

# DNS Infrastructure Enumeration and Passive Reconnaissance: A Comparative Analysis of Nslookup and Dig

Juan Pablo Vega Villamil, *Computer Systems Engineer*

**Abstract**—This report documents a structured passive reconnaissance exercise. By utilizing Nslookup, Dig, and Whois, we identify critical infrastructure components of cisco.com and netacad.com. The study focuses on DNS record types, reverse lookups (PTR), and comparative tool analysis to define an organization's external attack surface.

## I. INTRODUCTION

PASSIVE reconnaissance allows for the gathering of intelligence without direct target interaction. This laboratory analyzes DNS as a primary source of network topology and administrative data.

## II. DNS DISCOVERY VIA NSLOOKUP

Initial queries were performed on *cisco.com* to identify basic IP addressing and local resolver status.

```
kali㉿Kali: ~
File Actions Edit View Help
(kali㉿Kali)-[~]
$ nslookup
> cisco.com
Server:      192.168.100.1
Address:     192.168.100.1#53

Non-authoritative answer:
Name:  cisco.com
Address: 72.163.4.185
Name:  cisco.com
Address: 2001:420:1101:1::185
> 
```

Fig. 1. Initial Nslookup query for cisco.com identifying host addresses.

To identify authoritative name servers, the query type was set to ns. The following output confirms the presence of Akamai-managed nodes and internal Cisco name servers:

```
> set type=ns
> cisco.com
Non-authoritative answer:
cisco.com nameserver = ns3.cisco.com.
cisco.com nameserver = ns1.cisco.com.
cisco.com nameserver = a28-64.akam.net.
cisco.com nameserver = ns2.cisco.com.
cisco.com nameserver = a3-64.akam.net.
```

The primary server was identified as **72.163.4.185**. For *netacad.com*, an external resolver (Google 8.8.8.8) was used to bypass local resolution issues:

```
$ nslookup netacad.com 8.8.8.8
```

Laboratory of Information Security: Passive Reconnaissance Phase. Report generated February 2026.

```
Server: 8.8.8.8
Non-authoritative answer:
Name: netacad.com
Address: 44.207.12.186
Address: 34.205.80.89
```

## III. RECORD TYPE ANALYSIS

Using the any flag, we extracted all available DNS record types.

```
kali㉿Kali: ~
File Actions Edit View Help
> server 8.8.8.8
Default server: 8.8.8.8
Address: 8.8.8.8#53
> set type=any
> netacad.com
;; Connection to 8.8.8.8#53(8.8.8.8) for netacad.com failed: timed out.
Server: 8.8.8.8
Address: 8.8.8.8#53

Non-authoritative answer:
Name: netacad.com
Address: 44.207.12.186
Name: netacad.com
Address: 34.205.80.89
netacad.com nameserver = ns-1476.awsdns-56.org.
netacad.com nameserver = ns-1911.awsdns-46.co.uk.
netacad.com nameserver = ns-748.awsdns-29.net.
netacad.com nameserver = ns-240.awsdns-30.com.
netacad.com origin = ns-1476.awsdns-56.org
netacad.com mail addr = awsdns-hostmaster.amazon.com
netacad.com serial = 1
netacad.com refresh = 7200
netacad.com retry = 900
netacad.com expire = 1209600
netacad.com minimum = 86400
netacad.com mail exchanger = 20 alt1.aspmx.l.google.com.
netacad.com mail exchanger = 10 aspmx.l.google.com.
netacad.com mail exchanger = 30 aspmx3.googlemail.com.
netacad.com mail exchanger = 30 aspmx2.googlemail.com.
netacad.com mail exchanger = 20 alt2.aspmx.l.google.com.
netacad.com text = "linkedin-site-verification=f83d41fa-4926-4fc1-bc86-399f34d2ec82"
netacad.com text = "google-site-verification=TxuIwljruI4690Kael5KB7LvxjIR3g2v0iy8RKy02Ak"
netacad.com text = "93hd7nffv5d7h3vbwrc14q6n5cjkjbc2"
netacad.com text = "facebook-domain-verification=9a8xflw2lo4qxwm9cq3rk3d0etc8bu"
netacad.com text = "identrust_validate=GHH1lQD22HMMNen8L8V2x96QqwXOWYA8Y7Tu58KT1JnGv"
netacad.com text = "v=spf1 include:_spf.google.com
include:amazonse.com ~all"
netacad.com text = "5c9ty312qzq7yyvly7mmk11nrpp6k"
netacad.com text = "google-site-verification=g7CVgKXjcGaA02xXIzPksT9HPpA9_LY0_Uab0_DRtg"
Authoritative answers can be found from:
> 
```

