Don Bosco Institute of Technology, Mumbai 400070
Department of Information Technology

Experiment No. : 7

Date: 12/10/22

Name: Swasti Jain
Batch: B
Roll No: 24

Title: Network Reconnaissance tools/commands.

Problem Definition : Use following Network Reconnaissance tools/commands to gather information about network and domain registrars. WHOIS, dig, traceroute, nslookup.

Prerequisite : Networking commands

Theory :

1) who is - The whois command tries to reach ARPANET host internic.net where it examines auser-name database to obtain information. The whois command should be used only by users on ARPANET.

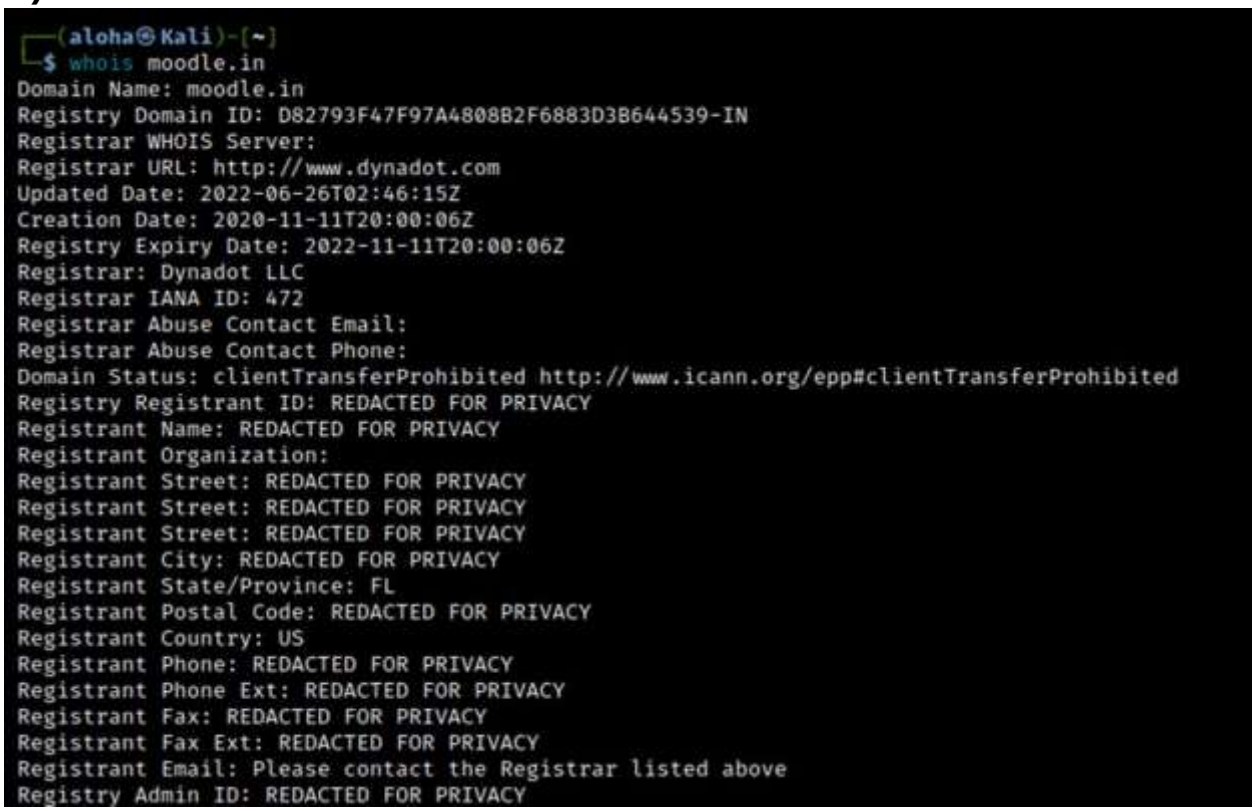
2) dig - dig command stands for Domain Information Groper. It is used for retrieving informationabout DNS name servers. It is basically used by network administrators. It is used for verifying and troubleshooting DNS problems and to perform DNS lookups.

3) traceroute - The traceroute command attempts to trace the route an IP packet follows to anInternet host by launching UDP probe packets with a small maximum time-to-live (Max_ttl variable), then listening for an ICMP TIME_EXCEEDED response from gateways along the way.

4) nslookup - The nslookup command queries internet domain name servers in two modes.Interactive mode allows you to query name servers for information about various hosts and domains, or to print a list of the hosts in a domain.

Results :

1.) Whois



2.) Dig

```
┌──(aloha㉿Kali)-[~]
└─$ dig dbit.in

; <<>> DiG 9.18.6-2-Debian <<>> dbit.in
;; global options: +cmd
;; Got answer:
;; →»HEADER«← opcode: QUERY, status: NOERROR, id: 49027
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;dbit.in.                       IN      A

;; ANSWER SECTION:
dbit.in.                3600    IN      A       15.206.23.229

;; Query time: 27 msec
;; SERVER: 10.0.1.148#53(10.0.1.148) (UDP)
;; WHEN: Mon Sep 12 00:49:51 EDT 2022
;; MSG SIZE  rcvd: 52
```

3.)traceroute

```
┌──(aloha㉿Kali)-[~]
└─$ traceroute dbit.in
traceroute to dbit.in (15.206.23.229), 30 hops max, 60 byte packets
 1  10.0.2.2 (10.0.2.2)  0.161 ms  0.213 ms  0.159 ms
 2  10.0.2.2 (10.0.2.2)  68.328 ms  68.201 ms  68.159 ms
```

4.)nslookup

```
┌──(aloha㉿Kali)-[~]
└─$ nslookup 15.206.23.229
229.23.206.15.in-addr.arpa      name = ec2-15-206-23-229.ap-south-1.compute.amazonaws.com.

Authoritative answers can be found from:
```

References :
Networking Commands