

Факультет компьютерных технологий и прикладной математики

Кафедра вычислительных технологий

02.03.02

Информационная безопасность

Лабораторная работа № 9

Тема: Sandbox. Антиспам (ASSP).

Цель работы

Получение теоретических и практических навыков работы с песочницами и файловыми антивирусами. Изучить работу почтового сервера, получить практические навыки работы по защите от спама.

Указания к работе

Вначале студенты изучают теоретическую часть. Далее каждый студент должен выполнить задания, а также ответить на вопросы к лабораторной работе. За проделанную работу студент может получить оценку от «неудовлетворительно» до «отлично». Для получения оценки «удовлетворительно» студент должен выполнить ВСЕ задания к лабораторной работе. Оценка «хорошо» ставится, если студент ответил на ВСЕ вопросы к лабораторной работе. Оценка «отлично» студент получает, если подготовлен отчёт по лабораторной работе.

ОЦЕНКУ ЗА ПРОДЕЛАННУЮ РАБОТУ МОЖНО ПОВЫСИТЬ ДО СДАЧИ СЛЕДУЮЩЕЙ ЛАБОРАТОРНОЙ РАБОТЫ.

Теоретическая часть

Часть 1

Вредоносная программа (англ. malware, malicious software – «злонамеренное программное обеспечение») – любое программное обеспечение, предназначенное для получения несанкционированного доступа к вычислительным ресурсам самой ЭВМ или к информации, хранимой на ЭВМ, с целью несанкционированного использования ресурсов ЭВМ или причинения вреда (нанесения ущерба) владельцу информации, и/или владельцу ЭВМ, и/или владельцу сети ЭВМ путём копирования, искажения,

удаления или подмены информации. Многие антивирусы считают крэки, кейгены и прочие программы для взлома вредоносными программами или потенциально опасными.

Песочница (англ. Sandbox) – это ограниченная среда в вашей системе для исполнения гостевых программ без доступа к главной операционной системе. Это закрытое для доступа извне виртуальное пространство, в котором можно работать с программным обеспечением без изменения системных файлов.

Песочница (от англ. Sandbox, схожие понятия – англ. honeypot, англ. fishbowl) – в компьютерной безопасности механизм для безопасного исполнения программ. Песочницы часто используют для запуска не протестированного кода, непроверенного кода из неизвестных источников, а также для запуска и обнаружения вирусов.

Песочница – в компьютерной безопасности специально выделенная среда для безопасного исполнения компьютерных программ.

Песочница обычно представляет собой жёстко контролируемый набор ресурсов для исполнения гостевой программы – например, место на диске или в памяти. Доступ к сети, возможность сообщаться с главной операционной системой или считывать информацию с устройств ввода обычно либо частично эмулируют, либо сильно ограничивают. Песочницы представляют собой пример виртуализации. Повышенная безопасность исполнения кода в песочнице зачастую связана с большой нагрузкой на систему — именно поэтому некоторые виды песочниц используют только для неотлаженного или подозрительного кода.

Cuckoo Sandbox – система для автоматического исследования вредоносного ПО, эксплоитов, вредоносных скриптов, документов, архивов и ссылок. Система способна проверять документы pdf, doc, xls, rtf, скрипты Python, JS, DLL-библиотеки, бинарники, jar и многое другое.

Файловый Антивирус – компонент модуля «Защита» компьютера, контролирующей файловую систему компьютера. Он запускается при старте

операционной системы, постоянно находится в оперативной памяти компьютера и проверяет все открываемые, сохраняемые и запускаемые файлы. Каждый файл, к которому вы обратитесь, будет перехвачен Файловым Антивирусом и проверен на присутствие известных вирусов.

Clam AntiVirus – пакет антивирусного ПО, работающий во многих операционных системах, включая Unix-подобные ОС, OpenVMS, Microsoft Windows и Apple Mac OS X.

Главная цель Clam AntiVirus – интеграция с серверами электронной почты для проверки файлов, прикрепленных к сообщениям. В пакет входит масштабируемый многопоточный демон clamd, управляемый из командной строки сканер clamscan, а также модуль обновления сигнатур по Интернету freshclam.

