Enumerate Infrastructure and Application Admin Interface

AIM:

To famialiarize tools for enumerating Infrastructure and Application Admin Interface.

Description:

Administrator interfaces may be present in the application or on the application server to allow certain users to perform privileged activities on the site. Tests should be undertaken to reveal if and how this privileged functionality can be accessed by an unauthorized or standard user.

An application may require an administrator interface to enable a privileged user to access functionality that may make changes to how the site functions. Such changes may include:

- user account provisioning
- site design and layout
- data manipulation
- configuration changes

In many instances, such interfaces do not have sufficient controls to protect them from unauthorized access. Testing is aimed at discovering these administrator interfaces and accessing functionality intended for the privileged users.

There are a wide variety of administration interfaces for different technologies. For example:

- Remote management protocols such as SSH, PowerShell, RDP and VNC
- Browser-based management such as cloud-based web consoles and appliance configuration panels
- APIs that expose management functionality
- Thick clients - typically, software installed on a device that drives an administration protocol or API in the background

Some systems are managed through code and configuration files rather than the interfaces listed above. This can also be a form of system administration.

Administration interfaces are an attack surface. Only legitimate administrators should be able to communicate with them. You should isolate these interfaces using architectural controls and constrain who can connect to the system and from where. This will help to protect against attacks such as brute forcing administrator login, or using an exploit to gain access.

There are a number of ways that you can reduce the exposure of your management interfaces. For example:

- ✓ You could create a dedicated management network that only authorised administrators have physical access to.
- ✓ You could place your administration interfaces behind a VPN that only authenticated administrators and devices can use.
- ✓ You could implement an IP allow list to restrict the devices or networks that can access the administration interface.

Some architectural controls are stronger than others. For example, IP allow lists can be overcome if the attacker is able to share the IP address space, or spoof it. They can also be difficult to maintain.

Depending on your risk appetite, it may be necessary to combine multiple mitigations to adequately protect your administration interfaces.The mitigations that you choose will depend on a number of factors, including where the interface is located, what it allows access to and who the administrators are that need access to it.

Implementation guidance

- ✓ Only permit authorised devices. It should not be possible for untrusted devices to access your administration interfaces. Architectural controls should be implemented to ensure that the origin of administration activities is a trusted device. This helps to reduce the attack surface.
- ✓ Use browse down, not browse up. If an attacker compromises a less trusted device, they will inherit it’s accesses. If that device can be used to browse up to a more critical system, the attacker can do so too. See 1 - Gain trust in your management devices for more information.
- ✓ Authenticate the administrator. Administrators must be authenticated before carrying out their duties. Authentication should be achieved using well known protocols.
- ✓ Utilise multi-factor authentication. Where available, MFA should be enabled on administrator accounts. This introduces a high hurdle for an attacker to jump, but has little effect on administrators. Remember that this isn’t bulletproof: if an adversary has

access to the PAW, they can piggyback on an authenticated session after MFA has been completed.

- ✓ Protect your administration credentials. Discourage administrators from writing credentials on post-it notes and consider the use of a password manager. Also ensure that credentials are not hard-coded into software projects, as they could mistakenly be published to a code repository. If certificates are used for authentication, carefully protect them. See our password guidance for more information.
- ✓ Use Privilege Access Management. See 4 - Use privileged access management for more information.
- ✓ Use secure protocols. The protocol that is used to carry traffic from a Privileged Access Workstation to the administration interface should be encrypted. If it is not, an attacker could view the traffic and manipulate it. For example, APIs using HTTPS should be preferred over Telnet. You should investigate what protocol is used by any thick client and ensure that these connections are protected too.
- ✓ Update your administration infrastructure. Updates should be installed to ensure that your systems are patched against known vulnerabilities. These updates should be installed as soon as possible, because attackers put effort into understanding them, searching for the vulnerabilities that they patch.
- ✓ Monitor administration activities. See 5 - Log and audit administration activities for more information.
- ✓ Implement procedural policies governing system administrators. System administration policies should cover a wide number of topics. For example, the number of administrators should be bounded with upper and lower limits that are appropriate to your environment. Further, the principal of least privilege should be applied, and a robust 'joiners, movers and leavers' process should be defined.

Procedure:

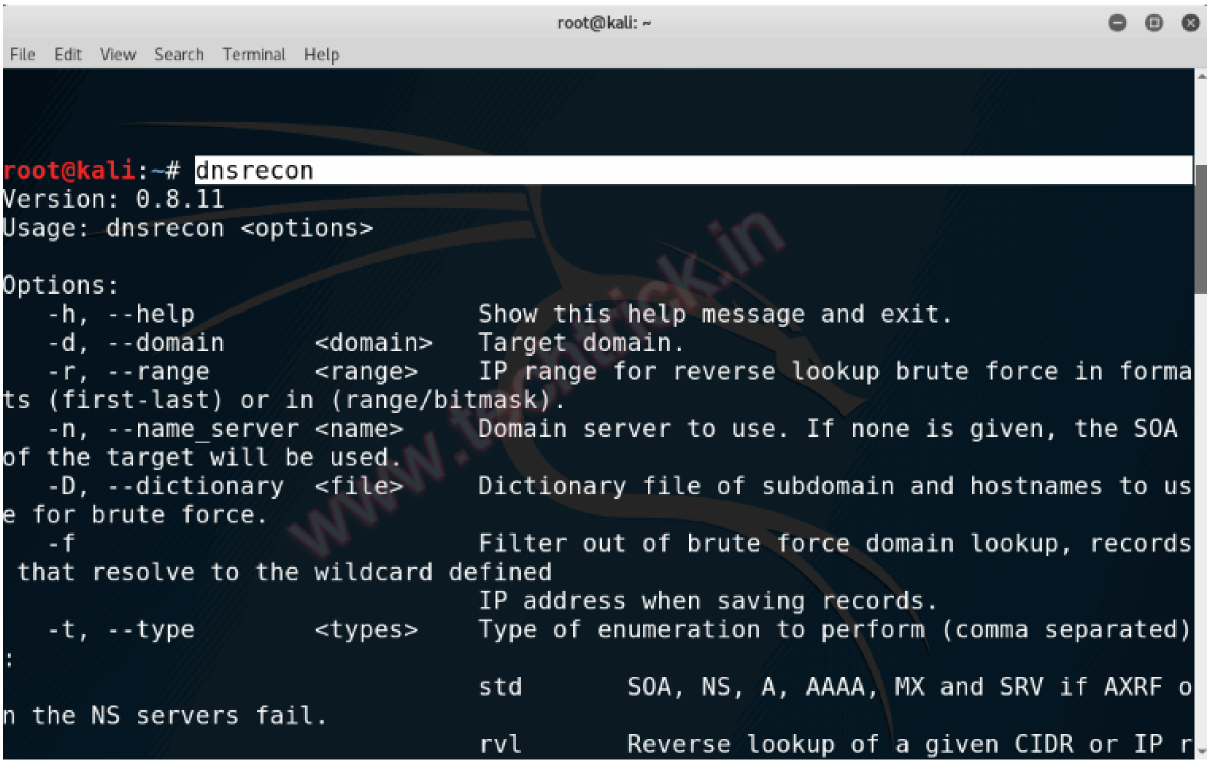
✓ ***Dnsrecon***

DNSRecon is a Python script that provides the ability to perform:

