Footprinting

TOPICS

- Reconnaissance
- What is footprinting?
- Objectives of footprinting
- Footprinting Threats
- Footprinting Methods
- Footprinting Countermeasures

RECALL – PHASES OF HACKING

- Reconnaissance (Gathering target info)
- Scan (Extracting more information)
- Gain Access (Breaking in and get control)
- Maintain Access (Retain system ownership)
- Cover Tracks (Hide evidence)

RECONNAISSANCE

- The preparatory phase where an attacker seeks to gather information about the target before launching an attack
- Scope may include the target's clients, employees, operations, network and systems
- Easier to attack a target if it is known on a broad scale

RECONNAISSANCE TYPES

Passive	Acquire info without interacting directly with the target
	e.g. Search public records or news releases
Active	Involves interacting with the target directly by any means
	e.g. telephone calls to the help desk or tech department

FOOTPRINTING

- Process of gathering resources regarding a target computer / organization
  - Collect network information
  - Determine operating system versions
- Performed before an attack
- Resources may be in the form of
  - IP addresses
  - Email addresses
  - Phone numbers

OBJECTIVES OF FOOTPRINTING

- Main objective is to find the easiest way to break into an organization
- Footprinting helps to :
  - Reduce attack area by limiting the range of loopholes that you can try
  - Build an information database of the target's weaknesses
  - Know the target's security posture in order to create the hacking plan

OBJECTIVES OF FOOTPRINTING

We want to collect info about the…

Network	System	Organization
• Domain name • Network blocks • Phone numbers • IP addresses of hosts	• User and group names • Banners • System names • Passwords	• Employee details • Websites • Background • Press releases

FOOTPRINTING THREATS

FOOTPRINTING METHODS

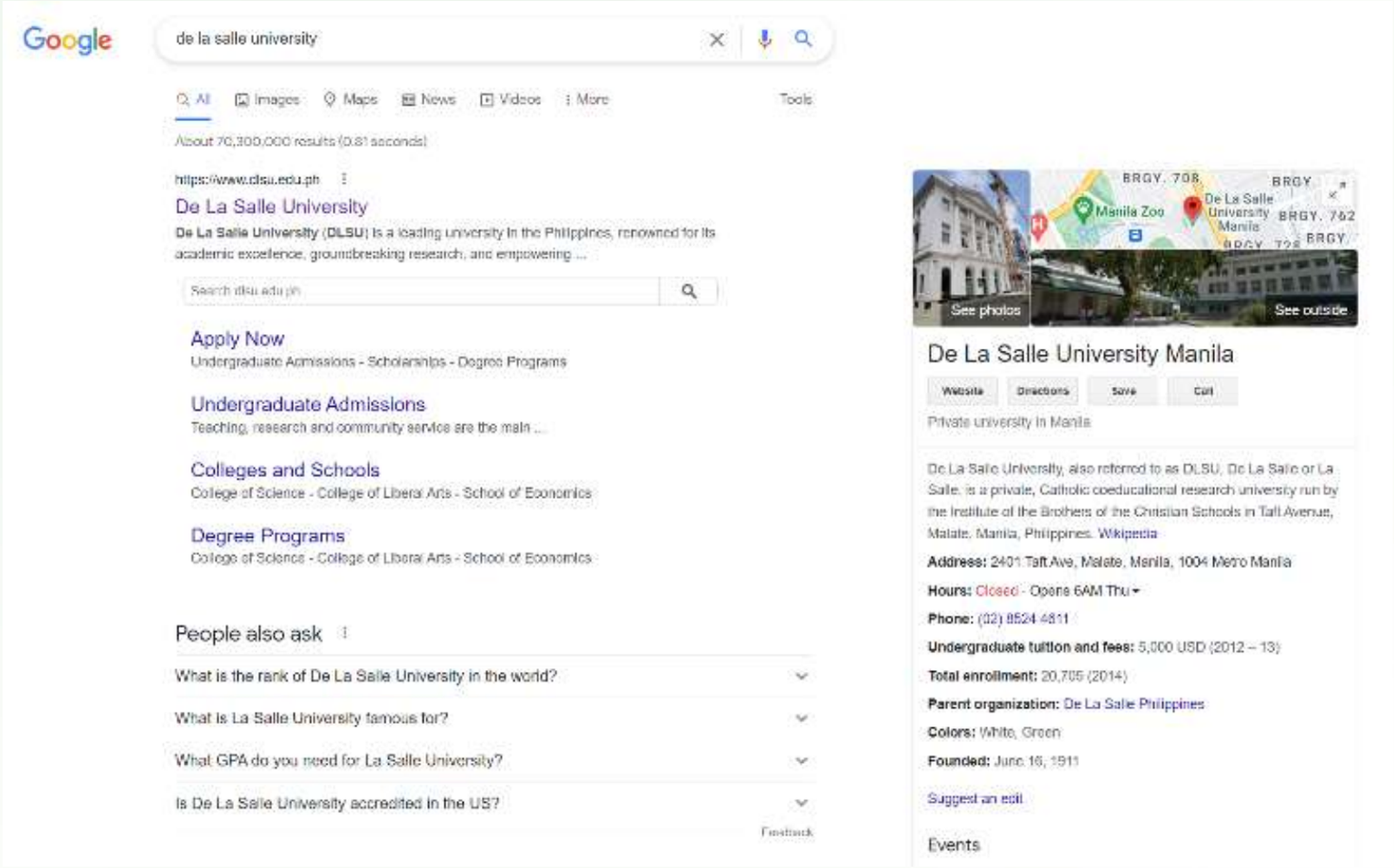
- Internet Footprinting
- Website footprinting
- Whois footprinting
- DNS footprinting
- Network footprinting
- Google hacking

