УДК 004.7.056.53 Вестник УрФО № 1(19) / 2016, стр. XX–XX

Варлатая С. К., Калужин Е. А., Гросман А. К.

МЕТОДИКА ОБНАРУЖЕНИЯ НЕЛЕГАЛЬНОГО ДОСТУПА В КОРПОРАТИВНОЙ СЕТИ ПРЕДПРИЯТИЯ

В данной статье рассмотрена атака на получениенелегального доступа. Проанализированы возможные способы ее реализации. Разработана методика, основанная на выявлении аномального поведения атакующего. Предложен математический способ сравнения действий пользователя, а так же способ формирования и обновления базы данных действий.

Ключевые слова: *информационная безопасность, получение нелегального доступа, система обнаружения вторжений.*

Varlataya S. K., Kalyuzhin E. A., Grossman A. K.

METHODS OF DETECTING ILLEGAL ACCESS TO CORPORATE NETWORK

This article describes the attack on obtaining illegal access. The possible ways of its realization. A technique based on the detection of abnormal behavior of the attacker. The mathematical way to compare user actions, as well as a way to create and update the database operations.

Keywords: *information security, obtaining illegal access, intrusion detection system.*

Введение

Получение нелегального доступа – вход злоумышленника в систему от лица легитимного пользователя. Наиболее распространённый способ проведения данного вида атак является использование человеческого фактора. Например, в статье [1] автор рассматривает халатность и доверчивость персонала как основную причину утечки информации.

Другой способ реализации атаки на получение нелегального доступа - использование уязвимостей прикладного программного обеспечения, многие из которых можно найти в банке данных угроз ФСТЭК [2].

Получив нелегальный доступ, злоумышленник нарушает конфиденциальность, целостность и доступность информации, что влечет огромный ущерб предприятию. Кроме того, в отличие от атак на повышение при-

вилегий, которые можно предотвратить с помощью разграничения доступа, данный вид атак сложнее детектировать, поэтому остро встает вопрос о создании действенной методики по обнаружению такого рода атак.

В данной статье представлена методика, основанная на том, что поведение злоумышленника, получившего доступ к профилю работника, будет отличаться от поведения легитимного пользователя, так как действия злоумышленника носят деструктивный характер.

Состояние проблемы

Данная проблема широко обсуждается как в научных кругах, так и среди специалистов-практиков по информационной безопасности.

В статье [3] проводится анализ возможных путей защиты от атак на получение нелегального доступа, описывается концепция метода обнаружения таких атак, основанного на обнаружении аномального поведения пользователей. С одной стороны, продемонстрирована эффективность метода, с другой стороны, авторы выделяют ряд проблем, затрудняющих реализацию предложенной ими методики на практике. Для того, чтобы обнаружить аномальное поведение, требуется создать эталонную базу данных действий пользователей. Она формируется путем накопления информации о действиях пользователей. Этот процесс требует большое количество времени, вычислительных мощностей и памяти.

Для того, чтобы снизить количество места, занимаемого базой данных действий пользователей в статье [4] автор предлагает вести запись только определенных действий, например поисковых запросов. Данная методика основана на том, что если поведение атакующего отличается в целом, то будут отличаться и отдельные команды.

В научной работе[5] проводится сравнительный анализ сигнатурного метода обнаружения атак и метода, основанного на выявлении аномального поведения. Авторы подчеркивают преимущества второго и предлагают свой алгоритм. Его основная идея заключается в подсчете корреляции частоты использования команд пользователя в текущем и предыдущих сеансах. На основе полученного коэффициента корреляции делается вывод о легитимности пользователя. Однако проблема формирования базы данных, в которой хранится информация о частоте использования команд, остается открытой.

Таким образом, при построении системы обнаружения атак на получение нелегального доступа, чаще всего используется метод, основанный на обнаружении аномального поведения пользователей. Реализация этого метода сопровождается следующими сложностями:

- создание базы данных действий пользователей
- обновление базы данных действий пользо-вателей
- создание набора правил, по которым оценивается отклонение поведения пользователя.

Рис.1 Структурная схема методики обнаружения нелегального доступа

Постановка задачи

Целью данной работы является разработка методики обнаружения нелегального доступа. Для достижения поставленной цели была построена математическая модель поведения пользователя в системе, предложен алгоритм численной оценки и сравнения поведения пользователей. Также предложен способ создания и обновления базы данных действий пользователей.

Общее описание методики

Весь процесс обнаружения нелегального доступа можно представить в виде двух фаз (рис.1): фазы создания базы данных действий пользователей и фазы обнаружения. Обе фазы функционируют параллельно во время сессии пользователя.

