Некоммерческое акционерное общество
“АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ”
Институт систем управления и информационных технологий

Защита корпоративного сервера на базе Linux–сервера

ВЫПОЛНИЛ: СИБ-15-2
ИБРАГИМУЛЫ Е.
НАУЧНЫЙ РУКОВОДИТЕЛЬ: СТ. ПРЕП. ЗУЕВА Е.А.

Цель работы

- Защита корпоративного сервера на базе Linux–сервера

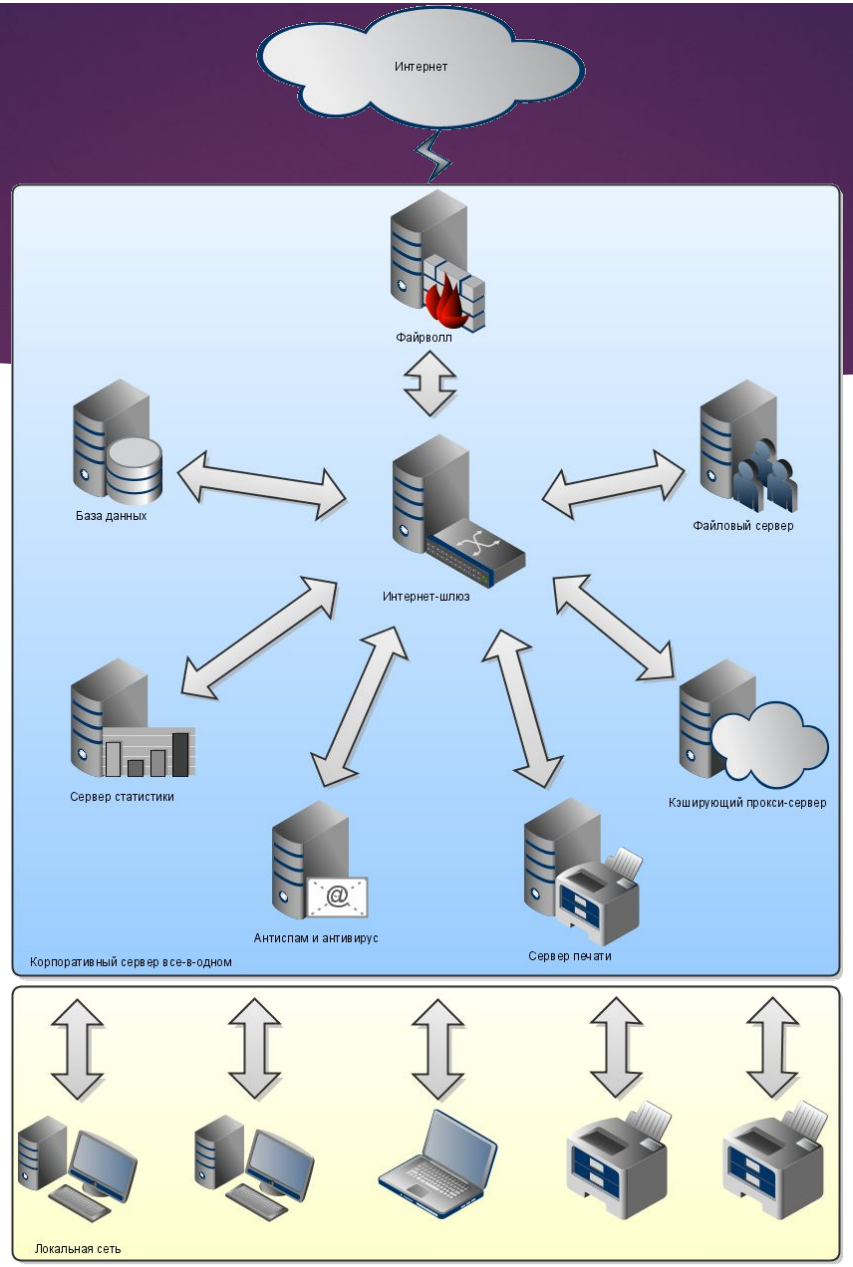
- Как защитить сервер от нежелательных атак?
- Какие выбрать методы защиты?
- Как реализовать эти методы?

Актуальность данной темы

- Каждый Linux сервер является уязвимым. Используя эти уязвимости злоумышленники могут нанести большой вред корпоративной сети. А чтобы закрыть уязвимые места, нужно ломать свою же систему самому.

Задачи

- Введение в тему защита корпоративного сервера на базе Linux-сервера
- Выбор операционной системы (Centos7)
- Поднятие сервера
- Демонстрация атаки без защиты
- Установка защиты
- Результат защиты


Интернет
Файрволл
База данных
Интернет-шлюз
Файловый сервер
Сервер статистики
Кэширующий прокси-сервер
Антиспам и антивирус
Сервер печати
Корпоративный сервер все-в-одном
Локальная сеть

