

Travail pratique 1

Présenté à M. Bresteau  
INF4420A Sécurité informatique

Fait par :

Étienne Asselin 1773922  
Vincent Rodier 1744784  
Groupe laboratoire 01

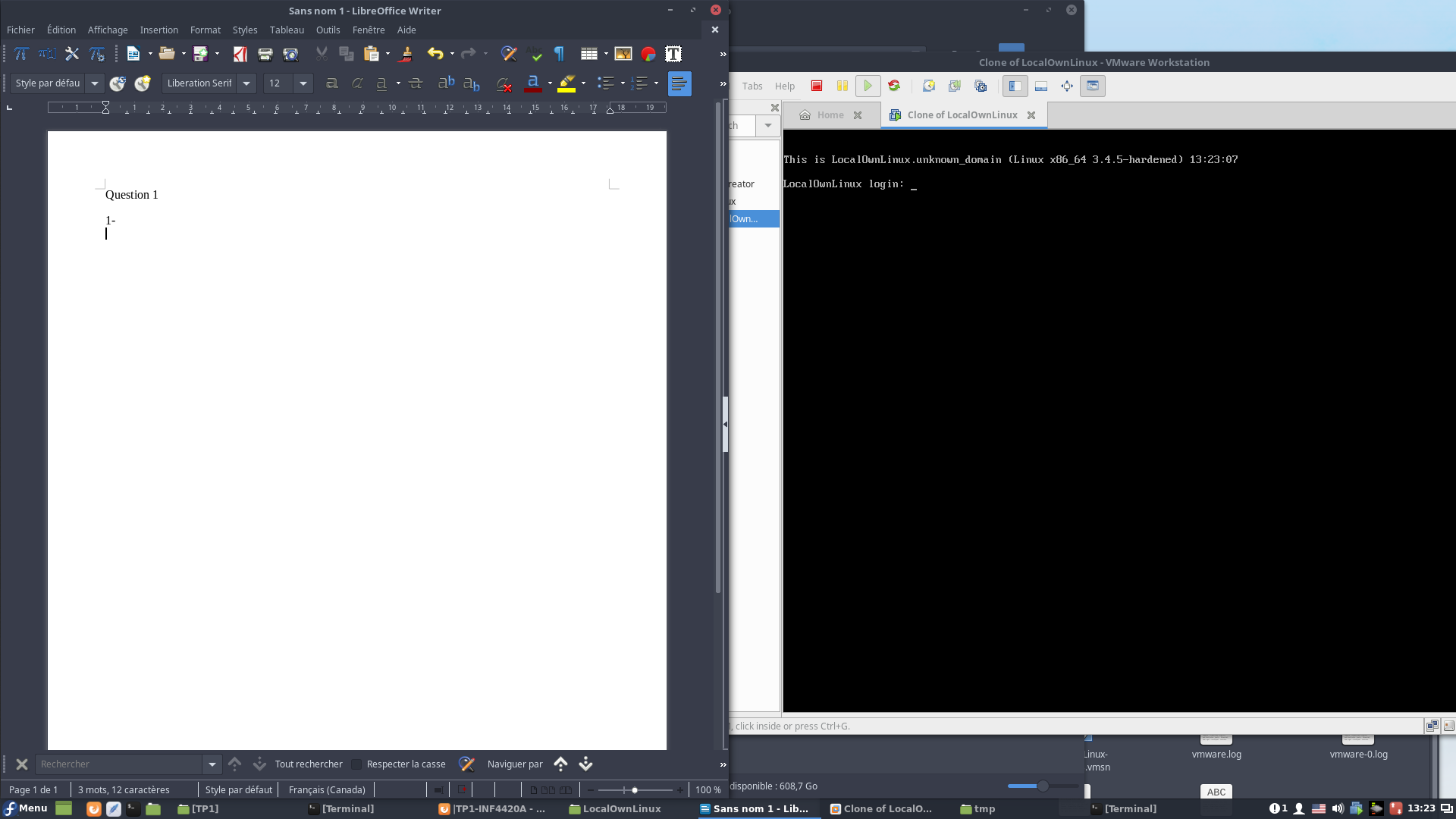
Le vendredi 9 février 2018  
École Polytechnique de Montréal

Question 1

Phase de reconnaissance

1. Démarrer la machine virtuelle (VM) et essayer de vous connecter à une session. Que constatez-vous ?

Rep : Il est impossible de se connecter sans les informations de connexion.



2. Redémarrez la VM et au démarrage appuyez sur F2 pour rentrer dans le BIOS. Que se passe-t-il ?

Rep : On doit absolument entrer un mot de passe pour pouvoir accéder au BIOS.



3. Appuyez sur Echap pour continuer le boot de la machine. A l’écran de Grub (fond violet), appuyer sur une touche quelconque (sauf Entrée). Cet écran présente les différentes options de boot pour la machine, dans notre cas il n’y a qu’une seule ligne correspond au système Gentoo Linux. Habituellement il est possible d’éditer la ligne de commande correspondante en appuyant sur la touche e.

