МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ
«БРЕСТСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
ФАКУЛЬТЕТ ЭЛЕКТРОННО-ИНФОРМАЦИОННЫХ СИСТЕМ
Кафедра интеллектуальных информационных технологий

РЕФЕРАТ

по дисциплине

«Современные методы защиты компьютерных систем»

Выполнила:
студентка 4-го курса,
ФЭИС,
группы ИИ-22
Сокол С.М.

Брест 2024

Вариант 3

1 ТЕМА 1 – NetFlow

NetFlow представляет собой мощную технологию мониторинга и анализа сетевого трафика, разработанную компанией Cisco. Она позволяет детально отслеживать и анализировать информацию о потоках данных, проходящих через сеть, фиксируя такие параметры, как IP-адреса источника и назначения, порты, протоколы, объём переданных данных и временные метки. Эта технология обеспечивает не только глубокое понимание текущих сетевых процессов, но и даёт возможность оперативно реагировать на возникающие угрозы или изменения в структуре трафика. Благодаря этим возможностям, NetFlow широко используется для повышения безопасности, оптимизации работы сетей и планирования их масштабирования. Сегодня NetFlow внедряется не только на устройствах Cisco, но и поддерживается в ряде других сетевых решений, что делает её универсальным инструментом анализа.

Основные аспекты работы NetFlow:

Сбор статистики – технология фиксирует ключевые параметры каждого сетевого потока, включая IP-адреса, порты, протоколы, объём переданных данных и временные метки. Эти данные формируют основу для анализа и построения графиков сетевой активности, позволяя увидеть картину использования сети в реальном времени.

Пример: администратор сети может с помощью NetFlow определить, что определённое устройство генерирует аномально высокий трафик, что может указывать на заражение вредоносным ПО или попытку несанкционированного доступа.

Анализ трафика – с помощью собранной статистики можно строить детализированные отчёты, отслеживать аномалии, выявлять подозрительную активность и эффективно распределять сетевые ресурсы. Анализ данных помогает выявлять источники нагрузки, потенциальные атаки или неправильно настроенные устройства, а также улучшать общее управление сетью.

Пример: при анализе можно определить пики нагрузки, вызванные DDoS-атакой, и принять меры по её нейтрализации, включая использование механизмов фильтрации или ограничения доступа.

Интеграция с системами безопасности – NetFlow активно используется в системах обнаружения вторжений (IDS) и предотвращения атак (IPS). Собранная информация помогает в настройке правил и фильтров для предотвращения DDoS-атак, несанкционированного доступа или утечек данных.

Например, интеграция NetFlow с SIEM-системами позволяет отслеживать угрозы в реальном времени и уведомлять команду безопасности о подозрительных событиях.

Долгосрочное хранение и тренды – хранение исторических данных о трафике позволяет анализировать тренды использования сети, что полезно для планирования апгрейдов инфраструктуры и оценки потребностей в пропускной

способности. Кроме того, долгосрочные данные могут использоваться для судебной экспертизы или внутреннего аудита.

Пример: администратор может использовать данные NetFlow для прогнозирования роста трафика и определения момента, когда потребуется увеличить пропускную способность сети, а также для идентификации потенциальных узких мест.

Преимущества технологии NetFlow:

- обеспечивает прозрачность сетевого трафика;
- позволяет быстро выявлять неисправности и аномалии;
- снижает риски, связанные с атаками, за счёт раннего обнаружения подозрительной активности;
- улучшает планирование и модернизацию сети;
- снижает затраты на эксплуатацию благодаря оптимизации использования ресурсов.

2 ТЕМА 2 – WAF (Web Application Firewall)

WAF, или веб-аппликационный файрвол, представляет собой комплекс программных мониторов и фильтров, которые используются для обнаружения и предотвращения сетевых атак на веб-приложения. Устанавливаясь между веб-ресурсом и внешними запросами, WAF анализирует весь входящий и исходящий HTTP-трафик на предмет вредоносной активности. Эта технология особенно актуальна для защиты сайтов и веб-сервисов, работающих с конфиденциальными данными.

Основные возможности WAF:

Анализ запросов – WAF проверяет все HTTP-запросы на наличие вредоносного кода, следуя различным подходам, таким как сигнатурный анализ, правила и механизмы анализа аномалий. Современные WAF могут также использовать нейросети и индикаторы атак для повышения эффективности.

Пример: WAF может обнаружить попытки SQL-инъекций или XSS-атак и заблокировать их до того, как они нанесут вред системе.

Действия при обнаружении угроз – при обнаружении подозрительного запроса WAF может:удалить из запроса опасные данные (по аналогии с антивирусом, который лечит заражённые файлы), полностью заблокировать запрос, заблокировать источник атаки на уровне сети, что предотвращает дальнейшие обращения с данного IP.

Пример: если злоумышленник пытается внедрить скрипт через форму ввода, WAF может автоматически удалить этот скрипт или заблокировать отправителя, предотвращая повторные попытки атак.

Сигнатуры – представляют собой набор байтов, соответствие которым проверяется в передаваемых данных. Этот подход позволяет быстро и эффективно обнаруживать известные угрозы. Однако злоумышленники могут обфусцировать вредоносную нагрузку, что снижает эффективность метода.

Пример: WAF может сравнить входящий трафик с базой известных атак и

обнаружить совпадения, предотвращая возможное внедрение эксплойтов.

Правила – использование правил позволяет выявлять новые типы атак на основе анализа поведения запросов. Для их разработки может применяться машинное обучение, но это требует значительных вычислительных ресурсов.

