INTRO TO RECONNAISSANCE

What is Reconnaissance?

Reconnaissance is the initial phase of a penetration test or security assessment where the hacker gathers as much information as possible about a target system or network.This phase helps the ethical hacker understand the system's architecture, vulnerabilities, and potential points of entry, with the goal of identifying weakness before attempting any exploits.

Types of Reconnaissance:

. Passive Reconnaissance
. Active Reconnaissance

Aspect	Passive Reconnaissance	Active Reconnaissance
Definition	Involves gathering information without direct interaction with the target.	Involves direct interaction with the target system to gather information.
Technique Used	Analyzing public information sources, social media,and using OSINT tools.	Port Scanning,Vulnerability scanning and network probing(using nmap nessus)
Risk of Detection	Lower risk of detection as it does not involve direct interaction with the target	Higher risk of detection due to engagement with the target system.
Information Accuracy	Less detailed information,relying on publicly available data.	More accurate and detailed information about the target

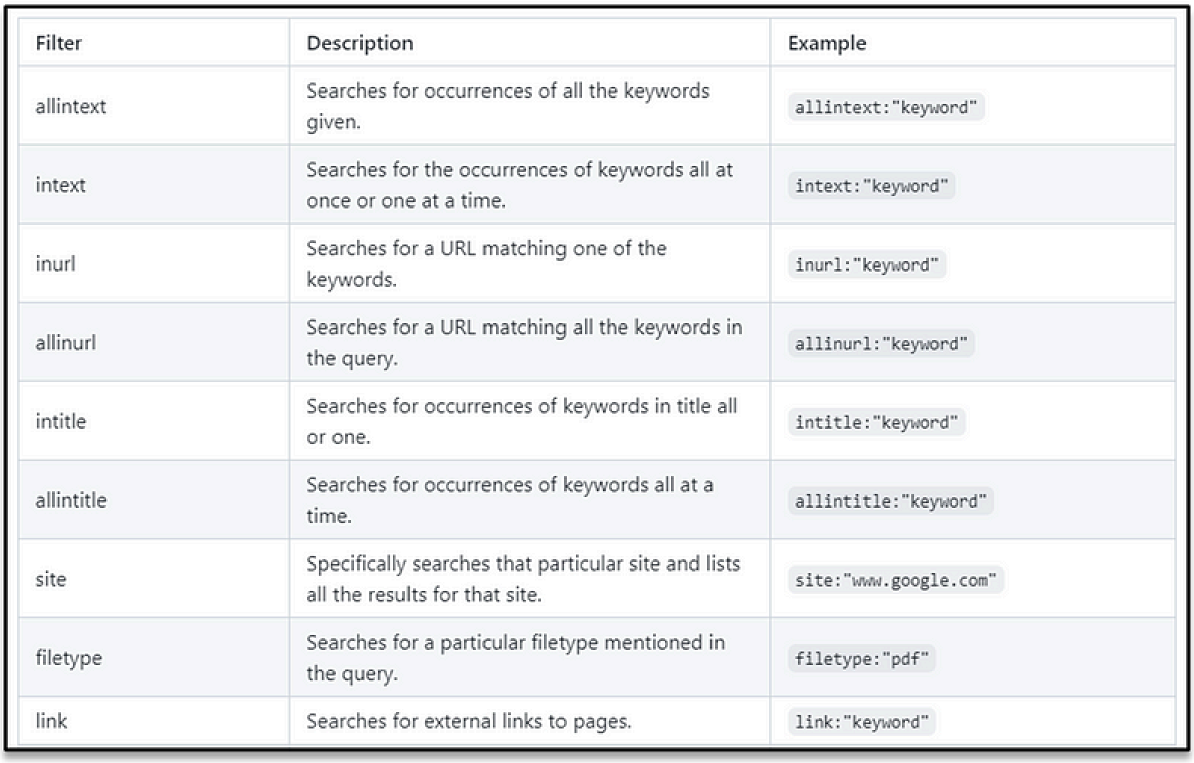
Resource Intensity	Only use available public information;less resource-intensive	More resource intensive and time consuming .
Vulnerability Identification	Limited ability to identify vulnerabilities since it does not interact directly	Identify specific vulnerabilities and weakness in sysytem
Use Cases	Useful for initial reconnaissance phases to gather background information .	Ideal for penetration testing where detailed system insights are needed

Passive Reconnaissance(GOOGLE DORKING)

