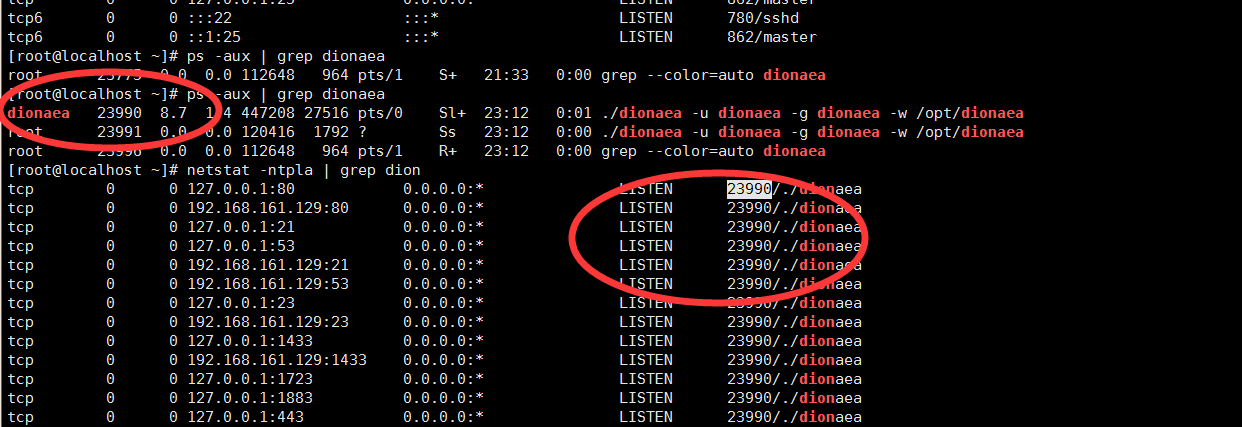
官方文档

<https://dionaea.readthedocs.io/en/latest/index.html>

基本介绍：

安全性：可以使用chroot环境运行。



安装：

没有centos 的安装介绍，使用第三种安装方式

yum install autoconf automake check vim wget curl

sudo yum groupinstall 'Development Tools'

yum install gcc gcc-c++ make openssl-devel

yum install git autoconf\* libtool-\*

sudo yum install libcur\* libxml\* openssl\*

sudo yum install -y epel-release

sudo yum install -y python34 python34-devel python34-PyYAML

# Install pip3

sudo bash -c "curl https://bootstrap.pypa.io/get-pip.py | python3.4"

yum -y install python-pip

pip install Cython

pip3 install Cython

yum install -y glib2-devel libnetfilter\_queue libnetfilter\_queue-devel libnl-devel libpcap-devel libtool udns udns-devel

yum install libev-devel

yum install libssl-dev libudns-dev

yum install loudmouth

git clone https://github.com/buffer/libemu

cd libemu

autoreconf -vi

./configure --prefix=/usr/lib

make

make install

注意：安装目录和include 目录为

--with-emu-lib=/usr/lib/lib --with-emu-include=/usr/lib/include

mkdir /opt/dionaea

cd /opt/dionaea

git clone <https://github.com/DinoTools/dionaea>

cd dionaea/

autoreconf -vi

./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/lib --with-emu-include=/usr/lib/include --with-nl-include=/usr/include/ --with-nl-lib=/usr/lib

make

sudo make install

groupadd dionaea

useradd -g dionaea -s /usr/sbin/nologin dionaea

chown -R dionaea:dionaea /opt/dionaea/

运行选项的意义分别是：

-c：指定运行程序所使用的配置文件，默认下配置文件是/opt/dionaea/etc/dionaea.conf。

-D：后台运行。

-g：指定启动后切换到某个用户组，默认下保持当前组。

-G：收集垃圾数据，用于调试内存泄露。不能用于 valgrind 软件。

-h：帮助信息。

-H：帮助信息，包括默认值信息。

-l：选择事件记录级别，可以选择 all, debug, info, message, warning, critical, error 这些值，多选使用“,”做分隔，排除使用“-”。

