What is Passive Footprinting?

Passive Footprinting is **gathering information about the target without direct interaction**

Examples of Passive Footprinting

- Finding information through search engines
- Collecting location information on the target through web services
- Performing people search using social networking sites and people search services
- Gathering financial information about the target through financial services
- Gathering information using groups, forums, blogs, and NNTP Usenet newsgroups
- Collecting information through social engineering on social networking sites
- Extracting information about the target using Internet archives
- Gathering information using business profile sites
- Monitoring website traffic of the target
- Tracking the online reputation of the target

Footprinting is **the first step in information gathering** in which an **investigator collects information about a subject. This can be done passively or actively.**

Investigators can also **engage directly with a subject**, depending on the **needs and goals of an investigation.**

Trough **footprinting and investigator can gather information about a subject without directly accessing or observing the subject.**

There is no single methodology for footprinting, as information can be traced in a number of ways--but, footprinting should be carried out in an organized manner in order to gather all the crucial information about a subject.

What is Active Footprinting?

Active Footprinting is **gathering information about the subject without direct interaction.**

Examples of Active Footprinting

- Extracting website links and gathering wordlists from the subjects website
- Extracting metadata of published documents and files
- Gathering information through email tracking
- Harvesting email lists Performing Whois lookup
- Extracting DNS information
- Performing traceroute analysis
- Performing social engineering

Information Obtained Through Footprinting

- Organization information
- Employee details
- Telephone numbers
- Location
- Background of the organization
- Domain and sub-domains
- IP addresses of the reachable systems
- Whois record
- Domain Name Service (DNS)
- Operating System information
- Location of Web Servers
- Users and Passwords

Using Information Obtained

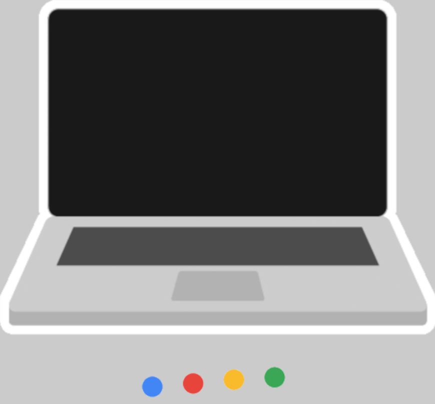
- Employee details (employee names, contact addresses, designations, and work experience)
- Addresses and mobile/telephone numbers Branch and location details
- Partners of the organization Web links to there company-related sites
- Background of the organization
- Web technologies News articles, press releases, and related documents
- Legal documents related the organization
- Patents and trademarks related the organization
- Gain access to organizational information and use such information to identify key personnel
- Launch social engineering tactics to extract sensitive data about the entity.

Search engines are the **main sources of key information about a subject or organization.** They play a **major role in extracting critical details about a subject from the Internet.**

These **results include web pages, videos, images, etc.** and are **ranked and displayed according their relevance.**

Search engines can **extract organization information** such as **technology platforms, employee details, login pages, intranet portals, contact information.**

The information **helps the an investigator in performing and designing social engineering to extract additional information.** This is also used in pre-texting or using a 'ruse'.



TYPES OF SEARCH ENGINES

REGAULAR SEARCH ENGINE = Google, Bing, Yahoo, Etc.

IOC SEARCH ENGINGES = Indicator of Compromise

FTP SEARCH ENGINGES = File Transfer Protocol

Advanced Search Operators

site: This operator restricts search results the specified site or domain.

allinurl: This operator restricts results to only the pages containing all the query terms specified in the URL.

inurl: This operator restricts the results tonly the pages containing the specified word in the URL.

cache: This operator displays Google's cached version of a web page instead of the current version of the web page.

allintitle: This operator restricts results to only the pages containing all the query terms specified in the title.

intitle: This operator restricts results to only the pages containing the specified term in the title.

inanchor: This operator restricts results to only the pages containing the query terms specified in the anchor text on links to the page.

allinanchor: This operator restricts results to only the pages containing all query terms specified in the anchor text on links to the pages.

link: This operator searches websites or pages that contain links the specified website or page.

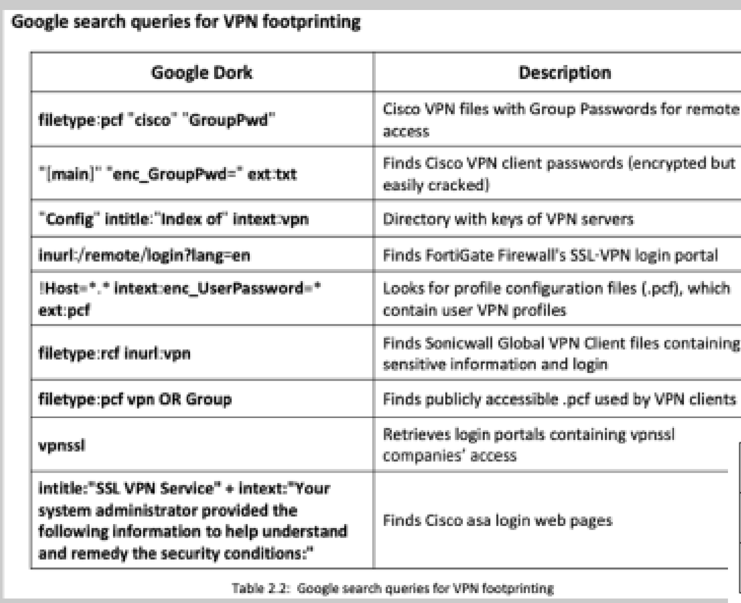
related: This operator displays websites that are similar or related to the URL specified.

info: This operator finds information for the specified web page.

location: This operator finds information for a specific location.

filetype: This operator allows you to search for results based on a file extension.

