МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Политехнический институт Факультет приборостроения, информационных технологий и электроники	Кафедра «Информационная безопасность систем и технологий»
Специальность 10.05.02 –	Информационная безопасность телекоммуникационных систем
Специализация —	Разработка защищенных телекоммуникационных систем

ДИПЛОМНАЯ РАБОТА

на тему

МОДЕЛЬ ВЫСОКОИНТЕРАКТИВНОЙ СИСТЕМЫ, ПРЕДНАЗНАЧЕННОЙ ДЛЯ ИССЛЕДОВАНИЯ ПОВЕДЕНИЯ ЗЛОУМЫШЛЕННИКА ВО ВСТРАИВАЕМЫХ УСТРОЙСТВАХ

Студент _____ Губарева Валерия Алексеевна

Руководитель _____ Д.С. Евдокимов

Нормоконтролёр _____ А.Г. Фатеев

Рецензент руководитель проектов ООО «Диджитал Секьюрити»

_____ Б.В. Рютин

Работа допущена к защите (протокол заседания кафедры от _____ № _____)

Заведующий кафедрой _____ С.Л. Зефиров

Работа защищена с отметкой _____ (протокол заседания ГЭК от _____ № ____)

Секретарь ГЭК _____ А.Г. Фатеев

Пенза 2018

Оглавление

Введение.....4
1 Высокоинтерактивные системы, предназначенные для исследования поведения злоумышленника во встраиваемых системах.....6
1.1 Общие сведения о высокоинтерактивных системах, предназначенных для исследования поведения злоумышленника во встраиваемых системах6
1.2 Примеры существующих высокоинтерактивных систем, предназначенных для встраиваемых устройств.....12
1.3 Способы обнаружения высокоинтерактивных систем злоумышленниками.....16
1.4 Проблемы, присущие высокоинтерактивным системам.....20
1.5 Сбор сведений о злоумышленнике высокоинтерактивной системой...24
1.6 Собираемые высокоинтерактивной системой сведения.....27
1.7 Составление представления о нарушителе на основе собираемой высокоинтерактивной системой информации.....34
1.8 Оценка ущерба для системы, нанесенного действиями злоумышленника.....35
2 Встраиваемые устройства.....36
2.1 Общие сведения о встраиваемых устройствах.....36
2.2 Уязвимости во встраиваемых устройствах, влияющие на их защищенность.....37
2.3 Последствия атак на встраиваемые устройства.....41
3 Модель высокоинтерактивной системы, предназначенной для исследования поведения злоумышленника во встраиваемых устройствах.....43
3.1 Требования к модели высокоинтерактивной системы, предназначенной для исследования поведения злоумышленника во встраиваемых устройствах.....43
3.2 Модель высокоинтерактивной системы, предназначенной для исследования поведения злоумышленника встраиваемых устройствах.…43

3.3. Применение модели высокоинтерактивной системы для встраиваемых устройств.....45
3.4 Анализ результатов применения модели высокоинтерактивной системы для встраиваемых устройств.....46
3.5 Рекомендации по разработке высокоинтерактивных систем для встраиваемых устройств.....49
4 Вредные психофизиологические факторы, влияющие на сердечно-сосудистую систему специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие.....52
4.1 Вредные психофизиологические факторы, влияющие на сердечно-сосудистую систему специалиста по защите информации.....52
4.2 Методы и средства физической культуры, снижающие их воздействие 53
Заключение.....57
Список используемых источников.....58
Приложение А Алгоритм работы высокоинтерактивной системы для встраиваемых устройств.....60
Приложение Б Схема вторжения злоумышленника в высокоинтерактивную систему.....62
Приложение В Поведение злоумышленника в высокоинтерактивной системе. .64
Приложение Г Реагирование высокоинтерактивной системы на действия злоумышленника.....66
Приложение Д Акт о внедрении.....68
Приложение Е Протокол проверки ВКР в системе Антиплагиат.....70

Введение

В настоящее время в обществе возрастает роль информационной сферы, наравне с этим возрастает необходимость защиты информации и весьма актуальным является вопрос кибер-безопасности. Тот факт, что кибератаки представляют собой настоящую угрозу, подтверждается статистическими данными. Для защиты информационных систем и их пользователей крайне важно собирать точную информацию о вредоносных действиях злоумышленников.

Одним из способов защиты является использование высокоинтерактивных систем, являющихся своего рода приманками для злоумышленников и позволяющих обнаруживать атаки, противодействовать им и собирать статистически данные мотивах и возможностях атакующего. Владение сведениями о возможностях злоумышленника позволяет создавать средства для предотвращения атак на реальную информационную систему.

Актуальность данной темы заключается в том, что существующие на данный момент высокоинтерактивные системы для встраиваемых устройств достаточно просты для злоумышленников. Поэтому есть необходимость в разработке более усовершенствованных систем, использование которых способно предотвращать проникновение злоумышленников в реальные системы. Для этого будет создана модель высокоинтерактивной системы, позволяющая до создания реальной системы отладить механизмы предотвращения атак и сбора информации о злоумышленнике.

Целью данной выпускной квалификационной работы является исследование существующих реализаций высокоинтерактивных систем для встраиваемых устройств, уязвимостей во встраиваемых устройствах и разработка на их модели высокоинтерактивной системы, предназначенной для исследования поведения злоумышленника во встраиваемых устройствах.

Для достижения цели выпускной квалификационной работы были поставлены следующие задачи:

В ВКР должны быть рассмотрены следующие вопросы:

– обзор существующих реализаций высокоинтерактивных систем, предназначенных для исследования поведения злоумышленника во встраиваемых устройствах;

– проблемы, присущие высокоинтерактивным системам;

– способы обнаружения высокоинтерактивных систем злоумышленником;

– составление модели нарушителя на основании данных об атакующем злоумышленнике;

– составление рекомендаций по разработке модели высокоинтерактивной системы, предназначенной для исследования поведения злоумышленника во встраиваемых устройствах;

– составление модели высокоинтерактивной системы, предназначенной для исследования поведения злоумышленника во встраиваемых устройствах;

– результаты применения модели высокоинтерактивной системы, предназначенной для исследования поведения злоумышленника во встраиваемых устройствах.

1 Высокоинтерактивные системы, предназначенные для исследования поведения злоумышленника во встраиваемых системах

1.1 Общие сведения о высокоинтерактивных системах, предназначенных для исследования поведения злоумышленника во встраиваемых системах

Эффективное администрирование сетевой безопасности в значительной степени зависит от понимания существующих угроз в сети Интернет. Для защиты информационных систем и их пользователей крайне важно собирать точную, о действиях злоумышленников. Тот факт, что кибератаки представляют собой настоящую угрозу, подтверждается практически ежедневно появляющимися сообщениями о взломе и заражении каких-либо устройств и появлении ботнетов, состоящих из тысяч зараженных устройств. Обнаружение огромного количества уязвимостей и их широкое распространение привлекают общественное внимание к их безопасности. Зачастую злоумышленники эксплуатируют уязвимости раньше, чем производители успевают создавать и распространять исправления. Использования только на традиционных линий защиты, таких как системы обнаружения вторжений и брандмауэры, недостаточно для целостного охвата про обнаружении новых моделей атак.

Высокоинтерактивные системы (в данном контексте для краткости будет использоваться термин honeypot, но следует помнить, что существуют также низкоинтерактивные honeypot-ы) — это компьютерные ресурсы (виртуальные или физические машины), предназначенные для эмуляции слабостей безопасности и уязвимостей информационной системы, целью которых является своевременное обнаружение атак, противодействие злоумышленникам, сбор информации о их мотивах и возможностях и отвлечение злоумышленника от реальных систем. Их основная задача — исследовать угрозы, с которыми могут столкнуться организации, например, какие инструменты они используют злоумышленники для атака на системы, какими ресурсами владеют, какие преследуют цели.

Собираемая honeypot-ами информация позволяет получить представление о возможностях и ресурсах злоумышленника, а также облегчает процесс генерации сигнатур для систем обнаружения (предотвращения) вторжений. Привлечение внимания злоумышленника к встраиваемой система осуществляется за счет имитации различных уязвимостей, при этом производится сокрытие реальной структуры защищаемой системы и ее ресурсов, навязывание ему ложной информации за счет эмуляции несуществующих сетевых сегментов, серверов, рабочих станций, их уязвимостей и передаваемого трафика.

Возможности высокоинтерактивных систем практически безграничны, что делает их чрезвычайно мощным оружием. Поэтому очевидно, что использование такого мощного инструмента ставит под угрозу реальную систему, в которой расположена высокоинтерактивная. Это возможно потому что скомпрометировав высокоинтерактивную систему злоумышленник может проникнуть в реальную. Значительный объем работы должен быть направлен на смягчение этих рисков.

Чаще всего высокопоставленные приманки размещаются в контролируемой среде, например, за межсетевым экраном. Возможность контролировать атакующего происходит не от самой высокоинтерактивной системы, а от устройства контроля доступа к сети — во многих случаях это межсетевой экран. Использование межсетевого экрана дает злоумышленнику доступ только к honeypot-ам, находящимся за ним, но он не позволяет злоумышленнику использовать honeypot для запуска атак. Такая архитектура очень сложна для развертывания и поддержки, особенно если стоит задача не дать понять злоумышленнику, что он находится не в реальной системе.

Функции высокоинтерактивных систем:

– сбор и контроль данных («прослушивание» сетевого трафика и ведение журналов для последующего анализа);

– обнаружение атак;

– выявление источника атаки;

– идентификация злоумышленника и информации о нем (IP-адрес или IP-префикс, протокол передачи данных, порт, страна, User agent, операционная система);

– определение цели атаки;

– контроль действий злоумышленника;

– реагирование на действия злоумышленника, в том числе блокирование его активности;

– введение злоумышленника в заблуждение путем скрытия или подмены информации, по которой он может понять, что атакует не реальную систему, а honeypot, а также путем изменения конфигурации системы;

– обеспечение возможности взаимодействия администратора с высокоинтерактивной системой [1].

Высокоинтерактивные системы для встраиваемых устройств являются частным случаем высокоинтерактивных систем.

Многие организации, чья деятельность направлена на противодействие злоумышленникам, используют высокоинтерактивные системы для сбора информации об атаках и на основе этого создают средства защиты. Примером сбора высокоинтерактивными системами для встраиваемых устройств может служить исследование Лаборатории Касперского, на основании которого было собрано множество статистических данных по ботнетах, атакующих встраиваемые устройства. Например, распределение обращений злоумышленников к встраиваемым устройствам по портам (протоколов Telnet и SSH), географическое распределение зараженных устройств, географическое распределение IP-адресов серверов, с которых загружается вредоносное ПО на устройства [2].

Высокоинтерактивные системы не защищены от ложно-позитивных и ложно-негативных срабатываний. Любые сигнатуры, которые вызывают ложно-позитивные срабатывания, должны быть полностью или полностью изменены. Это призвано уменьшить количество ложных срабатываний, что сделает

процесс обнаружения и оповещения более эффективным. Однако есть еще одна проблема: путем изменения и устранения большого количества сигнатур есть шанс добиться обратного результата — большое количество ложно-негативных срабатываний. Риск ложно-негативных ошибок состоит в том, что может произойти успешная атака, но системы ее не обнаружат и не предупредят об активности.

Многие высокоинтерактивные системы, независимо от того, основаны ли они на подписях, проверке протокола или какой-либо другой методологии, потенциально могут пропустить новые или неизвестные атаки.

Высокоинтерактивная система работает непрерывно и в случае обнаружения любой активности начинает записывать в журнал мониторинга все происходящие события. Далее проводится анализ всех записанных высокоинтерактивной системой данных. Выделяются возможные ложные срабатывания. Затем на основе уже собранной информации с использованием сторонних программ и утилит можно определить больше информации о злоумышленнике. Например, по IP -адресу или User Agent-у определить страну из которой злоумышленником была произведена атака. При этом стоит отметить тот факт, что злоумышленники обычно стараются не раскрывать информацию о себе подменяя ее или маскируя.

Алгоритм работы высокоинтерактивной системы приведен в приложении А на рисунке А.1.

На данной схеме изображена реальная система, одним из компонентов которой является камера видеонаблюдения. В операционную систему, прошивку или приложения на этой камере были искусственно внедрены уязвимости, которые могут эксплуатироваться злоумышленником, а также средства обнаружения проникновений и утилиты для логирования действий злоумышленника в системе.

Схема вторжения злоумышленника в высокоинтерактивную систему приведена в приложении Б на рисунке Б.1.

После получения доступа к операционной системе или прошивке устройства злоумышленник будет собирать информацию об операционной системе и окружении, искать какие приложения установлены, прослушивать трафик. Это можно отнести к пассивной атаке. К активным действиям относится: загрузка утилит, вредоносного ПО, руткитов и бекдоров; повышение привилегий пользователя; попытки изменения конфигурации системы; эксплуатация имеющихся в системе уязвимостей. После злоумышленник может попытаться скрыть следы своего присутствия в системе, но это тоже обнаруживается высокоинтерактивными системами.

Схема поведения злоумышленника в высокоинтерактивной системе приведена в приложении В на рисунке В.1.

Для предотвращения последствий сбора злоумышленником информации о системе при разработке honeypot-а следует маскировать или подменять артефакты системы в которой он установлен, а также скрывать файлы и приложения. Помимо этого можно создавать файлы и устанавливать приложения, наличие которых может навести злоумышленника на мысль о том, что это реально используемое устройство.

Подмена сетевого трафика заключается в том, что исходящие и входящие пакеты заменяются пакеты, по содержимому которых злоумышленник может решить, что находится в реальной система.

Схема реагирования высокоинтерактивной системы на действия злоумышленника приведена в приложении Г на рисунке Г.1.

Высокоинтерактивные системы могут быть расположены:

– в локальной сети. Такие высокоинтерактивные системы собирают информацию об атаках на ресурсы внутри сети;

– в демилитаризованной зоне. В таком случае, высокоинтерактивная система будет собирать информацию об атаках на общедоступные ресурсы, такие как, например, веб-сервер.

Вероятность ложных срабатываний высокоинтерактивной системы, расположенной в демилитаризованной зоне выше, так как обычные пользователи могут случайно проникнуть в нее.

Достоинства высокоинтерактивных систем:

– идея высокоинтерактивных систем лежит в том, что совершать действия в них будут только злоумышленники, благодаря этому частота ложных срабатываний сведена к минимуму;

– требуют минимальных затрат ресурсов;

– имеют простой принцип действия — при обнаружении любой активности в системе необходимо отслеживать происходящее и реагировать на эти действия должным образом, так как обычно их конфигурируют таким образом, чтобы случайный пользователь не мог попасть в высокоинтерактивную систему;

– не перегружаются трафиком и не имеют проблем с исчерпанием вычислительных ресурсов;

– могут работать с зашифрованным трафиком или в сети, функционирующей по протоколу IPv6, так как не имеет значения, какая информация поступает на вход высокоинтерактивной системы, она в любом случае будет обнаружена и зафиксирована;

– не требуют больших вычислительных мощностей, поэтому для их размещения могут использоваться практически любые устаревшие встраиваемые устройства.

Недостатки высокоинтерактивных систем:

– имеют ограниченную область применения, так как могут отслеживать только деятельность, которая непосредственно направлена на них;

– применение honeypot-ов обуславливает риск полной компрометации реальной системы, частью которой они являются, также они могут использоваться злоумышленниками для атак на другие компьютерные системы;

– возможные сложности с «маскированием» высокоинтерактивной системы — злоумышленник может понять, что он находится не в реальной системе, и попытаться обмануть honeypot. Например, если злоумышленник идентифицировал использование высокоинтерактивной системы, то он может атаковать ее от имени реального компьютера целевой системы. Высокоинтерактивная система обнаружит эту атаку и ошибочно оповестит администратора о том, что обнаружена подозрительная активность, порождая цепочку разбирательств, ведущих по ложному следу, а в это время злоумышленник сможет сосредоточить свои силы на атаке реальной системы, что может повлечь за собой серьезные последствия [1];

– необходимость постоянной доработки высокоинтерактивной системы вследствие того, что она рано или поздно будет изучена злоумышленниками, а также в силу того, что возможности злоумышленников непрерывно растут.

