Atelier 3 : Reconnaissance

Dans cet atelier, vous allez faire une « reconnaissance » de l'Université Cheikh Anta Diop de Dakar (UCAD) en utilisant une variété de sites web disponibles publiquement ou des outils logiciels open source.

Activités

Partie 1 – Systèmes autonomes, Autonomous Systems (AS)

De nombreuses organisations ont configuré leurs réseaux en tant que systèmes autonomes (AS), ce qui leur permet d'utiliser plusieurs fournisseurs de services Internet et d'acheminer le trafic entre eux comme ils le souhaitent.

Il existe de nombreux outils en ligne qui vous permettent de rechercher des informations sur les systèmes autonomes pour un nom d'organisation ou un nom de domaine donné, par exemple :

- MXToolbox – https://mxtoolbox.com/asn.aspx (astuce : rechercher une adresse IP)
- HackerTarget – https://hackertarget.com/as-ip-lookup/ (astuce : rechercher une adresse IP)
- ANSLookup – https://asnlookup.com/ (astuce : rechercher un acronyme)

Livrables :

- Quel est le numéro du système autonome de l'UCAD ?

CIDR (Classless Inter-Domain Routing) est une méthode d'attribution d'adresses IP et de routage IP. La notation CIDR est une représentation compacte d'une adresse IP et de son préfixe de routage associé. La notation est construite à partir d'une adresse IP, d'une barre oblique (/) et d'un nombre entier.

Par exemple, l'entrée CIDR 10.3.22.0/24 signifie que les 24 bits supérieurs de l'adresse (10.3.22) restent constants et que les 8 bits inférieurs sont variables et représentent les ordinateurs du sous-réseau. 10.3.22.0 est la première adresse et 10.3.22.255 est la dernière, soit un total de 256 adresses possibles dans cette plage.

Livrables :

- Quel est le sous-réseau au format CIDR qui est associé au numéro du système autonome de l'UCAD ?

Partie 2 – Shodan

Shodan est un moteur de recherche permettant de trouver des dispositifs spécifiques, et des types de dispositifs, qui existent en ligne. Les recherches les plus populaires portent sur des choses comme webcam, linksys, cisco, netgear, SCADA, etc. Il fonctionne en scannant l'ensemble de l'Internet et en analysant les bannières renvoyées par les différents appareils. Grâce à ces informations, Shodan peut vous dire, par exemple, quel serveur Web (et sa version) est le plus populaire, ou combien de serveurs FTP anonymes existent à un endroit donné, et quels sont la marque et le modèle de l'appareil.

Quelques références :

- Exemples de requêtes de recherche Shodan : https://github.com/jakejarvis/awesome-shodan-queries
- Tirer le meilleur parti des recherches Shodan (blog SANS sur les tests de pénétration) : https://www.sans.org/blog/getting-the-most-out-of-shodan-searches/

Créez un compte Shodan (nécessaire pour utiliser la plupart des fonctionnalités du site), puis répondez aux questions suivantes.

Livrables :

Commencez une nouvelle recherche Shodan :

- Rechercher les hôtes avec le nom de domaine **ucad.sn**. Combien Shodan en a-t-il trouvé ?
  Astuce : utilisez le filtre **hostname:** pour votre requête.

Lancez une nouvelle recherche Shodan et répondez à ces questions dans l'ordre :

- Rechercher des hôtes dans le sous-réseau CIDR de l'UCAD. Combien Shodan en a-t-il trouvé ? Astuce : utilisez le filtre **net** pour votre requête.
- Parmi les hôtes trouvés dans la question précédente, combien d'entre eux exécutent Microsoft IIS httpd ou Apache comme serveur web ? Astuce : vous pouvez effectuer une recherche descendante dans le panneau de gauche ou ajouter le filtre **produit: "xxx"** à votre requête.
- Parmi les hôtes trouvés dans la question précédente, quelles sont les versions des serveurs Microsoft IIS httpd et/ou Apache ?

- Parmi les hôtes trouvés dans la question précédente, plusieurs ont des certificats SSL (pour HTTPS). Quels sont les noms communs (c'est-à-dire les noms de domaine) pour lesquels ces certificats sont émis ?
- Pour la question précédente sur les certificats SSL, quelle était la requête de recherche Shodan que vous avez saisie ?

