Samurai
– protégez vos applications web

Régis Senet

La sécurité des sites internet est aujourd'hui l'un des aspects de la sécurité le le plus souvent négligé. Les failles web permettent des actions de plus en plus importantes de la part des pirates informatiques. Samurai ou plus précisément Samurai Web Testing Framework ou encore Samurai WTF est donc un LiveCD spécialisé dans les tests de pénétration sur les applications web. Il a pour objectif de devenir LA plateforme de référence en qualité de pénétration des applications web devant le très complet BackTrack.

La sécurité des sites internet est aujourd'hui l'un des aspects de la sécurité en entreprise le plus souvent négligé alors qu'il devrait être une priorité dans n'importe quelle organisation. De plus en plus, les pirates informatiques concentrent leurs efforts sur les applications web afin d'obtenir une approche des informations confidentielles et abuser des données sensibles comme les détails de clients, les numéros de carte de crédit et autre.

Les applications web réalisant des achats en ligne, des authentifications d'utilisateurs ou utilisant simplement tous types de contenu dynamique permettent à l'utilisateur d'interagir avec des données contenues dans une base de données. Sur certaines applications, ces données peuvent être personnelles voire sensibles. Si ces applications web ne sont pas sécurisées, votre base de données entière court un risque réel.

Comme tous systèmes informatiques, une application web doit répondre à trois caractéristiques :

- Confidentialité
- Disponibilité
- Intégrité

La sécurisation des réseaux et l'installation d'un pare-feu ne fournissent aucune protection contre les attaques web car elles sont lancées sur le port 80 (le port par défaut pour les sites Internet) qui doit rester ouvert. Pour la stratégie de sécurité la plus complète, il est donc urgent d'auditer régulièrement vos applications web pour vérifier la présence de vulnérabilités exploitables.

Pourquoi s'attaquer à une application web ?

Les failles web permettent des actions de plus en plus importantes de la part des pirates informatique. Il est fini le temps où le piratage d'un site Web consistait à afficher une simple fenêtre sur la page de l'utilisateur ou bien le vol d'un cookie. De nos jours, le piratage d'une application Web est nettement plus dangereux que cela : défaçage complet ou partiel d'un site Internet ou accès aux données sensibles des utilisateurs. Les raisons de ces actions ? Les pirates informatiques sont principalement motivés par deux raisons :

- La gloire: Le défaçage d'un site rentre souvent dans cette catégorie de piratage. En effet, le défaçage d'un site sert parfois à marquer son territoire ou simplement à se faire connaître par le monde des pirates en modifiant le site cible.
- L'argent : Les pirates sont souvent attirés par l'appât du gain qu'il soit direct ou indirect. Un gain direct est un gain leur revenant personnellement alors qu'un gain indirect se définirait plus comme étant une perte pour l'entreprise cible. En effet, le vol d'informations confidentielles comme les numéros de carte bleue par exemple est un commerce de plus en plus porteur sur le net.

En exemple de gain indirect, en 2006, ChoicePoint a payé 10 millions de dollars dans les peines civiles et 5 millions dans le dédommagement de consommateurs après que 163 000 dossiers financiers personnels de consommateurs avaient été compromis dans sa base de données. De même, un pirate informatique a gagné l'approche à plus de cinq millions de numéros de cartes de crédit en février 2003 grâce à une attaque d'application web. Il est temps d'inclure les sites web dans la politique de sécurité des entreprises et ceci de manière draconienne. Pour ce faire, nous allons maintenant vous présenter *Samurai Web Testing Framework*.

Figure 2. BootSplash de Samurai

Qu'est ce que Samurai ?

Avec la démocratisation des LiveCD spécialisés, Samurai n'a pu déroger à la règle. Samurai ou plus précisément Samurai Web Testing Framework ou encore Samurai WTF est donc un LiveCD spécialisé dans les tests de pénétration sur les applications web.

Figure 1. Ecran de boot du Live CD

Samurai WTF est un LiveCD fondé sur un environnement GNU/Linux. Bien que moins habituelle qu'OpenBSD, FreeBSD et autre, Samurai WTF s'appuie sur une distribution Ubuntu 8.04 LTS ayant pour nom de code *The Hardy Heron*. Cette version a été publiée en version stable le 24 avril 2008 soit à peine quelques mois avant la sortie de la première version de Samurai WTF.

Samurai s'appuyant sur Ubuntu, GNOME (*GNU Network Object Model Environment*) se trouve être l'environnement graphique par défaut.

Samurai WTF est donc un LiveCD préconfiguré pour les tests de pénétration des sites web. Le LiveCD contient les meilleurs outils de cette catégorie qu'ils soient Open Source ou bien gratuits.

