Laboratoire Sécurité des Systèmes d'Information (SSI)

Rapport de Projet

NF-ANALYZER

BATIER Léa, MESNIER Florian, HOLOIA Georges

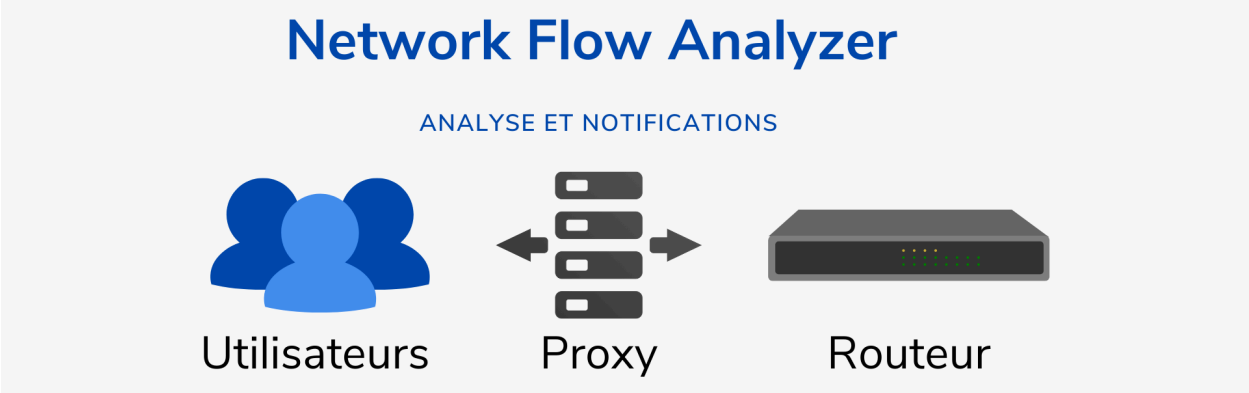
Groupe 19

BORDEAUX YNOV CAMPUS

Tables des matières

Introduction

Notre projet est une solution utile pour les particuliers et les TPE/PME. Notre but est de déployer un proxy et un HIDS (host-based intrusion detection system) qui seront connecter à la box internet par un Raspberry pi; ce dernier analysera les connexions entrantes pour détecter des potentiels malwares. En cas de détection, l'utilisateur recevra une notification. Cette solution sera facile à mettre en place pour l'utilisateur et peu coûteuse.



Ce projet s'inscrit également dans le cadre de notre projet fil rouge de Master permettant l'obtention du titre RNCP; de ce fait nous avons consacré une partie de notre temps à la réalisation des livrables nécessaires liés à ce projet. Ces livrables sont majoritairement orientés gouvernance de la cybersécurité (PCA/PRA, plan d'action, etc...). Pour réaliser ce projet nous nous plaçons en tant qu'entreprise de consulting choisi par une TPE/PME afin de l'aider à sécuriser ces systèmes et à améliorer sa résilience.

Justification du projet

La cybersécurité est souvent perçue comme complexe pour plusieurs raisons, tant chez les particuliers que dans les petites et moyennes entreprises (TPE/PME), d'où l'intérêt de créer une solution peu coûteuse, simple d’utilisation et de mise en place.

Beaucoup de particuliers et de petites entreprises ne possèdent pas les compétences techniques nécessaires pour comprendre pleinement les menaces et les mesures de sécurité nécessaires. La cybersécurité implique souvent des concepts techniques complexes.

Pour les TPE/PME en particulier, les ressources financières et humaines sont souvent limitées. Investir dans des solutions de cybersécurité peut sembler coûteux et nécessite souvent des compétences spécialisées qui ne sont pas toujours disponibles en interne.

Les outils de cybersécurité eux-mêmes peuvent être complexes à mettre en place et à gérer. Les logiciels antivirus, les pare-feu et autres solutions de sécurité peuvent nécessiter une configuration et une maintenance expertes, ce qui peut être décourageant pour les utilisateurs moins techniques.

Notre solution permettra de répondre à ces difficultés tout en sensibilisant plus de monde à la cybersécurité et ses enjeux.

Organisation du projet

Dans le cadre de notre projet, nous avons accordé une grande importance à la répartition équitable des tâches entre les membres de l'équipe, à savoir Léa, Florian et Georges. Cette répartition a été soigneusement planifiée en fonction des connaissances et des compétences de chacun, dans le but d'optimiser notre efficacité collective.

