Toutes les parties sont à remettre sur Github Classroom. Les delais sont strictes càd que vous aurez 0 si en cas de non-respect des délais. Vous traiterez la fiche avec le chargé de TD/TP avant toute remise des rapports.

1 Commandes de bases [5.5 pts]

1. Taper la commande vous permettant d'afficher le système installé
2. Taper la commande vous permettant d'afficher la distribution installée
3. Taper la commande vous permettant de connaitre les utilisateurs en cours du système
4. Taper la commande vous permettant d'ouvrir un nouveau terminal en mode utilisateur
5. Taper la commande permettant de fermer le terminal
6. Rediriger les 5 dernières commandes que vous venez de taper dans le fichier partie1.txt (**history 5 > partie1.txt**)

2 Commande utilisateurs [10.5 pts]

1. Afficher à l'écran à quoi sert la commande man.
2. Taper la commande qui permet de lister le contenu du repertoire /etc
3. Taper la commande vous permettant de lister de manière détaillée le contenu du répertoire /etc
4. Taper la commande vous permettant d'afficher le contenu du répertoire /dev
5. Taper la commande vous permettant d'afficher le contenu du fichier /etc/passwd
6. Taper la commande vous permettant d'afficher le contenu du fichier /etc/shadow (Affiche à l'écran du terminal le résultat)
7. Taper la commande vous permettant d'afficher par ordre alphabétique les utilisateurs définis dans le fichier /etc/passwd
8. Taper la commande vous permettant de rechercher tous les fichiers du répertoire /etc contenant la chaine de caractères "root"
9. Taper la commande vous permettant de rechercher la localisation du fichier "stdio.h" dans le système
10. Taper la commande vous permettant d'afficher le nombre de lignes, mots et de caractères que comportent le fichier /etc/passwd
11. Rediriger les 10 dernières commandes que vous venez de taper dans le fichier partie2.txt (**history 10 > partie2.txt**)

3 Gestions des répertoires [8.5 pts]

1. Créer les deux dossiers **HACKER** et **CRACKER** en une seule commande dans le répertoire où tu te situes
2. Renommer le dossier **CRACKER** avec le nom **BLACKHAT**
3. Créer (en une seule commande) le fichier toto.txt et y ajouter le message suivant (**I ..... because ..... iiiiiiiii.**)
4. Copier le fichier toto.txt dans les répertoires **ANDIN** et **BLACKHAT** (en une seule commande)
5. Crée un lien symbolique(raccourci) pour chacun dossiers précédents que vous nommerez à votre guise.
6. Taper la commande pour supprimer les dossiers **HACKER** et **BLACKHAT**
7. Taper une commande qui pourra vous permettre de vérifier si les liens symboliques existe toujours après suppression des deux dossiers
8. Rediriger les 7 dernières commandes que vous viens de taper dans le fichier partie3.txt (**history 8 > partie3.txt**)

4 Recherche et tri [14.5 pts]

1. Taper la commande permettant d'afficher la liste de **tous** les fichiers d'un repertoire.
2. Taper la commande permettant d'extraire la ligne 14 d'un fichier texte nommé **fichier.txt**.
3. Taper la commande permettant d'effacer un fichier nommé **fichier.txt**
4. Taper la commande permettant d'afficher le nombre de lignes d'un fichier nommé **exemple.txt**.
5. Taper la commande permettant d'afficher les fichiers d'un repertoire dont le nom commence par une lettre entre **a** et **e**.
6. Taper la commande permettant de trier un fichier nommé **data.txt** par ordre décroissant alphabétique de ce fichier.
7. Taper la commande permettant de trier un fichier nommé **data.txt** par ordre croissant numérique.
8. Taper la commande permettant de chercher dans toute l'arborescence (**répertoire /**) les fichiers dont les noms se termine par « **.c** ».
9. Taper la commande permettant de chercher dans toute l'arborescence les fichiers dont les noms commencent par « **X ou x** ».
10. Taper la commande permettant de chercher dans toute l'arborescence les fichiers dont les noms ne contiennent pas de chiffres.
11. Taper la commande permettant d'afficher à l'écran le contenu du fichier « **affiche.txt** »de telle sorte que tout les « **:** »sont remplacé par « **;** ». C.-à-d. si le contenu du fichier affiche.txt est « toto :billy :soso », votre commande devra afficher à l'écran « toto ;billy ;soso ».
12. Taper la commande permettant d'afficher à l'écran les repertoires dont les noms se terminent par « **se ou Se** ».
13. Taper la commande permettant de chercher dans **/usr** les fichiers dont la taille dépasse 1Mo (2000 blocs de 500Ko) et dont les droits sont fixés à 755 (-rwxr-xr-x).

Cont.

14. Taper la commande permettant de savoir combien de fichiers sont dans toute l'arborescence (**répertoire /**) vous appartenant et ayant les droits fixés à 466 (-rw-rw-rw-).
15. Rediriger les 14 dernières commandes que vous venez de taper dans le fichier partie4.txt (**history 14 >partie4.txt**).

