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.

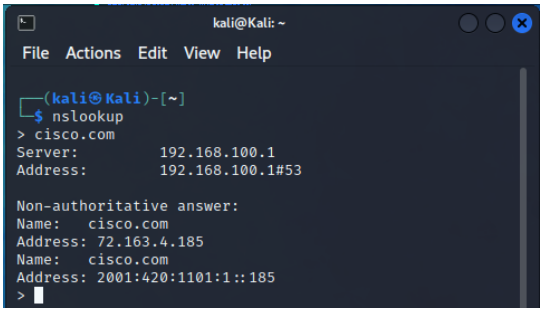


Fig. 1. Initial Nslookup query for cisco.com identifying host addresses.

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
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.

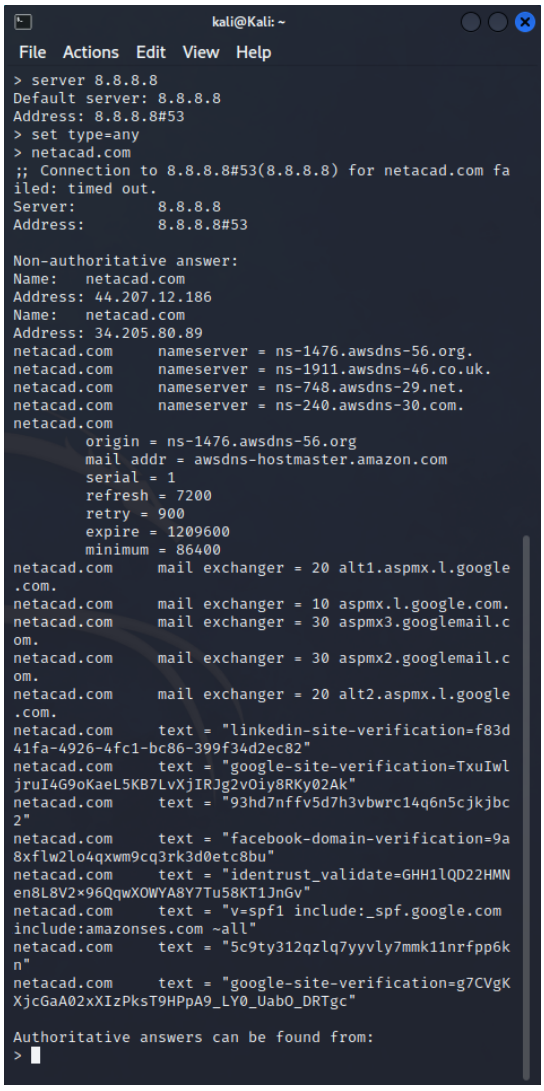


Fig. 2. DNS 'any' query results showing A, AAAA, NS, MX, and TXT records.

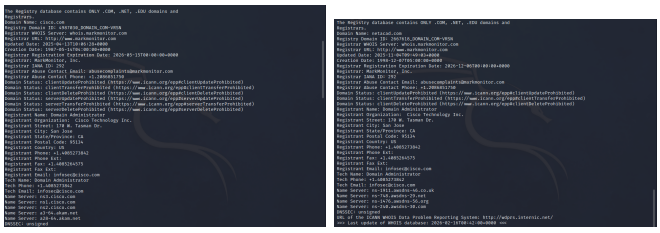
As seen in Fig. 2, the following records were identified:

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

- **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.



(a) (b)

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**.

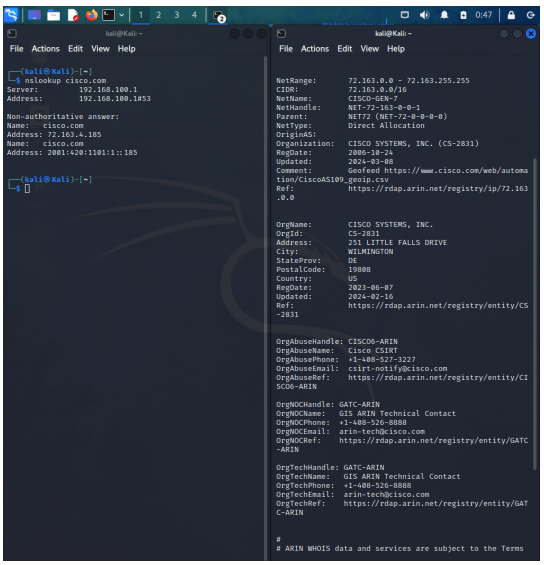


Fig. 4. Comparison: Nslookup results vs. Whois IP range identification.

V. Comparative Tool Analysis: Dig vs. Nslookup

A comparative study revealed significant differences in output structure.

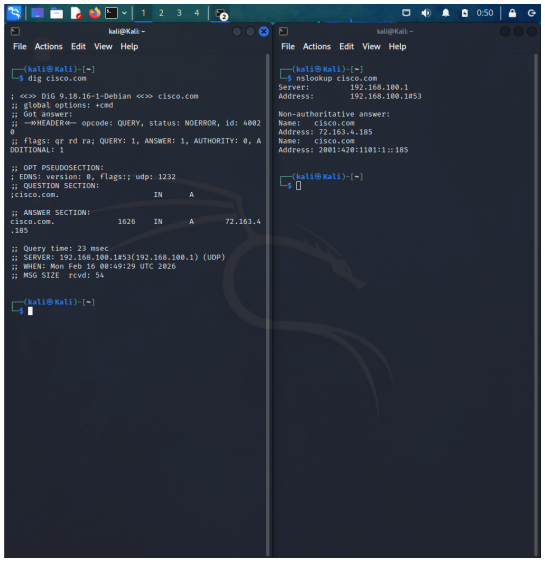
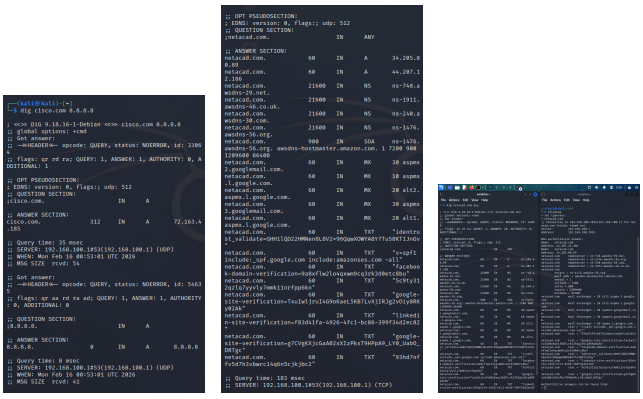


Fig. 5. Nslookup (A/AAAA) vs. Dig (Default A) output comparison.

```
┌──(kali㉿Kali)-[~]
└─$ dig cisco.com AAAA

; <<>> DiG 9.18.16-1-Debian <<>> cisco.com AAAA
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5651
9
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, A
DDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;cisco.com.                     IN      AAAA

;; ANSWER SECTION:
cisco.com.              1070    IN      AAAA    2001:420
:1101:1::185

;; Query time: 59 msec
;; SERVER: 192.168.100.1#53(192.168.100.1) (UDP)
;; WHEN: Mon Feb 16 00:52:02 UTC 2026
;; MSG SIZE  rcvd: 66
```

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

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



(a) p8 (b) p9 (c) p10

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.