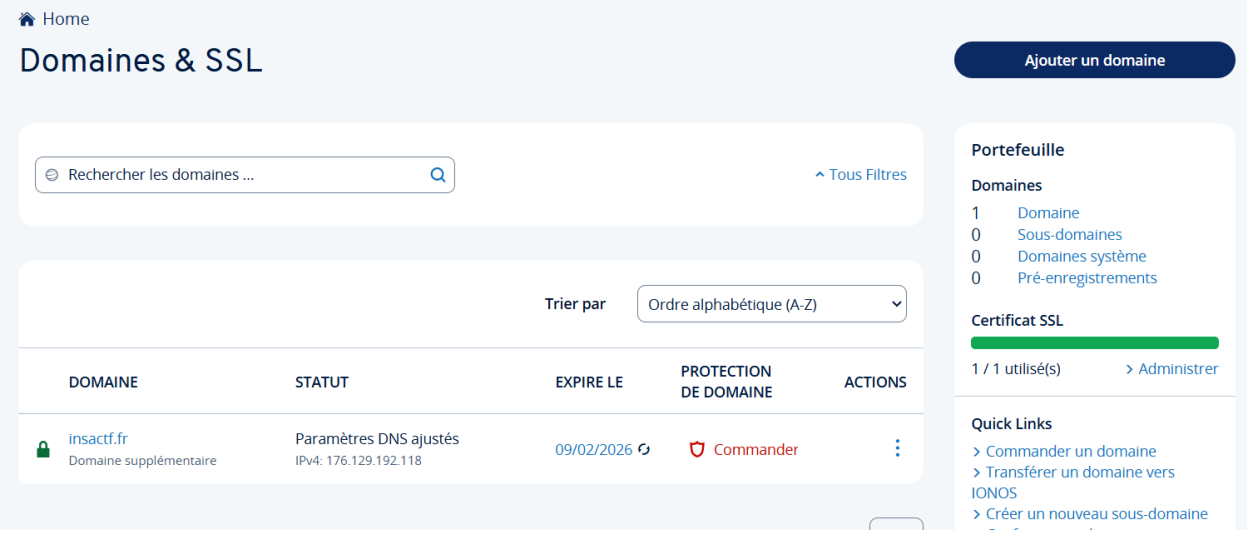
RAPPORT DU PROJET INSACTF

Préambule

Ce projet est conçu pour refléter un environnement réel, plutôt qu'un simple défi CTF. Les outils utilisés sont largement répandus dans le monde professionnel et ont une grande valeur applicative. L'objectif principal est de maîtriser l'utilisation d'outils essentiels tout en développant des compétences en observation, en analyse des situations, en réflexion logique et en exploitation des vulnérabilités de manière efficace.

1. Acheter un nom de domaine

Acheter un domaine auprès de n'importe quel fournisseur de domaines, et j'ai choisi IONOS.



Configurer l'enregistrement

2. Configurer SSL/TLS

Téléchargez le fichier de clé (private key), le certificat et l'intermédiaire sur IONOS.

et les ajouter au serveur Web

```
root@huy:~#  cat /home/huy/intermediate1.cer /home/huy/intermediate2.cer > /etc/ssl/certs/chain.pem
root@huy:~# ls -l /etc/ssl/certs/chain.pem
-rw-r--r-- 1 root root 4135 Feb 20 00:34 /etc/ssl/certs/chain.pem
root@huy:~# ls -l /etc/ssl/certs/insactf.fr_ssl_certificate.cer
-rw-r--r-- 1 root root 2208 Feb 15 00:50 /etc/ssl/certs/insactf.fr_ssl_certificate.cer
root@huy:~# ls -l /etc/ssl/private/_.insactf.fr_private_key.key
-rw------- 1 root root 1678 Feb 15 00:49 /etc/ssl/private/_.insactf.fr_private_key.key
root@huy:~#
```

3. Déployer le Web

Configurer le fichier **/etc/apache2/sites-available/default-ssl.conf**

```
 GNU nano 7.2                  /etc/apache2/sites-available/default-ssl.conf *
<VirtualHost *:443>
        ServerAdmin webmaster@localhost

        ServerName insactf.fr
        ServerAlias www.insactf.fr
        DocumentRoot /var/www/insa

        ErrorLog ${APACHE_LOG_DIR}/insa_error.log
        CustomLog ${APACHE_LOG_DIR}/insa_access.log combined

        SSLEngine on

        SSLCertificateFile      /etc/ssl/certs/insactf.fr_ssl_certificate.cer
        SSLCertificateKeyFile   /etc/ssl/private/_.insactf.fr_private_key.key
        SSLCertificateChainFile /etc/ssl/certs/chain.pem

        <FilesMatch "\.(?:cgi|shtml|phtml|php)$">
                SSLOptions +StdEnvVars
        </FilesMatch>
        <Directory /usr/lib/cgi-bin>
                SSLOptions +StdEnvVars
        </Directory>
</VirtualHost>
```

Activez le module SSL dans Apache pour prendre en charge HTTPS et activez l'hôte virtuel pour SSL (default-ssl.conf), ce qui oblige Apache à utiliser le certificat SSL pour servir HTTPS.

- **a2enmod ssl**
- **a2ensite default-ssl.conf**

```
root@huy:/etc/apache2/sites-available# a2enmod ssl
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Module socache_shmcb already enabled
Module ssl already enabled
root@huy:/etc/apache2/sites-available# a2ensite default-ssl.conf
Site default-ssl already enabled
root@huy:/etc/apache2/sites-available#
```

Créer le repertoire **/var/www/insa** et ajoutez le code source Web ici.

