

# **M11 – Seguretat Informàtica – UF1**

**Pràctica 2 – SEGURETAT LÒGICA: FUNCIO HASH CRIPTOGRÀFICA**

**Nil Massó**



ASIX 2			
M11 – Seguretat Informàtica – UF1		Tipus	Individual
Cognoms, Nom:	Massó Cabaña, Nil	Curs	2022-23
Observacions:			

## Table of Contents

Enllaços:.....	1
Pràctica 5 – Recollida passiva d'informació.....	1
Exercici 1: Shodan. Recollida passiva d'informació. (3,5 punts).....	2
Exercici 2: Netcraft. Recollida passiva d'informació. (2 punts).....	3
Exercici 3: Whatweb. Recollida passiva d'informació. (2 punts).....	4
Exercici 4: Paràmetres avançats de cerca de Google. Recollida passiva d'informació. (2,5 punts) .....	5

- A l'hora d'avaluar i qualificar el treball es tindran en compte els aspectes estètics, de correctesa lingüística (sintàctica i ortogràfica) a més del que s'hagi comentat al cicle formatiu sobre la redacció de documentació tècnica i manuals.

- El mòdul professional pertany a uns estudis orientats al món laboral, cosa que fa que un cop complerts els requisits mínims la nota resultant serà condicionada per la quantitat i qualitat del treball individual realitzat per cada alumne.

- **Recordeu crear una portada i un índex.**

## Enllaços:

<https://thehackernews.com/>

<https://thehackernews.com/2022/02/critical-flaws-discovered-in-cisco.html>

<https://www.shodan.io/>

<https://www.sans.org/blog/getting-the-most-out-of-shodan-searches/>

<https://osintcurio.us/2021/05/13/searching-with-shodan/>

<https://gitlab.com/shodan-public/nrich>

<https://www.javatpoint.com/ethical-hacking-netcraft>

<https://asciinema.org/a/468923>

<https://hacksheets.medium.com/whatweb-what-is-that-website-e01a58498b7e>

<https://osintframework.com/>

<https://sitereport.netcraft.com/>

<https://ahrefs.com/blog/google-advanced-search-operators/>

<https://www.exploit-db.com/google-hacking-database>

## Pràctica 5 – Recollida passiva d'informació.

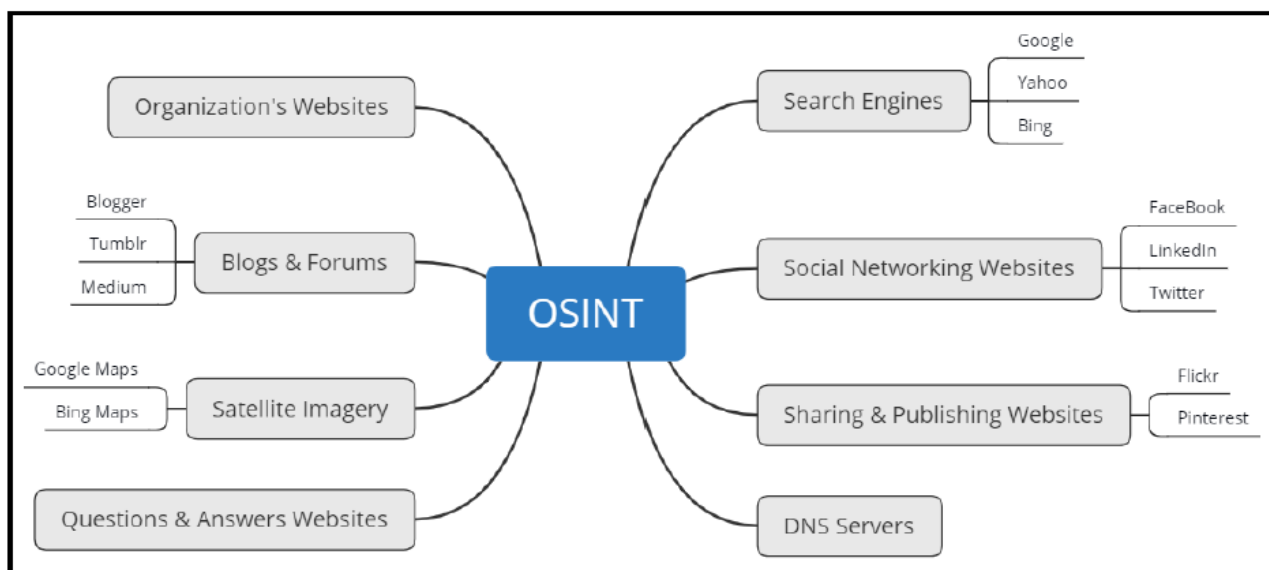
Fes els exercicis següents. Contesteu directament sota dels enunciats. Poseu-hi captures de pantalla si ho considereu necessari.

