ROYAUME DU MAROC

مكتب التكوين المهني وإنعاش الشغل

Office de la Formation Professionnelle et de la Promotion du Travail

Audit de Vulnérabilités réseau

www.ofppt.info

OFPPT

DIRECTION **R**ECHERCHE ET **I**NGENIERIE DE **F**ORMATION

SECTEUR NTIC

Sommaire

1. Audit de Vulnérabilités : Concepts et approche proactive

1.1. Introduction

L'audit de vulnérabilité permet d'adopter une approche automatisée et exhaustive des tests de sécurité. En aucun cas il remplace le test d'intrusion qui lui intervient en amont de tout projet sécurité car il permet de déceler des faiblesses sur les architectures. De plus, le test d'intrusion permet également de sensibiliser la direction aux problématiques sécurité et aide dans bien des cas à obtenir des budgets pour la sécurité. L'audit de vulnérabilités possède une approche plus régulière que le test d'intrusion, il doit permettre de mesure le niveau de sécurité et de contrôler l'imperméabilité du réseau. Dans le cas ou les résultats ne sont pas satisfaisants, l'audit de vulnérabilités doit conduire à un processus de remediation des vulnérabilités découvertes. En entreprise, on s'attache aujourd'hui davantage a la gestion des vulnérabilité qui contient la phase d'audit mais aussi tous les processus permettant la distribution des informations pour la remediation et le contrôle récurent des installations.

1.2. Le concept de l'audit de vulnérabilités

Aujourd'hui, votre réseau informatique possède un niveau de sécurité élevé. Vos serveurs et machines sont à jour, aucune vulnérabilité connue touche vos systèmes, mais demain ? En effet, tous les jours de nouvelles vulnérabilités sont découvertes. Ces failles peuvent toucher les systèmes d'exploitation ou services que vous possédez au sein de votre infrastructure. Comment être alerté au plus tôt de la présence d'une vulnérabilité qui affecte vos équipements ? Cette problématique trouve sa réponse dans les audits de vulnérabilités récurrents et l'adoption d'une démarche proactive.

Pourquoi attendre que votre service de veille vous avertisse de la sortie d'une nouvelle faille alors que vous pourriez, a peine quelques heures après sa découverte, en tester la présence réelle sur vos machines et détecter instantanément si vous êtes vulnérable ou non ?

De nombreuses solutions d'audits de vulnérabilités automatisés existent. Les technologies ont beaucoup évoluée et il est désormais possible de détecter avec une grande précision les vulnérabilités connues. L'audit automatisé et récurrent permet d'adopter une démarche proactive dans la gestion des vulnérabilités qui peuvent toucher vos réseaux.

Pour garantir dans le temps un niveau de sécurité élevé, il est impératif de tester de manière récurrente et rapprochée l'ensemble des éléments critiques qui constituent votre infrastructure.

1.3. La qualité d'une solution d'audits de vulnérabilités

La qualité d'une solution d'audits de vulnérabilités réside dans plusieurs facteurs:

- La taille et la fréquence de mise à jour de la base de connaissances.
- La précision de la détection des vulnérabilités notamment face aux problématique des faux positifs ou faux négatifs.
- La capacité de la solution à extraire des rapports détaillés et exploitables pour des techniciens ou une direction informatique.
- La capacité de la solution à s'adapter à l'entreprise notamment face aux problématiques de centralisation de la gestion de la solution et aux problématiques d'entreprises multi-sites.

1.4. Une approche proactive

Une démarche proactive dans la gestion des vulnérabilités est la clé du maintien d'un niveau de sécurité élevé sur vos systèmes. Il faut aller au devant des vulnérabilités et les traiter le plus rapidement possible avant un incident.
Un audit de vulnérabilités se déroule généralement en quatre phases. Ces phases sont les piliers de la démarche proactive de gestion de vulnérabilités.

1.4.1. Phase de découverte

La première phase d'un audit de vulnérabilités est la découverte des machines à auditer. Il faut connaître avec précision son périmètre réseau aussi bien interne que externe. Certaines solutions offrent des fonctionnalités de mapping qui permet d'effectuer un inventaire du parc interne ou externe et de choisir les machines à tester. Évidemment les machines dites "sensibles" sont les premières à auditer mais il ne faut pas néanmoins négliger les autre y compris les stations de travail qui, nous l'avons vu avec l'arriver de vers comme "sasser" ou "blaster", sont des cibles de choix pour les développeurs de virus.