Часть 2

Почтовый сервер, сервер электронной почты, мейл-сервер – в системе пересылки электронной почты так обычно называют агент пересылки сообщений (англ. mail transfer agent, MTA). Это компьютерная программа, которая передаёт сообщения от одного компьютера к другому. Обычно почтовый сервер работает «за кулисами», а пользователи имеют дело с другой программой – клиентом электронной почты (англ. mail user agent, MUA).

Спам (англ. spam) – рассылка коммерческой и иной рекламы или подобных коммерческих видов сообщений лицам, не выразившим желания их получать. Также название распространяемых материалов. Распространителей спама называют спамерами.

В общепринятом значении термин «спам» в русском языке впервые стал употребляться применительно к рассылке электронных писем. Незапрошенные сообщения в системах мгновенного обмена сообщениями (например, ICQ) носят название SPIM (англ.) русск. (англ. Spam over IM).

Доля спама в мировом почтовом трафике составляет от 60% (2006) до 80% (2011). Самый большой поток спама распространяется через электронную почту. В настоящее время доля вирусов и спама в общем трафике электронной почты составляет по разным оценкам от 70 до 95 процентов.

Anti-Spam SMTP Proxy (ASSP) – это ПО с открытым исходным текстом, платформонезависимый SMTP прокси-сервер, в котором реализованы белые списки и фильтрация на основании теоремы Байеса.

Антиспамовый сервер собирает письма со спамом и нормальную почту, потом на основании вероятности встречи слов из анализируемого письма в каждой из коллекций (спам или не-спам) сервер делает вывод о том, является ли письмо спамом или нет.

Другие возможности ASSP:

1. Настройка через веб-интерфейс в браузере.
2. Автоматическое ведение белого списка.
3. Наличие необрабатываемых адресов и доменов.
4. Адреса для сбора спама.
5. Поддержка дополнительных регулярных выражений для идентификации спама и не-спама.
6. Обнаружение спама, кодированного MIME.
7. Автоматическое ведение баз спама и нормальной почты.
8. Защита от пересылки почты третьими лицами.
9. Простейший контроль вирусов.
10. Наличие почтового интерфейса для управления и пополнения коллекций спама и нормальной почты.
11. Проверка отправителя по RBL и SPF.

Задания к лабораторной работе

Часть 1

Если будут проблемы с установкой Cuckoo Sandbox, можно установить какую-нибудь альтернативу. Например, Viper, Binary Analysis Next Generation, Mal Tindex и др. <https://linuxsecurity.expert/tools/cuckoo-sandbox/alternatives/>

Установка Cuckoo Sandbox

Если будут проблемы с установкой, воспользуйтесь документацией Cuckoo sandbox <http://docs.cuckoosandbox.org/en/latest/installation/>

Установка зависимостей

```
cd /tmp
sudo apt-get update
$ sudo apt-get install python python-pip python-dev libffi-dev libssl-dev $
sudo apt-get install python-virtualenv python-setuptools $ sudo apt-get install
libjpeg-dev zlib1g-dev swig
$ sudo apt-get install mongodb
$ sudo apt-get install postgresql libpq-dev
$ sudo apt-get install qemu-kvm libvirt-bin ubuntu-vm-builder bridge-utils
python-libvirt
$ sudo pip install XenAPI
sudo apt-get install mariadb-server -y
pip install lxml
pip install cybox==2.0.1.4
pip install maec==4.0.1.0
pip install django
pip install py3compat
pip install pymongo
sudo apt-get install ssdeep python-pyrex subversion libfuzzy-dev -y
pip install pydeep
cd /tmp
wget https://github.com/plusvic/yara/archive/v2.1.0.tar.gz
tar xzf v2.1.0.tar.gz
cd yara-2.1.0
chmod +x build.sh
cd yara-python
python setup.py build
```

```
python setup.py install
cd /tmp
add-apt-repository ppa:pi-rho/security
apt-get update
apt-get install volatility
```

Установка Virtualbox

```
sudo apt install virtualbox
```

Установка Cuckoo Sandbox

```
useradd cuckoo
usermod -a -G vboxusers cuckoo
id cuckoo
cd /opt
wget cd
tar xzf cuckoo_1.1.tar.gz
```

Настройка БД

```
sudo mysql -u root -p
> create database cuckoo;
> grant all privileges on cuckoo.* to cuckoo@localhost identified by
'cuck00pass' ;
> flush privileges;
> quit;
```

