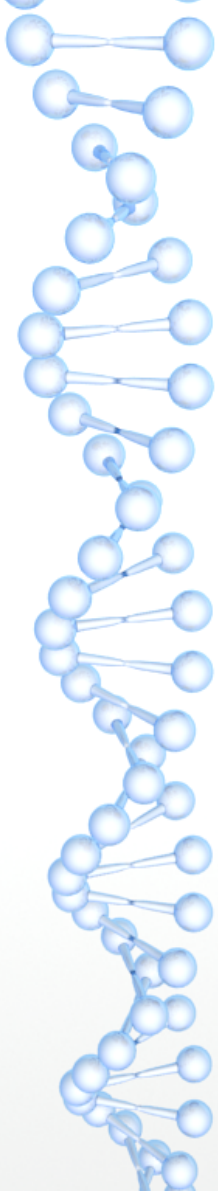
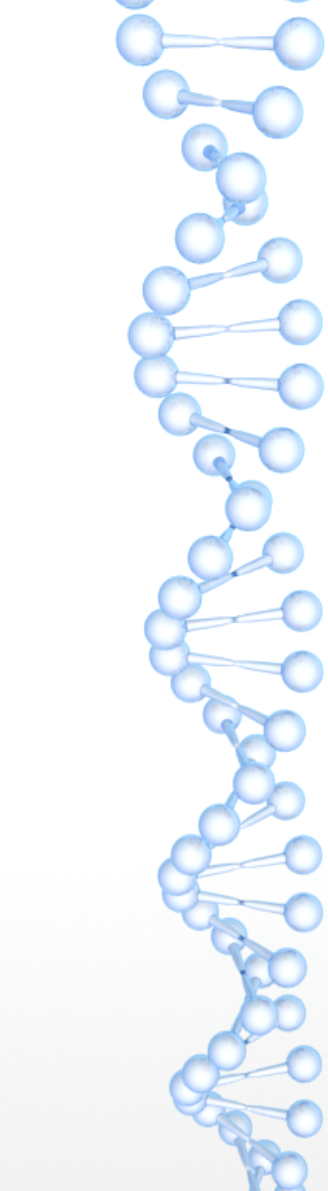


Penetration Testing
Information Gathering

TzNOG6
Dar-Es-Salaam



Penetration Testing
Information Gathering

Prior to an attack, the penetration tester should know as much as possible about the target environment and the characteristics of the system.

The more targeted information the penetration tester finds, the better the chances of identifying the easiest and fastest way to succeed.

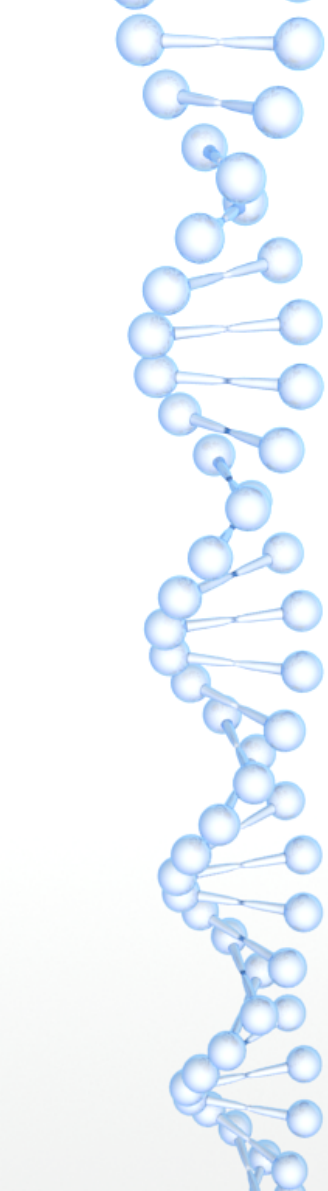
Black-box testing requires more reconnaissance than white-box testing because testers do not get too much data.

