

№1.2 – GREP

Цель работы:

- Научиться базовым функциям команды GREP.

Задачи практической работы:

- Вы проводите поиск в Интернете, и видите, что используются две разные версии Python, и вы не знаете, какая из них был установлен в вашей системе установщиком Ubuntu или Debian, и устанавливал ли он какие-либо дополнительные модули?
- Допустим, у вас возникли проблемы с вашим веб-сервером Apache, и вы обратились к одному из многих форумов в сети с просьбой о помощи. Добрая душа, которая вам ответила, попросила вас отправить содержимое вашего файла `/etc/apache2/sites-available/default-ssl`. Разве вам не было бы легче, если бы вы могли просто удалить все закомментированные строки?
- Например, предположим, что у вас есть целая папка, полная музыкальных файлов разных форматов. Вы хотите найти все файлы `.mp3` у исполнителя ABC, но вы не хотите никаких ремиксов. Как поступить?
- Как отобразить количество строк до или после строки поиска?
- Как вывести количество строк совпадения?
- Как выяснить количество совпадений?
- Как найти файлы по заданным номерам строк?
- Произвести поиск рекурсивной строки во всех каталогах.
- Произвести поиск строк в архивах файлах Gzip. (создать zip архив см.п.1.10)

Вы проводите поиск в Интернете, и видите, что используются две разные версии Python, и вы не знаете, какая из них был установлен в вашей системе

установщиком Ubuntu или Debian, и устанавливал ли он какие-либо дополнительные модули?

Для этого потребуется команда `dpkg` который предоставляет возможность взаимодействия с пакетам, например их установку или **поиск** (флаг `-l`)

```
(root@kali)-[/home/cym4atblu]
# dpkg -l | grep -i python
ii  creddump7                                0.1+git20190429-1.1      a
l   Python tool to extract credentials and secrets from Windows registry hives
ii  cython3                                  0.29.36-1                a
d64 C-Extensions for Python 3
ii  faraday-agent-dispatcher                 2.4.0-0kali1             a
l   helper to develop integrations with Faraday (Python 3)
ii  greenbone-feed-sync                     23.7.0-0kali1            a
l   New script for syncing the Greenbone Community Feed (Python 3)
ii  ipython3                                8.14.0-1                 a
l   Enhanced interactive Python 3 shell
ii  isympy-common                           1.12-3                   a
l   Python shell for SymPy
ii  isympy3                                  1.12-3                   a
l   Python3 shell for SymPy
ii  libpython2-stdlib:amd64                 2.7.18-3                 a
d64 interactive high-level object-oriented language (Python2)
```

Делаем вывод о том что установлены версии python 2.7 и 3.11

Допустим, у вас возникли проблемы с вашим веб-сервером Apache, и вы обратились к одному из многих форумов в сети с просьбой о помощи. Добрая душа, которая вам ответила, попросила вас отправить содержимое вашего файла `/etc/apache2/sites-available/default-ssl`. Разве вам не было бы легче, если бы вы могли просто удалить все закомментированные строки?

Для этого можно применить `grep` с флагом `-v` который выводит всю информацию за исключением строк, содержащих указанную подстроку, поэтому для того что бы вывести некомментируемые строки укажем

```

(root@kali)-[/home/cym4atblu]
# grep -v "#" /etc/apache2/sites-available/default-ssl.conf
<VirtualHost *:443>
    ServerAdmin webmaster@localhost

    DocumentRoot /var/www/html

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    SSLEngine on

    SSLCertificateFile      /etc/ssl/certs/ssl-cert-snakeoil.pem
    SSLCertificateKeyFile   /etc/ssl/private/ssl-cert-snakeoil.key

    <FilesMatch "\.(?:cgi|shtml|phtml|php)$">
        SSLOptions +StdEnvVars
    </FilesMatch>
    <Directory /usr/lib/cgi-bin>
        SSLOptions +StdEnvVars
    </Directory>

```

Например, предположим, что у вас есть целая папка, полная музыкальных файлов разных форматов. Вы хотите найти все файлы .mp3 у исполнителя ABC, но вы не хотите никаких ремиксов. Как поступить?

Для этого воспользуемся уже знакомой командой `grep` с флагом `-iv` который позволит отфильтровать все фиты

```

(cym4atblu@kali)-[~/music]
$ ls
ABC-1.mp3  ABC.txt  ABC_feat.MBC-2.mp3  DSC-s.mp3

(cym4atblu@kali)-[~/music]
$ sudo find -name "ABC*.mp3" | grep -iv "feat"
./ABC-1.mp3

```

Как отобразить количество строк до или после строки поиска?

для выполнения подобного запроса понадобятся флаги -A и -B у функции grep, которые отображают согласованные строки и количество строк, которые присутствуют до или после строки поиска.

```
(cym4atblu@kali)-[~/music]
$ sudo ifconfig | grep -A 10 eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
      inet6 fe80::a00:27ff:fee7:ef15 prefixlen 64 scopeid 0x20<link>
      ether 08:00:27:e7:ef:15 txqueuelen 1000 (Ethernet)
      RX packets 346 bytes 138147 (134.9 KiB)
      RX errors 0 dropped 0 overruns 0 frame 0
      TX packets 316 bytes 30748 (30.0 KiB)
      TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0

(cym4atblu@kali)-[~/music]
$ sudo ifconfig | grep -B 10 eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
```

Как вывести количество строк совпадения?

