Р.А.БОЖКО[1], М.В.КОЛОСОВА[2], Т.А.ПУЛКО[3]

КОМПЛЕКС ДЛЯ АНАЛИЗА ЗАЩИЩЕННОСТИ ХОСТОВ В СЕТИ ИНТЕРНЕТ

[1]Учреждение образования «Белорусская государственная академия связи», г. Минск, Республика Беларусь, начальник военной кафедры

[2]Учреждение образования «Белорусская государственная академия связи», г. Минск, Республика Беларусь, методист учебной части военной кафедры

[3]Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь, доцент кафедры защиты информации, кандидат технических наук, доцент

Важнейшей проблемой нашего времени становится информационная безопасность. Важным этапом обеспечения информационной безопасности является идентификация потенциальных рисков. Имеется большое количество материалов, посвященных проведению анализа защищенности Веб-приложений. Например, библиотека документов OpenWebApplicationSecurityProject (OWASP), содержащая полное руководство по поиску всевозможных уязвимостей, их классификацию, рекомендации к процессу проведения анализа защищенности. Интересен открытый стандарт OpenSourceSecurityTestingMethodologyManual (OSSTMM), который рассматривает анализ защищенности Веб-приложений в контексте комплексного процесса проведения тестирования на проникновение. Кроме того, для этой цели были созданы сканеры безопасности, которые требуют финансовых вложений. Более доступным способом является создание с помощью общедоступного программного обеспечения комплексов для анализа защищенности хостов. Комплекс может состоять из следующих модулей.

Модуль сетевого сканирования предоставляет единый интерфейс для запуска сетевого сканера. Пользователь выбирает один из заданных режимов сканирования, задает цели сканирования и далее происходит передача требуемых параметров на вход внешнего сетевого сканера. В качестве внешнего сетевого сканера можно использовать Nmap, но есть возможность использовать и другой сетевой сканер. Как результат работы данного модуля получаем файл в формате XML с информацией об узлах сети. В файле содержится следующая информация: адрес узла, имя узла, список обнаруженных портов и служб на них, версия ОС. Полученный файл ядро передает модулю дополнительного сканирования.

Модуль дополнительного сканирования по результатам работы модуля сетевого сканирования проводит дополнительное сканирование для того, чтобы получить более детальную информацию. Модуль состоит из множества независимых скриптов, которые на вход принимают адрес узла и номер порта. Как результат работы модуля, выдается xml файл с уточненной информацией об узлах сети. Полученный файл ядро передает модулю анализа результатов сканирования.

Модуль анализа результатов сканирования принимает данные от модуля дополнительного тестирования и производит их структурирование – для каждого узла строится XML элемент, который содержит информацию о данном узле. Результатом работы данного модуля является файл, содержащий все узлы в сети хоста и установленные на него сетевые службы.

Хранилище уязвимостей хранит информацию об известных уязвимостях. Для каждой уязвимости определена сигнатура, содержащая: имя уязвимости, описание уязвимости, условие присутствия, опасность по шкале CVSS.

Модуль первичного анализа занимается поиском уязвимостей из хранилища, условие которых удовлетворяет состоянию хотя бы одного узла в сети хоста. Стоит заметить, что условие может выполняться не полностью, но данная уязвимость может присутствовать, поэтому помимо найденных уязвимостей модуль предоставляет вероятность того, что данная уязвимость может присутствовать.

Модуль поддержки принятия решений сокращает список выявленных возможных уязвимостей путем опроса оператора. То есть модуль просматривает список обнаруженных уязвимостей и если условие выявленной уязвимости выполняются не полностью или недостаточно информации от сканера, то оператору задается уточняющий вопрос, который позволит уменьшить уровень неточности путем принятия решения, присутствует ли данная уязвимость на конкретном узле хоста.

Взаимодействие модулей друг с другом происходит через ядро. На вход каждого следующего модуля ядро передает результат предыдущего модуля. Полученный после работы программы файл предоставляется пользователю, как конечный результат, с результатами исследования сети хоста.

При разработке программного средства предпочтительно использовать средства разработки Apache. Свободный веб-сервер, представляющий собой кросплатформенное программное обеспечение способное работать практически на любой операционной системе, поддерживающей стандарты POSIX или среду Windows API: BSD, MicrosoftWindows, Linux, Mac OS.

