

Information Gathering

- مبدأيا عشان نت target لازم انك تجمع عنه كل المعلومات الكافية بالبلدي كده مينفعش اروح اسرق بيت منغير ماعرف هما كام فرد فالبيت وايه الحاجات اللي ممكن ادخل منها فا ده بالطبط اهمية تجميع المعلومات
- في عندنا طريقتين عشان نقدر نجمع معلومات عن ال target
- اول حاجه ان اجمع manually ودي مش محتاج شرح يعني مانيوال يعني بتدور انت بنفسك يعني بتخش تشوف انت الشركه اللي بتتارجيتها واعضاءها من خلال السيرش وطبعا اول ما نتكلم عن السيرش as a security يبقى بنتكلم عن Google Dork

Google Dorking

ال Google Dorking أو اللي بيتقال عليه كمان Google Hacking هو استخدام أوامر معينة في محرك بحث جوجل عشان تلاقي معلومات حساسة مش المفروض تبقى متاحة للعامة، زي ملفات الباسورد، الكاميرات، صفحات تسجيل دخول، معلومات السيرفر، ... إلخ.

- يعني مثلا انا عاوز ف محرك البحث يظهرلي كل النتائج عن موقع معين يبقى اكتب site:facebook مثلا بص كده الجدول ده

أهم Google Dorks Queries

نوع الاستخدام	Google Dork Query	الوظيفة
فهارس وملفات مفتوحة	intitle:"index of"	يعرض ملفات وفولدرات مكشوفة على الإنترنت
تسجيل الدخول	inurl:login	يعرض صفحات تسجيل الدخول
لوحة تحكم الادمن	inurl:admin	يعرض لوحات التحكم الخاصة بالمواقع
معلومات السيرفر	intitle:"phpinfo()"	يعرض صفحة فيها معلومات السيرفر الخاصة بـ PHP
كاميرات مراقبة	"camera" inurl:view.shtml	يعرض كاميرات مراقبة متاحة أونلاين بدون حماية
ملفات كلمات المرور	intext:"password"	يبحث عن كلمة "password" داخل صفحات الويب
قواعد بيانات	filetype:sql	يبحث عن ملفات SQL تحتوي على قواعد بيانات
ملفات لوج	filetype:log	يعرض ملفات Log ممكن تحتوي على معلومات حساسة
ملفات بيئة (env.)	filetype:env inurl:.env	يعرض ملفات env. اللي ممكن تحتوي على بيانات حساسة
phpMyAdmin	"phpmyadmin" "server at"	يعرض لوحات phpMyAdmin المكشوفة على الإنترنت
ملفات XML	ext:xml inurl:login	يعرض ملفات XML تحتوي على بيانات تسجيل دخول
البحث داخل موقع محدد	site:example.com	يعرض نتائج البحث داخل موقع معين فقط

- لازم تحل لابات علي THM عن ال google dorking عشان skill مهمه جدا
-تاني حاجه بقي وهي تجميع المعلومات عن طريق المواقع والادوات

Sites

1. hunter.io => كويس بس مش احسن حاجه عشان مدفوع
 2. Osint Framework
 3. crunchbase.com => بيجباك الشركات اللي استحوزت عليها الشركه اللي بتسررش عنها ودي مهمه جدا في البيج باونتي
 4. whois.com => في منها اداة برضو علي كالي
 5. <http://www.zone-h.org/archive/special=1>
 6. <http://www.zone-h.org/archive/special=1>
 7. socradar.io => معلومات عن الشركه بشكل عام
 8. dehashed.com => اي موقع او شركه بيتم اختراقها التسريبات بتاعتها بتنزل هنا
 9. aleph.occrp.org
 10. bgp.he.net => search by ASN
- bug bounty ده عبارته عن رقم كده تابع لكل شركه ليها **Autonomous System Number** او **ASN** يعني ايه
ip range وال subdomains بيكون رقم خاص بيهم بيعرفك الاسكوب بتاعهم اللي المفروض تهانت عليه وال
program
Google الخاص بـ ASN ده رقم الـ **AS15169** →

Shodan & Censys

- دول بقي موقعين جامدين اوي بالذات shodan بس censys جامد كمان ويمكن اجمد من shodan كمان بس عشان هو
بيحتاج اشتراك و shodan برضو بس shodan ممكن تدخل اكونت الجامعه وتأخذ الاشتراك البريميوم ببلاش
- المهم يعني دول موقعين بنكتبلهم فال search بتاعهم الـ ASN بتاع اي شركه هيجباك كل الأيبيات بتاعتهم وايه الأيبيات دي
عباره عن ايه سواء كاميرا او راوتر او جهاز عادي وايه البورتات المفتوحه عليه ومكانه وكل المعلومات

Import bookmarks... New notebook - Data... mythology/redteamin... Porkbun Webmail :: In... Video Compressor Onl... Vulnerability & Exploit ... VULNERABILITY LAB - ... Oxd hack

Shodan Maps Images Monitor Developer More...

