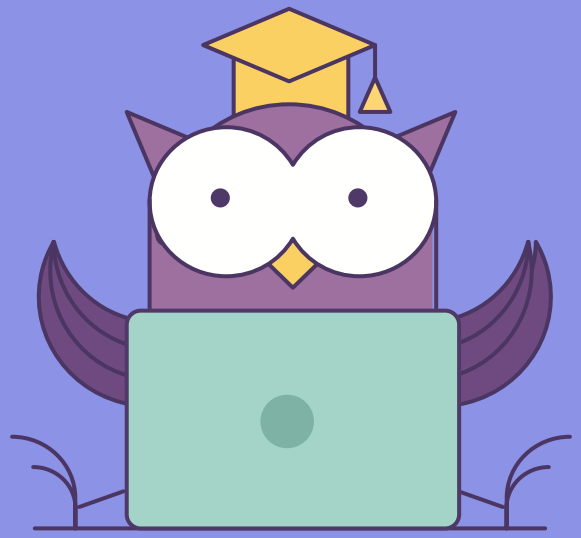
ОНЛАЙН-ОБРАЗОВАНИЕ

OTUS

Основные методы модификации трафика

Колесников Александр Александрович

Меня хорошо слышно && видно?



Напишите в чат, если есть проблемы!

Ставьте + если все хорошо

Содержание

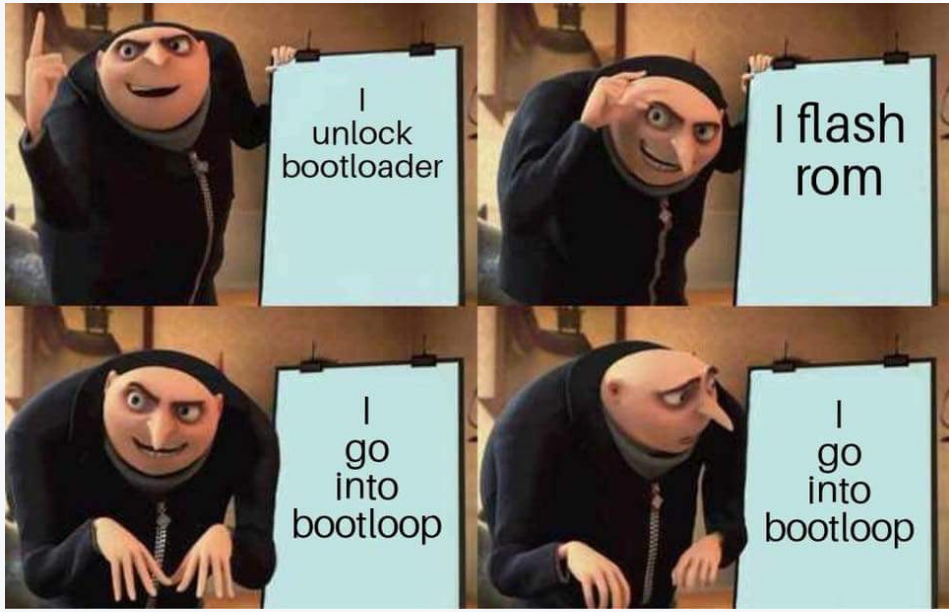
- **Перенаправление трафика в сети**
  - Основные понятия
  - MiTM
  - Особенности

- **EtterCap**
- **SSLStrip**
- **BetterCap**
  - Основные понятия
  - Состав программы
  - Атаки