Обеспечение безопасности рабочей станции

- **Защита загрузчик GRUB**

Обеспечение безопасности сервера

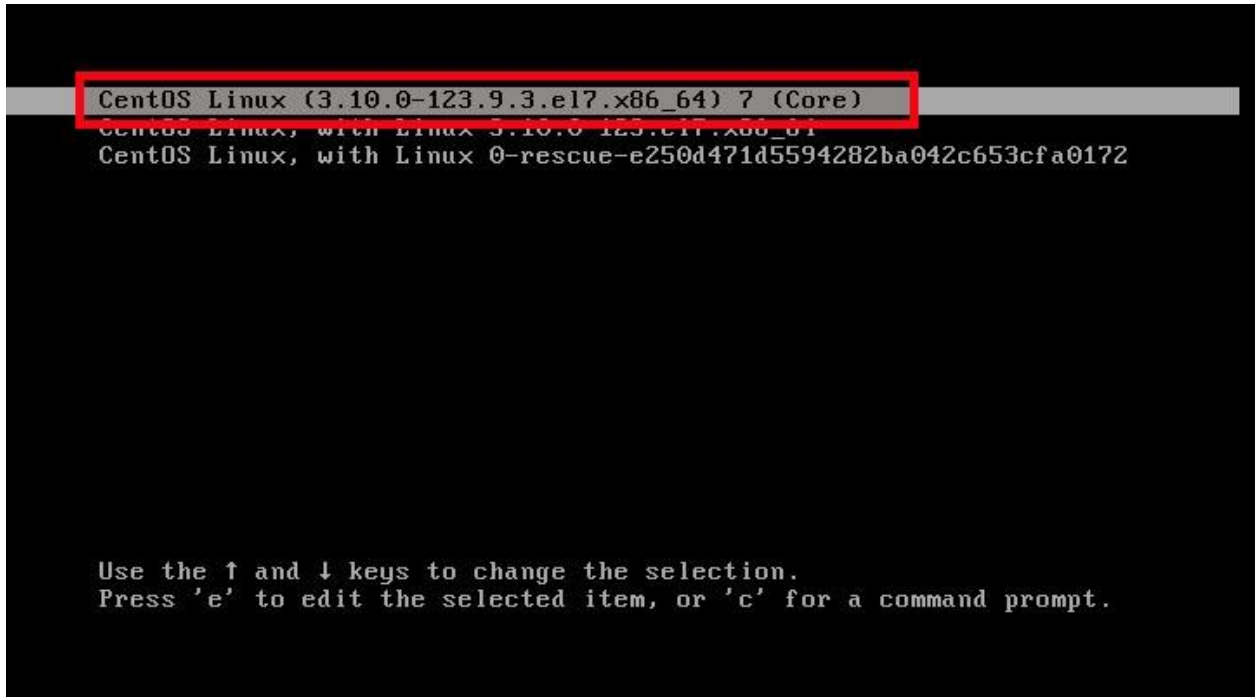
- Защита HTTP-сервера Apache

Обеспечение безопасности рабочей станции

- Если есть доступ к загрузке - это все равно, что доступ к паролю root. Любой, кто может получить доступ к загрузчику, также может легко получить доступ к правам root в вашей системе. Когда у злоумышленника есть физический доступ к загрузчику, практически нет возможности остановить его. Вот почему нам необходимо защитить паролем Grub, чтобы добавить дополнительный уровень безопасности.

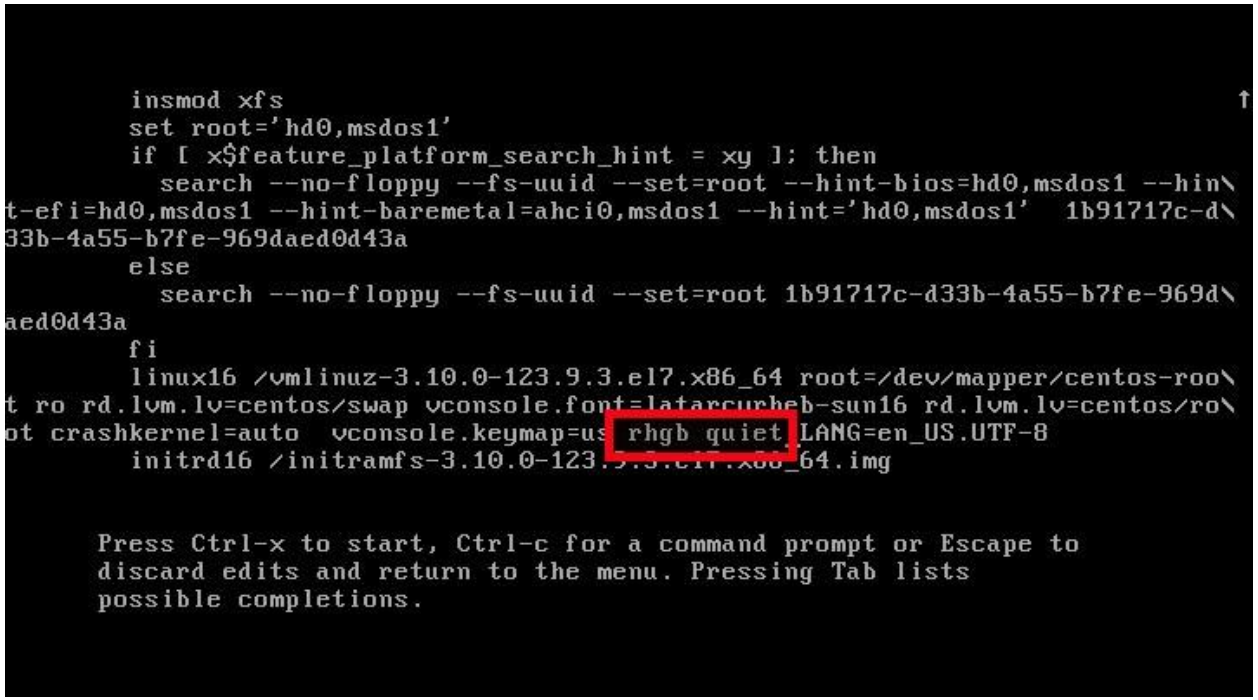
Обеспечение безопасности рабочей станции

- В меню загрузки выберем ядро, которое мы хотите загрузить, и нажимаем e, чтобы отредактировать выбранную загрузочную запись.



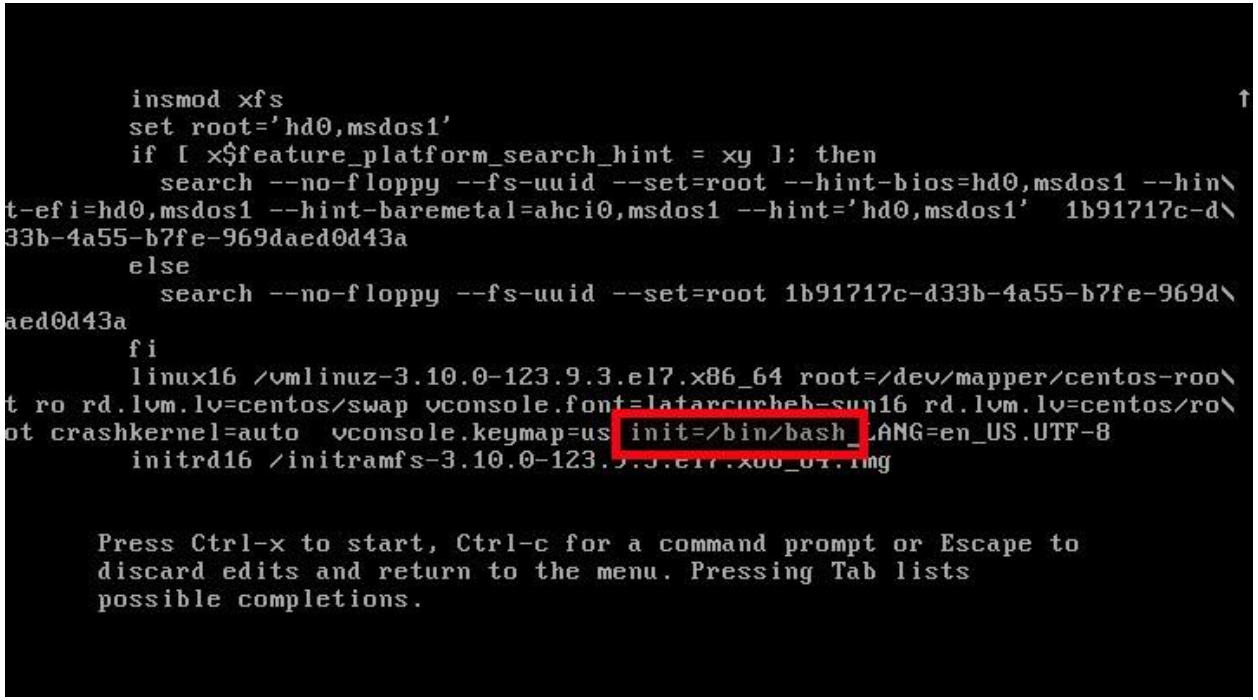
Обеспечение безопасности рабочей станции

