

Day 2 Assignment

INFORMATION GATHERING

1. Google Dorking:

Google

S

inurl:login site:google.com intext:passw

All

Images

News

Videos

Maps

Shopping

தமிழில் தேடுங்கள்

Q

லோகின் பச்சுலோர்து

https://support.google.com · thread

Forgot login password - Google Classroom Community

11-Oct-2019 — Hello! Welcome to the Google for Education forum! Usually, your Google login credentials would be the same credentials you need to login to ...

People also search for

Q

Onlinesbi login

Q

SBI login password reset

Q

SBI online password reset using ATM card details

Q

www.onlinesbi.com forgot username and password

http://feedproxy.google.com · ...

How To Reset Login Password Of OnlineSBI With ATM Card Details

12-Dec-2017 — State Bank of India (SBI) offers an easy way for its customers to reset their login ID and password.

https://support.google.com · thread

Strange login/password info saved in my passwords section - Google Support

30-Oct-2019 — My ex from 6 years ago, somehow has a login/password saved on my account. This is from 6 years ago, and there is no other password/login ...

https://support.google.com · thread

How do I recover my old login password for the website XNXX - Google Support

22-Aug-2020 · 1 answer
Garry. Google cannot help with third party apps, devices, or websites. Google would have no idea at all how these work, their sign in ...

https://support.google.com · answer

Gmail remembers my login email and password - Android - Legal Help

Gmail remembers my login email and password. If you're signed in to your mobile device with your Google Account, you're signed in automatically to the Gmail ...

http://feedproxy.google.com · it...

SBI Internet Banking: How To Change Login, Profile Passwords Of SBI Accounts

12-Dec-2017 — If one has an internet banking login id and password, he/she can easily avail a slew of services like making transactions, applying for new ...

https://cloud.google.com · reference

gcloud auth application-default login | Cloud SDK Documentation

Overview · create · delete · list · set-password · gcloud survey, gcloud tasks. Overview · create-app-engine-task · create-http-task · delete · describe ...

2. Google Hacking Database:



Google Hacking Database

Filters

Reset All

Show 15

Quick Search

Dork Category Author

intitle:"geovision inc." inurl:login.htm	Pages Containing Login Portals	s Thakur
intitle:"7100 login" "lancom"	Various Online Devices	s Thakur
intitle:"vigor login page"	Pages Containing Login Portals	s Thakur
intitle:"ADB Broadband" login intext:"ADB Broadband S.p.A" -.com	Pages Containing Login Portals	s Thakur
intitle:"Login - Hitron technologies"	Pages Containing Login Portals	s Thakur
intitle:"DGS-3100 Login"	Pages Containing Login Portals	s Thakur
intitle:"lg smart ip device" -.com	Various Online Devices	s Thakur
intitle:"3G wireless gateway" "login" intext:"huawei technologies"	Pages Containing Login Portals	s Thakur
intitle:"ADMINISTRATO	Pages	

3. Funding emails using hunter.io



microsoft.com

Search

{last}{f}@microsoft.com

m llers@microsoft.com

3 sources ▾

t ben.andersen@microsoft....

5 sources ▾

n duan@microsoft.com

13 sources ▾

c rvo@microsoft.com

19 sources ▾

i ra@microsoft.com

8 sources ▾

34,267 more results for "microsoft.com"

Sign up to uncover the email addresses, get the full results, search filters, CSV downloads and more. Get 25 free searches/month.

[Create a free account](#)

Hunter is used by 2,000,000+ professionals
and chosen by leading companies.

Google

IBM

Manpower

Microsoft

Adobe

invision

4. Who is lookup:

WHOIS Search Results:

