Information Gathering

- مبدأيا عشان تتtarget لازم انك تجمع عنه كل المعلومات الكافيه بالبلدي كده مينفعش اروح اسرق بيت منغير ماعرف هما كام فرد فالبيت وايه الحاجات اللي ممكن ادخل منها فا ده بالظبط 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 واعضائها من خلال السيرش وطبعا اول ما نتكلم عن السيرش as a security يبقي بنتكلم عن Google Dork

Google Dorking

الGoogle 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 النتايج عن موقع معين يبقي 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

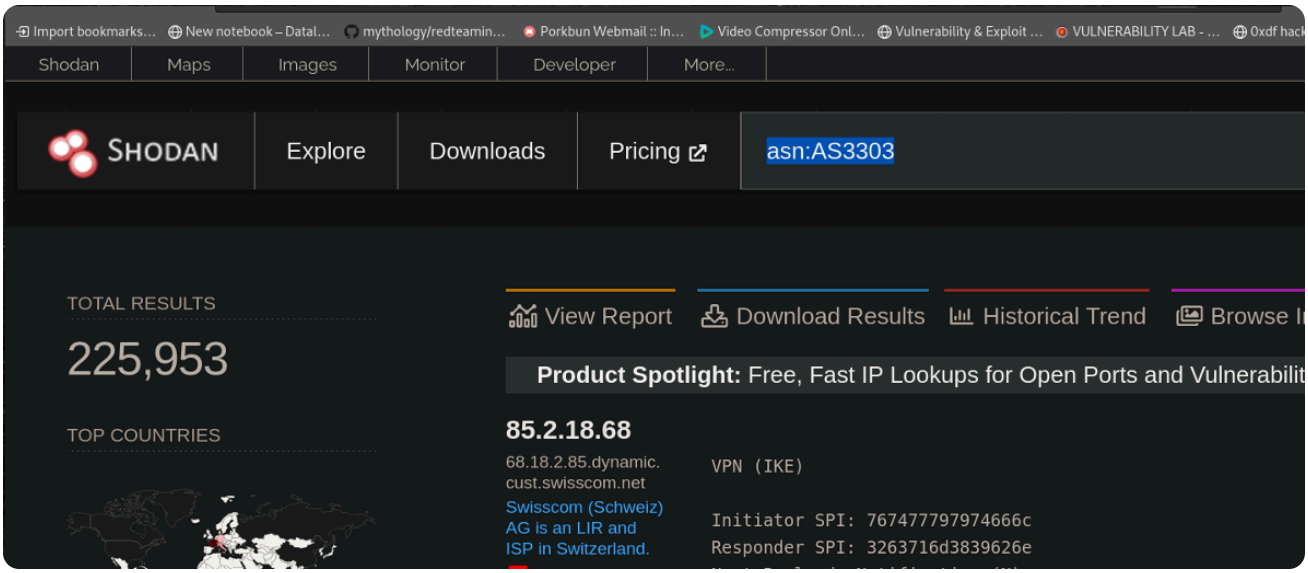
- لازم تحل لابات علي THM عن الgoogle dorking عشان skill مهمه جدا
-تاني حاجه بقي وهي تجميع المعلومات عن طريق المواقع والادوات

