Sylvain THIROINE

Fiche n ° 4 : NESSUS

1 – Installation

a) Créez un compte en allant sur le site : https://www.tenable.com/products/nessus/nessus-essentials
b) Télécharger le fichier Nessus-#.##.#-debian6_votre système.deb et enregistrez le dans le dossier téléchargement
c) Dans le terminal :
d) Allez dans le dossier téléchargement
e) Tapez la commande suivante : sudo dpkg -i Nessus-#.##.#-debian6_votre système.deb
f) Démarrer le service Nessus : sudo systemctl start nessusd.service
g) Dans le navigateur FIREFOX : tapez l'URL suivante https://localhost:8834/

2 – Configuration

a) Sélectionner l'option Nessus Essentials et cliquer sur SKIP pour saisir le code d'activation reçu par mail
b) Remplir les champs nom d'utilisateur et mot de passe
c) Installations de plugins qui prendra un certain temps en fonction de votre connexion internet

3 – Liste des modèles de scan

a) Basic Network Scan

Analyse complète du système adaptée à tous les hôtes

b) Advanced Scan

Configurer une analyse sans utiliser aucune recommandation

c) Advanced Dynamic Scan

Configure une analyse dynamique des plugins sans recommandations

d) Malware Scan

Rechercher des logiciels malveillants sur les systèmes Windows et Unix

e) Mobile Device Scan

Accéder aux appareils mobiles via Microsoft Echange ou un MDM (Mobile Device Management, gestion des terminaux mobiles)

f) Web Application Tests

Rechercher les vulnérabilités Web publiées et inconnues à l'aide du scanner Nessus

g) Credentialed Patch Audit

Authentifier auprès des hôtes et énumérer les mises à jour manquantes

h) Intel AMT Security Bypass

Il est possible d'initialiser l'attaque à distance. L'exploitation ne nécessite aucune forme d'authentification Intel AMT/ISM à 11.6 élévation de privilèges

i) Spectre and Meltdown

Meltdown et **Spectre** sont deux vulnérabilités résultant de l'exécution d'un code spécial de bas niveau appelé « code noyau », qui s'exécute notamment au cours d'un processus connu sous le nom d'exécution spéculative.

j) WannaCry Ransomware

WannaCry est un exemple de crypto-ransomware, un type de programme malveillant utilisé par les cybercriminels pour extorquer de l'argent.

k) Ripple20 Remote Scan

19 vulnérabilités affectant une bibliothèque TCP/IP implémentée dans de nombreux objets connectés et appareils. Une analyse à distance vers les hôtes d'empreintes digitales exécutant potentiellement la pile treck dans le réseau

l) Zerologon Remote Scan

Zerologon est **une vulnérabilité dans la cryptographie du processus Netlogon de Microsoft qui permet une attaque contre les contrôleurs de domaine Microsoft Active Directory**. Zerologon permet à un pirate de se faire passer pour n'importe quel ordinateur, y compris le contrôleur de domaine racine.

m) Solorigate

De multiples vulnérabilités ont été découvertes dans les produits SolarWinds. **Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, une atteinte à la confidentialité des données et une élévation de privilèges**.

n) Proxylogon : MS Exchange

Par « ProxyLogon », le chercheur entend deux failles. La principale (CVE-2021-26855) **permet de contourner l'authentification en envoyant, via Outlook Web Access, des requêtes HTTP arbitraires ers des ressources statiques**. Elle ouvre la voie à l'exploitation de la seconde faille (CVE-2021-27065)

o) PrintNightmare

Baptisée « PrintNightmare », elle **autorise l'exécution de code arbitraire à distance par l'intermédiaire du spouleur d'impression** (Windows Print Spooler). À juste titre, il s'agit d'un service en charge de gérer automatiquement une file d'attente d'impressions de documents.

p) Active Directory Starter Scan

Rechercher des erreurs de configuration dans Active Directory

q) Log4Shell

Log4Shell, également connue par son numéro CVE-2021-44228, **est une vulnérabilité zero-day exploitée par exécution de code arbitraire et touchant l'utilitaire Java Log4j**. Cette vulnérabilité est divulguée à Apache par l'équipe de sécurité cloud d'Alibaba le 24 novembre 2021 et publiée le 9 décembre 2021.

r) Log4Shell Remote Checks
s) Log4Shell Vulnérabilité Ecosystem

t) CISA Alerts AA22-011A and AA22-047A

AA22-011A : Comprendre et atténuer les cybermenaces parrainées par l'État russe contre les infrastructures critiques américaines
AA22-047A : Des cyber acteurs parrainés par l'État russe ciblent des réseaux d'entrepreneurs de défense autorisés pour obtenir des informations et des technologies sensibles de défense américaine

u) Contileaks

Code source du ransomware Conti qui a été divulgué.