- **mkdir /var/www/insa**
- **chown -R www-data:www-data /var/www/insa**

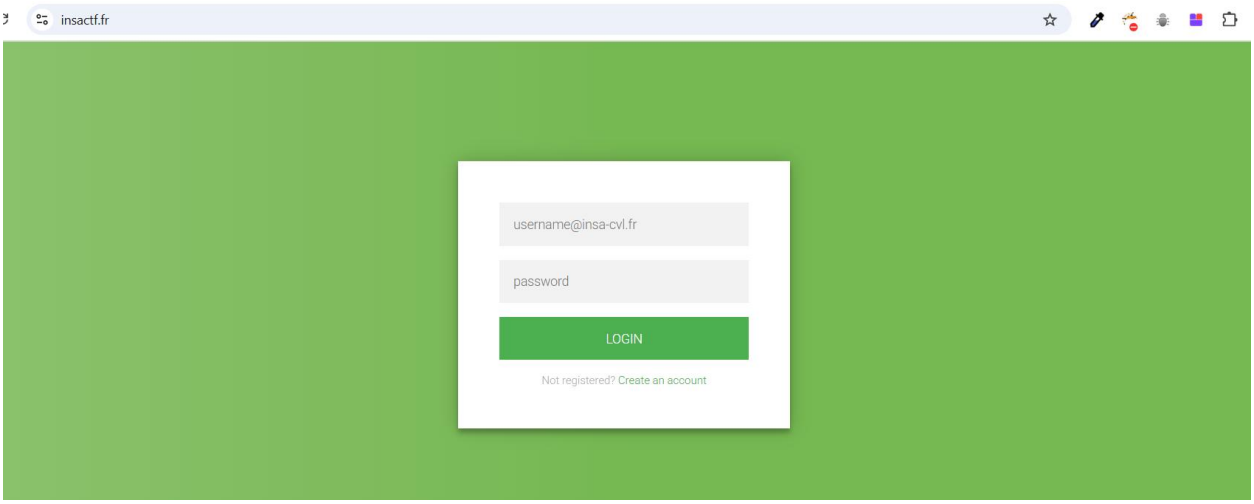
```
root@huy:/var/www/insa# ls -l
total 40
drwxrwxr-x 3 www-data www-data 4096 Feb 16 03:37 archive123
-rw-rw-r-- 1 www-data www-data  168 Feb 19 17:53 configdb.php
-rw-rw-r-- 1 www-data www-data 3744 Feb 16 03:37 dashboard.php
-rw-rw-r-- 1 www-data www-data  595 Feb 16 03:37 decode.php
-rw-rw-r-- 1 www-data www-data  638 Feb 16 03:37 encode.php
-rw-rw-r-- 1 www-data www-data 1499 Feb 16 03:37 getnumero.php
drwxrwxr-x 2 www-data www-data 4096 Feb 16 03:37 hiddenn
-rw-rw-r-- 1 www-data www-data 2868 Feb 16 03:37 login.php
-rw-rw-r-- 1 www-data www-data   54 Feb 16 03:37 robots.txt
-rw-rw-r-- 1 www-data www-data 2221 Feb 16 03:37 style.css
root@huy:/var/www/insa#
```

Redémarrer Apache2

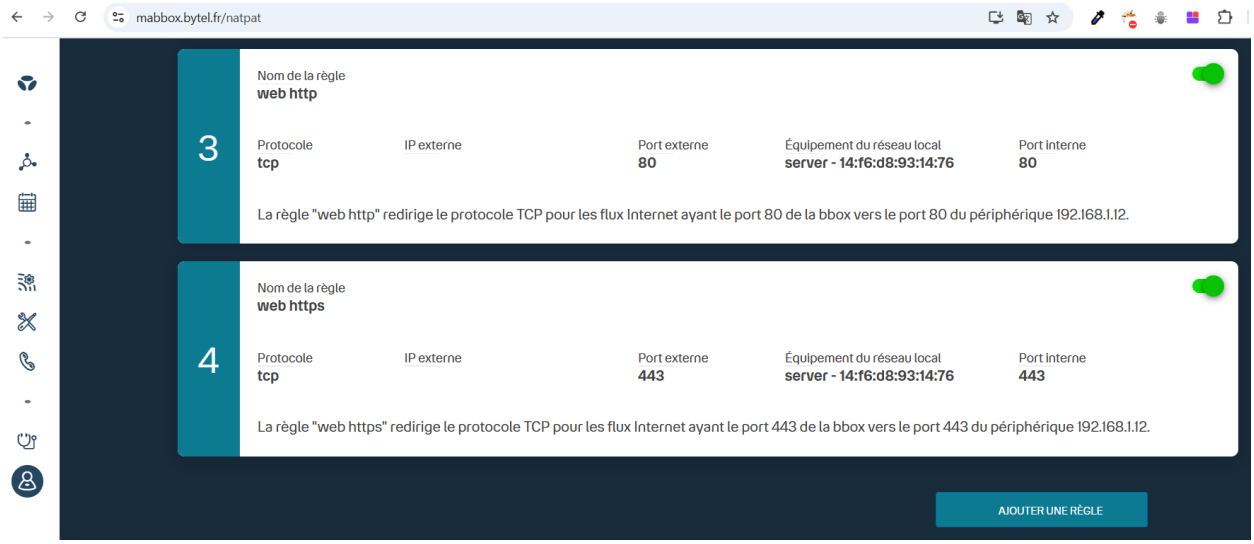
- **sudo systemctl restart apache2**

```
root@huy:/var/www/insa# sudo systemctl restart apache2
root@huy:/var/www/insa#
```