L'ensemble de ces outils se divise en trois catégories distinctes :

- Reconnaissance
- Découverte
- Exploitation

Nous présenterons plus en détails l'ensemble de ces catégories dans le prochain module. Nous présenterons également en détails les outils les plus importants disponibles sur ce LiveCD.

Origine du projet

Le projet Samurai Web Testing Framework a vu le jour pour sa première mise en ligne le 08 Octobre 2008 sous sa version 0.1 grâce au travail de *Kevin Johnson* et *Justin Searle*. Kevin et Justin sont deux analystes en sécurité informatique expérimentés ainsi que des administrateurs réseaux et pen-tester aguerris. Actuellement à sa version

0.4, Samurai WTF se voit s'améliorer de version en version en fixant d'éventuels bugs sur les logiciels présents ainsi qu'en ajoutant de nouveaux logiciels. Parallèlement à l'évolution du projet et sa prise d'importance, deux autres développeurs, *Franck DiMaggio* et *Brian Bentley* sont venus s'ajouter au projet afin de travailler aux côtés des deux initiateurs du projet. Samurai WTF a pour objectif de devenir LA plateforme de référence en qualité de pénétration des applications web devant le très complet BackTrack qui à déjà énormément d'importance aux yeux de tous les professionnels de la sécurité informatique. Une nouvelle version 0.5 est attendue intégrant le tout dernier KDE (KDE 4.1) fondé sur Kubuntu 8.10

Démarrage du LiveCD

Comme sur l'ensemble des distributions GNU/Linux, le boot du CD propose de nombreuses possibilités quant aux actions à entreprendre. Encore une fois, Samurai WTF ne déroge pas à la règle.

A partir du menu, il est possible :

- De démarrer Samurai Web Testing Framework en mode graphique (safe mode ou pas).
- D'installer Samurai Web Testing Framework en dur en utilisant l'outil de partitionnement connu d'Ubuntu.
- De vérifier que le CD ou le DVD n'a aucun défaut.
- De faire un test de mémoire (option disponible sur tous les LiveCD)
- De démarrer à partir du disque dur. Cette option trouve sont utilité lorsque le CD se trouve dans le lecteur au démarrage mais que l'on veut booter normalement sur notre disque dur.

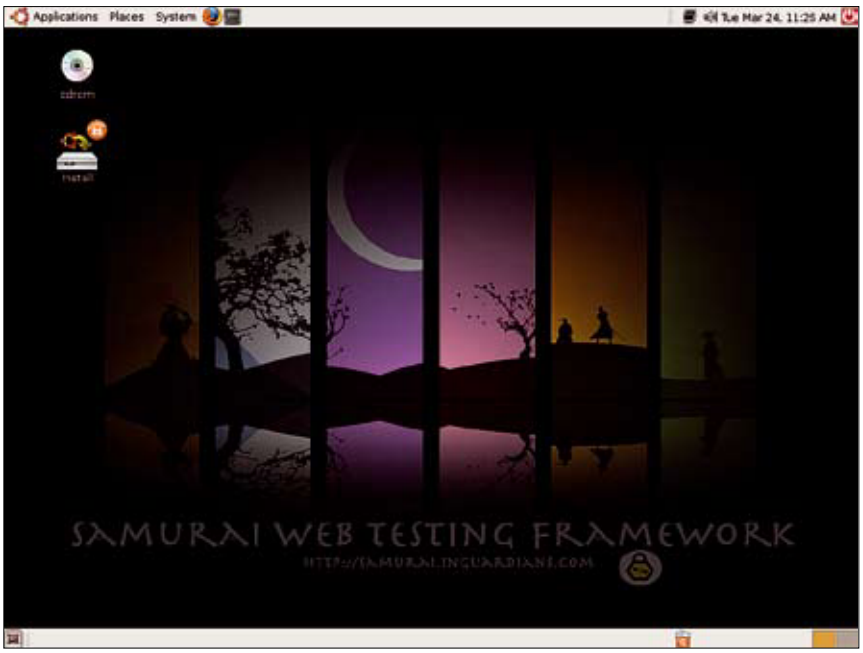

Figure 4. Bureau de Samurai sous Gnome

Un des intérêts du LiveCD est qu'il ne laisse pas de trace car toutes les informations utilisées au cours de son utilisation seront perdues lors de l'extinction de la machine. Pour cette raison, nous allons utiliser la première option *Start Samurai Web Testing Framework in Graphical Mode* qui est l'option par défaut permettant simplement de lancer Samurai WTF en mode graphique.

Le mode graphique se lance donc affichant le bootsplash de Samurai WTF durant le chargement de tous les modules (voir Figure 2).

