УДК 004.822:514

МОДЕЛИ И РЕАЛИЗАЦИЯ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ В КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ ПРЕДПРИЯТИЯ С ИСПОЛЬЗОВАНИЕМ ИНТЕЛЛЕКТУАЛЬНОГО ПОДХОДА

В.А. ВИШНЯКОВ, М.Г. МОЗДУРАНИ ШИРАЗ

Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь

Поступила в редакцию 2 декабря 2017

Аннотация. Приведена методика обнаружения вторжений в корпоративной информационной системе (КИС) по трем уровням. Представлены модели автономной и сетевой систем обнаружения вторжений (СОВ), включающие ряд компонент. Разработана и внедрена СОВ на базе инструментария Snort. В ходе исследований были выполнены задачи: построена виртуальная компьютерная сеть КИС; проанализированы возможные ее уязвимости; настроена и подготовлена к работе СОВ для КИС с использованием интеллектуального подхода (знания в виде правил); произведена проверка работоспособности СОВ путем моделирования различных атак и их обнаружения.

Ключевые слова: система обнаружения вторжений, методика, модель, правило, корпоративная система управления.

Abstract. The methodic of intrusion detection in corporate information systems (CIS) on three levels are done. Models of autonomic and net intrusion detection systems (IDS) including some components are presented. IDS on the base of Snort is worked out and used. During its investigation some tasks were executed: creating the virtual computer net for CIS, analyzing its possible vulnerability; attuning and preparing IDS for CIS with intellectual approach (knowledge in rules view); checking of IDS activity during simulation various attacks and their detection.

Keywords: intrusion detection system, methodic, model, rule, corporate management system.

Doklady BGUIR. 2017, Vol. 110, No. 8, pp. 79-84
Models and realization of intrusion detection in enterprise corporate information system with intellectual approuch
U.A. Vishniakou, M.G. Mosdurany Shiras

Введение

Система обнаружения вторжений – программное или аппаратное средство, предназначенное для выявления фактов неавторизованного доступа (вторжения или сетевой атаки) в компьютерную систему или сеть [1]. СОВ становятся необходимым дополнением инфраструктуры сетевой безопасности. В дополнение к межсетевым экранам (Firewall), СОВ участвуют в мониторинге подозрительной активности. Они могут обнаружить атакующих, которые обошли Firewall, и сформировать отчет об этом администратору сети, который предпримет дальнейшие шаги по предотвращению атаки. Технологии обнаружения проникновений не делают систему абсолютно безопасной, тем не менее практическая польза СОВ неоспорима.

Рост угроз вторжений вызывает необходимость совершенствования подходов и методов обеспечения информационной безопасности в средах облачных вычислений, поиска новых решений в области создания систем защиты информации (СЗИ). Вместе с традиционными средствами защиты, такими как антивирусы, детекторы уязвимостей, межсетевые экраны и детекторы вторжений, применяются средства автоматизации защиты, включающие корреляторы событий, программы обновлений, средства аутентификации, авторизации и администрирования, системы управления рисками. Интеллектуальные СЗИ для обнаружения вторжений в качестве интеллектуального инструмента используют нейронные сети, системы нечеткой логики и экспертные системы [3].

Методика и модели обнаружения вторжений

Методика работы по уровням. Рассмотрим модели СОВ для различных уровней КИС, их достоинства и недостатки [1, 2]. Системы обнаружения атак прикладного уровня собирают и анализируют информацию от конкретных приложений, например, от систем управления базами данных, веб-серверов или межсетевых экранов. Достоинства этого подхода: он позволяет обнаруживать атаки, пропускаемые средствами, которые функционируют на других уровнях, снизить требования к ресурсам за счет контроля не всех приложений, а только одного из них. Недостатки: уязвимости прикладного уровня могут подорвать доверие к обнаружению атак на данном уровне; атаки, проводимые на нижних уровнях сети и операционной системы (ОС), остаются за пределами рассмотрения данных средств.

Системы обнаружения вторжений уровня ОС собирают и анализируют информацию, отражающую ее деятельность в форме журналов регистрации. Достоинства подхода: системы данного класса могут контролировать доступ к информации в виде «кто получил доступ и к каким ресурсам»; появляется возможность отображения аномальной деятельности конкретного пользователя для любого приложения, отслеживания изменений режимов работы, связанных со злоупотреблениями; работа в сетевом окружении, в котором используется шифрование. Появляется способность работать в коммутируемых сетях и возможность контроля конкретного узла, подтверждение «успешности» или «неудачности» атаки, обнаружение атак, пропускаемых средствами, функционирующими на другом уровне, а также возможность проведения автономного анализа.