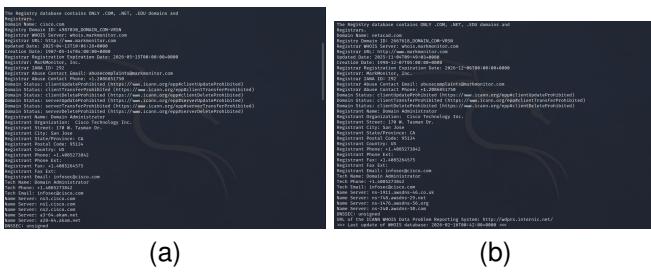
Fig. 2. DNS 'any' query results showing A, AAAA, NS, MX, and TXT records.

As seen in Fig. 2, the following records were identified:

- **A / AAAA:** IPv4 and IPv6 host mappings.
- **NS:** Authoritative name servers.
- **MX:** Mail exchange servers for routing email.
- **TXT:** Descriptive text for domain security (e.g., SPF/DKIM).

#### IV. PASSIVE RECOGNITION VIA WHOIS

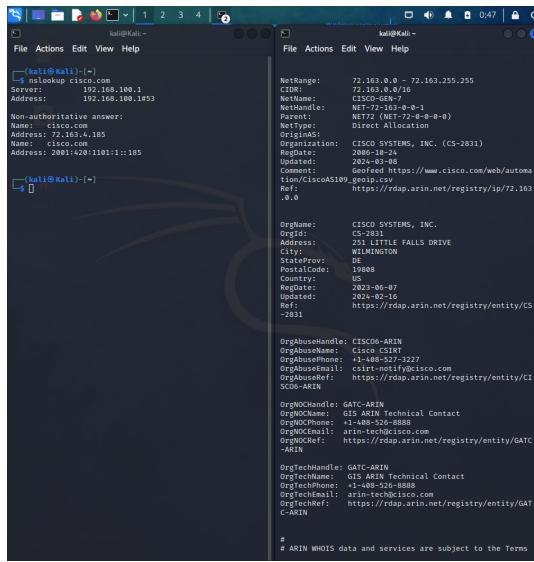
Whois queries provide ownership and registration data. Queries for *cisco.com* and *netacad.com* confirmed their cloud-based management via MarkMonitor.



The Whois database contains over 100,000,000 entries and 200 million domains. It includes information such as registrant, administrative, technical, and billing contacts, as well as domain status, expiration date, and creation date. The data is presented in a tabular format with columns for each field.

Fig. 3. Whois registration data for (a) *cisco.com* and (b) *netacad.com*.

By performing a Whois lookup on the resolved IP (72.163.4.185), we identified the CIDR block: **72.163.0.0/16**.

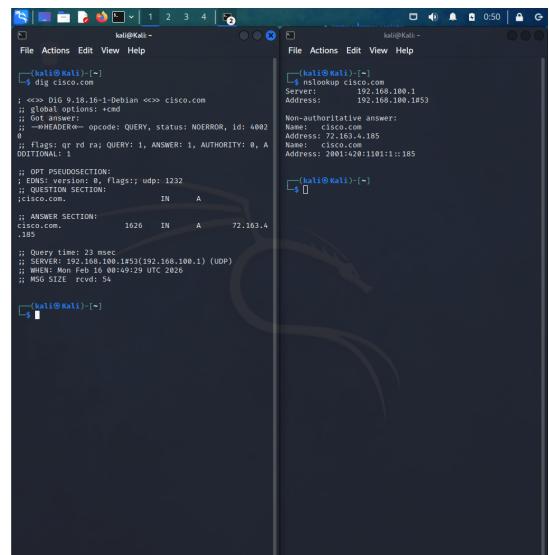


The screenshot shows two terminal windows side-by-side. The left window displays the output of an nslookup command for the IP address 72.163.4.185, which returns the range 72.163.0.0 - 72.163.255.255. The right window shows the output of a whois command for the same IP, which also identifies the range 72.163.0.0 - 72.163.255.255. Both outputs include detailed registration information for the domain *cisco.com*.