Цель занятия

1. Изучить основные методы подмены и модификации трафика

2. Закрепить полученные знания в практической работе



01

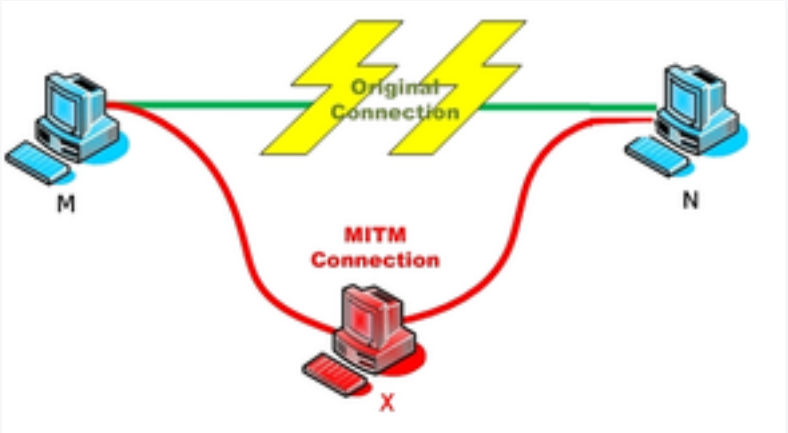
Перенаправление трафика в сети

Основные понятия

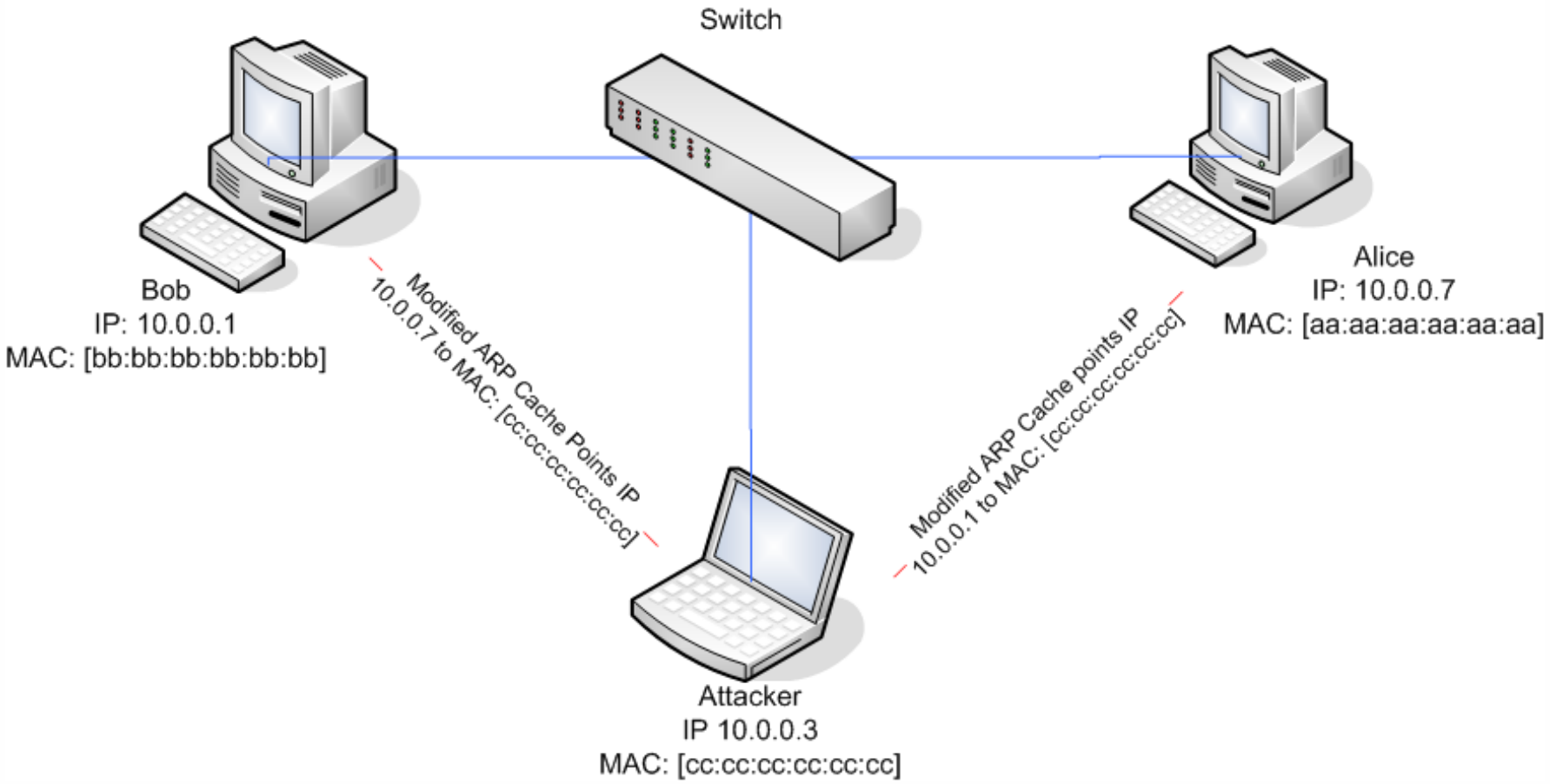
MITM - тип атак, в которых происходит встраивание атакующего в сеть. Атакующий при этом может слушать и модифицировать трафик