**Recordeu a citar TOTES les fonts utilitzades**

**Recollida passiva d'informació.**

Utilitzem mètodes d'aproximació que no suposen contacte directe amb l'objectiu.

**OSINT (open-source intelligence)**



Font: Learn Kali Linux 2019. Glen D. Singh.

Es tracta d'aprofitar la informació que les pròpies companyies i organitzacions posen a la xarxa per a promocionar-se. Podem esbrinar dades sobre el tipus de plataformes o aplicacions que fan servir a les seves xarxes. Eines com Maltego, theHarvester, Shodan, OSRFramework, Netcraft, WhatWeb, whois,...

Info i actualitat sobre vulnerabilitats: <https://thehackernews.com/>

## Exercici 1: Shodan. Recollida passiva d'informació. (3,5 punts)

És un motor de **cerca** de **dispositius** connectats a internet. Té servidors per tot el món que recullen informació sobre els dispositius, i aquesta informació es pot consultar. Exemples de cerques típiques són: "**webcam**", "**default passwords**", "**routers**", "**video games**".

Shodan és l'eina que fan servir investigadors, professionals de la seguretat, grans empreses i equips de resposta a emergències informàtiques (CERT).

- Els investigadors poden utilitzar Shodan per extreure informació sobre quins dispositius estan connectats, on estan connectats i quins serveis estan exposats.
- Els professionals de la seguretat poden utilitzar Shodan com a part d'un pla de proves de penetració per descobrir dispositius que s'han de **reforçar** (hardening) per prevenir possibles atacs.
- Les grans empreses utilitzen professionals de la seguretat que haurien de conèixer eines com Shodan per determinar el perfil de risc actual dels dispositius connectats de l'empresa.
- Shodan també és una eina utilitzada per individus i grups amb intencions malicioses coneguts habitualment com a threat actors.

**Llegiu** aquesta notícia <https://thehackernews.com/2022/02/critical-flaws-discovered-in-cisco.html> i

busqueu informació dels dispositius afectats a Shodan (<https://www.shodan.io/>). Creeu un compte **gratuït**.

Podeu fer servir les cerques avançades de Shodan (<https://www.sans.org/blog/getting-the-most-out-of-shodan-searches/> <https://osintcurio.us/2021/05/13/searching-with-shodan/> ) que us permeten  **cercar per producte, xarxa, os, port, país,...**

Localitzeu i mostreu amb captures de pantalla **almenys dos dispositius** que encara tinguin vulnerabilitats i que no hagin estat actualitzats. **Atenció:** No intenteu loginar-vos als dispositius què trobeu. (1 punts)

**24.239.126.20** Regular View Raw Data History

// TAGS: self-signed // LAST SEEN: 2022-11-15

### General Information

Hostnames: dynamic-acs-24-239-126-20.zoominternet.net  
Domains: ZOOMINTERNET.NET  
Country: United States  
City: Meadville  
Organization: Armstrong  
ISP: Armstrong  
ASN: AS27364

### Web Technologies

MOOTOOLS

### Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

**CVE-2022-0778** The BN\_mod\_sqrt() function, which computes a modular square root, contains a bug that can cause it to loop forever for non-prime moduli. Internally this function is used when parsing certificates that contain elliptic curve public keys in compressed form or explicit elliptic curve parameters with a base point encoded in compressed form. It is possible to trigger the infinite loop by crafting a certificate that has invalid explicit curve parameters. Since certificate parsing

### Open Ports

21 80 443 5432 5600 8880

// 21 / TCP 652854496 | 2022-11-15T06:05:48.996518

220-FileZilla Server version 0.9.41 beta  
220-written by Tim Kosse (Tim.Kosse@gmx.de)  
220-Please visit http://sourceforge.net/projects/filezilla/  
530 Login or password incorrect!  
214-The following commands are recognized:  
USER PASS CUST GDS PWD PORT PASS TYPE  
LIST REST CPOP RETR STOR SIZE DELE MKD  
PWD RWRB RMTS ABOR SYST XCOPY APPD NLST  
PDIR SPAD SCOP RMD XRD RFP SPFL EPRT  
Auth ADAT PWD PROT FEAT MODE OPTS HELP  
ALLO MLST MLSD SITE PWSM STRU CLMT MFMT  
WQOP  
214 Have a nice day.  
211-Features:  
RMTS  
REST STREAM  
SIZE  
MLST type\*"l",modify\*;  
MLSD  
UTFR  
CLMT  
MFMT  
211 End