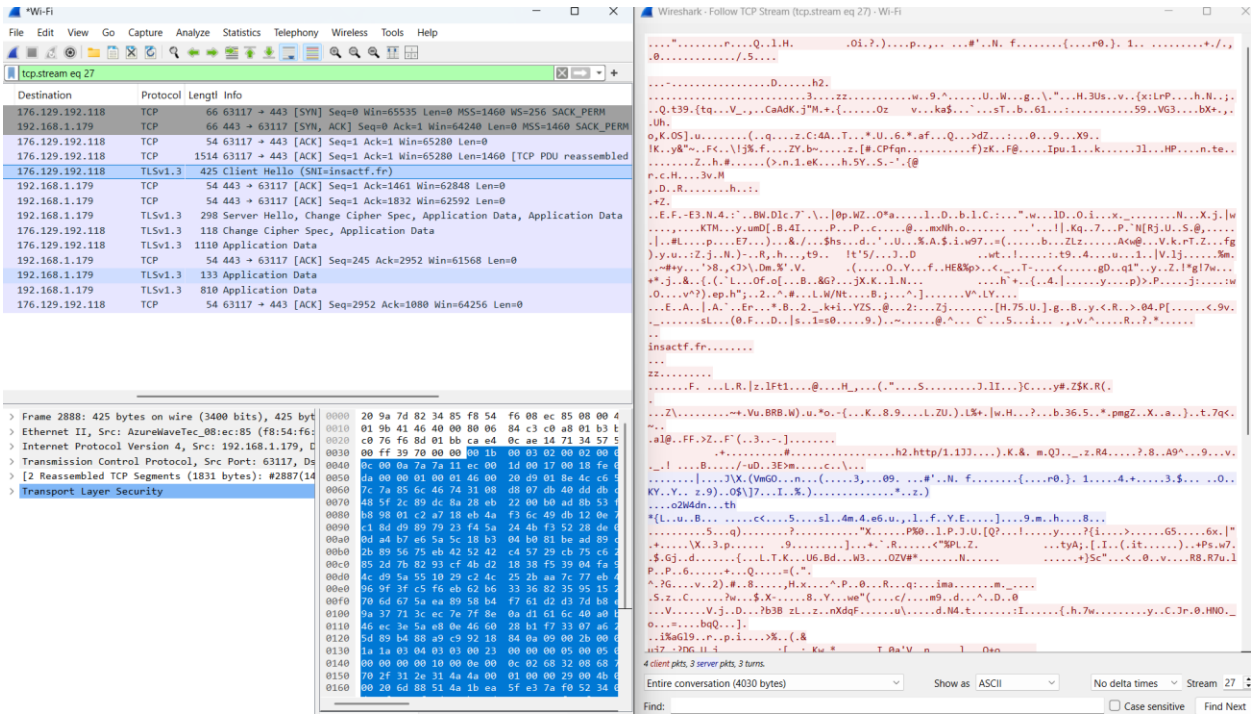
Tester le Web sur le navigateur



Pour que tout le monde dans le monde puisse accéder au site Web, nous devons accéder à la passerelle par défaut pour ouvrir le port (port forwarding) et le pointer vers le serveur Web.



Les données sont cryptées après l'utilisation de SSL/TLS



4. Installer IPS/IDS

Dans ce projet, j'utilise Suricata. Il s'agit de l'un des systèmes IDS/IPS (open source) les plus puissants et les plus populaires disponibles aujourd'hui. Il est largement utilisé dans les institutions financières, les gouvernements, les entreprises et la communauté de la cybersécurité. Je vais installer Suricata sur le serveur Web.

Configurer Suricata

Le fichier **/etc/suricata/suricata.yaml** est le fichier de configuration principal de Suricata. Il contient tous les paramètres importants pour que Suricata fonctionne correctement.

- **nano /etc/suricata/suricata.yaml**

```
  GNU nano 7.2                          /etc/suricata/suricata.yaml
%YAML 1.1
---

# Suricata configuration file. In addition to the comments describing all
# options in this file, full documentation can be found at:
# https://docs.suricata.io/en/latest/configuration/suricata-yaml.html

# This configuration file generated by Suricata 7.0.3.
suricata-version: "7.0"

##
## Step 1: Inform Suricata about your network
##

vars:
  # more specific is better for alert accuracy and performance
  address-groups:
    HOME_NET: "[192.168.1.0/24]"
    #HOME_NET: "[192.168.0.0/16]"
    #HOME_NET: "[10.0.0.0/8]"
    #HOME_NET: "[172.16.0.0/12]"
    #HOME_NET: "any"

    EXTERNAL_NET: "!$HOME_NET"
```

```
# Linux high speed capture support
af-packet:
  - interface: wlo1
    # Number of receive threads. "auto" uses the number of cores
    #threads: auto
    # Default clusterid. AF_PACKET will load balance packets based on flow.
    cluster-id: 99
    # Default AF_PACKET cluster type. AF_PACKET can load balance per flow or per hash.
    # This is only supported for Linux kernel > 3.1
    # possible value are:
    #  * cluster_flow: all packets of a given flow are sent to the same socket
    #  * cluster_cpu: all packets treated in kernel by a CPU are sent to the same socket
    #  * cluster_qm: all packets linked by network card to a RSS queue are sent to the s
    #  socket. Requires at least Linux 3.14.
    #  * cluster_ebpf: eBPF file load balancing. See doc/userguide/capture-hardware/ebpf
    #  more info.
    # Recommended modes are cluster_flow on most boxes and cluster_cpu or cluster_qm on
    # with capture card using RSS (requires cpu affinity tuning and system IRQ tuning)
    # cluster_rollover has been deprecated; if used, it'll be replaced with cluster_flow
    cluster-type: cluster_flow
    # In some fragmentation cases, the hash can not be computed. If "defrag" is set
    # to yes, the kernel will do the needed defragmentation before sending the packets.
    defrag: yes
    # To use the ring feature of AF_PACKET, set 'use-mmap' to yes
    #use-mmap: yes
    # Lock memory map to avoid it being swapped. Be careful that over
```

```
# Cross platform libpcap capture support
pcap:
  - interface: wlo1
    # On Linux, pcap will try to use mmap'ed capture and will use "buffer-size"
    # as total memory used by the ring. So set this to something bigger
    # than 1% of your bandwidth.
    #buffer-size: 16777216
    #bpf-filter: "tcp and port 25"
    # Choose checksum verification mode for the interface. At the moment
    # of the capture, some packets may have an invalid checksum due to
    # the checksum computation being offloaded to the network card.
    # Possible values are:
```

```
##
## Configure Suricata to load Suricata-Update managed rules.
##

default-rule-path: /var/lib/suricata/rules

rule-files:
  #- suricata.rules
  - /var/lib/suricata/rules/custom_suricata.rules

##
## Auxiliary configuration files.
##
```

```
#
# Takes a 'seed' that needs to be same across sensors and tools
# to make the id less predictable.

# enable/disable the community id feature.
community-id: true
# Seed value for the ID output. Valid values are 0-65535.
community-id-seed: 0

# HTTP X-Forwarded-For support by adding an extra field or overwriting
# the source or destination IP address (depending on flow direction)
# with the one reported in the X-Forwarded-For HTTP header. This is
```

Parce que le fichier de règles par défaut est très compliqué, pour la commodité du projet, j'écrirai un fichier de règles simple et adapté au projet. Il existe deux règles principales : la détection DDoS et la détection d'accès non autorisé au système via SSH.

