

|  |  |  |  |
| --- | --- | --- | --- |
| ***Devoir 1*** |  | | ***Pondération : 25%*** |
| **Travail individuel** | | | |
| ***Identification de l’étudiant(e)*** | | | |
| ***Nom*** | ***Prénom*** | | ***Matricule*** |
|  |  | |  |
| ***Sigle et titre du cours*** | | ***Trimestre*** | |
| **CR470 – TESTS D’INTRUSION** | | **H-2023** | |
| ***Chargé de cours*** | ***Chargé de travaux pratiques*** | | ***Date Remise*** |
| **Hector Bustillo (Groupe 1)**  **Ngonga Henry (Groupe 2)** | **Saïd Cherkaoui** | | **9 Février 2023** |

**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 40 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 du devoir 1**

Partie 1 - Reconnaissance

Section 1-1

1. En utilisation toute l’information publique de Polymtl.ca disponible dans linkedin, Facebook ou toutes autres sources d’information, trouver les informations suivantes:
2. Les noms des dirigeants (utile pour phishing)
3. Les technologies utilisées et justifier la provenance (ex: job pour un sysadmin Linux avec un minimum de 5 ans dans Red Hat)
4. Des adresses courriels

Autres sources pertinentes d’information:

* <http://www.pentest-standard.org/index.php/Intelligence_Gathering>
* <http://www.vulnerabilityassessment.co.uk/Penetration%20Test.html>

Section 1-2 - Maltego

1. Utiliser Maltego pour procéder aux étapes de reconnaissances de <https://www.megacorpone.com/> pour soutirer de l’information au sujet des serveurs DNS, WEB et les adresses courriels.

Partie 2 - Scanning

Section 2-1 - Prérequis

1. Installer une VM de Metasploitable 2 dans un mode NAT. Le username et le mot de passe par défaut est root.  
   Ref. : <https://www.vulnhub.com/entry/metasploitable-2,29/>
2. Installer une VM de Kali en mode NAT.
3. Assurez-vous que les deux VM sont en mesures de communiquer (Ping) entre elles.

Section 2-2 – Scanning

1. À partir de la VM de Kali vers la VM de Metasploitable2.
2. À partir de Kali vers le site <http://scanme.nmap.org/>

Effectuer les requêtes suivantes et les réponses doivent être mises dans la partie 2 du Gabarit.

1. Fast scan
2. SYN scans – all ports
3. TCP Connect scans – top ports
4. UDP scans – top 100 ports
5. OS fingerprinting
6. Un Version Scan sur les ports 21, 22, 23 et 53
7. Un Version scan sur les ports ouverts trouvés en (5)
8. Un scan NSE sur les ports ouverts trouvés en (5)

Partie 3 – Scans de vulnérabilités

Section 3-1 - Requis:

1. VM de Win XP (rendu disponible par le prof) en mode NAT pour utiliser avec le logiciel VMware WorkStation

<https://polymtlca0-my.sharepoint.com/:u:/g/personal/hector_bustillo_polymtl_ca/ESK6HoR6_5BJop1bcmtEIyYBgUt6B94fh7ISawWr4Eb9PQ?e=WZoYkt&isSPOFile=1>

Pour importer dans le logiciel VirtualBox

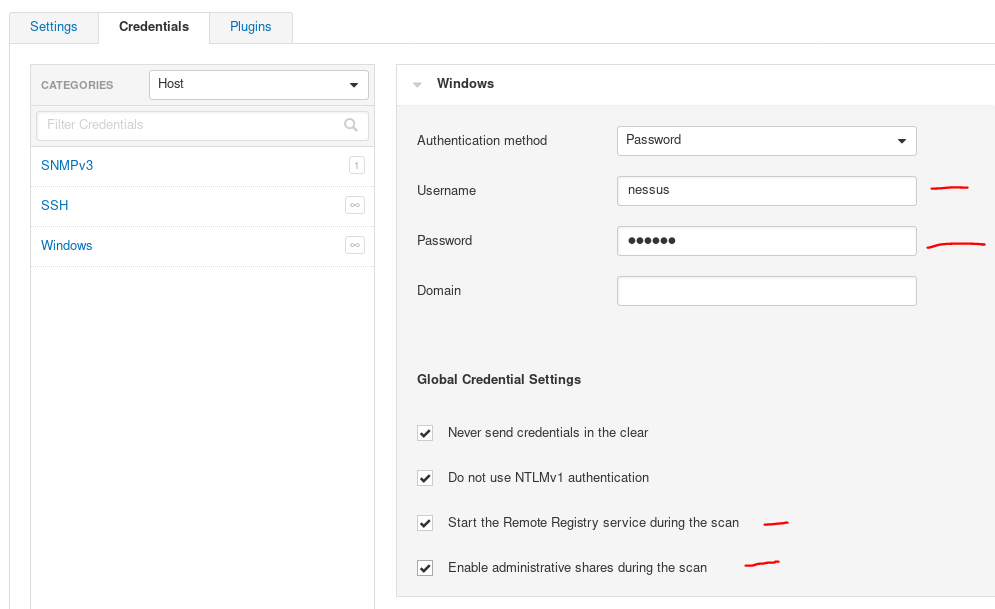
[Export\_VM\_XP.zip](https://polymtlca0-my.sharepoint.com/:u:/g/personal/said_cherkaoui_polymtl_ca/EaSN67PZPXlIjJ_cXUjAd_MBTqfetx7kpjIERctQc6XBNA?e=HGhFJ0)

