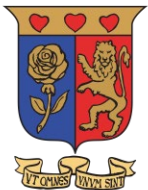


Topic: Footprinting and reconnaissance

BY: DAVID OMASETE



Strathmore
UNIVERSITY





Hacking Steps

- ☐ Reconnaissance
- ☐ Scanning
- ☐ Gaining Access
- ☐ Maintaining Access
- ☐ Clearing Tracks

What is Footprinting?

- Footprinting is the first step in the evaluation of the security posture of the target organization's IT infrastructure
- is the process of gathering all available information about an organization.



Types of Footprinting

- Passive Footprinting
- Active Footprinting



Passive Footprinting

- Passive footprinting is a method in which the attacker never makes contact with the target systems.
- HOW IS THIS DONE?

Active footprinting

- Active footprinting involves the use of tools and techniques that can aid you in gathering more information about your target.
- Target is more likely to notice your efforts

Active Footprinting



Strathmore
UNIVERSITY

How is this done?

Information Obtained in Footprinting



Strathmore
UNIVERSITY

- Network Information
- System Information
- Organization Information

Network Information



- You can gather network information by performing Whois database analysis, trace routing, and so on

Network Information



Strathmore
UNIVERSITY

- Domain and sub-domains
- IP addresses of the reachable systems
- Whois record
- DNS records, and related information

Ping.eu




Strathmore
UNIVERSITY

ping.eu

Online Ping, Traceroute, DNS lookup, WHOIS, Port check, Reverse lookup, Proxy checker, Bandwidth meter, Network calculator, Network mask calculator, Country by IP, Unit converter

Your IP is **105.160.60.37**

Online service DNS lookup

 **DNS lookup** – Look up DNS record

IP address or host name:

Go

Using domain server:

Name:

127.0.0.1

Address:

127.0.0.1#53

Aliases:

strathmore.edu has address **198.57.179.99**

strathmore.edu mail is handled by 15 aspmx4.googlemail.com.

strathmore.edu mail is handled by 0 aspmx.l.google.com.

strathmore.edu mail is handled by 5 alt1.aspmx.l.google.com.

strathmore.edu mail is handled by 15 aspmx5.googlemail.com.

strathmore.edu mail is handled by 10 aspmx2.googlemail.com.

strathmore.edu mail is handled by 10 aspmx3.googlemail.com.

strathmore.edu mail is handled by 5 alt2.aspmx.l.google.com.

Other functions:

[Ping](#) | [Traceroute](#) | [DNS lookup](#) | [WHOIS](#) | [Port check](#) | [Reverse lookup](#) | [Proxy checker](#) | [Bandwidth meter](#) |

[Network calculator](#) | [Network mask calculator](#) | [Country by IP](#) | [Unit converter](#)

System Information

- You can gather system information by performing network footprinting, DNS footprinting, website footprinting, email footprinting, and so on.
- Web Server OS- eg Apache Web server
- Location of web servers

Organization Information



Strathmore
UNIVERSITY

- You can query the target's domain name against the Whois database and obtain valuable information.

Whois



Strathmore
UNIVERSITY

 **WHOIS**[DOMAINS](#)[WEBSITE](#)[CLOUD](#)[HOSTING](#)[SERVERS](#)[EMAIL](#)[SECURITY](#)[WHOIS](#)[SUPPORT](#)[LOGIN](#)

safaricom.co.ke

Updated 1 second ago



Domain Information

Domain:	safaricom.co.ke
Registrar:	Safaricom Limited
Registered On:	2003-02-12
Expires On:	2022-12-31
Updated On:	2019-03-15
Status:	ok
Name Servers:	ns1.safaricombusiness.co.ke ns2.safaricombusiness.co.ke ns3.safaricombusiness.co.ke ns4.safaricombusiness.co.ke



Registrant Contact

Interested in similar domains?

thesafaricom.com

[Buy Now](#)

insafaricom.com

[Buy Now](#)

safaricomgroup.net

[Buy Now](#)

safaricomonline.com

[Buy Now](#)

4safaricom.com

[Buy Now](#)

safaricomonline.net

[Buy Now](#)

thesafaricom.net

[Buy Now](#)

Objectives of Footprinting



Strathmore
UNIVERSITY

- Know security posture
- Produce focus area
- Identify vulnerabilities
- Draw network maps



Footprinting Threats

- Social Engineering
- Systems and Network Attacks
- Information leakage
- Privacy loss
- Corporate espionage

Footprinting Methodology



Strathmore
UNIVERSITY

- Through search engines
- Web services
- Social networking sites
- Website Footprinting
- Social Engineering



Search Engines

- Search Engines are the main sources to locate key information
- Examples of search engines are Google, Bing, Yahoo
- Like Google; search for anything

Advanced Google Hacking Technique



Strathmore
UNIVERSITY

- Google Hacking Database
- Google Hacking Techniques

Goohle Hacking Techniques

- allinurl
- inurl
- allintitle
- inanchor
- intitle



Strathmore
UNIVERSITY

Google Hacking Database



Strathmore
UNIVERSITY

- Repository containing valuable information
- For example: Passwords, Usernames, online shopping information etc

What can a hacker do with Google hacking?



