

4. Polecenie nslookup

4.1 Przebieg ćwiczenia

a) Proszę sprawdzić dostępność tego polecenia.

Z jakimi opcjami można wywoływać to polecenie, jakiego typu informacje można

dzięki opcjom uzyskać? (jeśli opcji jest dużo sprawdź działanie polecenie z 3 – 4 opcjami – przedstaw wyniki).

Zapytanie Nslookup - dzięki temu poleceniu możemy zobaczyć ile jest rekordów A i zobaczyć Adresy Ip każdego z nich. Poza rekordami zostaną wyświetlane wszystkie rekordy

AAAA jeśli takowe istnieją:

```
C:\Users\Mateusz>nslookup www.wp.pl
Server:  funbox.home
Address: 192.168.1.1

Non-authoritative answer:
Name:      www.wp.pl
Address:   212.77.98.9

C:\Users\Mateusz>nslookup www.et.put.poznan.pl
Server:  funbox.home
Address: 192.168.1.1

Non-authoritative answer:
Name:      sphinx.et.put.poznan.pl
Address:   150.254.11.7
Aliases:   www.et.put.poznan.pl
```

Polecenie -type=soa - zawiera informacje o głównym serwerze DNS dla domeny.

Zawiera również dodatkowe informacje o domenie takie jak adres e-mail administratora, numer seryjny i informacje o częstotliwości synchronizacji rekordów w domenie.

```
C:\Users\Mateusz> nslookup -type=soa www.wp.pl
Server:  funbox.home
Address: 192.168.1.1

wp.pl
      primary name server = ns1.wp.pl
      responsible mail addr = dnsmaster.wp-sa.pl
      serial = 2023011198
      refresh = 900 (15 mins)
      retry   = 600 (10 mins)
      expire  = 86400 (1 day)
      default TTL = 3600 (1 hour)

C:\Users\Mateusz>
```

Polecenie -query=any - pozwala na wyświetlenie zawartości wszystkich rekordów domeny.

```
C:\Users\Mateusz> nslookup -query=any www.wp.pl
Server:  funbox.home
Address:  192.168.1.1

Non-authoritative answer:
www.wp.pl          internet address = 212.77.98.9
```

Polecenie -debug - polecenie to dostarcza ważne i szczegółowe informacje dla zapytania DNS, jak i dla odpowiedzi.

```
ANSWERS:
-> www.wp.pl
    internet address = 212.77.98.9
    ttl = 264 (4 mins 24 secs)

-----
Non-authoritative answer:
-----

Got answer:
HEADER:
    opcode = QUERY, id = 3, rcode = NOERROR
    header flags: response, want recursion, recursion avail.
    questions = 1, answers = 0, authority records = 1, additional = 0

QUESTIONS:
    www.wp.pl, type = AAAA, class = IN
AUTHORITY RECORDS:
-> wp.pl
    ttl = 3515 (58 mins 35 secs)
    primary name server = ns1.wp.pl
    responsible mail addr = dnsmaster.wp-sa.pl
    serial = 2023011198
    refresh = 900 (15 mins)
    retry = 600 (10 mins)
    expire = 86400 (1 day)
    default TTL = 3600 (1 hour)

-----
Name: www.wp.pl
Address: 212.77.98.9

C:\Users\Mateusz> nslookup -debug www.wp.pl
-----

Got answer:
HEADER:
    opcode = QUERY, id = 1, rcode = NOERROR
    header flags: response, auth. answer, want recursion, recursion avail.
    questions = 1, answers = 1, authority records = 0, additional = 0

QUESTIONS:
    1.1.168.192.in-addr.arpa, type = PTR, class = IN
ANSWERS:
-> 1.1.168.192.in-addr.arpa
    name = funbox.home
    ttl = 0 (0 secs)

-----
Server: funbox.home
Address: 192.168.1.1

-----

Got answer:
HEADER:
    opcode = QUERY, id = 2, rcode = NOERROR
    header flags: response, want recursion, recursion avail.
    questions = 1, answers = 1, authority records = 0, additional = 0

QUESTIONS:
```