csc-isac

Release 0.1

Jul 15, 2020

Contents:

Welcome to CSC-ISAC Project to control all the things into one project Honeypots

CHAPTER 1

Introduction

CSC-ISAC Threat Intelligence Sharing Platform is one of grant project from ISIF Foundation. The goal of the project is to consume information gathers from independent sensors (ex. Honeypots, IDS, Endpoint Detection) to have a centralized database and has independent analysis team to be able to share with the cyber security community inside South East Asia Region. Our baseline Threat Intelligence Platform based on several open source project such as:

1. Honeypot
2. MISP (Malware Information Sharing Platform)
3. NodeRed

We Integrate those open source project to cooexist and collaborate together to perform analysis and sharing platform for our community.

1.1 Threat Intelligence

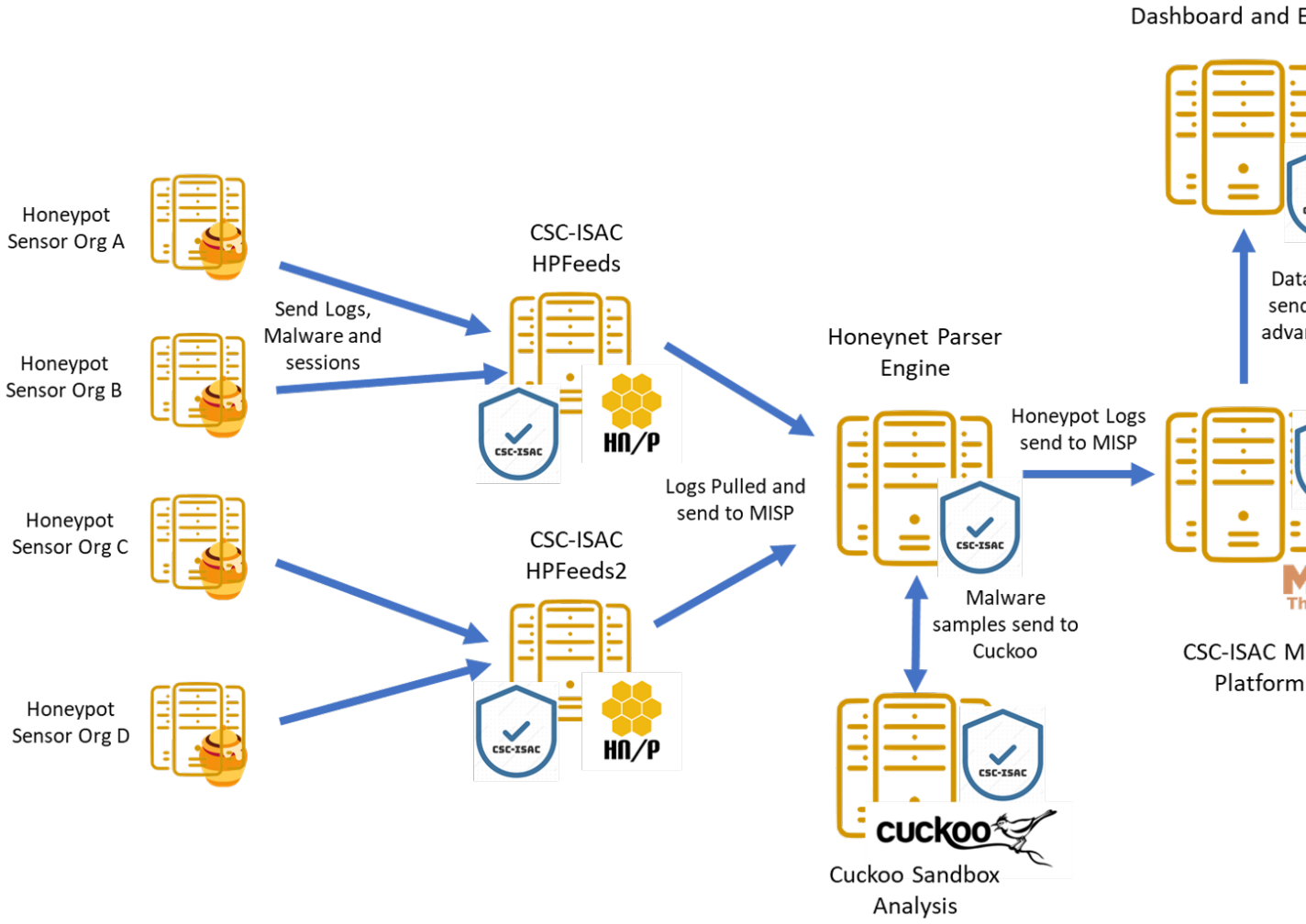
Threat intelligence is knowledge that allows you to prevent or mitigate cyberattacks. Rooted in data, threat intelligence gives you context that helps you make informed decisions about your security by answering questions like who is attacking you, what their motivations and capabilities are, and what indicators of compromise in your systems to look for. source: https://www.recordedfuture.com/threat-intelligence-definition/

1.2 What is Honeypot

A machine that attracts “Attacker”. It was made as weak and as interesting as the creator can be to attract the “Attacker” so that the “Attacker” will be interested and injecting something to the honeypot like it was the real machine.

