XXXII Неделя науки СПбГПУ. Материалы межвузовской научно-технической конференции. Ч.V : С.168-169

УДК 50.41.00

Е.Ю.Перетягина (5 курс, каф. ИБКС), В.В.Платонов, д.т.н., проф.

РАЗРАБОТКА ЦИКЛА ЛАБОРАТОРНЫХ РАБОТ ПО ДИСЦИПЛИНЕ ПАСОИБ

Активная «разведка» (составление схемы сети) – это процесс сканирования сети или подсети с целью определения доступных серверов и уязвимых служб. Это, как правило, первая фаза взлома, которую также называют зондированием. Для специалистов по защите информации обнаружение процесса составления схемы сети – серьезное предупреждение о предстоящем взломе. Сам взлом может происходить в течение нескольких секунд, поэтому предварительное сканирование часто является единственным признаком готовящегося нападения.

Проблема определения типа и версии операционной системы (ОС) удаленного сетевого узла является весьма актуальной на начальном этапе реализации атаки на хост. В зависимости от того, какая ОС установлена на удаленном хосте, атакующий будет планировать свои дальнейшие действия, воздействуя на известную «дыру» (если таковая имеется) в безопасности установленной на хосте ОС. При этом, чем точнее атакующий определит тип и версию ОС удаленного хоста, тем эффективней будет выполнен его «взлом».

Существует масса различных способов получить информацию об ОС удаленного хоста. Многие из них основаны на использовании механизма опроса стека TCP/IP. Как правило, реакцией узла на любое удаленное воздействие (входящий пакет данных, запрос) является пакет данных, посылаемый источнику воздействия. Как показывает практика, различные ОС при работе в сети по-разному реагируют на один и тот же запрос. Исследовав особенности реакций на запрос ОС, версии которых заранее известны, можно набрать определенную статистику, сопоставив реакции на запрос с типом ОС. На таком принципе основаны методы идентификации ОС при помощи ICMP- и SYN-сканирования.

Еще один важный элемент большинства спланированных заранее нападений – это составление карты сети. Он заключается в выявлении активных хостов сети, а также построении топологии сети.

Данный цикл работ состоит из двух частей и включает в себя семь работ. Первая часть посвящена изучению некоторых методов исследования сети, в частности, методам определения ОС удаленного сетевого узла с использованием ICMP- и SYN-сканирования, а также наиболее распространенным способам составления карты сети. Помимо непосредственно изучения способов активной разведки в работах также предлагается задуматься о возможных вариантах защиты от подобного рода сканирования.

Вторая часть практикума подразумевает выполнение 4-х работ и посвящена исследованию возможностей и защитных характеристик персональных МЭ на примере работы Tiny Personal Firewall 4.5.

Хотелось бы отметить, что в любом случае точное определение операционной системы удаленного сетевого узла, а также получение злоумышленником другой информации о сети и расположенных в ней хостах становится весьма затруднительным при грамотном администрировании системы в целом.

Важно также помнить, что чем раньше взломщик будет остановлен при попытке получить информацию о системе, тем менее уязвима она будет к атаке.

Выполнение данного цикла лабораторных работ с освоением приведенных теоретических сведений позволит ознакомиться с некоторыми методами активной

«разведки», а также приобрести навыки практической защиты от них при помощи персонального МЭ (ПМЭ).

Необходимо понимать, что чем раньше будут определены наличие взлома или попытка взлома, тем меньше ущерба будет нанесено системе. Таким образом, зная методы, которыми пользуется злоумышленник для сбора информации, есть шанс обнаружить попытку взлома до того как будет проведена атака.

Хотелось бы также отметить, что ПМЭ является достаточно удобным и эффективным средством защиты отдельного компьютера от внешних посягательств. С ним можно быть уверенным, что компьютер не станет легкой добычей для злоумышленников, а правильно настроенный ПМЭ станет непреодолимой преградой для многих из них. В связи с этим четыре лабораторных работы второй части данного цикла посвящены изучению возможностей и защитных характеристик одного из представителей ПМЭ – Tiny Personal Firewall 4.5. Так как набор представляемых различными ПМЭ возможностей по повышению защищенности узла примерно одинаков, то исследование принципа работы и предоставляемых средств защиты одного из них, в частности Tiny Personal Firewall 4.5, является вполне достаточным для составления общего впечатления о ПМЭ и приобретения навыков защиты хоста с их помощью.

Безусловно, данный цикл лабораторных работ не способен охватить все методы определения операционной системы удаленного сетевого узла и составления карты сети, но, тем не менее, выполнение первой части данного курса с изучением приведенных теоретических сведений дает представление о наиболее распространенных методах активной разведки, знание принципа действия которых определяет предложения по защите от них.