Metasploit Lab

Présentation

Ce Labtainer explore l'utilisation de l'outil metasploit qui est installé sur un système Kali Linux (attaquant) et est destiné à apprendre des techniques de pénétration simples sur un hôte metasploitable délibérément vulnérable (victime).

Remarque : l'ordinateur de l'attaquant est configuré avec l'adresse IP 192.168.1.3 alors que l'ordinateur victime est 192.168.1.2

Démarrer le laboratoire

Le laboratoire est lancé à partir du répertoire de travail labtainer sur votre hôte sur votre hôte ou votre machine virtuelle Linux. Exécutez la commande:

```
labtainer metasploit
```

Un lien vers le manuel de ce laboratoire sera affiché.
Les terminaux virtuels résultants sont connectés à l'ordinateur de l'attaquant (ubuntu@attacker) et à celui de la victime (ubuntu@victim).
Attention : il va y avoir une phase de téléchargement assez importante (plusieurs Go) et la machine virtuelle demande environ 8 Go de plus.

Tâches

1. Vérifier la connectivité entre l'attaquant et la victime

- Un simple ping depuis l'attaquant vers le système victime sera suffisant.

2. Obtenez une liste des services vulnérables sur la victime

- Un scan de ports 'nmap' de la victime sera suffisant.

NB : Vous constaterez que la machine victime (en réalité une machine metasploitable - cat /etc/issue- a de nombreux ports ouverts, nous allons tenter de voir si les services installés sont vulnérables à l'aide de la console metasploit.

3. Service rlogin configuré de manière vulnérable (port 513)

- Se connecter à distance à la victime avec **rlogin** (avec privilège root)

- Afficher le contenu d'un fichier appartenant au dossier /root

4.Service ingreslock Vulnerable (port 1524)

- Utiliser telnet pour accéder au service *ingreslock* et obtenir le privilège root

- Afficher le fichier appartenant au dossier root comme ci-dessus

- Terminer la connexion telnet

5. Service distccd Vulnerable (port 3632)

- Démarrer la console Metasploit sur l'attaquant

Notez que vous verrez un avertissement au sujet d'une base de données manquante, vous pouvez ignorer cela. WARNING: No database support: No database YAML file

- Rechercher un exploit pour distccd, de quand date-t-il, quel est son Rank ?

NB : le Rank indique les risques d'effets de bord constitutifs à une attaque que vous pourriez infliger à la machine cible. N'oubliez pas que vous vous positionnez en tant que consultant en cybersécurité et que votre but n'est pas de détruire la machine cible mais de contrôler ses vulnérabilités.

- Utiliser l'exploit (à l'aide de la commande *use*)

- Saisir la commande **info** afin d'afficher les détails sur la vulnérabilité exploitable.

- Vous pouvez également afficher uniquement les options relatives à cet exploit à l'aide de la commande **options.**

- Définir l'option 'RHOST' (pour Remote Host) est une variable qui fait référence à l'adresse IP de la machine cible. Nous allons préciser la cible qui est la victime.

- Exécuter l'exploit

Remarque : lorsque l'exploit a réussi, aucune invite n'est affichée, mais un shell est créé, vous pouvez y saisir les commandes souhaitées.

- Vérifier que vous êtes bien sur la machine victime à l'aide de la commande **hostname** qui retourne le nom de la machine sur laquelle nous sommes. Saisissez-la et observez : vous êtes bien chez la victime !

- Afficher le contenu du fichier appartenant au dossier root comme précédemment

- Tapez **Ctrl-C** puis **y** pour sortir de l'exploit et de la console msfconsole.

6. Service IRC daemon Vulnerable (port 6667)

- Démarrer la console Metasploit sur l'attaquant

- Rechercher un exploit pour unreal_ircd, de quand date-t-il, quel est son Rank ?

- Utiliser l'exploit (à l'aide de la commande *use*)

- Visualiser et définir les options (option RHOST), exécuter l'exploit et afficher le nom de l'hôte et le fichier appartenant au dossier root comme précédemment.

Remarque : lorsque l'exploit a réussi, aucune invite n'est affichée, mais un shell est créé, vous pouvez y saisir les commandes souhaitées.

- Quittez la victime et sortez de la console metasploit.

7. Service VSFtpd Vulnerable (port 21)

- Relancer la console Metasploit sur l'attaquant
- Rechercher un exploit pour vsftpd, de quand date-t-il, quel est son Rank ?
- Utiliser l'exploit (à l'aide de la commande *use*)
- Visualiser et définir les options (option RHOST), exécuter l'exploit et afficher le nom de l'hôte et le fichier appartenant au dossier root comme précédemment.
- Quittez la victime et sortez de la console metasploit.

8. Service Samba Vulnerable (port 139)

- Relancer la console Metasploit sur l'attaquant
- Rechercher un exploit pour samba usermap_script
- Utiliser l'exploit (à l'aide de la commande *use*)
- Visualiser et définir les options (option RHOST), exécuter l'exploit et afficher le nom de l'hôte et le fichier appartenant au dossier root comme précédemment.
- Quittez la victime et sortez de la console metasploit.

9. Service HTTP (php) Vulnerable (port 80)

- Relancer la console Metasploit sur l'attaquant
- Rechercher un exploit pour php_cgi
- Utiliser l'exploit (à l'aide de la commande *use*)
- Visualiser et définir les options (option RHOST), exécuter l'exploit

Remarque *: lorsque l'exploit est réussi, une invite « meterpreter» est affichée, vous pouvez lancer un shell dans cette invite*

- De l'invite meterpreter, taper la commande **shell,** afficher le nom de l'hôte et le fichier appartenant au dossier root comme précédemment.
- Quittez la victime et sortez de la console metasploit.

Arrêter le labtainer

Lorsque le laboratoire est terminé, ou si vous souhaitez arrêter de travailler pendant un certain temps, dans le terminal qui vous a permis de le lancer, exécutez : stoplab

Vous pouvez toujours redémarrer le Labtainer et continuer votre travail. Lorsque le Labtainer est arrêté, un fichier zip est créé et copié dans un emplacement affiché par la commande « stoplab ». Une fois le laboratoire terminé, vous pouvez envoyer ce fichier zip au formateur pour correction éventuelle.