Обнаружение брутфорс-атак в протоколе удалённого доступа SSH методами анализа сетевого трафика

П.В.Пилькевич, email: pavel.piksel2012@mail.ru 1
В.И.Луцышен, email: valutsishen@mail.ru 2

1 Севастопольский государственный университет, институт «Радиоэлектроника и информационная безопасность», кафедра «Информационная безопасность»

Аннотация. *Предложенный подход позволяет обнаружить факт проведения брутфорс-атаки на протокол удалённого доступа методами анализа сетевого трафика и поиска ключевых пакетов в нём. Определены особенности сетевого трафика, характерные для протокола SSH.*

Ключевые слова: *протоколы удалённого доступа, протокол SSH, брутфорс-атаки, анализ сетевого трафика*.

Введение

В условиях повсеместной цифровизации общества первостепенное значение приобретает защита информации с целью предотвращения несанкционированного доступа к данным. Одним из самых широко используемых методов авторизации является использование ключевой пары логин/пароль.

Наиболее популярным методом взлома логина/пароля является подбор учетных данных путем поочередного перебора возможных комбинаций (Brute Force). Данный метод отличается своей простотой и лёгкостью в исполнении, не требует особых профессиональных навыков и подготовки. Целью данного исследования является определение сигнатуры брутфорс-атаки путем анализа участка трафика с целью выработки эффективных мер противодействия.

1. Основная часть

Компьютерная атака – это целенаправленное несанкционированное воздействие на информацию, на ресурс автоматизированной информационной системы или получение несанкционированного доступа к ним с применением программных или программно-аппаратных средств [2].

Полный перебор (или метод «грубой силы», англ. brute force) является одним из самых известных методов взлома учётных записей пользователей. Согласно математическим законам, любая задача может быть решена методом полного перебора. Сформировалось несколько способов формирования списка паролей. Основными являются подбор

по заранее подготовленным спискам, либо путём прямой генерации паролей по указанному шаблону (длина пароля, возможные символы, разнообразие символов).

Протокол передачи данных — набор соглашений интерфейса логического уровня, которые определяют обмен данными между различными программами [4]. В проведённом исследовании использовался протокол SSH – этот сетевой протокол прикладного уровня позволяет производить удалённое подключение к устройствам и туннелировать трафик. Основные преимущества используемого протокола:

– использование множества видов ассиметричного шифрования, применяемого во время передачи данных протоколом;

– неограниченный размер передаваемой информации во время удалённого подключения;

– благодаря высокой безопасности протокола с его помощью можно так же безопасно использовать любой другой сетевой протокол;

– операции протокола можно подробно изучить методами анализа сетевого трафика и системных логов.

Преимущества протокола SSH позволяют безопасно передавать информацию между двумя удалёнными хостами так, чтобы подменить или расшифровать поток данных злоумышленнику было практически невозможно. Это порождает крупную угрозу – если злоумышленник каким-то образом получает доступ к удалённому соединению по SSH, его действия будет так же трудно определить и пресечь инциденты информационной безопасности [1].

Одним из наиболее распространённых методов получения злоумышленником доступа к удалённому протоколу SSH является атака перебора учётных данных грубой силой (Brute Force). Зачастую, это связано с низкой сложностью паролей, выбираемых пользователями, что и приводит к несанкционированному доступу со стороны злоумышленника. Подобные атаки можно пресекать, анализируя сетевой трафик информационной системы [3].

Для проведения эксперимента требуется эмулировать брутфорс-атаку на протокол SSH. Для этого используется программное обеспечение с открытым кодом для перебора паролей Hydra. Это обусловлено популярностью используемого ПО и возможностями многопоточного перебора, что позволяет увеличивать эффективность перебора.

Для отслеживания и анализа сетевого трафика использовалась программа-анализатор сетевого трафика Wireshark.

