

Sécurité – Authentification et droits

Objectifs

L'objectif de ce TP est de mettre en place et comprendre le fonctionnement des protocoles de sécurité, l'authentification, la gestion des droits sous Debian.

Nous verrons plusieurs choses, dont :

- La création de comptes utilisateurs (authentification et droits)
- Les protocoles sécurisés
- La sécurisation des mots de passe

Ressources

- Vous aurez besoin de la VM DebianTpSécurité disponible sous forme de .ova
- Du mémento de commandes Unix ci-dessous
- Droits sous linux ainsi que les commandes associées : https://wiki.debian.fr/xyz/Commandes_utilisateurs_et_groupes HYPERLINK
["https://wiki.debian.fr/xyz/Commandes_utilisateurs_et_groupes"](https://wiki.debian.fr/xyz/Commandes_utilisateurs_et_groupes) HYPERLINK
["https://wiki.debian.fr/xyz/Commandes_utilisateurs_et_groupes"](https://wiki.debian.fr/xyz/Commandes_utilisateurs_et_groupes) HYPERLINK
["https://wiki.debian.fr/xyz/Commandes_utilisateurs_et_groupes"](https://wiki.debian.fr/xyz/Commandes_utilisateurs_et_groupes) HYPERLINK
["https://wiki.debian.fr/xyz/Commandes_utilisateurs_et_groupes"](https://wiki.debian.fr/xyz/Commandes_utilisateurs_et_groupes) HYPERLINK
["https://wiki.debian.fr/xyz/Commandes_utilisateurs_et_groupes"](https://wiki.debian.fr/xyz/Commandes_utilisateurs_et_groupes) HYPERLINK
- Des logiciels Wireshark et Putty sur votre machine hôte

Commande	Libellé	Exemple
adduser	Ajouter un utilisateur	adduser « <i>nom_utilisateur</i> »
deluser	Supprimer un utilisateur	deluser « <i>nom_utilisateur</i> »
passwd	Gérer le mot de passe	passwd « <i>nom_utilisateur</i> »
groups	Afficher les groupes d'appartenance	groups « <i>nom_utilisateur</i> »
groupadd	Créer un groupe	groupadd gmer
usermod	Ajouter un utilisateur à un groupe	usermod -aG gmer « <i>nom_utilisateur</i> »
	Utilisateurs	/etc/passwd
	Mots de passe	/etc/shadow
	Groupes	/etc/group
chown	Changer le propriétaire d'un fichier	chown upoisson fliste.txt
chgrp	Changer le groupe propriétaire d'un fichier	chgrp gmer fliste.txt
chmod	Changer les droits d'accès d'un fichier	chmod ug+rwX fliste.txt
-R .	Appliquer les droits sur toute une arborescence. (. désignant le répertoire courant)	chmod -R u+X .
pwd	Afficher le répertoire courant	pwd

cd	Retourner dans le répertoire home	cd
more	Afficher page par page	cat liste.txt more
grep	Filtrer un résultat Exemple : afficher les lignes du fichier qui contiennent le mot group	cat auth.log grep group

Prérequis

Vous devez installer la machine virtuelle DebianTpSécurité.ova en utilisant le mode importation de VirtualBox (comme lors du TP2-Découverte_VirtualBox)

ÉTAPE 1 - Création d'utilisateurs sous linux

Utilisateurs :

Nom complet : **Vint Cerf** (1943 -) - *Ingénieur et inventeur du protocole TCP/IP*

Nom d'ouverture de session : **vcerf**

Mot de passe : **123456**

Nom complet : **Dennis Ritchie** (1941-2011) - *Ingénieur et Inventeur d'Unix et du C*

Nom d'ouverture de session : **dritchie**

Mot de passe : **Password**

Nom Complet : **Margaret Hamilton** (1936 -) - *Ingénieure NASA et inventeuse des concepts de développement moderne*

Nom d'ouverture de session : **mhamilton**

Mot de passe : **password0**

Nom Complet : **Hedy Lamarr** (1914-2000 - *Actrice et Inventeuse de techniques de transmissions sécurisées par ondes radio à la base des protocoles sans-fil modernes*)

Nom d'ouverture de session : **hlamarr**

Mot de passe : **Hedlama4567**

Groupes :

Agence :

- vcerf
- dritchie
- mhamilton

- hlamarr

Comptabilité :

- vcerf
- mhamilton

Ventes :

- dritchie
- hlamarr



Veuillez indiquer ci-dessous, les commandes de création des utilisateurs et groupes.