SHODAN Explore Downloads Pricing [asn:AS3303](#)

TOTAL RESULTS
225,953

View Report Download Results Historical Trend Browse I

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilit

TOP COUNTRIES

85.2.18.68
68.18.2.85.dynamic.cust.swisscom.net
Swisscom (Schweiz)
AG is an LIR and ISP in Switzerland.

VPN (IKE)
Initiator SPI: 767477797974666c
Responder SPI: 3263716d3839626e

Limited Time Beta Program Access: Censys Internet Intelligence Platform is here! [Try it first! →](#)

censys [Hosts](#) [autonomous_system.asn:3303](#) [Search](#) [Register](#) [Log In](#)

[Results](#) [Report](#) [Docs](#) [Subscriptions](#)

Host Filters

Labels:

- 47.68K network.device.vpn
- 16.17K login-page
- 15.47K network.device
- 14.66K remote-access
- 7,814 jquery
- [More](#)

Autonomous System:

- 125.51K SWISSCOM Swisscom Switzerland Ltd

Location:

- 125.31K Switzerland
- 166 France
- [More](#)

Hosts
Results: 125,507 Time: 0.10s

92.107.128.217
Linux SWISSCOM Swisscom Switzerland Ltd (3303) Thurgau, Switzerland
remote-access network.device.vpn email
25/SMTP 443/OPENVPN 465/SMTP 587/SMTP 8443/HTTP

92.107.184.118 (118.184.107.92.dynamic.cust.swisscom.net)
Linux SWISSCOM Swisscom Switzerland Ltd (3303) Geneva, Switzerland
file-sharing vue.js media-streaming iot login-page
80/HTTP 123/NTP 137/NETBIOS 443/HTTP 445/SMB
3265/UNKNOWN 3702/WS_DISCOVERY 5000/HTTP 5001/HTTP 5055/HTTP
5357/HTTP 6881/KRPC 7878/HTTP 8080/HTTP 8989/HTTP
9091/HTTP 9117/HTTP 9696/HTTP 32400/HTTP 51413/UNKNOWN

Email Gathering

- طب لو عاوز اشوف الايميلات بتاعت موظفين الشركة؟
- عندك تلت مواقع يا باشا

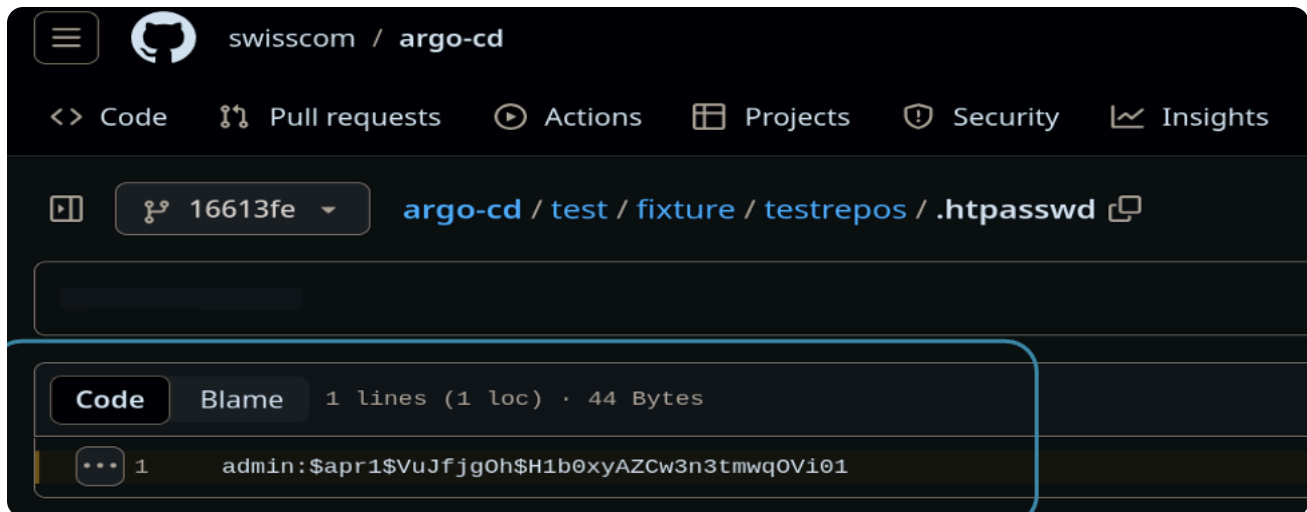
1. <https://app.prospeo.io/domain-search>
2. <https://newapp.anymailfinder.com/>
3. <https://app.snov.io/>