- Находим строку rhgb quiet:



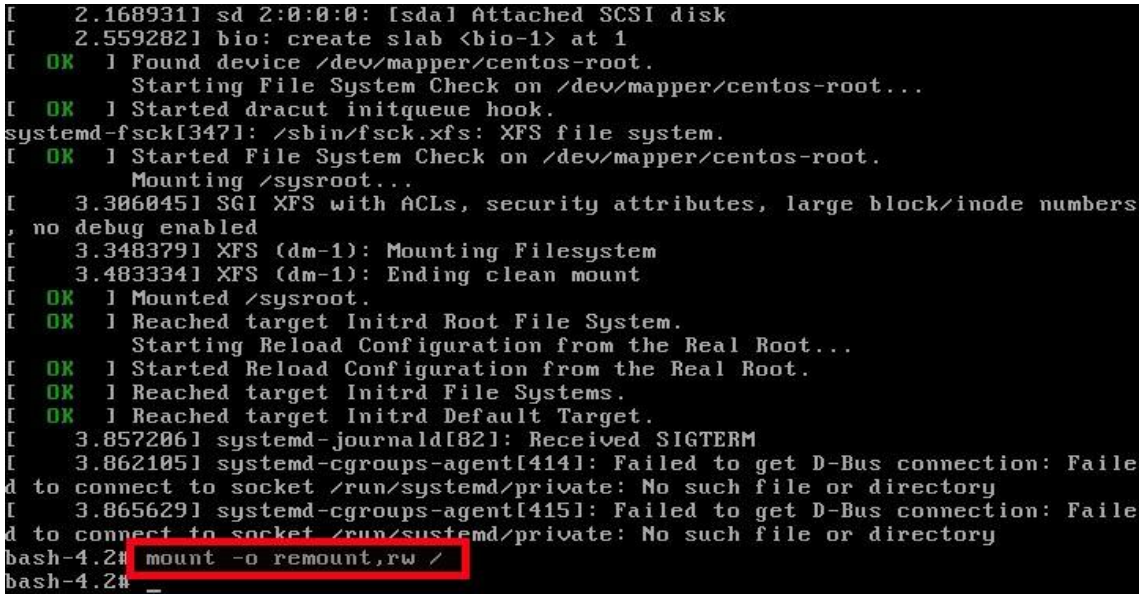
Обеспечение безопасности рабочей станции

- и замените его на **init=/bin/bash**



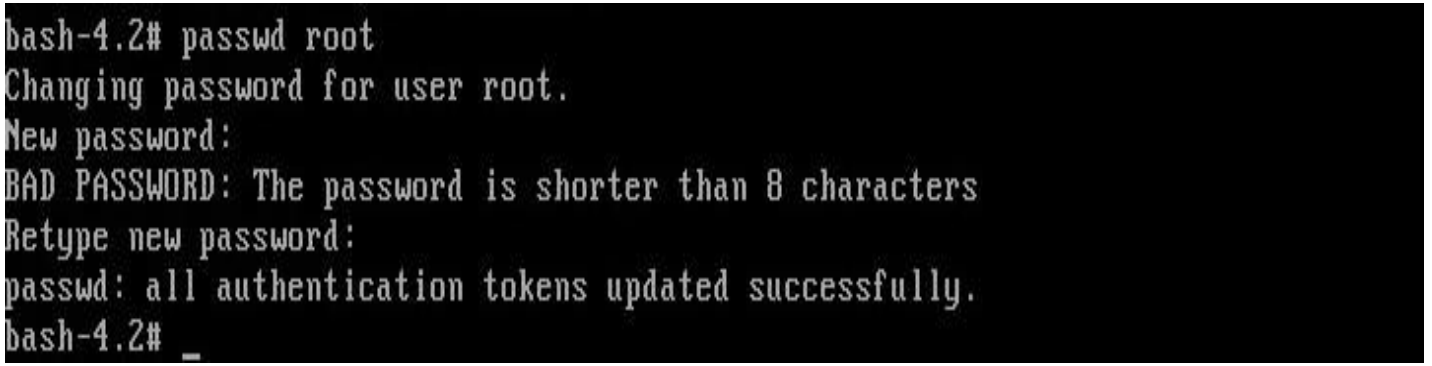
Обеспечение безопасности рабочей станции

- Затем нажимаем CTRL + X, чтобы войти в однопользовательский режим.
- Вводим следующую команду, чтобы смонтировать корневую (/) файловую систему в режим чтения / записи.