v) Ransomware Ecosystem

Vulnérabilités utilisées par les groupes de ransomware et leur s affiliés

w) **2022 Threat Landscape Report TLR**

un scan pour détecter les vulnérabilités présentées dans notre rapport de fin d'année

4 – Utilisation

a) Cliquer sur « New Scan » pour lancer un modèle de scan
b) Choisir le modèle de scan que l'on veut effectuer
c) Remplir les champs en fonction de la demande
d) Exécuter le scan
e) Analyse du scan en cliquant sur la ligne du scan en cours

5 – Glossaire

B

Base de connaissances : ou Knowledge Base (KB) en anglais. La base de connaissances du serveur Nessus est une matrice stockée en mémoire pendant toute la durée du scan (à la fin du scan, cette matrice est libérée). Elle contient des renseignements sur les hôtes cibles, recueillis pendant un scan. Parmi ces informations, on retrouve la liste des ports ouverts, le type et la version de service réseau associé aux ports ouverts, le type de système d'exploitation, etc. Le but premier de cette base de connaissances était de réduire la redondance au niveau des tests et rendre accessibles les informations pour les plugins.

Buffer overflow : ou dépassement/débordement de tampon. Conséquence causée par un processus qui, lors de l'écriture dans un tampon, écrit à l'extérieur de l'espace alloué au tampon, écrasant ainsi des informations nécessaires au processus. Le comportement de l'ordinateur devient alors imprévisible et peut se caractériser par un blocage du programme, voir de tout le système.

C

CCE : Common Configuration Enumeration. CCE est un groupe de travail qui contribue au développement du CCE List par des discussions, conférences, meetings. Cette CCE List est divisée en plusieurs fichiers Excel pour correspondre aux différentes plates-formes. Elle permet d'énumérer, pour chaque faute de configuration, un identifiant unique, une description, les problèmes techniques rencontrés, ...

CPE : Common Platform Enumeration. CPE est un dictionnaire pour le stockage structuré de données de systèmes, de plates-formes et de packages. CPE inclut un langage de description de contenu complexe.

CVE : Common Vulnerabilites and Exposures. CVE est un dictionnaire public de vulnérabilités connues, associées à leurs risques.

CVSS : Common Vulnerability Scoring System. CVSS est un framework opensource permettant de mesurer la gravité de l'impact qu'ont les vulnérabilités par une génération de score précis. CVSS est la référence des outils de mesure pour les entreprises et le gouvernement. CVSS segmente les risques (en métrique basique,

temporelle et environnementale) et les pondèrent par des formules mathématiques. Grâce à CVSS, Nessus peut appliquer des criticités aux failles de sécurité.

D

DoS : Denial of Service ou déni de service en français. Une attaque déni de service est caractérisée par une tentative explicite par des attaquants afin d'empêcher les utilisateurs légitimes d'un service, d'utiliser ce service. On peut définir une attaque par déni de service comme une attaque qui a pour but de rendre indisponible un service (bloquer un serveur de fichiers, rendre impossible l'accès à un serveur web, empêcher la distribution de mails dans une entreprise ou rendre indisponible un site internet).

DDoS : Distributed Denial of Service. Le principe est d'utiliser plusieurs sources (daemons en esclave) pour l'attaque et des maîtres (masters) qui les contrôlent. Le pirate utilise des maîtres (tout en effaçant ses traces) pour contrôler plus facilement les sources. En effet, il a besoin de se connecter (en TCP) aux maîtres pour configurer et préparer l'attaque. Les maîtres se contentent d'envoyer des commandes aux sources en UDP. Pour installer les daemons et les masters, le pirate utilise des failles connues (buffer overflow sur des services RPC, FTP ou autres).

F

Faux positif : Résultat d'une prise de décision à deux choix (positif ou négatif) déclaré à tort, là où il est **en réalité négatif.**

G

Garbage Collector poor : ou ramasse-miettes, ou récupérateur de mémoire. Un Garbage Collector est un mécanisme de gestion automatique de mémoire. Il est responsable du recyclage de la mémoire préalablement allouée puis inutilisée. Dans le cas d'un Garbage Collector poor, on alloue de la mémoire pour chaque token et on associe un compteur à chaque token. Quand le token arrive à 0, on libère la mémoire.

I

IDS : Intrusion Detection System ou système de détection d'intrusions. Un IDS est un mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysé (un réseau ou un hôte défini). Il permet d'avoir une connaissance sur les tentatives d'intrusions (réussies ou échouées).

Injection : Injection de code visant à exploiter une faille de sécurité d'une application. Cette vulnérabilité est présente lorsque le développeur laisse un champ texte trop permissif par l'utilisateur par exemple. L'utilisateur peut alors encapsuler une partie de code et détourner des authentifications (par exemple).

