

|  |  |  |  |
| --- | --- | --- | --- |
| ***Devoir 2*** |  | | ***Pondération : 25%*** |
| **Travail individuel** | | | |
| ***Identification de l’étudiant(e)*** | | | |
| ***Nom*** | ***Prénom*** | | ***Matricule*** |
|  |  | |  |
| ***Sigle et titre du cours*** | | ***Trimestre*** | |
| **CR470 – TESTS D’INTRUSION** | | **A-2022** | |
| ***Chargé de cours*** | ***Chargé de travaux pratiques*** | | ***Date Remise*** |
| **Hector Bustillo (Groupe 1)**  **Ngonga Henry (Groupe 2)** | **Saïd Cherkaoui** | | **24 octobre 2022** |

**Des pénalités seront appliquées si la remise n’est pas faite dans ce Gabarit en Word.**

**Toutes les réponses doivent être mises dans la case correspondante à la question.**

**Aucun fichier joint à ce document et aucun lien ne seront acceptés. Uniquement les textes et les copies d’écran des résultats seront acceptées.**

**Un rapport avec un maximum de 30 pages.**

**Des pénalités seront appliquées si la remise n’est pas faite dans ce Gabarit en Word.**

**Les réponses doivent être mises dans la case correspondante à la question.**

**Un rapport avec un maximum de 20 pages.**

**Un ra**

**Énoncé détaillé**

**Objectif**

L’objectif de ce projet est d’élaborer et d’approfondir vos connaissances sur un sujet donné selon les critères spécifiés par le professeur. Il s’agit d’un travail où l’élève devra élaborer une stratégie de tests d’intrusion

**Étapes de réalisation**

**Partie 1 (/60)**

1. Définir et mettre en place **une** des stratégies d’attaque suivantes :
2. WEB
3. Post exploitation
4. Social engineering
5. Wifi

Nous tiendrons compte des critères de correction suivants :

1. Originalité de l’attaque (/20)
2. La complexité (/20)
3. L’exécution et l’intégration de la solution (/10)
4. Les tests effectués pour valider la solution (/10)

**NB**: On vous invite à ne pas utiliser les exemples vus en classe mais plutôt à vous y référer. Ceci pourrait impacter les deux premiers critères de correction.

**Partie 2 (/40)**

1. a.) Utilisez votre prénom et nom de famille fusionné (Ex : MichelTremblay) pour générer les types de hash suivants :
   1. MD5
   2. SHA1
   3. Bcrypt
   4. MD4

b.) Procéder ensuite au déchiffrement du Hash généré et indiquez vos étapes pour y parvenir.

**Livrable**

1. **Un rapport Word obligatoire** **dans le ce Gabarit** incluant les deux sections suivantes :
   1. Partie 1 : Expliquer votre démarche pour la mise en place, les tests et la configuration de la solution choisie.
   2. Partie 2 : La procédure pour procéder au Hash et au déchiffrement ainsi que les résultats obtenus.
2. Il s’agit d’un travail individuel.
3. Il est important d’inclure des captures d’écran détaillées afin de bien démontrer la mise en place, la configuration, les tests et le bon fonctionnement.
4. Le rapport doit suffisamment être clair et détaillé de telle sorte qu’on puisse le donner à une personne technique et qu’elle puisse reproduire le projet.
5. La date limite de remise du devoir 2 est le **22 Novembre 2021 à 23h55** via le site de Moodle.

**Important d’inclure les sections suivantes dans tous les rapports de laboratoire :**

1. **Page titre**
2. **Table des matières**
3. **Analyse et évidences**
4. **Conclusion et ou recommandations**
5. **Références**

**Réponses détaillées**

**Table des matières :**

**Introduction …………………………………………………………………………….……..……………… page**

**Partie 1 Définition de la stratégie d’attaque …………………….………………………………….…. page**

**Mise en place ………………..…………………………………………………………..……… page**

**L’exécution …………………………………………………..……………………..………..…... page**

**Les tests …………………….……………………….……………………………..………..…... page**

**Partie 2 Génération Hash ……..………………………………………………………………………..…. page**

**Section 2-1 MDS……..……………………………………………………………………..……..… page**

**Section 2-2 SHA1……..………………………………………………………….…..………..…..... page**

**Section 2-3 Bcrypt……..……………………………………………………………..……..……... page**

**Section 2-2 MD4……..……………………………………………………………..…………..…... page**

**Conclusion …………………………………………………………………………….………………….….. page**

**Références ……………………………………………………………………………………………….….. page**

**Introduction :**

**Ce travail a pour but de mettre en pratique les notions qui ont été acquis pendant les séances de cours, ce travail de pentester ou il s’agit de faire un post exploitation a été fait en 2 semaines s’étalant sur plusieurs jours du 15 mars et a pris fin le 30 mars 2023. Ce travail avait pour but d’appliquer les étapes à suivre pour effectuer un test de pénétration et persistance.**