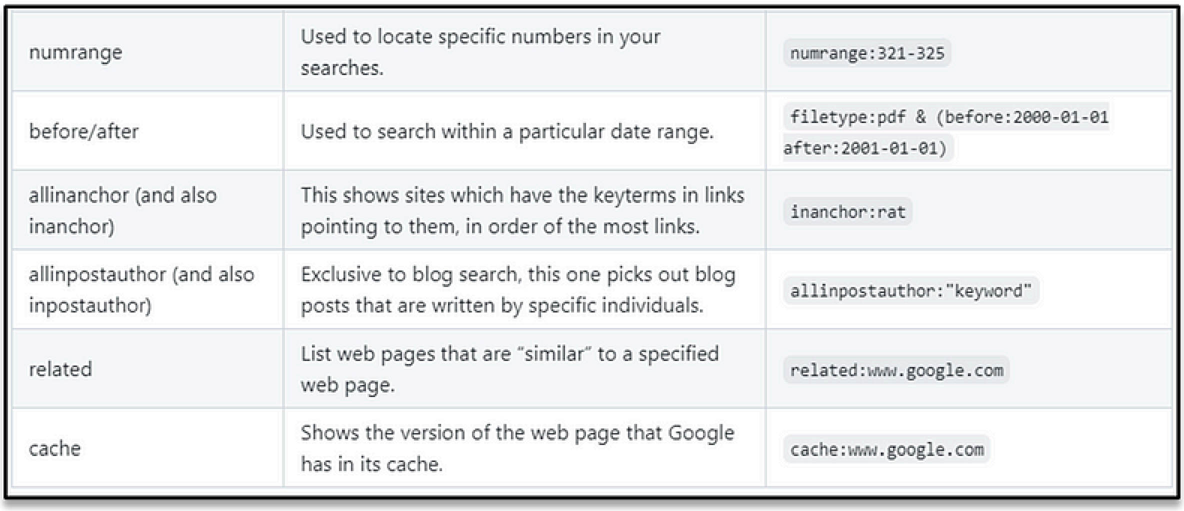
What is Google Dorking?

Google Dorking is known as Google Hacking which refers to the use of advanced search operators in Google to find specific information that is not typically visible through regular search queries. It involves leveraging Google's powerful search engine to locate hidden data on websites such as sensitive files, configuration files, or vulnerabilities that may have been accidentally exposed.

Google dork cheatsheet:



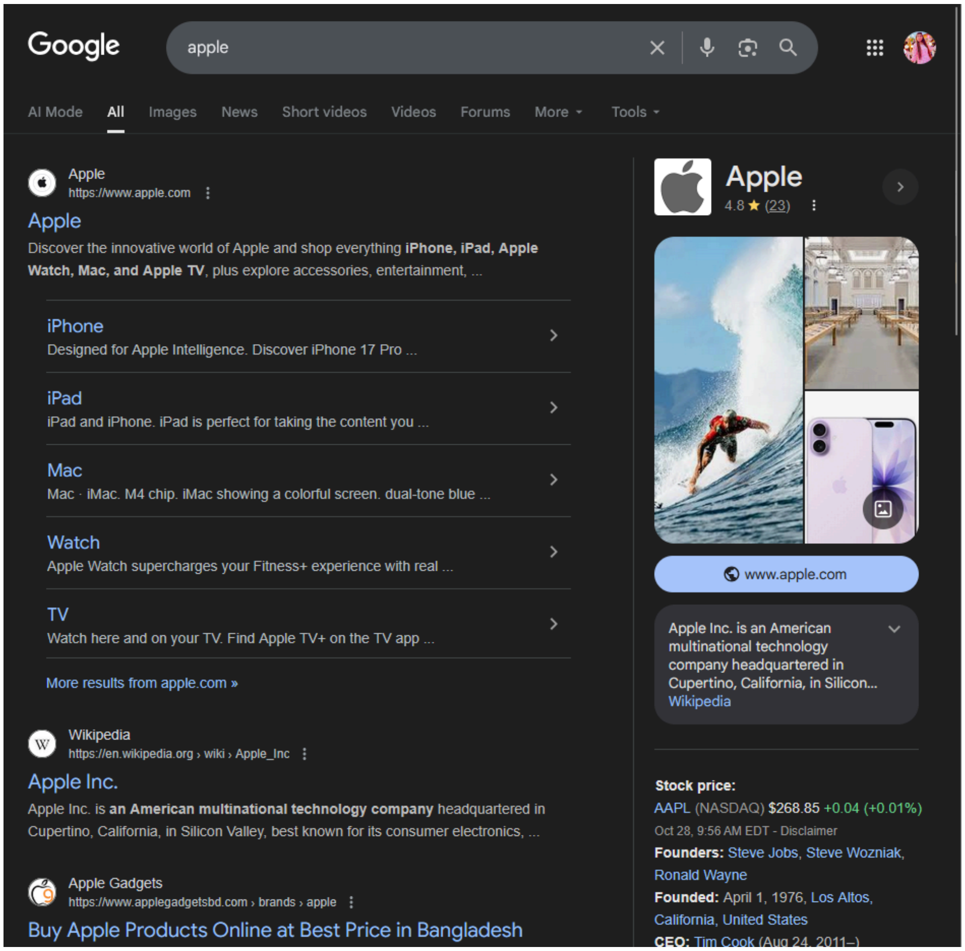
Filter	Description	Example
allintext	Searches for occurrences of all the keywords given.	`allintext:"keyword"`
intext	Searches for the occurrences of keywords all at once or one at a time.	`intext:"keyword"`
inurl	Searches for a URL matching one of the keywords.	`inurl:"keyword"`
allinurl	Searches for a URL matching all the keywords in the query.	`allinurl:"keyword"`
intitle	Searches for occurrences of keywords in title all or one.	`intitle:"keyword"`
allintitle	Searches for occurrences of keywords all at a time.	`allintitle:"keyword"`
site	Specifically searches that particular site and lists all the results for that site.	`site:"www.google.com"`
filetype	Searches for a particular filetype mentioned in the query.	`filetype:"pdf"`
link	Searches for external links to pages.	`link:"keyword"`