1.2 Примеры существующих высокоинтерактивных систем, предназначенных для встраиваемых устройств

Высокоинтерактивная система HoneyThing — это honeypot для IoT устройств. Он был разработан как маршрутизатор с встроенным веб-сервером RomPager и поддерживает протокол TR-069. Службы TR-069 и HTTP работают на разных портах в одной системе, а также существует поддержка протокола Telnet. Служба Telnet (работающая на 23 порту, например) может быть добавлена в систему при необходимости. Это позволяет злоумышленнику получить доступ к shell-у и дает возможность эмулировать некоторые команды оболочки, что может вызвать критичные для системы последствия [3].

Honeypot для роутеров эмулирует бекдор «TCP-32764», найденный в роутерах в 2013 году. Этот бекдор позволял злоумышленнику отправлять команды уязвимым маршрутизаторам на 32764-й TCP-порт с помощью командной строки с учетной записи администратора без прохождения аутентификации [4].

Telnet IoT honeypot является сервером Telnet, реализованным на языке Python. Действует по принципу работы вредоносного программного обеспечения для IoT устройств, собирает статистику IoT ботнетов, беспрепятственно распространяющихся по протоколам Telnet из-за слабых паролей. Данный honeypot работает со всем версиями протокола Telnet. Система имеет архитектуру клиент/сервер. Клиентом фактически является сама высокоинтерактивная система, принимающая соединения по протоколу Telnet, затем данные отправляются на сервер для последующего анализа [5].

Пример результатов работы высокоинтерактивной системы Telnet IoT honeypot приведен на рисунке 1.

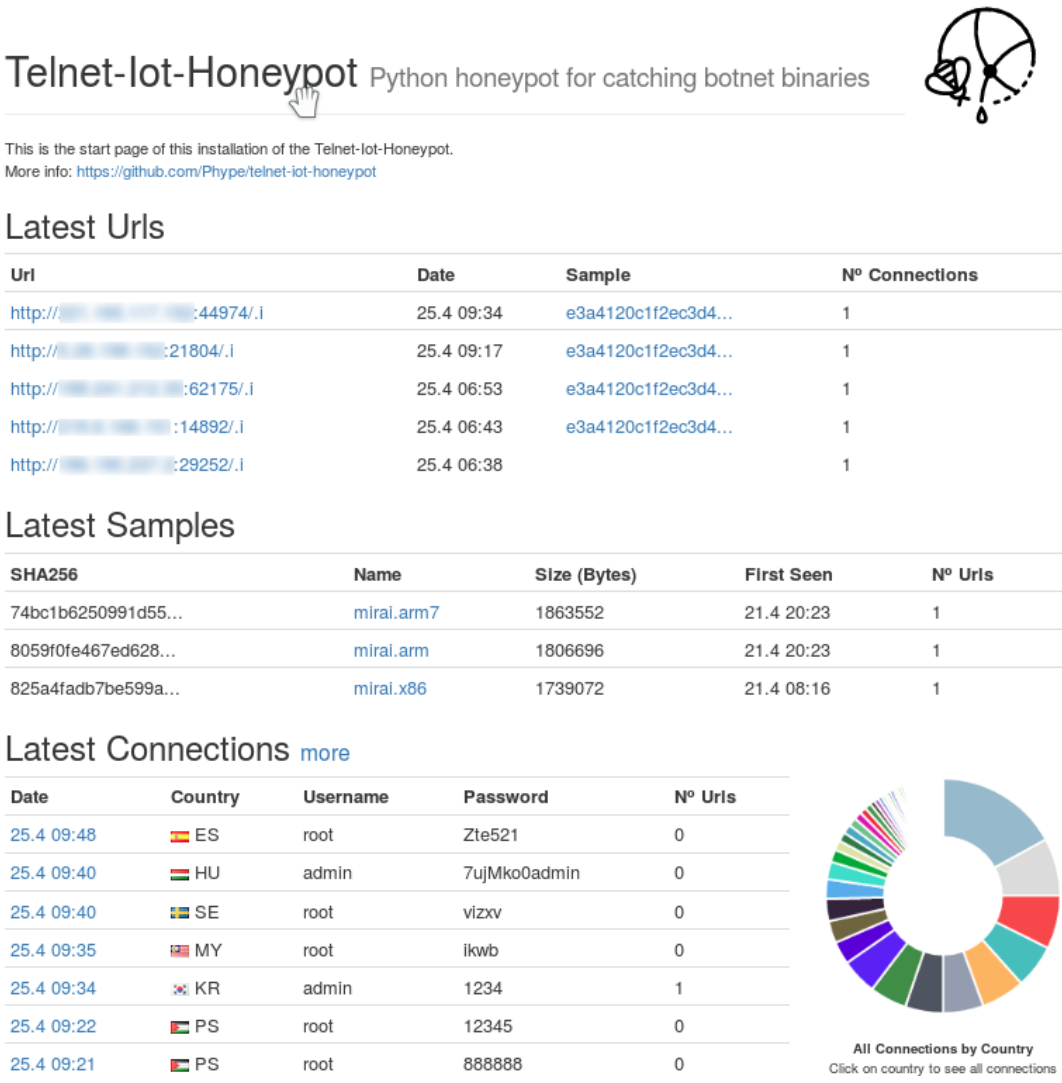

Рисунок 1 — Результаты работы высокоинтерактивной системы Telnet IoT honeypot

Honeypot NodeJS является одним из видов URI для ботов, предназначенных для атак. Функционирует подобно SQL-инъекциям, а именно обслуживает часто запрашиваемые ресурсы и адаптируется к новым эксплойтам путем динамического создания новых ресурсов. Доступна опция сохранения бинарных файлов для их последующего анализа. Кроме того, если эта опция включена, она запускает веб-сервер на 40298 порту для отображения состояния honeypot-а и полученных им данных, которые впоследствии будут проанализированы специалистами [6].

IoT Honeypot — высокоинтерактивная система для IoT устройств. Предназначен для работы с атаками на протокол Telnet, по которому взаимодействуют различные IoT устройства, работающие на разных архитектурах процессора, таких как ARM, MIPS и PPC. Эта высокоинтерактивная система располагается между атакующим злоумышленником и операционной системой Openwrt, используемой для эмуляции служб Telnet для IoT устройств [7].

Результаты работы IoT Honeypot-а приведены на рисунке 2.

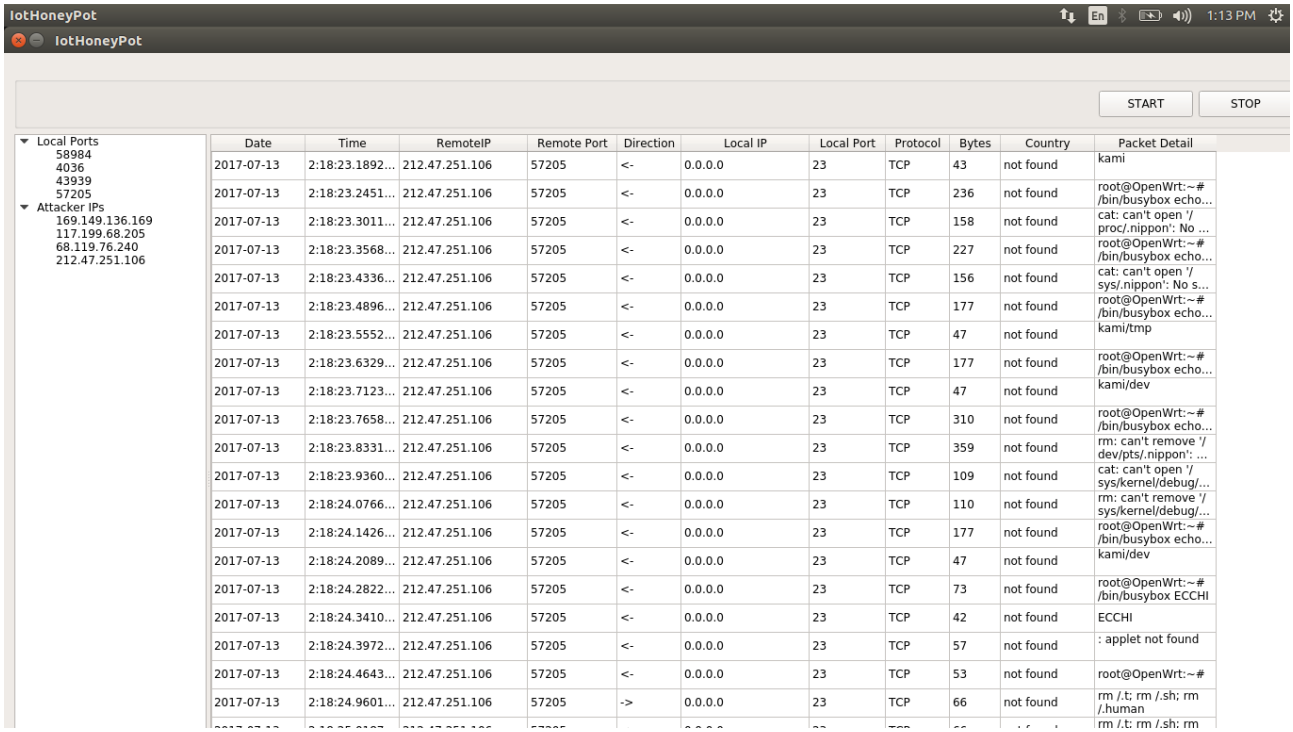

Рисунок 2 — Результаты работы IoT Honeypot-а

Sysdig Falco — высокоинтерактивная система, предназначенная для обнаружения аномальной активности в приложениях для встраиваемых устройств. После развертывания Falco использует модуль ядра Sysdig и библиотеки пользовательского пространства для мониторинга событий, соответствующих одному из условий, определенных в правилах. Правила могут создаваться администратором безопасности и их можно изменять и дополнять по мере необходимости. Если происходит соответствующее правилу событие, то информация о данном событии записывается в журнал мониторинга. Также есть возможность использовать программу генерации событий event-generator, имитирующую действия злоумышленника. Эта программа призвана помочь при настройке высокоинтерактивной системы [8].

Bluepot — это Bluetooth Honeypot, исходный код написан на языке программирования Java, предназначен для работы на ОС семейства GNU/Linux. Эта высокоинтерактивная система имеет функции приема и хранения любых вредоносных программ, с помощью которых его атакуют злоумышленники и имеет возможность взаимодействия с общими атаками на Bluetooth, такими как «BlueBugging» и «BlueSnarfing». Подключение по Bluetooth обеспечивается через аппаратные Bluetooth-ключи. Система также позволяет отслеживать атаки через графический пользовательский интерфейс, который предоставляет графики, списки, панель мониторинга и дальнейший подробный анализ из файлов журналов мониторинга [9].

Пример использования высокоинтерактивной системы bluepot приведен на рисунке 3.

XMPP IoT Honeypot — высокоинтерактивная система для встраиваемых устройств, реализованная на основе протокола XMPP. Включает в себя два основных модуля: клиент и сервер. Злоумышленник может получить доступ к этому honeypot-у несколькими отправив HTTP-запрос на открытый порт.

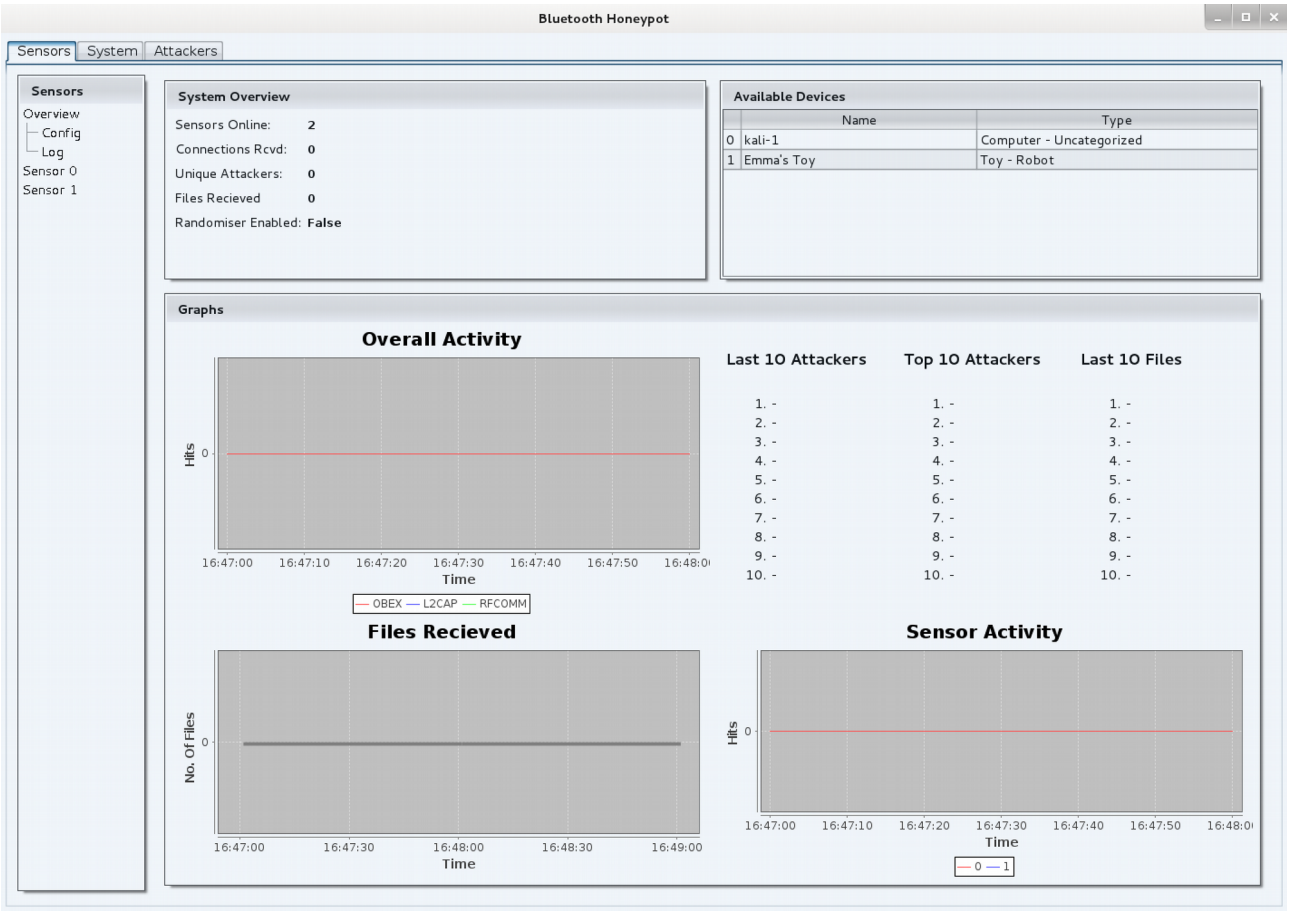

Рисунок 3 — Пример работы высокоинтерактивной системы bluepot

Можно заметить, что основная часть honeypot-ов работает на основании протоколов SSH и Telnet, но возможно создавать honeypot-ы по тому же принципу, но на основании других протоколов. Это возможно по той причине, что для анализа данных о злоумышленнике нет особой разницы, по каком протоколу он проникает в систему, равно как и для злоумышленника не важен протокол, по которому он атакует систему. Разница заключается лишь в информационных полях протоколов — в каких-то случаях можно получить больше информации о злоумышленнике, в каких-то — меньше.

1.3 Способы обнаружения высокоинтерактивных систем злоумышленниками

Зачастую высокоинтерактивные системы используют реальные службы в виртуальной среде, поэтому их можно обнаружить, найдя библиотеки или от-

ладчики и программное обеспечение, предназначенные для виртуализации. Ниже будут приведены способы распознавания виртуальных машин.