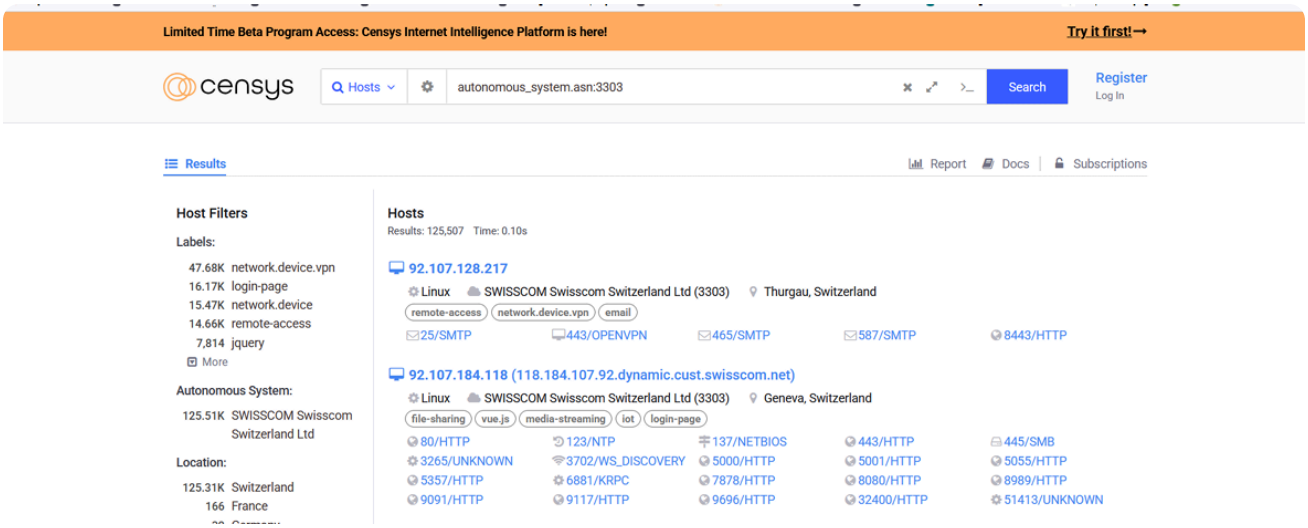
Sites

1. hunter.io => كويس بس مش احسن حاجه عشان مدفوع
2. Osint Framework
3. crunchbase.com => بيجبلك الشركات اللي استحوزت عليها الشركه اللي بتسرش عنها ودي مهمه جدا في البج 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
    Autonomous System Number او **ASN** يعني ايه ده عباره عن رقم كده تابع لكل شركه ليها bug bounty program بيكون رقم خاص بيهم بيعرفك الاسكوب بتاعهم اللي المفروض تهانت عليه وال subdomains وال ip range الخاص بـ Google. 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 وshodan برضو بس shodan ممكن تدخل اكونت الجامعه وتاخد الاشتراك البريميوم ببلاش
- المهم يعني دول موقعين بتكتبلهم فالsearch بتاعهم الASN بتاع اي شركه هيجبلك كل الأيبيهات بتاعتهم وايه الأيبيهات دي عباره عن ايه سواء كاميرا او راوتر او جهاز عادي وايه البورتات المفتوحه عليه ومكانه وكل المعلومات





