

MAS/INF/258
رقم الترخيص

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE



UNIVERSITE MOHAMED BOUDIAF - M'SILA
FACULTE DES MATHÉMATIQUES ET
DE L'INFORMATIQUE



DEPARTEMENT D'INFORMATIQUE

MEMOIRE de fin d'étude
Présenté pour l'obtention du diplôme de MASTER
Domaine : Mathématiques et Informatique
Filière : Informatique
Spécialité : Technologie de l'Information et de Communication

Par: DAHIA Youcef

SUJET

Sécurisation des applications web

Soutenu publiquement le : / /2016 devant le jury composé de:

.....	Université de M'sila	Président
Mr. BENAZI Makhlouf	Université de M'sila	Rapporteur
.....	Université de M'sila	Examineur
.....	Université de M'sila	Examineur

Promotion : 2015 /2016

Table des matières

	Titre	Page
	Remerciement	
	Table des matières	
	Liste des tableaux	
	Liste des figures	
	Liste des abréviations	
	Introduction générale	1
	Chapitre 1: Outils de la sécurité informatique	
	1 Introduction	3
	2 Terminologie de la sécurité informatique	3
	3 L'objectif de la sécurité informatique	4
	4 Les normes de la sécurité informatique	4
	4.1 L'Organisation Internationale de normalisation	4
	4.2 La gestion de la sécurité des systèmes d'information	6
	5 Les mécanismes de sécurité	6
	5.1 Cryptage	7
	5.1.1 Algorithmes de cryptographie symétrique (à clés secrète)	7
	5.1.2 Algorithmes de cryptographie asymétrique (à clé publique et privée)	7
	5.2 Le tunneling et les Virtual Private Network (VPN)	8
	5.3 Pare-feu	9
	5.4 Antivirus	10
	5.5 Solution de détection/prévention d'intrusion IDS/IPS	10
	5.6 Reverse proxy	11
	6 Conclusion	12
	Chapitre 2 : La sécurité des applications	
	1 Introduction	13
	2 Principes et concepts des applications web	13
	3 Typologie des attaques web	14
	4 Bonnes pratiques et contre mesure de sécurisation des applications web	16
	4.1 PLAN	16

4.1.1 Architecture applicative	16
4.1.2 Définition des règles de sécurité	17
4.1.3 Appréciation des risques	18
4.2 Définition et application des règles pare-feu	18
4.2.1 Définition de la défense en profondeur	18
4.2.2 Le cloisonnement	19
4.2.3 La haute disponibilité	20
4.2.4 Défense multi-niveau des services	21
4.2.5 Choix des outils et formation du personnel	22
4.3 Check	22
4.4 ACT	23
5. Conclusion	23

Chapitre 3 : Analyse conceptuelle

1 Introduction	24
2 Définition des objectifs	24
3 Modélisation de l'architecture projetée	24
3.1 Diagramme de cas d'utilisation	25
3.1.1 Identification des acteurs du système	25
3.1.2 Identification des cas d'utilisation	25
3.2 Diagramme d'activité	28
4 Architecture	31
5 Choix des outils et technologies à implémenter	33
5.1 Le système d'exploitation	34
5.2 Pare-feu Endian Firewall	34
5.2.1 Netfilter	34
5.2.2 IDS/IPS SNORT	35
5.3 Reverse Proxy SQUID	36
6 Conclusion	37

CHAPITRE 4 : Implémentation et réalisation

1 Introduction	38
2 Préparation de la plate-forme de test	38
2.1 Les composants de la plate-forme de test	38
2.2 Plan d'adressage de la plate-forme	39

3 Installation et configuration du pare-feu Endian Firewall	39
3.1 Installation	39
3.2 Configuration	40
3.3 Définition et application des règles pare-feu	40
3.3.1 Trafic inter-Zone	40
3.3.2 Trafic entrant	41
3.3.3 Trafic sortant	42
3.4 Configuration de la sonde de prévention d'intrusion	42
4 Installation et configuration du reverse proxy SQUID	43
4.1 Installation	43
4.2 Configuration	44
5 Audit et surveillance	45
5.1 Mise en place de la station d'audit	45
5.2 Les interfaces de surveillance du trafic	46
6 Conclusion	47
Conclusion générale	48

Bibliographie et webographie

Annexes

Résumé

Figure 3.6 : Diagramme d'activité de sauvegarde	31
Figure 3.7 : Architecture projetée pour la plate-forme du site web	32
Figure 4.1 : Plan d'adressage de la plate-forme	39
Figure 4.2 : La configuration du trafic inter-Zone	41
Figure 4.3 : La configuration de trafic entrant	41
Figure 4.4 : La configuration de la source NAT	42
Figure 4.5 : La configuration du trafic sortant	42
Figure 4.6 : La configuration la sonde de prévention d'intrusion	43
Figure 4.7 : L'interface journalisation du trafic	46
Figure 4.8 : Surveillance de la plate-forme avec l'outil Ntop	47

Introduction générale

L'émergence du web et la dynamique que connaît l'industrie informatique ont impacté notre vie, et nous ont rendu dépendant l'utilisation de ces technologies pour effectuer toute sorte de transaction.