Обеспечение безопасности рабочей станции

- Теперь сменим пароль пользователя root с помощью команды:
- passwd root



Обеспечение безопасности рабочей станции

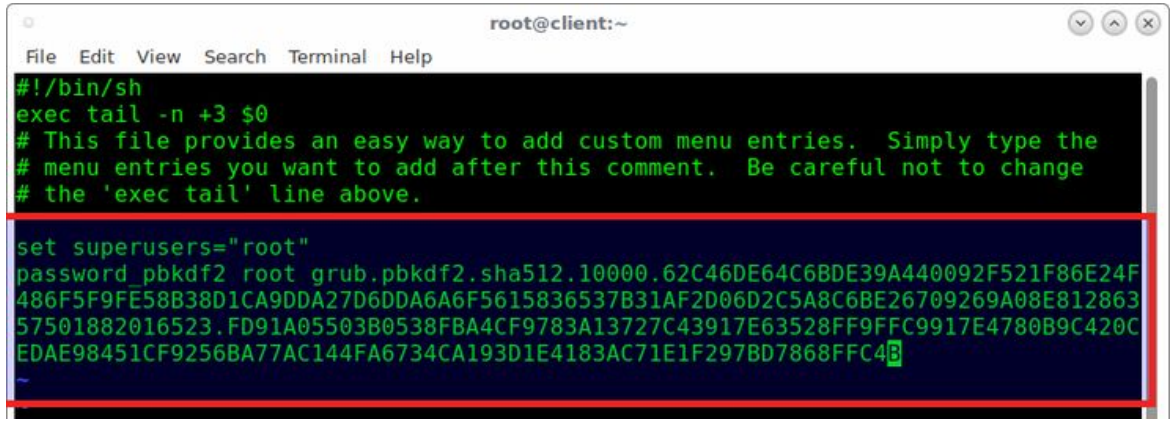
- Выполним следующую команду для обновления linux.
- touch /.autorelabel
- Затем вводим следующую команду, чтобы применить изменения и перезапустить CentOS 7:
- exec /sbin/init
- Пишем команду exit
- Reboot
- Теперь мы сможем войти в CentOS 7 от имени пользователя root с новым паролем.

Обеспечение безопасности рабочей станции

- Меры защиты:
- создаем зашифрованный пароль, используя приведенную ниже команду в качестве пользователя root:
- $ grub2-mkpasswd-pbkdf2
- Теперь мы зашифровали пароль для защиты загрузчика Grub2. Мы должны добавить пароль в пользовательский файл меню Grub2, который находится в каталоге /etc/grub.d/, и, наконец, обновить главный конфигурационный файл Grub2, то есть /etc/grub.cfg.

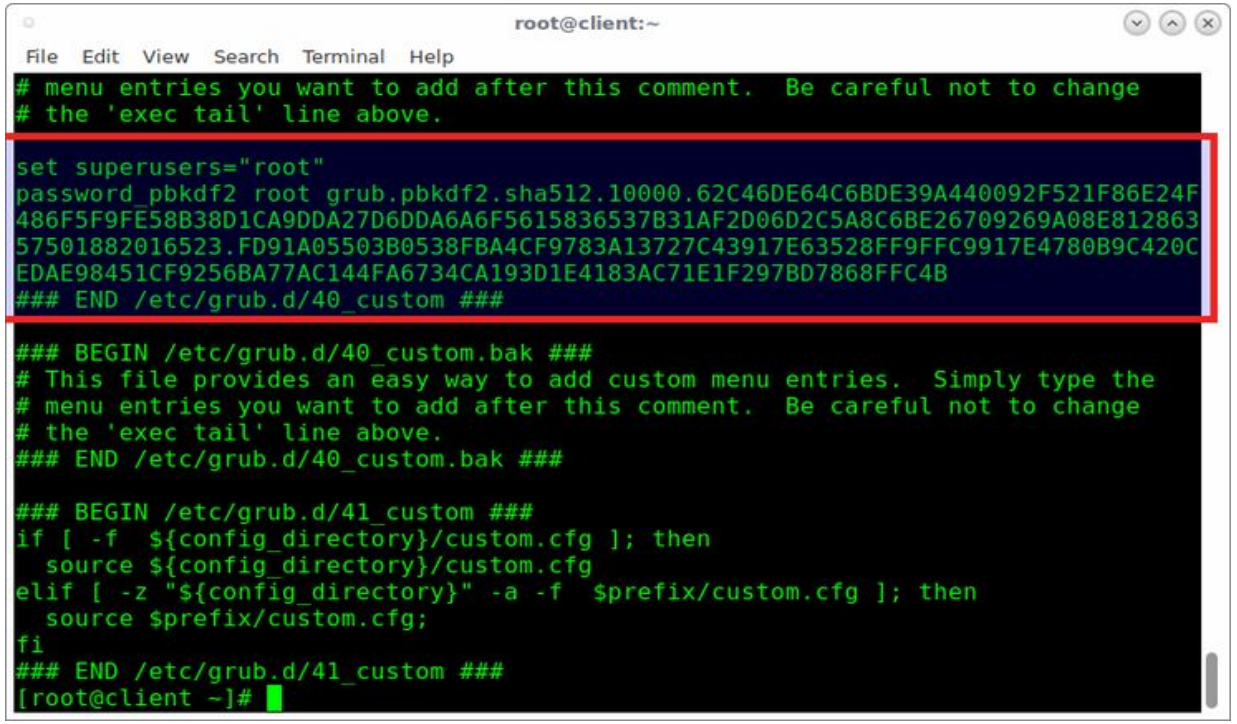
Обеспечение безопасности рабочей станции

- Затем отредактируйтем конфигурационный файл Grub2 в качестве пользователя root:
- $ vi /etc/grub.d/40_custom
- Добавим следующие строки. Убедимся, что мы вставили правильный пароль, который мы создали ранее.



