

REPUBLIQUE DU SENEGAL



Un peuple - un but - une foie

GROUPE
ISI

Institut - Supérieur - d'informatique

Installation et utilisation de RECON - NG sur Kali Linux

Présenté par : Jude BELA

REC  **N-ng**



KALI LINUX

SOMMAIRE

-  INTRODUCTION
-  INSTALLATION
-  CONFIGURATIONS
-  TESTS

REC N-ng

Recon-NG est un outil open source destiné à la reconnaissance et à la collecte d'informations OSINT. Avec une interface modulaire en ligne de commande, il automatise l'extraction de données, comme les domaines et adresses IP, pour des analyses précises et rapides.

■ Avantages

Recon-NG offre plusieurs avantages, notamment l'automatisation des tâches de collecte d'informations, ce qui le rend rapide et efficace, ainsi que sa modularité qui permet une personnalisation selon les besoins. Il génère également des rapports détaillés pour une analyse approfondie et dispose d'une interface en ligne de commande intuitive, adaptée même aux débutants motivés.

■ Inconvegnants

Recon-NG, bien qu'efficace, peut présenter des défis tels qu'une courbe d'apprentissage élevée pour les débutants, une dépendance aux modules nécessitant des configurations spécifiques, et des résultats limités par les sources accessibles. De plus, son statut open source peut exiger des mises à jour et une maintenance régulières.

AVANTAGES & INCONVEGNANTS



CONFIGURATIONS

3. marketplaces create ims_computers

- Rôle : Crée un nouveau workspace (espace de travail) nommé ims_computers.

4. marketplaces search ssl

- Rôle : Recherche les modules disponibles liés au mot-clé ssl dans la marketplace de recon-ng.

5. marketplaces info ssl

- Rôle : Affiche des détails sur un module qui contient ssl dans son nom.

```
jude@jb: ~  
Fichier Actions Éditer Vue Aide  
[recon-ng][default] > workspaces create ims_computers  
[recon-ng][ims_computers] > marketplace search ssl  
[*] Searching module index for 'ssl' ...  
  
+-----+-----+-----+-----+-----+-----+-----+-----+  
| Path | Version | Status | Updated | D | K |  
+-----+-----+-----+-----+-----+-----+-----+-----+  
| recon/domains-hosts/ssl_san | 1.0 | not installed | 2019-06-24 | | |  
| recon/hosts-hosts/ssltools | 1.0 | not installed | 2019-06-24 | | |  
| recon/ports-hosts/ssl_scan | 1.1 | not installed | 2021-08-24 | | |  
+-----+-----+-----+-----+-----+-----+-----+-----+  
  
D = Has dependencies. See info for details.  
K = Requires keys. See info for details.  
  
[recon-ng][ims_computers] > marketplace info ssl  
  
+-----+-----+-----+-----+-----+-----+-----+-----+  
| path | recon/domains-hosts/ssl_san |  
| name | SSL SAN Lookup |  
| author | Zach Grace (@ztgrace) zgrace@403labs.com and Bryan One1 (@BryanOne186) onel@oneleet.com |  
| version | 1.0 |  
| last_updated | 2019-06-24 |  
| description | Uses the ssltools.com API to obtain the Subject Alternative Names for a domain. Updates the 'hosts' table with the results. |  
| required_keys | [] |  
| dependencies | [] |  
| files | [] |  
| status | not installed |  
+-----+-----+-----+-----+-----+-----+-----+-----+  
  
+-----+-----+-----+-----+-----+-----+-----+-----+  
| path | recon/hosts-hosts/ssltools |  
| name | SSLTools.com Host Name Lookups |  
| author | Tim Maletic (borrowing from the ssl_san module by Zach Graces) |  
| version | 1.0 |  
+-----+-----+-----+-----+-----+-----+-----+-----+
```

TESTS

6. option set SOURCE imscomputers.com

- Rôle : Définit la source de données (dans ce cas, un nom de domaine) pour le module à exécuter.

7. info

- Rôle : Affiche les informations sur le module actuellement sélectionné.

8. input

- Rôle : Permet d'entrer manuellement des données dans la base de données de recon-ng.

```
jude@jb: ~
Fichier Actions Éditer Vue Aide
[recon-ng][ims_computers][hackertarget] > options set SOURCE imscomputers.com
SOURCE => imscomputers.com
[recon-ng][ims_computers][hackertarget] > info

Name: HackerTarget Lookup
Author: Michael Henriksen (@michenriksen)
Version: 1.1

Description:
Uses the HackerTarget.com API to find host names. Updates the 'hosts' table with the results.

Options:
Name      Current Value      Required  Description
-----
SOURCE    imscomputers.com   yes       source of input (see 'info' for details)

Source Options:
default      SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
<string>    string representing a single input
<path>      path to a file containing a list of inputs
query <sql> database query returning one column of inputs

[recon-ng][ims_computers][hackertarget] > input

+-----+
| Module Inputs |
+-----+
| imscomputers.com |
+-----+

[recon-ng][ims_computers][hackertarget] > █
Stories
Company
News
```

TESTS

```
jude@jb: ~
Fichier Actions Éditer Vue Aide
SOURCE imscomputers.com yes source of input (see 'info' for details)

Source Options:
default SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
<string> string representing a single input
<path> path to a file containing a list of inputs
query <sql> database query returning one column of inputs

[recon-ng][ims_computers][hackertarget] > input

+-----+
| Module Inputs |
+-----+
| imscomputers.com |
+-----+

[recon-ng][ims_computers][hackertarget] > run

-----
IMSCOMPUTERS.COM
[*] Country: None
[*] Host: imscomputers.com
[*] Ip_Address: 193.203.239.72
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----
[*] Country: None
[*] Host: mail.imscomputers.com
[*] Ip_Address: 185.135.132.69
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----

SUMMARY
[*] 2 total (2 new) hosts found.
[recon-ng][ims_computers][hackertarget] > █
```

9. run

- Rôle : Exécute le module actuellement chargé.

MERCI POUR VOTRE ATTENTION



Présenté par :

Jude BELA étudiant L2 RI ISI GROUPE

 +221 78 305 26 04

 judebela@imscomputers.com

 www.imscomputers.com