Une fois l'ensemble des modules chargés, un écran de login apparaît.

Par défaut, le seul et unique identifiant pour la connexion se compose de login *samurai* couplé au mot de passe *samurai* (voir Figure 3). Par la suite, rajoutez éventuellement des utilisateurs grâce à la commande `useradd` ou bien grâce au gestionnaire graphique que contient Samurai WTF afin de restreindre l'utilisation du LiveCD.

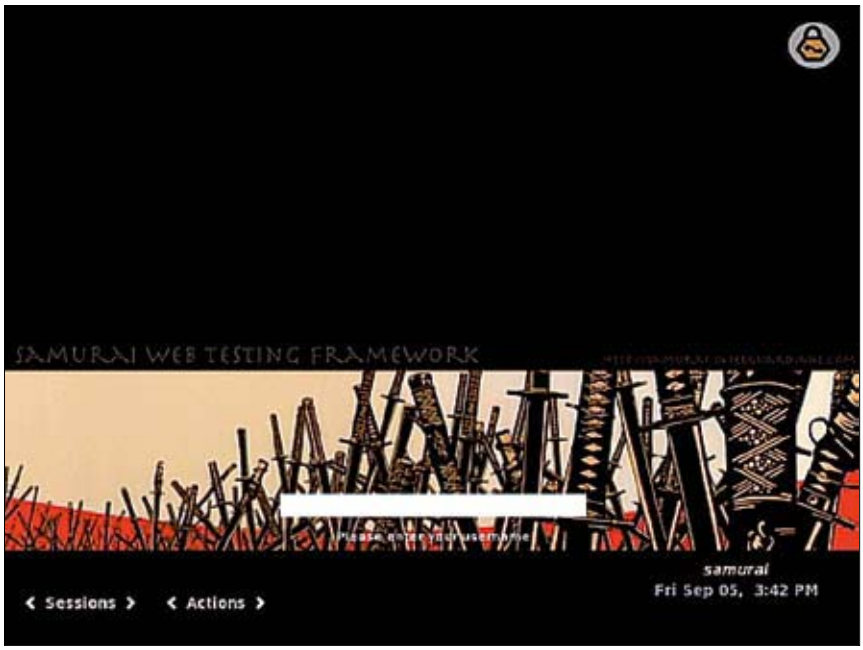

Figure 3. Ecran de login

Une fois loggé, profitez pleinement de l'ensemble des fonctionnalités dont ce LiveCD regorge.

Les menus présents dans Samurai sont très intuitifs et très clairs permettant de vous adapter rapidement même si vous n'avez jamais installé une version d'Ubuntu (voir Figure 4 et 5).

Samurai et ses outils

Le LiveCD dispose approximativement d'une trentaine d'outils destinés à mettre à mal tout type d'application web. Comme nous vous l'avions indiqué dans le module précédent, l'ensemble de ces outils peut se décomposer en trois catégories, à savoir :

- Reconnaissance
- Découverte
- Exploitation

Reconnaissance

La partie reconnaissance est une partie très importante dans la mise en place d'une attaque (que celle-ci soit portée contre une application web ou autre). Dans le cas d'une application web, il s'agit de faire de la récupération d'information sur la cible. La prise de connaissance peut inclure la récupération d'adresses mail, des informations concernant le titulaire de l'hébergement ainsi que bien d'autre possibilités. Pour ces récupérations d'informations, les outils Fierce domain Scanner ainsi que Maltego sont disponibles sur Samurai WTF.

Découverte/Exploitation

Les parties découverte et reconnaissance sont généralement regroupées en une seule phase lorsqu'il s'agit d'outil automatisé. La découverte d'une faille, que ce soit des mauvaises configurations du serveur, des failles de type cross site scripting (XSS), injection SQL, inclusion de fichier ou bien d'autres encore permet de mettre en évidence la présence d'une faille sans pour autant l'exploiter à 100%. La partie exploitation quant à elle consiste à tenter d'explorer la faille sous toutes ses coutures. Pour ces parties, des outils bien connus comme W3AF, BeEF ou bien encore AJAXShell ont été incorporés.

La présentation des outils que contient le LiveCD Samurai WTF ne se fera pas en fonction d'une appartenance à une catégorie (reconnaissance, découverte et/ou exploitation) mais dans un ordre alphabétique comme présenté dans le menu du LiveCD. Nous allons tenter de vous présenter le plus précisément possible les outils importants.