Léa occupe le rôle de coordinatrice du projet. Sa responsabilité principale est de superviser la progression globale du projet et de s'assurer que les délais sont respectés. Elle gère également la bonne réalisation des livrables attendus (le rapport et la présentation). Elle s'occupe aussi des livrables de gouvernance nécessaires au titre RNCP.

Florian et Georges ont pris en charge le développement technique du projet; dû à leurs compétences en programmation et en conception, ils sont responsables de la mise en œuvre des aspects techniques du projet, assurant ainsi son bon fonctionnement.

Cette répartition des tâches nous permet non seulement de capitaliser sur les forces individuelles de chaque membre de l'équipe, mais également de garantir que chaque contributeur apporte une valeur significative au projet dans son ensemble. Cette approche a renforcé notre capacité à atteindre nos objectifs de manière efficace et efficiente.

Afin de visualiser au mieux la répartition des tâches et l'avancement du projet nous avons réalisé un excel pour suivre l'évolution globale du projet.

Voici un exemple d'une infime partie de notre Excel :

ynov CAMPUS

AVANCEMENT DES TACHES
RNCP35078 - Expert informatique et systèmes d'information

BLOC	Date et type d'évaluation	Compétences	Personnes désignées pour la tâche	Avancement des tâches	Avancement du bloc
Bloc 1 : Analyser et définir la stratégie du système d'information	**Juin 2024 / Soutenance orale**	C1.1. Elaborer la stratégie du SI à partir du diagnostic des besoins	Léa, Hugues	60%	38,57%
		C1.2. Déterminer la politique de sous-traitance et partenariale à mettre en place	Florian,Georges	70%	
		C1.3. Etablir un plan d'activité et/ ou un plan d'urbanisation du SI	0	0%	
		C1.4. Identifier les projets d'évolution du SI	0	0%	
		C1.5. Estimer les coûts de la mise en œuvre du SI	0	0%	
		C1.6. Participer à la définition de la stratégie de sécurité du SI	Léa,Hugues,Georges	60%	
		C1.7. Collaborer à la réalisation d'un audit du SI de l'entreprise	Florian,Hugues	70%	
		C1.8. Piloter la production d'un PCA et/ou d'un PRA	Léa,Hugues	5%	
		C1.9. Participer à la production d'un plan d'action	Léa, Florian	5%	
		C1.10. Conduire le plan d'évolution du SI	Léa, Florian	0%	

Exemple pour la feuille "AVANCEMENT DES TÂCHES" , bloc 1

Notre Excel comprend neuf feuilles nous permettant une organisation détaillée et optimisée. Chaque personne du groupe remplit régulièrement le fichier afin de connaître l'avancée précise du projet.

GRILLE D'EVALUATION D'UN BLOC DE COMPETENCES
Expert informatique et systèmes d'information

Lien du drive Bloc 1 :

BLOC	Compétences	Livrable attendu	Critères d'évaluation
Analyser et définir la stratégie du système d'information	C1.1. Elaborer la stratégie du SI à partir du diagnostic des besoins	Une présentation des besoins métier par secteur d'activité. Une présentation des orientation du SI et des axes stratégiques	Les besoins métiers sont détaillés, analysés et correspondent au secteur d'activité. Les orientations du SI et les axes stratégiques sont clairement définis et conformes aux besoins métiers préalablement présentés.
	C1.2. Déterminer la politique de sous-traitance et partenariale à mettre en place	Une présentation de la politique de sous-traitance.	Les différentes possibilités de sous-traitants sont listées avec : - leur nom ; - les avantages et inconvénients de leurs offres. Le choix d'une sous-traitance est défini avec des arguments étayés. (ex : bénéfices / risques)
	C1.3. Etablir un plan d'activité et/ ou un plan d'urbanisation du SI	Une présentation d'un plan d'urbanisation du SI.	Les composants majeurs du SI sont identifiés sur le plan d'urbanisation
	C1.4. Identifier les projets d'évolution du SI	Une présentation des évolutions SI envisagées	Les composants impactés par des évolutions sont identifiés. Les pistes d'évolutions retenues sont justifiées. Elles sont cohérentes avec le secteur d'activité, le besoin client et son contexte technique
	C1.5. Estimer les coûts de la mise en œuvre du SI	Une présentation d'une estimation budgétaire	Les propositions sont correctement budgétées. La méthode utilisée pour réaliser le budget est décrite et justifiée. L'ensemble respecte le budget du client.
	C1.6. Participer à la définition de la stratégie de sécurité du SI	Une présentation d'actions pour améliorer la sécurité du SI	Les actions proposées sont détaillées avec des arguments justifiant leur utilité (ex : avantages, inconvénients, gains attendus). Ces actions génèrent une prévision d'amélioration concrète et mesurable de la sécurité du SI.
	C1.7. Collaborer à la réalisation d'un audit du SI de l'entreprise	Une présentation de l'audit sécurité	L'audit de sécurité couvre l'ensemble du système du client. Une synthèse du résultat de l'audit est réalisée.
	C1.8. Piloter la production d'un PCA et/ou d'un PRA	Une présentation d'un PCA et/ou d'un PRA	Le PCA et/ou PRA répond au système du client. Les points de vigilance du PCA et/ou PRA sont décrits avec des actions pour les contrôler.
	C1.9. Participer à la production d'un plan d'action	Une présentation d'un plan d'action	La plan d'action est jalonné jusqu'à l'atteinte de l'objectif fixé. Le plan d'action respecte les délais du projet.
	C1.10. Conduire le plan d'évolution du SI	Une présentation d'une roadmap	La roadmap contient des objectifs clairs (ex : SMART). La roadmap doit s'appuyer sur la stratégie fixée.

