Н. В. Белоголовая
(*ГрГУ им. Я. Купалы, Гродно*)

МОДЕЛИРОВАНИЕ СЕТЕВЫХ АТАК В СРЕДЕ ЭМУЛЯТОРА GRAPHICAL NETWORK SIMULATOR-3 (GNS3)

При изучении технологий компьютерных сетей и методов обеспечения их безопасности наибольшие затруднения вызывает формирование практических навыков их взлома и защиты. Опыт показывает, что заметного эффекта в этих вопросах можно добиться благодаря использованию программ-эмуляторов и методов моделирования сетевых атак. В работе рассматриваются возможности сетевого эмулятора GNS3 для изучения распространенной сетевой атаки – ARP-спуфинга и методов защиты от нее. Инфраструктура атаки моделируется в среде эмулятора, защита строится на основе технологии Dynamic ARP Inspection. ARP-spoofing (подмена ARP) – разновидность сетевой атаки типа MITM, применяемая в сетях с использованием протокола ARP. Подмена ARP заключается в нарушении назначений MAC-IP для отдельных устройств в сети. Эксплуатируемая уязвимость состоит в том, что любое устройство в сети может ответить на запрос ARP, независимо от того, является ли оно адресатом данного запроса. За счет этой уязвимости было проведено огромное количество атак. Используя легкодоступные инструменты, злоумышленник может «отравить» кэш ARP других хостов в локальной сети, заполнив его неверными данными. Наиболее простым способом для наглядного подтверждения успешной атаки является использование встроенной в GNS3 утилиты WireShark.

В ходе работы в эмуляторе GNS3 была построена компьютерная сеть, включающая маршрутизатор, коммутатор и два конечных устройства. После этого выполнена ARP-атака с помощи утилиты Metasploit и, далее, на коммутаторе была настроена защита с использованием технологии Dynamic ARP Inspection. Построенная модель позволяет наглядно убедиться в эффективности работы технологии Dynamic ARP Inspection и важности ее настройки для защиты от сетевой атаки. В симуляторе GNS3 возможно построение более сложных атак, с целью наглядного обучения студентов. Существует несколько способов использования таких моделей в учебном процессе: демонстрационные стенды и соревнования в формате CTF (Capture The Flag, Захват Флага).