Недостатки подхода: уязвимости прикладного уровня могут подорвать доверие к обнаружению атак на этом уровне; атаки, проводимые на нижних или более высоких уровнях, остаются за пределами рассмотрения данных средств; запуск механизмов аудита для фиксирования всех действий в журналах регистрации может потребовать выделения дополнительных ресурсов; метод зависит от конкретной платформы; расходы на эксплуатацию и управление процессом обнаружения атак уровня ОС выше, чем при других подходах; средства данного класса неприменимы для обнаружения атак на маршрутизаторы и другое сетевое оборудование; при недостатке данных эти системы могут «пропускать» отдельные атаки.

Системы обнаружения вторжений уровня сети собирают информацию из сетевого трафика. Выполняться эти системы могут как на обычных компьютерах, так и на специализированных (Cisco IDS, AirDefense Server Appliance) или интегрируются в маршрутизаторы или коммутаторы (Cisco IOS Firewall Feature Set, Cisco IDS blade, Cisco Catalyst 6500 IDS Module). В первых двух случаях анализируемая информация собирается посредством захвата и анализа пакетов, при этом обращение к сетевым интерфейсам осуществляется в беспорядочном (promiscuous) режиме .

Достоинства СОВ: данные поступают без каких-либо специальных требований для механизмов аудита, использование систем не оказывает влияния на источники данных. Системы могут контролировать и обнаруживать следы атаки типа «отказ в обслуживании» и одновременно большое число узлов сети. СОВ имеют низкую стоимость эксплуатации, характеризуются трудностью скрытия следов для злоумышленника, обнаруживают атаки в реальном масштабе времени и подозрительные события. Им присуще обнаружение атак, пропускаемых средствами, функционирующими на других уровнях, независимость от используемых в организации ОС и прикладного программного обеспечения.

Недостатки СОВ: атаки, реализуемые на более высоких уровнях, остаются за пределами рассмотрения данных средств; системы данного класса неприменимы в сетях, использующих канальное и прикладное шифрование; системы неэффективно работают в коммутируемых сетях; существенно зависят от конкретных сетевых протоколов; подходы к мониторингу на сетевом уровне не могут работать на высоких скоростях.

Модели. Все системы обнаружения атак можно разделить на две категории − автономные и клиент-серверные системы [1, 2]. Первые выполняют сбор информации, ее анализ и реагирование на одном компьютере. Системы второй категории строятся по иному принципу. В наиболее критичных точках корпоративной сети устанавливаются агенты системы обнаружения атак (модули слежения, сенсоры), которые отвечают за выявление атак и реагирование на них. Все управление осуществляется с центральной консоли, на которую также передаются все сигналы тревоги. Модель автономной системы обнаружения атак может быть представлена кортежем *MIDSa = (IM, MM, WH, KB, MID, GI, MR)*, где *IM* – модуль работы с

источником информации, отвечает за взаимодействие с журналом регистрации, сетевой картой или ядром ОС для получения данных, на основе которых делается вывод о наличии или отсутствии атаки; *MM* – модуль управления, служит для управления компонентами системы обнаружения атак и обеспечения взаимодействия между ними; *WH* – хранилище данных, является журналом регистрации, в котором содержится информация о зафиксированных атаках и подозрительных событиях; *KB* – база знаний, может быть как локальной, так и клиент-серверной, содержит информацию, на основании которой принимается решение о том, зафиксирована ли атака в записях выбранного источника или нет. В зависимости от используемых методов анализа эта база знаний может хранить сигнатуры атак или профили пользователей и т. д.; *MID* – модуль обнаружения атак, выполняет сопоставление правил базы знаний с записями выбранного источника; *GI* – графический интерфейс, облекает всю работу системы обнаружения атак в удобную для администратора форму. При помощи графического интерфейса осуществляется как управление, так и сбор информации от всех компонентов системы обнаружения атак; *MR* – модуль реагирования, оповещает о вторжении и записывает его в журнал регистрации. В том случае, если система обнаружения атак построена как автономный агент, то все указанные модули находятся на одном компьютере.