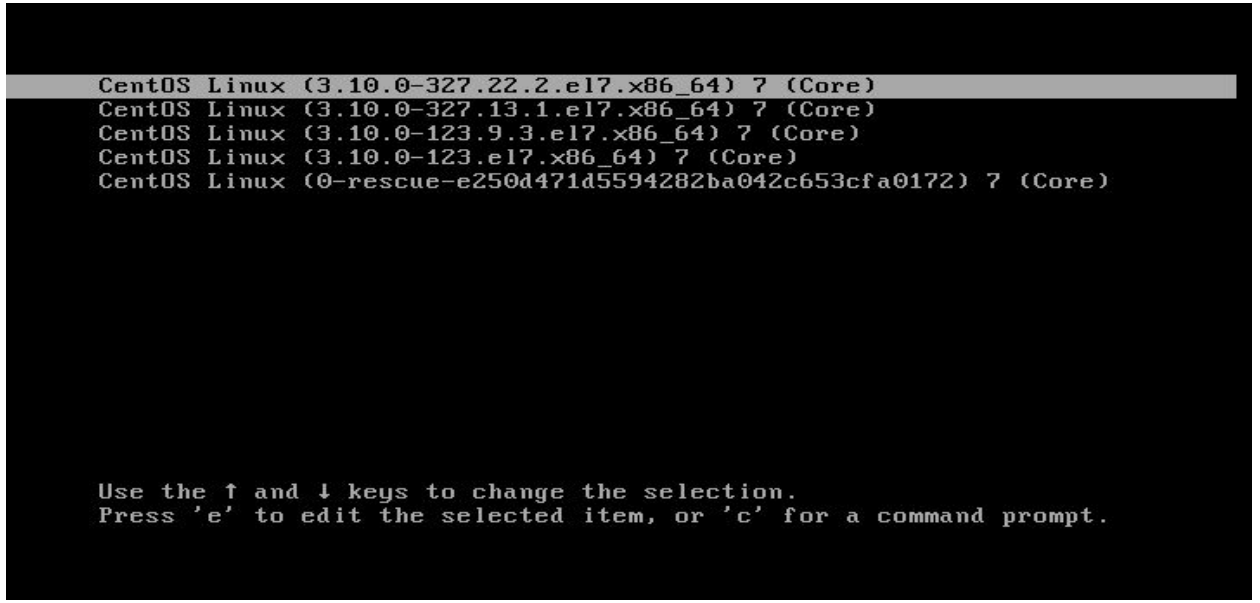
Обеспечение безопасности рабочей станции

- Нажмите ESC и введите :wq, чтобы сохранить и закрыть файл.
- Вы можете проверить правильность установки пароля в файле /etc/grub2.cfg, как показано ниже.
- $ cat /etc/grub2.cfg



Обеспечение безопасности рабочей станции

- Все настроено. Перезагружаем свою систему, чтобы проверить, защищен ли загрузчик.
- После перезагрузки системы попробуем отредактировать загрузчик Grub2. Для этого нажимаем e.

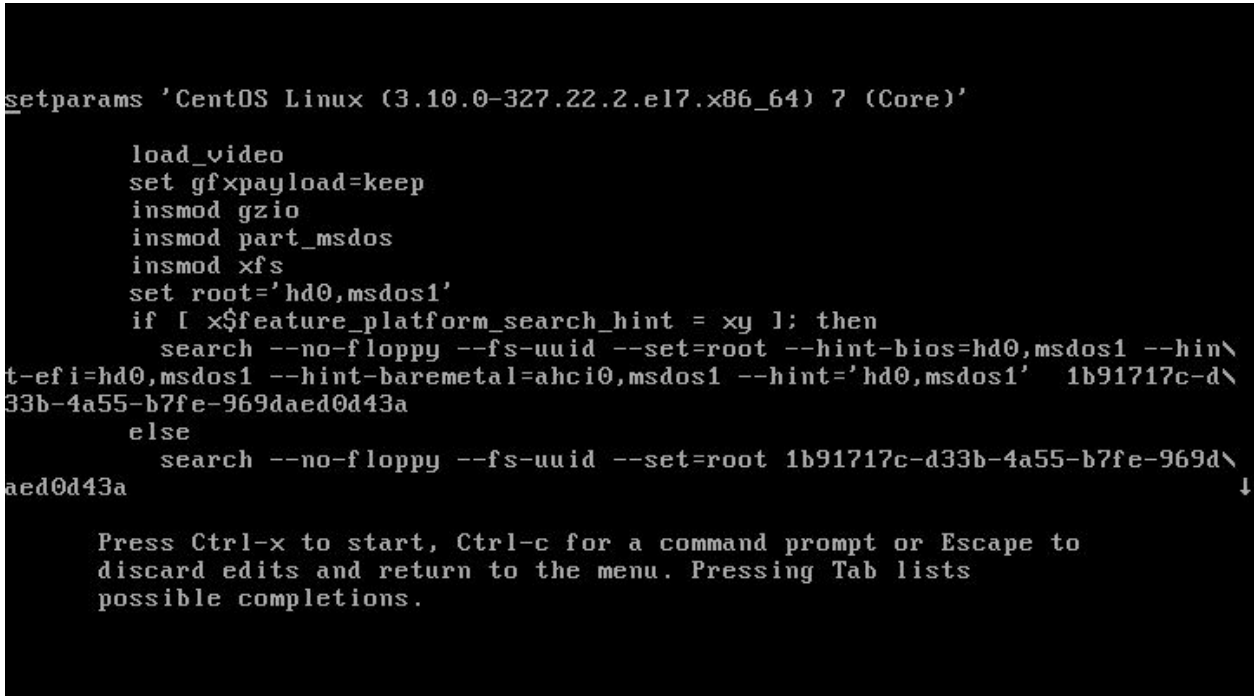


Обеспечение безопасности рабочей станции

- Нам будет предложено ввести имя пользователя и пароль, которые мы задали на предыдущем шаге.

Обеспечение безопасности рабочей станции

- Если мы введем правильное имя пользователя и пароль, то сможем редактировать загрузчик Grub2.

