

# **Информационная безопасность**

**Идентификация и аутентификация, управление доступом**

Нзита Диатезилуа Катенди

# Содержание

<b>Цель работы</b>	<b>4</b>
<b>Теоретические сведения</b>	<b>5</b>
Идентификация . . . . .	5
Аутентификация . . . . .	5
Управление доступом . . . . .	6
Журналы аутентификации . . . . .	6
<b>Выполнение лабораторной работы</b>	<b>7</b>
Процессы и технологии аутентификации . . . . .	8
Управление доступом . . . . .	9
<b>Выводы</b>	<b>11</b>
<b>Список литературы</b>	<b>12</b>

# Список иллюстраций

1	Проверка статус службы SSH . . . . .	7
2	Идентификация . . . . .	8
3	Просмотр неудачных попыток входа . . . . .	8
4	Процессы и технологии аутентификации . . . . .	9
5	Настройка прав доступа к файлу . . . . .	10
6	Управление доступом . . . . .	10

# Цель работы

Целью данной работы является механизмов идентификации и аутентификации пользователей в компьютерных системах, а также ознакомление с методами управления доступом к ресурсам.

# Теоретические сведения

## Идентификация

Идентификация – это процесс распознавания личности пользователя системой. При идентификации пользователь предоставляет уникальные данные, такие как имя пользователя, номер идентификационной карты или другой уникальный идентификатор, который позволяет системе определить, кто именно обращается к её ресурсам. Этот процесс не подтверждает достоверность предоставленной информации, а лишь служит для определения личности пользователя.

## Аутентификация

Аутентификация – это процесс подтверждения того, что пользователь действительно является тем, за кого себя выдает. Этот процесс следует после идентификации и предполагает проверку предоставленных пользователем данных. Существует несколько методов аутентификации:

Однофакторная аутентификация: Использование одного метода подтверждения, например, пароля.

Многофакторная аутентификация: Использование нескольких методов подтверждения, например, пароля и отпечатка пальца или смс-кода.

## Управление доступом

Управление доступом – это процесс регулирования прав и привилегий пользователей для доступа к ресурсам информационной системы. Существует несколько моделей управления доступом:

Дискреционное управление доступом (DAC): Доступ к ресурсам предоставляется владельцем ресурса на своё усмотрение.

Обязательное управление доступом (MAC): Доступ к ресурсам регулируется системой на основе заранее установленных политик безопасности.

Ролевая модель управления доступом (RBAC): Доступ к ресурсам предоставляется на основе ролей, назначенных пользователям.

## Журналы аутентификации

Журналы аутентификации – это записи, которые ведёт система для фиксации всех попыток входа пользователей, как успешных, так и неудачных. Анализ этих журналов позволяет выявлять подозрительные активности, такие как множественные неудачные попытки входа, что может свидетельствовать о попытках взлома или несанкционированного доступа. В операционных системах на базе Linux такие журналы обычно хранятся в файлах `/var/log/auth.log` или `/var/log/secure`.

# Выполнение лабораторной работы

Перед началом лабораторной работы необходимо убедиться, что служба SSH (Secure Shell) активна и настроена на вашем компьютере. SSH позволяет безопасно подключаться к системе удалённо и является распространённым инструментом для управления серверами. (рис. @fig:001)

```
(dknzita@dknzita):[~]
$ sudo systemctl status ssh
[sudo] password for dknzita:
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: disabled)
   Active: active (running) since Fri 2024-10-11 11:07:55 EDT; 1h 8min ago
  Invocation: d14c8d89e14f4abb87af20a29623082c
     Docs: man:sshd(8)
           man:sshd_config(5)
   Process: 7182 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
  Main PID: 7184 (sshd)
    Tasks: 1 (limit: 2269)
   Memory: 5.2M (peak: 39M)
      CPU: 29.322s
   CGroup: /system.slice/ssh.service
           └─7184 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Oct 11 12:15:46 dknzita sshd[42511]: PAM 1 more authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=127.0.0.1
Oct 11 12:15:47 dknzita sshd[42475]: Failed password for invalid user testuser from 127.0.0.1 port 52134 ssh2
Oct 11 12:15:47 dknzita sshd[42558]: Failed password for invalid user testuser from 127.0.0.1 port 37934 ssh2
Oct 11 12:15:47 dknzita sshd[42530]: Failed password for invalid user testuser from 127.0.0.1 port 52168 ssh2
Oct 11 12:15:47 dknzita sshd[42475]: Connection closed by invalid user testuser 127.0.0.1 port 52134 [preauth]
Oct 11 12:15:47 dknzita sshd[42475]: PAM 3 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=127.0.0.1
Oct 11 12:15:47 dknzita sshd[42475]: PAM service(sshd) ignoring max retries; 4 > 3
Oct 11 12:15:47 dknzita sshd[42558]: Connection closed by invalid user testuser 127.0.0.1 port 37934 [preauth]
Oct 11 12:15:48 dknzita sshd[42530]: Connection closed by invalid user testuser 127.0.0.1 port 52168 [preauth]
Oct 11 12:15:48 dknzita sshd[42530]: PAM 1 more authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=127.0.0.1
```