K

Kerberos : Protocole d'authentification réseau utilisant un système de ticket au lieu de mots de passe en texte clair. Ce principe renforce la sécurité des systèmes d'information en empêchant un intrus d'intercepter le mot de passe. Kerberos utilise un chiffrement par clé symétrique.

M

Man In The Middle : Attaque qui a pour but d'intercepter les communications entre 2 parties sans que ni l'une ni l'autre ne puisse se douter que le canal de communication a été compromis.

O

OVAL : Open Vulnerability and Assessment Language. OVAL est un ensemble de standards pour promouvoir des informations relatives à la sécurité et pour standardiser le transfert de ces informations pour tous les outils de sécurité.

P

Plugins : Un plugin correspond en réalité à un script NASL. Dans le logiciel Nessus, on appelle *plugins* des failles de sécurité par abus de langage, puisque Nessus télécharge une liste de plugins et que l'administrateur Nessus peut développer ses propres scripts qui viennent se greffer à l'existant. L'utilisateur peut sélectionner les plugins qui l'intéresse pour spécifier les attaques.

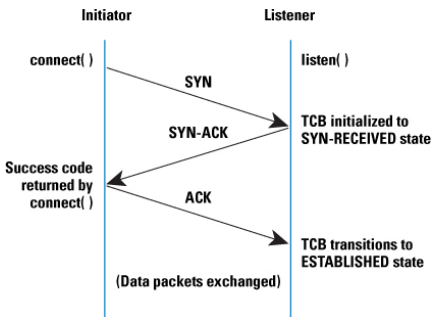
S

SCAP : Security Content Automation Protocol. SCAP est une méthode permettant la gestion des vulnérabilités de manière automatique, leurs mesures et leurs évaluations. SCAP se compose de plusieurs standards pour l'énumération de failles de sécurité et des problèmes de configuration liés à la sécurité. Parmi ces standards, on retrouve :

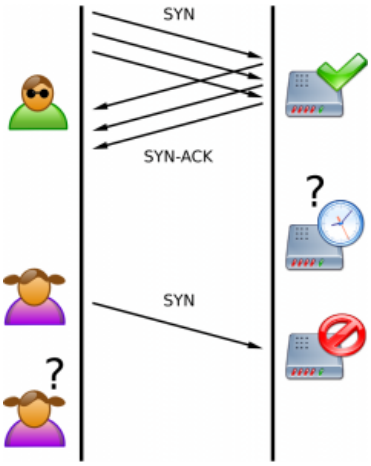
- CVE (Common Vulnerabilities and Exposures)
- CCE (Common Configuration Enumeration)
- CPE (Common Platforme Enumeration)
- CVSS (Common Vulnerability Scoring System)
- XCCDF (Extensible Configuration Checklist Description Format)
- OVAL (Open Vulnerability and Assessment Language)

Se sont ces mêmes standards qui sont utilisés pour développer des applications telles que les scanners de vulnérabilité, IDS/IPS (Intrusion Detection System/Intrusion Prevention System), anti-malware, ...

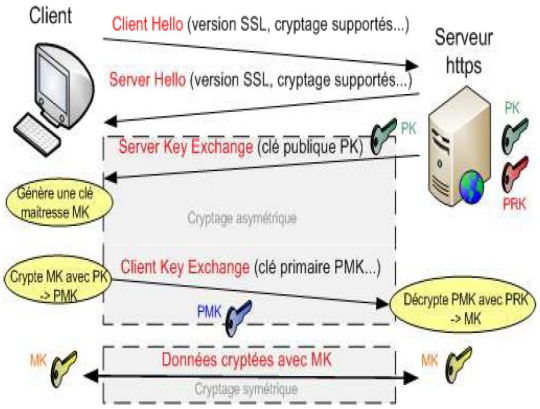
SYN : Numéro de séquence de synchronisation pour une demande de connexion TCP. Ce *flag* est mis à 1 uniquement dans le premier paquet d'une demande de connexion. Si la connexion est correctement établie, alors l'émetteur reçoit une réponse TCP avec le *flag* ACK mis à 1. C'est le three way handshake :



SYN flood : Attaque visant à atteindre un déni de service par inondation de requêtes SYN vers la cible



SSL : Secure Sockets Layer. Le protocol SSL a été proposé au départ par Netscape et permet des connexions sécurisées. Il permet une authentification réciproque entre le client et le serveur à l'aide de clés symétriques, mais également des transactions cryptées entre le client et le serveur.



X

XCCDF : Extensible Configuration Checklist Description. XCCDF est un langage qui permet de normaliser des documents de sécurité de type checklist et benchmarks dans des fichiers XML.