INTERNET FOOTPRINTING

- Easiest way to find information – use what is publicly available
- An important characteristic of this technique: it's legal
- Approaches:
  - Company websites
  - Internet archives
  - Social Networks
  - Search Engines

WEBSITE FOOTPRINTING

Search for a company's website through search engines



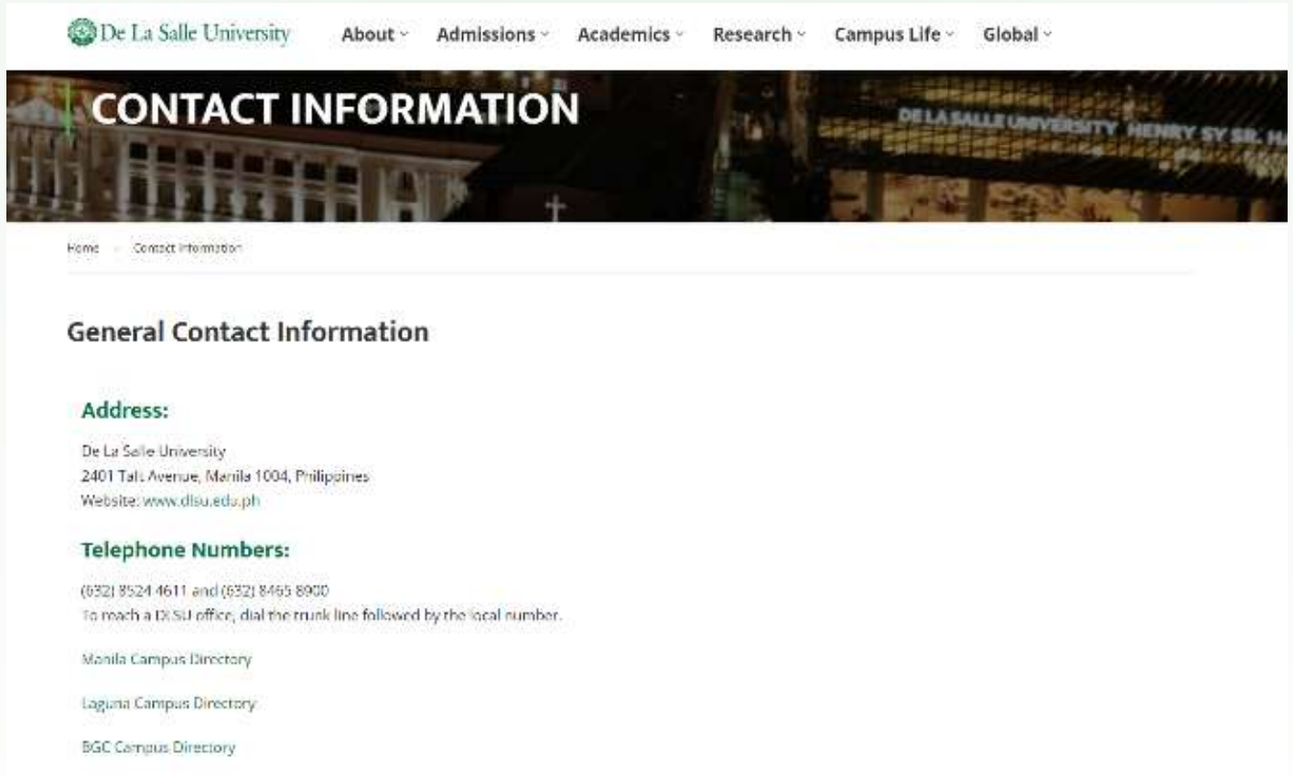
WEBSITE FOOTPRINTING

An organization's website indirectly provides a wealth of information

- Business Units
- Contact numbers
- Physical Address
- Employees
- Ads
- Links to internal sites

WEBSITE FOOTPRINTING

Business units, contact information and addresses help in deciding which relevant areas to target when doing further information gathering



WEBSITE FOOTPRINTING

Employee listings may yield names of people to target within the organization (e.g. for social engineering) as well as possible contact info

Dean	Dr. Rafael A. Cabredo
Associate Dean	Dr. Charibeth K. Cheng
Assistant Dean, External Affairs and Lasallian Mission	Dr. Shirley B. Chu
Assistant Dean, Research and Graduate Studies	Dr. Christine Diane L. Ramos
Director, Consulting and Education Center	Dr. Ma. Rowena R. Caguiat
Head, Technical Support Group	Mr. Gregory G. Cu
Department of Computer Technology	
Chair	Dr. Marnel S. Peradilla
Vice Chair	Ms. Arlyn Verina L. Ong-Tiu
Coordinator, Graduate Studies (MINFSEC)	Ms. Arlyn Verina L. Ong-Tiu
Coordinator, Instructional Computer Technology Laboratory	Mr. Clement Y. Ong
Department of Information Technology	
Chair	Dr. Michelle Renee D. Ching
Vice Chair	Ms. Lissa Andrea K. Magpantay
Coordinator, Graduate Studies (DIT)	Dr. Michelle Renee D. Ching
Coordinator, Graduate Studies (MSIT/MIT)	Ms. Lissa Andrea K. Magpantay
