université de TOURS

Réagir face à une cyber-attaque

Lukas Théotime - Max Doualan - Nathan Martel

SAÉ6Cyber01

pfsense

Sommaire

université de TOURS

01

Introduction

Introduction du projet, objectifs réalisés et outils utilisés

Que fallait-il faire ?

Objectifs :

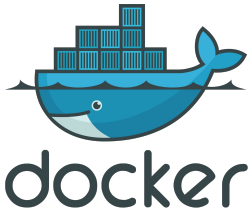
- ➔ Collecte et traitement des événements de sécurité ;
- ➔ Blocage des acteurs de menaces ;
- ➔ Génération d'alertes sur le SIEM et notifications.

Outils principaux utilisés :

- ➔ Firewalling Pfsense ;
- ➔ Stack ELK (Elasticsearch, Logstash, Kibana) ;
- ➔ Service docker (env conteneurisé).

Logo de la stack ELK

Logo de PFsense



Logo de Docker

université de TOURS

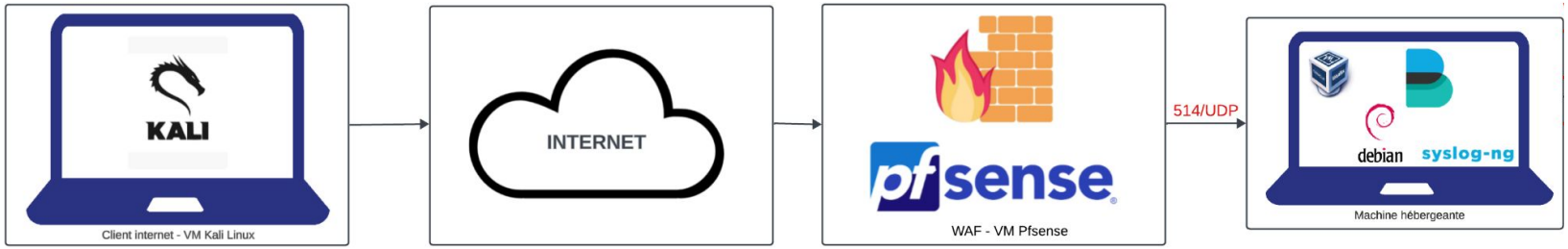
02

Architecture

