Вопрос 1) NetFlow.

NetFlow — это технология от Cisco, предназначенная для мониторинга и анализа сетевого трафика. Она позволяет собирать и анализировать информацию о потоках данных в сети.

Сбор статистики: регистрирует информацию о каждом сетевом потоке, включая IP-адреса отправителя и получателя, используемые порты, протоколы, объем переданных данных и временные метки.Вопрос

2) WAF

Web Application Firewall (WAF) — это программное решение, предназначенное для защиты веб-приложений от сетевых атак. WAF устанавливается перед защищаемым веб-ресурсом и анализирует все входящие HTTP-запросы, проверяя их на наличие вредоносного кода и потенциально опасной активности.

Принципы работы WAF:

1. **Анализ трафика:**

- WAF использует сигнатуры, правила и методы анализа аномалий для обнаружения угроз.

- В некоторых случаях применяются нейронные сети и индикаторы атак для повышения эффективности.

2. **Действия при обнаружении угроз:**

- Опасные данные в запросе могут быть удалены, как это делает антивирус с зараженными файлами.

- Запрос может быть полностью заблокирован.

- Возможно блокирование источника атаки на уровне IP-адреса, предотвращая дальнейшие обращения.

Механизмы защиты WAF:

1. **Сигнатуры:**

- Представляют собой набор байт, соответствие которым проверяется в передаваемых данных.

- Обнаружение сигнатуры в запросе приводит к его блокировке.

- Ограничения метода:

  - Возможность обхода сигнатур за счет обфускации вредоносного кода.

  - Необходимость своевременного обновления базы для защиты от новых атак.

2. **Правила:**

- Используются для выявления атак на основе анализа поведения запросов.

- Позволяют обнаруживать даже неизвестные угрозы.

- Недостатки:

  - Высокая трудоемкость создания правил вручную.

  - Значительные затраты ресурсов при использовании машинного обучения для автоматической настройки.

Машинное обучение в WAF может повысить адаптивность системы, но требует мощного оборудования и сложной реализации.

Вопрос 3) Deshadow, Desync

Эти термины связаны с методами атак на веб-приложения, использующих несоответствия в обработке данных между различными компонентами системы или уровнями сетевой инфраструктуры. Такие атаки используют разницу в понимании данных клиентом, сервером, прокси или другими промежуточными системами, что позволяет злоумышленникам обходить механизмы защиты, внедрять вредоносные данные или получать несанкционированный доступ.

Deshadow — это атака, цель которой состоит в том, чтобы обойти механизмы авторизации или скрыть вредоносные действия, используя слабости в реализации системы. Чаще всего используется при работе с веб-приложениями, имеющими проблемы в обработке сессий, токенов или другого динамического контента.

Несоответствие обработчиков данных: Проблемы возникают, когда различные компоненты системы (например, веб-сервер и прокси) интерпретируют данные по-разному.

Desync-атака (или HTTP Request Smuggling) — это тип атаки, при которой злоумышленник использует расхождения в обработке HTTP-запросов между сервером и прокси-сервером или другими промежуточными системами. Это

позволяет внедрять вредоносные запросы, нарушать работу приложений или красть данные пользователей.

Разделение запросов: Злоумышленник отправляет запрос с противоречивыми заголовками. Один сервер интерпретирует часть запроса как завершённую, а другой продолжает его обработку, что позволяет внедрять новый запрос или данные.

Deshadow и Desync — это серьезные угрозы для веб-приложений, которые используют недостатки в обработке данных для обхода авторизации, кражи данных и внедрения вредоносных запросов. Эти атаки сложны для обнаружения, но современные WAF, регулярное тестирование приложений и настройка серверов могут значительно снизить риск их успешной реализации.

Вопрос 4) DNS, ICMP, SSH

DNS:
DNS (Domain Name System) – это система, которая переводит понятные человеку доменные имена в IP-адреса, которые используют компьютеры для связи друг с другом. Представьте, что DNS – это как телефонная книга интернета. В обычной телефонной книге, если вам нужно найти номер телефона человека, вы ищете его по имени, и книга предоставляет вам номер. Точно так же DNS помогает находить IP-адреса, когда вы вводите доменное имя.