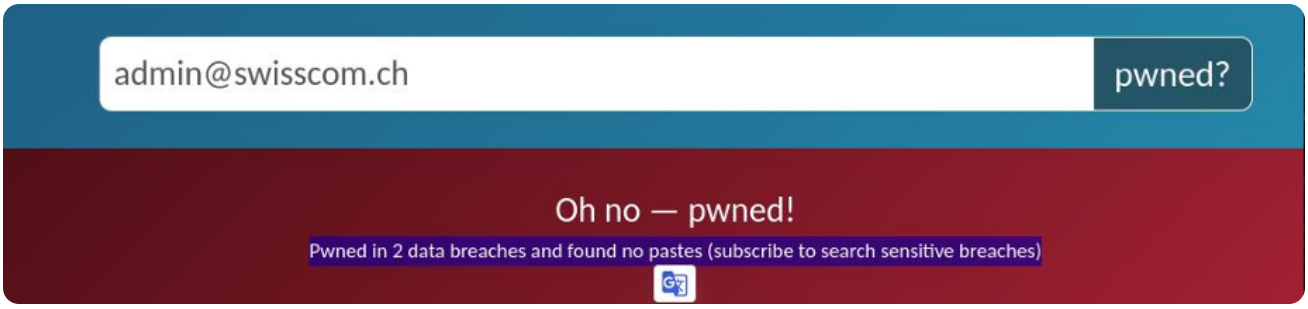
Email Gathering

- طب لو عاوز اشوف الايميلات بتاعت موظفيين الشركه؟
- عندك تلت مواقع يا باشا

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

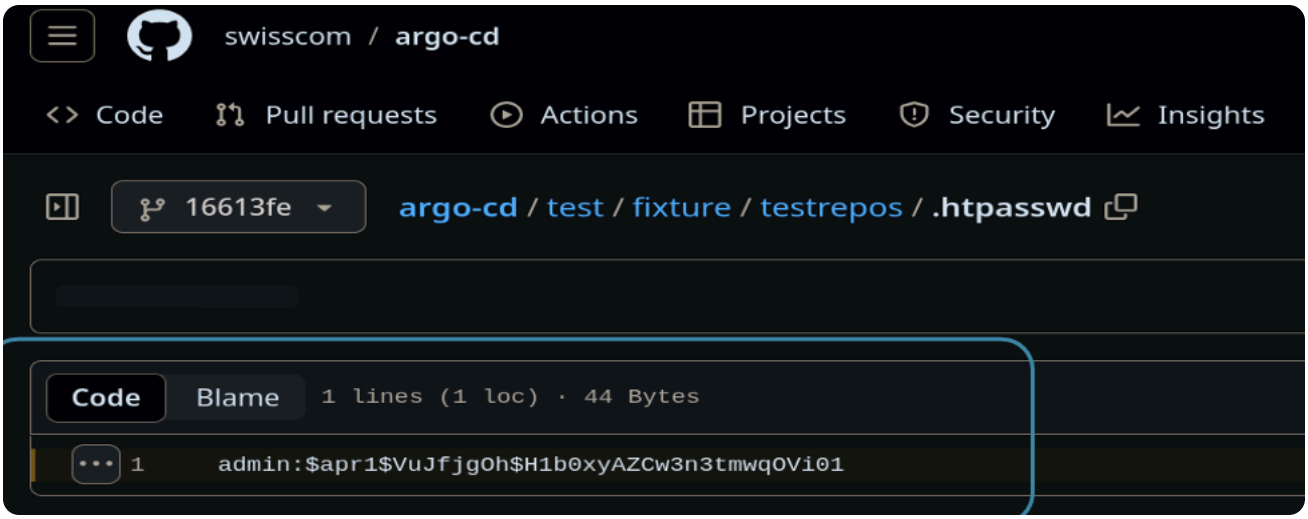
- طب انا دلوقتي جمعت الايميلات عاوز اشوف هل هيا ليها تسريب ولا لأ قبل كده عشان اشوف ممكن اوصل لحاجه يبقي هنستخدم هنا سايت اسمه `haveibeenpwned`

https://haveibeenpwned.com



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 وهيطلعلك repos تابعه ليهم ممكن توصل لحاجه من خلالهم ممكن يكون في باسوردات متسربه او متسابه كده فاهم



Tools

- نيجي بقي لكالي ونشتغل علي الtools

1. **Whois**
   هيخلص امتي ومعمول من امتي وهكذا domainدي بتجبلي معلومات عن ال toolال

```
┌──(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#clientD
   Domain Status: clientTransferProhibited https://icann.org/epp#clien
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientU
   Name Server: DNS1.SWISSCOM.COM
```

DNS

- قبل مانكمل عاوز اقولك عن الdns ده عباره عن سيرفر بيحول الdomain بتاع الموقع للip
- انا دلوقتي مثلا عشان اسجل رقم صحبي ياسر بقولو ايه هات رقمك يسطا فا يقولي خد اهو اهو الرقم ده هو الIP وانا بقي بسجل الرقم ده باسم ياسر ياسر هنا هو الDomain
- نفس الكلام فوق بيحصل فالمواقع او السيرفرات عمتا انا لما باجي افتح موقع وليكن مثلا google.com بيكون في DNS Server بياخد كلمة Google.com بيحولها لIP ويجبلك الموقع الحاجه اللي بتحول الdomain ل ip نفسها اسمه DNS Record

