

Repérer les actes malveillants

Via l'analyse de logs

(les comprendre pour essayer de les anticiper)

Reza EL GALAI
Responsable formations en cybersécurité
Université de Technologie de Troyes
reza.elgalai@utt.fr

Plan de la présentation

- Qui suis-je ?
- Web, Deepweb, Darknet, Darkweb
- OSINT & Hacking
- Les 5 phases d'une attaque cyber
- Anticiper l'attaque

Qui suis-je ?

- Responsable de la Sécurité des Systèmes d'Information (RSSI) à l'UTT
- Responsable du Mastère Spécialisé® « Expert Forensic et Cybersécurité »
- Responsable de la Licence Professionnelle « Enquêteur Technologies Numériques »
- Responsable du développement de l'offre de formation continue à l'UTT
- Impliqué dans l'associatif : CyberEdu, CECyF, ECTEG
- Chef d'escadron (CEN) RC de la Gendarmerie Nationale
- *Plus de 30 ans d'expérience dans l'enseignement et la formation*
- *Activités principales d'enseignements dans la formation continue (adultes)*
- *Méthodologie par l'exemple et les Retex*
- *Cours interactifs avec les auditeurs (Quizz, Exercices, Activités pédagogiques)*

Web, Deepweb, Darknet, Darkweb

Définitions
Fonctionnement de Tor

Web, Deepweb, Darknet, Darkweb – Kézako ?

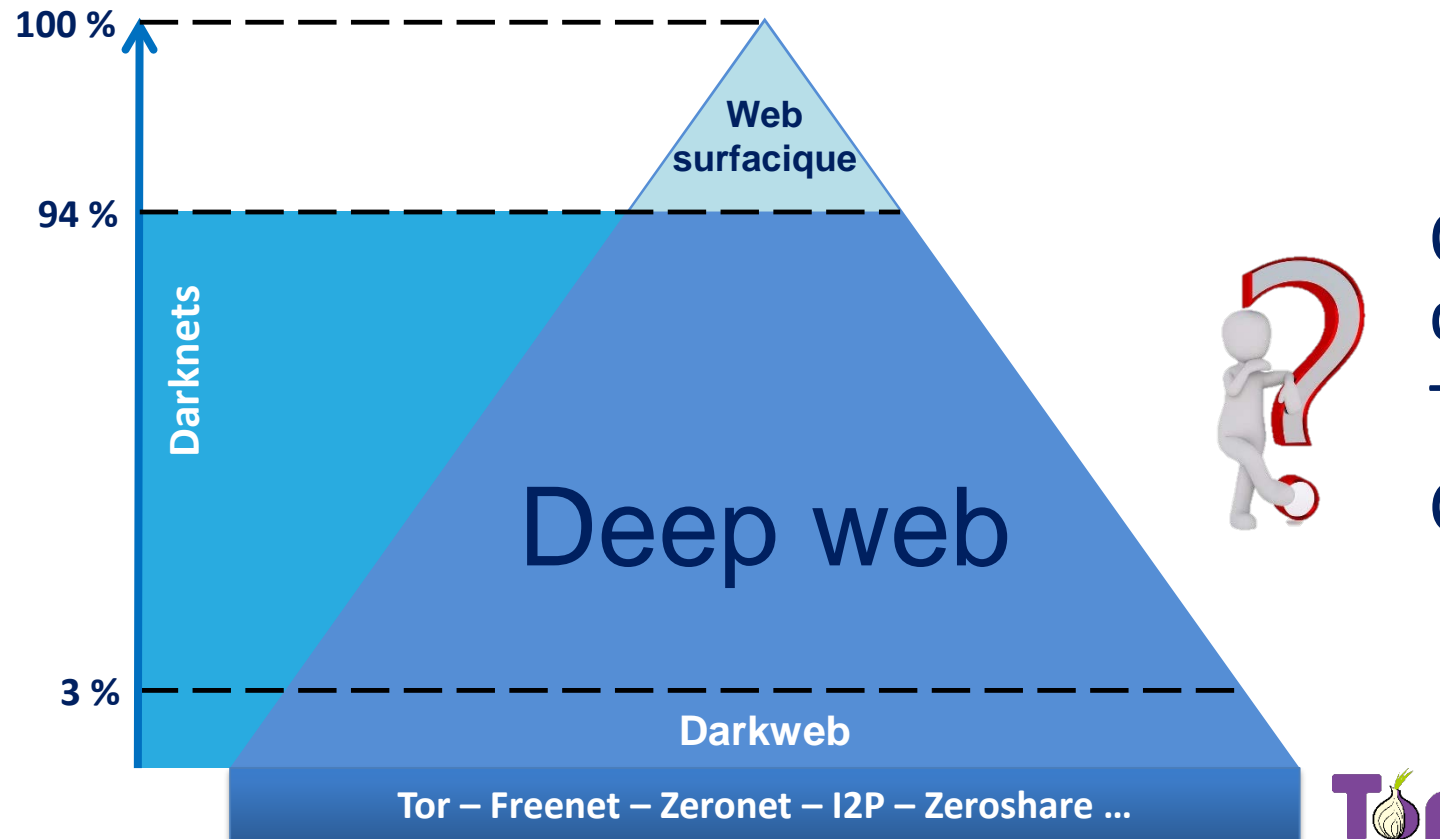
Qu'est-ce que :

- a) Le web ?
- b) Le deepweb ?
- c) Le(s) darknet(s) ?
- d) Le darkweb ?



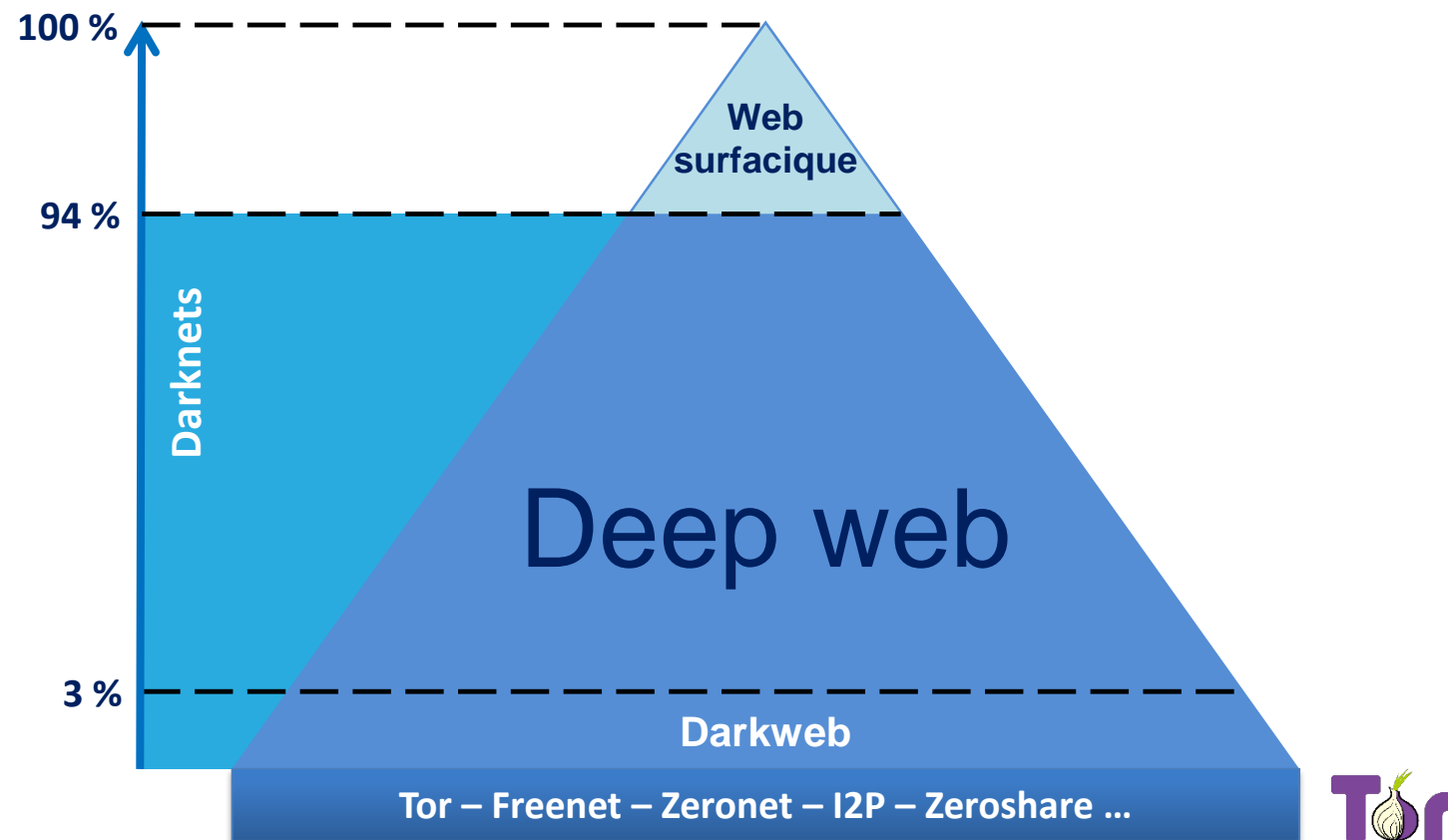
Un schéma valant mieux qu'un long discours ...

Web, Deepweb, Darknet, Darkweb – Kézako ?



Que trouve-t-on sur le darkweb ?
Tout y est illégal ?
Comment y accède-t-on ?

Que trouve-t-on sur le darkweb ?



De l'illégal :

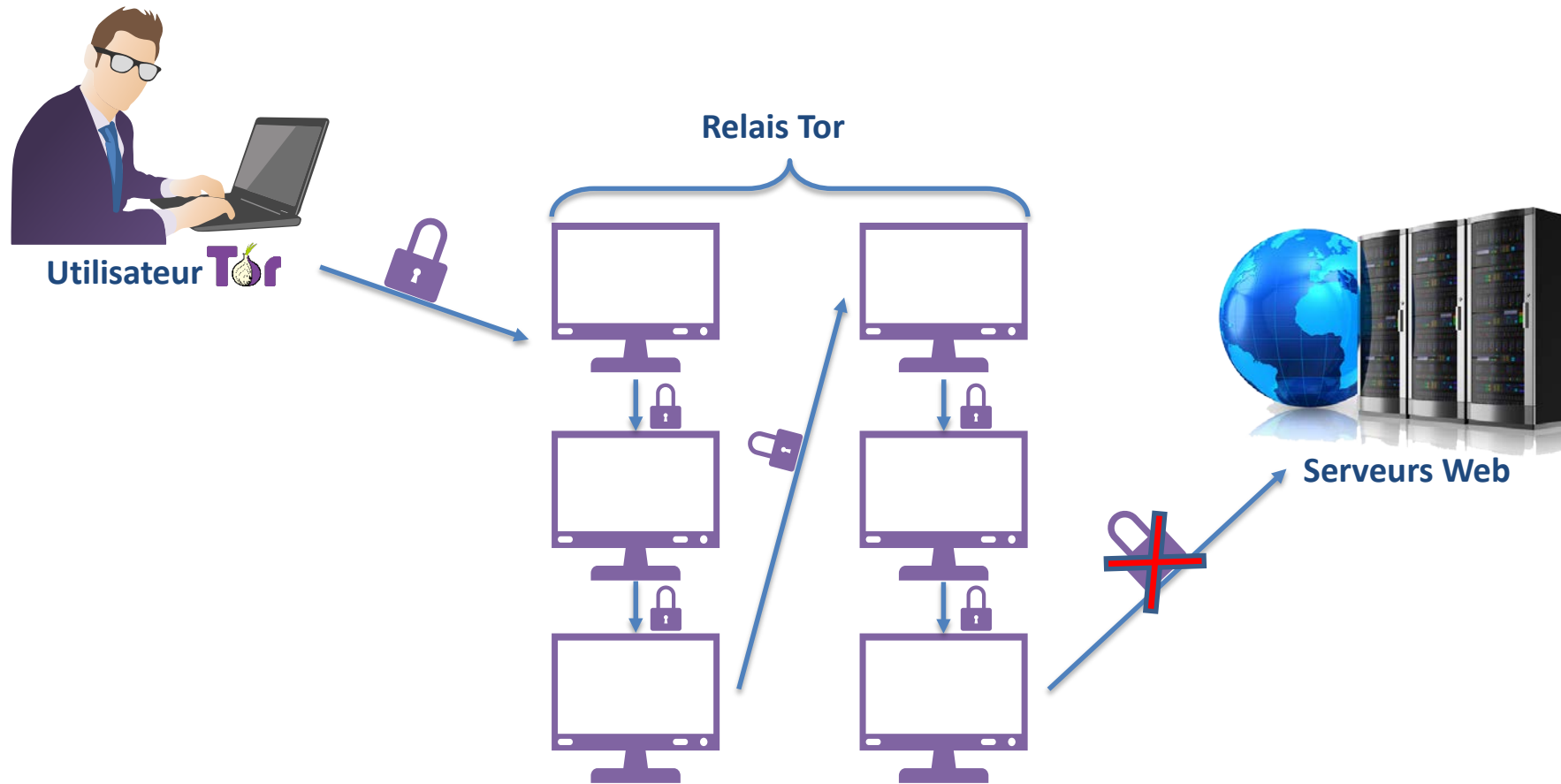
- Des armes
- De la drogue
- De la fausse monnaie
- Des faux médicaments
- Des tueurs à gages
- Des faux papiers
- De la prostitution
- Des contenus pédopornographiques
- **Des informations qui ont fuité**

Du légal :

- Des lanceurs d'alertes
- Des journalistes

➤ Accès par logiciels spécifiques => anonymat, chiffrement

Principe de fonctionnement de Tor



OSINT & Hacking

Définitions
Activités ludiques

OSINT & Hacking : What is it ?

