METHODOLOGIE DE CONDUITE D'UN PEN TEST

Ce guide à pour objectif de donner les grandes lignes pour mener à bien un audit opérationnel de la sécurité d'une entreprise.

Afin de juger la matérialité du risque soulevé par les différents points d'audit et faciliter la mise en œuvre d'un plan d'actions, il faut hiérarchiser les recommandations en fonction de trois niveaux de matérialité suivants :

Niveau 1 : les mesures préconisées devraient être suivies rapidement.

Niveau 2 : les améliorations devraient être prises en compte à moyen terme.

Niveau 3 : les recommandations correspondent aux meilleures pratiques et peuvent être mises en œuvre à plus long terme.

L'ensemble de cette étude a été menée avec Kali Linux qui est une boîte à outil pour l'audit de la sécurité des entreprises.

Apres avoir finir d'installer Kali linux :

-Ouvrez Un Terminal

-Tapez leafpad /etc/apt/sources.list

-Effacez ce qui se trouve à l'intérieur et entrez :

deb http://http.kali.org/kali kali-rolling main contrib non-free

Ensuite faire mise à niveau et la mise à jour :

root@pentest:~#apt-get upgrade

root@pentest:~#apt-get update

I. Découverte des données publiques

La découverte de données publique peut se faire par l'analyse du site web de l'entreprise cible.

1. Accès au fichier robots du site

Cette analyse peut se faire par l'étude du fichier robots.txt du site web.

Cela peut se faire dans le navigateur par l'action suivante :

monsite.ci/robots.txt

Ce fichier peut permettre l'indexation de dossiers et fichiers sensibles du site. L'option **Sitemap** indique au « crawler » et « spider » le lien vers notre site map, qui peut donner l'architecture globale d'un site web.

Il faut donc supprimer le fichier robots.txt s'il existe car un site web peut fonctionner sans lui.

2. Telnet sur le site web

L'action suivante peut être effectuée : **telnet www.monsite.ci 80**

Le telnet est un protocole assez bavard qui peut permettre lorsque la tentative de connexion au serveur distant échoue de donner le système d'exploitation de celui-ci, le type de serveur web utilisé et la version du serveur web. Ce qui représente une mine d'information importante pour un pirate car il est orienté.

Il faut s'assurer qu'à la longue le serveur ne puisse pas répondre au telnet.

3. Utilisation de whois

Voici la syntaxe d'utilisation : **whois monsite.ci**

Cette commande lancée depuis Kali linux peut de découvrir les informations sur l'enregistrement du site web.

On peut donc avoir la date de la dernière mise à jour, des informations personnelles sur celui qui fait l'enregistrement comme son numéro de téléphone personnel etc.

4. Utilisation de dnsenum

Le scan avec dnsenum permet de récupérer les enregistrements DNS liées au site et permet de savoir combien de serveurs prennent le relais pour le site et aussi l'adresse IP serveur de messagerie professionnel si-il en existe un. Cette action peut permettre de vérifier le transfert de zone entre les différents serveurs DNS du FAI. Le succès du transfert de zone qui provient d'une mauvaise configuration

des zones au niveau d'un serveur DNS donnera au pirate les noms d'hôtes associé aux adresses IP et de facto l'organisation du réseau.

Syntaxe : **dnsenum monsite.ci**

5. Utilisation de theharvester

Le scan avec theharvester permet d'avoir des informations sur le domaine, les sous domaines, adresse email, des noms d'hôtes, ici la recherche a été faite avec le moteur de recherche Google.

Syntaxe : **theharvester -d monsite.ci –l 100 -b google**

6. Scan des vulnérabilités du site cible monsite.ci

Pour le scan des vulnérabilités web nous conseillons d'utiliser le Framework **OpenVas** qui est un « fork » du célèbre scanner **Nessus**.

Par défaut il n'est pas installé dans Kali, il faut donc l'installer voici la procédure.

apt-get install openvas

openvas-setup

Lors de la procédure d'installation un mot de passe par défaut vous sera donné, veuillez l'écrire quelque part car vous en aurai besoin pour la première connexion.

La première connexion se déroule comme suit :

https://127.0.0.1:9392 il faut changer le mot de passe donné lors de l'installation au profit de votre propre mot de passe.