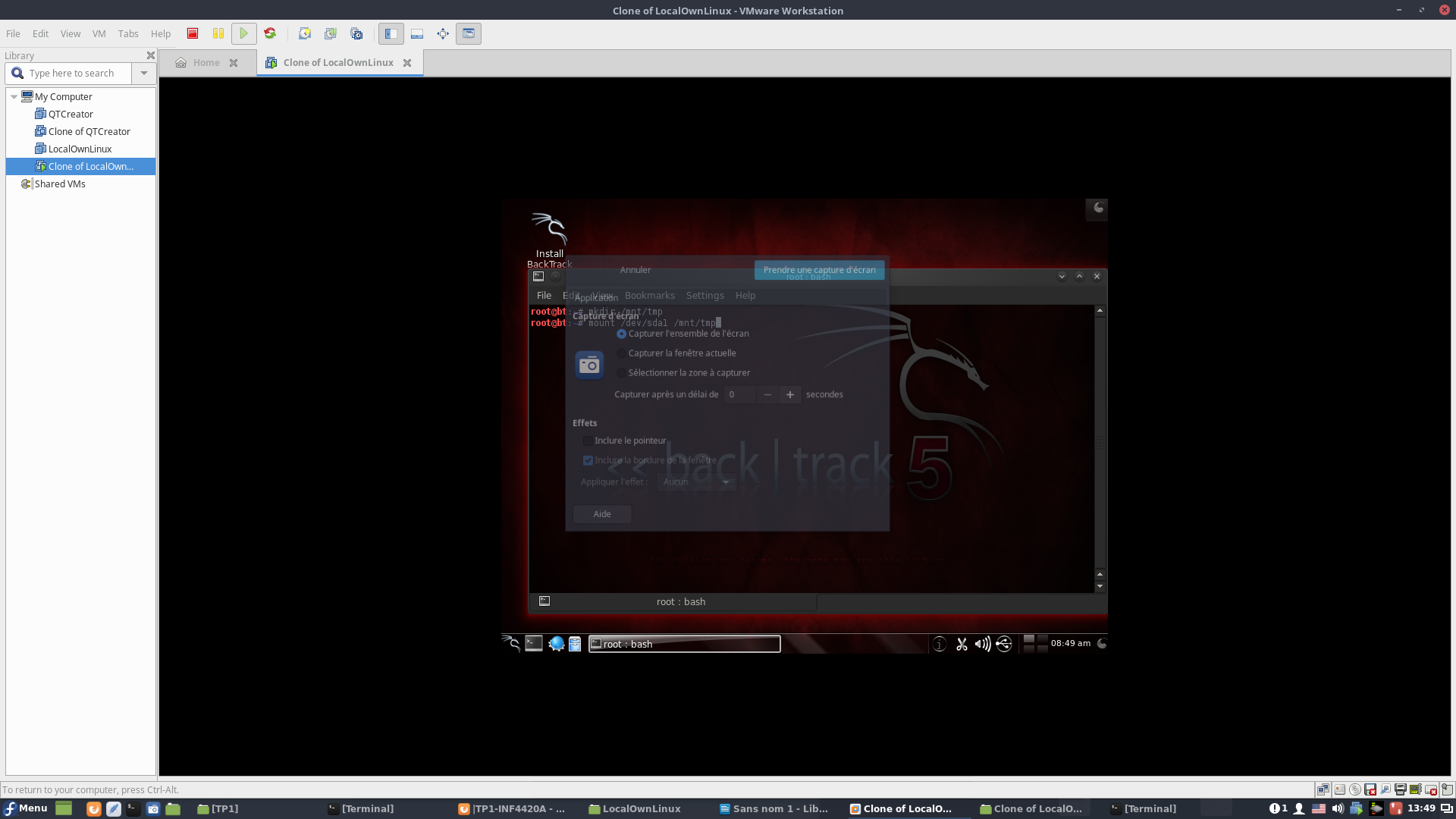
4. Est-ce possible dans notre cas ? Sinon, pourquoi ?

Rep : Dans notre cas, il n’est pas possible d’éditer la ligne de commande. Il préalablement entré un mot de passe afin d’accéder à des options supplémentaires.