- **nano /var/lib/suricata/rules/custom_suricata.rules**

```
  GNU nano 7.2                                    /var/lib/suricata/rules/custom_suricata.rules *
# DDoS Attack
alert ip any any -> $HOME_NET 80 (msg:"Detect DDoS Attack"; flow:to_server,established; threshold: type both, track by_src, count 100, seconds 10; sid:1000001;)
alert ip any any -> $HOME_NET 443 (msg:"Detect DDoS Attack"; flow:to_server,established; threshold: type both, track by_src, count 100, seconds 10; sid:1000002;)

# SSH brute-force
alert tcp any any -> $HOME_NET 22 (msg:"Detect SSH Brute Force"; flow:to_server,established; threshold: type both, track by_src, count 50, seconds 30; sid:1000003;)
```

Vérifier si la règle est mal écrite syntaxiquement.

- **sudo suricata -T -c /etc/suricata/suricata.yaml -v**

```
root@huy:~# sudo suricata -T -c /etc/suricata/suricata.yaml -v
Notice: suricata: This is Suricata version 7.0.3 RELEASE running in SYSTEM mode
Info: cpu: CPUs/cores online: 8
Info: suricata: Running suricata under test mode
Info: suricata: Setting engine mode to IDS mode by default
Info: exception-policy: master exception-policy set to: auto
Info: logopenfile: fast output device (regular) initialized: fast.log
Info: logopenfile: eve-log output device (regular) initialized: eve.json
Info: logopenfile: stats output device (regular) initialized: stats.log
Info: detect: 1 rule files processed. 3 rules successfully loaded, 0 rules failed, 0
Info: threshold-config: Threshold config parsed: 0 rule(s) found
Info: detect: 3 signatures processed. 0 are IP-only rules, 0 are inspecting packet payload, 0 inspe
Notice: suricata: Configuration provided was successfully loaded. Exiting.
root@huy:~#
```

Enregistrez et arrêtez Suricata pour l'exécuter en mode test (avant le déploiement réel).

- **sudo systemctl restart suricata**
- **sudo systemctl stop suricata**

```
root@huy:~# sudo systemctl restart suricata
root@huy:~# sudo systemctl stop suricata
root@huy:~#
```

Exécuter Suricata en mode test. (**wlo1** est le nom de la carte réseau)

- **sudo suricata -c /etc/suricata/suricata.yaml -i wlo1**

```
root@huy:~# sudo suricata -c /etc/suricata/suricata.yaml -i wlo1
i: suricata: This is Suricata version 7.0.3 RELEASE running in SYSTEM mode
i: threads: Threads created -> W: 8 FM: 1 FR: 1   Engine started.
```

Démarrer Kali et attaquer le serveur pour vérifier si les règles fonctionnent correctement.

- **tail -f /var/log/suricata/fast.log**

```
┌──(kali㉿kali)-[~]
└─$ hydra -l admin -P /usr/share/wordlists/rockyou.txt ssh://192.168.1.12
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or sec
ret service organizations, or for illegal purposes (this is non-binding, these *** ignore law
s and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-02-19 09:41:18
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to re
duce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from
a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~8
96525 tries per task
[DATA] attacking ssh://192.168.1.12:22/
[STATUS] 301.00 tries/min, 301 tries in 00:01h, 14344099 to do in 794:15h, 15 active
[STATUS] 227.00 tries/min, 681 tries in 00:03h, 14343724 to do in 1053:09h, 10 active
[STATUS] 195.57 tries/min, 1369 tries in 00:07h, 14343036 to do in 1222:20h, 10 active
```

```
root@huy:~# tail -f /var/log/suricata/fast.log
02/19/2025-15:44:07.737053  [**] [1:1000003:0] Detect SSH Brute Force [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.179:49191 -> 192.168.1.12:22
02/19/2025-15:44:39.008236  [**] [1:1000003:0] Detect SSH Brute Force [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.179:49201 -> 192.168.1.12:22
02/19/2025-15:45:10.284394  [**] [1:1000003:0] Detect SSH Brute Force [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.179:49264 -> 192.168.1.12:22
02/19/2025-15:45:46.849038  [**] [1:1000003:0] Detect SSH Brute Force [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.179:49294 -> 192.168.1.12:22
02/19/2025-15:46:05.947513  [**] [1:1000003:0] Detect SSH Brute Force [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.179:49329 -> 192.168.1.12:22
02/19/2025-15:46:41.753898  [**] [1:1000003:0] Detect SSH Brute Force [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.179:49349 -> 192.168.1.12:22
02/19/2025-15:47:16.545124  [**] [1:1000003:0] Detect SSH Brute Force [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.179:49384 -> 192.168.1.12:22
02/19/2025-15:47:51.156206  [**] [1:1000003:0] Detect SSH Brute Force [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.179:49395 -> 192.168.1.12:22
02/19/2025-15:48:12.020817  [**] [1:1000003:0] Detect SSH Brute Force [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.179:49693 -> 192.168.1.12:22
02/19/2025-15:48:42.456146  [**] [1:1000003:0] Detect SSH Brute Force [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.179:49737 -> 192.168.1.12:22
```