- طب انا دلوقتي جمعت الايميلات عاوز اشوف هل هيا ليها تسريب ولا لا قبل كده عشان اشوف ممكن اوصل لحاجه بيقى هنستخدم هنا سايت اسمه [haveibeenpwned](#)



Github

- حد هيقولي ياعم انت عبيط؟ جيت هب ايه اللي هتجمع منو معلومات اقولك اه عادي ممكن توصل لحاجه عادي من خلاله
- هتكتب اسم الشركه فالسيرش وشكرا وهيطلعك repos تابعه ليهم ممكن توصل لحاجه من خلالها ممكن يكون في باسوردات متسربه او متسابه كده فاهم



Tools

- نيجي بقي لكالي ونشتغل علي الtools

1. Whois

هخلص امتي ومعمول من امتي وهكذا domain بتجيلي معلومات عن الtool

```
(hossam@hossam) - [~]
$ whois swisscom.com
Domain Name: SWISSCOM.COM
Registry Domain ID: 2074961_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.corehub.net
Registrar URL: http://corehub.net
Updated Date: 2023-08-20T07:01:42Z
Creation Date: 1996-08-20T04:00:00Z
Registry Expiry Date: 2024-08-19T04:00:00Z
Registrar: Corehub, S.R.L.
Registrar IANA ID: 15
Registrar Abuse Contact Email: abuse@corehub.net
Registrar Abuse Contact Phone: +34935275235
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Name Server: DNS1.SWISSCOM.COM
```

DNS

- قبل ما نكمل عاوز اقولك عن ال dns ده عبارته عن سيرفر بيحول ال domain بتاع الموقع لل ip
- انا دلوقتي مثلا عشان اسجل رقم صحي ياسر بقولو ايه هات رقمك يسطا فا بقولي خد اهو اهو الرقم ده هو ال IP وانا بقي بسجل الرقم ده باسم ياسر ياسر هنا هو ال Domain
- نفس الكلام فوق بيحصل فالمواقع او السيرفرات عمدا انا لما باجي افتح موقع وليكن مثلا google.com بيكون في DNS Server بياخد كلمة Google.com بيحولها ل IP ويجيبك الموقع الحاجه اللي بتحول ال domain ل ip نفسها اسمه DNS Record

1. A Record

لما تطلب الموقع ip هو اللي يجيبك ال ip بال domain ده اللي بيربط ال

2. CNAME Record

يجبك ال ابيها بتاعتهم برضو subdomains بالموقع بتاعك وال cloud شغلانته بيربط سيرفرات ال

3. MX Record

mail servers ده مختص انه يجبك ابيها ال

4. PTR

domain ل ip ده بيعمل العكس بقي بيحول ال

- طب ايه الأدوات اللي تخليني احول من ال domain لل ip؟

1. dig

```
dig google.com
```

```
dig google.com CNAME
```

```
dig google.com MX
```

