ООО «Стратегия Защиты»

ПРОГРАММНЫЙ МОДУЛЬ
Система предупреждения кибератак «Сонар-1М»
Шифр: СПК «Сонар-1М»

Руководство системного администратора

2018

АННОТАЦИЯ

Настоящий документ - руководство для системного администратора программного комплекса СПК «Сонар-1М». Документ описывает процесс установки, настройки и запуска СПК «Сонар-1М». Для осуществления действий, описанных в данном руководстве, системный администратор должен иметь знания в области UNIX-подобных операционных систем, а также обладать навыками работы в TCP/IP - сетях, иметь общие представления о модели OSI, а также стеке протоколов TCP/IP.

Документ состоит из следующих частей:

- раздел «Назначение программы». Здесь указаны сведения о назначении программы и информация, достаточная для понимания функций программы и ее эксплуатации
- раздел «Условия выполнения программы». Здесь указаны условия, необходимые для выполнения программы (минимальный состав аппаратных и программных средств и т.п.).
- раздел «Установка программы». Здесь приведены последовательности действий системного администратора для установки, настройки программного комплекса.
- раздел «Вызов и загрузка программы». Здесь указаны действия для выполнения запуска, останова и перезагрузки программного комплекса.
- раздел «Администрирование программы». Здесь описаны действия по выполнению типовых задач входящий в обязанности администратора СПК «Сонар-1М».

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

1.1 Назначение

Программный комплекс SONAR-Framework предназначен для выполнения анализа трафика в режиме «реального времени», выявление уязвимостей, связанных с ошибками в конфигурациях системного программного обеспечения и сетевого оборудования, которые могут быть использованы нарушителем для реализации атак на систему и компрометации защищаемых данных.

1.2 Функциональные возможности

Функционал СПК «СОНАР-1М» включает в себя:

- инспектирование входящего и исходящего сетевого трафика;
- анализ входящего и исходящего трафика по сигнатурам, сравнение сигнатур с набором правил (политик), имеющихся в составе модуля. При соответствии сигнатур осуществляется запись в журнал отчета, фиксируя следующие поля:
  - дата и время события (инцидента);
  - краткая идентификация сигнатуры;
  - ip-адрес и порт отправителя;
  - ip-адрес и порт получателя;
  - данные (при их наличии).
- при обнаружении вредоносных сигнатур, атак и прочих аномалий модуль осуществляет распределение событий по срабатыванию, видам атак, сигнатурам, типам событий и собирает статистику по инцидентам;
- формирование отчетов о произошедших событиях и инцидентах.

В составе СПК «СОНАР-1М» присутствует Web-интерфейс управления организующий следующие действия:

- мониторинг за инцидентами, произошедшими в контролируемой системе или сети;
- наблюдение за атаками с распределением по видам атак;
- отображение диаграмм по ip-адресам, портам и событиям;
- геолокацию атак;
- сводную информацию по событиям за текущий день или за выбранный период;

- вывод отчетов по событиям за текущий день или за выбранный период;
- подсчет обнаруженных событий, выводит информаци по наиболее часто встречающимся сигнатурам, самым частым атакующим и атакуемым ip-адресам.

1.3 Функциональные ограничения

Для выполнения анализа трафика требуется подключение сервера СПК «СОНАР-1М» к порту, работающему в режиме зеркалирования трафика (SPAN порту), поскольку программный комплекс выполняет пассивное сканирование уязвимостей удаленных подсетей и устройств.

По результатам проводимого анализа зарегистрированные инциденты безопасности помещаются в базу данных и хранятся локально. Необходимый объем устройств хранения информации зависит от интенсивности трафика и требований по времени хранения событий. Рекомендуется выделять объем исходя из расчета – 500Мб в неделю при регистрации 100 событий ежедневно.

Развернутый программный комплекс занимает до 4 Гб дискового пространства.

2. УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ

2.1 Требования к техническим средствам

2.1.1 Минимальные системные требования (нерекомендуемые):

- Сервер с процессором Intel Atom 1.6 Ггц;
- 1 Гб ОЗУ;
- 20 Гб свободного места на жестком диске ПЗУ;
- 1 ethernet-карта.

2.1.2 Оптимальные (рекомендуемые) системные требования:

- Сервер, с процессором Intel Xeon 2 ГГц;
- 4 Гб ОЗУ;
- 300 Гб свободного места на жестком диске, желательно, распределение отдельного диска или раздела для /SONAR, /var;
- 2 ethernet-карты с поддержкой pf_ring.

2.2 Требования к программным средствам

SONAR-Framework включает несколько готовых программных пакетов, подготовленных для работы с операционной системой CentOS 6.9. Для корректного функционирования комплекса в системе должны быть установлены следующие компоненты:

- mysql-server-5.1.73
- php-5.3.3
- libpcap-1.4.0
- apache-2.2.15

Примечание: версии программных компонентов должны быть не ниже указанных.

3. УСТАНОВКА ПРОГРАММЫ

3.1 Установка операционной системы CentOS 6.9, настройка системного окружения Вход в web-интерфейс

Установить операционную систему (ОС) CentOS 6.9 с компакт диска, следуя всем инструкциям. В процессе необходимо настроить имя компьютера, сетевые интерфейсы, установить минимальный набор пакетов ОС, создать пароль для системного администратора (root), а также создать системного пользователя и также задать ему пароль.

Далее, загрузиться в ОС, ввести логин: root , и его пароль. На всякий случай отключить правила SELINUX, для этого закомментировать все строки, а затем добавить строчку SELINUX=disabled в файле /etc/selinux/config, затем, перезагрузиться и вновь зарегистрироваться в системе от имени пользователя root. Далее, желательно, обновить систему до актуальной версии пакетов, выполнив команды:

```
yum list updates

yum update -y
```

Процесс обновления может занять продолжительное время. Затем, необходимо подключить репозиторий epel, выполнив команду:

```
yum install -y epel-release
```

3.2 Установка пакетов, необходимых для работы СПК «СОНАР-1М». Все пакеты ставятся при помощи менеджера пакетов yum (который подтягивает все необходимые зависимости) и rpm.

3.2.1 Установка MySQL-сервер:

```
yum install -y mysql-server
```

3.2.2 Установить следующие пакеты :

```
yum install -y libnet libpcap tcllib tcl-mysqltcl tclx tcpdump daq libcap-ng dkms libyaml wget
```

3.2.3 Установить пакет tcpflow:

```
cd /etc/yum.repos.d/
```

```
wget https://forensics.cert.org/cert-forensics-tools-release-el6.rpm

rpm -Uvh cert-forensics-tools-release*rpm

yum --enablerepo=forensics install tcpflow
```

3.2.4 Установить пакет P0f:

```
wget ftp.tu-chemnitz.de/pub/linux/dag/redhat/el6/en/x86_64/rpmforge/RPMS/p0f-2.0.8-1.el6.rf.x86_64.rpm

rpm -ihv  p0f-2.0.8-1.el6.rf.x86_64.rpm
```

3.2.5 Установить пакеты pf_ring:

```
cd /etc/yum.repos.d/

wget http://packages.ntop.org/centos/ntop.repo -O ntop.repo

rpm -ivh https://dl.fedoraproject.org/pub/epel/epel-release-latest-6.noarch.rpm

wget https://copr.fedoraproject.org/coprs/saltstack/zeromq4/repo/epel-6/saltstack-zeromq4-epel-6.repo

rpm -ivh http://packages.ntop.org/rpm6/extra/hiredis-0.10.1-3.el6.x86_64.rpm http://packages.ntop.org/rpm6/extra/hiredis-devel-0.10.1-3.el6.x86_64.rpm

yum install -y pfring pfring-dkms pciutils
```

3.3 Установка и настройка дистрибутива СПК «СОНАР-1М».

3.3.1 Копирование дистрибутива.