1.3 Deployment Architecture

Our Architectures considering a scalable environment that can be integrated with various organizations and even researchers that want to contribute with our CSC-ISAC Community. The architecture is presented as follows:



1.4 Disclaimer

CSC-ISAC Threat Intelligence Platform is distributed as it is, in the hope that it will be useful, but without any warranty neither the implied merchantability or fitness for a particular purpose.

Whatever you do with this tool is uniquely your own responsibility.

1.5 Community Guidelines

The CSC-ISAC (Cyber Security Community - Information Sharing and Analysis Center) Organization is a non-profit organization incorporated as a Stichting in the Indonesia and it's mainly dedicated to support of the development and

growth of Threat Intelligence Sharing & Analysis Community across Asia Pasific Region, specifically in integration with honeypot installation and other open source platform

The organization is initally funded by ISIF Grants and operates to secure financial and infrastructure support to our software projects and coordinates the development and contributions from the community.

CHAPTER 2

Installation

In this manual you will learn to install honeypot (specifically, Dionaea and Cowrie honeypot) using existing docker images that have been created and distributed through github or docker hub.

2.1 Preparing The Honeypot Sensor

2.2 Cowrie

Cowrie is a medium interaction honeypot that works on two protocols, Secure Shell (SSH) and Telnet. Cowrie will record any activity that happened in the honeypot throughout the whole session.

Services and port number list: Secure Shell (SSH) : port 22 Telnet : port 23

In this section, you will learn how to install and run cowrie honeypot using docker. The installation of cowrie is implemented by using existing Dockerfile that is required to be reconfigured before the user builds the docker image.

Firstly, clone the honeypot Dockerfile by using this command:

```
Docker pull cowrie/cowrie
```

Then, run the docker image by using this command:

```
Docker run cowrie:devel
```

At this moment, you would notice that cowrie honeypot us listening on port 2222 for SSH protocol and 2223 for telnet protocol. This however, will not ensure that you will gain any data since those two port numbers are considered as illegitimate ports usage. Thus, a change is needed to set the port number into the default port number for each service. In order to configure the settings of the docker image, you will need to access the docker image as root:

```
docker exec -u 0 -ti container_id /bin/bash
```

Once you get inside the docker images as root, run this command to install the necessary tools in order to access the settings.

```
Apt-get update
Apt-get install nano
Apt-get install authbind
```

After that, access the "etc" directory inside the "cowrie-git" folder by using this command:

```
Cd /cowrie-git/etc
```

Now, copy the the configuration file "cowrie.cfg.dist" into "cowrie.cfg" and open it using the command below:

```
cp cowrie.cfg.dist cowrie.cfg
nano cowrie.cfg
```

Then, change the configuration in the script:

```
[ssh]
enabled = true
listen_endpoints = tcp:22:interface:0.0.0.0

[telnet]
enabled = true
listen_endpoints = tcp:23:interface:0.0.0.0


[output_hpfeeds]
enabled = true
server = ip_address
port = 10000
identifier = your_identifier
secret = your secret
debug = false

[output_hpfeeds3]
enabled = true
server = ip_address
port = 10000
identifier = your_identifier
secret = your_secret
debug = false
```

Add the command above inside the script ("cowrie.cfg" file), save the changes and proceed to build the docker image by going to the path /home/your_user/tpotce/docker. When you reach that path, execute this command to build cowrie's docker image:

```
sudo docker build cowrie
```

Once it is finished, you will need to push the repository into docker hub so that you can run it. In order to push the docker image into docker hub, you should register yourself in the docker hub website. After that, initiate a docker login by using the command :

```
Docker login --username=your_username --email=your_email@domain.com
```

If everything worked out, you will get a similar message

```
WARNING: login credentials saved in /home/username/.docker/config.json
Login Succeeded
```

Now, you can check your docker image. You will see similar messages

The repository "none" means that your docker image has been successfully built, but does not have any repository yet. Now, you have to push the docker image "none" to your repository. First of all, make sure to create a repository in your docker hub account through the website. Then, using this command to tag the docker image you would like to push into the repository: docker tag image_id your_username/repo_name:tag_name

After you successfully tag your docker image, push it into the repository by using this command:

```
docker push yourusername/repo_name
```

Once it is pushed, it will presentate the previously pushed docker image with the name of its repository

Finally, you just need to run the docker image that you have built. Simply enter the command below to run the docker:

```
Sudo docker run image_name:tag_name
```

Note that if you can run the command without giving any input the tag of the docker image. However, the tag will be considered as latest by default. Therefore, it is recommended to use the complete command to avoid any confusion if you have docker images with the same name but different settings or configuration.

