## Day 2 Assignment

INFORMATION GATHERING

1.Google Dorking:

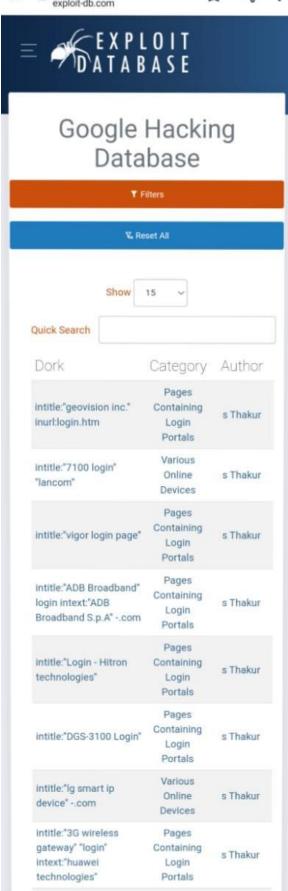


 $\label{eq:condition} Overview \cdot create \cdot delete \cdot list \cdot set-password \cdot gcloud survey, \\ gcloud tasks. Overview \cdot create-app-engine-task \cdot create-http-$ 

task · delete · describe ...

2.Google Hacking Database:

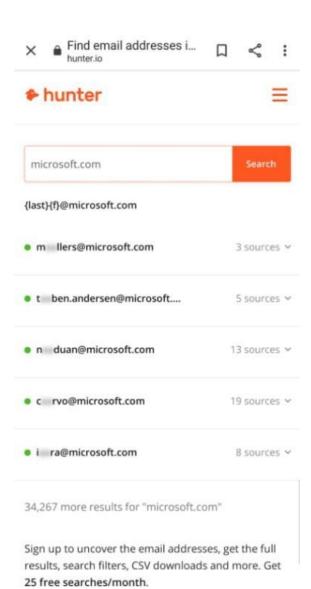




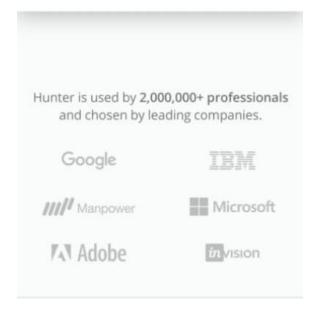
Pages

intitle: ADMINISTRATO

3. Funding emails using hunter.io



Create a free account



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: +1.4258828080

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

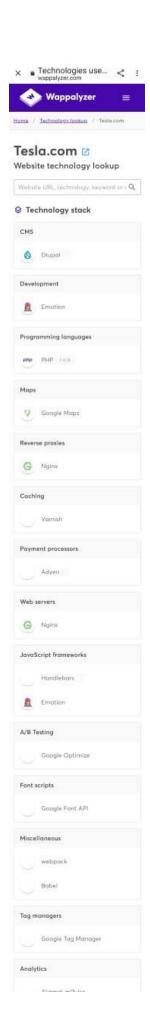
Name Server: ns4-205.azure-dns.info

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:



## 6. Profil3r:

Example:

```
$ ~ python3 profil3r.py username

Version 1.1.3 - Developped by Rog3rSmith
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
)o dailymotion
FORUM
• 0 9X00sec
• 0 jeuxvideo.com
MUSIC
• soundcloud
PROGRAMMING
• github
• pastebin
SOCIAL
• facebook
• instagram
• tikkok
• twitter
TCHAT
• skype
```

7.sublis3r:

Example:

```
Sublist3r : python - Konsole
 File Edit View Bookmarks Settings Help
[ahmed@secgeek ~/Sublist3r]$ python <u>sublist3r.py</u> -d yahoo.com -b -t 50 -p 80,443,21,22
                    # Coded By Ahmed Aboul-Ela - @aboul3la
 -] 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 ld.yahoo.com - Found open ports: 80
2010.yearinreview.yahoo.com
                     Sublist3r: python
```

## **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/
```