- Check all NS Records for Zone Transfers.
- Enumerate General DNS Records for a given Domain (MX, SOA, NS, A, AAAA, SPF and TXT).
- Perform common SRV Record Enumeration.

- Top Level Domain (TLD) Expansion.
- Check for Wildcard Resolution.
- Brute Force subdomain and host A and AAAA records given a domain and a wordlist.
- Perform a PTR Record lookup for a given IP Range or CIDR.
- Check a DNS Server Cached records for A, AAAA and CNAME
- Records provided a list of host records in a text file to check.
- Enumerate Hosts and Subdomains using Google

type DnsRecon on the kali linux terminal.

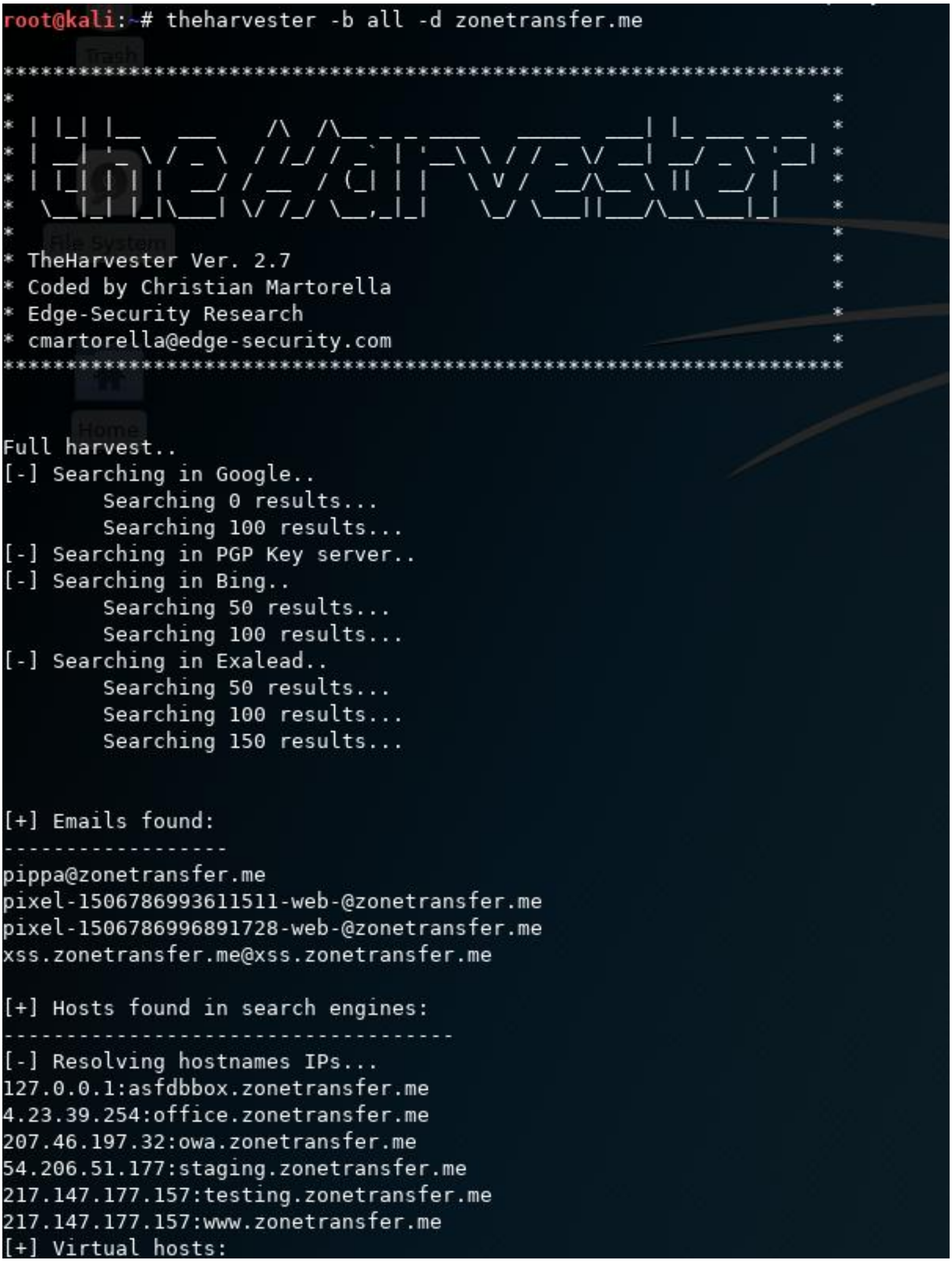


```
root@kali:~# dnsrecon
Version: 0.8.11
Usage: dnsrecon <options>

Options:
   -h, --help                   Show this help message and exit.
   -d, --domain      <domain>   Target domain.
   -r, --range       <range>    IP range for reverse lookup brute force in forma
ts (first-last) or in (range/bitmask).
   -n, --name_server <name>     Domain server to use. If none is given, the SOA
of the target will be used.
   -D, --dictionary  <file>     Dictionary file of subdomain and hostnames to us
e for brute force.
   -f                           Filter out of brute force domain lookup, records
 that resolve to the wildcard defined
                                IP address when saving records.
   -t, --type        <types>    Type of enumeration to perform (comma separated)
:
                                std       SOA, NS, A, AAAA, MX and SRV if AXRF o
n the NS servers fail.
                                rvl       Reverse lookup of a given CIDR or IP r
```