Если система разработана с учетом архитектуры «клиент-сервер», то в ней выделяются два основных уровня – сенсор (sensor) и консоль (console). Сенсор отвечает за обнаружение и реагирование на атаки, а также за передачу сведений об обнаруженных несанкционированных действиях на консоль управления. Модель системы обнаружения атак может быть представлена кортежем *MIDSs* = (*MS, MC*), где *MS* − модель сенсора; *MC* − модель консоли. Модель сенсора представим в виде шестерки: *MS* = (*IM, MM, WH, KB, MID, MR*).

Сенсор обычно запускается на компьютере как сервис или daemon и работает круглосуточно. Поскольку оповещение об атаках передается сенсором на консоль, то модуль графического интерфейса, отображающий эти данные, в сенсоре отсутствует. Консоль предназначена для управления сенсорами и сбора информации от всех сенсоров, подключенных к ней. Ее модель представим в виде тройки: *MC* = (*MM, WH, GI*).

Одна консоль может координировать большое число сенсоров, так же как и сенсор может посылать информацию сразу на несколько консолей, реализуя их резервирование. По такому принципу построены системы RealSecure Network Sensor и Cisco IDS. Для того чтобы две консоли одновременно не смогли изменять настройки удаленного сенсора, одной из них присваивается специальный статус. Только консоли, имеющей указанный статус, предоставлено право на изменение конфигурации сенсоров и выполнение над ними других операций. В основе данного механизма лежат принципы, похожие на заложенные в межсетевой экран Check Point Firewall, согласно которым в один момент времени только один администратор может подключиться к межсетевому экрану с правами Read/Write. Все остальные администраторы работают исключительно в режиме Read.

В хранилище данных содержится информация, полученная от всех сенсоров, на консоли отсутствуют модули, отвечающие за получение данных из источников информации, их анализ и реагирование на атаки. Все перечисленные функции возложены на сенсоры. Сделано это с той целью, чтобы в случае выхода из строя консоли или канала связи между консолью и сенсором функционирование последних никак бы не нарушалось. В этом случае сенсоры продолжают работать в автономном режиме, по-прежнему обнаруживая атаки и реагируя на них. Как только соединение с консолью восстанавливается, сенсоры посылают ей всю накопленную информацию.

Моделирование системы выявление вторжений

Конфигурирование системы. Рассмотрим реализацию вышеприведенных методов и моделей в сетевой структуре. Для моделирования СОВ была создана сеть из нескольких виртуальных машин (ВМ), на них установлены ОС Windows и Linux. Рассмотрим пошагово этапы моделирования сети с использованием выбранного программного средства виртуализации − продукт VMware Workstation [3]. Данная программа компании VMware VMware Workstation позволяет установить на ВМ более 200 различных типов ОС, в числе которых DOS, Windows, Linux, FreeBSD, Netware, Solaris и Virtual Appliances [3]. Также в данном программном решении предусмотрен удобный перенос виртуальной машины на любую среду виртуализации от компании

VMware (например, vSphere или ESXi), что позволяет протестировать возможности проверяемого объекта на больших мощностях по сравнению со стандартной клиентской рабочей станцией.

Создаем клиентский персональный компьютер под управлением ОС Windows 7 (далее – ВМ 1). Выбираем конфигурацию Custom для более эффективного распределения и использования ресурсов локальной рабочей станции, указываем аппаратную совместимость создаваемой ВМ с другими продуктами VMware. Определяем место или устройство, с которого будет производиться установка ОС. Это возможно как с внешнего привода компьютера, так и из образа на жестком диске. Указывается имя гостевой ОС и тип загрузочного диска. После этого конфигурируется процессор. Для стабильного функционирования системы достаточно одного двухъядерного процессора.

Следующим пунктом установки идет определение объема оперативной памяти рабочей станции. Учитывая минимальные системные требования Windows 7 и цели проведения испытаний, объем памяти с рекомендуемого минимума был поднят до 2 Гб. Указываем контроллеры ввода/вывода (выбираем рекомендуемые), тип жесткого диска и его объем. Разделим виртуальный диск на несколько файлов, чтобы упростить перемещение ВМ с одной локальной рабочей станции на другую. Полученная конфигурация может быть изменена непосредственно перед окончательным завершением создания тестового стенда. Можно удалить принтер или звуковую карту, перераспределить выделенные ресурсы или добавить новые устройства.

Аналогичным образом созданы еще две виртуальные машины под управлением ОС Debian. Одна система будет использоваться непосредственно для функционирования СОВ Snort (далее – ВМ 2), а вторая будет предполагаемым атакующим с установленным дистрибутивом Kali Linux 2017.1 (далее – ВМ 3). Пропишем настройки сети на каждой ВМ, чтобы они могли взаимодействовать друг с другом. IP-адреса были назначены согласно таблице.