// 80 / TCP 1242793706 | 2022-11-08T17:18:53.236304

Apache httpd 2.4.41

HTTP/1.1 200 OK  
Date: Sun, 04 Nov 2022 17:18:52 GMT  
Server: Apache/2.4.41 (Ubuntu) OpenSSL/1.1.1c PHP/7.2.29  
Content-Length: 772  
Content-Type: text/html; charset=UTF-8

**109.233.191.130** Regular View Raw Data History

// TAGS: self-signed // LAST SEEN: 2022-11-14

### General Information

Hostnames: ip-109-233-191-130.oriontelekom.rs  
Domains: ORIONTELEKOM.RS  
Country: Serbia  
City: Belgrade  
ISP: Društvo za telekomunikacije Orion telekom doo Beograd-Zemun  
ASN: AS9125

### Web Technologies

BOOTSTRAP GOOGLE HOSTED LIBRARIES JQUERY MOOTOOLS PHP

### Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

**CVE-2018-19396** ext/standard/var\_unserialize in PHP 5.x through 7.1.24 allows attackers to cause a denial of service (application crash) via an unserialize call for the com\_dotnet, or variant class.

**CVE-2018-19395** ext/standard/varc in PHP 5.x through 7.1.24 on Windows allows attackers to cause a denial of service (NULL pointer dereference and application crash) because com and com\_safearray\_proxy return NULL in com\_properties\_get in ext/com\_dotnet/com\_handlers.c, as demonstrated by a serialize call on COM("WScript.Shell").

### Open Ports

53 88 161 443 554 2222 3389 8080 8081

// 88 / TCP 90268723 | 2022-11-12T05:05:07.971239

HTTP/1.1 404 Not Found  
Date: Sat, 12 Nov 2022 06:05:05 GMT  
Server: umbserver  
Content-Length: 176  
Content-Type: text/html  
Connection: close

// 161 / UDP 1314237642 | 2022-10-20T14:46:17.898969

SNMP:  
Versions:  
3  
EngineID Format: text  
Engine Boots: 0  
Engine Data: 8093a8c04  
Enterprise: 14988  
Engine Time: 0:00:00

// 443 / TCP 105365934 | 2022-10-28T07:48:02.794909

Apache httpd 2.4.54

HTTP/1.1 200 OK  
Date: Fri, 28 Oct 2022 07:48:02 GMT  
Server: Apache/2.4.54 (Ubuntu) OpenSSL/1.0.2u PHP/5.6.40  
X-Powered-By: PHP/5.6.40  
Transfer-Encoding: chunked  
Content-Type: text/html; charset=UTF-8

### SSL Certificate

Certificate:  
Data:  
Version: 3 (Rx2)  
Serial Number: 2 (0x2)  
Signature Algorithm: sha256WithRSAEncryption  
Issuer: C=RS, ST=Serbia, L=Pancovo, O=Network Manager, OU=IT, OU=com.networkmanager.rs/emailAddress=wadim@networkmanager.rs

**Comenteu**, segons els ports que tenen oberts, a quins tipus d'**aplicacions o serveis** donen accés . (1 punts)

Webcams

**Comenteu** alguna **vulnerabilitat** CVE d'aquests dispositius i què podrien suposar per a la seguretat de la seva xarxa. Sou capaços de trobar algun exploit d'aquesta vulnerabilitat a <https://www.exploit-db.com/> i comentar-la? (1,5 punts)

Si, a traves de les vulnerabilitats existents pots pivotar per arribar a tenir acces i comprometre tota la xarxa

## Exercici 2: Netcraft. Recollida passiva d'informació. (2 punts)

Us permet trobar **informació d'un domini**, com ara el sistema operatiu del servidor de hosting, les tecnologies web utilitzades, contactes de correu, informació del bloc de xarxa utilitzat...