Qu'est-ce que :

- a) L'OSINT
- b) Le Hacking



OSINT & Hacking : What is it ?

- **OSINT**

- **O**pen **S**ource **I**NTelligence
- Renseignement en sources ouvertes
- Acquérir des données depuis des sources publiquement accessibles

- **Hacking**

- Attaquer le système, le réseau ou les applications
- En exploitant leurs vulnérabilités
- Pour accéder frauduleusement aux données du système
- Vol, destruction, altération des données

OSINT & Hacking : What is it ?

- **OSINT**

- Open Source **INT**elligence
- Renseignement en sources ouvertes
- Acquérir des données depuis des sources publiquement accessibles



Lesquelles ?

- **Hacking**

- Attaquer le système, le réseau ou les applications
- En exploitant leurs vulnérabilités
- Pour accéder frauduleusement aux données du système
- Vol, destruction, altération des données

OSINT & Hacking : What is it ?

- **OSINT**

- Open Source **INT**elligence
- Renseignement en sources ouvertes
- Acquérir des données depuis des sources publiquement accessibles



Lesquelles ?

- **Hacking**

- Attaquer le système, le réseau ou les applications
- En exploitant leurs vulnérabilités
- Pour accéder frauduleusement aux données du système
- Vol, destruction, altération des données



Pourquoi ?

OSINT : sources publiques, lesquelles ?

- **Sources publiquement accessibles ?**

OSINT : sources publiques, lesquelles ?

- **Sources publiquement accessibles ?**

- Facebook
 - Instagram
 - Twitter
 - LinkedIn
 - Viadeo
- } SOCMINT
- Moteurs de recherche (au sens large)

Hacking : Pourquoi?

- **Quelles sont les motivations du hacker ?**

Hacking : Pourquoi?

- **Quelles sont les motivations du hacker ?**
 - Financières
 - Vengeance
 - Hacktivismisme
 - Espionnage
 - Vol de la Propriété Intellectuelle
 - Nuire à l'image
 - Réputation / être reconnu
 - Pour s'amuser

Hacking : Pourquoi?

- **Quelles sont les motivations du hacker ?**

- Financières
- Vengeance
- Hacktivismisme
- Espionnage
- Vol de la PI
- Nuire à l'image
- Réputation / être reconnu
- Pour s'amuser



Proposez des exemples

Recherche documentaire

- Citez quelques cas récents de cyberattaques, ayant visé :
 - Des États
 - Des services publics
 - De grands groupes de différents secteurs
- Quelles étaient les motivations des hackers ?
- Chantage au RGPD

Cyberattaques médiatisées

Samsung piraté : 190 Go de données confidentielles récupérées par les hackers

7 Mar. 2022 - 9:20 1 23

Jean-Baptiste A.

Après Nvidia, le groupe de hackers Lapsus\$ a piraté Samsung et a réussi à collecter pas moins de 190 Go de données confidentielles. L'affaire est plus que délicate pour le constructeur puisque la sécurité de ses smartphones Galaxy fait partie du hack.

Le Monténégro touché par une cyberattaque de grande ampleur

Par Romain Challand (@challandromain) | Publié le 29/08/22 à 14h01

TAP Air Portugal piraté : les données de 1,5 million de clients dans la nature



Alexandre Boero
20 septembre 2022 à 11h30

2

Avis Cyber sécurité

Essonne. Centre hospitalier visé par une cyberattaque: une rançon de 10 millions de dollars demandée

L'hôpital de Corbeil-Essonnes a été attaqué par un rançongiciel, dans la nuit de samedi 20 à dimanche 21 août 2022. Un plan blanc a été déclaré pour éviter que les patients n'en pâtissent.

La ville de Caen touchée par une cyberattaque, certains services publics paralysés

VU AILLEURS Caen a été victime d'une attaque informatique – dont la nature reste inconnue – le 26 septembre aux alentours de 17 heures. Depuis, le site internet de la ville, la messagerie interne et les services d'état civil sont inopérants. Une plainte a été déposée.

ALICE VITARD | PUBLIÉ LE 27 SEPTEMBRE 2022 À 10H06

Les 5 phases d'une attaque cyber

Méthodologie d'une attaque cyber

- Généralement en 5 étapes :
 - 1) Reconnaissance
 - 2) Scan
 - 3) Obtenir l'accès
 - 4) Maintenir l'accès
 - 5) Effacer ses traces

Reconnaissance

Reconnaissance passive
Reconnaissance active

Attaque cyber : Reconnaissance

- Consiste à rassembler des informations sur la cible, souvent plusieurs mois avant l'attaque :
 - **Reconnaissance passive** :
 - OSINT (moteurs de recherche, blog, forum)
 - **Reconnaissance active** :
 - Se rendre sur place, parler aux gens, ingénierie sociale

Reconnaissance passive : moteurs de recherche

- Comment fonctionne un moteur de recherche ?
 - Parcourt les pages web via un robot (crawler)
 - Indexe les données dans une base de données
 - Répond à la requête de l'utilisateur suivant un algorithme secret
 - Requête par mots simples
 - Requête avancée en utilisant les google dorks

Je cherche le terme « cyberedu » sur Google

<https://www.ssi.gouv.fr> > entreprise > formations > cybe... ▾

[CyberEdu | Agence nationale de la sécurité des ... - l'ANSSI](#)

→ **CyberEdu** est un projet initié par l'ANSSI à la suite de la publication du Livre blanc sur la défense et la sécurité nationale en 2013. Il a pour objectif d' ...

Reconnaissance passive : Google dorks




- Google dorks ...

url <https://www.ssi.gouv.fr/entreprise/formations/cybe...>

titre [CyberEdu | Agence nationale de la sécurité des ... - l'ANSSI](#)

texte CyberEdu est un projet initié par l'ANSSI à la suite de la publication du Livre blanc sur la défense et la sécurité nationale en 2013. Il a pour objectif d' ...

- ... utiles pour effectuer des recherches :

- dans un lien http ou **url** de la page,  **url** <https://www.ssi.gouv.fr/entreprise/formations/cybe...>
- dans le **titre** de la page,  **titre** [CyberEdu | Agence nationale de la sécurité des ... - l'ANSSI](#)
- dans le **texte** descriptif de la page,  **texte** CyberEdu est un projet initié par l'ANSSI à la suite de la publication du Livre blanc sur la défense et la sécurité nationale en 2013. Il a pour objectif d' ...
- dans des fichiers spécifiques, avec un contenu précis

Reconnaissance passive : Exemple de Google dorks

url <https://www.ssi.gouv.fr/entreprise/formations/cyberedu>

titre [CyberEdu | Agence nationale de la sécurité des ... - l'ANSSI](#)

texte CyberEdu est un projet initié par l'ANSSI à la suite de la publication du Livre blanc sur la défense et la sécurité nationale en 2013. Il a pour objectif d' ...

inurl:

Google inurl:cyberedu

<https://www.cyberedu.fr>

CyberEdu

CyberEdu est une association très active pour former les formateurs et les formatrices de l'enseignement du supérieur pour que la cybersécurité entre dans toute ...
Vous avez consulté cette page de nombreuses fois. Date de la dernière visite : 23/10/21

<https://www.cyberedu.fr/pages/labellisation>

Labellisation - CyberEdu

Le label CyberEdu a pour objectif de référencer les formations de l'enseignement supérieur qui intègrent dans leurs cours des contenus sur la sécurité du ...

<https://www.cyberedu.fr/pages/le-projet>

Le Projet - CyberEdu

Projet initié par l'ANSSI à la suite de la publication du Livre blanc sur la Défense et la sécurité nationale en 2013, le projet CyberEdu a pour objectif ...

intitle:

Google intitle:cyberedu

<https://www.lemondeinformatique.fr/actualites/lire-cyberedu>

CyberEdu et l'Afpa veulent former 4 000 spécialistes ...

30 oct. 2017 — Formation : L'association CyberEdu créée par l'Anssi s'est associée à l'Agence nationale pour la formation professionnelle des adultes pour ...

[https://www.lemondeinformatique.fr/actualites/lire-u...](https://www.lemondeinformatique.fr/actualites/lire-un-label-cyberedu)

Un label CyberEdu pour deux formations du Cesi

19 mars 2019 — Le label CyberEdu a pour objectif de référencer les formations de l'enseignement supérieur qui intègrent dans leurs cours des contenus sur la ...

https://twitter.com/asso_cyberedu

CyberEdu (@asso_cyberedu) / Twitter

Le label CyberEdu a été décerné à la licence pro Systèmes Automatisés, Réseaux et Informatique Industrielle (SARII), option Automatismes et Informatique ...

Reconnaissance passive : Google dorks

- Facilitent les recherches de documents :
 - Confidentiels,
 - diffusés par erreur,
 - qui sont des versions de travail,
 - qui ont fuité,
 - qui sont des bases de données de coordonnées.
- Voyons quelques exemples de documents « sensibles ».

Reconnaissance passive : Exemples de documents

DIRECTION DES AUDITS DE SÉCURITÉ **CONFIDENTIEL**

DIRECTION DES AUDITS DE SÉCURITÉ
20, rue de Rome
75008 PARIS
Fax : 01 53 42 08 49
Tél. : 01 53 42 00 37



DERAILEMENT DU TRAIN N°3657 EN GARE DE BRETIGNY-SUR-ORGE LE 12 JUILLET 2013

RAPPORT D'ENQUÊTE N°2013 - AS - 056

Enquête assurée par : [redacted] chef de mission ASC Traction, responsable de la mission d'enquête
[redacted] chef de mission ASC Infra
[redacted] adjoint au chef de mission ASNO Infra
[redacted] chef de mission ASC Matériel
[redacted] auditeur ASNO Exploitation

Chambre régionale
des comptes
Occitanie



Le Président

lettre recommandée avec A.R.

CONFIDENTIEL

Le 07/08/2017

Réf. : GR / 17 / 1696

Madame la Présidente,

Je vous prie de bien vouloir trouver ci-joint le rapport comportant les observations par la chambre régionale des comptes sur le contrôle des comptes et de la g Occitanie.

Il est accompagné de la réponse reçue à la chambre dans le délai prévu par code des juridictions financières.

GAC GROUP
Innovation & Performance
for Impact

DECISION
ETUDES & CONSEIL

Evaluation intermédiaire du programme Nano 2022
Rapport de synthèse

13 juin 2022 – Document confidentiel

© 2022 [redacted] - Confidentiel

CONFIDENTIEL

La formation des élus locaux

INSPECTION GÉNÉRALE
DE L'ADMINISTRATION
N° 19066-R

INSPECTION GÉNÉRALE
DES AFFAIRES SOCIALES
N° M2019-08491

INSPECTION GÉNÉRALE
DES ÉLUS LOCAUX

1 janvier 2020

CONFIDENTIEL

Rapport de la mission relative
au contrôle qualité de la gestion
de crise sanitaire

Etabli par
Par Richard LIZUREY
Général d'armée (2s), rappelé à l'activité
avec l'appui d'Amélie PUCCINELLI
Inspectrice de l'administration

1er Juin 2020

PP
PREFECTURE DE POLICE

DIRECTION DE LA SÉCURITÉ DE PROXIMITÉ
DE L'AGGLOMÉRATION PARISIENNE
ETAT-MAJOR
Département Commandement Opérationnel
Pôle Planification
Code INSEE : 75056370
Tél. : 01 53 71 28 91
Réf. : 2018/105440

Note
à
tous chefs de service

Paris, le 07 décembre 2018

Objet : Dispositif de la DSPAP dans le cadre du rassemblement national des gilets jaunes sur la capitale le samedi 08 décembre 2018.