Exemple de la feuille "Grille Eval Bloc 1"

Chaque bloc d'évaluation y est détaillé précisément pour éviter de réaliser un hors sujet.

Notre fichier comprend également les détails de notre client fictif et le RACI qui est l'essence de l'organisation de projet.

Schéma de l’infrastructure

Voici un schéma de l’infrastructure pour la mise en place de notre solution chez un particulier :

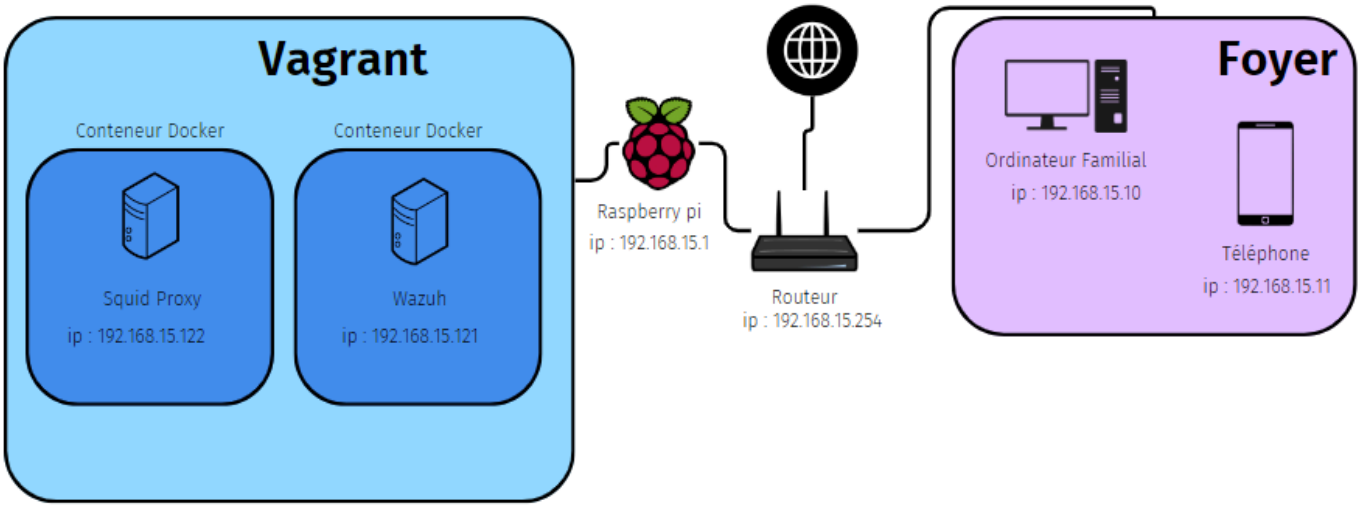


Schéma d'infrastructure pour un particulier.

Description de la mise en place du projet

Outils utilisés

Dans le cadre de notre projet, nous avons exploité un ensemble varié d'outils technologiques pour réaliser une solution robuste et adaptable à nos clients. Avec Docker, nous avons simplifié le déploiement et la gestion de nos applications, créant des environnements de conteneurs isolés et efficaces. Vagrant, quant à lui, nous a offert la flexibilité nécessaire pour configurer rapidement des environnements de développement virtuels, garantissant une cohérence dans nos processus de développement. Nous avons intégré Squid Proxy, un serveur proxy puissant permettant une gestion fine des accès et une optimisation des performances. Enfin, avec Wazuh, nous avons assuré une surveillance continue de la sécurité, détectant et répondant aux menaces potentielles grâce à une analyse intelligente des journaux et des événements.