2.2.1 Listening on port 22 and 23

```
Note: this service emulated by Cowrie so the attacker will be trapped
```

At this moment, you would notice that cowrie honeypot us listening on port 2222 for SSH protocol and 2223 for telnet protocol. This however, will not ensure that you will gain any data since those two port numbers are considered as illegitimate ports usage. Thus, a change is needed to set the port number into the default port number for each service. In order to configure the settings of the docker image, you will need to access the docker image as root:

```
docker exec -u 0 -ti container_id /bin/bash
```

Once you get inside the docker images as root, run this command to install the necessary tools in order to access the settings.

```
Apt-get update
Apt-get install nano
Apt-get install authbind
```

After that, access the "etc" directory inside the "cowrie-git" folder by using this command:

```
Cd /cowrie-git/etc
```

Now, copy the the configuration file "cowrie.cfg.dist" into "cowrie.cfg" and open it using the command below:

```
Cp cowrie.cfg.dist cowrie.cfg
Nano cowrie.cfg

sudo touch /etc/authbind/byport/23
sudo chown cowrie:cowrie /etc/authbind/byport/23
sudo chmod 770 /etc/authbind/byport/23
```

Port redirection commands are system-wide and need to be executed as root. A firewall redirect can make your existing SSH server unreachable, remember to move the existing server to a different port number first.

The following firewall rule will forward incoming traffic on port 22 to port 2222 on Linux:

```
sudo iptables -t nat -A PREROUTING -p tcp --dport 22 -j REDIRECT --to-port 2222
```

Or for telnet:

```
sudo iptables -t nat -A PREROUTING -p tcp --dport 23 -j REDIRECT --to-port 2223
```

```
$ sudo touch /etc/authbind/byport/23
$ sudo chown cowrie:cowrie /etc/authbind/byport/23
$ sudo chmod 770 /etc/authbind/byport/23
```

2.3 Dionaea

Dionaea honeypot is a low interaction honeypot that works in multiple protocols that is listed below as well as its default port number:

```
FTP            : port 20/TCP and 21/TCP
Nameserver     : port 42/TCP
TFTP           : port 69/UDP
HTTP           : port 80/TCP
HTTPS          : port 443/TCP
MSRPC          : port 135/TCP
SNMP           : port 161/UDP
SMB            : port 445/TCP
MS-SQL         : port 1433/TCP
MYSQL          : port 3306/TCP
SIP            : port 5060/TCP
SIP-TLS        : port 5061/TCP
Memcached      : port 11211 (both TCP and UDP)
```

In this section, you will learn how to install and run dionaea honeypot using docker. The installation of dionaea is implemented by using existing Dockerfile that is required to be reconfigured for personal use and enabling additional features.

Firstly, clone the honeypot Dockerfile by using this command:

```
Docker pull dinotools/dionaea-docker
```

Then, proceed to run the docker image by executing the command provided below:

```
Docker run dinotools/dionaea-docker
```

After that, access the config folder inside the docker image that has been built as root/administrator account by entering the command :

```
Docker -u 0 -ti container_id /bin/bash
```

Once you proceed, enter the folder etc that is located with the specified path /opt/dionaea/etc/dionaea/ihandlers with the command

```
cd opt/dionaea/etc/dionaea/ihandlers
```

Once you change your directory there, you need to add “hpfeeds.yaml” inside the ihandlers folder. Inside the ihandler folder, execute this command to add the file “hpfeeds.yaml”.

```
Sudo nano hpfeeds.yaml
```

With the command above, it will display an empty file. You need to put these commands in order to implement the changes inside the docker image.

```
- name: hpfeeds
  config:
  # fqdn/ip and port of the hpfeeds broker
  server: "10.20.100.100"
  port: 10000
  ident: "sensor-dionaea"
  secret: "password1234"
# dynip_resolve: enable to lookup the sensor ip through a webservice
  dynip_resolve: "http://hpfriends.honeycloud.net/ip"
# Try to reconnect after N seconds if disconnected from hpfeeds broker
    # reconnect_timeout: 10.0
```

After that, you need to restart the docker container so that the changes that you have made before are implemented. This can be run through the command :

```
Docker restart container_id
```

Finally, in order to ensure that the honeypot actually works, you can use net-tools to display which port have been utilized in order to ensure that the honeypot services have been successfully executed. It can be utilized by using this command:

```
Netstat -plnt
```

After that, make sure every protocol that you enabled in dionaea (all services are enabled by default settings) is listening to the proper port (default port number of each service). You can check it from the screenshot below. To ensure that all of your services provided by dionaea are running on default ports, please refer to the brief explanation of cowrie in the section above.