Domain Name: microsoft.com
Registry Domain ID: 2724960_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: <http://www.markmonitor.com>
Updated Date: 2021-04-07T12:58:15-0700
Creation Date: 1991-05-01T21:00:00-0700
Registrar Registration Expiration Date: 2022-05-02T00:00:00-0700
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895770
Domain Status: clientUpdateProhibited
(<https://www.icann.org/epp#clientUpdateProhibited>)
Domain Status: clientTransferProhibited
(<https://www.icann.org/epp#clientTransferProhibited>)
Domain Status: clientDeleteProhibited
(<https://www.icann.org/epp#clientDeleteProhibited>)
Domain Status: serverUpdateProhibited
(<https://www.icann.org/epp#serverUpdateProhibited>)
Domain Status: serverTransferProhibited
(<https://www.icann.org/epp#serverTransferProhibited>)
Domain Status: serverDeleteProhibited
(<https://www.icann.org/epp#serverDeleteProhibited>)
Registry Registrant ID:
Registrant Name: Domain Administrator
Registrant Organization: Microsoft Corporation
Registrant Street: One Microsoft Way,
Registrant City: Redmond
Registrant State/Province: WA
Registrant Postal Code: 98052
Registrant Country: US
Registrant Phone: +1.4258828060
Registrant Phone Ext:
Registrant Fax: +1.4259367329
Registrant Fax Ext:
Registrant Email: admin@domains.microsoft
Registry Admin ID:
Admin Name: Domain Administrator
Admin Organization: Microsoft Corporation
Admin Street: One Microsoft Way,
Admin City: Redmond
Admin State/Province: WA
Admin Postal Code: 98052
Admin Country: US
Admin Phone: +1.4258828080
Admin Phone Ext:
Admin Fax: +1.4259367329
Admin Fax Ext:
Admin Email: admin@domains.microsoft
Registry Tech ID:
Tech Name: MSN Hostmaster
Tech Organization: Microsoft Corporation
Tech Street: One Microsoft Way,
Tech City: Redmond
Tech State/Province: WA
Tech Postal Code: 98052
Tech Country: US
Tech Phone: +1.4258828080
Tech Phone Ext:
Tech Fax: +1.4259367329
Tech Fax Ext:
Tech Email: msnhst@microsoft.com
Name Server: ns2-205.azure-dns.net
Name Server: ns4-205.azure-dns.info
Name Server: ns3-205.azure-dns.org
Name Server: ns1-205.azure-dns.com
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting

5. Website technology using wappalyzer:

Tesla.com

Website technology lookup

Website URL, technology, keyword or 

Technology stack

CMS

 Drupal


Development

 Emotion

Programming languages

 PHP 7.4.16

Maps

 Google Maps

Reverse proxies

 Nginx

Caching

 Varnish

Payment processors

 Adyen

Web servers

 Nginx

JavaScript frameworks

 Handlebars

 Emotion

A/B Testing

 Google Optimize

Font scripts

 Google Font API

Miscellaneous

 webpack

 Babel

Tag managers

 Google Tag Manager

Analytics

 Google Analytics

6. Profil3r :

Example:

```
$ ~ python3 profil3r.py username

  _____
 /  _  _  _  \
|  _ \| | | | | | |
| |_) | | | | |
|  _ \| | | | |
|_| \_|_|_|_|_|

Version 1.1.3 - Devellopped by Rog3rSm1th
You can buy me a coffee at : https://www.buymeacoffee.com/givocefo

● Select services (<up>, <down> to move, <space> to select, <a> to toggle, <i> to invert)
EMAIL
● email
ENTERTAINMENT
> ◯ dailymotion
FORUM
◯ 0x00sec
◯ jeuxvideo.com
MUSIC
◯ soundcloud
PROGRAMMING
◯ github
◯ pastebin
SOCIAL
● facebook
◯ instagram
◯ tiktok
● twitter
TCHAT
◯ skype
```

```
$ ~ python3 profil3r.py username
```



Version 1.1.3 - Developed by Rog3rSm1th

You can buy me a coffee at : <https://www.buymeacoffee.com/givocefo>

• Select services **done (4 selections)**

Profil3r will search :

- [+] email
- [+] facebook
- [+] pastebin
- [+] twitter

└─ EMAIL ✓

└─username@gmail.com	[SAFE]
└─username@yahoo.com	[BREACHED]
└─username@hotmail.com	[BREACHED]

