# CIT 285 - Lab #9: DNS Security

## Introduction

In this lab, we will research the names and IP addresses of several domains to determine how much information is exposed through domain registration and DNS configuration. We will run our security tools on Kali, a Linux distribution designed for network security and penetration testing.

**References**

1. DiG HOWTO, http://www.madboa.com/geek/dig/
2. dig man page, man dig

## 2: Domain Registration

We will run whois in the terminal window to find domain registration information. The output of this command is long, so we will pipe it through less to paginate it. To see the entire output, use the space bar to move between the pages.

2.1: Use the command below to answer the following

* Who is the administrative point of contact for NKU's domain?
* Who is the technical point of contact for NKU's domain?
* What information is provided for the DNS Name Servers used at NKU?

**# whois nku.edu | less**

**The administrative point of contact for NKU’s domain is domain admin with the NKU address and number. The technical point of contact for NKU’s domain is the address of NKU and the phone number. The DNS name servers used are NS4.NKU.ESU and NS5.NKU.EDU**

Text

Description automatically generated

## 3: DNS Lookups with whois & DiG

The DiG (Domain information Groper) command can be used to lookup DNS information. It is a replacement for the older nslookup tool, which is still available on most Linux and Windows systems.

By default dig provides long output with much information we don't need, so we will often use the +nocomments +nostats options to remove the irrelevant output.

Compare the results from the commands dig and nslookup.

# dig [www.nku.edu](http://www.nku.edu) + nocomments + nostats

# dig [www.nku.edu](http://www.nku.edu)

# nslookup [www.nku.edu](http://www.nku.edu)

3.1: What is the IP address of the DNS servers used by devices on NKU’s network?

3.2: What is the IP address of [www.nku.edu](http://www.nku.edu) web server? If none provided, write none.

The IP address of the DNS servers used by devices is 172.28.102.11. The IP address of NKU web server is 172.28.102.11

3.3: Dig can lookup a name using another DNS server too.

* What IP address is returned when the Google public DNS server is used with dig to return information about [www.nku.edu](http://www.nku.edu)?
* Is this an internal (private) or external (public) IP address of [www.nku.edu](http://www.nku.edu)?
* Use whois to find the IP address range for the IP returned. What is the IP range in CIDR notation?

$ dig @8.8.8.8 [www.nku.edu](http://www.nku.edu/) +nocomments +nostats

192.122.237.48 . This is an internal IP address. The ip range in CIDR notation is 192.122.237.0/24

3.4: When the name [www.nku.edu](http://www.nku.edu) is resolved internally (devices on NKU’s network) and externally (devices not on NKU’s network), different servers will be used. The internal servers will be listed in the /etc/resolv.conf file configured in the Setup Lab or in the outputs of the above dig commands.

* Provide those IPs and the IP found in the previous step below.
  + *Remember that internal and external IP addresses refer to private and public addresses.*

|  |  |
| --- | --- |
| Internal DNS server(s) | **192.122.237.48** |
| External DNS server(s) | **172.28.102.11** |

## 4: DNS Reconnaissance

You can obtain the list of all name to IP address mappings for a domain by performing a DNS zone transfer. However, most DNS servers do not permit zone transfers as that information is highly useful to threat planning when trying to attack a network. To work around this limitation, DNS reconnaissance tools have been developed to find some of the names in a domain.

4.1: First, we'll use dnsrecon to perform reverse DNS lookups of all of **NKU's public IP** addresses using the range of IP’s found in the previous question. In the commands below, replace PUBLIC\_ip/EXTERNAL\_DNS\_server with the IP found as the External DNS server IP and replace FIRST\_IP with the first IP address in NKU's public IP address range, and replace LAST\_IP with the last IP address in that range.

$ whois PUBLIC\_ip/EXTERNAL\_DNS\_server

$ dnsrecon -w -r FIRST\_IP-LAST\_IP

* List or screenshot the DNS names found in the box below

Text

Description automatically generated

4.2: Reverse DNS lookups will not find all of the CNAME (common name) aliases used for virtual web hosting, so in this step we will use Dmitry (Deep magic Information Gathering Tool) to find more hosts. Additional information about Dmitry can be found at <https://tools.kali.org/information-gathering/dmitry>

$ dmitry –s nku.edu | less

* What hosts were found?

Inside.nku.edu, informatics, map, directory, campusrec, chaselaw, onlinedegrees, jobs, and canvas, all ending with .nku.edu

Text

Description automatically generated

4.3: Were any of the names found in the above question not found with dnsrecon? If so, how many more were found?

**From what ive seen everything found in the dnsrecon was found in the last question. The dnsrecon searched for all ip address of the public.**