Соответствие между виртуальными машинами и IP-адресами

Виртуальная машина	Операционная система	IP-адрес	Маска подсети
ВМ 1	Windows 7 x64 Ultimate	192.168.17.128	255.255.255.0
ВМ 2	Debian 8.7.1	192.168.17.151	255.255.255.0
ВМ 3	Kali Linux 2017.1	192.168.17.136	255.255.255.0

Для правильного функционирования и корректной установки СОВ Snort проводится настройка ВМ путем выполнения ряда команд. Создаем структуру папок для размещения конфигурации Snort, новые файлы для «черных» и «белых» списков и локальных правил, изменяем правила доступа к новым директориям и копируем конфигурационные файлы из директории, в которую мы загрузили их.

Правила для СОВ. Snort предлагает 3 пакета правил: правила для сообщества, правила для зарегистрированных пользователей и правила для подписчиков. Загрузка и установка правил для сообщества осуществляется командами. Загрузка и установка правил для сообщества осуществляется следующими командами:

– wget https://www.snort.org/rules/community -O ~/community.tar.gz;

– sudo tar -xvf ~/community.tar.gz -C ~/;

– sudo cp ~/community-rules/* /etc/snort/rules;

– sudo sed -i 's/include \$RULE_PATH/#include \$RULE_PATH/' /etc /snort/snort.conf.

Для загрузки правил (зарегистрированные пользователи) используются команды:

– wget https://www.snort.org/rules/snortrules-snapshot-2976.tar.gz?oink-code=<oinkcode> -O ~/registered.tar.gz;

– sudo tar -xvf ~/registered.tar.gz -C /etc/snort.

Как только все конфигурационные файлы и файлы правил сформированы, прописываем пути к ним в конфигурационном файле snort.conf и осуществоям первый запуск. Для этого открываем вышеуказанный файл и редактируем пути к правилам:

– sudo nano /etc/snort/snort.conf;

– var RULE_PATH rules;

– var SO_RULE_PATH so_rules;

– var PREPROC_RULE_PATH preproc_rules;

– var WHITE_LIST_PATH /etc/snort/rules;

– var BLACK_LIST_PATH /etc/snort/rules;

– include $RULE_PATH/local.rules.

Приступаем к тестовому запуску Snort. Для этого нужно выполнить следующую команду: sudo snort -T -c /etc/snort/snort.conf.

Ключи запуска СОВ многообразны, каждый может изменять настройки файла snort.conf. Snort может быть запущен в четырех режимах:

1 Режим сниффера – перехват и чтение пакетов из сети и отображение их на экране в виде продолжительного потока в консоли.

2. Режим пакетного журналирования – чтение пакетов из сети и запись их на диск в так называемый log-файл.

3. Обнаружение вторжений – Snort анализирует сетевой трафик и выполняет какие-либо действия в зависимости от вида атак.

4. Режим работы совместно с МСЭ iptables.

Настройка и тестирование. Настроим МСЭ для взаимодействия со Snort [4]. Рассмотрим одно из существующих аномальных правил. Предположим, что злоумышленник решил выявить уязвимость компьютеров сети путем сканирования их портов. Утилитой с такими возможностями является Nmap, которая предназначена для настраиваемого сканирования IP-сетей с любым количеством объектов. Для проверки работоспособности СОВ просканируем компьютер с ip-адресом 192.168.17.151 «невидимым» FIN методом. Для этого введем команду nmap -sF 192.168.17.151. После просмотра файла alert с предупреждениями обнаруживаем, что СОВ обнаружила сканирование портов с указанием IP-адресов сканирующей и сканируемой машины. Также в этом файле указана ссылка на сайт с подробным описание атаки. Правила, отвечающие за выявление атак, связанных со сканированием портов, хранятся в файле «scan.rules».

Для тестирования СОВ на предприятии перенесем созданную ранее сеть из нескольких ВМ на виртуальный сервер, развернутый на базе программного продукта VMware vSphere. Основная область применения vSphere – платформа виртуализации для облачных вычислений. Несмотря на это, данный продукт также применяется не только в вычислительных целях, но и в качестве мощного исследовательского инструмента. После переноса сети вновь запускаем ВМ и приступаем к непосредственному процессу испытаний.
В качестве экспериментального теста осуществлена DoS-атака на компьютер под управлением Windows 7, находящийся в созданной подсети. После завершения атаки проверяем наличие изменений в log-файлах Snort. При открытии файла сделанное предположение подтверждается: система зафиксировала атаку на подчиненную ВМ. Журнал содержит огромное количество записей, свидетельствующих о том, что была реализована атака SYN Flood.

