2025

DOCUMENTATION TECHNIQUE - NIKTO

Présenté par :

ZOUAOUI Mehdi

2024

SOMMAIRE

1. Introduction à Nmap.....Page 1

2. Installation de Nikto.....Page 2

3. Mettre à jour les Pluggins de Nikto.....Page 2

4. Utilisation de Nikto.....Page 2-3

5. Utilisation derrière un proxy.....Page 3

6. Conclusion.....Page 4

2024

DOCUMENTATION TECHNIQUE NIKTO

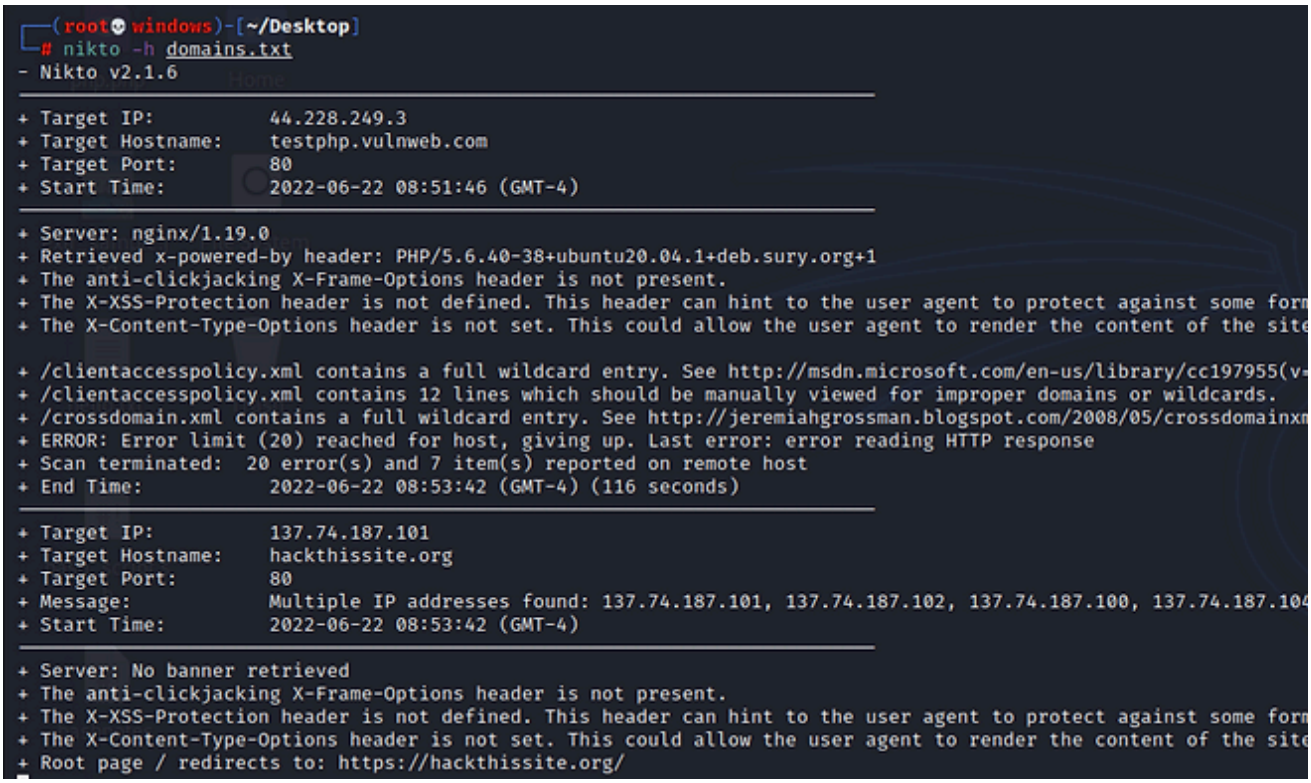
1. Introduction à Nikto

Nikto c'est quoi ?

Nikto est un scanner de vulnérabilités web en open-source, utilisé dans les tests d'intrusion pour analyser les serveurs web. Il permet de détecter rapidement des failles connues, des mauvaises configurations, et des comportements suspects sur les services HTTP/HTTPS.

Il peut notamment identifier :

- **Fichiers dangereux ou obsolètes.**
- **Scripts vulnérables.**
- **Pages d'administration accessibles.**
- **Bannières d'information révélant la version du serveur.**
- **Problèmes SSL/TLS.**



DOCUMENTATION TECHNIQUE NIKTO

2. Installation de Nikto

ArchLinux / Manjaro :

yaourt -S nikto

Ubuntu / Linux Mint :

sudo apt-get install nikto

3. Mettre à jour les Pluggins de Nikto

Dès l'installation de Nikto est terminée, il faut mettre à jour les pluggins :

sudo nikto -update

4. Utilisation de Nikto

Pour lancer un simple scan :

nikto -h [URL]

- *[URL]= l'url de votre choix. A savoir, par défaut Nikto scanne sur le port 80.*

Scanner sur le port 443 :

nikto -h [URL] -p 443

ou

nikto -h https://[URL]:443/

DOCUMENTATION TECHNIQUE NIKTO

Scanner sur plusieurs port à la fois :

nikto -h [URL] -p 20,21,25,443

5. Utilisation derrière un proxy

pour pouvoir utiliser nikto derrière un proxy, il faut éditer son fichier de configuration :

ArchLinux / Manjaro :

sudo nano /usr/share/nikto/nikto.conf

Ubuntu / Linux Mint :

sudo nano /etc/nikto/config.conf

Préciser le proxy :

```
# Proxy settings -- still must be enabled by -useproxy
PROXYHOST=proxy.domaine.tld
PROXYPORT=8080
#PROXYUSER=proxyuserid
#PROXYPASS=proxypassword
```

- *PROXYHOST: l'url ou l'IP du serveur proxy*
- *PROXYPORT: le port du proxy*
- *PROXYUSER: l'utilisateur si besoin*
- *PROXYPASS: le mot de passe de l'utilisateur si besoin*

Utilisation de Nikto derrière un proxy :

nikto -h [URL] -useproxy

exemple :
nikto -h http://[URL]:443/ -F txt -o scan.txt -useproxy

- *Nikto ira scanner l'url sur le port 443 en passant par un proxy et envoyer le résultat dans le fichier scan.txt.*

DOCUMENTATION TECHNIQUE NMAP

6. Conclusion

Nikto est un programme très pratique pour scanner les failles de sécurité de son serveur web et son exécution est assez rapide (suivant l'architecture matériel de l'hôte).

Par contre, attention aux petits malins qui voudraient utiliser Nikto pour scanner les sites web des copains (ou pas) pour leur faire une mauvaise farce en détectant une ou plusieurs failles de sécurités sur le site web, Nikto est repérable dans les logs et évidemment avec l'IP de celui qui scanne