Que contient le fichier **/etc/passwd** ?

Il contient les informations des utilisateurs.

Que contient ce fichier **/etc/group** ?

C'est un dossier root assigné à chaque utilisateur.

Tapez la commande **pwd**. Que vous affiche cette commande ?

pwd est la commande qui sert à afficher le chemin par lequel on est passé.

Home/vcerf

Connectez-vous avec le compte vcerf et tapez la commande **pwd**. Que vous affiche cette commande, cette-fois ci ?

Home/utilisateur

Pour généraliser, indiquez le répertoire racine des utilisateurs ?

Home/utilisateur

Quels sont les droits par défaut de l'utilisateur sur sa racine ?

777

Pour poursuivre notre découverte, allez dans le répertoire de Logs (les journaux) qui sont dans le dossier **/var/log** sous Debian.

Quel journal contient les événements de création de compte utilisateur ?

Auth.log

Quel événement indique la création d'un nouveau groupe ?

groupeadd

Quel événement indique qu'un nouvel utilisateur a été affecté à un groupe ?

add to group

Quel journal contient les événements de connexion/déconnexion d'un utilisateur ?

Auth.log

Notes

ÉTAPE 2 - Mot de passe, l'art de le récupérer ou de le casser

L'excellent [HYPERLINK "https://zythom.fr/2019/10/politique-de-securite-des-mots-de-passe/"](https://zythom.fr/2019/10/politique-de-securite-des-mots-de-passe/)
[HYPERLINK "https://zythom.fr/2019/10/politique-de-securite-des-mots-de-passe/"](https://zythom.fr/2019/10/politique-de-securite-des-mots-de-passe/) [HYPERLINK](https://zythom.fr/2019/10/politique-de-securite-des-mots-de-passe/)
["https://zythom.fr/2019/10/politique-de-securite-des-mots-de-passe/"](https://zythom.fr/2019/10/politique-de-securite-des-mots-de-passe/) [Zythom](https://zythom.fr/2019/10/politique-de-securite-des-mots-de-passe/) [HYPERLINK](https://zythom.fr/2019/10/politique-de-securite-des-mots-de-passe/)
["https://zythom.fr/2019/10/politique-de-securite-des-mots-de-passe/"](https://zythom.fr/2019/10/politique-de-securite-des-mots-de-passe/) [HYPERLINK](https://zythom.fr/2019/10/politique-de-securite-des-mots-de-passe/)
["https://zythom.fr/2019/10/politique-de-securite-des-mots-de-passe/"](https://zythom.fr/2019/10/politique-de-securite-des-mots-de-passe/) [HYPERLINK](https://zythom.fr/2019/10/politique-de-securite-des-mots-de-passe/)
["https://zythom.fr/2019/10/politique-de-securite-des-mots-de-passe/"](https://zythom.fr/2019/10/politique-de-securite-des-mots-de-passe/) a écrit très récemment un article sur [les mots de passe](#) que je vous engage fortement à lire en entier pour vous personnellement mais aussi pour votre vie professionnelle future.

La partie la plus importante de l'article à retenir est la suivante :

"[...] Un bon mot de passe doit comporter **au minimum 12 signes mélangeant au moins trois des quatre types de signes suivants : des majuscules, des minuscules, des chiffres ou des caractères spéciaux** (comme par exemple !#?%). Cette recommandation est conforme aux préconisations 2018 de la CNIL et de l'ANSSI.
[...]"

La seule remarque que nous pouvons faire sur cet article se trouve sur la longueur d'un mot de passe. Il préconise 12 caractères mais c'est vraiment le minimum acceptable aujourd'hui. Pour des comptes utilisateurs sans privilèges particuliers, c'est suffisant effectivement.

Mais pour des comptes plus importants comme des comptes techniques "root", "administrateur", "enable" (équipements cisco) ou des comptes "VIP" comme des comptes de PDG ou de grands directeurs, il est vraiment impératif de passer à des longueurs de 16 caractères minimum (plus c'est grand, mieux c'est) ou d'utiliser une authentification multi-facteurs (mail avec code, token, biométrie, etc)

L'une des méthodes pour casser un mot de passe est le social engineering. Cette méthode consiste à demander à une personnes son mot de passe. En effet, bon nombre de personne par méconnaissance fournissent encore leurs mots de passe à des personnes qui leurs semblent être de confiance. Je vous conseille le livre de Charles Cohle « Je sais qui vous êtes », ainsi que ce site https://assiste.com/Mots_de_passe_Test_de_solidite.html.

