# Индивидуальный проект этап 3

## Использование Hydra

Александр Андреевич Шуплецов

# Содержание

# Список иллюстраций

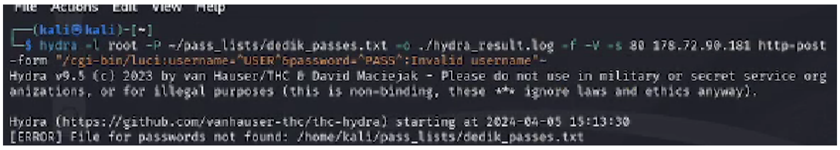
# Список таблиц

# 1 Цель работы

Попробовать в действии Hydra.

# 2 Выполнение работы

1. Используем пример из задания для работы с Hydra.

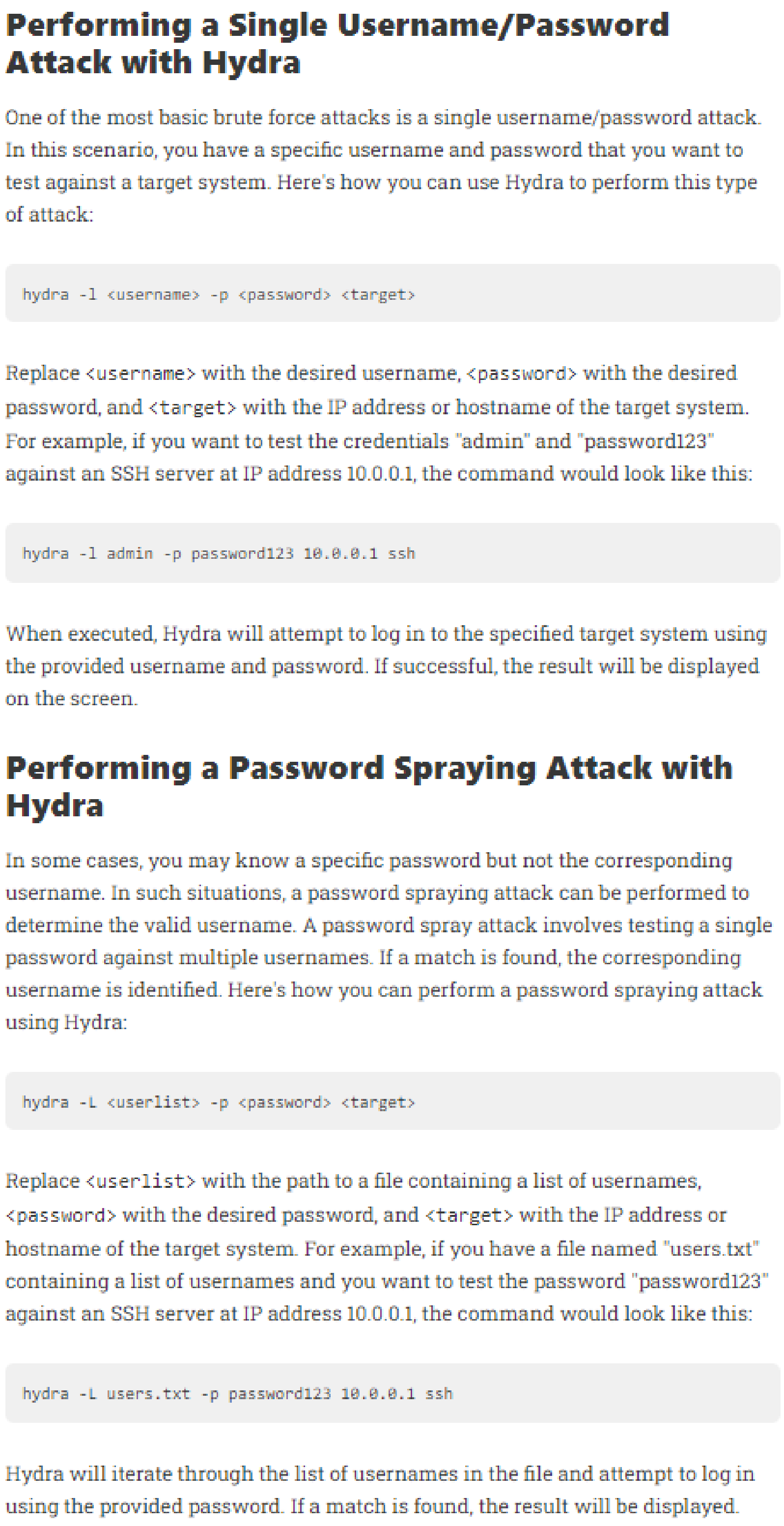


```
┌──(kali㉿kali)-[~]
└─$ hydra -l root -P ~/pass_lists/dedik_passes.txt -o ./hydra_result.log -f -V -s 80 178.72.90.181 http-post
-form "/cgi-bin/luci:username=^USER^&password=^PASS^:Invalid username"-
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service org
anizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-05 15:13:30
[ERROR] File for passwords not found: /home/kali/pass_lists/dedik_passes.txt
```