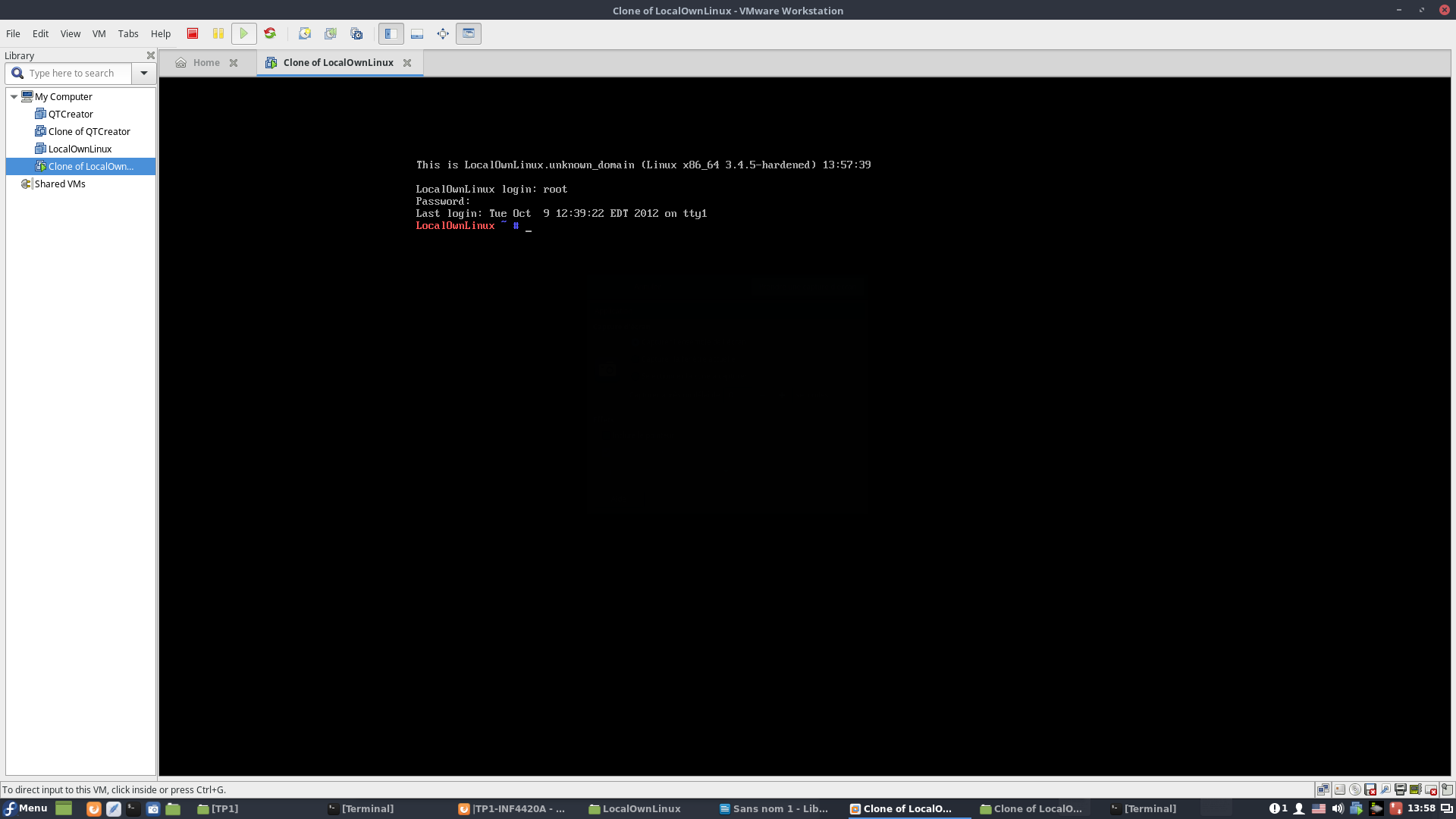


Réalisation de l’attaque

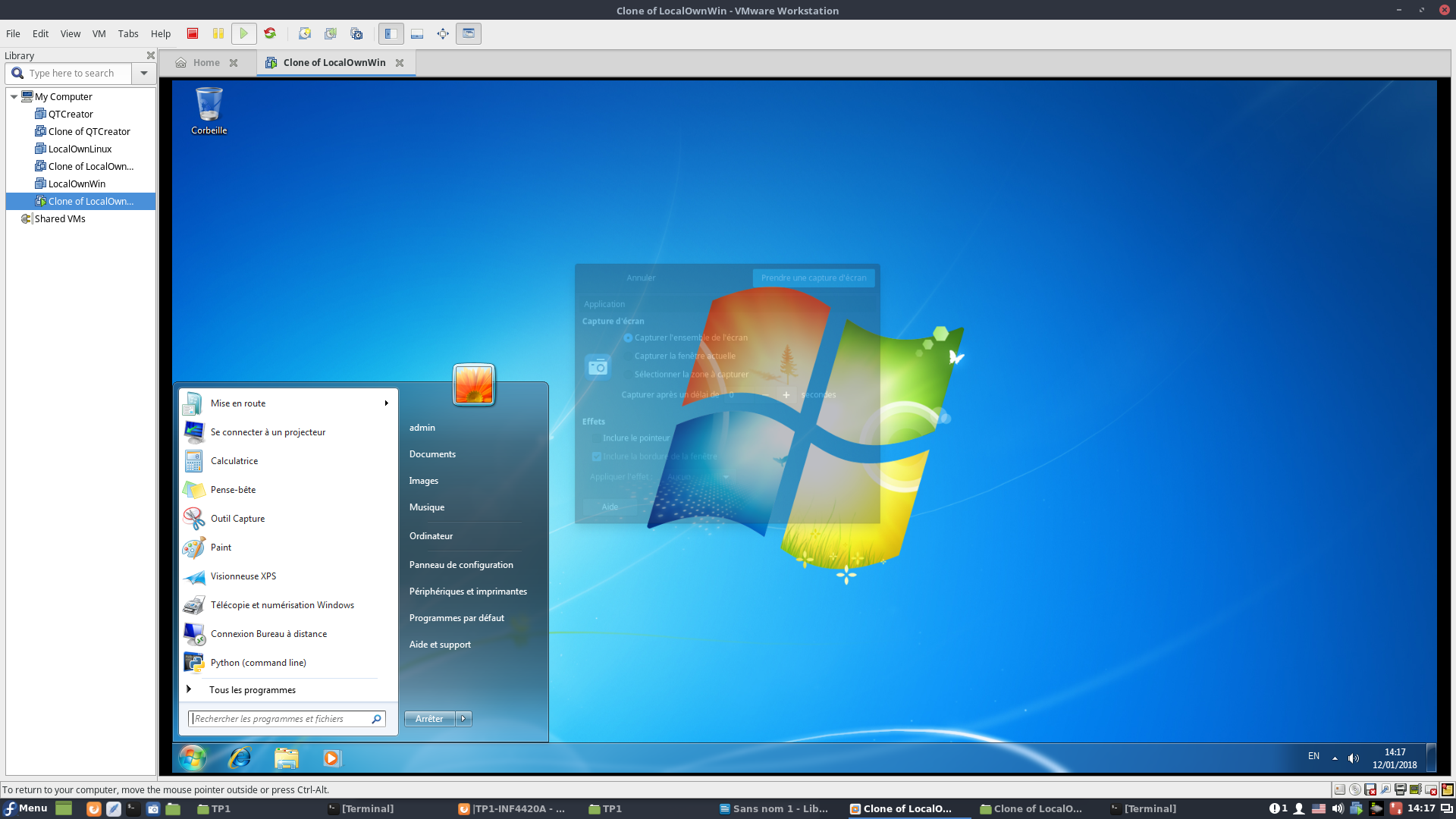
Étape 1 à 4 réaliser :



Réalisation des étapes 5 à 7 :



Preuve de la réalisation de l’attaque sur la machine virtuel Windows :



**Question 7 Machine LocalOwnWin**

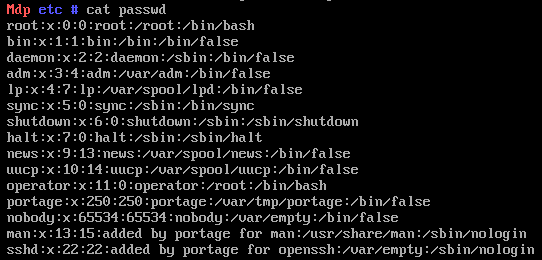
5. Expliquez à quoi sert ce fichier SAM

Le fichier SAM correspond à Sécurity Account Manager. C’est un fichier dans lequel est enregistrer les mots de passes des usagers. C’est mots de passes sont hasher et peuvent servent à l’authentification des utilisateurs sur la machine.

