|  |  |
| --- | --- |
| **Academic Year** | **: 2021-22 Sem-I** |
| **Class** | **: TY BTech Instrumentation & Control** |
| **Course Name** | **: Cyber Security** |
| **Name** | **: Shaunak Deshpande** |
| **Division** | **: IC-C** |
| **Roll No.** | **: 39** |
| **G.R. No.** | **: 11911180** |
| **Lab Number** | **: 01** |
| **Experiment** | **: Study of Network Reconnaissance tools.** |

**WHOIS Lookup**

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 a domain name or an IP address block, but is also used for a wider range of other information. It is a widely used Internet record listing that identifies who owns a domain and how to get in contact with them. The Internet Corporation for Assigned Names and Numbers (ICANN) regulates domain name registration and ownership. Whois records have proven to be extremely useful and have developed into an essential resource for maintaining the integrity of the domain name registration and website ownership process.

WHOIS example in reconnaissance in steps:

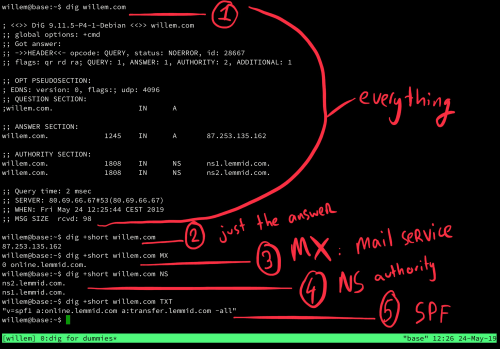
* Start with the phishing webpage: aeroconf2014[.]org
* Get the email address from Whois: info (at) usa[.]gov[.]us
* Reverse the email into a list of current AND historic domain names
* Use Whois history on these domains to surface a new and interesting email: keyvan[.]ajaxtm (at) gmail[.] com
* Reverse this new email into a list of curent and historic domain names
* Do a Whois lookup on the short-lived domain: dddddddddd445624[.]com
* Pull the registrant name from this record: Ali Alavi
* Reverse this registrant name into a list of current and historic domains
* Investigate a few of the associated domains, say for example: youthpartyofiran[.]com
* Go deep into Whois history on this domain and pull out a new associated email: ali\_alavi97 (at) yahoo[.]com
* And so on.

[Source](https://www.domaintools.com/support/what-is-whois-information-and-why-is-it-valuable#:~:text=Whois%20is%20a%20widely%20used,get%20in%20contact%20with%20them.&text=Whois%20records%20have%20proven%20to,registration%20and%20website%20ownership%20process)

**Dig**

The 'dig'-command stands for Domain information groper is a tool for questioning DNS nameservers for information about IP-addresses, hostnames, mail servers and other kinds of network settings. The dig-command is available on Unix, macOS, GNU/Linux and Windows.

Example:



1) dig willem.com will return all information about the question, answer, authority (the one that answered the question) and statistics of the actual query (like how long it took to get an answer).

2) dig +short willem.com omits all the extra information and only returns the answer. Here you can see that willem.com points to IP-address 87.253.135.162.

3) dig +short willem.com MX will show you the mailer exchange (MX) records. MX-records are crucial for email to arrive at the right server. Basically it's the designation of the post office responsible for email linked to the domain name. For willem.com this is a mail services called online.lemmid.com. Other popular mail services are Office365 and Google Gmail. Using dig you can find out what mail service somebody is using.

4) dig +short willem.com NS will show you the name servers that are responsible for handling queries for this domain name. Usually these are the servers operated by the domain name registry, your domain name provider. Using dig you can find what kind of domain name provider somebody is using (in the case of willem.com, that's Lemmid).

5) dig +short willem.com TXT will return the text record linked to the domain name, this is where you'll find the so called SPF-record. The SPF-record is another crucial part of email, its useful to dig a little deeper into SPF.

[Source](https://willem.com/blog/2019-05-24_dig-for-dummies/)

**Traceroute**

Quite simply, a traceroute procedure allows you to find out precisely how a data transmission (like a Google search) traveled from your computer to another. Essentially, the traceroute compiles a list of the computers on the network that are involved with specific Internet activity.

The traceroute identifies each computer/server on that list and the amount of time it took the data to get from one computer to the next. If there was a hiccup or interruption in the transfer of data, the traceroute will show where along the chain the problem occurred.

Aside from being somewhat interesting, performing a traceroute also has a very practical use: If someone is having difficulty accessing a particular website or computer, performing a traceroute can help find out where the problem is occurring along the network.

How to use:

On a PC using Windows, you can perform a traceroute using the traceroute utility on the Windows operating system (as long as you are not attempting to tap into heavily secured networks). You’ll need to know the domain name, IP address, or name of the specific computer you’re trying to reach.

Using the traceroute utility, you would type “tracert x“—where “x” stands for the IP address, the domain name or the computer name.

If using Macintosh OS X or any subsequent versions, you may use either the Terminal program or the network utility to generate a traceroute. The utility will display the traceroute on your screen.

[Source](https://whatismyipaddress.com/traceroute#:~:text=Traceroute%20defined.&text=Essentially%2C%20the%20traceroute%20compiles%20a,one%20computer%20to%20the%20next.)

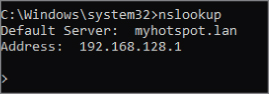
**NSLookup**

The main use of nslookup is to help with any DNS issues you may have. You can use it to find the IP address of a host, find the domain name of an IP address, or find mail servers on a domain. This tool can be used in an interactive and a noninteractive mode. In Lab 1.3, you'll use nslookup.

Open a command prompt or a terminal window.

To work in interactive mode, type nslookup at the prompt and press Enter. You will get an nslookup prompt, as you see in Figure 1.4. To escape the prompt, press Ctrl+C.

Screenshot for using nslookup prompt to work in the interactive mode.



To work in noninteractive mode, type nslookup www.example.com at the prompt to acquire DNS information for the specific site

Text

Description automatically generated

[Source](https://subscription.packtpub.com/book/security/9781119552932/4/ch04lvl1sec07/nslookup)