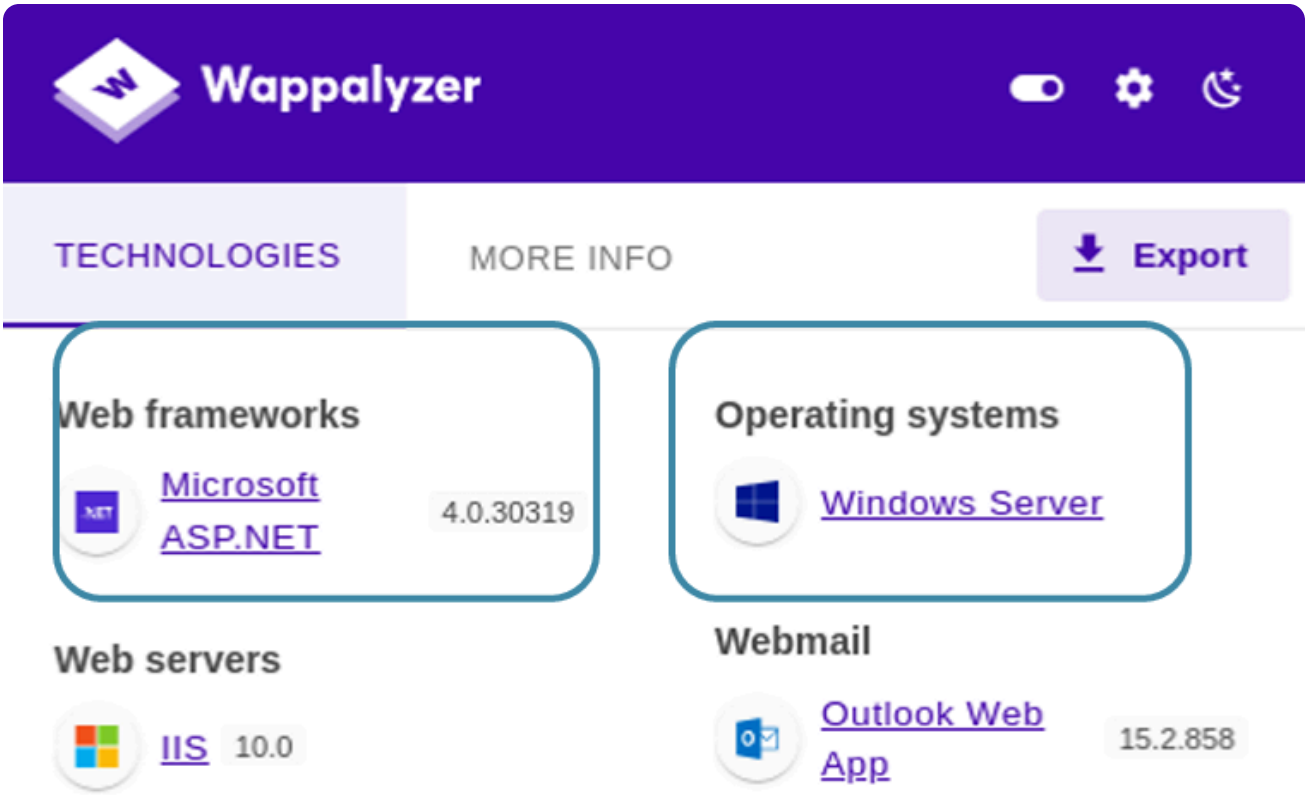
1. A Record
   لما تطلب الموقع ipوهو اللي بيجبلك ال ipبال domainده اللي بيربط ال
2. CNAME Record
   يجبلك الايبيهات بتاعتهم برضو subdomainsبالموقع بتاعك والـ cloudده شغلانته بيربط سيرفرات ال
3. MX Record
   ده مختص انه يجبلك ايبيهات ال mail servers
4. PTR
   ده بيعمل العكس بقي بيحول ال ip ل domain

- طب ايه الأدوات اللي تخليني احول من الdomain للip؟

1. dig
   `dig google.com`
   `dig google.com CNAME`
   `dig google.com MX`
   `dig +short google.com` => بيجبلك الأيبي علاطول من غير اي تفاصيل تانيه
2. nslookup
   `nslookup <domain>`

Wappalyzer

- دي عباره عن extension بتنزلها علي المتصفح بتاعك بتوريك الtechnologies 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

`<whateweb <domain`

```
└─$ whatweb local.ch
http://local.ch [301 Moved Permanently] Country[UNITED STATES][US], IP[34.65.54.1
 Moved Permanently]
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

- الاداة دي جميله جدا عباره عن انك لما يكون معاك CIDR بتاع target معين او رينج ايبيهات يعني بتديهولو وهو بيفصصلك كل ip ويديك الdomain بتاعه

- الـ `prips` دي اللي بتتفصص الأيبيهات وبعد كده بعملها indirect للأداة hackervdns بتاخد 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
```