Question 2

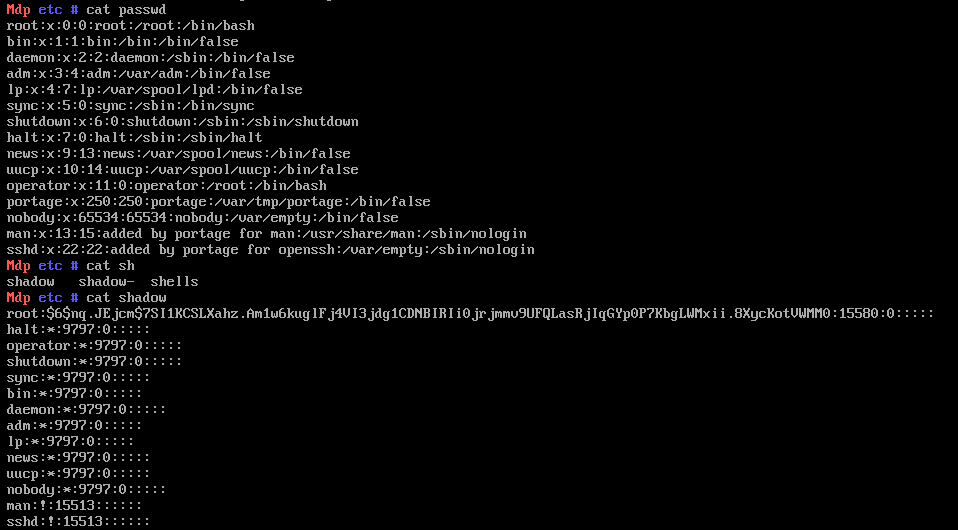
1. Examinez le fichier /etc/passwd. Contient-il des mots de passe ? Pourquoi? Quelles sont ses permissions d’accès? Pourquoi ?

Le fichier ne semble pas contenir de mot de passe explicite. Plusieurs personnes ont accès à ce fichier en lecture et il ne serait pas sécuritaire de simplement écrire les mots de passes dans un fichier. L’auteur du fichier à des droits de lecture et d’écriture, tandis que tous les autres utilisateurs ont simplement les droits en lecture.

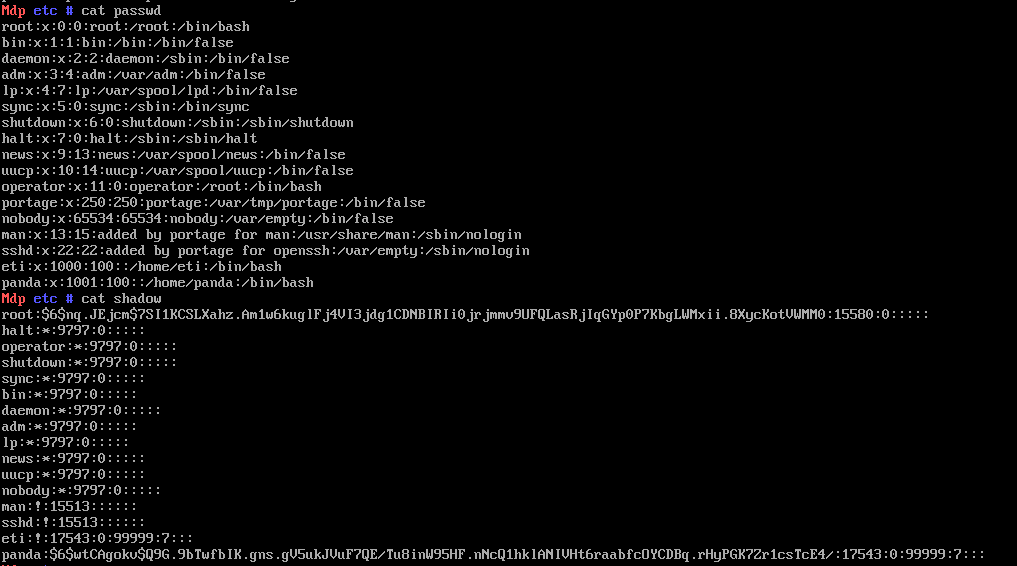


1. Observez ce qui se passe dans les fichiers passwd et shadow. Lequel ou lesquels de ces deux fichiers sont modifiés ? Pourquoi ?

Les deux fichiers sont modifiés. Les deux fichiers contiennent une ligne supplémentaire avec le nom du nouvel utilisateur. Le fichier shadow semble cependant contenir la valeur hasher du mot de passe de l’utilisateur.

Avant :  
  
Après :

1. Qu'est-ce que vous remarquez dans les fichiers passwd et shadow? Lequel de ces deux fichiers change? Pourquoi ? Où se trouve donc l’information du mot de passe? Quelles sont les permissions du fichier shadow et pourquoi ?

Le fichier passwd n’a pas subi de modification à la suite du changement du mot de passe de l’utilisateur, mais le fichier shadow oui. L’information du mot de passe est contenue dans la longue chaine de caractère suivant le nom de l’utilisateur (mot de passe hasher). Les permissions du fichier shadow sont d’écriture et de lecture pour le créateur du fichier. Les utilisateurs faisant parti d’un certain groupe on accès au fichier shadow en lecture seulement et les autres utilisateurs n’ont simplement aucun droit. Les droits du fichier shadow sont strict puisqu’il contient des informations sensibles de sécurité. Ainsi seulement son créateur (root) à droit d’accéder à se fichier en mode écriture.  
  




