Lab Assignment 6

Aim: Study the use of network reconnaissance tools to gather information about networks and domain registrars.

Lab Outcome Attainment: LO3

Commands:

Whois

Query and response protocol that gives you the information of domain registrant and registrar. Available as the utility in Linux systems.

https://whois.domaintools.com/

The important information that attackers look for: Email, registry expiry date, update date, registrant information

Attacks possible: domain hijacking, phishing, information gathering through social engineering

Traceroute

```
[root@rhel8dev ~]# traceroute www.google.com
traceroute to www.google.com (216.58.194.100), 30 hops max, 60 byte
packets
 1  _gateway (192.168.2.1)  2.396 ms  2.726 ms  3.057 ms
 2  145.sub-66-174-43.myvzw.com (66.174.43.145)  119.355 ms  119.315
ms  119.508 ms
 3  * * *
 4  10.209.189.140 (10.209.189.140)  120.321 ms  119.836 ms  120.009
ms
 5  66.sub-69-83-106.myvzw.com (69.83.106.66)  119.042 ms  119.489
ms  119.156 ms
 6  2.sub-69-83-107.myvzw.com (69.83.107.2)  120.039 ms  125.954 ms
101.450 ms
 7  112.sub-69-83-96.myvzw.com (69.83.96.112)  110.757 ms  108.485
ms  122.108 ms
 8  112.sub-69-83-96.myvzw.com (69.83.96.112)  115.028 ms  121.073
ms  125.537 ms
 9  116.sub-69-83-96.myvzw.com (69.83.96.116)  121.793 ms  124.769
ms  124.434 ms
10  Bundle-Ether10.GW6.DFW13.ALTER.NET (140.222.237.123)  128.082 ms
128.400 ms  126.509 ms
11  google-gw.customer.alter.net (204.148.43.118)  106.276 ms
107.885 ms  105.718 ms
12  108.170.252.129 (108.170.252.129)  99.725 ms  101.797 ms
108.170.252.161 (108.170.252.161)  101.671 ms
13  108.170.230.109 (108.170.230.109)  101.207 ms  100.515 ms
99.730 ms
14  dfw06s48-in-f100.1e100.net (216.58.194.100)  99.059 ms  94.502
ms  94.015 ms
[root@rhel8dev ~]#
```

Traceroute, by default, measures 30 hops of 60-byte packets.

If a packet is not acknowledged within the expected timeout, an asterisk is displayed.

What do these stars (asterisks) mean? Were the packets dropped? Are they timed out?

There are two possibilities when it comes to these stars. First, ICMP/UDP may not be configured. If the `traceroute` command completes successfully and you see these stars, most likely the device that was hit was not configured to reply to ICMP/UDP traffic. This result does not mean that the traffic wasn't passed. The second possibility is that the packets were dropped due to an issue on the network. These results are usually packet timeouts, or the traffic has been blocked by a firewall.

Execute following commands:

traceroute www.google.com

traceroute -m 20 www.google.com

traceroute -T www.google.com

traceroute -m 20 -I www.yahoo.com

How traceroute works?

Dig

Dig stands for (**Domain Information Groper**) is a network administration command-line tool for querying **Domain Name System** (**DNS**) name servers.

It is useful for verifying and troubleshooting **DNS** problems and also to perform **DNS** lookups and displays the answers that are returned from the name server that were queried.

Dig is part of the BIND domain name server software suite.

By default dig looks for the **"A"** (address) record of the domain specified, but you can specify other records also. The **MX** or **Mail eXchange** record tells mail servers how to route the email for the domain. Likewise **TTL**, **SOA** etc.

Dig yahoo.com (by default A records)

Dig yahoo.com +short

Dig yahoo.com -t ns #(name server record)

Dig yahoo.com -t mx #(mail servers list)

dig yahoo.com any +noall +answer #(all records)

dig yahoo.com mx +noall +answer redhat.com ns +noall +answer #(multiple websites' DNS speqcific query.

Nikto

Web vulnerability scanner

Find vulnerabilities of websites and attacks possible for them and their solutions

Nikto -Help

nikto -h google.com

#nikto -h websitename -ssl <enter>

Theharvester

The Harvester is a tool that was developed in python. Using this you can gather information like emails, subdomains, hosts, employee names, open ports and banners from different public sources like search engines, PGP key servers, and SHODAN computer database.

How to use this harvester tool ?

theharvester -d [domain name] -b [search engine name / all][options] [parameters]

Option's

-d: Domain to search or company name.

-b: Data source: baidu, bing, bingapi, dogpile, google, googleCSE, googleplus, google-profiles, linkedin, pgp, twitter, vhost, yahoo, all.

-s: Start in result number X (default: 0).

-v: Verify hostname via DNS resolution and also search for virtual hosts.

-f: Save the results into an HTML and XML file (both).

-n: Perform DNS reverse query on all ranges discovered.

-c: Perform DNS brute force for the domain name.

-t: Perform DNS TLD expansion discovery.

-e: Use this DNS server.

-l: Limit the number of results to work with (bing goes from 20 to 20 results, google 100 to 100, and pgp doesn't use this option).

-h: Use SHODAN database to query discovered hosts.

$theHarvester –help

$theHarvester -d Microsoft.com -l 500 -b google

#theHarvester -d microsoft.com -l 100 -b google

#theHarvester -d microsoft.com -l 500 -b linkedin

#theHarvester -d microsoft.com -l 500 -b netcraft

#theHarvester -d microsoft.com -l 500 -b all

Dmitry:

Deepmagic Information Gathering Tool

DMitry has the ability to perform TCP port scan on host targets, search subdomain on a target host, whois lookup, E-mail address search on target hosts.

Command for whois lookup, to retrieve netcraft info, search for subdomains, search for email addresses,

dmitry -wnse -o dmitry-info.txt yahoo.com

Command for port scanning

dmitry -pb -o dmitry-portscaninfo.txt yahoo.com