DirBuster

DirBuster est une application écrite en Java permettant de « brutefocer » les dossiers contenus dans une application web. Une attaque par dictionnaire serait plus appropriée du fait que DirBuster va tenter de faire correspondre des répertoires présents sur le serveur avec une liste de répertoires dans des fichiers texte. Le but de cette application est donc de trouver des dossiers ou bien même des fichiers sans liens pointant vers eux et pouvant s'avérer très intéressants (dossier *admin* par exemple ou la présence d'un *passwd.txt* etc.)

L'interface graphique (voir Figure 6) est très intuitive et excessivement simple d'utilisation. En effet, il est simplement nécessaire de spécifier une URL cible ainsi qu'un dictionnaire de dossiers/fichiers.

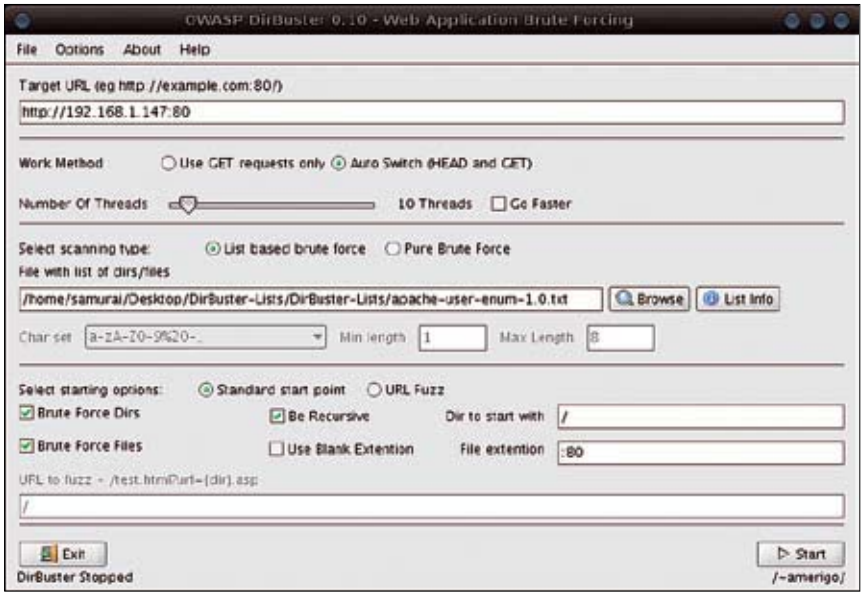

Figure 6. Interface graphique de DirBuster

Une fois ces deux éléments spécifiés, DirBuster va tenter chaque combinaison une à une jusqu'à avoir une réponse positive du serveur. (Requête 200 en général).

Le projet DirBuster est un projet de l'OWASP (*Open Web Application Security Project*) ayant pour objectif de rendre le Web de plus en plus sécuritaire.

Fierce

Fierce ou plus précisément *Fierce Domain Scanner* est petit script écrit en Perl dont le but est d'auditer la sécurité des applications web. Il est capable de tester des domaines qui ne sont pas continus. Fierce Domain Scanner analyse un domaine et tente d'identifier des sites qui sont susceptibles d'être des cibles potentielles d'une attaque web. *Fierce Domain Scanner* trouve sa place dans la catégorie des outils de reconnaissance.

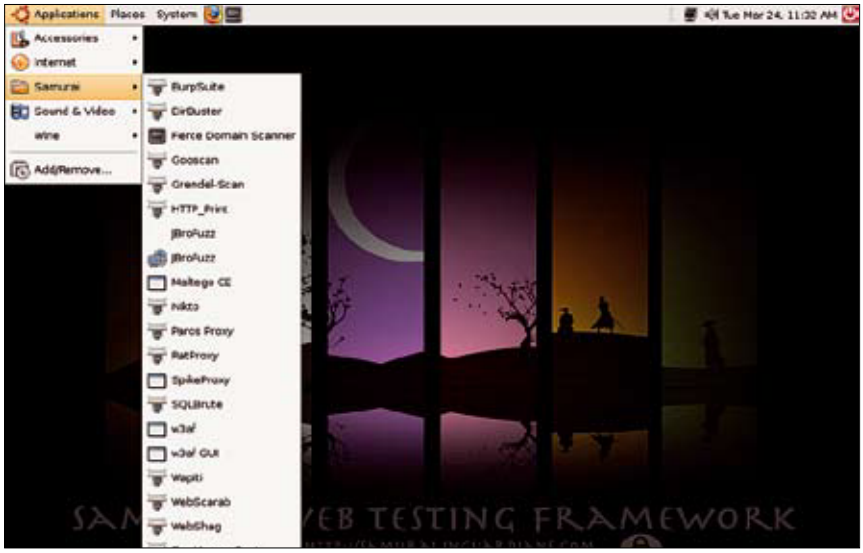

Figure 5. Les menus sous Samurai

GooScan

GooScan est un scanner de vulnérabilités pour page web, fonctionnant à partir de requêtes avec le moteur de recherche Google. C'est un utilitaire assez puissant uniquement présent en ligne de commande. Cet outil permet de ne pas faire de recherches directement sur la cible en elle-même mais en premier lieu en passant par le moteur de recherche Google afin de récupérer le maximum d'informations sans toucher au système cible. Tout comme Fierce, GooScan trouve sa place dans la catégorie des outils de reconnaissance (voir Figure 7).