Description de l'architecture, mise
en place d'un système de firewalling

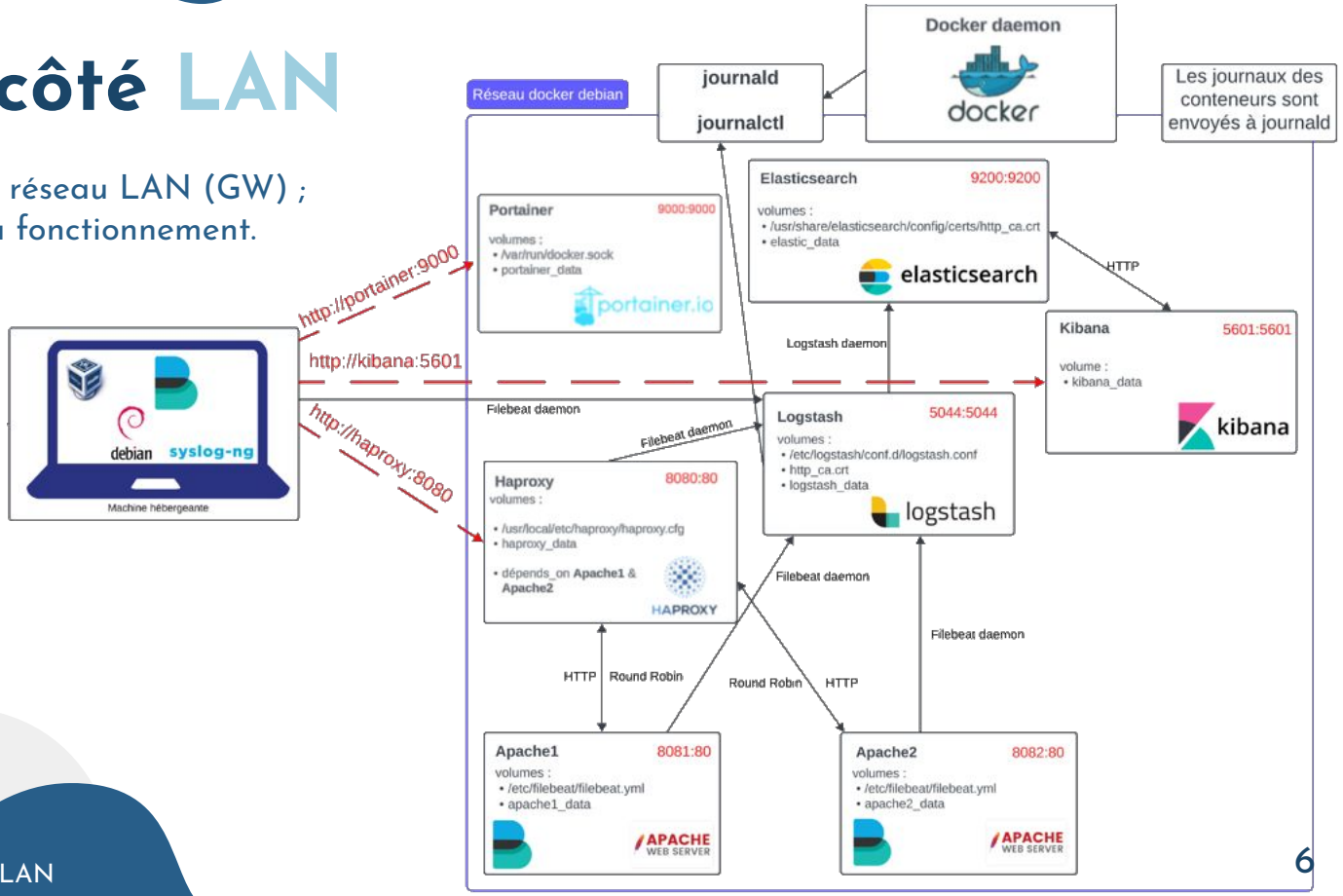
Architecture côté WAN

- ➔ VM Kali Linux simulant l'acteur de menace ;
- ➔ Firewall PFsense en amont du LAN ;
- ➔ VM Debian simulant le LAN

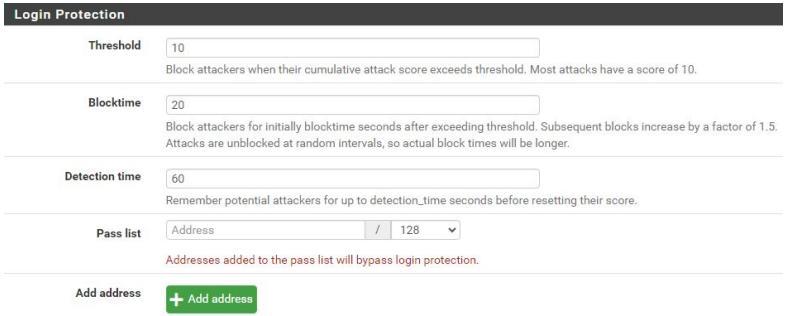


Architecture côté LAN

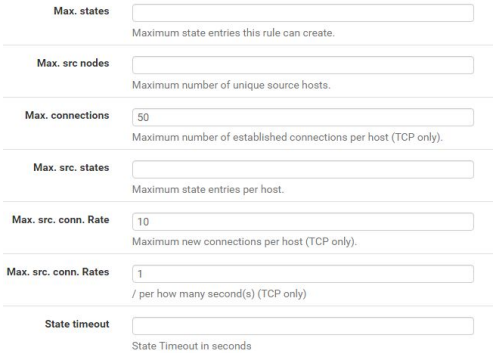
- ➔ VM Debian hébergeant le réseau LAN (GW) ;
- ➔ 7 conteneurs nécessaire au fonctionnement.



Configuration du pfSense



Configuration de la protection SSH du pfSense



Configuration de la protection TCP

- ➔ Bloquer en fonction d'un score
- ➔ Temps de blocage (x1.5)
- ➔ Temps en mémoire

- ➔ 7 paramètres dont 3 TCP
- ➔ Temps de blocage de pfSense
- ➔ Bloque toutes attaques rapides via TCP