-L：选择域，支持通配符“\*”和“?”，多选使用“,”，排除使用“-”。

-u：指定启动后切换到某个用户，默认下保持当前用户。

-p：记录 pid 到指定文件。

-r：指定启动后切换根目录到指定目录，默认下不切换。

-V：显示版本信息。

-w：设定进程工作目录，默认下为/opt/dionaea。

cd /opt/dionaea/bin

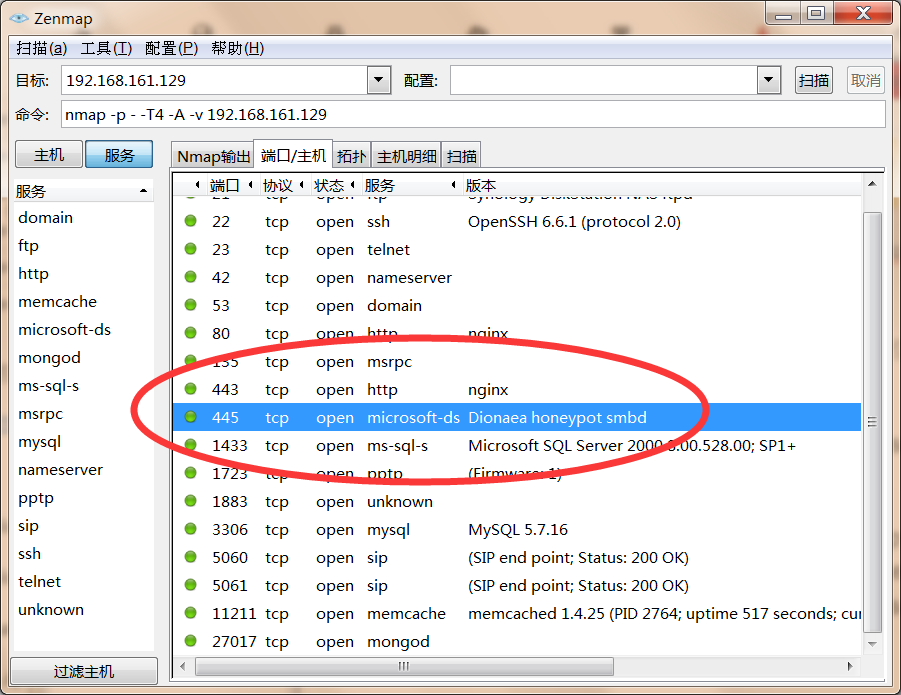
运行测试

./dionaea -l all,-debug -L '\*'

./dionaea -l all,-debug -L 'con\*,py\*'

运行

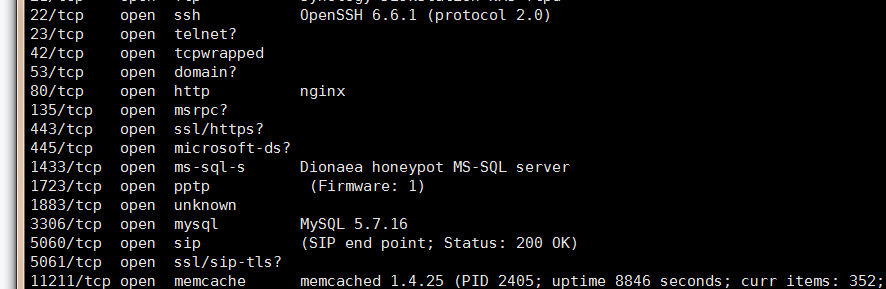
./dionaea -u dionaea -g dionaea -w /opt/dionaea



修改配置文件,变更指纹信息 SMB的445端口指纹: /opt/dionaea/lib/dionaea/python/dionaea/smb/include/smbfields.py 中

MConditionalField(UnicodeNullField("OemDomainName", "WORKGROUP") ConditionalField(UnicodeNullField("ServerName", "HOMEUSER-3AF6FE")

WORKGROUP和HOMEUSER-3AF6FE,变更信息



MSSQL的1433端口指纹: /opt/dionaea/lib/dionaea/python/dionaea/mssql/mssql.py的 r.VersionToken.TokenType = 0x00修改为0xAA

FTP的21端口指纹: /opt/dionaea/lib/dionaea/python/dionaea/ftp.py self.reply(WELCOME\_MSG, "Welcome to the ftp service") 修改为 self.reply(WELCOME\_MSG, "Welcome to the svn service")