Fig. 4. Comparison: Nslookup results vs. Whois IP range identification.

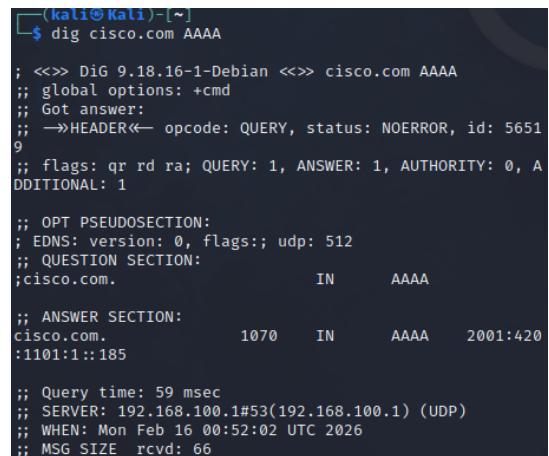
#### V. COMPARATIVE TOOL ANALYSIS: DIG VS. NSLOOKUP

A comparative study revealed significant differences in output structure.



This figure compares the output of nslookup and dig for the domain *cisco.com*. The nslookup output shows both A and AAAA records, while the dig output only shows the A record. The dig output includes additional header information and a longer list of non-authoritative answers.

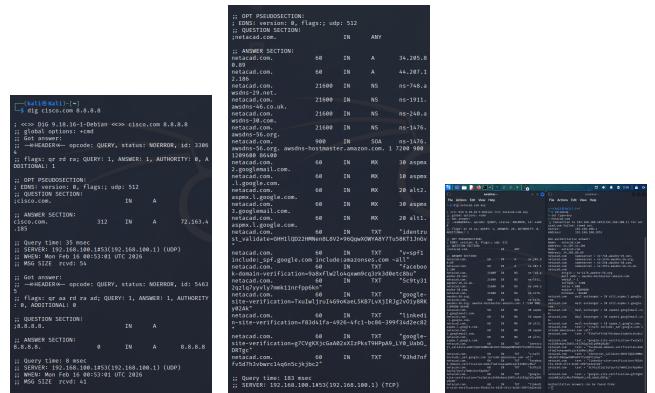
Fig. 5. Nslookup (A/AAAA) vs. Dig (Default A) output comparison.



This screenshot shows an explicit IPv6 (AAAA) query using the dig command. The output shows the AAAA record for the domain *cisco.com*, indicating the IPv6 address 2001:408:1101:1::185.

Fig. 6. Explicit IPv6 (AAAA) query using Dig.

While nslookup is efficient for quick checks, dig provides superior grouping when querying multiple record types.



This figure illustrates advanced Dig queries using specific servers and the 'any' flag. It shows multiple dig commands for various domains (cisco.com, arin.net, google.com) using different servers (nslookup.cisco.com, 192.168.100.1, 192.168.100.1, 8.8.8.8) and the 'any' flag to request all record types. The output shows various record types (A, AAAA, NS, CNAME, etc.) grouped by domain.

Fig. 7. Comparison of advanced Dig queries using specific servers and the 'any' flag.

## VI. REVERSE DNS LOOKUPS (PTR)

The \*\*PTR (Pointer)\*\* record is used for reverse DNS resolution, mapping an IP to a hostname. This is crucial for identifying infrastructure roles.

Querying the primary DNS server:

```
$ dig -x 72.163.5.201  
;; ANSWER SECTION:  
201.5.163.72.in-addr.arpa. 1800 IN PTR ns1.cisco.com.
```

Further exploration on 72.163.1.1 revealed an HSRP (Hot Standby Router Protocol) device:

```
$ dig -x 72.163.1.1  
;; ANSWER SECTION:  
1.1.163.72.in-addr.arpa. 1800 IN PTR hsrp-72-163-1-1.cisco.com.
```

## VII. CONCLUSION

Passive DNS reconnaissance provides a high-fidelity map of a target's external infrastructure. While nslookup remains a standard tool, dig offers the verbosity required for complex audits. Identifying CIDR ranges and PTR records allows engineers to pinpoint critical assets like HSRP routers and authoritative name servers without generating alerts on the target network.

## REFERENCES

- [1] ISC, "BIND 9 Administrator Reference Guide," 2023.
- [2] MarkMonitor, "Domain Management Security Reports," 2025.