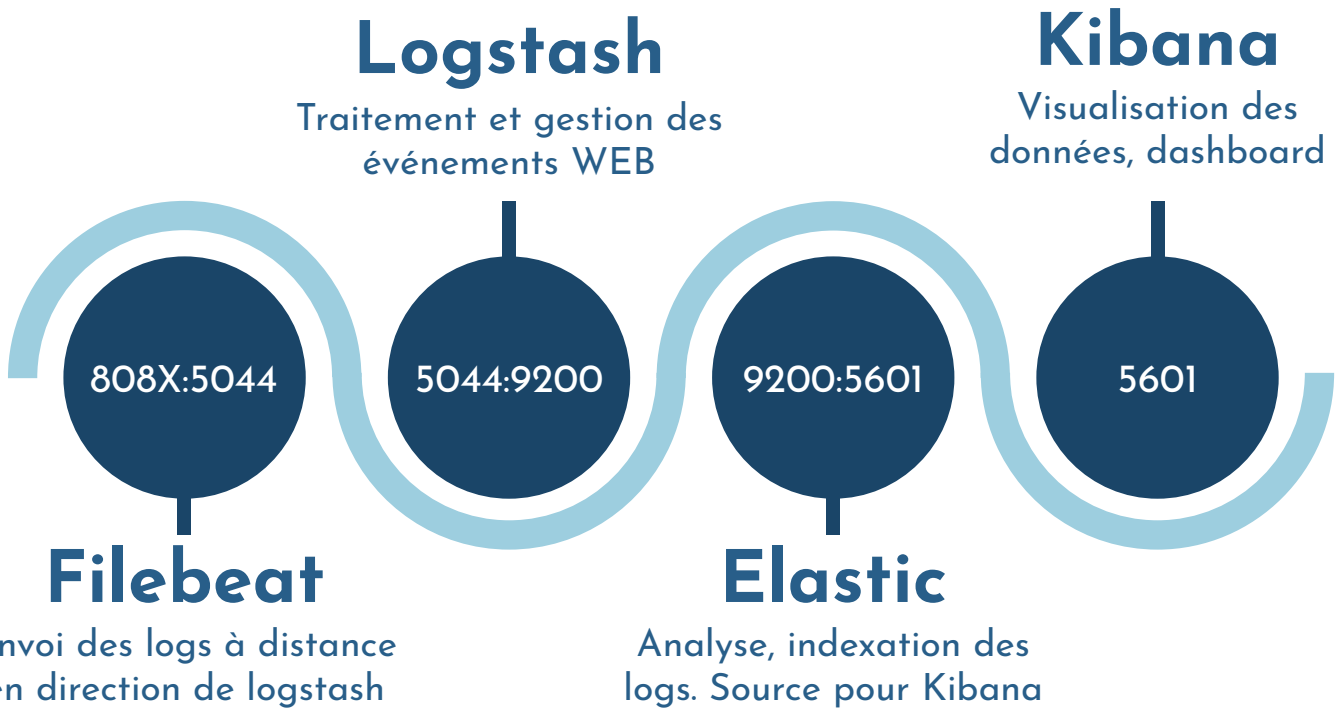
université de TOURS

03

Gestion des logs

Acheminement des événements de sécurité sur le réseau

Gestion des logs WEB



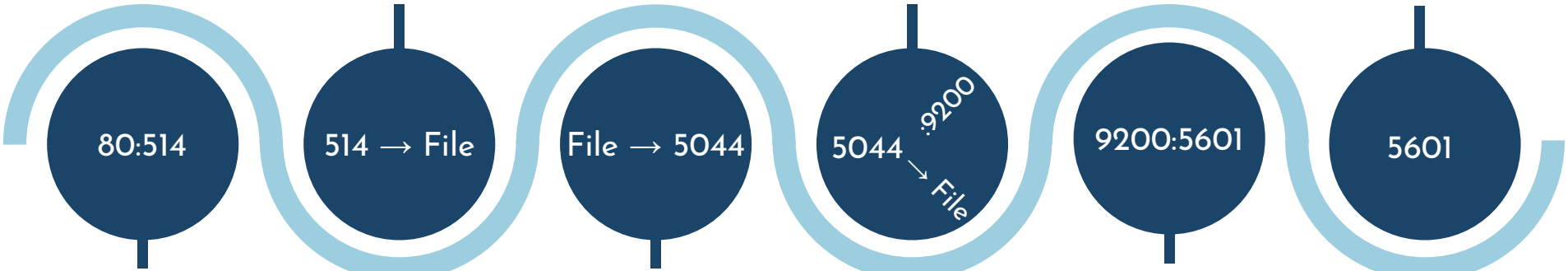
Gestion des logs de Pfsense

université de TOURS

Debian
Écoute, filtrage et stockage des logs avec syslog-ng

Logstash
Traitement et gestion des événements FW

Kibana
Visualisation des données, dashboard



Pfsense
Envoi des logs à distance dans le FW

Debian
Envoi des logs à distance en direction de logstash

Elastic
Analyse, indexation des logs. Source pour Kibana

université de TOURS

04

Attaques et notifications

Acheminement des événements de sécurité sur le réseau

Attaque sur compte SSH

- Tentative de brute force (Hydra THC)
- Perte d'accès au firewall
- Logs envoyés par SSHguard à la stack ELK

