B3_TP3– Choisir un bon mot de passe (1h)

L'entreprise Egnora, que vous avez récemment intégrée en tant qu'administrateur réseau, suspecte une possibilité d'intrusion interne dans le SI.
Une faille de sécurité dans l'OS Debian a été annoncée sur le site https://www.cert.ssi.gouv.fr/avis/CERTFR-2023-AVI-0687/ .
Vous possédez une image d'une des machines des employés de l'entreprise, avec différents comptes utilisateurs, sous forme de machine virtuelle (VM : WEBegnaro.ova).
Cette machine est une linux, Debian.
Le DSI vous demande de vérifier le niveau de compromission de l'OS des machines de l'entreprise, d'identifier si des mots de passe sont compromis. Vous lui rédigerez ensuite un mail, indiquant le niveau de compromission de l'OS et les mots de passe impactés. Vous proposerez une démarche pour sécuriser le SI.

Ce TP permet d'aborder le choix de mots de passe forts afin de sécuriser l'accès à son compte.
Dans un premier temps vous consulterez l'alerte CVE (Common Vulnerabilities and Exposures) sur le site de l'Anssi et vérifierez la compromission.
Dans un deuxième temps , vous utiliserez un outil de piratage de mot de passe pour récupérer le mot de passe d'un utilisateur.
Dans un troisième temps, vous sécuriserez l'accès à ces comptes en choisissant des mots de passe forts.

Le travail se fera sur deux vm : EGNORA-TP3.ova et kali-linux-2020.3-vbox-amd64-TP3.*ova*

Vérifier une version d'OS et sa vunérabilité face à une CVE :

On ne vous demande pas d'utiliser la **CVE** (vu en deuxième année avec utilisation de **metasploit** sur **VM kali**) mais on vous demande de savoir lire une alerte et de savoir identifier si votre système est compromis.

Common Vulnerabilities and Exposures ou **CVE** est un dictionnaire des informations publiques relatives aux vulnérabilités de sécurité. Le dictionnaire est maintenu par l'organisme MITRE, soutenu par le département de la Sécurité intérieure des États-Unis.

Metasploit, *Metasploit Pen Testing Tool**,** est un projet (*open source*, sous* Licence BSD *modifiée) en relation avec la sécurité des systèmes informatiques. Son but est de fournir des informations sur les vulnérabilités de systèmes informatiques, d'aider à la pénétration et au développement de signatures pour les* systèmes de détection d'intrusion *(IDS, Intrusion Detection System).*
Le plus connu des sous-projets est le Metasploit Framework, un outil pour le développement et l'exécution d'exploits (logiciels permettant d'exploiter à son profit une vulnérabilité) contre une machine distante.

Comparable aux produits commerciaux tels que CANVAS d'Immunity ou Core Impact, Metasploit peut être utilisé par les administrateurs pour tester la vulnérabilité des systèmes informatiques afin de les protéger, ou par les pirates et les script kiddies à des fins de piratage. Comme la plupart des outils de sécurité informatique, Metasploit peut être utilisé à la fois de manière légale et à la fois pour des activités illégales.

Le fait que Metasploit ait émergé en tant que plate-forme de développement dans la sécurité, a conduit, ces derniers temps, la publication de vulnérabilités logicielles souvent accompagnées d'un module d'exploitation pour Metasploit pour ces dernières, afin de mettre en évidence l'exploitabilité, le risque et les mesures de prévention contre ces bogues particuliers2,3.

Kali Linux est une distribution Linux basée sur Debian et sortie le 13 mars 2013. Son objectif est de fournir un ensemble d'outils nécessaires aux tests de sécurité informatique. **Metasploit** est un outil disponible dans la kali.

1° Allez sur le site de l'anssi et identifiez la vulnérabilité, https://www.cert.ssi.gouv.fr/avis/CERTFR-2023-AVI-0687/ , peut-on devenir root sur l'OS des machines d'Egnora ?

2° Indiquez la version de l'OS et des sources Linux, installées sur les machines d'Egnora.

