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

Experiment No. : 7

Name: Lavena Babu **Roll No.:** 29 **Date:** 12/09/22

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

Pre-requisite : Networking commands

Theory :

Reconnaissance is an important first stage in any ethical hacking attempt. Before it's possible to exploit a vulnerability in the target system, it's necessary to find it. By performing reconnaissance on the target, an ethical hacker can learn about the details of the target network and identify potential attack vectors.

Reconnaissance efforts can be broken up into two types: passive and active. While both versions can be effective, passive reconnaissance prioritizes subtlety (ensuring that the hacker is not detected), while active reconnaissance is used for cases where collecting information is more important than remaining undetected.

Top passive recon tools

In passive reconnaissance, the hacker never interacts directly with the target's network. The tools used for passive reconnaissance take advantage of unintentional data leaks from an organization to provide the hacker with insight into the internals of the organization's network.

1. Wireshark
2. Google
3. FindSubDomains.com
4. VirusTotal
5. Shodan

Top active recon tools

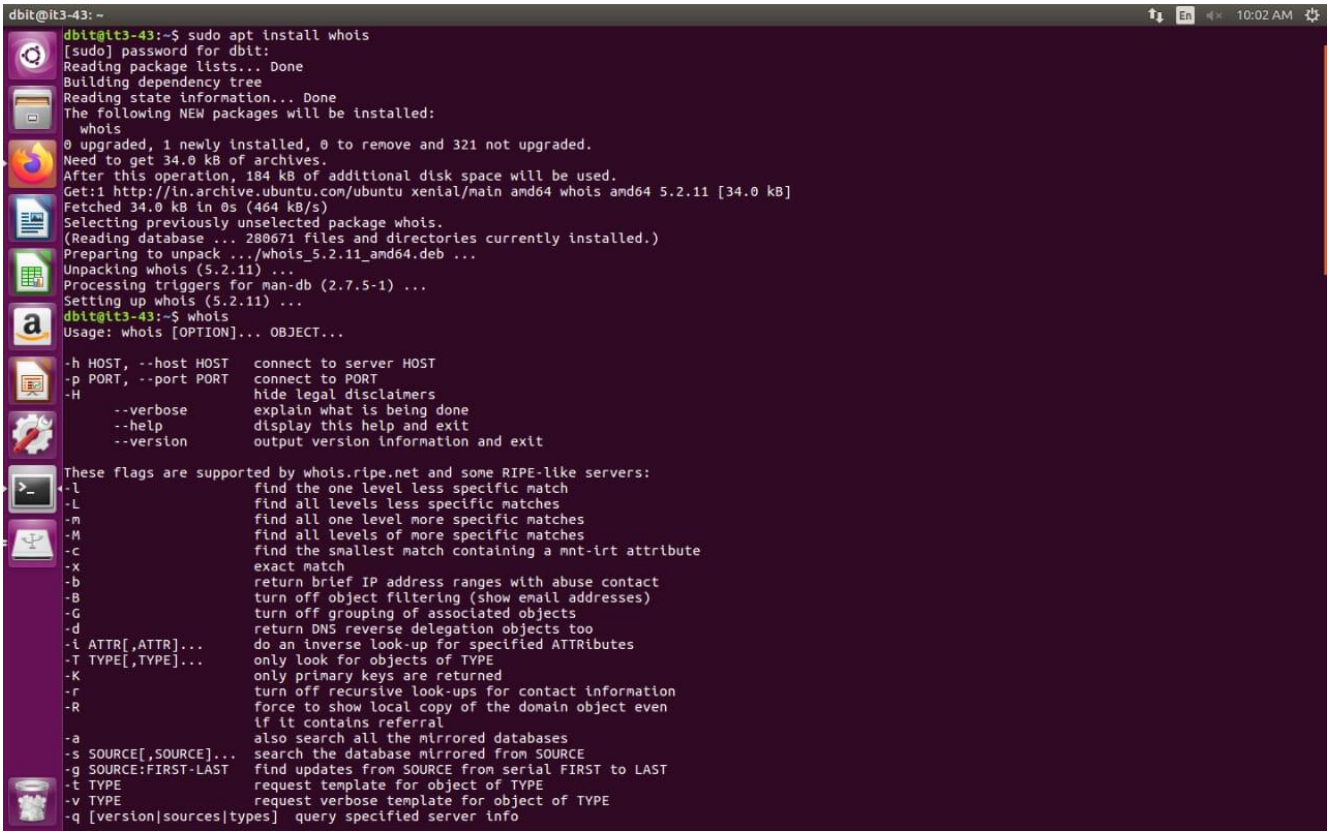
Tools for active reconnaissance are designed to interact directly with machines on the target network in order to collect data that may not be available by other means. Active reconnaissance can provide a hacker with much more detailed information about the target but also runs the risk of detection.