Настройка cuckoo

Включаем запись дампа памяти:

```
memory_dump = on
```

Настраиваем подключение к бд:

```
connection = mysql://cuckoo:cuck00pass\@localhost/cuckoo
```

Увеличиваем временные лимиты:

```
default = 240
```

```
critical = 1200
```

```
vm_state = 600
```

* Файл /opt/cuckoo/conf/memory.conf

Отключаем сохранение дампов памяти:

```
delete_memdump = yes
```

* Файл /opt/cuckoo/conf/processing.conf

Включаем анализ оперативной памяти:

```
memory = yes
```

* nano /opt/cuckoo/conf/virtualbox.conf

Меняем режим работы Virtualbox:

```
mode = headless
```

Меняем названия виртуальной машины с cuckoo1 на WindowsXP:

```
machines = WindowsXP
```

```
[WindowsXP]
```

```
label = WindowsXP
```

* Файл /opt/cuckoo/conf/reporting.conf

Включим импорт отчётов в MongoDB для работы веб интерфейса

```
[mongodb]
```

```
enabled = yes
```

На этом настройка Cuckoo закончена, теперь приступим к Virtualbox и гостевой ОС.

Настройка сети

```
vboxmanage hostonlyif create
```

```
vboxmanage modifyvm "WindowsXP" --nic1 hostonly --hostonlyadapter1  
vboxnet0 --nicpromisc1 allow-all --hwvirtex off --vtxvpid off
```

Настройка общих папок

```
mkdir -p /opt/cuckoo/shares/setup
```

```
mkdir -p /opt/cuckoo/shares/WindowsXP
```

```
vboxmanage sharedfolder add "WindowsXP" --name "WindowsXP" --  
hostpath /opt/cuckoo/shares/WindowsXP --automount
```

```
vboxmanage sharedfolder add "WindowsXP" --name setup --hostpath  
/opt/cuckoo/shares/setup --automount --readonly
```

```
vboxmanage modifyvm "WindowsXP" --nictrace1 on --nictracefile1  
/opt/cuckoo/shares/WindowsXP/dump.pcap
```


Включение доступа по RDP

Порт можете указать любой.

```
vboxmanage modifyvm "WindowsXP" --vrdeport 5000 --vrde on
```

На этом конфигурация виртуальных контейнеров полностью закончена, осталось настроить iptables, tcpdump:

```
iptables -A FORWARD -o eth0 -i vboxnet0 -s 192.168.56.0/24 -m conntrack --ctstate NEW -j ACCEPT
```

```
iptables -A FORWARD -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
```

```
iptables -A POSTROUTING -t nat -j MASQUERADE
```

```
sysctl -w net.ipv4.ip_forward=1
```

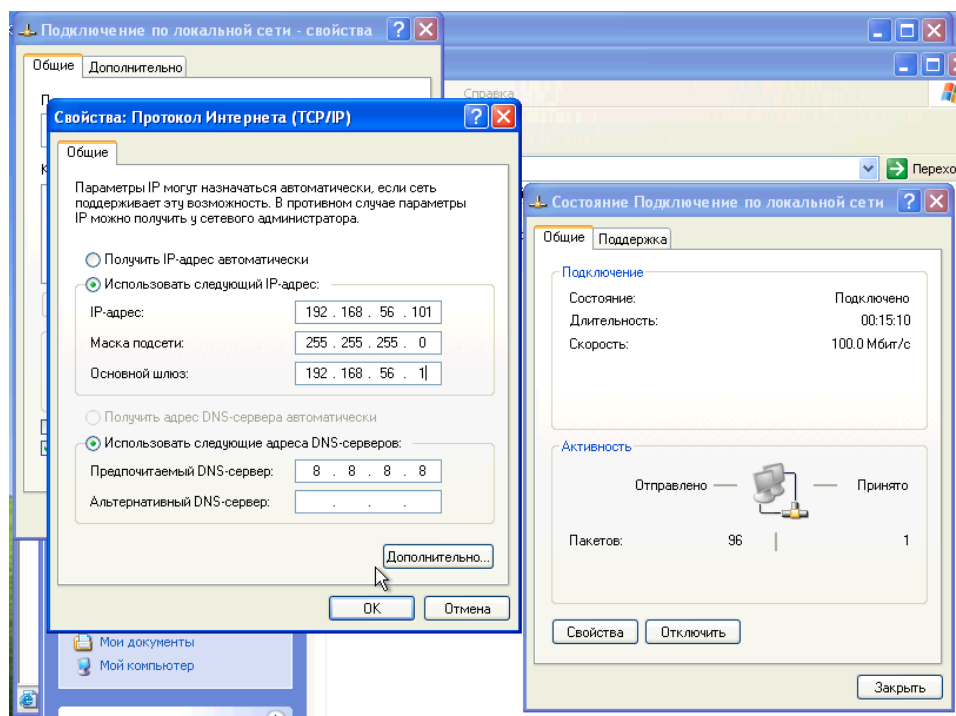
```
setcap cap_net_raw,cap_net_admin=eip /usr/sbin/tcpdump
```

```
getcap /usr/sbin/tcpdump
```

```
ifconfig vboxnet0 192.168.56.1
```

