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

Активный поиск

Запросы к DNS-сервису организации

1. Опрос DNS сервиса на известные ему записи раскрывающие доменные имена, связанные с доменом 2-го уровня. Т.е. выполнение запросов к таким DNS записям, как: CNAME, MX, NS, SRV и т.д. Подробнее

A – используется для указания доменного имени, например, testdomain.com, на IP-адрес его хост-сервера;
MX – записи, отвечающие за обмен электронной почтой;
NS – предназначены для идентификации DNS-серверов, ответственных за домен;
SRV – записи для выделения службы, размещенной на определенных серверах;
PTR – обратный поиск DNS: с помощью IP вы можете получить связанный с ним домен;
SOA – начало записи: это информация о зоне DNS и других записях DNS;
CNAME – сопоставляет целевое доменное имя с другим доменным именем.

Чтобы получить записи всех типов можно использовать тип запроса ANY

```
┌──(kali㉿kali)-[~]
└─$ nslookup -q=ANY cyber-ed.ru 8.8.8.8
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   cyber-ed.ru
Address: 178.154.245.151
cyber-ed.ru     nameserver = ns2.reg.ru.
cyber-ed.ru     nameserver = ns1.reg.ru.

Authoritative answers can be found from:


┌──(kali㉿kali)-[~]
└─$ nslookup -q=ANY cyber-ed.ru ns1.reg.ru
Server:         ns1.reg.ru
Address:        194.58.117.17#53
```

```
Name:   cyber-ed.ru
Address: 178.154.245.151
```

2. Перебор доменных имен. Делаем или используем готовый список возможных поддоменов и опрашиваем DNS сервис в формате *слово.example.com*. Есть списки часто используемых поддоменов. Называются gists. В Kali они есть по /usr/share/wordlists/amass/bitquark_subdomains_top100K.txt Или можно в google "subdomain wordlist site:gist.github.com".

```
#!/bin/bash

DOMAIN=$1
FILE=$2

while read -r subdomain; do
  echo "${subdomain}.${DOMAIN}"
done < "${FILE}" > ${DOMAIN}.txt
```

Пример использования утилиты subfinder со стандартным словарем для перебора доменных имен:

```
subfinder -d cyber-ed.ru
```

В kali они называются gists. Есть скрипт в Black hat bash

Последняя версия через docker:

```
docker run projectdiscovery/subfinder:latest -d cyber-ed.ru
```

3. Выполнение запроса AXFR. AXFR запрос, или Zone transfer — это процесс передачи копии базы данных с DNS-зоной от главного сервера к вторичному. В идеале трансфер зоны ограничен только для определенных доверенных серверов, но неправильно сконфигурированные серверы разрешают трансферы любому, кто их попросит.

Пример выполнения такого запроса: `nslookup -q=AXFR example.com` (зачастую требует указания конкретного DNS-сервера, к которому будет отправлен запрос).

```
—$ nslookup -q=AXFR cyber-ed.ru ns1.reg.ru
Server:         ns1.reg.ru
Address:        176.99.13.15#53
```

```
** server can't find cyber-ed.ru: NOTAUTH
; Transfer failed.
```

4. amass

```
amass enum -d <host>
```

Текущая 4 версия. Работает архидолго, находит не так чтобы много. Но может найти что-то интересное. Формат вывода:

```
test.cyber-ed.ru (FQDN) --> a_record --> 185.215.4.43 (IPAddress)
infra.cyber-ed.ru (FQDN) --> a_record --> 84.54.44.31 (IPAddress)
84.201.128.0/18 (Netblock) --> contains --> 84.201.134.36 (IPAddress)
84.54.44.0/23 (Netblock) --> contains --> 84.54.44.31 (IPAddress)
200350 (ASN) --> managed_by --> AS200350 - Yandex.Cloud LLC (RIROrganization)
```

amass v3

Работает быстрее, доступен через docker

```
docker run caffix/amass:v3 enum -d <host>
```

Для amass v3 ключ -passive запрещает искать ip адреса. Ключи amass v3 и v4 сильно отличаются.

5. The Harvester

-b указывается источник данных (sitedossier, duckduckgo
-d домен

```
#!/usr/bin/python
import sys
import os
if len(sys.argv) < 2:
    sys.exit(-1)
providers = [ 'duckduckgo', 'bing', 'baidu', 'dnsdumpster', 'hunter', 'sitedossier' ]
for a in providers:
    cmd = 'theHarvester -d {0} -b {1} -f {2}.html'.format(sys.argv[1], a, a)
    os.system(cmd)
```

6. Другие инструменты:

- Sublist3r — OSINT инструмент поиска поддоменов
- assetfinder — пассивный сканер поддоменов на Go
- Также страница Shodan.io, Google

Пассивный поиск

Использование служб и сайтов, которые произвели активный поиск за нас или агрегировали известную информацию среди открытых источников. Примеры:

- dnsdumpster.com
- shodan.io
- censys.io
- crt.sh
- pentest-tools.com

Объединение данных из разных источников

Нужно преобразовать выходную информацию к одному формату и сделать итоговый список имен. Задача: сохранить файлы из разных источников по одному шаблону и создать итоговый файл (включая вручную созданные из web ресурсов файлы). Шаблон создаваемых файлов: domain_tool.txt (например bobrobotirk.ru_subfinder.txt). Часть скрипта по объединению файлов:

```
#!/bin/bash

DOMAIN=$1
OUTPUT_FILE="$DOMAIN/subdomains_merged.txt"

mkdir -p $DOMAIN
#вызов инструментов

cat "$DOMAIN/${DOMAIN}_"*.txt | sort | uniq > "$OUTPUT_FILE"
```

Осталось в часть *#вызов инструментов* добавить конкретные инструменты.

Описание nslookup

-type=TEXT	записи определенного типа

Перебор DNS записей из списка доменных имен

Revision #17
Created 18 September 2025 16:17:31 by Admin
Updated 13 November 2025 07:45:59 by Admin