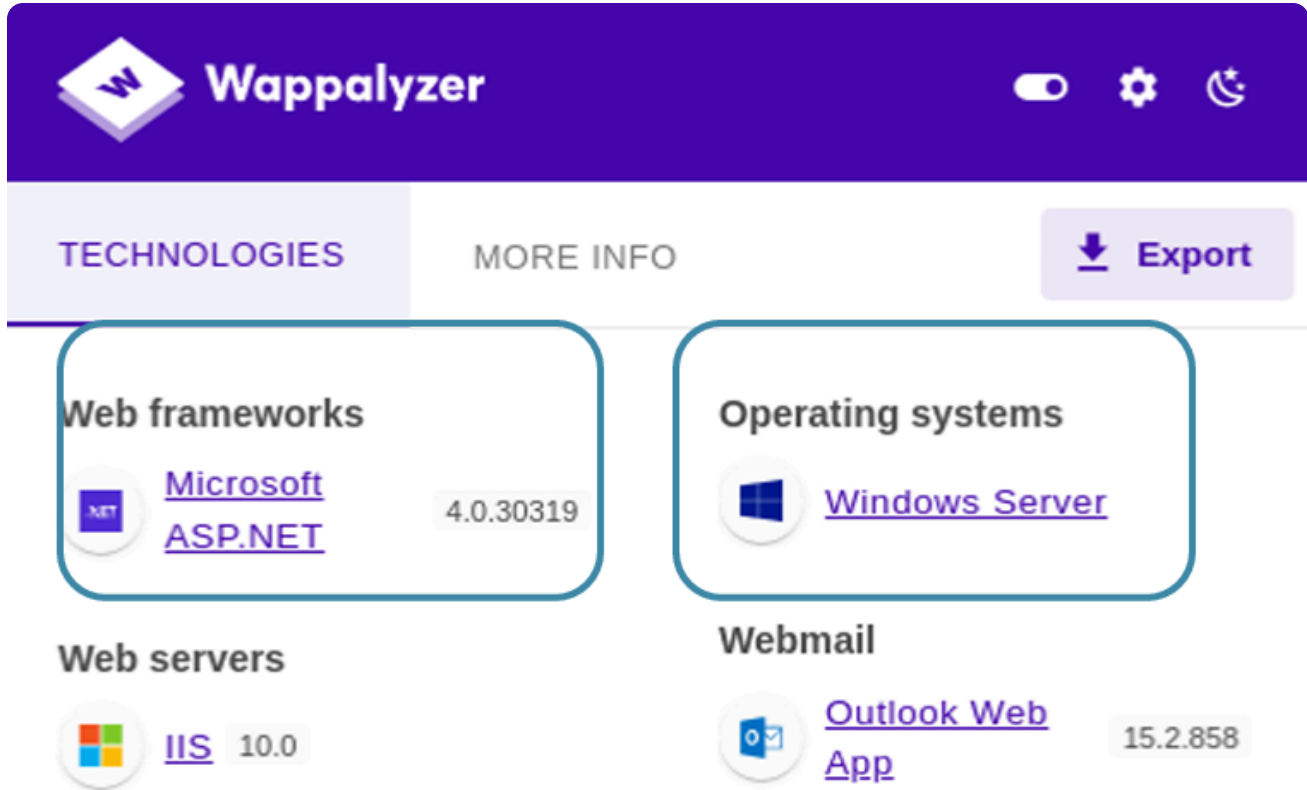
```
dig +short google.com => يجبك الأبي علاطول من غير اي تفاصيل ثانيه
```

2. nslookup

```
nslookup <domain>
```

Wappalyzer

- دي عبارة عن extension بتنزلها علي المتصفح بتاعك بتوريك ال technologies اللي معمول بيها سايت معين



- بص دي مثلا هنا الموقع بيقولك انه شغال علي microsoft server ومعمول بلغه C# بفريك ورك .NET.

Whatweb

- دي بتديلك شوية معلومات عن موقع ويب معين

<whatweb <domain

```
(hossam@hossam) - [~]
$ whatweb local.ch
http://local.ch [301 Moved Permanently] Country[UNITED STATES][US], IP[34.65.54.101]
https://www.local.ch/ [200 OK] Cookies[sessionid], Country[UNITED STATES][US], Em
y[sessionid], IP[34.65.54.101], Open-Graph-Protocol[website], Script[application/
port-Security[max-age=15724800; includeSubDomains], Title[local.ch - Geschäftsver
ol-allow-origin], X-Powered-By[Next.js]
```

Hackrevdns

- الأداة دي جميله جدا عباره عن انك لما يكون معاك CIDR بتاع target معين او رينج ايبهات يعني بتديهولو وهو بيخلصلك كل ip وتديك الdomain بتاعه

```
hakluke-$ prips 173.0.84.0/24 | hakrevdns
173.0.84.110 he.paypal.com.
173.0.84.109 twofasapi.paypal.com.
173.0.84.114 www-carrier.paypal.com.
173.0.84.77 twofasapi.paypal.com.
173.0.84.102 pointofsale.paypal.com.
173.0.84.104 slc-a-origin-pointofsale.paypal.com.
173.0.84.111 smsapi.paypal.com.
173.0.84.203 m.paypal.com.
173.0.84.105 prm.paypal.com.
173.0.84.113 mpltapi.paypal.com.
173.0.84.8 ipnpb.paypal.com.
173.0.84.2 active-www.paypal.com.
173.0.84.4 securepayments.paypal.com.
...
```

- الـ `prips` دي اللي بتتفحص الأيبهات وبعد كده بعملها indirect للأداة `hackervdns` بتاخذ كل ip وتديك الdomain بتاعه

TheHarvester

- الأداة دي جميله جدا وتقدر تجمعلك كل حاجه عن الtarget بس فكرتها انها بتحتاج APIs كتير وهيا هتجمعلك من كل حته كل المعلومات

```
<theHarvester -d <domain> -b <search-engine
```