Pourquoi la longueur est importante (<https://www.ssi.gouv.fr/administration/precautions-elementaires/calculer-la-force-dun-mot-de-passe/>), car c'est le rempart ultime contre le bruteforce qui est la méthode radicale pour trouver un mot de passe lorsqu'on a épuisé toutes les autres solutions.

Parmi celles-ci, il y a le cassage de mot de passe par dictionnaire (<https://korben.info/une-liste-de-15-milliards-de-mots-de-passe.html>). Comme son nom l'indique l'attaquant utilise un dictionnaire de mot de passe testés un par un.

Par table arc en ciel, il s'agit de faire coïncider le Hash d'un système avec des Hash référencés dans des tables.

Enfin, les attaquants combinent souvent les diverses méthodes ci-dessus.

Notes

- **Récupération de mot de passe en protocole Telnet**

Nous allons installer un serveur telnet sur notre machine virtuelle.

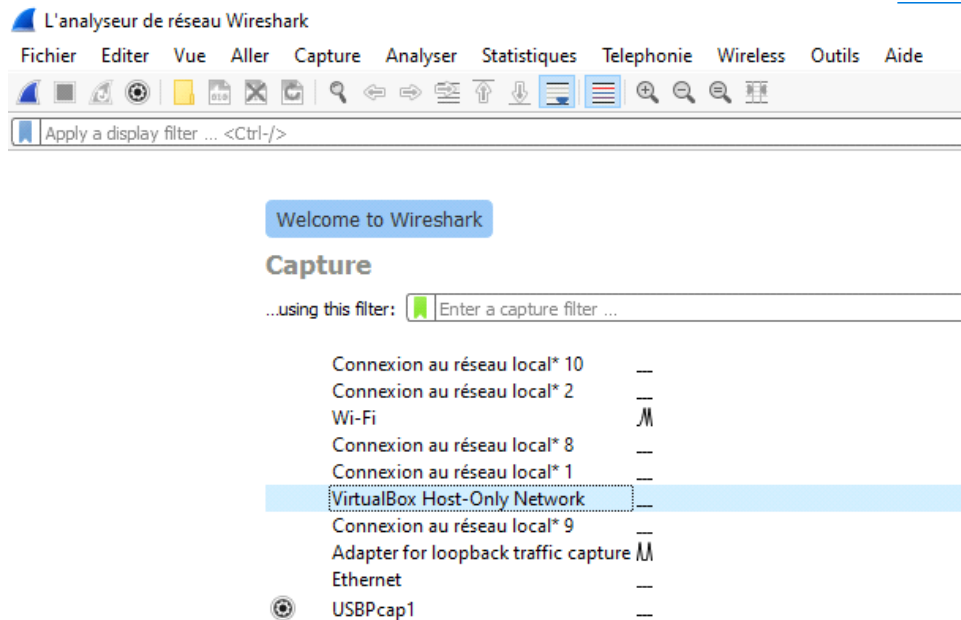
```
$ sudo apt install telnetd
```

Vous devez basculer votre machine virtuelle en Réseau Privé Hôte, puis dans avancé vous devez mettre le mode promiscuité sur Allow All. Votre machine virtuelle est prête.

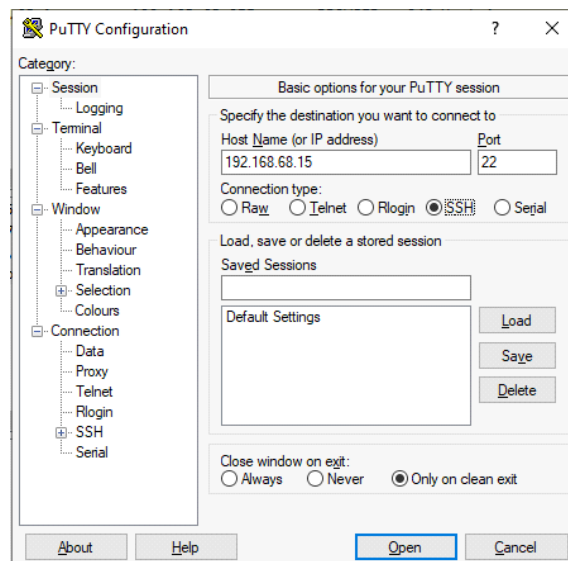
Relevez l'adresse IP de votre machine virtuelle.