A présent tout peut se faire en ligne : achat électronique, réseaux sociaux, transaction bancaire... etc.

Cette évolution constante et révolutionnaire de l'utilisation des nouvelles technologies de l'information et de la communication a affecté tous les domaines, et a résulté des menaces pouvant nuire à la vie privé et aux données personnelles ainsi qu'aux données confidentielles des personnes ou entreprises.

Pour ces raisons, l'aspect sécurité a été mis en avant. Il représente à présent un actif crucial pour l'entreprise, qui doit assurer un cadre sécurisé aussi bien pour elle que pour ses utilisateurs.

Les experts de la sécurité informatique affirment que le risque zéro ne peut être atteint, Néanmoins les bonnes pratiques sont de vigueur, et peuvent le réduire considérablement.

Le contexte hostile du monde de l'internet, l'apparition constante des menaces, ainsi que la complexité des applications web qui va de pair avec l'émergence des nouvelles technologies, nous mettons face à des problématiques récurrentes qui sont:

Comment sécuriser une application web?

Comment maintenir la sécurité d'une application web?

Quelles sont les démarches à entreprendre pour la sécurisation d'une application web?

C'est dans ce contexte que s'inscrit ce travail dont l'objectif est double. Premièrement d'effectuer une étude approfondie sur la sécurité informatique en général et la sécurité sur la toile en particulier ainsi que les menaces auxquelles les entreprises doivent faire face.

Deuxièmement, il s'agit de mettre en pratique les connaissances acquises, afin de sécuriser l'application web, ce besoin fera l'objet de notre mémoire.

A cet effet, nous allons aborder dans cette étude l'aspect sécurité des applications web et les bonnes pratiques à prendre en considération dans une architecture sécurisée et à haute disponibilité.

Dans la partie pratique nous allons définir une architecture type en se basant sur les bonnes pratiques de la sécurisation des applications web et mettre en place les outils indispensables qui feront l'objet d'une barrière frontale afin d'assurer la sécurité à quatre niveaux:

- La limitation des accès à travers la mise en place et la configuration d'un pare feu Open source Endian firewall.
- La sécurisation de l'accès au site web à travers l'implémentation et la configuration d'un proxy reverse Open source SQUID.
- Le contrôle des paquets entrants et sortants à travers une solution de détection d'intrusion Open source Snort.

Notre mémoire est organisé comme suit:

Le chapitre 1 propose une étude sur les fondements de la sécurité informatique dans sa globalité et les outils de sécurité les plus répandus et leurs fonctionnements.

Le chapitre 2 nous présentons un aperçu sur le mécanisme et les concepts de base des applications web, nous exposons brièvement les vulnérabilités et menaces les plus répandues, et nous abordons les bonnes pratiques à prendre en considération pour la sécurisation des applications web.

Le chapitre 3 présente l'analyse conceptuelle dans laquelle nous exposons une étude de l'existant et les objectifs estompés, et nous utilisons une annotation pour la modélisation de l'architecture que nous allons implémenter et enfin nous énumérons les outils choisis tout en argumentant notre choix.

Le Chapitre 4 est un aperçu de toutes les étapes effectuées dans l'implémentation de l'architecture et la mise en production des outils sur les quels notre choix a porté.

Conclusion générale

L'étude menée tout au long de notre mémoire avait pour objectif de répondre aux problématiques suivantes:

Comment sécuriser une application web?

Comment maintenir la sécurité d'une application web?

Quelles sont les démarches à entreprendre pour la sécurisation d'une application web?

Pour apporter les éléments de réponse nécessaires à ces problématiques, nous avons décortiqué l'aspect de la sécurité informatique dans sa globalité et la sécurité des application web en particulier en prenant en compte l'évolution permanente des technologies de l'information qui va de pair avec la multiplication des menaces auxquelles nous devons faire face.

L'étude théorique a été suivie par une analyse conceptuelle qui nous a permis d'identifier les besoins et de modéliser l'architecture projetée.