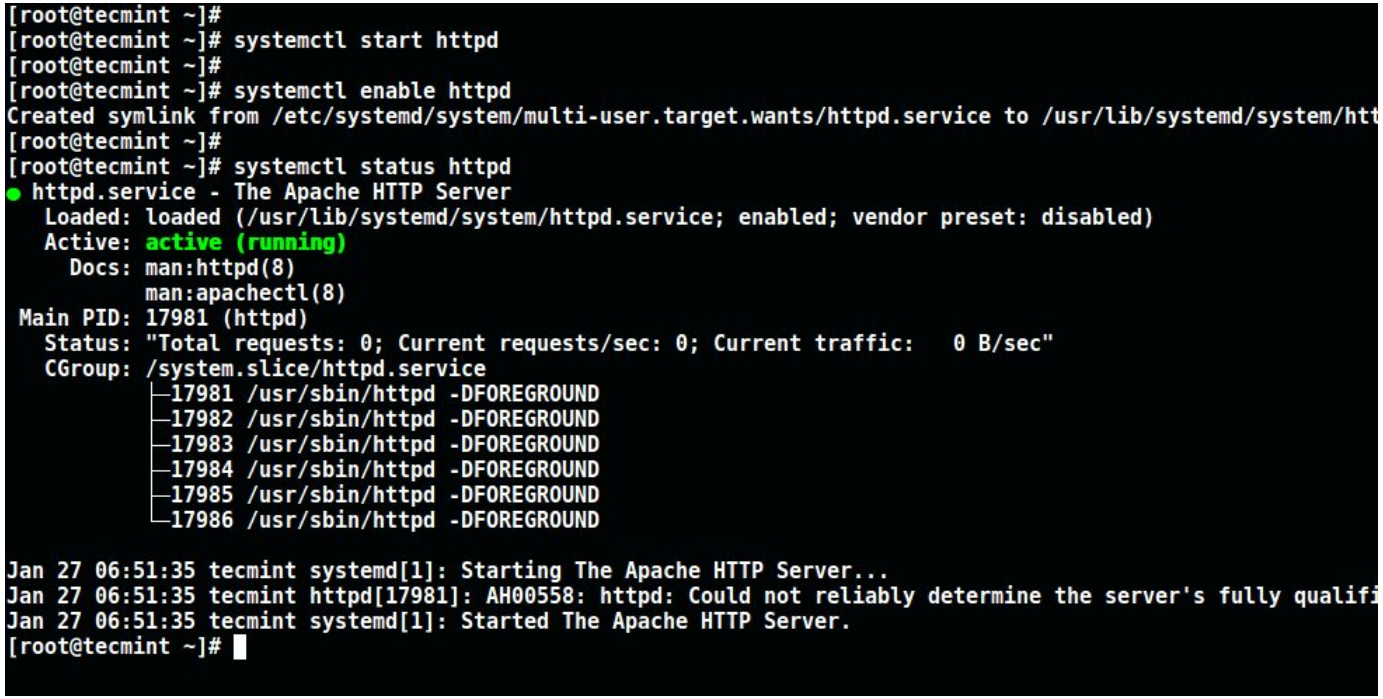


Обеспечение безопасности сервера

- Dos-атака slowloris атака проводиться на веб сервисы, которые работают по протоколу http, так же при помощи slowloris можно положить сайт одним устройством.

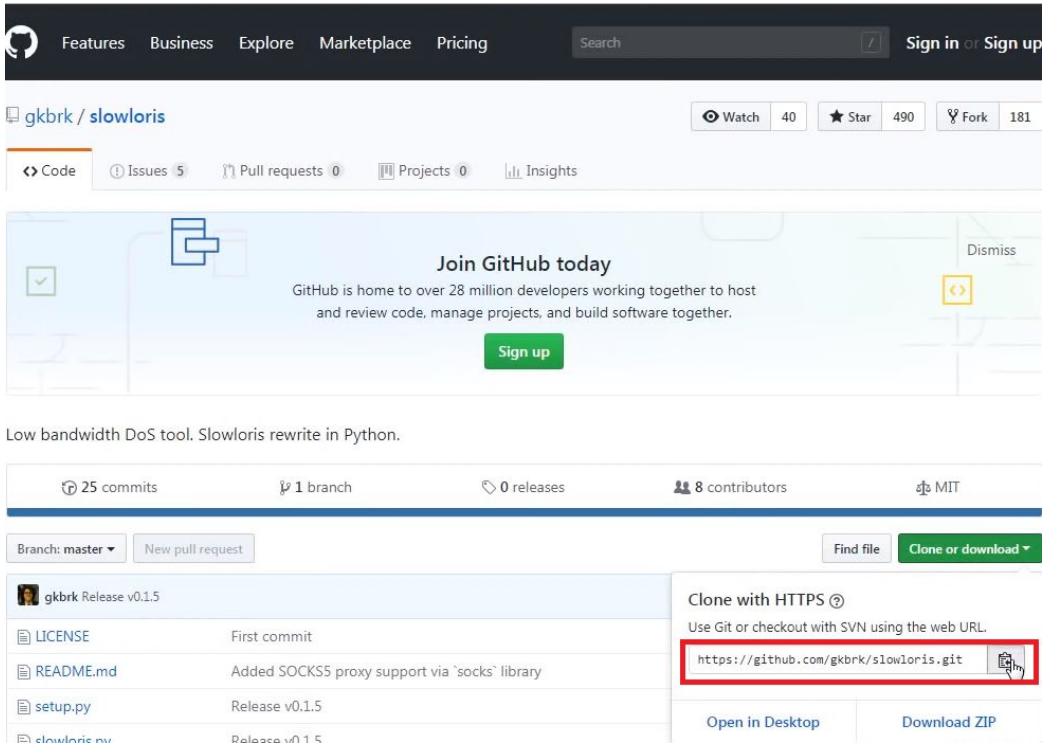
Обеспечение безопасности сервера

- Для демонстрации данной атаки, я поднял на виртуальной машине Centos 7 сервер с apache. Эта машина выступает в роле жертвы.



