АНАЛИЗ УЯЗВИМОСТЕЙ И ИНСТРУМЕНТОВ ОСУЩЕСТВЛЕНИЯ СЕТЕВЫХ АТАК

Василий Гусликов, Михаил Стеркул
Славянский университет (Республика Молдова)

The counteraction problem to network attacks Is investigated. The characteristic is given attacks of type DoS and DDoS, intended for a conclusion out of operation operating system services. Questions of security of network resources on the basis of tools of operating system Windows XP are considered.
Ключевые слова: *операционная система, защита, сетевые атаки, DDoS, DoS.*

Актуальность темы заключается в том, что наряду с растущей популярностью операционная система Windows все в большей степени привлекает взломщиков, хакеров или просто любителей ради баловства написать программы взлома, вирусы именно для этой операционной системы. **Целью работы** явилось исследование возможностей сетевых атак на примере ОС Windows XP и разработка рекомендаций по их преодолению. **Предметом исследования** выступали сетевые инструменты Windows XP и их уязвимости при сетевых атаках.

Конечно, существуют вредоносные программы и для других ОС, но их значительно меньше. Главная причина этому, то, что такие ОС как Linux, Unix, FreeBSD и другие, как правило, контролируются опытными администраторами, которые полностью проверяют работоспособность как внутренней сети, так и каждой машины. Кроме того, сеть может быть защищена брандмауэром и даже если какой-то программе удастся преодолеть защиту, администратор сразу заметит активности и легко разберется, откуда исходит опасность по исходящему ICMP или UDP трафику [5].

Основная опасность грозит тем системам, которые управляются обычными пользователями, их компьютеры часто не имеют защиты или имеют, но не умеют пользоваться своими брандмауэрами. Кроме того, компания Microsoft наградила операционную систему Windows XP очень мощными инструментами, которыми не стесняются пользоваться хакеры. В частности самая популярная версия Windows поддерживает механизм SOCK_RAW, который является очень мощным инструментом и открывает большие возможности для взлома.

Этот тип “гнезд” обеспечивают доступ к протоколам наиболее низкого уровня и даже к сетевым

интерфейсам. В частности, в системе Unix raw sockets пользуются инструментом getethers, предназначенным для сбора информации о компьютерах, подключенных к сети Ethernet. Один из побочных эффектов поддержки raw sockets - возможность замены обратного адреса в IP- и ICMP-пакетах [3].

В далеком 2001 году, когда только должна была выйти операционная система Windows, разгорелись споры о том, нужна ли в ОС поддержка sockets raw. Тогда президент компании Gibson Research Corporation, Стив Гибсон обратился к компании Microsoft с предложением убрать этот мощный инструмент и не давать хакерам в руки столь мощное оружие. Но компания Microsoft не восприняла слова известного специалиста по компьютерной безопасности и заявила, что задуманное будет воплощено в жизнь. Во-первых, аргументируют они «raw sockets уже были реализованы в Windows 2000, и, как говорится, ничего страшного не произошло. Во-вторых, безопасность за счет отклонения от стандартов - порочная практика».

Именно с этого момента пользователи самой популярной ОС стали грозным оружием в руках сообразительных хакеров. Сами того не зная, вы можете быть одним из воинов многочисленной армии, так называемых «зомби» - компьютеров, которые атакуют заданную цель [1].

Атаки, предназначенные для вывода из строя служб операционной системы, подразделяются на два типа DoS и DDoS.

Атака DoS - Denial of Service, этот тип атак известен давно, его применяют не только для того, чтобы отключить службы или положить сервер, но часто прикрываются такой атакой при взломе сервера. Подобные действия хакеры называют «наводнением». Сервер закидывается запросами о соединении, при этом атакующий компьютер не отвечает, а посылает запрос снова и снова. Это продолжается до тех пор, пока буфер не будет переполнен. Когда это случится соединение с сервером станет невозможным [1].

Атака DDoS - Distributed Denial of Service, является модификацией DoS и отличается тем, что при проведении атаки используются скоординированные действия многочисленных компьютеров-посредников, которые играют активную роль. Для этого на машины внедряются специальные программы – «зомби», поддерживающие связь с неким управляющим центром. По его команде «зомби» начинают генерировать ICMP или UDP пакеты и передают их по адресу жертвы [1].

Подобные атаки сейчас часто применяются хакерами, даже существует негласный сервис, которым может воспользоваться каждый.

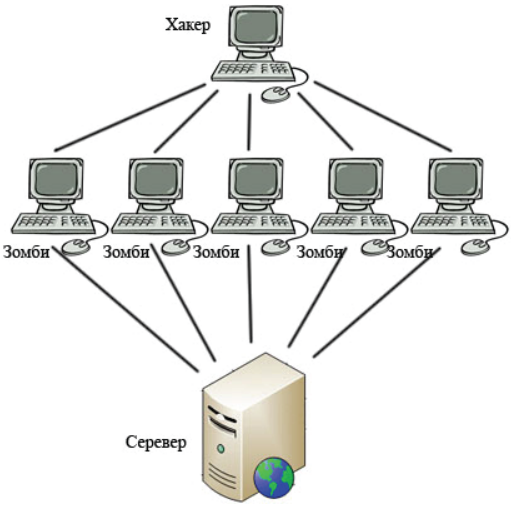

Рис. 1. **Пример DDoS атаки**

Конечно, всего этого не стоит опасаться, если установить и обновлять на компьютере антивирусные системы и брандмауэр. Таким образом, можно на 90% исключить возможность того, что компьютер станет еще одной боевой единицей армии «зомби». Но, в принципе, любой хакер может воздействовать на персональный компьютер пользователя на еще более низком уровне - разработав драйвер, который, по сути, будет троянской программой, открывающей доступ к информации и ресурсам. Именно по этой причине для обеспечения уверенности в 100% защите компьютера рекомендуется приобретать и устанавливать только лицензионное программное обеспечение

Литература:

1. Крис Касперски. Техника сетевых атак. Приемы противодействия. – М.: СОЛОН-Р, 2001. – стр. 311, 313, 315
2. Тим Паркер, Каранжит Сиян. TCP/IP. Для профессионалов. – М.: Питер, 2005. – 859 с.
3. Р. Элсенпитер, Т. Дж. Велт. Windows XP Professional. Администрирование сетей. – М.: Эком, 2006. – стр. 275
4. Вильям Столингс. Network Security Essentials. Applications and Standards. – М.: Вильямс, 2002. – 432 с.
5. http://ru.wikipedia.org DoS-атака