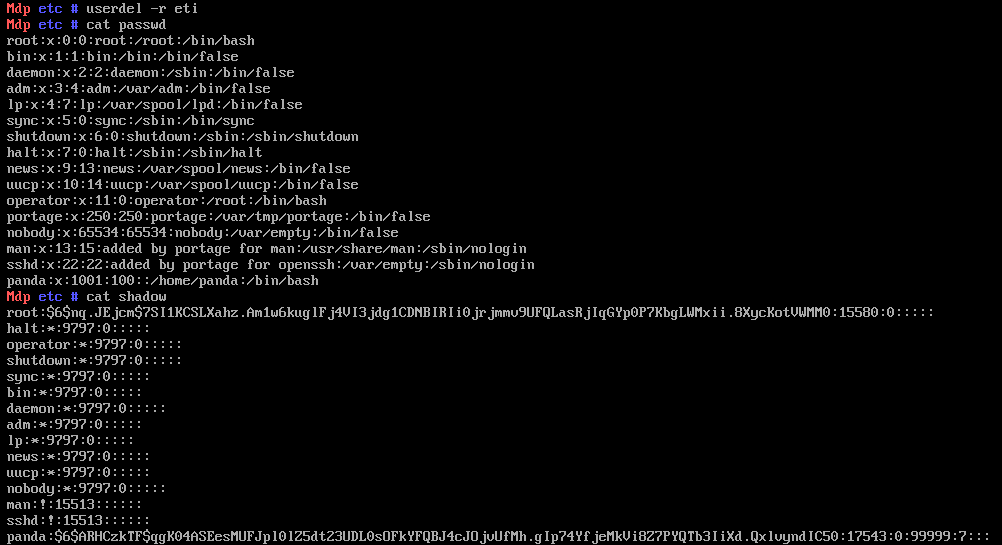
1. Changez à nouveau le mot de passe du même utilisateur et donnez-lui le \*même\* mot de passe. Est-ce que les informations du mot de passe ont changé? Pourquoi?

Les informations du mot de passe ont changé puisque en “modifiant” le mot de passe, un nombre générer automatiquement que l’on appelle « salt » est regénérer et se salt est ajouté au mot de passe avant d’être hasher, donc même si le mot de passe est identique, le salt ne l’est pas et donc le résultat du hash est différent.

1. Estce que ceci est possible? Expliquez pourquoi. Quel est le problème?

Oui il est possible de se connecter au deuxième compte avec le mot de passe du premier compte. Cela est possible parce que le hash mis par force au deuxième utilisateur est un hash valide. Le problème est donc que si on peut modifier le fichier shadow, nous avons seulemtn besoin de connaitre un seul mot de passe

1. Effacez cet utilisateur avec la commande $ userdel –r NOM. Qu'est-ce qui se passe dans passwd et shadow ?

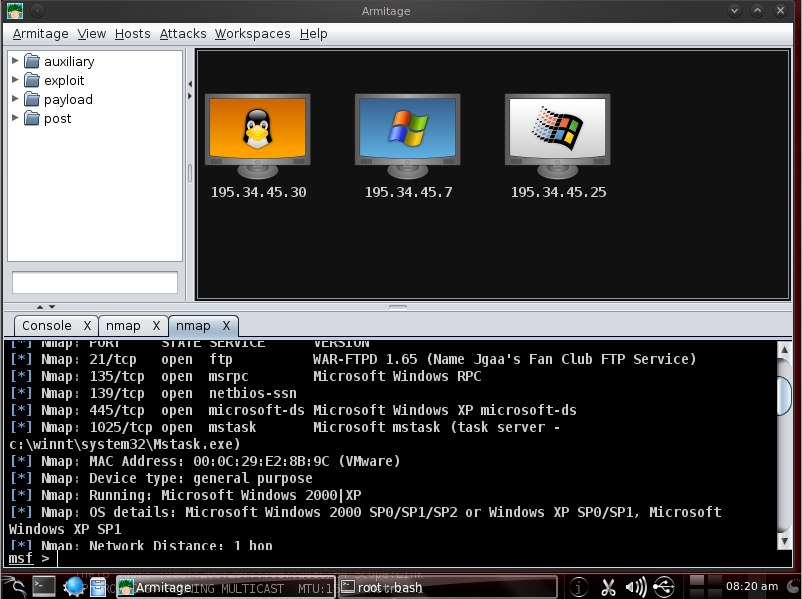
L’entrée de l’utilisateur est supprimée.   


Question 3

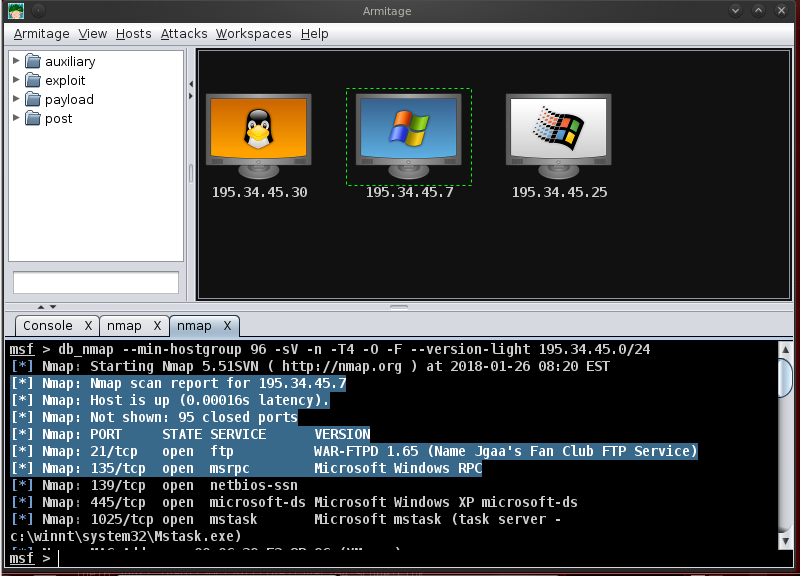
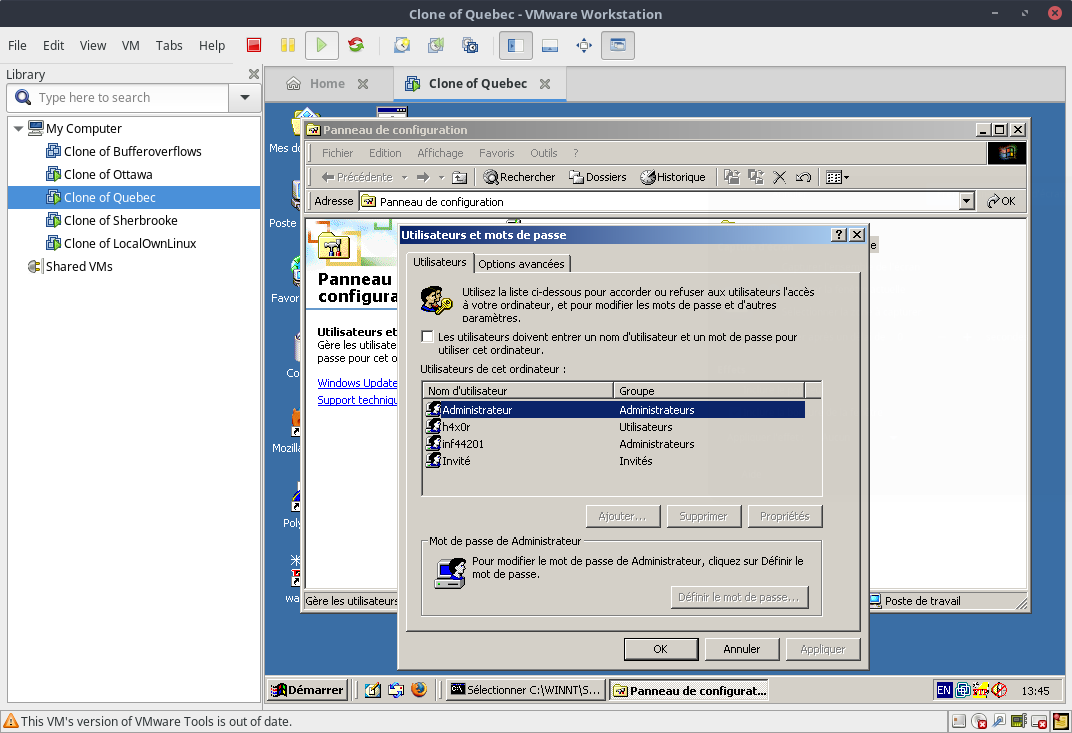
décrivez quels mots de passe vous avez trouvés, à quels usagers ils correspondent et sur laquelle des deux machines (1 et 2) ils se trouvent.

