ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОЙ ИММУННОЙ СИСТЕМЫ В СИСТЕМАХ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

Бекматов Акмал Курбонмахматович, Кутдусова Эльмира Рауфовна, Эгамбердиев Хожиакбар Салохитдинович

Ташкентский университет информационных технологи им. Мухаммада ал-Хоразмий

АННОТАЦИЯ

Безопасность жизненно важна для эффективного функционирования компьютерных сетей. IDS (системы обнаружения вторжений) являются одним из важных строительных блоков безопасной и надежной сети и широко используются вместе с другими программами и концепциями безопасности. Со временем их важность только растет. В последнее время было проведено много интересных исследований биологических иммунных систем как модели для обнаружения вторжений. В этой статье мы рассмотрим IDS, включая обзор его типов и методов, и исследуем различные конструкции IDS, основанные на концепции искусственного интеллекта, вдохновленной биологией: искусственная иммунная система (AIS), которая может стать будущим направлением в области проектирования IDS.

Ключевые слова: *системы обнаружения вторжений; IDS; Искусственная иммунная система; АИС; Компьютерная сетевая безопасность; Безопасность; Теория опасности*

I. ВВЕДЕНИЕ В IDS

1. IDS (Intrusion Detection System — Система обнаружения вторжений)

IDS играют важную роль в сетевой безопасности путем мониторинга, обнаружения и реагирования на несанкционированные действия и вторжения

[1], и существуют в различных формах уже около двадцати пяти лет [2]. IDS были охарактеризованы как «единственное проактивное средство обнаружения и реагирования на угрозы, исходящие как внутри, так и за пределами корпоративной сети» [1].

2. Типы. По сути, существует два типа IDS: на основе хоста и на основе сети (или трафика). IDS на основе хоста фокусируются на изучении данных (обычно данных журнала и активности системы) на отдельных компьютерах, в то время как IDS на основе сети анализируют данные, которые передаются по сети (обычно сетевая IDS будет подключена к сетевому маршрутизатору, межсетевому экрану или подобному точка управления в сети) [1].

3. Роль. Очень важно четко понимать роль и место IDS в сетевой безопасности. Сетевой администратор должен знать, где и как использовать IDS, имея в виду, что IDS считается устройством мониторинга, а не устройством управления (таким как, например, межсетевой экран). Термины IDS и Firewall не следует рассматривать как два разных названия для одной концепции. По аналогии, если рассматривать брандмауэр как забор вокруг дома, то IDS будет системой охранной сигнализации [1].

4. Пассивная и реактивная IDS. IDS обычно характеризуются как «пассивные» или «реактивные». При обнаружении вторжения пассивная система регистрирует информацию и отправляет сигнал тревоги администратору или консоли. Реактивная IDS (также известная как IPS или система защиты от вторжений) [3] способна выполнять действие в ответ на вторжение [4]. Однако использование IPS не получило широкого распространения из-за сложности отличить реальные угрозы от нормального поведения (проблема «ложного срабатывания») [8]. E. Методы IDS используют ряд методов для обнаружения вторжений, в том числе: обнаружение сигнатур, мониторинг цели, обнаружение аномалий и скрытые зонды. «Обнаружение сигнатуры» использует сведения о ранее идентифицированных схемах вторжений для обнаружения подобных вторжений. Это также называется «обнаружением злоупотреблений». «Целевой

мониторинг» фокусируется на системных ресурсах. Это скорее корректирующий элемент управления, который обнаруживает любые изменения в диапазоне помеченных ресурсов. Системы мониторинга могут попытаться обратить вспять любое обнаруженное вторжение, вернув файлы / ресурсы, которые были изменены в результате вторжения, к их предыдущей форме [1]. «Обнаружение аномалий» - еще один, менее распространенный метод, используемый при обнаружении вторжений. В этом методе IDS определяет нормальное поведение отслеживаемой системы (которое в основном определяется путем сканирования поведения сети в течение определенного периода времени), а затем любое аномально поведение будет помечено как возможное вторжение, объединяя обнаружение сигнатур и обнаружение аномалий для обнаружения вторжения. Этот подход пытается обнаружить атаки, при которых злоумышленник пытается осуществить вторжение в течение длительного периода времени [1]. На этом этапе важно ввести понятие «ложные срабатывания». Ложные срабатывания - это количество ложных срабатываний системы IDS. Другими словами, IDS отмечает поведение у нас есть надежная IDS, так как неправильная сигнализация может отвлечь администратора или консоль от реальных угроз. Они также снижают скорость системы из-за потребления ресурсов. А это приведет к увеличению уязвимости системы [2].