Department of Software Technology	
Chair	Dr. Briane Paul V. Samson
Vice Chair	Mr. Neil Patrick A. Del Gallego
Coordinator, BSCS Thesis and BSIET Capstone	Mr. Edward P. Ilghe
Coordinator, Graduate Studies	Dr. Ethel C. Ong
Laguna Campus Coordinator (BSCS)	Ms. Ma. Christine A. Gendrano (1st Term) Dr. Arnulfo P. Azcarraga (2nd & 3rd Terms)
Laguna Campus Program Director	Mr. Neil Patrick A. Del Gallego
Laguna Campus, Program Coordinator (BSIET)	Mr. Ryan Samuel M. Dimaunahan

WEBSITE FOOTPRINTING

Job ads, especially those for IT positions, may give clues regarding the organization's infrastructure

Qualifications:

1. Bachelor's Degree in Computer Science, Software Engineering, Information Systems, or a related field; preferably with an MBA or a Master's Degree in Information Technology
2. At least 15 years of IT work experience; 5 years of which should be managing overall IT operations in a senior leadership capacity
3. With an understanding of cloud computing, business intelligence tools & technologies, cyber security
4. With a working knowledge of project management principles

Job Description/Summary

1. Managing IT staff and developing department goals
2. Managing the University's Application Needs needs on an outsourced basis
3. Adopting IT best practices which include metrics-driven delivery of IT services
4. Developing and overseeing the IT budget
5. Planning, deploying and maintaining IT systems, policies, and processes
6. Ensuring IT strategies and processes support University-wide goals
7. Overseeing relationships with vendors, contractors, and service providers
8. Staying updated on IT trends and emerging technologies