5 Ransomware pour une distribution Unix/Linux [15.5 pts]

Une entreprise souhaite mener une attaque de type **ransomware** sur des systèmes dont ils ont un accès dérobé. On fait appel à vous pour écrire le cœur du virus qui devra chiffrer en utilisant l'algorithme de Cesar tous les dossiers et fichiers se trouvant à la racine utilisateur (*home*).

1. Concrètement votre virus, doit être sous la forme d'un script **bash**, qui entrera dans chaque dossier du repertoire et :

   — Pour chaque dossier, changer le nom du dossier en appliquant l'algorithme de Cesar à trois décalages, donc un dossier avec le nom DJOB deviendra GMRE.

   — Pour chaque fichier, si le contenu est textuel, appliquer l'algorithme de Cesar à trois décalages.

   Par précaution pour vous-même, écrivez l'antidote de votre virus afin de vous prémunir en cas d'une attaque réflexive.
   Appelez vos deux programmes (virus et antidote)
   NOM_PRENOM_VIRUS.sh et NOM_PRENOM_CORR.sh où NOM et PRÉNOM correspondent à vos noms et prénoms.
2. D'après vous, quelles sont les principes de sécurités qu'il faut appliquer pour se prémunir de ce type d'attaques ? Mettez vos préconisations dans un fichier preconisation.sh.

6 Hacker un point d'accès [20.5 pts]

À la suite de vos exploits avec le ransomware, on vous appelle pour faire tomber le point d'accès d'une entreprise en menant une attaque de type **DOS**.

1. Que signifie **DOS** ? Faîtes un schéma explicatif simple pour illustrer.
2. Le point d'accès utilise WPA2 pour l'authentification et encrypter les communications. À quoi sert une PSK ? Pour quelles raisons
3. Commencer par lister l'ensemble des interfaces réseaux de votre station/pc.
   `airmon-ng`
   Démarrer airmon-ng sur wlan1
   `airmon-ng start wlan1`

   Cette commande crée une nouvelle interface en mode monitor ayant comme nom, par exemple, **wlan1mon** suivant votre système. Vérifier l'existence de cette interface en faisant un **ifconfig**.
4. Lancer l'analyse des réseaux environnants à l'aide de **airodump-ng**
   `airodump-ng wlan1mon`

Cont.

À partir de l'analyse de airodump-ng, récupérer le BSSID (@MAC du point d'accès) et le numéro de canal de fréquence utilisé par le point d'accès. Quitter.

5. Capturer avec **tshark** le traffic sur l'interface wlan1mon provenant uniquement du point d'accès cible en utilisant un filtre de capture (-f) dans un fichier **airodump.pcap**.
   `tshark -i wlan1mon -f "wlan host BSSID"`
   Dorénavant, analysons spécifiquement notre point d'accès en spécifiant le canal (-c), et le bssid (–bssid).
6. Faire un man airodump-ng pour plus d'information.
7. Faire un **ping** à partir de votre interface wlan0 pour simuler éventuellement du traffic.
   Vous devriez obtenir toutes les stations connectées. Notez le BSSID du point d'accès et les @MAC des stations connectées.
8. Arrêter la capture, étudier le fichier airodump.pcap.
   Dorénavant, nous allons injecter des trames afin de forcer la déconnection de tous les clients du point d'accès cible.
9. Capturer avec tshark le traffic sur l'interface wlan1mon provenant uniquement du point d'accès cible en utilisant un filtre de capture (-f) dans un fichier **deauth.pcap**.
10. Nous allons injecter du traffic avec aireplay-ng en utilisant l'attaque 0. Choisissez l' @MAC d'une station et déconnecter là du réseau.
    `aireplay-ng -0 0 -a BSSID -c @MAC_STATION wlan1mon`
11. Vérifier que la station est bien déconnectée. Arrêter la capture et l'attaque. Analyser la capture deauth.pcap. Expliquer le fonctionnement de l'attaque. Illustrer avec des fragments de la capture de traffic deauth.pcap. En particulier, identifier les trames correspondant à l'attaque et les trames de reauthentification.
12. Enregistrer vos commandes et vos réponses dans un fichier partie6.txt.

7 Couvrir ses traces [10 pts]

Après votre aventure sur le point d'accès, il s'avère que vous avez laissé trop de traces sur votre station qui peuvent vous porter préjudice dans l'avenir. Il vous faut nettoyer vos traces en supprimant les logs de votre système.

1. Pour vous, un fichier log représente quoi ?
2. Où sont sauvegardés la plupart des logs dans une distribution Linux ? Et Windows ? Et MacOs ?
3. Localisez et supprimer les logs qui concernent les démarrages de votre ordinateur, l'historique de vos commandes et les différentes connexions sur votre PC.
4. Avez-vous Une méthode pour éviter de générer trop de logs sur votre station lors d'une attaque ? Décrivez là.
5. Enregistrer vos commandes et vos réponses dans un fichier partie7.txt.

The End.