II. HIDS и NIDS

1. HIDS (Host Intrusion Detection System), IDS на основе хоста, также называемая HIDS, отслеживает и собирает данные на главном компьютере. Затем эти данные могут быть проанализированы локально или агрегированы на другом компьютере для аналитических операций. HIDS, как правило, очень хорошо обнаруживает внутренние злоупотребления, а также может обнаруживать неавторизованных пользователей, которые вошли в систему. Слабые стороны HIDS в том, что он может стать громоздким и очень ресурсоемким, а также, если программа-злоумышленник или человек каким-то образом отключит процесс

сбора данных на хосте, тогда HIDS не сможет полностью выполнить свою задачу [2].

2. NIDS (Network Intrusion Detection System) - Сетевые системы обнаружения вторжений (или NIDS) работают посредством мониторинга сетевого трафика. Они сканируют сетевые потоки, чтобы обнаружить возможные вторжения. Эта система потенциально очень хороша в обнаружении неавторизованных пользователей еще до получения доступа к компьютеру. Если сеть использует зашифрованные пакеты или высокоскоростную сеть, то метод NIDS может оказаться неэффективным. К сожалению, эти два (шифрование и высокоскоростные сети) все чаще используются [1]. Конечно, стоит упомянуть, что вторая проблема может быть решена с помощью высокоскоростных сетевых ответвителей, которые представляют собой устройства, обеспечивающие доступ к данным, передаваемым в сети, но все еще существуют проблемы, такие как цена на это сетевое оборудование [2].

3. Характеристики этих двух HIDS и NIDS полностью различаются данными, которые они анализируют, но их можно использовать в качестве дополнений. Если NIDS является слабым, полезен HIDS, а там, где HIDS не подходит, можно использовать NIDS. Сильная система безопасности - это система, в которой используются оба метода [1]. Будущее IDS может быть объединением как NIDS, так и HIDS, работающих как система, а не только одной из них. Другими словами, граница между этими двумя исчезает. Также считается, что распределенные вычисления будут играть большую роль в будущих IDS. Не будет центрального компьютера, который проверяет все пакеты и затем принимает решение о соответствующих действиях. Все компьютеры будут сканировать свой собственный трафик, а затем отправлять результаты на центральный компьютер. Центральный компьютер (или его администратор) просмотрит результаты и затем примет решение. Это сэкономит время и сократит усилия по борьбе со вторжениями [2].

III. IDS основанные на AIS.

AIS (Artificial immune systems - Искусственные иммунные системы) - это алгоритм машинного обучения, который способен обнаруживать атаки, сохраняя оригинальные функции без какого-либо вмешательства со стороны внешней среды. Идея метода состоит в том, чтобы включить био-вдохновленный элемент иммунной системы человека, который, как было доказано, успешно решает различные проблемы, особенно в компьютерной области.

Проводится много работы и обсуждений IDS и связанных областей. Об одном из них мы поговорим в следующей части: Биологическая модель для IDS.

1. Новый подход к IDS Биологические системы выжили миллиард лет благодаря интеллектуальным и уникальным способам. В последнее время использование биологических моделей, таких как нейронные сети и генетические алгоритмы, при моделировании и решении вычислительных задач было чрезвычайно успешным [9]. Многие традиционные методы IDS способны обнаруживать и предотвращать только известные вторжения и в большинстве своем статичны. Они не могут реагировать на новые вторжения в сеть. AIS (аббревиатура от «Искусственная иммунная система»), который представляет собой новую горячую точку для исследований, кажется потенциальным решением этой проблемы, поскольку и сетевая безопасность, и безопасность организма должны отражать реакции на постоянно меняющуюся среду [5] [16].

