УДК 004.056.53

СИСТЕМА ОБНАРУЖЕНИЯ ПЕРВОНАЧАЛЬНОГО ДОСТУПА НАРУШИТЕЛЯ В ИНФОРМАЦИОННУЮ СИСТЕМУ

Дедков В.Н.

гр.367241

Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь

Научный руководитель: Борботько Т.В. – доктор технических наук, заведующий кафедрой защиты информации

Аннотация. В материалах доклада рассматриваются основные принципы работы, архитектуры и технологии, задачи и цели систем обнаружения вторжений (IPS) и предотвращения вторжений (IDS).

Ключевые слова: системы обнаружения вторжений (IPS) и предотвращения вторжений (IDS).

Введение. Система обнаружения первоначального доступа нарушителя в информационную систему является важным компонентом защиты цифровой инфраструктуры организации, в ходе чего анализируется принцип работы и функциональные возможности такой системы, которая предназначена для обнаружения попыток несанкционированного доступа к информационной системе на ранних стадиях. В данном докладе обсуждаются методы и алгоритмы, используемые в таких системах, включая учет поведенческих аномалий, анализ сетевого трафика и обнаружение атак на основе сигнатур. Также приводятся примеры практического применения таких систем и их роль в обеспечении безопасности информационной инфраструктуры организации. Подчеркивается важность постоянного мониторинга и

обновления таких систем, чтобы быть эффективными в обнаружении новых и продвинутых методов атаки.

Система обнаружения первоначального доступа нарушителя в информационную систему (анализатор, IDS) – это инструмент, предназначенный для выявления и реагирования на попытки несанкционированного доступа к компьютерным сетям и информации.

Задачей такой системы является обнаружение и анализ сетевого трафика и его сравнение с предопределенными правилами и шаблонами. При обнаружении подозрительной активности система сигнализирует об инциденте и принимает меры по его блокированию или реагированию на него.

Основная цель системы обнаружения первоначального доступа – предотвращение вторжений, а также своевременное выявление и устранение уязвимостей в информационной системе. Она способна обнаруживать различные виды атак, включая внедрение вредоносного кода, сканирование портов, подбор паролей и другие методы несанкционированного доступа к системе.

Плюсы использования системы обнаружения первоначального доступа включают:

- Возможность обнаружения и блокирования атак на ранних стадиях, помогая предотвратить ущерб и негативные последствия для организации.
- Повышение уровня безопасности и защиты системы путем обнаружения новых и неизвестных атак, которые могут обойти традиционные средства защиты.
- Улучшение возможностей реагирования на инциденты безопасности и проведение детального анализа произошедших событий.
- Сокращение времени, затрачиваемого на обнаружение и реагирование на нарушения безопасности.

Однако, следует учесть, что система обнаружения первоначального доступа не является панацеей для всех угроз и уязвимостей. Ее эффективность может быть ограничена, особенно в случае новых и неизвестных угроз. Поэтому, для полноценной защиты информационной системы, рекомендуется комбинировать ее использование с другими методами и средствами безопасности.

Основная часть. Рассмотрим системы IPS и IDS.

IDS расшифровывается как Intrusion Detection System — система обнаружения вторжений. IPS, или Intrusion Prevention System, — система предотвращения вторжений. По сравнению с традиционными средствами защиты — антивирусами, спам-фильтрами, файерволами — IDS/IPS обеспечивают гораздо более высокий уровень защиты сети.

Антивирус анализирует файлы, спам-фильтр анализирует письма, файервол — соединения по IP. IDS/IPS анализируют данные и сетевое поведение. Продолжая аналогию с хранителями правопорядка, файервол, почтовые фильтры и антивирус — это рядовые сотрудники, работающие «в поле», а системы обнаружения и предотвращения вторжений — это старшие по рангу офицеры, которые работают в отделении. Рассмотрим эти системы подробнее.

Архитектура и технология IDS.

Принцип работы IDS заключается в определении угроз на основании анализа трафика, но дальнейшие действия остаются за администратором. Системы IDS делят на типы по месту установки и принципу действия.