Очевидным способом обнаружения высокоинтерактивных систем является поиск ошибок реализации, например, несоответствий используемым протоколам передачи информации. Также системы могут быть обнаружены с использованием временных характеристик. Реальные системы будут быстрее обрабатывать запросы, особенно в многопоточном режиме.

На любой виртуальной машине обязательно будет установлено специфическое оборудование для видеоадаптера, жесткого диска, идентификатора процессора, версии BIOS, MAC-адреса сетевой карты, также виртуальные машины оставляют следы в системе в виде запущенных вспомогательных процессов, драйверов и других специфических объектов. При просмотре реестра виртуальной машины можно найти ключи, характерные только для виртуальных машин.

Для просмотра идентификатора жесткого диска в диспетчере устройств на виртуальной машине необходимо найти значение ключа с именем «0» в ветке реестра. Именно в этом месте перечисляются все дисковые накопители в системе, и первым, как раз в ключе с именем «0», будет тот диск, с которого произошла загрузка системы.

Далее злоумышленник может попробовать определить версию BIOS. Она содержится в ключе «SystemProductName». К примеру, для среды виртуализации VMware в ключе будет содержаться строка вида «VMware Virtual Platform», а для VirtualBox — «VBOX — 1».

Данные о видеоадаптере можно найти в соответствующей ветке. В этой ветке перечислено все, что подключено к шине PCI, в том числе и видеокарта.

Идентификатор процессора можно определить ассемблерной инструкцией CPUID, которая также дает много полезной информации о нем. Вид выдаваемой этой командой информации зависит от содержимого регистра EAX.

Пример использования инструкции CPUID:

```
... _asm { mov eax, 0x40000000 cpuid mov ID_1, ebx mov ID_2, ecx mov ID_3, edx } ...
```

Идентифицировать сетевую карту можно по MAC-адресу (три байта MAC-адреса сетевой карты определяют ее производителя, производители виртуальных машин в этом плане не исключение), но эта информация может оказаться недостоверной, потому что адрес можно поменять, чем обычно пользуются создатели высокоинтерактивных систем.

Злоумышленник также может попробовать найти в системе вспомогательные процессы, окна и другие «подозрительные» с его точки зрения объекты.

Для работы практически всем виртуальным машинам необходимо наличие дополнений к гостевой операционной системе, например VBoxGuestAddition для VirtualBox. Эти дополнения оставляют в системе следы в виде запущенных процессов, факт наличию которых дает понять что это виртуальная система. Помимо самих процессов, демаскирующим признаком могут стать окна, открытые этими процессами и дополнительные файлы, используемые ими.

В файловой системе виртуальных машинах содержатся файлы, присущие только средам виртуализации. По их наличию злоумышленник может понять тот факт, что он находится именно в виртуальной машине, а не в реальной системе [10]. Помимо этого разработчики высокоинтерактивных систем, основанных на реальных встраиваемых устройствах, могут специально добавлять подобные файлы для введения злоумышленников в заблуждение.

На рисунке 4 приведен пример файлов, найденных при исследовании системы. Данные файлы могут содержаться только в среде виртуализации VMware и их наличие сообщит злоумышленнику о том, что он находится именно в ней.

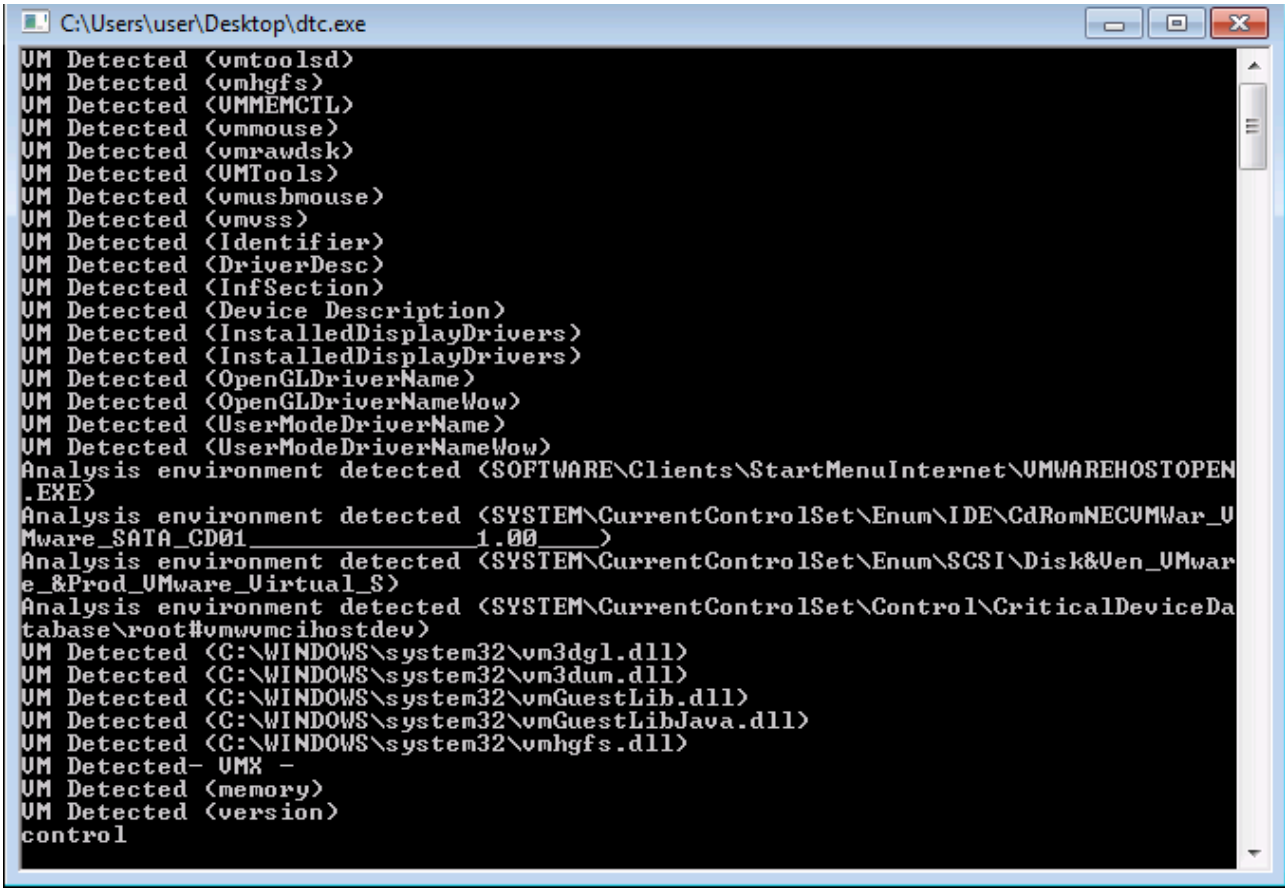

Рисунок 4 — Файлы в среде виртуализации VMware

Наличие файлов, приведенных на рисунке 5, даст понять злоумышленнику тот факт, что он находится в среде виртуализации Virtualbox.

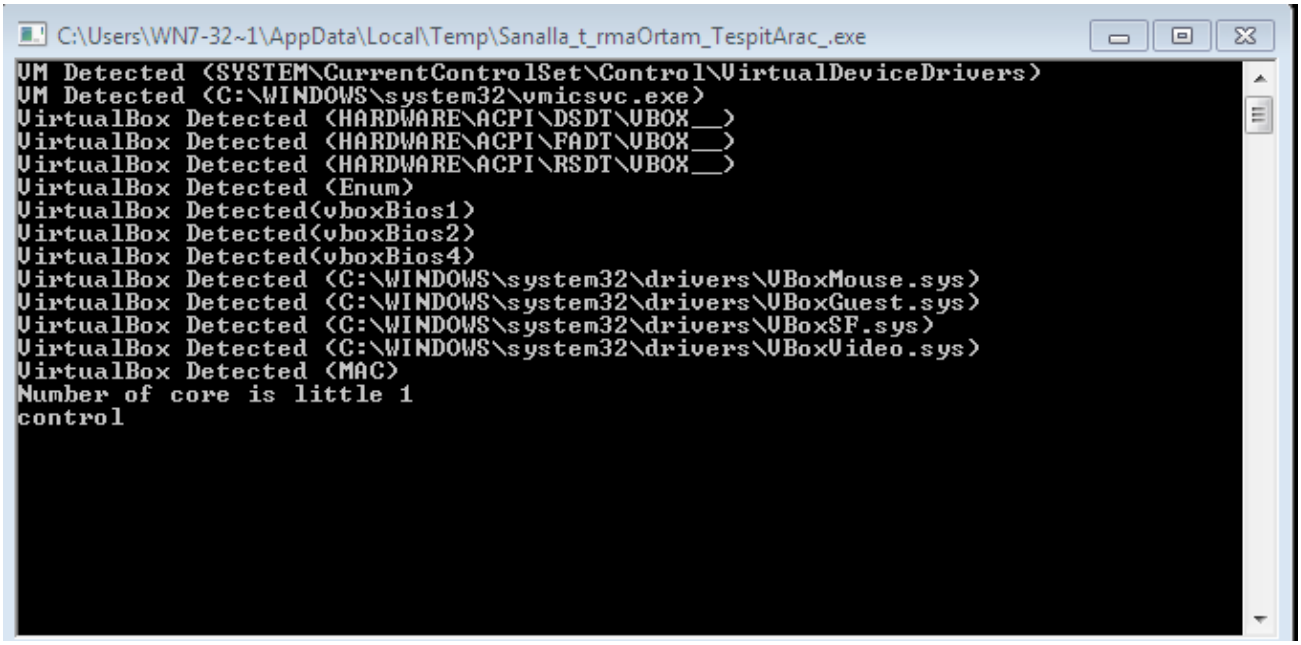

Рисунок 5 — Файлы в среде виртуализации Virtualbox

Среду виртуализации QEMU можно обнаружить проверив два раздела реестра:

`HARDWAREDEVICEMAPScsiScsi Port 0Scsi Bus 0Target Id 0Logical Unit Id 0Identifier`

`HARDWAREDescriptionSystemSystemBiosVersion`

При этом следует помнить, что содержимое этих разделов легко подменить. Данное утверждение относится ко всем вышеперечисленным методам.

Для повышения безопасности высокоинтерактивных систем для встраиваемых устройств рекомендуется скрывать или подменять все их артефакты, включая среду виртуализации.

Схема, иллюстрирующая действия злоумышленника при проникновении в высокоинтерактивную систему, приведена в приложении Г на рисунке Г.1.

Попытки замаскировать высокоинтерактивную систему для встраиваемых устройств под какую-либо плату или под реальное устройство также могут обнаруживаться злоумышленниками. Различия между физическими процессорами и виртуальными аппаратными средствами обнаруживаются из-за упрощения проектирования, а также по производительности ввода-вывода. Например, современные чипсеты трудно моделировать и для простоты виртуальная платформа VMware всегда эмулирует чипсет i440bx, что приводит к абсурдным конфигурациям оборудования: два процессора AMD Opteron и 8 ГБ оперативной памяти на материнской плате Intel. Операционные системы работают в таких необычных средах, потому что прошивка не требует делать проверку ОС чипсета.

1.4 Проблемы, присущие высокоинтерактивным системам

Основные проблемы, с которыми можно столкнуться при использовании высокоинтерактивных систем:

– узкая направленность. Высокоинтерактивная система «видит» только

ту активность, которая направлена на нее, но если злоумышленник проникнет в реальную систему, то honeypot не сообщит об этом. С другой стороны этот недостаток может быть достоинством, так как для работы высокоинтерактивной системы не требуется больших затрат ресурсов;

– развертывание и управление. Высокоинтерактивные системы сложны в установке и настройке. Сложность добавляет тот факт, что система должна не только соответствовать поставленным целям, но также корректно функционировать, чтобы злоумышленник не заподозрил тот факт, что он находится не в реальной системе. Отчасти эта проблема решается использованием виртуальных систем;

– безопасность. Безопасность высокоинтерактивных систем заключается в защите от последствий их компрометации злоумышленником. Для этого необходимо ограничивать сетевой доступ к системе, например, используя стандартные механизмы, такие как межсетевые экраны. Их основной задачей является ограничение доступа трафика из высокоинтерактивной системы во внешнюю сеть;

– обнаружение. Если злоумышленник обнаружит факт того, что он находится не в реальной системе, а в honeypot-е, то он постарается уничтожить следы своего пребывания в системе и тем самым избежать раскрытия какой-либо информации о себе. Если злоумышленник может с помощью каких-либо явных признаков определить, что система является honeypot-ом, то такая система не является стойкой к обнаружению и требует доработки. Помимо этого злоумышленник, обнаружив, что он находится в высокоинтерактивной системе, может совершить действия, задетектировав которые высокоинтерактивная система сообщит о факте атаки администратору безопасности. И в то время, пока силы специалистов будут направлены на анализ произошедшего, злоумышленник проникнет в реальную систему. Исходя из этого появляется еще одна проблема — высокоинтерактивные системы необходимо делать непохожими одна на другую в силу того, что

злоумышленники не отставая от создателей высокоинтерактивных систем собирают информацию о них;

– повторная атака. Данная проблема тесно связана с проблемой обнаружения. Однажды атакованная злоумышленником высокоинтерактивная системы может быть использована для нападения, проникновения или нанесения вреда другим системам. Чем проще honeypot, тем меньше риск. Например, honeypot, который эмулирует несколько сервисов, трудно скомпрометировать и использовать для атаки на другие системы. Напротив, сложный honeypot, дает злоумышленнику больше возможностей и ресурсов для атаки на другие устройства и системы. Злоумышленник, обнаруживший наличие высокоинтерактивной системы на устройстве, может затем использовать его для запуска пассивных или активных атак против других устройств и систем;

– изоляция. Действия, произведённые злоумышленником внутри высокоинтерактивной системы, в том числе и её компрометация, не должны оказывать влияние на остальные элементы реальной системы. Для этого могут быть использованы брандмауэры.

Из-за их недостатков, высокоинтерактивные системы не могут стать заменой других механизмов безопасности, такие как антивирусы, брандмауэры и системы обнаружения вторжений. Они эффективны только как часть системы защиты, работая с существующими механизмами безопасности. Исходя из рассмотренных проблем, присущих высокоинтерактивным системам, можно выделить основные критерии, по которым можно производить их оценивание:

– гибкость. Этот критерий определяет возможность изменения высокоинтерактивной системы под параметры реальной системы, в которой она установлена. В первую очередь гибкость определяется наличием тех или иных ограничений, продиктованных применяемыми технологиями и особенностями архитектуры;

– сложность обнаружения. Критерий показывает, насколько

высокоинтерактивная система отличается от реальной и как быстро, в следствие этого, злоумышленник поймет, что попал в honeypot. Сложность обнаружения наличия высокоинтерактивной системы зависит от особенностей ее функционирования;

– функциональность. Этот параметр высокоинтерактивной системы связан с гибкостью, но не эквивалентен ей. Под функциональностью понимается объем возможностей высокоинтерактивной системы, необходимый для достижения определенной цели. Система может быть негибкой, но при этом функциональной. Например, можно представить гипотетический honeypot, имитирующий работу ftp-сервера, но не предоставляющий возможности работы в качестве web-сервера;

– производительность. Этот параметр показывает, насколько производительность высокоинтерактивной системы отличается от производительности реальной системы. Если показатели значительно отличаются, то злоумышленнику достаточно будет сделать несколько временных тестов, чтобы сделать вывод о том, в реальной или в высокоинтерактивной системе он находится [11];

– наличие демаскирующих признаков. Если злоумышленник может с помощью каких-либо демаскирующих признаков определить, что система является высокоинтерактивной, а не реальной, то такая система не является стойкой к обнаружению;

– изоляция. Проникновение злоумышленника в реальную систему через высокоинтерактивную может привести к критичным последствиям. Если есть вероятность его проникновения, то необходимо использовать сторонние средства, которые не позволят произойти подобному. Такие, как брандмауэры и межсетевые экраны.