Ces outils nous ont permis de réaliser notre solution et de la rendre facilement déployable chez le client. Nos clients pourront rapidement mettre en place notre solution sur leurs propres machines, quel que soit leur système d'exploitation, en suivant des étapes simples et en utilisant des commandes familières. Cela élimine la nécessité d'avoir des connaissances approfondies en configuration système ou en administration, rendant notre solution accessible à un plus large éventail de clients.

Vagrant

Nous avons opté pour l'utilisation de Vagrant, un outil puissant qui a grandement facilité la gestion de nos environnements. Vagrant est une plateforme open-source qui permet de créer et de configurer rapidement des environnements de développement virtuels, offrant ainsi une solution portable et reproductible pour le déploiement de logiciels.

En intégrant Vagrant dans notre processus de développement, nous avons pris en compte la facilité de déploiement pour nos futurs clients, qu'ils possèdent ou non des compétences techniques approfondies. Vagrant simplifie considérablement le processus de déploiement

en créant des environnements de développement virtuels prêts à l'emploi, ce qui signifie que nos clients n'auront pas à se soucier de configurer manuellement les infrastructures nécessaires.

En offrant une expérience de déploiement fluide et sans tracas, nous nous assurons que nos clients puissent bénéficier rapidement des avantages de notre solution, tout en réduisant les obstacles techniques qui pourraient entraver son adoption. En fin de compte, l'intégration de Vagrant dans notre processus de développement renforce notre engagement à fournir une solution accessible et conviviale, qui peut être déployée facilement par tous.

Wazuh

Dans le cadre de notre projet, nous avons fait appel à Wazuh, une plateforme de gestion de la sécurité qui offre une surveillance continue des environnements informatiques. Wazuh est une solution open-source conçue pour aider les organisations à détecter, répondre et gérer les menaces de sécurité de manière proactive.

Wazuh fonctionne en collectant et en analysant les journaux, les événements et les données de sécurité à partir de diverses sources telles que les fichiers journaux système, les bases de données et les applications web. En utilisant des techniques avancées de corrélation et d'analyse des journaux, Wazuh identifie les comportements suspects, les vulnérabilités et les attaques potentielles, ce qui permet aux équipes de sécurité informatique de réagir rapidement pour atténuer les risques.

Une des fonctionnalités clés de Wazuh est son système de détection d'intrusion (IDS), qui surveille en temps réel les activités réseau et système à la recherche de comportements malveillants. En détectant et en alertant sur les menaces dès qu'elles se produisent, Wazuh permet aux organisations de prendre des mesures préventives pour protéger leurs systèmes et leurs données.

De plus, Wazuh offre des fonctionnalités avancées de gestion des incidents, telles que la corrélation d'événements, la remédiation automatisée et la génération de rapports détaillés sur la sécurité. En fournissant une visibilité complète sur l'état de la sécurité informatique, Wazuh aide les organisations à renforcer leur posture de sécurité et à répondre efficacement aux défis croissants de la cybersécurité.

L’intégration de Wazuh dans notre projet reflète notre engagement à aider nos clients à être mieux sécurisés et à mieux appréhender le monde de la cybersécurité.

Docker

Nous avons opté pour l'utilisation de Docker, une technologie de virtualisation légère et flexible qui a grandement facilité le déploiement et la gestion de nos applications. Docker permet de créer, de distribuer et d'exécuter des applications dans des conteneurs logiciels, offrant ainsi un environnement isolé et cohérent pour le développement et le déploiement d'applications.

Contrairement à la virtualisation traditionnelle, où chaque application est exécutée dans sa propre machine virtuelle, Docker utilise des conteneurs légers qui partagent les ressources du système hôte. Cela permet d'optimiser l'utilisation des ressources et de réduire les surcharges liées à la virtualisation, tout en offrant un déploiement rapide et reproductible des applications.

En résumé, l'utilisation de Docker dans notre projet a considérablement simplifié le processus de développement et de déploiement des applications, tout en améliorant l'efficacité opérationnelle et la flexibilité de notre infrastructure.

Squid Proxy

Nous avons choisi d'intégrer Squid Proxy, un serveur proxy hautement configurable et polyvalent, qui a joué un rôle essentiel dans la gestion et la sécurisation du trafic Internet.

Squid Proxy agit comme une passerelle intermédiaire entre les utilisateurs et Internet, permettant de contrôler et de filtrer les requêtes HTTP, HTTPS, FTP et d'autres protocoles réseau.