**Les participants :**

**Pentester Mohamed Malick Balde**

**Choisir la stratégie d’attaque que vous voulez développer parmi cette liste**

**WEB**

**Post exploitation**

**Social engineering**

**WIFI**

**…Post exploitation**

**Quel est votre choix ?**

|  |  |
| --- | --- |
| **Partie 1 :** | **Définition des stratégies d’attaque** |
| **Questions:** | **Réponses et copies écrans de la section** |
| 1. **Définition de la stratégie** | Pour ce travail, nous allons faire un Post Exploitation sur deux de nos machines le but est de trouver des failles, vulnérabilités, exploitables et faire un post exploitation en utilisant ces failles a la fin nous allons proposer des plans d’actions permettent d’améliorer la sécurité des système.  Pour parvenir a faire un exploit premièrement nous allons nous rassurer que les deux machines communique « Ping » avec notre machine d’attaque, sur notre machine d’attaquant nous allons faire un scanning ‘**nmap’** de port sur la machine Metasploit2 en fin de voir quelle sont les port ouverte et vulnérables, une fois que nous avons les ports ouvertes nos recherche se basera sur ces port s’ils sont vulnérable ou pas pour en savoir nous allons nous servir du site **Exploit-db.com** et nous aurons plus de détails sur les ports ouverts ou faire un **search** sur la version du port et nous plusieurs exploit a utilise en fin d’atteindre l’objectif qui est le post exploitation.  En tant que pentester nous savons que le logiciel **Adobe Reader** 9.0 est vulnérable**,** donc nous allons télécharger ce logiciel dans la machine windows10 et l’installer, dans notre machine d’attaquant Kali nous allons générer un fichier d’exploitation qui est **evil.pdf,** une fois le fichier généré nous allons le placer dans la racine du dossier de kali linux ou se trouve le dossier web html qui est www ‘‘/home/kali/.msf4/local/evil.pdf’’ une fois le fichier PDF placer, sur la machine windowse10 nous allons nous essayer d’accéder à la page web de la machine kali avec son IP qui est **192.168.29.132/evil.pdf**, normalement nous aurons une page vierge et nous allons enregistrer la page sous le format PDF et essayer de l’ouvrir avec le logiciel Adobe que nous avons installé dans la machine windows10, sur la machine kali nous allons utiliser un **handler** pour rester à l’écoute une fois exécuté nous aurons une sessions **meterpreter**. Bien sur nous pouvons envoyer un courriel ou un lient ou l’utilisateur peut cliquer ou télécharger notre fichier evil.pdf sur la machine windows10 aussi, mais cela serait un peu du social engineering. Et une fois nous avons une sessions nous pouvons utiliser le logiciel **ThefatRat** que j’ai cloner dans kali en fin de faire une persistance et de créer un Backdoor pour nous permettre de revenir, même si la vulnérabilité a été corrigé |
| 1. **Mise en place** | Pour effectuer ce travail nous aurons besoins de trois machines, une machine kali linux qui sera notre machine d’attaquant une machine metasploit2 et une machine windows10 qui serons les machines victimes et nous allons faire une configuration et des updates dans nos machines. |
| 1. **L’exécution et l’intégration de la solution** | Pour pouvoir attaquer la machine metasploitable2 j’utilise deux méthodes après avoir faire un scanne de port avec leurs versions je constate qu’il avait plusieurs ports ouverts qui sont le 22 qui est ssh le 23 qui est telnet et même la vulnérabilité smb, donc je me sers de deux port le ssh et le telnet mais pour arriver à cela j’ai dû créer un fichier texte que j’ai appelé Username.txt    Le fichier Username.txt qui va me servir a faire une modification des options de l’exploit que je vais utiliser    Et là je vais utiliser un exploit ssh qui est user auxiliary/scanner/ssh/ssh\_login, cependant je vais modifier les options qui sont User\_file, le Pass\_File le Verbose je le mets a True je fais un run pour que ça puisse m’ouvrir une session avec les informations de connexions que je vais utiliser pour se connecter à la machine metasploitable2    Nous voyons ici l’adresse IP de la machine Metasploit2 qui est 192.1168.29.131 :22 -success ‘msfadmin : msfadmin’ ce qui est les informations de login de notre machine metasploit, donc de la nous pouvons ouvrir un autre terminal et essayer de se connecter avec un ssh suivie de l’adresse IP de la victime    Cette partie est celle pour le port 23 qui est le telnet que j’utilise les mêmes procédures en modifiant les options et utiliser le fichier Username.txt que j’ai créer    Nous voyons ici l’adresse IP de la machine Metasploit2 qui est 192.1168.29.131 :23 -success ‘msfadmin : msfadmin’ ce qui est les informations de login de notre machine metasploit, donc de là nous pouvons ouvrir un autre terminal et essayer de se connecter avec un telnet suivie de l’adresse IP de la victime    **Windows10 Post exploitation**  Pour la machine windows10 je vais exploiter une vulnérabilité Adob\_Reader la version 9.0 donc je télécharger le dossier zip d’Adobe sur le site OLDVERSION.com et l’installe dans ma machine windows10      Dans notre machine kali nous allons nous rendre dans msfconsole et utilise l’exploit **windows/fileformat/adobe\_pdf\_embedded\_**exe qui va nous permettre d’exploiter les failles de Adobe Reader et pour cela nous allons modifier les options de cet exploit, dans cette capture nous voyons le nom de fichier qui est evil.pdf et le message qui va s’affiche sur l’écran de la victime qui lui dira de cliquer « Launch\_message »      Et fait exploit pour créer notre fichier evil.pdf et ça nous donne le chemins du fichier et je copie le directory du fichier ‘/home/kali/.msf4/local/evil.pdf’ pour le mettre dans le répertoire qui est dans sous-kali et ce fichier qu’on va essayer de transférer dans la machine windows |
| 1. **Les tests effectués pour valider la solution** | **Postexploitation Metasploitable2**  Et la j’ouvre un autre terminale Kali en fin d’excuter les commande telnet et ssh avec l’adresse ip de ma machine victime qui est la 192.168.29.131  telnet 192.68.29.131    Et J’utilise les informations que mon exploit m’a fourni avec la session ouvert en fin que je puisse me loguer dans la machine avec le port 23        Et voire l’écran de la machine victime et le fichier momo.txt créer depuis de la machine kali    **Windows10 Post exploitation**  La partie Windows10 j’ouvre le navigateur et inscrit l’adresse IP de ma machine kali ainsi que le fichier evil.pdf, normalement sa doit me fournir une page vierge mais mon c’est comme si mon pare-feu le bloque mais l’idée une foi qu’on arrive à accéder sur la page vierge nous devons enregistre la page vierge après l’ouvrir avec l’application ADOB Reader et ouvrir un session handler dans kali qui va rester en écoute une fois le fichier est exécuté    Ici nous allons faire un Set sur le LHost l’adresse IP KALI    On fait exploit notre handler est à l’écoute et une fois l’utilisateur exécutera le fichier enregistrer nous allons obtenir une sessions meterpreter et nous avons le contrôle de la machine windows10 tel est la procédure de mon exploit windows10    Mais mon par feu ne veut pas je l’ai désactiver mais il reste toujours bloqué et comme vous voyez mon handler est a l’écoute de l’exécution    Et une fois nous avons une sessions meterpreter nous allons utiliser la commande ‘ run persistance -A -I -P -r‘ ceux-ci permet de faire une persistance -A permet démarrer automatiquement le handler et -I est pour l’intervalle de connexions -P donner un port qui n’est pas utilisé et -r l’adresse de la machine kali qui recevra les donnes de la machine attaqué. Et cette commande run nous permettra de créer un script dans la machine windows10 attaquer.  Une autre option pour créer un Backdoor nous pouvons utiliser TheFatRat et pour cela nous devons l’installer **Théâtral** et une fois l’installer on a un menue et nous allons choisir l’options 6 pour créer notre Backdoor qu’on a obtenue avec le meterpreter      Et de là nous allons choisir 1 et définir les options la création du fichier, le port et IP de notre machine kali et transfère ce fichier dans le dossier html kali et suivre les mêmes procédure dans windows. |

