BARI ANKIT (56)

Exp 6 : Study the use of network reconnaissance tools like WHOIS, dig,traceroute, nslookup to gather information about networks and domain registrars.

Network Reconnaissance Tools: WHOIS, Dig, Traceroute, NSLookup

Network reconnaissance is the process of gathering information about a network, domain, or IP address. It is often the first step in the process of penetration testing or identifying potential vulnerabilities in a network. The tools WHOIS, dig, traceroute, and nslookup are commonly used in this phase to gather detailed information about domains, IP addresses, and network paths.

Let's dive into each tool and explain its use:

---

1. WHOIS

WHOIS is a query and response protocol used for querying information about domain names, IP addresses, and network resources from domain registrars or databases. When you perform a WHOIS lookup, you can find who owns a domain, their contact information, domain registration dates, and other useful details.

Common Use Cases:

- **Domain Registration Information: WHOIS is used to obtain information about who owns a domain name, when it was registered, and when it expires.**
- **Contact Information: Get the registrant's name, organization, email, and phone number (if not private).**
- **IP Ownership: You can query WHOIS for details about an IP address to identify which organization owns that IP block.**

Example Command:

bash

Copy

whois example.com

Sample Output:

yaml

Copy

Domain Name: EXAMPLE.COM

Registrar: XYZ, Inc.

Registrant Name: John Doe

Registrant Organization: Example Inc.

Registrant Email: johndoe@example.com

Creation Date: 2000-01-01

Expiration Date: 2024-01-01

WHOIS Field Explanations:

- **Domain Name: The name of the domain.**
- **Registrar: The organization responsible for managing domain registrations.**
- **Registrant Name: The individual or company that owns the domain.**
- **Creation Date: The date the domain was registered.**
- **Expiration Date: The date the domain is set to expire.**
- **Nameservers: DNS servers associated with the domain.**

Privacy Consideration:

In many cases, registrants may choose to hide their contact information through domain privacy protection services. When this is done, WHOIS results may show generic information like "Domain Privacy" instead of personal details.

---

2. Dig (Domain Information Groper)

Dig is a powerful DNS query tool used to perform DNS lookups. It provides detailed information about DNS records, such as A, MX, NS, TXT, and CNAME records. It is an excellent tool for diagnosing DNS-related issues and gathering DNS-related data about a domain.

Common Use Cases:

- **DNS Lookup: You can query DNS records (A, MX, NS, etc.) to find IP addresses, mail servers, and nameservers.**
- **DNS Troubleshooting: Dig can be used to troubleshoot DNS resolution issues, view TTL (Time to Live) values, and more.**
- **Subdomain Discovery: You can use dig to find all DNS records associated with a domain.**

Example Command:

bash

Copy

dig example.com

Sample Output:

yaml

Copy

; <<>> DiG 9.10.6 <<>> example.com

;; global options: +cmd

;; Got answer:

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12345
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2
;; QUESTION SECTION:
;example.com.                IN      A
;; ANSWER SECTION:
example.com.          3600    IN      A       93.184.216.34
;; AUTHORITY SECTION:
example.com.          86400   IN      NS      a.iana-servers.net.
example.com.          86400   IN      NS      b.iana-servers.net.
;; ADDITIONAL SECTION:
a.iana-servers.net.   86400   IN      A       199.43.135.53
b.iana-servers.net.   86400   IN      A       199.43.133.53
```

Output Explanation:

- **ANSWER SECTION: Shows the IP address (93.184.216.34) associated with the domain.**
- **AUTHORITY SECTION: Lists the authoritative nameservers for the domain.**
- **ADDITIONAL SECTION: Shows additional records, in this case, the IP addresses of the authoritative nameservers.**

Common Dig Queries:

- **A record (IP address of a domain):**

bash

Copy

```
dig example.com A
```

- **MX record (Mail Exchange, email servers for the domain):**

bash

Copy

```
dig example.com MX
```

- **NS record (Nameservers for the domain):**

bash

Copy

```
dig example.com NS
```

- **TXT record (Used for verification purposes, e.g., SPF records):**

bash

Copy

dig example.com TXT

---

3. Traceroute

Traceroute is a network diagnostic tool used to track the path that packets take from the source machine to the destination (host). It shows each hop along the way, the IP addresses of the routers involved, and the round-trip time (RTT) for each hop.

Common Use Cases:

- **Network Troubleshooting: Traceroute can help identify where packets are being delayed or where the network path is failing.**
- **Identify Routing Issues: Determine where network issues (e.g., latency or packet loss) are occurring along the path.**
- **Network Path Analysis: Understand how packets travel across the network, which can help identify the physical location or intermediate hops in the network.**

Example Command:

bash

Copy

traceroute example.com

Sample Output:

nginx

Copy

traceroute to example.com (93.184.216.34), 30 hops max, 60 byte packets

1 192.168.1.1 (192.168.1.1) 0.460 ms 0.424 ms 0.391 ms

2 10.10.10.1 (10.10.10.1) 1.220 ms 1.181 ms 1.144 ms

3 * * *

4 172.217.12.206 (172.217.12.206) 19.120 ms 19.085 ms 19.051 ms

5 108.177.9.129 (108.177.9.129) 34.567 ms 34.531 ms 34.489 ms

6 example.com (93.184.216.34) 44.342 ms 44.313 ms 44.271 ms

Output Explanation:

- **Hop 1, 2: Shows the local network routers (your router and then the next hop).**
- **Hop 3: A * indicates that the router didn't respond in time (common for firewalls blocking ICMP packets).**
- **Hop 4-6: Shows the route from intermediate routers, and finally, the destination IP (example.com).**

Use Cases:

- **Diagnosing Latency: Identify if a specific router or network link is causing**

high latency or packet loss.

- Routing Analysis: Trace the path that packets take, which can be useful for understanding network topology.

---

4. NSLookup (Name Server Lookup)

NSLookup is a command-line tool used for querying DNS (Domain Name System) records. It can be used to find information about domain names, such as the IP address associated with a domain or the nameservers for a domain.

Common Use Cases:

- DNS Lookup: Find out the A record (IP address) or MX record (mail servers) for a domain.
- Checking Nameservers: Query which nameservers are responsible for a particular domain.
- Reverse DNS Lookup: Find the domain name associated with an IP address.

Example Command:

bash

Copy

nslookup example.com

Sample Output:

yaml

Copy

Server: UnKnown

Address: 192.168.1.1

Non-authoritative answer:

Name: example.com

Addresses: 93.184.216.34

Reverse Lookup:

bash

Copy

nslookup 93.184.216.34

Sample Output:

yaml

Copy

Server: UnKnown

Address: 192.168.1.1

Non-authoritative answer:

34.216.184.93.in-addr.arpa name = example.com.

Output Explanation:

- **NSLookup provides the IP address associated with the domain (93.184.216.34), or the domain name corresponding to the IP address in the reverse lookup.**

Use Cases:

- **DNS Troubleshooting: If you suspect a problem with DNS resolution, NSLookup can help you understand how the system resolves domain names.**
- **Domain Lookup: Quickly retrieve domain or subdomain information and associated IP addresses.**