Можно сделать вывод о том, что СОВ справилась с задачей обнаружения вторжения в КИС предприятия, вплоть до подробного протоколирования атаки со стороны злоумышленника. Как и в случае с FIN-сканированием при помощи утилиты Nmap, СОВ не только зафиксировала атаку, но и отобразила подробную информацию о том, с какого адреса велась атака, использованные пакеты, протоколы, а также указала ссылки на интернет-ресурсы, где можно получить более полные сведения о подобной атаке.

Заключение

1. Представлены модели систем обнаружения атак по различным уровням КИС (прикладной, ОС, сети), рассмотрены их достоинства и недостатки. Модель системы обнаружения

атак включает 7 компонент: модуль работы с источником информации, хранилище данных, база знаний, графический интерфейс, три модули (управления, обнаружения атак, реагирования).

2. С целью повышения надежности защиты информации в корпоративной сети предприятия была разработана и внедрена система обнаружения вторжений на базе СОВ Snort. Для осуществления поставленной цели в ходе работы были выполнены задачи: смоделирована виртуальная компьютерная сеть; проанализированы возможные ее уязвимости; настроена и подготовлена к работе СОВ в данную виртуальную сеть; произведена проверка работоспособности СОВ путем моделирования различных атак и зондирований сети.

3. Смоделированная СОВ может эффективно использоваться для обеспечения защиты информации и контроля данных в КИС для малых и средних предприятий, имеющих в своем составе локальную вычислительную сеть.

Список литературы

1. IDS/IPS – Системы обнаружения и предотвращения вторжений [Электронный ресурс]. – Режим доступа : http://www.netconfig.ru/server/ids-ips/. – Дата доступа: 12.11.2017.
2. Вишняков В.А. Информационная безопасность в корпоративных системах, электронной коммерции и облачных вычислениях: методы, модели, программно-аппаратные решения. Минск: Бестпринт, 2016. 276 с.
3. Официальный сайт компании VMware [Электронный ресурс]. – Режим доступа: https://www.vmware.com/ru.html. – Дата доступа: 12.10.2017.
4. McAfee Network Security Manager [Электронный ресурс]. – Режим доступа: http://www.mcafee. com/ru/ products/network-security-manager.aspx. − Дата доступа: 17.09.17.

References

1. IDS/IPS – Intrusion detection and protection systems [Electronic data]. – Access mode: http://www.netconfig.ru/server/ids-ips/. – Date of access: 12.11.2017.
2. Vishnjakov V.A. Informacionnaja bezopasnost' v korporativnyh sistemah, jelektronnoj kommercii i oblachnyh vychislenijah: metody, modeli, programmno-apparatnye reshenija. Minsk: Bestprint, 2016. 276 s. (in Russ.)
3. Oficial site of VMware company [Electronic data]. – Access mode: https://www.vmware.com/ru.html. – Date of access: 12.10.2017.
4. McAfee Network Security Manager [Electronic data]. – Access mode: http://www.mcafee. com/ru/ products/network-security-manager.aspx. − Date of access : 17.09.17.

Сведения об авторах

Вишняков В.А., д.т.н., профессор, профессор кафедры защиты информации Белорусского государственного университета информатики и радиоэлектроники.

Моздурани Шираз М.Г., аспирант кафедры защиты информации Белорусского государственного университета информатики и радиоэлектроники.

Адрес для корреспонденции

220013, Республика Беларусь,
г. Минск, ул. П. Бровки, д. 6,
Белорусский государственный университет информатики и радиоэлектроники
тел. +375-17-245-75-69;
e-mail: vish2002@mail.ru
Вишняков Владимир Анатольевич

Information about the authors

Vishniakou U.A., D. Sci., professor, professor of information security department of Belarussian state university of informatics and radioelectronics.

Mosdurany Shiras M.G., PG student of information security department of Belarussian state university of informatics and radioelectronics.

Address for correspondence

220013, Republic of Belarus,
Minsk, P. Brovki st., 6,
Belarussian state university
of informatics and radioelectronics
+375-17-245-75-69;
e-mail: vish2002@mail.ru
Vishniakou Uladzimir Anatolievich