How to Apply: The application letter should be addressed to:

Joanne V. Mar
Executive Director
Community, Culture and Human Resources Services Office

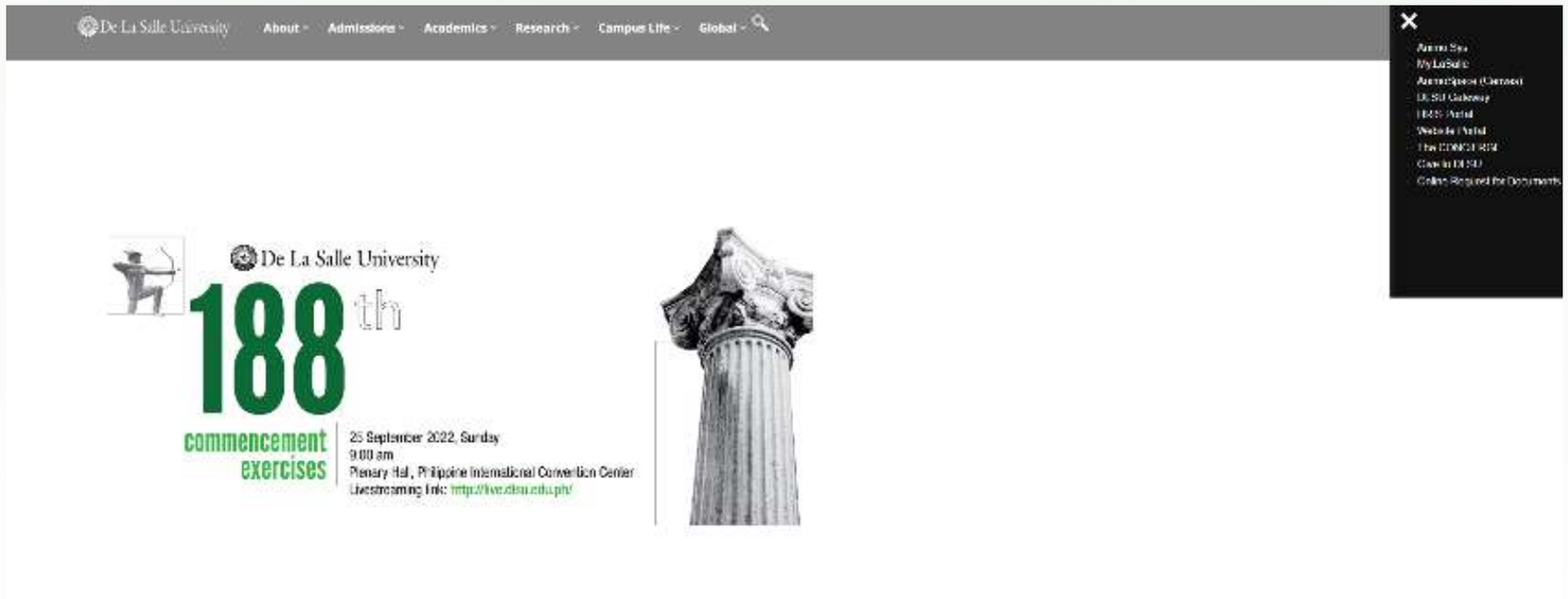
Send the application letter and required documents listed below to opmrecruitment@dlsu.edu.ph, citing the reference number of the vacancy in the subject of the email.