1. Nmap
2. Nessus
3. OpenVAS
4. Nikto
5. Metasploit

Network reconnaissance is a crucial part of any hacking operation. Any information that a hacker can learn about the target environment can help in identification of potential attack vectors and targeting exploits to potential vulnerabilities. By using a combination of passive and active reconnaissance tools and techniques, a hacker can maximize the information collected while minimizing their probability of detection.

Results :

WHOIS




```
dbit@it3-43:~$ whois google.com
connect: Network is unreachable
dbit@it3-43:~$ whois www.google.com
connect: Network is unreachable
dbit@it3-43:~$ whois geeksforgeeks.org
connect: Network is unreachable
dbit@it3-43:~$ whois www.geeksforgeeks.org
connect: Network is unreachable
```

dig

```
dbit@it3-43:~$ dig google.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20607
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 9

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             69      IN      A       216.58.203.14

;; AUTHORITY SECTION:
google.com.             108310  IN      NS      ns1.google.com.
google.com.             108310  IN      NS      ns2.google.com.
google.com.             108310  IN      NS      ns4.google.com.
google.com.             108310  IN      NS      ns3.google.com.

;; ADDITIONAL SECTION:
ns1.google.com.         86100   IN      A       216.239.32.10
ns1.google.com.         108893  IN      AAAA    2001:4860:4802:32::a
ns2.google.com.         86100   IN      A       216.239.34.10
ns2.google.com.         108893  IN      AAAA    2001:4860:4802:34::a
ns3.google.com.         86100   IN      A       216.239.36.10
ns3.google.com.         108893  IN      AAAA    2001:4860:4802:36::a
ns4.google.com.         86100   IN      A       216.239.38.10
ns4.google.com.         108893  IN      AAAA    2001:4860:4802:38::a

;; Query time: 3 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Mon Sep 12 10:06:29 IST 2022
;; MSG SIZE  rcvd: 303

dbit@it3-43:~$
```

traceroute

```
dbit@it3-43:~$ sudo apt install traceroute
[sudo] password for dbit:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  traceroute
0 upgraded, 1 newly installed, 0 to remove and 321 not upgraded.
Need to get 45.5 kB of archives.
After this operation, 177 kB of additional disk space will be used.
Get:1 http://in.archive.ubuntu.com/ubuntu xenial/universe amd64 traceroute amd64 1:2.0.21-1 [45.5 kB]
Fetched 45.5 kB in 0s (1,962 kB/s)
Selecting previously unselected package traceroute.
(Reading database ... 280680 files and directories currently installed.)
Preparing to unpack .../traceroute_1%3a2.0.21-1_amd64.deb ...
Unpacking traceroute (1:2.0.21-1) ...
Processing triggers for man-db (2.7.5-1) ...
Setting up traceroute (1:2.0.21-1) ...
update-alternatives: using /usr/bin/traceroute.db to provide /usr/bin/traceroute (traceroute) in auto mode
update-alternatives: using /usr/bin/lft.db to provide /usr/bin/lft (lft) in auto mode
update-alternatives: using /usr/bin/traceproto.db to provide /usr/bin/traceproto (traceproto) in auto mode
update-alternatives: using /usr/sbin/tcptraceroute.db to provide /usr/sbin/tcptraceroute (tcptraceroute) in auto mode
```

```
dbit@it3-43:~$ traceroute google.com
traceroute to google.com (142.250.192.78), 30 hops max, 60 byte packets
 1  newipcop.lan.dbit.in (10.0.1.1)  0.355 ms  0.321 ms  0.302 ms
 2  newipcop.lan.dbit.in (10.0.1.1)  0.277 ms !X  0.264 ms !X  1.477 ms !X
```

nslookup

```
dbit@it3-43:~$ nslookup google.com
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.192.78

dbit@it3-43:~$
```

References :

https://resources.infosecinstitute.com/topic/top-10-network-recon-tools/