

EIP Vigilate

Etude de l'existant (EDE)

1^{er} février 2015

Résumé du document

Ce document détaille l'étude de l'existant de notre EIP Vigilate. L'EDE commence par un rappel de notre sujet d'EIP, Vigilate qui est un outil de sécurité informatique permettant d'informer rapidement les utilisateurs des nouvelles vulnérabilités connues qui les concernent.

Il existe différentes solutions actuellement, c'est ce dont on va parler dans ce document.

Nesus est l'un des plus importants scanner de vulnérabilités mais il va devoir scanner de nombreux plugins avant de tester celui qui nous intéresse réellement.

Shalvik Protect quant à lui va servir à installer les corrections proposées par les éditeurs des programmes vulnérables mais ne peut que détecter l'absence de ces correctifs et pas la réelle présence d'une vulnérabilité

Le CERT/CSIRT n'est pas un programme, mais un groupe de personnes dédié à la sécurité dans une entreprise, il va prendre en compte toutes les étapes pour avoir un système d'information sécurisé.

Cisco Security Manager est un SIEM (security event information management) qui permet d'afficher en temps réel les événements de sécurité de l'infrastructure réseau, cependant un certain niveau de connaissance réseau est nécessaire pour pouvoir utiliser cet outil.

CERT-XMCO est ce qui se rapproche le plus de Vigilate, néanmoins le filtrage n'est pas très précis et le service n'est pas accessible publiquement.

Dans la partie 3 nous montrerons que notre solution se distingue des autres dans leur fonctionnement, en effet il ne s'agit pas d'un véritable scanner de vulnérabilité mais d'un service qui permet d'avertir rapidement les personnes voulant suivre l'état de vulnérabilité de certains programmes en particulier.

En conclusion, une synthèse des différences entre les solutions montre que Vigilate se positionne dans un endroit qui n'est pas assez couvert dans le marché des solutions actuel de suivis de vulnérabilités.

Description du document

Titre	[2017][Vigilate][EDE]
Date	31/01/2015
Auteur	Kévin SOULES
Responsable	Kévin SOULES
Email	vigilate.2017@labeip.epitech.eu
Sujet	Etude de l'existant
Mots clés	Ede, sécurité, vulnérabilités, concurrence
Version du modèle	1.0

Tableau des révisions

Date	Auteur	Section(s)	Commentaires
24/01/15	Kévin Soules		Création du document
27/01/15	Kévin Soules	Chapitre 1 et 2.1	Recherche de liste de solutions. Rédaction du texte d'un premier concurrent. Remplissage des rappels.
28/01/15	Prune Budowski	Chapitre 1	Amélioration des rappels
29/01/15	Prune Budowski	Chapitre 3.3.2	Rédaction de la partie "Ce qui ne sera pas couvert"
29/01/15	Daniel Mercier	Chapitre 2.2	Rédaction du texte du deuxième concurrent.
29/01/15	Kévin Soules	Chapitre 2.3	Rédaction du texte du troisième concurrent.
30/01/15	Morgane Harscoat	Chapitre 2.4	Début de rédaction du texte du quatrième concurrent.
30/01/15	Kévin Soules	Chapitre 2.5	Rédaction du texte du cinquième concurrent.
31/01/15	Kévin Soules	Conclusion, Glossaire	Matrice de préférence. Rédaction d'un glossaire.
31/01/15	Prune Budowski	Résumé, Conclusion, Chapitre 3.1	Rédaction du résumé. SWOT. Rédaction de la partie "Ce que vous apportez".
31/01/15	Daniel Mercier	Toutes	Corrections.
01/01/15	Morgane Harscoat	Toutes	Corrections.

