Программное обеспечение

«Программный комплекс Bot-Trek TDS»

Руководство по установке и эксплуатации

Содержание

1 ОБЩИЕ СВЕДЕНИЯ 3
1.1 Введение 3
1.2 Назначение ПО 3
2 ПРОГРАММНО-АППАРАТНЫЕ СРЕДЫ ФУНКЦИОНИРОВАНИЯ ПО 4
3 КОМПЛЕКТАЦИЯ 5
4 УСТАНОВКА 7
4.1 Предварительная подготовка к установке 7
4.2 Установка Bot-Trek TDS 8
4.2.1 Текст скрипта install.sh 9
4.2.1.1 Установка зависимостей 10
4.2.1.2 Установка Suricata 11
4.2.1.3 Установка tds-registry 14
4.2.1.4 Установка tds-shell 15
4.2.1.5 Установка sensor-api 15
4.2.1.6 Установка web 15
5 НАСТРОЙКА 16
5.1 Настройка интерфейса управления 17
5.1.1 Настройка интерфейса управления по протоколу DHCP 17
5.1.2 Настройка интерфейса управления вручную 18
5.2 Настройка интерфейсов анализа трафика 18
5.3 Создание учетных записей 19
5.4 Настройка NTP серверов 19
6 ПОДДЕРЖАНИЕ ФУНКЦИОНИРОВАНИЯ ПО 20

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Введение

Настоящий документ содержит руководство администратора программного обеспечения «Программный комплекс Bot-Trek TDS» (далее – Bot-Trek TDS, ПО).

1.2 Назначение ПО

Программный комплекс Bot-Trek TDS является средством защиты конфиденциальной информации (системой обнаружения вторжений уровня сети) и предназначен для автоматизированного обнаружения компьютерных атак (вторжений) и вредоносного ПО в сетевом трафике при помощи сигнатурного метода выявления атак и эвристического анализа. Изделие устанавливается на границе сети с целью повышения уровня защищенности ИС, ЦОД, серверов и коммуникационного оборудования, АРМ пользователей.

2 ПРОГРАММНО-АППАРАТНЫЕ СРЕДЫ ФУНКЦИОНИРОВАНИЯ ПО

Изделие функционирует в среде операционной системы специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (версия 1.6) Релиз «Смоленск» на отдельно выделенном сервере СОВ.

Для функционирования подсистемы аудита и базы данных системы обнаружения вторжений используется СУБД PostgreSQL версия 9.6 (входит в состав операционной системы специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (версия 1.6) Релиз «Смоленск»).

Для хранения базы решающих правил используется файловая система ОС «Astra Linux Special Edition».

Для хранения событий, генерируемых сенсором, еще не попавших в базу, используется Redis – сетевое журналируемое хранилище данных типа «ключ - значение» (входит в состав операционной системы специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (версия 1.6) Релиз «Смоленск»).

3 КОМПЛЕКТАЦИЯ

Состав дистрибутива приведен в таблице 1.

Таблица 1

Директория		Описание
TDS_SENSOR:		Корневая директория
–	libhtp	Директория с пакетом библиотеки libhtp для Suricata
–	logrotate	Директория с конфигурационным файлом для ротации логов Suricata
–	requirements	Директория с зависимостями для Python кода
–	suricata	Директория с пакетом Suricata 4.0.4
–	suricatarules	Директория с пакетом сигнатур Suricata
–	tds-api-common	Директория с пакетом REST API продукта
–	tds-registry	Директория с пакетом tds-registry
–	tds-shell	Директория с пакетом консоли управления tds-shell
–	sensor-cert-web	Директория с пакетов веб-интерфейса управления
–	install.sh	Установочный скрипт
–	backup.sh	Скрипт для резервного копирования
–	restore.sh	Скрипт восстановления из бекапа

Список файлов и их описание приведен в таблице 2.