В первой фазе собирается информация о действиях пользователей. Информацию о действиях конкретного пользователя называется профиль поведения. Профили поведения формируют базу данных действий пользователей.

Во второй фазе сравниваются текущие действия пользователя с действиями, взятыми из базы данных. Модуль сравнения сравнивает эти действия, а модуль принятия решений принимает решение о том, является ли данный пользователь легитимным.

Описание принципа сравнения действий пользователя

Основная идея заключается в том, чтобы каждому возможному действию (копирование, редактирование, просмотр и т.д.) присвоить определенное числовое значение.

Эти числовые значения записываются в матрицу A (рис. 2). Строки матрицы определяют пользователя системы, а столбцы их действия, тогда A_{ij} – числовое значение j-ого действия i-ого пользователя. Обозначим набор этих числовых значений как X_k, $k=\{1,2,\ldots,n\}$.

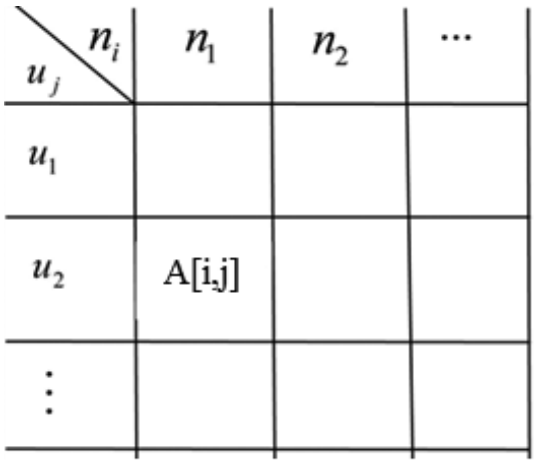

Рис. 2. Пример матрицы действий пользователей

Так как числовые значения из набора X_k являются дискретными случайными числами, то X_k можно охарактеризовать с помощью математического ожидания M, дисперсии E и среднего линейного отклонения H. Профиль поведения пользователя определяется как вектор $\vec{C}$ с координатами M, E и H.

Для нахождения вышеуказанных характеристик рассчитывается среднее значение величины:

$$\overline{X} = \frac{1}{n}\sum_{k=1}^{n} X_k, \quad (1)$$

Математическое ожидание, дисперсия и среднее линейное отклонение рассчитываются по следующим формулам:

$$M = \overline{X}, \quad (2)$$

$$E = \frac{1}{n-1}\sum_{k=1}^{n}(X_k - \overline{X})^2, \quad (3)$$

$$H = \frac{1}{n}\sum_{k=1}^{n}\left|X_k - E\right|, \quad (4)$$

С помощью координат вектора модуль сравнения, сравнивает вектор C_1, взятый из базы данных действий, с вектором C_2, сформированным в текущей сессии пользователя. Коэффициент сходства K определяется путем нахождения угла между векторами.

$$\cos\left(\vec{C}_1, \vec{C}_2\right) = \frac{\vec{C}_1 \times \vec{C}_2}{\left|\vec{C}_1\right| \times \left|\vec{C}_2\right|}, \quad (6)$$

$$\mathrm{K} = \arccos\left(\vec{C}_1, \vec{C}_2\right), \quad (7)$$

Далее коэффициент сходства передается в модуль принятия решения. Если угол K больше $K_{\text{крит}}$, то пользователь классифицируется как атакующий.

Значение $K_{\text{крит}}$ устанавливается руководством предприятия исходя из экспертной оценки информационных активов.

Формирование и обновление базы данных действий пользователей

Информация о каждом действии пользователя в виде числовых значений записывается в матрицу действий пользователей и хранится в структурированном виде.

