Пассивные сетевые атаки.

Пассивные сетевые атаки - это тип атак, при котором злоумышленник перехватывает или наблюдает за сетевым трафиком без вмешательства в него или изменения его содержимого. В отличие от активных атак, где злоумышленник активно взаимодействует с системой или сетью, пассивные атаки в основном направлены на получение информации и незаметное наблюдение за действиями пользователей и ресурсами сети.

Вот несколько распространенных примеров пассивных сетевых атак:

Перехват трафика (Traffic Sniffing): Злоумышленник использует снифферы (инструменты для перехвата сетевого трафика) для мониторинга сетевого трафика и анализа передаваемых данных. Это позволяет злоумышленнику получить доступ к конфиденциальной информации, такой как логины, пароли, данные банковских карт и другие секретные данные, передаваемые в сети без использования шифрования.

Пассивное подслушивание (Passive Eavesdropping): Злоумышленник пассивно прослушивает и записывает сетевой трафик, чтобы получить доступ к конфиденциальной информации, передаваемой между устройствами. Например, злоумышленник может использовать методы подслушивания Wi-Fi сетей или прослушивание сетевых кабелей для перехвата данных.

Анализ трафика (Traffic Analysis): Злоумышленник анализирует метаданные и характеристики сетевого трафика, не расшифровывая его содержимое. Например, злоумышленник может анализировать размер пакетов, их время передачи, источники и назначения, чтобы получить информацию о действиях пользователей, посещаемых веб-сайтах, потоке работы и других аспектах сетевой активности.

Отслеживание (Tracking): Злоумышленник использует различные методы для отслеживания активности пользователей в сети, такие как использование файлов cookie, скрытых пикселей (web beacons) или других технологий отслеживания. Это позволяет злоумышленнику получить информацию о привычках и предпочтениях пользователя для использования в маркетинговых целях или в киберпреступной деятельности.

Целью пассивных сетевых атак является получение конфиденциальной информации, разведка, выявление уязвимостей в сети или мониторинг действий пользователей без их согласия.

Сканирование сети

Сканирование сети - это процесс исследования и обнаружения устройств, хостов и сервисов, находящихся в сети, а также выявления уязвимостей и конфигурационных проблем. Сканирование сети позволяет администраторам сети получить информацию о структуре сети, обнаружить несанкционированные устройства или службы, а также выявить уязвимости для последующего обеспечения безопасности.

Способы обнаружения хостов: ICMP; ARP; RST сегменты TCP; Ответы на несуществующие DNS-запросы; Прослушивание трафика и т.д.

Вот некоторые инструменты, которые можно использовать для сканирования сети:

Nmap: Nmap (Network Mapper) является одним из наиболее популярных инструментов для сканирования сети. Он позволяет обнаруживать хосты, сканировать открытые порты, определять используемые службы, анализировать операционные системы и многое другое. Nmap поддерживает различные методы сканирования и имеет гибкие настройки.

Wireshark: Wireshark представляет собой мощный анализатор сетевого трафика, который позволяет захватывать и анализировать пакеты данных, передаваемые по сети. С помощью Wireshark можно изучить сетевую активность, идентифицировать потенциальные проблемы, анализировать протоколы и трафик, а также обнаруживать уязвимости.

Nessus: Nessus - это популярный инструмент для сканирования уязвимостей. Он автоматизирует процесс обнаружения и классификации уязвимостей в системах и сетях. Nessus может выполнять сканирование уязвимостей хостов, веб-приложений, баз данных и других компонентов сети, предоставляя детальную информацию о найденных проблемах.

OpenVAS: OpenVAS (Open Vulnerability Assessment System) - это открытый инструмент для сканирования уязвимостей, который является альтернативой коммерческому продукту Nessus. OpenVAS обнаруживает уязвимости в системах, операционных системах, сетевых протоколах и других компонентах, а также предоставляет рекомендации по устранению проблем.

Nikto: Nikto - это инструмент для сканирования веб-серверов с целью обнаружения уязвимостей и потенциальных проблем безопасности. Он ищет известные уязвимости веб-приложений, проверяет наличие незащищенных файлов и настройки сервера, а также осуществляет анализ на наличие скрытых директорий и файлов.

Это только некоторые из инструментов, доступных для сканирования сети. Важно отметить, что сканирование сети должно выполняться в соответствии с применимым законодательством и с согласия владельца сети или системы.

Сканирование портов

Сканирование портов - это процесс исследования сетевых портов на удаленном узле с целью определения, какие порты открыты, закрыты или фильтруются брандмауэром. Это важный шаг в анализе безопасности сети и выявлении потенциальных уязвимостей. Существует несколько методов сканирования портов, вот некоторые из них:

1. TCP Connect Scan: Это один из наиболее распространенных методов сканирования портов. В этом методе сканер пытается установить полноценное TCP-соединение с каждым сканируемым портом на удаленном узле. Если соединение устанавливается успешно, порт считается открытым. Если соединение отклоняется или не устанавливается, порт считается закрытым или фильтруется.
2. SYN Scan (Half-Open Scan): Этот метод использует особенность протокола TCP, известную как полуоткрытое (half-open) соединение. Сканер отправляет запросы SYN на сканируемые порты, и если получает ответ SYN/ACK, то порт считается открытым. Если получает ответ RST, то порт считается закрытым, а если не получает ответа, то порт считается фильтруемым.
3. UDP Scan: В отличие от TCP, протокол UDP является безсоединительным, и многие утилиты сканирования портов предлагают специальные методы сканирования UDP-портов. В этом методе сканер отправляет UDP-пакеты на сканируемые порты и анализирует ответы. Если получает ответ, порт считается открытым или фильтруемым. Если получает ICMP Destination Unreachable, порт считается закрытым.
4. XMAS Scan: Это метод сканирования, при котором сканер отправляет пакеты с установленными флагами FIN, URG и PSH на сканируемые порты. Если получает ответ RST, порт считается закрытым. Если получает ответ RST/ACK, порт считается фильтруемым. Если не получает никакого ответа, порт может считаться открытым или фильтруемым.

