WarBerry

Information Security Inc.

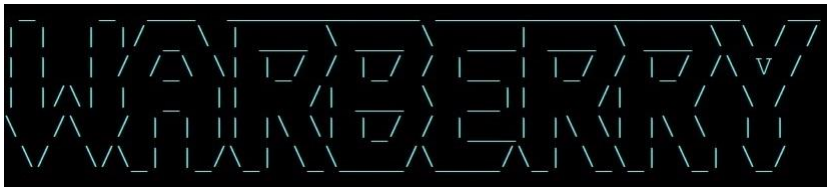
iSEC
information security inc.

Contents

- About WarBerry
- Testing Environment
- Installing WarBerry
- Using WarBerry
- References

About WarBerry

- **WarBerryPi** was built to be used as a hardware implant during red teaming scenarios where we want to obtain as much information as possible in a short period of time with being as stealth as possible. Just find a network port and plug it in



About WarBerry

- The scripts have been designed in a way that the approach is targeted to avoid noise in the network that could lead to detection and to be as efficient as possible. The WarBerry script is a collection of scanning tools put together to provide that functionality

Testing Environment

- Kali Linux 2017 on Raspberry Pi 3 model B

```
root@WarBerry:~# 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 WarBerry

- Create the following directories: /home/pi/WarBerry/Tools and /home/pi/WarBerry/Results

```
mkdir -p  /home/pi/WarBerry/Results
mkdir -p  /home/pi/WarBerry/Tools
```

Installing WarBerry

- Installing CME (https://github.com/byt3bl33d3r/CrackMapExec/wiki/Installation)

```
root@WarBerry:/home/pi/WarBerry# apt-get install crackmapexec
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  python-gevent python-greenlet python-msgpack python-netaddr python-termcolor
Suggested packages:
  python-gevent-doc python-gevent-dbg python-greenlet-doc python-greenlet-dev python-greenlet-dbg ipython
  python-netaddr-docs
The following NEW packages will be installed:
  crackmapexec python-gevent python-greenlet python-msgpack python-netaddr python-termcolor
0 upgraded, 6 newly installed, 0 to remove and 0 not upgraded.
Need to get 2309 kB of archives.
After this operation, 9244 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

Installing WarBerry

- Clone the GitHub repository

```
# git clone https://github.com/secgroundzero/warberry.git
Cloning into 'warberry'...
remote: Counting objects: 1681, done.
remote: Total 1681 (delta 0), reused 0 (delta 0), pack-reused 1681
Receiving objects: 100% (1681/1681), 6.49 MiB | 3.37 MiB/s, done.
Resolving deltas: 100% (847/847), done.
```

Installing WarBerry

- The structure should be as following -> /home/pi/WarBerry/warberry

```
root@WarBerry:/home/pi/WarBerry/warberry# pwd
/home/pi/WarBerry/warberry
```

Installing WarBerry

- Running setup.sh

```
              # cd warberry/
              /warberry# ls
README     REPORTING  decrypt.py  run_responder.py  src          wrapper.py
README.md  SCREENS    password    setup.sh          warberry.py  xml_producer.py
              /warberry# chmod +x setup.sh
              /warberry# ./setup.sh
Hit:1 http://ftp.ne.jp/Linux/packages/kali/kali kali-rolling InRelease
Reading package lists... Done
W: http: aptMethod::Configuration: could not load seccomp policy: Invalid argument
W: http: aptMethod::Configuration: could not load seccomp policy: Invalid argument
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
```

