

Experiment 07

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

--

Roll No.	70
Name	MAYURI SHRIDATTA YERANDE
Class	D15-B
Subject	Security Lab
LO Mapped	LO3: Explore the different network reconnaissance tools to gather information about networks

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

Introduction:

Reconnaissance (or simply Recon) is the initial phase in the Pen Testing process. The goal of recon is to gather as much information about the target as you can. More information, the more beneficial it will be for further phases of pen testing.

There are two strategies of recon i.e, Active and Passive reconnaissance.

- Active Recon : It means interacting directly with a target to gather information. This is not recommended because it violates the rule of “hiding traces” in pen testing.
- Passive Recon : It means gathering information about a target using vast information present on the internet. In it, we aren’t interacting directly with the target so there is no fear of recording or logging our activity by target.

Implementation:-

1. WHOIS

WHOIS searches for an object in a WHOIS database. WHOIS is a query and response protocol that is widely used for querying databases that store the registered users of an internet resource, such as domain name or an IP address block, but is also used for a wider range of information.

```
ubuntu@ubuntu:~$ whois google.com
Domain Name: GOOGLE.COM
Registry Domain ID: 2138514_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2019-09-09T15:39:04Z
Creation Date: 1997-09-15T04:00:00Z
Registry Expiry Date: 2028-09-14T04:00:00Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: NS1.GOOGLE.COM
Name Server: NS2.GOOGLE.COM
```

2. DIG

dig command stands for Domain Information Groper. It is used for retrieving information about DNS name servers. It is basically used by network administrators. It is used for verifying and troubleshooting DNS problems and to perform DNS lookups. Dig command replaces older tools such as nslookup and the host.

```
ubuntu@ubuntu:~$ dig youtube.com

; <<>> DiG 9.18.1-1ubuntu1-Ubuntu <<>> youtube.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 31569
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;youtube.com.                IN      A

;; ANSWER SECTION:
youtube.com.                 5       IN      A      142.250.67.238

;; Query time: 4 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Thu Sep 22 09:43:44 UTC 2022
;; MSG SIZE rcvd: 56
```

3. NSLOOKUP

Nslookup (stands for “Name Server Lookup”) is a useful command for getting information from the DNS server. It is a network administration tool for querying the Domain Name System (DNS) to obtain domain name or IP address mapping or any other specific DNS record. It is also used to troubleshoot DNS-related problems.

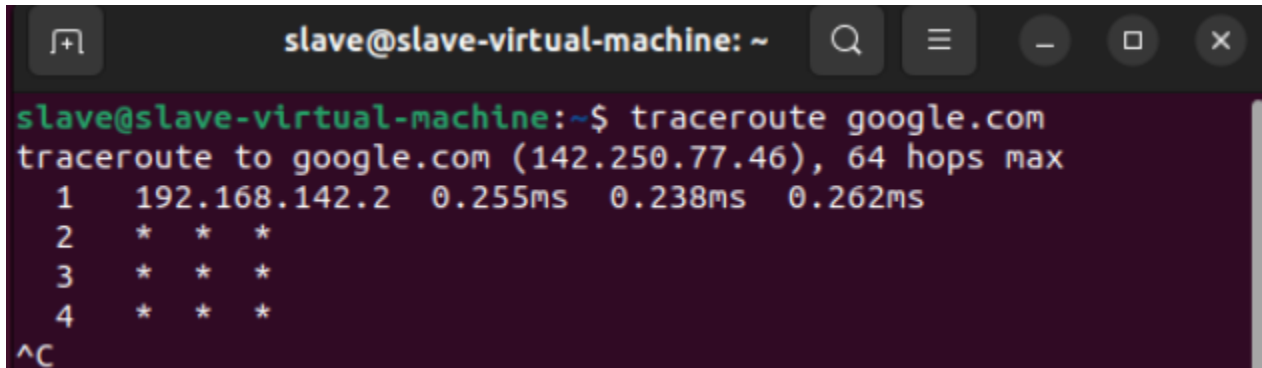
NSLOOKUP followed by the domain name will display the “A Record” (IP Address) of the domain. Use this command to find the address record for a domain. It queries domain name servers and gets the details.

```
ubuntu@ubuntu:~$ nslookup google.com
Server:          127.0.0.53
Address:         127.0.0.53#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.183.110
Name:   google.com
Address: 2404:6800:4009:827::200e
```

4. TRACEROUTE

Traceroute command in Linux prints the route that a packet takes to reach the host. This command is useful when you want to know about the route and about all the hops that a packet takes. traceroute command sends three packets to the hop and each of the time refers to the time taken by the packet to reach the hop.



```
slave@slave-virtual-machine: ~  
slave@slave-virtual-machine:~$ traceroute google.com  
traceroute to google.com (142.250.77.46), 64 hops max  
 1  192.168.142.2  0.255ms  0.238ms  0.262ms  
 2  * * *  
 3  * * *  
 4  * * *  
^C
```

Conclusion: In this experiment, Network reconnaissance tools like WHOIS, dig, traceroute, nslookup were studied and used in order to gather information about networks and domain registrars.