Cours 13 :

Phase 3 : Gagner l'accès

JACQUEMIN Mathieu

Disclaimer

- Ce cours a été créé dans le but d'informer et d'éduquer les participants sur les sujets liés à la cybersécurité. L'ensemble des techniques présentées le sont à titre pédagogique et préventif afin de pouvoir se prémunir d'attaque potentiel.
- Certaines des techniques présentées sont illégales et dangereuses si elles sont utilisées à mauvais escient, sans maitrise, et sans consentement.
- Il est interdit d'utiliser ces techniques contre toute entité dont vous ne disposez pas le consentement. Dans le cadre d'un accord pour audit, il est obligatoire d'agir dans le cadre d'un contrat parfaitement défini, écrit, et signé par les deux parties.
- Vous devez respecter la loi en vigueur ainsi qu'utilisez les techniques avec éthique et responsabilité.
- Je me dédouane de toute responsabilité en cas de problème ou d'incidents à la suite de ce cours.
- Vous êtes seul responsable de l'usage fait des connaissances enseignées.

Phase 3 : Gagner l'accès

Accès concret au système visé

Utilisation d'une ou plusieurs vulnérabilités (humaines ou logicielles)

Basée sur les informations trouvées dans les étapes précédentes

Les diverses façons

- Les vulnérabilités des logiciels
- Les vulnérabilités matérielles
- Les vulnérabilités de configuration
- Les vulnérabilités d'utilisateur

Maintenir l'accès et se cacher

Pas utilisé dans le hacking éthique

Utilisation de portes dérobées pour se faciliter l'accès

Suppression de fichiers logs/sauvegardes pour couvrir les traces

Les vulnérabilités des logiciels

Ces vulnérabilités sont la conséquence de faiblesses dans la conception, la mise en œuvre ou l'utilisation d'un logiciel, mais il s'agit souvent d'anomalies liées à des erreurs de programmation ou à de mauvaises pratiques

D'où l'importance des mises à jour

La procédure d'exploitation d'une vulnérabilité logicielle est appelée exploit.

Rappel DICT

Les indicateurs de sécurité informatique

Disponibilité

Intégrité

Confidentialité

Traçabilité

Rappel DICT

Les indicateurs de sécurité informatique

Disponibilité → Accessible et utilisable

Intégrité → Source sure et non modifiée

Confidentialité → Seulement les personnes habilitées

Traçabilité → Impossible de nier

Les vulnérabilités des logiciels

Exemples

https://cert.ssi.gouv.fr/

https://www.exploit-db.com/

Les vulnérabilités matérielles

Ces vulnérabilités sont liées aux faiblesses physiques des équipements informatiques (tels que les ordinateurs, les serveurs, les réseaux, les périphériques, etc) ou d'infrastructure (badges d'accès, porte non sécurisée, etc)

La rétro-ingénierie (ou reverse engineering) consiste à étudier un objet pour en déterminer le fonctionnement interne ou la méthode de fabrication.