Пример: WAF может определить, что определённый пользователь делает слишком много запросов за короткий промежуток времени, что может быть признаком автоматизированной атаки или попытки взлома.

Интеграция с DevOps – современные WAF могут интегрироваться в процессы CI/CD, обеспечивая безопасность веб-приложений на этапе их разработки и развертывания. Это позволяет быстрее устранять уязвимости и предотвращать возможные угрозы ещё до выхода приложения в продакшн.

Почему WAF необходим для бизнеса:

- защита от угроз, которые обходят традиционные файрволы;
- защита клиентских данных от утечек и кибератак;
- поддержка соответствия нормативным требованиям, таким как PCI DSS;
- обеспечение непрерывной работы веб-приложений;
- снижение затрат на устранение последствий атак.

3 ТЕМА – Deshadow и Desync

Deshadow и Desync – это техники атак на веб-приложения, основанные на несоответствиях в обработке данных между различными компонентами системы. Такие атаки используют разницу в интерпретации данных сервером, клиентом или прокси, что позволяет злоумышленникам обходить механизмы защиты, внедрять вредоносные данные или получать несанкционированный доступ.

Deshadow

Атака Deshadow направлена на обход авторизации или сокрытие вредоносных действий. Основной механизм – использование слабостей в обработке сессий, токенов или динамического контента.

Проблемы обработки данных – различные компоненты системы (например, веб-сервер и прокси) могут интерпретировать одни и те же данные по-разному, создавая уязвимости.

Пример: злоумышленник может подделать токен авторизации, который будет принят одной частью системы и отклонен другой.

Манипуляция сессиями – злоумышленники могут использовать методы переподмены сессий для обхода ограничений доступа.

Desync (HTTP Request Smuggling)

Desync-атака использует расхождения в обработке HTTP-запросов между сервером и прокси или другими промежуточными системами. Цель атаки – внедрение вредоносных запросов или данных.

Пример атаки – злоумышленник отправляет запрос с конфликтующими заголовками. Один сервер воспринимает часть запроса как завершённую, а другой – продолжает обработку. Это создаёт возможность для внедрения нового запроса.

Пример: отправка запроса с некорректным заголовком Content-Length для разделения одного HTTP-запроса на два.

Методы защиты:

- использование актуальных версий ПО;
- конфигурирование серверов для исключения конфликтов;
- интеграция с WAF для отслеживания и блокировки подозрительных запросов;
- проведение регулярного тестирования на уязвимости.

4 ТЕМА – DNS, ICMP и SSH

DNS (Domain Name System)

DNS, или система доменных имен, представляет собой иерархическую систему имен, используемую для преобразования читаемых доменных имен (например, www.example.com) в числовые IP-адреса (например, 192.0.2.1), которые компьютеры используют для связи друг с другом.

Ключевые аспекты:

- Структура DNS: объясните иерархию DNS, включая корневые серверы, домены верхнего уровня (TLD), и вторичные домены. Опишите, как работает процесс разрешения имен, включая рекурсивные и авторитетные серверы;
- Типы записей DNS: рассмотрите различные типы записей DNS, такие как A (адрес), AAAA (IPv6 адрес), CNAME (псевдоним), MX (почтовый обменник) и TXT (текстовая запись);
- DNSSEC (DNS Security Extensions): объясните, как DNSSEC повышает безопасность DNS, добавляя цифровые подписи к записям, чтобы предотвратить атаки типа "человек посередине";
- Атаки на DNS: обсудите распространенные уязвимости, такие как DNS Spoofing и DDoS-атаки на DNS-серверы.

ICMP (Internet Control Message Protocol)

ICMP – это сетевой протокол, который используется для передачи сообщений об ошибках и информационных сообщений между узлами сети. ICMP является частью протокольного стека IP и обычно используется для диагностики и управления сетевыми соединениями.

Ключевые аспекты:

- Функции ICMP: опишите основные функции ICMP, такие как диагностика сетевых проблем, передача сообщений об ошибках (например, Destination Unreachable) и отправка запросов (например, Echo Request и Echo Reply);
- Использование ICMP: обсудите инструменты, использующие ICMP, такие как Ping (для проверки доступности узла) и Traceroute (для определения маршрута к узлу);
- Безопасность ICMP: осветите риски безопасности, связанные с использованием ICMP, такие как ICMP Flood и Ping of Death, а также

методы защиты от них;
- Различия между ICMP и другими протоколами: сравните ICMP с другими транспортными протоколами, такими как TCP и UDP, в контексте их функций и областей применения.

SSH (Secure Shell)

SSH – это протокол сетевой безопасности, который предоставляет безопасный доступ к удаленным системам через незащищенные сети. Он позволяет пользователям управлять серверами и выполнять команды на удаленных машинах с высокой степенью защиты.

Ключевые аспекты:

- Структура SSH: объясните, как SSH использует симметричное и асимметричное шифрование для обеспечения безопасности данных. Обсудите механизмы аутентификации, такие как пароли и ключи SSH;
- Компоненты SSH: опишите основные компоненты, такие как SSH-клиент, SSH-сервер и SSH-ключи. Обсудите, как происходит установка соединения и обмен ключами;
- Преимущества SSH: Обсудите преимущества использования SSH по сравнению с другими протоколами, такими как Telnet, включая шифрование данных и защиту от атак;
- Использование SSH в практических задачах: приведите примеры использования SSH для администрирования серверов, передачи файлов (с помощью SCP и SFTP) и создания туннелей.