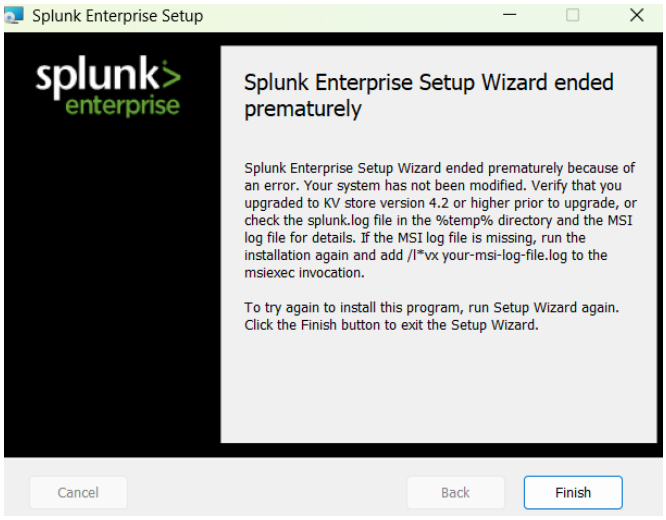
```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 -S -p 443 --flood 192.168.1.12

[sudo] password for kali:
HPING 192.168.1.12 (eth0 192.168.1.12): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

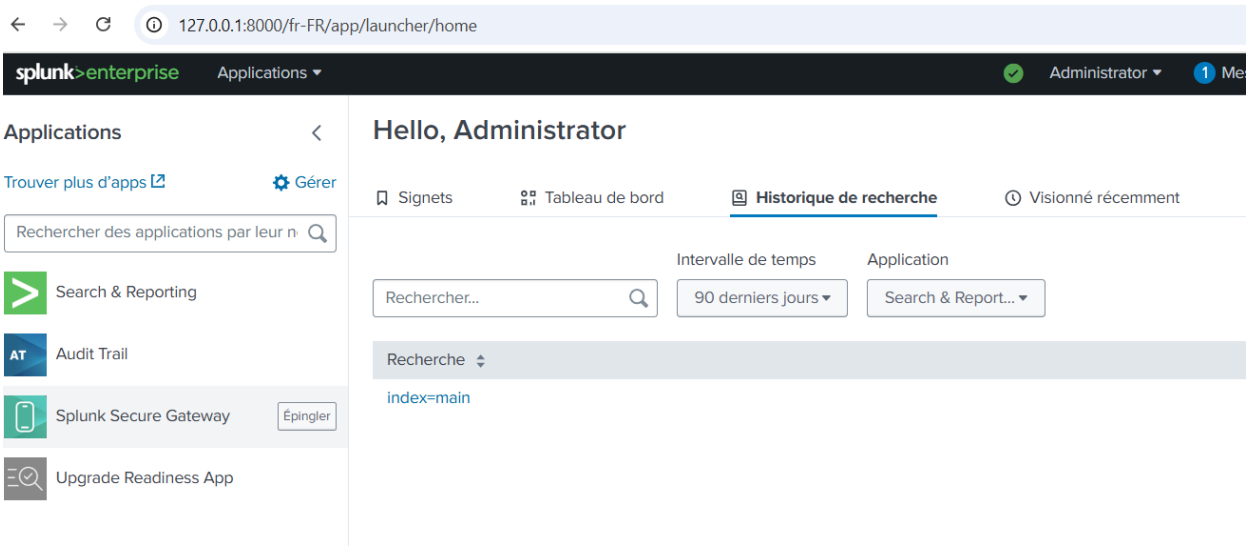
```
02/19/2025-15:55:41.068708  [**] [1:1000002:0] Detect DDoS Attack [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.179:929 -> 192.168.1.12:443
02/19/2025-15:55:53.808382  [**] [1:1000002:0] Detect DDoS Attack [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.179:57087 -> 192.168.1.12:443
02/19/2025-15:56:03.423403  [**] [1:1000002:0] Detect DDoS Attack [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.179:57080 -> 192.168.1.12:443
02/19/2025-15:56:15.609358  [**] [1:1000002:0] Detect DDoS Attack [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.179:55794 -> 192.168.1.12:443
02/19/2025-15:56:49.771100  [**] [1:1000002:0] Detect DDoS Attack [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.179:54771 -> 192.168.1.12:443
```

5. Installer Splunk Enterprise (SE) et Splunk Universal Forwarder (SUF)

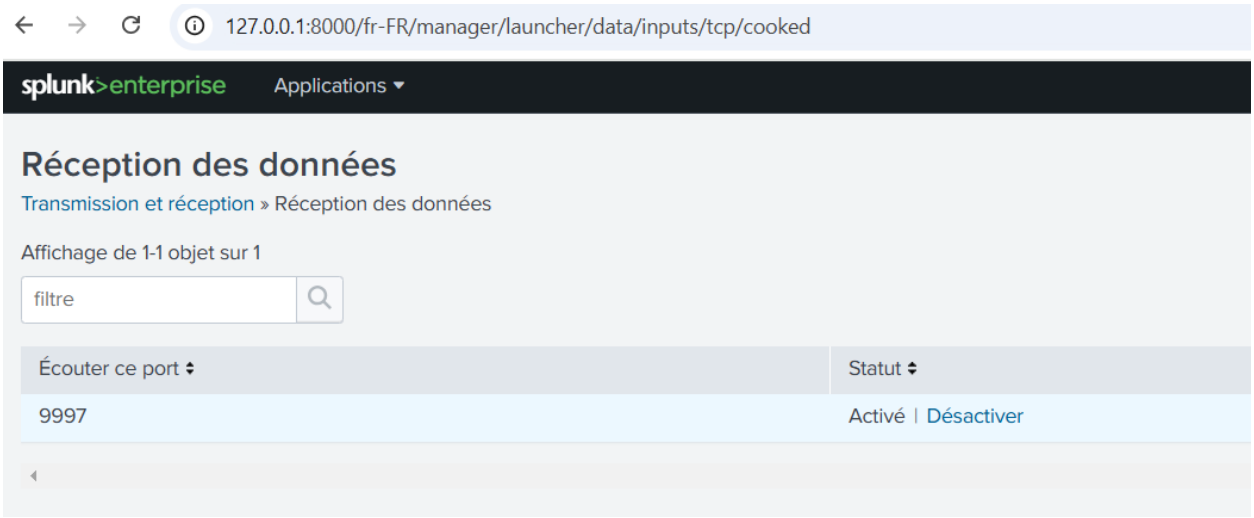
SE est une puissante plate-forme de surveillance et d'analyse de journaux utilisée pour collecter, stocker, rechercher, analyser et visualiser des données provenant de diverses sources. SE est très populaire dans la pratique, notamment dans les domaines de la sécurité, de la surveillance des systèmes et du traitement des journaux à grande échelle (SIEM). Dans ce projet, SE reçoit des données de SUF.

Installer SE sur la machine Windows





Ouvrir le port de réception des données, port 9997 (port par défaut)



SUF est un composant de Splunk utilisé pour collecter et envoyer des données (logs) provenant de différentes sources à SE pour analyse. SUF permet d'optimiser la collecte et la transmission des données sans installer ni configurer SF sur tous les serveurs.

Installer SF sur le serveur Web

```
root@huy:~#  sudo /opt/splunkforwarder/bin/splunk status
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
splunkd is running (PID: 3159).
splunk helpers are running (PIDs: 3194).
root@huy:~#
```

Ajouter un serveur de transfert au SUF, lui permettant d'envoyer des données de journal à un SE

- **sudo /opt/splunkforwarder/bin/splunk add forward-server 192.168.1.179:9997**