✓ ***theHarvester***

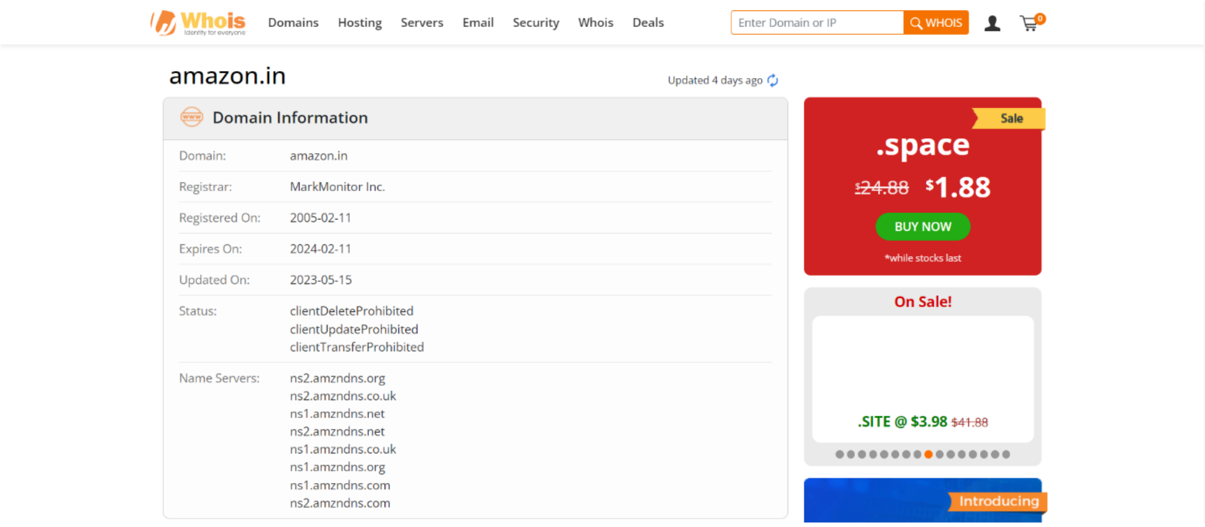
theHarvester is a command-line tool included in Kali Linux that acts as a wrapper for a variety of search engines and is used to find email accounts, subdomain names, virtual hosts, open ports / banners, and employee names related to a domain from different public sources (such as search engines and PGP key servers). In recent versions, the authors added the capability of doing DNS brute force, reverse IP resolution, and **Top-Level Domain** (**TLD**) expansion.

✓ In the following example, theHarvester is used to gather information about zonetransfer.me:



```
root@kali:~# theharvester -b all -d zonetransfer.me

*******************************************************************
*                                                                 *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __| '_ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* TheHarvester Ver. 2.7                                           *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*******************************************************************


Full harvest..
[-] Searching in Google..
        Searching 0 results...
        Searching 100 results...
[-] Searching in PGP Key server..
[-] Searching in Bing..
        Searching 50 results...
        Searching 100 results...
[-] Searching in Exalead..
        Searching 50 results...
        Searching 100 results...
        Searching 150 results...


[+] Emails found:
------------------
pippa@zonetransfer.me
pixel-1506786993611511-web-@zonetransfer.me
pixel-1506786996891728-web-@zonetransfer.me
xss.zonetransfer.me@xss.zonetransfer.me

[+] Hosts found in search engines:
------------------------------------
[-] Resolving hostnames IPs...
127.0.0.1:asfdbbox.zonetransfer.me
4.23.39.254:office.zonetransfer.me
207.46.197.32:owa.zonetransfer.me
54.206.51.177:staging.zonetransfer.me
217.147.177.157:testing.zonetransfer.me
217.147.177.157:www.zonetransfer.me
[+] Virtual hosts:
```

- ✓ ***Finding subdomain info***



amazon.in

Updated 4 days ago

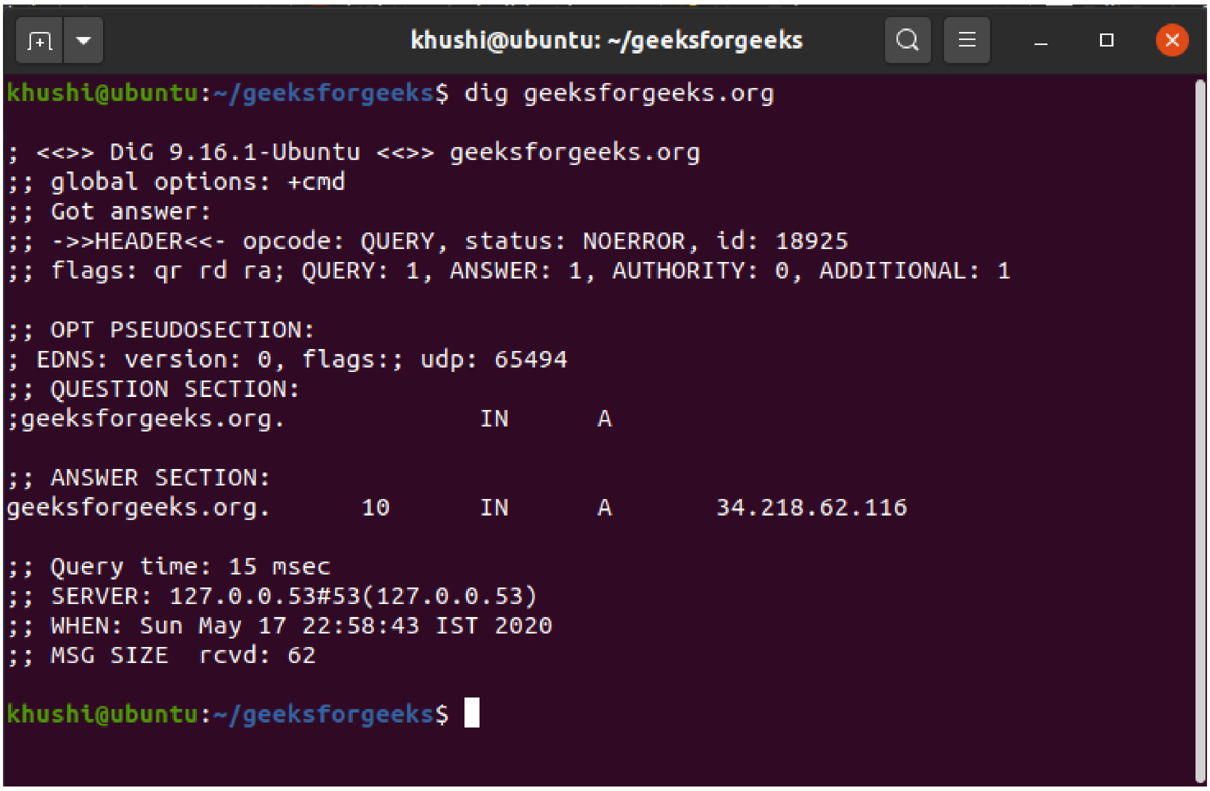
Domain Information

Domain: amazon.in
Registrar: MarkMonitor Inc.
Registered On: 2005-02-11
Expires On: 2024-02-11
Updated On: 2023-05-15
Status: clientDeleteProhibited
clientUpdateProhibited
clientTransferProhibited
Name Servers: ns2.amzndns.org
ns2.amzndns.co.uk
ns1.amzndns.net
ns2.amzndns.net
ns1.amzndns.co.uk
ns1.amzndns.org
ns1.amzndns.com
ns2.amzndns.com