Aneu a <https://sitereport.netcraft.com/> per a trobar les tecnologies dels següents dominis:

- <https://www.netcraft.com>
- <https://www.sapalomera.cat>

Feu **captures de pantalla** i **comenteu** (ajudeu-vos amb <https://www.javatpoint.com/ethical-hacking-netcraft> ) la informació dels apartats per a cada domini :

- Network (adreça IP, DNS, país, ...) (0,4 punts)

Network			
Site	<a href="https://www.netcraft.com">https://www.netcraft.com</a>	Domain	netcraft.com
Netblock Owner	Cloudflare, Inc.	Nameserver	ns1.netcraft.com
Hosting company	Cloudflare	Domain registrar	namecheap.com
Hosting country	US	Nameserver organisation	whois.namecheap.com
IPv4 address	172.67.25.239 (VirusTotal)	Organisation	Privacy service provided by Withheld for Privacy ehf, Kalkofnsvegur 2, Reykjavik, 101, Iceland
IPv4 autonomous systems	AS13335	DNS admin	hostmaster@netcraft.com
IPv6 address	2606:4700:10:0:0:ac43:19ef	Top Level Domain	Commercial entities (.com)
IPv6 autonomous systems	AS13335	DNS Security Extensions	unknown
Reverse DNS	unknown	Latest Performance	<a href="#">Performance Graph</a>

Ns que vols que comenti

- IP delegation (**0,4 punts**)



IP delegation			
IPv4 address (172.67.25.239)			
IP range	Country	Name	Description
::ffff:0.0.0.0/96	United States	IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
↳ 172.0.0.0-172.255.255.255	United States	NET172	Various Registries (Maintained by ARIN)
↳ 172.64.0.0-172.71.255.255	United States	CLOUDFLARENET	Cloudflare, Inc.
↳ 172.67.25.239	United States	CLOUDFLARENET	Cloudflare, Inc.
IPv6 address (2606:4700:10:0:0:ac43:19ef)			
IP range	Country	Name	Description
::/0	N/A	ROOT	Root inet6num object
↳ 2600::/12	United States	NET6-2600	American Registry for Internet Numbers
↳ 2606:4700::/32	United States	CLOUDFLARENET	Cloudflare, Inc.
↳ 2606:4700:10:0:0:ac43:19ef	United States	CLOUDFLARENET	Cloudflare, Inc.

- Hosting history (**0,4 punts**)

Hosting History				
Netblock owner	IP address	OS	Web server	Last seen
<a href="#">Amazon.com, Inc. 1918 8th Ave SEATTLE WA US 98101-1244</a>	13.224.71.13	unknown	Apache	13-Apr-2022
Amazon.com, Inc. 1918 8th Ave SEATTLE WA US 98101-1244	13.32.172.37	unknown	Apache	11-Feb-2022
Amazon.com, Inc. 1918 8th Ave SEATTLE WA US 98101-1244	13.224.226.13	unknown	Apache	17-Jan-2022
Amazon.com, Inc. 1918 8th Ave SEATTLE WA US 98101-1244	99.86.119.25	unknown	Apache	5-Nov-2021
Amazon.com, Inc. 1918 8th Ave SEATTLE WA US 98101-1244	13.224.221.125	unknown	Apache	19-Oct-2021
Amazon.com, Inc. 1918 8th Ave SEATTLE WA US 98101-1244	13.32.170.127	unknown	Apache	9-Oct-2021
Amazon.com, Inc. 1918 8th Ave SEATTLE WA US 98101-1244	143.204.178.26	unknown	Apache	17-Sep-2021
Amazon.com, Inc. 1918 8th Ave SEATTLE WA US 98101-1244	143.204.178.91	unknown	Apache	24-Aug-2021
Amazon.com, Inc. 1918 8th Ave SEATTLE WA US 98101-1244	143.204.182.27	unknown	Apache	18-Jun-2021
Amazon.com, Inc. 1918 8th Ave SEATTLE WA US 98101-1244	52.85.104.94	unknown	Apache	15-May-2021

- SSL/TLS (tipus certificat, llargada clau, algorisme, emissor, validesa)(**0,4 punts**)

