УДК 004.056.53

Анализ уязвимостей системных компонент маршрутизаторов и обнаружение атак на них

Е.А. Орехов, Д.В. Прокопенко, А.Е. Романенков, А.П. Цанда
Московский физико-технический институт (государственный университет)

Защита от угроз является приоритетной задачей администрирования сети. Особое внимание в решении данной задачи следует уделять сетевому оборудованию. К примеру, в случае получения доступа к роутеру, у злоумышленника появляется идеальный инструмент для достижения следующих целей:

- мониторинг сети
- кража данных
- организация атак на прочие устройства.

Возможными методами компрометации маршрутизаторов являются изменение их конфигураций, либо модификация или подмена образов систем. В последнее время участились случаи подобных атак. Этому свидетельствует официальное предостережение Cisco, ведущего вендора сетевого оборудования, выложенное на официальном сайте компании 11 августа 2015 года. В нем говорится о нескольких прецедентах подмены операционных систем маршрутизаторов. Причем, как заявляется, во всех случаях доступ к устройствам был получен с использованием действующих учетных записей, обладающих правами администратора. Одной из зафиксированных атак, ставшей причиной данного обращения, является SYNful Knock. Этот способ компрометации роутера использует имплантат – модифицированный образ Cisco IOS, позволяющий загружать различные функциональные модули из сети Интернет и устанавливать удаленный доступ к устройству.

Cisco поставляет встроенное решение предназначенное для верификации образа операционной системы. Оно основано на сравнении хеш-сумм анализируемого и эталонного образов. Однако, подобный имплантат, внедряясь в систему, способен имитировать ожидаемую реакцию на некоторые системные команды с целью усложнения анализа. По этой причине, мы считаем, что существует более действенный метод проверки целостности системы.

В основе нашего решения лежит более глубокое исследование различных системных компонент. Детальному анализу подвергаются следующие объекты: образ межсетевой оперативной системы, конфигурационные файлы, энергонезависимая и оперативная память.

Файл IOS подвергается побитовому сравнению с изначально хранящимся на доверенном сервере эталоном для подтверждения его консистентности. Данный способ верификации позволяет охватить больший диапазон возможных атак, чем сравнение значений хеш-функций. Это связано с вышеозначенной способностью некоторых модифицированных образов мимикрировать под легитимную систему.

Конфигурационные файлы в свою очередь сравниваются с версиями, уже прошедшими проверку и сохраненными на сервер. Таким образом обеспечивается защита от несанкционированных изменений конфигураций.

Энергонезависимая память также нуждается в проверке. Это связано с тем, что злоумышленник может записывать в неё необходимые для усложнения анализа, устойчивые к перезапуску файлы. Так, например, в энергонезависимой памяти может находиться инфицированный образ системы, который в ответ на верификационный запрос будет выдавать расположенную здесь же валидную версию. В подобных случаях следует сравнить объем свободного места в памяти с расчётным.

Анализ дампа оперативной памяти является наиболее трудоемкой и плохо поддающейся масштабированию задачей. Это связано с различными вариантами его построения у разных

производителей. Возможным вариантом решения данной проблемы является использование антивирусного ПО, которое производит поиск вредоносных сигнатур.

Таким образом, разработанная модель позволяет произвести глубокий и достоверный анализ возможных атак на сетевое оборудование, связанных с подменой или каким-либо несанкционированным изменением системных файлов.

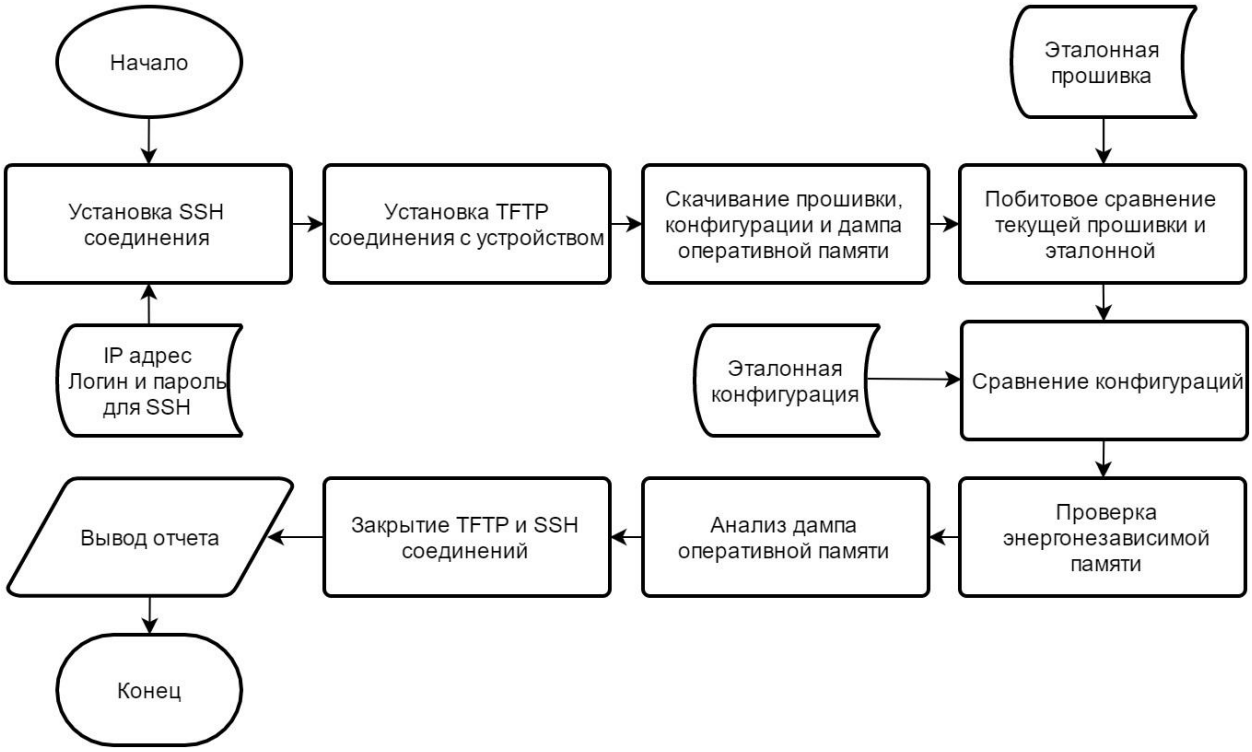

Рис. 1 Блок-схема алгоритма работы предлагаемого решения

Литература

1. *Zettler K.* NSA Laughs at PCs, Prefers Hacking Routers and Switches. // Wired, 2013
2. *Hau B., Lee T., Homan J.* A CISCO IMPLANT SYNful Knock. // San Jose, 2015
3. *Cisco.* Cisco IOS Software Integrity Assurance.