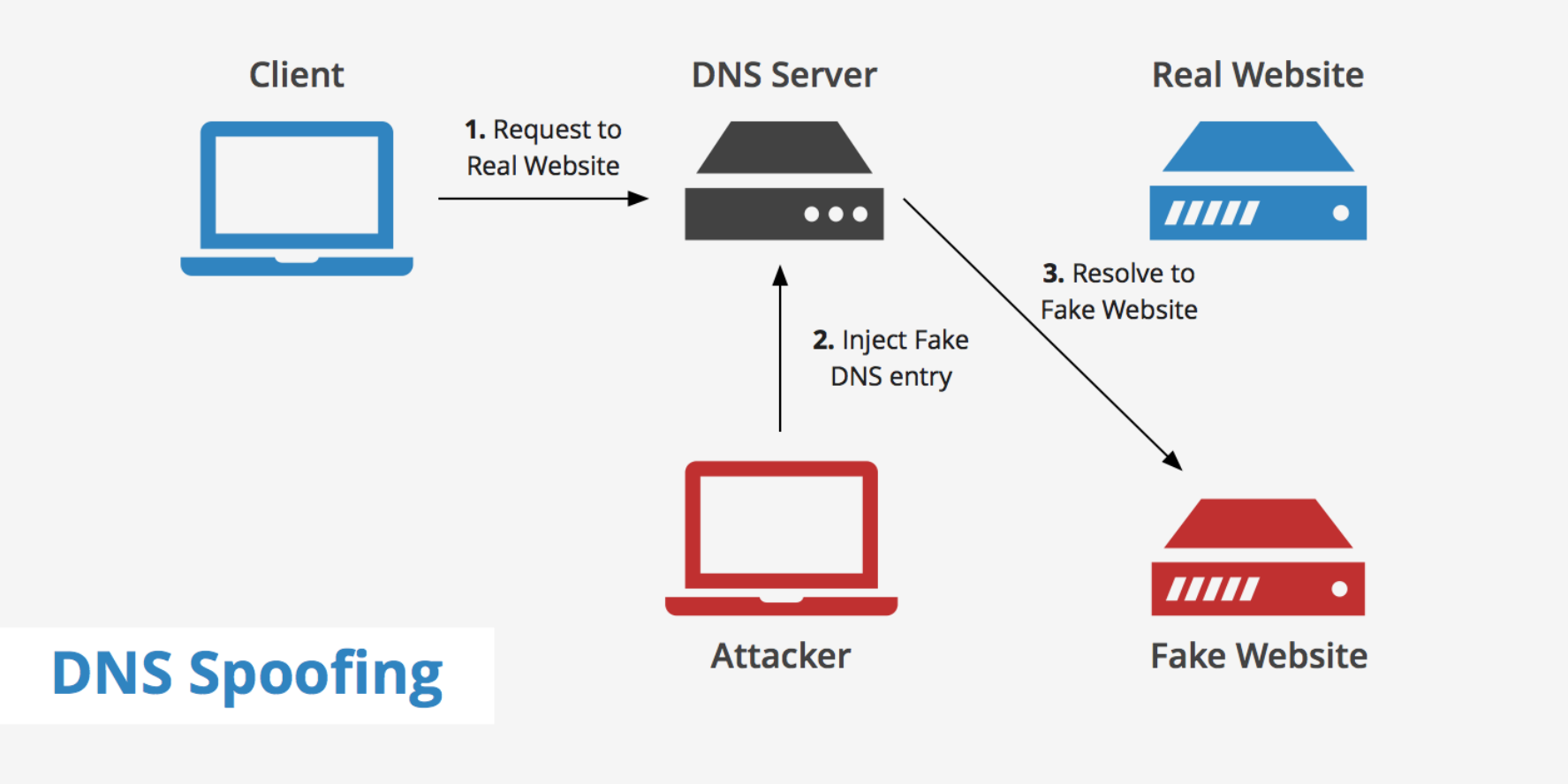
ARPSpoofing - атака направленная на перенаправление трафика в сети.