После установки и настройки Windows переходим непосредственно на саму гостевую ОС.

Следующим образом настроим подключение к сети (dns можете указать любой):



Установим VboxTools с диска, который подключен к системе.

Устанавливаем Python 2.7: <http://python.org/download/>.

Устанавливаем <http://www.activestate.com/activepython>.

Устанавливаем PIL Python модуль, для создания скриншотов:
<http://www.pythonware.com/products/pil/>.

Отключаем автоматическое обновление Windows.




Отключаем брандмауэр.

Копируем агент из сетевой папки setup в папку C:\Python27, Ставим агент на автозагрузку, для этого добавляем в ветку реестра (пуск->выполнить->regedit) HKLMSOFTWARE\Microsoft\Windows\CurrentVersion\Run строковый параметр.

Имя: «Agent»

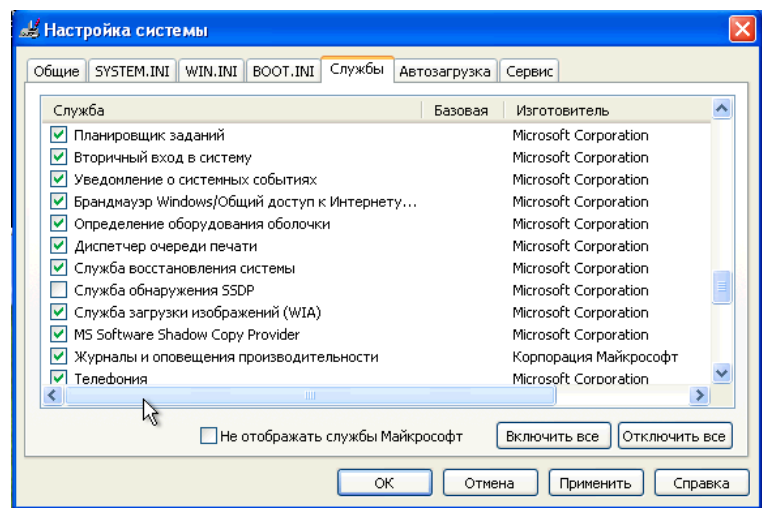
Тип: «REG_SZ»

Содержание: «C:\Python27\agent.pyw»

	(По умолчанию)	REG_SZ	(значение не присвоено)
	VBoxTray	REG_SZ	C:\WINDOWS\system32\VBoxTray.exe
	Agent	REG_SZ	C:\Python27\agent.pyw