1.4.2. Phase de détection

La phase de détection ou "Assessment" correspond à la détection des vulnérabilités présentes sur les machines testées. Cette phase doit être opérée de manière récurrente et automatisée. A partir de la base de connaissance de la solution d'audits, celle-ci va déterminer les vulnérabilités présentes sur une ou plusieurs machines ou éléments actifs. En fonction de la solution utilisée, cette phase peut être plus ou moins intrusive. Certains éditeurs de solutions d'audit de vulnérabilités

adoptent une politique "non intrusive" afin de pouvoir tester sans risques des serveurs en production.

1.4.3. Phase d'analyse des résultats

Cette phase correspond à l'exploitation des résultats de la phase de test. La solution d'audits de vulnérabilités doit être à même de fournir un reporting précis pour les équipes techniques, détaillant les problèmes rencontrés, l'impact sur les machines et les solutions pour corriger les failles. Certains solutions offrent également des rapport dits "Executive" qui n'étant pas techniques, s'adressent plus à une direction informatique faisant un état des lieux du niveau de sécurité global du système informatique et fournis également des rapports d'analyse de tendance sur une période donnée. Cela permet en outre aux directions de visualiser l'efficacité de leurs équipes sécurité et de pouvoir visualiser leurs retours sur investissements dans le domaine de la protection de l'infrastructure informatique de l'entreprise.

1.4.4. Phase de remediation

Cette dernière phase a pour but de gérer au mieux les interventions qui font suite aux découvertes. Certaines solutions d'audits de vulnérabilités fournissent une plateforme d'attribution de ticket lors de la découverte d'une vulnérabilité. Le ticket adressé à un technicien lui permet de mettre en place une action curative et de tracer les événements de remediation. Le processus de remediation doit être l'aboutissement d'un audit de vulnérabilités.

2. les scanners

2.1. Présentation des scanners

L'objectif avoué d'un scanner est de répondre correctement aux annonces de vulnérabilités qui se développent de façon vertigineuse. Avec l'augmentation constante Des réseaux distants ou d'entreprise, de la demande de plus en plus croissante de services d'accès distant et la multiplication des systèmes d'exploitations et de leurs fonctionnalités toujours plus nombreuses, il n'a jamais été aussi difficile de tout surveiller et de tout maîtriser au niveau de la sécurité

Pour aider l'entreprise dans cette lutte contre les failles de sécurité, il existe de nombreux outils dont les Scanners, qui sont les outils permettant la détection et d'évaluation de la vulnérabilité. Il en existe de nombreuses versions, commerciales ou open source. De formes et de dimensions variables et donnant des résultats différents

2.2. Fonctionnement des scanners

La vulnérabilité réseau, et notamment celle des OS, se déclinent sous de nombreuses formes. Néanmoins en peut tout de même les regrouper dans deux catégories principales Qui sont

-les points d'exposition locaux

-les points d'exposition distants

Concernant les points distants, l'administrateur bénéficie des différentes méthodes permettant d'automatiser l'évaluation de la vulnérabilité. L'une d'elle nécessite un outil d'exploration des ports comme NMAP (cela renvoie une liste de ports ainsi qu'un type d'OS). L'inconvénient est que m'Administrateur se retrouve noyé sous un flot de données.

Cela ne peut guère convenir a une utilisation sur des grands réseaux d'entreprise Car sous le nombre d'informations, il reste encore a définir des informations telle que de savoir ce qui écoute aux ports concernés, la version du dit service et il reste ensuite a recouper toutes ces données par rapport aux failles de sécurités connues. Ce qui devient long et fastidieux.

Si a cette idée de recherche de port et d'OS on ajoute un mécanisme d'indentification de Type/service étant a l'écoute sur un port X, on obtiendrait déjà une analyse beaucoup plus fine du système.

Si on complète cette méthode d'analyse par une comparaison avec les listes de failles connues en fonction des paramètres précèdent, on commence déjà à avoir une idée des trous de sécurité des OS du réseau

Une fois toutes ces données compilées, on obtient un scanner réseau. La majorité des scanners rapportent les données de vulnérabilités, un mécanisme d'évaluation ainsi qu'un mécanisme de rapport.