✓ ***Dig***

dig command stands for Domain Information Groper. It is used for retrieving information about DNS name servers. It is basically used by network administrators. It is used for verifying and troubleshooting DNS problems and to perform DNS lookups. Dig command replaces older tools such as nslookup and the host.

dig geeksforgeeks.org



```
khushi@ubuntu:~/geeksforgeeks$ dig geeksforgeeks.org

; <<>> DiG 9.16.1-Ubuntu <<>> geeksforgeeks.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18925
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;geeksforgeeks.org.             IN      A

;; ANSWER SECTION:
geeksforgeeks.org.      10      IN      A       34.218.62.116

;; Query time: 15 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Sun May 17 22:58:43 IST 2020
;; MSG SIZE  rcvd: 62

khushi@ubuntu:~/geeksforgeeks$ 
```

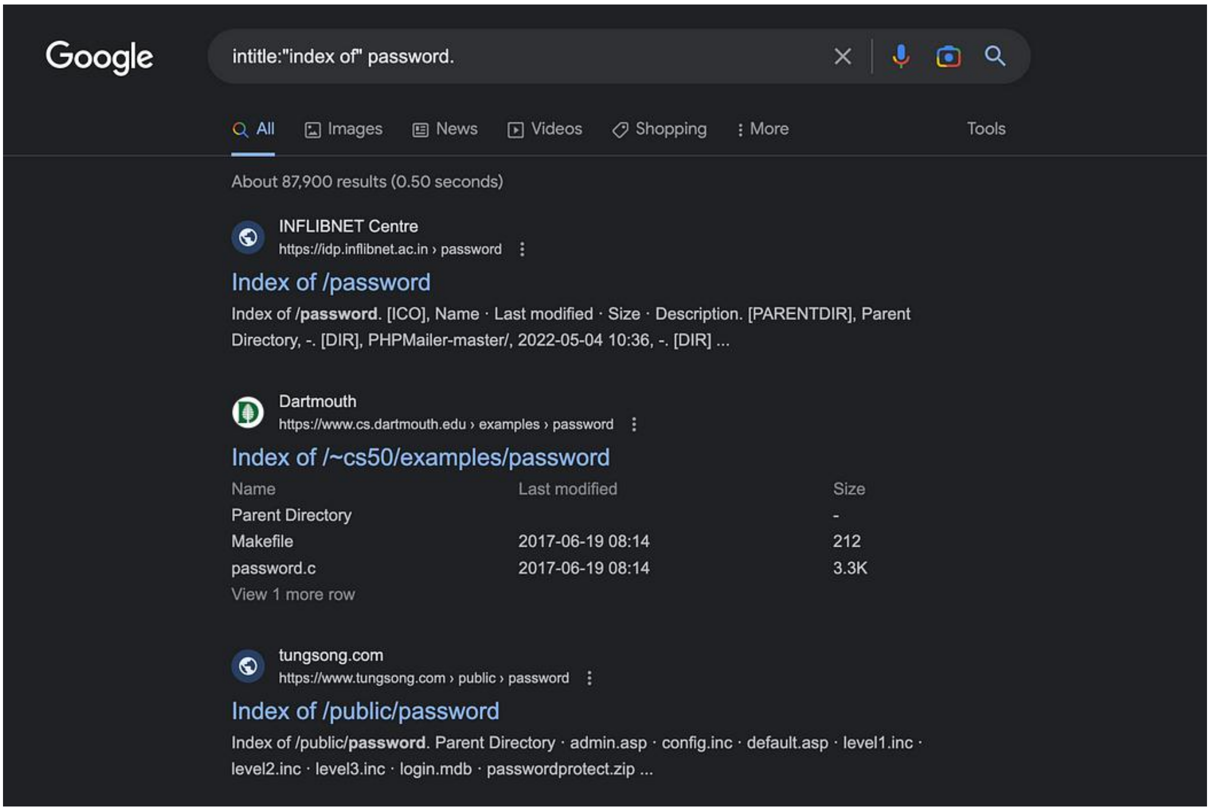
- ✓ **Google Dorking**

  A Google Dork is a special search term. These terms, when used with regular search keywords, can help us discover hidden resources crawled by Google.

Here are some of the most common operators used in Google Dorking.

Intitle operator

The “**intitle**” operator searches for web pages with specific words or phrases in the title tag. For instance, if you’re looking for pages that contain the phrase “password” and have “index of” in the title, you would use the search term:intitle:”index of” password.



intitle:"index of" password.

About 87,900 results (0.50 seconds)

INFLIBNET Centre
https://idp.inflibnet.ac.in › password

Index of /password

Index of /**password**. [ICO], Name · Last modified · Size · Description. [PARENTDIR], Parent Directory, -. [DIR], PHPMailer-master/, 2022-05-04 10:36, -. [DIR] ...

