Cahier des charges du TFE

Mise en œuvre d’un test d’intrusion du wifi, de l’AD et du site internet de la HEH.

2023 - 2024

Rosin Guillaume

***Présentation du TFE 2023 - 2024***

# Titre provisoire

Mise en œuvre d’un test d’intrusion du wifi, de l’AD et du site internet de la HEH.

# Objectif :

Mon objectif consiste à mener un pentest en mode whitebox, greybox et blackbox du site Web, de l’AD et du WIFI de l'infrastructure informatique de la HEH en utilisant la méthodologie « PTES » :

L'objectif consiste à réaliser des tests d'intrusion en vue de détecter d'éventuelles vulnérabilités. Ensuite, il s'agira de tenter de les exploiter, notamment pour déterminer la possibilité d'acquérir des droits administrateurs ou d'accéder à des données confidentielles.

La méthodologie « PTES » :

* Interactions au préalable avec les clients ciblés
* Collecte de renseignements
* Evaluation des menaces
* Exploitation
* Post-exploitation
* Mouvement latéral
* Rapports

# Description des phases :

Phase 1 : Interactions au préalable avec le client :

Durant la phase de pré-engagement nous préparons le test d’intrusion proprement dit. Durant cette étape, je poserai de nombreuses questions et nous nous mettrons notamment d’accords avec mon prometteur et mon client sur les tests autorisés et non autorisés.

Phase 2 : La collecte de renseignements :

La phase de collecte d’informations est un élément essentiel de toute évaluation de sécurité. C'est la phase au cours de laquelle je dois rassembler toutes les informations disponibles sur l'HEH, ses employés, ses infrastructures et son organisation. La collecte d’informations est la phase la plus fréquente et la plus vitale du processus de test d’intrusion.

Phase 3 : Evaluation des menaces :

Au cours de la phase d’évaluation des menaces, j’examine et analyse les informations recueillies lors de la phase de collecte d'informations.

L’objectif de cette phase est d’identifier les principales cibles au sein d’une entreprise et les sources de menaces les plus probables afin de mieux préparer la phase d’attaque.

Phase 4 : Exploitation :

Au cours de cette étape, je recherche et mets en œuvre des moyens de profiter des vulnérabilités détectées pour obtenir des informations, des privilèges ou encore des accès.

Par exemple si je veux obtenir un shell inversé, je peux modifier le PoC pour exécuter le code, afin que le système cible se reconnecte à nous via une connexion cryptée à une adresse IP que j’aurai spécifié. La préparation d’un exploit fait donc principalement partie de la phase d’exploitation.

Phase 5 :

Imaginons que j'aie réussi à exploiter avec succès le système cible au cours de la phase d'exploitation. Tout comme lors de cette phase, je dois à nouveau délibérer sur l'opportunité d'opter pour des techniques de test évasif lors de la post-exploitation. Étant déjà sur le système à ce stade, il devient considérablement plus complexe d'éviter toute détection. La post-exploitation vise à recueillir des informations sensibles et pertinentes du point de vue de la sécurité locale, ainsi que des informations cruciales pour l'entreprise, qui nécessitent souvent des privilèges plus élevés que ceux d'un utilisateur standard. Cette étape englobe divers aspects tels que les tests évasifs, le pillage, l'élévation de privilèges et l'exfiltration de données.

Phase 6 :

Si tout s'est bien passé et que j’ai réussi à pénétrer le réseau de l'HEH et à rassembler des informations stockées localement et à élever mes privilèges, j’entre ensuite dans la phase « Lateral Movement ». L’objectif ici est de tester ce qu’un attaquant pourrait faire sur l’ensemble du réseau. Après tout, l’objectif principal n’est pas seulement d’exploiter avec succès un système accessible au public, mais également d’obtenir des données sensibles ou de trouver tous les moyens par lesquels un attaquant pourrait rendre le réseau inutilisable. L’un des exemples les plus courants est celui des ransomwares. Si le réseau de l’HEH est infecté par un ransomware, celui-ci peut se propager sur l’ensemble du réseau. Il verrouille tous les systèmes à l'aide de diverses méthodes de cryptage, les rendant inutilisables pour l'ensemble du département jusqu'à ce qu'une clé de décryptage soit saisie.