Pour cela, ouvrez la vm d'Egnora et dans une console, tapez ces commandes :

- Pour obtenir la version de l'OS : $lsb_release -a

- Pour obtenir la version des sources Linux : $cat /proc/version

-Pour obtenir la version du kernel (noyau) : uname -r

3° Conclure sur la compromission de l'OS des machines d'Egnora et les risques encourus :

Pouvez vous lire les fichiers /etc/shadows et /etc/password en tant qu'administrateur de la machine (root Rootsio2017)

fichier contenant les identifiants :

```
root@debian:/home/etudiant# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
_apt:x:104:65534::/nonexistent:/bin/false
rtkit:x:105:110:RealtimeKit,,,:/proc:/bin/false
dnsmasq:x:106:65534:dnsmasq,,,:/var/lib/misc:/bin/false
avahi-autoipd:x:107:111:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
messagebus:x:108:112::/var/run/dbus:/bin/false
usbmux:x:109:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false
speech-dispatcher:x:110:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
lightdm:x:111:116:Light Display Manager:/var/lib/lightdm:/bin/false
pulse:x:112:117:PulseAudio daemon,,,:/var/run/pulse:/bin/false
avahi:x:113:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
colord:x:114:121:colord colour management daemon,,,:/var/lib/colord:/bin/false
saned:x:115:122::/var/lib/saned:/bin/false
hplip:x:116:7:HPLIP system user,,,:/var/run/hplip:/bin/false
etudiant:x:1000:1000:etudiant,,,:/home/etudiant:/bin/bash
vboxadd:x:999:1::/var/run/vboxadd:/bin/false
alice:x:1001:1001:,,,:/home/alice:/bin/bash
bob:x:1002:1002:,,,:/home/bob:/bin/bash
eric:x:1003:1003:,,,:/home/eric:/bin/bash
eve:x:1004:1004:,,,:/home/eve:/bin/bash
```

fichier contenant les mots de passe:

```
root@debian:/home/etudiant# cat /etc/shadow
root:$6$2j8Hkor7$l7zky06VWwKaB6tO3P2kxVFAIJm8NTk96nZ5nUIn5JTyRBLuJZOMb8Q0vAAicaRH6mgZiFofafEgOoxZKLR0B/:17442:0:99999:7:::
daemon:*:17442:0:99999:7:::
bin:*:17442:0:99999:7:::
sys:*:17442:0:99999:7:::
sync:*:17442:0:99999:7:::
games:*:17442:0:99999:7:::
man:*:17442:0:99999:7:::
lp:*:17442:0:99999:7:::
mail:*:17442:0:99999:7:::
news:*:17442:0:99999:7:::
uucp:*:17442:0:99999:7:::
proxy:*:17442:0:99999:7:::
www-data:*:17442:0:99999:7:::
backup:*:17442:0:99999:7:::
list:*:17442:0:99999:7:::
irc:*:17442:0:99999:7:::
gnats:*:17442:0:99999:7:::
nobody:*:17442:0:99999:7:::
systemd-timesync:*:17442:0:99999:7:::
systemd-network:*:17442:0:99999:7:::
systemd-resolve:*:17442:0:99999:7:::
systemd-bus-proxy:*:17442:0:99999:7:::
_apt:*:17442:0:99999:7:::
rtkit:*:17442:0:99999:7:::
dnsmasq:*:17442:0:99999:7:::
avahi-autoipd:*:17442:0:99999:7:::
messagebus:*:17442:0:99999:7:::
usbmux:*:17442:0:99999:7:::
speech-dispatcher:!:17442:0:99999:7:::
lightdm:*:17442:0:99999:7:::
pulse:*:17442:0:99999:7:::
avahi:*:17442:0:99999:7:::
colord:*:17442:0:99999:7:::
saned:*:17442:0:99999:7:::
hplip:*:17442:0:99999:7:::
etudiant:$6$pGan3HTk$wPnM6RHAVnCCdRDT.3QWID.L9n6KU.VML4TKd8j8QbPeVvysnCk9DLT.SQ6gyHPp37d.vWkR2jhBDw0X4OpGS/:17442:0:99999:7:::
vboxadd:!:17442::::::
alice:$6$ki9Eow/k$f7P3l5UETauVvdKu6FXIw.g5XdMomIxsoh5TgbBXwpScRYiuCx.0kAewT/Ph7A7RqE/vpabLwWMmkj.xAPlEV/:17538:0:99999:7:::
bob:$6$CBY9OgoC$fSFyAwetWiNq.Vurm/toNZ6tAD5zfLe1./3XSgMAxkvj39UZp1W1LFbshzufI/b6OWNpycfmfFt8g3YAW7EE30:17538:0:99999:7:::
eric:$6$GVjEItuQ$ihCmfH1JwMTBZJZ4cD7ZsYdNWVCcfX9QRWVakMz9UAKKYtgbD8TOopT7Hdlj3ZvONdpBXGTvZmzELGFH7cc5X.:17538:0:99999:7:::
eve:$6$cRV1kSHJ$1lcboKMM9KHPowXveCypkUFjw/Hw5bADCMLI0PFleCpqQZkUniSvysZukTNtpWiJfYe4vQGkKdf9cc2XcEndy1:17538:0:99999:7:::
```

