Project Title

DNS Record Enumeration Using the `host` Command

Objective

To gain practical experience in querying and analyzing DNS records using the `host` command-line utility, enabling insight into how domain name resolution works and understanding different types of DNS data like A, MX, NS, and SOA records.

Skills Learned

- DNS fundamentals and record types (A, MX, NS, SOA)
- How to query specific DNS servers
- Analysis of domain resolution paths
- Troubleshooting DNS issues via direct queries
- Working with terminal-based DNS utilities

Tools Used

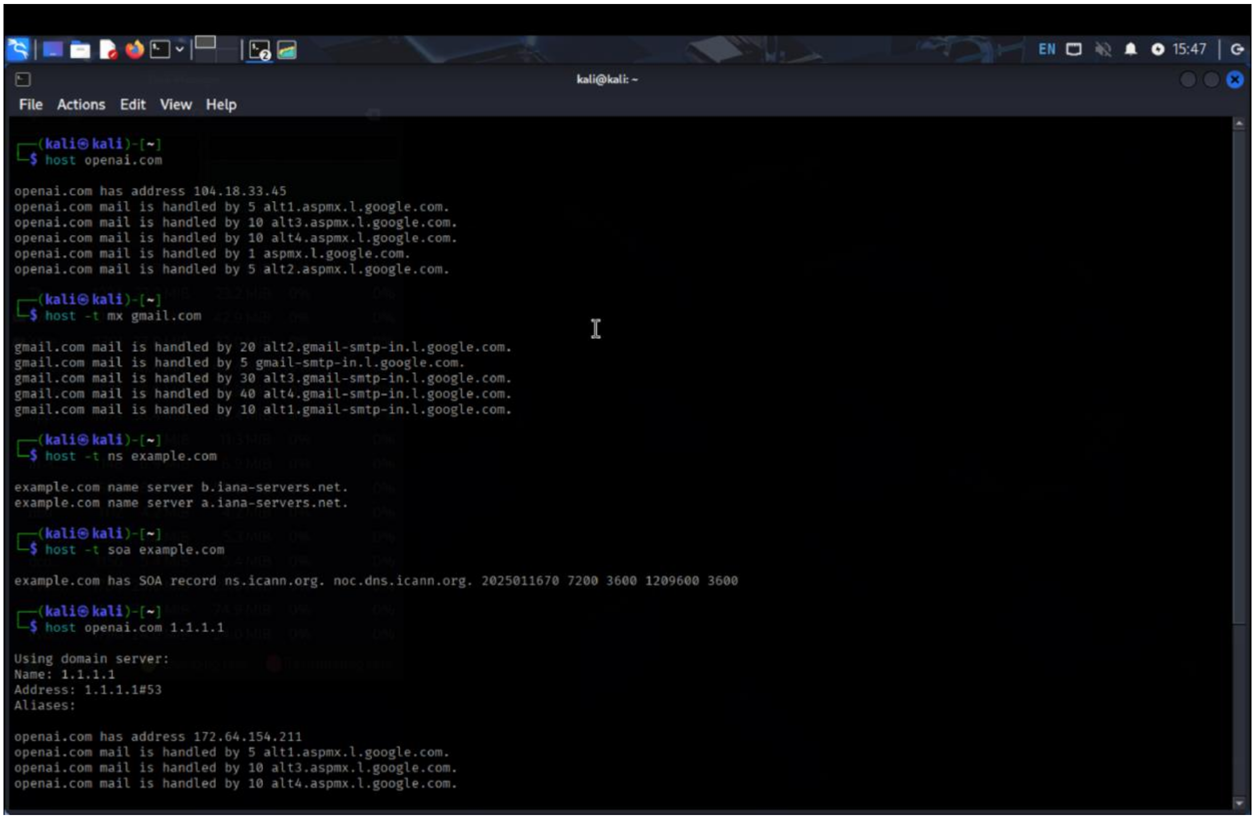
- **Operating System:** Kali Linux (or any Linux distro)
- **Command-Line Utility:** `host`

