# 2. Footprinting and Reconnaissance

HACKER SCHOOL™

# ETHICAL HACKING

# Theory

## Footprinting

Footprinting is the process of collecting information related to the target network. Footprinting helps in identifying Various ways to intrude into an Organization's network system.

In this step attacker tries to gather publicly available sensitive information, using which he/she can carry out social engineering, perform system or network level attacks, that can cause substantial financial loss or damage the reputation of an individual or organization. This step helps an attacker in gaining a basic idea of network structure and organization's infrastructure details.

## Why perform Footprinting

- Footprinting is the first step of the attacking process. Hackers use to gather information about the target environment, usually to find ways to break into that environment.
- Footprinting allows an attacker to know about the security posture of an organization.
- It helps in reducing attacker's attack surface to a specific range of IP address, networks, domain name, remote access, etc.
- It allows an attacker to build their information database about the target's organization security weakness and plan attacks accordingly.

## Terminology

**Passive Information Gathering:** Is the process of collecting information about the target from the publicly accessible resources

**Active Information Gathering:** Is the process of gather information about the target by using techniques likes social engineering, grabbing information by visiting personal blogs or websites, or through direct interaction with the individual or employees of the organization.

## What kind of information is needed

**Network Information:**

Domain name, Network blocks, IP address of computers in the target network, TCP and UDP services running, details related to IDS running.

**System Information:**

User and group names, system banners, routing tables information, system architecture, remote system names.

**Organization Information:**

Employee details, organization website details, location details, address and phone numbers, information related to security policies implemented, and any non-technical information about the organization.

## How to perform Footprinting

- Through search engines
- Through social networking sites
- Through official websites
- Direct communication with the target
- Through job portals
- Through DNS enumeration

## Google Hacking

Google is a vast resource where millions of pages are available for an average user to search. But getting useful information out of those results is a challenging task, to extract the desired information (information that is useful to attack target individual or network) we can take help of Google search operators also known as google dorks. This technique is called Google Hacking.

By using these google dorks, we query Google to reveal sensitive data, useful for the reconnaissance stage of an attack, sensitive data such as emails associated with an individual or an organization, database files with usernames and passwords, unprotected directories with confidential documents, URLs to login portals, different types of system logs such as firewall and access logs etc.,

## whois lookup

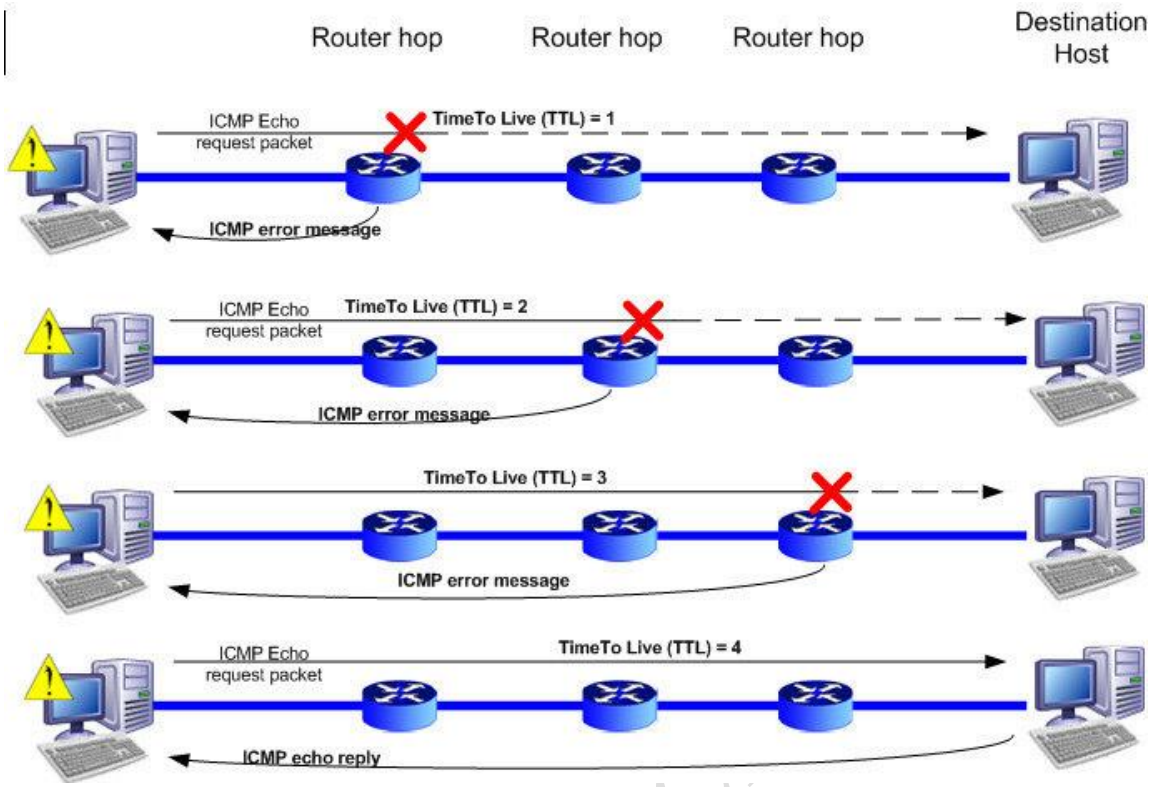
While purchasing a domain, the user (registrant) has to provide their contact details, like address, phone number, email id, etc., those registration details along with domain validity information is usually stored in a publicly available database called whois database.

Domain registrars will protect this information from not to be published on the internet based on the request made by users, at extra cost. Domain registration details will not be available on the internet if they opt domain privacy, of course, domain registrar information will be available, whoever wants to get that domain information should contact the registrar, and if the registrar finds the query is legitimate, they will provide the Domain registrant details. By using the free online and offline tools, we extract domain registrant Information from publicly available Whois database. This process is known as whois lookup.

## Traceroute

While the data packet is in transit, it passes through multiple network nodes to reach the destination. If the data packet fails to reach the destination, the user will not know the reason behind the failure; network administrators use traceroute program to trace the packet from source to destination to identify the actual cause of the problem so that they can investigate and resolve the issue.

Traceroute tool is used to extract details about the path that a packet takes from the source to a specific destination.




## Domain

A domain name is an identification string that defines a group of computers that can be accessed and administered with a common set of rules and procedures. Within the Internet, domains are defined by the IP address. All devices sharing a common part of the IP address are said to be in the same domain.

In general, a domain name identifies a network domain, or it represents an Internet Protocol (IP) resource, such as a personal computer used to access the Internet, a server computer hosting a web site, or the web site itself or any other service communicated via the Internet. Domains are formed by the rules and procedures of the Domain Name System (DNS). Any name registered in the DNS is a domain name.

## Subdomain

In the Domain Name System (DNS) hierarchy, a subdomain is a domain that is a part of another (main) domain. Subdomains are created to organize and navigate to different sections of your website. You can create multiple subdomains or child domains on your main domain.

The most common use of a subdomain is for creating a testing or staging version of a website. Often developers will test new plugins and updates on a subdomain before publishing them live on the Internet. Another common use of a subdomain is to create an online eCommerce store. Often companies want a separate subdomain to handle transactions because eCommerce sites typically require a more complex set up.

## What if We Skip Footprinting?

We should not skip Footprinting. Hacker or penetration tester's success will not always depend on sophisticated tools used to perform attacks, but information gathered at Footprinting plays a crucial role in gaining access to the target. Want to know how?

**Scenario**: Information gathered in this step can help us bypass some security controls for example login credentials for one of the computers in the network may be DOB or first name of the employee. As we know some necessary information about an employee, we can try to guess the username or password by observing hint.

**Conclusion**: launching attacks without proper knowledge about the target may affect the success of the attack.

# Countermeasures

- Revise the information before publishing on blogs, social networking sites, and websites.
- Never upload highly classified documents online.
- Privatize the who is lookup registration details by applying for anonymous registration with the web hosting service provider.
- Never click the link in emails or mobiles, if received from an unknown sender.
- Use pseudo-names in blogs and social networking sites to not leak personal information.
- Avoid opening third-party social networking sites or websites from office premises.
- Use IDS in corporate networks to detect Footprinting attacks done by hackers.