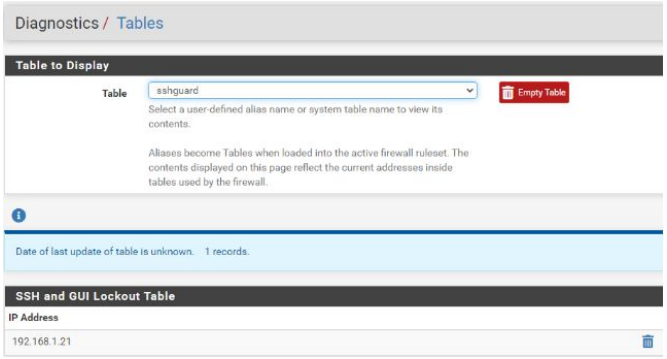
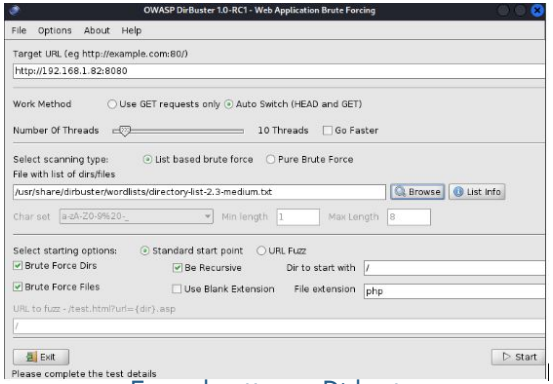


Table des IP bannies

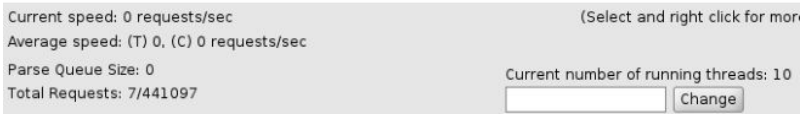
Logs dans pfSense

Logs reçus dans Kibana

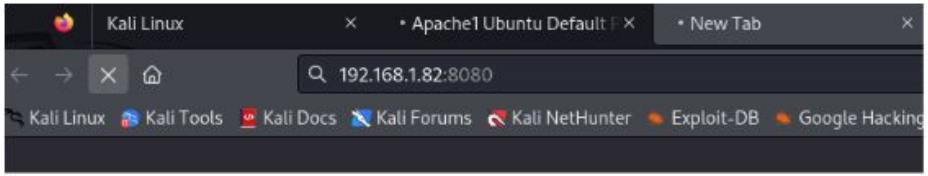
Attaque Dirbuster



Exemple attaque Dirbuster



Attaque arrêté



Plus d'accès au site

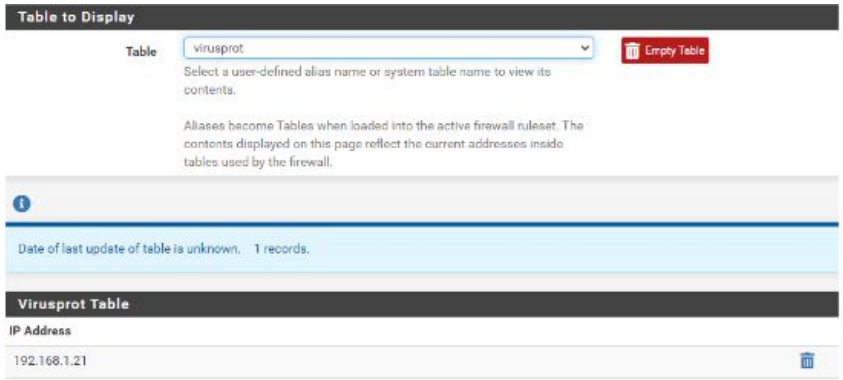


Table des IP bannies

- ➔ 7 requêtes avant bannissement
- ➔ Perte d'accès aux sites à cause de la règle

Notifications par e-mail

Essai n°1

Envoi de mail avec PFsense suite à une attaque.

Essai n°2

Module Watchers sur l'interface Kibana

Essai n°3

Module ommail avec rsyslog avec relais postfix

Essai n°4

Script bash personnel couplé à un cron et postfix

Fonctionnement de l'alerte

```
root@4ea7ba528ead: /usr/share/elasticsear...   debian@debian12: ~
#!/bin/bash

LOG_FILE="/var/log/pfsense/pfsense.log"

if grep -q "Blocking" "$LOG_FILE"; then
   ligne=$(grep "Blocking" "$LOG_FILE")

   echo "$ligne" | mail -s "Alerte : Attaque brute force bloqu" ayressios@gmail.com

   echo "" > /var/log/pfsense/pfsense.log

fi
```