2. Обзор AIS (HIS) «Иммунная система - это совокупность биологических процессов в организме, которые защищают от болезней путем выявления и уничтожения патогенов и опухолевых клеток [6]». «Эпитоп» - это узнаваемая характеристика молекулы с точки зрения иммунной системы. Одно из больших преимуществ иммунной системы - способность различать «своих» и «чужих» [15], то есть то, что является эндогенным (своим) для хозяина, а что - чужим. Теперь мы представим два других важных понятия: антиген и антитело. Антигены - это чужеродные молекулы на «злоумышленниках», то есть эпитопы, которые иммунная система распознает как чужеродные. Антитела - это часть иммунной системы, которая отвечает за обнаружение антигенов и связывание с

ними. Количество антител намного меньше количества антигенов. Фактически возможное количество антигенов близко к бесконечному; но возможное количество антител - нет. Таким образом, очевидно, что у нас не будет однозначного соответствия антигена и антитела или идеального совпадения из-за неравенства в количестве антигенов и антител. Вдохновленные успехом биологических иммунных систем, системы на основе AIS пытаются разработать систему, в которой небольшое количество антител может обнаруживать большое количество антигенов, даже те антигены, с которыми система сталкивается впервые. Кроме того, иммунная система многослойна, первый из которых (и, возможно, самый эффективный) - это физический барьер кожи [15]. Несколько антигены не могут даже пересечь этот первый слой. Данный патоген (который представляет собой организм, способный вызывать заболевание и отличный от антигена, который может быть обнаружен на поверхности патогена [17]), который может проникать через кожный барьер, может быть устранен комбинацией плотности и температуры. Патогены, которые могут выжить и пересечь предыдущие два слоя, затем столкнутся с двумя компонентами иммунной системы, сначала с «врожденной иммунной системой», которая имеет неспецифический ответ и демонстрирует максимальный немедленный ответ и не имеет памяти, то есть не является антигеном. конкретный. Врожденная иммунная система присутствует почти во всех формах жизни [16]. Если патоген пересекает все эти слои, о нем позаботится вторая часть иммунной системы, которая является «адаптивной иммунной системой», которая демонстрирует специфические ответы на отдельные антигены. Как правило, существует задержка между воздействием антигена и максимальной реакцией на этот антиген. Адаптивная иммунная система в основном основана на двух типах лимфоцитов: Т-клетках и В-клетках [6]. «Иммунная система имеет четыре основных свойства: обнаружение, разнообразие, обучение и толерантность» [5]. Обнаружение происходит, когда «фрагменты патогена и рецептор на поверхности лимфоцитов химически связываются» [5]. Существует

разнообразие рецепторов клеток, поскольку иммунная система должна быть уверена, что по крайней мере группа рецепторов обнаружит вторжение. Что наиболее важно, адаптивная иммунная система обладает памятью и будет гораздо более энергично реагировать на антигены, с которыми она ранее сталкивалась - отсюда концепция «иммунитета» и основа иммунизации [5]. Иммунная система должна обнаруживать и устранять патогены как можно скорее, поэтому клетки должны учиться и адаптироваться с патогеном. Также они должны уметь запоминать патогены, чтобы иметь возможность справиться с повторным вторжением [5]. Процесс, при котором иммунная система становится «невосприимчивой» к определенному набору эпитопов, известен как «толерантность». Фактически, можно сказать, что иммунная система «толерантна» ко всем эндогенным эпитопам, то есть ко всем молекулам, присущим организму [7]. AIS вдохновлен этими характеристиками биологической иммунной системы. По сути, AIS относится к адаптивным системам, которые «изучают», что является родным, а что чуждым системе или сети. Можно сказать, что это новый вычислительный искусственный подход после генетических алгоритмов, нейронных сетей и эволюционных вычислений в области искусственного интеллекта [5].

3. Использование AIS в разработке IDS.

Очевидно, что между AIS и IDS есть общие черты. Оба они используют распознавание образов и обнаружение аномалий, чтобы защитить систему, которая зависит от них (соответственно, организм и компьютерная сеть), от сбоев, связанных с безопасностью. Следовательно, IDS может быть спроектирована на основе AIS. Исследователи предложили IDS на основе AIS, которые используют обнаружение сигнатур и аномалий по сравнению с традиционными, которые почти все используют одну из техник IDS. Часть обнаружения сигнатур обнаруживает известные вторжения, а часть обнаружения аномалий используется для обнаружения новых типов вторжений [5]. Мы можем идентифицировать положительный отбор, отрицательный отбор и клональные

алгоритмы как варианты для системы искусственного иммунитета [9]. Самыми популярными моделями AIS, которые использовались для разработки IDS, являются модели отрицательного отбора [5]. Алгоритм отрицательного отбора - это алгоритм обнаружения изменений, представленный С. Форрестом посредством анализа функций Т-клеток [12].