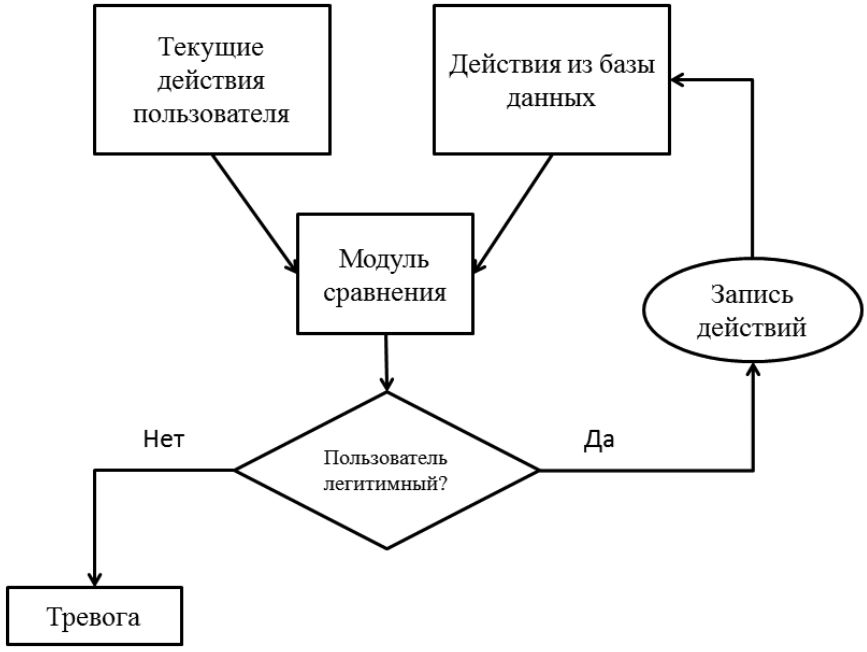

Рис. 3 Структурная схема механизма обновления профиля

Информация профиля обновляется следующим образом: если пользователь классифицирован как злоумышленник, его действия не записываются в профиль, если классифицирован как легитимный, то его действия записываются по окончании сеанса. Этот механизм можно представить в виде следующей структурной схемы(рис.3)

Заключение

В данной статье предложена методика обнаружения атак на получение нелегального доступа, основанная на аномальном поведении злоумышленника. Был разработан способ сравнения действий пользователя и предложен его математический алгоритм. Особенности предложенного способа:

- с увеличением базы данных действий пользователей увеличивается точность определения
- гибкость за счет возможности изменять K_крит, что позволяет адаптировать механизм к изменению в системе
- простота реализации

Также предложен способ создание и обновления базы данных. Она представлена в виде матрицы, а все действия записаны в числовом виде. Это позволяет значительно уменьшить занимаемый ей объем памяти.

Обновление базы данных действий происходит после каждого сеанса пользователя, что обеспечивает её актуальность и как следствие увеличивает точность.

Примечания

1. Родин О. П. Проблема персонала в сфере информационной безопасности //Вестник Тамбовского университета. Серия: Естественные и технические науки. Выпуск № 1 / том 12 / 2012 с.164-165

2. Банк данных угроз ФСТЭК [Электронный ресурс]: http://bdu.fstec.ru/ (дата обращения 22.03.2016)

3. «A Cloud Intrusion Detection Dataset For Cloud Computing and Masquerade Attacks»Hisham A. Kholidy. 2012 Ninth International Conference on Information Technology - New Generations

4. Modeling User Search Behavior for Masquerade Detection. Malek Ben Salem. Recent Advances in Intrusion Detection: 14th International Symposium, Raid 2011, Menlo Park, Ca, USA, September 20-21, 2011: Proceedings

5. Study on Masquerade User Detection Techniques usingSchonlau's Data Set & Simple Cipher Substitution. Nitish V. Lad, Sagar S. Sawant. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)Volume 4 Issue 5, May 2015

Варлатая Светлана Климентьевна, кандидат технических наук, профессор, руководитель направления «Информационная безопасность» Дальневосточного Федерального Университета. 690950, Приморский край, Владивосток, остров Русский, ДВФУ. E-mail: sk-varl@rambler.ru

Калужин Егор Александрович, студент 4 курса по направлению «Информационная безопасность» Дальневосточного Федерального Университета. 690950, Приморский край, Владивосток, остров Русский, ДВФУ. E-mail: workout24@mail.ru

Гросман Алексей Константинович, студент 3 курса по направлению «Прикладная геодезия» Дальневосточного Федерального Университета. 690950, Приморский край, Владивосток, остров Русский, ДВФУ. E-mail: egorcool-90@mail.ru

Varlataya Svetlana Klimentyevna, candidate of engineering sciences, professor, the head of the direction of information security. Far Eastern Federal University. 690950, Primorsky Region, Vladivostok, Russkiyisland, FEFU. E-mail: sk-varl@rambler.ru

Kaluzhin Egor Alexandrovich, student, 4th gradeof the direction of information security. Far Eastern Federal University. 690950, Primorsky Region, Vladivostok, Russkiyisland, FEFU.E-mail: workout24@mail.ru

Grosman Aleksey Konstantinovich, student, 3th grade of the direction of applied geodesy. Far Eastern Federal University. 690950, Primorsky Region, Vladivostok, Russkiyisland, FEFU. E-mail: egorcool-90@mail.ru