L'outil openvas permet après analyse de générer un rapport sous format pdf.

Mais on peut aussi utiliser pour le scan des vulnérabilités web l'outil **golismero**.

Syntaxe : **golismero scan www.monsite.ci**

II. Étude de l'infrastructure réseau

Pour faire l'étude de l'infrastructure pour y découvrir les vulnérabilités, nous procéderons avec deux approches qui sont :

- Etude des vulnérabilités depuis l'extérieur
- Etude des vulnérabilités à l'intérieur du réseau

1. Etude des vulnérabilités depuis l'extérieur

Lors des interviews avec le responsable en charge du réseau il peut vous fournir les adresses IP publiques utilisées par les équipements d'entrée que le routeur et le pare feu.

Il faut faire d'abord faire un scan de ports sur ces plages pour tenter de découvrir des vulnérabilités dans le cas où les équipements réseau comme les routeurs sont des CISCO. On utilisera plusieurs outils pour réaliser cela. Nous utiliserons comme plage d'adresse publique fictive **196.47.10.1 à 196.47.10.5**.

a. cisco-ocs

Cet outil cisco-ocs peut faire des scans par plage sur des équipements CISCO.

```
root@pentest:~# cisco-ocs 196.47.10.1 196.47.10.5
********************************          OCS          v          0.2
**********************************
****                                    ****
****              coded by OverIP              ****
****              overip@gmail.com               ****
****              under GPL License              ****
****                                    ****
****      usage: ./ocs xxx.xxx.xxx.xxx yyy.yyy.yyy.yyy          ****
****                                    ****
****          xxx.xxx.xxx.xxx = range start IP          ****
****           yyy.yyy.yyy.yyy = range end IP           ****
****                                    ****
**************************************************************************
***
(196.47.10.1) Filtered Ports
```

Ce résultat obtenu veut dire que c'est derrière l'adresse 196.47.10.1 que se trouve le pare feu qui peut être par exemple un CISCO ASA.
Il faut donc s'assurer que ce point d'entrée est plus fortifié avec toutes les mises à jour car c'est le point d'entrée et de sortie du réseau.

b. cisco-global-exploiter

L'outil CISCO global exploiter contient actuellement 14 vulnérabilités découvertes sur les équipements CISCO.
En passant en revue une par une différente vulnérabilité, nous avons remarqué que le pare feu ASA 5510 de notre entreprise fictive par exemple est vulnérable à l'attaque 9 (Cisco 514 UDP Flood Denial of Service Vulnerability) par exemple.
Syntaxe : cge.pl adresse ip numéro attaque (1 à 14)

- **Exemple 1**

root@pentest:~# cge.pl 196.47.10.1 9
Input packets size : 1024

Packets sent ...
Please enter a server's open port : 23

Now checking server status ...
Vulnerability successful exploited. Target server is down …

Le problème survient lorsque le système CISCO IOS reçoit un nombre important de paquet malformés UDP. Ce qui amènera le système à utiliser toutes les ressources disponibles du CPU ce qui rend le système indisponible.

Ce qui fait qu'un pirate peut utiliser cette faille pour mener une attaque par déni de service (DOS) avec succès sur tout système CISCO vulnérable.

Ce qui signifie que si cette attaque était répétée plusieurs fois cela entrainerait l'interruption complète de la connexion internet de l'entreprise et il faudrait faire un reset du pare feu et le reconfigurer.

- **Exemple 2**

root@pentest:~# cge.pl 196.47.10.1 3

Vulnerability successful exploited with [http://196.47.10.1/level/17/exec/....] ...

Le résultat nous indique que sur les 14 vulnérabilités répertoriées dans l'outil ce routeur est vulnérable à l'attaque 3 (**Cisco IOS HTTP Auth Vulnerability**).

Lorsque le serveur HTTP est activé et que l'autorisation locale est utilisée, il est possible de contourner l'authentification et d'exécuter n'importe quelle commande sur le périphérique Cisco. Cela donne à un utilisateur distant la possibilité d'obtenir un contrôle complet sur le périphérique - toutes les commandes seront exécutées avec le plus haut privilège (niveau 15).