1.5 Сбор сведений о злоумышленнике высокоинтерактивной системой

У каждой высокоинтерактивной системы есть функция регистрации произошедших инцидентов в журналы. Возможные инциденты зависят от типа используемого honeypot-a. Поэтому важно определить проблемы, которые должны быть исследованы, до фактического развертывания honeypot-a. Для решения одной проблемы можно использовать разные высокоинтерактивные системы, каждая из которых имеет свой собственный подход и точность.

Цель сбора и контроля данных состоит в обеспечении невозможности использования скомпрометированных компонентов (ресурсов) для атаки или для нанесения вреда другим системам после проникновения злоумышленника в высокоинтерактивную систему. Сбор данных гарантирует, что можно обнаружить и зарегистрировать все действия нарушителей, даже если они замаскированы или зашифрованы.

По версии автора книги Honeypots: Tracking Hackers Ланса Спицнера злоумышленники, атакующие высокоинтерактивные системы делятся на два типа: script-kiddies и blackhats.

Script-kiddies. Злоумышленников, относящихся к этому типу не интересует, принадлежит ли устройство крупной организации или обычному пользователю. Их цель — взломать как можно больше систем приложив минимальные усилия. Зачастую они используют общедоступные инструменты и различные известные уязвимости. Производят сканирование большого количества диапазонов IP-адресов с целью найти как можно больше уязвимых устройств. Большинство таких злоумышленников низкоквалифицированы и их действия редко наносят большой ущерб.

Blackhats. Злоумышленники этого типа профессионалы своего дела. Их цель — сложные системы, имеющие большую ценность для владельца. Они атакуют системы с определенными намерениями, их нападение обычно связано с финансовыми или национальными мотивами, такими как терроризм, спонси-

руемый государством. Их действия могут быть направлены на запуск DoS-атаки или создание ботов из устройств, которые будут автоматически распространяться и заражать другие устройства. Могут использовать как общедоступные инструменты, так и свои личные разработки и уязвимости нулевого дня. Хотя злоумышленников с такой высокой квалификацией мало, их атаки гораздо более опасны. Зачастую успешные атаки долго остаются незамеченными для высокоинтерактивных систем [12].

Для составления представления о злоумышленнике необходимо определить информацию, которую будет собирать высокоинтерактивная система. Р. МакГрю [13] предположил, что описание атаки на высокоинтерактивную систему должно содержать информацию по следующим критериям:

– масштаб и глубина — масштаб атаки описывается количеством затронутых машин, а глубина — это степень воздействия на систему;

– сложность — характеризует уровень знаний, необходимых для выполнения конкретной атаки;

– маскировка — качество скрытия следов своего присутствия в системе злоумышленником;

– источник атаки — злоумышленник должен быть, насколько это возможно, идентифицирован;

– уязвимость — это недостаток в системе/протоколе, позволяющий совершить атаку;

– инструменты — инструменты, использованные при атаке, например, руткиты или бекдоры.

Масштаб и глубина могут быть получены из частоты атак, степени воздействия атаки и по степени заражения системы.

Частота атак измеряется по следующим критериям:

– количество вторжений злоумышленника за единицу времени;

– количество источников атаки за единицу времени;

– количество новых источников атаки за единицу времени;

– соотношение количества источников к количеству атак;

– соотношение новых источников атаки за единицу времени к общему количеству атак за все время работы системы;

– количество полученных пакетов за единицу времени;

– объем полученных данных за единицу времени;

– длительность интервалов времени между активностью в высокоинтерактивной системе.

Маскировка злоумышленника определяется по тому, насколько качественно он скрывает следы своего присутствия в системе.

Уязвимость, используемая злоумышленником должна быть определена для ведения дальнейшей статистики. Это необходимо в силу того, что обычно в высокоинтерактивной системе присутствует сразу несколько уязвимостей, статистика собирается по каждой из них. Помимо этого один злоумышленник может одновременно атаковать сразу несколько уязвимостей и не все его попытки атак будут успешными.

Источник атаки обычно можно определить с помощью мета-данных сетевых пакетов, однако первоисточник атаки может быть сложно идентифицировать, поскольку злоумышленник будет пытаться скрывать свое присутствие в системе.

Пример сообщения от высокоинтерактивной системы о том, что была обнаружена активность в системе, приведен на рисунке 6.

Особенностью функционирования данной высокоинтерактивной системы является то, что сообщения об атаках отправляются администратору безопасности на электронную почту.

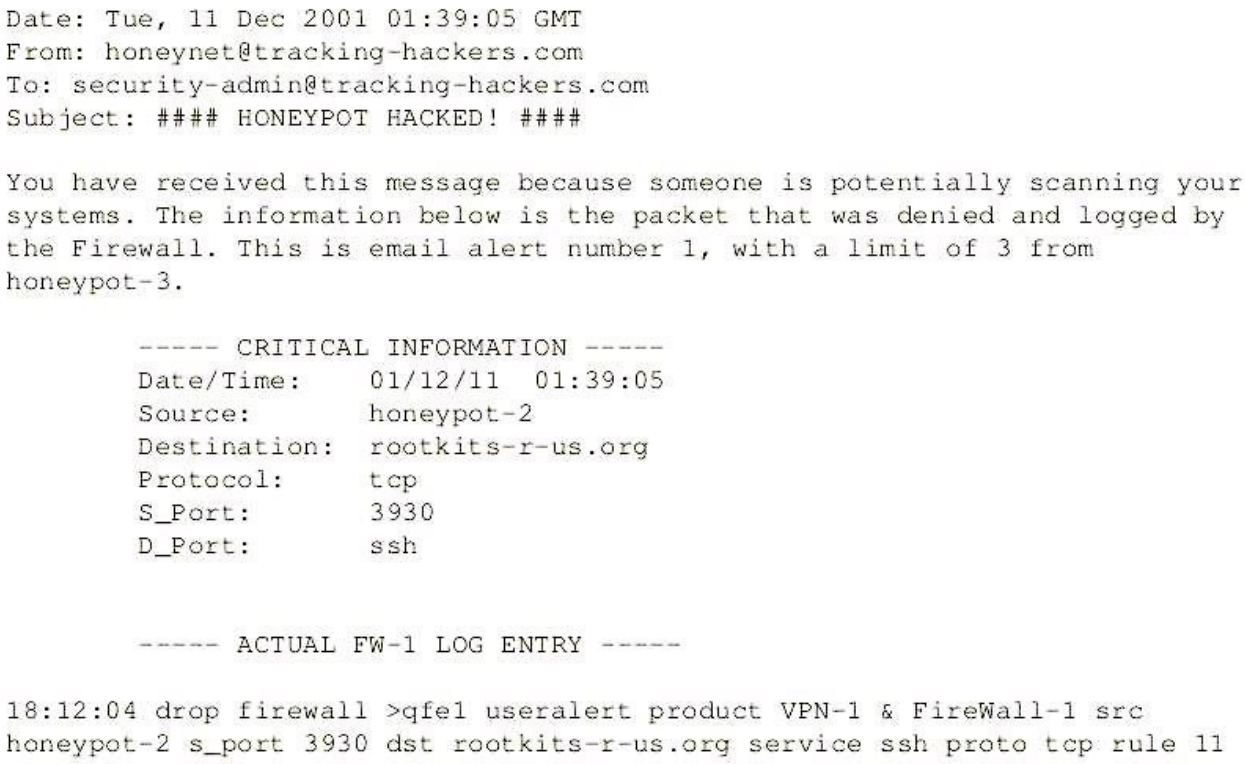

Рисунок 6 — Сообщение от высокоинтерактивной системы об обнаружении активности

1.6 Собираемые высокоинтерактивной системой сведения

К информации о злоумышленнике относится:

- IP-адрес или IP-префикс;
- порт;
- протокол передачи данных;
- дата и время атаки;
- имя домена;
- страна;
- User agent;
- операционная система;
- URL.

Пример собранной высокоинтерактивной системой информации о злоумышленнике приведен на рисунке 7.

Date	Time	IP of Attacker	Proto	Src Pt	Dst Pt
01/11/05	00:12:03	216.232.130.32	tcp	3765	http
01/11/05	00:25:13	216.140.131.115	tcp	1202	http
01/11/05	00:46:23	202.85.165.108	tcp	2046	sunrpc
01/11/05	01:19:09	216.161.236.121	tcp	1278	http
01/11/05	01:47:58	216.78.152.78	tcp	3729	http
01/11/05	01:53:26	216.79.219.137	tcp	3033	http
01/11/05	02:28:09	216.160.69.157	tcp	3144	http
01/11/05	02:35:12	216.191.169.200	tcp	1477	http
01/11/05	02:45:11	216.231.43.128	tcp	4852	http
01/11/05	03:33:24	216.187.238.114	tcp	4519	http
01/11/05	04:07:04	216.80.147.224	tcp	1346	Http
01/11/05	05:17:23	216.151.90.150	tcp	2400	http
01/11/05	05:48:24	216.205.68.202	tcp	1801	http
01/11/05	06:38:44	216.102.57.26	tcp	2663	http

Рисунок 7 — Собранная высокоинтерактивной системой информация

К информации о honeypot-е относится:

– UserID;

– имя домена/URL.

Идентификация злоумышленника может иметь разную степень детализации в зависимости функционала honeypot-а. Однако нужно учитывать, что злоумышленник практически всегда будет пытаться скрыть себя и, к примеру, есть шанс получить поддельный IP-адрес, также IP-адреса могут перемещаться с хоста на хост, поскольку провайдеры сети Интернет используют пулы IP-адресов. Поэтому высокоинтерактивные системы объединяют IP-адреса с меткой времени и определяют источник атаки как IP-адрес, с которого злоумышленник атакует цель, например, в течение одного дня.

Существуют honeypot-ы, которые классифицируют URL-адреса на основе URL-адреса и содержимого страницы.

Чтобы определить операционную систему, из которой происходят атаки, обычно используются дополнительные инструменты, такие как p0f, которые

распознают атакующую ОС, анализируя состав пакетов, поскольку каждая операционная система создает их по-разному.

После идентификации источника атаки на высокоинтерактивную систему нужно определить цель атаки. Обычно целью для злоумышленника является:

– программное обеспечение;
– уязвимость в системе;
– сервис;
– прошивка;
– операционная система;
– аппаратное обеспечение;
– устройство целиком (такое возможно, если конкретный уровень архитектуры не определен).

Некоторые honeypot-ы для более быстрого и точного определения цели атаки используют следующий подход: «одна цель атаки (уязвимая служба) — один сетевой порт». Номера портов задаются Internet Assigned Numbers Authority (IANA) и доступны в официальных списках. Если высокоинтерактивная система контролирует всю сеть, каждый отдельный IP-адрес можно рассматривать как цель для злоумышленника [14].

Используя совокупность некоторой уже известной информации о злоумышленнике можно узнать больше о нем. Для этого можно использовать сторонние программы и утилиты. Например, программы SamSpade и Ethereal, утилита fwhois, а для анализа бинарных файлов могут использоваться инструменты статического анализа исполняемых файлов типа IDA Pro, radare2.

Пример определения владельца доменного имени USIT.net при помощи утилиты fwhois приведен на рисунке 8.

```
otto $fwhois USIT.NET@whois.networksolutions.com
[whois.networksolutions.com]

Registrant:
OneMain.com (USIT-DOM)
   1127 North Broadway
   Knoxville, TN 37917
   US

   Domain Name: USIT.NET

   Administrative Contact, Billing Contact:
      Hostmaster, EarthLink  (EHT413)  dns-admin@EARTHLINK.NET
      EarthLink, Inc.
      1430 W. Peachtree St NW Suite 400
      Atlanta, GA  30309
      US
      (404) 815-0770 (972) 481-5884
   Technical Contact:
      EarthLink Network, Domain Admin.  (ELN-DA) hostmaster@EARTHLINK.NET
      EarthLink Network, Inc.
      1430 W Peachtree St NW Ste 400
      Atlanta, GA 30309
      US
      626-296-2400
      Fax- - - - - 626-296-5113
```

Рисунок 8 — Определение владельца домена

Пример определения владельца IP-адреса, полученного высокоинтерактивной системой при сборе информации о действиях злоумышленника, программой SamSpade приведен на рисунке 9.

С помощью данной программы возможно идентифицировать пул адресов, которому принадлежит IP-адрес с которого идет атака. Далее возможно определить Интернет-провайдера, который распределяет IP-адреса клиентам. По этой информации можно отслеживать владельца сети и IP-адреса и, возможно, самого злоумышленника.

Данная информация может быть некорректной в силу того, что IP-адрес — это первое, что злоумышленники обычно скрывают. Для этого обычно используются VPN, proxy-сервера или браузер TOR.

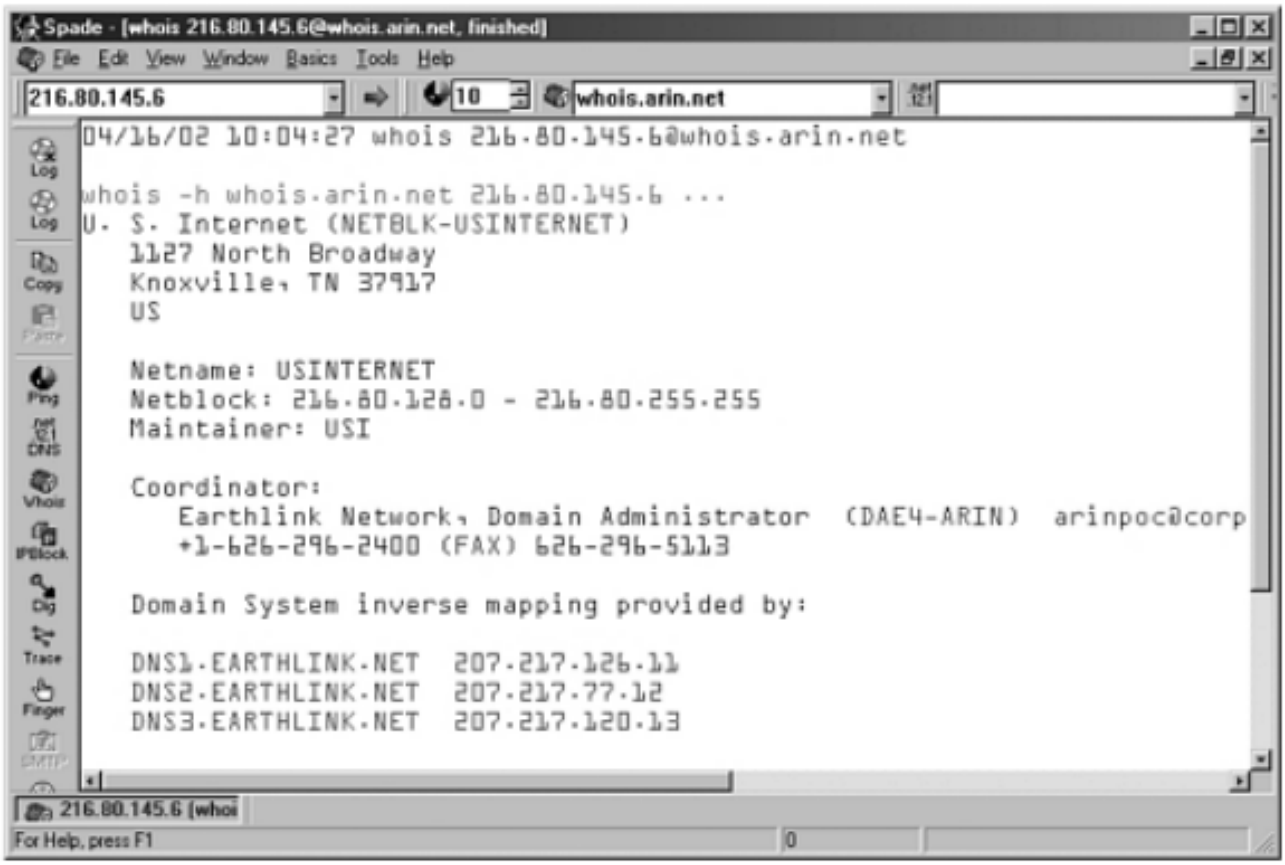

Рисунок 9 — Определение владельца IP-адреса

Пример использования инструмента Wireshark для анализа бинарного файла, переданного злоумышленником по протоколу FTP и полученного высокоинтерактивной системой при анализе действий злоумышленника и оставленных им следов в системе, приведен на рисунке 10.