для этого можно воспользоваться флагом -C, который выводит N строк до и после найденного совпадения

```
(cym4atblu@kali)-[~/music]
$ sudo ifconfig | grep -C 6 lo:
      ether 08:00:27:e7:ef:15 txqueuelen 1000 (Ethernet)
      RX packets 346 bytes 138147 (134.9 KiB)
      RX errors 0 dropped 0 overruns 0 frame 0
      TX packets 316 bytes 30748 (30.0 KiB)
      TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
      inet6 ::1 prefixlen 128 scopeid 0x10<host>
      loop txqueuelen 1000 (Local Loopback)
      RX packets 4 bytes 240 (240.0 B)
      RX errors 0 dropped 0 overruns 0 frame 0
      TX packets 4 bytes 240 (240.0 B)
```

Как выяснить количество совпадений?

для выяснения количества строк совпадения можно воспользоваться флагом -c

```
(cym4atblu@kali)-[~/music]
$ sudo ifconfig | grep -c RX
4
```

Как найти файлы по заданным номерам строк?

для этого укажем флаг -n и слово, номер строки содержащее его мы хотим узнать

```
(cym4atblu@kali)-[~/pt2]
$ cat Reveille.txt
He can't avoid conflict
He's lost 'cause he's incomplete
He's in between, somewhere in between, in between the sleepless shadows
Battling to break the love that's 'guaranteed to make you bleed thicker than blood'
He don't want it, but craves what he can't escape
He's staring straight through his fate and now he's face to face
You want to fall down, well this could make your dreams come true
Because the devil was an angel too
Look at me now, making the same mistakes I said I'd never make again-
But now I'm back in the same place
Look at me now, somebody stole my soul-
I feel the breaks go and I'm spinning out of control
Come step into a brave new world-
Not even worth it
Decent comes quick and now he's anything but perfect
And still he worships that fundamental bullshit talk
'The path you carve yourself is the path to walk'
Now walk alone-
Play it to the bone
Don't make it right just because he got his sickness from that venomous bite
We want to fall down, well this could make our dreams come true
Because the devil was an angel too
It's gonna be alright, everything's okay
Mothers tears will fall and wash it all away
Suck, suck it- suck, suck it up

(cym4atblu@kali)-[~/pt2]
$ grep -n "devil" Reville.txt
8:Because the devil was an angel too
22:Because the devil was an angel too
```

Произвести поиск рекурсивной строки во всех каталогах.

для этого существует флаг -r

```

(cym4atblu@kali)-[/etc/ssh]
$ grep -r "no"
ssh_config:# ForwardAgent no
ssh_config:# ForwardX11 no
ssh_config:# HostbasedAuthentication no
ssh_config:# GSSAPIAuthentication no
ssh_config:# GSSAPIDelegateCredentials no
ssh_config:# GSSAPIKeyExchange no
ssh_config:# GSSAPITrustDNS no
ssh_config:# BatchMode no
ssh_config:# Tunnel no
ssh_config:# PermitLocalCommand no
ssh_config:# VisualHostKey no
ssh_config:# UserKnownHostsFile ~/.ssh/kno
ssh_config:# HashKnownHosts yes
grep: ssh_host_rsa_key: Permission denied
grep: ssh_host_ed25519_key: Permission denied
sshd_config:#RekeyLimit default none
sshd_config:#AuthorizedPrincipalsFile none
sshd_config:#AuthorizedKeysCommand none
sshd_config:#AuthorizedKeysCommandUser nobody
sshd_config:# For this to work you will also need host keys in /etc/ssh/ssh_kno
sshd_config:#HostbasedAuthentication no
sshd_config:# Change to yes if you don't trust ~/.ssh/kno
sshd_config:#IgnoreUserKnownHosts no
sshd_config:#IgnoreRhosts yes
sshd_config:# To disable tunneled clear text passwords, change to no here!
sshd_config:#PermitEmptyPasswords no
sshd_config:#KbdInteractiveAuthentication no
sshd_config:#KerberosAuthentication no
sshd_config:#KerberosGetAFSToken no
sshd_config:#GSSAPIAuthentication no
sshd_config:#GSSAPIKeyExchange no
sshd_config:# and KbdInteractiveAuthentication to 'no'.
sshd_config:#GatewayPorts no
sshd_config:#PrintMotd no
sshd_config:#PermitUserEnvironment no
sshd_config:#UseDNS no
sshd_config:#PermitTunnel no
sshd_config:#ChrootDirectory none
sshd_config:#VersionAddendum none
sshd_config:# no default banner path
sshd_config:#Banner none
sshd_config:# override default of no subsystems
sshd_config:#Match User anoncvs
sshd_config:# X11Forwarding no
sshd_config:# AllowTcpForwarding no
sshd_config:# PermitTTY no
grep: ssh_host_ecdsa_key: Permission denied

```

- Произвести поиск строк в архивах файлов Gzip. (создать zip архив см.п.1.10)

то же самое, только используем zgrep вместо обычного zgrep

```
(cym4atblu@kali)-[~/pt2]
$ zip Reveille.zip Reveille.txt
adding: Reveille.txt (deflated 48%)

(cym4atblu@kali)-[~/pt2]
$ zgrip -in "conflict" Reveille.txt
Command 'zgrip' not found, did you mean:
  command 'zgrep' from deb gzip
  command 'zgrep' from deb zutils
Try: sudo apt install <deb name>

(cym4atblu@kali)-[~/pt2]
$ zgrep -in "conflict" Reveille.txt
1:He can't avoid conflict

(cym4atblu@kali)-[~/pt2]
$ zgrep -in "conflict" Reveille.zip
1:He can't avoid conflict
```