numrange	Used to locate specific numbers in your searches.	`numrange:321-325`
before/after	Used to search within a particular date range.	`filetype:pdf & (before:2000-01-01 after:2001-01-01)`
allinanchor (and also inanchor)	This shows sites which have the keyterms in links pointing to them, in order of the most links.	`inanchor:rat`
allinpostauthor (and also inpostauthor)	Exclusive to blog search, this one picks out blog posts that are written by specific individuals.	`allinpostauthor:"keyword"`
related	List web pages that are "similar" to a specified web page.	`related:www.google.com`
cache	Shows the version of the web page that Google has in its cache.	`cache:www.google.com`

1.Search term:

I was willing to search for a fruit “apple” but what I got as a result. not a wrong one but just confusing.



Apple
https://www.apple.com

Apple

Discover the innovative world of Apple and shop everything **iPhone, iPad, Apple Watch, Mac, and Apple TV**, plus explore accessories, entertainment, ...

iPhone
Designed for Apple Intelligence. Discover iPhone 17 Pro ...

iPad
iPad and iPhone. iPad is perfect for taking the content you ...

Mac
Mac · iMac. M4 chip. iMac showing a colorful screen. dual-tone blue ...

Watch
Apple Watch supercharges your Fitness+ experience with real ...

TV
Watch here and on your TV. Find Apple TV+ on the TV app ...

More results from apple.com »

Wikipedia
https://en.wikipedia.org › wiki › Apple_Inc

Apple Inc.

Apple Inc. is **an American multinational technology company** headquartered in Cupertino, California, in Silicon Valley, best known for its consumer electronics, ...

Apple Gadgets
https://www.applegadgetsbd.com › brands › apple

Buy Apple Products Online at Best Price in Bangladesh

Apple
4.8 ★ (23)

www.apple.com

Apple Inc. is an American multinational technology company headquartered in Cupertino, California, in Silicon... Wikipedia

Stock price: AAPL (NASDAQ) $268.85 +0.04 (+0.01%)
Oct 28, 9:56 AM EDT - Disclaimer