Данный инструмент позволяет перехватывать весь входящий и исходящий трафик, передаваемый сетевому протоколу, для дальнейшего анализа. По собранному трафику можно определить какие действия совершал злоумышленник в ходе атаки, какие инструменты были использованы им для атаки высокоинтерактивной системы, а также перехватить пакеты, которые злоумышленник посылал системе.

Помимо инструмента Wireshark для более детального исследования бинарных файлов используются такие программы как OllyDbg, IDA Pro и radare2.

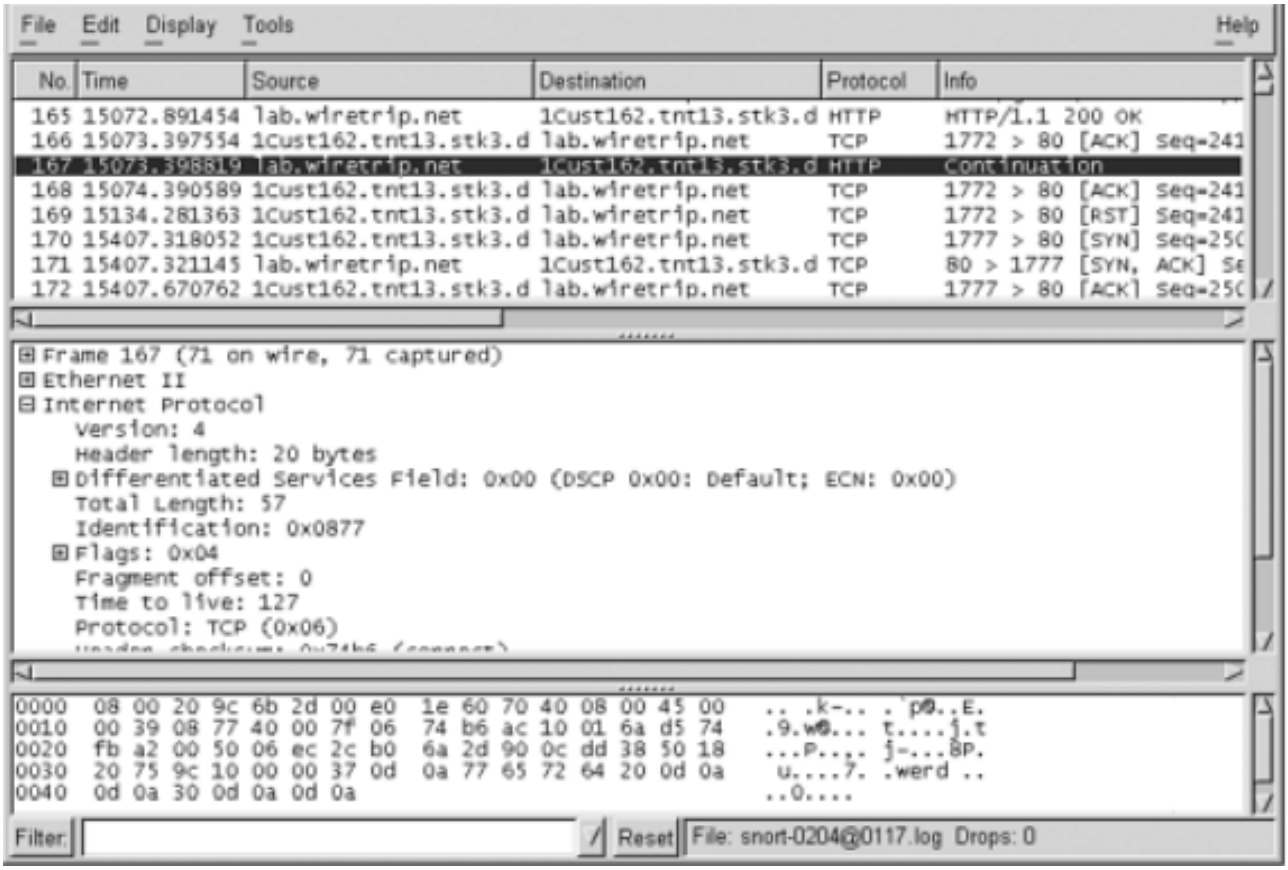

Рисунок 10 — Анализ бинарного файла

Пример анализа HTTP-пакета, отправленного злоумышленником и перехваченного высокоинтерактивной системой, приведен на рисунке 11. По содержимому передаваемых злоумышленником пакетов можно определить какую операционную систему он использовал, какие программы установлены в ней и многое другое. При этом злоумышленники как и создатели высокоинтерактивных систем обычно стараются скрывать или подменять подобную информацию для введения противника в заблуждения.

Из результатов анализа очевидно, что злоумышленник использовал операционную систему Windows NT 5.0 на которой установлены следующие программы: Microsoft Excel, Microsoft Word и Microsoft Powerpoint, а также user-agent Mozilla версии 4.0.

```
02/04-06:25:09.372695 213.116.251.162:1760 -> 172.16.1.106:80
TCP TTL:111 TOS:0x0 ID:10948 IpLen:20 DgmLen:382 DF
***AP*** Seq: 0x8E2366BE  Ack: 0x2CAE7C1B  Win: 0x2238  TcpLen: 2(
47 45 54 20 2F 20 48 54 54 50 2F 31 2E 31 0D 0A  GET / HTTP/1.1..
41 63 63 65 70 74 3A 20 69 6D 61 67 65 2F 67 69  Accept: image/gi
66 2C 20 69 6D 61 67 65 2F 78 2D 78 62 69 74 6D  f, image/x-xbitm
61 70 2C 20 69 6D 61 67 65 2F 6A 70 65 67 2C 20  ap, image/jpeg,
69 6D 61 67 65 2F 70 6A 70 65 67 2C 20 61 70 70  image/pjpeg, app
6C 69 63 61 74 69 6F 6E 2F 76 6E 64 2E 6D 73 2D  lication/vnd.ms-
65 78 63 65 6C 2C 20 61 70 70 6C 69 63 61 74 69  excel, applicati
6F 6E 2F 6D 73 77 6F 72 64 2C 20 61 70 70 6C 69  on/msword, appli
63 61 74 69 6F 6E 2F 76 6E 64 2E 6D 73 2D 70 6F  cation/vnd.ms-po
77 65 72 70 6F 69 6E 74 2C 20 2A 2F 2A 0D 0A 41  werpoint, */*..A
63 63 65 70 74 2D 4C 61 6E 67 75 61 67 65 3A 20  ccept-Language:
65 6E 2D 75 73 0D 0A 41 63 63 65 70 74 2D 45 6E  en-us..Accept-En
63 6F 64 69 6E 67 3A 20 67 7A 69 70 2C 20 64 65  coding: gzip, de
66 6C 61 74 65 0D 0A 55 73 65 72 2D 41 67 65 6E  flate..User-Agen
74 3A 20 4D 6F 7A 69 6C 6C 61 2F 34 2E 30 20 28  t: Mozilla/4.0 (
63 6F 6D 70 61 74 69 62 6C 65 3B 20 4D 53 49 45  compatible; MSIE
20 35 2E 30 31 3B 20 57 69 6E 64 6F 77 73 20 4E   5.01; Windows N
54 20 35 2E 30 3B 20 48 6F 74 62 61 72 20 32 2E  T 5.0; Hotbar 2.
30 29 0D 0A 48 6F 73 74 3A 20 6C 61 62 2E 77 69  0)..Host: lab.wi
72 65 74 72 69 70 2E 6E 65 74 0D 0A 43 6F 6E 6E  retrip.net..Conn
65 63 74 69 6F 6E 3A 20 4B 65 65 70 2D 41 6C 69  ection: Keep-Ali
76 65 0D 0A 0D 0A                                ve.....
```

Рисунок 11 — Анализ HTTP-пакета

На основании собранных данных о действиях и ресурсах злоумышленника возможно предсказывать его поведение и на основании этого динамически изменять конфигурацию высокоинтерактивной системы. Смысл этих действий направлен на повышение эффективности использования высокоинтерактивных систем для встраиваемых устройств. Помимо этого, на основании собранных данных генерируются сигнатуры для систем обнаружения вторжения и межсетевых экранов.

При этом важно помнить, что злоумышленники могут подделывать информацию о себе и маскировать свои действия. Обычно таким занимаются опытные злоумышленники — blackhats, последствия действий которых могут быть критичными для устройств или систем.

1.7 Составление представления о нарушителе на основе собираемой высокоинтерактивной системой информации

Смысл создания и использования высокоинтерактивной системы в том, чтобы собирать информацию о злоумышленниках и на основе собранной информации предпринимать меры по защите встраиваемых систем. Помимо этого на основе собираемой информации можно создавать сигнатуры для межсетевых экранов и антивирусов.

К наиболее важным сведениям из всех, собираемых о злоумышленнике, относятся сведения об используемых им средствах и его ресурсах. Остальные данные, такие как страна, IP-адрес и другие собираются в основном для статистики.

Как было сказано выше, высокоинтерактивные системы могут располагаться внутри локальной сети и в демилитаризованной зоне. От расположения honeypot-а зависит то, какую информацию он сможет собрать, ее количество и выводы, которые можно сделать проанализировав собранную информацию.

Обычно высокоинтерактивные системы, расположенные вне сети, подвержены автоматизированным атакам, исходящим от ботов или ботнетов, помимо атак от реальных злоумышленников. Данные об атаках от ботнетов могут не учитываться при составлении модели нарушителя. Их стоит выделять в отдельную категорию нарушителей, так как их поведение значительно отличается от поведения реальных злоумышленников.

Высокоинтерактивные системы, расположенные внутри сети, обычно детектируют атаки только от реальных злоумышленников. Это происходить потому, что для обнаружения высокоинтерактивной системы внутри локальной сети необходимы определенные знания и умения. Вероятность случайного попадания в такую «ловушку» стремится к нулю. На основании собираемых о злоумышленниках данных (п. 1.6) можно составить модель нарушителя, где по

масштабу и глубине атаки, сложности проникновения в систему, уровню маскировки злоумышленником своих следов, эксплуатируемым им уязвимостям и используемым для этого инструментам можно определить его возможности. При этом нарушитель всегда будет действовать извне системы и его действия, направленные на систему, будут преднамеренными, а уровень защищенности высокоинтерактивной системы определяется тем, какие уязвимости внедрены в нее разработчиками.

Имея представления о нарушителе можно работать в направлении создания защитных средств для встраиваемых устройств, что является актуальным ввиду большого числа атак ботнетов.

1.8 Оценка ущерба для системы, нанесенного действиями злоумышленника

Для оценки ущерба от произведенной злоумышленником атаки можно проанализировать его действия, направленные на систему. Затем, необходимо определить ценность активов, затронутых им во время атаки. На основании ценности активов можно предположить величину ущерба, в случае, если бы злоумышленник проник в реальную систему, а не в высокоинтерактивную.

2 Встраиваемые устройства

2.1 Общие сведения о встраиваемых устройствах

Встраиваемые устройства представляют собой некоторую комбинацию аппаратного и программного обеспечения, которая содержит специализированную вычислительную систему. Таким образом, термин относится к любым вычислительным системам, отличным от персональных компьютеров общего назначения или мейнфреймов. Зачастую они являются кибер-физическими системами, интегрирующими вычисления и физические процессы.

В настоящее время встраиваемые устройства используются и для управления промышленными системами и в потребительской технике: телекоммуникационное оборудование, банкоматы, бытовая техника, GPS-трекеры и навигационное оборудование, медицинское оборудование, детские игрушки, устройства для «умного дома», к ним также относятся роутеры, камеры видеонаблюдения и т. д.

Вычислительные ресурсы встраиваемых устройств весьма ограничены, поэтому зачастую в них отсутствуют или слабо реализованы функции безопасности. Также они могут иметь преднамеренные программные закладки — бекдоры (backdoors), загруженные в прошивку оборудования производителем или оставленные разработчиками тестовые аккаунты, которые на этапе тестирования устройств использовались для проверки их работоспособности. К бекдорам относятся логины и пароли по умолчанию в роутерах или потайные ходы для доступа в роутерах, базовых станциях и мобильных телефонах, программируемых контроллерах промышленных систем [15].

С распространением встраиваемых устройств растет число ботнетов, основанных на них же. Ботнеты обычно используют уязвимости в веб-приложениях встраиваемых устройств и множество других уязвимостей, эксплуатация которых компрометирует устройство полностью. Например, в 2016 году появилась информация о ботнете Mirai, основанном на роутерах и других встраива-

емых устройствах [16]. В 2017 году стало известно о ботнете Reaper, заразившем около 1 млн. камер видеонаблюдения и роутеров [17].

2.2 Уязвимости во встраиваемых устройствах, влияющие на их защищенность

Уязвимости, имеющиеся во встраиваемых устройствах, можно отнести к нескольким категориям в зависимости от их происхождения:

– ошибки программирования. Многие из уязвимостей во встраиваемых устройствах связаны с преднамеренными и непреднамеренными ошибками программирования. Преднамеренные программные ошибки закладки — бекдоры, загруженные в прошивку оборудования производителем — например, логины и пароли по умолчанию в роутерах или потайные ходы для доступа в роутерах, базовых станциях и мобильных телефонах, программируемых контроллерах промышленных систем;

– уязвимости в веб-интерфейсе. Большинство встраиваемых устройств имеют веб-интерфейс управления, через который их можно настраивать и управлять ими. Однако приложения, работающие на этих устройствах, обычно редко обновляются либо не обновляются никогда. Следовательно, эти устройства могут быть подвержены воздействию сетевых атак, которые используют уязвимости веб-интерфейса;

– слабый контроль доступа. На многих встраиваемых устройствах стоят слабые пароли или пароли по умолчанию, а некоторые устройства имеют жестко закодированные пароли, обеспечивающие доступ к бекдорам тем, кто знает эти пароли. Такие уязвимости позволяют злоумышленникам легко обходить механизмы контроля доступа прикладывая минимальные усилия;

– слабости в криптографии. Некоторые устройства используют криптографические механизмы для аутентификации или для сохранения конфиденциальности информации. Часто криптографические механизмы не используются должным образом, что приводит к критическим сбоям безопасно-

сти. Примеры включают использование слабых генераторов случайных чисел для генерации криптографических ключей или уязвимостей в протоколах, использующих криптографические примитивы.

Исходя из типов уязвимостей во встраиваемых устройствах, можно заметить, что большинство из них относятся к безопасности операционных систем и прошивок, имеющихся во встраиваемых устройствах. Это говорит о полном отсутствии или недостаточной реализации безопасной разработки [18] и именно они приводят к появлению ботнетов. И даже если разработчики беспокоятся о доверенной загрузке и многослойном шифровании, то это не спасает от проблем связанных с безопасностью приложений.

При этом некоторые подобные уязвимости редко можно встретить в ПО для компьютеров и ЭВМ, а ещё сложнее проэксплуатировать их из-за появившихся различных механизмов для повышения их безопасности на уровне ОС. Причины того, почему разработчики встраиваемых устройств довольно медленно перенимают опыт безопасной разработки у разработчиков компьютеров и ЭВМ, могут быть абсолютно разные. Главное то, что разработчики вредоносного ПО для встраиваемых устройств опережают разработчиков защитных механизмов и из-за этого безопасность встраиваемых устройств остается на крайне низком уровне.

К примеру, в ботнете Reaper есть Lua-интерпретатор, идея использования которого пришла от создателей вредоносного ПО для компьютеров и ЭВМ. Его использование позволяет быстрее расширять функционал вредоносных программ. Недавно появилось сообщение об обновленном ботнете Mirai — Satori [16], который использует эксплойты к уязвимостям в прошивках и операционных системах и учитывая тот факт, что исходники ботнета Mirai находятся в публичном доступе, сообщения о заражении все большего числа встраиваемых устройств будут появляться чаще и чаще.