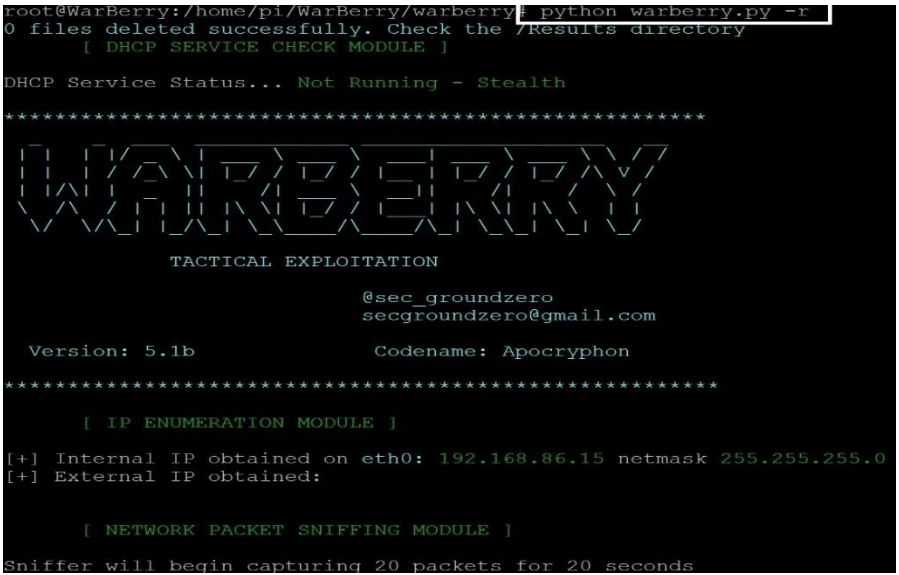
Using WarBerry

- WarBerry help menu

```
root@WarBerry:/home/pi/WarBerry/warberry# python warberry.py -h

[-] Warberry Usage [-]

Options:

  --version                        show program's version number and exit
  -h, --help                       show this help message and exit
  -p PACKETS, --packets=PACKETS    Number of Network Packets to capture
  -I IFACE, --interface=IFACE      Network Interface to use. Default: eth0
  -N NAME, --name=NAME             Hostname to use. Default: Auto
  -i INTENSITY, --intensity=INTENSITY   Port scan intensity. Default: T1
  -Q, --quick                      Scan using threads. Default: Off
  -P, --poison                     Turn Poisoning on/off. Default: On
  -t, --time                       Responder timeout time. Default: 900 seconds
  -H, --hostname                   Do not Change WarBerry hostname Default: Off
  -e, --enumeration                Disable Enumeration mode. Default: Off
  -M, --malicious                  Enable Malicious only mode Default: Off
  -B, --bluetooth                  Enable Bluetooth Scanning. Default: Off
  -W, --wifi                       Enable WiFi Scanning. Default: Off
  -r, --recon                      Enable Recon only mode. Default: Off
  -S, --sniffer                    Enable Sniffer only mode. Default: Off
  -C, --clear                      Clear previous output folders in ../Results
  -m, --man                        Print WarBerry man pages


example usage: sudo python warberry.py -r                    Use only the recon modules
               sudo python warberry.py -H -I wlan0           Use the wlan0 interface and dont change hostname
               sudo python warberry.py -I eth0 -i -T3        Use the eth0 interface and T3 scanning intensity
               sudo python warberry.py -I eth0 -N HackerPC   Use the eth0 interface and change hostname to HackerPC
```

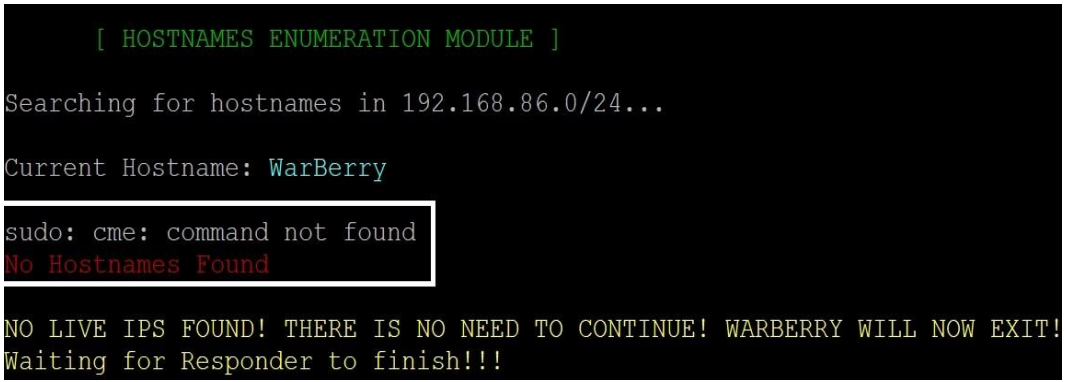
Using WarBerry

- Using only the recon modules



Using WarBerry

- If getting the following error when running warberry.py



Using WarBerry

- Resolve it by replacing “cme” with “crackmapexec” in /* /home/pi/WarBerry/warberry/src/util/utils.py */

```
root@WarBerry:/home/pi/WarBerry/warberry/src/utils# pwd
/home/pi/WarBerry/warberry/src/utils
root@WarBerry:/home/pi/WarBerry/warberry/src/utils# grep --color crackmapexec utils.py
            subprocess.call('sudo crackmapexec %s --timeout=5 | tr -cd "\11\12\15\40-\176" > ../Results/hostnames' %
 CIDR, shell=True)
root@WarBerry:/home/pi/WarBerry/warberry/src/utils#
```

References

- Kitploit
http://www.kitploit.com/2016/05/warberrypi-turn-your-raspberry-pi-into.html

- Kali Linux
https://www.kali.org/downloads/

- Raspberry Pi 3
https://www.raspberrypi.org/products/raspberry-pi-3-model-b/