Experiment No. 6

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

Objectives:

• To understand network information discovery.

• To study various basic network commands to gather network information.

• To understand passive attack technique.

Outcomes: The learner will be able to

Apply basic network command to gather basic network information.

Hardware / Software Required: Unix/Linux

Theory:

1. WHOIS: WHOIS is the Linux utility for searching an object in a WHOIS database. The WHOIS database of a domain is the publicly displayed information about a domains ownership, billing, technical, administrative, and nameserver information. Running a WHOIS on your domain will look the domain up at the registrar for the domain information. All domains have WHOIS information.
   WHOIS database can be queried to obtain the following information via WHOIS:
   - Administrative contact details, including names, email addresses, and telephone numbers
   - Mailing addresses for office locations relating to the target organization
   - Details of authoritative name servers for each given domain

   Example: Querying Facebook.com

   ssc@ssc-OptiPlex-380:~$ whois facebook.com

   Whois Server Version 2.0

   Domain names in the .com and .net domains can now be registered

   with many different competing registrars. Go to http://www.internic.net

   for detailed information.

   Server Name: FACEBOOK.COM.BRETLANDTRUSTMERCHANDISINGDEPART.COM

   IP Address: 69.63.176.11

   Registrar: GOOGLE INC.

   Whois Server: whois.rrpproxy.net

   Referral URL: http://domains.google.com

Server Name:

FACEBOOK.COM.DISABLE.YOUR.TIMELINE.NOW.WITH.THE.ORIGINAL.TIMELINE-REMOVE.NET

IP Address: 8.8.8.8

Registrar: ENOM, INC.

Whois Server: whois.enom.com

Referral URL: http://www.enom.com

Server Name:

FACEBOOK.COM.GET.ONE.MILLION.DOLLARS.AT.WWW.UNIMUNDI.COM

IP Address: 209.126.190.70

Registrar: PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM

Whois Server: whois.PublicDomainRegistry.com

Referral URL: http://www.PublicDomainRegistry.com

Server Name: FACEBOOK.COM.LOVED.BY.WWW.SHQIPHOST.COM

IP Address: 46.4.210.254

Registrar: ONLINENIC, INC.

Whois Server: whois.onlinenic.com

Referral URL: http://www.OnlineNIC.com

Server Name: FACEBOOK.COM.MORE.INFO.AT.WWW.BEYONDWHOIS.COM

IP Address: 203.36.226.2

Registrar: INSTRA CORPORATION PTY, LTD.

Whois Server: whois.instra.net

Referral URL: http://www.instra.com

Server Name:

FACEBOOK.COM.ZZZZZ.GET.LAID.AT.WWW.SWINGINGCOMMUNITY.COM

IP Address: 69.41.185.229

Registrar: TUCOWS DOMAINS INC.

Whois Server: whois.tucows.com

Referral URL: http://www.tucowsdomains.com

Domain Name: FACEBOOK.COM

Registrar: MARKMONITOR INC.

Sponsoring Registrar IANA ID: 292

Whois Server: whois.markmonitor.com

Referral URL: http://www.markmonitor.com

Name Server: A.NS.FACEBOOK.COM

Name Server: B.NS.FACEBOOK.COM

Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited

Status:clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited

Status:clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited

Status:serverDeleteProhibited

http://www.icann.org/epp#serverDeleteProhibited

Status:serverTransferProhibited
http://www.icann.org/epp#serverTransferProhibited

Status:serverUpdateProhibited http://www.icann.org/epp#serverUpdateProhibited

Updated Date: 28-sep-2012

Creation Date: 29-mar-1997

Expiration Date: 30-mar-2020

>>> Last update of whois database: Fri, 17 Jul 2015 04:12:12 GMT <<<

The Registry database contains ONLY .COM, .NET, .EDU domains and Registrars.

For more information on Whois status codes, please visit

https://www.icann.org/resources/pages/epp-status-codes-2014-06-16-en.

Domain Name: facebook.com

Registry Domain ID: 2320948_DOMAIN_COM-VRSN

Registrar WHOIS Server: whois.markmonitor.com

Registrar URL: http://www.markmonitor.com

Updated Date: 2014-10-28T12:38:28-0700

reation Date: 1997-03-28T21:00:00-0800

Registrar Registration Expiration Date: 2020-03-29T21:00:00-0700

Registrar: MarkMonitor, Inc.