Il est à noter qu'il existe des méthodes plus performantes pour découvrir des vulnérabilités. Notamment en créant des logiciels qui en plus de tester les services et les ports, tentent aussi d'exploiter ces failles pour les vérifier. Si cette méthode donne indéniablement plus de résultats, elle a aussi pour elle le désavantage de faire planter certains systèmes et services, ce qui peut être avec de certaines conséquences

2.3. Qualités a rechercher dans un scanner

A l'utilisation préalable d'un scanner il est nécessaire de déterminer aux mieux les besoins en les besoins en vulnérabilités, en terme d'OS et de parc machines. En effet certains produits seront plus particulièrement adaptés a l'utilisation des tel ou tel OS.

Néanmoins ils doivent tous répondre à un minimum de résultats fonctionnels

2.3.1 Exhaustivité des contrôles de vulnérabilité et justesse des contrôles

Les scanners détectent toujours un maximum de vulnérabilités. Néanmoins, votre choix doit toujours porter sur un produit qui vous offrira les failles des niveaux ADMIN/ROOT

2.3.2 Etendue des contrôles (Local / Distant)

Certains scanners sont plus performants que d'autres, prenez bien le temps de rechercher la encore le bon produit, car un scanner qui laisserai passer de trop grosses failles serait un handicap certain pour la justesse de votre sécurité réseau

2.3.3. Gestion des mises a jour

Comme les sytémes d'exploitation, le scanner repose sur un base de détection qui doit être mise a jour pour détecter les nouvelles failles reconnues et vous permettre au mieux d'intervenir pour combler les failles de sécurité

2.3.4. Gestion et capacité de rapport

Quel rapport vous donne votre scanner ? Arrivez vous a interpréter et a décrypter les informations q'il vous renvoie ? Toutes ces questions doivent trouver une réponse claire Préventivement a l'achat de votre scanner. Même le meilleur scanner du monde ne vous seras évidemment d'aucune utilité si vous ne comprenez pas les rapports qu'il vous transmet.

2.3.5. Aspect budgétaire (gestion des licences, par nœud, par serveur etc.)

La c'est l'aspect financier qui va prédominer, veuillez a bien vous informer sur la façon dont est distribué le produit, car la vous pouvez vous retrouver suivant votre topologie avec une facture très salée alors qu'un produit conçurent (pas forcément moins bon) vous évitera parfois une dépense conséquente et inutile

!! Il est important de préciser que a l'instar de tous les produits de sécurité, les scanners N'échappent pas à certain défaut et par la même sont incapables de trouver toutes les vulnérabilités ; ne pensez donc pas qu'un scanner seul puisse vous permettre de régler toutes les failles de sécurité.

Le défaut récurent des scanners concerne aussi la question des mises a jour (journalière, Mensuelles, trimestrielles).

Il est possible de trouver des Informations sur le Top Des failles de sécurité sur le site www.sans.org/top20.htm ainsi que des outils A l'adresse www.sans.org/tools04.pdf