配置：主配置文件介绍

主配置文件位置：/opt/dionaea/etc/dionaea/dionaea.cfg

配置项说明：

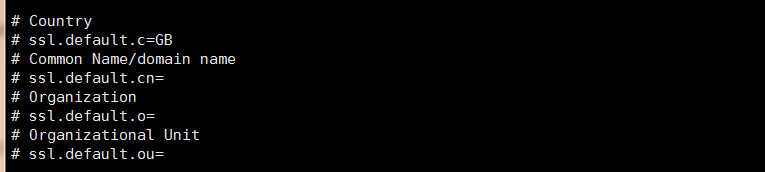
**download.dir：各种蜜罐服务的全局下载目录**

**listen.mode:设置蜜罐绑定的IP以及网卡**

**modules：dionaea加载的模块列表**

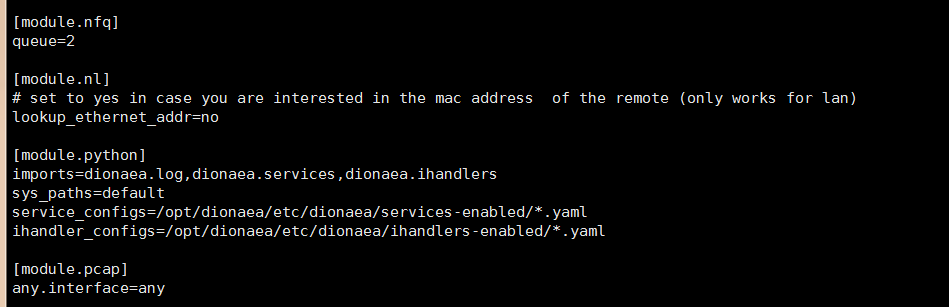
**processors：dionaea使用的处理器列表**

**设置服务器的国家地区**

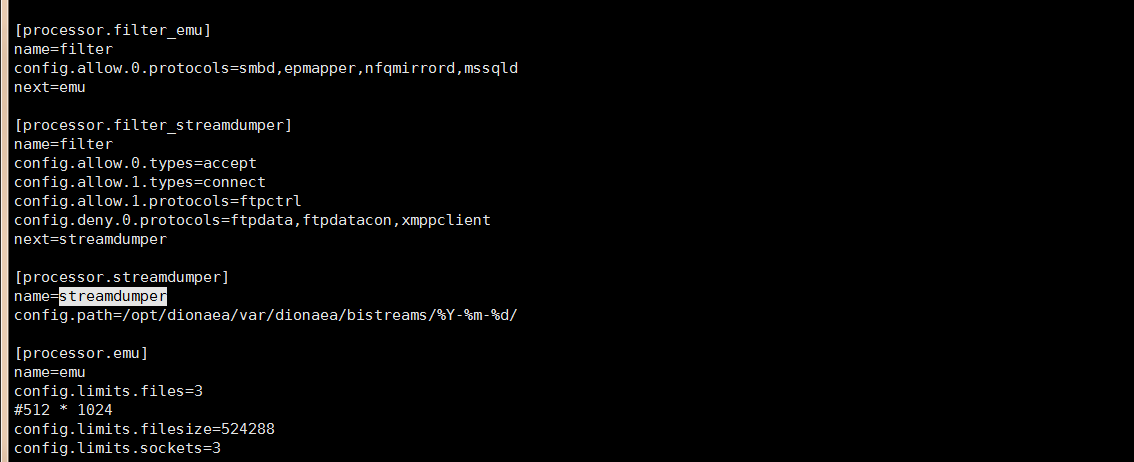


[logging]：日志记录模块。只是用于调试，不建议用来追踪攻击

设置启动时加载的模块



配置处理器以及处理顺序



模块：dionaea的模块curl（处理http），emu（处理shellcoke），pcap（处理连接信息），python（python支持） 及分别作用。

服务：各种服务蜜罐的配制方法

目前支持的协议类型和服务有Black hole，EPMAP，FTP，HTTP，Memache，Mirror，MongoDB，MQTT，MSSQL，MySQL，nfq，PPTP，SMB、tftp、UPnP，SIP(VoIP)，同时还支持IPv6和TLS（Transport Layer Security，传输层安全）。

日志：可选的日志记录方式。并没有分析，还要配合分析软件

支持的方式有：emuprofile、fail2ban、ftp、hpfeeds、log\_db\_sql、log\_incident、log\_json、log\_sqlite、nfq、p0f、store、submit\_http、submit\_http\_post、tftp\_download、VirusTotal

处理器：可选的攻击处理器。默认就好。

依赖包安装的其他方式。注意安装目录跟include目录。此处没有用到

git clone git://git.netfilter.org/libnfnetlink.git

cd libnfnetlink/

./autogen.sh

./configure --prefix=/usr

make

make install

git clone git://git.netfilter.org/libnetfilter\_queue.git

cd libnetfilter\_queue/

./autogen.sh

./configure PKG\_CONFIG\_PATH=/usr/local/lib/pkgconfig

make

make install

git clone <https://github.com/ThomasAdam/liblcfg>

cd liblcfg/code/

autoreconf -vi

./configure --prefix=/opt/dionaea

make install

cd /root

git clone https://github.com/buffer/libemu

cd libemu

autoreconf -vi

./configure --prefix=/opt/dionaea

make install

cd /root

git clone git://anongit.freedesktop.org/libevdev

cd libevdev/

autoreconf -vi

./configure --prefix=/opt/dionaea

make install

可视化：没弄。<http://www.vuln.cn/6165>。在同一台机器上。不好。

   DionaeaFR(https://github.com/RootingPuntoEs/DionaeaFR)是用于前端web展示Dionaea的数据。

https://github.com/rubenespadas/DionaeaFR