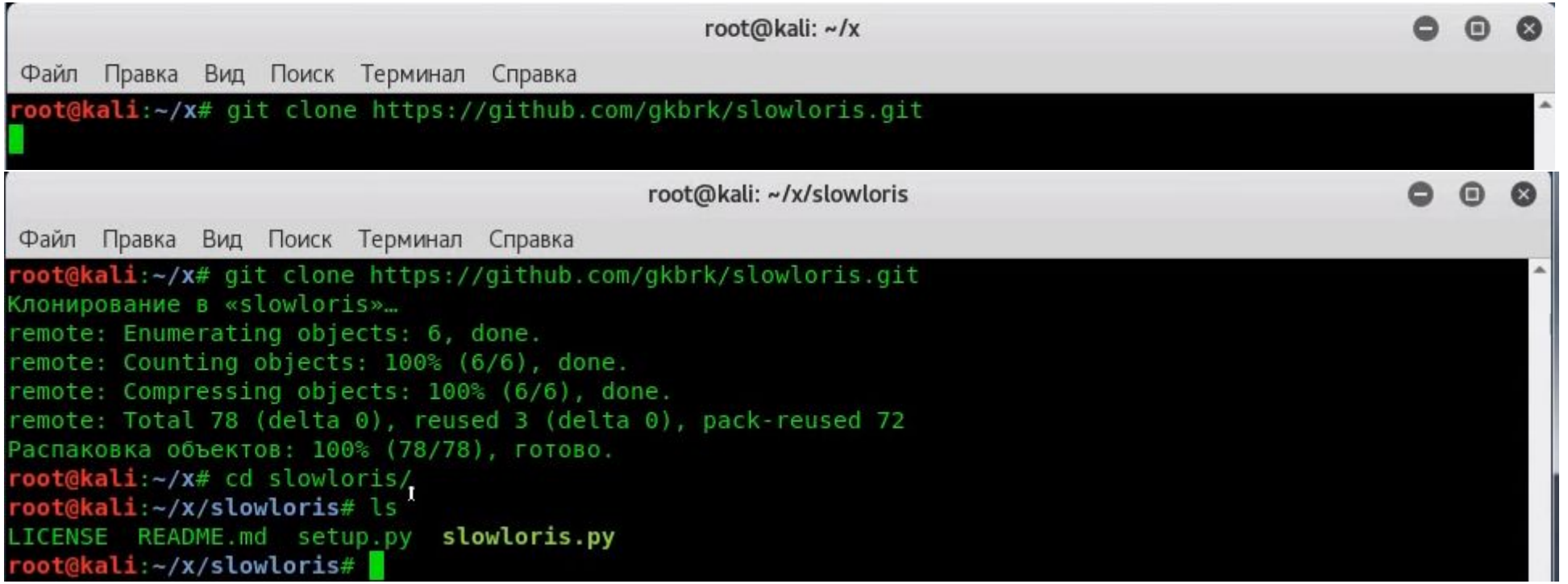
Обеспечение безопасности сервера

- Так же для атаки на понадобиться kali linux. Для начала нам нужно перейти в google и пишем slowloris github.



Обеспечение безопасности сервера

- Скачиваем его на kali linux.



Обеспечение безопасности сервера

Проверить уязвима ли жертва к данной атаки можно при помощи nmap

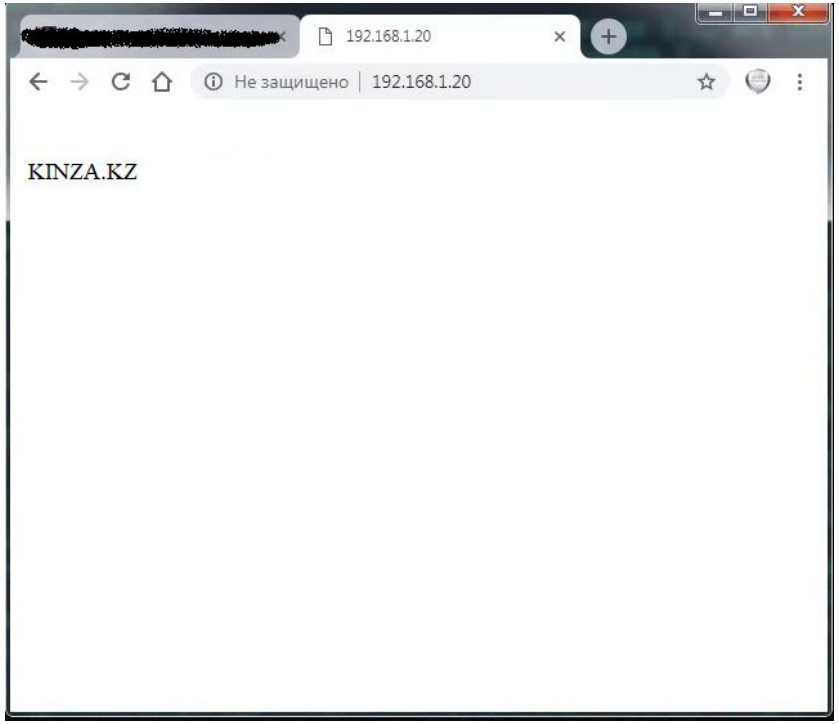
```
root@kali:~/x/slowloris# nmap --script http-slowloris-check 192.168.1.20
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-27 20:31 MSK
Stats: 0:00:10 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 25.00% done; ETC: 20:32 (0:00:30 remaining)
Nmap scan report for 192.168.1.20
Host is up (0.00093s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_      http://ha.ckers.org/slowloris/
MAC Address: 08:00:27:65:46:55 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 311.53 seconds
root@kali:~/x/slowloris#
```