## SSL/TLS

Assurance	Organisation validation	Perfect Forward Secrecy	Yes
Common name	sni.cloudflaressl.com	Supported TLS Extensions	<a href="#">RFC8446</a> <a href="#">key share</a> , <a href="#">RFC8446</a> <a href="#">supported versions</a> , <a href="#">RFC4366</a> <a href="#">server name</a> , <a href="#">RFC7301</a> <a href="#">application-layer protocol negotiation</a>
Organisation	Cloudflare, Inc.	Application-Layer Protocol Negotiation	h2
State	California	Next Protocol Negotiation	Not Present
Country	 US	Issuing organisation	Cloudflare, Inc.
Organisational unit	Not Present	Issuer common name	Cloudflare Inc ECC CA-3
Subject Alternative Name	<a href="#">sni.cloudflaressl.com</a> , <a href="#">www.netcraft.com</a>	Issuer unit	Not Present
Validity period	From Apr 18 2022 to Apr 17 2023 (11 months, 4 weeks, 1 day)	Issuer location	Not Present
Matches hostname	Yes	Issuer country	 US
Server	cloudflare	Issuer state	Not Present
Public key algorithm	id-ecPublicKey	Certificate Revocation Lists	<a href="#">http://crl3.digicert.com/CloudflareIncECCCA-3.crl</a> <a href="#">http://crl4.digicert.com/CloudflareIncECCCA-3.crl</a>
Protocol version	TLSv1.3	Certificate Hash	OGG5NzpFG5Yf8BV2yHSPF/L3eFg
Public key length	256	Public Key Hash	a6bf06557d19024bd4d923eeeca8c7d2d3a5575277e2668467d737722515802cd
Certificate check	ok	OCSP servers	<a href="#">http://ocsp.digicert.com</a> - 100% uptime in the past 24 hours <a href="#">Performance Graph</a>
Signature algorithm	ecdsa-with-SHA256	OCSP stapling response	No response received
Serial number	0x07588b5126603e425fe849bd14847efd		
Cipher	TLS_AES_256_GCM_SHA384		
Version number	0x02		

- Site Technology (Server side, client side, CMS) (0,4 punts)



Site Technology (fetched 23 days ago)		
<b>HTTP Accelerator</b>		
A web accelerator is a proxy server that reduces web site access times.		
Technology	Description	Popular sites using this technology
Cloudflare <a href="#">↗</a>	Content delivery network and distributed domain name server service	<a href="http://www.inspq.qc.ca">www.inspq.qc.ca</a> , <a href="http://www.foxnews.com">www.foxnews.com</a> , <a href="http://www.notion.so">www.notion.so</a>
<b>Client-Side</b>		
Includes all the main technologies that run on the browser (such as JavaScript and Adobe Flash).		
Technology	Description	Popular sites using this technology
JavaScript <a href="#">↗</a>	Widely-supported programming language commonly used to power client-side dynamic content on websites	<a href="http://stackoverflow.com">stackoverflow.com</a> , <a href="http://my308053-ss0.crm.ondemand.com">my308053-ss0.crm.ondemand.com</a>
<b>Content Delivery Network</b>		
A content delivery network or content distribution network (CDN) is a large distributed system of servers deployed in multiple data centers in the Internet. The goal of a CDN is to serve content to end-users with high availability and high performance.		
Technology	Description	Popular sites using this technology
Cloudflare <a href="#">↗</a>	Content delivery network and distributed domain name server service	<a href="http://www.canva.com">www.canva.com</a> , <a href="http://www.coingecko.com">www.coingecko.com</a> , <a href="http://www.ecosia.org">www.ecosia.org</a>

### Exercici 3: Whatweb. Recollida passiva d'informació. (2 punts)

**Whatweb** és una aplicació opensource que és capaç de **reconèixer les tecnologies** que es fan servir per a servidors web, adreces d'email, web frameworks i bases de dades.

La trobareu a la **distribució kali Linux** tot i que la podeu instal·lar en qualsevol altre distribució.

La seva utilització es fa des de la línia de comandes *whatweb <objectiu>*.

*whatweb -v <objectiu>* ens activa el mode verbose i dona més informació.

Té diferents nivells d'agressivitat per a combinar velocitat/discreció i fiabilitat amb la opció `-aggression`

Més informació a <https://hacksheets.medium.com/whatweb-what-is-that-website-e01a58498b7e>

.

**Proveu whatweb -v** amb els següents objectius:

- <https://sapalomera.cat>
- <https://www.netcraft.com>
- Una màquina virtual metasploitable (la teniu al Moodle) accessible des del vostre kali Linux.

