

Réagir face à une cyber-attaque

Lukas Théotime - Max Doualan - Nathan Martel

Sommaire

01

Introduction

Introduction du projet, objectifs réalisés et outils utilisés

02

Architecture

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

03

Gestion des logs

Acheminement des événements de sécurité sur le réseau

04

Attaques et notifications

Simulation d'attaques et gestion des alertes par e-mail

05

Conclusion

Conclusion générale et ouverture

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

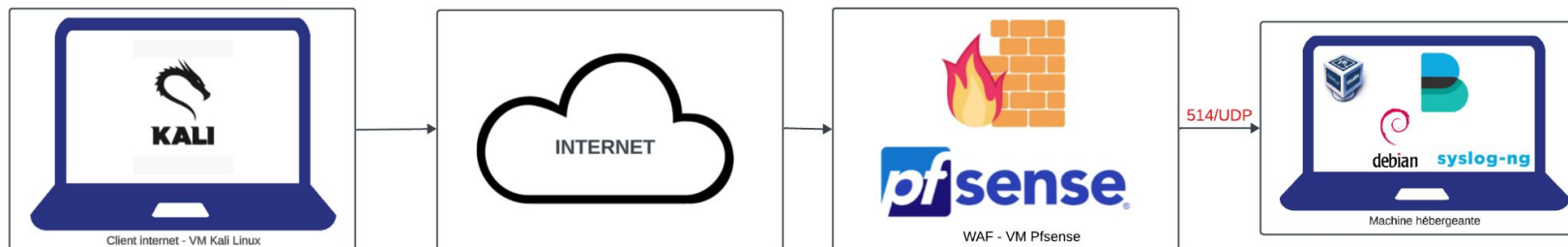
02

Architecture

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

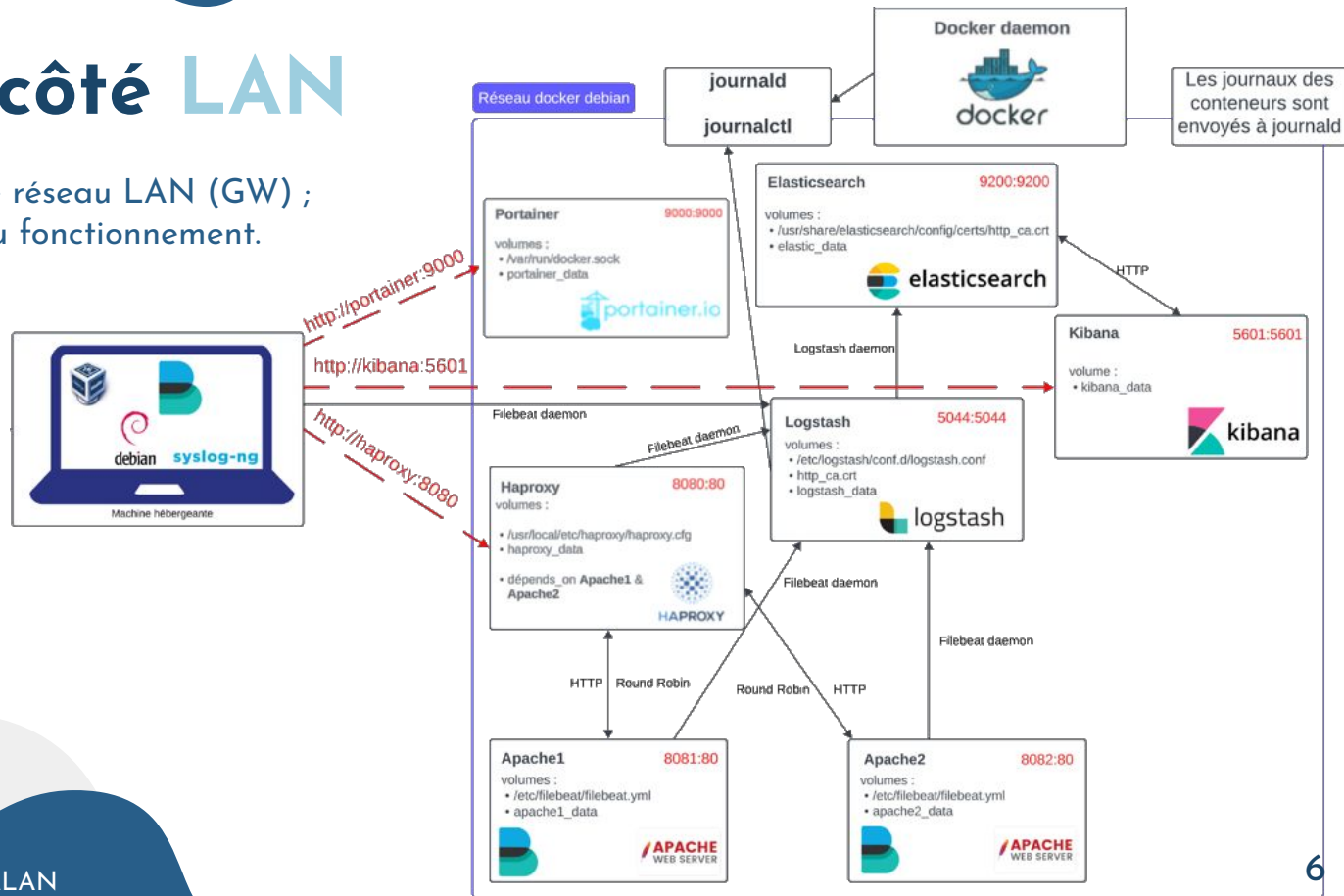
Architecture côté WAN

- 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

Login Protection

Threshold
Block attackers when their cumulative attack score exceeds threshold. Most attacks have a score of 10.

Blocktime
Block attackers for initially blocktime seconds after exceeding threshold. Subsequent blocks increase by a factor of 1.5. Attacks are unblocked at random intervals, so actual block times will be longer.

Detection time