1. VM de Kali (disponible dans le WEB) en mode NAT
2. Vm de Metasploitable 2 (disponible dans le WEB) en mode NAT

Section 3-2 – Scans de vulnérabilités

Téléchargez et configurez la VM de Windows XP rendue disponible par votre prof.

Utilisateurs de la VM XP :

1. User : admin PW : (à vous de deviner)
2. User :Nessus PW : nessus
3. User :Openvas PW : openvas
4. Procéder à un scan avancé de Nessus de la VM Win XP, sans authentification (sans username et mot de passe)
5. Procéder à un scan de la VM Win XP avec authentification en utilisant le compte Nessus. (voir capture)
6. Comparer les vulnérabilités trouvées en (1) sans authentification et (2) avec authentification. Expliquer.
7. Procéder à un scan de vulnérabilités de la VM Metasploitable 2.
8. Générer un rapport HTML du scan de Win XP avec authentification.
9. Identifier et expliquer (3) trois vulnérabilités critiques sur la VM XP et (3) sur la VM Metasploitable2.
10. Identifier et expliquer une mesure de mitigation pour la plateforme XP et Metasploitable2 .
11. Exporter le scan créé en (2) soit celui avec authentification dans Metasploit de la VM de Kali.

Partie 4 – Exploitation

Section 4-1 - Requis:

Il s’agira dans cette portion d’obtenir un Shell de Meterpreter sur l’application Easy File Management Server installée sur la VM XP. Pour ce faire, vous devez au préalable démarrer l’application Easy File Management Server. Voir les étapes en Annexes.

Section 4-2 – Phase d’exploitation

1. Pour la phase d’exploitation, procéder aux étapes suivantes:
2. Montrez, en indiquant les étapes, que votre exploit a réussi.
3. Prenez une capture de la VM XP (via votre shell Meterpreter)
4. Effectuer un transfert d’un fichier de Kali vers Win XP (via votre shell Meterpreter)
5. Montrer clairement les étapes d’utilisation d’un Keylogger.
6. Est-il possible de prendre une photo à partir du Shell? Comment?
7. Dans cette portion, utiliser votre créativité pour démontrer l’exploitation d’une autre vulnérabilité sur la VM XP

Annexe A

Démarrage de l’application Easy File Management Server qui est installée sur la VM XP.

|  |  |  |
| --- | --- | --- |
| 1. Ouvrir l’application dans Win XP et cliquez sur Try it! (sans spécifier le username et le mot de passe) | 1. Démarrer le service en cliquant sur Start. Voir flèche. Notez l’adresse IP. | 1. Testez en ouvrant un navigateur à partir d’une autre VM ou de votre poste physique et tapez l’adresse IP identifier en (2) soit celle de XP. Voyez si vous obtenez la page d’authentification suivante. |

**Réponses détaillées**

**Table des matières :**

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

**Partie 1 Reconnaissance …………………………………………….………………………………….…. page**

**Section 1-1 ……………..……………………………………………………………………..……… page**

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

**Partie 2 Titre 2 …………………..……………………………………………………………………….…. page**

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

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

**Partie 3 Titre 3 ………………….……………………………………………………………………….…. page**

**Section 3-1 ……………..……………………………………………………………………..…….… page**

**Section 3-2 ………………..……………………………………………………………..………..……. 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 pentest a été fait en 2 semaines s’étalant sur plusieurs jours du 24 janvier et a prit fin le 08 février 2023. Ce travail avait pour but d’appliquer les étapes à suivre pour effectuer un test de pénétration.**

