**Статический и динамический IP**

**Статический IP-адрес** – это постоянный адрес, который назначается устройству и не меняется.

(Для устройств, которым необходимо постоянное адресное пространство)

**Динамический IP-адрес** – это временный адрес, который предоставляется устройству на время его подключения к сети через DHCP-сервер.

(Может меняться при каждом подключении)

**Разница:**

**Статические** – фиксированы.

**Динамические** – могут изменяться при каждом подключении.

**Метод сканирования протоколов IP**

Включает отправку пакетов на определённые IP-адреса и порты с целью обнаружения активных устройств, а также сбора информации о конфигурации и восприимчивости к уязвимостям.

(Позволяет определить, какие порты открыты)

**На какие пакеты ОС должны ответить флагом RST?**

Большинство операционных систем должны ответить флагом RST (Reset) на нераспознанные пакеты TCP, которые не соответствуют установленным соединениям.

Это может быть вызвано пробросом пакетов на несуществующий порт, ошибкой в протоколе или попытками послать пакеты в закрытые соединения.

**Honeypot**

**Honeypot** – это намеренно уязвимая система, созданная для привлечения злоумышленников с целью изучения их методов и инструментов, чтобы улучшить безопасность сети.

***Цели*:**

1. Исследование поведения злоумышленников
2. Выявление уязвимостей
3. Сбор данных о потенциальных угрозах

Злоумышленники преследуют различные цели: кража конфиденциальной информации, установка вредоносного ПО, проведение DDoS-атак.

**Методы выявления Honeypot:**

1. **Исследование сетевой активности** – если система реагирует на неожиданные или странные запросы, это может указывать на Honeypot.
2. **Проверка наличия уязвимостей** – устойчивость к известным уязвимостям, которые могут быть имитированы.
3. **Использование анализа трафика** – для выявления аномалий в поведении системы.

**Наказание за взлом**

**УК РФ статья 272**

**"Несанкционированный доступ к компьютерам, их сетям и информации"**

Устанавливает наказание до 7 лет лишения свободы в зависимости от степени тяжести преступления, а также может включать штрафы и ограничения свободы.

**DHCP**

**DHCP (Dynamic Host Configuration Protocol)** – это сетевой протокол, автоматически назначающий IP-адреса и другие параметры конфигурации (маска подсети, шлюз и DNS-серверы) устройствам в сети, позволяя им подключаться к сети без ручной настройки.

**RPC-сканирование**

**RPC (Remote Procedure Call)** – это метод, позволяющий находить активно работающие RPC-серверы и их версии, чтобы получить точки для атаки.

**Работает по правилу клиент-сервер:**

1. **Клиент** отправляет запрос на сервер, сообщая какую функцию он хочет выполнить и какие данные нужно использовать.
2. **Сервер** получает запрос, выполняет функцию и отправляет результат обратно клиенту.

**Методы сканирования Nmap**

1. **TCP connect scan (-sT)** – полное установление TCP-соединения.
2. **SYN scan (-sS)** – полусоединение, работающее быстрее.
3. **TCP ACK scan (-sA)** – определяет фильтрацию пакетов.
4. **UDP scan (-sU)** – сканирует открытые UDP-порты.
5. **Version detection (-sV)** – определяет версию сервиса.
6. **OS detection (-O)** – определяет ОС целевого узла.
7. **Ping scan (-sn)** – опрос сети на наличие активных хостов.

(Методы позволяют профессионалам по безопасности проводить аудит и оценку защищенности систем)