

Assignment Number: 6

Name: Divya Shah; Branch: I.T (T.E.); Roll Number: 115

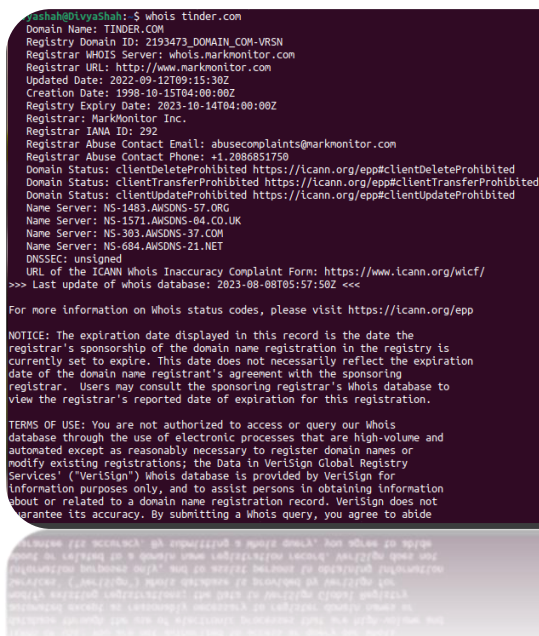
24/08/2023

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

LO mapped: LO3

Theory:

The whois command is used to retrieve information about domain names, IP addresses, and their associated registrants, contacts, and more.



```

yashah@DivyaShah:~$ whois tinder.com
Domain Name: TINDER.COM
Registry Domain ID: 2193473.DOMAIN.COM-VRSN
Registrar WHOIS Server: whois.narkmonitor.com
Registrar URL: http://www.narkmonitor.com
Updated Date: 2022-09-12T09:15:30Z
Creation Date: 1998-10-15T04:00:00Z
Registry Expiry Date: 2023-10-14T04:00:00Z
Registrar: NarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@narkmonitor.com
Registrar Abuse Contact Phone: +1.2886851759
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Name Server: NS-1483.AWSDNS-57.ORG
Name Server: NS-1571.AWSDNS-84.CO.UK
Name Server: NS-303.AWSDNS-37.COM
Name Server: NS-684.AWSDNS-21.NET
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2023-08-08T05:57:50Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar. Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
warrant its accuracy. By submitting a Whois query, you agree to abide

```

This command to retrieve basic information about a domain name

The dig command is a powerful tool for querying DNS (Domain Name System) servers to retrieve information about domain names, IP addresses, and various DNS records.

```
divyashah@DivyaShah:~$ dig tinder.com
; <<>> DiG 9.18.1-1ubuntu1.3-Ubuntu <<>> tinder.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56345
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 4, ADDITIONAL: 1

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

;; ANSWER SECTION:
tinder.com.                46      IN      A      52.84.150.60
tinder.com.                46      IN      A      52.84.150.54
tinder.com.                46      IN      A      52.84.150.39
tinder.com.                46      IN      A      52.84.150.55

;; AUTHORITY SECTION:
tinder.com.                46891   IN      NS      ns-1483.awsdns-57.org.
tinder.com.                46891   IN      NS      ns-1571.awsdns-04.co.uk.
tinder.com.                46891   IN      NS      ns-303.awsdns-37.com.
tinder.com.                46891   IN      NS      ns-684.awsdns-21.net.

;; Query time: 60 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Tue Aug 08 11:34:03 IST 2023
;; MSG SIZE rcvd: 240

divyashah@DivyaShah:~$
```

To perform a basic DNS lookup for a domain name

The traceroute command is used to trace the route that packets take from your computer to a destination IP address or domain name. It shows you each hop (router) that the packet passes through on its way to the destination.

```
divyashah@DivyaShah:~$ traceroute -m 5 tinder.com
traceroute to tinder.com (52.84.150.39), 5 hops max
 1  10.0.2.2  0.642ms  0.896ms  0.590ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *

divyashah@DivyaShah:~$
```

To specify the number of hops (maximum TTL value) using the -m option

The nslookup command is used to query DNS (Domain Name System) servers to retrieve information about domain names, IP addresses, and related DNS records.

```
divyashah@DivyaShah:~$ nslookup tinder.com
Server:      127.0.0.53
Address:     127.0.0.53#53
```

```
Non-authoritative answer:
```

```
Name:   tinder.com
Address: 52.84.150.60
Name:   tinder.com
Address: 52.84.150.39
Name:   tinder.com
Address: 52.84.150.55
Name:   tinder.com
Address: 52.84.150.54
```

```
qql622: 25'84'120'24
```

```
qql622: 25'84'120'24
```

```
qql622: 25'84'120'24
```

```
qql622: 25'84'120'24
```

To perform a basic DNS lookup for a domain name

Nikto is a web server vulnerability scanner that helps you identify security vulnerabilities and potential issues on web servers.

```
Nikto v2.1.5
-----
Target IP:      52.84.150.39
Target Hostname: tinder.com
Target Port:    80
Start Time:     2023-08-08 11:48:47 (GMT+5.5)
-----
Server: CloudFront
Retrieved via header: 1.1 dcb6371435a8fec6aa5c3b2c88c86d30.cloudfront.net (CloudFront)
The anti-clickjacking X-Frame-Options header is not present.
Uncommon header 'x-amz-cf-pop' found, with contents: BOM50-C1
Uncommon header 'x-cache' found, with contents: Redirect from cloudfront
Uncommon header 'x-amz-cf-id' found, with contents: K5ssAlJ_onQX2KI1cLnGkZzIz8RBNPzk7d2HJhecY250n0eUj5wbXg==
Root page / redirects to: https://tinder.com/
No CGI Directories found (use '-C all' to force check all possible dirs)
Server banner has changed from 'CloudFront' to 'nginx' which may suggest a WAF, load balancer or proxy is in place
Server leaks inodes via ETags, header found with file /robots.txt, fields: 0xH/6f 0x189bdf59680
Uncommon header 'x-dns-prefetch-control' found, with contents: on
Uncommon header 'x-xss-protection' found, with contents: 1; mode=block
Uncommon header 'strict-transport-security' found, with contents: max-age=15552000; includeSubDomains
Uncommon header 'content-security-policy' found, with contents: script-src * 'unsafe-inline' 'unsafe-eval'; style-src * 'unsafe-inline' blob;; img-src * data: blob;; media-src * data:
Uncommon header 'x-webkit-csp' found, with contents: script-src * 'unsafe-inline' 'unsafe-eval'; style-src * 'unsafe-inline' blob;; img-src * data: blob;; media-src * data:
Uncommon header 'x-download-options' found, with contents: noopen
Uncommon header 'x-frame-options' found, with contents: SAMEORIGIN
Uncommon header 'x-content-security-policy' found, with contents: script-src * 'unsafe-inline' 'unsafe-eval'; style-src * 'unsafe-inline' blob;; img-src * data: blob;; media-src * data:
Uncommon header 'referrer-policy' found, with contents: origin-when-cross-origin
Uncommon header 'x-content-type-options' found, with contents: nosniff
'robots.txt' contains 3 entries which should be manually viewed.
Cookie AWSALB created without the httponly flag
Cookie AWSALBCORS created without the httponly flag
Uncommon header 'x-render-method' found, with contents: SSR
divyashah@DivyaShah:~$
```

DMitry (Deepmagic Information Gathering Tool) is a command-line tool used for information gathering about a target. It can retrieve a variety of information about a domain, IP address, or hostname.

