Revues des bases:

- Nmap

Nmap est un outil gratuit, open source et puissant utilisé pour découvrir les hôtes et les services sur un réseau informatique. Dans notre exemple, nous utilisons Nmap pour analyser cette machine afin d'identifier tous les services exécutés sur un port particulier. Nmap a de nombreuses fonctionnalités ; un tableau résume certaines de ses fonctionnalités ci-dessous.

Drapeau Nmap	Description
-sV	Tente de déterminer la version des services en cours d'exécution
-p <x> ou -p-	Analyser le port <x> ou analyser tous les ports
-Pn	Désactiver la découverte d'hôte et rechercher les ports ouverts, bref désactive le ping
-UN	Permet la détection du système d'exploitation et de la version, exécute des scripts intégrés pour une énumération plus poussée
-sC	Scannez avec les scripts Nmap par défaut
-v	Mode verbeux
-sU	Analyse des ports UDP
-sS	Analyse du port TCP SYN

- GOBUSTER

Gobuster est un outil permettant de forcer les URI (répertoires et fichiers), les sous-domaines DNS et les noms d'hôtes virtuels. Pour cette machine, nous allons nous concentrer sur son utilisation pour forcer les répertoires. Téléchargez Gobuster ici , ou si vous utilisez Kali Linux, exécutez `sudo apt-get install gobuster`.

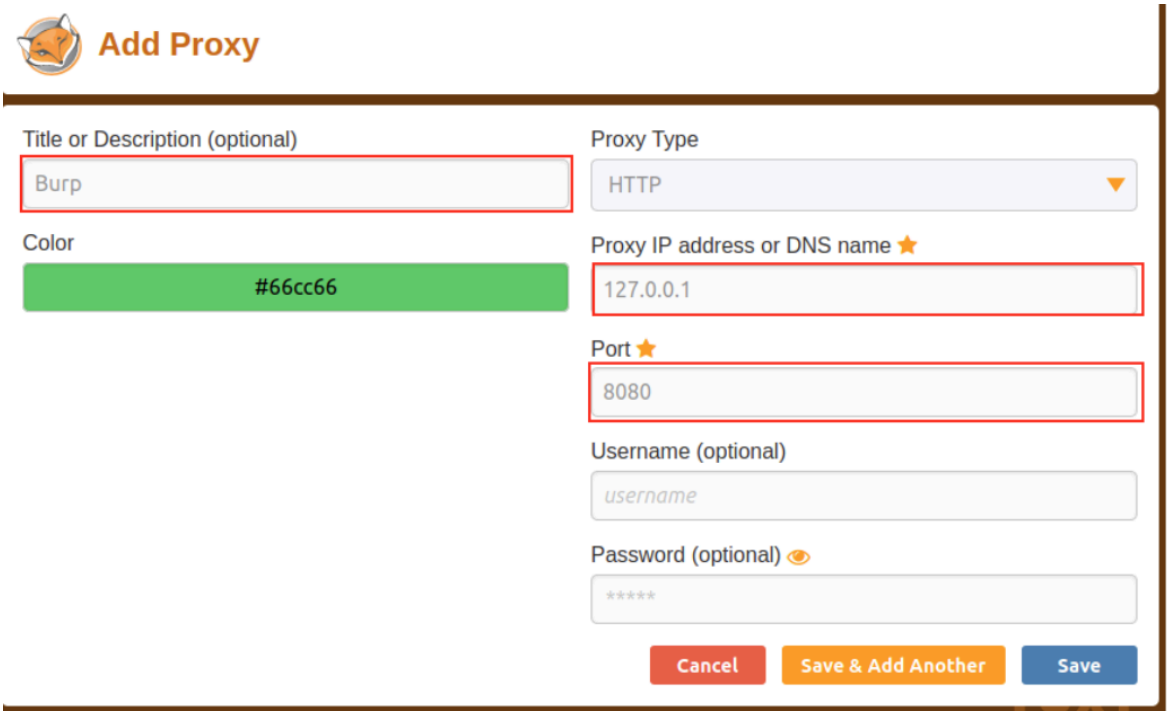
Pour commencer, vous aurez besoin d'une liste de mots pour Gobuster (qui sera utilisée pour parcourir rapidement la liste de mots afin d'identifier si un répertoire public est disponible. Si vous utilisez Kali Linux , vous pouvez trouver de nombreuses listes de mots sous `/usr/share/wordlists`. Vous pouvez également utiliser la liste de mots pour les répertoires situés à `/usr/share/wordlists/dirbuster/directory-list-1.0.txt` dans l'AttackBox.