Table des matières

1	Rappel de l'EIP	6
1.1	Qu'est-ce qu'un EIP et Epitech	6
1.2	Sujet de votre EIP	6
1.3	Glossaire	6
2	Les projets existants	8
2.1	Nessus	8
2.1.1	Présentation	8
2.1.2	Historique	8
2.1.3	Description	8
2.1.4	Points positifs	9
2.1.5	Points Négatifs	9
2.1.6	Références	9
2.2	Shalvik Protect	9
2.2.1	Présentation	9
2.2.2	Historique	10
2.2.3	Description	10
2.2.4	Points positifs	10
2.2.5	Points Négatifs	10
2.2.6	Références	10
2.3	CERT/CSIRT	11
2.3.1	Présentation	11
2.3.2	Historique	11
2.3.3	Description	11
2.3.4	Points positifs	12
2.3.5	Points Négatifs	12
2.3.6	Références	12
2.4	Cisco Security Manager	12
2.4.1	Présentation	12
2.4.2	Historique	12
2.4.3	Description	12
2.4.4	Points positifs	12
2.4.5	Points Négatifs	12

2.4.6	Références	12
2.5	CERT-XMCO	13
2.5.1	Présentation	13
2.5.2	Historique	13
2.5.3	Description	13
2.5.4	Points positifs	13
2.5.5	Points Négatifs	13
2.5.6	Références	13
3	Positionnement de votre projet	14
3.1	Ce que vous apportez	14
3.2	Ce qui ne sera pas couvert	14
4	Conclusion	15
4.1	Matrice de préférence	15
4.2	SWOT	16

Chapitre 1

Rappel de l'EIP

1.1 Qu'est-ce qu'un EIP et Epitech

Epitech, école de l'innovation et de l'expertise informatique propose un cursus en 5 années, basé sur une pédagogie par projet (à réaliser seul ou en groupe). L'un de ces projets, l'EIP (Epitech Innovating Project), réalisé par groupe de 6 à 15 étudiants, démarre au cours de la 3ème année et se déroule sur 2 ans et demi. Ce projet doit être particulièrement innovant car son objectif est d'être commercialisable à la fin de la 5ème année d'Epitech.

1.2 Sujet de votre EIP

Le but de Vigilate est d'avertir les utilisateurs des services obsolètes ou potentiellement vulnérables affectant en particulier leur infrastructure (sites web, réseau d'entreprise, logiciels), dans le but de les informer des risques techniques encourus et des éventuelles mises à jour ou corrections à appliquer. Cela sans effectuer de scan de vulnérabilité. On fournit cependant un outil de scan de programme qui envoie la liste sur notre plateforme web.

1.3 Glossaire

- C -

CVE : Common Vulnerabilities and Exposures, c'est un numéro qui renvoie à la fiche descriptive complète d'une vulnérabilité précise. Exemple : CVE-2013-4343.

CSIRT : Computer Security Incident Response Team, une équipe chargée d'assurer la sécurité d'une entreprise.

CERT : Computer Emergency Response Team, marque déposée représentant les CSIRT certifiés.

- F -

Fingerprint : Déduction de la version d'un programme/système d'exploitation en fonction de la façon dont il répond à nos requêtes sur le réseau.

Fork : Création d'un nouveau programme en utilisant le code source du premier.

- G -

GPL : General Public License, licence dédié aux logiciels libres.

- P -

Patch : Un correctif qui corrige un bug ou une vulnérabilité dans un programme.

- S -

SCADA : Supervisory Control and Data Acquisition, système de télégestion à grande échelle utilisé dans l'industrie.

Chapitre 2

Les projets existants

2.1 Nessus

2.1.1 Présentation

Ce scanner de vulnérabilité couvre plusieurs points clé [2] : Scan du réseau, détection de problèmes de configuration, gestion des patchs de sécurité, scan web, scan SCADA, détection de certains malwares. C'est donc une solution complète qui satisfait une bonne part de services informatiques. Un sondage le classe même dans le scanner de vulnérabilité le plus utilisé.