Voici une présentation complète de la chaîne:

`[nom d'utilisateur]: [mot de passe]: [date du dernier changement de mot de passe]: [âge minimum du mot de passe]: [âge maximum du mot de passe]: [période d'avertissement]: [période d'inactivité]: [date d'expiration]: [inutilisé]`

https://fr.denizatm.com/pages/47031-what-is-the-linux-etc-shadow-file-and-what-does-it-do

Pirater un mot de passe *(source : Cisco)*

> **Attention** : cette partie du TP montre la vulnérabilité de mots de passe simples. L'utilisation d'un logiciel de crack de mot de passe comme John the Ripper doit être réservée à un usage pédagogique ou de test de vos propres comptes ! L'article 323-1 du code Pénal dit :
>
> « Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende.
>
> Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100000 € d'amende.
>
> Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à cinq ans d'emprisonnement et à 150 000 € d'amende. »

Ouvrez la VM kali.*ova* sur le réseau. En plus du compte habituel etudiant, deux comptes utilisateurs, Alice, Bob, ont été créés. Vous allez récupérer les mots de passe de connexion de ces comptes à l'aide de **John the Ripper**, un outil open source de piratage de mot de passe.

John the Ripper réalise des **attaques par dictionnaire**, c'est-à-dire qu'il teste de nombreuses combinaisons afin de cracker le mot de passe. Il existe toutes sortes de dictionnaires disponibles sur Internet pouvant être utilisés pour cette attaque (dictionnaire classique, dictionnaire des prénoms, dictionnaire des noms d'auteurs, dictionnaire des marques commerciales...).

- ✔ Démarrez la VM et connectez-vous sous le compte kali kali.

Vous avez récupéré au auparavant les fichiers shadow et passwd dans le repertoire /home/kali/Documents/fichiers/ , que vous allez regrouper dans un seul fichier mypasswd et vous allez l'utiliser pour essayer de craquer les mots de passe.

- ✔ Ouvrez une fenêtre de terminal et tapez la commande unshadow pour regrouper les fichiers:

```
$/usr/sbin/unshadow Documents/fichiers/passwd Documents/fichiers/shadow > Documents/fichiers/mypasswd
```

Cette commande regroupe le contenu du fichier passwd où sont stockés les comptes d'utilisateurs et celui du fichier shadow où les mots de passe sont stockés pour les placer dans un nouveau fichier nommé « *mypasswd* ».

- ✔ Affichez le contenu du fichier *mypasswd*. Les mots de passe apparaissent-ils en clair ?
- ✔ Saisissez la commande suivante dans le terminal. John the ripper affiche-t-il les mots de passe ?

```
$ /usr/sbin/john --show Documents/fichiers/mypasswd
```

À l'invite de commandes, saisissez maintenant la commande suivante :

```
$ /usr/sbin/john --wordlist=/usr/share/john/password.lst --rules Documents/fichiers/mypasswd --format=crypt
```

Le programme John the Ripper utilise un dictionnaire prédéfini appelé *password.lst* et une série standard de « règles » prédéfinies pour exploiter ce dictionnaire et récupérer tous les hashs de mots de passe de type md5crypt et crypt.

Les mots de passe pour chaque compte s'affichent.

- ✔ Notez ces mots de passe :

alice		eric	
bob		eve	

L'exercice montre qu'un mot de passe de « mauvaise qualité » peut facilement être piraté.

Choisir un mot de passe fort

Qu'est-ce que la « **force** » d'un mot de passe ? *(source : ANSSI)*

Par abus de langage, on parle souvent de **« force » d'un mot de passe** pour désigner sa **capacité à résister à une énumération de tous les mots de passe possibles**.

Cette « force » dépend de la longueur L du mot de passe et du nombre N de caractères possibles. Elle suppose que le mot de passe est choisi de façon aléatoire. Elle se calcule aisément par la formule N^L. Mais il est plus difficile d'estimer si la valeur ainsi obtenue est suffisante ou pas.

