ВЫЯВЛЕНИЕ ПОДОЗРИТЕЛЬНОЙ АКТИВНОСТИ В РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СЕТЯХ С ИСПОЛЬЗОВАНИЕМ ПЕРСПЕКТИВНОЙ ТЕХНОЛОГИИ СЕТЕЙ ПРИМАНОК (HONEYNET)

Максин И.С.,
Россия, г. Шуя

Автоматизация различных видов деятельности организации на концептуальной платформе корпоративной информационной среды (КИС) обеспечивает рациональную интеграцию информационных и вычислительных ресурсов и позволяет создать мощную сетевую инфраструктуру, отвечающую требованиям международных стандартов. Одновременно с усилением зависимости от информационных и коммуникационных технологий (ИКТ), существенно возрастает уязвимость по отношению к угрозам информационной безопасности (ИБ). Ослабление внимания к вопросам организации и совершенствования защиты сетевой инфраструктуры, как показывает практика, неизбежно ведет к нарушению нормальной деятельности учреждения и к существенным экономическим потерям.

Традиционные методы защиты информации (ЗИ) в большей мере ориентированы на защиту от конкретных видов угроз и атак и, как правило, реализуются в виде набора программных и аппаратных компонентов, функционирующих относительно независимо друг от друга; характеризуются неразвитыми адаптационными возможностями, пассивными механизмами обнаружения атак, большим процентом ложных срабатываний, значительной деградацией трафика целевых информационных потоков из-за большого объема ресурсов, выделяемых на защиту, и т. п. [1]

Для решения проблемы информационной безопасности многие исследователи сосредоточили внимание на развитии системы обнаружения вторжений (IDS) и системы предотвращения вторжений (IPS). Чтобы создать

эффективный механизм защиты ресурсов сети, нужно ясно представлять концептуальную модель вторжения и используемые злоумышленником методы. Идентификация и описание процесса вторжений с помощью детально разработанного механизма мониторинга – один из наиболее продуктивных подходов, в котором точное и ясное понимание логики и действий злоумышленника – основание для создания более сильной и прочной IDS. Это также является ключом к обеспечению оптимальной информационной защиты и достижению целей создаваемой системы безопасности. Подробно процесс вторжения представлен на рисунке ниже. [2]

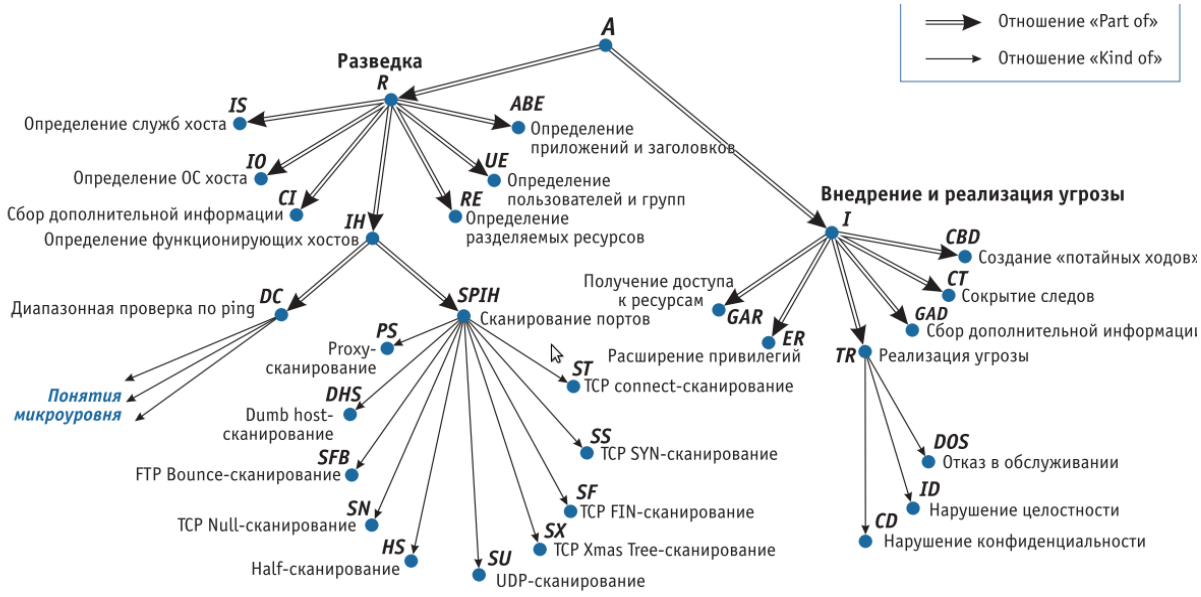

Рис. 1. Реализация вторжения

Чтобы улучшить производительность IDS и уменьшить информационные потери и риски, требуется идентифицировать непосредственно сам процесс вторжения.