Vous devez maintenant installer les logiciels Putty et Wireshark sur vote machine hôte, si vous ne les avez pas déjà.

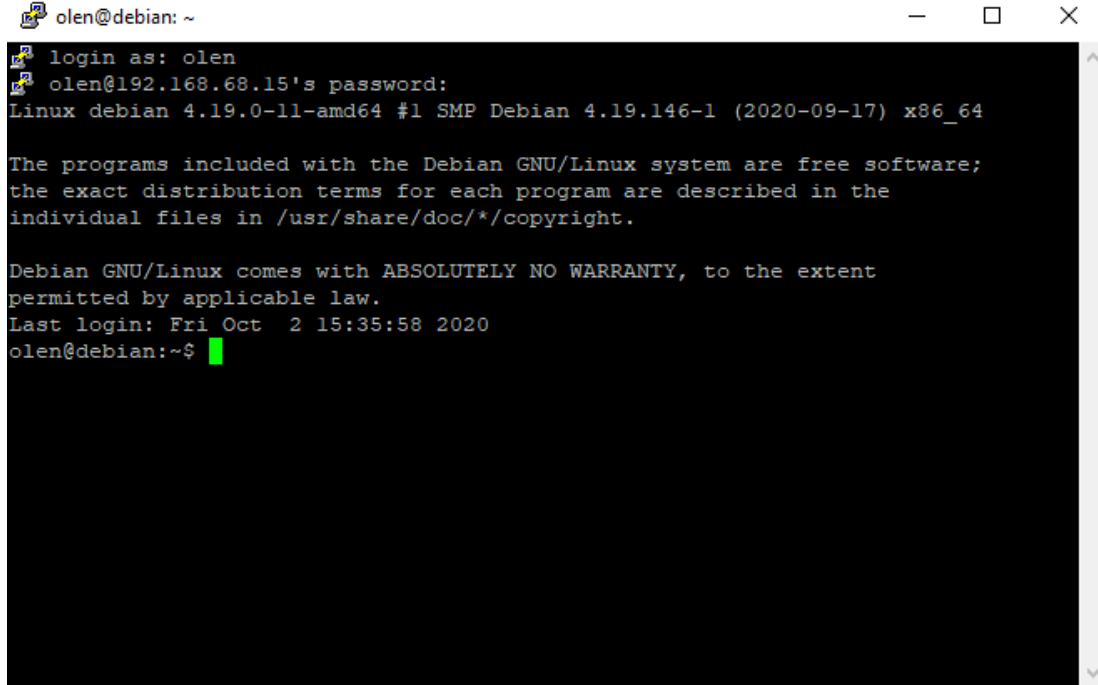
Lancer Wireshark en surveillance sur la carte VirtualBox Host-Only Network.



Lancez Putty de votre machine hôte, sur l'adresse de votre machine virtuelle en mode Telnet



Identifiez-vous normalement sur votre machine virtuelle Identifiant : **olen**, Mot de Passe : **OLEN@bts2021**



```
olen@debian: ~  
login as: olen  
olen@192.168.68.15's password:  
Linux debian 4.19.0-11-amd64 #1 SMP Debian 4.19.146-1 (2020-09-17) x86_64  
  
The programs included with the Debian GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
Last login: Fri Oct  2 15:35:58 2020  
olen@debian:~$
```

Sur Wireshark, vous voyez passer du trafic. Une fois identifié sur votre machine virtuelle, coupez la capture du trafic (cliquez sur le carré rouge) réseau de Wireshark en cliquant sur le carré rouge en haut à gauche. Ensuite appliquez un filtre sur le trafic Telnet et développez la rubrique Telnet

VirtualBox Host-Only Network

Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

telnet

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.68.1	192.168.68.15	TELNET	56	Telnet Data ...
2	0.000536	192.168.68.15	192.168.68.1	TELNET	90	Telnet Data ...
11	6.556360	192.168.68.1	192.168.68.15	TELNET	55	Telnet Data ...
12	6.556774	192.168.68.15	192.168.68.1	TELNET	60	Telnet Data ...
14	6.831270	192.168.68.1	192.168.68.15	TELNET	55	Telnet Data ...
15	6.831627	192.168.68.15	192.168.68.1	TELNET	60	Telnet Data ...
17	7.081919	192.168.68.1	192.168.68.15	TELNET	55	Telnet Data ...
18	7.082268	192.168.68.15	192.168.68.1	TELNET	60	Telnet Data ...
20	7.280994	192.168.68.1	192.168.68.15	TELNET	55	Telnet Data ...