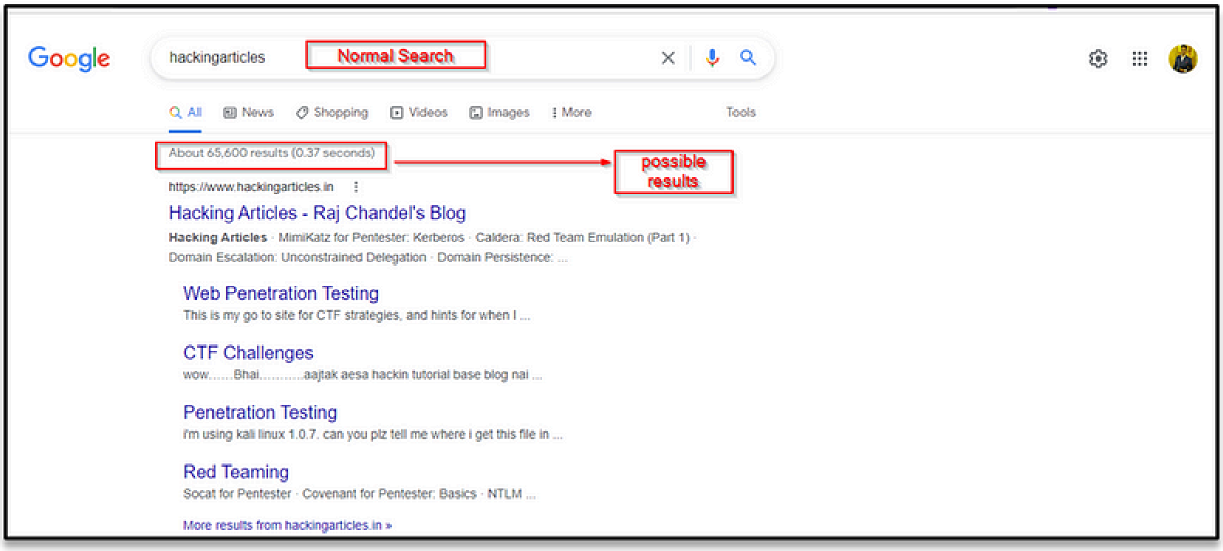
Founders: Steve Jobs, Steve Wozniak, Ronald Wayne

Founded: April 1, 1976, Los Altos, California, United States

CEO: Tim Cook (Aug 24, 2011–)

2.Syntax

1. Inurl



About 65,600 results (0.37 seconds)

https://www.hackingarticles.in

Hacking Articles - Raj Chandel's Blog

Hacking Articles · MimiKatz for Pentester: Kerberos · Caldera: Red Team Emulation (Part 1) · Domain Escalation: Unconstrained Delegation · Domain Persistence: ...

Web Penetration Testing

This is my go to site for CTF strategies, and hints for when I ...

CTF Challenges

wow......Bhai...........aajtak aesa hackin tutorial base blog nai ...

Penetration Testing

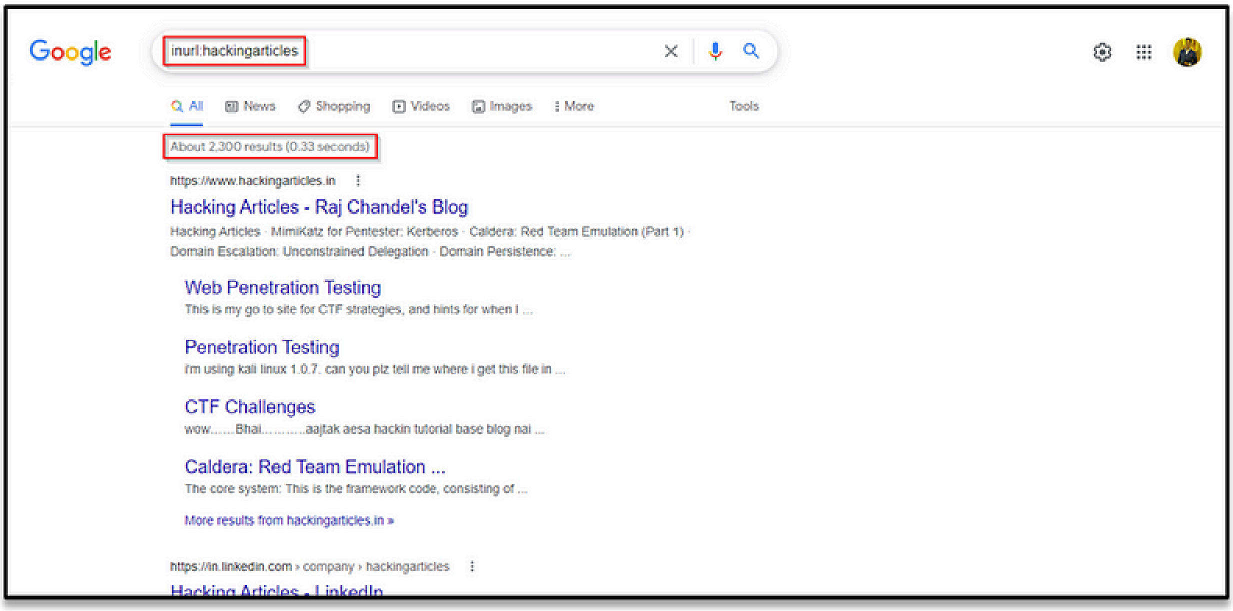
i'm using kali linux 1.0.7. can you plz tell me where i get this file in ...