Registrar IANA ID: 292

Registrar Abuse Contact Email: abusecomplaints@markmonitor.com

Registrar Abuse Contact Phone: +1.2083895740

Domain Status: clientUpdateProhibited
(https://www.icann.org/epp#clientUpdateProhibited)

Domain Status: clientTransferProhibited

(https://www.icann.org/epp#clientTransferProhibited)

Domain Status: clientDeleteProhibited
(https://www.icann.org/epp#clientDeleteProhibited)

Registry Registrant ID:

Registrant Name: Domain Administrator

Registrant Organization: Facebook, Inc.

Registrant Street: 1601 Willow Road,

Registrant City: Menlo Park

Registrant State/Province: CA

Registrant Postal Code: 94025

Registrant Country: US

Registrant Phone: +1.6505434800

Registrant Phone Ext:

Registrant Fax: +1.6505434800

Registrant Fax Ext:

Registrant Email: domain@fb.com

Registry Admin ID:

Admin Name: Domain Administrator

Admin Organization: Facebook, Inc.

Admin Street: 1601 Willow Road,

Admin City: Menlo Park

Admin State/Province: CA

Admin Postal Code: 94025

Admin Country: US

Admin Phone: +1.6505434800

Admin Phone Ext:

Admin Fax: +1.6505434800

Admin Fax Ext:

Admin Email: domain@fb.com

Registry Tech ID:

Tech Name: Domain Administrator

Tech Organization: Facebook, Inc.

Tech Street: 1601 Willow Road,

Tech City: Menlo Park

Tech State/Province: CA

Tech Postal Code: 94025

Tech Country: US

Tech Phone: +1.6505434800

Tech Phone Ext:

Tech Fax: +1.6505434800

Tech Fax Ext:

Tech Email: domain@fb.com

Name Server: b.ns.facebook.com

Name Server: a.ns.facebook.com

DNSSEC: unsigned

URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/

>>> Last update of WHOIS database: 2015-07-16T21:08:30-0700 <<<

(1) allow, enable, or otherwise support the transmission of mass unsolicited, commercial advertising or solicitations via e-mail (spam); or

(2) enable high volume, automated, electronic processes that apply to MarkMonitor.com (or its systems).

MarkMonitor.com reserves the right to modify these terms at any time.

By submitting this query, you agree to abide by this policy.

MarkMonitor is the Global Leader in Online Brand Protection.

MarkMonitor Domain Management(TM)

MarkMonitor Brand Protection(TM)

MarkMonitor AntiPiracy(TM)

MarkMonitor AntiFraud(TM)

Professional and Managed Services

Visit MarkMonitor at http://www.markmonitor.com

Contact us at +1.8007459229

In Europe, at +44.02032062220

ssc@ssc-OptiPlex-380:~$

2. Dig: Dig is a networking tool that can query DNS servers for information. It can be very helpful for diagnosing problems with domain pointing and is a good way to verify that your configuration is working. The most basic way to use dig is to specify the domain we wish to query:

   Example:

   $ dig duckduckgo.com

   ; <<>> DiG 9.8.1-P1 <<>> duckduckgo.com

   ;; global options: +cmd

   ;; Got answer:

   ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64399

   ;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 0

   ;; QUESTION SECTION:

   ;duckduckgo.com. IN A

   ;; ANSWER SECTION:

duckduckgo.com. 99 IN A 107.21.1.61

duckduckgo.com. 99 IN A 184.72.106.253

duckduckgo.com. 99 IN A 184.72.106.52

duckduckgo.com. 99 IN A 184.72.115.86

;; Query time: 33 msec

;; SERVER: 8.8.8.8#53(8.8.8.8)

;; WHEN: Fri Aug 23 14:26:17 2013

;; MSG SIZE rcvd: 96

The lines above act as a header for the query performed. It is possible to run dig in batch mode,

so proper labeling of the output is essential to allow for correct analysis.

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64399

;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 0

The next section gives us a technical summary of our query results. We can see that the query

was successful, certain flags were used, and that 4 "answers" were received.