À la mi-2001, Cisco a publié un avis de sécurité concernant une vulnérabilité liée à son serveur HTTP IOS. Cette vulnérabilité (la vulnérabilité d'autorisation HTTP de Cisco IOS) a affecté diverses versions de Cisco IOS de 11.3 à 12.2, fonctionnant sur des douzaines de modèles de routeurs et de commutateurs de Cisco.

c. cisco-auditing-tool

Cet outil permet de tenter de lancer une attaque par dictionnaire en vue de récupérer les mots de passe d'accès sur un équipement CISCO distant sur lequel tourne les services Telnet, SSH, Web, NTP et SNMP.

Syntaxe :

root@pentest:~# CAT -h 196.47.10.1 -p 23 -a /usr/share/wordlists/nmap.lst

Cisco Auditing Tool - g0ne [null0]

Checking Host: 196.47.10.1

Guessing passwords:

problem connecting to "196.47.10.1", port 23: connection timed-out at /usr/share/cisco-auditing-tool/plugins/brute line 7

L'option « -p 23 » représente le port de connexion ici le port 23 pour telnet, on peut aussi faire le test pour le port 445 (https) et 22 (SSH).

d. Cisco torch

Cet outil fait un scan de masse, c'est-à-dire tente de découvrir la présence de service telnet, SSH, Web, NTP et SNMP dans l'objectif d'y lancer une attaque.

root@pentest:~# **cisco-torch -A 196.47.10.1**
Using config file torch.conf...
Loading include and plugin ...

```
#####################################################################
#   Cisco Torch Mass Scanner                #
#   Becase we need it...                        #
#   http://www.arhont.com/cisco-torch.pl                #
#####################################################################
```

List of targets contains 1 host(s)
1786: Checking 196.47.10.1 ...
HUH db not found, it should be in fingerprint.db
Skipping Telnet fingerprint
--->
- All scans done. Cisco Torch Mass Scanner -
---> Exiting.

Au vu du résultat l'on ne voit qu'aucun de ces services mentionnés ne tourne sur le pare feu.

Il faut faire attention pour ne pas activer sur le routeur les services non essentiels car ils pourraient être exploiter par un pirate pour mener une attaque sur le routeur.il faut aussi prendre des mots de passe assez complexes utilisant des caractères spéciaux.

2. Etude des vulnérabilités depuis l'intérieur

a. Scan des vulnérabilités

Pour cette étude des vulnérabilités des machines du réseau, il faut tenter une découverte des machines du réseau.

- **Outil nbtscan**

Syntaxe :

root@pentest:~# nbtscan 192.168.10.1-254

Doing NBT name scan for addresses from 192.168.10.1-254

IP address NetBIOS Name Server User MAC address

- **Outil netdiscover**

On peut aussi utiliser l'outil netdiscover.

Syntaxe :

root@pentest:~# netdiscover -r 192.168.10.0/24

Après avoir découvert les adresses IP des machines du réseau local, on peut passer au scan des ports au niveau des serveurs par exemple.

L'outil par excellence du scan de ports est **nmap**. Mais il existe une version graphique de nmap qui est **zenmap**.

- **Exemple**

root@pentest:~# nmap -O 192.168.10.254

(option -O : Operating System)

Starting Nmap 7.25BETA1 (https://nmap.org) at 2019-05-01 15:18 CET

Nmap scan report for 192.168.10.254

Host is up (0.0013s latency).

Not shown: 998 closed ports

PORT STATE SERVICE

23/tcp open telnet

80/tcp open http

MAC Address: 00:14:F2:6D:2E:89 (Cisco Systems)

Device type: WAP|router

Running: Cisco IOS 12.X

OS CPE: cpe:/h:cisco:aironet_ap350 cpe:/h:cisco:aironet_ap1100 cpe:/h:cisco:aironet_ap1200 cpe:/o:cisco:ios:12.3 cpe:/h:cisco:catalyst_2600

OS details: Cisco Aironet 350, 1100, 1200, or 1131AG WAP; or Cisco 2600 router (IOS 12.3)

Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 2.93 seconds

- **Outil Nessus**

L'un des scanner de vulnérabilités réseau les plus connu est Nessus. Il n'est pas disponible par défaut dans Kali, il faut le télécharger et l'installer.