> Frame 11: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{99DAD5A6-0674-41B7-B2E2-474322606872}, ...

> Ethernet II, Src: 0a:00:27:00:00:11 (0a:00:27:00:00:11), Dst: PcsCompu_7f:0f:92 (08:00:27:7f:0f:92)

> Internet Protocol Version 4, Src: 192.168.68.1, Dst: 192.168.68.15

> Transmission Control Protocol, Src Port: 49979, Dst Port: 23, Seq: 3, Ack: 37, Len: 1

▼ Telnet

Data: e

```

0000 08 00 27 7f 0f 92 0a 00 27 00 00 11 08 00 45 00  ..'....'....E.
0010 00 29 6e fe 40 00 80 06 82 6f c0 a8 44 01 c0 a8  ..)n@...o..D...
0020 44 0f c3 3b 00 17 84 63 92 39 38 c3 0d 35 50 18  D...;...c..98..5P.
0030 20 12 01 70 00 00 65                               ..p...e

```

wireshark_VirtualBox Host-Only Network_20201002155110_a02960.pcapng | Paquets: 104 · Affichés: 53 (51.0%) · Perdus: 0 (0.0%) | Profile: Default

Pour pouvoir visualiser une information intéressante, commencez par les ligne telnet du bas et remontez ligne après ligne en visualisant bien le contenu de Data dans la rubrique Telnet.



Notez ci-dessous les informations que vous avez pu récolter ?

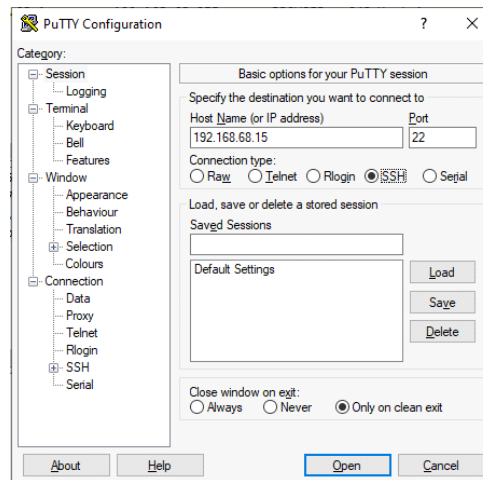
Le nom d'utilisateur (olen@debian) ainsi que le mot de passe sous la forme de packets de 55 de longueur.

Que cela signifie-t-il ?

On sniffe les packets de la connexion telnet afin d'effectuer une opération de man in the middle.

- Récupération de mot de passe en protocole SSH

Une fois les constatations effectuées, relancez la capture du trafic et connectez-vous sur votre machine virtuelle avec Putty en mode SSH.



Avez-vous le même résultat qu'avec le protocole Telnet ? Pourquoi, selon vous ?

Non, tout est encrypté.

Notes

- **Cassage de mot de passe avec l'application John The Ripper**

Nous allons installer le package "John The Ripper" sur notre VM.



N'oubliez pas qu'il faut mettre votre carte réseau en NAT avant d'installer le package.

```
$ sudo apt install john
```

Vous pouvez observer dans le fichier `/etc/shadow` que les mots de passe sont bien chiffrés :

Exemple :

```
btssn:$6$5MWg3vZx$hMhooYHa.PCg0g8aD8u4A5mQ.....:17559:0:99999:7:::  
mhamilton:$6$5ccnst7Q$QiRzoaZA1x5ypOrONklC.....:17559:0:99999:7:::  
[...]
```

Et lancer John The Ripper pour tenter de casser ces mots de passe :

```
$ sudo john /etc/shadow
```

Normalement, la découverte des mots de passe les plus simples devrait prendre qq secondes. Pour les mots de passe les plus compliqués, ça peut prendre des jours, des mois ou beaucoup plus... suivant la puissance de la machine.



Quel constat pouvez-vous faire sur le cassage des mots de passe ?

Les mots de passe les plus simples comme 123456 et Password prennent moins de 45 secondes.

Essayez de donner une explication à l'ordre de cassage des mots de passe.

Les outils de bruteforce ont un dictionnaire de bash conséquent et les comparent séquentiellement.

Notes