Belphegore

Présentation de l'Outil `Belphegore`

2.1. Description Générale

`Belphegore` est un **script shell interactif**, basé sur un **menu CLI** (Command Line Interface), qui automatise :

- l'installation des outils nécessaires,
- l'accès rapide à des fonctionnalités de test réseau,
- l'initiation à des techniques d'analyse offensive/défensive.

2.2. Structure Modulaire

L'outil est divisé en **quatre grands modules** :

1. **Scanner & Surveillance réseau**
2. **Écoute & Sniffing**
3. **Attaques réseau (offensives)**
4. **Défense & Sécurité réseau**

Chacun de ces modules propose des sous-fonctions accessibles par menu.

Fonctionnalités Détaillées

3.1. Vérification & Installation des Dépendances

Au lancement, le script vérifie la présence des outils suivants (et les installe si nécessaire) :

- **Analyse réseau** : `nmap`, `arp-scan`, `tshark`, `tcpdump`, `ss`
- **Pentesting** : `hping3`, `ettercap`, `netcat`
- **Défense** : `fail2ban`, `chkrootkit`, `iptables`
- **Outils Python** : `pip3`, `shodan` (via `pip` avec API Key)

Particularité : Si la clé API Shodan n'est pas trouvée, le script en demande une à l'utilisateur.

Menu 1 – Scanner Réseau

- **Scan Shodan** : interrogation de l'API publique avec mots-clés.
- **Scan local Nmap** : scan syn lent et fragmenté (évitant les IDS).
- **ARP-scan** : détection des machines sur le réseau local.
- **Ping Sweep personnalisé** : balayage d'un sous-réseau donné.

Menu 2 – Sniffing & Surveillance

- **Tcpdump** : capture de tout le trafic réseau (non filtré).
- **Tshark** : analyse temps réel, arrêt automatique après 10 Go.
- **ss** : affichage des connexions réseau actives.
- **who** : liste des utilisateurs connectés au système.

Menu 3 – Attaques Réseau (à utiliser dans un cadre légal)

- **SYN Flood** : simulation d'une attaque DoS sur une cible.
- **Bruteforce FTP** : scan par script Nmap de mot de passe FTP.
- **MITM** : lancement d'Ettercap en mode graphique.
- **Port Knocking** : (fonctionnalité non encore implémentée).

Ces fonctions sont à **n'utiliser que dans un environnement de test ou lab autorisé**.

Menu 4 – Défense Réseau

- **Fail2ban** : démarrage du service de bannissement.

- **Blocage IP** : ajout dynamique de règles `iptables`.
- **Chkrootkit** : détection des rootkits.
- **Afficher les règles** `iptables` en vigueur.

Avantages de l'Outil

Point fort	Détail
Simplicité d'usage	Menu textuel clair, même pour débutant
Automatisation	Vérification & installation des outils
Formation	Permet d'expérimenter de vrais outils pro
Polyvalence	Offensive, défensive, analyse réseau
Adaptabilité	Script modifiable facilement

Limites & Améliorations Possibles

Limite	Suggestion d'amélioration
Absence de logs	Ajouter un fichier `belphegore.log`
Aucune vérification des IP	Utiliser des regex ou `ipcalc`
Port knocking absent	Implémenter un enchaînement de ports via `iptables`
Aucune confirmation sur actions sensibles	Ajouter des prompts de confirmation
Commandes longues non interruptibles	Proposer des durées ou des filtres

Annexes

- **Liste des outils utilisés :**

  `nmap`, `arp-scan`, `tshark`, `tcpdump`, `ss`, `fail2ban`, `chkrootkit`, `hping3`, `ettercap`, `iptables`, `shodan`, `who`, `netcat`

- **Prérequis système :**
  - Système Linux (Ubuntu/Debian conseillé)
  - Droits `sudo` pour les commandes système
  - Connexion Internet pour installation & Shodan

https://imgur.com/a/AHVRcSS