УДК 004.056.53: 621.391.7

Повышение безопасности сетевых коммуникаций на транспортном уровне

А.В. РОСЛЯКОВ, заведующий кафедрой сетей и систем связи ПГУТИ доктор технических наук, профессор, Д.А. ЕФРЕМОВ, студент

Повышение безопасности сетевых коммуникаций на транспортном уровне
Enhancing the Security of Network Communications at the Transport Layer

Сетевые приложения для взаимодействия на транспортном уровне в сетях IP имеют специальные числовые идентификаторы, называемые портами. Для передачи информации на транспортном уровне к заголовкам транспортного протокола добавляются значения порта отправителя и порта получателя. Это необходимо для сопоставления пришедших данных с приложением в операционной системе, однако это открывает серьезную брешь в сетевой безопасности.

Проблема заключается в незащищенности приложений от сканирования портов, которое представляет собой последовательное обращение к каждому порту для выявления работающих приложений, получение их версии, и в последующих атаках.

В статье проанализированы существующие методы противодействия сканированию портов, предложена новая реализации метода на основе технологии Port Knocking. Выявлены ее достоинства и недостатки, определены области возможного практического применения.

Network applications for communication at the transport level in IP networks have special numeric identifiers called ports. To transmit information at the transport layer, the value of the sender's port and the recipient's port are added to the headers of the transport protocol. This is necessary to match the incoming data with the application in the operating system, however, this opens up a serious breach in network security.

The problem lies in the vulnerability of applications from port scanning, which is a sequential access to each port to identify running applications, get their version and for subsequent attacks.

The article analyzes the existing methods of countering port scanning, a new implementation of the method based on Port Knocking technology is proposed. Its advantages and disadvantages are revealed, areas of possible practical application are identified.

Ключевые слова: транспортный уровень, сетевая безопасность, Port Knocking, сканирование портов, Stunnel.

Keywords: *transport layer, network security, Port Knocking, port scanning, Stunnel.*

Введение

В IP-сетях для взаимодействия сетевых приложений на транспортном уровне L4 используются специальные числовые идентификаторы соединения — сетевые порты. Одна из проблем безопасности использования портов в IP-сетях заключается в их незащищенности от сканирования. Сканеры представляют собой программное обеспечение (ПО), предназначенное для выявления “открытых” портов, т. е. для обнаружения портов, не защищенных правилами межсетевого экрана и находящихся в режиме прослушивания.

Использование данного класса ПО позволяет злоумышленникам собирать информацию о сетевых приложениях, в некоторых случаях их версию, тип и другие полезные данные. Собранная информация может использоваться для точечных атак на определенное приложение или с целью получить доступ ко всей операционной системе (ОС) с последующим нарушением ее работоспособности. Но чаще всего таким атакам подвержены серверные системы, так как они представляют наибольший интерес у злоумышленников и включают большое количество приложений по сравнению с хостами, работающими в сети.

Сканирование портов не представляет большой сложности, так как их количество ограничено с учетом 16-битной адресации, а номера конкретных специфичных портов выделяются и регистрируются организацией IANA (Internet Assigned Numbers Authority — Администрация адресного интернет-пространства).

Проблема безопасного использования общеизвестных портов стала особенно актуальна с появлением поисковой системы Shodan [1], которая, по сути, предоставляет метаданные о том, какие приложения работают на том или ином сервере, подключенном к сети Интернет. Более того, она позволяет производить поиск по этим метаданным.

Исследование основных трендов атак, выполненное компанией по IT-безопасности CheckPoint в 2022 г., показало, что наиболее частый вектор атак — незащищенные серверы с открытыми портами (рис. 1).

Статью целиком читайте в бумажной версии журнала