ОБНАРУЖЕНИЕ УЯЗВИМОСТЕЙ В ИНФОКОММУНИКАЦИОННОЙ СЕТИ ПРЕДПРИЯТИЯ, НА ОСНОВЕ КОРРЕЛЯЦИИ ДАННЫХ ПОЛУЧАЕМЫХ ИЗ РАЗЛИЧНЫХ ИСТОЧНИКОВ

В.Ф. Кулиш, Т.В. Борботько, Аль-Гбури Хуссейн Кахтан Халаф

Мероприятия по оценке защищенности инфокоммуникационных сетей основываются на анализе их уязвимостей, которые позволяют определить вероятные способы получения несанкционированного доступа к ним нарушителем, что в дальнейшем дает возможность разработать или совершенствовать систему защиты инфокоммуникационной сети. Практическая реализация таких мероприятий позволяет своевременно обнаруживать сервисы, отладочные интерфейсы и приложения, функционирующие в инфокоммуникационной сети предприятия, по ошибке администратора оказавшиеся доступными из сети Интернет.

Обнаружение уязвимостей основывается на ряде последовательных итераций позволяющих сформировать списки зарегистрированных доменных имен в анализируемой инфокоммуникационной сети, хостов и открытых на них портах. Типовой подход, используемый для получения указанных сведений, основан на сканировании сети предприятия за счет использования прикладного программного обеспечения (Nessus, Qualys и т.д.), в том числе с открытым исходным кодом (dnsmap, nmap и т.д.).

Однако с появлением таких сервисов в сети Интернет как Shodan (https://shodan.io) и Censys (https://censys.io), периодически сканирующих весь диапазон адресов протокола IP версии 4, обнаружение уязвимостей может быть реализовано за счет получения информации от указанных информационных ресурсов, сопоставления ее и преставления в удобном для оператора виде для последующего анализа. Указанные сервисы имеют интерфейсы прикладного программирования, что предлагается использовать для создания прикладного программного обеспечения для анализа уязвимостей инфокоммуникационной сети предприятия.

Разработанное программное средство получает информацию от указанных сервисов, из которой выбираются сведения, относящиеся к анализируемой инфокоммуникационной сети предприятия. На основании полученной информации от сервисов Shodan и Censys формируются два списка доступных хостов сети и открытых портах с указанием даты последнего сканирования. Полученные таким образом списки объединяются в один отчет с учетом даты последнего сканирования, который впоследствии будет анализироваться оператором.

Таким образом, разработанное программное средство позволяет получать сведения об уязвимостях инфокоммуникационной сети предприятия, без подключения к анализируемой сети, за счет корреляции данных (результатов сканирования сети) получаемых от сервисов Shodan и Censys.

ЗАЩИТА ИНФОРМАЦИИ В СЕТЯХ G-PON

Д.Н. Курбыко, Н.В. Тарченко

Основной особенностью всех xPON сетей является то, что нисходящий поток достигает всех оптических сетевых блоков (ONU), подключенных к сети. Злоумышленник после некоторых манипуляций с перепрограммированием ONU может добиться того, что будет получать информацию, адресованную другим пользователям. Система безопасности xPON сетей как раз должна уметь противостоять такого рода угрозам, как «прослушивание».

Основной алгоритм шифрования, использующийся в технологии G-PON — это расширенный стандарт криптозащиты (AES). Этот алгоритм шифрования относится к виду так называемых блочных кодов, который обрабатывает блоки данных длинной 16 байт.

Стандарт AES поддерживает несколько режимов шифрования данных, однако в технологии G-PON используется только один из них. Он получил название «шифрование со счётчиком» Counter Mode (CTR). Шифратор создает поток, состоящий из 16 байтных псевдослучайных шифроблоков. По заданному алгоритму шифроблоки взаимодействуют с входной нешифрованной информацией, в результате чего на выходе получается зашифрованная информационная последовательность. На приемной стороне происходит обратная операция, в которой участвуют те же самые шифроблоки и зашифрованная информационная последовательность. В результате получается исходная нешифрованная информационная последовательность.

Когда датаграмма отправляется OLT или принимается ONU, то в ней содержится информация о первом байте заголовка. В первом байте заголовка находится значение криптосчетчика. Для конкретной датаграммы это значение используется в качестве начального значения счетчика