

Индивидуальный проект этап 3

Информационная безопасность

Ким И. В. НФИбд-01-21

Российский университет дружбы народов, Москва, Россия

Цели и задачи

Установить hydra на kali linux

Выполнение работы

Установил последние обновления системы sudo командой - apt-get update &&
sudo apt-get upgrade && sudo apt-get dist-upgrade

```
(ksudzuki@KSudzuki)-[~]  
$ sudo apt-get update && sudo apt-get upgrade && sudo apt-get dist-upgrade  
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]  
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [20.1 MB]
```

После обновления системы установил важные компоненты, необходимые для hydra

```
(ksudzuki@KSudzuki)-[~]
$ sudo apt-get -y install build-essential
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
build-essential is already the newest version (12.10).
build-essential set to manually installed.
The following packages were automatically installed and are no longer required:
  chrome-gnome-shell fonts-liberation2 gnome-backgrounds ibverbs-providers libarmadillo12 libassuan0 libavfilter9 libavformat60
  libblosc2-3 libboost-iostreams1.83.0 libboost-thread1.83.0 libcephfs2 libdisplay-info1 libgdal34t64 libgeos3.12.2 libgfpapi0 libgfrpc0
  libgfxdr0 libglusterfs0 libibverbs1 libimobiledevice6 libjsoncpp25 liblua5.2-0 libnghttp3-3 libplacebo338 libplist3 libpoppler134
  libpostproc57 libproxy1-plugin-gsettings libproxy1-plugin-networkmanager libproxy1-plugin-webkit libpython3.11-dev
  libpython3.11-minimal libpython3.11-stdlib libpython3.11t64 libqt6dbus6t64 libqt6gui6t64 libqt6network6t64 libqt6opengl6t64
  libqt6openglwidgets6t64 libqt6printsupport6t64 libqt6sql6t64 libqt6test6t64 libqt6widgets6t64 libqt6xml6t64 librados2 librdmacm1t64
  libssh-gcrypt-4 libusbmuxd6 libwireshark17t64 libwiretap14t64 libwsutil15t64 openjdk-17-jre openjdk-17-jre-headless python3-jose
  python3-lib2to3 python3-rsa python3.11 python3.11-dev python3.11-minimal rwho rhod samba-vfs-modules
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

После обновления системы установил важные компоненты, необходимые для hydra

```
(ksudzuki@KSudzuki)-[~]
$ sudo apt-get install git
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
git is already the newest version (1:2.45.2-1).
git set to manually installed.
The following packages were automatically installed and are no longer required:
chrome-gnome-shell fonts-liberation2 gnome-backgrounds ibverbs-providers libarmadillo12 libassuan0 libavfilter9 libavformat60
libblosc2-3 libboost-iostreams1.83.0 libboost-thread1.83.0 libcephfs2 libdisplay-info1 libgdal34t64 libgeos3.12.2 libgfpapi0 libgfrpc0
libgfxdr0 libglusterfs0 libibverbs1 libimobiledevice6 libjsoncpp25 liblua5.2-0 libnghttp3-3 libplacebo338 libplist3 libpoppler134
libpostproc57 libproxy1-plugin-gsettings libproxy1-plugin-networkmanager libproxy1-plugin-webkit libpython3.11-dev
libpython3.11-minimal libpython3.11-stdlib libpython3.11t64 libqt6dbus6t64 libqt6gui6t64 libqt6network6t64 libqt6opengl6t64
libqt6openglwidgets6t64 libqt6printsupport6t64 libqt6sql6t64 libqt6test6t64 libqt6widgets6t64 libqt6xml6t64 librados2 librdmacm1t64
libssh-gcrypt-4 libusbmuxd6 libwireshark17t64 libwiretap14t64 libwsutil15t64 openjdk-17-jre openjdk-17-jre-headless python3-jose
python3-lib2to3 python3-rsa python3.11 python3.11-dev python3.11-minimal rwho rwho-d samba-vfs-modules
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