Когда вы вводите адрес веб-сайта, например, , в строку браузера, DNS помогает найти нужный IP-адрес, чтобы ваш браузер мог подключиться к нужному серверу. IP-адрес – это уникальный числовой идентификатор, который используется для идентификации устройства в сети. Всякий раз, когда вы отправляете запрос на веб-сайт, ваш браузер отправляет этот запрос через интернет на сервер, который затем отвечает данными, которые вы видите на экране.

Процесс начинается с того, что ваш компьютер или устройство отправляет запрос на ближайший DNS-сервер, который обычно предоставляется вашим интернет-провайдером. Этот сервер называется рекурсивным резолвером. Если этот сервер знает нужный IP-адрес, он возвращает его вашему браузеру. Если нет, запрос передается на другие DNS-серверы, пока не будет найден правильный адрес.

Рекурсивный резолвер: если записи нет в локальном кеше, запрос отправляется на рекурсивный DNS-сервер. Этот сервер выполняет роль посредника, который ищет нужную информацию, обращаясь к другим серверам.

Корневые серверы: если рекурсивный сервер не знает IP-адрес, он отправляет запрос на один из корневых серверов. Корневые серверы знают, какой сервер отвечает за каждый домен верхнего уровня (TLD), такой как .com, .net, .org и так далее.

Авторитетный сервер: сервер TLD (например, для .com) отвечает, какой сервер управляет доменом example.com. Рекурсивный резолвер направляет запрос на

авторитетный DNS-сервер для example.com, который содержит точные данные о домене.

Возвращение IP-адреса: авторитетный сервер возвращает IP-адрес, связанный с example.com, рекурсивному резолверу, который, в свою очередь, возвращает его вашему браузеру.

Подключение к веб-сайту: теперь, когда браузер знает IP-адрес, он может отправить запрос непосредственно на сервер, чтобы загрузить содержимое веб-сайта.

Корневые серверы: на вершине иерархии находятся корневые серверы. Эти серверы являются начальной точкой для всех DNS-запросов. В мире существует всего 13 корневых серверов, но каждый из них дублирован на множество серверов по всему миру для обеспечения надежности и доступности. Корневые серверы содержат информацию о доменах верхнего уровня (TLD) и направляют запросы к соответствующим серверам.

Домен верхнего уровня (TLD): под корневыми серверами находятся сервера доменов верхнего уровня (TLD), таких как .com, .net, .org, .ru и другие. Эти сервера управляют определенными доменными зонами. Например, сервер для домена .com знает, какие авторитетные серверы управляют доменами второго уровня в зоне .com. Серверы TLD обеспечивают организацию и управление доменами верхнего уровня и направляют запросы к авторитетным серверам, которые содержат детальную информацию о доменах второго уровня.

Авторитетные серверы: на следующем уровне находятся авторитетные DNS-серверы. Эти серверы содержат информацию о конкретных доменах и отвечают на запросы о них. Например, авторитетный сервер для example.com содержит записи, которые указывают на IP-адреса, связанные с этим доменом. Авторитетные серверы предоставляют окончательную информацию, необходимую для завершения DNS-запроса.

Рекурсивные резолверы: резолвер - это важный компонент системы доменных имен (DNS), который служит посредником между конечным пользователем и сетью DNS-серверов, обеспечивая преобразование доменных имен в IP-адреса. Когда пользователь вводит адрес веб-сайта в браузере или запускает приложение, которое требует доступа к интернет-ресурсам, запрос на преобразование доменного имени в IP-адрес отправляется именно рекурсивному резолверу. Резолверы получают запросы от пользователей и выполняют весь процесс поиска нужной информации, обращаясь к другим DNS-серверам. Начинают они с корневых серверов, затем обращаются к серверам TLD и авторитетным серверам, пока не найдут нужный IP-адрес. Рекурсивные резолверы часто предоставляются интернет-провайдерами (ISP) или публичными сервисами, такими как Google Public DNS или Cloudflare DNS. Они кешируют ответы на определённое время, чтобы ускорить последующие запросы к тому же доменному имени.

Каждый из этих уровней играет важную роль в обеспечении надежной и эффективной работы DNS-системы. Корневые серверы, сервера TLD и авторитетные серверы работают вместе, чтобы обеспечить быстрое и точное разрешение доменных имен в IP-адреса.