



Mémoire pour l'obtention du diplôme
de Post-Graduation Spécialisée en Sécurité Informatique

Thème

Elaboration d'une politique de sécurité pour les
applications web contre les attaques de reconnaissance

Elaboré par:

- **TOUALBIA Riadh**
- **KHITER Said**

Encadré par :

- **Mr. DERHAB Abdelouahid**

Soutenu devant le juré :

- **Mr DJENOURI. Djamel, Président, Maître de Recherche A, CERIST.**
- **Mme ALIANE. H, Examinatrice, Maître de Recherche B, CERIST.**
- **Mlle BOUCHAMA. S, Examinatrice, Attachée de Recherche, CERIST.**

-Février 2012-

Remerciements

Ce mémoire est le fruit d'un travail acharné au sein du CERIST et comme un tel travail nécessite la contribution de plusieurs personnes, nous profitons de cette occasion pour les remercier à travers ces quelques phrases.

Nous tenons tout d'abord à remercier notre promoteur Monsieur DERHAB Abdelouahid pour la confiance qu'il nous a témoignée en nous proposant ce sujet, sa disponibilité tout au long du projet, ses encouragements et sa patience. Les discussions scientifiques qu'il a su générer, ses remarques et ses suggestions nous ont permis de finaliser ce document.

Nous exprimons toute notre profonde gratitude et nous les remercions pour le personnel du service formation du CERIST.

Nous remercions les membres du jury pour avoir bien voulu juger notre travail.

Sommaire

Introduction générale.....	1
----------------------------	---

Chapitre I

Les attaques de reconnaissance contre les applications web

I. Définitions générales.....	2
I.1. Définition d'une application web.....	2
I.2. Accès à l'application web.....	2
I.3. Réalisation des applications web.....	2
I.4. Les enjeux principaux des développeurs et hébergeurs.....	2
I.5. Risques liés aux applications web.....	3
I.6. Vulnérabilités des applications web.....	3
I.7. Attaques de reconnaissance des applications web.....	4
II. Reconnaissance Passive.....	4
II.1. Site web de la compagnie.....	5
II.2. Google.....	5
II.3. Forums & Newsgroups.....	5
II.4. Dumpster diving.....	5
II.5. Ingénierie sociale.....	5
III. Reconnaissance active.....	6
III.1. Reconnaissance à partir du web.....	6
III.1.1. Recherche dans les serveurs WHOIS.....	6
III.1.2. Samspace.....	7
III.1.3. Interrogation du site NETCRAFT.....	8
III.2. Reconnaissance à partir de l'interrogation des serveurs DNS.....	9
III.2.1. NS Lookup.....	9
III.2.2. Dig.....	9
III.2.3. HOST.....	9
III.3. Reconnaissance du réseau.....	11
III.3.1. Les traceurs.....	11
III.3.1.1. Traceroute.....	11
III.4. Reconnaissance du serveur.....	12
III.4.1. Pings and ping sweeps.....	12
III.4.2. Port scanning.....	13
III.4.2.1. Le scanner NMAP.....	13
III.4.2.1.1. Avantages de NMAP.....	13
III.4.2.1.2. Quelques commandes de NMAP.....	13
III.4.3. Scanneurs de vulnérabilités des applications web.....	14
III.4.3.1. Nessus.....	14
III.4.3.2. Nikto.....	15
III.5. Reconnaissance de l'application web.....	16
III.5.1. HTTrack Website Copier.....	16
III.5.2. Les navigateurs web.....	17
III.5.2.1. Internet Explorer.....	17

III.5.2.2.Firefox.....	18
III.5.3.Suites intégrés de test (Integrated Testing Suites).....	18
III.5.3.1.Exemples de ces outils	19
III.5.3.1.1.Paros	19
III.5.3.1.2:Burp Suite	20
III.5.3.1.3.Websecurify	20
III.5.3.1.4.OWASP's WebScarab	21