- Application Letter
- Detailed Curriculum Vitae including a recent passport-sized photograph

Apply for job

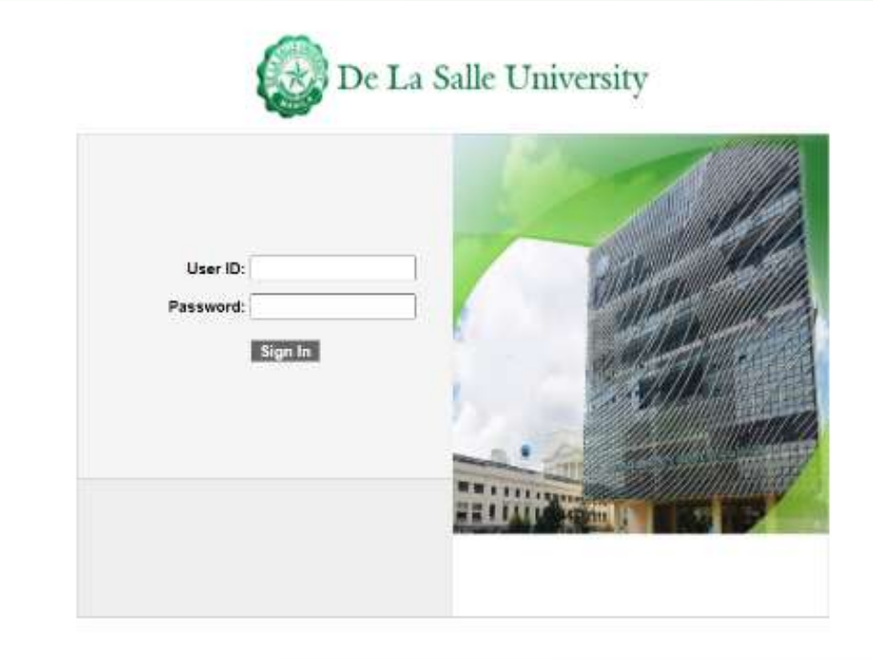
WEBSITE FOOTPRINTING

Websites may lead to links to internal sites or more protected areas of an organization's network