L'une des principales fonctions de Squid Proxy est de mettre en cache les pages Web fréquemment consultées, ce qui permet d'accélérer l'accès aux ressources en réduisant le temps de chargement des pages pour les utilisateurs. En stockant localement les copies des pages Web demandées, Squid Proxy peut répondre aux futures demandes provenant des utilisateurs sans avoir à accéder à nouveau aux serveurs distants, ce qui réduit la bande passante nécessaire et améliore les performances du réseau.

En intégrant Squid Proxy, nous avons pu bénéficier d'une solution robuste et évolutive pour la gestion du trafic Internet, offrant à la fois des avantages en termes de performance, de sécurité et de contrôle d'accès. En fin de compte, l'utilisation de Squid Proxy nous aide à fournir une solution complète qui répond aux besoins de connectivité et de sécurité de nos utilisateurs.

Description technique du projet

Notre environnement virtuel créé par vagrant comprend deux machines linux ubuntu 22.04, une pour notre serveur proxy Squid et un autre pour notre serveur Wazuh.

Fichier Vagrantfile

```
#VM Wazuh
  config.vm.define "NFA-wazuh" do |wazuh| # to change: vm name to display
in "vagrant status" command.
    wazuh.vm.provider "Wazuh" do |vb|
      vb.name = "NFA-wazuh" # to change: the name to display in VirtualBox
GUI.
      vb.memory = "4000" # to change: RAM amount.
      vb.cpus = 2 # to change: total number of vcpus.
    end
    wazuh.vm.box = "generic/ubuntu2204"
    wazuh.vm.provision "shell", path: "provision-vm-wazuh.sh"
    wazuh.vm.hostname = "nf-analyzer-wazuh.fr" # to change: the vm
hostname.
    wazuh.vm.network "private_network", ip: "192.168.15.121"
    wazuh.vm.network "forwarded_port", guest: 443, host: 8443
    wazuh.vm.network "forwarded_port", guest: 80, host: 8080
  end
  #VM Proxy Squid
  config.vm.define "NFA-prox" do |squid| # to change: vm name to display in
"vagrant status" command.
    squid.vm.provider "Proxy" do |vb|
      vb.name = "NFA-proxy" # to change: the name to display in VirtualBox
GUI.
      vb.memory = "2048" # to change: RAM amount.
      vb.cpus = 2 # to change: total number of vcpus.
    end
    squid.vm.box = "generic/ubuntu2204"
    squid.vm.provision "shell", path: "provision-prox.sh"
    squid.vm.hostname = "nf-analyzer.fr" # to change: the vm hostname.
    squid.vm.network "private_network", ip: "192.168.15.122"
  end
```

Nos deux machines sont configurées par un script de provision pour que chaque solution soit montée automatiquement au lancement de vagrant.

Fichier provision proxy squid

```
#!/bin/bash
#configuration système :
sudo apt update && sudo apt upgrade -y
sudo apt-get install expect -y
wget -q -c -N
https://raw.githubusercontent.com/maravento/blackweb/master/blackweb.tar.gz &&
cat blackweb.tar.gz* | tar xzf -
#Configuration Docker :
echo 'vm.max_map_count=262144' | sudo tee -a /etc/sysctl.conf
sudo sysctl -p
sudo useradd admdocker
sudo echo 'admdocker:nfadocker' | sudo chpasswd
sudo mkdir /home/admdocker
sudo chown admdocker:admdocker /home/admdocker
sudo chmod 700 /home/admdocker
sudo chmod u+w /home/admdocker
sudo usermod -s /bin/bash admdocker
sudo usermod -aG sudo admdocker
sudo curl -sSL https://get.docker.com/ | sh
sudo systemctl start docker
sudo curl -L
"https://github.com/docker/compose/releases/download/v2.12.2/docker-compose-$(u
name -s)-$(uname -m)" -o /usr/local/bin/docker-compose
sudo chmod +x /usr/local/bin/docker-compose
sudo usermod -aG docker admdocker
echo 'admdocker ALL=(ALL) NOPASSWD: ALL' | sudo tee -a /etc/sudoers
sudo cp blackweb.txt /home/admdocker/
sudo chown admdocker:admdocker /home/admdocker/blackweb.txt
#Script pour se loger à un autre user :
echo '#!/usr/bin/expect
set username "admdocker"
set password "nfadocker"
spawn su - $username
expect "Password:"
send "$password\r"
interact' | sudo tee /home/vagrant/login_expect.sh
chmod +x login_expect.sh
sudo mkdir /var/spool/squid/
./login_expect.sh
#Fichier docker-compose.yml :
echo 'version: "3"
services:
```

```
  proxy:
    image: ubuntu/squid
    ports:
      - "3128:3128"
    environment:
      - TZ=UTC
    volumes:
      - ./squid.conf:/etc/squid/squid.conf
      - ./blackweb.txt:/etc/squid/blackweb.txt' | sudo tee
/home/admdocker/docker-compose.yml
#Fichier de config squid :
echo 'http_port 3128
cache_dir ufs /var/spool/squid 100 16 256
acl all src all # ACL pour autoriser/refuser tous les réseaux (Source = All) -
ACL obligatoire
acl Safe_ports port 80 # Port HTTP = Port sure
acl Safe_ports port 443 # Port HTTPS = Port sure
acl Safe_ports port 21 # Port FTP = Port sure
http_access deny !Safe_ports
#Blacklist Domain
acl domain_blacklist dstdomain "/etc/squid/blackweb.txt"
acl domain_blacklist dstdomain .youtube.com
http_access deny domain_blacklist
# Block torrent files
acl TorrentFiles rep_mime_type -i mime-type application/x-bittorrent
http_reply_access deny TorrentFiles
deny_info TCP_RESET TorrentFiles
#Block flash video
acl deny_rep_mime_flashvideo rep_mime_type video/flv
http_reply_access deny deny_rep_mime_flashvideo
access_log /var/log/squid/access.log' | sudo tee /home/admdocker/squid.conf
#Lancement du conteneur :
sudo docker-compose --verbose up -d
```