2.4 Preparing HPFeeds

The followings are the built for HPFeeds (mostly from scratch)

2.5 HPFeeds MongoDB Scratch Built 1 Container

The following are the built for HPFeeds from scsratch for 1 container:

1. First, update your existing list of packages

```
$ sudo apt update
```

2. Next install a few prerequisite package

```
$ sudo apt install docker.io
```

3. Run mongo docker

```
$ docker run -d -p 27017-27019:27017-27019 --name mongodb mongo:latest
```

4. We can do anything what we want with the docker but first of all it's always better to update and upgrade the docker first:

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

5. After we finish updating and upgrading, we need to install wget git nano sudo:

```
$   apt install -y ubuntu-server wget git nano sudo
```

6. Because we install the ubuntu-server there will be some configuration that we should config but for the simplicity sake I have listed below my answer:

```
$   31
```

```
 3. Amharic                                        52. Irish
 4. Arabic                                         53. Italian
 5. Arabic (Morocco)                               54. Japanese
 6. Arabic (Syria)                                 55. Japanese (PC-98)
 7. Armenian                                       56. Kazakh
 8. Azerbaijani                                    57. Khmer (Cambodia)
 9. Bambara                                        58. Korean
 10. Bangla                                        59. Kyrgyz
 11. Belarusian                                    60. Lao
 12. Belgian                                       61. Latvian
 13. Berber (Algeria, Latin)                       62. Lithuanian
 14. Bosnian                                       63. Macedonian
 15. Braille                                       64. Malay (Jawi, Arabic Keyboard)
 16. Bulgarian                                     65. Maltese
 17. Burmese                                       66. Maori
 18. Chinese                                       67. Moldavian
 19. Croatian                                      68. Mongolian
 20. Czech                                         69. Montenegrin
 21. Danish                                        70. Nepali
 22. Dhivehi                                       71. Norwegian
 23. Dutch                                         72. Persian
 24. Dzongkha                                      73. Polish
 25. English (Australian)                          74. Portuguese
 26. English (Cameroon)                            75. Portuguese (Brazil)
 27. English (Ghana)                               76. Romanian
 28. English (Nigeria)                             77. Russian
 29. English (South Africa)                        78. Serbian
 30. English (UK)                                  79. Sinhala (phonetic)
 31. English (US)                                  80. Slovak
 32. Esperanto                                     81. Slovenian
 33. Estonian                                      82. Spanish
 34. Faroese                                       83. Spanish (Latin American)
 35. Filipino                                      84. Swahili (Kenya)
 36. Finnish                                       85. Swahili (Tanzania)
 37. French                                        86. Swedish
 38. French (Canada)                               87. Switzerland
 39. French (Democratic Republic of the Congo)     88. Taiwanese
 40. French (Guinea)                               89. Tajik
 41. French (Togo)                                 90. Thai
 42. Georgian                                      91. Tswana
 43. German                                        92. Turkish
 44. German (Austria)                              93. Turkmen
 45. Greek                                         94. Ukrainian
[More] 31

 46. Hebrew                                        95. Urdu (Pakistan)
 47. Hungarian                                     96. Uzbek
 48. Icelandic                                     97. Vietnamese
 49. Indian                                        98. Wolof
Country of origin for the keyboard: 31
```

```
$ 1
```

```
Please select the layout matching the keyboard for this machine.

  1. English (US)
  2. English (US) - Cherokee
  3. English (US) - English (Colemak)
  4. English (US) - English (Dvorak)
  5. English (US) - English (Dvorak, alt. intl.)
  6. English (US) - English (Dvorak, intl., with dead keys)
  7. English (US) - English (Dvorak, left-handed)
  8. English (US) - English (Dvorak, right-handed)
  9. English (US) - English (Macintosh)
  10. English (US) - English (US, alt. intl.)
  11. English (US) - English (US, euro on 5)
  12. English (US) - English (US, intl., with dead keys)
  13. English (US) - English (Workman)
  14. English (US) - English (Workman, intl., with dead keys)
  15. English (US) - English (classic Dvorak)
  16. English (US) - English (intl., with AltGr dead keys)
  17. English (US) - English (programmer Dvorak)
  18. English (US) - English (the divide/multiply keys toggle the layout)
  19. English (US) - Russian (US, phonetic)
  20. English (US) - Serbo-Croatian (US)
Keyboard layout: 1
```

```
$ 1
```

```
Configuring console-setup
-------------------------

  1. ARMSCII-8          6. GEORGIAN-PS    11. ISO-8859-11  16. ISO-8859-2  21. ISO-8859-7  26.
  2. CP1251             7. IBM1133        12. ISO-8859-13  17. ISO-8859-3  22. ISO-8859-8  27.
  3. CP1255             8. ISIRI-3342     13. ISO-8859-14  18. ISO-8859-4  23. ISO-8859-9  28.
  4. CP1256             9. ISO-8859-1     14. ISO-8859-15  19. ISO-8859-5  24. KOI8-R
  5. GEORGIAN-ACADEMY  10. ISO-8859-10    15. ISO-8859-16  20. ISO-8859-6  25. KOI8-U
Encoding to use on the console: 1
```

```
$ 20
```

```
Please choose the character set that should be supported by the console font.

If you don't use a framebuffer, the choices that start with "." will reduce the number of
colors on the console.

  1. . Arabic
  2. # Armenian
  3. # Cyrillic - KOI8-R and KOI8-U
  4. # Cyrillic - non-Slavic languages
  5. # Cyrillic - Slavic languages (also Bosnian and Serbian Latin)
  6. . Ethiopic
  7. # Georgian
  8. # Greek
  9. # Hebrew
  10. # Lao
  11. # Latin1 and Latin5 - western Europe and Turkic languages
  12. # Latin2 - central Europe and Romanian
  13. # Latin3 and Latin8 - Chichewa; Esperanto; Irish; Maltese and Welsh
  14. # Latin7 - Lithuanian; Latvian; Maori and Marshallese
  15. . Latin - Vietnamese
  16. # Thai
  17. . Combined - Latin; Slavic Cyrillic; Hebrew; basic Arabic
  18. . Combined - Latin; Slavic Cyrillic; Greek
  19. . Combined - Latin; Slavic and non-Slavic Cyrillic
  20. Guess optimal character set
Character set to support: 20
```

