
# Flashlight

Information Security Inc.

# Contents

- About Flashlight
- Testing Environment
- Installing Flashlight
- Using Flashlight
- References

# About Flashlight

- Automated Information Gathering Tool for Penetration Testers

# Testing Environment

- Kali Linux 2017

```
root@kali2017:~# cat /etc/*rel*
DISTRIB_ID=Kali
DISTRIB_RELEASE=kali-rolling
DISTRIB_CODENAME=kali-rolling
DISTRIB_DESCRIPTION="Kali GNU/Linux Rolling"
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
ID=kali
VERSION="2017.3"
VERSION_ID="2017.3"
ID_LIKE=debian
ANSI_COLOR="1;31"
HOME_URL="http://www.kali.org/"
SUPPORT_URL="http://forums.kali.org/"
BUG_REPORT_URL="http://bugs.kali.org/"
```

# Installing Flashlight

- Installing dependencies

```
root@kali2017:~# apt-get install nmap tshark tcpdump dsniff phantomjs
Reading package lists... Done
Building dependency tree
Reading state information... Done
dsniff is already the newest version (2.4b1+debian-28).
dsniff set to manually installed.
nmap is already the newest version (7.60+dfsg2-1kali1).
nmap set to manually installed.
phantomjs is already the newest version (2.1.1+dfsg-2).
tcpdump is already the newest version (4.9.2-1).
tcpdump set to manually installed.
tshark is already the newest version (2.4.2-1).
tshark set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

# Installing Flashlight

- Clone GitHub repository

```
root@kali2017:~# git clone https://github.com/galkan/flashlight.git
Cloning into 'flashlight'...
remote: Counting objects: 505, done.
remote: Total 505 (delta 0), reused 0 (delta 0), pack-reused 505
Receiving objects: 100% (505/505), 110.86 KiB | 313.00 KiB/s, done.
Resolving deltas: 100% (310/310), done.
```

# Installing Flashlight

- Resolve “/usr/local/bin/phantom.js Doesn’t Exists On The System”

```
root@kali2017:~/flashlight# ./flashlight.py -v  -s passive -p passive-pro-01 -i eth0 -o /root/Desktop/flashlight_test -l /root/D
esktop/log
/usr/local/bin/phantomjs Doesn't Exists On The System
root@kali2017:/usr/local/bin# pwd
/usr/local/bin

root@kali2017:/usr/local/bin# which phantomjs
/usr/bin/phantomjs
root@kali2017:/usr/local/bin# ln -s /usr/bin/phantomjs phantomjs
root@kali2017:/usr/local/bin# file phantomjs
phantomjs: symbolic link to /usr/bin/phantomjs
root@kali2017:/usr/local/bin# ls -alh phantomjs
lrwxrwxrwx 1 root staff 18 Nov 16 20:49 phantomjs -> /usr/bin/phantomjs
```

# Installing Flashlight

- Resolve “/usr/local/bin/rasterize.js Doesn’t Exists On The System”

```
root@kali2017:~/flashlight# ./flashlight.py -v  -s passive -p passive-pro-01 -i eth0 -o /root/Desktop/flashlight_test -l /root/D
esktop/log_ve -p passive-pro-01 -i eth0 -o /root/Desktop/flashlight_test -l /root/De
/usr/local/bin/rasterize.js Doesn't Exists On The System
root@kali2017:/usr/bin# find / -name "rasterize.js"
/root/CyberChef/node_modules/phantomjs-prebuilt/lib/phantom/examples/rasterize.js
/usr/share/doc/phantomjs/examples/rasterize.js
root@kali2017:/usr/bin# ln -s /usr/share/doc/phantomjs/examples/rasterize.js /usr/local/bin/rasterize.js
root@kali2017:/usr/bin#
```

# Using Flashlight

- Running Flashlight

```
root@kali2017:~# cd flashlight/
root@kali2017:~/flashlight# ls -hla
total 60K
drwxr-xr-x   6 root root 4.0K Nov 16 20:28 .
drwxr-xr-x 112 root root  12K Nov 16 20:28 ..
drwxr-xr-x   2 root root 4.0K Nov 16 20:28 config
-rw-r--r--   1 root root  909 Nov 16 20:28 flashlight-blackhat-arsenal.md
-rwxr-xr-x   1 root root  267 Nov 16 20:28 flashlight.py
drwxr-xr-x   8 root root 4.0K Nov 16 20:28 .git
drwxr-xr-x   2 root root 4.0K Nov 16 20:28 images
drwxr-xr-x   7 root root 4.0K Nov 16 20:28 lib
-rw-r--r--   1 root root 1.1K Nov 16 20:28 LICENSE.txt
-rw-r--r--   1 root root  15K Nov 16 20:28 README.md
```

# Using Flashlight

- Running Flashlight -> the help menu

