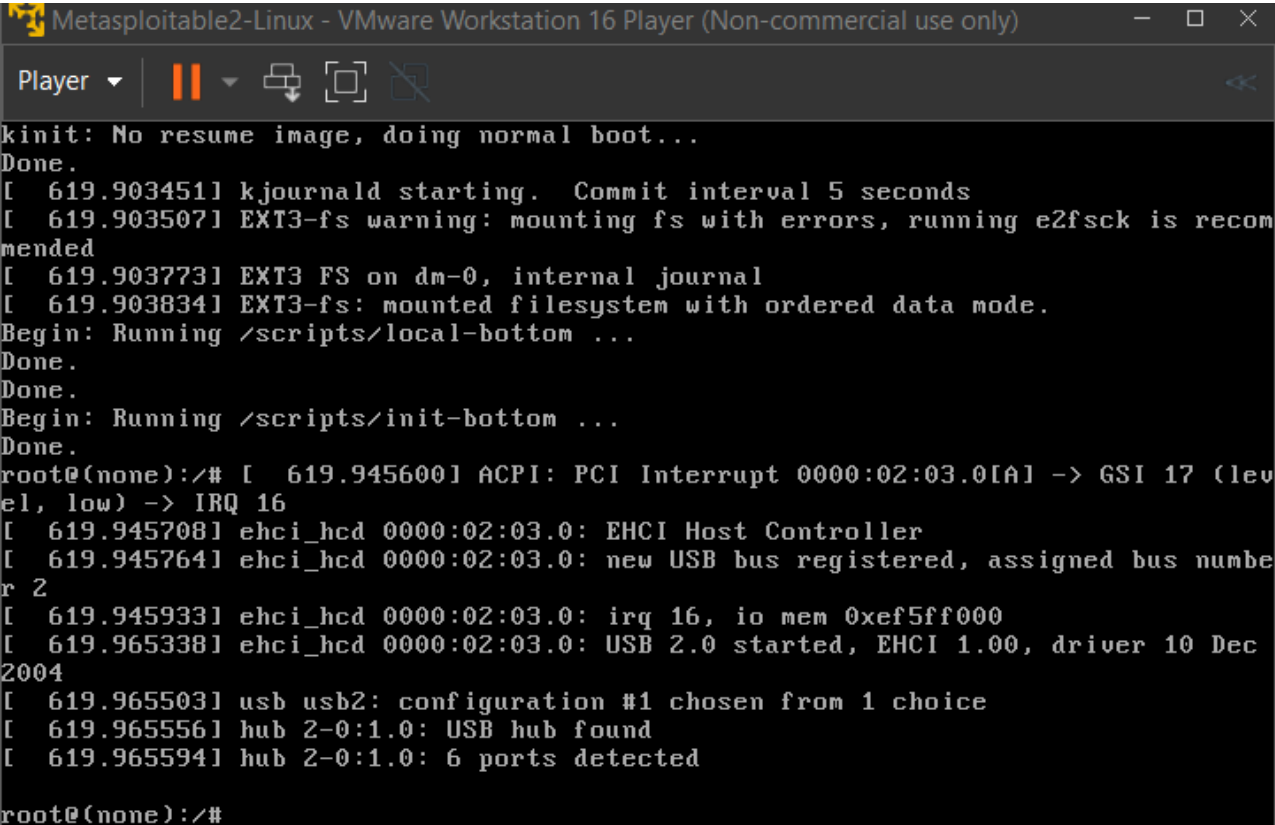
```
init=/bin/bash;
```



```
Metasploitable2-Linux - VMware Workstation 16 Player (Non-commercial use only)
Player
[ Minimal BASH-like line editing is supported.  For
the first word, TAB lists possible command
completions.  Anywhere else TAB lists the possible
completions of a device/filename.  ESC at any time
exits. ]
<loitable-root rw init=/bin/bash
```

7. Нажимаем для выхода из меню правки и выполните запуск системы, нажав "b".