```
root@huy:~#  /opt/splunkforwarder/bin/splunk add forward-server 192.168.1.179:9997
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Your session is invalid.  Please login.
Splunk username: admin
Password:
192.168.1.179:9997 forwarded-server already present
root@huy:~#
```

Créez un fichier **inputs.conf** pour configurer les sources de données que SUF enverra à SE

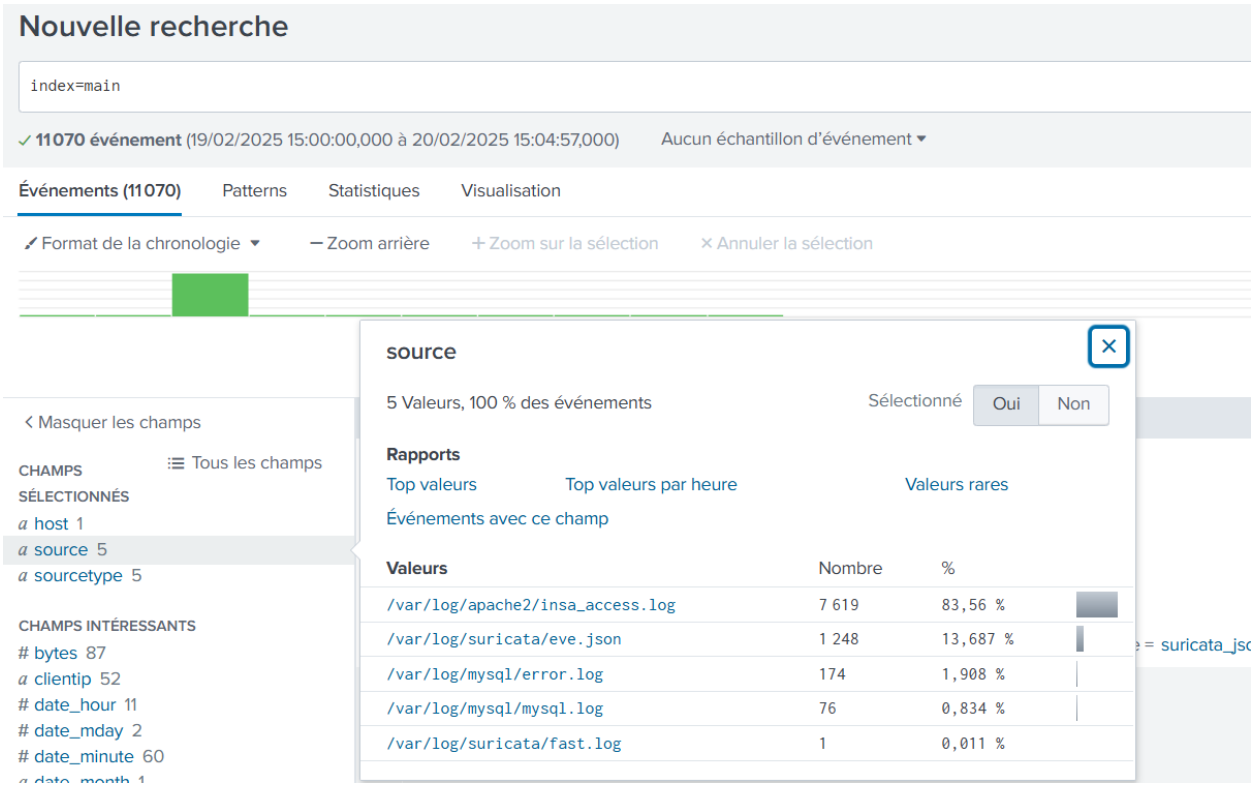
```
  GNU nano 7.2                 /opt/splunkforwarder/etc/system/local/inputs.conf
[monitor:///var/log/apache2/insa_access.log]
index = main
host = ubuntu-server
sourcetype = access_combined
disabled = false

[monitor:///var/log/suricata/fast.log]
index = main
host = ubuntu-server
sourcetype = suricata_fast
disabled = false

[monitor:///var/log/suricata/eve.json]
index = main
host = ubuntu-server
sourcetype = suricata_json
disabled = false

[monitor:///var/log/mysql/mysql.log]
index = main
host = ubuntu-server
sourcetype = mysql_query
disabled = false

[monitor:///var/log/mysql/error.log]
index = main
host = ubuntu-server
sourcetype = mysql_error
disabled = false
```

Redémarrer SUF

- **sudo /opt/splunkforwarder/bin/splunk restart**

```
root@huy:~# sudo /opt/splunkforwarder/bin/splunk restart
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Stopping splunkd...
Shutting down.  Please wait, as this may take a few minutes.

Stopping splunk helpers...

Done.
splunkd.pid doesn't exist...

Splunk> Be an IT superhero. Go home early.

Checking prerequisites...
        Checking mgmt port [8089]: open
        Checking conf files for problems...
                Invalid key in stanza [monitor:///var/log/mysql/mysql.log] in /opt/splunkforwarder/etc/
system/local/inputs.conf, line 23: disables (value: false).
                Your indexes and inputs configurations are not internally consistent. For more informat
ion, run 'splunk btool check --debug'
        Done
        Checking default conf files for edits...
        Validating installed files against hashes from '/opt/splunkforwarder/splunkforwarder-9.4.0-6b4e
be426ca6-linux-amd64-manifest'
        All installed files intact.
        Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Done