Tasks Performed

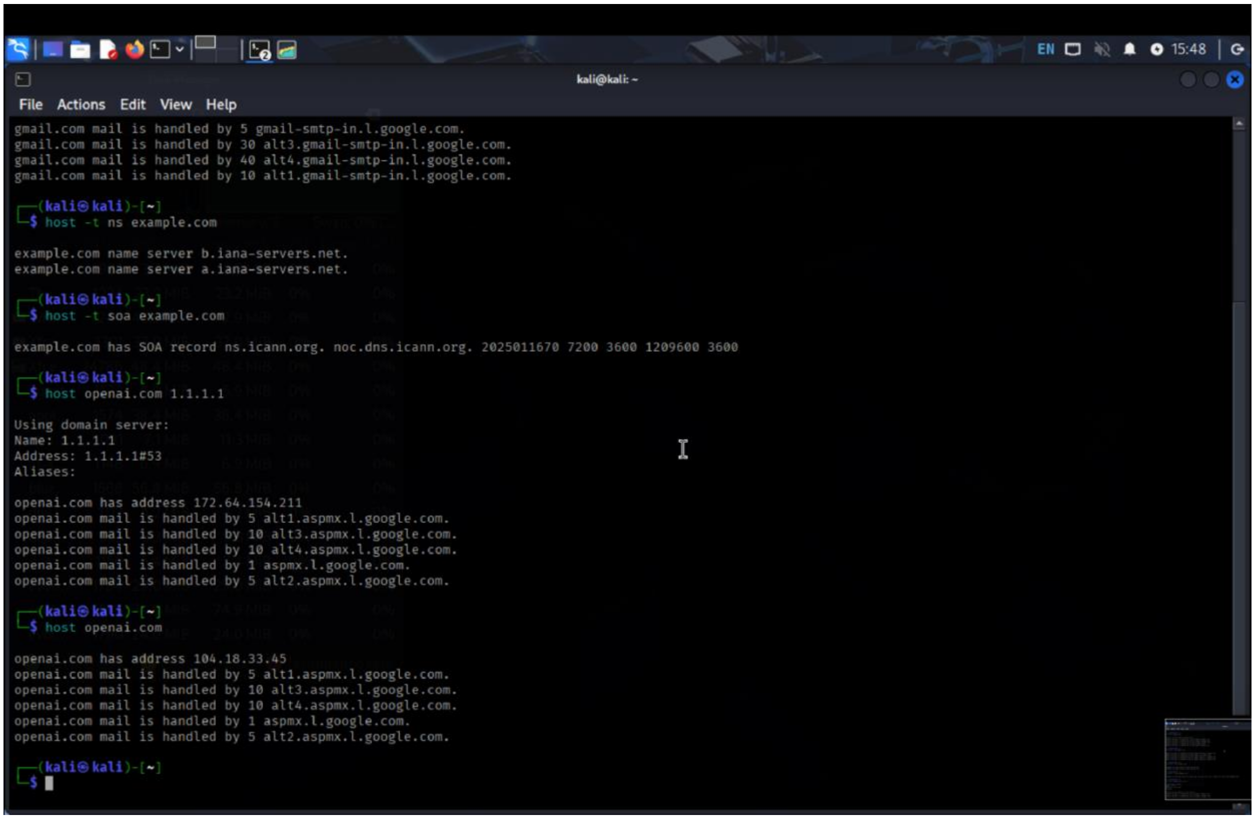
Level	Description
🟢 **Basic**	Queried `openai.com` using `host` to obtain its A (IP address) record.
🟡 **Intermediate**	Queried the domain's MX records to find the mail servers responsible for handling email.
🔴 **Advanced**	Used `host -t ns` and `host -t soa` to examine name servers and SOA records for deeper DNS metadata.
🔴 **Advanced**	Queried a **custom DNS server** using `host` and compared results with default resolver.

