**Footprinting and Reconnaissance Experiment: Using Google for Company Information**

**Objective:**  
To gather publicly available information about a company using Google search techniques.

**Steps to Perform the Experiment:**

**Step 1: Define Your Target Company**

* Choose a company you want to investigate.
* Make sure your search is legal and ethical, following all privacy guidelines.

**Step 2: Perform Basic Google Searches**

* Start with a general search:
* Company Name
* Example:
* Microsoft

**Step 3: Use Advanced Google Search Operators**

1. **Find the company's official website:**
2. site:companywebsite.com

Example:

site:microsoft.com

* + This filters results to only show pages from the official website.

1. **Find specific file types (e.g., PDFs, Docs, XLSX):**
2. site:companywebsite.com filetype:pdf

Example:

site:microsoft.com filetype:pdf

1. **Find sensitive directories or subdomains:**
2. site:companywebsite.com inurl:admin
3. site:companywebsite.com inurl:login
4. **Discover employee names and emails:**
5. "@company.com"

Example:

"@microsoft.com"

1. **Check for cached pages:**
2. cache:companywebsite.com
   * This shows an older version of the website.
3. **Search for related companies or competitors:**
4. related:companywebsite.com

**Step 4: Gather Social Media Information**

* Search for the company’s social media presence:
* Company Name site:linkedin.com
* Company Name site:twitter.com
* Company Name site:facebook.com
* Check employee profiles, posts, and company updates.

**Step 5: Use Google Dorking for Deeper Insights**

* Example queries:
  + Find internal documents:
  + site:companywebsite.com confidential
  + Find exposed directories:
  + intitle:"index of" "parent directory" site:companywebsite.com
  + Find possible vulnerabilities:
  + site:companywebsite.com "Error 404" OR "SQL syntax error"

**Step 6: Summarize Findings**

* Document the collected information:
  + Company address, contact details
  + Publicly available documents (PDFs, reports, whitepapers)
  + Employee names and job roles
  + Possible security vulnerabilities (if any)

**Precautions & Ethical Considerations**

* Only use publicly available data.
* Do not attempt to bypass security measures.
* Do not engage in illegal activities (hacking, phishing, etc.).
* Respect privacy and data protection laws.

Would you like me to refine the steps further or include specific case studies? 🚀