|  |
| --- |
| Partie 2 : Génération HACH |

|  |  |
| --- | --- |
| **Questions :** | **Réponses et copies écrans de la section** |
| **Section A : MD5** |  |
| 1. **Procédure pour générer HASH** | Création du dictionnaire |
| 1. **Déchiffrement** |  |
| 1. **Résultats obtenus** |  |
| **Section B : SHA1** |  |
| 1. **Procédure pour générer HASH** |  |
| 1. **Déchiffrement** |  |
| 1. **Résultats obtenus** |  |
| **Section C : Bcrypt** |  |
| 1. **Procédure pour générer HASH** |  |
| 1. **Déchiffrement** |  |
| 1. **Résultats obtenus** |  |
| **Section D : MD4** |  |
| 1. **Procédure pour générer HASH** |  |
| 1. **Déchiffrement** |  |
| 1. **Résultats obtenus** |  |

**Conclusion :**

Ce devoir m’a permis de mettre en pratique les connaissances que j’ai acquis dans ce cours CR470, ou nous avons détaillées les étapes à suivre en fin de pouvoir effectuer une attaque de teste d’intrusion en cyber sécurité. Dans ce travail nous commençons par faire de la reconnaissance et comment effectuer une reconnaissance en fin de récupérer les informations qui nous pourrons être utiles, on a eu à faire du scanning des ports avec quoi on pourra utiliser pour gagner l’accès et j’ai eu à utiliser des sites web comme Exploit-db qui nous facilite à avoir des informations trouver lors du scanning des ports ouverts ainsi que la version. En guise de conclusion il serait très important d’appliquer des patchs et fermer tous les port qui ne sont pas utilisé ou bien créer des honeypots pour tromper le hacker, mais le mieux est de les fermer si elles sont pas utilisé, d’effectué des mis-a-jours sur nos logiciel qu’on utilise et faire une sensibilisation aux reste des employés de ne pas ouvrir des documents qui sont télécharger sur des site inconnue.

**Références :**

<http://www.oldversion.fr/windows/acrobat-reader-9-0>

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

<http://www.oldversion.com/windows/acrobat-reader/>

**Annexe B : Grille de correction**





