TD

Recherche d'Informations en Source Ouverte

2 janvier 2023

1 Scans actifs

I. (3 points) **Scans nmap : Application sur un serveur présent sur Internet**

(1) À partir de l'outil `nmap` et des options `-n -sn`, déterminez si l'hôte d'adresse IP 164.132.172.108 est fonctionnel ou non :

- Quelles sont les options passées à l'outil ? À quoi servent-elles ?
- Quelle technique utilise `nmap` pour détecter un hôte ?
  - Par rapport à ce qui a été vu en cours, avec des serveurs directement accessibles sur le réseau local, quelle différence observez-vous au niveau de la technique de détection utilisée ?
  - Vous pouvez observer les paquets échangés graphiquement à partir de l'outil `wireshark` (installation à partir de la commande `apt install wireshark`)

II. (4 points) **Scan nmap : découverte des services sur le système ciblé !**

(1) Détecter les ports ouverts/fermés/filtrés sur le système d'adresse IP 164.132.172.108 !

- Pour les ports TCP :
  - `nmap -n -sS -PN 164.132.172.108`
- Pour les ports UDP :
  - `nmap -n -sU -PN 164.132.172.108`

(2) À partir de captures wireshark, quelle différence pouvez-vous noter entre ces deux protocoles ?

(3) Quelle différence y a-t-il entre UDP et TCP pour découvrir un service présent sur une cible ? Qu'est-ce que cela implique lors de la découverte des services des cibles présentes ?

(4) Doit-on scanner l'ensemble des ports TCP/UDP (0→65535) ?

- Quelle stratégie peut-on mettre en place pour gagner en efficacité ?
- À quel compromis ?
- Quelle option fournissez-vous donc à `nmap` ?

III. (4 points) **Scan nmap : identifier les services accessibles**

(1) Identifiez les services accessibles fonctionnant sur les ports découverts précédemment !

- `nmap -sV -p ports 164.132.172.108`, remplacez `ports` par les ports déjà détectés comme accessibles !

(2) Est-il possible de connaitre les versions de ces services ?

(3) Certains de ces services / systèmes sont-ils vulnérables ?
- Scripts NSE (*nmap scripting engine*) :
  - `--script "not intrusive"`
  - `--script "default and safe"`
  - `--script "(default or safe) and http-*"`

Les scripts sont accessibles dans les répertoires de `nmap` où ils peuvent être analysés
- Par exemple : `ls /usr/share/nmap/scripts/http-*`

2 Récupération d'informations publiques

IV. (3 points) **Informations de premier niveau**

(1) Récupérez l'adresse IP des sites :
- `http://ensta.fr`,
- `https://cours.pelicanux.net`.

(2) À quoi sert l'outil `whois` ? Quelles informations permet-il de récupérer ?

(3) À partir de cet outil, déterminez :
- Les contacts administratifs
- Le réseau dans lequel l'IP du site est située

(4) À quoi sert l'outil `dig` ?

(5) À partir de cet outil, pour chacun de ces domaines, déterminez :
- Les serveurs DNS permettant la résolution domaine ↔ IP,
- Les serveurs de mails permettant de recevoir les courriels.

V. (4 points) **Shodan !**

(1) Rendez-vous sur le site `https://shodan.io`. À partir des résultats précédents, déterminez les versions et les services utilisés sur les adresses obtenues !

(2) Concernant l'adresse 164.132.172.108, retrouvez-vous les résultats obtenus de manière active ? Quelle(s) différence(s) avez-vous pu noter ?

VI. (2 points) **Google dorks !**

(1) Rechercher les fichiers présents sur le site de votre école :
- de type PDF,
- de type Word (doc, docx, xls, xlsx)
- de type text
- de type php

(2) De nouveaux liens peuvent-ils être intéressants dans le cadre d'un test d'intrusion ?

(3) Ces requêtes permettent-elles de découvrir des informations sensibles (fichiers de sauvegarde, fichiers contenant des mots de passe) ?