Dartmouth
https://www.cs.dartmouth.edu › examples › password

Index of /~cs50/examples/password

Name	Last modified	Size
Parent Directory		-
Makefile	2017-06-19 08:14	212
password.c	2017-06-19 08:14	3.3K

View 1 more row

tungsong.com
https://www.tungsong.com › public › password

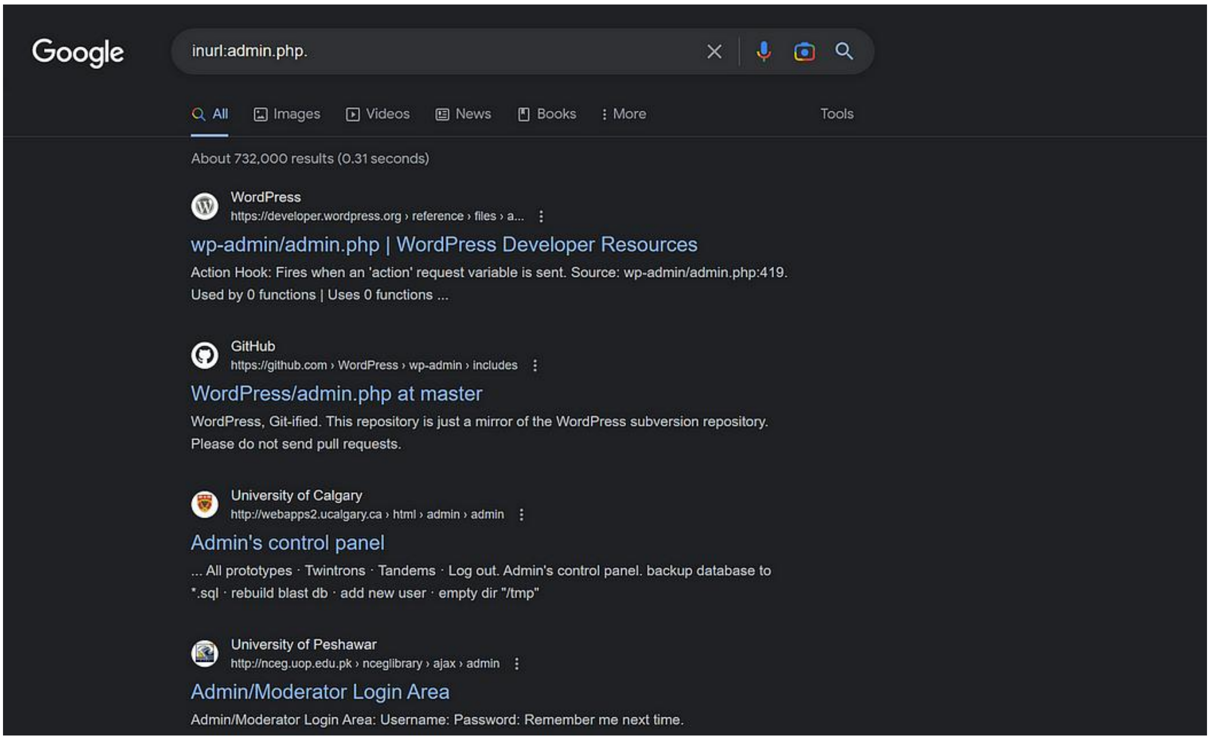
Index of /public/password

Index of /public/**password**. Parent Directory · admin.asp · config.inc · default.asp · level1.inc · level2.inc · level3.inc · login.mdb · passwordprotect.zip ...

In title. Image by the author.

Inurl operator

The “**inurl**” operator searches for web pages that contain specific words or phrases in the URL. For example, if you’re looking for pages that contain “admin.php” in the URL, you would use the search term:inurl:admin.php.



inurl:admin.php.

About 732,000 results (0.31 seconds)

WordPress
https://developer.wordpress.org › reference › files › a...
wp-admin/admin.php | WordPress Developer Resources
Action Hook: Fires when an 'action' request variable is sent. Source: wp-admin/admin.php:419. Used by 0 functions | Uses 0 functions ...

GitHub
https://github.com › WordPress › wp-admin › includes
WordPress/admin.php at master
WordPress, Git-ified. This repository is just a mirror of the WordPress subversion repository. Please do not send pull requests.

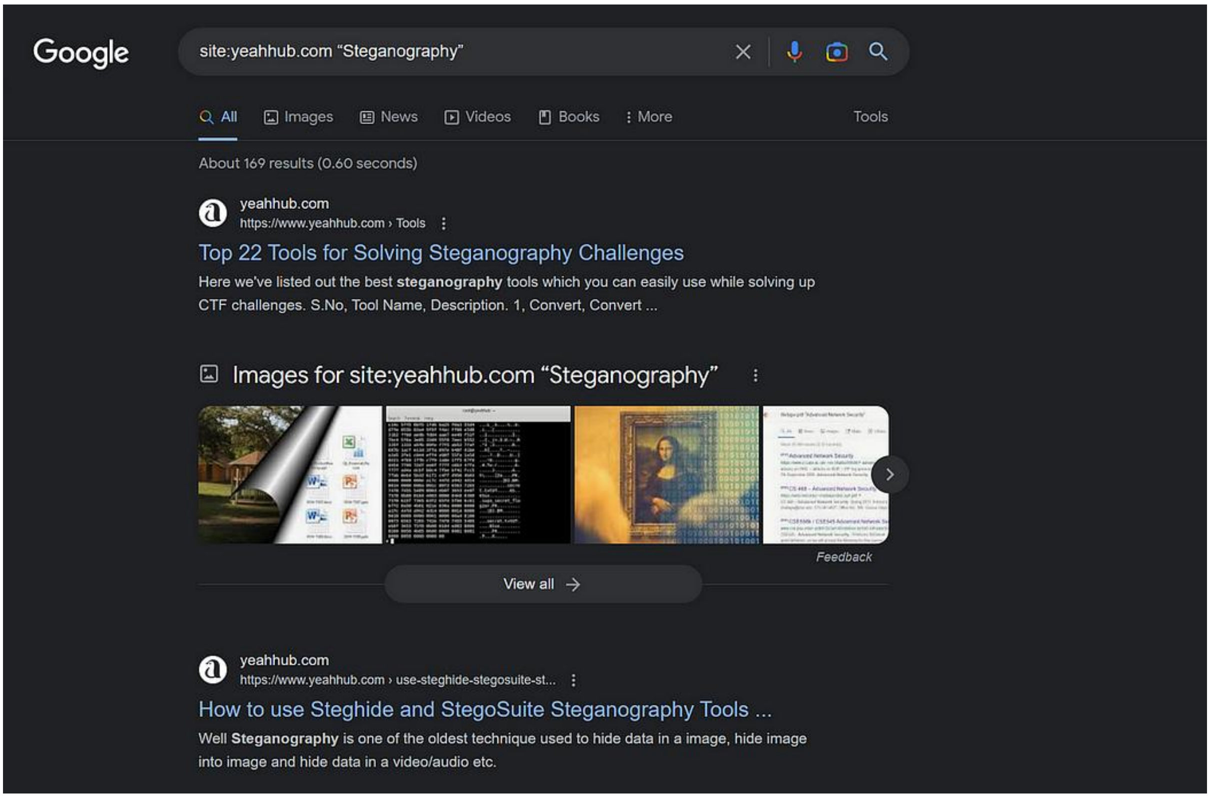
University of Calgary
http://webapps2.ucalgary.ca › html › admin › admin
Admin's control panel
... All prototypes · Twintrons · Tandems · Log out. Admin's control panel. backup database to *.sql · rebuild blast db · add new user · empty dir "/tmp"

University of Peshawar
http://nceg.uop.edu.pk › nceglibrary › ajax › admin
Admin/Moderator Login Area
Admin/Moderator Login Area: Username: Password: Remember me next time.