Рис. 2.1: пример из задания

2. Изучим атаку Username/password и атаку Password Spraying в Hydra.



## Performing a Single Username/Password Attack with Hydra

One of the most basic brute force attacks is a single username/password attack. In this scenario, you have a specific username and password that you want to test against a target system. Here's how you can use Hydra to perform this type of attack:

```
hydra -l <username> -p <password> <target>
```

Replace `<username>` with the desired username, `<password>` with the desired password, and `<target>` with the IP address or hostname of the target system. For example, if you want to test the credentials "admin" and "password123" against an SSH server at IP address 10.0.0.1, the command would look like this:

```
hydra -l admin -p password123 10.0.0.1 ssh
```

When executed, Hydra will attempt to log in to the specified target system using the provided username and password. If successful, the result will be displayed on the screen.

## Performing a Password Spraying Attack with Hydra

In some cases, you may know a specific password but not the corresponding username. In such situations, a password spraying attack can be performed to determine the valid username. A password spray attack involves testing a single password against multiple usernames. If a match is found, the corresponding username is identified. Here's how you can perform a password spraying attack using Hydra:

```
hydra -L <userlist> -p <password> <target>
```

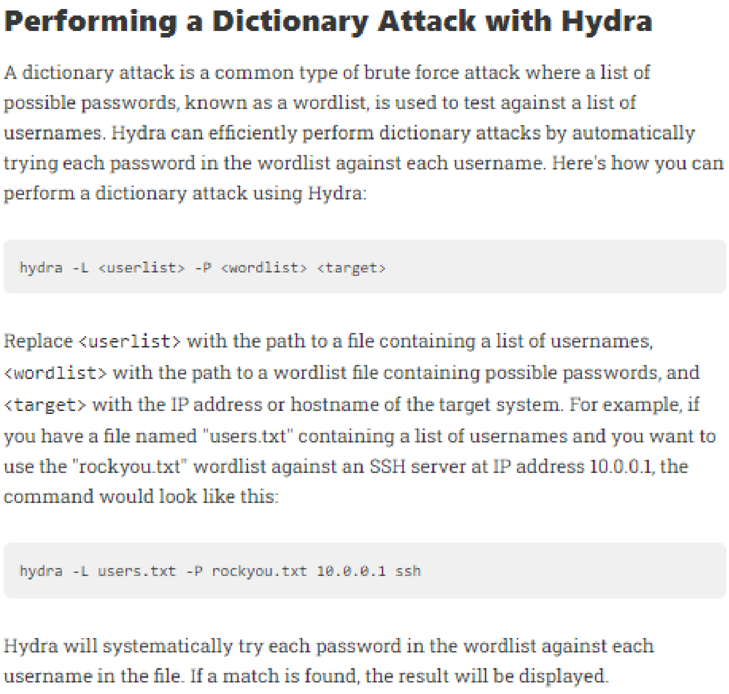
Replace `<userlist>` with the path to a file containing a list of usernames, `<password>` with the desired password, and `<target>` with the IP address or hostname of the target system. For example, if you have a file named "users.txt" containing a list of usernames and you want to test the password "password123" against an SSH server at IP address 10.0.0.1, the command would look like this:

```
hydra -L users.txt -p password123 10.0.0.1 ssh
```

Hydra will iterate through the list of usernames in the file and attempt to log in using the provided password. If a match is found, the result will be displayed.