P.J. :

1. réquisition du parquet de Paris
2. ordre particulier des transmissions
3. fiche interpellation
4. le tableau des violences urbaines
5. arrêté du Préfet de police du 6 décembre 2018
6. liste des interdits de paraître à Paris.

DOCUMENT DE TRAVAIL SSMSI

15 mars 2022

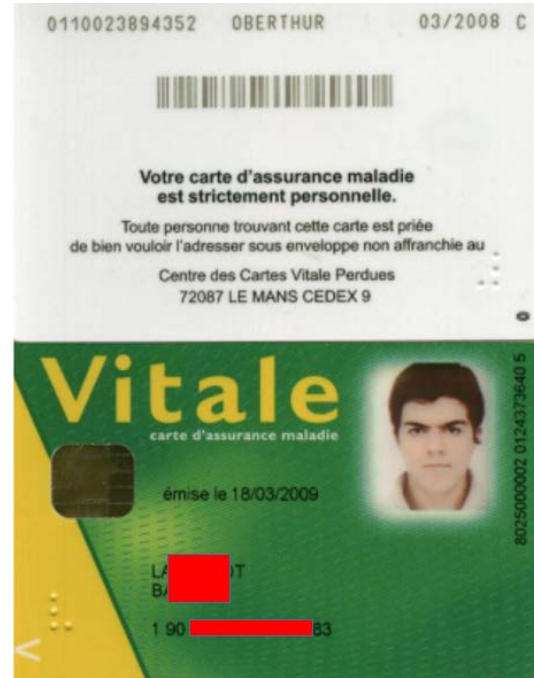
amende forfaitaire délictuelle pour usage de stupéfiants : premiers éléments d'évaluation

CONFIDENTIEL - Diffusion restreinte

Rapport de la mission relative au contrôle qualité de la gestion de crise sanitaire

recommandations par ordre d'apparition dans le rapport

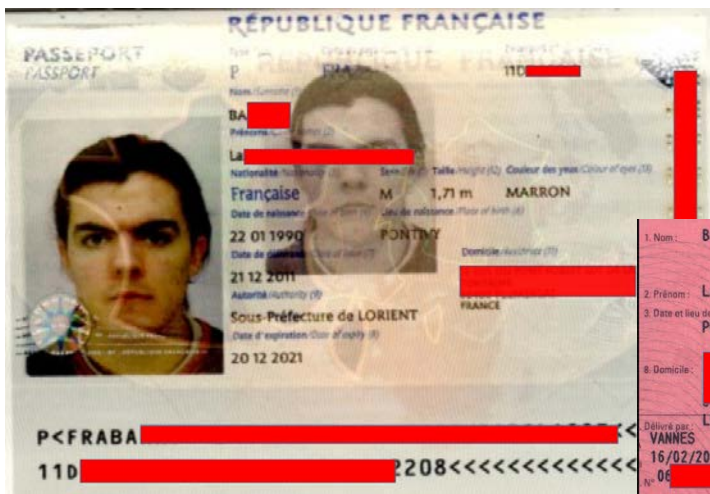
Reconnaissance passive : Exemples de documents



NOM: [redacted]

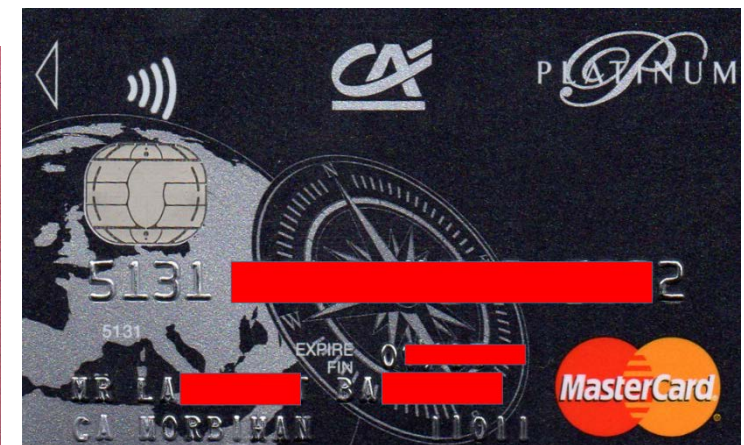
Vaccinations antipoliomyélitique Antidiphthérique – Antitétanique Anticoquelucheuse			Vaccinations antirougeoleuse – Antirubéolique Antiourlienne – Antityphoparatyphoïdique Autres vaccinations		
Date	Vaccin – Dose	Signature et cachet du médecin	Date	Vaccin – Dose	Signature et cachet du médecin
16/4/96	DT Polio 1994	Docteur René DURENNAUT Spécialité: 07 25, Rue de la Courbe 55000 PONTIVY	16/12/11	Pravira n°1 Lot A9CC2A	
15/4/96	DT Polio 1994		08/06/2012	Pravira n°1 Lot A9CC2A	
26/6/97	DTP		16/12/11	Pravira n°1 Lot A9CC2A	
30/02	DT Polio		13/01/12	Pravira n°2 Lot A9CC2A	
05/11/2012	DT Polio		08/06/12	Pravira n°3 Lot A9CC2A	
13/01/2012	DT Polio		16/01/12	Pravira n°4 Lot A9CC2A	
			16/01/12	Pravira n°5 Lot A9CC2A	
			16/01/12	Pravira n°6 Lot A9CC2A	
			16/01/12	Pravira n°7 Lot A9CC2A	
			16/01/12	Pravira n°8 Lot A9CC2A	
			16/01/12	Pravira n°9 Lot A9CC2A	
			16/01/12	Pravira n°10 Lot A9CC2A	
			28 AOUT 2012	Mervac Novartis Lot: M11057	
			28 AOUT 2012	Ixiaro Novartis Lot: JEV118788	
			28 AOUT 2012	Vaccin rabique Pasteur Lot: G1425-2	

Les mentions portées sur cette page ont valeur de certificats de vaccination. A remplir lisiblement et complètement.



1. Nom: BA [redacted]
2. Prénom: LA [redacted] T. [redacted] E
3. Date et lieu de naissance: 22/01/1990 PONTIVY (056)
8. Domicile: [redacted]
Délivré par: VANVES 16/02/2009
N° 06 [redacted]

CATÉGORIES DE VÉHICULES POUR LESQUELLES LE PERMIS EST VALABLE	DEPUIS LE	JUSQU'AU	RESTRICTIONS	MENTIONS	TIMBRE
A1	29/01/2009	*****			
A	29/01/2009	*****			
B1	29/01/2009	*****			
B	29/01/2009	*****			
C	*****	*****			
D	*****	*****			
B	*****	*****			
C	*****	*****			
D	*****	*****			



Reconnaissance passive : Exemples de documents

The image displays several examples of documents used for passive recognition:

- Carte Nationale d'Identité (CNI):** Three French national identity cards are shown for individuals named Patrick, Ellies, and Andre. Each card includes a photo, signature, and personal details like date of birth and sex.
- Permis de Conduire (Driving License):** A driving license for Stephane-Claude Edmond is visible, listing categories A, B, C, and D.
- Relevé d'Identité Bancaire (RIB):** Two bank account opening forms are shown:
 - CIC Est:** Includes fields for IBAN (FR76 3008 73...), BIC (CEPAFRPP), and account details for Agence de Mulhouse Franklin.
 - La Banque Postale:** Includes fields for RIB (FR93 2004 1010 051...), BIC (PSSTFRPLIL), and account details for Centre Financier de Lille.
- Other Documents:** Partially visible documents include a driving license for Benji and a document for Jean-François Cayrat.

Reconnaissance passive : Où trouver des dorks ?



Google Hacking Database

Show 15

Date Added	#	Dork	Category
2022-09-19		intext:"index of" ".sql"	Files Containing Juicy Info
2022-09-19		intitle:"index of" inurl:superadmin	Files Containing Juicy Info
2022-09-19		intitle:"WAMPSEVER Homepage"	Files Containing Juicy Info
2022-09-19		inurl: json beautifier online	Files Containing Juicy Info
2022-09-19		intitle:"IIS Windows Server"	Files Containing Juicy Info
2022-09-19		intitle:"index of" inurl:SUID	Files Containing Juicy Info
2022-09-19		intitle:"index of" intext:"Apache/2.2.3"	Files Containing Juicy Info
2022-08-18		inurl:"index.php?page=news.php"	Advisories and Vulnerabilities
2022-08-18		inurl:/sym404/root	Files Containing Juicy Info
2022-08-17		inurl:viewer/live/index.html	Various Online Devices



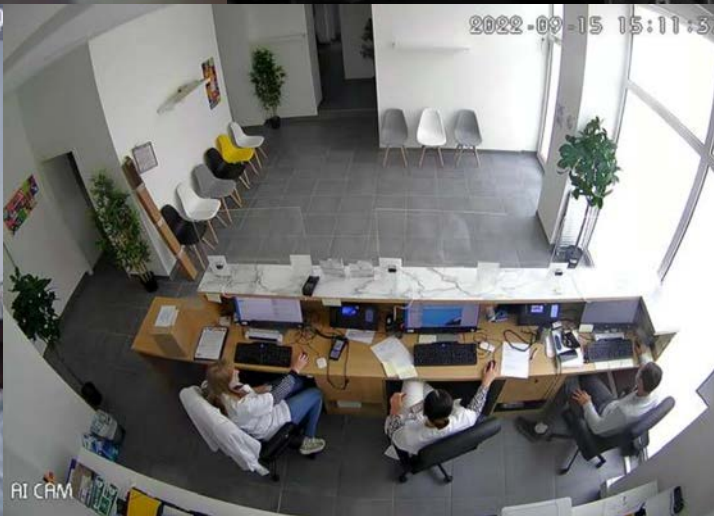
Le moteur de recherche Shodan

Principe de fonctionnement
Exemples

Reconnaissance passive : Shodan

- Shodan est un moteur de recherche d'objets connectés :
 - Parcourt les adresses IP
 - Interroge les ports
 - Identifie les services en fonction de la bannière de réponse
 - Répond à la requête de l'utilisateur