```
root@kali2017:~/flashlight# ./flashlight.py -h
usage: Usage: use --help for further information

Flashligth: Light your ways through Pentest

optional arguments:
  -h, --help            show this help message and exit
  -p PROJECT, --project PROJECT
                        Project Name
  -s {active,passive,screen,filter}, --scan_type {active,passive,screen,filter}
                        Scan Type
  -d DESTINATION, --destination DESTINATION
                        Target Ip/Host Name
  -c FILE, --config FILE
                        Configuration File
  -i INTERFACE, --interface INTERFACE
                        Interface
  -f PCAP, --pcap_file PCAP
                        Pcap File for Filtering
  -r RASTERIZE, --rasterize RASTERIZE
                        Rasterize Js File For ScreenShot
  -t THREAD, --thread THREAD
                        Thread Number
  -o OUTPUT, --output OUTPUT
                        Output Directory
  -a, --alive           Ping Scan to Investigate Which Ip Address Are Up
                        Before Scanning
  -g GATEWAY, --gateway GATEWAY
                        Specify Gateway
  -l FILE, --log FILE   Log File
  -k PASSIVE_TIMEOUT, --passive_timeout PASSIVE_TIMEOUT
                        Passive Scan Timeout Value
  -m, --mim             Capture the Traffic When Performing Man in The Middle
  -n, --nmap-optimize   Use Some Extra Nmap Options To Optimize Scanning For
                        Performance Tuning
  -v, --verbose         Verbose Output
  -V, --version         show program's version number and exit
```

# Using Flashlight

- Running Flashlight -> Passive Scan

```
root@kali2017:~/flashlight# ./flashlight.py -v  -s passive -p passive-pro-01 -i eth0 -o /root/Desktop/flashlight_test -l /root/D
esktop/log
FLASHLIGHT : 2017-11-16 20:52:58 :  START: Tcpdump
[=============================================================================================] 100%

FLASHLIGHT : 2017-11-16 20:53:14 :  STOP: Tcpdump
FLASHLIGHT : 2017-11-16 20:53:14 :  Finished Passive Scan. Results saved in /root/Desktop/flashlight_test/output/passive-pro-01/
pcap/ folder
```

# Using Flashlight

- Running Flashlight -> Passive Scan, Directory Structure and pcap

```
root@kali2017:~/flashlight# cd /root/Desktop/flashlight_test/output/passive-pro-01/
root@kali2017:~/Desktop/flashlight_test/output/passive-pro-01# ls -hla
total 20K
drwxr-xr-x 5 root root 4.0K Nov 16 20:52 .
drwxr-xr-x 3 root root 4.0K Nov 16 20:46 ..
drwxr-xr-x 2 root root 4.0K Nov 16 20:46 nmap
drwxr-xr-x 2 root root 4.0K Nov 16 20:52 pcap
drwxr-xr-x 2 root root 4.0K Nov 16 20:52 screen
root@kali2017:~/Desktop/flashlight_test/output/passive-pro-01#
root@kali2017:~/Desktop/flashlight_test/output/passive-pro-01#
root@kali2017:~/Desktop/flashlight_test/output/passive-pro-01# cd nmap
root@kali2017:~/Desktop/flashlight_test/output/passive-pro-01/nmap# ls
root@kali2017:~/Desktop/flashlight_test/output/passive-pro-01/nmap# cd ..
root@kali2017:~/Desktop/flashlight_test/output/passive-pro-01# ls
nmap  pcap  screen
root@kali2017:~/Desktop/flashlight_test/output/passive-pro-01# cd pcap
root@kali2017:~/Desktop/flashlight_test/output/passive-pro-01/pcap# ls
20171116205258.pcap
root@kali2017:~/Desktop/flashlight_test/output/passive-pro-01/pcap# tcpdump -r 20171116205258.pcap
reading from file 20171116205258.pcap, link-type EN10MB (Ethernet)
20:52:58.639299 IP 192.168.10.15.2319 > linux.rtma.tk.ssh: Flags [.], ack 1679695346, win 2047, lengt
20:52:58.743917 IP 52.169.5.206.1065 > 192.168.10.95.1231: Flags [.], seq 293360019:293368503, ack 15
484
20:52:58.743973 IP 52.169.5.206.1065 > 192.168.10.95.1231: Flags [.], seq 8484:12726, ack 1, win 513,
20:52:58.744072 IP 192.168.10.95.1231 > 52.169.5.206.1065: Flags [.], ack 12726, win 31113, length 0
```

# Using Flashlight

- Running Flashlight -> Passive Scan, Arp Spoof