Compte tenu de l'importance de l'aspect sécuritaire des applications web, nous avons utilisé les outils fondamentaux de sécurité et appliqué les bonnes pratiques dans une architecture proposée.

Les principales contributions se résument comme suit:

- L'application du processus de sécurité des système informatique en se basant sur le modèle PDCA afin de faire ressortir les étapes à suivre;
- Concevoir une architecture sécurisée qui concorde avec précision avec le niveau de sécurité attendu;
- Concocter les outils adéquats et fiables et les utiliser et configurer comme étant une barrière de sécurité frontale;
- Mettre en relief l'aspect prévention à travers la mise en œuvre des outils nécessaires à la prévention d'intrusion;

Toutefois, nous pouvons envisager différentes perspectives afin de maintenir le niveau de sécurité, à titre d'exemple nous citons:

- Mise en place d'outil pour tester la vulnérabilité du site web.
- La mise en place d'un tunnel VPN.

Pour finir, nous devons signaler que notre mémoire, comme tout travail de recherche, n'est pas libre de quelques lacunes et limites. Celles-ci sont principalement dues aux raisons suivantes:

- Courte durée.

- Ressources matérielles et logicielles limitées pour l'implémentation de l'environnement de test;

[1] et [2] Professeur REMAUKERS Jean. «Cours de sécurité informatiques Université de Namur, Belgique 2012.

[3] Site officiel du moteur de recherche Wikipedia. «Organisation Internationale de Normalisation» http://fr.wikipedia.org/wiki/Organisation_internationale_de_normalisation.

[4] Site officiel de l'Organisation Internationale de Normalisation. <http://www.iso.org>

[5] Site du dictionnaire informatique. <http://dictionnaire.pronetx.com/>

[6] par Alban Jacquemin et Adrien Mercier. «Les firewalls» [pdf].

[7] Robert S. Mueller, RSA Cyber Security Conference (1/03/2012): <http://www.fbi.gov/news/speeches/countering-threats-in-the-cyber-world-outsmarting-cyber-criminals-and-spies>

[8] Site officiel du Web Application Security Consortium, WASC. <http://www.wascapsec.org/>

[9] WASC «Web Application Security Consortium Threat Classification» <http://projects.wascapsec.org/WASC-TC-v2-0.pdf>

[10] Site officiel du OWASP «Top 10 List» https://www.owasp.org/index.php/Top_10_2013-Top_10

[11] Site officiel du moteur de Recherche Wikipedia. «Défense en profondeur» https://fr.wikibooks.org/wiki/DPS/DEFENSE_en_profondeur

[12] Forum des développeurs et IT pro. «UML2 - de l'apprentissage à la pratique» <http://laurent-aubert-developers.com/CoursUML/>

[13] Site officiel d'Endian Firewall <http://www.endian.com/>

[14] Guide de configuration – Netfilter-iptables – REFERENCE OPPIDA/DOC/2009/AUA/534/1.4.

[15] Site officiel de SourceFire «SNORT» <http://www.sourcefire.com/fr/les-actes-les-actes-open-source/>

Bibliographie et webographie

- [1] et [2] Professeur REMAEKERS Jean. «Cours de sécurité informatique» .Université de Namur. Belgique.2012.
- [3] Site officiel du moteur de recherche Wikipedia.« Organisation Internationale de Normalisation ».http://fr.wikipedia.org/wiki/Organisation_internationale_de_normalisation.
- [4] Site officiel de l'Organisation Internationale de Normalisation. <http://www.iso.org>
- [5] Site du dictionnaire informatique. <http://dictionnaire.phpmyvisites.net>
- [6] par Alban Jacquemin et Adrien Mercier . Les firewalls[pdf].
- [7] Robert S. Mueller, RSA Cyber Security Conférence (1/03/2012) :
<http://www.fbi.gov/news/speeches/combating-threats-in-the-cyber-world-outsmartingterrorists-hackers-and-spies>
- [8] Site officiel du Web Application Security Consortium WASC.
<http://www.webappsec.org/>
- [9] WASC. «Web Application Security Consortium: Threat Classification».http://projects.webappsec.org/f/WASC-TC-v2_0.pdf
- [10] Site officiel du OWASP , Top 10 List :
https://www.owasp.org/index.php/Top_10_2013-Top_10
- [11] Site officiel du moteur de Recherche Wikipedia. «Défense en profondeur ».
https://fr.wikipedia.org/wiki/D%C3%A9fense_en_profondeur .
- [12] Forum des développeurs et IT pro. « UML2 - de l'apprentissage à la pratique »<http://laurent-aubibert.developpez.com/Cours-UML/>
- [13] Site officiel d'Endian Firewall <http://www.endian.com>
- [14] Guide de configuration Netfilter-iptables REFERENCE:
OPPIDA/DOC/2009/AUA/534/1.4.
- [15] Site officiel de SourceFire. « SNORT »
<http://www.sourcefire.com/fr/technologies-open-source>