Reconnaissance passive : Accès caméras avec Shodan

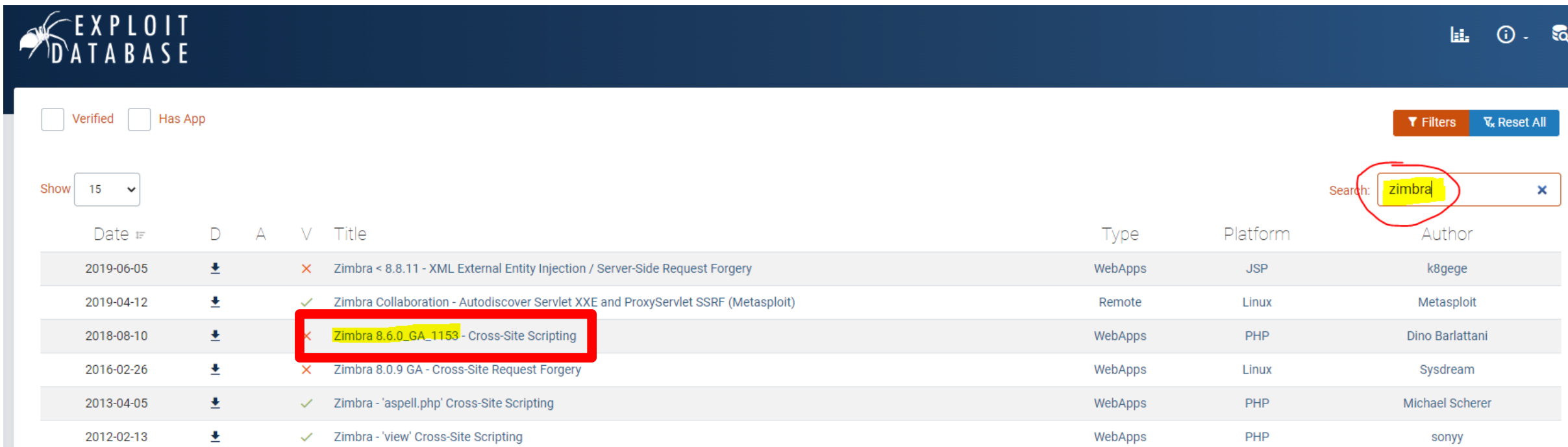


Reconnaissance passive : Accès caméras avec Shodan

// FOUND 1,139 RESULTS



Reconnaissance passive : Shodan & vulnérabilités



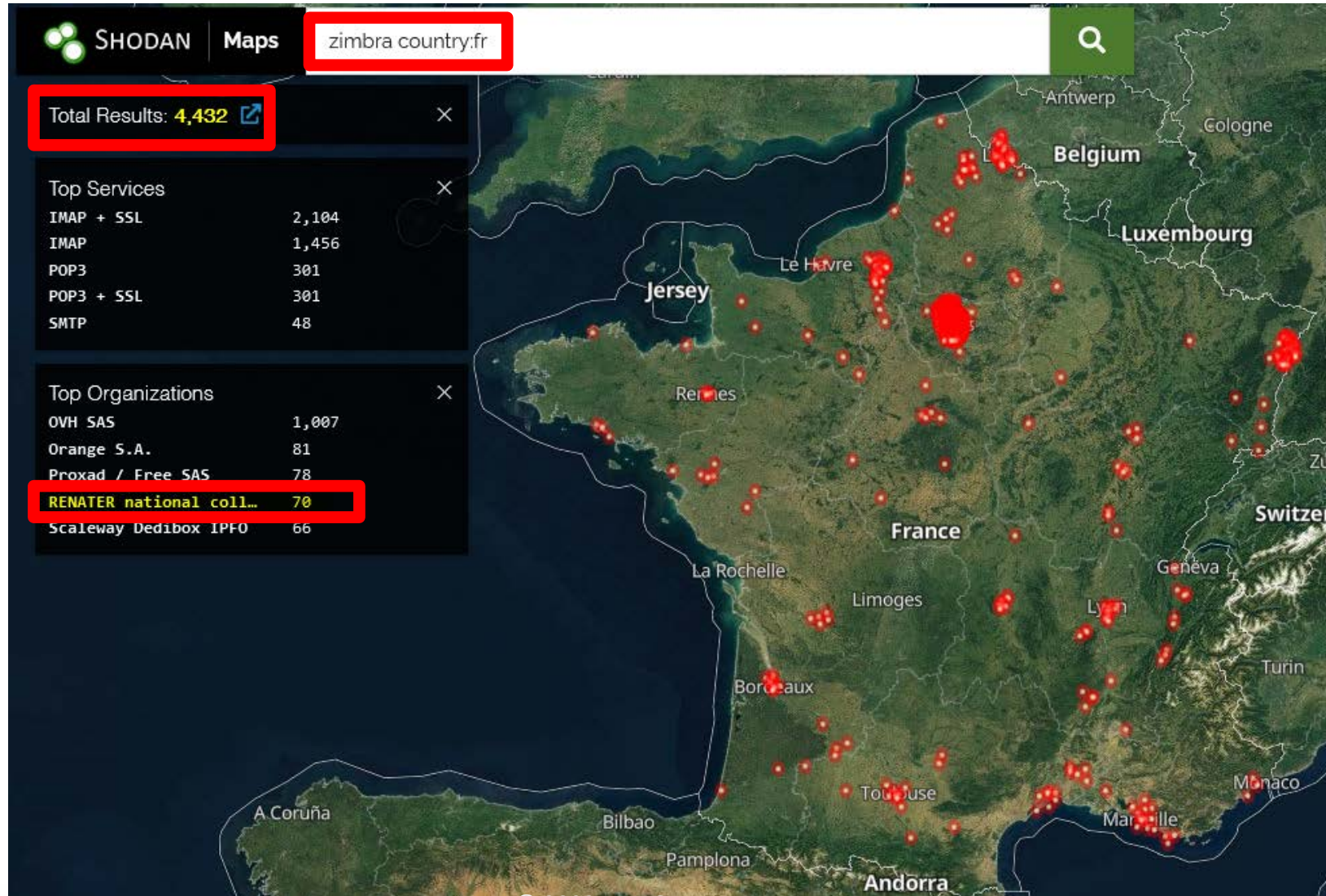
The screenshot shows the Exploit Database interface with a search for 'zimbra'. The search results table is as follows:

Date	D	A	V	Title	Type	Platform	Author
2019-06-05	↓		×	Zimbra < 8.8.11 - XML External Entity Injection / Server-Side Request Forgery	WebApps	JSP	k8gege
2019-04-12	↓		✓	Zimbra Collaboration - Autodiscover Servlet XXE and ProxyServlet SSRF (Metasploit)	Remote	Linux	Metasploit
2018-08-10	↓		×	Zimbra 8.6.0_GA_1153 - Cross-Site Scripting	WebApps	PHP	Dino Barlattani
2016-02-26	↓		×	Zimbra 8.0.9 GA - Cross-Site Request Forgery	WebApps	Linux	Sysdream
2013-04-05	↓		✓	Zimbra - 'aspell.php' Cross-Site Scripting	WebApps	PHP	Michael Scherer
2012-02-13	↓		✓	Zimbra - 'view' Cross-Site Scripting	WebApps	PHP	sony

- Qu'est-ce que le logiciel Zimbra ? ____
- Qu'est-ce que l'IMAP et l'IMAPS ? ____
- Sur quels ports trouve-t-on ces protocoles? ____
- Quelle est la différence entre ces protocoles ? ____



Reconnaissance passive : Exemple avec Shodan



Reconnaissance passive : Exemple avec Shodan

The screenshot displays the Shodan Maps interface. At the top, the search bar contains the query `zimbra 8.6.0_GA_1153 country:fr`. Below the search bar, a sidebar on the left provides summary information:

- Total Results: 01** (with a link icon)
- Top Services:**
 - IMAP + SSL: 34
 - IMAP: 27
- Top Organizations:**
 - OVH SAS: 11
 - ikoula france serveur...: 8
 - Agencja Interaktywna ...: 4
 - Orange S.A.: 4
 - Dedicated Servers: 3

The main map shows a satellite view of France and neighboring countries (Belgium, Luxembourg, Switzerland, Andorra). Red pins indicate the locations of the search results, with a significant cluster in the Paris region and other scattered locations across France and the UK (Jersey).

Reconnaissance passive : Exemple avec Shodan

- Exemple de résultat, avec la recherche : `zimbra 8.6.0_GA_1153 country:fr`

The screenshot shows a Shodan search result for a Zimbra server. The search query is `zimbra 8.6.0_GA_1153 country:fr`. The results are displayed in a grid layout. On the left, there is a 'General Information' section with the following details:

- Hostnames: `www.mail.[redacted].fr, mail.[redacted].fr`
- Domains: `[redacted].FR`
- Country: **France**
- City: **Paris**
- Organization: **Ecole [redacted]**
- ISP: **OVH SAS**
- ASN: `[redacted]`

On the right, there is an 'Open Ports' section showing a list of open ports: 22, 25, 53, 110, 123, 143, 389, 443, 465, 587, 995, 7071, 8080, 8443. The port 143 is highlighted in a black box with the text `143/tcp`.

Below the open ports, there is a list of timestamps and IP addresses, with the most recent one being `2022-09-25T00:03:06.966657`.

On the far right, there is a section showing the output of a Zimbra IMAP server connection, including the following text:

```
* OK IMAP4 ready
* CAPABILITY ACL BINARY CATENATE CHILDREN CONDSTORE ENABLE ESEARCH ESORT I18N
tx SASL-IR SEARCHRES SORT THREAD=ORDEREDSUBJECT UIDPLUS UNSELECT WITHIN XLIST
A001 OK completed
* ID ("NAME" "Zimbra" "VERSION" "8.6.0_GA_1153" "RELEASE" "20141215151116")
A002 OK completed
A003 BAD invalid command
* BYE Zimbra IMAP server terminating connection
A004 OK completed
```

Reconnaissance passive : Exemple avec Shodan

- Exemple de résultat, avec la recherche : `zimbra 8.6.0_GA_1153 country:fr`

51.2...173

Regular View Raw Data History

// TAGS: starttls // LAST SEEN: 2022-09-25

General Information

Hostnames: www.mail...fr, mail...fr

Domains: ...FR

Country: France

City: Paris

Organization: Ecole ... SAS

ISP: OVH SAS

ASN: ...

Open Ports

22 25 53 110 123 143 389 443 465 587 995 7071 8080 8443

143/tcp

```
2022-09-25T00:03:06.966657
2022-08-19T10:19:36.504239
2022-08-14T10:20:21.278447
2022-08-06T16:42:10.719996
2022-06-23T23:35:46.473657
2022-06-21T18:18:59.693001
2022-06-15T14:53:16.708347
2022-06-13T22:06:58.100120
2022-06-11T13:00:51.346260
2022-05-29T14:44:19.258282
```

```
* OK IMAP4 ready
* CAPABILITY ACL BINARY CATENATE CHILDREN CONDSTORE ENABLE ESEARCH ESORT I18N
tx SASL-IR SEARCHRES SORT THREAD=ORDEREDSUBJECT UIDPLUS UNSELECT WITHIN XLIST
A001 OK completed
* ID ("NAME" "Zimbra" "VERSION" "8.6.0_GA_1153" "RELEASE" "20141215151116")
A002 OK completed
A003 BAD invalid command
* BYE Zimbra IMAP server terminating connection
A004 OK completed
```

Reconnaissance passive : Exemple avec Shodan

- Exemple de résultat, avec la recherche : `zimbra 8.6.0_GA_1153 country:fr`

51.2... 173

Regular View Raw Data History

// TAGS: starttls // LAST SEEN: 2022-09-25

General Information

Hostnames: `www.mail.fr, mail.fr`

Domains: `...E.FR`

Country: **France**

City: **Paris**

Organization: **Ecole ...**

ISP: **OVH SAS**

ASN: `...`

Open Ports

22 25 53 110 123 **143** 389 443 465 587 995 7071 8080 8443

Scan Results

143/ tcp

```
2022-09-25T00:03:06.966657
2022-08-19T10:19:36.504239
2022-08-14T10:20:21.278447
2022-08-06T16:42:10.719996
2022-06-23T23:35:46.473657
2022-06-21T18:18:59.693001
2022-06-15T14:53:16.708347
2022-06-13T22:06:58.100120
2022-06-11T13:00:51.346260
2022-05-29T14:44:19.258282
```

```
* OK IMAP4 ready
* CAPABILITY ACL BINARY CATENATE CHILDREN CONDSTORE ENABLE ESEARCH ESORT I18N
tx SASL-IR SEARCHRES SORT THREAD=ORDEREDSUBJECT UIDPLUS UNSELECT WITHIN XLIST
A001 OK completed
* ID ("NAME" "Zimbra" "VERSION" "8.6.0_GA_1153" "RELEASE" "20141215151116")
A002 OK completed
A003 BAD invalid command
* BYE Zimbra IMAP server terminating connection
A004 OK completed
```

Reconnaissance passive : Exemple avec Shodan

- Exemple de résultat, avec la recherche : `zimbra 8.6.0_GA_1153 country:fr`

51.2...173

Regular View Raw Data History

// TAGS: starttls // LAST SEEN: 2022-09-25

General Information

Hostnames: `www.mail...e.fr, mail...e.fr`

Domains: `...E.FR`

Country: **France**

City: **Paris**

Organization: **Ecole ...**

ISP: **OVH SAS**

ASN: `...`

Open Ports

22 25 53 110 123 **143** 389 443 465 587 995 7071 8080 8443

143/tcp

```
2022-09-25T00:03:06.966657
2022-08-19T10:19:36.504239
2022-08-14T10:20:21.278447
2022-08-06T16:42:10.719996
2022-06-23T23:35:46.473657
2022-06-21T18:18:59.693001
2022-06-15T14:53:16.708347
2022-06-13T22:06:58.100120
2022-06-11T13:00:51.346260
2022-05-29T14:44:19.258282
```

```
* 0 IMAP4 ready
* CAPABILITY ACL BINARY CATENATE CHILDREN CONDSTORE ENABLE ESEARCH ESORT I18N
tx SASL-IR SEARCHRES SORT THREAD=ORDEREDSUBJECT UIDPLUS UNSELECT WITHIN XLIST
1001 OK completed
* ID ("NAME" "Zimbra" "VERSION" "8.6.0_GA_1153" "RELEASE" "201412151116")
A002 OK completed
A003 BAD invalid command
* BYE Zimbra IMAP server terminating connection
A004 OK completed
```