7. We need to clone hpfeeds by typing the command above:

```
$ git clone https://github.com/pwnlandia/mhn.git
```

8. Go to mhn/scripts by typing the command above:

```
$ cd mhn/scripts
```

9. We need to install hpfeeds by execute this command:

```
$ ./install_hpfeeds.sh
```

10. After the installation of hpfeeds we need to install mnemosyne we can do that by executing this:

```
$ ./install_mnemosyne.sh
```

11. To check the successful installation and to check the process we can type the command below for checking the hpfeeds process:

```
$ supervisorctl status hpfeeds-broker
```

and the result can be similar to this:

```
root@djap-hpe:/mhn/scripts# supervisorctl status hpfeeds-broke
hpfeeds-broker                   RUNNING   pid 3215, uptime 0:
```

Congrats! You have installed the HPFeeds from Scratch in 1 container!

2.6 HPFeeds MongoDB Scratch Built Separate Container

The following are the built for HPFeeds MongoDB from scratch for separate container:

1. First, update your existing list of packages

```
$ sudo apt update
```

2. Next install a few prerequisite package

```
$ sudo apt install docker.io
```

3. Run mongo docker

```
$ docker run -d -p 27017-27019:27017-27019 --name mongodb mongo:latest
```

4. After We run docker mongo we need to run another docker ubuntu for hosting docker HPFeeds we can do that by typing:

```
$ docker run -ti --network=host --name hpfeeds1804 ubuntu:bionic
```

5. We can do anything what we want with the docker but first of all it's always better to update and upgrade the docker first:

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

6. After we finish updating and upgrading, we need to install wget git nano sudo:

```
$   apt install -y ubuntu-server wget git nano sudo
```