Ddos-attack
BOOM
PC
Password
Hacking
Hacking
Mail
Protection
PETYA
Virus Attack

# Practicals

# INDEX





**THIS DOCUMENT INCLUDES ADDITIONAL PRCTICALS WHICH MAY OR MAY NOT BE COVERED DURING CLASSROOM TRAINING. FOR MORE DETAILS APPROACH LAB COORDINATORS**

# Practical 1: Finding domain registration details with Whois tool

**Description:** Whenever companies or any service provider purchase domain or IP addresses, they will submit their information to the IANA. This information is stored in whois database and it is publicly available to access. By using **Whois** tool in parrot Linux we can get information about who is the owner of the site (registrant) and who is the registrar.

**Prerequisites:** whois tool installed in your system

**Step 1:** WHOIS is used to gather information related to the domain name and DNS details of the target.

- Enter the following command to perform **Whois** operation on target. In this case, we are targeting **hackthissite.org**

```
fish /home/user
File  Edit  View  Search  Terminal  Help
user@parrot-virtual ~> whois hackthissite.org
Domain Name: HACKTHISSITE.ORG
Registry Domain ID: D99641092-LROR
Registrar WHOIS Server: whois.enom.com
Registrar URL: http://www.enom.com
Updated Date: 2020-07-12T08:05:03Z
Creation Date: 2003-08-10T15:01:25Z
Registry Expiry Date: 2021-08-10T15:01:25Z
Registrar Registration Expiration Date:
Registrar: eNom, Inc.
Registrar IANA ID: 48
Registrar Abuse Contact Email: abuse@enom.com
Registrar Abuse Contact Phone: +1.4252982646
Reseller:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registrant Organization: Data Protected
Registrant State/Province: WA
Registrant Country: US
Name Server: C.NS.BUDDYNS.COM
Name Server: F.NS.BUDDYNS.COM
Name Server: G.NS.BUDDYNS.COM
Name Server: H.NS.BUDDYNS.COM
Name Server: J.NS.BUDDYNS.COM
```

# Practical 2: Extracting Emails and subdomains details using the harvester

**Description:** This practical teaches you about how to grab employee emails and company subdomain information that is publicly available on the internet, using **theharvester** tool. This tool will look for the information about a given domain, in all differ platforms using different search engines.

**Prerequisites:** theharvester tool installed in your system

**Step 1:** This tool is to gather emails, subdomains, hosts, employee names, open ports and banners from different public sources like Google, Bing and other search engines.

```
┌─[user@parrot-virtual]─[~]
└──╼ $theHarvester -d gmail.com -l 1000 -b bing
table results already exists

*******************************************************************
*                                                                 *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __ *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|     *
*                                                                 *
* theHarvester 3.1.0                                          *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************


[*] Target: gmail.com

[*] Searching Bing.
        Searching 0 results.

[*] No IPs found.

[*] Emails found: 107
----------------------
1st16star@gmail.com
20200907145718.120980-1-luca.boccassi@gmail.com
```

```
[*] Emails found: 107
---------------------
1st16star@gmail.com
20200907145718.120980-1-luca.boccassi@gmail.com
aaron.monrroy@gmail.com
acronpharma@gmail.com
acronpharmaceutical@gmail.com
acronpharmaceuticals@gmail.com
adhemas@gmail.com
aibe.bci@gmail.com
akhlesh.agarwal@gmail.com
allaboutdogscr@gmail.com
anjouvt@gmail.com
anyreva7@gmail.com
atechindia@gmail.com
austmedia@gmail.com
aypearl@gmail.com
bernesepuppies@gmail.com
bobhightree@gmail.com
bramopsteeg@gmail.com
bright.scientifics@gmail.com
brucatofis@gmail.com
campoverlook@gmail.com
caroldiva@gmail.com
cirp.universal@gmail.com
coryaulrich@gmail.com
cpotto@gmail.com
cps.rudrapur@gmail.com
```

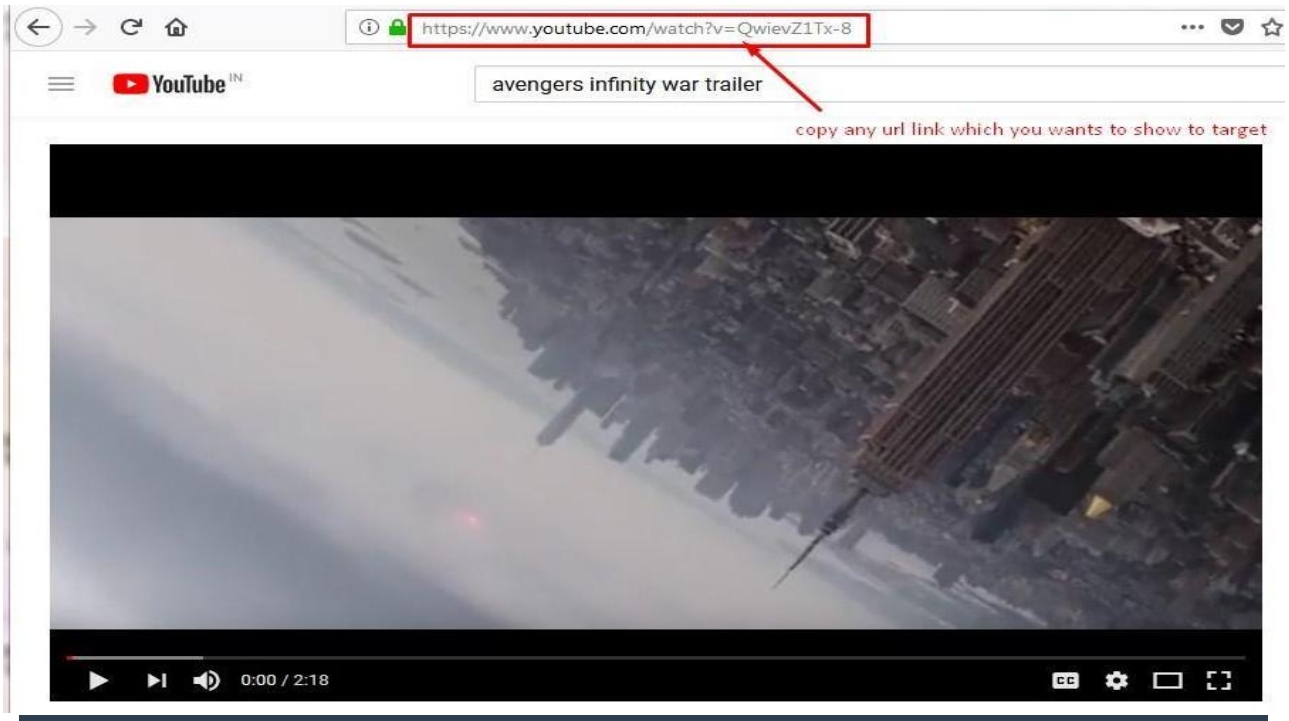
```
[*] Hosts found: 4
---------------------
imap.gmail.com:74.125.200.108, 74.125.200.109
pop.gmail.com:172.217.194.109, 172.217.194.108
smtp.gmail.com:74.125.24.109
www.gmail.com:172.217.163.37
┌─[user@parrot-virtual]─[~]
└──╼ $
```

