NANTES ynov CAMPUS

Sommaire

1. Rappels de Cybersécurité

/ ! \ Attention : Quand on parle de cybersécurité on ne parle pas que d'informatique. Par exemple l'ingénierie sociale qui consiste à récupérer des informations sur quelqu'un en l'interrogeant est un risque lié à la cybersécurité et ne demande aucune connaissance en informatique

La cybersécurité est une chose qui se développe de plus en plus aujourd'hui car nous avons eu une prise de conscience sur l'importance de la donnée en entreprise. Il est donc primordial de la sécuriser.

De plus il existe aujourd'hui beaucoup d'outils qui permettent à n'importe qui de réaliser une intrusion assez facilement sans forcément avoir des connaissances en informatique ce qui renforce l'idée de sécuriser nos données.

Lors d'un audit dans les entreprises le niveau de sécurité (CMMI) est évalué selon les niveaux suivants :

Source : https://www.manager-go.com/gestion-de-projet/modele-cmmi.htm

Remarque : La plupart des entreprises en France n'atteignent même pas le niveau 3

2. Rappels d'Intrusion

/ ! \ Important à retenir : L'article de la loi qui définit une intrusion dans un SI est le L. 323-1 :

L'article **L. 323-1 du Nouveau code pénal** prévoit que « le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende ».

Lors d'une intrusion la 1ère chose à identifier et attaquer est l'application la plus vulnérable de l'entreprise.

Lors d'un Pentest en entreprise il est important de savoir quelle IP nous allons devoir attaquer. Il est aussi important d'avoir un contrat avec le client ainsi qu'une couverture en cas de dommage sur un serveur par exemple (sauvegarde de côté, assurance…).

Il existe différents types de pentest :

- La boite noire : Ici nous ne partons de rien, aucunes infos connues par défaut
  Avantage : représentatif d'une attaque réelle
  Inconvénient : peu être très coûteux pour l'entreprise cliente

- La boite blanche : Ici à l'inverse de la boite noire nous avons toutes les informations sur l'entreprise (les code source des applis, les bibliothèques utilisées…)
  Avantage : réduction du temps d'audit
  Inconvénient : Besoin de plusieurs compétences spécifiques et donc d'une équipe de test plus grande

- La boite grise : Ici nous avons le mélange de la boite noire et blanche

Nous retrouvons différents types d'attaquants :

- Les concurrents directs
- Les « Insiders » : les personnes ayant accès au réseau de l'entreprise
- Les groupes criminels (phishing, corruption de site)
- Les groupes « Etatique » (spear phishing, DDOS)

Les groupes criminels peuvent utiliser les outils d'attaques suivants :

- C2 (Command & Control)
- Cobalt Strike

3. Découverte de l'outil OpenCTI

Information sur l'outil :

Le projet **OpenCTI** a été initié en septembre 2018 par l'ANSSI et co-développé avec le CERT-EU en l'absence de solutions complètement appropriées pour structurer, stocker, organiser, visualiser et partager la connaissance de l'ANSSI en matière de cybermenace, à tous les niveaux.

Cet outil s'installe généralement dans un environnement cloud sur un cluster kubernetes car il demande beaucoup de ressources et de stockage.

Cet outil peut être lié à un EDR ou un SIEM pour obtenir de meilleurs performances. L'EDR ou le SIEM vont détecter une intrusion ou un comportement suspect et tout sera « loggé » dans l'outil CTI afin d'avoir une traçabilité.

4. Analyse de surfaces d'attaques

Une surface d'attaque est une surface d'exposition de l'organisation qu'un attaquant pourrait exploiter.

Il existe différentes façons de réduire la surface d'exposition, par exemple :

- Analyser les services externes
- Analyser les AS
- Analyser les entrées DNS (avec dnsdumpster.com)

5. Découverte d'outils d'analyses

Outil n°1 : Shodan (www.shodan.io)

Shodan est un moteur de recherche créé en 2009 par John Matherly. Ce site référence le résultat de balayages de ports massifs effectués sur le réseau Internet

Exemple de test de port : **« port:161 country:cm »**

Outil n°2 : ZoomEye qui est la version Chinoise de Shodan

Outil n°3 : LeakIX (leakix.net)