**Les participants :**

**Pentester Mohamed Malick Balde**

**Voir (nbr points) de chaque question dans la Grille de correction en annexe B**

|  |
| --- |
| Partie 1 : Reconnaissance |

|  |  |  |
| --- | --- | --- |
| Questions : | Réponses et copies écrans de la section |  |

|  |  |
| --- | --- |
| **Section a :**  En utilisation toute l’information publique de Polymtl.ca disponible dans linkedin, Facebook ou toutes autres sources pertinentes d’information :   * <http://www.pentest-standard.org/index.php/Intelligence_Gathering> * <http://www.vulnerabilityassessment.co.uk/Penetration%20Test.html>   Trouver les informations suivantes:  **Question 1 : (nbr points)**  Les noms des dirigeants (utile pour phishing) | Pour cette partie je fais une recherche sur google en utilisant « site :https://.ca intitle :dirigeants » et ce la me redirige vers une page sur le site poly ou je peux trouver le nom des dirigeants qui est le print ecrant et les autres c’est avec linkedin.  Mr D’almeinda ayite qui est un analyste admine du système  Mm Amelie Tanguay directrice ressource humaines  Mr Brunelle Michel chef de section développement |
| **Question 2 : (nbr points)**  Les technologies utilisées et justifier la provenance  (Ex: job pour un sysadmin Linux avec un minimum de 5 ans dans Red Hat) | Job : Analyste informatique-systèmes spécialisés 3 ans d’expérience connaissance des environnements : Hyper-V, Active Directory, VMWARE, Linux, Unix, Windows  <https://www.linkedin.com/jobs/view/3443003623/?refId=dT8%2FlEwJ9FmrGplkZJqJpA%3D%3D&trackingId=vB8aSELytXqocxLhQJYcNg%3D%3D>  Job : Technicienne en informatique 2 ans d’expérience pertinente Linux Ubuntu, Windows serveur 2019, windows serveur 2022, Système de virtualisation HyperV  <https://www.linkedin.com/jobs/view/3449626844/?refId=dT8%2FlEwJ9FmrGplkZJqJpA%3D%3D&trackingId=EOgfPZXqCFK6D6sfRPCoVQ%3D%3D> |
| **Question 3 : (nbr points)**  Les adresses courriels des quelques personnes importantes | Pour les adresses courriels des personnes important j’utilise « Whois » et a travers ces captures nous retrouvons les adresse e-mail de l’administrateur et du technicien qui est «Admin Email: [fmorin@polymtl.ca](mailto:fmorin@polymtl.ca) , Tech Email: [fmorin@polymtl.ca](mailto:fmorin@polymtl.ca)  ; [francis.wanko-naa@polymtl.ca](mailto:francis.wanko-naa@polymtl.ca) ; [david.de-cotis@polymtl.ca](mailto:david.de-cotis@polymtl.ca) ; [amelie.tanguay@polymtl.ca](mailto:amelie.tanguay@polymtl.ca) » |
| **Section b : (nbr points)**  Utiliser **Maltego** pour procéder aux étapes de reconnaissances de  <https://www.megacorpone.com/>  pour soutirer de l’information au sujet des **serveurs DNS, WEB et les adresses courriels**. |  |