[16] Site officiel du blog informatique et des nouvelles technologies EASEO <http://blog.easeo.fr/aides-howto/00site-internet/reverse-proxy-httpttps-avec-squid-3-sous-debian>

1 TOP 10 des menaces les plus répandues OWASP

L'OWASP établit périodiquement une liste exhaustive appelée "TOP 10" classant ainsi les menaces les plus répandues des applications web par ordre d'importance, la version la plus récente (2013), éditée par l'OWASP, est comme suit :

1) Injection

Une faille d'injection, telle l'injection SQL, OS et LDAP, se produit quand une donnée non fiable est envoyée à un interpréteur en tant qu'élément d'une commande ou d'une requête. Les données hostiles de l'attaquant peuvent duper l'interpréteur afin de l'amener à exécuter des commandes interdites, ou accéder à des données non autorisées.

Nous allons présenter dans ce qui suit quelques scénarios d'attaque :

Scénario 1 :

Une application utilise des données non fiables dans la construction de l'appel SQL vulnérable suivant :

```
String query = "SELECT * FROM accounts WHERE  
accountId = request.getParameter('id')";
```

Scénario 2 :

Pareillement, la confiance aveugle d'une application aux frameworks peut déboucher sur des requêtes toujours vulnérables (p.ex. HibernateQueryLanguage (HQL)) :

```
Query HQLQuery = session.createQuery("FROM accounts  
WHERE accountId = request.getParameter('id')");
```

L'attaquant modifie le paramètre 'id' dans son navigateur et envoie :
id=1*1.

Par exemple :

```
http://example.com/app/accountView?id=1*1
```

Le sens des deux requêtes est modifié pour retourner toutes les lignes de la table accounts. Les pires attaques peuvent altérer des données, voire invoquer des procédures stockées.

2) Violation de gestion d'authentification et de session

Les fonctions applicatives relatives à l'authentification et la gestion de session ne sont souvent pas mises en œuvre correctement, permettant aux attaquants de compromettre les

ملخص :

إن عدد الهجمات ضد الشركات تنمو بشكل متزايد، مما يسبب خسائر كبيرة، وبالتالي فإن الحاجة لأمن المعلومات للشركات يصبح ذات أهمية بالغة .

لقد طورت عدة سياسات وأدوات لتزويد آليات الدفاع الفعال من بينها جدار الحماية، نظام كشف/منع التسلل، الوسيط، الهدف منها هو تحديد وتبادل كل ما يمر عبر الشبكة من الداخل والخارج والسماح بالمرور للمخولين فقط .

في مشروعنا هذا قمنا باقتراح مخطط حماية بسيط وفعال والذي يتكون من ثلاث وحدات: جدار الحماية، نظام كشف/منع التسلل، الوسيط، هاته الوحدات تعمل معا لضمان السياسة الأمنية .

الكلمات المفتاحية : جدار الحماية ، تصفية ، تطبيق الويب ، السياسة الأمنية .

Abstract:

The number of attacks against companies are growing which can cause significant losses, thus the need of IT security becomes so important.

Several policies and tools have been developed to provide effective defense mechanisms which include firewalls, Intrusion detection/prévention system (IDS/IPS), reverse proxy, their goal is to filter all traffic exchanged with the outside network and allow only authorized traffic.

In our project we proposed a simple and effective architecture for securing web applications which consists of three modules : Endian Firewall, IDS /IPS, reverse proxy. Those modules work together to ensure our security policy.

Key-Words: Firewall, filter, web application, security policy.

Résume :

Le nombre d'attaques contre les entreprises ne cessent d'augmenter ce qui peut entrainer des pertes conséquentes, ainsi, le besoin des entreprises en sécurité informatique devient de plus en plus important.

Plusieurs politiques et des outils ont été développés pour fournir des mécanismes de défense efficaces parmi lesquels on trouve les pare-feux, Système de détection/prévention d'intrusion (IDS/IPS), reverse proxy, leur but étant de filtrer tout le trafic échangé avec le réseau extérieur et de ne laisser passer que le trafic autorisé.

Dans notre projet on a proposé une architecture simple et efficace pour la sécurisation des applications web qui se compose de trois modules : Endian Firewall, IDS /IPS, reverse proxy, ses ensemble outils peut assurer la politique de sécurité.

Mots clés : Pare feu, filtrer, application web, politique de sécurité.