2.1.2 Historique

C'est Renaud Deraison qui en 1998 développe son scanner de vulnérabilité. Libre à son commencement (licence GPL), en 2002 il co-fonde Tenable Network Security [3] et c'est en 2005 qu'il change la licence de Nessus en programme propriétaire. [4] C'est à ce moment-là que son petit frère OpenVAS, fork libre de Nessus (licence GPL) voit le jour [5]. Depuis, ces deux programmes évoluent chacun de leur côté.

2.1.3 Description

Nessus est fourni avec une grande base de plugins permettant de détecter des vulnérabilités. Ces plugins sont écrits dans un langage dédié (nasl).

Un scan nessus s'effectue en plusieurs étapes [6] :

- Découverte du réseau
- Scan de port sur les machines découvertes
- Fingerprint pour récupérer les informations de version des services distants
- Possibilité d'avoir un scan authentifié et de récupérer des informations en se connectant directement sur la machine. (ssh/WMI)

- Plusieurs type d'attaques effectuées (de certaines peu agressives, à certaines pouvant enrêner une indisponibilité momentané de la machine ou du service ciblé)

Une fois le scan effectué, un rapport détaillé (html/wml/pdf) est généré, avec la description de chaque problème rencontrés, l'adresse de la machine vulnérable, le niveau de sévérité de la vulnérabilité et d'une solution générique pour résoudre le problème.

2.1.4 Points positifs

C'est un outil très complet. Il permet d'effectuer aussi bien des audits ciblés qu'un suivi régulier de l'état de vulnérabilité du système d'information.

2.1.5 Points Négatifs

Pour qu'une nouvelle vulnérabilité soit signalée, plusieurs étapes sont nécessaires :

- Il faut que l'éditeur publie un plugin nasl permettant de découvrir la nouvelle vulnérabilité.
- Il faut que le scanner synchronise sa base de données de plugin. (Souvent de façon quotidienne)
- Il faut qu'un scan soit relancé (des fois quotidiennement) et qu'il se termine. En effet, malgré l'affichage des vulnérabilités trouvées en direct sur l'interface, le scanner va devoir tester plusieurs milliers de plugins avant de tester le tout dernier qui nous intéresse. Évidement on pourrait relancer un scan avec seulement ce seul plugin, mais là nous dépassons la dimension automatique du test.

2.1.6 Références

- [1] <http://www.tenable.com/products/nessus>
- [2] <http://www.tenable.com/products/nessus/nessus-vulnerability-scanner/features>
- [3] <http://techcrunch.com/2012/09/05/tenable-accel-series-a/>
- [3] http://news.cnet.com/Nessus-security-tool-closes-its-source/2100-7344_3-5890093.html
- [5] <http://lists.wald.intevation.org/pipermail/openvas-discuss/2005-December/000100.html>
- [6] http://static.tenable.com/documentation/nessus_6.2_user_guide.pdf

2.2 Shalvik Protect

2.2.1 Présentation

Shalvik Protect est une solution de gestion de patch (patch management en anglais). Cette solution permet de gérer les patches pour les systèmes d'exploitation, les environnements virtuels et les applications tierces.

2.2.2 Historique

Originellement appelé HFNetChk (HotFix Network Check), Shalvik protect est créé au début des années 2000.

La fonctionnalité de gestion de patch est ajoutée à la version 3 de HFNetChk qui ne serait jamais mis en vente, cette fonctionnalité est donc disponible pour les clients de Shalvik à partir de la version 4.0. Aujourd'hui Shalvik Protect en est à la version 9.

2.2.3 Description

Une solution de gestion de patchs permet de faciliter l'installation des correctifs.

En effet Shalvik Protect va, régulièrement récupérer les nouveaux patchs disponibles et regarder si ils sont appliqués sur les machines du réseaux dans lequel il est installé.

Les patchs non installés sont signalés à l'utilisateur et Shalvik protect propose ensuite de les installer sur toutes les machines concernées.