Принимая во внимание то, что вторжение может проходить в несколько этапов, а на каждом этапе используются различные техники (см. рис. 1), рационально применять многоуровневую IDS, основанную на распределенной многоагентной сети Honeynet (HN) для решения проблемы сетевой безопасности. В такой модели обнаружение вторжений основано на

оптимальном распределении агентов на каждом уровне КВС. Большинство атак обнаруживается по распределенным каналам или происходит по организованному сценарию. Поэтому перспективные IDS должны обладать возможностью больших систем и давать свидетельство вторжения на основе объединенной информации от распределенных агентов.

Автоматизация системы защиты информации на основе многоагентной технологии HN, позволит снять с администраторов безопасности часть операций по мониторингу объекта защиты и перенастройке системы ЗИ. Автоматизация процесса окончательной настройки средств ЗИ позволит эффективно осуществлять перенастройку системы ЗИ в соответствии с изменениями объекта защиты и топологии сети. [3]

Honeynet (HN) – это сеть из ресурсов (т. н. Honeypot), представляющих собой приманку для злоумышленников, которая должна подвергнуться атаке или несанкционированному исследованию, что впоследствии позволит изучить стратегию злоумышленника и определить перечень средств противодействия вторжению. HN имитирует часть сетевой инфраструктуры КВС с признаками повышенной уязвимости, что и привлекает злоумышленника. Цель развертывания HN – сбор информации о вторжениях в интересах выявления точной картины вторжения. Любая активность на компонентах HN считается заведомо не авторизованной и требует последующего анализа. Этот подход позволяет существенно повысить эффективность защиты информации в сети.

Компоненты многоагентной системы HN представляют собой систему интеллектуальных агентов защиты, развернутые в среде виртуализации, реализующие определенные функции с целью обеспечения требуемого класса защищенности. Интеллектуальностью в данном случае является способность агента самостоятельно выполняющая задание, указанное администратором или агентом защиты более высокого уровня, в течение длительных промежутков времени [4].

Программная реализация такого подхода представляет собой комплекс программного обеспечения (ПО) развернутый в среде виртуализации, что

делает его наиболее гибким и масштабируемым. Комплекс поставляется в виде образа виртуальной машины (OVA) с ОС Linux и предустановленным и настроенным ПО. В состав ПО входят: Kojoney SSH и Kippo SSH приманки, Dionaea honeypot, интерактивная низкоуровневая приманка Honeyd, Thug honeyclient для анализа атак и др. Помимо этого, комплекс содержит предварительно настроенные скрипты для визуализации и обработки данных - Kippo-Graph, Honeyd-Viz, а также полный комплект анализа и экспертизы средств защиты и системы сетевого мониторинга, такие как NTOP, p0f, Etherape, Nmap, DFF, Wireshark, ClamAV, Ettercap, Automater, UPX, PDFTK, Flasm, PDF- парсер, Pyew, dex2jar и многое другое.

Предлагаемый комплекс устанавливается на любой компьютер в сегменте КВС и настраивается под соответствующие требования топологии сегмента. Полнофункциональные скрипты для визуализации Kippo-Graph и Honeyd-Viz представляют данные полученные от Kippo SSH и Honeyd в удобном для администратора виде по средствам веб-интерфейса. На случай появления подозрительной активности комплекс содержит богатый набор инструментов описанный выше. Более подробно с комплексом можно ознакомится по адресу bruteforce.gr.

Внедрение подобных систем, входящих в состав комплекса интегрированной защиты сетевых ресурсов следует считать обоснованным и перспективным направлением для дальнейшего исследования. Внедрение HN несет в себе не только усиление защиты систем, но и возможность глубокого изучение инцидентов политики ИБ.

Литература

1. *Надеждин Е.Н., Шептуховский В.А., Максин И.С.* Проблемные вопросы создания защищённой корпоративной информационной образовательной среды // Информационная среда образования и науки. 2011. Вып. 5. URL: http://www.iiorao.ru/iio/pages/izdat/ison/publication/ison_2011/num_5_2011 (дата обращения: 18.11.2013).

2. *Максин И.С., Малышев В.А.* Концепция многоагентных систем автоматизированной поддержки интегрированной защиты сетевых ресурсов информационной образовательной среды региона // Материалы V международной научно-методической конференции «Шуйская сессия студентов, аспирантов, молодых ученых». Шуя, 2012.

3. *Максин И.С., Малышев В.А.* Распределённая динамическая honeynet («сеть-ловушка») на основе скрытой модели Маркова // Материалы VI международной конференции «Параллельные вычисления и задачи управления». М.: ИПУ РАН, 2012.

4. *Хусни, Афанасьев С.В.* Архитектура и моделирование Honeynet // Проблемы информационной безопасности. Компьютерные системы. СПб., 2008.