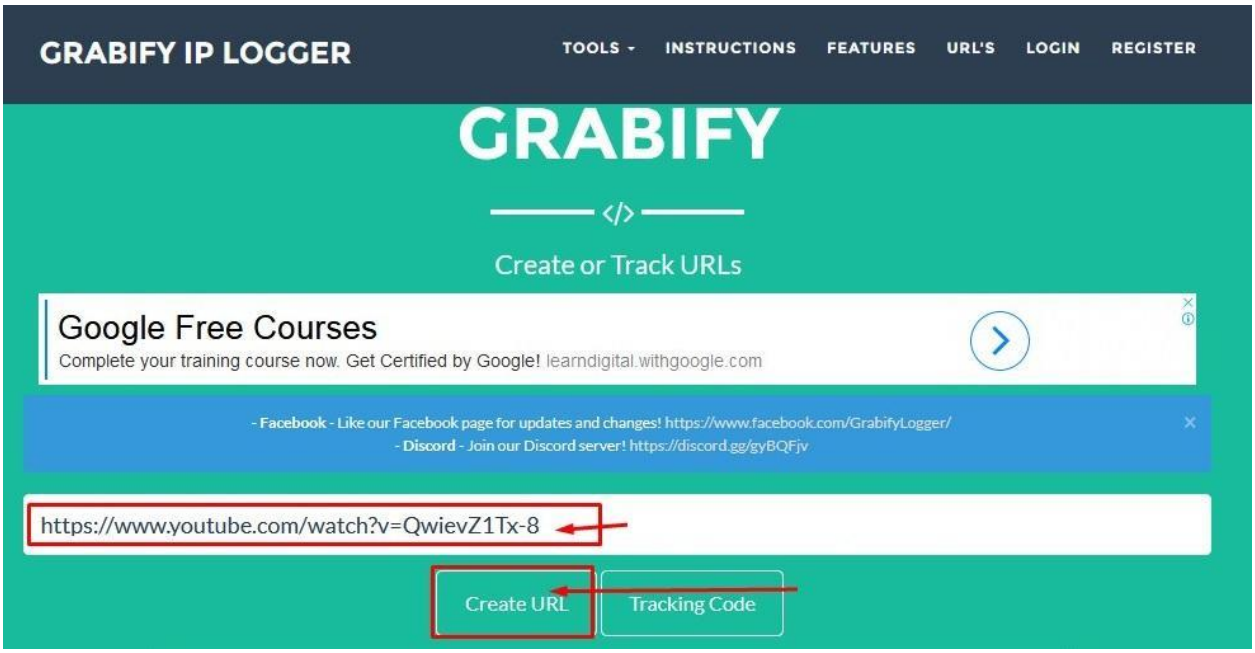
# Practical 3: To find out targets IP address using IP tracking technique.

**Description:** In this practical we will discuss how to convert normal URL (any web link) into trackable, sharing that URL to the target and getting the target information once he clicks that link. That information includes his public IP address, which device he used to open the link, OS and browser details, ISP location etc.

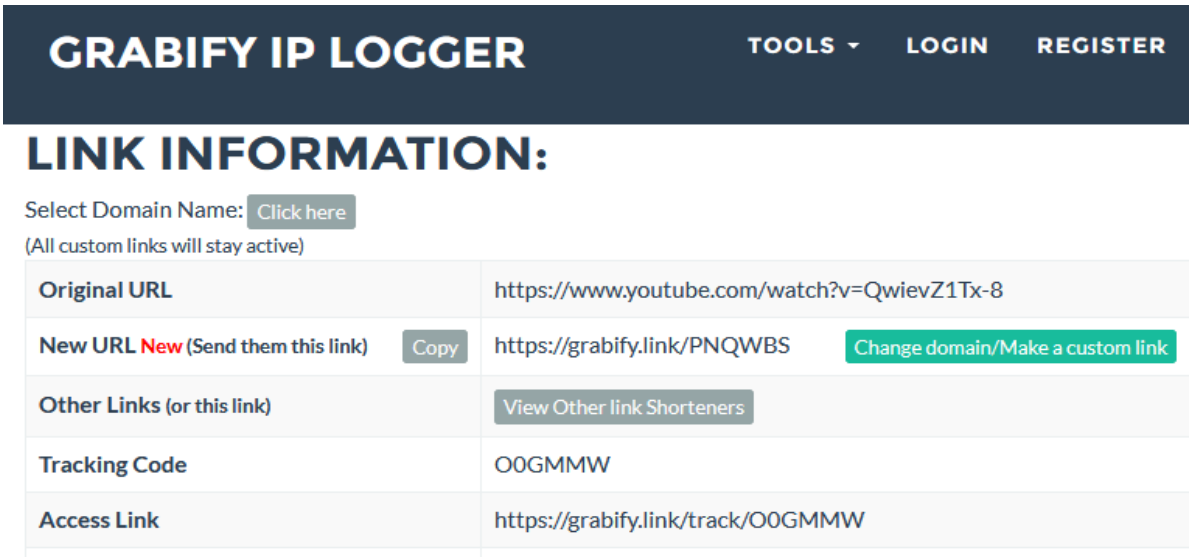
**Step 1:** Visit Grabify IP logging website https://grabify.link/

- This website creates a tracking link which helps in identifying targets IP address. To perform this task, we are trying to convince our target to click on it tracking link that redirects target towards a YouTube video. Create an IP tracking link by using Grabify website; it requires valid URL (In this case we are converting YouTube video link as an IP tracking link)

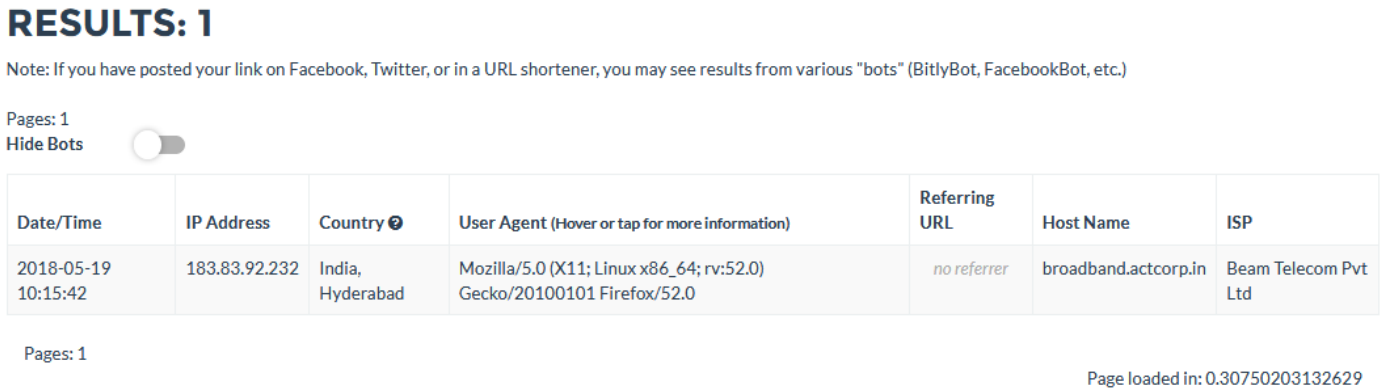


**Step 2:** After clicking on **Create URL** button, the website generates IP tracking URL displayed in **New URL section**, which you can share with a target to grab IP address.




**Step 3:** If the target clicks on the link, the target's IP address will be displayed on the same page as shown below



# Practical 4: Footprinting domain using Recon-ng tool

**Description:** In this practical we will learn how to gather information using the Recon-ng tool. This tool has different inbuilt modules. We can use those modules as per our requirements that means what type of information we want to gather and using which search engine etc.