Что касается целей атак на встраиваемые устройства, можно выделить следующие уровни архитектуры:

– аппаратное обеспечение;

– прошивка;

– операционная система;

– приложения;

– устройство целиком (такое возможно, если конкретный уровень архитектуры не определен).

Важно отметить, что зачастую нет четкого различия между прошивкой и операционной системой встраиваемого устройства, поскольку во многих случаях они не имеют реальной ОС, а их прошивка обеспечивает типичные функциональные возможности ОС (например, управление ресурсами). Кроме того, атаки могут быть нацелены не на сами встроенные устройства, а на протокол, используемый этими устройствами для связи или управления.

Предпосылки для атак на встраиваемые устройства:

– устройство, имеющее доступ к сети Интернет. Многие уязвимости встраиваемых устройств могут быть использованы злоумышленником удаленно, если устройство подключено к Интернету. Атакующему не нужны права доступа. Единственным требованием является то, что злоумышленник может потенциально обнаружить устройство и подключиться к нему по сети Интернет;

– локальный или удаленный доступ к устройству. Это условие требует, чтобы злоумышленник имел некоторые привилегии, которые допускают наличие у него прав доступа к устройству. Часто для доступа к устройству достаточно иметь права обычного пользователя;

– физический доступ к устройству. Для совершения атаки злоумышленнику необходимо иметь возможность физического доступа к устройству;

– физическая близость злоумышленника. В некоторых случаях злоумышленнику не нужен физический доступ. Ему достаточно находиться в непосредственной близости от устройства. Например, для атак устройства, имеющие

функцию беспроводной связи, злоумышленнику будет достаточно находиться в радиусе действия целевого устройства.

Все атаки можно сгруппировать по нескольким типам:

– захват управления программами. Атаки этого типа нарушают нормальный процесс управления программами, запущенными на встраиваемом устройстве. Это может привести к выполнению кода, введенного злоумышленником;

– реверс-инжиниринг. Злоумышленник может получить конфиденциальную информацию (например, учетную запись пользователя или администратора), анализируя программное обеспечение (прошивку или приложение) во встроенном устройстве. Используя методы реверс-инжиниринга, злоумышленник может обнаруживать уязвимости в коде (например, ошибки синтаксического анализа), которые могут быть использованы другими методами атаки на систему;

– внедрение вредоносных программ. Злоумышленник может заразить встраиваемое устройство вредоносным программным обеспечением. Вредоносная программа, которая заражает устройство, может изменить его поведение, что может иметь катастрофические последствия;

– инъекция пакетов. Этот метод является атакой, направленной на протоколы, используемые встраиваемыми устройствами. Подобным типом атаки является манипуляция с программой, запущенной на встроенном устройстве. Такие атаки используют уязвимости синтаксического анализа в реализации протоколов или других программах;

– прослушивание трафика. Это метод пассивной атаки, при котором злоумышленник наблюдает только за сообщениями, отправленными и принимаемыми встроенным устройством. Эти сообщения могут содержать конфиденциальную информацию, которая слабо защищена или вообще не защищена криптографическими средствами;

– атаки перебора (брутфорс). Этот тип атак направлен на криптографические алгоритмы, такие как шифры, также существуют атаки на пароли, которые осуществляются методом перебора словарей. В обоих случаях атаки перебора возможны только в том случае, если пространство поиска достаточно мало. Как уже было сказано выше, во многих встраиваемых устройствах слабая парольная политика и криптографические механизмы, поэтому атака перебора может нанести большой урон;

– использование уязвимостей. Многие злоумышленники используют эксплойты для уже известных уязвимостей во встраиваемых устройствах. Этот вид атак может использоваться для массовой атаки на устройства. Злоумышленники запускают ботнеты на основе уже зараженных устройств, эти устройства атакуют и заражают другие устройства, распространяясь как компьютерные черви.

Помимо вышеперечисленных атак злоумышленник может использовать какой-то незащищенный механизм, как если бы он был обычным пользователем. Например, злоумышленник может обращаться к файлам на встроенном устройстве точно так же, как и любой другой пользователь, если на нем нет механизма управления доступом [15].

2.3 Последствия атак на встраиваемые устройства

Последствия атак на встраиваемые устройства могут быть следующими:

– отказ в обслуживании. Наибольшее количество производимых атак приводит отказу в обслуживании, а именно к неисправностям, приводящим к частичному или полному прекращению работы встраиваемого устройства;

– исполнение вредоносного кода. Последствием атаки может быть выполнение на устройстве вредоносного кода, введенного злоумышленником. Это также включает в себя различные веб-скрипты и SQL-инъекции, что может изменить его поведение устройства;

– нарушение целостности. Результатом атак бывает нарушение целостности некоторых данных или исходного кода прошивки устройств. Это включает в себя изменение файлов и параметров конфигурации, а также приложений на устройстве;

– утечка информации. В некоторых случаях результат атаки — это несанкционированное получение злоумышленником некоторой информации;

– несанкционированный доступ. Многие атаки приводят к тому, что злоумышленник получает несанкционированный доступ к устройству. Это не только включает случаи, когда злоумышленнику, у которого нет доступа к устройству, удается логически его получить, но также и случаи, когда злоумышленник уже имея доступ, повышает привилегии;

– снижение уровня защищенности устройства. Злоумышленник своими действиями может привести к тому, что устройство будет использовать более слабые алгоритмы или политики безопасности, чем те, которые он фактически поддерживает [15].

3. Модель высокоинтерактивной системы, предназначенной для исследования поведения злоумышленника во встраиваемых устройствах

3.1 Требования к модели высокоинтерактивной системы, предназначенной для исследования поведения злоумышленника во встраиваемых устройствах

Требования:

– модель должна давать возможность получения представления об атакующем злоумышленнике (его возможностях и ресурсах);

– модель должна давать возможность мониторинга только той происходящей в ней сетевой и файловой активности, по которой можно получить представление об атакующем злоумышленнике;

– модель должна давать возможность оценить ущерб от произведенной атаки.

3.2 Модель высокоинтерактивной системы, предназначенной для исследования поведения злоумышленника встраиваемых устройствах

Высокоинтерактивная система для встраиваемых устройств является частным случаем высокоинтерактивных систем. Модель высокоинтерактивной системы, предназначенной для исследования поведения во встраиваемых устройствах приведена на рисунке 12.

Модель состоит из взаимосвязанных модулей, состоящих из компонентов, каждый из которых выполняет конкретную функцию. Функции каждого модуля и компонента будут описаны ниже.

На основе данной модели может быть создана высокоинтерактивная система, имитирующая роутер, камеру видеонаблюдения или любое другое встраиваемое устройство.

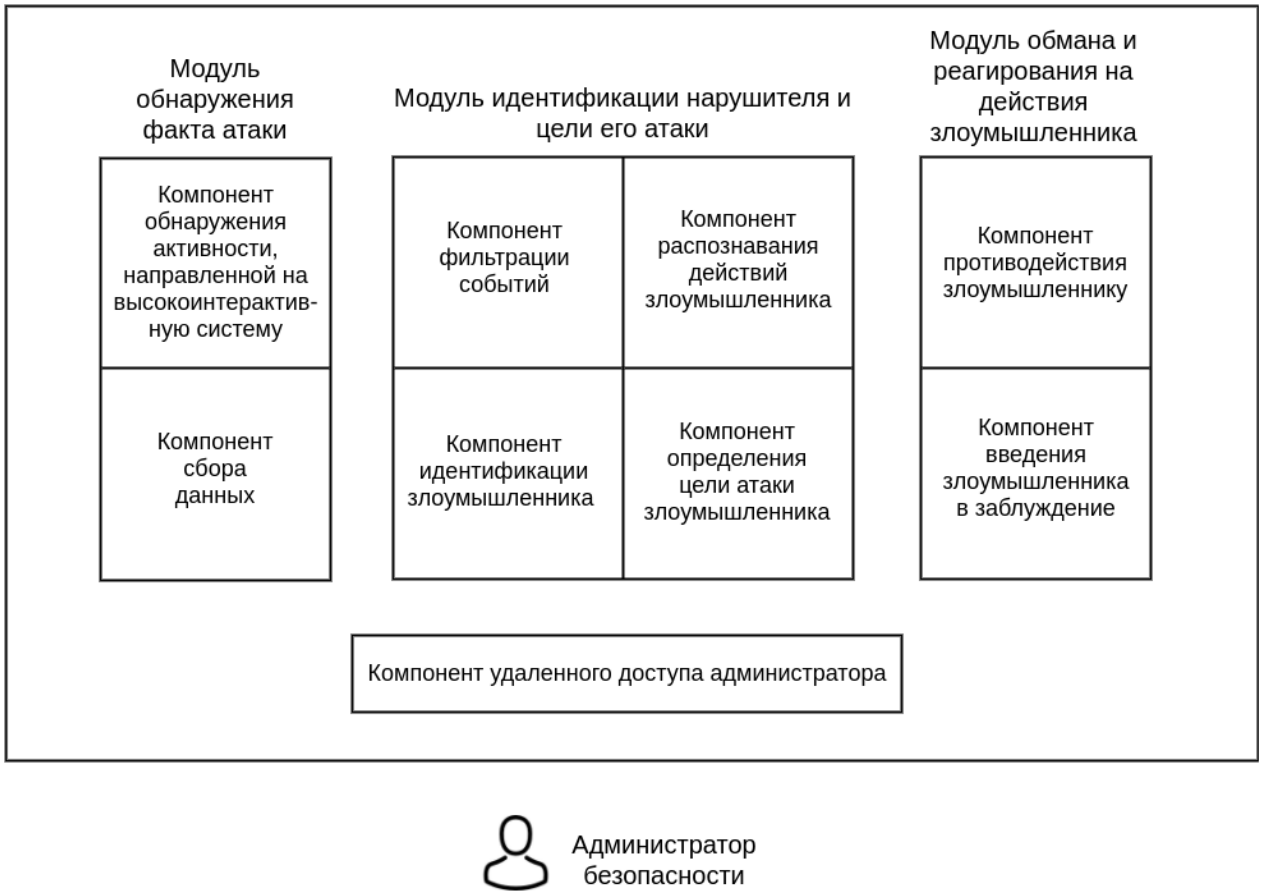

Рисунок 12 — Модель высокоинтерактивной системы для встраиваемых устройств

Модуль обнаружения факта атаки состоит из компонента обнаружения активности и компонента сбора данных. Компонент обнаружения активности, направленной на высокоинтерактивную системы, запускает компонент сбора данных. Компонент сбора данных записывает в журналы мониторинга всю активность, направленную на высокоинтерактивную систему.

В модуль идентификации нарушителя и цели его атаки входят следующие компоненты: фильтрации событий, идентификации злоумышленника, распознавания действий злоумышленника и определения цели атаки злоумышленника. В компоненте фильтрации событий из всей собранной предыдущим компонентом информации выделяется та, которая непосредственно связана с атаками на высокоинтерактивную систему. Компонент идентификации злоумышленника предназначен для описания возможностей и ресурсов злоумышленника, также на

основании этих данных может быть составлена модель нарушителя. В компоненте распознавания действий злоумышленника происходит идентификация всех его действий внутри сети, по которым можно определить его возможности и ресурсы. Компонент определения цели атаки злоумышленника основан на действии двух предыдущих компонентов и позволяет определить цель, на которую направлены действия злоумышленника.

Модуль обмана и реагирования на действия злоумышленника состоит из компонента противодействия злоумышленнику и компонента введения злоумышленника в заблуждение. Компонент противодействия злоумышленнику предназначен для блокирования его действий, направленных на высокоинтерактивную систему. Компонент введения злоумышленника в заблуждение используется для скрытия и/или подмены информации, по которой он может понять, что атакует honeypot, а не реальную систему, и динамического изменения конфигурации системы.

Компонент удаленного доступа администратора позволяет администратору безопасности следить за работой высокоинтерактивной системы и в случае необходимости вмешиваться.

3.3. Применение модели высокоинтерактивной системы для встраиваемых устройств

На основе модели высокоинтерактивной системы для встраиваемых устройств был создан прототип реальной высокоинтерактивной системы. При создании прототипа высокоинтерактивной системы для встраиваемых устройств был использован исходный код высокоинтерактивной системы Sysdig Falco в с открытым исходным кодом [8].

События, детектируемые высокоинтерактивной системой Sysdig Falco:

- запуск оболочки внутри контейнера;
- порождение дочернего процесса серверным;

– доступ к конфиденциальным файлам (например, /etc/shadow);
– запись посторонней информации в каталоги (например, в /dev);
– исходящие сетевые соединения.

Falco работает по правилам, определяющим события, которые должны детектироваться системой. Правила записываются на высокоуровневом, удобочитаемом для человека, языке. Таким образом можно адаптировать по-своему.

После развертывания Falco использует модуль ядра Sysdig и библиотеки пользовательского пространства для просмотра всех событий, происходящих в системе. Если происходит соответствующее правилу событие, то информация об этом записывается в журнал мониторинга. Это соответствует требованию о мониторинге только той сетевой активности, по которой можно получить представление о злоумышленнике. Исходя из целей, преследуемых установкой высокоинтерактивной системы, администратор безопасности или лицо, отвечающее за ее настройку, создает свой список правил, по которым будет работать высокоинтерактивная система.

Работоспособность прототипа высокоинтерактивной системы была проверена путем ее запуска на одноплатном компьютере Raspberry Pi 3. При проверке работоспособности системы была использована тестовая программа event_generator, генерирующая события от лица злоумышленника, тем самым имитирующая реальную атаку [19].

3.4 Анализ результатов применения модели высокоинтерактивной системы для встраиваемых устройств

Результаты работы прототипа приведены на рисунках 13 и 14.

На рисунке 13 приведены действия атакующего злоумышленника, которые генерируются программой event_generator.

Программа запускается следующим образом:

```
user@user:~$ docker start falco-event-generator
user@user:~$ docker attach falco-event-generator
```

```
***Action read_sensitive_file
Reading /etc/shadow...
***Action spawn_shell
Spawning a shell to run "ls > /dev/null" using system()...
***Action system_procs_network_activity
Becoming the program "sha1sum" and then performing network activity
***Action network_activity
Opening a listening socket on port 8192...
***Action system_user_interactive
Forking a child that becomes user=daemon and then tries to run /bin/
ogin...
login: must be suid to work properly
***Action user_mgmt_binaries
Becoming the program "vipw" and then running the program /bin/ls
NOTE: does not result in a falco notification in containers
***Action exec_ls
bin      home     media    proc     sbin     sys      var
dev      httpd    mnt      root     sha1sum  tmp      vipw
etc      lib      mysqld   run      srv      usr
***Action write_binary_dir
Writing to /bin/created-by-event-generator-sh...
***Action write_etc
Writing to /etc/created-by-event-generator-sh...
***Action write_rpm_database
Writing to /var/lib/rpm/created-by-event-generator-sh...
***Action change_thread_namespace
Calling setns() to change namespaces...
NOTE: does not result in a falco notification in containers, unless
ontainer run with --privileged or --security-opt seccomp=unconfined
***Action create_files_below_dev
Creating /dev/created-by-event-generator-sh...
***Action db_program_spawn_process
Becoming the program "mysql" and then spawning a shell
***Action spawn_shell
Spawning a shell to run "ls > /dev/null" using system()...
***Action exfiltration
Reading /etc/shadow and sending to 10.5.2.6:8197...
***Action mkdir_binary_dirs
Creating directory /bin/directory-created-by-event-generator-sh...
Could not create directory "/bin/directory-created-by-event-generato
-sh": File exists
```

Рисунок 13 — Результаты работы прототипа высокоинтерактивной системы

На рисунке 14 — реакция высокоинтерактивной системы на действия злоумышленника. При анализе событий можно заметить, что каждое действие злоумышленника детектируется высокоинтерактивной системой.

