Outils

GFI LANguard Network Security Scanner

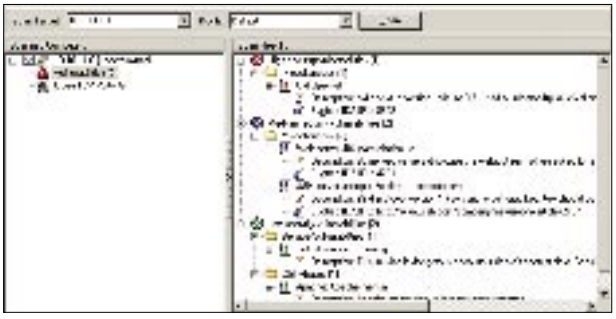
Système : *Windows*
Licence : *Commerciale/gratuiciel (en fonction de la version)*
But : *Scannage et évaluation du niveau de sécurité*
Page d'accueil : *http://www.gfi.com/*

GFI LANguard Network Security Scanner permet de scanner un ou plusieurs ordinateurs dans le réseau. À la suite du scannage, vous obtenez l'évaluation de la sécurité et une liste de points faibles.

Démarrage rapide : Admettez que vous voulez évaluer la sécurité d'un des ordinateurs de votre réseau fonctionnant comme serveur. Lancez LANguard installé au préalable, et ensuite, vous cliquez sur *New Scan* disponible sur la barre d'outils supérieure du programme. Dans la liste déroulante *Scan Type*, vous choisissez l'option *Single computer* (ordinateur seule). Bien sûr, si vous voulez scanner simultanément plusieurs ordinateurs, vous pouvez choisir une des options disponibles (par exemple, la liste d'ordinateurs, la plage d'adresses, le domaine). Vous sélectionnez *Another Computer* et vous entrez l'adresse IP de la machine à scanner.

Ensuite, vous choisissez le profil de scannage. LANguard offre quelques profils de base et permet de créer les profils personnalisés. Pour consulter les types des tests entrant dans un profil donné, il faut cliquer sur *Configuration->Scanning Profiles* dans la fenêtre *Tools Explorer.* Il est recommandé d'effectuer la première analyse à partir du profil par défaut (*Default*). Si l'on scanne des machines n'appartenant pas au réseau local, le profil *Slow Networks* est fort utile (il permet les latences dans la communication).

Après avoir sélectionné le profil (dans votre cas *Default*), cliquez sur *OK* et attendez jusqu'à ce que LANguard termine le scannage. Les brèves descriptions des actions effectuées sont disponibles dans la fenêtre *Scanner Activity Window.* Une fois le scannage terminé, dans la fenêtre *Scanned Computers* cliquez sur le caractère + accompagnant le symbole et l'adresse de l'ordinateur. Les options disponibles s'affichent (leur nombre dépend du profil sélectionné et des résultats de l'analyse). Si vous cliquez sur *Vulnerabilities* dans la fenêtre *Scan Results*, la liste des failles trouvées est affichée. Les failles sont divisées en très dangereuses (*High security vulnerabilities*), moyennement dangereuses (*Medium...*) et peu dangereuses (*Low...*). Hormis une courte description de l'erreur, vous obtenez aussi l'identificateur de la liste *Bugtraq* ou un lien à la page décrivant la faille donnée.



La liste des failles trouvées lors du scannage

Après un clic dans la fenêtre *Scanned Computers* sur l'icône *Open TCP Ports*, vous obtenez dans la fenêtre *Scan Results,* la liste des ports TCP ouverts avec les informations provenant de LANguard sur les programmes fonctionnant sur le port donné. LANguard possède aussi les mécanismes pour le relevé de l'empreinte digitale (le nom du système d'exploitation reconnu se trouve à côté de l'adresse de la machine dans la fenêtre *Scanned Computers*). Un double clic sur le numéro du port dans la fenêtre *Scan Results* lance automatiquement le telnet sur le port donné.

Les rapports de l'analyse de la machine peuvent être consultés ou enregistrés au format HTML (uniquement la version commerciale) après un clic sur l'option sélectionnée de la liste *Scan Filters* (*Current Scan*) dans la fenêtre *Tools Explorer,* et ensuite sur l'icône représentant une disquette disponible sur la barre d'outils supérieure du programme.

Autres qualités :

- permet le scannage automatique à des heures précises, l'envoi des rapports via email,
- télécharge automatiquement (pendant chaque lancement) les mises à jour des bases de données contenant les informations sur les failles, les correctifs, etc.

Défauts : La plupart des options avancées (telles que scannage automatique et le reporting) ne sont disponibles qu'en version commerciale. Dans la version de démonstration, ces options deviennent inactives après 30 jours de l'utilisation et LANguard peut être utilisé sous les termes de la licence freeware.

Tomasz Nidecki

ATTENTION !