Httpprint

Httpprint est un logiciel qui relève les « empreintes » d'un serveur web (voir Figure 8). Httpprint détecte avec exactitude les caractéristiques du serveur Web distant même si certains administrateurs système tentent de cacher ces caractéristiques en changeant certains paramètres ainsi que les bannières.

Httpprint utilise des signatures pour la reconnaissance des différents types de serveur web. Il est possible d'ajouter ses propres signatures à la base de données déjà présente.

Maltego

Maltego est un outil qui détermine les relations et les liens réels entre le monde (personnes, entreprises, organisations, sites web, etc ...). Maltego permet de trouver simplement et de manière graphique, des informations telles que des documents, les différentes adresses e-mail d'une personne, des numéros de téléphone qui pourraient lui être associés, des renseignements sur l'infrastructure, mais aussi collecter des informations, et bien d'autres choses encore. Trouvant sa place dans les outils de type « reconnaissance »,

Maltego est réputé pour être l'un des meilleurs outils de cette catégorie. Il permet également d'automatiser des actions de types « footprinting » en vue de tests de pénétration prévus ultérieurement. Il permet grâce au nom d'une société par exemple de remonter jusqu'à son infrastructure technique à savoir les serveurs DNS, les serveurs Web, les serveurs Mail, les hébergeurs et ainsi de suite (voir Figure 9 et 10).

La version 2.0 de Maltego présente sur Samurai WTF est également présente sur la version finale de BackTrack III

Nikto

Nikto est un scanner de serveur Web dont le but est de trouver automatiquement les risques liés à la configuration ainsi qu'aux versions utilisées. Plusieurs types de tests sont effectués sur le serveur cible grâce à Nikto. Ainsi Nikto vous indiquera les versions utilisées et les éventuels problèmes en rapport avec ces dernières. D'autres tests portent sur la configuration du serveur en elle-même comme le *Directory indexing*, l'utilisation de l'option TRACE, la vulnérabilité aux injections XSS ou injections SQL, la présence d'informations système révélées (via `phpinfo()` par exemple), etc. Nikto teste en tout et pour tout plus de 2500 points clefs à la recherche de failles exploitables par un pirate informatique à l'encontre d'une application web que ce soit l'application web elle-même ou le serveur la supportant.

Paros

Paros ou plus précisément Paros Proxy intervient sur le volet de la sécurité applicative. En émulant le navigateur web, il va permettre de tester des actions sur des services et des applications en ligne, et ainsi évaluer leur niveau de sécurité. Paros Proxy offre notamment la possibilité de capturer une requête, de la réécrire avant de la réacheminer. Toutes les données sur HTTP et HTTPS entre le serveur et le client, y compris les cookies, peuvent donc être interceptées et modifiées.

RatProxy

RatProxy a pour but d'aider les développeurs de sites internet à mieux identifier les failles potentielles de leurs créations. Cet outil est proposé par le géant Google qui après l'avoir réalisé en interne a décidé de publier le code pour qu'il soit accessible par tout le monde. L'outil est multiplateforme mais nécessite Cygwin afin de fonctionner sous Windows. Comme son nom l'indique, RatProx se configurera en premier lieu comme un proxy. Puis, il faudra ensuite visiter le site internet à tester et l'application de manière quasi automatique testera et rédigera un rapport au format HTML. RatProxy a pour but de dénicher des problèmes de sécurité les plus communs (Injection XSS, injection SQL etc.). Dans l'utilisation, RatProxy se rapproche donc énormément de Paros et de WebScarab (Voir un peu plus bas)