3. Les outils de vulnérabilités réseau

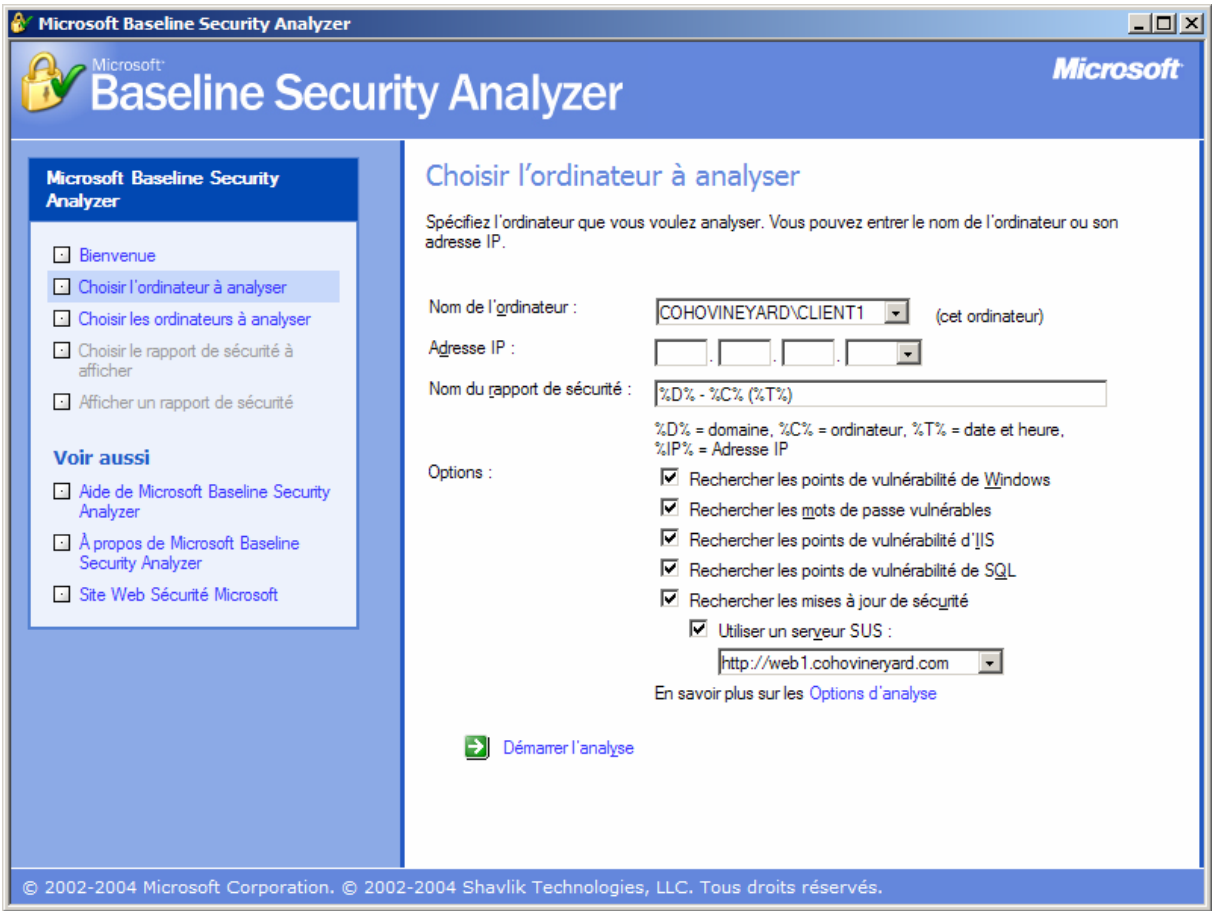
3.1. MBSA

MBSA est un outil d'analyse des vulnérabilités de sécurité qui vous informe de l'état d'ordinateurs clients et de serveurs. MBSA est compatible avec Windows NT 4.0, Windows 2000, Windows XP et Windows Server 2003 et windows 2008 . Il recherche les erreurs de configuration courantes dans le système d'exploitation, les services Internet (IIS), Microsoft SQL Server. et les applications de bureau, et peut vérifier les mises à jour de sécurité manquantes pour Windows, les services IIS, SQL Server et Microsoft Exchange Server.

MBSA inclut une interface utilisateur graphique et un utilitaire de ligne de Commande pour l'exécution de scripts et l'automatisation. MBSA peut analyser des ordinateurs uniques, une plage d'adresses IP ou tout un domaine ou groupe de travail. Les résultats de ces analyses peuvent être enregistrés dans des rapports à des fins d'évaluation ou d'archivage.

MBSA fournit deux méthodes pour analyser un environnement réseau et déterminer l'état des mises à jour. Vous pouvez réaliser une analyse à l'aide de l'interface utilisateur graphique ou utiliser un script pour automatiser l'analyse à l'aide de l'interface de ligne de commande.
Par ailleurs, Windows XP et Windows Server 2003 incluent deux utilitaires, Systeminfo et WMIC, qui vous permettent de déterminer l'état des mises à jour sur un ordinateur.

Interface utilisateur graphique de MBSA



L'interface utilisateur graphique (voir illustration précédente) vous permet d'analyser un ou plusieurs ordinateurs. Les résultats de l'analyse s'affichent dans MBSA sous forme d'un rapport et sont enregistrés dans un fichier. L'interface utilisateur graphique de MBSA est conçue pour les analyses à caractère unique qui ne seront pas répétées régulièrement. Vous pouvez effectuer une analyse individuelle après avoir déployé une mise à jour critique pour vous assurer que la mise à jour a été correctement installée sur les ordinateurs affectés.