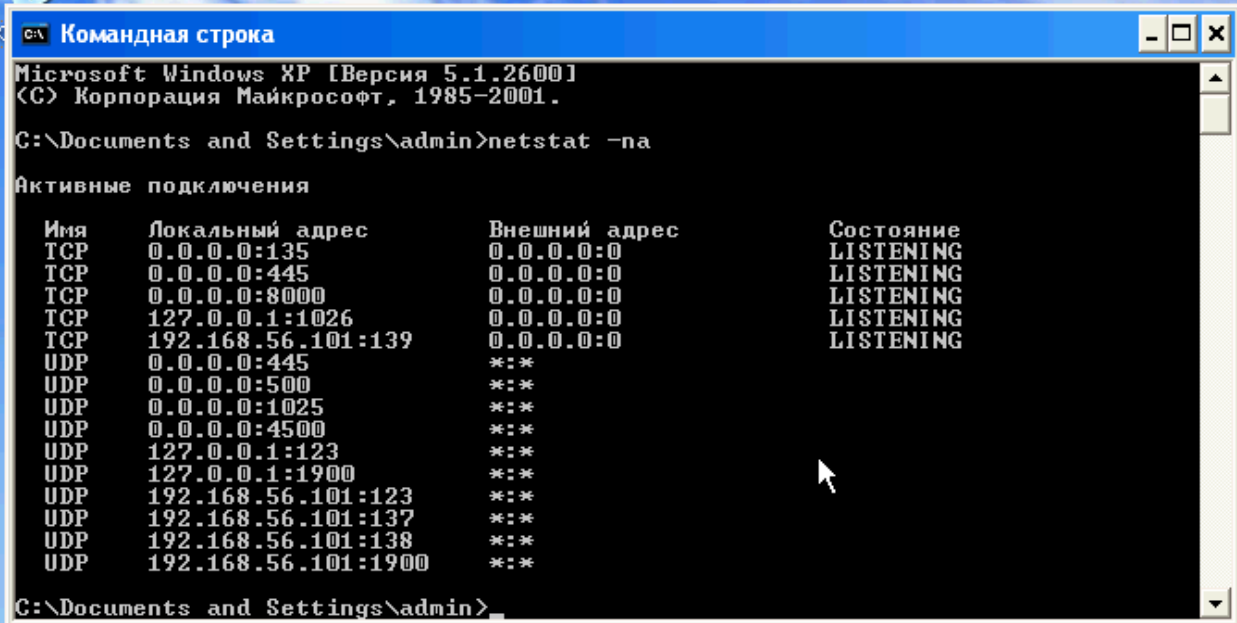
Включаем IE, в настройках ставим домашней страницей пустую вкладку, по желанию в свойствах обозревателя выключаем все защитные механизмы.

Отключаем SSDP: пуск->выполнить->msconfig и в разделе службы отключаем «Служба обнаружения SSDP», чтобы в отчётах не фигурировали сетевые запросы этой службы.



Перезагружаемся и в появившемся при загрузке окне выбираем «При перезагрузке не выводить это сообщение» и ОК.

После перезагрузки гостевой ОС, пуск->выполнить->cmd и в консоли набираем netstat -na и смотрим есть ли агент на 8000-ом порту.



```
Microsoft Windows XP [Версия 5.1.2600]
(C) Корпорация Майкрософт, 1985-2001.

C:\Documents and Settings\admin>netstat -na

Активные подключения

Имя      Локальный адрес      Внешний адрес      Состояние
TCP      0.0.0.0:135           0.0.0.0:0          LISTENING
TCP      0.0.0.0:445           0.0.0.0:0          LISTENING
TCP      0.0.0.0:8000          0.0.0.0:0          LISTENING
TCP      127.0.0.1:1026        0.0.0.0:0          LISTENING
TCP      192.168.56.101:139    0.0.0.0:0          LISTENING
UDP      0.0.0.0:445           ***
UDP      0.0.0.0:500           ***
UDP      0.0.0.0:1025          ***
UDP      0.0.0.0:4500          ***
UDP      127.0.0.1:123         ***
UDP      127.0.0.1:1900        ***
UDP      192.168.56.101:123    ***
UDP      192.168.56.101:137    ***
UDP      192.168.56.101:138    ***
UDP      192.168.56.101:1900   ***

C:\Documents and Settings\admin>
```

По желанию устанавливаем различное уязвимое ПО старых версий (браузеры, Flash player, Java, Acrobat Reader...)

На этом установка гостевой ОС закончена. Делаем снапшот (не выключая гостевую ОС) <vboxmanage snapshot «WindowsXP» take «WindowsXPSnap01» --pause>

И выключаем: <vboxmanage controlvm «WindowsXP» poweroff>

Запуск Cuckoo Sandbox <python cuckoo.py>

Загрузите вредоносное ПО для проверки работы Cuckoo Sandbox. Здесь есть небольшой список ресурсов с образцами вредоносного ПО <https://zeltser.com/malware-sample-sources/>. Например, можете загрузить с <http://malshare.com/>.

Чтобы отправить файл в Cuckoo на анализ используйте команду submit: <python submit.py /path/to/binary>

Запустите web-интерфейс cuckoo и просмотрите результаты <python web.py>

Часть 2

На две виртуальные машины с операционной системой Linux установить почтовый сервер Zimbra Collaboration Server. [На странице загрузки](#) можете посмотреть, какие системы поддерживаются.