Ряд исследователей выдвинули идеи относительно IDS на основе AIS. «Хофмейр» представила модель LISYS, которая использует отрицательный отбор, период толерантности, порог активации, срок службы детекторов, совместную стимуляцию, уровень чувствительности, динамические детекторы, зрелые детекторы и детекторы памяти для разработки адаптивной динамической системы обнаружения аномалий с более низким уровнем ложных срабатываний. [10]. CDIS - еще одна модель, которая использует отрицательный отбор плюс созревание аффинности («созревание аффинности - это процесс, с помощью которого В-клетки продуцируют антитела с повышенной аффинностью к антигену в ходе иммунного ответа» [18]). Концептуальная модель Кима - это еще одна модель, которая сочетает отрицательный отбор с клональным отбором (который определяет, как иммунная система реагирует на злоумышленников, используя В- и Т-клетки) и эволюцией библиотеки генов для достижения распределенной, самоорганизованной и легкой IDS. В дополнение к этим моделям и многим другим существует новая модель, в которой используется оператор вакцины, который отправляет выделенную информацию о конкретной проблеме в клетки, чтобы сэкономить время и вычисления [10].

4. Распределенные IDS и AIS

Если мы разработаем распределенную IDS, у нас будет распределенная сеть, в которой каждый компьютер позаботится о себе сам. Таким образом, если один хост выйдет из строя при обнаружении вторжений, другие части сети будут продолжать работать. Кроме того, поскольку каждый компьютер имеет свои собственные правила IDS, настроить IDS проще. Кроме того, поскольку у нас есть распределенная система, в наших системах могут быть разные

операционные системы[17]. Также у нас не будет центрального компьютера, который должен заботиться об обнаружении вторжений во всей сети, и, следовательно, процесс IDS больше не будет слишком затратным по времени и ресурсам, и в очереди обработки не будет больших файлов журналов. Также у нас могут быть определенные узлы в нашей сети, которые поддерживают безопасность системы. Теперь интересно знать, что иммунная система в организме человека распределена до некоторой степени; Антитела вырабатываются определенными типами клеток и циркулируют в крови. Т-клетки продуцируются в узкой кости. Затем отдельные клетки, вырабатывающие антитела, обслуживают все тело. Таким образом, IDS, основанные на иммунной системе, будут самоорганизованными[18]. Такие процессы, как обновление сигнатур вторжений, будут выполняться хостами без вмешательства администратора. Таким образом, сеть будет актуальной, несмотря на любые изменения в среде. Другие полезные аспекты IDS, основанная на AIS, будет многоуровневой, как мы описали ранее. Это означает, что злоумышленник не может добиться успеха, преодолев только один уровень IDS. Несколько уровней будут контролировать одну конкретную точку компьютерной сети, в то время как каждый из них имеет свою архитектуру, что затрудняет атаку злоумышленника. Более того, успешное вторжение на один или несколько хостов не поможет злоумышленнику получить доступ ко всем хостам (потому что они используют разные конфигурации, и IDS будут разными), и, таким образом, скорость атаки будет снижена. Также будет одноразовая IDS на основе AIS. Это означает, что он не зависит от одного компонента, и его компоненты могут быть легко заменены другими компонентами [5].

Как мы уже упоминали, ведется большая работа над системами обнаружения вторжений на основе AIS. Текущие алгоритмы IDS, использующие AIS, основаны на категоризации «я» и «не-я», поскольку они полагаются на классическую иммунологию. Но иммунологи обнаруживают проблемы с классическим методом самодискриминации, поэтому возникает новая теория

под названием «Теория опасности». Теория опасности (Danger theory или коротко DT) основана на корреляции сигналов и обеспечивает «обоснованность» иммунного ответа. Таким образом уменьшается количество ложных срабатываний. Фактически, DT предлагается в качестве дополнительного компонента в AIS [8] [13].

ЗАКЛЮЧЕНИЕ В этой статье мы обсудили IDS, важную часть современных систем сетевой безопасности, а также рассмотрели современные типы, компоненты и методы в IDS. По нашему мнению, в IDS и сетевой безопасности открылись новые горизонты, вдохновленные биологическим моделированием и искусственным интеллектом. Так биологические иммунные системы и системы обнаружения вторжений имеют некоторые общие характеристики, и подходы к IDS, вдохновленные иммунными системами, вполне могут оказаться плодотворными.