5. Null Scan: В этом методе сканер отправляет пакеты без установленных флагов на сканируемые порты. Если получает ответ RST, порт считается закрытым. Если не получает никакого ответа, порт может считаться открытым или фильтруемым.

Это только несколько примеров методов сканирования портов. Есть и другие методы, такие как FIN Scan, Idle Scan, ACK Scan и т. д. Важно помнить, что сканирование портов должно выполняться только в рамках законных целей и с согласия владельца сети, чтобы избежать нарушения законодательства и этических принципов.

Утилита nmap.
Сканирование сети

Сканирование сети, с целью обнаружения хостов:
sudo nmap -sn 10.10.0.0/24

"-sn" - это опция Nmap, которая указывает на выполнение сканирования с использованием сканирования Ping. Опция "-sn" означает "Ping Sweep" или "No port scan", т.е. без сканирования портов.

"10.10.0.0/24" - это диапазон IP-адресов, который будет сканироваться. "/24" здесь представляет сетевую маску в формате CIDR, указывающую, что все адреса в диапазоне 10.10.0.0 до 10.10.0.255 будут сканироваться.

Некоторые другие опции:
"-PA" - это опция Nmap, которая указывает на выполнение сканирования с использованием TCP-флага ACK. Опция "-PA" означает "ACK Scan". В этом режиме Nmap отправляет пакеты с TCP-флагом ACK на целевые хосты в указанном диапазоне IP-адресов и анализирует ответы, чтобы определить, является ли хост активным.

"-PU" означает "UDP Scan". В этом режиме Nmap отправляет UDP-пакеты на целевые хосты в указанном диапазоне IP-адресов и анализирует ответы, чтобы определить, является ли хост активным.

"-PS" - это опция Nmap, которая указывает на выполнение сканирования с использованием TCP-флага SYN. Опция "-PS" означает "SYN Scan". В этом режиме Nmap отправляет пакеты с TCP-флагом SYN на целевые хосты в указанном диапазоне IP-адресов и анализирует ответы, чтобы определить, является ли хост активным.

"-PR" - это опция Nmap, которая указывает на выполнение ARP-сканирования. Опция "-PR" означает "ARP Ping Scan". В этом режиме Nmap отправляет ARP-запросы на целевые хосты в указанном диапазоне IP-адресов и анализирует ответы, чтобы определить, является ли хост активным.

Сканирование портов.

sudo nmap -sS 10.10.0.10
где:
Опция "-sS" означает "TCP SYN Scan". В этом режиме Nmap отправляет пакеты SYN на указанные порты целевых хостов и анализирует ответы, чтобы определить, какие порты открыты, закрыты или фильтрованы.

Некоторые другие опции:

"-sT": Эта опция указывает Nmap на выполнение сканирования TCP-портов с использованием полного установления соединения (full connect scan). В режиме -sT Nmap устанавливает полные TCP-соединения с целевыми портами и анализирует ответы, чтобы определить, какие порты открыты, закрыты или фильтрованы.

"-sA": Эта опция выполняет сканирование ACK-портов. В этом режиме Nmap отправляет пустые пакеты ACK на указанные порты и анализирует ответы, чтобы определить состояние портов. Это может быть полезно для обнаружения наличия фильтров на портах или для определения состояния сетевых устройств.

"-sW": Эта опция выполняет сканирование Window-портов. В этом режиме Nmap отправляет пакеты с установленным окном (Window) на указанные порты и анализирует ответы, чтобы определить состояние портов. Это позволяет проверить, какие порты могут быть уязвимыми для атак, связанных с управлением окнами TCP.

"-sM": Эта опция выполняет сканирование портов с использованием пакетов Maimon (Maimon Scan). В этом режиме Nmap отправляет пакеты Maimon на указанные порты и анализирует ответы, чтобы определить состояние портов. Пакеты Maimon являются частью техники сканирования портов, разработанной Феликсом Маймоном.

"-sU": Эта опция выполняет сканирование UDP-портов. В режиме -sU Nmap отправляет UDP-пакеты на указанные порты и анализирует ответы (если таковые есть), чтобы определить состояние портов. Так как протокол UDP не предоставляет механизма подтверждения доставки пакетов, сканирование UDP-портов сложнее, чем сканирование TCP-портов.

"-sV" - это опция Nmap, которая указывает на выполнение сканирования портов с определением версий сервисов. Опция "-sV" означает "Version Detection". В этом режиме Nmap отправляет запросы к открытым портам хостов и анализирует ответы, чтобы определить, какие сервисы работают на этих портах и какие версии этих сервисов используются.

"-O" - Определение операционной системы хоста.
"-A" - активирует определение версии ОС с использованием скриптов и трассировки, получается наиболее развернутый отчет.

Больше опций в документации.