Chapitre II

Politique de sécurité des applications web

I. Protection de l'entreprise.....	23
I.1.les informations publiques.....	23
I.2. Protéger les lignes téléphoniques et les adresses e-mails.....	23
I.3. Les annonces publicitaires.....	24
I.4. Protéger les informations internes.....	24
I.5. Se protéger contre l'ingénierie sociale	24
II. Sécurité des moyens informatiques.....	24
II.1. La défense au niveau réseau	24
II.1.1.Prévention des attaques de reconnaissance réseau	24
II.1.2.Prévention des attaques contre les serveurs DNS	24
II.2. Sécurité du Serveur Web	25
II.2.1. Gestion du contrôle d'accès (Managing Access control	25
II.2.2. Maintenir les répertoires et les structures de données	25
II.2.3. Elimination de vulnérabilités de Scripting	25
II.2.4. Activité de journalisation	26
II.2.5. Maintenir l'intégrité	26
III. Sécurité des applications web	27
III.1. Avant le développement.....	27
III.2. La sécurité dans la conception.....	27
III.2.1. Un peu de bon sens.....	27
III.2.2. Éloge de la simplicité.....	27
III.2.3. La sécurité par l'obscurité.....	27
III.3. La sécurité dans le développement.....	27
III.3.1. Contrôle et vérification des entrées	27
III.3.2. Contrôle de sorties.....	28
III.4. Gestion de sessions	28
III.5. Authentification.....	29
III.6. Utilisation de la cryptographie	29
IV. Vérification de la sécurité de l'application web	29
IV.1. Raison de la vérification.....	29
IV.2.Méthodes de vérification.....	29
IV.2.1. Audit des spécifications.....	29
IV.2.2. Audit de code	30
V. Cas pratique (Sécurité IIS 7.0)	30
VI. Test d'intrusion.....	32

Chapitre III

Déploiement d'une application web Sécurisée sous IIS 7.0

I .Présentation d'IIS7	33
I.1. Présentation générale	33
I.2. Nouvelle architecture.....	33
I.3. Nouvelle administration	33
II. Installation du rôle Serveur Web (IIS	35
II.1. Installation du Serveur IIS	35
II.2 Installation des modules Complémentaires	37
II.2.1. ASP.NET	37
III. Installer un site Web	38
III.1. Création et configuration d'un site web	38
IV. Sécurisation du serveur IIS 7.0	41
IV.1. Sécurisation du réseau	41
IV.1.1. Network Access Protection	41
IV.1.2. Pare-feu	41
IV.1.2. IDS	42
IV.2. Sécuriser le système d'exploitation.....	42
IV.2.1. Configuration de la sécurité du système	42
IV.2.2. Liste de contrôle de sécurité Post-Installation	43
IV.2.3. Installation d'outils anti-malwares.....	44
IV.2.4. Sécurité du système de fichier	44
IV.2.5. Cryptage du système de fichier.....	45
IV.3. Sécuriser IIS 7.0	46
IV.3.1. Sécurité basée TCP/IP	46
IV.3.1.1. Sécurité des adresses IP.....	46
IV.3.1.2. Sécurité des ports (Port Security	47
IV.3.2. Simple Path-Based Security.....	47
IV.3.2.1. Defining and Restricting the Physical Path.....	48
IV.3.2.2. Default Document or Directory Browsing	49
IV.3.3. Configuration des extensions de type MIME	49
IV.3.4. Configurer les restrictions sur les extensions ISAPI et les applications CGI	51
IV.3.5. Configuration de filtrage des requêtes.....	52
IV.3.5.1. Filtrage par extension de fichier.....	52
IV.3.5.2. Filtrage par les mots clé http.....	52
IV.3.5.3. Filtrage basé sur les limites de la requête	52
IV.3.5.4. Filtrage basé sur les séquences d'URL (URL Sequence.....	53
IV.3.5.5. Journalisation du filtrage des requêtes	53
IV.3.6. Sécurité des pages d'erreurs d'IIS 7.0	54
IV.4. Journalisation et traçage d'IIS 7.0.....	55
IV.4.1. Journalisation (Logging	55
IV.4.2. Traçage	57
IV.4.2.1. HTTP Status Codes.....	57
IV.4.2.2. Traçage des requêtes échouées	57

Chapitre IV

Validation de la politique de sécurité

I. Test d'intrusion	60
II. BackTrack Linux	60
II.1.Objectifs de BackTrack Linux.....	60
II.2.Installation de BackTrack 5	61
III. Méthodologie de test de BackTrack Linux.....	63
III.1. Target scoping (portée de la cible	63
III.2. Information gathering (collecte d'information.....	64
III.3.Target discovery (découverte de la cible.....	64
III.4.Enumerating target (énumération de la cible.....	64
III.5.Vulnerability mapping (cartographie des vulnérabilités	64
IV. Test de la politique de sécurité du serveur web IIS 7.0	64
IV.1.Target scoping	64
IV.2.Information gathering	64
IV.2.1.DNS information extraction	65
IV.2.2.Route information.....	65
IV.3. Target discovery	66
IV.3.1.Déterminer si la cible est active	67
IV.3.2.OS fingerprinting.....	67
IV.4.Enumerating target	68
IV.4.1.Port scanning.....	68
IV.5.Service enumeration	69
IV.6.Vulnerability Mapping.....	70
Conclusion générale.....	72