**Вопрос 1) NetFlow.**

**NetFlow** — это технология, разработанная Cisco для мониторинга и анализа сетевого трафика. Она используется для сбора и анализа данных о потоках трафика в сети.

**Основные функции:**

1. **Сбор статистики**: фиксирует данные о каждом сетевом потоке, включая IP-адреса источника и назначения, порты, протоколы, объем переданных данных и время.
2. **Мониторинг производительности**: позволяет анализировать, как используется сеть.
3. **Обеспечение безопасности**: помогает выявлять аномалии в сетевом трафике, которые могут свидетельствовать о кибератаках.
4. **Оптимизация сети**: помогает администратору обнаруживать узкие места в сети.

**Как работает:**

1. Устройства (например, маршрутизаторы и коммутаторы) собирают данные о потоках.
2. Эти данные передаются на сервер NetFlow Collector для анализа.
3. Анализируются потоки для определения, откуда и куда идет трафик, а также его объем.

**Применение:**

* Обнаружение DoS-атак.
* Анализ использования полосы пропускания.
* Планирование сети.

**Альтернативы:**

* sFlow, IPFIX (усовершенствованный стандарт NetFlow).

NetFlow — мощный инструмент для управления и защиты сетей.

**Вопрос 2) WAF**

Web application firewall (WAF) — это совокупность программных мониторов и фильтров, предназначенных для обнаружения и блокирования сетевых атак на веб-приложение. WAF устанавливается перед защищаемым веб ресурсом и анализирует все передаваемые HTTP запросы на наличие вредоносного кода и потенциально опасную активность злоумышленников. При проведении анализа WAF основывается на различных механизмах сигнатурного анализа, правилах, средствах анализа аномалий. Также в своей работе WAF могут использовать нейросети и различные индикаторы атак.

В случае обнаружения плохих запросов WAF может выполнить следующие действия: удалить из запроса опасные данные по аналогии с тем, как антивирус пытается лечить зараженные файлы, также запрос может быть заблокирован целиком. Так возможна блокировка источника атаки на сетевом уровне, то есть, мы блокируем все обращения с данного IP.

По аналогии с другими средствами защиты WAF используют различные механизмы для выявления опасных активностей. Такими механизмами является использование сигнатур и правил.

Сигнатуры, это по сути набор байт на соответствие которым анализируются передаваемые данные. Сигнатуры построены по принципу вхождения определенной последовательности символов в запрос. Если при анализе сигнатура обнаружена - запрос блокируется. И чем точнее составлен набор сигнатур, тем выше вероятность отразить атаку. Проблема такого подхода заключается в том, что злоумышленник может обфусцировать передаваемую вредоносную нагрузку, то есть поменять передаваемый набор байт и тем самым попытаться обойти WAF. Ну а кроме того, базы сигнатур могут не содержать сигнатуры самых актуальных атак по причине того, что разработчики еще их не написали для самых новых атак.

Альтернативным или дополняющим вариантом является использование правил. Правила для выявления атак теоретически позволяют выявлять даже новые атаки на основе анализа поведения запросов. Однако, для составления правил вручную требуются значительные ресурсы. И в качестве решения разработчики WAF часто используют машинное обучение, когда система сама какое-то время обучается на передаваемых данных. Недостатками использования машинного обучения являются высокие требования к аппаратным ресурсам и сложность 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.

**ICMP (Internet Control Message Protocol)** — это сетевой протокол, используемый для обмена диагностической информацией и управления сетевыми соединениями в среде TCP/IP. Он играет ключевую роль в работе сети, позволяя устройствам передавать сообщения об ошибках, оповещать о недоступности узлов или маршрутов, а также сообщать о перегрузке сети.

Протокол ICMP не используется для передачи данных между приложениями. Вместо этого он обеспечивает вспомогательные функции, поддерживая корректную работу других протоколов, таких как IP. Например, когда маршрутизатор не может доставить пакет из-за ошибки, он отправляет сообщение ICMP отправителю, уведомляя о проблеме. Такие сообщения могут содержать информацию о недоступности хоста, превышении времени жизни пакета (TTL) или достижении предельной нагрузки маршрутизатора.

ICMP также используется для диагностики и мониторинга сети. Одним из самых известных примеров его применения является команда ping, которая отправляет ICMP-запросы на целевой узел, измеряя время отклика и проверяя доступность устройства. Еще одной распространенной командой является traceroute, которая отслеживает маршрут пакета до целевого хоста, предоставляя информацию о промежуточных узлах.

Несмотря на свою полезность, ICMP может быть использован злоумышленниками для проведения атак. Например, ICMP flood — это атака, при которой сеть или устройство перегружаются большим количеством запросов, что приводит к недоступности сервиса. Еще один пример — Smurf-атака, при которой ICMP-запросы с подмененным IP-адресом отправляются на широковещательный адрес, перегружая целевую систему множеством ответов.

Чтобы защититься от злоупотреблений ICMP, сети часто ограничивают его использование, фильтруя подозрительные запросы или отключая ненужные функции на устройствах. Однако полное отключение ICMP может затруднить диагностику и устранение неполадок в сети, поэтому важно настроить протокол так, чтобы он оставался полезным инструментом без значительных рисков для безопасности.

**SSH (Secure Shell)** — это криптографический сетевой протокол, предназначенный для безопасного удаленного управления компьютерами и передачи данных по незащищенным сетям, таким как интернет. Он обеспечивает шифрование всех передаваемых данных, включая команды, результаты их выполнения и аутентификационные данные, что делает невозможным их перехват или изменение. SSH используется для удаленного подключения к серверам, управления ими и выполнения различных команд. Основным преимуществом SSH является его высокая безопасность по сравнению с более старыми протоколами, такими как Telnet или Rlogin, которые не обеспечивают шифрования. В SSH используется публично-ключевая криптография для аутентификации, что позволяет гарантировать, что к серверу подключается только доверенное устройство. Протокол также включает механизмы защиты от атак типа "man-in-the-middle" и обеспечения целостности данных. SSH имеет множество применений, включая безопасную передачу файлов через SCP (Secure Copy Protocol) и SFTP (Secure File Transfer Protocol).