Ethical Hacking & Penetration Testing

Assignment 1:

Objective: Use whois to gather information about a domain name of your choice. Perform a nslookup query on the same domain to obtain its IP address and DNS information.

What is WHOIS

- Purpose: WHOIS is a protocol and public database used to look up registration information for domain names and IP addresses.

- What it reveals: Domain registrant (name and contact details) when not redacted, registrar, registration and expiration dates, nameservers, and status. It can also indicate privacy protections or proxy services in use.

- How it's used in practice: You query a domain to confirm ownership details, see who manages the domain, and identify the authoritative name servers. It's commonly used for domain management, ownership verification, and basic reconnaissance in an approved lab setting.

 I selected tryhackme.com website to get the information from WHOIS.

Here is the gathered information about tryhackme.com with the help of WHOIS.

root@SunilVijay:~# whois tryhackme.com

  Domain Name: TRYHACKME.COM

  Registry Domain ID: 2282723194_DOMAIN_COM-VRSN

  Registrar WHOIS Server: whois.namecheap.com

  Registrar URL: http://www.namecheap.com

  Updated Date: 2025-05-11T14:06:02Z

  Creation Date: 2018-07-05T19:46:15Z

  Registry Expiry Date: 2034-07-05T19:46:15Z

  Registrar: NameCheap, Inc.

  Registrar IANA ID: 1068

  Registrar Abuse Contact Email: abuse@namecheap.com

  Registrar Abuse Contact Phone: +1.6613102107

  Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited

  Name Server: KIP.NS.CLOUDFLARE.COM

  Name Server: UMA.NS.CLOUDFLARE.COM

  DNSSEC: unsigned

  URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/

>>> Last update of whois database: 2025-10-13T12:50:00Z <<<

What is nslookup

- Purpose: nslookup is a DNS query tool used to obtain information about DNS records for a domain.

- What it can fetch:

  - A records (IPv4 address)

  - AAAA records (IPv6 address)

  - NS records (name servers)

  - CNAME, MX, and other DNS records depending on options

- How it's used in practice: It helps verify the domain's DNS configuration, resolve domain names to IPs, and understand the domain's hosting setup. It is often used in labs to study how DNS responds to queries and to confirm network reachability.

Here is the result in nslookup

nslookup tryhackme.com

Server: 192.168.50.2

Address: 192.168.50.2#53

Non-authoritative answer:

Name: tryhackme.com

Address: 104.20.29.66

Name: tryhackme.com
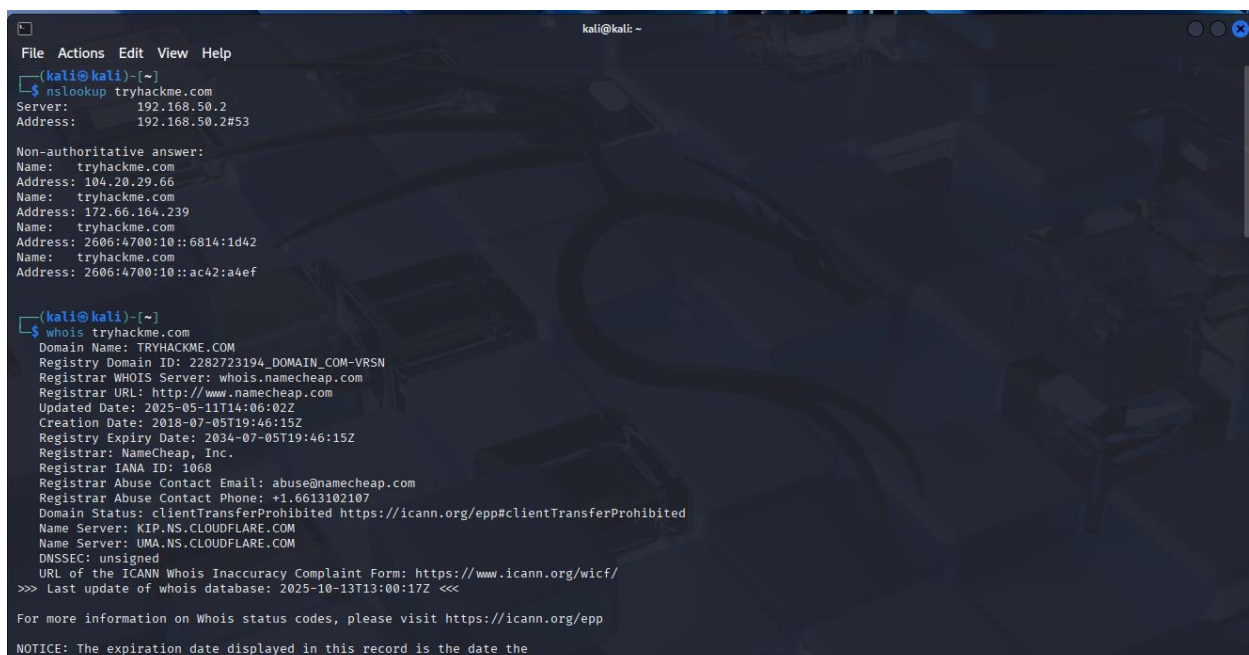
Address: 172.66.164.239

Name: tryhackme.com

Address: 2606:4700:10::6814:1d42

Name: tryhackme.com

Address: 2606:4700:10::ac42:a4ef

Key differences

- Focus: WHOIS provides registration and ownership data; nslookup provides DNS resolution data (how the domain name maps to IPs and where those records are served from).

- Data exposure: WHOIS data can be restricted or redacted by privacy protections; DNS records (visible via nslookup) are typically publicly accessible.

- Use cases: WHOIS for ownership, contact, and registration details; nslookup for diagnosing DNS resolution, connectivity, and hosting configurations.