Рис. 2.2: классические атаки в Hydra

3. Изучим атаку Dictionary в Hydra, как классический вид брутфорс атаки.



## Performing a Dictionary Attack with Hydra

A dictionary attack is a common type of brute force attack where a list of possible passwords, known as a wordlist, is used to test against a list of usernames. Hydra can efficiently perform dictionary attacks by automatically trying each password in the wordlist against each username. Here's how you can perform a dictionary attack using Hydra:

```
hydra -L <userlist> -P <wordlist> <target>
```

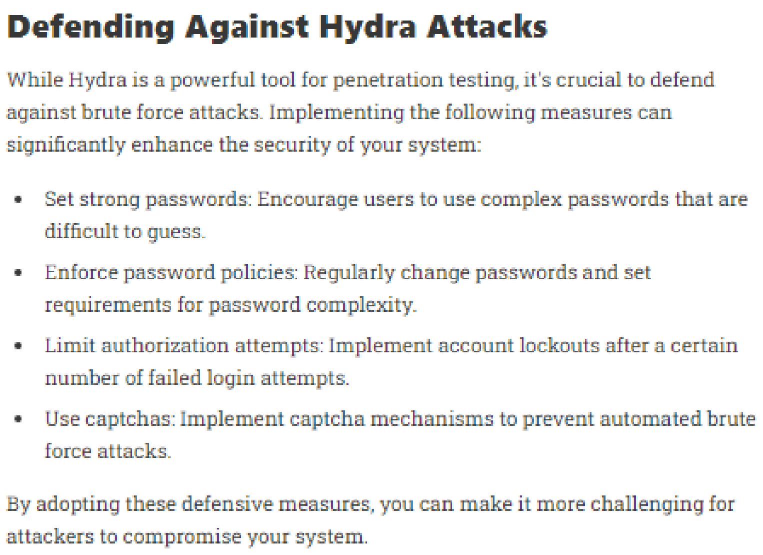
Replace `<userlist>` with the path to a file containing a list of usernames, `<wordlist>` with the path to a wordlist file containing possible passwords, and `<target>` with the IP address or hostname of the target system. For example, if you have a file named "users.txt" containing a list of usernames and you want to use the "rockyou.txt" wordlist against an SSH server at IP address 10.0.0.1, the command would look like this:

```
hydra -L users.txt -P rockyou.txt 10.0.0.1 ssh
```

Hydra will systematically try each password in the wordlist against each username in the file. If a match is found, the result will be displayed.

Рис. 2.3: атака Dictionary в Hydra

4. Изучим основные способы защиты от атак Hydra.



### Defending Against Hydra Attacks

While Hydra is a powerful tool for penetration testing, it's crucial to defend against brute force attacks. Implementing the following measures can significantly enhance the security of your system:

- Set strong passwords: Encourage users to use complex passwords that are difficult to guess.
- Enforce password policies: Regularly change passwords and set requirements for password complexity.
- Limit authorization attempts: Implement account lockouts after a certain number of failed login attempts.
- Use captchas: Implement captcha mechanisms to prevent automated brute force attacks.

By adopting these defensive measures, you can make it more challenging for attackers to compromise your system.

Рис. 2.4: способы защиты от Hydra атак

# 3 Выводы

Я попробовал в действии Hydra.

# Список литературы

Кулябов Д.С. "Материалы к учебному проекту" ROD TRENT - Using Kali Linux and Hydra for Attack Testing and Alert Generation, 2023