Скопировать дистрибутив СПК «СОНАР-1М». Дистрибутив файлов СПК «СОНАР-1М» скопировать по сети или с любого носителя в каталог /root/sonar, затем сделать этот каталог текущим и выполнить дальнейшие действия:

```
mkdir -p /root/sonar
```

```
cp -v <носитель_с_дистрибутивом_СПК «СОНАР-1М»> /root/sonar/

cd /root/sonar
```

3.3.2 Установка пакета СПК «СОНАР-1М»: система обнаружения вторжений:

```
rpm -ihv sonar-ids*.rpm
```

3.3.3 Установка пакета СПК «СОНАР-1М»: сенсор:

```
rpm -ihv --force sonar-tcl*.rpm

rpm -ihv sonar-sensor*.rpm

rpm -ihv sonar-barnyard2*.rpm
```

3.4 Настройка СУБД MySQL для работы с СПК «СОНАР-1М»

– Запустить сервис mysql:

```
/etc/init.d/mysqld start
```

– Создать новый пароль для пользователя root mysql-сервера:

```
/usr/bin/mysqladmin -u root password 'sonar12345678'
```

– Если после выполнения прядущего пункта возникает ошибка:

```
mysqladmin: connect to server at 'localhost' failed
```

то следует выполнить сбор пароля администратора базы данных. Для этого нужно перезапустить MySQL-сервер в safe-режиме с опцией --skip-grant-tables:

```
/etc/init.d/mysqld stop

mysqld_safe  --skip-grant-tables --user=root &
```

– Подключиться к серверу MySQL пользователем root без пароля

```
mysql  -u root

use mysql;
```

```
update user set authentication_string=password("sonar12345678") where User='root';

flush privileges;

quit
```

– Далее необходимо выйти из режима safe и перезапустить сервер MySQL в обычном режиме.

```
killall -9 mysqld_safe mysqld

chown mysql /var/lib/mysql/mysql.sock.lock

/etc/init.d/mysqld start
```

– Создать базу данных для СПК «СОНАР-1М»:

```
mysql -u root -p mysql

    <ввести пароль root-а для MySQL>

mysql> CREATE USER 'sguil'@'localhost' IDENTIFIED BY 'sonar12345678';

mysql> GRANT ALL PRIVILEGES ON sguildb.* TO 'sguil'@'localhost' IDENTIFIED BY "sonar12345678";

mysql> GRANT FILE ON *.* to 'sguil'@'localhost' IDENTIFIED BY "sonar12345678";

mysql> FLUSH PRIVILEGES;

mysql>exit

mysql -u sguil -p -e "CREATE DATABASE sguildb"

<ввести пароль sonar12345678>

mysql -u sguil -p -D sguildb < /usr/local/share/doc/sql_scripts/create_sguildb.sql

<ввести пароль sonar12345678>
```

3.4.1 Установка Web-интерфейса СПК «СОНАР-1М»:

– Установка web-сервера apache2:

```
yum install -y httpd
```

– Запуск процесса httpd и внесение в автозапуск:

```
/etc/init.d/httpd start

chkconfig httpd on
```

– Разрешить доступ на Web-сервер (можно не делать, так как это действие выполняется автоматически при установке sonar-web-пакета):

```
service iptables stop && chkconfig iptables off
```

– Установка php5:

```
yum install -y php-mysql
```

– Установка поддержки https:

```
yum install -y mod_ssl

mkdir /etc/ssl/private

chmod 700 /etc/ssl/private

openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout
/etc/ssl/private/apache-selfsigned.key                    -out
/etc/ssl/certs/apache-selfsigned.crt
```

– Далее ввести:

```
Country Name (2 letter code) [XX]:RU

Locality Name (eg, city) [Default City]:SPb

Organization Name (eg, company) [Default Company Ltd]:RNB

Organizational Unit Name (eg, section) []:IT

Common Name (eg, your name or your server's hostname) []:

Email Address []:
```

Далее выполнить команду:

```
openssl dhparam -out /etc/ssl/certs/dhparam.pem 2048
```

Подождать, пока сгенерируются ключи.

