



# DOCUMENTATION SNIFFER

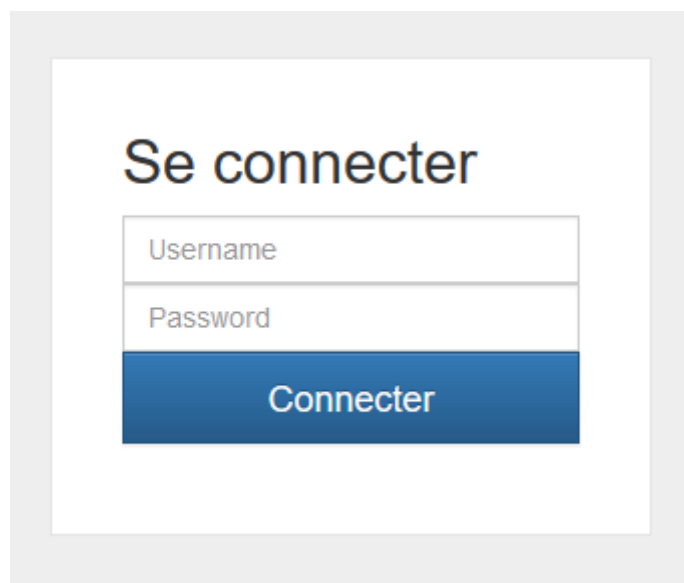
NICOLAS CHARPENTIER, WILLIAM  
GALBY, SALMA HLILI, FREDERIQUE  
ROGANDJI, LOIC VANDERSCHOOTEN

## Connexion

Pour se connecter a l'application sniffer il faut saisir les informations suivantes :

Login : alexis

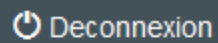
Mot de passe : ynov



The image shows a login form with the title "Se connecter". It contains two input fields: "Username" and "Password". Below the fields is a blue button labeled "Connecter".

## Déconnexion

Pour se déconnecter de l'application sniffer il suffit de cliquer sur le lien « déconnexion » a gauche de l'interface de l'application.

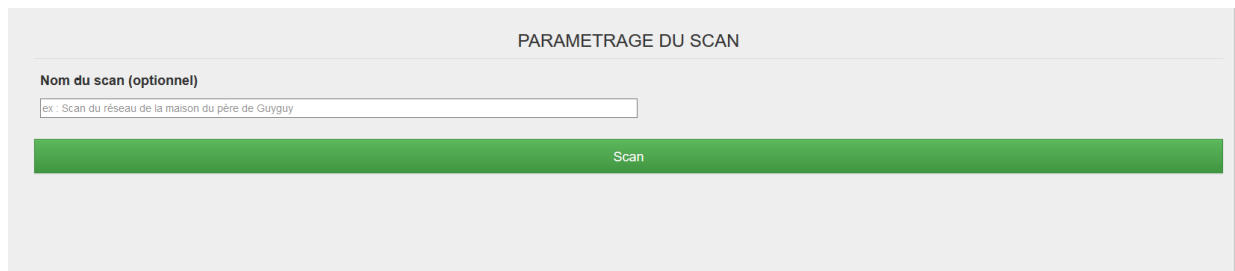


The image shows a dark grey button with a power icon and the text "Deconnexion".

## Scan

Le sniffer permet à l'utilisateur d'identifier le réseau sur lequel il se trouve. Cette fonctionnalité est assurée par le scan. Dans les faits l'application va faire remonter dans l'interface les différentes machines présentes sur le réseau afin de pouvoir effectuer des actions en relation avec ces machines par la suite.

Pour lancer le scan, donnez lui un nom, puis cliquez sur « Scan » ou touche clavier « Entré ».



PARAMETRAGE DU SCAN

**Nom du scan (optionnel)**

ex : Scan du réseau de la maison du père de Guyguy

Scan

## Sniff

Le sniffer permet aussi à l'utilisateur de « renifler » les échanges de données entre les différentes machines du réseau. La fonctionnalité Sniff prend donc en paramètres les adresses IP sélectionnées ainsi que les ports afin de préciser sur quel canal l'utilisateur souhaite afficher les données. L'application permet aussi à l'utilisateur de choisir le nombre de paquet que l'utilisateur souhaite « renifler ». Pour faciliter le paramétrage du sniff l'application propose de sniffer le réseau avec des ports prédéfinis tel que le web ou les mail.