|  |
| --- |
| Partie 2 : Scanning |

|  |  |
| --- | --- |
| Questions : | Réponses et copies écrans de la section |
| **Prérequis:**   1. Installer une VM de Metasploitable 2 dans un mode NAT. Le username et le mot de passe par défaut est root. Ref. : <https://www.vulnhub.com/entry/metasploitable-2,29/> 2. Installer une VM de Kali en mode NAT. 3. Assurez-vous que les deux VM sont en mesures de communiquer (Ping) entre elles.  Scanning   En utilisant la commande « nmap » , Effectuez les requêtes suivantes :  **Question 1 : (nbr points)**  Ping scans – fast scan | Scanning à partir de la VM de Kali vers la VM de Metasploitable2.  **Mettre la copie d’écran de la commande et les résultats dans Réponse A**   |  |  | | --- | --- | |  | Réponse A: |   Scanning à partir de la VM de Kali vers le site <http://scanme.nmap.org/>  **Mettre la copie d’écran de la commande et les résultats dans Réponse B**   |  |  | | --- | --- | |  | Réponse B: | |
| **Question 2 : (nbr points)**  SYN scans – all ports | Scanning à partir de la VM de Kali vers la VM de Metasploitable2.  **Mettre la copie d’écran de la commande et les résultats dans Réponse A**     |  |  | | --- | --- | |  | Réponse A: |   Scanning à partir de la VM de Kali vers le site <http://scanme.nmap.org/>  **Mettre la copie d’écran de la commande et les résultats dans Réponse B**   |  |  | | --- | --- | |  | Réponse B: | |
| **Question 3 : (nbr points)**  TCP Connect scans – top ports | Scanning à partir de la VM de Kali vers la VM de Metasploitable2.  **Mettre la copie d’écran de la commande et les résultats dans Réponse A**     |  |  | | --- | --- | |  | Réponse A: |   Scanning à partir de la VM de Kali vers le site <http://scanme.nmap.org/>  **Mettre la copie d’écran de la commande et les résultats dans Réponse B**   |  |  | | --- | --- | |  | Réponse B: | |
| **Question 4 : (nbr points)**  UDP scans – top 100 ports | Scanning à partir de la VM de Kali vers la VM de Metasploitable2.  **Mettre la copie d’écran de la commande et les résultats dans Réponse A**     |  |  | | --- | --- | |  | Réponse A: |   Scanning à partir de la VM de Kali vers le site <http://scanme.nmap.org/>  **Mettre la copie d’écran de la commande et les résultats dans Réponse B**   |  |  | | --- | --- | |  | Réponse B: | |
| **Question 5 : (nbr points)**  OS fingerprinting scans | Scanning à partir de la VM de Kali vers la VM de Metasploitable2.  **Mettre la copie d’écran de la commande et les résultats dans Réponse A**     |  |  | | --- | --- | |  | Réponse A: |   Scanning à partir de la VM de Kali vers le site <http://scanme.nmap.org/>  **Mettre la copie d’écran de la commande et les résultats dans Réponse B**   |  |  | | --- | --- | |  | Réponse B: | |
| **Question 6 : (nbr points)**  Un Version Scan sur les ports 21, 22, 23 et 53 | Scanning à partir de la VM de Kali vers la VM de Metasploitable2.  **Mettre la copie d’écran de la commande et les résultats dans Réponse A**     |  |  | | --- | --- | |  | Réponse A: |   Scanning à partir de la VM de Kali vers le site <http://scanme.nmap.org/>  **Mettre la copie d’écran de la commande et les résultats dans Réponse B**   |  |  | | --- | --- | |  | Réponse B: | |
| **Question 7 : (nbr points)**  Un Version scan sur les ports ouverts trouvés en (5) | Scanning à partir de la VM de Kali vers la VM de Metasploitable2.  **Mettre la copie d’écran de la commande et les résultats dans Réponse A**     |  |  | | --- | --- | |  | Réponse A: |   Scanning à partir de la VM de Kali vers le site <http://scanme.nmap.org/>  **Mettre la copie d’écran de la commande et les résultats dans Réponse B**   |  |  | | --- | --- | |  | Réponse B: | |
| **Question 8 : (nbr points)**  Un scan NSE sur les ports ouverts trouvés en (5) | Scanning à partir de la VM de Kali vers la VM de Metasploitable2.  **Mettre la copie d’écran de la commande et les résultats dans Réponse A**     |  |  | | --- | --- | |  | Réponse A: |   Scanning à partir de la VM de Kali vers le site <http://scanme.nmap.org/>  **Mettre la copie d’écran de la commande et les résultats dans Réponse B**   |  |  | | --- | --- | |  | Réponse B: | |

