Effectuer une recherche passive d'informations concernant le domaine sectools.org, en vous basant sur ce cours, ainsi que le document ISSAF.

1) Où est situé le site web de l'entreprise

```
whois sectools.org
```

```
Domain Name: SECTOOLS.ORG
Registry Domain ID: D104142653-LROR
Registrar WHOIS Server: whois.fabulous.com
Registrar URL: http://www.fabulous.com
Updated Date: 2020-01-14T05:39:23Z
Creation Date: 2004-03-23T23:38:24Z
Registry Expiry Date: 2028-03-23T23:38:24Z
Registrar Registration Expiration Date:
Registrar: Sea Wasp, LLC
Registrar IANA ID: 411
Registrar Abuse Contact Email: support@fabulous.com
Registrar Abuse Contact Phone: +61.282133006
Reseller:
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Registrant Organization: Insecure.Com LLC
Registrant State/Province: WA
Registrant Country: US
Name Server: NS1.LINODE.COM
Name Server: NS2.LINODE.COM
Name Server: NS3.LINODE.COM
Name Server: NS4.LINODE.COM
Name Server: NS5.LINODE.COM
DNSSEC: unsigned

Registrant Country: US => maybe RIR: ARIN
```

2) Que disent les moteurs de recherche de cette cible

- En utilisant le moteur de rehcerche **SPYSE** : spyse.com
- Apache 2.4.6
- Centos
- 49 CVE découvertes (illisible => version payante)
- mx : mail.titan.net
- Certificat let's encrypt, RSA SHA-256 2048 bits
  - Plusieurs noms de domaines dont : https://svn.nmap.org/ anciennes version des produits d'insecure.

3) Quels sont les employés, ont-ils des sites web perso

- Nmap étant une association open source, je ne pense pas qu'il y est d'employé. Néanmoins, theHarvester me renvois des noms. Par eventualité je les listes, même si je doute qu'il y ai le moindre rapport avec sectools.

```
sudo theHarvester -d sectools -b linkedin
```

```
Henri Hurmerinta - Application Specialist - Visma
Luigi Gentile - Chief Information Security Officer - Reply
Mardian Gunawan - Security Consultant - Consultant
Maria Kahilampi - Entrepreneur - CoCo-Palvelut Ky
Mika Kosunen - Web Developer - Legenda
Pallav Raj Gurung - Manager - Morgan Stanley
Pekka Vesanen - Salesmanager - Veho Group Oy Ab
Ramanjaneya Devi Madem - Technical Leader - Cisco
Samrend Hasan - Project Manager - Blueraft
Yadu Mathur - Staff Software Engineer - Walmart Labs
```

- Henri Hurmerinta : **https://community.visma.com/t5/media/gallerypage/user-id/265037/tab/all**
- Luigi Gentile : **Rien trouvé**
- Mardian Gunawan : **Rien trouvé**
- Maria Kahilampi : **Rien trouvé**
- Mika Kosunen : **http://www.mikakosunen.com/**
- Pallav Raj Gurung :
  - **http://rajgurung.com/**
  - **https://github.com/rajgurung**
- Pekka Vesanen : **Rien trouvé**
- Ramanjaneya Devi Madem : **Rien trouvé**
- Samrend Hasan : **Rien trouvé**
- Yadu Mathur : **Rien trouvé**

4) Que pense les sites de reporting financier concernant ce domaine

Pas compris

5) Quel est le taux de disponibilité du site ?

Je n'ai pas trouvé de moyen d'avoir l'uptime du site sectools.org, alors j'ai pris l'uptime de l'hebergeur. Uptime services linode : https://status.linode.com/

6) Que renvoient les sites de supervision de domaines

Pas compris

7) Que trouve t'on concernant ce domaine sur les réseaux p2p

8) Présent sur les chat IRC

Channel officiel IRC : #nmap sur freenode.net

9) Y a-t-il des recrutement en cours ?

Non, rien sur les sites :

```
- sectools.org
- indeed.fr
- linkedin.fr
```

10) Y a-t-il des posts sur les newsgroup ?

Pas compris

11) Quelles informations donnent le registar ?

Voir question 1

12) Y a-t-il présence d'un reverse DNS

```
dig -x 45.33.49.119
```

```
; <<>> DiG 9.16.2-Debian <<>> -x 45.33.49.119
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25990
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;119.49.33.45.in-addr.arpa.     IN      PTR

;; ANSWER SECTION:
119.49.33.45.in-addr.arpa. 86388 IN     PTR     ack.nmap.org.

;; Query time: 4 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: dim. oct. 04 16:29:28 CEST 2020
;; MSG SIZE  rcvd: 80
```

ack.nmap.org.

13) Que disent les DNS

```
dnsenum --enum sectools.org
```

```
Trying Zone Transfers and getting Bind Versions:
_____________________________________________
Trying Zone Transfer for sectools.org on ns4.linode.com ...
AXFR record query failed: NOTIMP

Trying Zone Transfer for sectools.org on ns3.linode.com ...
AXFR record query failed: NOTIMP

Trying Zone Transfer for sectools.org on ns2.linode.com ...
AXFR record query failed: NOTIMP

Trying Zone Transfer for sectools.org on ns5.linode.com ...
AXFR record query failed: NOTIMP

Trying Zone Transfer for sectools.org on ns1.linode.com ...
AXFR record query failed: NOTIMP
```

5 serveurs DNS hebergés chez LINODE.com, transfert de zone impossible.

14) Ce domaine est il présent dans les bases de données de spam ?

Sur le site : **dnsbl.info**

```
162.159.25.129

Blacklisted : dynip.rothen.com
```

```
162.159.27.72

Blacklisted : dynip.rothen.com
```

```
162.159.24.39

Blacklisted : dynip.rothen.com
```

```
162.159.26.99

Blacklisted : dynip.rothen.com
```

```
162.159.24.25

Blacklisted : dynip.rothen.com
```

```
mail : 64.13.134.2

Blacklisted : dynip.rothen.com
```

Numero personnel gordon fyodor lyon Vaskovich

https://www.whitepages.com/name/Fyodor-Vaskovich/Sunnyvale-CA/1c6shdu1

- Adresse : 370 Altair Way # 113 Sunnyvale CA
- Téléphone : (650) 989-4206

tips

- shodan.io efficace pour trouver des devices
- maltego très bien pour commencer à faire de l'ingéniérie sociale.
- the harvester, il faut config avec des clés api des moteur de recherches
- metagoofil, trouver des documents sur un domaine : Metagoofil –d nmap.org –t pdf