Remember potential attackers for up to detection_time seconds before resetting their score.

Pass list / 128
Addresses added to the pass list will bypass login protection.

Add address

Configuration de la protection SSH du pfSense

Max. states
Maximum state entries this rule can create.

Max. src nodes
Maximum number of unique source hosts.

Max. connections
Maximum number of established connections per host (TCP only).

Max. src. states
Maximum state entries per host.

Max. src. conn. Rate
Maximum new connections per host (TCP only).

Max. src. conn. Rates
/ per how many second(s) (TCP only)

State timeout
State Timeout in seconds

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

03

Gestion des logs

Acheminement des événements de sécurité sur le
réseau

Gestion des logs WEB

Logstash

Traitement et gestion des événements WEB

Kibana

Visualisation des données, dashboard

808X:5044

Filebeat

Envoi des logs à distance en direction de logstash

5044:9200

9200:5601

Elastic

Analyse, indexation des logs. Source pour Kibana

5601

Gestion des logs de Pfsense

Debian

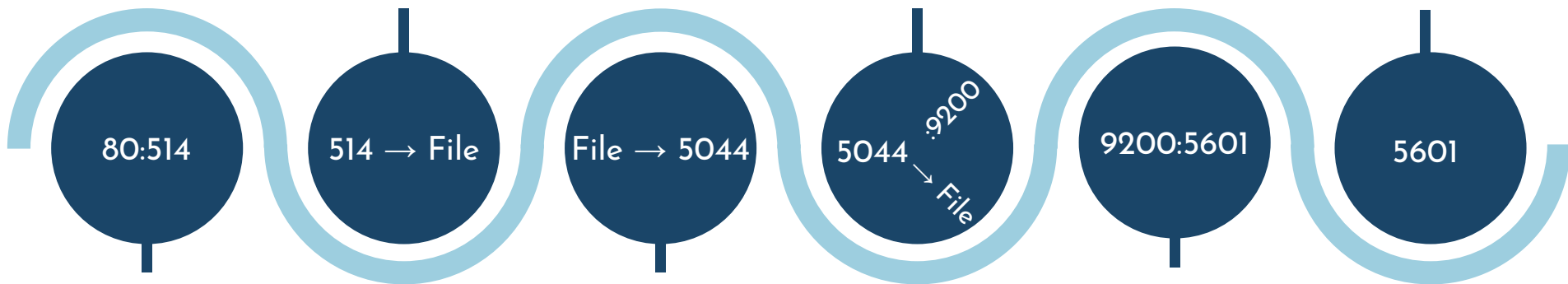
Écoute, filtrage et stockage
des logs avec syslog-ng