;; QUESTION SECTION:

;duckduckgo.com. IN A

;; ANSWER SECTION:

duckduckgo.com. 99 IN A 107.21.1.61

duckduckgo.com. 99 IN A 184.72.106.253

duckduckgo.com. 99 IN A 184.72.106.52

duckduckgo.com. 99 IN A 184.72.115.86

The above section of the output contains the actual results we were looking for. It restates the

query and then returns the matching DNS records for that domain name.

Here, we can see that there are four "A" records for "duckduckgo.com". By default, "A" records

are returned. This gives us the IP addresses that the domain name resolves to.

The "99" is the TTL (time to live) before the DNS server rechecks the association between the

domain name and the IP address. The "IN" means the class of the record is a standard internet

class.

;; Query time: 33 msec

;; SERVER: 8.8.8.8#53(8.8.8.8)

;; WHEN: Fri Aug 23 14:26:17 2013

;; MSG SIZE rcvd: 96

These lines simply provide some statistics about the actual query results. The query time can

be indicative of problems with the DNS servers.

3. Traceroute: Traceroute prints the route that packets take to a network host. Traceroute utility uses the TTL field in the IP header to achieve its operation. For users who are new to TTL field, this field describes how much hops a particular packet will take while traveling on network. So, this effectively outlines the lifetime of the packet on network. This field is usually set to 32 or 64.Each time the packet is held on an intermediate router, it decreases the TTL value by 1. When a router finds the TTL value of 1 in a received packet then that packet is not forwarded but instead discarded. After discarding the packet, router sends an ICMP error message of —Time exceededو back to the source from where packet generated. The ICMP packet that is sent back contains the IP address of the router. So now it can be easily understood that traceroute operates by sending packets with TTL value starting from 1 and then incrementing by one each time. Each time a router receives the packet, it checks the TTL field, if TTL field is 1 then it discards the packet and sends the ICMP error packet containing its IP address and this is what traceroute requires. So traceroute incrementally fetches the IP of all the routers between the source and the destination.

   Example:

   $traceroute example.com

   traceroute to example.com (64.13.192.208), 64 hops max, 40 byte packets

   1 72.10.62.1 (72.10.62.1) 1.000 ms 0.739 ms 0.702 ms

   2 10.101.248.1 (10.101.248.1) 0.683 ms 0.385 ms 0.315 ms

   3 10.104.65.161 (10.104.65.161) 0.791 ms 0.703 ms 0.686 ms

   4 10.104.65.161 (10.104.65.161) 0.791 ms 0.703 ms 0.686 ms

5 10.0.10.33 (10.0.10.33) 2.652 ms 2.260 ms 5.353 ms

6 acmkokeaig.gs01.gridserver.com (64.13.192.208) 3.384 ms 8.001 ms 2.439 ms

4. Nslookup: The nslookup command is used to query internet name servers interactively for information. nslookup, which stands for "name server lookup", is a useful tool for finding out information about a named domain. By default, nslookup will translate a domain name to an IP address (or vice versa). For instance, to find out what the IP address of microsoft.com is, you could run the command:

   Example:

   $nslookup microsoft.com

   Server: 8.8.8.8

   Address: 8.8.8.8#53

   Non-authoritative answer:

   Name: microsoft.com

   Address: 134.170.185.46

   Name: microsoft.com

   Address: 134.170.188.221

   Here, 8.8.8.8 is the address of our system's Domain Name Server. This is the server our system is configured to use to translate domain names into IP addresses. "#53" indicates that we are communicating with it on port 53, which is the standard port number domain name servers use to accept queries. Below this, we have our lookup information for microsoft.com. Our name server returned two entries, 134.170.185.46 and 134.170.188.221. This indicates that microsoft.com uses a round robin setup to distribute server load. When you accessmicrsoft.com, you may be directed to either of these servers and your packets will be routed to the correct destination. You can see that we have received a "Non-authoritative answer" to our query. An answer is "authoritative" only if our DNS has the complete zone file information for the domain in question. More often, our DNS will have a cache of information representing the last authoritative answer it received when it made a similar query, this information is passed on to you, but the server qualifies it as "non authoritative": the information was recently received from an authoritative source, but the DNS server is not itself that authority.

Conclusion:

The network reconnaissance tools like Whois, Dig, Traceroute, NSlookup are generally used for gathering information about network and domain.