Interface de ligne de commande de MBSA

L'interface de ligne de commande est fournie par l'utilitaire mbsacli.exe. Cet utilitaire, installé en même temps que MBSA, permet d'effectuer les mêmes opérations que l'utilitaire graphique avec des commutateurs. Le tableau suivant répertorie les commutateurs de mbsacli.exe les plus couramment utilisés.

3.2. GFI LANguard

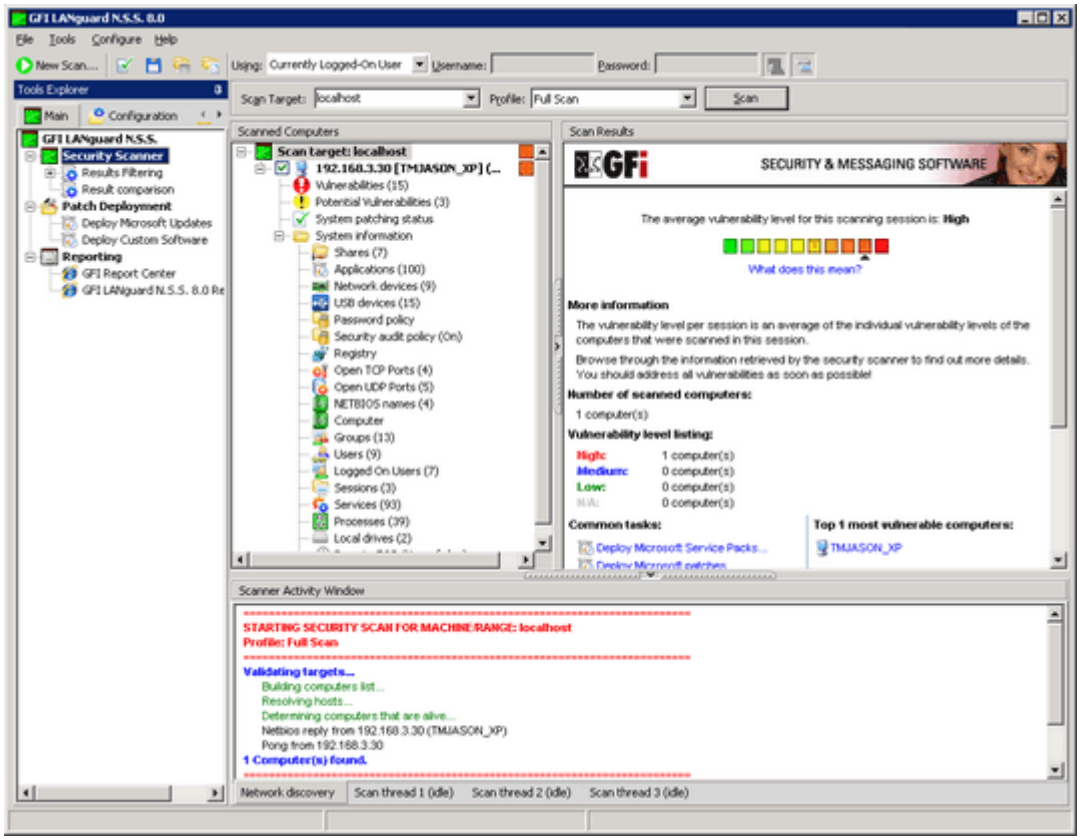
GFI LANguard Network Security Scanner (N.S.S.) est une solution maintes fois primée qui adresse les trois piliers de gestion des vulnérabilités: balayage de sécurité, gestion de patches et inspection de réseau avec une seule console intégrée. En balayant le réseau entier, il identifie tous les problèmes de sécurité possibles et en utilisant sa puissante fonctionnalité de reportage détaillé, il vous donne les outils dont vous avez besoin pour détecter, évaluer, rapporter et rectifier toutes les menaces.

- Balayage des vulnérabilités
- Gestion de patches
- Inspection de matériel de réseau et de logiciel.