Scan

Scan de ports et de services

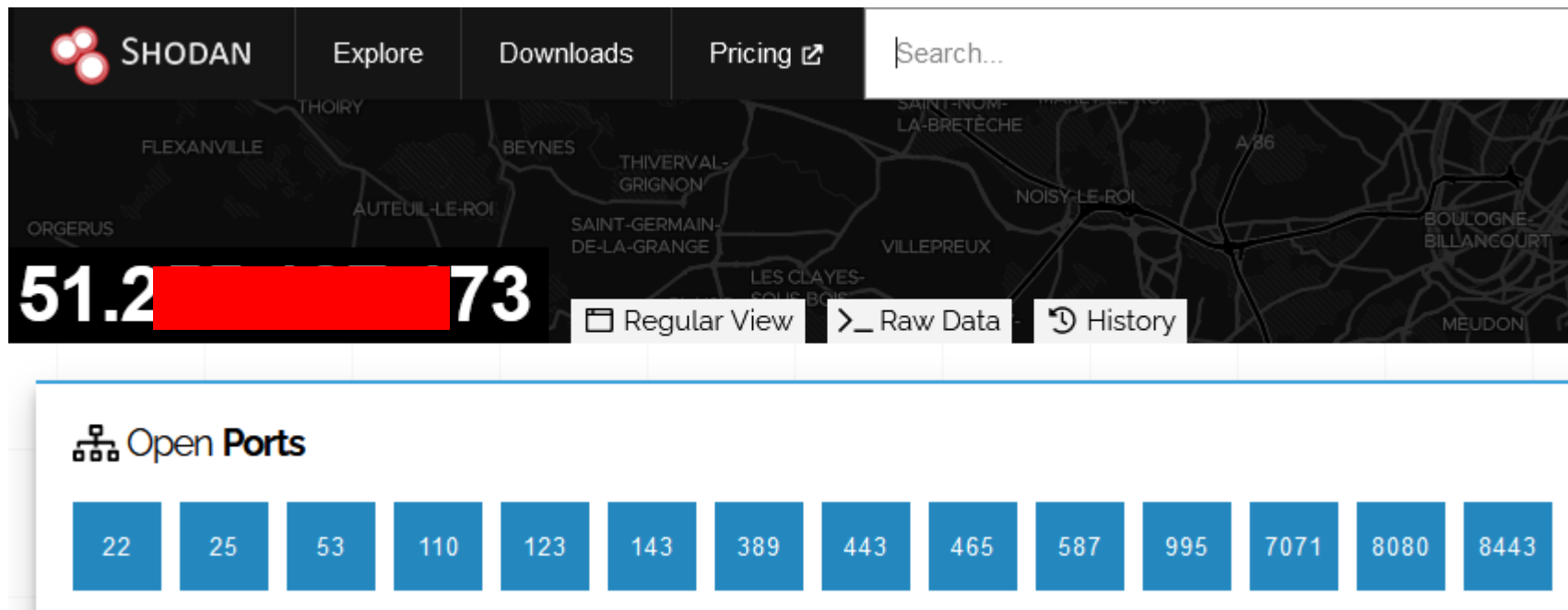
Un peu de Droit

Scan de matériels réseau

Scan de vulnérabilités

Scan : logiciel nmap

- Permet de connaître les services proposés par un serveur
 - Logiciel le plus utilisé **nmap**
 - Laisse des traces sur le serveur => risque d'être détecté



The screenshot displays the SHODAN search interface. At the top, there are navigation tabs for 'Explore', 'Downloads', and 'Pricing', along with a search bar. Below the navigation is a map showing various locations. A large red box obscures the search results, with the numbers '51.2' and '73' visible on either side. Below the map, there are buttons for 'Regular View', 'Raw Data', and 'History'. At the bottom, there is a section titled 'Open Ports' with a grid of blue buttons containing the following port numbers: 22, 25, 53, 110, 123, 143, 389, 443, 465, 587, 995, 7071, 8080, and 8443.



Scan : Exemple de scan de ports et de services

```
# Nmap 7.91 scan initiated Thu Dec 10 14:04:19 2020 as: nmap -sC -sV -A -oN nmap.log 10.10.207.102
Nmap scan report for 10.10.207.102
Host is up (0.25s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|  STAT:
| FTP server status:
|   Connected to ::ffff:10.8.82.14
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   At session startup, client count was 4
|   vsFTPD 3.0.3 - secure, fast, stable
|_End of status
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|  2048 e2:5c:33:22:76:5c:93:66:cd:96:9c:16:6a:b3:17:a4 (RSA)
|  256 1b:6a:36:e1:8e:b4:96:5e:c6:ef:0d:91:37:58:59:b6 (ECDSA)
|_ 256 fb:fa:db:ea:4e:ed:20:2b:91:18:9d:58:a0:6a:50:ec (ED25519)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu Dec 10 14:05:00 2020 -- 1 IP address (1 host up) scanned in 40.76 seconds
```

```
# nmap -A -T4 scanme.nmap.org playground

Starting nmap ( https://nmap.org/ )
Interesting ports on scanme.nmap.org (205.217.153.62):
(The 1663 ports scanned but not shown below are in state: filtered)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 3.9p1 (protocol 1.99)
53/tcp    open  domain
70/tcp    closed gopher
80/tcp    open  http     Apache httpd 2.0.52 ((Fedora))
113/tcp   closed auth
Device type: general purpose
Running: Linux 2.4.X|2.5.X|2.6.X
OS details: Linux 2.4.7 - 2.6.11, Linux 2.6.0 - 2.6.11
Uptime 33.908 days (since Thu Jul 21 03:38:03 2005)

Interesting ports on playground.nmap.org (192.168.0.40):
(The 1659 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE          VERSION
135/tcp    open  msrpc           Microsoft Windows RPC
139/tcp    open  netbios-ssn    Microsoft Windows netbios-ssn
389/tcp    open  ldap?
445/tcp    open  microsoft-ds   Microsoft Windows XP microsoft-ds
1002/tcp   open  windows-icfw?
1025/tcp   open  msrpc           Microsoft Windows RPC
1720/tcp   open  H.323/Q.931    CompTek AquaGateKeeper
5800/tcp   open  vnc-http       RealVNC 4.0 (Resolution 400x250; VNC TCP port: 5900)
5900/tcp   open  vnc             VNC (protocol 3.8)
MAC Address: 00:A0:CC:63:85:4B (Lite-on Communications)
Device type: general purpose
Running: Microsoft Windows NT/2K/XP
OS details: Microsoft Windows XP Pro RC1+ through final release
Service Info: OSs: Windows, Windows XP

Nmap finished: 2 IP addresses (2 hosts up) scanned in 88.392 seconds
```


Scan : Exemple de scan de ports et de services

```
# Nmap 7.91 scan initiated Thu Dec 10 14:04:19 2020 as: nmap -sC -sV -A -oN nmap.log 10.10.207.102
Nmap scan report for 10.10.207.102
Host is up (0.25s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
|_ftp_banner: Anonymous FTP login allowed (FTP code 230)
|_ftp_syst:
|_STAT:
|_FTP server status:
|_Connected to ::ffff:10.8.82.14
|_Logged in as ftp
|_TYPE: ASCII
|_No session bandwidth limit
|_Session timeout in seconds is 300
|_Control connection is plain text
|_Data connections will be plain text
|_At session startup, client count was 4
|_vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
|_ssh_hostkey:
|_2048 e2:5c:33:22:76:5c:93:66:cd:96:9c:16:6a:b3:17:a4 (RSA)
|_256 1b:6a:36:e1:8e:b4:96:5e:c6:ef:0d:91:37:58:59:b6 (ECDSA)
|_256 85:84:41:41:10:01:01:10:01:50:00:00:00:00:00:00 (ED25519)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
|_http_server_header: Apache/2.4.29 (Ubuntu)
|_http_title: Apache2 Ubuntu Default Page: It works
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu Dec 10 14:05:00 2020 -- 1 IP address (1 host up) scanned in 40.76 seconds
```

```
# nmap -A -T4 scanme.nmap.org playground

Starting nmap ( https://nmap.org/ )
Interesting ports on scanme.nmap.org (205.217.153.62):
(The 1663 ports scanned but not shown below are in state: filtered)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 3.9p1 (protocol 1.99)
53/tcp    open  domain
70/tcp    closed gopher
80/tcp    open  http     Apache httpd 2.0.52 ((Fedora))
113/tcp   closed auth
Device type: general purpose
Running: Linux 2.4.X|2.5.X|2.6.X
OS details: Linux 2.4.7 - 2.6.11, Linux 2.6.0 - 2.6.11
Uptime 33.908 days (since Thu Jul 21 03:38:03 2005)

Interesting ports on playground.nmap.org (192.168.0.40):
(The 1659 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE VERSION
135/tcp   open  msrpc    Microsoft Windows RPC
139/tcp   open  netbios-ssn
389/tcp   open  ldap?
445/tcp   open  microsoft-ds Microsoft Windows XP microsoft-ds
1002/tcp  open  windows-icfw?
1025/tcp  open  msrpc    Microsoft Windows RPC
1720/tcp  open  H.323/Q.931 CompTek AquaGateKeeper
5800/tcp  open  vnc-http RealVNC 4.0 (Resolution 400x250; VNC TCP port: 5900)
5900/tcp  open  vnc      VNC (protocol 3.8)
MAC Address: 00:A0:CC:63:85:4B (Lite-on Communications)
Device type: general purpose
Running: Microsoft Windows NT/2K/XP
OS details: Microsoft Windows XP Pro RC1+ through final release
Service Info: OSs: Windows, Windows XP

Nmap finished: 2 IP addresses (2 hosts up) scanned in 88.392 seconds
```

Scan : Exemple de scan de ports et de services

```
# Nmap 7.91 scan initiated Thu Dec 10 14:04:19 2020 as: nmap -sC -sV -A -oN nmap.log 10.10.207.102
Nmap scan report for 10.10.207.102
Host is up (0.25s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
|_ftp_banner: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|  STAT:
| FTP server status:
|   Connected to ::ffff:10.8.82.14
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   At session startup, client count was 4
|   vsFTpd 3.0.3 - secure, fast, stable
|_End of status
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
|_ssh-hostkey:
|  2048 e2:5c:33:22:76:5c:93:66:cd:96:9c:16:6a:b3:17:a4 (RSA)
|  256 1b:6a:36:e1:8e:b4:96:5e:c6:ef:0d:91:37:58:59:b6 (ECDSA)
|_ 256 85:84:31:41:00:01:01:10:01:50:00:00:00:00:00:00 (ED25519)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
|_http_server_header: Apache/2.4.29 (Ubuntu)
|_http_title: Apache2 Ubuntu Default Page: It works
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu Dec 10 14:05:00 2020 -- 1 IP address (1 host up) scanned in 40.76 seconds
```

```
# nmap -A -T4 scanme.nmap.org playground
Starting nmap ( https://nmap.org/ )
Interesting ports on scanme.nmap.org (205.217.153.62):
(The 1663 ports scanned but not shown below are in state: filtered)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 3.9p1 (protocol 1.99)
53/tcp    open  domain
70/tcp    closed gopher
80/tcp    open  http     Apache httpd 2.0.52 ((Fedora))
113/tcp   closed auth
Device type: general purpose
Running: Linux 2.4.X|2.5.X|2.6.X
OS details: Linux 2.4.7 - 2.6.11, Linux 2.6.0 - 2.6.11
Uptime 33 908 days (since Thu Jul 21 03:38:03 2005)

Interesting ports on playground.nmap.org (192.168.0.40):
(The 1659 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE VERSION
135/tcp   open  msrpc    Microsoft Windows RPC
139/tcp   open  netbios-ssn
389/tcp   open  ldap?
445/tcp   open  microsoft-ds Microsoft Windows XP microsoft-ds
1002/tcp  open  windows-icfw?
1025/tcp  open  msrpc    Microsoft Windows RPC
1720/tcp  open  H.323/Q.931 CompTek AquaGateKeeper
5800/tcp  open  vnc-http RealVNC 4.0 (Resolution 400x250; VNC TCP port: 5900)
5900/tcp  open  vnc      VNC (protocol 3.8)
MAC Address: 00:A0:CC:63:85:4B (Lite-on Communications)
Device type: general purpose
Running: Microsoft Windows NT/2K/XP
OS details: Microsoft Windows XP Pro RC1+ through final release
Service Info: OSs: Windows, Windows XP

Nmap finished: 2 IP addresses (2 hosts up) scanned in 88.392 seconds
```



Danger !