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

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

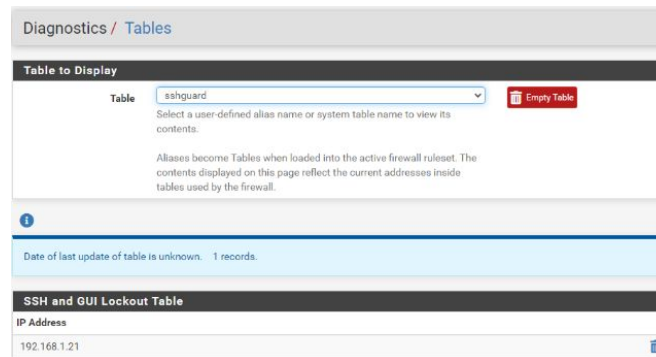


Table des IP bannies

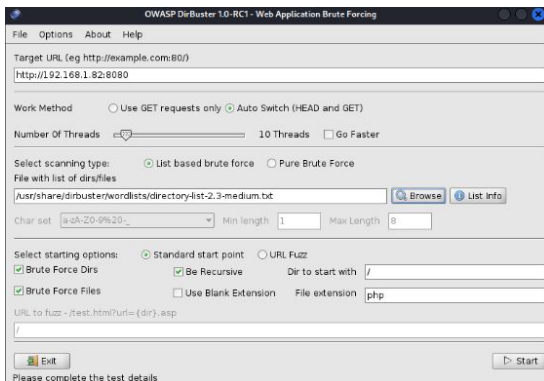
2024-03-26 03:46:56.530257+01:00	sshguard	70212	Blocking "192.168.1.21/32" for 480 secs (1 attacks in 0 secs, after 4 abuses over 6188 secs.)
2024-03-26 03:48:56.529381+01:00	sshguard	70212	Attack from "192.168.1.21" on service SSH with danger 10.

Logs dans pfSense

↓ @timestamp	↓ message.keyword
✓ Mar 20, 2024 @ 19:22:01.052	Mar 20 19:22:00_gateway 1 2024-03-26T12:44:36.371138+01:00 NLN.home.arpa sshguard 70212 - - Blocking "192.168.1.21/32" for 960 secs (1 attacks in 0 secs, after 5 abuses over 3828 secs.)
✓ Mar 20, 2024 @ 19:02:58.956	Mar 20 19:02:57_gateway 1 2024-03-26T03:48:56.530257+01:00 NLN.home.arpa sshguard 70212 - - Blocking "192.168.1.21/32" for 480 secs (1 attacks in 0 secs, after 4 abuses over 6188 secs.)
✓ Mar 20, 2024 @ 19:00:40.852	Mar 20 19:00:40_gateway 1 2024-03-26T02:37:43.061418+01:00 NLN.home.arpa sshguard 70212 - - Blocking "192.168.1.21/32" for 240 secs (1 attacks in 0 secs, after 3 abuses over 1915 secs.)
✓ Mar 20, 2024 @ 19:00:38.848	Mar 20 19:00:38_gateway 1 2024-03-26T02:34:10.000639+01:00 NLN.home.arpa sshguard 70212 - - Blocking "192.168.1.21/32" for 120 secs (2 attacks in 1144 secs, after 2 abuses over 1702 secs.)

Logs reçus dans Kibana

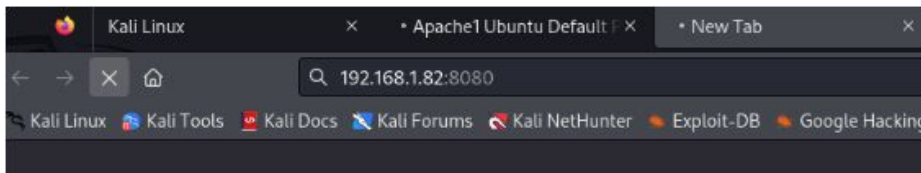
Attaque Dirbuster



Exemple attaque Dirbuster

Current speed: 0 requests/sec
Average speed: (T) 0, (C) 0 requests/sec
Parse Queue Size: 0
Total Requests: 7/441097
Current number of running threads: 10
[Change]

Attaque arrêté



Plus d'accès au site

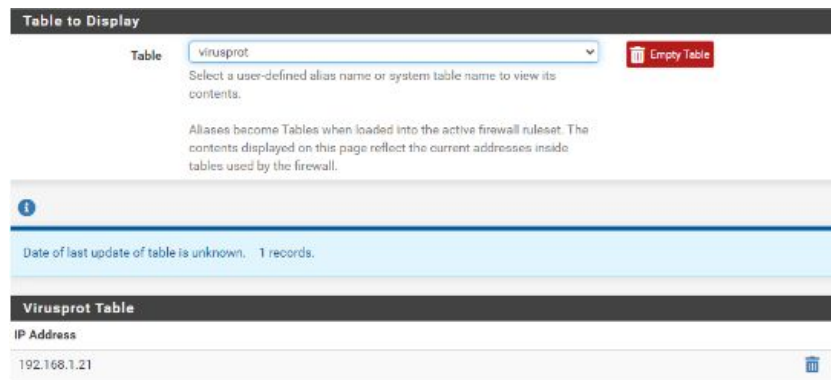


Table des IP bannies

- 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@4ea/ba528ead: /usr/share/elasticsear...  x  debian@debian12: ~  x
#!/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 bloquée" 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 bloquée

Boîte de réception x



root <ayressios@gmail.com>

À moi ▼

mer. 20 mars 18:57 (il y a 20 heures)



```
{
  "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"
        }
      }
    }
  }
}
```

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

Merci de votre écoute

Lukas THÉOTIME
Max DOUALAN
Nathan MARTEL