└─ FACEBOOK ✓

└─<https://facebook.com/username>

└─ PASTEBIN ✓

└─<https://pastebin.com/u/username>

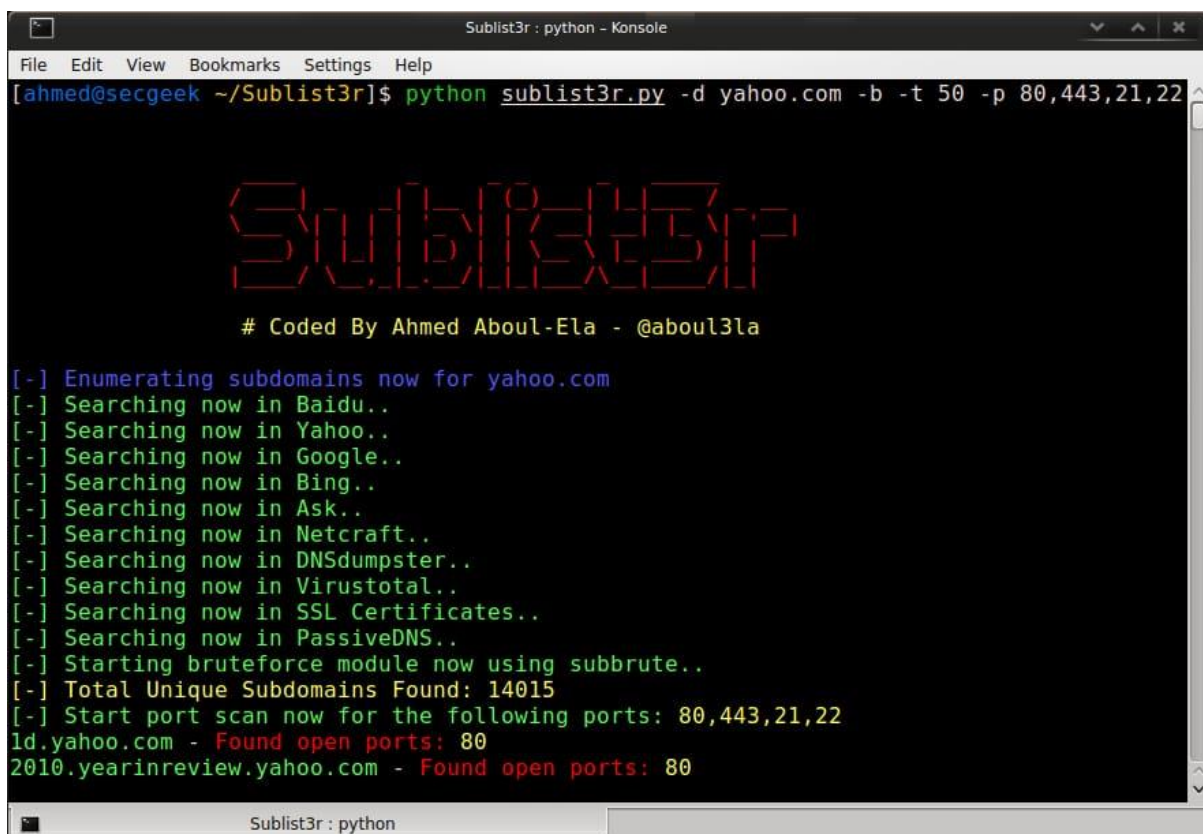
└─ TWITTER ✗(No results)

[+] Report was generated in ./reports/username.json

\$ - █

7.sublis3r :

Example:



```
Sublist3r : python - Konsole
File Edit View Bookmarks Settings Help
[ahmed@secgeek ~/Sublist3r]$ python sublist3r.py -d yahoo.com -b -t 50 -p 80,443,21,22

  Sublist3r

# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for yahoo.com
[-] 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 SSL Certificates..
[-] Searching now in PassiveDNS..
[-] Starting bruteforce module now using subbrute..
[-] Total Unique Subdomains Found: 14015
[-] Start port scan now for the following ports: 80,443,21,22
1d.yahoo.com - Found open ports: 80
2010.yearinreview.yahoo.com - Found open ports: 80
```

SCANNING :

1.dirb : (looking for files)

Example:

```
root@kali:~# dirb http://webscantest.com/
```

```
-----  
DIRB v2.22  
By The Dark Raver  
-----
```

```
START_TIME: Mon Oct 30 08:05:15 2017  
URL_BASE: http://webscantest.com/  
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt  
  
-----
```

```
GENERATED WORDS: 4612
```

```
---- Scanning URL: http://webscantest.com/ ----  
==> DIRECTORY: http://webscantest.com/business/  
==> DIRECTORY: http://webscantest.com/cart/  
==> DIRECTORY: http://webscantest.com/css/  
+ http://webscantest.com/favicon.ico (CODE:200|SIZE:5430)  
==> DIRECTORY: http://webscantest.com/icons/  
==> DIRECTORY: http://webscantest.com/images/  
+ http://webscantest.com/index.php (CODE:200|SIZE:4346)  
==> DIRECTORY: http://webscantest.com/report/  
==> DIRECTORY: http://webscantest.com/rest/  
+ http://webscantest.com/robots.txt (CODE:200|SIZE:101)  
+ http://webscantest.com/server-status (CODE:403|SIZE:295)  
==> DIRECTORY: http://webscantest.com/soap/  
-----
```