Таблица 2

Файл	Путь	Тип файла	Описание
libhtp2_0.5.26-1_amd64.deb	TDS_SENSOR/libhtp/	Пакет	Зависимость Suricata
suricata	TDS_SENSOR/logrotate/	Текст	Файл конфигурации журналирования Suricata
suricatarules_1.0.13-1199_all.deb	TDS_SENSOR/suricatarules/	Пакет	Пакет разрешающих правил Suricata
suricata_4.0.4-2_amd64.deb	TDS_SENSOR/suricata	Пакет	Пакет системы обнаружения вторжений Suricata
click-6.7-py2.py3-none-any.whl	TDS_SENSOR/requirements/	Пакет	Зависимость Python для sensor-cert-web
Django-2.0.6-py3.5-none-any.whl	TDS_SENSOR/requirements/	Пакет	Зависимость Python для sensor-cert-web

Файл	Путь	Тип файла	Описание
Flask-1.0.2-py2.py3-none-any.whl	TDS_SENSOR/requirements/	Пакет	Зависимость Python для sensor-cert-web
itsdangerous-0.24-py3-none-any.whl	TDS_SENSOR/requirements/	Пакет	Зависимость Python для sensor-cert-web
Jinja2-2.10-py2.py3-none-any.whl	TDS_SENSOR/requirements/	Пакет	Зависимость Python для sensor-cert-web
MarkupSafe-1.0-cp35-cp35m-linux_x86_64.whl	TDS_SENSOR/requirements/	Пакет	Зависимость Python для sensor-cert-web
pythondialog-3.4.1-py3-none-any. whl	TDS_SENSOR/requirements/	Пакет	Зависимость Python для sensor-cert-web
pytz-2018.4-py3-none-any.whl	TDS_SENSOR/requirements/	Пакет	Зависимость Python для sensor-cert-web
terminaltables-3.1.0-py3-none-any. whl	TDS_SENSOR/requirements/	Пакет	Зависимость Python для sensor-cert-web
Werkzeug-0.14.1-py2.py3-none-any.whl	TDS_SENSOR/requirements/	Пакет	Зависимость Python для sensor-cert-web
sensor-api_1.0.20-1_all.deb	TDS_SENSOR/tds-api-common	Пакет	Пакет с REST API
tds-registry_1.1.4-1_all.deb	TDS_SENSOR/tds-registry	Пакет	Пакет с вспомогательной утилитой tds-registry
tds-shell_0.1_all.deb	TDS_SENSOR/tds-shell	Пакет	Пакет с консольным интерфейсом управления
sensor-cert-web_0.1.0_all.deb	TDS_SENSOR/sensor-cert-web	Пакет	Пакет с WEB интерфейсом управления

4 УСТАНОВКА

Для установки компонентов изделия администратор должен обладать навыками работы в системе UNIX/Linux.

Последовательность установки программы приведена ниже:

1) Выполнение предварительной подготовки.
2) Настройка локали; Установка зависимостей.
3) Установка Suricata.
4) Установка tds-registry.
5) Установка tds-shell.
6) Установка sensor-api.
7) Установка web.

4.1 Предварительная подготовка к установке

Установка изделия осуществляется на сервер СОВ с установленной ОС «Astra Linux Special Edition».

Пользователь root создается при установке ОС.

При установке ОС «Astra Linux Special Edition» необходимо задать пароль учетной записи ОС root. Данная учетная запись root используется при установке изделия.

В случае если ОС «Astra Linux Special Edition» не установлена на техническое средство необходимо выполнить следующие действия:

1) Вставить в CD/DVD привод диск с ОС «Astra Linux Special Edition».
2) Скопировать образ ОС «Astra Linux Special Edition» на жесткий диск:

   dd if=/dev/cdrom of=/opt/cd.iso bs=1M
3) Создать папку для монтирования ISO файла установочного диска:

   mkdir /opt/repo
4) Монтировать ISO файл в созданную папку:

mount -o loop /opt/cd.iso /opt/repo

5) Вставить в CD/DVD привод диск разработчиков.

6) Скопировать образ диска разработчиков ОС «Astra Linux Special Edition» на жесткий диск:

   dd if=/dev/cdrom of=/opt/cd-dev.iso bs=1M

7) Создать папку для монтирования ISO файла диска разработчиков:

   mkdir /opt/repo-dev

8) Монтировать ISO файл в созданную папку:

   mount -o loop /opt/cd-dev.iso /opt/repo-dev

9) Указать репозитории в /etc/apt/sources.list:

   deb file:///opt/repo smolensk contrib main non-free

   deb file:///opt/repo-dev smolensk contrib main non-free

10) Обновить репозитории:

    apt-get update

4.2 Установка Bot-Trek TDS

Перед установкой Bot-Trek TDS необходимо:

- проверить правильность подключения клавиатуры и монитора к серверу;
- проверить наличие CD/DVD привода в составе сервера, в случае отсутствия необходимо подключить переносной CD/DVD привод;
- вставить CD-диск с дистрибутивом изделия в CD/DVD привод;
- нажать комбинацию клавиш <Ctrl+Alt+F2> для перехода в консольный режим и ввести имя и пароль пользователя root.