root@huy:~#
```

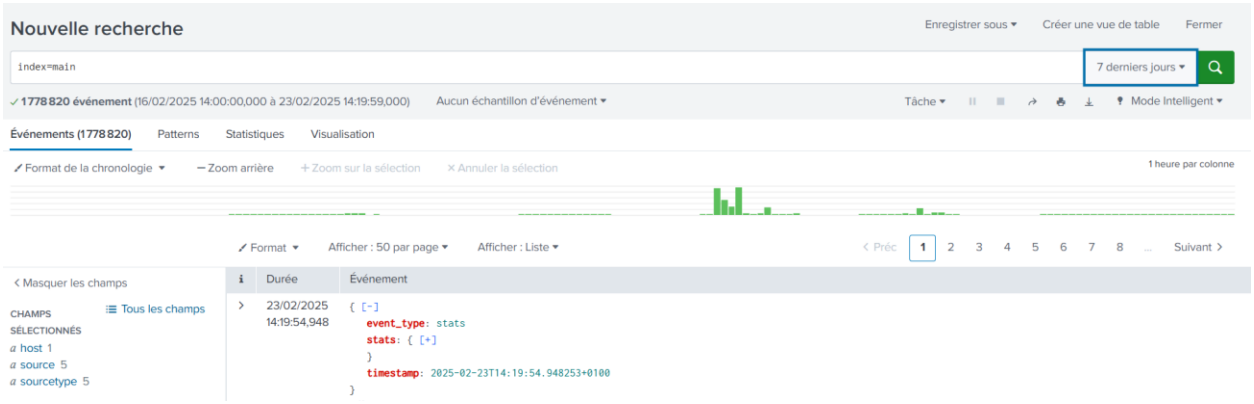
Vérifier si SE a bien reçu tous les journaux



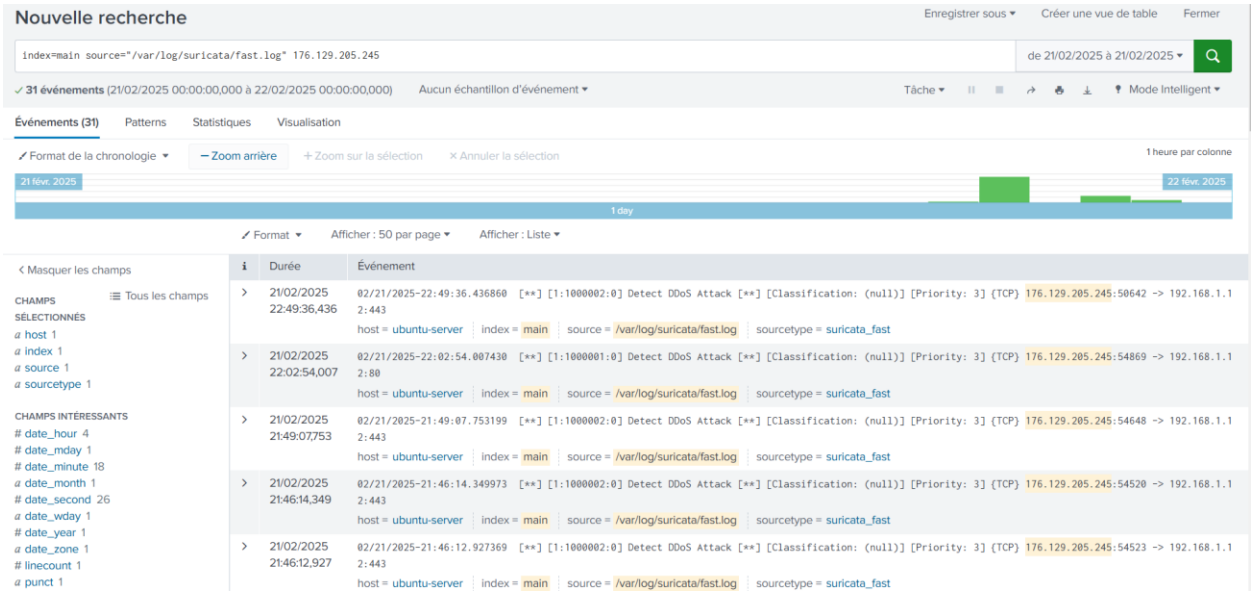
6. Organiser l'attaque (redteam) et la défense (blueteam)

Après avoir présenté le site web à toute l'école, les jeunes passionnés de cybersécurité en général et de CTF en particulier ont commencé à l'exploiter. Je peux le voir à travers le SE.

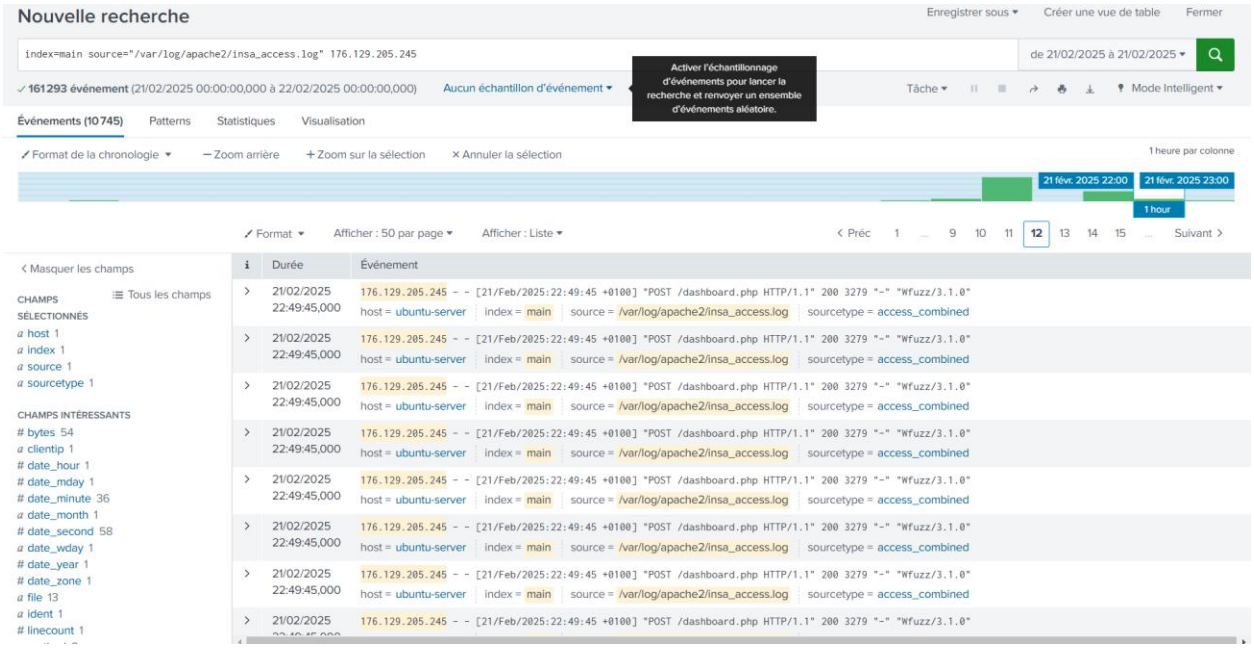
Beaucoup d'événements ont eu lieu au cours des 7 derniers jours.



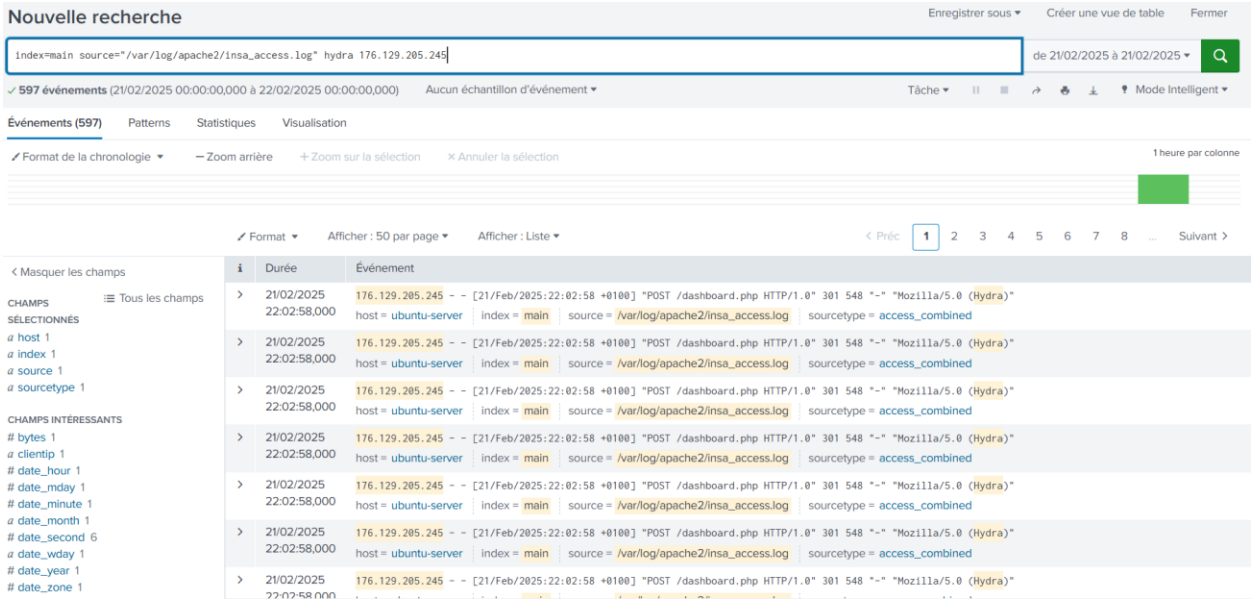
SE a reçu de nombreuses alertes "**Detect DDoS Attack**" en provenance de l'adresse IP **176.129.205.245**



Il est possible que l'attaquant ait effectué un brute-force avec Wfuzz et Hydra, ce qui a entraîné l'affichage du message "**Detect DDoS Attack**".




