

Доклад

Идентификация и аутентификация, управление доступом

Нзита Диатезилуа Катенди

11 октября 2024 г.

Российский университет дружбы народов, Москва, Россия

Информация

- Нзита Диатезилуа Катенди
- студент
- Российский университет дружбы народов
- 1032215220@pfur.ru
- <https://github.com/NzitaKatendi>

Вводная часть

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

Задачи:

- Понять ключевые понятия идентификации, аутентификации и управления доступом.
- Рассмотреть современные методы и технологии.
- Показать примеры из практики.
- Сделать выводы о важности этих аспектов в ИТ-системах.

Инструмент Kali Linuz, bash

Выполнение лабораторной работы

Проверка статус службы SSH

```
(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

```
(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


```
(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

```
(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

```
(dknzita@dknzita)-[~]  
$ touch secret.txt  
  
(dknzita@dknzita)-[~]  
$ chmod 600 secret.txt  
File System  
  
(dknzita@dknzita)-[~]  
$ ls -l secret.txt  
-rw----- 1 dknzita dknzita 0 Oct 11 11:21 secret.txt
```

Рис. 5: Настройка прав доступа к файлу secret.txt

```
(dlnzita@dlnzita) [~]
$ 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 (l:/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 1583:16h, 15 active
[STATUS] 105.33 tries/min, 316 tries in 00:03h, 14344084 to do in 2269:39h, 15 active
```

Рис. 6: Управление доступом

Заключение

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

1. Фредрикс, Дж. “Кибербезопасность: введение в управление доступом”. Москва: Издательство “Наука”, 2019.
2. Брук, Д. “Основы сетевой безопасности”. СПб: Питер, 2020.
3. Документация Kali Linux: Официальное руководство. <https://www.kali.org/docs/>.
Руководство по использованию journalctl.
<https://man7.org/linux/man-pages/man1/journalctl.1.html>.
4. Стандартная документация SSH. <https://www.openssh.com/manual.html>.