Why This Matters (Real-World Impact)

In cybersecurity and IT support roles, DNS misconfigurations and domain hijacking are critical concerns. Mastery of tools like `host` enables fast domain diagnostics, aids in blue team investigations, and prepares you to troubleshoot and secure enterprise DNS infrastructures with confidence.



```
┌──(kali㉿kali)-[~]
└─$ host openai.com

openai.com has address 104.18.33.45
openai.com mail is handled by 5 alt1.aspmx.l.google.com.
openai.com mail is handled by 10 alt3.aspmx.l.google.com.
openai.com mail is handled by 10 alt4.aspmx.l.google.com.
openai.com mail is handled by 1 aspmx.l.google.com.
openai.com mail is handled by 5 alt2.aspmx.l.google.com.

┌──(kali㉿kali)-[~]
└─$ host -t mx gmail.com

gmail.com mail is handled by 20 alt2.gmail-smtp-in.l.google.com.
gmail.com mail is handled by 5 gmail-smtp-in.l.google.com.
gmail.com mail is handled by 30 alt3.gmail-smtp-in.l.google.com.
gmail.com mail is handled by 40 alt4.gmail-smtp-in.l.google.com.
gmail.com mail is handled by 10 alt1.gmail-smtp-in.l.google.com.

┌──(kali㉿kali)-[~]
└─$ host -t ns example.com

example.com name server b.iana-servers.net.
example.com name server a.iana-servers.net.

┌──(kali㉿kali)-[~]
└─$ host -t soa example.com

example.com has SOA record ns.icann.org. noc.dns.icann.org. 2025011670 7200 3600 1209600 3600

┌──(kali㉿kali)-[~]
└─$ host openai.com 1.1.1.1

Using domain server:
Name: 1.1.1.1
Address: 1.1.1.1#53
Aliases:

openai.com has address 172.64.154.211
openai.com mail is handled by 5 alt1.aspmx.l.google.com.
openai.com mail is handled by 10 alt3.aspmx.l.google.com.
openai.com mail is handled by 10 alt4.aspmx.l.google.com.
```



```
gmail.com mail is handled by 5 gmail-smtp-in.l.google.com.
gmail.com mail is handled by 30 alt3.gmail-smtp-in.l.google.com.
gmail.com mail is handled by 40 alt4.gmail-smtp-in.l.google.com.
gmail.com mail is handled by 10 alt1.gmail-smtp-in.l.google.com.

┌──(kali㉿kali)-[~]
└─$ host -t ns example.com

example.com name server b.iana-servers.net.
example.com name server a.iana-servers.net.

┌──(kali㉿kali)-[~]
└─$ host -t soa example.com

example.com has SOA record ns.icann.org. noc.dns.icann.org. 2025011670 7200 3600 1209600 3600

┌──(kali㉿kali)-[~]
└─$ host openai.com 1.1.1.1

Using domain server:
Name: 1.1.1.1
Address: 1.1.1.1#53
Aliases:

openai.com has address 172.64.154.211
openai.com mail is handled by 5 alt1.aspmx.l.google.com.
openai.com mail is handled by 10 alt3.aspmx.l.google.com.
openai.com mail is handled by 10 alt4.aspmx.l.google.com.
openai.com mail is handled by 1 aspmx.l.google.com.
openai.com mail is handled by 5 alt2.aspmx.l.google.com.

┌──(kali㉿kali)-[~]
└─$ host openai.com

openai.com has address 104.18.33.45
openai.com mail is handled by 5 alt1.aspmx.l.google.com.
openai.com mail is handled by 10 alt3.aspmx.l.google.com.
openai.com mail is handled by 10 alt4.aspmx.l.google.com.
openai.com mail is handled by 1 aspmx.l.google.com.
openai.com mail is handled by 5 alt2.aspmx.l.google.com.

┌──(kali㉿kali)-[~]
└─$ 
```