Strathmore
UNIVERSITY

- An attacker can create complex queries that filter large amounts of information.

Footprinting through Web-Services



Strathmore
UNIVERSITY

- Finding Company's Top-level Domains(TLDs) .com, .net, .edu and Sub Domains
- Sub domains can be found using Netcraft or trial and error.

Website Footprinting Using Web Spiders



Strathmore
UNIVERSITY

- Web spider (also known as web crawler or web robot) applications that crawl through a website, reporting information they find.
- Search engines rely on web spidering to provide the info they need to respond to web searches



Website Footprinting

- Software used and its version
- Operating system used
- Sub-directories and parameters
- Scripting platform

Mirroring Entire Website

- Website mirroring is the process of creating an exact replica or clone of the original website. Users can duplicate the websites by using mirroring tools such as HTTrack Web Site Copier, and NCollector Studio

Benefits of Web mirroring



Strathmore
UNIVERSITY

- It is helpful for offline site browsing
- It supports an attacker in spending more time viewing and analyzing the website for vulnerabilities and loop holes
- It assists in finding directory structure and other valuable information from the mirrored copy without multiple requests to the web server

Footprinting Through Networking Sites

- Maintain profile -Contact info, location and related information.
- Connect to friends, chatting -Friends list, friend's info and related information.
- Share photos and videos-Identity of a family members, interests and related information.
- Play games, join groups -Interests



Email Footprinting

- Tracking Email Communications
- Details found-Recipient's system IP address:
 - Proxy detection
 - Links
 - Email received and Read:
 - Operating system and Browser information

What can be found in an email header



Strathmore
UNIVERSITY

- Sender's mail server
- Data and time received by the originator's email servers
- Authentication system used by the sender's mail server
- Data and time of message sent
- A unique number assigned by mr.google.com to identify the message
- Sender's full name
- Senders IP address and address from which the message was sent

Sender's full name

Networking Footprinting

- Locate the Network Range-internal structure of the network.
- Traceroute-finding the route of the target host on the network is necessary to test against man-in-the-middle attacks

Footprinting Through Social Engineering

- **Eavesdropping**
- **Shoulder surfing**
- **Dumpster Diving**



Strathmore
UNIVERSITY

Footprinting Countermeasures

- Restrict the employees to access social networking sites from organization's network
- Configure web servers to avoid information leakage
- Educate employees to use pseudonyms on blogs, groups, and forums

Footprinting Countermeasures

- Do not reveal critical information in press releases, annual reports, product catalogues and so on.
- Limit the amount of information that you are publishing on the website/ Internet
- Use footprinting techniques to discover and remove any sensitive information publicly available

Footprinting Countermeasures

- Conduct periodically security awareness training to educate employees
- Develop and enforce security policies such as information security policy, password policy and so on to regulate the information that employees can reveal to third parties
- Set apart internal and external DNS or use split DNS, and restrict zone transfer to authorized servers



Footprinting Penetration

- A footprinting pen test helps in determining an organization's information on the Internet such as network architecture, operating systems, applications, and users.

Benefits of Footprinting Testing

- Prevent information leakage
- Prevent social engineering attempts
- Prevent DNS record retrieval from publically available servers

Footprinting Pen Testing

- Step 1: Get proper authorization from the organization
- Step 2: Define the scope of the assessment- the range of systems to be tested. Also provides the pen tester's limitation
- Step 3: Perform footprinting through search engines



Footprinting Pen Testing

- Step 4: Perform footprinting through web services
- Step 5: Perform footprinting through social networking sites
- Step 6: Perform website footprinting



Footprinting Pen Testing

- Step 7: Perform email footprinting
- Step 8: Gather competitive intelligence
- Step 9: Perform Whois footprinting
- Step 10: Perform Social engineering
- Step 11: Document all the findings



Strathmore
UNIVERSITY

Thank you!

Any Questions?