DNSSpoofing - атака, которая является производной атаки ARPSpoofing. Отличием является то, что помимо подмены MAC-IP пары, так же подменяется ответ DNS сервера.



ARPSpoofing



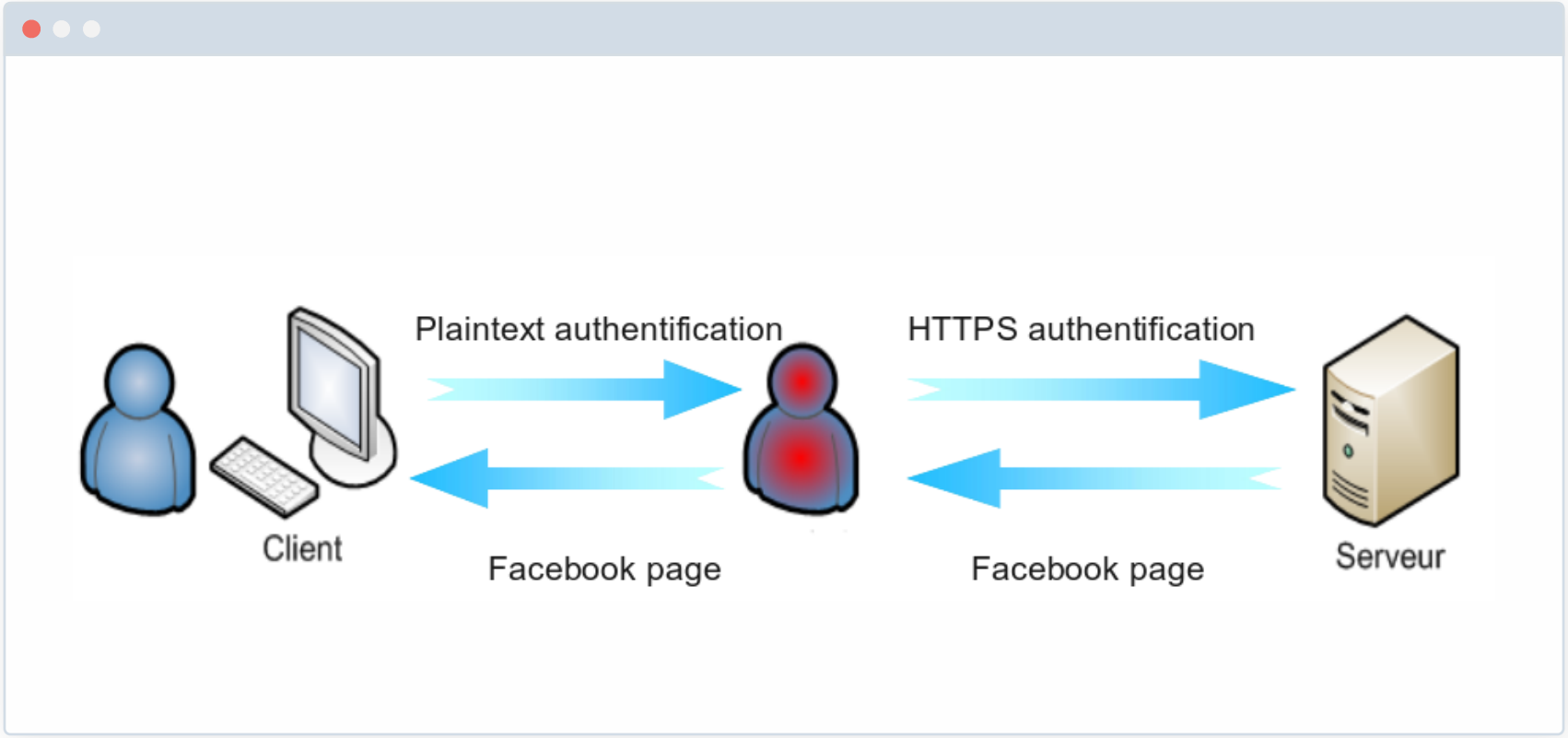

Client
DNS Server
Real Website
1. Request to Real Website
3. Resolve to Fake Website
2. Inject Fake DNS entry
Attacker
Fake Website
DNS Spoofing

MiTM

Цель атаки: получения информации, которая передается по каналу связи

Условия: Атака возможна, если атакующий может подключиться между клиентом и сервером.

Критерий успешности: Атакующий без ведома клиента читает и модифицирует трафик



Особенности современного MITM

Против чего применяют:

- DNS
- SSL (HTTPS)
- Wi-Fi
- Email
- Любого другого протокола, который встраивается для дополнительной безопасности

Что ищут в трафике:

- Учетные данные: логин и пароль от ресурса
- Токены доступа к системам

Какие есть меры противодействия:

- VPN
- HSTS

HSTS

HTTP Strict Transport Security - механизм, который принудительно активирует защищенное соединение через протокол HTTPS.

Как работает:

- Сервер устанавливает специальный заголовок: Strict-Transport-Security
- После получения браузером заголовка, он обязан переходить на аналоги ссылок HTTPS даже если клиент вводит HTTP

Дополнительные условия защиты:

- Дополнительную защиту встроили в сами браузеры. Теперь в каждом браузере есть список самых популярных ресурсов. Их Public Key вшиты в исходный код браузера.
- Название метода защиты - **HTTP Public Key Pinning**

Некоторые сайты из HSTS

- Google
- Википедия
- PayPal
- Twitter

HSTS - насколько это плохо для атакующего

HSTS - отбросил большое количество атак на соединение