PARAMETRAGE DU SNIFF

<b>Protocole(s)</b> -TCP- -UDP- -ICMP- -ARP- <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<b>Port(s)</b> ex : 110-120-80
<b>Prédéfini(s)</b> -COURRIEL- -WEB- <input type="checkbox"/> <input type="checkbox"/>	<b>Nombre de paquet</b> <input type="text"/>

Sniffer

Afin de lancer le sniff, renseignez les champs que vous désirez puis cliquez sur le bouton « Sniffer », et non touche clavier « Entré ».

- Note :
- Les ports doivent être séparés par des « - ».
  - Si le nombre de paquets n'est pas défini, il sera à 3 par défaut.
  - Si le navigateur indique que la page ne répond pas, c'est que le sniff ne trouve rien.

## Liste des Scans

La liste des scans affiche la liste des scans.

The screenshot shows the 'Données en base sur les scans précédents effectués' section. It includes a sidebar with navigation options like 'Liste des scans', 'Liste des sniffs', and 'Liste des victimes'. The main content area displays two scan entries:

- ids : 1**, nom : 1er, date : 2016-01-17. It lists 3 distinct victims:
 

idV	ipV	macV	idSnfk
1	192.168.79.1	00:50:56:c0:00:08	1
2	192.168.79.2	00:50:56:f7:ad:ee	1
3	192.168.79.254	00:50:56:ef:5b:95	1
- ids : 2**, nom : 11, date : 2016-01-17. It lists 3 distinct victims:
 

idV	ipV	macV	idSnfk
4	192.168.79.1	00:50:56:c0:00:08	2
5	192.168.79.2	00:50:56:f7:ad:ee	2
6	192.168.79.254	00:50:56:ef:5b:95	2

A green 'Supprimer' button is located at the bottom.

## Liste des sniffs

La liste des victimes affiche la liste des sniffs.

The screenshot shows the 'Données en base sur les sniffs précédents effectués' section. It displays three sniff entries:

- idSn : 1**, dateSn : 2016-01-17 22:05:37, FiltreSn : b\*00:00:00:00:00:00:00\*. It contains 2 packets:
 

idP	corpsP	macDestP	macSrcP	ipDestP	ipSrcP	portDestP	portSrcP	protocoleP	idSnfk
1	b?P?/?ac?e?3?af?7?d?e?d?e?i?vf?ad?/?0?3?0?6?e?5?v?ac?b?2?0?b*?1?F?4?i?v?3?ac?&?8?3?P?-B?/?0?d?ad?/?ac?/?f?/?ad?/?ec?/?1?/?1?2?d?0?7?u?b?b?d?c?/?a?z?u?8?2?h?e?z?w?e?f?e?b?/?v?9?b?a?3?w?c?2?w?0?/?b?b?5?5?v?1?2?v?1?u?b?c?/?c?7?u?d?/?ac?/?c?v?1?9?x?1?b?/ac?/?s?v?4?4?z?q?c?/?i?v?1?3?w?3?w?e?d?u?6?w?e?8?/?u?b?b?v?a?h?v?d?/?7?j?d?f?/?w?e?c?/?u?9?/?u?e?z?u?9?/?u?9?/?d?e?c?/?0?e?u?d?/?u?9?1?5?v<?c?3?w?e?/?u?0?1?u?9?/?1?/?b?u?d?d?L?/?	00:50:56:c0:00:08	00:0c:29:41:4b:9d	192.168.79.1	192.168.79.130	31899	22	6	1
2	b*00:00:00:00:00:00:00*	00:0c:29:41:4b:9d	00:50:56:c0:00:08	192.168.79.130	192.168.79.1	22	31899	6	1
- idSn : 2**, dateSn : 2016-01-17 22:11:46, FiltreSn : b\*00:00:00:00:00:00:00\*. It contains 3 packets:
 