Nmap показывает что жертва уязвима к атаке slowloris

Обеспечение безопасности сервера

Web страница нашего apache сервера



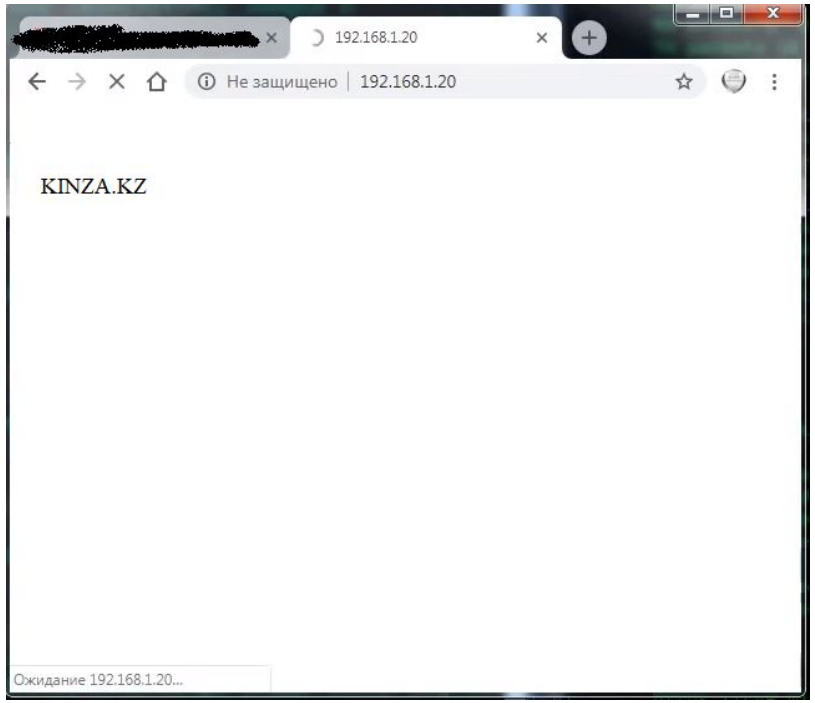
Обеспечение безопасности сервера

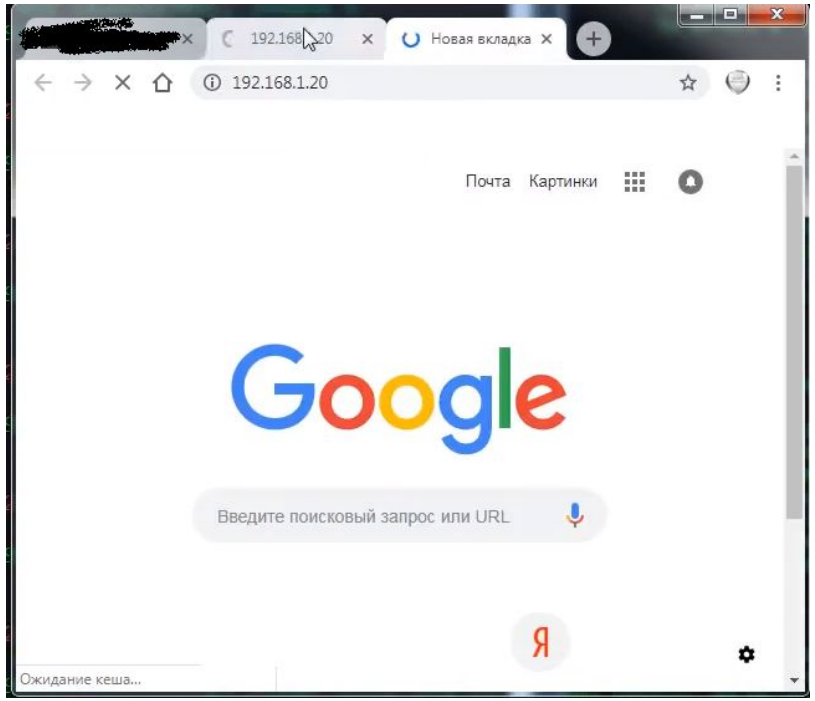
Запускаем нашу атаку

```
root@kali:~/x/slowloris# python slowloris.py 192.168.1.20
Attacking 192.168.1.20 with 150 sockets.
Creating sockets...
Sending keep-alive headers... Socket count: 150
```

Обеспечение безопасности сервера

При попытке обновить страницу видим, что сервер упал, при попытке открыть второе окно тоже ничего не происходит.





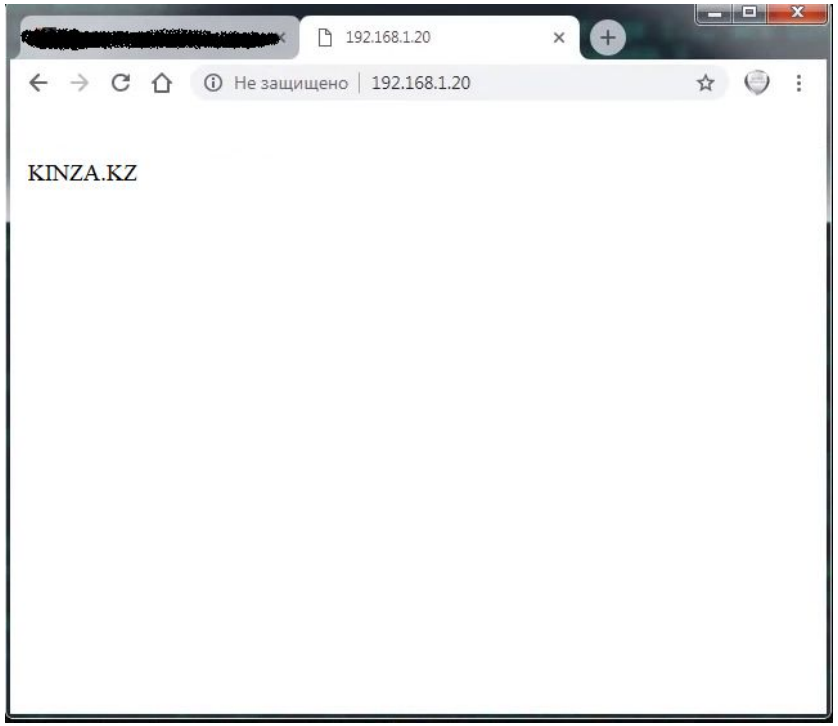
Обеспечение безопасности сервера

Остановим атаку

```
root@kali:~/x/slowloris# python slowloris.py 192.168.1.20
Attacking 192.168.1.20 with 150 sockets.
Creating sockets...
Sending keep-alive headers... Socket count: 150
Sending keep-alive headers... Socket count: 150
Sending keep-alive headers... Socket count: 150
Sending keep-alive headers... Socket count: 150
^C
Stopping Slowloris...
root@kali:~/x/slowloris#
```

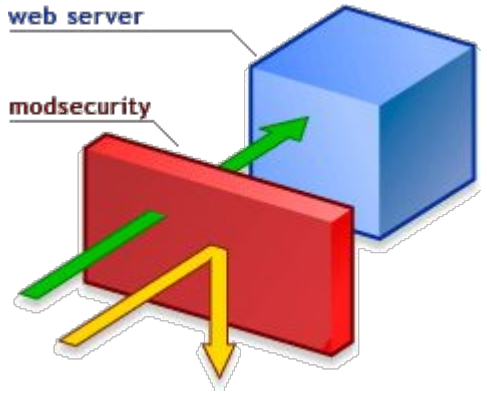
Обеспечение безопасности сервера

И страница веб сервера сразу же загрузилась. И сервер снова поднялся.



Обеспечение безопасности сервера

- Меры защиты:
- обезопасить работу сервера с помощью расширений mod_evasive и mod_security



Обеспечение безопасности сервера

- Пакет mod_evasive обеспечит защиту от DDOS flood-атак прикладного уровня, в то время как mod_security обеспечит защиту от направленных атак, в том числе и атаки медленного чтения.

  По своей сути, mod_security — это программный фаервол с открытым кодом, защищающий вебсервер, и разрабатываемый Trustwave SpiderLabs.

Обеспечение безопасности сервера

```
[Jan 27 05:41:38 2012] [warn] ModSecurity: Access denied with code 400. Too many
threads [101] of 100 allowed in WRITE state from xxx.xxx.xxx.xxx - Possible DoS
Consumption Attack [Rejected]
```

- Таким образом, сервер более не подвержен атаке медленного чтения и временно блокирует по IP адресу пользователей, производящих атаку.

Заключение

- В процессе написания работы на тему «Защита корпоративного сервера на базе Linux–сервера» поставленная цель была достигнута.
- При достижении поставленной цели были решены следующие задачи:

1. Поднятия сервера
2. Демонстрация атаки без защиты
3. Установка защиты
4. Результат защиты

Спасибо за внимание!