Надежность и гибкость конфигурации – главные достоинства Apache. Благодаря этому ПО можно осуществлять подключение внешних модулей, использующихся для предоставления данных, модифицировать сообщения об ошибках, применять СУБД для аутентификации пользователей. Apache оснащен встроенным механизмом виртуальных хостов. Благодаря этому на одном IP-адресе можно обслуживать большое количество веб-проектов (доменных имен), при этом отображая для каждого из них свое содержимое. Для каждого виртуального хоста имеется возможность указать сои настройки модулей и ядра, а также установить ограничения к доступу ко всему сайту либо некоторым файлам. С помощью Apache-ITK для каждого виртуального хоста можно запускать процесс httpd с идентификаторами gid и uid. Также есть модули, которые позволяют ограничивать и учитывать ресурсы сервера (трафик, RAM, CPU) отдельно для каждого виртуально хоста. Помимо этого, Apache поддерживает FastCGI и CGI, позволяющие выполнять программы на многих языках программирования (Java, sh, C, C++). PHP – скриптовый язык программирования общего назначения, интенсивно применяемый для разработки веб-приложений. В настоящее время поддерживается подавляющим большинством хостинг-провайдеров и является одним из лидеров среди языков программирования, применяющихся для создания динамических веб-сайтов.

PHP является языком программирования с динамической типизацией, не требующим указания типа при объявлении переменных, равно как и самого объявления переменных. Преобразования между скалярными типами зачастую осуществляются неявно без дополнительных усилий. Впрочем, PHP предоставляет широкие возможности и для явного преобразования типов. Начиная с пятой версии PHP обладает полной поддержкой ООП. Работа с классами была оптимизирована и теперь такой код работает достаточно быстро. PEAR-библиотека классов PHP с открытым исходным кодом. В стандартную поставку PHP входит система управления классами PEAR, которая позволяет легко скачивать и обновлять их.

MySQL – свободная реляционная система управления базами данных. MySQL является решением для малых и средних приложений. Входит в состав серверов WAMP, AppServ, LAMP и в портативные сборки серверов Денвер, XAMPP. Обычно MySQL используется в качестве сервера, к которому обращаются локальные или удаленные клиенты, однако в дистрибутив входит библиотека внутреннего сервера, позволяющая включать MySQL в автономные программы. Гибкость СУБД MySQL обеспечивается поддержкой большого количества типов таблиц: пользователи могут выбрать как таблицы типа MyISAM, поддерживающие полнотекстовый поиск, так и таблицы InnoDB, поддерживающие транзакции на уровне отдельных записей. Более того, СУБД MySQL поставляется со специальным типом таблиц EXAMPLE, демонстрирующим принципы создания новых типов таблиц.

Memcached – связующее программное обеспечение, реализующее сервис кэширования данных в оперативной памяти на основе парадигмы хеш-таблицы. С помощью клиентской библиотеки (для C/C++, Ruby, Perl, PHP, Python, Java, Csharp/.Net и др.) позволяет кэшировать данные в оперативной памяти множества доступных серверов. Распределение реализуется путем сегментирования данных по значению хэша ключа по аналогии с сокетами хэш-таблицы. Клиентская библиотека, используя ключ данных, вычисляет хэш и использует его для выбора соответствующего сервера. Ситуация сбоя сервера трактуется как промах кэша, что позволяет повышать отказоустойчивость комплекса за счет наращивания количества memcached серверов и возможности производить их горячую замену.

СПИСОК ИСПОЛЬЗОВАНЫХ ИСТОЧНИКОВ

1. Защита информации в компьютерных системах и сетях / Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф.; Под ред. В.Ф.Шаньгина. - М.: Радио и связь, 1999. - 328с.

2. Атака через INTERNET / Медведовский И.Д., СемьяновП.В., Платонов В.В.; Под ред. проф. Зегжды П.Д. - СПб: Мир и семья-95, 1998. -296с.: ил.

3. Международное исследование уязвимостей веб-сайтов сети Интернет, проведенное компанией PositiveTechnologies. – Электронные данные. – Режим доступа: https://www.ptsecurity.ru/.../.

4. Открытый проект о безопасности веб-приложений. – Электронные данные. – Режим доступа: http://owasp.org.