# La portée du pentest :

* Pentest Wifi :

Dans le cadre de ce test d'intrusion, il est demandé que j’effectue une évaluation approfondie de la sécurité du réseau Wi-Fi qui me sera accordée, en m'assurant de respecter scrupuleusement les autorisations qui me seront accordées. Les mesures spécifiques que je pourrai mettre en œuvre pour évaluer la sécurité du réseau dépendront des droits qui me seront conférés, et je m'engage à conduire cette analyse tout en observant les paramètres définis par mon département.

Dans le cadre de cette évaluation, je peux explorer divers aspects de la sécurité, par exemple en testant la robustesse des clés WPA2 des points d'accès, en réalisant une usurpation d'identité du point d'accès, la mise en place d'une analyse de réseau Wi-Fi, à laquelle je procéderai conformément aux autorisations spécifiques qui m'auront été accordées. L'objectif de ces activités est d'identifier toute vulnérabilité potentielle et de proposer des recommandations pour renforcer la sécurité globale du réseau Wi-Fi de mon département.

Exemples d’outils : Aircrack, responder, Spider, Wifite…

A screenshot of a computer screen

Description automatically generated

### Pentest Web :

Il est demandé que j’entreprenne une évaluation de la sécurité de la section du site qui me sera dédiée, en veillant à ce que chaque étape soit conforme aux autorisations qui me seront accordées. Les actions spécifiques que je pourrai entreprendre sur cette portion du site dépendront des permissions octroyées, et je m'engage à réaliser un test d'intrusion approfondi tout en respectant les paramètres définis par le département sciences et technologies.

Je demeure en attente des informations relatives aux permissions qui me seront octroyées afin d'effectuer des opérations sur l'infrastructure du site web

Exemples d’outils  Outil : johntheripper, fuff, Whois, OWASP, vHost Fuzzing, hashcat, nmap,…

### Pentest Active Directory :

En ce qui concerne ce test d'intrusion, j'ai obtenu l'approbation de M. Pietrzak pour évaluer l'infrastructure de l'Active Directory de l’HEH en vue de détecter d'éventuelles failles. J'ai été autorisé à mettre en œuvre l'ensemble de mes attaques conformément aux conditions établies. Avant d'appliquer ces attaques au service informatique, je soumettrai les commandes pour approbation, et je m'engage à rapporter en temps réel chaque attaque que je réalise.

Voici donc quelques exemples d’attaques :

-Identification des hôtes (Outil : Kerbrute, cme, nmap…)

-Identification de vulnérabilités potentielles tel que les exploits Windows tels que MS08-067, EternalBlue ou BlueKeep, abuser d’un servie exécuté dans le contexte SYSTEM accountSeImpersonate avec l’outil JuicyPotato, abuser des privilèges du compte de service et bien d’autres !

-Empoisonnement LLMNR/NBT-NS avec Linux et Windows

-Usurpation d’identité en réalisant une attaque MITM

-Enumération et récupération des politiques de mot de passe

-Création d’une liste d’utilisateurs cibles et pulvérisation de mots de passe.

-Enumération des contrôles de sécurité.

-Enumération des informations d’identification.

-Attaque en « Living Off The Land » (local)

-Kerberoasting

-Abus liés aux listes de contrôle d’accès (ACL).

-Enumération des listes de contrôle d’accès.

-Tactiques d’abus d’ACL.

-Vole de la base de données de mots de passe active directory avec DCSync.

-Réalisation de « pass-the-hash ».

-Connection aux partages SMB et exploitations.

-Réalisation d’un « reversed shell ».

Outil : GetUserSPN.py, Powerview, Bloodhound, Rubeus, Nmap, rpcclient, smbclient, smbmap, crackmapexec, metasploit, evil-winrm, inveigh.

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

|  |  |
| --- | --- |
| Signature étudiant | Signature du promoteur |