УДК 004.00

ПРОГРАММНЫЙ КОМПЛЕКС ТЕСТИРОВАНИЯ ЗАЩИЩЕННОСТИ ТЕРРИТОРИАЛЬНО РАСПРЕДЕЛЕННОЙ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ НА ОСНОВЕ ПРИМЕНЕНИЯ МНОГОАГЕНТНОГО ПОДХОДА

Захаров О.О. Военно-космическая академия имени А.Ф. Можайского
Научный руководитель – кандидат технических наук Дудкин А.С.
Военно-космическая академия имени А.Ф. Можайского

В докладе рассмотрена актуальность разработки кроссплатформенного инструмента для решения широкого спектра задач по тестированию и анализу защищенности территориально распределенной информационно-телекоммуникационной сети (ИТКС).

Введение. В современных условиях, системы защиты информации необходимо периодически подвергать испытанию. Специалисты по информационной безопасности (ИБ) должны убедиться в отсутствии уязвимых мест в исследуемой системе, руководство организации – в том, что деньги и иные ресурсы не были потрачены впустую. Для проверки вышеперечисленных условий существует множество методов (например, пентест, аудиты ИБ, киберучения и т.д.), но один из самых популярных и эффективных – Red Team Operations. Зачастую термин Red Teaming сравнивают с термином APT (Advanced Persistent Threat) – постоянной угрозой повышенной сложности, в ходе которой злоумышленник старается проникнуть в информационную систему любыми способами и средствами, закрепиться в ней и извлечь как можно больше выгоды.

Основная часть. Периодически подход Red Team Operations рассматривают как проверку на устойчивость к целевым атакам. Именно для экспертов «красной команды», которым необходимо работать с настоящей инфраструктурой заказчика, действовать втайне от сотрудников организации для проверки способности службы ИБ отразить атаку и активно, без ограничений по времени предназначен кроссплатформенный модульный программный комплекс. Тестирование защищенности ИТКС заключается в следующем: записыванием нажатия клавиш и их отсылкой на командный сервер, либо другими действиями (получением скриншотов экрана, поиском файлов на компьютере) можно вызвать реакцию средств защиты на все или некоторые производимые действия, что в свою очередь показывает как настроены эти средства и хватает ли у них возможностей для обнаружения подобного рода атак, а также проверит службу ИБ на способность отразить непредвиденную атаку, вовремя обнаружив ее и правильно отреагировав. Основное отличие от большинства существующих программных продуктов для тестирования защищенности ИТКС заключается в том, что данный подход позволяет проверять средства защиты ИТКС на этапах установки программы-агента, подключения к командному серверу (серверу экспертов) и проведения действий на самих устройствах сети, тогда как существующие проверяют ИТКС на уязвимости, стойкость паролей и т.д., что не полностью показывает состояние защищенности ИТКС, потому что преступник может применить иные тактики – социальная инженерию или уязвимость, еще не известную разработчику (0-day) и успешно проникнуть в систему.

Выводы. Разработанный программный продукт, позволяет тестировать защищенность распределенной ИТКС. В состав продукта входят командный сервер и программный агент под ОС Windows, заложена основа для различных операционных систем Linux, Mac OS, а также под другие аппаратные платформы. Программный агент под Windows, обладает достаточным базовым функционалом: получение снимков экрана, нажатых клавиш, выполнение команд через командный интерпретатор Windows, управление закреплением в системе, самоуничтожением. В программном комплексе реализована поддержка плагинов, позволяющих расширять его функционал.

Захаров О.О. (автор)

Дудкин А.С. (научный руководитель)