7. Because we install the ubuntu-server there will be some configuration that we should config but for the simplicity sake I have listed below my answer:

```
$   31
```

```
 3. Amharic                                          52. Irish
 4. Arabic                                           53. Italian
 5. Arabic (Morocco)                                 54. Japanese
 6. Arabic (Syria)                                   55. Japanese (PC-98)
 7. Armenian                                         56. Kazakh
 8. Azerbaijani                                      57. Khmer (Cambodia)
 9. Bambara                                          58. Korean
 10. Bangla                                          59. Kyrgyz
 11. Belarusian                                      60. Lao
 12. Belgian                                         61. Latvian
 13. Berber (Algeria, Latin)                         62. Lithuanian
 14. Bosnian                                         63. Macedonian
 15. Braille                                         64. Malay (Jawi, Arabic Keyboard)
 16. Bulgarian                                       65. Maltese
 17. Burmese                                         66. Maori
 18. Chinese                                         67. Moldavian
 19. Croatian                                        68. Mongolian
 20. Czech                                           69. Montenegrin
 21. Danish                                          70. Nepali
 22. Dhivehi                                         71. Norwegian
 23. Dutch                                           72. Persian
 24. Dzongkha                                        73. Polish
 25. English (Australian)                            74. Portuguese
 26. English (Cameroon)                              75. Portuguese (Brazil)
 27. English (Ghana)                                 76. Romanian
 28. English (Nigeria)                               77. Russian
 29. English (South Africa)                          78. Serbian
 30. English (UK)                                    79. Sinhala (phonetic)
 31. English (US)                                    80. Slovak
 32. Esperanto                                       81. Slovenian
 33. Estonian                                        82. Spanish
 34. Faroese                                         83. Spanish (Latin American)
 35. Filipino                                        84. Swahili (Kenya)
 36. Finnish                                         85. Swahili (Tanzania)
 37. French                                          86. Swedish
 38. French (Canada)                                 87. Switzerland
 39. French (Democratic Republic of the Congo)       88. Taiwanese
 40. French (Guinea)                                 89. Tajik
 41. French (Togo)                                   90. Thai
 42. Georgian                                        91. Tswana
 43. German                                          92. Turkish
 44. German (Austria)                                93. Turkmen
 45. Greek                                           94. Ukrainian
[More] 31

 46. Hebrew                                          95. Urdu (Pakistan)
 47. Hungarian                                       96. Uzbek
 48. Icelandic                                       97. Vietnamese
 49. Indian                                          98. Wolof
ountry of origin for the keyboard: 31
```

```
$ 1
```

```
Please select the layout matching the keyboard for this machine.

  1. English (US)
  2. English (US) - Cherokee
  3. English (US) - English (Colemak)
  4. English (US) - English (Dvorak)
  5. English (US) - English (Dvorak, alt. intl.)
  6. English (US) - English (Dvorak, intl., with dead keys)
  7. English (US) - English (Dvorak, left-handed)
  8. English (US) - English (Dvorak, right-handed)
  9. English (US) - English (Macintosh)
  10. English (US) - English (US, alt. intl.)
  11. English (US) - English (US, euro on 5)
  12. English (US) - English (US, intl., with dead keys)
  13. English (US) - English (Workman)
  14. English (US) - English (Workman, intl., with dead keys)
  15. English (US) - English (classic Dvorak)
  16. English (US) - English (intl., with AltGr dead keys)
  17. English (US) - English (programmer Dvorak)
  18. English (US) - English (the divide/multiply keys toggle the layout)
  19. English (US) - Russian (US, phonetic)
  20. English (US) - Serbo-Croatian (US)
Keyboard layout: 1
```

```
$ 1
```

```
Configuring console-setup
-------------------------

  1. ARMSCII-8         6. GEORGIAN-PS   11. ISO-8859-11  16. ISO-8859-2  21. ISO-8859-7  26.
  2. CP1251            7. IBM1133       12. ISO-8859-13  17. ISO-8859-3  22. ISO-8859-8  27.
  3. CP1255            8. ISIRI-3342    13. ISO-8859-14  18. ISO-8859-4  23. ISO-8859-9  28.
  4. CP1256            9. ISO-8859-1    14. ISO-8859-15  19. ISO-8859-5  24. KOI8-R
  5. GEORGIAN-ACADEMY  10. ISO-8859-10  15. ISO-8859-16  20. ISO-8859-6  25. KOI8-U
Encoding to use on the console: 1
```

```
$ 20
```

```
Please choose the character set that should be supported by the console font.

If you don't use a framebuffer, the choices that start with "." will reduce the number of
colors on the console.

  1. . Arabic
  2. # Armenian
  3. # Cyrillic - KOI8-R and KOI8-U
  4. # Cyrillic - non-Slavic languages
  5. # Cyrillic - Slavic languages (also Bosnian and Serbian Latin)
  6. . Ethiopic
  7. # Georgian
  8. # Greek
  9. # Hebrew
  10. # Lao
  11. # Latin1 and Latin5 - western Europe and Turkic languages
  12. # Latin2 - central Europe and Romanian
  13. # Latin3 and Latin8 - Chichewa; Esperanto; Irish; Maltese and Welsh
  14. # Latin7 - Lithuanian; Latvian; Maori and Marshallese
  15. . Latin - Vietnamese
  16. # Thai
  17. . Combined - Latin; Slavic Cyrillic; Hebrew; basic Arabic
  18. . Combined - Latin; Slavic Cyrillic; Greek
  19. . Combined - Latin; Slavic and non-Slavic Cyrillic
  20. Guess optimal character set
Character set to support: 20
```

8. We need to clone hpfeeds by typing the command above:

$ git clone https://github.com/pwnlandia/mhn.git

9. Go to mhn/scripts by typing the command above:

$ cd mhn/scripts

10. We need to install hpfeeds by execute this command:

$ ./install_hpfeeds.sh

11. After the installation of hpfeeds we need to install mnemosyne we can do that by executing this:

$ ./install_mnemosyne.sh

12. To check the successful installation and to check the process we can type the command below for checking the hpfeeds process:

$ supervisorctl status hpfeeds-broker

and the result can be similar to this:

```
root@djap-hpe:/mhn/scripts# supervisorctl status hpfeeds-broke
hpfeeds-broker                   RUNNING   pid 3215, uptime 0:
```

Congrats!!! You have built the HPFeeds from Scratch in separate container!

CHAPTER 3

Usage

In this manual you will learn to use the honeypot (specifically, HPFeeds and MISP with the community) using existing docker images that have been created and distributed through github or docker hub.

3.1 Starting HPFeeds

The following are the steps of how to start to use HPFeeds.