3.2.1. Balayage des vulnérabilités

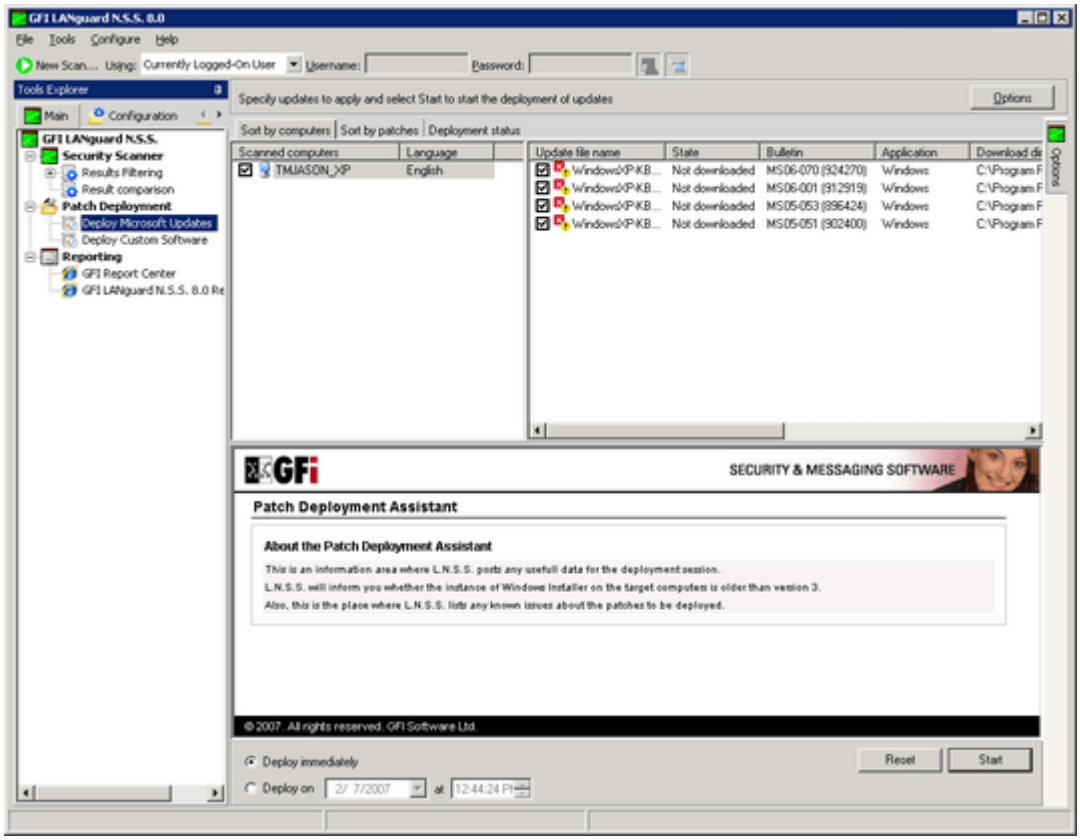
GFI LANguard N.S.S. vous donne la capacité d'effectuer des balayages sur des plateformes multiples (Windows, Mac OS, Linux) à travers tous les environnements et d'analyser l'état de santé de la sécurité de votre réseau à partir d'une seule source de données. Ceci assure que vous êtes en mesure d'identifier et de parer à toutes les menaces avant que les pirates ne les découvrent et ne les exploitent

GFI LANguard N.S.S. balaye les ordinateurs, identifie et classe les vulnérabilités par catégories de sécurité, recommande une ligne de conduite par catégorie et fournit les outils qui vous permettent de résoudre ces problèmes.



