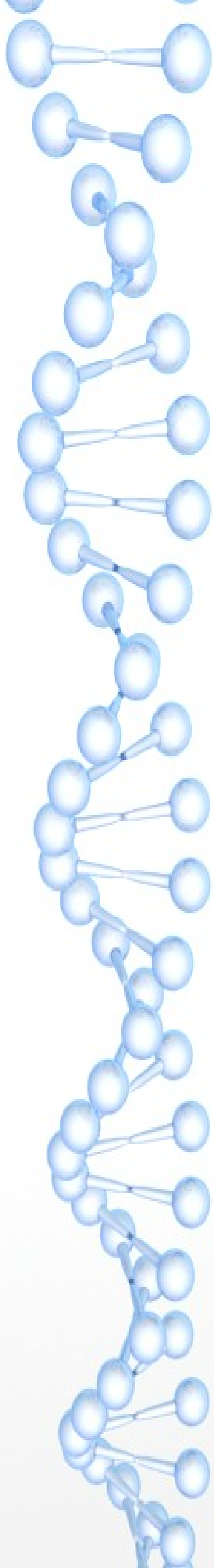

Foot-printing and Reconnaissance

“Drowning in a sea of information and
Starving for knowledge.”
~Rutherford D. Rogers

CEH | iLabAfrica | Strahtmore Uni.

What is Footprinting?

Determining profile of potential targets

Create a complete profile of an organization's security posture using a set of tools and techniques.

The profile usually includes detailed information about IP addresses and blocks, range of domain names, remote access, intranet structure, systems connected to the Internet …etc.

Steps involved

Usually, the process involves six steps:

- Determine scope of activities.
- Get proper authorization.
- Collect publicly available information
- WHOIS and DNS enumeration
- DNS Interrogation
- Network Reconnaissance

Publicly Available Information

Company websites and pages.

Physical location.

Related organizations.

Privacy, security policies adopted.

Disgruntled employees.

Google Information

- Google spider websites, exposing sensitive information on that web site due to various web server misconfigurations
- (such as directory indexing).
- basic usage
- Check information here: http://www.google.com/help/basics.html
- http://www.google.com/help/operators.html

Searching within a Domain

- The site: operator restricts the results to websites in a given domain:

  site:www.hackme.com

  NB: You can include or combine more than one operators

Filetype operator

- The filetype: operator (for some reason not included help/ops page)

  filetype:pdf site:revenue.go.ke

  This search will show us all the publicly exposed PDF files on the selected site.

  Other juicy files to search for:

  mysql dump filetype:sql

- ***"Powered by phpBB" inurl:"index.php?s" OR inurl:"index.php?style"***
-

Passive Reconnaissance - WHOIS Lookups

- Determine TLD for the domain, and which WHOIS server contains the information we're after.
- WHOIS information is based upon a tree hierarchy.
- ICANN (IANA) is the authoritative registry for all of the TLDs.

- Middle East WHOIS lookup (registrar): RIPE NCC, http://www.ripe.net/lir-services/member-support/info/list-of-members/mideast

Online tools

- Central Ops, http://centralops.net/
- NetCraft, http://netcraft.com/
- Domain Tools, http://www.domaintools.com/
- DNS Stuff, http://www.dnsstuff.com
- MX Toolbox, http://mxtoolbox.com
- RIPE, http://www.ripe.net/data-tools/db
- WHOIS, http://www.whois.com/whois/
- WHOIS, http://www.whois.sc/
- What Is My IP, http://www.whatismyip.com/
- InterNIC, http://www.internic.net/

Active Footprinting

- Involves port scanning identified hosts and checking if they are alive.
- Determine if there is a Firewall, loadbalancer and other network controls.

DNS Discovery

- Performed by looking at the WHOIS records for the domain's authoritative nameserver.

- Variations of the main domain name should be checked, and the website should be checked for references to other domains which could be under the target's control.

Banner Grabbing

- An enumeration technique used to glean information about computer systems on a network and the services running its open ports.
- Banner grabbing is used to identify network the version of applications and operating system that the target host are running.

- Usually performed on: HTTP, FTP, and SMTP
- Tools commonly used: Telnet, Nmap, and Netcat

Question(s)?

More Demo