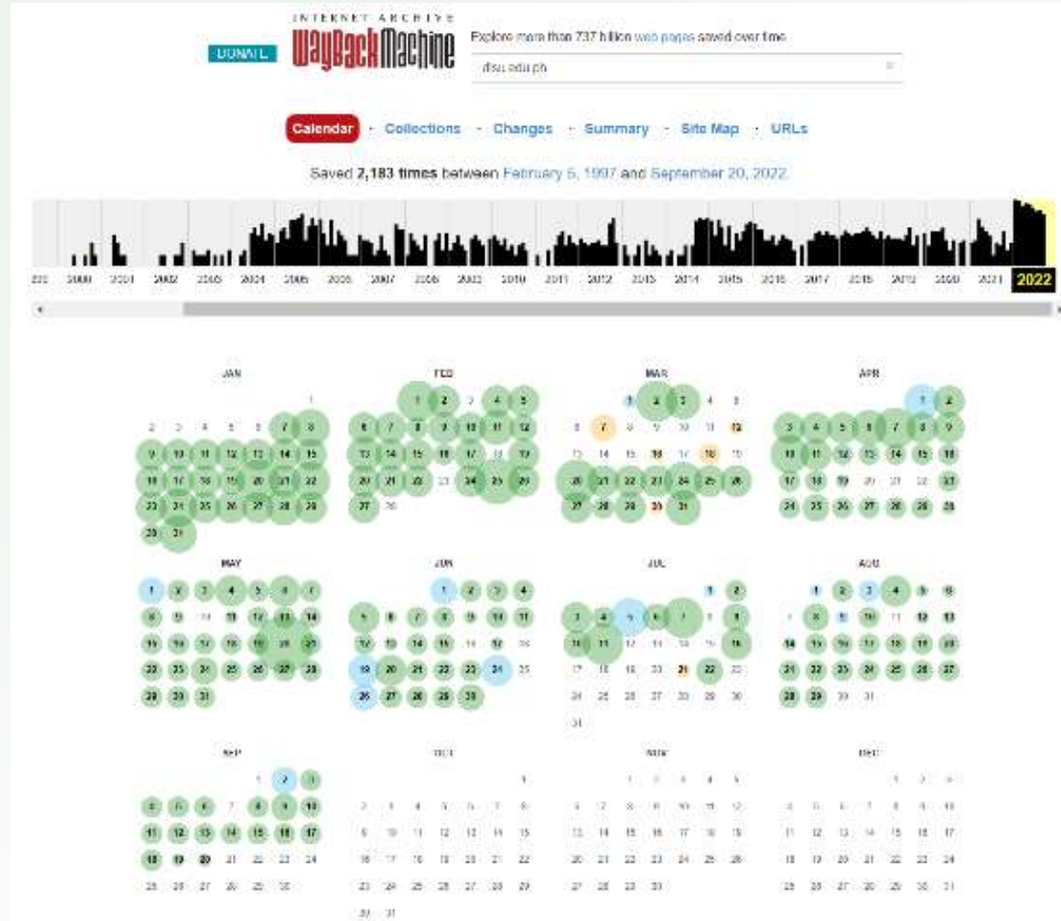
WEBSITE FOOTPRINTING

Websites may lead to links to internal sites or more protected areas of an organization's network



INTERNET ARCHIVES

Contain information on retired webpages – some of which could have been taken down due to security reasons
Ex: The Wayback Machine - www.archive.org



SOCIAL NETWORKING

Searching social networking sites for the organization's people can help gather information about their habits and contacts for possible social engineering

WHOIS FOOTPRINTING

- WHOIS databases are maintained by Internet RIRs and contain personal info of domain owners
- WHOIS Query returns
  - Domain name details
  - Contact details of domain owners
  - Domain name servers
  - Network range

WHOIS FOOTPRINTING

- Sample Sites
  - http://whois.domaintools.com
  - *https://www.**whois**.net/*
  - *https://**who.is**/*
  - https://viewdns.info/

DNS FOOTPRINTING

- DNS Records provide important information about location and type of servers

- Recall: DNS record types
  - A record – a host IP address
  - MX record – domain mail server
  - CNAME record – canonical (true) name of a host in case it has aliases
  - NS record – name server for a domain

DNS FOOTPRINTING

- Nslookup
  - Built in utility in Windows and Linux that allows querying of DNS entries
  - Use combination of WHOIS results and reverse DNS to look for clues as to which systems in an organization are interesting
  - By default shows A records. Use the command

    set type=<record type>

    to query the appropriate record type

DNS FOOTPRINTING

- DNS Zone Transfer
  - DNS zone transfers using the AXFR protocol are the simplest mechanism to replicate DNS records across DNS servers.

dig axfr zonetransfer.me @nsztm1.digi.ninja

NETWORK FOOTPRINTING

- Involves attempting to map out the network topology, locations of routers and firewalls of the target organization
- Having a visual map of the network gives a better idea how to reach the target systems and what safeguards may lie in between
- Start off from the network range taken from WHOIS tools

NETWORK FOOTPRINTING

- Tracert / traceroute
  - Tools works using the ICMP and manipulating IP header TTL values to force time exceeded messages to return to the tracing host
  - Allows discovery of routers / firewalls along the path to a target