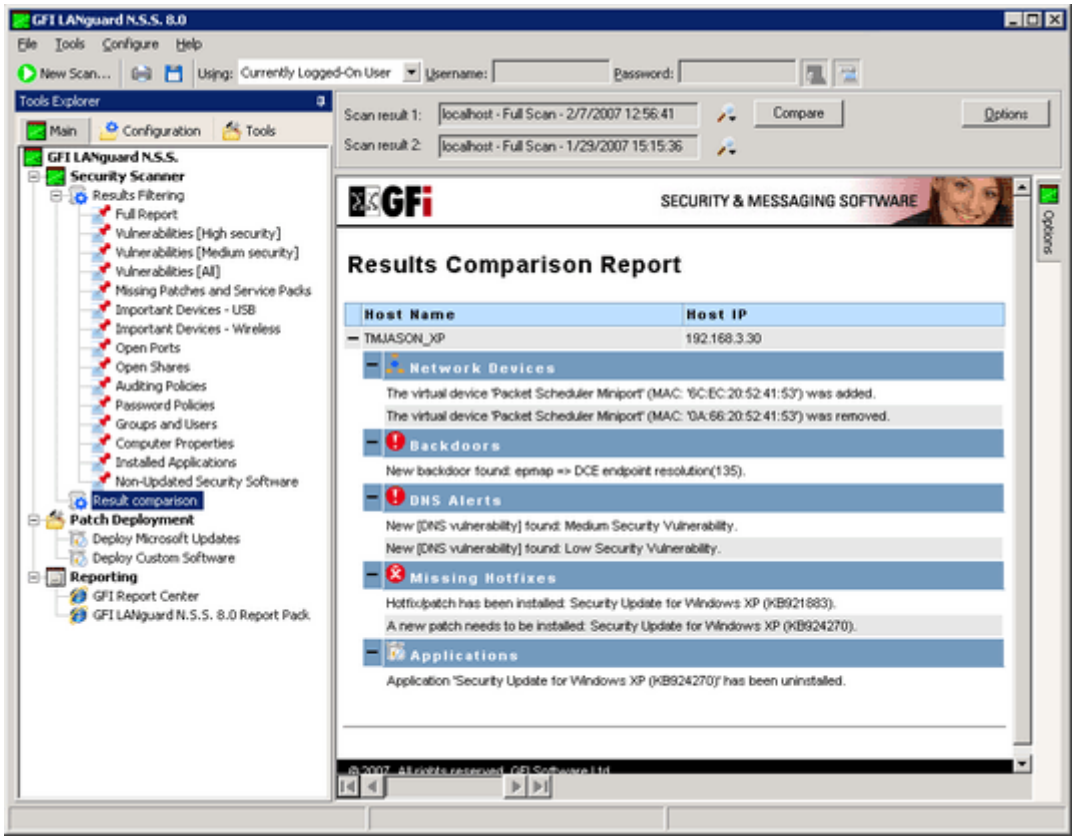
3.2.2. Gestion de patches

Lorsqu'un balayage est complété, GFI LANguard N.S.S. vous donne toutes les fonctionnalités et les outils dont vous avez besoin pour efficacement installer et gérer les patches sur toutes les machines installées sur des plateformes différentes de logiciel d'exploitation dans 38 langues. GFI LANguard permet également le téléchargement automatique des patches manquants aussi bien que le roulement en arrière des patches. D'autres logiciels personnalisés peuvent également être déployés. Ceci a comme conséquence un environnement uniformément configuré qui est protégé contre toutes sortes de vulnérabilités



3.2.3. Inspection de réseau et de logiciel

La fonction d'audit de GFI LANguard N.S.S. vous indique tout ce que vous devez savoir au sujet de votre réseau – les dispositifs USB branchés, les logiciels installés, les parties et ports ouverts, et les mots de passe faibles en cours de service. Les rapports détaillés de cette solution vous donnent un important aperçu instantané et en temps réel du statut de votre réseau. Les résultats de balayage peuvent être facilement analysés en utilisant des filtres et des rapports, de qui vous permet de sécuriser proactivement le réseau en verrouillant les ports ouverts, en supprimant les utilisateurs ou les groupes qui ne sont plus utilisés ou en désactivant les points d'accès aux connexions sans fil.



3.3. Nessus

3.3.1. Presentaion

Nessus est l'un des scanner de vulnérabilités le plus populaire et le plus utilisé pour auditer un réseau et déterminer les failles potentiels des stations/serveurs sur celui-ci. De plus jusqu'à la version 2, l'outil était totalement OpenSource sous licence GPL. La version 3 est toujours gratuite mais le code source n'est plus accessible.

Nessus est un projet qui débuta en 1998, il a été créé par **Renaud Deraison**. Il représente une solution robuste pour scanner les vulnérabilités d'un grand réseau d'entreprise.

