CYBERSECURITÉ HOMELAB

GOBUSTER

Projet

Janie Sarrazin

Cybersecurity-homelab_01_Gobuster

5 septembre 2025

Objectif:

Découvrir des pages cachées (ou non protégées) d'un site web

Sous-objectif :

Mettre en place un home lab en cybersécurité avec :

- Une VM Ubuntu Server (cible), hébergeant Apache et des répertoires cachés.

- Une VM Kali Linux (attaquante), pour utiliser Gobuster et découvrir ces répertoires.

- Documenter toutes les étapes, difficultés, solutions et apprentissages.

- **Outils utilisés**
    1. Virtualbox (gestionnaire de machine virtuelle)
    2. Ubuntu Server 22.04 (cible)
    3. Kali-linux (attaquant)

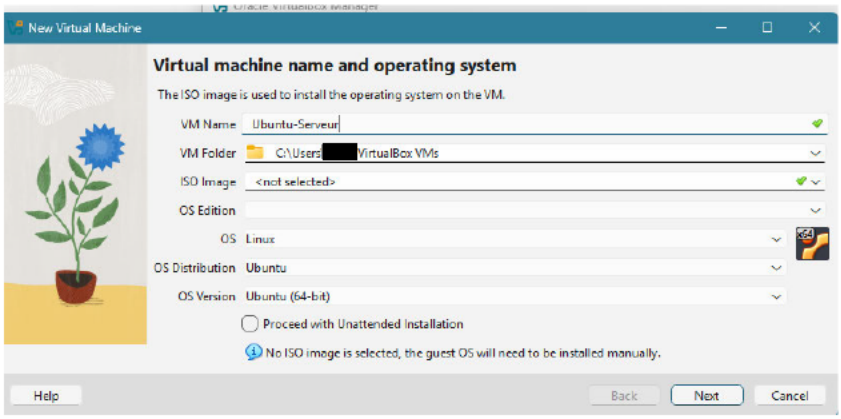
- **Étapes :**

1. Installation d'Ubuntu Server

- Téléchargement ISO. https://ubuntu.com/download/server?utm

- Installation en VM. (virtual box)

Configuration :



- **Mémoire (RAM)** : minimum 2 Go (2048 MB), 4 Go si tu peux.
- **Processeurs** : 2 (si ton PC le permet).
- **Disque dur** :
  - Crée un disque virtuel de 20–30 Go (VDI, dynamique).
- **Réseau** :
  - Pour un home lab → mets **"Réseau interne"** (Internal Network) si tu veux isoler la VM.
  - Ou **NAT** si tu veux qu'elle ait accès à Internet.

- Choix du partitionnement → LVM active.

- Creation Utilisateur et mot de passe.

- Installation optionnelle d'OpenSSH : non, pas pour toute suite

2. Configuration du réseau

- Problème initial : Kali ne voyait pas Ubuntu via NAT.

- Solution : ajout d'un Adapter 2 (Host-only) sur les deux VMs.

- Ubuntu n'avait pas d'IP Host-only → utilisation de `sudo dhclient enp0s8` puis configuration via Netplan.

- Vérification : `ping` entre Kali et Ubuntu fonctionne

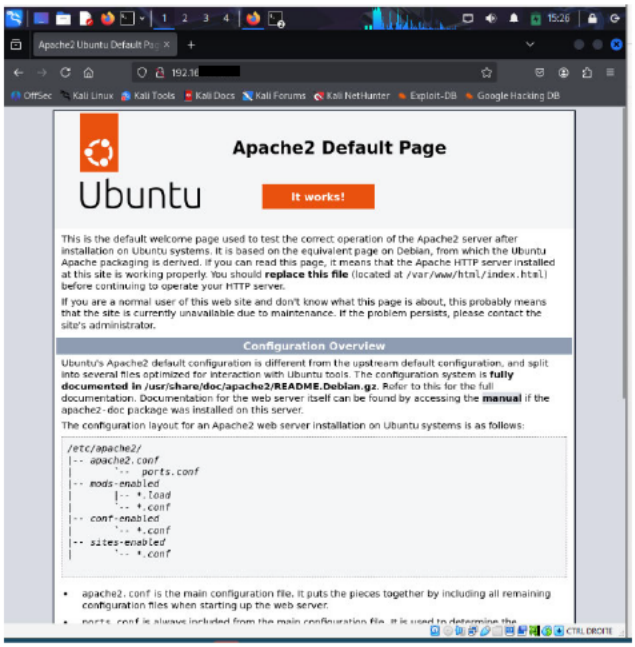
3. Installation et configuration d'Apache sur Ubuntu

Commande :

```
sudo apt update && sudo apt install apache2 -y
```

- Test avec `curl http://localhost` → page Apache par défaut.