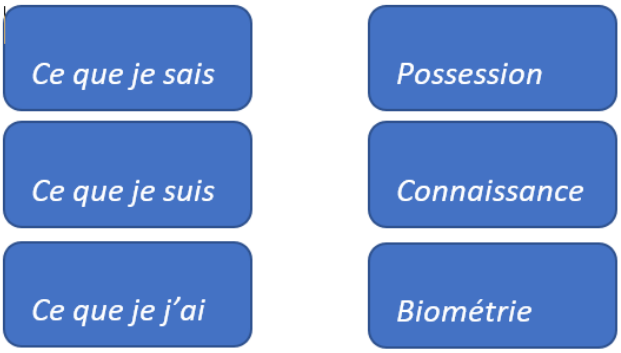
Quelques notions :

Identification et authentification

Pour accéder à des sites ou services informatiques, vous devez dans un premier temps, vous identifier (c'est le rôle de l'identifiant login) puis authentifier cette identité. L'authentification peut se faire de 3 manières :

Par **possession** (Clé, Carte Badge …).
Par **biométrie** (Empreintes digitales).
Par **connaissance** (Mot de passe).

Exercice : Relier chaque expression à sa méthode d'authentification



Le vol des mots de passe

L'authentification par mot de passe étant très répandue, c'est aussi la plus attaquée par les personnes mal intentionnées. Pour vous aider à comprendre ce qu'est un mot de passe fort, nous allons commencer par vous présenter certaines techniques de piratage des mots de passe.

Avant de commencer, il faut comprendre que si un Hacker parvient à voler votre mot de passe, il ne l'aura en général que sous une forme hashée appelée Hash (Cette notion sera détaillée plus tard dans la formation).

Pour vous donner une petite idée de ce que c'est, voici le Hash du mot de passe suivant :

*« **Mon mot de passe** » donne « **a33faecdf8616c3ca60664891caf18d7** » alors que*

*« **mon mot de passe** » donne « **28bbd531bd0b2d272233e703b1f38dba** » ce qui est radicalement différent.*

Testez par vous-même en lançant passwordMD5/HashGenerator.html dans votre navigateur.

Les méthodes de décryptage des mots de passe

Décryptage par force brute

Cette méthode consiste tout simplement à tester toutes les combinaisons de lettres, chiffres et symboles possibles jusqu'à retrouver le hash volé. Elle nécessite des ordinateurs très performants pour être menée à bien.

Décryptage par dictionnaire

Pour faciliter la mémorisation de leur mot de passe, beaucoup de gens utilisent des mots comme par exemple « MotDePasse ». Le décryptage par dictionnaire consiste donc à tester toutes les combinaisons de mots de "a""a""a" à "Zyrianes" " Zyrianes " " Zyrianes " jusqu'à ce que le hash généré corresponde au hash volé. On peut donc penser qu'avec ses 10 caractères, « MotDePasse » sera difficile à trouver mais il n'en est rien car il n'est constitué que de 3 mots.

Décryptage par permutation

Comme on a dit aux gens de durcir leurs mots de passe en y ajoutant des chiffres et ou des caractères spéciaux, certains se sont contentés d'ajouter « **123** » pour faire « **MotDePasse123** », mais les Hackeurs utilisent ces séquences chiffrées bien connues, avant après et entre les mots.

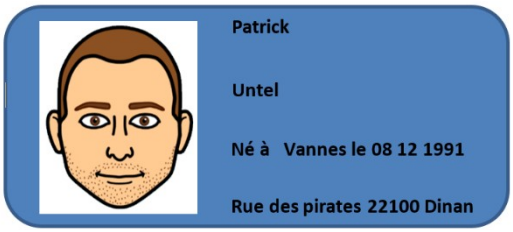
D'autres ont substitué certaines lettres par des caractères spéciaux comme dans la table suivante et « **MotDePasse**» est devenu « **Mo+2P@ss€**» mais là encore, les dictionnaires avec lettres permutées existent déjà.

a=@	B=8	c=(	d=6	E=3	E=€	De=2	g=9	H=#	i=1	i=!	k=<
o=0	q=9	s=5	s=$	t=+	v=>	v=<	w=uu	w=2u	x=%	y=?	l=1

Décryptage par ingénierie sociale

Pour rendre les choses plus complexes, les gens ont donc commencé à utiliser des phrases, mais pour les retenir plus facilement, ils ont utilisé des informations les concernant ! Grave erreur car il est très facile pour un hackeur de retrouver des informations personnelles sur les réseaux sociaux. Voyez plutôt l'exemple suivant.

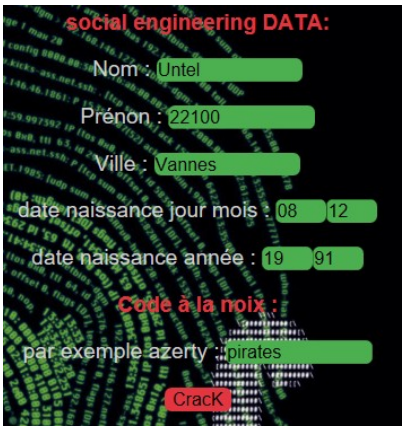
Sur un forum amateur peu sécurisé, nous avons dérobé le hash suivant « 624225bef60ef9d5b67a2c8899b83a8b » associé au compte de Caro Gublini. Essayons de retrouver son mot de passe en utilisant l'ingénierie sociale décryptage.mp4.



