Чугаев Никита Сергеевич БАСО-02-20

**Электронный отчет по сайту** [weforum.org](https://www.weforum.org)

**Оглавление**

1. Обнаружение сайта
2. Определяем Ip адрес
3. Определяем доменные имена, соответствующие почтовому серверу
4. Определяем доменные имена, соответствующие DNS-серверу
5. Определяем зону доменного имени, электронный адрес администратора и тд
6. Определяем все доступные записи DNS-сервера

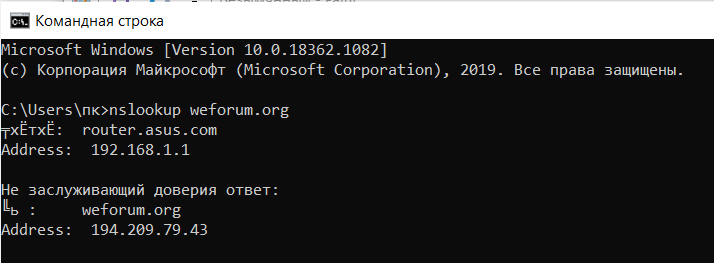
**1. Обнаружение сайта**

С помощью google dorks найдем нужный нам сайт используя следующий запрос: intitle:"forum" inurl:http after:2019 .

* Заголовок: Форум
* Тип шифрования: http
* Дата создания: После 2019

**2. Определяем Ip адрес**

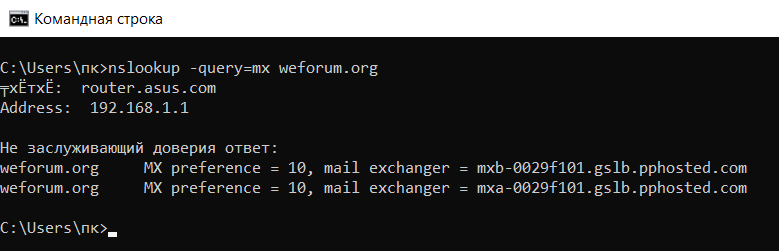
С помощь утилиты nslookup определяем Ip адрес сайта



weforum.org соответствует ip 194.209.79.43

**3. Определяем доменные имена, соответствующие почтовому серверу**

С помощь утилиты nslookup –query=mx узнаем соответствие доменных имен с почтовыми серверами домена

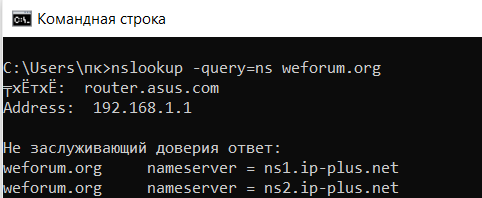


Данному домену соответственует один почтовый сервер

mxb-0029f101.gslb.pphosted.com , число 10 перед MX preference показывает нам приоритет, причем, чем меньше число, тем больше приоритет.

**4. Определяем доменные имена, соответствующие DNS-серверу**

С помощью утилиты nslookup –query=ns узнаем соответствие доменного имени DNS-серверу



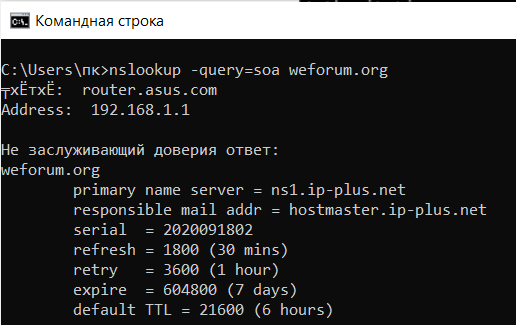
Доменному имени weforum.org соответсвуют два DNS-сервера:

ns1.ip-plus.net и ns2.ip-plus.net

**5. Определяем зону доменного имени, электронный адрес администратора и тд**

С помощью утилиты nslookup -query=soa узнаем следующую информацию:

* о зоне доменного адреса
* почтовый адрес администратора домена
* серийный номер файла зоны
* период времени, через который вторичный DNS-сервер отправит запрос первичному (в секундах)
* интервал для повторного соединения с первичным DNS-сервером (в секундах)
* время хранения кэша вторичного DNS-сервера (в секундах)
* стандартное время жизни пакета (в секундах)



Имя первичного DNS-сервера: ns1.ip-plus.net

Почтовый адрес администратора домена: hostmaster.ip-plus.net

Серийный номер: 2020091802

Период времени: 1800 секунд

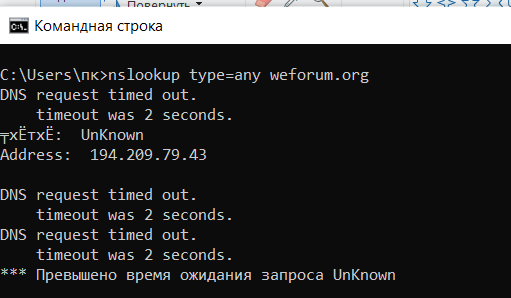
Время до повторного соединения: 3600 секунд

Время хранения кэша: 604800 секунд

Время жизни пакета: 21600 секунд

**6. Определяем все доступные записи DNS-сервера**

При использовании утилиты nslookup type=any узнаем все записи DNS-сервера, которые доступы для данного доменного имени



При использовании данной утилиты выходит ошибка.