Рис. 1: Проверка статус службы SSH

содержит информацию о пользователях системы. Каждая строка представляет одного пользователя с различными полями, такими как имя пользователя, UID, GID, домашний каталог и оболочка. (рис. @fig:002)

```
(dknzita@dknzita)-[~]
$ cat /etc/passwd
root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
```

Рис. 2: Идентификация

После генерации неудачных попыток входа необходимо проанализировать системные журналы, чтобы убедиться в фиксации этих событий. (рис. @fig:003)

Эта команда выводит все записи о неудачных попытках входа в систему, что помогает отслеживать попытки несанкционированного доступа.

```
(dknzita@dknzita)-[~]
$ sudo journalctl | grep "Failed password" | tail -n 10
Oct 11 12:15:45 dknzita sshd[42535]: Failed password for invalid user testuser from 127.0.0.1 port 37924 ssh2
Oct 11 12:15:45 dknzita sshd[42411]: Failed password for invalid user testuser from 127.0.0.1 port 40826 ssh2
Oct 11 12:15:46 dknzita sshd[42509]: Failed password for invalid user testuser from 127.0.0.1 port 52140 ssh2
Oct 11 12:15:46 dknzita sshd[42461]: Failed password for invalid user testuser from 127.0.0.1 port 52112 ssh2
Oct 11 12:15:46 dknzita sshd[42463]: Failed password for invalid user testuser from 127.0.0.1 port 52124 ssh2
Oct 11 12:15:46 dknzita sshd[42465]: Failed password for invalid user testuser from 127.0.0.1 port 52126 ssh2
Oct 11 12:15:46 dknzita sshd[42511]: Failed password for invalid user testuser from 127.0.0.1 port 52144 ssh2
Oct 11 12:15:47 dknzita sshd[42475]: Failed password for invalid user testuser from 127.0.0.1 port 52134 ssh2
Oct 11 12:15:47 dknzita sshd[42558]: Failed password for invalid user testuser from 127.0.0.1 port 37934 ssh2
Oct 11 12:15:47 dknzita sshd[42530]: Failed password for invalid user testuser from 127.0.0.1 port 52168 ssh2
```

Рис. 3: Просмотр неудачных попыток входа

## Процессы и технологии аутентификации

Современные методы:

- Биометрия (скан отпечатков пальцев, распознавание лица).
- Токены (одноразовые пароли, физические ключи).
- Протоколы (OAuth, SAML, Kerberos).

Создает SHA-512 хеш для пароля password123 и сохраняет его в файл hash.txt.



Использует словарь rockyou.txt для подбора пароля, соответствующего хешу в hash.txt (рис. @fig:004)

```
(dknzita@dknzita)-[~]
$ echo "password123" | openssl passwd -6 -stdin > hash.txt

(dknzita@dknzita)-[~]
$ john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
Warning: detected hash type "sha512crypt", but the string is also recognized as "HMAC-SHA256"
Use the "--format=HMAC-SHA256" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 SSE2 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Press 'q' or Ctrl-C to abort, almost any other key for status
password123 (?)
1g 0:00:00:02 DONE (2024-10-11 11:19) 0.4424g/s 623.0p/s 623.0c/s 623.0C/s teacher..tagged
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Рис. 4: Процессы и технологии аутентификации

Этот пример демонстрирует, как могут быть взломаны слабые пароли. Используйте его только на собственных тестовых системах и хешах.

## Управление доступом

Методы:

- DAC (Discretionary Access Control) – доступ на усмотрение владельца.
- MAC (Mandatory Access Control) – обязательный контроль доступа.
- RBAC (Role-Based Access Control) – контроль доступа на основе ролей.

Ограничение доступа к конфиденциальным документам в корпоративной сети на основе должностей

Устанавливает права доступа к файлу secret.txt, позволяя читать и записывать его только владельцу. (рис. @fig:005)

```
(dknzita@dknzita)-[~]
$ touch secret.txt

(dknzita@dknzita)-[~]
$ chmod 600 secret.txt

(dknzita@dknzita)-[~]
$ ls -l secret.txt
-rw----- 1 dknzita dknzita 0 Oct 11 11:21 secret.txt
```

Рис. 5: Настройка прав доступа к файлу

Использование Нудра для атаки методом перебора паролей на SSH (на тестовом сервере)

Пробуем подобрать пароль для пользователя testuser на локальном SSH-сервере, используя словарь rockyou.txt. (рис. @fig:006)

```
(dknzita@dknzita)-[~]
$ hydra -l testuser -P /usr/share/wordlists/rockyou.txt ssh://localhost
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-10-11 11:28:49
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (1:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://localhost:22/
[STATUS] 151.00 tries/min, 151 tries in 00:01h, 14344249 to do in 1503:10h, 15 active
[STATUS] 105.33 tries/min, 310 tries in 00:02h, 14344084 to do in 2209:39h, 15 active
```

Рис. 6: Управление доступом

Этот пример демонстрирует угрозу перебора паролей. Используйте только на тестовых системах с разрешением.

## **Выводы**

В ходе выполнения лабораторной работы были изучены основные механизмы идентификации и аутентификации пользователей, а также методы управления доступом к ресурсам информационных систем.

## **Список литературы**