```
root@kali2017:~/flashlight# ./flashlight.py -s passive -p passive-project-02 -i eth0 -g 192.168.10.1
-m -k 50 -v
FLASHLIGHT : 2017-11-16 21:17:26 :  Ip Forwarding Enabled
FLASHLIGHT : 2017-11-16 21:17:26 :  Getting Default Gw 192.168.10.1
FLASHLIGHT : 2017-11-16 21:17:26 :  START: Arpspoofing
FLASHLIGHT : 2017-11-16 21:17:26 :  START: Tcpdump
[                   ] 0%ff:ff:ff:ff:ff:ff 0806 42: arp reply 192.168.10.1 is-at 0:c:29:73:aa:2e

[====               ] 4%ff:ff:ff:ff:ff:ff 0806 42: arp reply 192.168.10.1 is-at 0:c:29:73:aa:2e


[========           ] 8%0:c:29:73:aa:2e ff:ff:ff:ff:ff:ff 0806 42: arp reply 192.168.10.1 is-at 0:c:
29:73:aa:2e
[============       ] 12%0:c:29:73:aa:2e ff:ff:ff:ff:ff:ff 0806 42: arp reply 192.168.10.1 is-at 0:c
:29:73:aa:2e
[================   ] 16%0:c:29:73:aa:2e ff:ff:ff:ff:ff:ff 0806 42: arp reply 192.168.10.1 is-at 0:c
```

# Using Flashlight

- Running Flashlight -> Active Scan

```
root@kali2017:~/flashlight# ./flashlight.py -v -a -p activepro -s active -d 192.18.10.0/24
FLASHLIGHT : 2017-11-16 21:46:08 :  START: Nmap Ping Scan
FLASHLIGHT : 2017-11-16 21:46:08 :  CMD - Ping Scan: /usr/bin/nmap -n -sn -T5 -iL /tmp/tmp40MtcI -oA /root/flashlight/output/activepro/nmap/PingScan-2
01711162146
FLASHLIGHT : 2017-11-16 21:47:01 :  STOP: Nmap Ping Scan
FLASHLIGHT : 2017-11-16 21:47:01 :  START: Active Scan Against:
FLASHLIGHT : 2017-11-16 21:47:01 :  START: Nmap PortScan
FLASHLIGHT : 2017-11-16 21:47:01 :  CMD - PortScan : /usr/bin/nmap -n -Pn -T5 --open -iL /tmp/tmpGZhJnf -sS -p T:21,22,23,25,80,443,445,3128,8080,U:53
,161 -sU -oA /root/flashlight/output/activepro/nmap/PortScan-201711162147
FLASHLIGHT : 2017-11-16 21:47:01 :  START: Nmap OsScan
FLASHLIGHT : 2017-11-16 21:47:01 :  CMD - OsScan : /usr/bin/nmap -n -Pn -O -T5 -iL /tmp/tmpGZhJnf -oA /root/flashlight/output/activepro/nmap/OsScan-20
1711162147
FLASHLIGHT : 2017-11-16 21:47:01 :  START: Nmap ScriptScan
FLASHLIGHT : 2017-11-16 21:47:01 :  CMD - ScriptScan : /usr/bin/nmap -n -Pn -T5 -iL /tmp/tmpGZhJnf -sS -p T:21,22,23,25,80,443,445,3128,8080,U:53,161
-sU --script=default,http-enum -oA /root/flashlight/output/activepro/nmap/ScriptScan-201711162147
FLASHLIGHT : 2017-11-16 21:47:01 :  STOP: Nmap PortScan
FLASHLIGHT : 2017-11-16 21:47:02 :  STOP: Nmap OsScan
FLASHLIGHT : 2017-11-16 21:47:03 :  STOP: Nmap ScriptScan
FLASHLIGHT : 2017-11-16 21:47:03 :  Finished Active Scan. Results saved in /root/flashlight/output/activepro/nmap/ folder
```

# References

- Kitploit
http://www.kitploit.com/2015/12/flashlight-automated-information.html

- Kali Linux 2017
http://www.kitploit.com/2017/09/kali-linux-20172-release-best.html