Partie 3 – Whois

Le système **WHOIS** permet d'accéder aux informations du répertoire stockées par les bureaux d'enregistrement des noms de domaine.

En utilisant whois (dans votre VM Kali), trouvez des informations sur le nom de domaine "**ucad.sn**".

```
$ whois ucad.sn
```

Livrables :

- Quelle est l'adresse électronique associée au contact technique pour le nom de domaine **ucad.sn** ?
- Quels sont les serveurs de noms faisant autorité pour le nom de domaine **ucad.sn** ?

Partie 4 – DNS

Sublist3r est un outil d'énumération DNS. Il utilise une combinaison de moteurs de recherche Internet et (optionnellement) la déduction par force brute pour fournir une liste de sous-domaines à partir d'un domaine de départ.

Références :

- Site de développement GitHub avec des exemples
- Documentation Kali

Tout d'abord, créez un compte gratuit sur VirusTotal. Après vous être inscrit et connecté, copiez votre **clé API** depuis votre profil.

Ensuite, installez Sublist3r (dans votre VM Kali) et un patch de code pour corriger l'intégration avec VirusTotal.

```
# Installez Sublist3r
$ sudo apt install sublist3r

# Apporter un correctif à Sublist3r en suivant les instructions de ce # lien :
https://github.com/aboul3la/Sublist3r/issues/194
$ wget
https://raw.githubusercontent.com/aboul3la/Sublist3r/3cb826c2f36f4972dfd286c704efc07de3a7f
94c/sublist3r.py
$ sudo mv sublist3r.py /usr/lib/python3/dist-packages/sublist3r.py

# Configurez votre clé API VirusTotal, qui sera utilisée pour        # Sublist3r
$ export VT_APIKEY="<votre-clé-API>"
```

En utilisant Sublist3r (dans votre VM Kali), obtenez une liste de sous-domaines pour le nom de domaine "**ucad.sn**".

```
# Lancez l'énumération
$ sublist3r --domain www.ucad.sn
```

Livrables :

- Fournir une liste de 5 sous-domaines de **ucad.sn** qui sont particulièrement « intéressants » et dont vous ne connaissiez pas l'existence avant de lancer le scan.

Le **DNS Dumpster** est un outil similaire avec une interface web. Utilisez le DNS Dumpster pour obtenir une liste de sous-domaines pour le nom de domaine "**ucad.sn**".

Livrables :

- Fournir l'image « Domain Map » de DNS Dumpster qui résume les résultats de la recherche pour "**ucad.sn**".

Fierce est un scanner de noms de domaine qui aide à localiser les espaces IP non contigus et les noms d'hôte par rapport à des domaines spécifiés. En d'autres termes, à partir d'un nom de domaine, il trouvera des sous-domaines et des serveurs proches ("proches" sur la base de

l'adresse IP) qui peuvent ou non partager le même nom de domaine. Cet outil n'effectue pas d'exploitation et ne scanne pas l'ensemble de l'internet sans discernement. Il est conçu spécifiquement pour localiser des cibles probables à l'intérieur et à l'extérieur d'un réseau d'entreprise. Comme il utilise principalement le DNS, vous trouverez souvent des réseaux mal configurés qui fuient l'espace d'adressage interne.

Références :

- Site des développeurs GitHub avec des exemples
- Documentation Kali

Utilisez Fierce (dans votre VM Kali) pour effectuer un scan DNS :

```
$ fierce --domain www.ucad.sn
```

Livrables :

- Fournir deux noms de domaines et leurs adresses IP.

Partie 5 – Certificats SSL

Les certificats SSL peuvent être une source utile de noms d'hôtes susceptibles d'être intéressants dans un test de pénétration. Vous pouvez inspecter les certificats SSL manuellement dans votre navigateur web, ou en utilisant diverses ressources en ligne, telles que :

- https://andrewmohawk.com/SSLAssociated/index.php
- https://www.ssllabs.com/ssltest/

Livrables :

- Pour le nom d'hôte **www.ucad.sn**, quels sont les « noms alternatifs » ou « noms DNS » figurant dans le certificat SSL ? Il s'agit d'une liste d'autres noms d'hôtes qui sont également signés/sécurisés par le même certificat. Vous pouvez le vérifier dans votre navigateur web ou à l'aide de l'un des outils de recherche en ligne répertoriés.