# Honeypot

Michael Koerfer - 26.05.2017

# Overview

- Hardware
- OS + Installation
- Setup Services
- Network Monitoring
- Live Demo
- Virtualization
- Sources

# Hardware

- Raspberry

- Checkout out a Raspberry Pi 3 Official Desktop Starter Kit

- ARM Cortex-A53 1.2GHz
- 1 GB RAM
- 16 GB MicroSD
- 1 x 100 Mbit/s / WiFi 802.11bgn
- Amazon $60

# OS + Installation

- Honeeepi

- First version (v201310) consisting of Dionaea, only Pi model B
- Second version (v201501) with Dionaea, Kippo, Conpot and Glastopf models Pi B and B +
- Third version (v201509) with Dionaea, Kippo, Conpot, Glastopf and honeyd models Pi 2, B and B +
- Fourth version (v201610) Dionaea, Cowrie, Conpot, Glastopf and honeyd, amun - Models Pi 3 and B
- Other tools

- Honeeepi packages

- Dionaea uses Python as a script language, using libemu to detect shellcodes, supports ipv6 and tls.

- Kippo was replaced by Cowrie!

- Conpot is an ICS honeypot with the aim of gaining insights into the motives and methods of the opponents targeting industrial control systems.

- Glastopf is a Python Web Application Honeypot.

- Cowrie is an SSH honeypot, designed to log brute force attacks and, most importantly, the entire shell interaction performed by the attacker.

# Installation

- Prepare SD card, unmount and delete existing partitions

- Download and unpack Honeeepi-Image depending on Pi version

  https://sourceforge.net/projects/honeeepi/

- Write the Honeeepi image to the SD card

  ```
  $ sudo dd bs = 2M if = honeeepi- "version" .img if = / dev / sdX
  ```

- Insert the SD card. Connect to the wired network and power on. Honeeepi starts with 'dhcpd' and 'sshd'

- Shortly wait and log on via SSH SSH port Standard: 9002 (V.2016.10) & 22 (previous versions)

- Login

  User: pi Password: honeeepi

- First Step

- File system extend to the entire SD card

```
$ sudo raspi-config
reboot
```

- System upgrade

```
$ sudo apt-get update && sudo apt-get upgrade
```

- Change hostname and password

```
$ sudo raspi-config
reboot
```

# Setup Services

- Conpot

- Login: pi

```
$ cd /honeeepi/conpot
$ sudo conpot --template default &          (for Siemens S7-200)*
$ sudo conpot --template kamstrup_382 &     (for smart meter)*
$ sudo conpot --template ipmi &             (ipmi)*
$ sudo conpot --template proxy &            (proxy)*
$ sudo conpot --template guardian_ast &     (AST tank monitoring)
* start as background
```

- Dionaea

- Login: pi

```
$ cd /honeeepi/dionaea-honeypot
$ sudo ./start.sh &
$ sudo ./start-p0f.sh &
```

- Glastopf

- Login: pi

```
$ sudo glastopf-runner &
```

- Cowrie

- Edit your ssh to different port number (from other services)

```
$ sudo vi /etc/ssh/sshd_config
```

- Restart SSH

```
$ sudo /etc/init.d/ssh restart

$ sudo su cowrie

$ cd /honeeepi/cowrie

$ ./start.sh (script start process as background)
```

- Kippo - EOL

- Edit your ssh to different port number (from other services)

```
$ sudo vi /etc/ssh/sshd_config
```

- Restart SSH

```
$ sudo /etc/init.d/ssh restart

$ sudo su kippo

$ cd /honeeepi/kippo

$ ./start.sh (script start process as background)
```

# Network Monitoring

- Ntop (Start as background)

- Login: pi

```
$ cd /opt/ntop-5.0.1
$ sudo ntop &
```

- Set admin password

  http://IP of honeeepi:3000

- Rpcapd

- Login: pi

```
$ sudo passwd root

$ cd /opt/rpcapd

$ sudo start.sh
```

- Configuration remote access with wireshark
- https://www.wireshark.org/docs/man-pages/wireshark.html

# Live Demo

# Honeypot

# Virtualization

- VMWare or VirtualBox*

- DTAG Community Honeypot Project

- > 8 GB RAM

- > 128 GB HDD/SSD

- Network via DHCP

- A working, non-proxied, internet connection

- Follow the DTAG Honeypot Project steps and enjoy

* **For bigger Networks**

# Sources

- The Honeynet Project

- https://www.honeynet.org/

- Honeeepi

- https://redmine.honeynet.org/projects/honeeepi/wiki

- DTAG Community Honeypot Project

- https://dtag-dev-sec.github.io/

- Github

- https://github.com/paralax/awesome-honeypots

# Questions ????????

# Thank you

Author: Michael Koerfer

E-mail: michael_koerfer@posteo.de

Twitter: @D_70WN