Penetration Testing
Information Gathering

- Scouting services may include Internet footprints for investigating targets, monitoring resources, monitoring personnel, processes, etc., scanning network information (such as IP addresses and system types), and social engineering public services such as help desks.

Penetration Testing
Information Gathering

- Reconnaissance is the first step in penetration testing, whether the penetration tester is known to confirm the target system, or to find known intelligence.
- When reconnaissance, the target environment must be defined according to the work area. .



Penetration Testing
Information Gathering

- Once the target is identified, a survey is performed to gather information about the target, such as which ports are used for communication, where the target is hosted, what services it provides to the customer, and so on.
- This data can be used to develop a plan to see what the best way to get the desired results

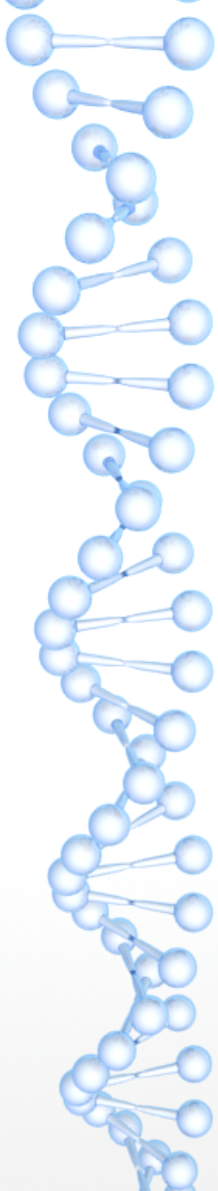
Penetration Testing
Information Gathering

- The results of the reconnaissance process should include a list of all target assets, what applications are associated with the asset, services to be used, and possible asset owners.
- Kali Linux provides a category labeled “Information Gathering”, which is a reconnaissance resource.
- Tools include tools for investigating networks, data centers, wireless networks, and host systems.

Penetration Testing
Information Gathering

- The bellow is a checklist of reconnaissance goals: Acknowledging the goals Defining the use of applications and services Acknowledging the type of system, confirming the available ports, confirming the running services, social engineering informat7ion, document discovery.
- https://www.tcra.go.tz/images/documents/policies/TheCyberCrimeAct2015.pdf
- Article 4,5,6,7,8,9,**10**,11,12
- Article 39-46 – ISP
- Law enforcement officers – all

Penetration Testing
Information Gathering



We will look commands/tools like **nslookup, host, dig & whois**

Always Use command **Man** for more usage details

. Interactive mode - #nslookup

Option
-A
-AAAA
-CNAME
-HINFO
-MB
-MG
-MR
-MX
-NS
-PTR
-TXT

Penetration Testing
Information Gathering

- **HOST**

host is a simple utility for performing DNS lookups. It is normally used to convert names to IP addresses and vice versa. When no arguments or options are given, host prints a short summary of its command line arguments and options.

- **Usage (man host)**

host: illegal option — h
Usage: host [-aCdlriTwv] [-c class] [-N ndots] [-t type] [-W time]
[-R number] [-m flag] hostname [server]
-a is equivalent to -v -t ANY
-c specifies query class for non-IN data
-C compares SOA records on authoritative nameservers
-d is equivalent to -v
-l lists all hosts in a domain, using AXFR
-i IP6.INT reverse lookups
-N changes the number of dots allowed before root lookup is done
-r disables recursive processing
-R specifies number of retries for UDP packets
-s a SERVFAIL response should stop query
-t specifies the query type
-T enables TCP/IP mode
-v enables verbose output
-w specifies to wait forever for a reply
-W specifies how long to wait for a reply
-4 use IPv4 query transport only
-6 use IPv6 query transport only
-m set memory debugging flag (trace|record|usage)
-V print version number and exit