Les vulnérabilités matérielles

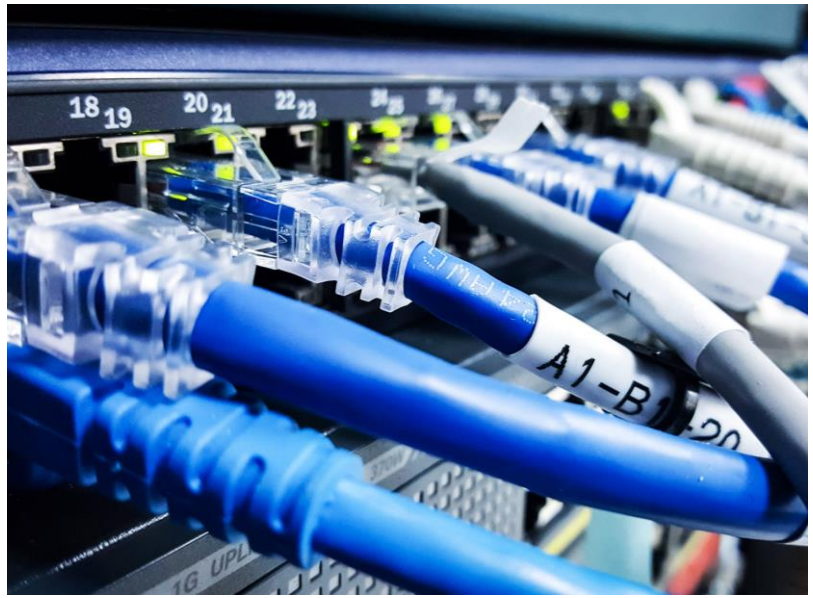
Exemples

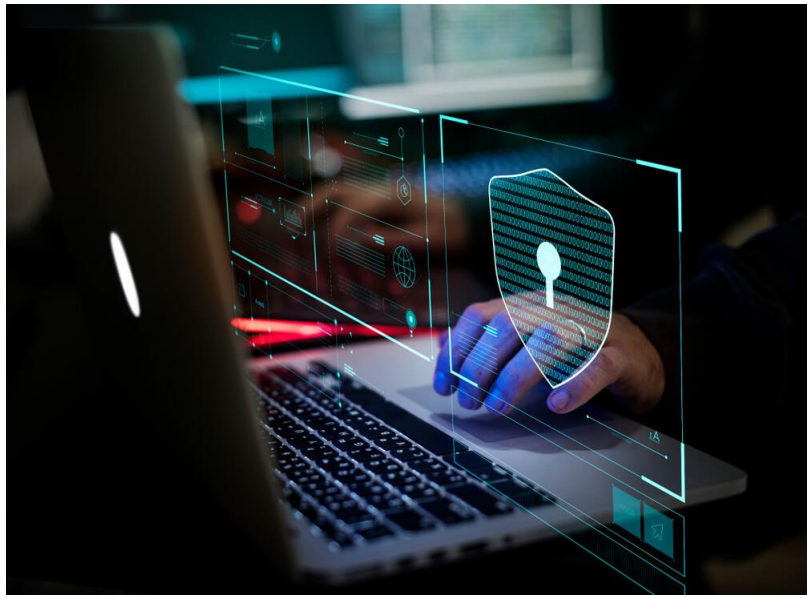
Vulnérabilité dans les IoT (internet of things)

Une porte d'accès physique non sécurisée par exemple, qui permet à un attaquant de physiquement accéder à un ordinateur ou à un réseau et de voler des informations ou de déployer des logiciels malveillants.

Les vulnérabilités de configuration

Il s'agit des cas de mauvaises configurations des systèmes et des réseaux qui peuvent entraîner une brèche de sécurité.





Les vulnérabilités de configuration

Exemples

- Les mots de passe par défaut non modifiés ou pas assez complexes
- L'absence de protection (Pare-feu, antivirus, etc)
- Partages non sécurisés
- Désactivation des mises à jour

Les vulnérabilités d'utilisateur

Ces vulnérabilités concernent les erreurs ou les mauvaises pratiques commises par les utilisateurs qui peuvent entraîner des violations de sécurité.

C'est pourquoi il faut sensibiliser les utilisateurs aux risques de sécurité et leur fournir des outils et des politiques pour les aider à adopter les bonnes pratiques de sécurité

L'ingénierie sociale est une méthode d'attaque utilisée par les cybercriminels pour parvenir à leurs fins. Cette approche repose avant tout sur la psychologie humaine. Le pirate informatique mise sur la naïveté des utilisateurs pour atteindre ses objectifs.

Les vulnérabilités d'utilisateur

Exemples

CENTRE DE GESTION DU GARD

Metasploit

Environnement de test d'intrusion avec l'utilisation d'exploits et de payloads pour tester la sécurité d'un système

Version gratuite : Metasploit Framework

Les exploits permettent d'exploiter une vulnérabilité pour entrer dans un système, tandis que les payloads permettent d'effectuer des actions une fois dedans (création d'une backdoor par exemple)

Metasploit

Exemple

TP

Voir Moodle