```
195659 Connect  root@localhost on challdifficile using Socket
195659 Quit
195660 Connect  root@localhost on challdifficile using Socket
195660 Query    SELECT * FROM users WHERE username = 'briffaut@insa-cvl.fr' AND password = 'chloe'
195660 Quit
195662 Connect  root@localhost on challdifficile using Socket
195661 Connect  root@localhost on challdifficile using Socket
195662 Query    SELECT * FROM users WHERE username = 'briffaut@insa-cvl.fr' AND password = 'lawrence'
195661 Quit
195662 Quit
195663 Connect  root@localhost on challdifficile using Socket
195663 Query    SELECT * FROM users WHERE username = 'briffaut@insa-cvl.fr' AND password = 'xbox360'
195663 Quit
195664 Connect  root@localhost on challdifficile using Socket
195664 Query    SELECT * FROM users WHERE username = 'briffaut@insa-cvl.fr' AND password = 'sheena'
195664 Quit
195665 Connect  root@localhost on challdifficile using Socket
195665 Quit
195666 Connect  root@localhost on challdifficile using Socket
195667 Connect  root@localhost on challdifficile using Socket
195666 Query    SELECT * FROM users WHERE username = 'briffaut@insa-cvl.fr' AND password = 'murphy'
195667 Quit
195666 Quit
195668 Connect  root@localhost on challdifficile using Socket
195668 Query    SELECT * FROM users WHERE username = 'briffaut@insa-cvl.fr' AND password = 'anamaria'
195668 Quit
195669 Connect  root@localhost on challdifficile using Socket
195670 Connect  root@localhost on challdifficile using Socket
195669 Query    SELECT * FROM users WHERE username = 'briffaut@insa-cvl.fr' AND password = 'gateway'
195670 Query    SELECT * FROM users WHERE username = 'briffaut@insa-cvl.fr' AND password = 'madalina'
195670 Quit
```


Nouvelle recherche
Enregistrer sous
Créer une vue de table
Fermer
index=main source="/var/log/apache2/insa_access.log" hydra 176.129.205.245
de 21/02/2025 à 21/02/2025
597 événements (21/02/2025 00:00:00,000 à 22/02/2025 00:00:00,000)
Aucun échantillon d'événement
Tâche
Mode Intelligent
Événements (597)
Patterns
Statistiques
Visualisation
Format de la chronologie
Zoom arrière
Zoom sur la sélection
Annuler la sélection
1 heure par colonne
Format
Afficher : 50 par page
Afficher : Liste
Préc
1
2
3
4
5
6
7
8
Suivant
Masquer les champs
Tous les champs
CHAMPS SÉLECTIONNÉS
a host 1
a index 1
a source 1
a sourcetype 1
CHAMPS INTÉRESSANTS
bytes 1
a clientip 1
date_hour 1
date_mday 1
date_minute 1
a date_month 1
date_second 6
a date_wday 1
date_year 1
date_zone 1
Durée
Événement
21/02/2025 22:02:58,000
176.129.205.245 - - [21/Feb/2025:22:02:58 +0100] "POST /dashboard.php HTTP/1.0" 301 548 "-" "Mozilla/5.0 (Hydra)"
host = ubuntu-server
index = main
source = /var/log/apache2/insa_access.log
sourcetype = access_combined