

\* important site for  
exploitations.

- CVE
- security focus



## معنى Footprinting أو جمع المعلومات :

هي آلية جمع أكبر قدر ممكن من البيانات والمعلومات عن المستهدف لاستكشاف طرق مختلفة للوصول الى نظام المستهدف.

## أنواع مصادر البيانات:

- الشركات والمؤسسات
- الأفراد
- الأنظمة
- الشبكات

جمع بيانات الشركات والمؤسسات	جمع بيانات الأفراد	جمع بيانات الأنظمة	جمع بيانات الشبكات
<ul style="list-style-type: none"> <li>بيانات الموظفين</li> <li>موقع الشركة</li> <li>بيانات تواصل الشركة</li> <li>الوكيلين</li> <li>سياسة الخصوصية للشركة</li> <li>الخدمات الخاص بالشركة</li> <li>سجل عن معلومات الشركة</li> <li>مواضيع أو أخبار عن الشركة</li> </ul>	<ul style="list-style-type: none"> <li>البيانات الشخصية</li> <li>أرقام التواصل</li> <li>تاريخ الميلاد</li> <li>الوكيلين</li> <li>جهة العمل</li> <li>التعليم</li> </ul>	<ul style="list-style-type: none"> <li>أسماء المستخدمين</li> <li>اسم النظام</li> <li>كلمات المرور</li> <li>هندسة وتفاصيل النظام</li> <li>نوع النظام</li> <li>بيانات SNMP</li> <li>نوع نظام التحكم</li> </ul>	<ul style="list-style-type: none"> <li>اسم النطاق</li> <li>اسم النطاق الداخلي</li> <li>منافذ الاتصال</li> <li>منافذ الشبكات</li> <li>IP Address of the system</li> <li>VPN points</li> <li>IDSes running</li> </ul>

\* جمع معلومات - الصور

tinEye.com

في الصورة يوجد هذا اسم meta data

وهذا فيشكل عن الصورة ومنه نعرف ما هي الصورة

\* موقع يجيب معلومات كثيرة عن الصورة

اننا نرى المعدل على الصورة نرى هذا meta data

\* ادوات في الينكس

exif, exiftool

## Active



الاتصال المباشر في نظام الضحية أو موقعة

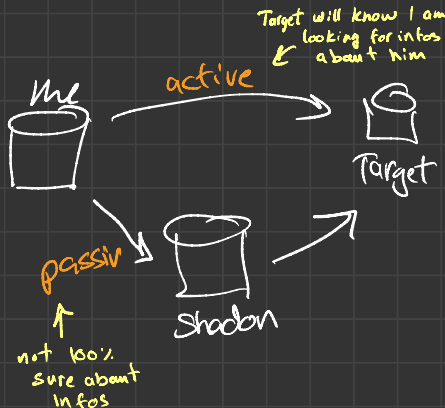
- تحميل الموقع كامل اوقلان للتحميل. أدوات تحليل
- موقع كامل ( Teleport pro, HTTPTrack )
- (website)
- تتبع البريد الإلكتروني

## Passive



المهاجم أو المخترق لا يتصل بالضحية أو بنظام الضحية أي اتصال مباشر

- محرك البحث
- Whois عبر البحث
- البحث عن DNS Lookup
- الشبكات الاجتماعية



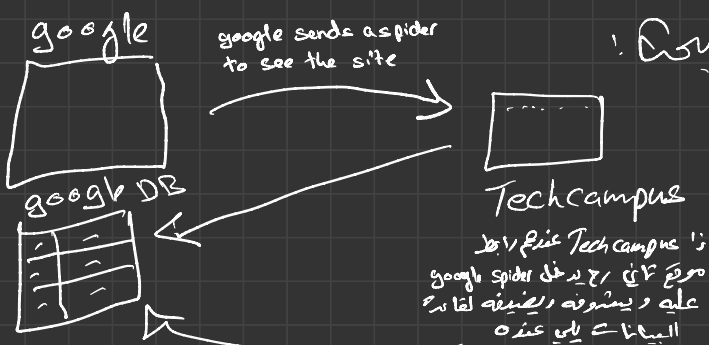
## GNU wget

القدرة على تحميل أي صورة، موقع، برنامج، backdoor ... أو أي رابط على جهاز الضحية أو الجهاز الحالي

```
Yaser@CHC:~/Desktop# wget https://chc-course.com
```

```
Yaser@CHC:~/Desktop# wget -m -p -E -k -np https://chc-course.com
```

تحميل كل شيء  
نفسه على أداة HTTPTrack





الجمعية العلمية  
الجامعة القادسية

## جمع المعلومات - المراقبة



CHC V2

مراقبة وتحليل المواقع الإلكترونية للشركة أو المؤسسة المستهدفة لمعرفة بعض البيانات المهمة.


- **تصليح موقع الضحية معطى بـ: **
- **البرامج التي يستخدونها و، رقم النسخة**
- **نظائر التشغيل المستخدم**
- **اسماء الملفات ومواقع الملفات وقواعد البيانات**
- **المصنعة والإضافات**
- **بيانات التواصل و بيانات CMS**


• **استخدام بعض الأدوات التالية للإنتشاف: **


- **Burp Suite**
- **Zaproxy**
- **Paros Proxy**
- **Website Informer**
- **Firebug**



<https://portswigger.net/>







---

Advanced	What you can do with it	Google this
<b>site:</b>	search only within a specific site	<b>site:</b> <a href="http://www.stanford.edu">www.stanford.edu</a>
<b>filetype:</b>	find a type of file: PDF, DOC, TXT ...	<b>filetype:</b> PDF
<b>define:</b>	find definitions for a word	<b>define:</b> audacity
<b>intitle:</b>	find words in the title of the webpage	<b>intitle:</b> inspirational
**	get ranges of numbers, dates, or prices	presidents 1800...1900
word * word	find other combinations of words between words	creative * writing
* word	search for word, but NOT simpson	homer * simpson
"word"	find exact words—no synonyms or plurals	"peace" "freedom"
*set of words*	search for exact set of words, quotes or phrases	"I have a dream"

[illegible]

\* Whois

\* فكرة انما لما استوفى الشركة طالبة وادى ضمان د FS معانا من كسبنا على FS وصلر  
\* لما اجبت عن شخص موظف في شركة اجبت عنه في linkedin

وتذكر دائما archive لا ينسى.