NETWORK FOOTPRINTING

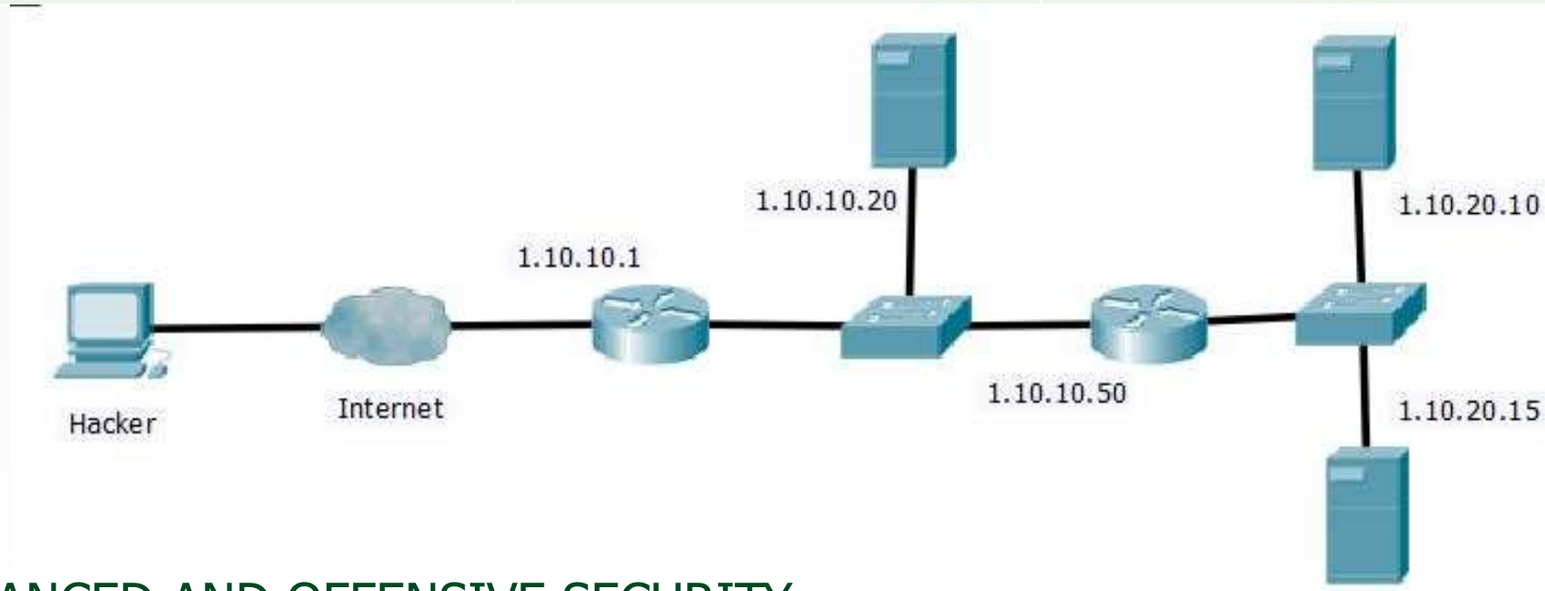
- Traceroute Analysis
  - Hackers do traceroutes to various hosts and put info together to form the network map
  - Ex:

Trace 1	Trace 2	Trace 3
1-10 Internet routers…	1-10 Internet routers…	1-10 Internet routers…
11 1.10.10.1	11 1.10.10.1	11 1.10.10.1
12 1.10.10.20 (done)	12 1.10.10.50	12 1.10.10.50
	13 1.10.20.10 (done)	13 1.10.20.15 (done)

NETWORK FOOTPRINTING

- Traceroute Analysis

Trace 1	Trace 2	Trace 3
1-10 Internet routers…	1-10 Internet routers…	1-10 Internet routers…
11 1.10.10.1	11 1.10.10.1	11 1.10.10.1
12 1.10.10.20 (done)	12 1.10.10.50	12 1.10.10.50
	13 1.10.20.10 (done)	13 1.10.20.15 (done)



GOOGLE HACKING

- Refers to the art of creating complex search queries
- Often leads to finding websites that are vulnerable to exploits
- Uses Google search operators to look for specific strings in results

GOOGLE HACKING: WHAT YOU CAN UNCOVER

With the right Google search strings, you can find:

- Advisories and server vulnerabilities
- Pages containing network vulnerability data
- Pages containing logon portals
- Error messages with sensitive info
- File containing passwords
- Sensitive directories

GOOGLE HACKING: SEARCH OPERATORS

Operator	What it does
“string”	Looks for an exact string match
intitle:string	Returns only webpages with a specific string in their title
inurl:string	Returns only webpages with a specific string in their URL
site:string	Returns only webpages if they belong to a specified domain
filetype:extension	Looks for matches with a specified file extension
intext:string	Looks for matches with the specified string in contents

GOOGLE HACKING: EXAMPLES

- May yield a lot of sensitive information
  - intitle:“Welcome to IIS 4.0”
  - “VNC Desktop” inurl:5800
  - filetype:pwd service
  - filetype:bak inurl:”htaccess|passwd|shadow|htusers”
  - filetype:properties inurl:db intext:password
  - “not for distribution” confidential site:edu
  - “This file was generated by Nessus”

FOOTPRINTING COUNTERMEASURES

- Review publicly available items and remove what is sensitive/not necessary
- Use anonimity features offered by domain name registrars or post false contact info
- Segregate public and private DNS info
- Configure routers and firewalls to limit responses to footprinting requests
- Use intrusion detection systems that can detect footprinting patterns