|  |
| --- |
| Partie 3 : Scan de vulnérabilités |

|  |  |
| --- | --- |
| Questions : | Réponses et copies écrans de la section |
| **Prérequis :**   1. VM de Win XP (rendu disponible par le prof) en mode NAT   <https://polymtlca0-my.sharepoint.com/:u:/g/personal/hector_bustillo_polymtl_ca/ESK6HoR6_5BJop1bcmtEIyYBgUt6B94fh7ISawWr4Eb9PQ?e=WZoYkt&isSPOFile=1>   1. VM de Kali (disponible dans le WEB) en mode NAT 2. Vm de Metasploitable 2 (disponible dans le WEB) en mode NAT    3. Scan de vulnérabilités   Téléchargez et configurez la VM de Windows XP **rendue disponible par votre prof.**  **Utilisateurs de la VM XP :**   1. User : admin PW : (à vous de deviner) 2. User :Nessus PW : nessus 3. User :Openvas PW : openvas   **----------------------------------------**  **Question 1 : (nbr points)**  Procéder à un scan avancé de Nessus de la VM Win XP, sans authentification (sans username et mot de passe) | Le mot de passe User : admin est Admin  L’adresse IP de la machine XP est 192.168.29.138  Pour metasploit est 192.168.29.131  ---------------------------------------------------------------------------------------------------------------------------  **Déposer les copies d’écran des résultats (Pas des liens et pas des fichiers annexes)**  Je vais faire un scanne sans authentification en specifiant l’adresse ip de la machine et le mask réseaux des machines |
| **Question 2 : (nbr points)**  Procéder à un scan de la VM Win XP avec authentification en utilisant le compte Nessus. (voir capture)  C:\Users\Lucian\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\F87E15B3.tmp | **Déposer les copies d’écran des résultats (Pas des liens et pas des fichiers annexes)**  Je fais un scanne avec authentifications sur le compte de Nessus, pour ce scanne j’ai du faire rentrer mon Username et passeword et modifier l’horreur dans l’ongle Schedule et Credentials |
| **Question 3 : (nbr points)**  Comparer les vulnérabilités trouvées en (1) sans authentification et (2) avec authentification. Expliquer. | **Un scanne vulnérabilité avec authentification effectué un scanne complet qui va rassemble tous les informations liées a la sécurité de notre système incluent les logiciels installés en fin de pouvoir effectué un scanne plus avancer et de nous les vulnérabilités de notre système comme le montre dans les captures le scanne avec authentification on découvre plus de vulnérabilités et tant dis que le sans authentification nous montre quelque vulnérabilité et dans mon cas pour le sans authentification après avoir fini de spécifier ma plage d’adresse IP qui est 192.168.29.138 pour le sans authentification quand je le lance c’est comme s’il vérifier le réseau au complet et me donne moyen de vulnérabilité comparer à celui avec authentification** |
| **Question 4 : (nbr points)**  Procéder à un scan de vulnérabilités de la VM Metasploitable 2 | **Déposer les copies d’écran des résultats (Pas des liens et pas des fichiers annexes)**  Je vais faire un scanne de la machine metasploitable 2        Cette partie nous montre les vulnerabilites dans metasploit ce qui est critique, elevé …. |
| **Question 5 : (nbr points)**  Générer un rapport HTML du scan de Win XP avec authentification. | **Déposer les copies d’écran des résultats (Pas des liens et pas des fichiers annexes)**  Je générer un rapport HTML du scan que j’ai fait avec authantification      **Ici après l’exploitation je le convertis en txt qui nous montre les balises forma Html** |
| **Question 6 : (nbr points)**  Identifier et expliquer (3) trois vulnérabilités critiques sur la VM XP et (3) sur la VM Metasploitable2. | **Vulnérabilités sur XP :**  Microsoft Windows XP Unsupported Installation Detection: Cette vulnérabilité touche le système d’exploitattion à distance ce qui fait qu’il n’est plus pris en charge car le manque de support indique qu’il y a aucun nouveau correctif de sécurité effectué il contient des failles de sécurité .  MS12-014: C’est une vulnérabilité qui est identifier par le CVE-2010-3138, elle permet l’exécution d’un code à distance arbitrairement en tant qu’utilisateur connecté ce qui fait qu’un attaquant pourrait alors installer des programmes afficher ou modifier et voire même supprimer des données  MS09-062: C’est une vulnérabilité qui pourrait permettre l’exécution d’un code à distance directement sur le hôte, l’attaquant a juste a envoyer un fichier image mal formé à un utilisateur et attendre que l’utilisateur l’ouvre avec une application de Microsoft  **Vulnérabilité Metasploitable2 :**  NFS Exported Share Information Disclosure : C’est un moins de partage NFS qui est (Network File System) il est exporter par le serveur a distance et il peut être monté par l’hôte d’analyse ce qui fait que un attaquant peut en tirer parti pour lire et écrire sur les fichiers hôte à distant sans qu’il n’ait l’autorisations.  Unix Operating System Unsupported Version Detection : Ce système d’exploitation n’est plus pris en charge car c’est une vulnerabilité qui n’a eu aucun nouveau correctif de sécurité, il contient des failles de sécurité ce qui fait qu’il n’est plus publié par le fournisseur  VNC Server 'password' Password: C’est une vulnérabilité qui touche la sécurité au niveau des mots de passes car le mot de passe qui est utilisé par le serveur VNC qui est exécuté par le hôte à distant est sécurisé avec un faible mot de passe, ce qui pourrait être facile pour un attaquant à distance qui n’est pas authentifie d’exploiter ou prendre le contrôle de notre système |
| **Question 7 : (nbr points)**  Identifier et expliquer une mesure de mitigation pour la plateforme XP et Metasploitable2 . | **Samba Badlock Vulnerability: Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.**  Cet mitigation à été recommandé parce que la vulnérabilité de Samba CVE-2021 -44142 permettait aux attaquants d’exécuter du code arbitraire sur les installations affecté de samba, sans être authentifié et peut même aller jusqu’à prendre le contrôle de votre machine. Donc pour éviter cela des correctifs ont été publiés en fin de renforcer le système de sécurité.  [Samba - Mises à jour de sécurité et informations](https://www.samba.org/samba/history/security.html) |
| **Question 8 : (nbr points)**  Exporter le scan créé en (2) soit celui avec authentification dans Metasploit de la VM de Kali. | **Déposer les copies d’écran des commandes et des résultats (Pas des liens et pas des fichiers annexes)**  **-Dans ce cas j’ai fais une capture d’écrant montrent ou cliquer pour commencer l’exportation du scan** |