После ввода данных пользователя root будет предоставлен доступ к командной строке ОС.

Установка Bot-Trek TDS выполняется только с помощью установочного скрипта install.sh, который находится в корне дистрибутива Bot-Trek TDS.

Запуск скрипта необходимо осуществлять под пользователем root.

Для установки изделия выполнить следующие действия:

- монтировать CD-диск с дистрибутивом;
- найти на CD-диске с дистрибутивом скрипт install.sh;
- запустить скрипт install.sh;
- В процессе установки появится всплывающее окно с подтверждением установки пакетов. Подтвердить установку.

4.2.1 Текст скрипта install.sh

```
#!/bin/bash #

Create paths

mkdir -p /etc/suricata/gib-rules/

mkdir -p /opt/tds

mkdir -p /var/lib/tds

if [ ! -f /var/lib/tds/registry ]; then

echo -e "{\n \"appliance_type\": \"sensor\"\n}" > /var/lib/tds /registry

fi

# Install requirements for API and Shell

apt-get install -yqq dialog python3-yaml redis-server postgresql-9.6 python3-requests python3-pip python3-psutil python3-psycopg2 python3-redis acl libhiredis0.13 libhyperscan4 libluajit-5.1-2 libnetfilter-log1 libltdl7 libpcap0.8 libgeoip1 libjansson4 libevent-pthreads-2.0-5 libnet1 libnetfilter-queue1 libpython-stdlib libpython2.7-minimal libpython2.7- stdlib python python-minimal python-simplejson python2.7 python2.7-minimal ethtool

# Install libhtp

dpkg -i libhtp/libhtp2_*.deb

# Install Suricata

dpkg -i suricata/suricata_*.deb
```

```
# Install Suricata rules
dpkg -i suricatarules/suricatarules_*.deb
# PyReq
pip3 install wheel --no-deps requirements/*.whl
# Install tds-registry
dpkg -i tds-registry/tds-registry_*.deb
# Install shell
dpkg -i tds-shell/tds-shell_*.deb
# Install Sensor API
dpkg -i tds-api-common/sensor-api_*.deb
# Install Sensor Web interface
dpkg -i sensor-cert-web/*.deb
# Configure logrotate
cp logrotate/* /etc/logrotate.d/
# Add tds user tds
useradd -m -p tds -s /usr/sbin/tds-shell tds
echo "tds ALL=(root) NOPASSWD:/opt/tds/tds-shell/tds_shell.py" >> /etc /sudoers
# Start services
systemctl start sensor-api.service
systemctl start sensor-cert-alerts.service
systemctl start sensor-cert-web.service
systemctl enable sensor-api.service
systemctl enable sensor-cert-alerts.service
systemctl enable sensor-cert-web.service
```

Примечание. Скрипт install.sh выполняет действия, описанные ниже.

4.2.1.1 Установка зависимостей

1) Прописание локалей

sudo echo -e 'LANGUAGE=en_US.UTF-8\nLC_ALL=en_US.

UTF-8\nLANG=en_US. UTF-8\nLC_TYPE=en_US.UTF-8\n' >> /etc/default/locale

sudo locale-gen en_US.UTF-8

sudo dpkg-reconfigure -f noninteractive locale

2) Установка зависимостей (системных пакетов) из состава ОС «Astra Linux Special Edition»:

sudo apt-get -yqq install postgresql-9.6 python3-redis python3-psutil python3-psycopg2 python3-yaml python3-virtualenv python3-pip python3- requests acl dialog libltdl7 geoip-database libgeoip1 libhiredis0.13 libhyperscan4 libluajit-5.1-2 libluajit-5.1-common libnetfilter-log1 libpcap0.8 ethtool redis-server libjansson4