- Accès depuis Kali : `http://192.xxx.xx.xx` → page Apache visible dans Firefox.



À ce stade, tu as un Ubuntu fonctionnel dans VirtualBox, prêt à être utilisé comme **serveur cible** pour tes labs (Gobuster, Nmap, etc.).

4. Création des répertoires cachés

```
sudo mkdir /var/www/html/admin
sudo mkdir /var/www/html/backup
sudo mkdir /var/www/html/test123
echo "Page admin secrète" | sudo tee /var/www/html/admin/index.html
echo "Backup du site" | sudo tee /var/www/html/backup/backup.txt
echo "Zone de test" | sudo tee /var/www/html/test123/index.html
```

5. Utilisation de Gobuster depuis Kali

- Problème : wordlist introuvable.

- Solution : installation du paquet `wordlists` + création d'une wordlist perso :

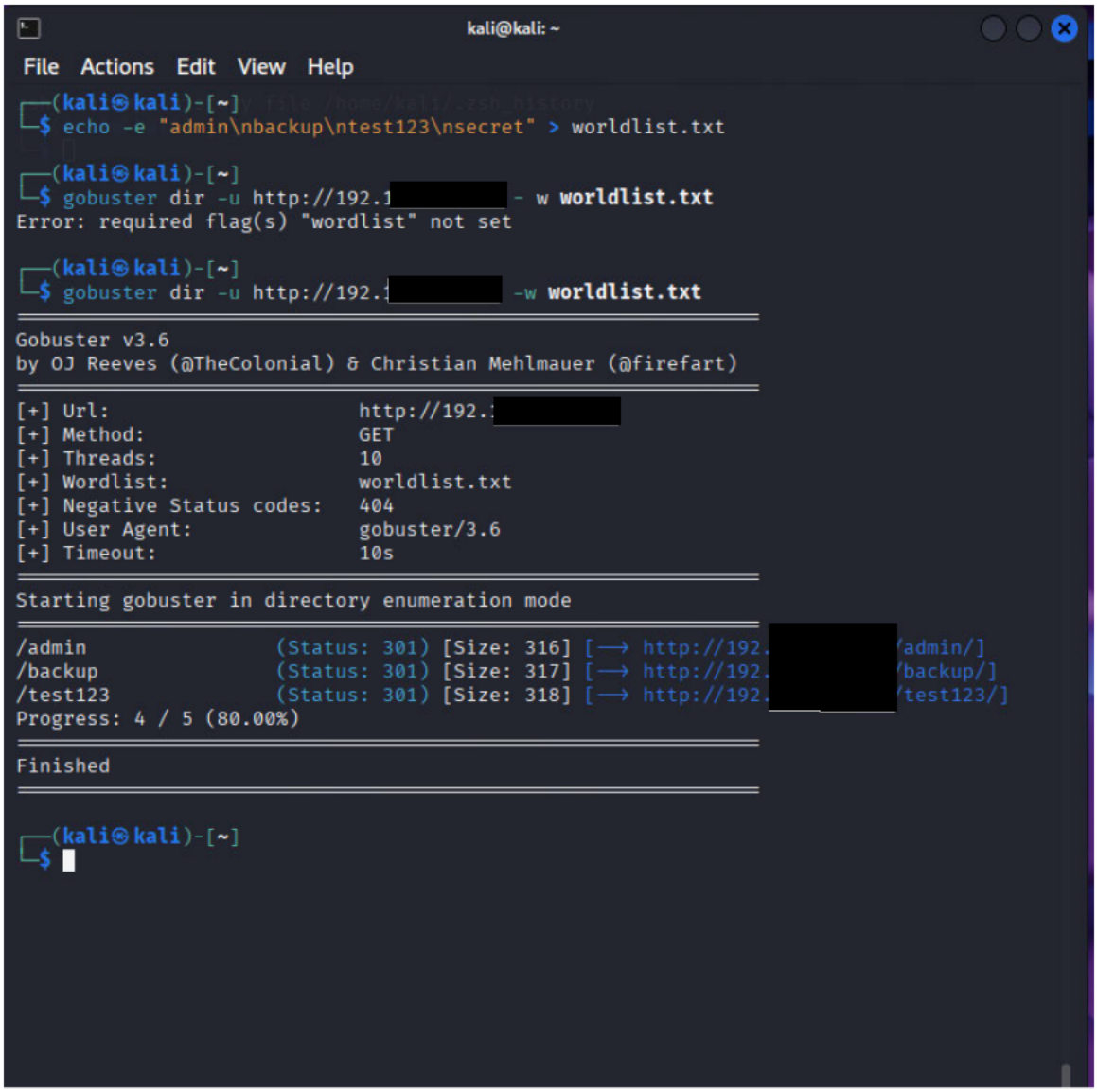
```
echo -e "admin\nbackup\ntest123\nsecret" > wordlist.txt
```