Dans la configuration ci dessus on configure le proxy Squid pour :

- qu'il écoute sur le port 3128;
- qu'il mette en cache les pages web visité;
- qu'il autorise les flux seulement sur les ports 80,443 et 21;
- blacklists des domaines à risque (porn, downloads, drugs, malware, spyware; trackers, bots, social networks, warez, weapons, etc.);
- qu'il bloque du téléchargement de torrent file;

- qu'il bloque l'accès aux pages utilisant Flash video.

Fichier provision Wazuh

```
#!/bin/bash
# Section "NFA - Solution"
if [[ $1 == "solution" ]]; then
    echo "[#]Executing commands for NFA - Solution"
    echo "..[#]Installation de Wazuh via Docker (single-node)"
    sudo loadkeys fr
    sudo apt update -y && sudo apt upgrade -y
    sudo apt install -y docker-compose
    git clone https://github.com/wazuh/wazuh-docker.git -b v4.7.4
    sudo su -l vagrant -c '
        cd ~/wazuh-docker/single-node
        sudo docker-compose -f generate-indexer-certs.yml run --rm
generator
        sudo docker-compose up -d
        wget
https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.7.
4-1_amd64.deb \
        && sudo WAZUH_MANAGER='192.168.56.1' WAZUH_AGENT_NAME='Solution'
dpkg -i ./wazuh-agent_4.7.4-1_amd64.deb
        sudo systemctl daemon-reload
        sudo systemctl enable wazuh-agent
        sudo systemctl start wazuh-agent
    '
    # si proxy :
    # echo "    environment:
    #   - HTTP_PROXY=YOUR_PROXY_ADDRESS_OR_DNS" >>
generate-indexer-certs.yml
fi
# Section "NFA - Proxy"
if [[ $1 == "proxy" ]]; then
    echo "Executing commands for NFA - Serveur Proxy"
    sudo apt update -y && sudo apt upgrade -y
    sudo su -l vagrant -c '
        cd ~/wazuh-docker/single-node
        sudo docker-compose -f generate-indexer-certs.yml run --rm
generator
        sudo docker-compose up -d
```

```
        wget
https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.7.
4-1_amd64.deb \
        && sudo WAZUH_MANAGER='192.168.56.2' WAZUH_AGENT_NAME='Proxy' dpkg
-i ./wazuh-agent_4.7.4-1_amd64.deb
        sudo systemctl daemon-reload
        sudo systemctl enable wazuh-agent
        sudo systemctl start wazuh-agent
    '
fi
```

Dans la configuration ci-dessus on configure le serveur Wazuh et une VM (user) pour :

- qu'il installe le serveur Wazuh en single node sur la VM "Solution";
- qu'il créer le script permettant d'installer l'agent Wazuh sur la VM "Solution" et la VM "user" pour qu'elle remonte sur le Dashboard.