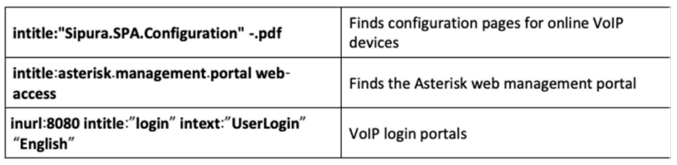
Note: Do not enter any spaces between the operator and the query. Some popular Google advanced search operators Also note that when you combine link: with another advanced operator, Google may not return all the pages that match. Also note, "you cannot combine a link: search with a regular keyword search."



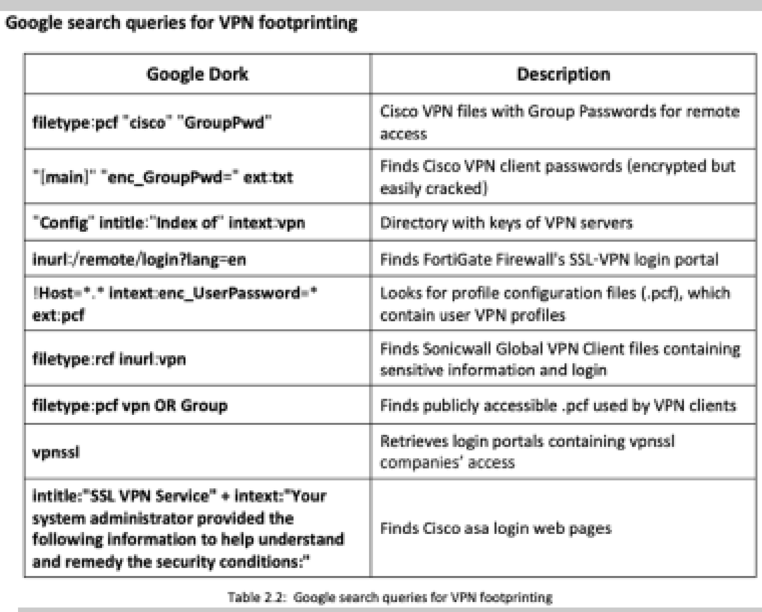
Google search queries for VPN footprinting

Google Dork	Description
filetype:pcf "cisco" "GroupPwd"	Cisco VPN files with Group Passwords for remote access
"[main]" "enc_GroupPwd=" ext:txt	Finds Cisco VPN client passwords (encrypted but easily cracked)
"Config" intitle:"Index of" intext:vpn	Directory with keys of VPN servers
inurl:/remote/login?lang=en	Finds FortiGate Firewall's SSL-VPN login portal
!Host=*.* intext:enc_UserPassword=* ext:pcf	Looks for profile configuration files (.pcf), which contain user VPN profiles
filetype:rcf inurl:vpn	Finds Sonicwall Global VPN Client files containing sensitive information and login
filetype:pcf vpn OR Group	Finds publicly accessible .pcf used by VPN clients
vpnssl	Retrieves login portals containing vpnssl companies' access
intitle:"SSL VPN Service" + intext:"Your system administrator provided the following information to help understand and remedy the security conditions:"	Finds Cisco asa login web pages

Table 2.2: Google search queries for VPN footprinting



intitle:"Sipura.SPA.Configuration" -.pdf	Finds configuration pages for online VoIP devices
intitle:asterisk.management.portal web-access	Finds the Asterisk web management portal
inurl:8080 intitle:"login" intext:"UserLogin" "English"	VoIP login portals



Google search queries for VPN footprinting

Google Dork	Description
filetype:pcf "cisco" "GroupPwd"	Cisco VPN files with Group Passwords for remote access
"[main]" "enc_GroupPwd=" ext:txt	Finds Cisco VPN client passwords (encrypted but easily cracked)
"Config" intitle:"Index of" intext:vpn	Directory with keys of VPN servers
inurl:/remote/login?lang=en	Finds FortiGate Firewall's SSL-VPN login portal
!Host=*.* intext:enc_UserPassword=* ext:pcf	Looks for profile configuration files (.pcf), which contain user VPN profiles
filetype:rcf inurl:vpn	Finds Sonicwall Global VPN Client files containing sensitive information and login
filetype:pcf vpn OR Group	Finds publicly accessible .pcf used by VPN clients
vpnssl	Retrieves login portals containing vpnssl companies' access
intitle:"SSL VPN Service" + intext:"Your system administrator provided the following information to help understand and remedy the security conditions:"	Finds Cisco asa login web pages

Table 2.2: Google search queries for VPN footprinting