Figure 7. L'outil GooScan en ligne de commande

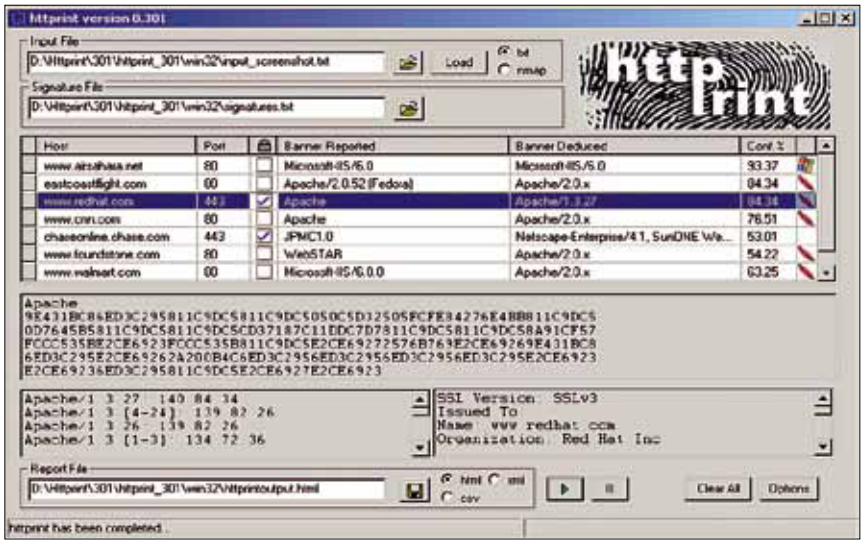

Figure 8. Relever les empreintes avec HTTPRINT

SQLBrute

SQLBrute est un petit outil intégralement écrit en Python permettant de bruteforcer les données à l'aide d'injection SQL aveugle (*Blind Injection SQL*). Il utilise une exploitation basée sur le temps de réponse ainsi que sur les erreurs de Microsoft SQL Server et Oracle. SQLBrute permet d'accélérer les traitements grâce à l'utilisation du multithreading, et ne nécessite aucune bibliothèque supplémentaire.

W3AF

W3AF ou encore *Web Application Attack* and Audit Framework est un logiciel entièrement écrit en Python. W3AF est un Framework très complet orienté test de pénétration des applications web (voir Figure 11 et 12). Comme son nom l'indique, il est orienté vers les audits et les attaques à l'encontre des applications web. Il trouve donc très bien sa place dans le LiveCD Samurai. W3AF est divisé en deux parties : le

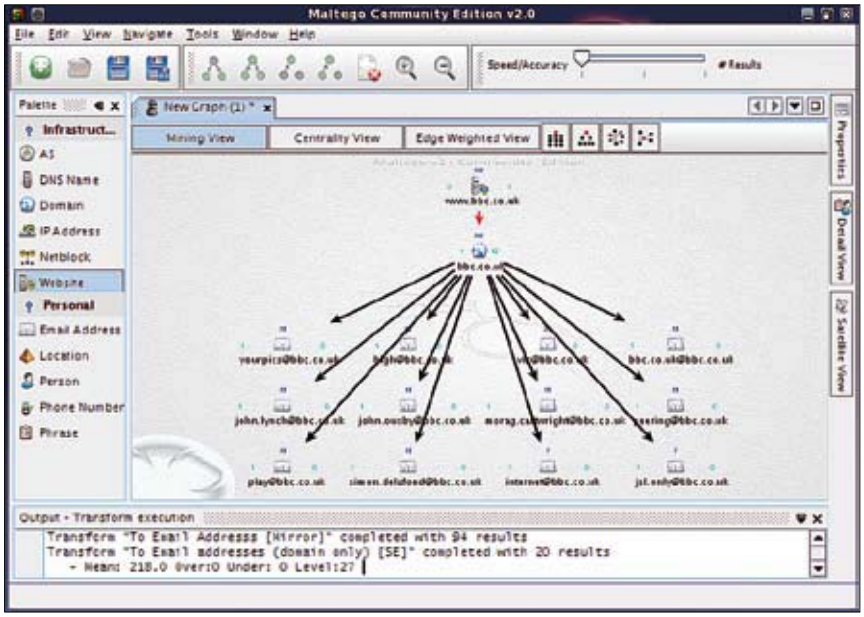

Figure 9. Utilisation de Maltego

Figure 10. Démarrage de Maltego

core qui gère les processus et la communication entre les plugins. Les plugins étant classés en 7 catégories distinctes (découverte, audit, grep, attaques, affichage, modifieurs de requêtes, évasion et *brute force*) permettant de faire de W3AF un outil très complet rentrant dans les trois catégories déjà évoquées à savoir : *reconnaissance*, *découverte* et *exploitation*.

Le Framework dispose d'une interface graphique très complète et très intuitive pour l'ensemble des actions qu'il propose. Le projet contient plus de 130 plugins qui permettent de chercher pour les injections SQL, les injections XSS, les inclusions de fichiers locaux/distants et bien plus encore.

Pour ceux qui le souhaitent, W3AF dispose aussi d'une interface en ligne de commande plus difficile à exploiter mais tout aussi puissante.