Commande finale réussie :

gobuster dir -u http://192.XXX.XXX.XXX -w wordlist.txt

Résultats :

```
/admin   (Status: 301)
/backup  (Status: 301)
/test123 (Status: 301)
(/secret non trouvé, normal car inexistant).
```


kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ echo -e "admin\nbackup\ntest123\nsecret" > worldlist.txt
(kali㉿kali)-[~]
$ gobuster dir -u http://192.1 - w worldlist.txt
Error: required flag(s) "wordlist" not set
(kali㉿kali)-[~]
$ gobuster dir -u http://192.1 -w worldlist.txt
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
[+] Url: http://192.
[+] Method: GET
[+] Threads: 10
[+] Wordlist: worldlist.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
Starting gobuster in directory enumeration mode
/admin (Status: 301) [Size: 316] [→ http://192. /admin/]
/backup (Status: 301) [Size: 317] [→ http://192. /backup/]
/test123 (Status: 301) [Size: 318] [→ http://192. /test123/]
Progress: 4 / 5 (80.00%)
Finished
(kali㉿kali)-[~]
$

Difficultés rencontrées & solutions

1. Problème de réseau (NAT seulement) → Solution : ajout Host-only Adapter.

2. Ubuntu sans IP sur enp0s8 → Solution : `dhclient` puis Netplan.

(programme qui permet a la machine d'obtenir une adresse IP depuis un serveur DHCP)

3. Apache non atteignable depuis Kali → Solution : utiliser IP Host-only (192.XXX.XX.XXX).

4. Wordlist manquante pour Gobuster → Solution : installation de `wordlists` et création d'une wordlist perso.

5. Erreur de syntaxe *(Espace)* Gobuster (- w au lieu de -w) → Solution : correction commande.

Apprentissages (notes additionnelles)

- sudo → exécuter avec privilèges root.

- ip a → afficher interfaces réseau.

- NAT vs Host-only → NAT pour Internet, Host-only pour VM ↔ VM.

- Gobuster : -u = URL, -w = wordlist.

- Wordlist = trousseau de clés testés par Gobuster. (mots commum comme : /admin, /login, /config) etc.

*il existe d'autre répertoire plus grand, aucune worldlist n'est parfaite. Ceci /sfpee34 ou /janie ne fonctionnerait pas.

- Codes HTTP : 200=OK, 301=redirigé, 403=interdit, 404=non trouvé.

- Importance de documenter erreurs et solutions.

Conclusion

Ce premier lab maison a permis de :

- Monter un environnement d’attaque/défense réaliste.
- Découvrir le rôle des wordlists dans la reconnaissance web.
- Comprendre la gestion réseau dans VirtualBox.
- Apprendre à interpréter les résultats de Gobuster.

Dans la réalité, Gobuster est illégale sans l'autorisation du propriétaire du site web mais il suffit donc d'entrer le code dans linux pour accéder à des pages cachées (ou non protégées) d'un site web.