Routersploit-multi-ip at present only support running on Linux system, and I only tested it on Kali-linux, porrot-os, Debian.

This repository is a wrapper of Routersploit(ref: https://github.com/threat9/routersploit). So, before run this program, you should download the newest version of Routersploit. And how to install Routersploit, have a refference at https://github.com/threat9/routersploit/blob/master/README.md

Because of unsupport of multi target scan method on Routersploit project, I modified some of the code to fit this meet.

USAGE:

1. download and install routersploit:

According to readme.md of routersploit repository, on debian-like linux system, tap code:

apt-get install python3-pip

git clone https://www.github.com/threat9/routersploit

cd routersploit

python3 -m pip install -r requirements.txt

cd ..

2.download routersploit-multi-ip and merge it with routersploit:

git clone https://github.com/WongWai95/routersploit-multi-ip

Now, you will have directories of routersploit and routersploit-multi-ip on the same directory.

Then, we will merge them by tapping:

```
cd routersploit-multi-ip/
cp -r * ../routersploit
```

```
root@i[redacted]:~# cd routersploit-multi-ip/
root@i[redacted]:~/routersploit-multi-ip# ls
ip_range.txt  multi_ip_scanner.sh  routersploit  rsf-scanner.py  scanner_output
root@i[redacted]:~/routersploit-multi-ip# cp -r * ../routersploit
root@i[redacted]:~/routersploit-multi-ip#
```

3. set the ips you wanna scan:

cd ../routersploit

nano ip_range.txt

Then, input ips, one per line

```
root@i[redacted]:~# cd routersploit-multi-ip/
root@i[redacted]:~/routersploit-multi-ip# ls
ip_range.txt  multi_ip_scanner.sh  routersploit  rsf-scanner.py  scanner_output
root@i[redacted]:~/routersploit-multi-ip# cp -r * ../routersploit
root@i[redacted]:~/routersploit-multi-ip# cd ../routersploit
root@i[redacted]:~/routersploit# nano ip_range.txt
```

```
  GNU nano 2.7.4                File: ip_range.txt                Modified

172.16.173.147
192.168.1.1
192.168.1.2

                              [ Read 2 lines ]
^G Get Help  ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos
^X Exit      ^R Read File  ^\ Replace    ^U Uncut Text ^T To Spell   ^_ Go To Line
```

4. Exploit

tap:

./multi_ip_scanner.sh

if necessary, run ‘chmod +x multi_ip_scanner.sh’

procedure starts…

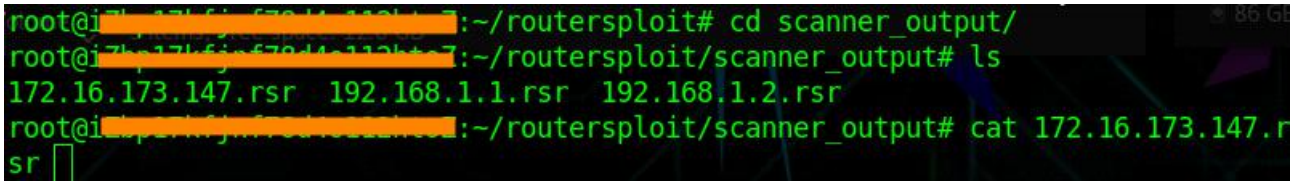
wait for ends!

5. look up results

by tapping:

cd scanner_output/

result of each ip exits in file named with ‘ip.rsr’.



Use explorer you like to visualize it!

```
[-] 172.16.173.147:80 http exploits/routers/multi/rom0 is not vulnerable
[-] 172.16.173.147:32764 custom/tcp exploits/routers/multi/tcp_32764_info_disclo
sure is not vulnerable
[-] 172.16.173.147:80 http exploits/routers/multi/misfortune_cookie is not vulne
rable
[-] 172.16.173.147:80 http exploits/routers/multi/gpon_home_gateway_rce is not v
ulnerable
[-] 172.16.173.147:32764 custom/tcp exploits/routers/multi/tcp_32764_rce is not
vulnerable
[-] 172.16.173.147:69 custom/udp exploits/routers/cisco/ucm_info_disclosure is n
ot vulnerable
[-] 172.16.173.147:53413 custom/udp exploits/routers/netcore/udp_53413_rce is no
t vulnerable
[-] 172.16.173.147:43690 custom/udp exploits/routers/huawei/hg520_info_disclosur
e is not vulnerable
[-] 172.16.173.147:1900 custom/udp exploits/routers/dlink/dir_300_645_815_upnp_r
ce is not vulnerable
[-] 172.16.173.147:39889 custom/udp exploits/routers/dlink/dwr_932b_backdoor is
not vulnerable
[-] 172.16.173.147:22 snmp exploits/routers/thomson/twg849_info_disclosure is no
t vulnerable

[-] Operation cancelled by user
root@iZbp17kfjnf78d4o112htoZ:~/routersploit/scanner_output#
```