

Revue 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 <u>Nmap</u>	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 <u>du système d'exploitation</u> et de la version, exécute des scripts intégrés pour une énumération plus poussée
-sC	Scannez avec les scripts <u>Nmap par défaut</u>
-v	Mode verbeux
-sU	Analyse des ports <u>UDP</u>
-sS	Analyse du port <u>TCP SYN</u>

- 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 <u>Gobuster</u>	Description
-x -k	L'un pour spécifier les extensions et l'autre pour éviter la résolution 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>	<u>Proxy</u> à utiliser pour les requêtes
-c < cookies <u>http</u> >	Spécifiez un cookie pour simuler votre authentification

Burpsuite:
pour le foxyproxy,



Add Proxy

Title or Description (optional)

Burp

Proxy Type

HTTP

Color

#66cc66

Proxy IP address or DNS name ★

127.0.0.1

Port ★

8080

Username (optional)

username

Password (optional) 👁

Cancel

Save & Add Another

Save

pour recuperer les reponses serveurs :

The screenshot shows the Burp Suite interface. On the left, the 'Tools' menu is open, and 'Proxy' is selected. The main panel displays the 'Response interception rules' configuration. The 'Intercept responses based on the following rules:' section is active, showing a table of rules. The first rule is enabled and has the operator 'Or' and match type 'Content type header'. The second rule is also enabled and has the operator 'Or' and match type 'Request'. The third rule is disabled and has the operator 'And' and match type 'Status code'. The fourth rule is disabled and has the operator 'And' and match type 'URL'. The 'Relationship' column shows 'Matches' for the first rule, 'Was modified' for the second, 'Does not match' for the third, and 'Is in target scope' for the fourth. The 'Condition' column shows 'text' for the first rule and '^304\$' for the third rule. The 'WebSocket interception rules' section is also visible below.

Enabled	Operator	Match type	Relationship	Condition
<input checked="" type="checkbox"/>	Or	Content type header	Matches	text
<input checked="" type="checkbox"/>	Or	Request	Was modified	
<input type="checkbox"/>	And	Status code	Does not match	^304\$
<input type="checkbox"/>	And	URL	Is in target scope	

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

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

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

```
[root:/tmp]# cat phpext.txt
.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 être soumis qu'on va retrouver dans les uploads (vu qu'on avait identifié le répertoire avec le dirbuster) il faut juste télécharger un shell (un code php par exemple qui va permettre d'établir la connexion avec ma machine)

Attention à éditer le code en y mettant la bonne ip et le bon port.

ensuite on soumet le fichier bien sûr en ayant mis au préalable ma machine en écoute avec netcat : nc -lnvp port.

puis je lance le fichier malware depuis le navigateur et bingo

ma commande préférée pour chercher .

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