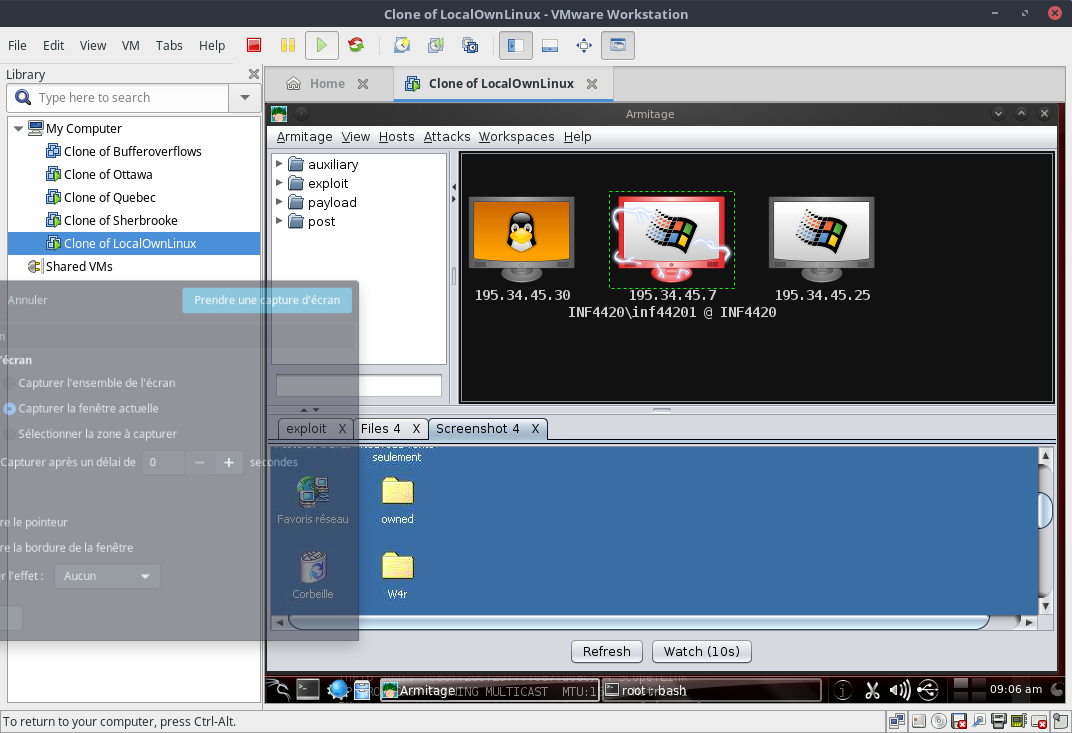
Question 4

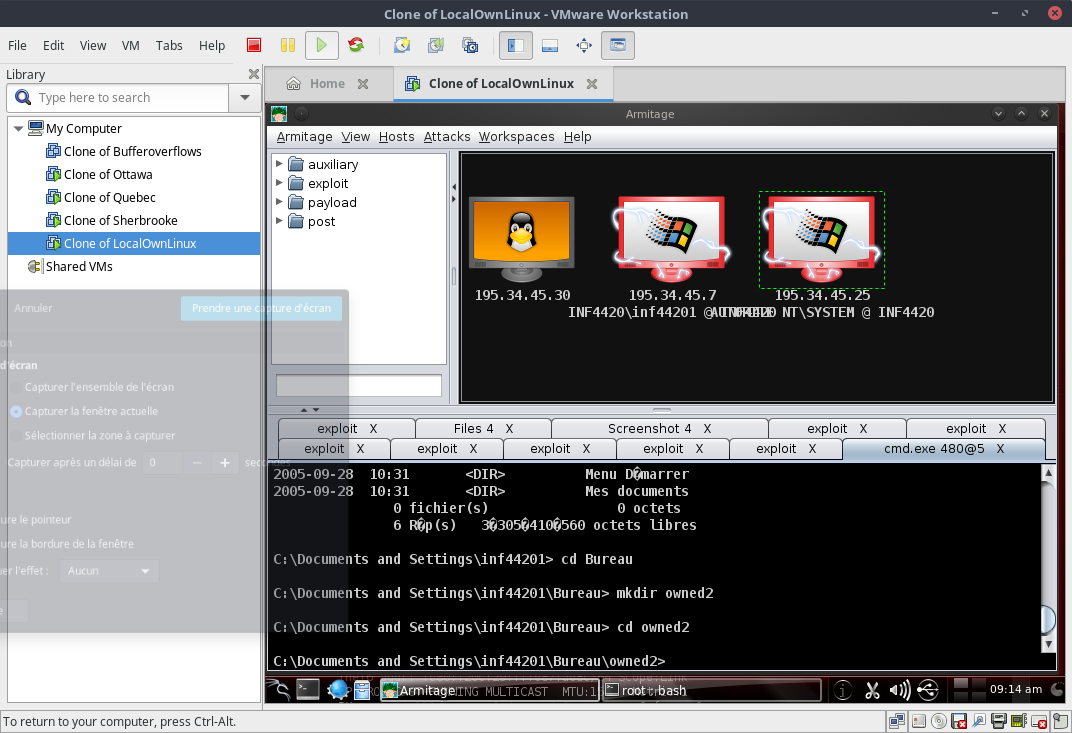
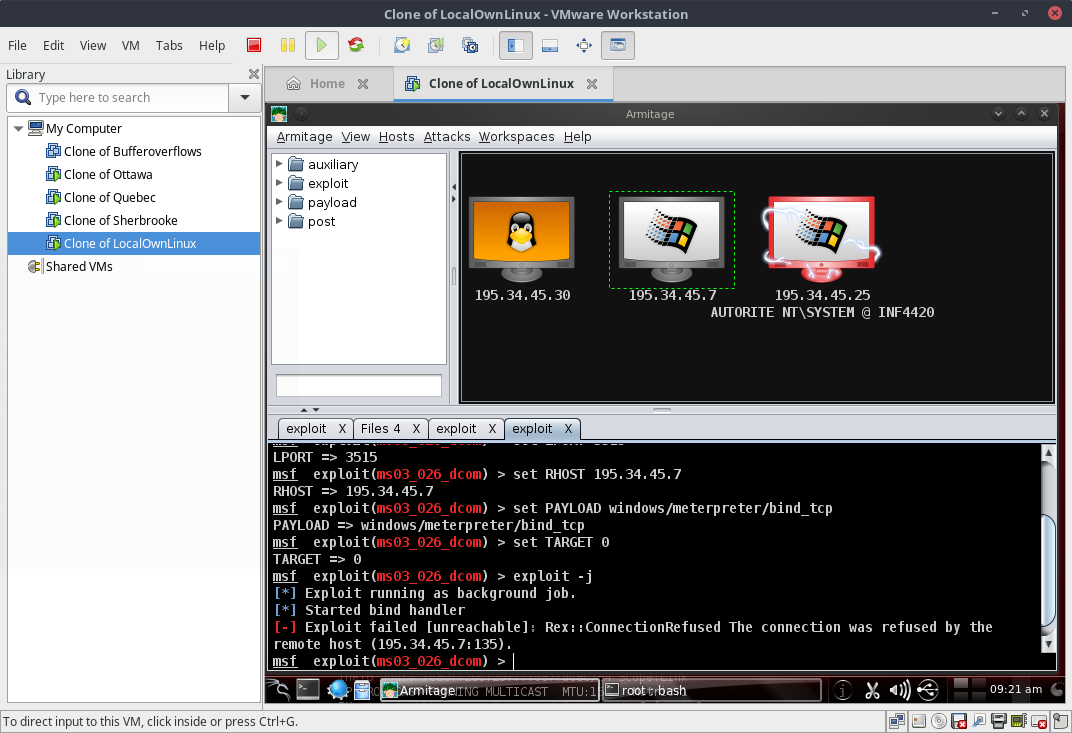
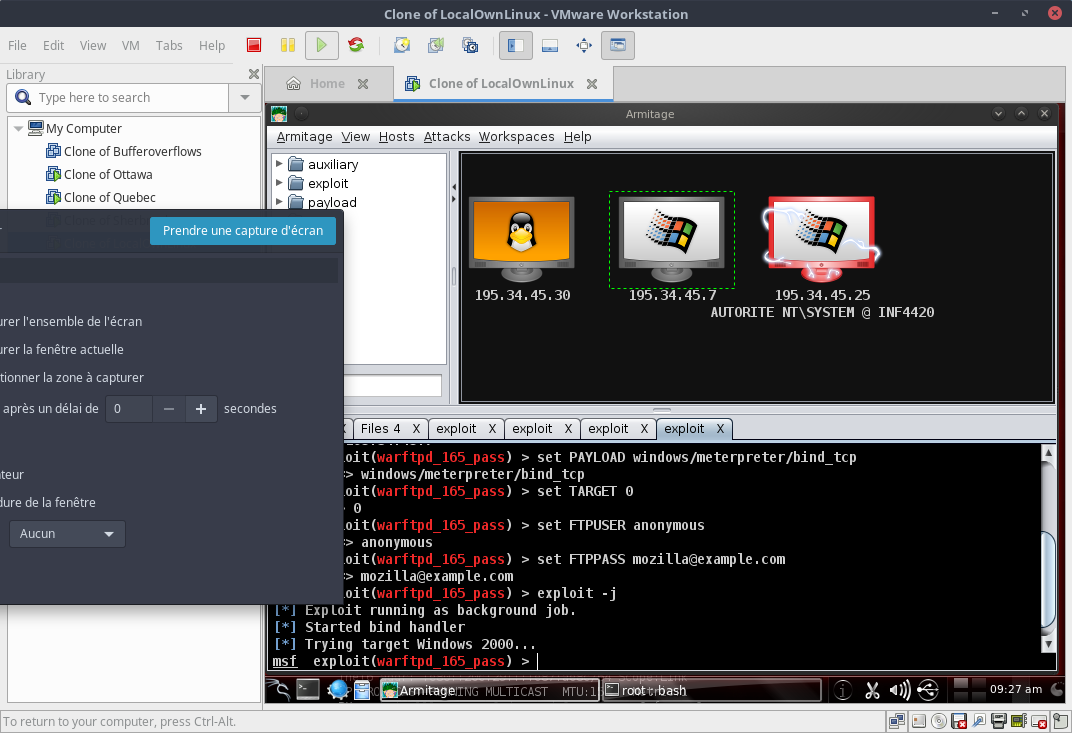
Phase de reconnaissance

1. Expliquez en quoi la modification effectuée en 2. ne serait pas nécessaire si vous étiez dans votre sous-sol chez votre mère en train de vouloir hacker les serveurs Québec, Ottawa et Sherbrooke ?  
     