In url. Image by the author.

Site operator

The “**site**” operator allows you to search within a specific website or domain. For instance, if you’re looking for pages on the example.com domain that contain the word “Steganography”, you would use the search term:site:yeahhub.com “Steganography”



site:yeahhub.com “Steganography”

About 169 results (0.60 seconds)

yeahhub.com
https://www.yeahhub.com › Tools
Top 22 Tools for Solving Steganography Challenges
Here we've listed out the best **steganography** tools which you can easily use while solving up CTF challenges. S.No, Tool Name, Description. 1, Convert, Convert ...

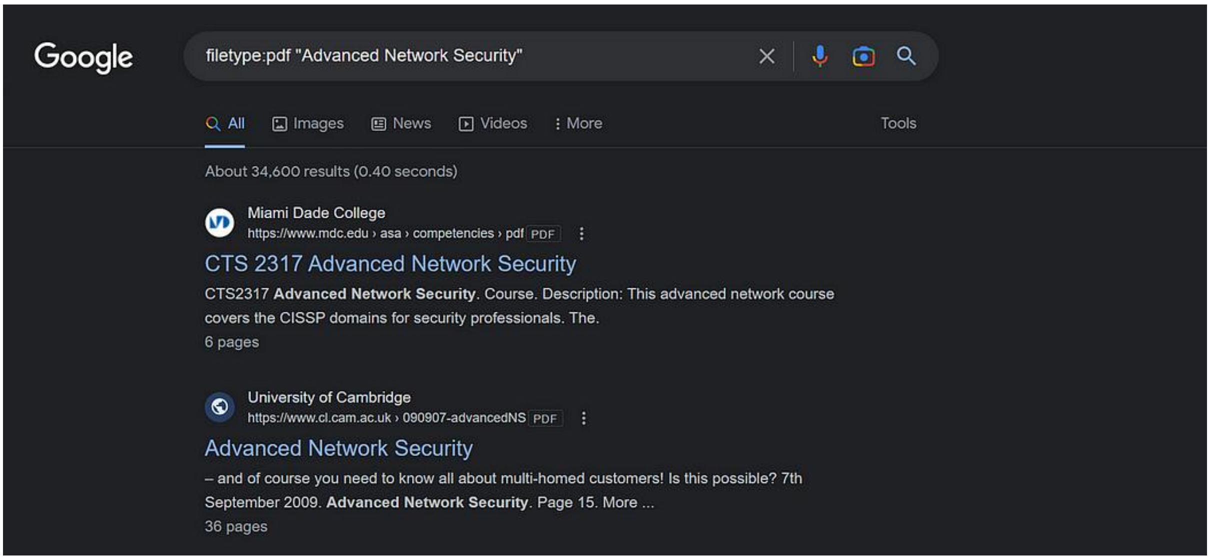
Images for site:yeahhub.com “Steganography”

yeahhub.com
https://www.yeahhub.com › use-steghide-stegosuite-st...
How to use Steghide and StegoSuite Steganography Tools ...
Well **Steganography** is one of the oldest technique used to hide data in a image, hide image into image and hide data in a video/audio etc.

In site. Image by the author.

Filetype operator

The “**filetype**” operator allows you to search for specific file types, such as PDFs or Word documents. For example, if you’re looking for PDF files that contain the phrase “confidential report”, you would use the search term:filetype:pdf "Advanced Network Security"



About 34,600 results (0.40 seconds)

Miami Dade College
https://www.mdc.edu › asa › competencies › pdf PDF

CTS 2317 Advanced Network Security

CTS2317 **Advanced Network Security**. Course. Description: This advanced network course covers the CISSP domains for security professionals. The.
6 pages