Red Teaming

Socat for Pentester · Covenant for Pentester: Basics · NTLM ...

More results from hackingarticles.in »

Filtered result using inurl syntax



About 2,300 results (0.33 seconds)

https://www.hackingarticles.in

Hacking Articles - Raj Chandel's Blog

Hacking Articles · MimiKatz for Pentester: Kerberos · Caldera: Red Team Emulation (Part 1) · Domain Escalation: Unconstrained Delegation · Domain Persistence: ...

Web Penetration Testing

This is my go to site for CTF strategies, and hints for when I ...

Penetration Testing

i'm using kali linux 1.0.7. can you plz tell me where i get this file in ...

CTF Challenges

wow......Bhai...........aajtak aesa hackin tutorial base blog nai ...

Caldera: Red Team Emulation ...

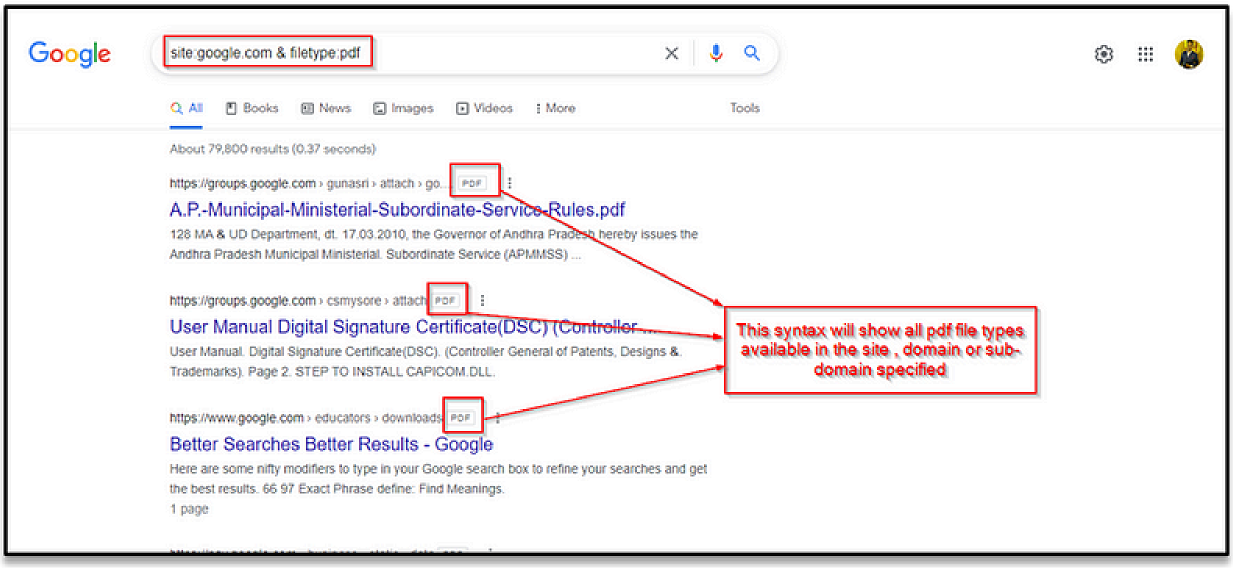
The core system: This is the framework code, consisting of ...

More results from hackingarticles.in »

https://in.linkedin.com › company › hackingarticles

Hacking Articles - LinkedIn

3.site and file type:



site:google.com & filetype:pdf

About 79,800 results (0.37 seconds)

https://groups.google.com › gunasri › attach › go... PDF

A.P.-Municipal-Ministerial-Subordinate-Service-Rules.pdf

128 MA & UD Department, dt. 17.03.2010, the Governor of Andhra Pradesh hereby issues the Andhra Pradesh Municipal Ministerial. Subordinate Service (APMMSS) ...

https://groups.google.com › csmysore › attach PDF

User Manual Digital Signature Certificate(DSC) (Controller ...

User Manual. Digital Signature Certificate(DSC). (Controller General of Patents, Designs & Trademarks). Page 2. STEP TO INSTALL CAPICOM.DLL.

https://www.google.com › educators › downloads PDF

Better Searches Better Results - Google

Here are some nifty modifiers to type in your Google search box to refine your searches and get the best results. 66 97 Exact Phrase define: Find Meanings.

1 page

This syntax will show all pdf file types available in the site , domain or sub-domain specified