Scan : Exemple de scan de ports et de services

```
root@reza-VirtualBox:~# nmap -v -A 192.168.144.10

Starting Nmap 7.60 ( https://nmap.org ) at 2022-09-26 20:49 CEST
NSE: Loaded 146 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 20:49
Completed NSE at 20:49, 0.00s elapsed
Initiating NSE at 20:49
Completed NSE at 20:49, 0.00s elapsed
Initiating Ping Scan at 20:49
Scanning 192.168.144.10 [4 ports]
Completed Ping Scan at 20:49, 0.20s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:49
Completed Parallel DNS resolution of 1 host. at 20:49, 0.01s elapsed
Initiating SYN Stealth Scan at 20:49
Scanning 192.168.144.10 [1000 ports]
Discovered open port 80/tcp on 192.168.144.10
Discovered open port 8080/tcp on 192.168.144.10
Discovered open port 22/tcp on 192.168.144.10
Discovered open port 443/tcp on 192.168.144.10
Discovered open port 53/tcp on 192.168.144.10
Completed SYN Stealth Scan at 20:50, 19.08s elapsed (1000 total ports)
Initiating Service scan at 20:50
Scanning 5 services on 192.168.144.10
PORT      STATE SERVICE  VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 df:e0:81:91:39:81:e0:77:ba:87:fc:56:5c:a7:1a:d5 (RSA)
|   256  be:bf:2b:7d:22:7d:c5:a2:92:2d:7d:74:05:21:1d:44 (ECDSA)
|_  256  34:0a:10:24:be:d5:1a:11:64:18:90:ad:ff:03:50:86 (EdDSA)
53/tcp    open  domain?
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
```

Scan : Exemple de scan de ports et de services

- Lecture des logs sur la machine scannée
 - On voit les traces laissées par **nmap** => potentiellement détectable

```
Sep 26 18:50:17 onetlab sshd[5048]: Did not receive identification string from 192.168.144.8 port 41418
Sep 26 18:50:17 onetlab sshd[5049]: Did not receive identification string from 192.168.144.8 port 41419
Sep 26 18:50:17 onetlab sshd[5050]: Did not receive identification string from 192.168.144.8 port 41420
Sep 26 18:50:17 onetlab sshd[5051]: Did not receive identification string from 192.168.144.8 port 41421
Sep 26 18:50:18 onetlab sshd[5052]: Protocol major versions differ for 192.168.144.8 port 41424: SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3 vs. SSH-1.5-NmapNSE_1.0
Sep 26 18:50:18 onetlab sshd[5055]: Protocol major versions differ for 192.168.144.8 port 41491: SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3 vs. SSH-1.5-Nmap-SSH1-Hostkey
Sep 26 18:50:19 onetlab sshd[5057]: Unable to negotiate with 192.168.144.8 port 41504: no matching host key type found. Their offer: ssh-dss [preauth]
```

```
192.168.144.8 - - [26/Sep/2022:18:50:18 +0000] "GET /robots.txt HTTP/1.1" 404 1093
192.168.144.8 - - [26/Sep/2022:18:50:18 +0000] "OPTIONS / HTTP/1.1" 200 -
192.168.144.8 - - [26/Sep/2022:18:50:18 +0000] "GET /.git/HEAD HTTP/1.1" 404 1096
192.168.144.8 - - [26/Sep/2022:18:50:18 +0000] "OPTIONS / HTTP/1.1" 200 -
192.168.144.8 - - [26/Sep/2022:18:50:18 +0000] "HEAD / HTTP/1.0" 200 -
192.168.144.8 - - [26/Sep/2022:18:50:18 +0000] "POST /sdk HTTP/1.1" 404 1086
192.168.144.8 - - [26/Sep/2022:18:50:18 +0000] "GET / HTTP/1.1" 200 1896
192.168.144.8 - - [26/Sep/2022:18:50:18 +0000] "OPTIONS / HTTP/1.1" 200 -
192.168.144.8 - - [26/Sep/2022:18:50:18 +0000] "CONNECT www.google.com:80 HTTP/1.0" 400 1169
192.168.144.8 - - [26/Sep/2022:18:50:18 +0000] "GET / HTTP/1.0" 200 1896
192.168.144.8 - - [26/Sep/2022:18:50:18 +0000] "PROPFIND / HTTP/1.1" 501 1107
192.168.144.8 - - [26/Sep/2022:18:50:18 +0000] "OPTIONS / HTTP/1.1" 200 -
192.168.144.8 - - [26/Sep/2022:18:50:18 +0000] "OPTIONS / HTTP/1.1" 200 -
192.168.144.8 - - [26/Sep/2022:18:50:18 +0000] "GET / HTTP/1.1" 200 1896
192.168.144.8 - - [26/Sep/2022:18:50:18 +0000] "POST / HTTP/1.1" 200 1896
192.168.144.8 - - [26/Sep/2022:18:50:18 +0000] "GET /nmaplowercheck1664218217 HTTP/1.1" 404 1107
```

Expliquez la différence d'heure ?



2022-09-26 20:49 CEST

Scan : Exemple de scan de ports et de services

- Lecture des logs sur la machine scannée
 - On voit les traces laissées par **nmap** => potentiellement détectable

```
Sep 26 18:50:17 onetlab sshd[5048]: Did not receive identification string from 192.168.144.8 port 41418
Sep 26 18:50:17 onetlab sshd[5049]: Did not receive identification string from 192.168.144.8 port 41419
Sep 26 18:50:17 onetlab sshd[5050]: Did not receive identification string from 192.168.144.8 port 41420
Sep 26 18:50:17 onetlab sshd[5051]: Did not receive identification string from 192.168.144.8 port 41421
Sep 26 18:50:18 onetlab sshd[5052]: Protocol major versions differ for 192.168.144.8 port 41424: SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3 vs. SSH-1.0-NmapNSE_1.0
Sep 26 18:50:18 onetlab sshd[5055]: Protocol major versions differ for 192.168.144.8 port 41491: SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3 vs. SSH-1.0-Nmap-SSH1-Hostke
Sep 26 18:50:19 onetlab sshd[5057]: Unable to negotiate with 192.168.144.8 port 41504: no matching host key type found. Their offer: ssh-dss [preauth]
```


```
192.168.144.8 - - [26/Sep/2022:18:50:18 +0000] "GET /robots.txt HTTP/1.1" 404 1093
192.168.144.8 - - [26/Sep/2022:18:50:18 +0000] "OPTIONS / HTTP/1.1" 200 -
192.168.144.8 - - [26/Sep/2022:18:50:18 +0000] "GET /.git/HEAD HTTP/1.1" 404 1096
192.168.144.8 - - [26/Sep/2022:18:50:18 +0000] "OPTIONS / HTTP/1.1" 200 -
192.168.144.8 - - [26/Sep/2022:18:50:18 +0000] "HEAD / HTTP/1.0" 200 -
192.168.144.8 - - [26/Sep/2022:18:50:18 +0000] "POST /sdk HTTP/1.1" 404 1086
192.168.144.8 - - [26/Sep/2022:18:50:18 +0000] "GET / HTTP/1.1" 200 1896
192.168.144.8 - - [26/Sep/2022:18:50:18 +0000] "OPTIONS / HTTP/1.1" 200 -
192.168.144.8 - - [26/Sep/2022:18:50:18 +0000] "CONNECT www.google.com:80 HTTP/1.0" 400 1169
192.168.144.8 - - [26/Sep/2022:18:50:18 +0000] "GET / HTTP/1.0" 200 1896
192.168.144.8 - - [26/Sep/2022:18:50:18 +0000] "PROPFIND / HTTP/1.1" 501 1107
192.168.144.8 - - [26/Sep/2022:18:50:18 +0000] "OPTIONS / HTTP/1.1" 200 -
192.168.144.8 - - [26/Sep/2022:18:50:18 +0000] "OPTIONS / HTTP/1.1" 200 -
192.168.144.8 - - [26/Sep/2022:18:50:18 +0000] "GET / HTTP/1.1" 200 1896
192.168.144.8 - - [26/Sep/2022:18:50:18 +0000] "POST / HTTP/1.1" 200 1896
192.168.144.8 - - [26/Sep/2022:18:50:18 +0000] "GET /nmaplowercheck1664218217 HTTP/1.1" 404 1107
```

Expliquez la différence d'heure ?



2022-09-26 20:49 CEST

Scan : Que dit la loi ?

- La technique c'est bien, mais penchons nous sur le Droit : 
 - Est-ce légal de réaliser un scan/balayage de ports ? _____
 - Quels sont les articles du code pénal qui traitent de la cybercriminalité ? _____
 - Est-ce qu'ils s'appliquent au scan/balayage de ports ? _____
 - Expliquer les sanctions financières infligées par l'article 323-1 du CP. _____

Scan : Scan du réseau

- Après les scans de serveurs, place aux scans d'équipements réseau
 - Switches,
 - routeurs,
 - imprimantes,
 - firewall,
 - ...

Scan : Scan de vulnérabilités - Nessus

- Exemple de rapport de Nessus :





192.168.206.134 Basic > 192.168.206.134 > 80 / tcp List Detail 64 results

Plugin ID	Name	Port	Severity
24011	WordPress Trackback Charset Decoding SQL Injection	www (80/tcp)	Medium
55976	Apache HTTP Server Byte Range DoS	www (80/tcp)	High
47830	CGI Generic Injectable Parameter	www (80/tcp)	Low
47832	CGI Generic On Site Request Forgery (OSRF)	www (80/tcp)	Medium
42427	CGI Generic SQL Injection (HTTP Headers)	www (80/tcp)	High
49067	CGI Generic HTML Injections (quick test)	www (80/tcp)	Medium
33817	CGI Generic Tests Load Estimation (all tests)	www (80/tcp)	Low
50494	CGI Generic Path Traversal (quick test)	www (80/tcp)	Medium
51972	CGI Generic Cross-Site Scripting (Parameters Names)	www (80/tcp)	Medium
51973	CGI Generic SQL Injection (Parameters Names)	www (80/tcp)	High
11139	CGI Generic SQL Injection	www (80/tcp)	High

Scan : Scan de vulnérabilités - OpenVAS

- Exemple de rapport d'OpenVAS :

Date	Status	Task	Severity	Scan Results					Actions
				High	Medium	Low	Log	False Pos.	
Thu Jan 9 03:05:08 2020	Done	Immediate scan of IP 192.168.11.137	N/A	0	0	0	0	0	 



Report: Results (312 of 734)

ID: 97cc63d0-65d7-45ee-8ca8-711df1baa7dd
Modified:
Created:
Owner: admin

Vulnerability	Severity	QoD	Host	Location	Actions
rexec Passwordless / Unencrypted Cleartext Login	10.0 (High)	75%	192.168.11.137	512/tcp	 
Samba End Of Life Detection	10.0 (High)	75%	192.168.11.137	445/tcp	 
Samba 'TALLOC_FREE()' Function Remote Code Execution Vulnerability	10.0 (High)	75%	192.168.11.137	445/tcp	 
PHP Multiple Vulnerabilities - Aug08	10.0 (High)	75%	192.168.11.137	80/tcp	 
PHP Version < 5.2.7 Multiple Vulnerabilities	10.0 (High)	75%	192.168.11.137	80/tcp	 
PHP End Of Life Detection (Linux)	10.0 (High)	75%	192.168.11.137	80/tcp	 
MySQL End Of Life Detection (Linux)	10.0 (High)	75%	192.168.11.137	3306/tcp	 
PostgreSQL End Of Life Detection (Linux)	10.0 (High)	75%	192.168.11.137	5432/tcp	 



Obtenir l'accès

Obtenir l'accès : Analyse des données

- Le hacker réunit toutes les informations collectées
- Analyse les vulnérabilités trouvées
- Analyse les systèmes trouvés
- Cartographie le réseau et ses équipements
- Cartographie les serveurs
- Établit des scénarios d'attaques pour s'introduire dans le système

Obtenir l'accès : Tentatives d'attaques

- Le hacker va tenter d'utiliser des scripts/méthodes d'attaques :
 - Phishing
 - Attaques par dépassement de tampon (Buffer overflow)
 - Attaques par injection de code (ex : injection SQL)
 - XML External Entity attack
 - Attaque par force brute
 - Attaque par spoofing
 - Attaque man in the middle
 - Attaque par déni de service
 - Session hijacking
 - Utilisation d'un exploit "zero day"

définir
ces attaques



Maintenir l'accès

Maintenir l'accès : les techniques

- Rebond sur d'autres machines
- Accès aux annuaires (LDAP, AD, Azure AD)
- Compromission d'autres machines
- Installation de chevaux de Troie
- Étendre ses privilèges (privilege escalation)
- Installer des rootkits
- Utilisation de comptes obsolètes (qu'on ne remarque pas)

Effacer ses traces

Effacer ses traces : les actions à mener

- Effacer les fichiers qu'il a utilisés pour s'introduire
- Supprimer les lignes de logs le concernant sur les serveurs
- Utilisation possible d'un rançongiciel (ransomware)

Anticiper l'attaque

Analyse de logs « à la main »
Utilisation de logiciels de type SIEM
Visualisation de données
Anticiper les attaques avec la CTI

Analyser pour anticiper

- Trouver l'introuvable
 - À la main, par une analyse des traces et journaux d'évènements
 - Automatiquement avec des logiciels de monitoring