University of Cambridge
https://www.cl.cam.ac.uk › 090907-advancedNS PDF

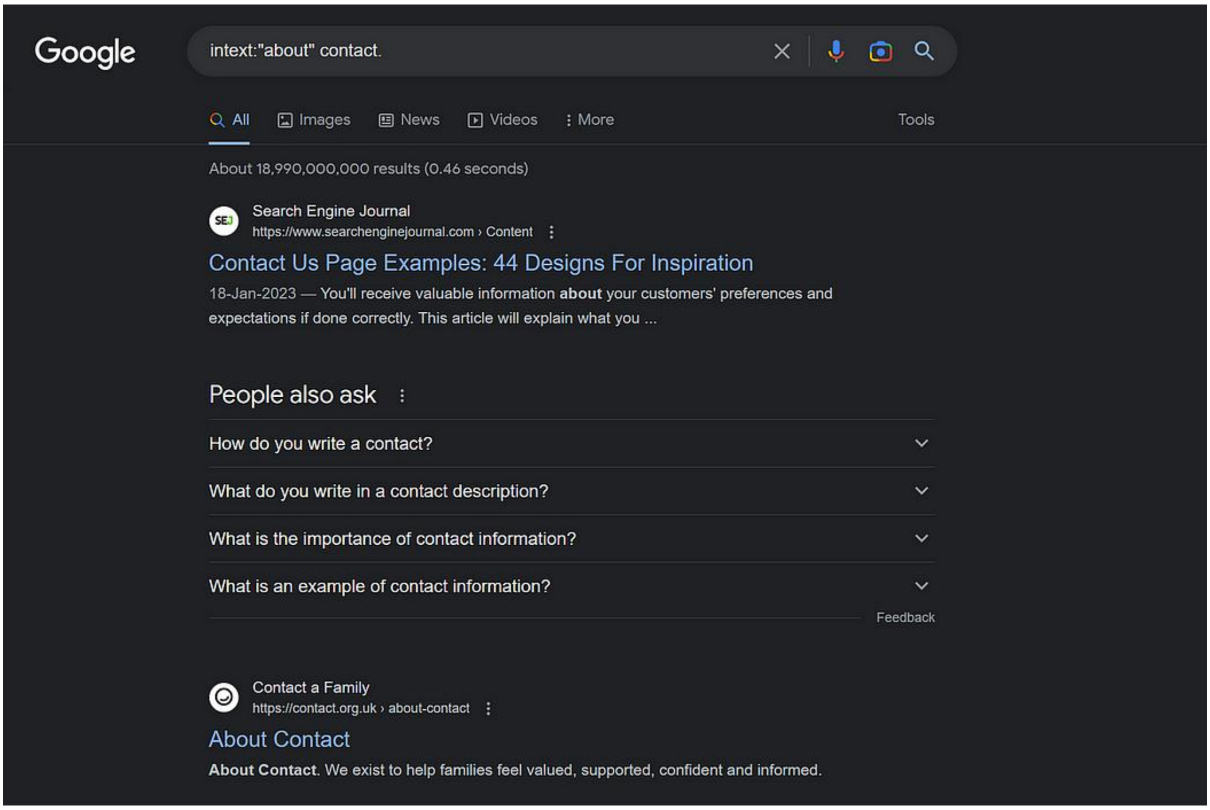
Advanced Network Security

– and of course you need to know all about multi-homed customers! Is this possible? 7th September 2009. **Advanced Network Security**. Page 15. More ...
36 pages

Filetype. Image by the author.

Intext operator

The “**intext**” operator searches for pages that contain specific words or phrases within the body of the page. For instance, if you’re looking for pages that contain both the words “login” and “password” within the body of the page, you would use the search term:intext:"about" contact.



intext:"about" contact.

About 18,990,000,000 results (0.46 seconds)

Search Engine Journal
https://www.searchenginejournal.com › Content

Contact Us Page Examples: 44 Designs For Inspiration

18-Jan-2023 — You'll receive valuable information **about** your customers' preferences and expectations if done correctly. This article will explain what you ...

People also ask

How do you write a contact?

What do you write in a contact description?

What is the importance of contact information?

What is an example of contact information?

Contact a Family
https://contact.org.uk › about-contact

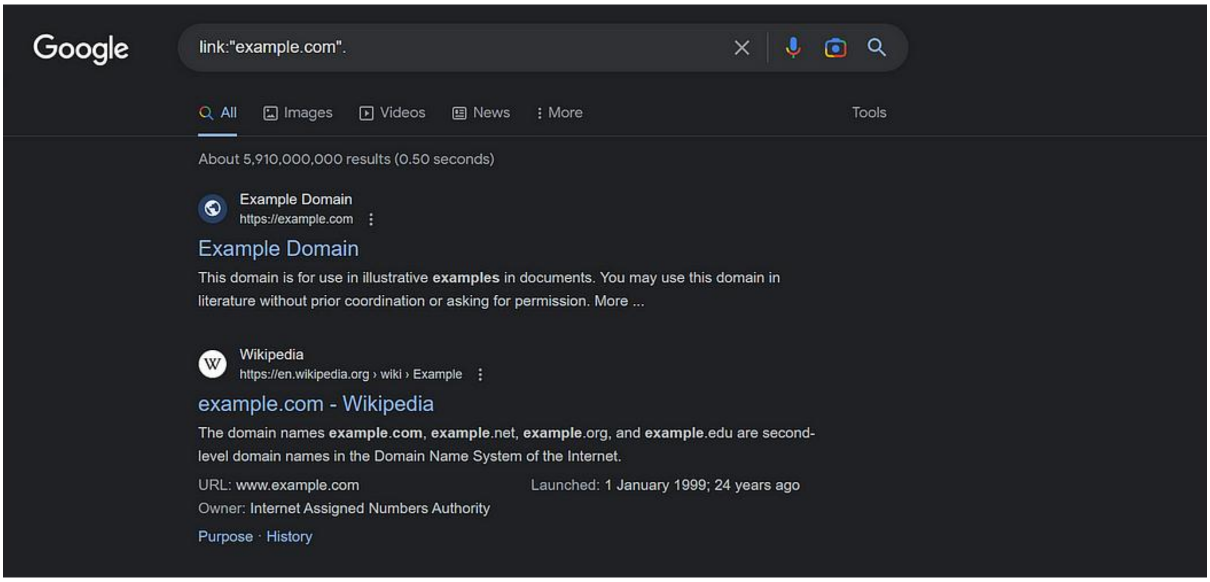
About Contact

About Contact. We exist to help families feel valued, supported, confident and informed.

In text. Image by the author.

Link operator

The "**link**" operator searches for web pages that link to a specific URL. For example, if you're looking for web pages that link to the example.com domain, you would use the search term:link:"example.com"



link:"example.com".

About 5,910,000,000 results (0.50 seconds)

Example Domain
https://example.com

Example Domain

This domain is for use in illustrative **examples** in documents. You may use this domain in literature without prior coordination or asking for permission. More ...

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

example.com - Wikipedia

The domain names **example.com**, **example**.net, **example**.org, and **example**.edu are second-level domain names in the Domain Name System of the Internet.

URL: www.example.com
Launched: 1 January 1999; 24 years ago
Owner: Internet Assigned Numbers Authority