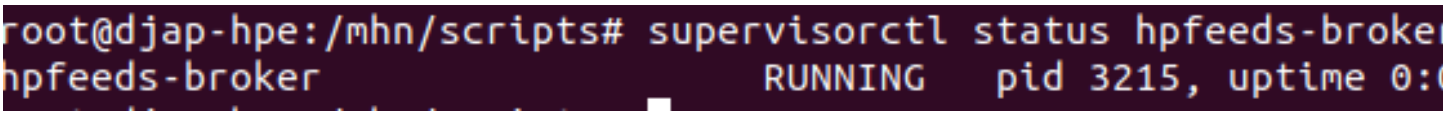
3.2 Start Using HPFeeds that Built from Scratch for 1 Container and Separate Container

The following are the steps for using HPFeeds MongoDB for 1 container and separate container:

1. To check the successful installation and to check the process we can type the command below for checking the hpfeeds process:

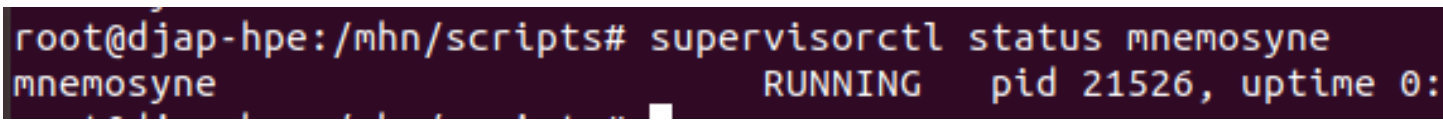
```
$ supervisorctl status hpfeeds-broker
```

and the result can be similar to this:



2. To check the process of the mnemosyne we can type the command below:

```
$ supervisorctl status mnemosyne
```



3. Then we should install pymongo to be able to run the add_user.py

```
$ pip install pymongo
```

4. To add the ident and secret we can do the command below for each honeypot there is different channel, for now we will be focussing on dionaea Honeypot.

```
$ python /opt/hpfeeds/broker/add_user.py sensor-dionaea(according to ident at hpfeeds.
↪yaml) password1234(according to secret at hpfeeds.yaml) "mwbinary.dionaea.
↪sensorunique,dionaea.capture,dionaea.capture.anon,dionaea.captures,dionaea.
↪connections" " "
```

```
root@djap-hpe:/mhn/scripts# python /opt/hpfeeds/broker/add_user.py sensor-dionaea password12
ary.dionaea.sensorunique,dionaea.capture,dionaea.capture.anon,dionaea.captures,dionaea.conne
"
```

5. Then we need to add the python script that is monitoring the MongoDB and send the JSON data when the data arrived at MongoDB

```
$ nano py123.py
```

And add this following python script:

Modify the URL into the URL of your Node-RED IP

```
from pymongo import Connection
import time
import requests
import json
url = 'http://192.168.1.100:1880/test'
db = Connection().mnemosyne
coll = db.hpfeed
cursor = coll.find(tailable=True)
while cursor.alive:
      try:
      doc = cursor.next()
      test = json.dumps(doc, indent=4, default=str)
      print (test)
      response = requests.post(url, data=test)
      except StopIteration:
      time.sleep(1)
```

6. Then we need to execute the python script by typing:

```
$ python3 py123.py
```

7. Then at the dionaea we should modify the hpfeed Edit the hpfeeds.yaml at /opt/dionaea/etc/dionaea/ihandlers-available:

```
$ nano /opt/dionaea/etc/dionaea/ihandlers-available/hpfeeds.yaml
```

```
- name: hpfeeds
  config:
    server: 10.20.100.14
    port: 10000
    ident: sensor-dionaea
    secret: password1234
```

Edit it like this, after that copy the hpfeeds.yaml to /opt/Dionaea/etc/Dionaea/ihandlers-enabled.

```
$ cd /opt/dionaea/etc/dionaea/ihandlers-available/hpfeeds.yaml /opt/dionaea/etc/
↪dionaea/ihandlers-enabled
```

8. Restart the Dionaea and the result will be like this:

```
[15122019 12:56:16] modules /home/rd/dionaea/src/modules.c:203: start module 0x563e03e2
[15122019 12:56:16] dionaea /home/rd/dionaea/src/dionaea.c:781: Installing signal handl
[15122019 12:56:16] dionaea /home/rd/dionaea/src/dionaea.c:818: Creating 2 threads in p
[15122019 12:56:18] connection /home/rd/dionaea/src/connection.c:2208: connection 0x563
connect/tcp/connecting [->] state: connecting->established
[15122019 12:56:18] connection /home/rd/dionaea/src/connection.c:2208: connection 0x563
connect/tcp/established [172.25.1.11:40820->172.25.1.9:10000] state: established->estab
```

9. We do the attack via ftp to Dionaea and the result will be:

```
[15122019 12:59:19] hpfeeds /dionaea/hpfeeds.py:381: accepted connection from  172.25.1.9
o 172.25.1.11:21
[15122019 12:59:19] log_sqlite /dionaea/logsql.py:697: accepted connection from 172.25.1.
to 172.25.1.11:21 (id=18151)
[15122019 12:59:23] ftp /dionaea/ftp.py:241: cmd 'b'USER''
[15122019 12:59:28] ftp /dionaea/ftp.py:241: cmd 'b'PASS''
[15122019 12:59:28] ftp /dionaea/ftp.py:241: cmd 'b'SYST''
```