Script installation agent Wazuh

Linux

```
#!/bin/bash
sudo ufw allow 1514
sudo ufw allow 1515
sudo ufw allow 55000
ubuntu_hostname=$(hostname)
wget
https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.7.4-1_
amd64.deb && sudo WAZUH_MANAGER="192.168.56.10"
WAZUH_AGENT_NAME="$ubuntu_hostname" dpkg -i ./wazuh-agent_4.7.4-1_amd64.deb

sudo systemctl daemon-reload
sudo systemctl enable wazuh-agent
sudo systemctl start wazuh-agent
```

Ce script configure le pare-feu pour permettre la communication avec l'agent Wazuh sur les bon ports, installe l'agent Wazuh sur la machine User (Linux) avec en paramètre notre serveur Wazuh et le nom d'hôte de la machine User, puis démarre le service de l'agent.

Windows

```
#Firewall Rule
New-NetFirewallRule -DisplayName "Wazuh Ports 1514 TCP" -Direction inbound
-Profile Any -Action Allow -LocalPort 1514 -Protocol TCP
New-NetFirewallRule -DisplayName "Wazuh Ports 1515 TCP" -Direction inbound
-Profile Any -Action Allow -LocalPort 1515 -Protocol TCP
New-NetFirewallRule -DisplayName "Wazuh Ports 55000 TCP" -Direction inbound
-Profile Any -Action Allow -LocalPort 55000 -Protocol TCP
New-NetFirewallRule -DisplayName "Wazuh Ports 1514 TCP" -Direction outbound
-Profile Any -Action Allow -LocalPort 1514 -Protocol TCP
New-NetFirewallRule -DisplayName "Wazuh Ports 1515 TCP" -Direction outbound
-Profile Any -Action Allow -LocalPort 1515 -Protocol TCP
New-NetFirewallRule -DisplayName "Wazuh Ports 55000 TCP" -Direction outbound
-Profile Any -Action Allow -LocalPort 55000 -Protocol TCP

#Wazuh-agent Install
Invoke-WebRequest -Uri
https://packages.wazuh.com/4.x/windows/wazuh-agent-4.7.4-1.msi -OutFile
${env.tmp}\wazuh-agent;
msiexec.exe /i ${env.tmp}\wazuh-agent /q WAZUH_MANAGER='192.168.56.10'
WAZUH_AGENT_NAME="$env:COMPUTERNAME" WAZUH_REGISTRATION_SERVER='192.168.56.10'

#run service
NET START Wazuh
```

Ce script configure les règles de pare-feu nécessaires, télécharge et installe l'agent Wazuh sur la machine Windows, puis démarre le service Wazuh.

Problèmes rencontrés et Solutions apportées

Au cours de la période de développement de notre projet, nous avons été confrontés à une série de problèmes qui ont varié en termes de gravité et d'impact sur nos objectifs.

Le premier défi majeur que nous avons rencontré concernait l'utilisation de Vagrant, une plateforme essentielle pour la configuration de nos environnements de développement. Alors que nous apportions des modifications au fichier de provisionnement, nous avons découvert l'existence d'une commande permettant de recharger automatiquement la configuration et de redémarrer la machine (`vagrant reload --provision)`. Cependant, cette commande ne fonctionnait pas comme prévu. À chaque tentative d'utilisation, la configuration de la machine était cassée, nous obligeant à reconstruire l'intégralité de la machine à partir de zéro à chaque changement de configuration. Cette inefficacité a entraîné d'importantes pertes de temps lors des tests de configurations, ralentissant ainsi notre progression et retardant les étapes ultérieures du projet.

Le deuxième défi majeur auquel nous avons été confrontés était lié à un manque d'organisation et à des changements de choix de solutions en cours de projet. Malgré nos efforts initiaux pour planifier et structurer notre travail, nous avons constaté que certains aspects de notre organisation nécessitaient une amélioration. En particulier, les changements fréquents dans nos choix de solutions et d'approches ont entraîné des retards significatifs dans la réalisation finale du projet. Ces changements ont introduit une certaine confusion au sein de l'équipe et ont nécessité des ajustements constants dans nos plans et nos priorités.

Apport du projet en matière de compétences

Hard Skills

Notre projet, réalisé en collaboration de trois personnes, nous a offert une opportunité précieuse d'acquérir un ensemble diversifié de compétences techniques essentielles. Nous avons plongé dans le monde de l'infrastructure informatique, ce qui nous a permis de développer une solide compréhension de la manière dont les systèmes fonctionnent et interagissent. En utilisant des outils tels que Vagrant, nous avons appris à configurer et à gérer des environnements de développement virtuels, ce qui est crucial pour le déploiement efficace de logiciels et d'applications. De plus, l'exploration de Wazuh, une solution de gestion de la sécurité, nous a donné une expérience pratique dans la mise en place et la surveillance de mesures de sécurité, renforçant ainsi nos compétences dans la protection des systèmes informatiques contre les menaces potentielles.