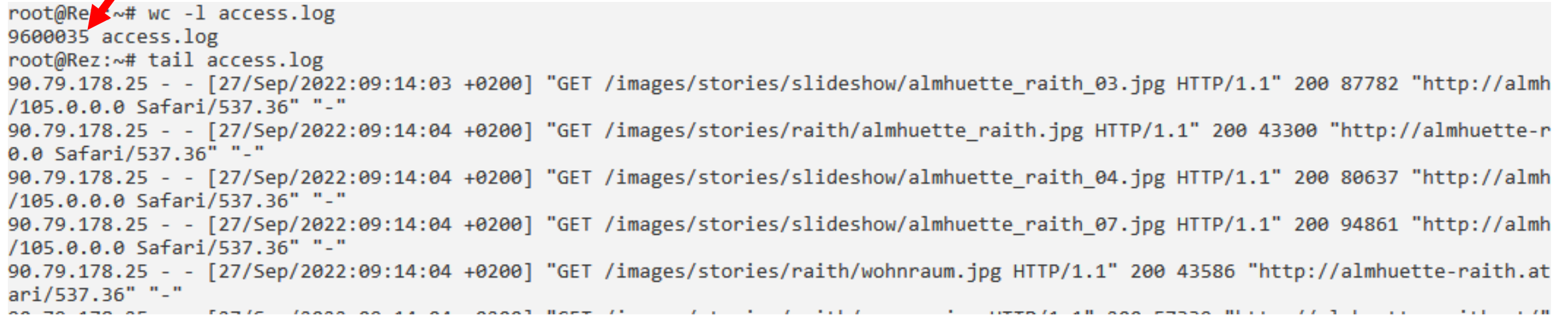
Analyse manuelle : prérequis

- Bonnes connaissances
 - Linux (cat, wc, awk, grep, sed, cut, head, tail, sort, uniq, diff)
 - Logiciels de type client/serveur (apache, mysql ...)
 - Structure de logs (access.log, error.log, auth.log, messages.log ...)
 - En réseau (TCP/IP, adressage ...)

Analyse manuelle : obtention du fichier

- Identifier et récupérer le fichier de logs
- <http://www.almhuetten-raith.at/apache-log/access.log>

9 millions de lignes !!!

A terminal window showing the execution of 'wc -l access.log' and 'tail access.log'. A red arrow points to the first line of the terminal output. The output shows the file size as 9600035 lines and several log entries for GET requests to image files.

```
root@Reza:~# wc -l access.log
9600035 access.log
root@Reza:~# tail access.log
90.79.178.25 - - [27/Sep/2022:09:14:03 +0200] "GET /images/stories/slideshow/almhuetten_raith_03.jpg HTTP/1.1" 200 87782 "http://almh
/105.0.0.0 Safari/537.36" "-"
90.79.178.25 - - [27/Sep/2022:09:14:04 +0200] "GET /images/stories/raith/almhuetten_raith.jpg HTTP/1.1" 200 43300 "http://almhuetten-r
0.0 Safari/537.36" "-"
90.79.178.25 - - [27/Sep/2022:09:14:04 +0200] "GET /images/stories/slideshow/almhuetten_raith_04.jpg HTTP/1.1" 200 80637 "http://almh
/105.0.0.0 Safari/537.36" "-"
90.79.178.25 - - [27/Sep/2022:09:14:04 +0200] "GET /images/stories/slideshow/almhuetten_raith_07.jpg HTTP/1.1" 200 94861 "http://almh
/105.0.0.0 Safari/537.36" "-"
90.79.178.25 - - [27/Sep/2022:09:14:04 +0200] "GET /images/stories/raith/wohnraum.jpg HTTP/1.1" 200 43586 "http://almhuetten-raith.at
ari/537.36" "-"
```

Analyse manuelle : structure du log apache

Adresse IP

Horodatage

Type de requête et Ressources demandées

```
90.79.178.25 - [27/Sep/2022:09:14:03 +0200] "GET /images/stories/slideshow/almhuetta raith 03.jpg HTTP/1.1" 200 87782  
"http://almhuetta-raith.at/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0  
Safari/537.36" "-"  
User Agent qui détermine le navigateur
```

- Utilisation d'une expression régulière pour définir l'adresse IP :

90.79.178.25

$^{\wedge}([0-9]{1,3}\.?)^{4}$

Au besoin, s'aider de <https://regex101.com/>

Analyse manuelle : Extraire des données

- ***Quelles sont les 3 adresses IP qui ont interrogé le plus de fois notre serveur apache, et de quel pays sont-elles issues ?***
- **Décomposition du problème :**
 - Extraire la 1^{ère} colonne qui contient les adresses IP
 - *On a des lignes, où la 1^{ère} colonne contient des caractères alphabétiques ...*
 - Les trier par ordre « alphabétique »
 - Compter chaque occurrence d'adresse IP
 - Ne garder que les 3 adresses IP les plus nombreuses

Analyse manuelle : Extraire des données

- Décomposition du problème :
 - Extraire la 1^{ère} colonne qui contient les adresses IP
 - *On a des lignes, où la 1^{ère} colonne contient des caractères alphabétiques ...*
 - Les trier par ordre « alphabétique »
 - Compter chaque occurrence d'adresse IP
 - Ne garder que les 3 adresses IP les plus nombreuses

```
root@Rez:~# awk '/^([0-9]{1,3}\.?)\{4}/ { print $1 }' access.log | sort | uniq -c | sort -rn | head -3
4305147 47.39.156.135
1959541 96.32.128.5
1572800 73.169.232.206
```

Analyse manuelle : Extraire des données

- Décomposition du problème :
 - Extraire la 1^{ère} colonne qui contient les adresses IP
 - *On a des lignes, où la 1^{ère} colonne contient des caractères alphabétiques ...*
 - Les trier par ordre « alphabétique »
 - Compter chaque occurrence d'adresse IP
 - Ne garder que les 3 adresses IP les plus nombreuses

```
root@Rez:~# awk '/^([0-9]{1,3}\.){4}/ { print $1 }' access.log | sort | uniq -c | sort -rn | head -3
4305147 47.39.156.135
1959541 96.32.128.5
1572800 73.169.232.206
```


Analyse manuelle : Extraire des données

- Décomposition du problème :
 - Extraire la 1^{ère} colonne qui contient les adresses IP
 - *On a des lignes, où la 1^{ère} colonne contient des caractères alphabétiques ...*
 - Les trier par ordre « alphabétique »
 - Compter chaque occurrence d'adresse IP
 - Ne garder que les 3 adresses IP les plus nombreuses

```
root@Rez:~# awk '/^([0-9]{1,3}\.){4}/ { print $1 }' access.log | sort | uniq -c | sort -rn | head -3
4305147 47.39.156.135
1959541 96.32.128.5
1572800 73.169.232.206
```

Analyse manuelle : Extraire des données

- Décomposition du problème :
 - Extraire la 1^{ère} colonne qui contient les adresses IP
 - *On a des lignes, où la 1^{ère} colonne contient des caractères alphabétiques ...*
 - Les trier par ordre « alphabétique »
 - Compter chaque occurrence d'adresse IP
 - Ne garder que les 3 adresses IP les plus nombreuses

```
root@Rez:~# awk '/^([0-9]{1,3}\.){4}/ { print $1 }' access.log | sort | uniq -c | sort -rn | head -3
4305147 47.39.156.135
1959541 96.32.128.5
1572800 73.169.232.206
```

Analyse manuelle : Analyser les données

- *Quelles sont les 3 adresses IP qui ont interrogé le plus de fois notre serveur apache, et de quel pays sont-elles issues ?*
- A présent, que nous avons les adresses IP, nous pouvons utiliser un site web de type « whois », qui peut nous donner le pays d'appartenance.
- Nous pouvons aussi utiliser les commandes **whois** ou **geoiplookup**

```
root@Rez:~# awk '/^([0-9]{1,3}\.?)^{4}/ { print $1 }' access.log | sort | uniq -c | sort -rn | head -3 | awk '{ print "geoiplookup ",$2 }' | sh
GeoIP Country Edition: US, United States
GeoIP Country Edition: US, United States
GeoIP Country Edition: US, United States
```

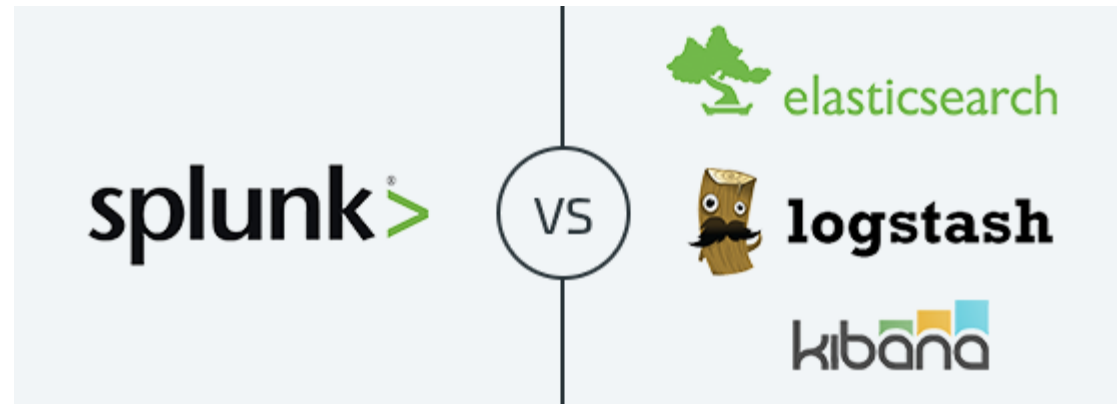
Analyse automatique : Principe de fonctionnement

- SIEM : Security Information and Event Management
- SOC : Security Operation Center



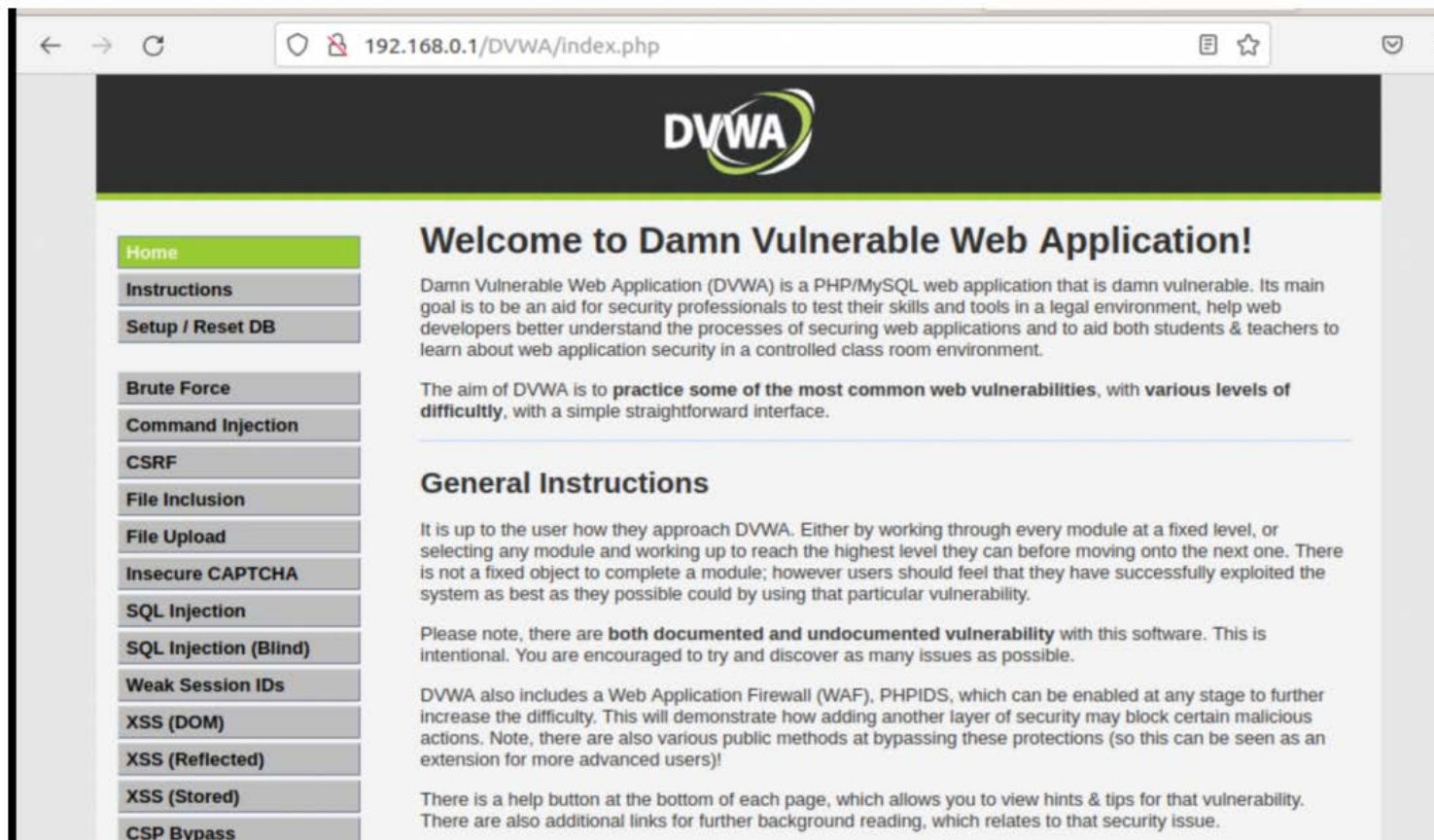
Analyse automatique : Les logiciels

- Outils les plus utilisés en entreprise :
 - Splunk – solution propriétaire
 - ELK (Elasticsearch, Logstash, Kibana) – solution open source