#host -t A google.com

Penetration Testing
Information Gathering

- **DIG**

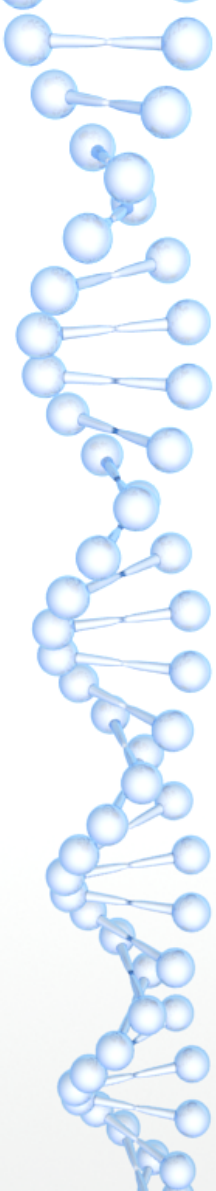
dig (which stands for domain information groper) is a flexible tool for interrogating DNS name servers. It performs DNS lookups and displays the answers that are returned from the name server(s) that were queried.

Most DNS administrators use dig to troubleshoot DNS problems because of its flexibility, ease of use and clarity of output. Other lookup tools tend to have less functionality than dig.

- **Usage (man dig)**

```
Usage:  dig [@global-server] [domain] [q-type] [q-class] {q-opt}
            {global-d-opt} host [@local-server] {local-d-opt}
            [ host [@local-server] {local-d-opt} [...]]
Where:  domain    is in the Domain Name System
        q-class  is one of (in,hs,ch,...) [default: in]
        q-type   is one of (a,any,mx,ns,soa,hinfo,axfr,txt,...) [default:a]
                 (Use ixfr=version for type ixfr)
        q-opt    is one of:
                 -4                  (use IPv4 query transport only)
                 -6                  (use IPv6 query transport only)
                 -b address[#port]   (bind to source address/port)
```

Penetration Testing
Information Gathering



DIY and observe

```
#dig google.com mx
#dig your domain mx

#dig google.com ns
#dig your domain ns

#dig google.com a +tcp
#dig your domain a +tcp
```

Penetration Testing
Information Gathering

- **WHOIS**

WHOIS is an Internet utility that shows the user additional information about a domain, the registrar of the domain, and the IP address.

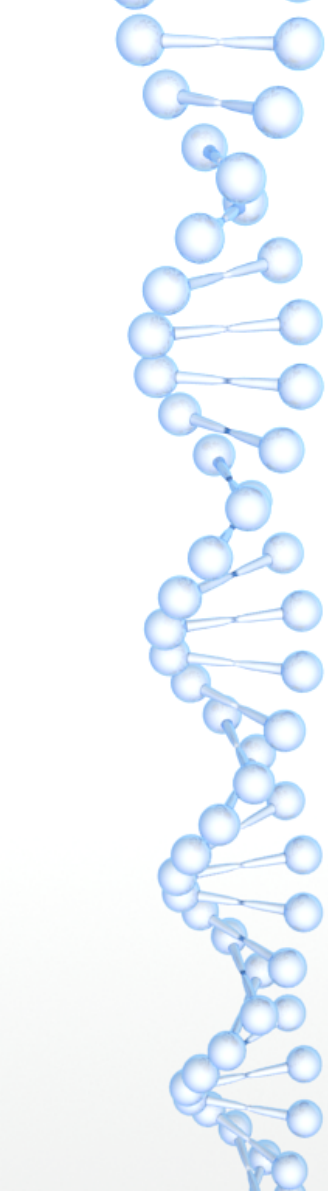
- **Usage (man whois)**

```
whois: option requires an argument -- 'h'
Usage: whois [OPTION]... OBJECT...

-h HOST, --host HOST   connect to server HOST
-p PORT, --port PORT   connect to PORT
-H                     hide legal disclaimers
      --verbose        explain what is being done
      --help           display this help and exit
      --version        output version information and exit
```

```
#whois google.com

#whois (your domain name)
```



End