Pour cela il faudra créer un compte sur le site **tenable.io** pour recevoir dans son mail professionnel un code d'installation, il impératif d'avoir un mail professionnel sinon la création du compte ne sera pas possible.

Après avoir télécharger le paquetage de Nessus, il faut à l'étape d'installation.

Syntaxe :

root@pentest:~# dpkg -i Nessus-7.0.0-debian6_amd64.deb

Suivre les instructions jusqu'à la fin.

Le démarrage du service lié à Nessus ce fait par la commande :

root@pentest:~# /etc/init.d/nessusd start ou **service nessusd start**

La connexion se fait par interface web :

https://127.0.0.1:8834 il faut changer le mot de passe donné lors de l'installation au profit de votre propre mot de passe.

Nessus nous donne alors le choix sur les types de vulnérabilités à rechercher :

1. Info (Simple info sur le système (os, ports ouverts, etc.))
2. Low (Vulnérabilités avec une incidence mineure)
3. Medium (moyen)
4. High (élevée)
5. Critical (critique)

- **Exemple**

Le rapport de scan avec Nessus du SERVEUR nous donne :

	Critique	**Elevée**	**Moyen**	**Bas**	**Info**
Nombre Vulnérabilités trouvés	4	2	8	2	33

b. tentative d'exploitation des vulnérabilités

Si l'on a découvert des potentielles vulnérabilités qui peuvent être utilisées par des personnes malveillantes au cours du scan avec Nessus.

On peut donc tenter d'exploiter ces vulnérabilités, nous utiliserons pour accomplir cette tâche l'outil d'exploitation **Armitage** qui est un Framework graphique de l'outil **Metasploit**.

Voici une explication rapide de l'utilisation de cet outil puissant :

Lancer Armitage, après le lancement faire un clic sur **Host**s > **Add Host**

On peut ajouter ensuite l'adresse IP du serveur, après cela l'ordinateur représentant l'hôte sera chargé dans l'outil.

Pour effectuer le scan faire clic droit sur l'ordinateur ensuite scan. L'outil utilisera les outils comme nmap pour effectuer le scan de ports de la machine.

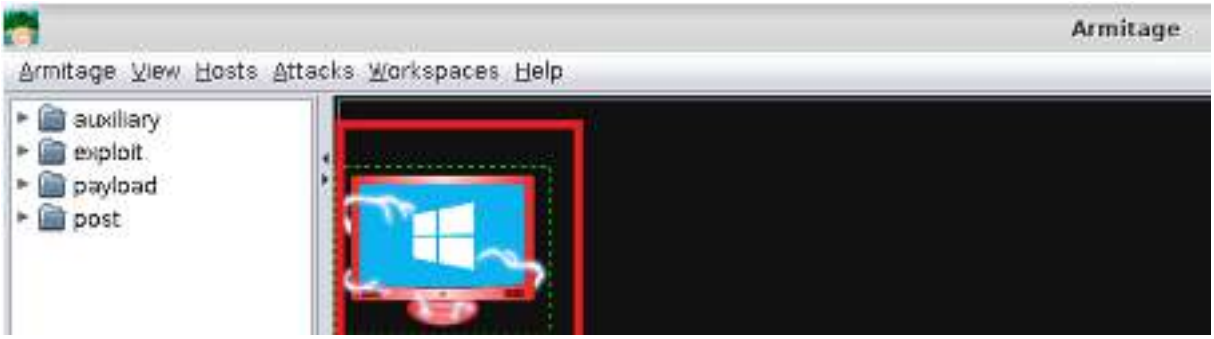
Après le scan on peut passer au lancement des attaques cela se fait par :

Attacks > **Find Attacks**

Armitage procédera au chargement des « payloads » de toutes les attaques possibles sur la cible en utilisant le Framework Metasploit.

Après cela on peut demander à l'outil de choisir la meilleure attaque parmi toutes celles qui a chargé, cela se fait par l'utilisation de l'option **Hail mary**.

Si l'hors de cette exécution on a des éclairs qui apparaissent sur la machine, c'est la preuve que cette machine est exploitable. On peut voir un exemple sur l'image ci-dessous.



Pour tenter une connexion avec cette machine on peut utiliser la bonne option de **Shell** qui apparait ensuite **Interact**.