2.2.4 Points positifs

Les solutions de gestion de patchs permettent de se protéger d'une vulnérabilité dès qu'elle est corrigée.

2.2.5 Points Négatifs

Les solutions de gestions de patchs ne permettent pas d'être averti de la découverte d'une nouvelle vulnérabilité.

Ces solutions ne sont pas non plus exhaustives, en effet elles ne couvrent qu'un certains nombre d'applications.

2.2.6 Références

<http://www.shavlik.com/products/protect/>

<http://www.landesk.com/blog/landesk-acquires-shavlik-from-vmware/>

<http://windowsitpro.com/systems-management/hfnetchk-microsofts-new-hotfix-tool>

2.3 CERT/CSIRT

2.3.1 Présentation

Les CSIRT (Computer Security Incident Response Team) ou CERT (Computer Emergency Response Team) sont des équipes dédiées à la gestion de la sécurité informatique et résoudre les incidents qui y sont liés.

2.3.2 Historique

Le premier CERT (nommé CERT/CC) a été créé en 1988 dans l'université américaine de Carnegie Mellon suite au premier vers informatique (Moris Worm). [1] Au début composé d'une petite équipe, ce CERT compte actuellement 150 professionnels de la sécurité informatique. [2]

CERT étant une marque déposée par CMU (Carnegie Mellon University) [3], le terme CSIRT est aussi utilisé.

Les CSIRT souhaitant utiliser le terme CERT peuvent en faire la demande auprès de CMU. Aujourd'hui, il existe en France 17 CSIRT validés par le CMU. [4]

2.3.3 Description

Les CSIRT ont plusieurs rôles :

- Centralisation d'information suite à un attaque informatique

- [•] Réception des informations

- [•] Analyse et corrélation des incidents

- Traitement des alertes et réaction aux attaques

- [•] Analyse technique

- [•] Partage d'informations avec les autres CSIRT

- [•] Intervention d'urgence

- Prévention/Formation

- [•] Diffusion d'informations dans le but de minimiser le risque d'incident et leurs éventuelles conséquences.

2.3.4 Points positifs

Gestion de bout en bout de la sécurité informatique du client.

2.3.5 Points Négatifs

Dans certains cas, équipe dédiée entièrement à un seul client.

Non adapté à une utilisation hors entreprise.

Nécessite d'avoir une personne physique dédié pour gérer la sécurité.

2.3.6 Références

[1][2] <http://www.cert.org/about>

[3][4] <http://www.cert.org/incident-management/csirt-development/cert-authorized.cfm>

2.4 Cisco Security Manager

2.4.1 Présentation

Cisco Security Manager permet aux organisations de gérer leurs infrastructures Cisco de manière centralisée et surveiller les menaces de sécurité potentielles.

2.4.2 Historique

2.4.3 Description

2.4.4 Points positifs

Réutilisation des objets et des règles de sécurité pour surveiller les menaces qui pèsent sur la sécurité et minimiser les erreurs potentielles.

Outils intégrés de bout en bout pour faciliter l'application cohérente de la politique et le dépannage rapide.

Gestion consolidée des événements pour permettre la consultation des événements historiques et en temps réel.

2.4.5 Points Négatifs

Nécessite un utilisateur formé aux bases de la sécurité et du réseau. La solution ne se destine qu'à certaines gammes de produits Cisco.

2.4.6 Références

http://www.cisco.com/web/FR/products/security/security_manager.html

2.5 CERT-XMCO

2.5.1 Présentation

XMCO est un cabinet de conseil indépendant spécialisé dans la sécurité des Systèmes d'information et en cyber-criminalité.

Ils commercialisent le produit CERT-XMCO qui est un outil de veille en vulnérabilité.

XMCO sont un CSIRT accrédité pour utiliser le terme CERT.

2.5.2 Historique

Fondé en 2002, ce cabinet indépendant emploie en 2013 22 consultants en sécurité informatique.