Soft Skills

Travailler en équipe sur ce projet nous a également offert une opportunité pour cultiver et affiner nos compétences personnelles. La communication efficace a été la clé de notre collaboration réussie, nous permettant de partager des idées, de résoudre des problèmes et de coordonner nos efforts de manière transparente. Nous avons développé notre capacité d'adaptation, apprenant à rester flexibles et réactifs dans des situations variables. De plus, la nécessité d'organiser et de gérer notre travail de manière efficace nous a enseigné des compétences précieuses en matière de gestion du temps et des ressources. En somme, ce projet nous a non seulement permis de renforcer nos compétences techniques, mais aussi de cultiver des qualités essentielles telles que la collaboration, la communication et la résolution de problèmes, qui sont indispensables dans tout environnement professionnel.

Axes d'amélioration pour le futur

Nous avons décalé un axe d’amélioration principal pour notre projet : automatiser la mise à jour de l'environnement, des outils et des logiciels utilisés. Cela présente plusieurs avantages en termes d'efficacité, de sécurité et de fiabilité. Voici quelques exemples qui mettent en lumière l'importance de cette amélioration :

- **Gain de temps et d'efficacité :** En automatisant les mises à jour, on évite la nécessité d'intervenir manuellement sur chaque composant du système, ce qui économise un temps précieux pour l’équipe et réduit les risques d'erreurs humaines.
- **Sécurité renforcée :** Les mises à jour régulières des logiciels et des outils sont essentielles pour garantir la sécurité de la solution. En automatisant ce processus, on s’assure que les derniers correctifs de sécurité sont rapidement appliqués, réduisant ainsi les vulnérabilités et les risques de cyberattaques.
- **Maintien de la compatibilité :** Avec l'évolution constante des technologies, il est crucial de s'assurer que notre solution reste compatible avec les versions les plus récentes des logiciels et des frameworks utilisés. L'automatisation des mises à jour garantit le fonctionnement de manière optimale sur les plateformes actuelles.
- **Fiabilité accrue :** En automatisant les mises à jour, on minimise les interruptions de service potentielles causées par des problèmes de compatibilité ou des bogues non corrigés. Cela garantit une expérience utilisateur fluide et fiable pour nos clients, renforçant ainsi la réputation de notre solution.

En résumé, l'automatisation de la mise à jour de l'environnement, des outils et des logiciels est un axe d'amélioration essentiel pour notre projet. Cela nous permettra de gagner en efficacité, de renforcer la sécurité, de maintenir sa compatibilité et d'assurer une expérience utilisateur fiable et satisfaisante.

Conclusion

En conclusion, notre projet représente une solution innovante et prometteuse pour les particuliers et les TPE/PME, offrant une protection efficace contre les malwares grâce à l'utilisation d'un proxy connecté à la box internet de l'utilisateur. Cependant, tout projet comporte des défis et des opportunités d'amélioration, et notre expérience n'a pas fait exception.

Un axe d'amélioration crucial identifié tout au long du développement est l'automatisation de la mise à jour de l'environnement, des outils et des logiciels utilisés. Cette amélioration permettra d'optimiser notre processus de développement, en garantissant une sécurité renforcée, une compatibilité continue et une fiabilité accrue de notre solution.

Par ailleurs, nous avons rencontré deux problèmes majeurs qui ont impacté la progression de notre projet. Le premier problème concernait l'utilisation de Vagrant, où la commande de recharge de la configuration (vagrant reload --provision) ne fonctionnait pas comme prévu, entraînant une perte de temps considérable lors des tests de configurations. Le deuxième problème était lié au manque d'organisation et aux changements de choix de solutions en cours de projet, ce qui a entraîné des retards significatifs dans la réalisation finale.

Malgré ces défis, notre équipe a su faire preuve de résilience et d'adaptabilité pour surmonter les obstacles rencontrés. Nous avons tiré des leçons précieuses de ces expériences, renforçant ainsi notre expertise et notre détermination.

En nous concentrant sur l'automatisation des mises à jour et en améliorant notre processus de gestion de projet, nous sommes confiants dans notre capacité à surmonter les défis futurs et à faire évoluer notre solution.