- Результат: права доступа изменены



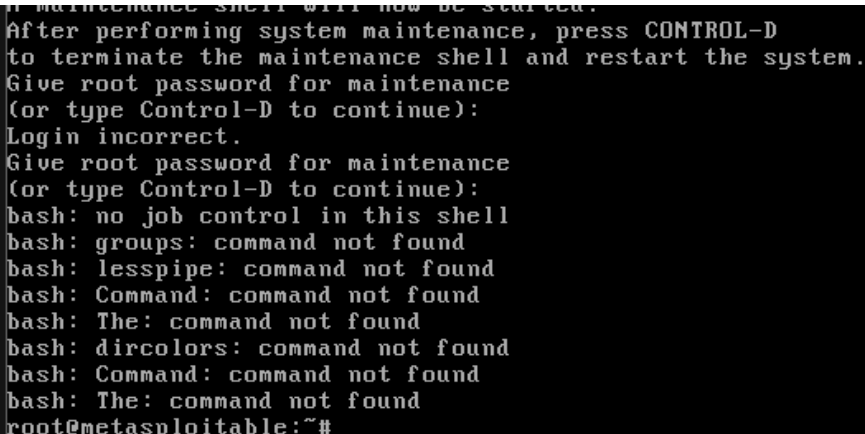
```

Metasploitable2-Linux - VMware Workstation 16 Player (Non-commercial use only)
Player
kinit: No resume image, doing normal boot...
Done.
[ 619.903451] kjournald starting. Commit interval 5 seconds
[ 619.903507] EXT3-fs warning: mounting fs with errors, running e2fsck is recommended
[ 619.903773] EXT3 FS on dm-0, internal journal
[ 619.903834] EXT3-fs: mounted filesystem with ordered data mode.
Begin: Running /scripts/local-bottom ...
Done.
Done.
Begin: Running /scripts/init-bottom ...
Done.
root@(none):/# [ 619.945600] ACPI: PCI Interrupt 0000:02:03.0[A] -> GSI 17 (level, low) -> IRQ 16
[ 619.945708] ehci_hcd 0000:02:03.0: EHCI Host Controller
[ 619.945764] ehci_hcd 0000:02:03.0: new USB bus registered, assigned bus number 2
[ 619.945933] ehci_hcd 0000:02:03.0: irq 16, io mem 0xef5ff000
[ 619.965338] ehci_hcd 0000:02:03.0: USB 2.0 started, EHCI 1.00, driver 10 Dec 2004
[ 619.965503] usb usb2: configuration #1 chosen from 1 choice
[ 619.965556] hub 2-0:1.0: USB hub found
[ 619.965594] hub 2-0:1.0: 6 ports detected
root@(none):/#

```

Установка нового пароля для root

- Цель: поставить новый пароль для root
- Ситуация: пароль не изменён
- Алгоритм:
 1. после загрузки ядра сменим пароль root командой `passwd root`;
 2. перезапустим систему командой `/sbin/reboot -f`;
 3. произведём обычный запуск системы и протестируем новый пароль.



```

A maintenance shell will now be started.
After performing system maintenance, press CONTROL-D
to terminate the maintenance shell and restart the system.
Give root password for maintenance
(or type Control-D to continue):
Login incorrect.
Give root password for maintenance
(or type Control-D to continue):
bash: no job control in this shell
bash: groups: command not found
bash: lesspipe: command not found
bash: Command: command not found
bash: The: command not found
bash: dircolors: command not found
bash: Command: command not found
bash: The: command not found
root@metasploitable:~#

```

- Результат: пароль изменён

Форензика

- Цель: ознакомиться с описанием форензики
- Результат: с описанием ознакомлен

Оформление результатов работы

```
root@metasploitable:~# grep "ROOT LOGIN" /var/log/auth.log | tail -1
May 19 13:04:00 metasploitable login[5291]: ROOT LOGIN on 'tty1'
root@metasploitable:~#
root@metasploitable:~#
root@metasploitable:~# ls -l /etc/shadow
-rw-r----- 1 root shadow 1355 2022-05-19 13:02 /etc/shadow
root@metasploitable:~#
root@metasploitable:~#
root@metasploitable:~# date
Sat May 19 14:03:23 EDT 2022
```

```
root@metasploitable:~# echo "Rustem Khakimullin"
Rustem Khakimullin
```