– Настройка php: в файле /etc/php.ini расскоментировать строчку и установить временную зону

```
date.timezone = Europe/Moscow
```

– Установка пакета СПК «СОНАР-1М»: web-интерфейс

```
rpm -ihv sonar-web*.rpm
```

3.5 Установка пакета СПК «СОНАР-1М» защиты дистрибутива sonar-ossec:

```
rpm -ihv sonar-ossec*.rpm
```

Необходимо прописать в файл /SONAR/ossec/etc/ossec.conf в раздел <global> ip-адреса АРМ администраторов с которых будет осуществляться работа с СПК «СОНАР-1М» и ip-адреса DNS-серверов. Пример раздела:

```
<global>
  <white_list>127.0.0.1</white_list>
  <white_list>::1</white_list>
  <white_list>^localhost.localdomain$</white_list>
  <white_list>172.16.1.3</white_list>
  <white_list>192.168.10.170</white_list>
</global>
```

Для редактирования файла:

```
vi /SONAR/ossec/etc/ossec.conf
```

3.5.1 Установка SONAR-framework, окончательная настройка и запуск:

```
rpm -ihv sonar-framework*.rpm
Добавить в файл /etc/my.cnf строчки:
group_concat_max_len = 100000
sql-mode=""
```

В файле /etc/httpd/conf/httpd.conf требуется задать ip-адрес СПК «СОНАР-1М» в переменной ServerName. Пример:

```
ServerName 172.16.1.135:80
```

Создать вспомогательные таблицы ip2c и mappings

```
cd /var/www/html/sonar/.scripts
cat squert.sql | mysql -u root -p -U sguildb -h localhost
<ввести пароль sonar12345678>
```

Заполнить таблицу ip2c из бекапа

```
gunzip < bak_ip2c_06072017.sql.gz | mysql -u sguil -p sguildb

<ввести пароль sonar12345678>
```

Инициализировать таблицу ip2c

```
/usr/bin/php -e /var/www/html/sonar/.inc/ip2c.php 0
```

Примечание: При необходимости обновить таблицу ip2c из интернета и потом сделать бэкап. Могут быть проблемы с кодировками.

```
tclsh ip2c.tcl

mysqldump -u sguil -p sguildb ip2c | gzip > /root/bak_ip2c_06072017.sql.gz
```

3.5.2 Перезапуск СПК «СОНАР-1М»:

```
/etc/init.d/sonar restart
```

3.5.3 Добавление пользователя - системного администратора СПК «СОНАР-1М»:

Ввести команду:

```
tclsh /SONAR/sbin/sonar_user_ctl.tcl -adduser admin

Please enter a passwd for admin:

Retype passwd:

User 'admin' added successfully
```

Добавить пользователя admin , пароль: Sonar12345678

4. ВЫЗОВ И ЗАГРУЗКА ПРОГРАММЫ

4.1 Управление службой СПК «СОНАР-1М»

Программный комплекс SONAR-Framework состоит из нескольких компонентов, взаимодействующих друг с другом, сведенных в одну серверную службу. Запуск службы выполняется автоматически при старте операционной системы.

Команда запуска службы SONAR -Framework

```
service sonar start
```

Команда останова службы SONAR -Framework

```
service sonar stop
```

Команда перезапуска службы SONAR -Framework

```
service sonar restart
```

Просмотр состояния службы SONAR -Framework

```
service sonar status
```

4.2 Запуск web-интерфейса СПК «СОНАР-1М»

Запустить web-интерфейс в браузере, введя адрес или доменное имя хоста и строчку запуска SONAR: https://<адрес_или_доменное_имя_хоста>/sonar/p-login.php, согласиться и принять сертификат, затем зайти в интерфейс СПК «СОНАР-1М», используя имя пользователя admin (см. Рисунок.1.)