   Dans le sous-sol de notre mère, il y a un routeur qui s’occuperait de changer notre adresse IP privé en adresse IP public.
2. Le scan à trouver 3 machines différentes avec les huit derniers bits d’adresse 30, 7 et 25. nMap permet de détecter tous les ports ouverts dans la plage d’adresse à scanner. Une fois un port détecter, le programme affiche les machines visibles.  
     
   

Exploitation de failles de sécurité connues

1. Dans le cas du système installé sur les machines de ce TP, nous avons remarqué que, sur une d’elle, le service rpcdcom écoute par défaut sur le port 135. Quelle est cette machine ?  
     
   Le scan à trouver le port 135 ouvert sur la machine avec l’adresse IP 195.34.45.7. C’est une machine qui roule le système d’exploitation Windows 2000 et qui correspond à la VM Québec.  
     
   
2. Utilisez l’exploit ms03\_026\_dcom sur cette machine. Cet exploit profite d’une faille de sécurité dans le service rpcdcom. Quel est le résultat ? Quelles sont les nouvelles possibilités avec cette machine cible ?  
     
   La machine est devenue rouge dans l’interface graphique. Il est maintenant possible d’utiliser un explorateur de fichier et de parcourir les fichiers de la victime entre autres. Il est aussi possible d’avoir un invité de commande. Une nouvelle option est disponible qui se nomme meterpreter1 qui permet d’avoir accès à beaucoup d’option sur l’ordinateur de la victime.
3. Grâce à l’exploit précédent ajoutez un utilisateur "h4x0r" avec le mot de passe "toto" sur la machine cible et créez un répertoire "owned" sur le bureau de l'utilisateur inf44201 (C:\Documents and Settings\inf44201\Bureau). Vous devez donner un listing des commandes que vous avez utilisées, une explication de votre démarche et une preuve des résultats (captures d’écran).  
     
   Afin de créer un nouvel utilisateur, nous avons ouvert un invité de commande et entré la ligne : net user h4x0r toto /ADD. Cela à créer un nouvel utilisateur nommé h4x0r avec le mot de passe toto. Pour créer un dossier sur le bureau, nous avons ouvert un explorateur de fichier et simplement ajouter le dossier sur le bureau.  
     
     
     
   



1. Une autre faille a aussi été détectée sur la même machine. Cette faille concerne le service WarFTPD et elle exploite le débordement de tampon dans la commande PASS de la version 1.65 de cette application. Comme vous le savez, WarFTPD est un serveur FTP utilisant par défaut le port 21. Trouvez cet exploit et utilisez-le afin de créer un répertoire sur la machine cible. Pour qu’il s’affiche il faut changer le « Exploit Rank » à « Poor » dans le menu « Armitage » et relancer la recherche des exploits.  
     
   Comme pour l’attaque de la question précédente, nous avons tout simplement ouvert un explorateur de fichier et nous avons créé un fichier nommé W4R sur le bureau. La figure de la question précédente sert aussi de preuve de notre réussite à cette question.
2. Pour cette attaque, nous avons utilisé l’exploit ms08\_067\_netapi sous l’onglet smb.   
   List de commande :  
   cd ../..  
   cd “Documents and settings/inf44201/Bureau”  
   mkdir owned2  
     
   
3. Vérifier que l’exploit n’est plus réalisable (capture d’écran).  
     
   
4. Redémarrez la machine et vérifier que l’exploit n’est plus réalisable (capture d’écran).  
     
   

Question 5

Question 6

1. Donnez la séquence exacte de caractères à entrer. Expliquez brièvement comment votre « hack » fonctionne.

Avec exactement 60 caractères aléatoires dans le champ username l’entré au site est toujours garanti. Il en est de même avec 100, 140 et 180 caractères aléatoires. Notre hack fonctionne en écrasant la valeur du nom d’utilisateur par une valeur arbitraire et en écrasant la valeur du mot de passe par le caractère de fin de ligne. Ainsi lorsque l’on se connecte avec par exemple 60 caractères, le nouveau nom d’utilisateur “root” est remplacé par les 20 derniers caractères entrés et le mot de passe est remplacé par “\0“ qui est ajouté lorsque l’on tente de se connecter.

1. Que faudrait-il changer dans le programme pour enlever ce problème de sécurité?

Possiblement en mettant un nombre de caractère maximum dans le champ username. Il serait aussi possible d’ajouter une variable canarie. Par exemple, en ajoutant une chaine de caractère directement après la déclaration du password et en vérifiant l’intégrité de cette variable avant chaque tentative de connexion.

Question 7

Notre hack exploite une vulnérabilité dans la fonction afficher. Lorsque le programme utilise la méthode scanf, tous les caractères dans le buffer d’entré sont pris en compte et il est donc possible de faire un buffer overflow. Il faut commencer par inscrire 20 caractères aléatoires afin de remplir la mémoire allouer au tableau pour le nom du fichier et ensuite inscrire un autre 8 caractères aléatoires afin de combler l’espace restante entre notre programme et l’endroit où est enregistrer la valeur du registre EIP. Les 4 prochains caractères qui sont inscrit correspondent donc à l’adresse de la prochaine instruction à exécuter (dans notre cas : 004010E0). On commence par entrer l’adresse par 0xE0 qui correspond au caractère « ù » dans le code ascii.

L’utilisation de la méthode fgets en spécifiant le bon nombre de caractère à prendre en entré à la place de la méthode scanf serait une façon de régler le problème de sécurité.