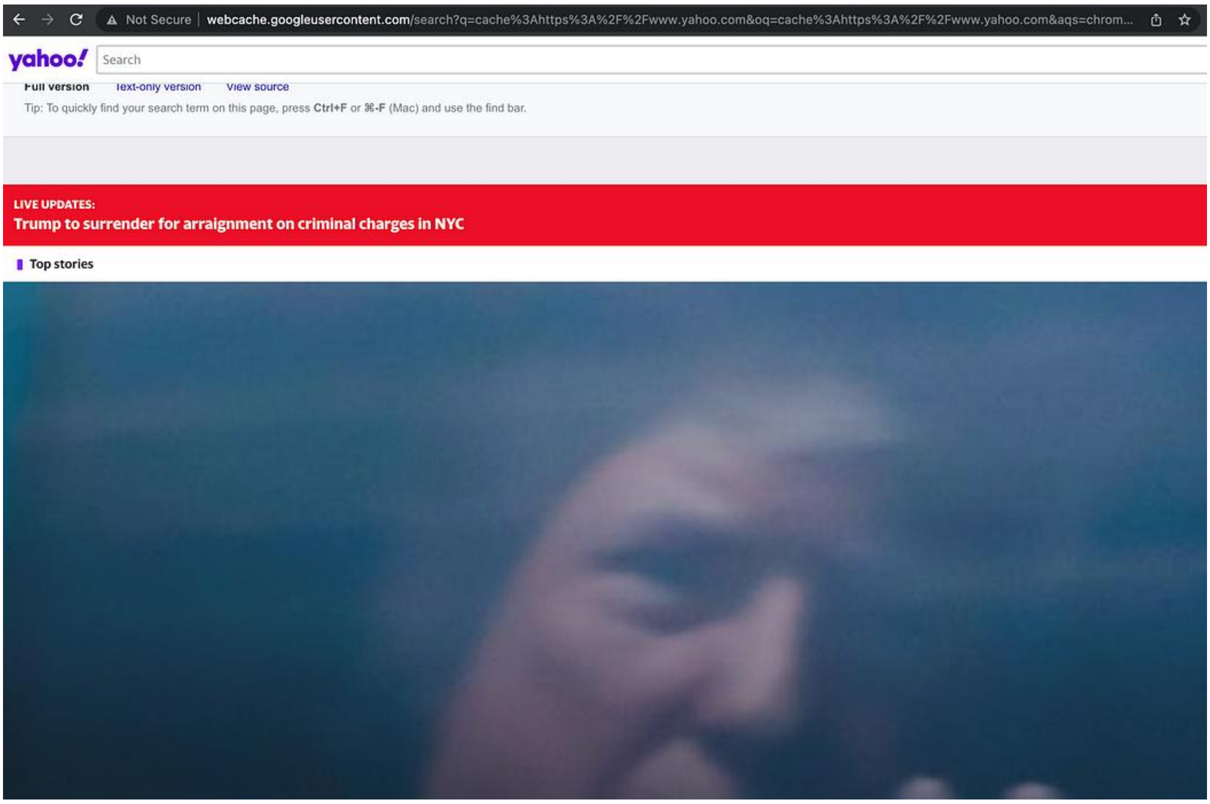
Purpose · History

Link operator. Image by the author.

Cache operator

The "**cache**" operator is used to retrieve the cached version of a web page. When you search for a website using Google, Google creates a cached version of that page in its system. This version can be useful if the original website is temporarily down or if you want to view an older version of the website.

Here is the syntax to find the cached version of yahoo.com.cache:https://www.yahoo.com



Not Secure | webcache.googleusercontent.com/search?q=cache%3Ahttps%3A%2F%2Fwww.yahoo.com&oq=cache%3Ahttps%3A%2F%2Fwww.yahoo.com&aqs=chrom...

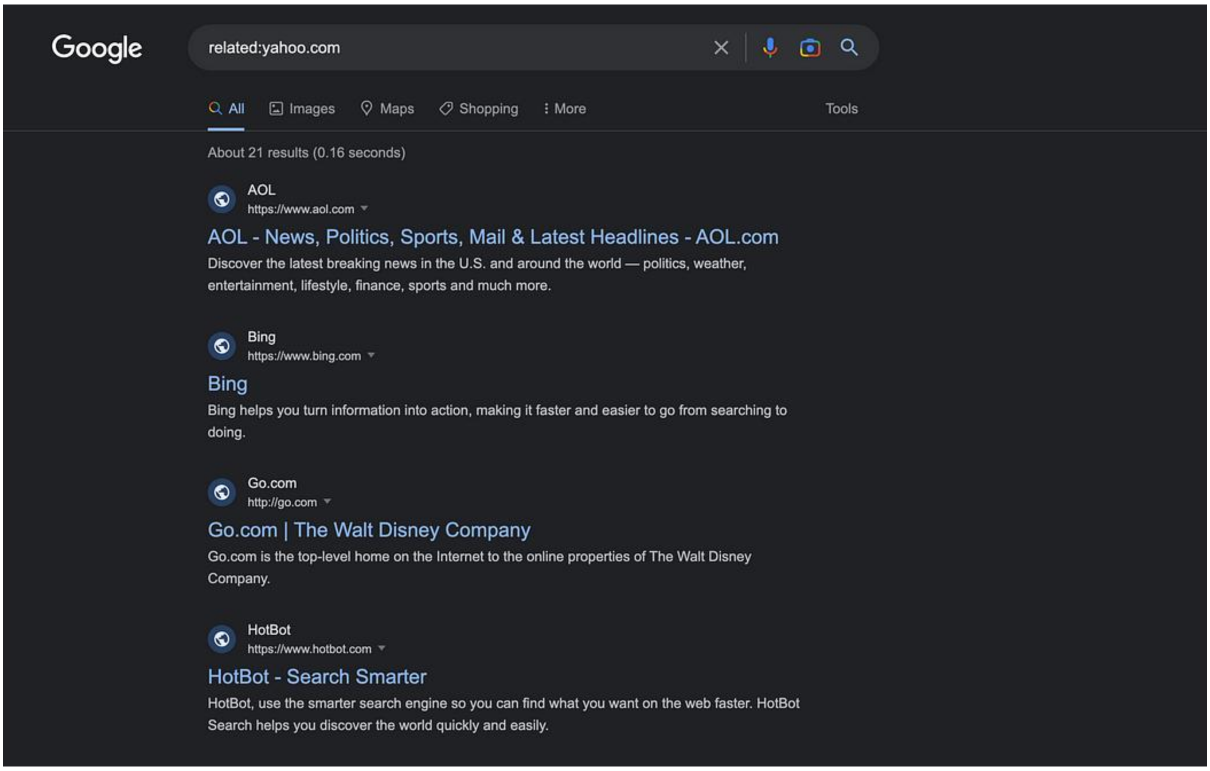
Tip: To quickly find your search term on this page, press **Ctrl+F** or **⌘-F** (Mac) and use the find bar.

LIVE UPDATES:
Trump to surrender for arraignment on criminal charges in NYC

Cached version of yahoo.com. Image by author.

Related operator

The "**related**" operator is used to find web pages that are related to a specific URL. Here is the syntax to use the "related" operator to find sites similar to yahoo.com.



related:yahoo.com

About 21 results (0.16 seconds)

AOL
https://www.aol.com
AOL - News, Politics, Sports, Mail & Latest Headlines - AOL.com
Discover the latest breaking news in the U.S. and around the world — politics, weather, entertainment, lifestyle, finance, sports and much more.

Bing
https://www.bing.com
Bing
Bing helps you turn information into action, making it faster and easier to go from searching to doing.

Go.com
http://go.com
Go.com | The Walt Disney Company
Go.com is the top-level home on the Internet to the online properties of The Walt Disney Company.

HotBot
https://www.hotbot.com
HotBot - Search Smarter
HotBot, use the smarter search engine so you can find what you want on the web faster. HotBot Search helps you discover the world quickly and easily.

Related operator. Image by author.

By combining these operators in creative ways, you can find specific types of information on the web that can be useful for penetration testing and other purposes.