Wapiti

Wapiti est un petit logiciel écrit entièrement en Python permettant d'auditer la sécurité d'une application Web. Le logiciel teste automatiquement de nombreuses attaques qu'un pirate tenterait de lancer une à une telles que l'inclusion de fichiers locaux, l'inclusion de fichiers distants, les injections SQL et les injections XSS. Wapiti est souvent utilisé en parallèle à Nikto qui remplit les mêmes fonctions que ce dernier. Tout comme Nikto, Wapiti trouve sa place dans les outils de découverte et d'exploitation.

WebScarab

Tout comme DirBuster, WebScarab est un outil issu de l'OWASP. WebScarab est un proxy applicatif libre écrit en Java permettant d'intercepter et de modifier les requêtes ainsi que les réponses HTTP (dans le même esprit que Paros). Il est important de comprendre que grâce à ce genre d'outils, les contrôles mis en place côté client par du JavaScript par exemple peuvent facilement être contournés comme la gestion des longueurs maximales d'un champ grâce à l'attribut « maxlength ». Les erreurs suite aux mauvais paramètres insérés dans des formulaires constituent l'une des premières vulnérabilités web décrétée par le guide de l'OWASP.

WebShag

Webshag est un outil multiplateforme écrit en Python, destiné à l'audit de serveurs web. Il regroupe une série de fonctionnalités utiles lors de tests d'intrusion de serveurs web, tels qu'un scanner d'URL ainsi qu'un fuzzer de fichiers. En outre, il intègre des fonctionnalités d'évasion IDS spécialement conçues pour compliquer la corrélation entre les nombreuses requêtes qu'il génère (pour ce faire, il est capable d'utiliser un serveur proxy différent pour chaque requête générée, voir Figure 13).

En plus des fonctionnalités décrites ci-dessus, Webshag propose de nouveaux outils, à l'image de son module permettant de récupérer la liste des noms de domaine hébergés par une adresse IP donnée.

Webshag propose une interface graphique très simple et très intuitive. Il existe également une version en ligne de commande pour la version GNU/Linux pour les plus téméraires d'entre vous.

ZeNmap

ZeNmap est simplement l'interface graphique du célèbre outil Nmap (voir Figure 14). Nmap est réputé pour être un excellent outil utilisable uniquement en ligne de commande pouvant décourager les moins téméraires d'entre nous. Les balayages proposés par ZeNmap vont du simple scan aux scans très spécifiques en passant par la détection de systèmes d'exploitation distants. L'ensemble de ces choix s'effectue grâce à une listbox rendant les configurations vraiment très simples. Voici à quoi ressemble cette interface graphique.

Les sorties de ZeNmap sont très claires et compréhensibles comparativement aux lignes de commande de la version *classique* Il est possible d'utiliser les profils prédéfinis par ZeNmap (*Intense Scan*, *Quick Scan*, *Operating System Detection* etc.) ou de taper directement les commandes dans la partie prévue à cet effet pour les plus confirmés cherchant un résultat précis.

Malgré des menus complets, certains outils ne sont pas disponibles à partir des menus que proposent Samurai WTF et sont donc uniquement accessibles via la ligne de commande (voir Figure 15).

Parmi ces outils, on retrouve :

- Dnswalk : Dnswalk est un débuggeur de DNS. Il exécute des transferts de zone sur les domaines indiqués et vérifie de plusieurs manières l'intégrité et l'exactitude de la base de données
- Httping : Httping correspond au ping pour les requêtes HTTP. Si la requête ne répond pas il se peut que la page n'existe pas ou bien qu'il y ait un souci relatif au serveur (présence d'un firewall)