Analyse automatique : Exemple DVWA

- Utilisation de DVWA (<https://github.com/digininja/DVWA>)



Analyse automatique : Exemple DVWA

- Attaque par injection SQL



The screenshot shows a web browser window displaying the DVWA (Damn Vulnerable Web Application) interface. The address bar shows the URL: `192.168.0.1/DVWA/vulnerabilities/sqli/?id="+or+1%3D1%3B&Submit=Submit#`. The page title is "Vulnerability: SQL Injection". On the left side, there is a navigation menu with buttons for "Home", "Instructions", "Setup / Reset DB", "Brute Force", and "Command Injection". The main content area features a "User ID:" label followed by a text input field containing the payload `" or 1=1;`, which is highlighted with a red rectangular box. To the right of the input field is a "Submit" button. Below the input field, there is a section titled "More Information".

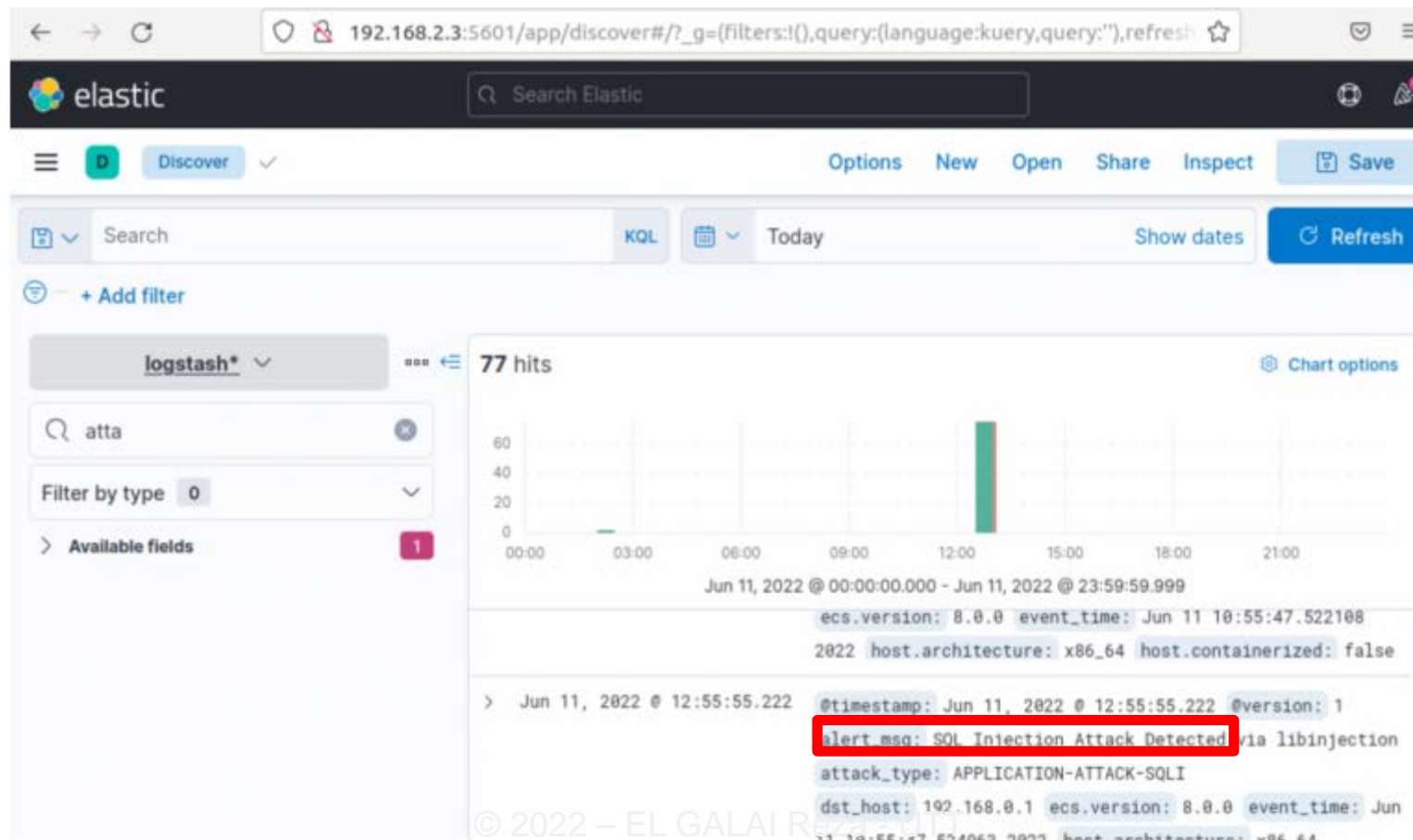
Analyse automatique : Exemple DVWA

- Détection de l'attaque dans les logs :

```
...AAM\""), "[file \"/usr/share/modsecurity-crs/rules/REQUEST-942-APPLICATION-ATTACK-SQLI.conf\"") [line \"/68\"") [id \"/942100\"") [msg \"/SQL Injection Attack Detected via libinjection\"") [data \"/Matched Data: s&1; found within ARGS:id: \"/\\\\\\\\\\\\\\\\x22 or '=1;\"") [severity \"/CRITICAL\"") [ver \"/OWASP_CRS/3.2.0\"") [tag \"/application-multi\"") [tag \"/language-multi\"") [tag \"/platform-multi\"") [tag \"/attack-sqli\"") [tag \"/paranoia-level/1\"") [tag \"/OWASP_CRS\"") [tag \"/OWASP_CRS/WEB_ATTACK/SQL_INJECTION\"") [tag \"/WASCTC/WASC-19\"") [tag \"/OWASP_TOP_10/A1\"") [tag \"/OWASP_AppSensor/CIE1\"") [tag \"/PCI/6.5.2\"") [hostname \"/192.168.0.1\"") [uri \"/DVWA/vulnerabilities/sqli/\"") [unique_id \"/YqR0s8a5lZDDy1Wg11UTogAAAAM\"")], "[file \"/usr/share/modsecurity-crs/rules/REQUEST-949-BLOCKING-EVALUATION.conf\"") [line \"/93\"") [id \"/949110\"") [msg \"/Inbound Anomaly Score Exceeded (Total Score: 8)\"") [severity \"/CRITICAL\"") [ver \"/OWASP_CRS/3.2.0\"") [tag \"/application-multi\"") [tag \"/language-multi\"") [tag \"/platform-multi\"") [tag \"/attack-generic\"") [hostname \"/192.168.0.1\"") [uri \"/DVWA/vulnerabilities/sqli/\"") [unique_id \"/YqR0s8a5lZDDy1Wg11UTogAAAAM\"")], "[file \"/usr/share/modsecurity-crs/rules/RESPONSE-980-CORRELATION.conf\"") [line \"/91\"") [id \"/980130\"") [msg \"/Inbound Anomaly Score Exceeded (Total Inbound Score: 8 - SQLI=5,XSS=0,RFI=0,LFI=0,RCE=0,PHPI=0,HTTP=0,SESS=0): individual paranoia level scores: 8, 0, 0, 0\"") [ver \"/OWASP_CRS/3.2.0\"") [tag \"/event-correlation\"") [hostname \"/192.168.0.1\"") [uri \"/DVWA/vulnerabilities/sqli/index.php\"") [unique_id \"/YqR0s8a5lZDDy1Wg11UTogAAAAM\"")], "handler": "application/x-httpd-php", "stopwatch": {"p1": 795, "p2": 3980, "p3": 90, "p4": 1001, "p5": 635, "sr": 171, "sw": 0, "l": 0, "gc": 0}, "response_body_dechunked": true, "producer": ["ModSecurity for Apache/2.9.3 (http://www.modsecurity.org/)", "OWASP_CRS/3.2.0"], "server": "Apache/2.4.41 (Ubuntu)", "engine_mode": "DETECTION_ONLY"}...
```

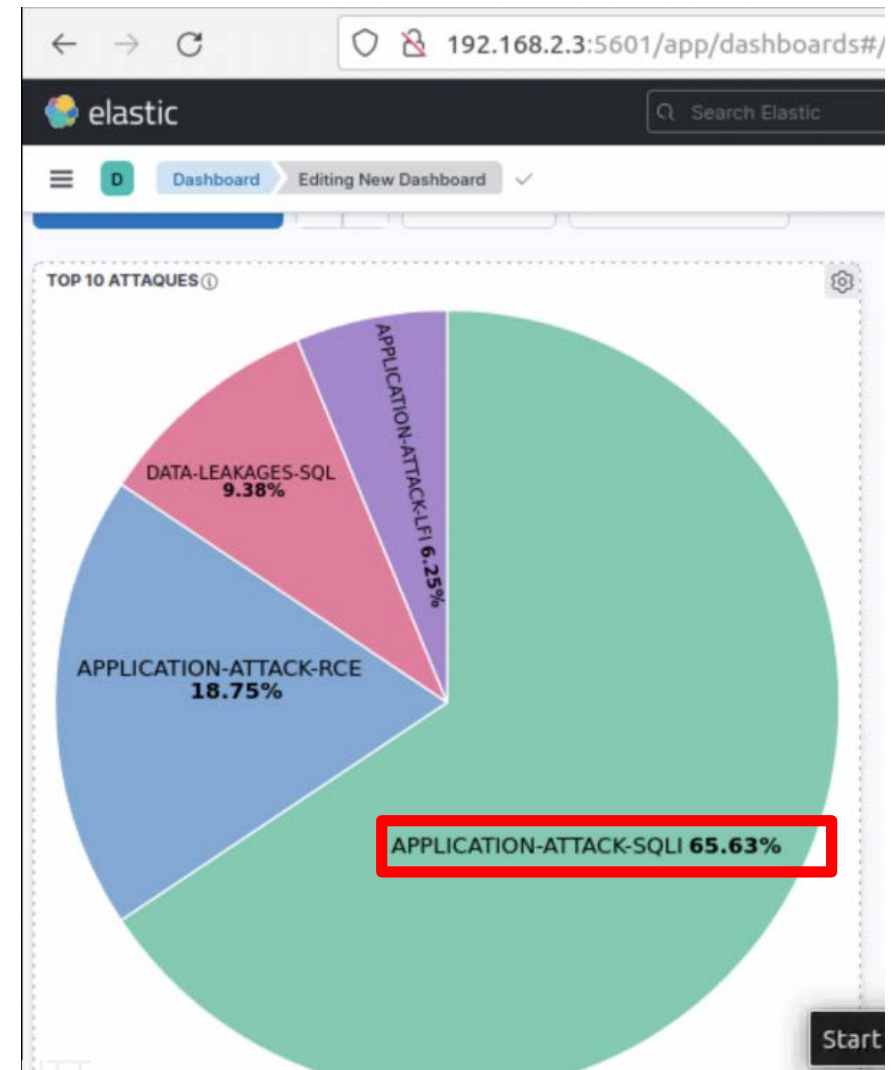

Analyse automatique : Exemple DVWA

- Visualisation de l'attaque sur la console ELK :



Analyse automatique : Exemple DVWA

Reporting sur Kibana après quelques attaques courantes.



Anticiper : La Cyber Threat Intelligence (CTI)

- Collecter des informations pour identifier/attribuer les menaces
- S'apparente au renseignement militaire
- S'appuie sur des indices de compromission (IOC)
- Les modes d'actions des attaquants y sont décrits (TTP)
- Fort recours à l'OSINT, SOCMINT, HUMINT
- Plateformes de partage d'informations
- Activité rattachée aux SOCs ou aux CERT/CSIRT

Merci de votre attention !