2.5.3 Description

Cette solution propose une interface Web permettant de suivre les bulletins publiés par XMCO eux même.

L'utilisateur peut choisir la période sur laquelle la liste des derniers bulletins s'affichent. Une recherche par mot clé est possible. Sur chaque bulletin est disponible une description.

Il est possible de cliquer sur un bulletin pour choisir si on veut en suivre l'évolution et en être averti (mail/sms)

Il est possible de filtrer les bulletin sur lesquelles ont veut recevoir une alerte.

2.5.4 Points positifs

Possibilité d'avoir un suivi exhaustif des bulletins de XMCO

2.5.5 Points Négatifs

Filtrage non évolué.

Trop d'informations pour un utilisateur qui lui s'intéresse qu'à ses produits.

Service non ouvert au public.

2.5.6 Références

<http://www.xmco.fr/veille-vulnerabilite-securite-cert-xmco-fr.html>

Chapitre 3

Positionnement de votre projet

3.1 Ce que vous apportez

Vigilate a pour principale qualité d'être facilement personnalisable, avec un système de configuration simple et précis. En effet, Vigilate va recenser un bon nombre de vulnérabilités très rapidement et toute n'intéressent pas forcément tout le monde. Notre but est donc d'informer vite et bien chaque personne sur leurs programmes ou leurs outils.

Un scanner va être mis en place, il ne sortira pas directement les vulnérabilités mais va permettre de notre côté de connaître la version des programmes que vous utilisez

Notre outil sera accessible via un site web ergonomique pour une utilisation simple et performante.

3.2 Ce qui ne sera pas couvert

Vigilate sert à prévenir des nouvelles vulnérabilités publiques, notre service ne propose pas de prestation chez le client pour les fixer. Cependant, des solutions de correctif urgent seront mises en avant dès que possible.

Il n'y aura pas de scan du réseau, de scan web, de scan du système, pour détecter des vulnérabilités qui ne sont pas publiquement connues.

Chapitre 4

Conclusion

4.1 Matrice de préférence

Dans cette matrice de préférence, nous comparons plusieurs points importants. La réactivité à une nouvelle menace, la simplicité d'utilisation de l'outil, qui est ciblé par cet outil et enfin la pertinence de l'information qui est remontée.

Projet	Réactivité	Simplicité	Cible	Pertinence de l'information
Nessus	Plutôt longue. Réactivité éditeur + temps de scan	Les scans classiques sont simplistes à utiliser mais la personnalisation de ceux-ci est plus compliqué	Entreprises.	Bonne. Seules les vulnérabilités trouvées sont remontées.
Shalvik Protect	Réactivité égale à celle des éditeurs de programmes.	Très simple il scan et installe les patches tout seul.	Entreprises.	Bonne. Elle concerne seulement les programmes installés sur la machine.
CERT/CSIRT	Très bonne. L'équipe est prête à répondre en cas d'urgence.	Très simple pour l'entreprise, ce n'est pas elle qui s'en occupe.	Entreprises, organisations.	Bonne. Elle est adaptée à la cible.
Cisco Security Manager	Bonne, dès qu'un événement interne est détecté.	Difficile. Nécessite une connaissance des technologies réseaux.	Entreprises, organisations	Bonne, elle concerne des événements internes.
CERT-XMCO	Bonne. Alerte dès qu'un bulletin est publié.	Assez simple.	Entreprises, organisations.	Mauvaise. Tous les bulletins sont affichés, et le filtrage ne se fait pas forcément très bien.
Vigilate	Très bonne. Dès qu'une vulnérabilité est rendu publique.	Très simple. Ergonomique.	Entreprises, organisations, revendeurs, webmasters, particuliers	Très bonne. Seule l'information qui concerne l'utilisateur est remonté.

4.2 SWOT

	Positive	Négative
Interne	Forces	Faiblesses
Externe	Opportunités	Menaces