Виды IDS по месту установки.

Два самых распространенных вида IDS по месту установки:

- Network Intrusion Detection System (NIDS);
- Host-based Intrusion Detection System (HIDS).

Первая работает на уровне сети, а вторая — только на уровне отдельно взятого хоста.

Сетевые системы обнаружения вторжения (NIDS).

Технология NIDS дает возможность установить систему в стратегически важных местах сети и анализировать входящий/исходящий трафик всех устройств сети. NIDS анализируют трафик на глубоком уровне, «заглядывая» в каждый пакет с канального уровня до уровня приложений.

NIDS отличается от межсетевого экрана, или файервола. Файервол фиксирует только атаки, поступающие снаружи сети, в то время как NIDS способна обнаружить и внутреннюю угрозу.

Сетевые системы обнаружения вторжений контролируют всю сеть, что позволяет не тратиться на дополнительные решения. Но есть недостаток: NIDS отслеживают весь сетевой трафик, потребляя большое количество ресурсов. Чем больше объем трафика, тем выше потребность в ресурсах CPU и RAM. Это приводит к заметным задержкам обмена данными и снижению скорости работы сети. Большой объем информации также может «ошеломить» NIDS, вынудив систему пропускать некоторые пакеты, что делает сеть уязвимой.

Хостовая система обнаружения вторжений (HIDS).

Альтернатива сетевым системам — хостовые. Такие системы устанавливаются на один хост внутри сети и защищают только его. HIDS также анализируют все входящие и исходящие пакеты, но только для одного устройства. Система HIDS работает по принципу создания снапшотов файлов: делает снимок текущей версии и сравнивает его с предыдущей, тем самым выявляя возможные угрозы. HIDS лучше устанавливать на критически важные машины в сети, которые редко меняют конфигурацию.

Другие разновидности IDS по месту установки.

Кроме NIDS и HIDS, доступны также PIDS (Perimeter Intrusion Detection Systems), которые охраняют не всю сеть, а только границы и сигнализируют об их нарушении.

Еще одна разновидность — VMIDS (Virtual Machine-based Intrusion Detection Systems). Это разновидность систем обнаружения угрозы на основе технологий виртуализации. Такая IDS позволяет обойтись без развертывания системы обнаружения на отдельном устройстве. Достаточно развернуть защиту на виртуальной машине, которая будет отслеживать любую подозрительную активность.

Виды IDS по принципу действия.

Все системы обнаружения атак IDS работают по одному принципу — поиск угрозы путем анализа трафика. Отличия кроются в самом процессе анализа. Существует три основных вида: сигнатурные, основанные на аномалиях и основанные на правилах.

Сигнатурные IDS.

IDS этой разновидности работают по схожему с антивирусным программным обеспечением принципу. Они анализируют сигнатуры и сопоставляют их с базой, которая должна постоянно обновляться для обеспечения корректной работы. Соответственно, в этом заключается главный недостаток сигнатурных IDS: если по каким-то причинам база недоступна, сеть становится уязвимой. Также если атака новая и ее сигнатура неизвестна, есть риск того, что угроза не будет обнаружена.

Сигнатурные IDS способны отслеживать шаблоны или состояния. Шаблоны — это те сигнатуры, которые хранятся в постоянно обновляемой базе. Состояния — это любые действия внутри системы.

Начальное состояние системы — нормальная работа, отсутствие атаки. После успешной атаки система переходит в скомпрометированное состояние, то есть заражение прошло успешно. Каждое действие (например, установка соединения по протоколу, не соответствующему политике безопасности компании, активизация ПО и т.д.) способно изменить состояние. Поэтому сигнатурные IDS отслеживают не действия, а состояние системы.

Как можно понять из описания выше, NIDS чаще отслеживают шаблоны, а HIDS — в основном состояния.

IDS, основанные на аномалиях.

Данная разновидность IDS по принципу работы в чем-то схожа с отслеживанием состояний, только имеет больший охват.