Программа запускается следующим образом:

```
user@user:~$ docker start falco
user@user:~$ docker attach falco
```

```
12:17:35.781219878: Warning Sensitive file opened for reading by non-
trusted program (user=root name=httpd command=httpd --action read_sen
sitive_file --interval 6 --once file=/etc/shadow parent=event_generat
or gparent=<NA> ggparent=<NA> gggparent=<NA>)
12:17:42.782153835: Notice A shell was spawned in a container with an
 attached terminal (user=root falco-event-generator (id=08800c953963)
 shell=sh parent=event_generator cmdline=sh -c ls > /dev/null termina
l=34835)
12:17:43.786439406: Notice Known system binary sent/received network
traffic (user=root command=sha1sum --action network_activity --interv
al 0 --once connection=127.0.0.1:8192)
12:17:44.787677304: Informational System user ran an interactive comm
and (user=bin command=login )
12:17:46.793249399: Error File below a known binary directory opened
for writing (user=root command=event_generator  file=/bin/created-by-
event-generator-sh)
12:17:47.793455312: Error File below /etc opened for writing (user=ro
ot command=event_generator  parent=<NA> file=/etc/created-by-event-ge
nerator-sh name=event_generator gparent=<NA> ggparent=<NA> gggparent=
<NA>)
12:17:48.793816944: Error Rpm database opened for writing by a non-rp
m program (command=event_generator  file=/var/lib/rpm/created-by-even
t-generator-sh)
12:17:49.794127985: Notice Namespace change (setns) by unexpected pro
gram (user=root command=event_generator  parent=<NA> falco-event-gene
rator (id=08800c953963))
12:17:50.794327262: Error File created below /dev by untrusted progra
m (user=root command=event_generator  file=/dev/created-by-event-gene
rator-sh)
12:17:51.797383508: Notice Database-related program spawned process o
ther than itself (user=root program=sh -c ls > /dev/null parent=mysql
d)
12:17:52.801505189: Warning Sensitive file opened for reading by non-
trusted program (user=root name=event_generator command=event_generat
or  file=/etc/shadow parent=<NA> gparent=<NA> ggparent=<NA> gggparent
=<NA>)
12:17:54.802369413: Error File below known binary directory renamed/r
emoved (user=root command=event_generator  operation=rename file=<NA>
 res=0 oldpath=/bin/true newpath=/bin/true.event-generator-sh )
12:17:54.802406624: Error File below known binary directory renamed/r
emoved (user=root command=event_generator  operation=rename file=<NA>
 res=0 oldpath=/bin/true.event-generator-sh newpath=/bin/true )
```

Рисунок 14 — Результат работы программы event-generator

Работоспособность высокоинтерактивной системы определяется по тому, может ли она детектировать любую активность внутри себя. По результатам работы данного прототипа видно, что вся активность злоумышленника детектируется высокоинтерактивной системой поэтому можно сделать вывод, что модель является адекватной и может быть использована для дальнейшей разработки реальной высокоинтерактивной системы для встраиваемых устройств.

Возможный ущерб от атаки злоумышленника можно оценить по ценности ресурсов, к которым он имел доступ.

Модель высокоинтерактивной системы будет требовать дальнейших доработок в связи с тем, что не прошло много времени с момента появления первых встраиваемых устройств и их конфигурация будет непрерывно совершенствоваться с течением времени, а также потому, что злоумышленники не стоят на месте и постоянно создают новые инструменты для атак и совершенствуют уже имеющиеся.

3.5 Рекомендации по разработке высокоинтерактивных систем для встраиваемых устройств

При разработке высокоинтерактивных систем наиболее важным является скрытие от злоумышленника всех артефактов системы, по которым он может определить, что это не реальная система, а высокоинтерактивная.

Большинство высокоинтерактивных систем работают в различных средах виртуализации, и это легко детектируется злоумышленником. Виртуальное оборудование должно быть достаточно похожим на физическое оборудование. Для скрытия этого факта необходимо подменять или удалять артефакты виртуальных машин. Примеры будут приведены ниже.

Для скрытия факта использования машины VMWare необходимо найти конфигурационный VMX файл, генерируемый на этапе создания машины, и в конец добавить строки:

```
isolation.tools.getPtrLocation.disable = «TRUE»
isolation.tools.setPtrLocation.disable = «TRUE»
isolation.tools.setVersion.disable = «TRUE»
isolation.tools.getVersion.disable = «TRUE»
monitor_control.disable_directexec = «TRUE»
monitor_control.disable_chksimd = «TRUE»
monitor_control.disable_ntreloc = «TRUE»
monitor_control.disable_selfmod = «TRUE»
monitor_control.disable_reloc = «TRUE»
monitor_control.disable_btinout = «TRUE»
monitor_control.disable_btmemspace = «TRUE»
monitor_control.disable_btpriv = «TRUE»
monitor_control.disable_btseg = «TRUE»
```

Эти действия призваны предотвратить детектирование злоумышленниками виртуального окружения через отслеживание адресного пространства памяти и счётчиков.

Помимо этого имеет смысл заменять поиском по реестру слова VMware/Virtual на Intel или IBM всё, что можно заметить, включая дисковые переменные.

Для скрытия факта использования среды виртуализации VirtualBox можно использовать дополнение VboxHardenedLoader. Это дополнение маскирует артефакты среды виртуализации VirtualBox или добавляет информацию, которой в средах виртуализации не бывает в отличие от реальных систем.

Информация, содержащаяся в среде виртуализации VirtualBox, которая заменяется дополнением VboxHardenedLoader на поддельную:

– информация о производителе, модели BIOS-а и материнской платы;
– модель и серийные номера хранителей информации;
– информация о производителе системы в ACPI таблице;

– физический адрес сетевого адаптера;

– данные об устройствах в системе;

– информация о графической подсистеме.

Помимо использования сред виртуализации возможно маскирование высокоинтерактивной системы под какое-либо устройство. Для этого можно делать следующие действия:

– подменять системные файлы с той целью, чтобы при использовании злоумышленником программ, определяющих тип системы или устройства, эти программы выводили заведомо ложные данные, введенные разработчиками;

– изменять выводы функций.

Учитывая все вышесказанное, можно прийти к выводу, что использование сред виртуализации и маскирование высокоинтерактивной системы под устройства достаточно трудоемкая задача. Наиболее оптимальным решением может быть использование устаревших встраиваемых устройств с искусственно добавленными уязвимостями и программами сбора информации о злоумышленнике.

4. Вредные психофизиологические факторы, влияющие на сердечно-сосудистую систему специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие

4.1 Вредные психофизиологические факторы, влияющие на сердечно-сосудистую систему специалиста по защите информации

По официальной статистике, ежегодно в России от сердечно-сосудистых заболеваний умирает около 1 млн. 300 тысяч человек, смертность по этой причине превышает половину числа всех смертей в стране. Россия лидирует по этому показателю среди развитых стран.

Одной из причин сердечно-сосудистых заболеваний является сидячий образ жизни, а работа специалиста по защите информации подразумевает долгое сидение за рабочим местом. Почему сидячий образ жизни так вреден? В основном потому, что положение сидя (или лежа) уменьшает нагрузку на сердечно-сосудистую систему, а также позволяет сердцу и кровеносным сосудам «расслабиться». В отличие от него, положение стоя вынуждает сердечно-сосудистую систему работать активнее, просто для поддержания нормального уровня артериального давления. Снижение исходного уровня сердечно-сосудистой деятельности, связанного с длительным сидением, может привести к относительной сердечной дезадаптации. Резкая перемена сидячего положения на стоячее может вызвать повышение артериального давление, что в некоторых случаях приводит к потере сознания.

Зачастую, люди, чья работа связана с сидячим образом жизни, страдают от плохой циркуляции крови в нижних конечностях, что приводит к развитию варикозного заболевания вен. При долгом сидении без смены положения сосуды пережимаются, кровь в них застаивается и не может двигаться как положено — вверх. Из-за этого стенки сосудов испытывают давление и когда оно становится избыточно высоким, кровь выталкивается и ее излишки растягивают вены. Но не столь опасно варикозное расширение вен, как являющийся её следствием

тромбофлебит, который ведет к образованию тромбов. Тромбы могут закупоривать вены образовывая флемботромбоз либо оторвавшись от стенки сосуда по кровотоку попасть в легкие. Это в большинстве случаев приводит к тяжёлым осложнениям, а иногда и к летальному исходу.

Помимо варикозного расширения вен сидячий образ жизни специалиста по защите информации опасен тем, что продолжительное отсутствие физической активности приводит к гипотоническим (пониженное артериальное давление) и гипертоническим (повышенное артериальное давление) заболеваниям.

4.2 Методы и средства физической культуры, снижающие их воздействие

Для снижения рисков от сидячего образа жизни необходимо заниматься физическими упражнениями, которые являются научно обоснованным методом профилактики заболеваний сердечно-сосудистой системы. Регулярные занятия физическими упражнениями уменьшают вероятность возникновения заболеваний органов кровообращения.

Для предотвращения и профилактики заболеваний сердечно-сосудистой системы физические упражнения рекомендуются всем, но особенно тем, у кого есть факторы риска, такие как сидячий образ жизни. В основном рекомендуются такие виды занятий, как гимнастические упражнения, бег, ходьба, плавание, ходьба на лыжах, туризм.

Гимнастические упражнения развивают мышечную силу, укрепляют связки, делают суставы более подвижными, совершенствуют координацию движений. Например, при гипотонической болезни силовые, скоростно-силовые и статические упражнения повышают артериальное давление, а при гипертонической болезни дыхательные упражнения и упражнения для мелких мышечных групп способствуют его снижению. Дыхательные упражнения и упражнения в расслаблении мышц также оказывают общее оздоровительное действие для всего организма.

Ходьба — основное средство в оздоровительной и лечебной физической культуре. Она является естественной для организма человека формой мышечной деятельности. Во время ходьбы в работу включается большинство мышц туловища, ног и рук. Поэтому людям, ведущим сидячий образ жизни рекомендуется больше передвигаться пешком, так как это самый доступный способ оздоровления организма, также не требующий практически никаких затрат.

В лечебных целях рекомендуется ходьба в медленном (от 60 до 70 шагов в минуту, скорость продвижения не более 3 км/ч), в среднем (от 80 до 100 шагов в минуту, скорость 4 км/ч) и в быстром (от 100 до 110 шагов в минуту, скорость 5 км/ч). Нежелательно ходить в более быстром темпе. В начале ходьбы следует делать более короткие шаги и держать медленный темп, затем шаг надо удлинять, а темп увеличивать. В время ходьбы необходимо следить за дыханием, а именно согласовывать его с шагами — выдох немного длиннее, чем вдох.

Следующее оздоровительное средство — бег. Бег помогает предупредить заболевания сердечно-сосудистой системы и нормализовать функции при начальных проявлениях болезни, повысить резервы организма. Однако это очень сильное средство, которое предъявляет значительные требования к опорно-двигательному аппарату, сердечно-сосудистой и дыхательной системам, поэтому при серьезных заболеваниях этих систем занятия бегом стоит отложить.

При многих заболеваниях сердечно-сосудистой системы можно подобрать такие скорость и длительность бега, которые не будут перегружать, но в то же время будут тренировать эту систему. Регулярные занятия бегом улучшают деятельность и других систем организма. Его лечебное действие заключается в том, что совершенствуются регулирующие системы (центральная и вегетативная нервные системы, эндокринная система). Помимо этого беговые тренировки повышают тонус парасимпатической системы (в покое снижается артериальное давление). В условиях жизни специалиста по защите информации волнения и стресс являются неотъемлемой частью его профессиональной деятельности и

повышают тонус симпатической нервной системы, а беговые тренировки уравновешивают взаимодействие этих систем.

Начинать занятия с лечебной целью следует с очень медленного бега — почти со скоростью ходьбы. Только через несколько месяцев занятий можно увеличивать темп, иначе можно вместо оздоровления причинить организму непоправимый вред. После бега рекомендуется выполнять ходьбу, упражнения на расслабление и растягивание мышц туловища и конечностей, а также дыхательные упражнения.

Ходьба на лыжах оказывает разнообразное воздействие на организм и включает в работу все мышечные группы, способствуя их укреплению, ускорению обмена веществ, улучшению функций дыхательной, сердечно-сосудистой и нервной систем, повышению физической работоспособности и закаливанию организма.

При занятиях ходьбой на лыжах стоит варьировать объем занятий в зависимости от температуры воздуха и силы ветра. При морозе и ветре продолжительность пребывания на воздухе необходимо сокращать. Наиболее благоприятными условиями занятий на лыжах является температура воздуха от минус 1 до минус 12° и сила ветра более 10 м/с.

При любом из вышеперечисленных занятий величину нагрузок необходимо дозировать по субъективным ощущениям занимающегося. Нагрузка не должна вызывать сильное утомление, а также необходимо следить за частотой сердечных сокращений (ЧСС), по которой можно судить о доступности физических нагрузок. Допустимый максимум ЧСС в зависимости от возраста определяется расчетом: для здоровых людей возраст вычитается из 220, для людей с факторами риска — из 200, а для людей, уже перенесших заболевания сердечно-сосудистой системы, — из 190.

Людям с активной фазой сердечно-сосудистых заболеваний не рекомендуются все вышеперечисленные занятия до момента выздоровления, а после

выздоровление необходимо дозировать нагрузки, чтобы не нанести вред ослабленному болезнью организму.

Результатом выполнения физических упражнений является повышение эффективности работы сердечно-сосудистой системы, повышение липопротеидов высокой плотности, или «хорошего» холестерина, и уменьшение триглицеридов в крови человека.

Можно сделать вывод, что имеет смысл уменьшить время, проводимое сидя, и перераспределить его на время, проводимое на ногах. Практически все люди могут извлечь пользу из регулярных занятий спортом, независимо от того, занимаются ли они спортом интенсивно или придерживаются умеренной оздоровительной нагрузки. Систематизированная физическая деятельность благотворно влияет на весь организм человека и, следовательно, помогает предотвратить большое количество проблем со здоровьем, в том числе снижает риск смертности от сердечно-сосудистых заболеваний.

Заключение

Активность злоумышленников, направленная на встраиваемые устройства, представляет большую опасность для пользователей устройств. Основная причина этого в том, что безопасность встраиваемых устройств находится на примитивном уровне. Одной из мер защиты могут быть высокоинтерактивные системы, предназначенные для исследования поведения злоумышленников.

Основной задачей дипломной работы было создание модели высокоинтерактивной системы, которая может стать основой для создания реальной высокоинтерактивной системы, имитирующей какое-либо встраиваемое устройство.

Были сформированы требования, которым должна соответствовать модель высокоинтерактивной системы для встраиваемых устройств и на основании требований построена модель высокоинтерактивной системы для встраиваемых устройств.

На основании вышеупомянутой модели с использованием исходного кода высокоинтерактивной системы Sysdig Falco был создан прототип высокоинтерактивной системы для встраиваемых устройств. По результатам работы прототипа был сделан вывод о том, что данная модель соответствует требованиям и может использоваться для разработки реальной высокоинтерактивной системы для встраиваемых устройств.

Результаты исследований по созданию модели высокоинтерактивной системы, предназначенной для исследования поведения злоумышленника во встраиваемых устройствах, использованы в научно-исследовательской работе по перспективам создания высокоинтерактивной системы, предназначенной для исследования поведения злоумышленника во встраиваемых устройствах. Акт о внедрении результатов ВКР приведен в приложении Д.

Таким образом, все пункты технического задания выполнены полностью.

Список используемых источников

1. И. В. Котенко, М. В. Степашкин. Обманные системы для защиты информационных ресурсов в компьютерных сетях // Труды СПИИРАН, Вып. 2, т. 1. — СПб.: СПИИРАН, 2004.

2. В. Кусков, М. Кузин, Д. Макрушин, Я. Шмелев, И. Грачев. Ловушки «интернета вещей» [Электронный ресурс]. — Режим доступа: https://securelist.ru/honeypots-and-the-internet-of-things/30874/ (дата обращения: 25.12.2017).

3. Honeything [Электронный ресурс]. — Режим доступа: https://github.com/omererdem/honeything (дата обращения: 26.12.2017).