Но: Работа механизма может быть корректной только при его корректной настройке:

- Заголовок: **Strict-Transport-Security: max-age=31536000; includeSubDomains; preload**
- При конфигурации, некоторые программисты и администраторы, не верно указывают значения для конфигурации механизма.

Где могут быть лазейки:

- max-age - есть рекомендации касательно установления этого поля, но оно может быть заполнено заведомо малым значением.
- includeSubDomains - указывается не на всех сайтах
- Preload -

02

Утилиты для модификации трафика

EtterCap

Набор утилит и фильтров, которые позволяют производить сниффинг и подмену контента на лету. Часто применяется для MITM атак

Особенность - в отличии от аналогичных пакетов, предоставляет не только способы атак, но и их обнаружений в сети

Основной сетевой функционал может быть расширен за счет плагинов.

Основные группы готовых плагинов:

- sniffing
- Spoofing
- DDos
- Checkers

SSLStrip

Скрипт на языке программирования python. Используется при атаках Mitm для понижения уровня безопасности соединения.

Из коробки предоставляет функционал по модифицированию HTTP трафика отправляемого по SSL

Особенности - не поддерживается уже 8 лет имеет проблемы в работе.

Существует аналог, SSLStrip+ новая версия, которая может бороться с HSTS ресурсами.

BetterCap

Относительно молодой проект, включает в себя все возможные утилиты для тестирования сетей на предмет уязвимостей.

Включает в себя тот же функционал, что и все предыдущие приложения.

Так же может быть расширен плагинами.

Из особенностей: может работать из коробки с Bluetooth и Wi-Fi

01

Модификация трафика

Александр Колесников

Спасибо
за внимание!