IDS, основанные на аномалиях, используют машинное обучение. Для правильной работы таких систем обнаружения угроз необходим пробный период обучения. Администраторам рекомендуется в течение первых нескольких месяцев полностью отключить сигналы тревоги, чтобы система обучалась. После тестового периода она готова к работе.

Система анализирует работу сети в текущий момент, сравнивает с аналогичным периодом и выявляет аномалии. Аномалии делятся на три категории:

- Статистические;
- аномалии протоколов;
- аномалии трафика.

Статистические аномалии выявляются, когда система IDS составляет профиль штатной активности (объем входящего/исходящего трафика, запускаемые приложения и т.д.) и сравнивает его с текущим профилем. Например, для компании характерен рост трафика по будним дням на 90%. Если трафик вдруг возрастет не на 90%, а на 500%, то система оповестит об угрозе.

Для выявления аномалий протоколов IDS-система анализирует коммуникационные протоколы, их связи с пользователями, приложениями и составляет профили. Например, веб-сервер должен работать на порту 80 для HTTP и 443 для HTTPS. Если для передачи информации по HTTP или HTTPS будет использоваться другой порт, IDS пришлет уведомление.

Также IDS способны выявлять аномалии, любую небезопасную или даже угрожающую активность в сетевом трафике. Рассмотрим, к примеру, случай DoS-атаки. Если попытаться провести такую атаку «в лоб», ее распознает и остановит даже файервол. Креативные злоумышленники могут рассылать пакеты с разных адресов (DDoS), что уже сложнее выявить. Технологии IDS анализируют сетевой трафик и заблаговременно предотвращают подобные атаки.

Заключение. В ходе данного доклада была рассмотрена проблема обнаружения первоначального доступа нарушителя в информационную систему. Были изучены различные методы и подходы к обнаружению таких угроз, а также рассмотрены основные принципы функционирования систем обнаружения.

Эффективное обнаружение первоначального доступа нарушителя требует комплексного подхода, включающего в себя как технические средства, так и процессы мониторинга и анализа данных. Кроме того, важным фактором является обновление и совершенствование систем обнаружения в соответствии с появляющимися угрозами.

Обнаружение первоначального доступа нарушителя в информационную систему является критически важным этапом в обеспечении безопасности данных и защите от кибератак. Развитие и совершенствование средств обнаружения является необходимым шагом для эффективной защиты информационных ресурсов.

Несмотря на сложность задачи обнаружения первоначального доступа нарушителя, современные технологии и методики позволяют создавать более надежные и эффективные системы обнаружения. Дальнейшие исследования и разработки в этой области могут значительно улучшить уровень безопасности информационных систем.

Список литературы

1. IDS / IPS (Intrusion Detection and Prevention System) [Электронный ресурс]. –Режим доступа: https://cloudnetworks.ru/inf-bezopasnost/ids-ips/ - Дата доступа: 14.02.2024.

2. Cybersecurity and Technology Controls [Электронный ресурс]. –Режим доступа: https://www.mitre.org/publications/technical-papers/cybersecurity-and-technology-controls Дата доступа: 16.02.2024.

3. IPS / IDS системы. Обнаружение и предотвращение вторжений [Электронный ресурс]. – Режим доступа: https://www.securityvision.ru/blog/obnaruzhenie-i-predotvrashchenie-vtorzheniy/ Дата доступа: 16.02.2024.

UDC 004.056.53

SYSTEM ZUR ERKENNUNG DES ERSTZUGRIFFS VON EINDRINGLINGEN IN EIN INFORMATIONSSYSTEM

Dedkov V.N.

gr.367241

Belarussische Staatliche Universität für Informatik und Radioelektronik, Minsk, Republik Belarus

Wissenschaftlicher Leiter: Borbotko T.V. - Doktor der Technischen Wissenschaften, Leiter des Lehrstuhls für Informationssicherheit

Zusammenfassung. Der Bericht behandelt die grundlegenden Arbeitsprinzipien, Architekturen und Technologien, Aufgaben und Ziele von Intrusion Detection Systems (IDS) und Intrusion Prevention Systems (IPS).

Schlüsselwörter: Intrusion Detection Systems (IDS) und Intrusion Prevention Systems (IPS).