3) Установка зависимостей (внешних пакетов) с CD-диска с дистрибутивом. Установку зависимостей необходимо проводить в следующем порядке:

python3 -m pip install requirements/build/pytz-2018.4-py3-none-any. whl

python3 -m pip install requirements/build/pythondialog-3.4.1-py3-noneany.whl

python3 -m pip install requirements/build/terminaltables-3.1.0-py3- none-any.whl

python3 -m pip install requirements/build/Werkzeug-0.14.1-py2.py3- none-any.whl

python3 -m pip install requirements/build/MarkupSafe-1.0-cp35-cp35mlinux_x86_64.whl

python3 -m pip install requirements/build/click-6.7-py2.py3-none-any. whl

python3 -m pip install requirements/build/itsdangerous-0.24-py3-noneany.whl

python3 -m pip install requirements/build/Jinja2-2.10-py2.py3-noneany.whl

python3 -m pip install requirements/build/Flask-1.0.2-py2.py3-noneany.whl

python3 -m pip install requirements/build/Django-2.0.6-py3-none-any. whl

4.2.1.2 Установка Suricata

1) Установить зависимости Suricata:

dpkg -i libhtp/libhtp2_0.5.26-1_amd64.deb

2) Установить Suricata:

dpkg -i suricata/suricata_4.0.4-2_amd64.deb

3) Установить правила Suricata:

dpkg -i suricatarules/suricatarules_1.0.13-1199_all.deb

4) Настроить ротацию логов для Suricata путем создания файла suricata в директории /etc/logrotate.d/ и добавлению в него следующих настроек:

```
/var/log/suricata/http.log
{
        daily
        missingok
        rotate 14
        compress
        delaycompress
        notifempty
        create 640 root adm
        sharedscripts
        postrotate
                /bin/kill -HUP $(cat /var/run/suricata.pid)
        endscript
}
/var/log/suricata/stats.log
{
        daily
        missingok
        rotate 14
        compress
        delaycompress
        notifempty
        create 640 root adm
        sharedscripts
        postrotate
                /bin/kill -HUP $(cat /var/run/suricata.pid)
```

```
endscript
}
/var/log/suricata/fast.log
{
        daily
        missingok
        rotate 14
        compress
        delaycompress
        notifempty
        create 640 root adm
        sharedscripts
        postrotate
                /bin/kill -HUP $(cat /var/run/suricata.pid)
        endscript
}
/var/log/unified_purge.log
{
        daily
        rotate 12
        missingok
        compress
}
/var/log/suricata/eve.json
{
        monthly
        rotate 6
        missingok
```

compress

delaycompress

notifempty

create 640 root adm

sharedscripts

postrotate

/bin/kill -HUP $(cat /var/run/suricata.pid)

endscript

}

/var/log/suricata/stats.json

{

daily

missingok

rotate 14

compress

delaycompress

notifempty

create 640 root adm

sharedscripts

postrotate

/bin/kill -HUP $(cat /var/run/suricata.pid)

endscript }

4.2.1.3 Установка tds-registry

1) Установить tds-registry:

   dpkg -i tds-registry/tds-registry_1.1.4-1_all.deb

2) Создать конфигурационный файл для registry:

   echo -e "{\n \"appliance_type\": \"sensor\"\n}" > /var/lib/tds /registry

4.2.1.4 Установка tds-shell

1) Установить пакет tds-shell:

   dpkg -i tds-shell/tds-shell_0.1_all.deb

2) Создать пользователя tds:

   useradd -m -p tds -s /usr/sbin/tds-shell tds echo "tds ALL=(root)
   NOPASSWD:/opt/tds/tds-shell/tds_shell.py" >> /etc /sudoers

4.2.1.5 Установка sensor-api

Установить пакет tds-api-common:

   dpkg -i tds-api-common/sensor-api_1.0.20-1_all.deb

4.2.1.6 Установка web

Установить пакет sensor-cert-web:

   dpkg -i sensor-cert-web/sensor-cert-web_0.1.0_all.deb # sensor_db, postgres, admin.

5 НАСТРОЙКА

Для настройки, проверки и восстановления работоспособности изделия используется текстовая консоль, предоставляющая доступ к возможностям диагностики и настройки изделия.

Чтобы войти в текстовую консоль с сервера СОВ необходимо нажать на клавиатуре комбинацию клавиш «Ctrl+Alt+F2».

С правами root ввести команду:

su – tds

на экране появится запрос на ввод имени и пароля пользователя (имя и пароль пользователя по умолчанию tds/tds). После чего будет произведен вход в командную среду пользователя tds (Пользователь tds создается на этапе установки изделия).