2. Эксперимент

В процессе эксперимента проводилось два типа атак – брутфорс-атака, в ходе которой верные учётные данные были обнаружены и атака, в процессе которой не удалось подобрать корректные ключи. В сети находится сервер, на котором доступно удалённое подключение по протоколу SSH (10.0.2.5) и атакующее устройство (10.0.2.4). В результате получено две таблицы:

Таблица 1

Участок сетевого трафика при вводе неверных учётных данных

№	Время	Отправитель	Получатель	Протокол	Длина	Информация
1	5,147852	10.0.2.4	10.0.2.5	SSHv2	118	Client: Encrypted packet (len=52)
2	5,148243	10.0.2.5	10.0.2.4	TCP	66	22 > 38500
3	5,148243	10.0.2.5	10.0.2.4	SSHv2	118	Server: Encrypted packet (len=52)
4	5,148322	10.0.2.4	10.0.2.5	SSHv2	134	Client: Encrypted packet (len=68)
5	5,148718	10.0.2.5	10.0.2.4	TCP	66	22 > 38500
6	5,157699	10.0.2.5	10.0.2.4	SSHv2	118	Server: Encrypted packet (len=52)
7	5,157776	10.0.2.4	10.0.2.5	SSHv2	150	Client: Encrypted packet (len=84)
8	5,158043	10.0.2.5	10.0.2.4	TCP	66	22 > 38500
9	7,405725	10.0.2.5	10.0.2.4	SSHv2	118	Server: Encrypted packet

						(len=52)
10	7,408426	10.0.2.4	10.0.2.5	TCP	66	38500 > 22

Рассмотрим вторую таблицу.

Таблица 2

Участок сетевого трафика при вводе верных учётных данных

№	Время	Отправитель	Получатель	Протокол	Длина	Информация
1	0,282607	10.0.2.4	10.0.2.5	SSHv2	118	Client: Encrypted packet (len=52)
2	0,282834	10.0.2.5	10.0.2.4	TCP	66	22 > 38504
3	0,282834	10.0.2.5	10.0.2.4	SSHv2	118	Server: Encrypted packet (len=52)
4	0,282964	10.0.2.4	10.0.2.5	SSHv2	134	Client: Encrypted packet (len=68)
5	0,283172	10.0.2.5	10.0.2.4	TCP	66	22 > 38504
6	0,292138	10.0.2.5	10.0.2.4	SSHv2	118	Server: Encrypted packet (len=52)
7	0,29230	10.0.2.4	10.0.2.5	SSHv2	150	Client: Encrypted packet (len=84)
8	0,29248	10.0.2.5	10.0.2.4	TCP	66	22 > 38504
9	0,302086	10.0.2.5	10.0.2.4	SSHv2	102	Server: Encrypted packet (len=36)
1	0,31954	10.0.2.4	10.0.2.5	TCP	66	38504 > 22

0	7					

В результате следует обратить внимание на пакеты, содержащие в себе ответ сервера на введённые данные и находящиеся под номером 9 в обоих таблицах. Таким образом, при введении верных учётных данных ответ от сервера будет содержать TCP-нагрузку длиной 36 бит, а при отправке неверных учётных данных 52 бита, что позволяет отследить факт обнаружения злоумышленниками верных учётных данных.

Заключение

В результате проведенного исследования найдена модель обнаружения факта успешного подбора учётных данных с помощью исследования сетевого зашифрованного трафика, вследствие чего в дальнейшем планируется разработать модуль для использования в системе обнаружения вторжений, направленный на обнаружение брутфорс-атак и исследования их результатов.

Список литературы

1. Анзина, А. В. Исследование аутентификации в протоколе SSH / А. В. Анзина, А. Д. Медведева, М. А. Лапина // Студенческая наука для развития информационного общества: Сборник материалов IX Всероссийской научно-технической конференции, Ставрополь, 19–21 декабря 2018 года. – Ставрополь: Северо-Кавказский федеральный университет, 2019. – С. 224-232.

2. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию [Текст]. – Введ. 2008-02-01. – Взамен ГОСТ Р 51275-99: введ. 2000-01-01.

3. Мешкова, Е. В. Обеспечение безопасности протокола SSH: шифрование, аутентификация сервера, аутентификация клиента / Е. В. Мешкова, Е. В. Митрошина // E-Scio. – 2017. – № 1(4). – С. 100-103.

4. Шелухин О.И. Системы обнаружения вторжений в компьютерные сети: учебное пособие / Шелухин О.И., Руднев А.Н., Савелов А.В. — Москва: Московский технический университет связи и информатики, 2013. — 88 с. — ISBN 2227-8397. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: http://www.iprbookshop.ru/63360.html (дата обращения: 30.03.2021). — Режим доступа: для авторизир. пользователей.