**Prerequisites:** Recon-ng tool installed in your system.

**Step 1:** To launch the recon-ng tool, execute the following command in terminal

```
┌─[user@parrot-virtual]─[~]
└──╼ $recon-ng
```

**Step 2:** by default, recon-ng comes with no module installed, so to install modules execute **marketplace install all** command.

```
                                        /\
                                       / \\ /\
    Sponsored by...                  /\  /\/  \\V  \/\
                                    / \\/ // \\\\\ \\ \/\
                                   // // BLACK HILLS \/ \\
                                  www.blackhillsinfosec.com

                 ____   ____   ____   ____ _____ _  ____   ____  ____
                |____] |___/ |____| |      |   | |____  |____ |
                |      |   \_ |    | |____  |   |  ____| |____ |____
                                    www.practisec.com

                        [recon-ng v5.1.1, Tim Tomes (@lanmaster53)]

[*] No modules enabled/installed.

[recon-ng][default] > marketplace install all
[*] Module installed: discovery/info_disclosure/cache_snoop
[*] Module installed: discovery/info_disclosure/interesting_files
[*] Module installed: exploitation/injection/command_injector
[*] Module installed: exploitation/injection/xpath_bruter
[*] Module installed: import/csv_file
[*] Module installed: import/list
[*] Module installed: import/masscan
[*] Module installed: import/nmap
[*] Module installed: recon/companies-contacts/bing_linkedin_cache
[*] Module installed: recon/companies-contacts/censys_email_address
[*] Module installed: recon/companies-contacts/pen
[*] Module installed: recon/companies-domains/censys_subdomains
```

**Step 2:** Execute the **marketplace search** command, to list out the modules.

```
[recon-ng][default] > marketplace search

  +-------------------------------------------------------------------------------------------+
  |                          Path                          | Version |     Status    |  Updated   | D | K |
  +-------------------------------------------------------------------------------------------+
  | dev/spyse_subdomains                                   | 1.0     | not installed | 2020-07-07 |   | * |
  | discovery/info_disclosure/cache_snoop                  | 1.0     | installed     | 2019-06-24 |   |   |
  | discovery/info_disclosure/interesting_files            | 1.1     | installed     | 2020-01-13 |   |   |
  | exploitation/injection/command_injector                | 1.0     | installed     | 2019-06-24 |   |   |
  | exploitation/injection/xpath_bruter                    | 1.2     | installed     | 2019-10-08 |   |   |
  | import/csv_file                                        | 1.1     | installed     | 2019-08-09 |   |   |
```

```
| recon/domains-contacts/pgp_search                | 1.4  | installed  | 2019-10-16 |   |   |
| recon/domains-contacts/whois_pocs                | 1.0  | installed  | 2019-06-24 |   |   |
| recon/domains-contacts/wikileaker                | 1.0  | installed  | 2020-04-08 |   |   |
| recon/domains-credentials/pwnedlist/account_creds | 1.0  | installed  | 2019-06-24 | * | * |
| recon/domains-credentials/pwnedlist/api_usage    | 1.0  | installed  | 2019-06-24 |   | * |
| recon/domains-credentials/pwnedlist/domain_creds | 1.0  | installed  | 2019-06-24 | * | * |
| recon/domains-credentials/pwnedlist/domain_ispwned | 1.0  | installed  | 2019-06-24 |   | * |
| recon/domains-credentials/pwnedlist/leak_lookup  | 1.0  | installed  | 2019-06-24 |   |   |
| recon/domains-credentials/pwnedlist/leaks_dump   | 1.0  | installed  | 2019-06-24 |   | * |
| recon/domains-credentials/scylla                 | 1.3  | installed  | 2020-09-25 |   |   |
| recon/domains-domains/brute_suffix               | 1.1  | installed  | 2020-05-17 |   |   |
| recon/domains-hosts/binaryedge                   | 1.2  | installed  | 2020-06-18 |   | * |
| recon/domains-hosts/bing_domain_api              | 1.0  | installed  | 2019-06-24 |   | * |
| recon/domains-hosts/bing_domain_web              | 1.1  | installed  | 2019-07-04 |   |   |
| recon/domains-hosts/brute_hosts                  | 1.0  | installed  | 2019-06-24 |   |   |
| recon/domains-hosts/builtwith                    | 1.0  | installed  | 2019-06-24 |   | * |
| recon/domains-hosts/censys_domain                | 1.0  | disabled   | 2019-08-22 |   | * |
| recon/domains-hosts/certificate_transparency     | 1.2  | installed  | 2019-09-16 |   |   |
| recon/domains-hosts/google_site_web              | 1.0  | installed  | 2019-06-24 |   |   |
| recon/domains-hosts/hackertarget                 | 1.1  | installed  | 2020-05-17 |   |   |
| recon/domains-hosts/mx_spf_ip                    | 1.0  | installed  | 2019-06-24 |   |   |
| recon/domains-hosts/netcraft                     | 1.1  | installed  | 2020-02-05 |   |   |
```

**Step 3:** To use a module, Execute the following command **modules load <module name>**

```
[recon-ng][default] > modules load recon/domains-hosts/bing_domain_web
[recon-ng][default][bing_domain_web] >
```

**Step 4:** Execute the **options list** command, to view the list of options.

```
[recon-ng][default][bing_domain_web] > options list

  Name    Current Value  Required  Description
  ------  -------------  --------  -----------
  SOURCE  default        yes       source of input (see 'info' for details)

[recon-ng][default][bing_domain_web] >
```

**Step 5:** Execute **options set SOURCE <domain name>** command, to set the domain address as a source

- Example: **options set SOURCE hackthissite.org**

```
[recon-ng][default][bing_domain_web] > options set SOURCE hackthissite.org
SOURCE => hackthissite.org
[recon-ng][default][bing_domain_web] > options list

  Name    Current Value     Required  Description
  ------  -------------     --------  -----------
  SOURCE  hackthissite.org  yes       source of input (see 'info' for details)

[recon-ng][default][bing_domain_web] >
```

**Step 6:** Execute the **run** command, to start the search for domains

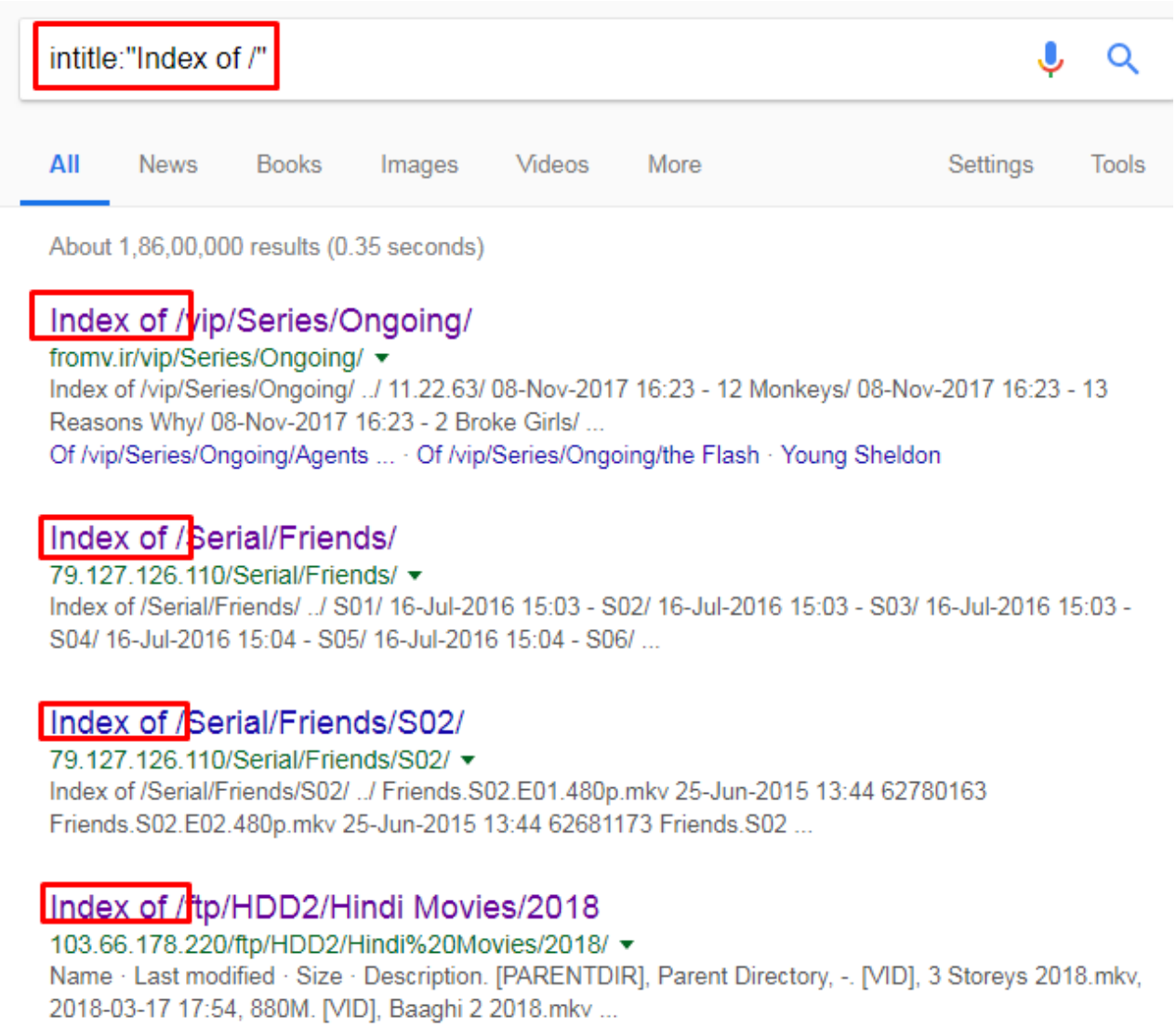
```
[recon-ng][default][bing_domain_web] > run

----------------
HACKTHISSITE.ORG
----------------
[*] URL: https://www.bing.com/search?first=0&q=domain%3Ahackthissite.org
[*] Country: None
[*] Host: legal.hackthissite.org
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------------
[*] Country: None
[*] Host: www.irc.hackthissite.org
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------------
[*] Country: None
[*] Host: pi.hackthissite.org
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
```