Feu **captures de pantalla** i **compareu i comenteu** en cada cas els resultats amb els obtinguts mitjançant Whatweb (si és que surten)

- Network **(0,4 punts)**

```
$ whatweb -v https://www.netcraft.com
WhatWeb report for https://www.netcraft.com
Status      : 403 Forbidden
Title       : Just a moment ...
IP          : 104.22.1.118
Country     : UNITED STATES, US
```

[Netcraft dona molta més informació d'aquest àmbit](#)

- IP delegation **(0,4 punts)**

[No surt](#)

- IP Geolocation **(0,4 punts)**

[Lo més proper a això es Country](#)

- SSL/TLS **(0,4 punts)**

- Site Technology (Server side, client side, CMS) **(0,4 punts)**

```
[ Cookies ]
  Display the names of cookies in the HTTP headers. The
  values are not returned to save on space.

  String      : __cf_bm

[ HTML5 ]
  HTML version 5, detected by the doctype declaration

File System

[ HTTPServer ]
  HTTP server header string. This plugin also attempts to
  identify the operating system from the server header.

  String      : cloudflare (from server string)

[ HttpOnly ]
  If the HttpOnly flag is included in the HTTP set-cookie
  response header and the browser supports it then the cookie
  cannot be accessed through client side script - More Info:
  http://en.wikipedia.org/wiki/HTTP_cookie

  String      : __cf_bm

[ Script ]
  This plugin detects instances of script HTML elements and
  returns the script language/type.

[ UncommonHeaders ]
  Uncommon HTTP server headers. The blacklist includes all
  the standard headers and many non standard but common ones.
  Interesting but fairly common headers should have their own
  plugins, eg. x-powered-by, server and x-aspnet-version.
  Info about headers can be found at www.http-stats.com

  String      : cf-chl-bypass,referrer-policy,permissions-policy,cf-ray (from headers)
```

## Exercici 4: Paràmetres avançats de cerca de Google. Recollida passiva d'informació. (2,5 punts)

Podem fer servir el cercador Google per a trobar sistemes vulnerables, informació oculta i altres recursos només afegint operadors de cerca a les nostres consultes.

Excloure paraules d'una cerca:

- Fer servir l'operador –
  - o Exemple cercar eines de proves de penetració i excloure kali. Cerquem:
    - penetration testing tools -kali

Aquí podeu trobar totes les opcions que admet **Google** per a restringir les cerques:

<https://ahrefs.com/blog/google-advanced-search-op-kalierators/>

**Utilitza tres de les opcions** que pots trobar a l'enllaç anterior per a fer alguna **cerca avançada**

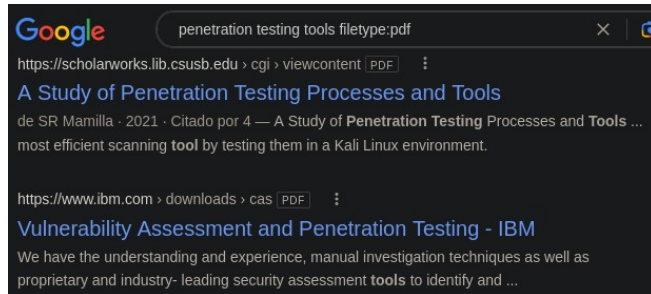
relacionada amb el pentesting.

Explica que pretens aconseguir amb la cerca, escriu-la i posa captura de pantalla del resultat. Si ho creus interessant pots posar captura de pantalla d'algun resultat en concret i comentar-lo.

Fins i tot hi ha una base de dades amb cerques d'aquest tipus: <https://www.exploit-db.com/google-hacking-database> on podeu trobar molts exemples de cerques.

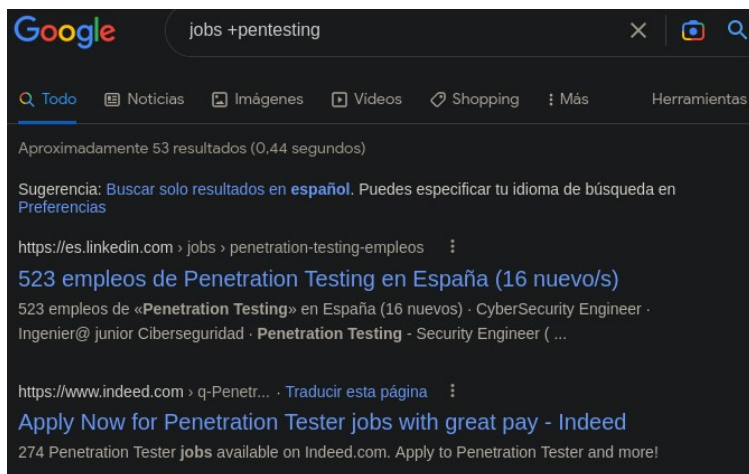
penetration testing tools filetype:pdf

Trobar documents pdf que parlin de pentesting



jobs +pentesting

Per trobar feines relacionades amb el pentesting



pentesting site:[www.kali.org](http://www.kali.org)

pentesting a dins la web de kali