L'entreprise GFI offre aux lecteurs de *hakin9* la version complète du programme limitée à 5 adresses IP. Pour en profiter, il faut installer la version disponible sur *hakin9.live*, et ensuite, s'enregistrer sur le site de l'éditeur (*http://www.gfi.com/pages/hakin9offer.htm*) pour obtenir via email le code série du programme. L'offre expire le 31 mars 2006.

Metasploit Framework

Système : *Windows, Linux, Mac OS X, Solaris, FreeBSD*
Licence : *GPL v2*
But : *Environnement de développement pour les tests d'intrusion et la création d'exploits*
Page d'accueil : *http://www.metasploit.com/*

Metasploit est un environnement de développement conçu pour faciliter le travail des personnes effectuant les tests d'intrusion et s'occupant de la sécurité réseau. Il contient une bibliothèque complète d'exploits et des outils servant à la création de nouveaux exploits.

Démarrage rapide : Admettez que les périphériques dans votre réseau utilisent le serveur FTP NetTerm NetFtpd sous la surveillance du système d'exploitation Windows 2000. Puisque vous savez que les anciennes versions de ce serveur été vulnérables aux attaques, vous voulez vérifier la sécurité de votre installation. Pour cela, vous vous servirez de *msfconsole* issu de Metasploit Framework.

Metasploit stocke les paramètres indispensables des variables d'environnement. Il suffit de donner les valeurs de certains paramètres pour pouvoir utiliser un exploit voulu. Commençez par choisir l'exploit à utiliser. La commande `show exploits` affiche la liste des exploits disponibles. Ensuite, au moyen de la commande `use netterm_netftpd_user_overflow`, chargez l'exploit qui exécute le débordement de tampon. Il faut remarquer que l'invite change.

Dans l'étape suivante, entrez l'adresse de l'hôte à tester en paramétrant la variable d'environnement à l'aide de la commande `set RHOST 10.0.0.1`. Il ne faut pas oublier que les variables d'environnement doivent être écrites en majuscules. Vous pouvez déterminer le port de l'hôte distant à l'aide de la commande `set RPORT 21`. Bien que cela paraisse inutile, c'est une méthode à adopter dans la pratique.

Il faut remarquer que la modularité caractéristique pour Metasploit permet de lier différents types de charges dans un exploit. Ainsi, il est facile de trouver celui qui satisfait à vos besoins. La liste de charges est disponible par la commande `show payloads`. Dans votre cas, vous utiliserez `win32_bind` qui vous connectera au shell distant sur le port déterminé, ici 4444. Pour cela, tapez la commande `set PAYLOAD win32_bind`.

Maintenant, vous pouvez démarrer l'exploit à l'aide de la commande `exploit`. La Figure 1 montre que l'attaque a réussi et vous avez obtenu l'accès au shell du système Windows sur l'hôte distant. Vous pouvez démarrer une commande quelconque avec les droits d'utilisateur qui a lancé l'application, et dans le cas du système Windows, ce sont souvent les droits d'administrateur. L'utilisateur doit être averti que ses programmes FTP exigent une modification ou une mise à jour.

Autres qualités : Metasploit constitue aussi une plateforme très importante permettant le développement d'exploits et de shellcodes. Il contient beaucoup d'outils destinés à analyser les fichiers exécutables, aussi bien au format ELF (Linux) que PE (Windows). Il comprend aussi les outils servant à capturer le contenu de la mémoire du processus en cours de son exécution, ce qui facilite l'analyse par le biais des instructions et des adresses de retour.

Les utilisateurs débutants de Metasploit retrouveront une interface Web très conviviale. Après le démarrage du programme *msfweb*, vous pouvez y accéder à l'adresse *http://localhost:55555*. Elle offre les mêmes fonctions que l'interface texte, mais est plus facile d'emploi.

Il faut dire que la mise à jour de la bibliothèque d'exploits est très facile, il suffit de taper une seule commande.

Défauts : L'interface Web sert à démarrer les exploits. D'autres éléments de la fonctionnalité de Metasploit Framework ne sont disponibles qu'au niveau de la console.

Carlos García Prado

Figure 1. *Démarrage de l'un des exploits*

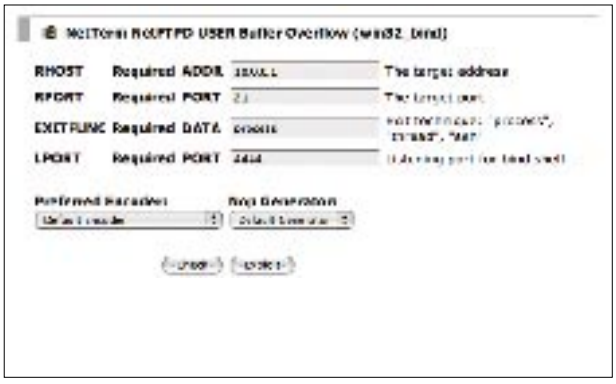


Figure 2. *Metasploit web interface*