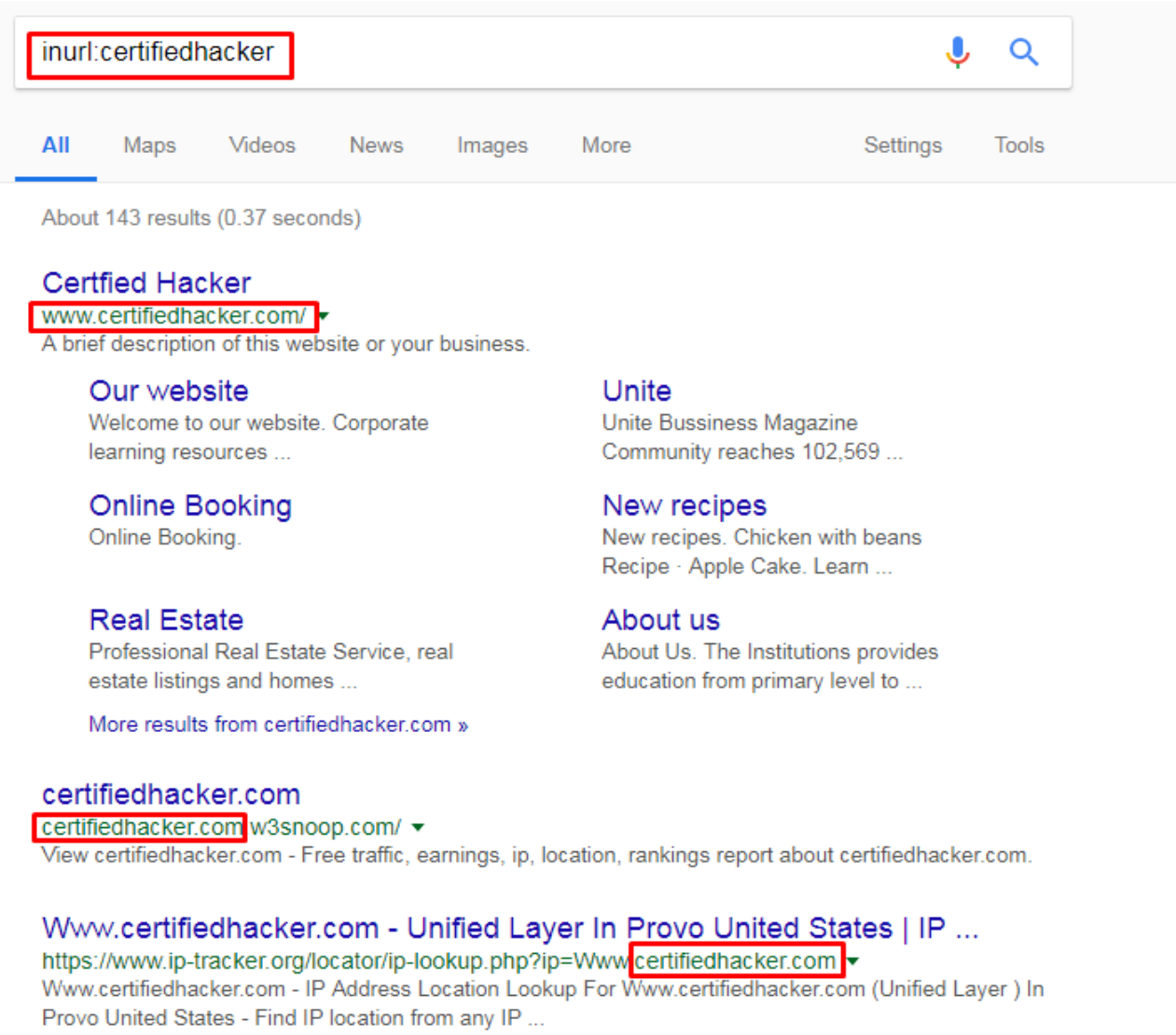
# Practical 5: Google Dorks

**Description:** In this practical we will learn how to optimize google search results, by eliminating unnecessary results. Based on what kind of information we require (like file formats and information related to particular domain etc,) We use those search operators to get optimized results. By using the techniques, we will be able to gather some sensitive information that is not protected properly.

**Operator 1:** If you search for **intitle:"Index of/"** on google search bar, it will display those pages that contain the term "Index of/" in the title of the website.