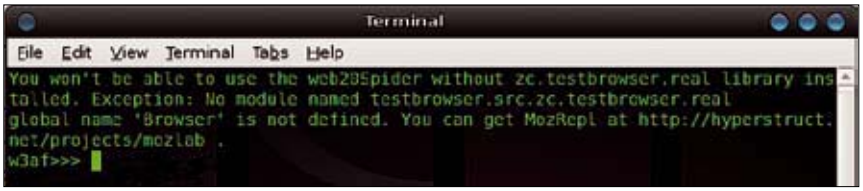

Figure 12. W3AF an ligne de commande

Figure 11. W3AF via son interface graphique

Figure 13. Ecran de lancement de WebShag

- Httrack : Httrack est simplement un *aspirateur de site*, c'est-à-dire qu'il vous donne la possibilité de télécharger l'intégralité d'une application web sur votre disque dur personnel en construisant récursivement tous les répertoires, récupérant HTML, images et fichiers du serveur vers votre ordinateur. Httrack réorganise la structure des liens en relatif.
- JTR : JTR ou est un puissant crackeur de mot de passe en ligne de commande fonctionnant tant sous Windows que sous GNU/Linux. John The Ripper procède à des attaques par bruteforce, c'est-à-dire en tentant toutes les combinaisons possibles (voir Figure 16).
- Netcat : Netcat est un utilitaire entièrement en ligne de commande permettant d'ouvrir des connexions réseau, que ce soit UDP ou TCP. En raison de sa polyvalence, netcat est aussi appelé le *couteau suisse TCP/IP*. Il peut être utilisé pour connaître l'état des ports par exemple.
- Nmap : Nmap est très certainement le scanneur de ports le plus connu et le plus utilisé dans le monde de la sécurité informatique (même Trinity l'utilise) ainsi que par les administrateurs réseau. Il est principalement conçu pour détecter les ports ouverts, identifier les services ainsi qu'obtenir des informations sur le système d'exploitation.

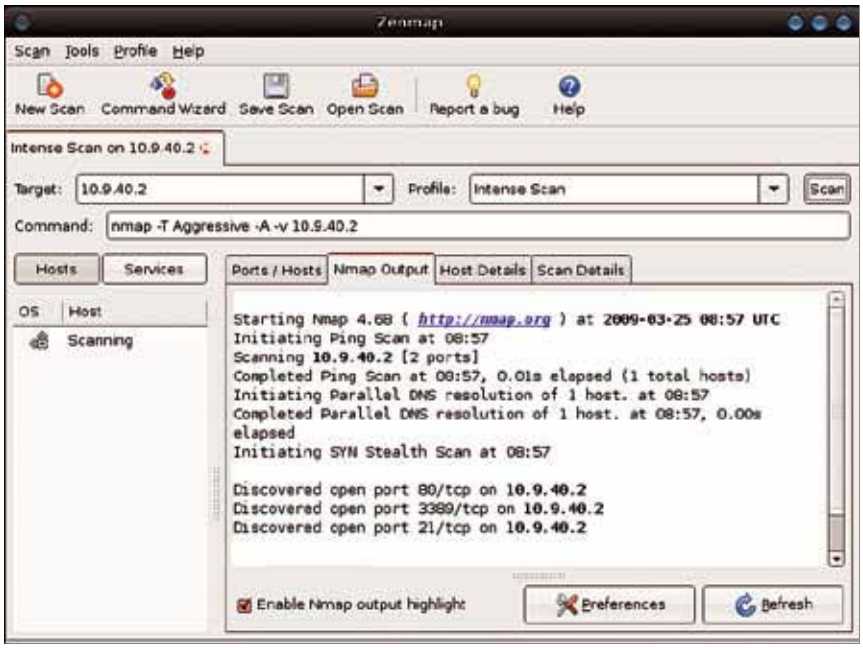

Figure 14. L'outil Nmap avec une interface graphique

Bien que très petit, nmap est un logiciel extrêmement complet permettant d'obtenir des résultats fort intéressants (voir Figure 17).

- Snarf : Snarf est un simple petit utilitaire en ligne de commande permettant de transférer des fichiers via les protocoles HTTP, gopher, finger et FTP sans aucune interaction avec l'utilisateur.

Le LiveCD Samurai dispose également de plusieurs outils non relatifs à la sécurité informatique permettant simplement de faire de Samurai une distribution complète. Vous retrouverez ainsi des programmes comme *Wine* permettant d'émuler des programmes Windows dans un environnement Linux. Des logiciels pour écouter de la musique ou pour accéder à Internet dans de bonne condition sont également disponibles.

Conclusion

L'ensemble des outils présents dans le live CD Samurai Web Testing Framework permet de le classer parmi les frameworks les plus complets en matière de pénétration des applications web. Bien que Samurai WTF soit encore un projet très jeune, il dispose déjà d'une grande maturité lui permettant d'avoir une place bien présente dans le milieu de la sécurité web.

Samurai WTF est en constante évolution et intègre de plus en plus d'outils que les professionnels de la sécurité utilisent régulièrement afin de satisfaire parfaitement leurs besoins.

Samurai WTF est donc une distribution sur laquelle il est important de garder un œil tant son évolution est impressionnante et son utilisation de plus en plus fréquente chez les professionnels.

Nous vous rappelons également que l'ensemble de ces outils bien que gratuits sont soumis à certaines restrictions qu'il est tenu de connaitre avant toute utilisation. Ces outils sont entièrement légaux mais il n'est autorisé de les utiliser que contre son propre réseau à moins d'avoir les autorisations nécessaires. Page d'accueil : *http://samurai.inguardians.com/*.