Процесс эволюции посредством клонирования и мутации - важные аспекты предложенного алгоритма для получения качественного решения в процессе обучения.

ЛИТЕРАТУРЫ

1. Paul Innella, Oba McMillan, "An Introduction to Intrusion Detection Systems", An Introduction to IDS, Tetrad Digital Integrity, LLC, SecurityFocus, December 6, 2001. [Online]. Available: http://www.securityfocus.com/infocus/1520.

2. Matthew Tanase, "The Future of IDS", The Future of IDS, SecurityFocus, December 4, 2001. [Online]. Available: http://www.securityfocus.com/infocus/1518.

3. Leslie T. O'Neill, "Future of IDS and IPS", Future of IDS and IPS, Network Security Journal, May 29, 2007. [Online].Available: http://www.networksecurityjournal.com/features/future-of-ids-ips-052907.

4. "Intrusion detection system", Intrusion detection system, Wikipedia, the free encyclopedia. [Online]. Available: http://en.wikipedia.org/wiki/Intrusion-detection_system#Passive_system_vs._reactive_system

5. Lu Hong, "Immune Mechanism Based Intrusion Detection Systems," nswctc, vol. 2, pp.568-571, 2009 International Conference on Networks Security, Wireless Communications and Trusted Computing, 2009.

6. "Immune System", Immune System, Wikipedia, the free encyclopedia. [Online]. Available: http://en.wikipedia.org/wiki/Immune_system.

7. "Immune Tolerance", Immune Tolerance, Wikipedia, the free encyclopedia. [Online]. Available: http://en.wikipedia.org/wiki/Immune_tolerance.

8. U. Aickelin, P. Bentley, S. Cayzer, J. Kim, and J. McLeod, "Danger theory: The link between AIS and IDS". In Proceedings of the ICARIS-2003, LNCS 2728, pp. 147-155, 2003.

9. N.V. Truong, C.V. Loi, "Intrusion Detection and Artificial Immune System", The Second NC Scientific Workshop on Computational Intelligence, 2009. [PowerPoint Presentation (.ppt)].

10. Xianjin Fang, Longshu Li, "An Artificial Immune Model with Vaccine operator for Network Intrusion Detection", 2008 IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application,vol. 1, pp. 488-491,19-20 Dec. 2008.

11. Andy Cuff, "Intrusion Detection Terminology (Part One)", SecurityFocus, 2003-09-03. [Online]. Available: http://www.securityfocus.com/infocus/1728.

12. Yingfeng Chen, Lianying Zhou, "An Innovative IDS immune System Model", 2004 IEEE International Conference on Systems, Man and Cybemetics , vol.5,pp. 4810-4814.

13. Haidong Fu, Xiguo Yuan, Liping Hu , "Design of a Four-layer Model Based on Danger Theory and AIS for IDS", pp. 6337-6340, 21-25 Sept. 2007.

14. Бекматов А.К., «Система обнаружения вторжений на основе биологически вдохновленной иммунной системы: врожденной и адаптивной» Эл. журнал. Образование и наука в 21 веке. Май 2022. Том 4 (2) 1158

15. Саламатова Т.А., Пугачев С.С., Жуков В.Г. «Обнаружение сетевых вторжений эволюционным иммунным алгоритмом клональной селекции.» Вестник SibGAU 2014, No. 4(56), P. 41-47

16. Саламатова Т.А. «О применении искусственных иммунных систем в системах превентивной защиты информации.» URL: https://cyberleninka.ru/article/n/o-primenenii-iskusstvennyh-immunnyh-sistem- v-sistemah-preventivnoy-zaschity-informatsii/viewer (дата обращения: 16.03.22).

17. Чернышев Ю.О., Григорьев Г.В., Венцов Н.Н., «Искусственные иммунные системы: обзор и современное состояние» Журнал «Программные продукты и системы» 2014 г. 136-141с.

18. В.И.Васильев, Р.Р.Шамсутдинов «Интеллектуальная система обнаружения сетевых атак на основе механизмов искусственной иммунной системы» Научный журнал «Моделирование, оптимизация и информационные технологии.» 523-530с. 2019г.