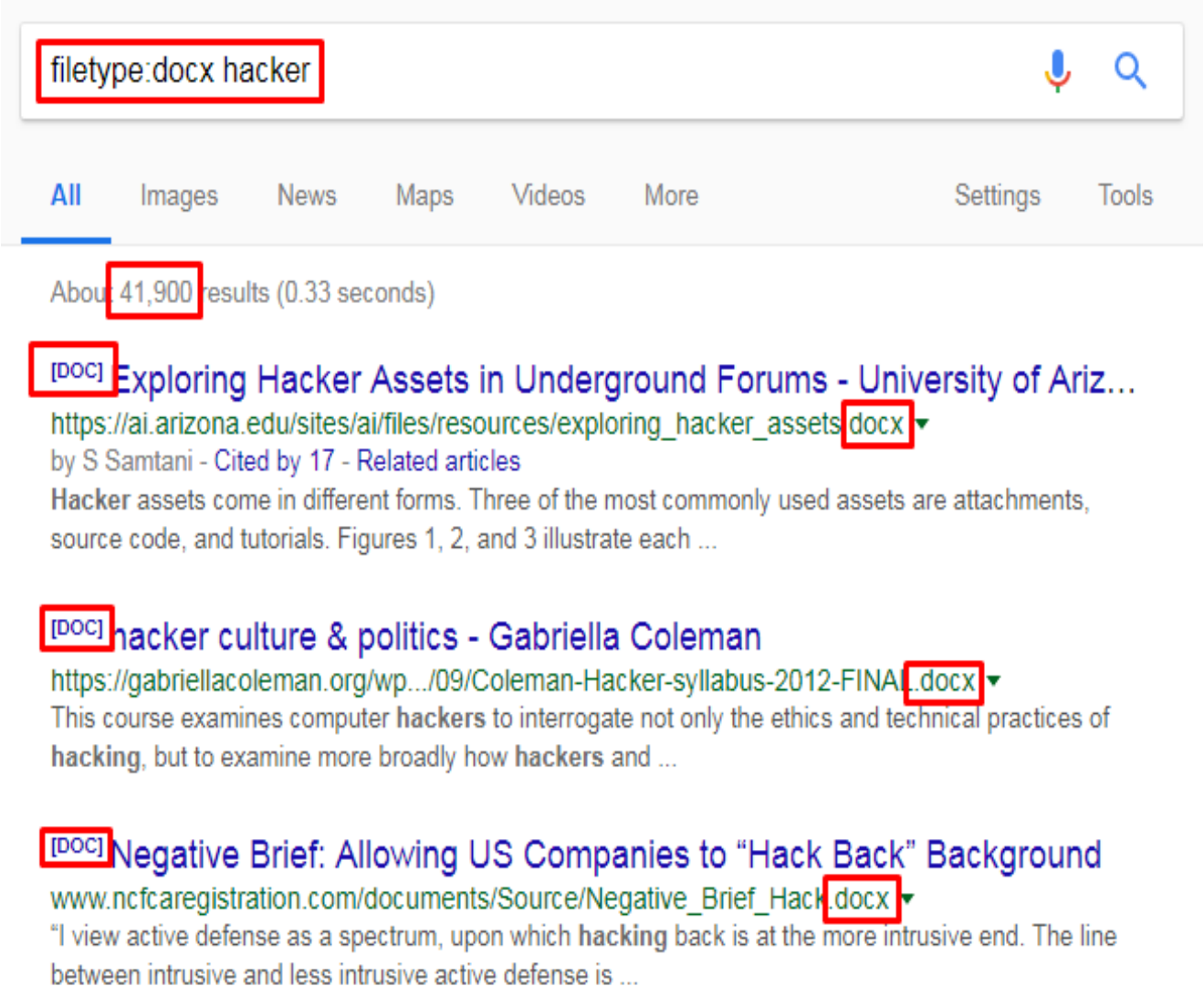


**Operator 2: inurl: certifiedhacker** will result in displaying those pages that contain the term "certifiedhacker" in the URL.

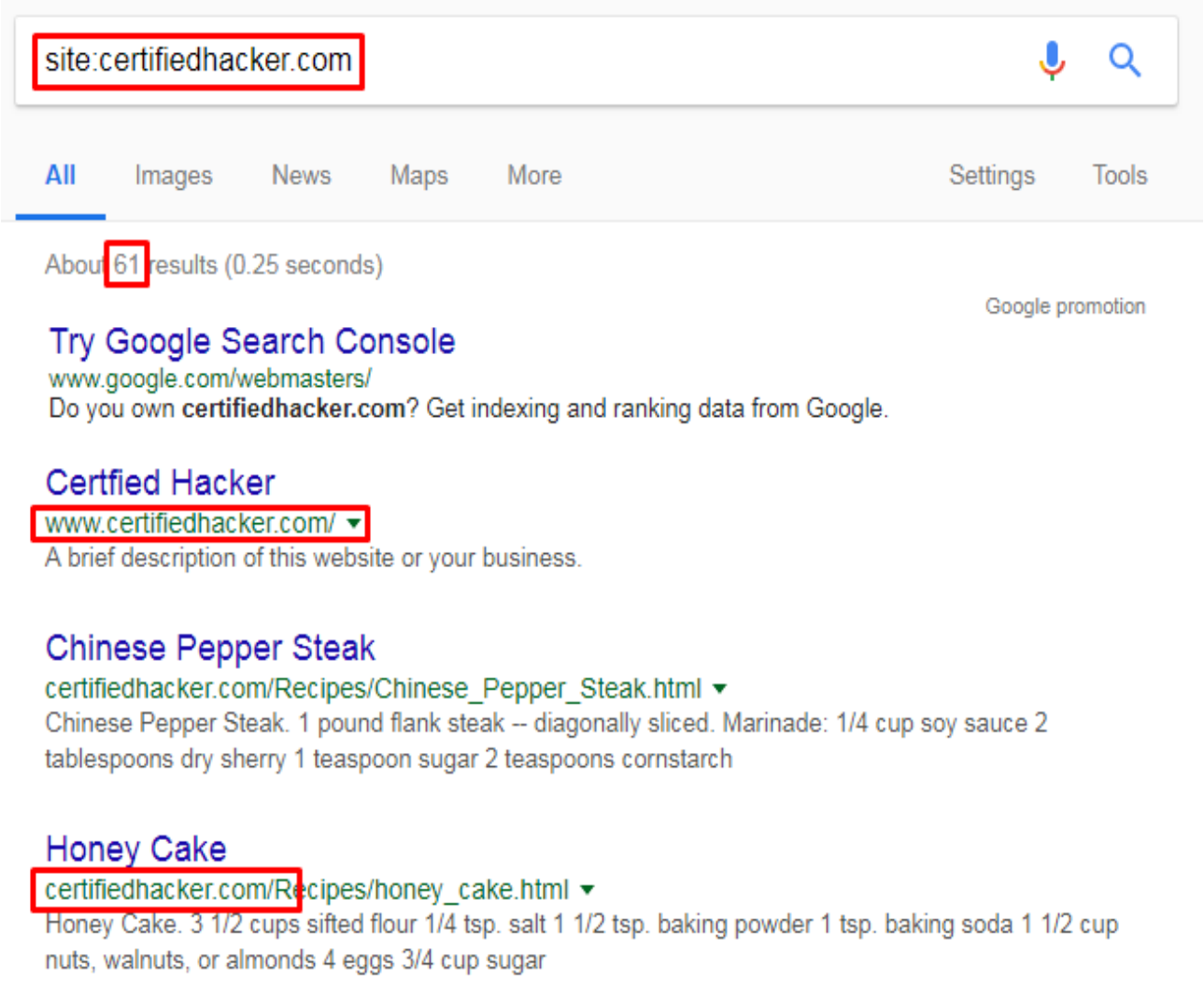


**Operator 3:** To find out files of a specific format, we can use **filetype:** followed by file type (pdf, docx, xlsx) and keyword.

- For example, **filetype:docx hacker** will display all word documents that contain word hacker.



**Operator 4: site: certifiedhacker.com** will display the results that contain the term "certifiedhacker" in the website URL.




**Operator 5: allintitle: trojan definition** will return results that contain words trojan and definition in web page titles.

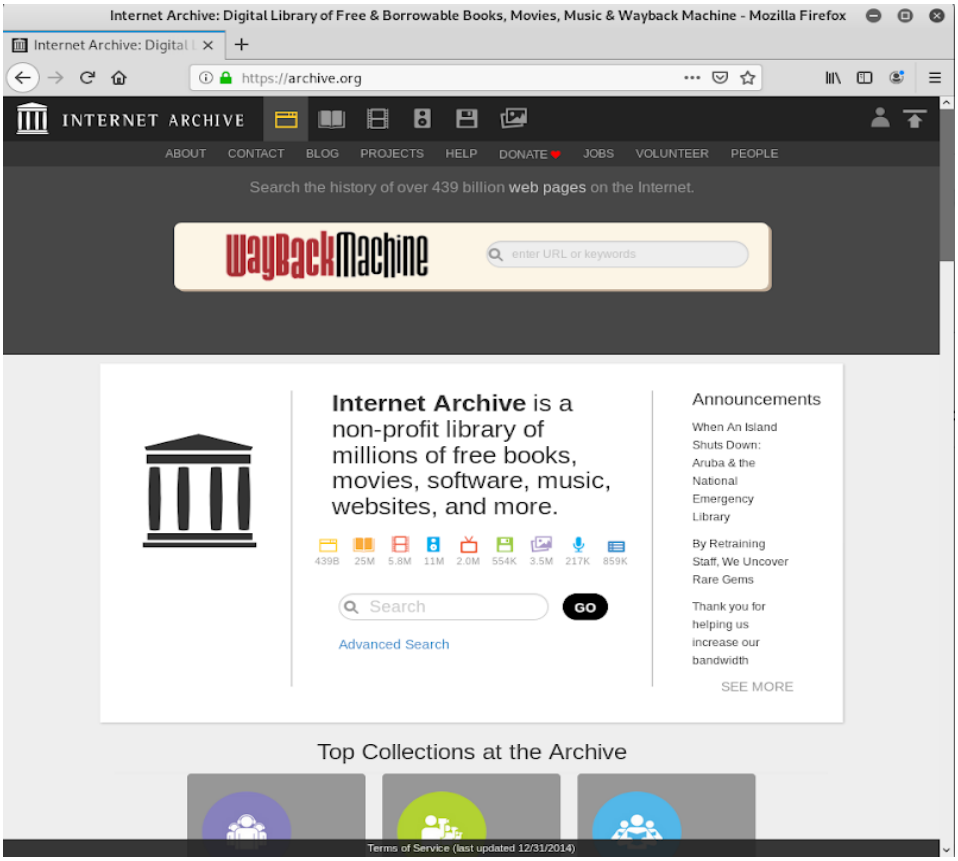
**Refer following web pages for advanced Google operators**