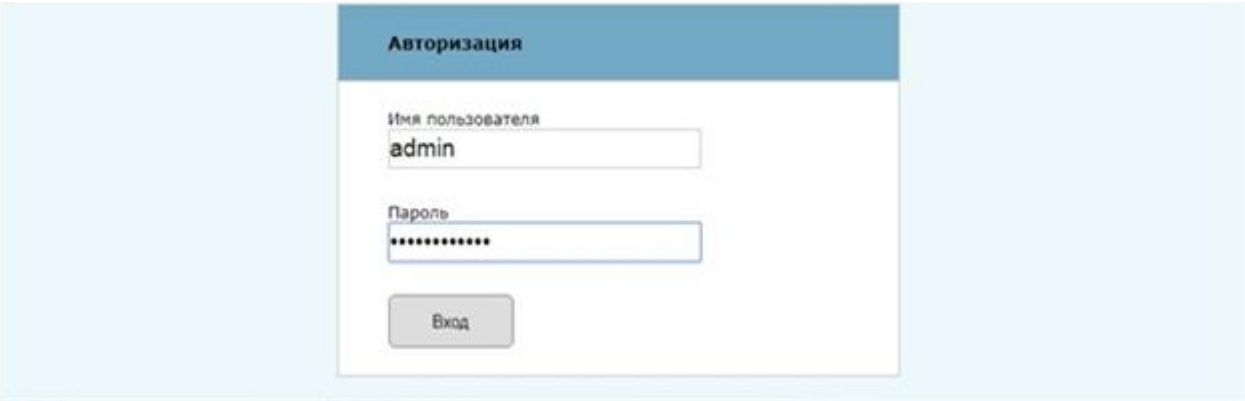

Рисунок.1. Web-интерфейс СПК «СОНАР-1М»

Дальнейшие действия описаны в руководстве оператора.

5. АДМИНИСТРИРОВАНИЕ ПРОГРАММЫ

5.1 Управление пользователями СПК «СОНАР-1М»

Управление пользователями web-интерфейса СПК «СОНАР-1М» выполняется посредством программы sonar_user_ctl.tcl.

Команда просмотра созданных пользователей:

```
sonar_user_ctl.tcl –u
```

Команда добавления нового пользователя:

```
sonar_user_ctl.tcl -adduser <username>
```

где вместо <username> нужно ввести имя нового пользователя

Команда удаления существующего пользователя:

```
sonar_user_ctl.tcl -deluser <username>
```

где вместо <username> нужно ввести имя удаляемого пользователя

Команда изменения пароля пользователя:

```
sonar_user_ctl.tcl –changepasswd <username>
```

где вместо <username> нужно ввести имя пользователя для которого нужно выполнить изменение пароля на новый.

Управления пользователями операционной системы CentOS 6.9 выполняется посредством стандартных утилит adduser, deluser, chattr.

5.2 Управление модулем собственной защиты

Управление модулем собственной защиты выполняется через файл /SONAR/ossec/etc/ossec.conf.

Для изменения уровня регистрируемых модулей событий необходимо в разделе <alerts> установить параметр <log_alert_level> числом от 1 до 16. Пример раздела:

```
<alerts>
     <log_alert_level>1</log_alert_level>
</alerts>
```

После внесения изменений требуется выполнить перезагрузку модуля СПК «СОНАР-1М»:

```
service sonar restart
```

5.3 Управление правилами анализа трафика

Файлы с правилами системы обнаружения вторжений расположены в директории / SONAR /conf/suricata/rules. Для подключения и отключения правил расположенных в данной директории необходимо отредактировать файл / SONAR /conf/suricata/suricata.yaml в разделе rule-files.

Для подключения нового правила следует добавить его название в раздел:

```
:rule-files:
     - botcc.rules
     - ciarmy.rules
     - new_rule.rules
```

Для отключения правила следует закомментировать его название в разделе:

```
:rule-files:
     - botcc.rules
#    - ciarmy.rules
     - new_rule.rules
```