Установите зависимости `<sudo apt-get install libgmp10 libperl5.18 unzip
paх sysstat sqlite3 dnsmasq wget libaio1>`

Откройте `<nano /etc/hostname>`. Измените имя хоста на «mail.sit.local»

Узнайте ip-адрес `<ifconfig>`.

Откройте `<sudo nano /etc/hosts>`. Добавьте строку «192.168.1.113 mail.sit.local mail», где 192.168.1.113 ваш ip-адрес.

Откройте `<sudo nano /etc/dnsmasq.conf>` И добавьте туда:

```
server=192.168.1.113
domain=sit.local
mx-host=sit.local, mail.sit.local, 5
mx-host=mail.sit.local, mail.sit.local, 5
listen-address=127.0.0.1
```

Перезагрузите виртуальную машину `<sudo reboot>`

Скачайте Zimbra для своей системы
<https://www.zimbra.com/downloads/zimbra-collaboration-open-source>.

Извлеките архив и перейдите в папку, которую извлекли из архива.

Запустите установку. `<sudo ./install.sh>`

Согласитесь с лицензионным соглашением. Y.

Устанавливайте все пакеты (Выбираете Y), кроме zimbra-dnscache (Выбирайте N, так как уже используем dnsmask).

Когда появится меню введите 6 и нажмите Enter.

Введите 4 и нажмите Enter, введите пароль администратора, минимум 6 символов.

Введите r и нажмите Enter, для возврата в главное меню, затем введите a и нажмите Enter, чтобы принять изменения.

На запросы «Save configuration data to a file» и «The system will be modified - continue?» введите у.

Ждите, пока Zimbra не установится

Чтобы проверить работу, можете ввести <su - zimbra> <zmcontrol status>.

Подключитесь к Zimbra в браузере <https://192.168.1.113/> или к странице администратора <https://192.168.1.113:7071/>.

На одну из виртуальных машин для защиты от спама установите ASSP (Anti-Spam SMTP Proxy Server). <http://sourceforge.net/projects/assp/>. Скачайте и разархивируйте ASSP.

```
sudo apt-get install build-essential pmttools libterm-readline-perl-perl libterm-  
readline-gnu-perl libyaml-perl libtext-glob-perl libnumber-compare-perl libio-  
compress-perl libemail-mime-perl libemail-send-perl libemail-valid-perl libfile-  
readbackwards-perl libwww-perl libmime-types-perl libmail-dkim-perl libmail-spf-  
perl libmail-srs-perl libnet-cidr-lite-perl libnet-dns-perl libnet-ldap-perl libnet-smtp-  
server-perl libthreads-perl libthread-queue-any-perl libtie-dbi-perl libsched-cron-  
perl libio-socket-ssl-perl libdbd-anydata-perl libdbd-csv-perl libdbd-ldap-perl  
libdbd-mock-perl libdbd-odbc-perl libdbd-mysql-perl libfile-find-rule-perl libfile-  
slurp-perl libfile-which-perl libfile-chmod-perl liblinux-usermod-perl libcrypt-rc4-  
perl libtext-pdf-perl libsmart-comments-perl libcam-pdf-perl libpdf-api2-perl  
imagemagick perlmagick poppler-utils xpdf libauthen-sasl-perl libnet-snmp-perl  
libsnmp-base libsnmp-dev libsnmp-perl snmp libsnmp-*perl libsnmpkit-dev  
libregexp-optimizer-perl libnet-smtp-tls-perl liblingua-stem-snowball-perl  
liblingua-identify-perl unzip libberkeleydb-perl
```

```
sudo apt-get install tesseract-ocr tesseract-ocr-*
```

```
sudo apt-get install libmodule-signature-perl libtest-pod-perl libtest-pod-  
coverage-perl libarchive-zip-perl
```

```
sudo apt-get install libssl-dev
```

sudo cpan

[...]

Would you like to configure as much as possible automatically? [yes]

[...]