- http://www.googleguide.com/advanced_operators_reference.html
- http://www.exploit-db.com

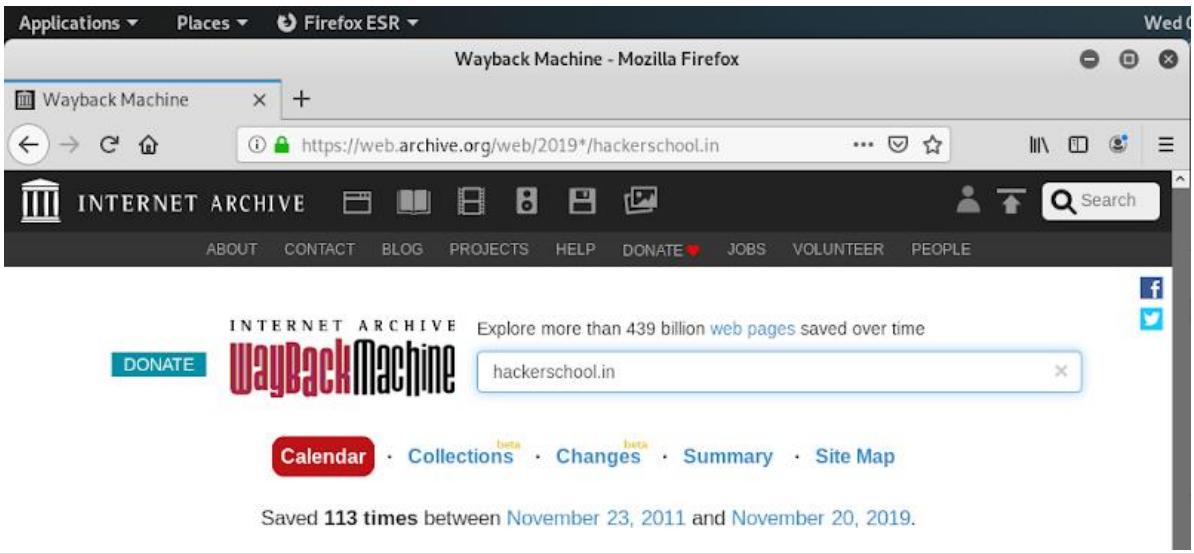
# Practical 6: Gathering information using Archive.org

**Description:** In this practical we will learn how to check if there is any sensitive information available on previous versions of organizations' website, that is not available on the latest version of websites.

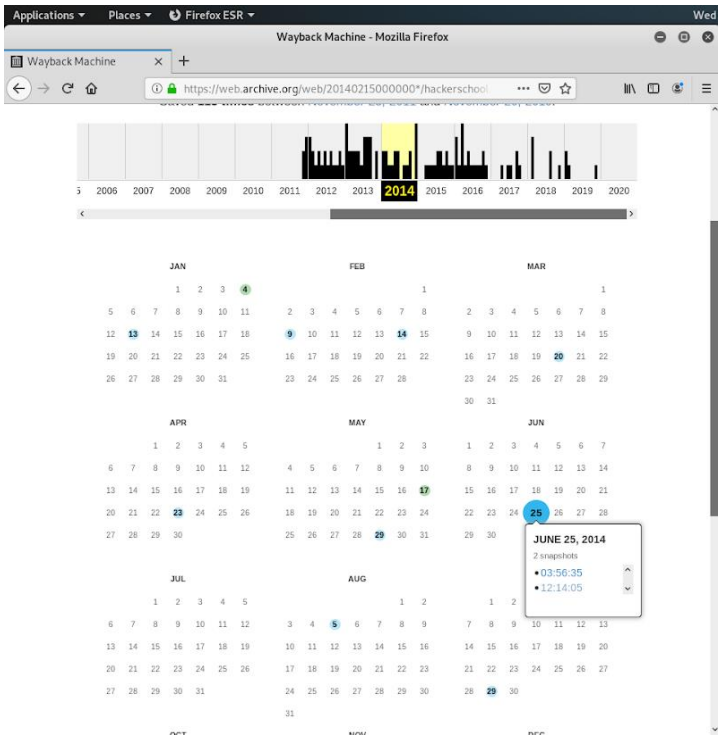
**Step 1: Archive.org** is an internet way back machine, where they keep backups of several websites on different dates. Open the web browser and enter **archive.org** in the URL section to visit the internet archive way back Machine.



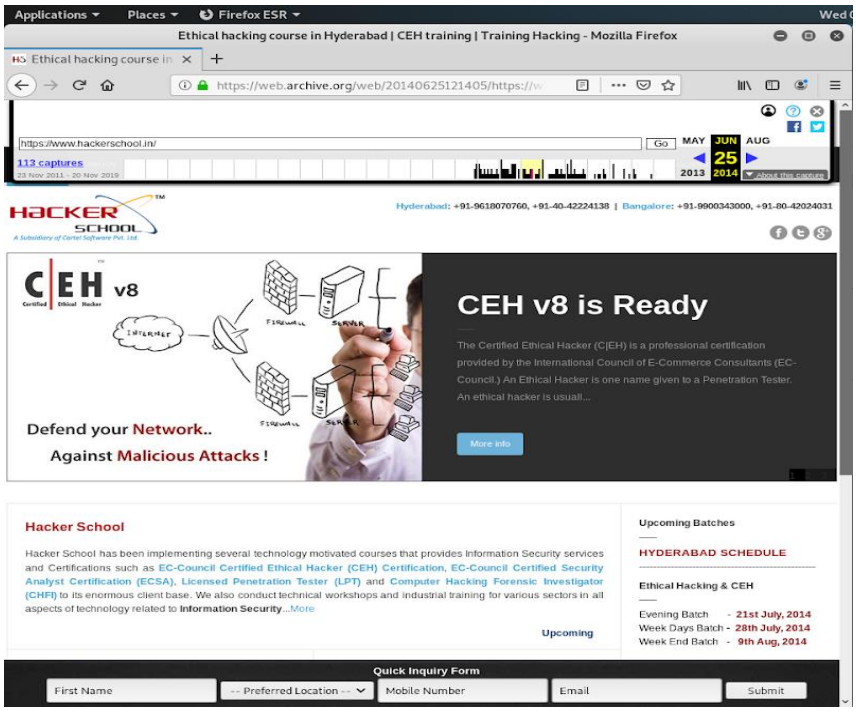

**Step 2:** In the search bar enter the website URL, which you want to see old versions of.



**Step 3:** Now it will show site backup details on year wise. Select which year we want to check the site information and then it will show that year's calendar. Select highlighted coloured circles on those dates they have taken the site backup. If we place mouse cursor on that date it will show us the time.




**Step 4:** In the above image we can see in the year 2014, when we place cursor on jun25, it is shown different timings when they made backup of HackerSchool site. Now select the time it will show us how exactly the site is and what information it has at that time.