Script bash

Test l'occurrence du mot Blocking

```
# m h  dom mon dow   command
* * * * * bash /home/blocking.sh
```

Crontab

Exécution toutes les minutes du script

Finalité de l'alerte

Alerte : Attaque brute force bloquÃe' Boîte de réception ×

root <ayressios@gmail.com> mer. 20 mars 18:57 (il y a 20 heures)
À moi

{"host":{"name":"debian12"},"tags":["pfsense_logs","beats_input_codec_plain_applied"],"message":"Mar 20 18:56:14 _gateway 1 2024-03-25T23:39:53.832168+01:00 NLM.home.arpa sshguard 79291 - - Blocking \"192.168.1.21/32\" for 20 secs (1 attacks in 0 secs, after 1 abuses over 0 secs.)","agent":{"type":"filebeat","version":"7.17.18","name":"debian12","hostname":"debian12","id":"c0749d68-db29-4158-8f0d-88afcfd8ce56","ephemeral_id":"435a8d37-a157-4f43-bf73-d554329039c4"},"ecs":{"version":"1.12.0"},"log":{"offset":182026,"file":{"path":"/var/log/pfsense/pfsense.log"}},"@timestamp":"2024-03-20T17:56:14.530Z","event":{"original":"Mar 20 18:56:14 _gateway 1 2024-03-25T23:39:53.832168+01:00 NLM.home.arpa sshguard 79291 - - Blocking \"192.168.1.21/32\" for 20 secs (1 attacks in 0 secs, after 1 abuses over 0 secs.)"},"@version":"1","input":{"type":"log"}}
{"host":{"name":"debian12"},"tags":["pfsense_logs","beats_input_codec_plain_applied"],"message":"Mar 20 18:56:14 _gateway 1 2024-03-25T23:40:45.769154+01:00 NLM.home.arpa sshguard 79291 - - Blocking \"192.168.1.21/32\" for 40 secs (1 attacks in 0 secs, after 2 abuses over 52 secs.)","ecs":{"version":"1.12.0"},"agent":{"version":"7.17.18","type":"filebeat","name":"debian12","hostname":"debian12","id":"c0749d68-db29-4158-8f0d-88afcfd8ce56","ephemeral_id":"435a8d37-a157-4f43-bf73-d554329039c4"},"log":{"offset":182904,"file":{"path":"/var/log/pfsense/pfsense.log"}},"@timestamp":"2024-03-20T17:56:14.530Z","event":{"original":"Mar 20 18:56:14 _gateway 1 2024-03-25T23:40:45.769154+01:00 NLM.home.arpa sshguard 79291 - - Blocking \"192.168.1.21/32\" for 40 secs (1 attacks in 0 secs, after 2 abuses over 52 secs.)"},"@version":"1","input":{"type":"log"}}
{"host":{"name":"debian12"},"tags":["pfsense_logs","beats_input_codec_plain_applied"],"message":"Mar 20 18:56:42 _gateway 1 2024-03-25T23:54:45.321441+01:00 NLM.home.arpa sshguard 79291 - - Blocking \"192.168.1.21/32\" for 80 secs (1 attacks in 0 secs, after 3 abuses over 892 secs.)","ecs":{"version":"1.12.0"},"agent":{"type":"filebeat","version":"7.17.18","name":"debian12","hostname":"debian12","id":"c0749d68-db29-4158-8f0d-88afcfd8ce56","ephemeral_id":"435a8d37-a157-4f43-bf73-d554329039c4"},"log":{"offset":192342,"file":{"path":"/var/log/pfsense/pfsense.log"}},"@timestamp":"2024-03-20T17:56:45.556Z","event":{"original":"Mar 20 18:56:42 _gateway 1 2024-03-25T23:54:45.321441+01:00 NLM.home.arpa sshguard 79291 - - Blocking \"192.168.1.21/32\" for 80 secs (1 attacks in 0 secs, after 3 abuses over 892 secs.)"},"@version":"1","input":{"type":"log"}}

université de TOURS

05

Conclusion

Conclusion générale et ouvertures

Conclusion

Objectifs réalisés

- Installation de l'infrastructure complète (Firewall, SIEM, serveurs WEB)
- Répartition de charge WEB (HaProxy)
- Simulations d'attaques depuis un WAN
- Notifications et alertes immédiates par e-mail

Difficultés rencontrées

- Notifications par e-mail
- Blocage des attaques (Utilisation Package)
  - Suricata, Crowdsec, Fail2ban..
- Double indexation des logs WEB/FW sur Kibana

université de TOURS

Merci

de votre écoute

Lukas THÉOTIME
Max DOUALAN
Nathan MARTEL