??????? IP

The Onion Router (TOR)

Tor Browser (сокр. от англ. The Onion Router) — свободное и открытое программное обеспечение для реализации второго (V2) и третьего (V3) поколения так называемой луковой маршрутизации. Это система прокси-серверов, позволяющая устанавливать анонимное сетевое соединение, защищённое от прослушивания. Рассматривается как анонимная сеть виртуальных туннелей, предоставляющая передачу данных в зашифрованном виде.

Луковая маршрутизация (англ. Onion routing) — технология анонимного обмена информацией через компьютерную сеть. Сообщения неоднократно шифруются и потом отсылаются через несколько сетевых узлов, называемых луковыми маршрутизаторами. Каждый маршрутизатор удаляет слой шифрования, чтобы открыть трассировочные инструкции и отсылать сообщения на следующий маршрутизатор, где все повторяется.

Таким образом, промежуточные узлы не знают источника, пункта назначения и содержания сообщения. Маршрутизаторы были названы луковыми, так как слои шифрования подобны чешуйкам луковицы.

Как воспользоваться TOR?

Инструментом TOR можно пользоваться, работая с браузером TOR, но чаще всего эксперты поднимают входной узел сети Tor как сервис и пользуются им в виде прокси.
Ранее мы рассматривали с вами инструмент proxychains, для того, чтобы использовать большинство CLI утилит через прокси.

Рассмотрим, как это можно реализовать, используя Tor:

```
$ sudo apt install proxychains tor -y                <- Установка
$ service tor start                                                <- Запуск сервиса Tor
на порту стандартном порту 9050
$ vim /etc/proxychains4.conf                                  <- Настройка Proxychains в
файле конфигурации
…
proxy_dns
socks4  127.0.0.1 9050
socks5  127.0.0.1 9050
…
$ proxychains nmap -targetaddress <- Запуск утилиты Nmap с использованием proxy Tor
```

Атаки на клиентов Tor

Tor Browser или использование Tor как прокси имеет набор проблем, которые возникают из-за особенностей конфигурации или из-за уязвимостей в отдельных версиях ПО. Большинство известных атак касаются проблем деанонимизации клиентов Tor и анализа трафика клиентов Tor.

Первый вид атак реализуется посредством установки входных и выходных узлов сети Tor, принадлежащих одному владельцу, который может по объему пакетов и времени запроса определять, что тот или иной входный и выходной трафик принадлежат одному и тому же клиенту.

Второй вид атак касается возможностей внедрения трафика, либо на стороне входного узла (дублирование пакетов запросов и поиск задублированных пакетов на выходе), либо на стороне выходного узла используя попытки завести клиентов сети Tor на свой сайт и замерять получаемые клиентом данные или заставить его выполнить DNS запросы в обход прокси.

Ротация IP адресов

Для постоянной смены IP адресов зачастую недостаточно пользоваться такими сервисами, как Tor или I2P, т.к. некоторые сервисы могут блокировать вас по факту принадлежности вашего IP к сетям анонимного доступа.

Также такие сети не позволяют выполнять множественные запросы, постоянно изменяя IP с высокой скоростью.

В качестве популярных решений существуют:

Сервисы:

- https://www.proxyrotator.com/
- https://stormproxies.com/
- https://brightdata.com/

Плагин для Burp Suite:

- IP Rotate

Консольные утилиты:

- Fireprox

Облачные провайдеры:

- Сервис Cloud Functions

- AWS API Gateway
- AWS Lambda

Дополнительная информация

- Как работает Tor
- Настройка I2P
- О proxy
- Cover Your Tracks, чтобы оценить фингерпринт в браузере
- Фреймворк контроля и управления гибко адаптируемый под задачи обхода обнаружения
- Чек-лист по обходу обнаружения антивирусами и EDR системами
- Набор статей на тему обхода обнаружения различными способами в различных ситуациях

Revision #1
Created 13 October 2025 08:55:26 by Admin
Updated 13 October 2025 08:58:55 by Admin