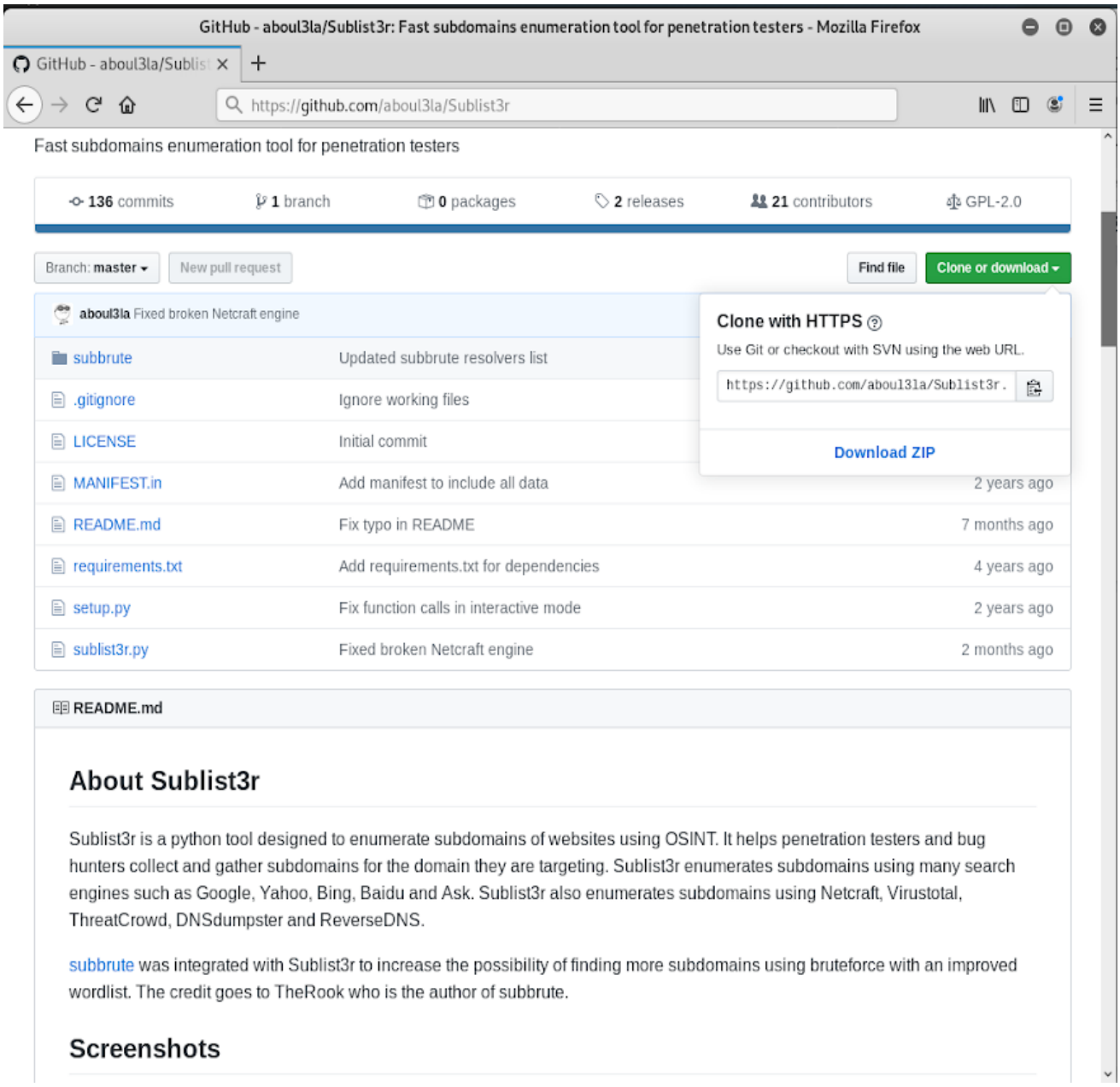



- This site will back up the entire website, so we can see different sections of the old target site and can check if any sensitive or useful information is available.

# Practical 7: Subdomain enumeration using Sublist3r tool

**Description:** In this practical we will learn how to clone the sublist3r tool from GitHub and how to enumerate subdomains of target websites using the sublist3r tool.

**Step 1:** Sublist3r is a python based open source tool we can clone from the GitHub site. Visit https://github.com/aboul3la/Sublist3r in the browser. Click on the green colour **clone or download** button, it will show us a link that we can use to clone the tool.



**Step 2:** To clone use the below command in the terminal.

- git clone https://github.com/aboul3la/Sublist3r.git

```
┌─[user@parrot-virtual]─[~/Documents]
└──╼ $git clone https://github.com/aboul3la/Sublist3r.git
Cloning into 'Sublist3r'...
remote: Enumerating objects: 383, done.
remote: Total 383 (delta 0), reused 0 (delta 0), pack-reused 383
Receiving objects: 100% (383/383), 1.12 MiB | 718.00 KiB/s, done.
Resolving deltas: 100% (213/213), done.
┌─[user@parrot-virtual]─[~/Documents]
└──╼ $ls
Sublist3r
```

**Step 3:** The above executed command will create a sublist3r directory. Navigate into the directory and check the files. We will see the sublist3r.py file.

```
┌─[user@parrot-virtual]─[~/Documents]
└──╼ $cd Sublist3r/
┌─[user@parrot-virtual]─[~/Documents/Sublist3r]
└──╼ $ls
LICENSE  MANIFEST.in  README.md  requirements.txt  setup.py  subbrute  sublist3r.py
```

**Step 4:** Execute the following command in terminal to see the help menu of the sublist3r tool.

- **Command**: python3 sublist3r --help

```
┌─[user@parrot-virtual]─[~/Documents/Sublist3r]
└──╼ $python3 sublist3r.py --help
usage: sublist3r.py [-h] -d DOMAIN [-b [BRUTEFORCE]] [-p PORTS] [-v [VERBOSE]] [-t THREADS] [-e ENGINES]
                    [-o OUTPUT] [-n]

OPTIONS:
  -h, --help            show this help message and exit
  -d DOMAIN, --domain DOMAIN
                        Domain name to enumerate it's subdomains
  -b [BRUTEFORCE], --bruteforce [BRUTEFORCE]
                        Enable the subbrute bruteforce module
  -p PORTS, --ports PORTS
                        Scan the found subdomains against specified tcp ports
  -v [VERBOSE], --verbose [VERBOSE]
                        Enable Verbosity and display results in realtime
  -t THREADS, --threads THREADS
                        Number of threads to use for subbrute bruteforce
  -e ENGINES, --engines ENGINES
                        Specify a comma-separated list of search engines
  -o OUTPUT, --output OUTPUT
                        Save the results to text file
  -n, --no-color        Output without color

Example: python sublist3r.py -d google.com
```

**Step 5:** Use the below command to enumerate the subdomains using the sublist3r tool.

- **Syntax:** Python3 sublist3r -d <target domain>
- **Command:** python3 sublist3r -d hackthissite.org

```
┌─[user@parrot-virtual]─[~/Documents/Sublist3r]
└──╼ $python3 sublist3r.py -d hackthissite.org

                 ____        _      _ _     _   _____
                / ___| _   _| |__  | (_)___| |_|___ / _ __
                \___ \| | | | '_ \| | / __| __| |_ \| '__|
                 ___) | |_| | |_) | | \__ \ |_ ___) | |
                |____/ \__,_|_.__/|_|_|___/\__|____/|_|

                # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for hackthissite.org
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
```

```
[-] Total Unique Subdomains Found: 49
www.hackthissite.org
admin.hackthissite.org
api.hackthissite.org
ctf.hackthissite.org
daemon.hackthissite.org
dns.hackthissite.org
vm-005.outbound.firewall.hackthissite.org
vm-050.outbound.firewall.hackthissite.org
vm-099.outbound.firewall.hackthissite.org
vm-150.outbound.firewall.hackthissite.org
vm-200.outbound.firewall.hackthissite.org
forum.hackthissite.org
forums.hackthissite.org
git.hackthissite.org
htsv4.hackthissite.org
irc.hackthissite.org
www.irc.hackthissite.org
lille.irc.hackthissite.org
wolf.irc.hackthissite.org
irc-ipv6.hackthissite.org
irc-v6.hackthissite.org
lille.irc-v6.hackthissite.org
wolf.irc-v6.hackthissite.org
irc-wolf.hackthissite.org
irc-www.hackthissite.org
jupiter.hackthissite.org
kage.hackthissite.org
legal.hackthissite.org
mail.hackthissite.org
mirror.hackthissite.org
```

- Like this we can enumerate subdomains of different websites using the sublist3r tool.