Чтобы войти в текстовую консоль удаленно с АРМ администратора необходимо ввести IP-адрес изделия, полученный в ходе настройки изделия, в терминальный клиент. В ответ на запрос ввести имя и пароль пользователя (имя и пароль пользователя по умолчанию tds/tds).

Настройка изделия состоит из следующих действий:

1) Настройка интерфейса управления.
2) Настройка интерфейсов анализа трафика.
3) Создание учетных записей.
4) Настройка NTP серверов.

Перед настройкой настоятельно рекомендуется изменить пароль для служебной учетной записи, используемой для взаимодействия функциональных компонентов СОВ с базой данных, устанавливаемый по умолчанию. Для этого необходимо выполнить следующие действия:

- если уже был произведен вход в текстовую консоль, то необходимо выйти из нее;
- войти в операционную систему с правами root выполнив команду:

  sudo su

- изменить пароль в конфигурационном файле для пользователя ADMIN в поле PASSWORD выполнив команду:

  nano sensor-web-cert/configs/registry

- изменить пароль в базе данных выполнив команду:

  sudo -u admin psql sensor_db

- после чего откроется консоль PostgeSQL;

- ввести:

  ALTER USER admin WITH PASSWORD “новый пароль”

- выйти из консоли PostgeSQL нажатием комбинации клавиш <Ctrl+Z>.

5.1 Настройка интерфейса управления

Существует два варианта настройки интерфейса управления:

1) По протоколу DHCP.

2) Вручную.

5.1.1 Настройка интерфейса управления по протоколу DHCP

1) Войти в текстовую консоль под пользователем tds (Пользователь tds создается на этапе установки изделия).

2) В стартовом окне текстовой консоли выбрать <Enter the shell>

3) Изменить пароль пользователя tds в соответствии с правилами формирования паролей, для чего в окне «Choose one of the options:» выбрать «Change password»

4) Подтвердить смену пароля нажатием <Yes>

В ответ на запрос системы ввести старый пароль и дважды ввести новый пароль.

В случае если пароль не соответствует политике безопасности программа выдаст предупреждение о невозможности смены пароля.

5) Выбрать «Network menu» (сетевое меню)

6) Выбрать «Configure network» (Настройка сети) и нажать «Ок»

7) Подтвердить выбор, нажав кнопку «Yes»

8) В всплывающем окне «Choose IP address configuration» (Выбрать конфигурацию IP-адреса) выбрать DHCP

5.1.2 Настройка интерфейса управления вручную

1) Войти под пользователем tds (Пользователь tds создается на этапе установки изделия).

2) В стартовом окне текстовой консоли выбрать <Enter the shell>

3) Выбрать «Network menu»

4) Выбрать «Configure network» и нажать «Ок»

5) Подтвердить выбор, нажав кнопку «Да»

6) Выбрать «Static»

7) Ввести IP-адрес интерфейса и нажать «ОК»

8) Ввести маску подсети

9) Ввести адрес шлюза

10) Выбрать адреса DNS по умолчанию (8.8.8.8 и 8.8.8.4) или ввести их вручную.

11) (Опционально) Ввести DNS сервера (если в п.10 выбрали вручную)

5.2 Настройка интерфейсов анализа трафика

1) Войти под пользователем tds (Пользователь tds создается на этапе установки).

2) В стартовом окне выбрать <Enter the shell>

3) Выбрать «Network menu»

4) Выбрать «Traffic monitor setup»

5) Выбрать интерфейсы, на которых будет осуществляться мониторинг

6) Нажать «ОК».

5.3 Создание учетных записей

1) Войти в графический интерфейс программы с ролью Администратор безопасности.

2) Логин и пароль по умолчанию: admin /tdsadmin.

3) Изменить пароль для администратора безопасности

4) Создать учетную запись аудитора (просмотр событий внутреннего аудита)

5) Создать учетную запись пользователя

5.4 Настройка NTP серверов

1) Войти в графический интерфейс программы.

2) Перейти в меню «Настройки приложения»

3) Настроить NTP сервер

6 ПОДДЕРЖАНИЕ ФУНКЦИОНИРОВАНИЯ ПО

Поддержание функционирования ПО состоит в контроле действия настроек, произведенных в рамках встраивания ПО. Иных регламентных мероприятий со стороны администратора заказчика ПО не требует.