Partie 3 : S

cités

|  |  |
| --- | --- |
| **4. Exploitation** |  |
| Il s’agira dans cette portion d’obtenir un Shell de Meterpreter sur l’application Easy File Management Server installée sur la VM XP.  **Section A :**  Pour ce faire, vous devez au préalable démarrer l’application Easy File Management Server**. Voir les étapes en Annexes.**  Pour la phase d’exploitation, procéder aux étapes suivantes:    **-----------------------------------**  **Question 1 : (nbr points)**  Montrez, en indiquant les étapes, que votre exploit a réussi. | **Déposer les copies d’écran des commandes et des résultats (Pas des liens et pas des fichiers annexes)** |
| **Question 2 : (nbr points)**  Prenez une capture de la VM XP (via votre shell Meterpreter) | **Déposer les copies d’écran des résultats (Pas des liens et pas des fichiers annexes)** |
| **Question 3 : (nbr points)**  Effectuer un transfert d’un fichier de Kali vers Win XP (via votre shell Meterpreter) | **Dans cette partie je fais un transfert de fichier de kali vers le win XP** |
| **Question 4 : (nbr points)**  Montrer clairement les étapes d’utilisation d’un Keylogger. | **La partie keylogger j’ai fait des recherches et c’est cette façon j’ai trouvé** |
| **Question 5 : (nbr points)**  Est-il possible de prendre une photo à partir du Shell? Comment? | **Déposer les copies d’écran des commandes et des résultats (Pas des liens et pas des fichiers annexes)** |
| **Section B : (nbr points)**  Dans cette portion, utiliser votre créativité pour démontrer l’exploitation d’une autre vulnérabilité sur la VM XP | **Déposer les copies d’écran des commandes et des résultats (Pas des liens et pas des fichiers annexes)** |

**Conclusion :**

Ce devoir m’a permis de mettre en pratique les connaissances que j’ai acquis pendant ces 4 semaines de cours dans le 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 a faire du scanning des ports avec quoi on pourra utiliser pour gagner l’accès et j’ai eu a utiliser des outils comme maltego qui nous facilite a trouver des adresses DNS etc… . En guise de conclusion il serait très importants d’appliquer les étapes énuméré ci haut en fin de pouvoir effectuer un bon teste d’intrusion et cela nous permettra de découvrir les failles qui sont dans notre réseaux ou système.

**Références :**

<https://www.offensive-security.com/metasploit-unleashed/keylogging/>

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

<https://www.tenable.com/plugins/nessus/42118>

[La vulnérabilité Samba: qu’est-ce que CVE-2021-44142 et comment y remédier (trendmicro.com)](https://www.trendmicro.com/en_gb/research/22/b/the-samba-vulnerability-what-is-cve-2021-44142-and-how-to-fix-it.html)

https://www.samba.org/samba/history/security.html

**Annexe B : Grille de correction**