idP	corpsP	macDestP	macSrcP	ipDestP	ipSrcP	portDestP	portSrcP	protocoleP	idSnfk
3	b*x?1e?x?c?d?1?c?u?f?c?v?e?3?y?U?Q?v?19?/*?c?/?0?e?u?b?/?s?d?2?/?1?4?u?2?/?u?6?>/?u?0?/?u?9?/?u?8?3?u?a?/?d?u?9?/?w?e?/?i?/?a?/?0?/?0?/?e?/?b?/?e?/?0?/?3?/?u?8?/?U?/?u?b?/?x?1?2?e?F?/?0?e?/?c?/?3?/?u?1?1?/?j?/?u?d?/?1?/?u?d?/?0?/?u?b?/?0?/?a?/?z?/?1?/?5?/?a?/?2?/?*?/?u?d?/?e?/?1?/?7?/?e?/?a?/?c?/?1?/?a?/?i?/?s?/?x?/?7?/?e?/?e?/?u?/?1?/?1?/?E?/?-/?u?d?/?0?/?3?/?1?/?0?/?u?/?7?/?e?/?c?/?u?/?d?/?e?/?9?/?v?/?b?/?6?/?i?/?7?/?a?/?d?/?3?/?x?/?b?/?a?/?b?/?u?/?c?/?u?/?9?/?7?/?b?/?e?/?u?/?d?/?f?/?u?/?9?/?c?/?j?/?x?1?/?3?/?w?e?/?d?/?5?/?1?/?6?/?w?e?/?d?/?	00:50:56:c0:00:08	00:0c:29:41:4b:9d	192.168.79.1	192.168.79.130	31899	22	6	2
4	b*00:00:00:00:00:00:00*	00:0c:29:41:4b:9d	00:50:56:c0:00:08	192.168.79.130	192.168.79.1	22	31899	6	2
- idSn : 3**, dateSn : 2016-01-17 22:43:56, FiltreSn : (empty).
- idSn : 4**, dateSn : 2016-01-17 (empty).

# DOCUMENTATION

## Liste des victimes

La liste des victimes affiche la liste des victimes.

Si on veut supprimer une victime, cela supprimera uniquement la victime pour son ID, mais elle sera toujours présente si elle a été scannée plusieurs fois.