После обновления системы установил важные компоненты, необходимые для hydra

```
(ksudzuki@KSudzuki)-[~]  
$ sudo apt-get install libssl-dev libssh-dev libidn1-dev libpcres-dev \ libgtk2.0-dev libmysqlclient-dev libpq-dev libsvn-dev \ firebird-dev libncp-dev  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
Package libmysqlclient-dev is not available, but is referred to by another package.  
This may mean that the package is missing, has been obsoleted, or  
is only available from another source  
However the following packages replace it:  
  libmariadb-dev-compat libmariadb-dev  
  
E: Unable to locate package libgtk2.0-dev  
E: Couldn't find any package by glob 'libgtk2.0-dev'  
E: Couldn't find any package by regex 'libgtk2.0-dev'  
E: Package 'libmysqlclient-dev' has no installation candidate  
E: Unable to locate package firebird-dev  
E: Unable to locate package libncp-dev
```


Клонировал репозиторий с Github

```
(ksudzuki@KSudzuki)-[~]  
$ git clone https://github.com/vanhauser-thc/thc-hydra.git  
Cloning into 'thc-hydra'...  
remote: Enumerating objects: 3607, done.  
remote: Counting objects: 100% (1392/1392), done.  
remote: Compressing objects: 100% (193/193), done.  
remote: Total 3607 (delta 1264), reused 1228 (delta 1199), pack-reused 2215 (from 1)  
Receiving objects: 100% (3607/3607), 3.30 MiB | 195.00 KiB/s, done.  
Resolving deltas: 100% (2449/2449), done.
```

Зашёл в директорию thc-hydra и выполнил команду - ./configure

```
(ksudzuki@KSudzuki)-[~]  
$ cd thc-hydra  
  
(ksudzuki@KSudzuki)-[~/thc-hydra]  
$ ./configure
```

Выполнил команду с помощью sudo make и sudo make install

```
(ksudzuki@KSudzuki)-[~/thc-hydra]
$ sudo make

Now type make install

(ksudzuki@KSudzuki)-[~/thc-hydra]
$ sudo make install

Now type make install
strip hydra pw-inspector
echo OK > /dev/null && test -x xhydra && strip xhydra || echo OK > /dev/null
mkdir -p /usr/local/bin
cp -f hydra-wizard.sh hydra pw-inspector /usr/local/bin && cd /usr/local/bin && chmod 755 hydra-wizard.sh hydra pw-inspector
echo OK > /dev/null && test -x xhydra && cp xhydra /usr/local/bin && cd /usr/local/bin && chmod 755 xhydra || echo OK > /dev/null
sed -e "s|^INSTALLDIR=.*|INSTALLDIR=\"/usr/local\"|" dpl4hydra.sh | sed -e "s|^LOCATION=.*|LOCATION=\"/etc\"|" > /usr/local/bin/dpl4hydra.sh
chmod 755 /usr/local/bin/dpl4hydra.sh
mkdir -p /usr/local/etc
cp -f *.csv /usr/local/etc
mkdir -p /usr/local/man/man1/
cp -f hydra.1 xhydra.1 pw-inspector.1 /usr/local/man/man1/
mkdir -p /usr/local/share/pixmaps/
cp -f xhydra.png /usr/local/share/pixmaps/
mkdir -p /usr/local/share/applications
desktop-file-install --dir /usr/local/share/applications xhydra.desktop
```

Проверил установилась ли hydra с помощью команды - hydra -help

```
(ksudzuki@KSudzuki)-[~]
$ hydra -help
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).

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:
-R      restore a previous aborted/crashed session
-I      ignore an existing restore file (don't wait 10 seconds)
-S      perform an SSL connect
-s PORT if the service is on a different default port, define it here
-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
-x MIN:MAX:CHARSET password brute-force generation, type "-x -h" to get help
-y      disable use of symbols in brute-force, see above
-r      use a non-random shuffling method for option -x
-e nsr   try "n" null password, "s" login as pass and/or "r" reversed login
-u      loop around users, not passwords (effective! implied with -x)
-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
-o FILE  write found login/password pairs to FILE instead of stdout
-b FORMAT specify the format for the -o FILE: text(default), json, jsonv1
-f / -F  exit when a login/pass pair is found (-M: -f per host, -F global)
-t TASKS run TASKS number of connects in parallel per target (default: 16)
-T TASKS run TASKS connects in parallel overall (for -M, default: 64)
-w / -W TIME wait time for a response (32) / between connects per thread (0)
-c TIME  wait time per login attempt over all threads (enforces -t 1)
-4 / -6  use IPv4 (default) / IPv6 addresses (put always in [] also in -M)
-v / -V / -d verbose mode / show login+pass for each attempt / debug mode
```

Установил hydra на kali linux