Would you like me to automatically choose some CPAN mirror sites for you? (This means connecting to the Internet) [yes]

cpan> install Test::Perl::Critic

cpan> install CPAN

cpan> reload cpan

cpan> force install Mail::SPF::Query

cpan> install Net::IP::Match::Regexp Net::SenderBase Net::Syslog
Thread::State Sys::MemInfo Crypt::CBC Crypt::OpenSSL::AES DBD::Log
DBD::MVS_FTPSQL DBD::Multiplex DBD::Ovrimos DBD::PgPP DBD::Sprite
DBD::Template DBD::mysqlPP DBIx::AnyDBD LEOCHARRE::DEBUG
LEOCHARRE::CLI PDF::Burst Image::OCR::Tesseract PDF::GetImages
PDF::OCR PDF::OCR2 Mail::DKIM::Verifier Convert::Scalar Unicode::GCString
Sys::CpuAffinity

cpan> exit

sudo apt-get install clamav clamav-daemon

sudo freshclam

sudo /etc/init.d/clamav-daemon start

sudo apt-get install libfile-scan-perl

sudo cpan

cpan[1]> test File::Scan::ClamAV

cpan[1]> look File::Scan::ClamAV

./cpan/build/File-Scan-ClamAV-1.91-Ik8fWD# make install

./cpan/build/File-Scan-ClamAV-1.91-Ik8fWD# exit

cpan[1]> exit

Скачивание ASSP и его настройка

<http://sourceforge.net/projects/assp/>

unzip ASSP_2.3.3_13137_install.zip

sudo mkdir -p /usr/share/assp

sudo mv -f assp/* /usr/share/assp

```
rm -rf assp ASSP_2.3.3_13137_install.zip Install.txt MacOSX-launchd.txt
quickstart.txt Win32-quickstart-guide.txt

sudo chown -R nobody:nogroup /usr/share/assp
sudo chmod 755 /usr/share/assp/assp.pl
sudo nano /etc/init.d/assp
```

Contents:

====

#!/bin/sh -e

Start or stop ASSP

#

original version by Ivo Schaap <ivo@lineau.nl> had issues on Debian4.

Modified by atramos.

#

BEGIN INIT INFO

Provides: ASSP (Anti-Spam SMTP Proxy)

Required-Start: \$syslog, \$local_fs

Required-Stop: \$syslog, \$local_fs

Default-Start: 2 3 4 5

Default-Stop: 0 1 6

Short-Description: Start ASSP

Description: Enable service provided by daemon.

END INIT INFO

PATH=/bin:/usr/bin:/sbin:/usr/sbin

case "\$1" in

start)

echo -n "Starting the Anti-Spam SMTP Proxy"

cd /usr/share/assp

perl assp.pl 2>&1 > /dev/null &

;;

```
stop)
echo -n "Stopping the Anti-Spam SMTP Proxy"
kill -9 ps ax | grep "perl assp.pl" | grep -v grep | awk '{ print $1 }'
;;
restart)
$0 stop || true
$0 start
;;
``*)``
echo "Usage: /etc/init.d/assp {start|stop|restart}"
exit 1
;;
esac
exit 0
===
```

```
sudo chmod 755 /etc/init.d/assp
```

```
sudo /usr/share/assp/assp.pl
```

Нажмите Ctrl+C

```
sudo update-rc.d assp defaults
```

```
sudo /etc/init.d/assp start
```

Переходим на http://antispam_host:55555

login:root

pass:nospam4me

Через машину без ASSP, отправляйте спам на машину с ASSP. Скриптов для генерации спама в интернете полно, но нужен такой, где можно использовать свой почтовый сервер (Например, можете использовать Social Engineer Toolkit). Посмотрите, как блокируется спам и как система обучается.

Вопросы к лабораторной работе

Часть 1

1. Что такое песочница?

2. Принцип работы песочниц.
3. Где используют песочницы?
4. Преимущества и недостатки песочниц.
5. Альтернативы использованию песочниц.
6. Что такое эмуляция?
7. Что такое эвристический анализ? В чем отличия от сигнатурного анализа?
8. Для чего нужен файловый антивирус?
9. Что такое вредоносное ПО?

Часть 2

1. Что такое почтовый сервер?
2. Принцип работы почтового сервера.
3. Что такое спам?
4. Что такое ASSP?
5. Как работает ASSP?
6. Можно ли полностью защитить почтовый сервер от спама?
7. Какие еще угрозы почтовому серверу существуют?
8. Какие методы защиты почтового сервера существуют?