10. The result of MongoDB should be like this:

```
> db.hpfeed.find().pretty()
{
        "_id" : ObjectId("5ea6dd6b659632541639a6b2"),
        "ident" : "sensor-dionaea",
        "timestamp" : ISODate("2020-04-27T13:26:03.173Z"),
        "normalized" : true,
        "payload" : {
                "local_host" : "192.168.160.3",
                "connection_type" : "accept",
                "connection_protocol" : "httpd",
                "local_port" : 80,
                "remote_port" : 56664,
                "remote_hostname" : "",
                "connection_transport" : "tcp",
                "remote_host" : "103.19.110.145"
        },
        "channel" : "dionaea.connections"
}
>
```

CHAPTER 4

Development

This is for development page where the development of this documentation will be updated regularly.

4.1 Development Notes

4.2 Git Branches

Git branches development here

4.3 Release Versioning

1. v1.0 = 30 June 2020 Updating Usage, Customization, and Development Page
2. v1.1 = 5 July 2020 Updating Usage and Development Page
3. v2.0 = 15 July 2020 Usage, Introduction, and Development modified, Customization deleted

4.4 Contributors

Documentation Editor = Patricia H Advisor = Yohanes S. and all ISIF's Project members

CHAPTER 5

Final Remarks

INi testing Final Remarks Page

5.1 Links

Links here

5.2 Join the Discussion!

Discussion join here

5.3 Support Us!

Please Support us for the sake of security together!

5.4 Supporters

Our beloved supporters goes here!

CHAPTER 6

License

CSC-ISAC Threat Intel Platform is copyrighted by the CSC-ISAC Organization and is licensed under the following GNU General Public License version 3.

GNU GENERAL PUBLIC LICENSE Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/> Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for

software and other kinds of works.

The licenses for most software and other practical works are designed

to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program–to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not

price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you

these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether

gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps:

(1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains

that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run

modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents.

States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and

modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of

works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this

License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work

in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based

on the Program.

To "propagate" a work means to do anything with it that, without

permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other

parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices"

to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided),

that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work

for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official

standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other

than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all

the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users

can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that

same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of

copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not

convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under

the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological

measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid

circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you

receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey,

and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to

produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

> a) The work must carry prominent notices stating that you modified it, and giving a relevant date.
>
> b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".
>
> c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.
>
> d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent

works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms

of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

> a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.
>
> b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.
>
> c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.
>
> d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.
>
> e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded

from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any

tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods,

procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or

specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the

Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a

requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided,

in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this

License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option

remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you

add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

> a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or
>
> b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or
>
> c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or
>
> d) Limiting the use for publicity purposes of names of licensors or authors of the material; or
>
> e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or
>
> f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further

restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you

must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the

form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly

provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your

license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is

reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the

licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or

run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically

receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An “entity transaction” is a transaction transferring control of an

organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party’s predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the

rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A “contributor” is a copyright holder who authorizes use under this

License of the Program or a work on which the Program is based. The work thus licensed is called the contributor’s “contributor version”.

A contributor’s “essential patent claims” are all patent claims

owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, “control” includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free

patent license under the contributor’s essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a “patent license” is any express

agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To “grant” such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license,

and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. “Knowingly relying” means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient’s use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or

arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is “discriminatory” if it does not include within

the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting

any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others’ Freedom.

If conditions are imposed on you (whether by court order, agreement or

otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have

permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of

the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the

Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future

versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different

permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY

APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING

WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided

above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

The file UserDB.txt is copyrighted by BoB / Team PEiD distributed under the following MIT license.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

The file jquery.js is copyrighted by John Resig and dual licensed under the MIT or GPL Version 2 licenses (see: http://jquery.org/license).

The files lightbox.js and lightbox.css are copyrighted by Lokesh Dhakar and licensed under the Creative Commons Attribution 2.5 License (see: http://creativecommons.org/licenses/by/2.5/).

The files bootstrap-fileupload.js, jasny-bootstrap.js, jasny-bootstrap.min.js, jasny-bootstrap.css, jasny-bootstrap.min.css, jasny-bootstrap-responsive.css, jasny-bootstrap-responsive.min.css are copyrighted by Jasny BV and licensed under the Apache License, Version 2.0.

The files bootstrap.min.js, bootstrap.min.css, bootstrap-responsive.min.css, glyphicons-halflings.png, glyphicons-halflings-white.png are copyrighted by Twitter, Inc. and licensed under the Apache License, Version 2.0.

CHAPTER 7

Indices and tables

- genindex
- modindex
- search