4. Honeypot for TCP 32764 [Электронный ресурс]. — Режим доступа: https://github.com/knalli/honeypot-for-tcp-32764 (дата обращения: 26.12.2017).

5. Telnet IoT honeypot [Электронный ресурс]. — Режим доступа: https://github.com/Phype/telnet-iot-honeypot (дата обращения: 26.12.2017).

6. NodeJS honeypot [Электронный ресурс]. — Режим доступа: https://github.com/ianliu-johnston/nodeJS_honeypot (дата обращения: 26.12.2017).

7. IoT honeypot [Электронный ресурс]. — Режим доступа: https://github.com/mukund26/iot_honeypot (дата обращения: 26.12.2017).

8. falco [Электронный ресурс]. — Режим доступа: https://github.com/draios/falco (дата обращения: 26.12.2017).

9. Bluepot [Электронный ресурс]. — Режим доступа: https://github.com/andrewmichaelsmith/bluepot (дата обращения: 26.12.2017).

10. Детектим виртуалки [Электронный ресурс]. — Режим доступа: https://xakep.ru/2013/11/08/61563 (дата обращения: 26.12.2017).

11. N. Provos, T. Holz. Virtual Honeypots: From Botnet Tracking to Intrusion Detection – Addison Wesley Professional, 2007.

12. Lance Spitzner. Honeypots: Tracking Hackers. 2002. 480 с.

13. R. McGrew. Experiences with honeypot systems: Development, deployment, and analysis // System Sciences. 2006.

14. M. Nawrocki, M. Wählisch, Thomas C. Schmidt, C. Keil, J. Schönfelder. A Survey on Honeypot Software and Data Analysis // Freie Universität Berlin. 2016.

15. D. Papp, Z. Ma, L. Buttyan. Embedded Systems Security: Threats, Vulnerabilities, and Attack Taxonomy // Thirteenth Annual Conference on Privacy, Security and Trust (PST). 2015

16. Mirai BotNet [Электронный ресурс]. — Режим доступа: https://github.com/jgamblin/Mirai-Source-Code (дата обращения: 26.12.2017)

17. IoT_reaper: A Rappid Spreading New IoT Botnet [Электронный ресурс]. — Режим доступа: http://blog.netlab.360.com/iot_reaper-a-rappid-spreading-new-iot-botnet-en/ (дата обращения: 26.12.2017)

18. Security development lifecycle [Электронный ресурс] – Режим доступа: https://www.microsoft.com/en-us/sdl (дата обращения: 26.12.2017)

19. event-generator [Электронный ресурс]. — Режим доступа: https://github.com/draios/falco/tree/dev/docker/event-generator (дата обращения: 26.12.2017)

Приложение А

(обязательное)

Алгоритм работы высокоинтерактивной системы для встраиваемых устройств

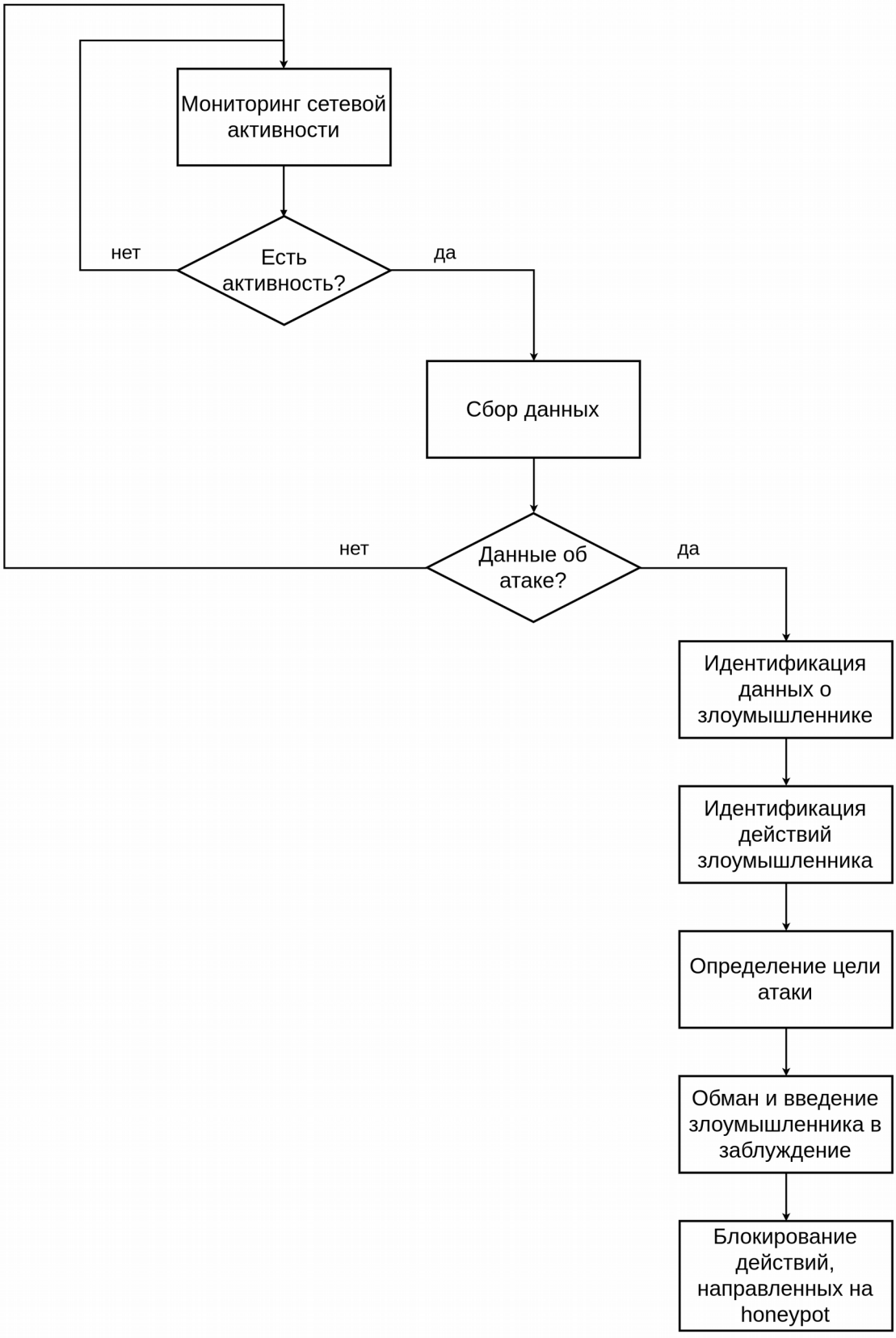
Мониторинг сетевой активности
Есть активность?
нет
да
Сбор данных
Данные об атаке?
нет
да
Идентификация данных о злоумышленнике
Идентификация действий злоумышленника
Определение цели атаки
Обман и введение злоумышленника в заблуждение
Блокирование действий, направленных на honeypot

Рисунок А.1

Приложение Б

(обязательное)

Схема вторжения злоумышленника в высокоинтерактивную систему

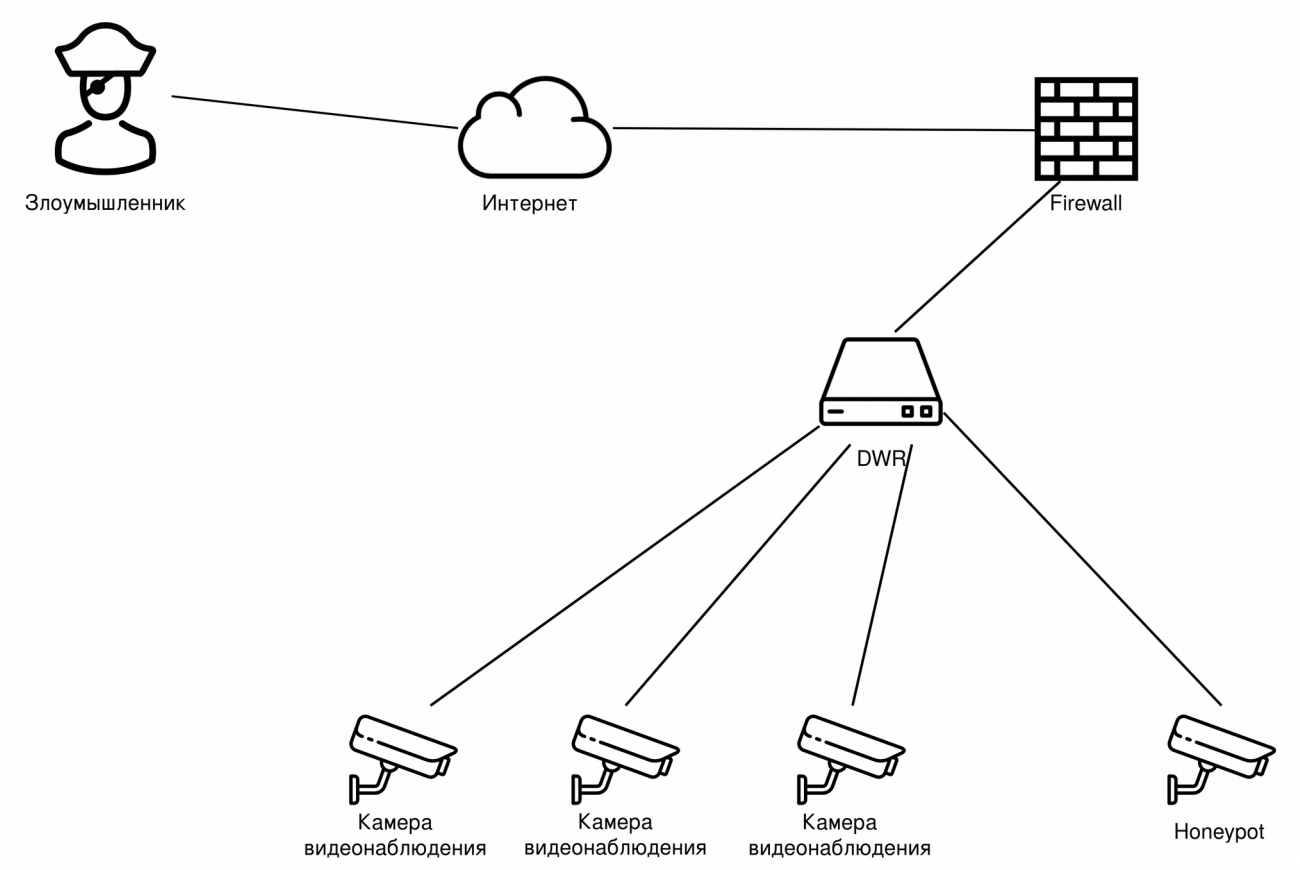
Злоумышленник
Интернет
Firewall
DWR
Камера видеонаблюдения
Камера видеонаблюдения
Камера видеонаблюдения
Honeypot

Рисунок Б.1

Приложение В

(обязательное)

Поведение злоумышленника в высокоинтерактивной системе

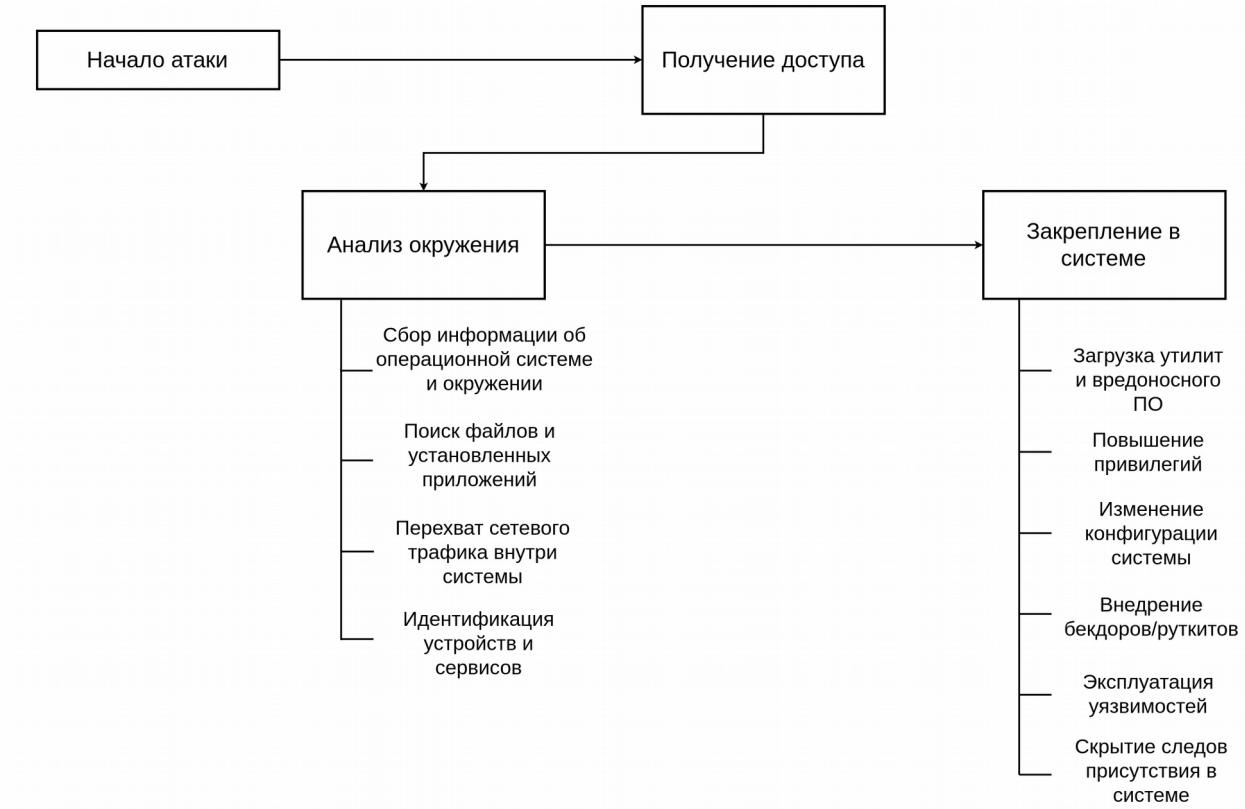
Начало атаки
Получение доступа
Анализ окружения
Закрепление в системе
Сбор информации об операционной системе и окружении
Поиск файлов и установленных приложений
Перехват сетевого трафика внутри системы
Идентификация устройств и сервисов
Загрузка утилит и вредоносного ПО
Повышение привилегий
Изменение конфигурации системы
Внедрение бекдоров/руткитов
Эксплуатация уязвимостей
Скрытие следов присутствия в системе

Рисунок В.1

Приложение Г

(обязательное)

Реагирование высокоинтерактивной системы на действия злоумышленника

Анализ окружения злоумышленником
Ответные действия системы
Сбор информации об операционной системе и окружении
Подмена названий и скрытие артефактов системы и окружения
Поиск файлов и установленных приложений
Переименование файлов и скрытие приложений
Перехват сетевого трафика внутри системы
Подмена сетевого трафика
Идентификация устройств и сервисов
Подмена названий и скрытые артефактов сервисов и устройств

Рисунок Г.1

Приложение Д

(обязательное)

Акт о внедрении

УТВЕРЖДАЮ

технический директор

ООО «Диджитал Секьюрити»

_____ Д.С. Евдокимов

«____»_____ 2017 г.

АКТ О ВНЕДРЕНИИ

результатов выпускной квалификационной работы

Губаревой В.А.

Комиссия в составе Ермолова А.В. (председатель), Селянина Д.Е. и Закирова Р.Т. постановила, что представленные в выпускной квалификационной работе результаты исследований по созданию модели высокоинтерактивной системы, предназначенной для исследования поведения злоумышленника во встраиваемых устройствах, использованы в научно-исследовательской работе по перспективам создания высокоинтерактивной системы, предназначенной для исследования поведения злоумышленника во встраиваемых устройствах.

Председатель комиссии:

руководитель проектов _____ А.В. Ермолов

Члены комиссии:

старший аналитик по информационной безопасности

_____Д.Е. Селянин

младший аналитик по информационной безопасности

_____Р.Т. Закиров

Приложение Е

(обязательное)

Протокол проверки ВКР в системе Антиплагиат