Le fait qu'il soit gratuit et donc n'entame pas le budget sécurité d'une entreprise, en fait une solution très populaire. Son mécanisme de "**plugins**" permet en plus à ses utilisateurs de développer leurs propres tests de vulnérabilités sans avoir à prendre part au développement du projet. Ces mêmes plugins qui sont la **base de connaissances** de Nessus sur les vulnérabilités peuvent être mis à jour rapidement en profitant d'une grande communauté qui maintient le projet en vie.

3.3.2. Composants de base

Ce qui fait de Nessus un tel outil est l'architecture unique sur laquelle il est construit. La flexibilité de l'architecture de Nessus prend en compte chaque élément du cycle de vie de sécurité. De l'exécution des scans de vulnérabilités sur des réseaux de grandes envergure, aux rapports sous forme de graphiques et d'hyperliens qui présentes les vulnérabilités, aux descriptions des vulnérabilités et leurs résolutions, tous ces aspects créent la base d'un réseau sain au niveau sécurité. Voici les principaux composants de Nessus :

- Le client et le serveur Nessus
- Les plugins Nessus
- La base de connaissances de Nessus

3.3.3. Client et serveur

À l'origine, les scanners de vulnérabilités étaient tous basés sur une architecture client. Un consultant introduisait son ordinateur portable au meilleur endroit d'un réseau d'entreprise et lançait son scan. Un scan sur une tel quantité d'adresses réseaux prend au minimum une demi-journée à quelques jours, selon la largeur du réseau et le détail des paramètres de scan. Ceci rendrait l'ordinateur portable inutilisable pour cette durée.

Le projet Nessus a pris en compte cet aspect des Vulnerability Assessments dès le début. Pour éviter ce problème et sûrement beaucoup d'autres, le projet Nessus a adopté un modèle d'architecture sous forme de client/serveur.

3.3.4. Les plugins

Un autre aspect de Nessus qu'il est le seul à proposer parmi les scanners de vulnérabilités est son langage de scripting (NASL : Nessus Attack Scripting Language). NASL offre un moyen de créer ses propres plugins de détection de vulnérabilités. L'avantage est que chacun peut apporter sa propre expertise de sécurité. On peut ainsi imaginer un réseau utilisant des protocoles ou services unique pour lesquels on pourra développer des plugins spécifiques.

NASL ressemble beaucoup au langage C. Il a été spécifiquement conçu avec la sécurité à l'esprit, car il communiquera seulement avec l'hôte qui est passé comme argument. Il n'exécutera pas non plus de commande locale. Avec cet "sandbox" autour de l'interface de NASL, il est peu probable qu'un faux plugin effectue des opérations illégales. NASL est

également construit pour communiquer des informations entre-eux. Ceci est réalisé par l'utilisation de la "base de connaissances".

3.3.5. La base de connaissances

La base de connaissances permet aux plugins récents d'enrichir les données collectées par des plugins plus anciens. Si on considére un plugin qui test l'existence d'un serveur web, et, si il est trouvé, lance des tentatives pour discerner quel serveur HTTP fonctionne réellement. Le plugin a la capacité de placer une valeur dans une variable de la base de connaissances de Nessus pour ce serveur. Si on prend un exemple spécifique, notre script NASL trouve la version d'Apache qui fonctionne sur le serveur Web distant. Le plugin place alors la variable "WWW/banner/80" à par exemple "/2.0.54 (Unix) PHP/4.3.4 mod_ssl/2.8.16 OpenSSL Apache/0.9.7a"

Ceci permet à un plugin sous adjacent au précédent de récupérer la valeur de la variable "WWW/banner/80". Il va ainsi pouvoir déterminer que le serveur utilise "OpenSSL/0.9.7a", et peut signaler que cette version du serveur est vulnérable, car c'est une version périmée d'OpenSSL. De cette façon, chaque information remontée par des plugins peut être utilisée par d'autres en cascades pour rentrer dans un niveau supérieur de détection de vulnérabilités. Renaud Deraison suggère que les auteurs de plugins emploient la base de connaissances autant que possible. Ceci servira à étendre les possibilités de Nessus et à accélérer l'exécution des futures plugins qui pourrons rechercher dans la base de connaissances des informations déjà récupérées

Note d'attention particulière.

Pour approfondir le sujet....

Proposition de références utiles permettant d'approfondir le thème abordé

Sources de référence

Citer les auteurs et les sources de référence utilisées pour l'élaboration du support