Exécutons maintenant Gobuster avec une liste de mots en utilisant `gobuster dir -u http://10.10.199.138:3333 -w`.

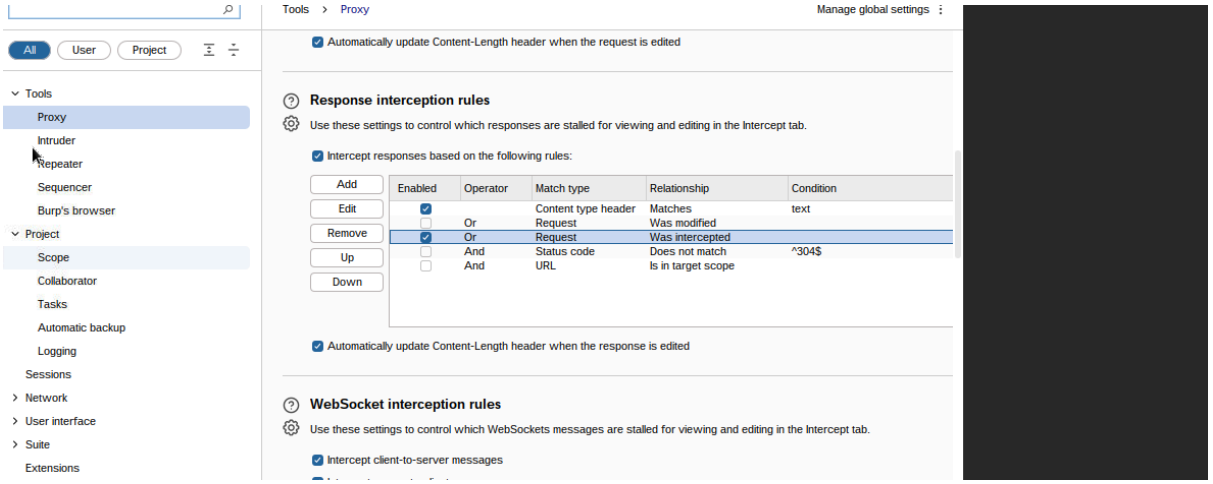
Drapeau Gobuster	Description
-x -k	L'un pour spécifier les extensions et l'autre pour eviter la resolution dns
-u	L'URL cible
-w	Chemin vers votre liste de mots
-U et -P	Nom d'utilisateur et mot de passe pour l'authentification de base
-p <x>	Proxy à utiliser pour les requêtes
-c < cookies http >	Spécifiez un cookie pour simuler votre authentification

Burpsuite:

pour le foxyproxy,



pour recuperer les reponses serveurs :



Compromettre un web serveur :

Utiliser burpsuite pour tester par exemple un fichier php avec différentes extensions grace à l'intruder: exemple de cas: Nous allons utiliser Intruder (utilisé

akobi banconlé

pour automatiser les attaques personnalisées). Pour commencer, créez une liste de mots avec les extensions suivantes :

- . php
- .php3
- .php4
- .php5
- .phtml

Maintenant, assurez-vous que BurpSuite est configuré pour intercepter tout le trafic de votre navigateur. Téléchargez un fichier ; une fois cette requête capturée, envoyez-la à l'intrus. Cliquez sur " `Payloads`" et sélectionnez le `Sniper`type d'attaque " ".

Cliquez maintenant sur l' `Position`onglet « s », recherchez le nom du fichier et « `Add §`» pour l'extension.

Passons au reverse shell dès qu'on sait quel fichier peut etre soumis qu'on va retrouver dans les uploads (vu qu'on avait identifié le repertoire avec le dirbuster) il faut juste telecharger un shell(un code php par exemple qui va permettre d'établir la connexion avec ma machine)
Attention à editer le code en y mettant la bonne ip et le bon port.

ensuite on soumet le fichier bien sur en ayant mis au prealable ma machine en ecoute avec netcat : nc -lnvp port.

puis je lance le fichier malware depuis le navigateur et bingo

ma commande préféré pour chercher .
find / -type f -user root -perm [4000par exemple pour le SUID] -exec [commande à traiter sur la sortie standard] {}\;