Потанин И.И.
Научный руководитель: доцент кафедры ФПМ, к.т.н. Макаров К.В.
Муромский институт (филиал) федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»
602264, Владимирская область, г. Муром, ул. Орловская, д.23
E-mail: razem1911@gmail.com

Определение состава виртуальной лаборатории эмуляции удаленных сетевых атак

Удалённая сетевая атака — информационное разрушающее воздействие на распределённую вычислительную систему, осуществляемое программными средствами по каналам связи. [1]

Повышение интереса к TCP/IP-сетям обусловлено бурным ростом сети Интернет. Однако это заставляет задуматься над тем, как защитить свои информационные ресурсы от атак из внешней сети. [1]

По характеру воздействия сетевые атаки бывают:

1. Пассивные.
2. Активные. [2]

Пассивное воздействие на распределённую вычислительную систему представляет собой некоторое воздействие, не оказывающее прямого влияния на работу системы, но в то же время способное нарушить её политику безопасности.

Активное воздействие на распределённую вычислительную систему — воздействие, оказывающее прямое влияние на работу самой системы (нарушение работоспособности, изменение конфигурации системы и т. д.), которое нарушает политику безопасности, принятую в ней. Активными воздействиями являются почти все типы удалённых атак.

По цели воздействия

1. Нарушение функционирования системы (доступа к системе).
2. Нарушение целостности информационных ресурсов (ИР).
3. Нарушение конфиденциальности ИР. [2]

Для проведения эмуляций удаленных сетевых атак в пределах учебной лаборатории требуется иметь в наличии: рабочие места на базе вычислительной техники, стенды сетей передачи информации с коммутацией пакетов и коммутацией каналов, структурированную кабельную систему, стойки с телекоммуникационным оборудованием, системой питания и вентиляции, обучающее программное обеспечение, эмуляторы активного сетевого оборудования. [3]

Как можно было заметить, для проведения и изучения последствий удаленных сетевых атак требуется большое количество аппаратуры, которая в свою очередь требует не малых затрат.

Актуальность темы создания виртуальной лаборатории эмуляции удаленных сетевых атак заключается в том, чтобы облегчить для учебных заведений процесс обучения студентов, снизив затраты на аппаратуру.

Целью данного научного исследования является определение состава виртуальной лаборатории.

В большинстве случаев, для использования данной лаборатории потребуется иметь в наличии персональный компьютер или же ноутбук. Все процессы практически полностью будут моделироваться на работающей машине.

При проведении удаленных сетевых атак в учебном заведении есть вероятность нарушить работу локальной вычислительной сети, внедрение же системы «Виртуальная лаборатория» исключает данную опасность, так как воздействие лаборатории будет распространяться только на ту электронно-вычислительную машину на которой она была запущена.

Для студентов будет возможным работа над проектами вне института, что повысит быстроту выполнения заданий, так как все необходимое всегда будет рядом в любое время.

Так же данная лаборатория будет составлять полный отчет о процессе работы по окончании тех или иных процессов, что в свою очередь так же поможет студентам при оформлении документации для сдачи.

В соответствии с федеральным государственным образовательным стандартом по направлению подготовки Информационная безопасность в состав виртуальной лаборатории должны входить следующие основные компоненты:

1. Модуль фрагментации данных.
2. Модуль нестандартных протоколов, инкапсулированных в IP.
3. Модуль перехвата пакетов на маршрутизаторе.
4. Модуль анализа сетевой информации.

Эти пункты являются основными в изучении сетевых атак, следовательно, их наличие обязательно для лаборатории.

В результате проведенного исследования был определен основной состав виртуальной криптографической лаборатории.

В заключении можно сказать, что удаленные сетевые атаки очень опасны, они могут вывести из строя множество систем и нарушить конфиденциальность данных. Следовательно, нужно приложить усилия к тому, чтобы в рамках образовательных программ была возможность полностью изучить их влияние на электронно-вычислительные машины и локальные вычислительные сети.

1. Медведовский И. Д., Семьянов П. В., Платонов В. В. АТАКА ЧЕРЕЗ INTERNET - Под науч. ред. проф. Зегжды П.Д. Серия: «Магистр» СПб Мир и семья 2004г. 296 с.

2. Шаньгин В. Ф. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СИСТЕМ И СЕТЕЙ. - М.: ИД "Форум": Инфра-М, 2008. — 416 с.

3. Фролов А. В., Фролов Г. В. Глобальные сети компьютеров. ПРАКТИЧЕСКОЕ ВВЕДЕНИЕ В INTERNET, E-MAIL, FTP, WWW И HTML, ПРОГРАММИРОВНАИЕ ДЛЯ WINDOWS SOCKETS. -М. : Диалог-МИФИ, 2006г. – 288 с.