idP	corpsP	macDestP	macSrcP	ipDestP	ipSrcP	portDestP	portSrcP	protocoleP	idSnrk
1	b7pUj uc9ae3rof7vdsue5uf7ad7ab3oGve5sa3u82ufa*1f4\\aa3vac&v83P>8I' v8dofxcF07b9ad2xc1x12x07v8b8c8a2v82p9uae2vefhefub4v8d9a83xc2x00 v8fndf59x12x1t8bdc8z7v8d'ccdcx119x1b8ae8v8f8d8qcd8v1x13v8c8ve8b8e8d1 v8bbaa8x8d7jv8f8vec=8v8f8v8z8v89d88cf8e8v815v8-c83v8e8v81v8d1x1v8b8d8L'	00:50:56:c0:00:08	00:0c:29:41:4b:9d	192.168.79.1	192.168.79.130	31899	22	6	1
3	b'x1e7ech1cu8k:ve3yUQx19'v8c:8e8e8v8x2x14v82v85-v8b8v883v8a0v8d8v89 v8fndf1-v8d8v8b8c8d8f8d8v88v8j2w7'8e8c8v81v8j8d8' v8db8d8a8z8e15 v8z8*v8a8x17h8cd8t8j8v8a828.18a85v78e88d8v813E=f8d8v'3j888j7'cc8v8d v8ag8Wv86v87v8d8v8a8Bv8dcv87b85e8v8f88c'x13v8x5v816v8ed'	00:50:56:c0:00:08	00:0c:29:41:4b:9d	192.168.79.1	192.168.79.130	31899	22	6	2
5	D'8vef8f8148v1b'v87'ecv8f8e8w8M8A8b8f8a818v100F'D8v8j'v8755v8f8b8d8vef8v80 v8ae8v8b8v803v8ab'v8d8v88v8ae: v8b8c: v8b8c: v8d8v88v88v88v88v8e1x8v819v86'v8a7 v848v19v8f8c7'v8e4v8f8v8a8j8v8m14v8d8L'c83v8e858M8v8a8e2v8b8v88c8v8b8v16v8f8f8117 v8aa8f18v8ecv8e37v8ada8ae'815Rv8e8v8ee'v8d4v8d8'	00:50:56:c0:00:08	00:0c:29:41:4b:9d	192.168.79.1	192.168.79.130	31899	22	6	8
7	b7'v8ed8e0O8a8f8c8v86v88v8e8f816'v8b8v8f8e8a-8v8aP8e8v8d8T8f1cc8v84v8e8f8d5 v8c3.2v8e812x8v8a8p8cc8v8c8v86M8v8f1Y8c8b888c8f8Q8a8f88v86v16Gv87v8cc8v86 v8x8.v81f8b3v8e8v8a8v8b8v8d8+v8d2x12x15v8d29v8a84v88j7Y'v8a2v8f8f8e8e885p8c8f v88v8f8v8d5Q8v86v82B8v86v803Dv8x18v8b8v8v8e8v8b8v83C8v8c8v81aP8e8v899'	00:50:56:c0:00:08	00:0c:29:41:4b:9d	192.168.79.1	192.168.79.130	31899	22	6	10
8	b'x8c8v8f8c3'8v83v8a8v83v8b8a8v8e8b8d8'8q8v8ee8v88v8d1P8v8a8v8f8v88v8a1v808 v8b8v8c8a8f81x17v8a8f8c8v8ca85v8ef8x13E8v8x1a7v82v12-c864@8j1x8d8v8d8v88 v8ba8v16v8d8v8e8YnD'v85'v82v8b8v8a8f8a8t8v85v88'v8e8v8d7v8d8v8e8v891vd1v8b8v81 v8e8f88v8e89'8v83v84v8f8P8x17v8acc8v8b8v8ba'v8d5v818v8b8c8v8d8v818v89@x15M8v8a8v8v8b7'	00:50:56:c0:00:08	00:0c:29:41:4b:9d	192.168.79.1	192.168.79.130	31899	22	6	12
9	b'v8e8a8v8v8b8b8v810v8a8q8v82v8a8v8e8v8d7v8c82v81b8v8e8v8d8c8e28f8x82v8dc v8d4v8e8y8d88v8e8v8c8v82f'8v8e8d8c8e-v89v8d8j8x1e8v88v89j8v8d1 b'8v8d3'v817v8b8L v8d3v8d3x1357v8e8v88x13v8v83v8e8v85-v803v8L'x1c8v8d8v8b8v8d8v83v887m8Rv8e8v8b7 v8d8v8:58v8a8'v8v8b8v8c8v811'cc8v8a8v8c8v8d1v81a8a1v8c8v8d8v8f8v8f8j8=-8v88v8d4.p8d8'	00:50:56:c0:00:08	00:0c:29:41:4b:9d	192.168.79.1	192.168.79.130	31899	22	6	13
10	b'v8d8Cv8b83'v8f8v8a2v89v8e8f8v88A8x1c8a8v8f8b8v88v88v8e4v8z8v82v8e8a8j'v8ae v8d8v1a8a8v8a8v8a8v8f819v8f8v8d8v8f8v8a8c8v8a3v8e8v8e8v816.v87v88c8v88v8a85-v808e82v87v8e8v8d3M8f8e8c8v8b8e8v8b8v89x16v8e8v8p8+v87v8c8v8d8v8d8v8d1v8c1 v898L4v802v8c8'v8c8j8v81av805b8v8a8v87v8e82v8d4v8d5v805v8a'v8e8-v85v8a82v8a8'	00:50:56:c0:00:08	00:0c:29:41:4b:9d	192.168.79.1	192.168.79.130	31899	22	6	14

## Scan en .CSV

Permet le téléchargement au format .CSV de la table SCAN.



```
cur = db.cursor()
cur.execute("SELECT * FROM SCAN")
data = cur.fetchall()

file=open("statics/scanscsv.csv", "wb")
f = csv.writer(file)

for row in data:
    f.writerow([str(row)])
cur.close()
db.close()
file.close()

Ce code est disponible, en commentaire, dans le fichier route.py route '/scanscv'
```

## Dernier trafic en .pcap

Ceci vous permettra de télécharger le fichier des derniers trafic au format .pcap.