Exercice

Dans votre navigateur, lancez « Hash generator.html » (revoir *Tuto Lancer hash generator.mp4*) et cliquez sur le lien caché dans la tête de mort pour accéder au logiciel « CrackPass ».

Utilisez « CrackPass » pour retrouver le mot de passe de Patrick à partir d'un hash volé sur un forum amateur «660c3d7be04783db06dc30d20dde3c41».



Aide :

Si vous ne trouvez pas, sachez que vous n'êtes pas obligé de respecter l'attribution des cases (vous pouvez mettre dans la case « Nom » le nom de la rue, le code postal ou tout autre info en votre possession. Vous pouvez aussi ajouter une info dans la case du bas !

Vol de mots de passe par Hameçonnage

Vous croyez recevoir de votre fournisseur d'accès, un courrier vous indiquant qu'il y a un problème avec votre messagerie et vous invitant à cliquer sur un lien pour y remédier. Mais au lieu d'arriver sur « MaMessagerie.com », « vous arrivez sur MaMessageri.com » qui va vous demander de taper votre mot de passe, et c'est là qu'une toute petite différence génère de gros ennuis !

Réutilisation de mots de passe

Beaucoup d'usagers utilisant le même mot de passe pour tous les sites, les hackeurs s'attaquent en général à des sites faiblement sécurisés comme des forums amateurs (voir cas de Patrick Untel) pour récupérer des mots de passe et les utiliser sur des sites rentables (banques ou messageries etc…).

Évaluation

Associer chaque situation à une techniques de récupération de mot de passe.

Réception d'un mail de ma banque me demandant de modifier mon mot de passe	Ingénierie sociale
Tester tous les mots du dictionnaire	Hameçonnage
Recherche des lieux de naissance, nom des enfants, adresse et autres informations personnelles.	Décryptage par dictionnaire
Tester tous les mots en remplaçant les « S » par des $	Attaque par force brute.
Tester toutes les combinaisons de caractères.	Décryptage par permutation

Sélectionner la définition correspondant à l'ingénierie sociale.

Mettre des informations personnelles dans son mot de passe	*Trouver des failles dans un réseau social.*	*Utiliser les informations personnelles pour trouver un mot de passe.*

Associer chaque mot de passe à une méthode pour le décryptage

Jean21Janvier1983	Dictionnaire
MotdePasse	Permutation
Pir@teInform@tique	Ingénierie sociale
Mot2Pa$$e	

Règles de création d'un mot de passe fort

Maintenant que vous avez une idée des méthodes utilisées pour décrypter les mots de passe, vous connaissez aussi le pourquoi des règles de création de mot de passe que voici.

Le mot de passe doit comporter au moins 10 caractères choisis parmi les 90 disponibles au clavier.

2 caractères donnent 90^2 ou 8100 combinaisons possibles.
6 caractères donnent 90^6 ou 531 milliards de combinaisons possibles. Un ordinateur de particulier testant 1 combinaison toutes les microsecondes ne mettra que

$\frac{531\,10^9}{10^6}=531000$ secondes ou alors $\frac{531000}{3600*24}$ = 6 jours.

10 caractères donnent 90^{10} combinaisons ou 35 *10^{18} soit environ 35 milliards de milliards.

Le même ordinateur de particulier mettre donc $\frac{90^{10}}{10^6*3600*24*365}$ =1 114 815 années au lieu de 6 jours

Exercice : Avec le même ordinateur testant 1 combinaison toutes les microsecondes Combien d'années faut-il si le mot de passe n'utilise que 10 lettres minuscules.

Bannir les mots du dictionnaire.

En moyenne, un adulte n'utilise que 3000 mots (entre 800 et 1500 pour un ado).

Exercice : Avec un ordinateur testant 1 combinaison toutes les microsecondes Combien d'heures faut-il pour décrypter un mot de passe constitué par 3 mots d'un dictionnaire de 3000 mots (exemple motdepasse).

Ne pas utiliser des mots du dictionnaire même avec des caractères spéciaux.

« Mot2pa$$e » ou « Mot2p@ss€ » ne sont pas plus compliqués à trouver que « Motdepasse ».

Eviter les rapports psycho-sociaux.

Nom, prénom, dates …

Eviter le lien avec le service web concerné.

« Mot2pa$$google », « Mot2pa$$gmail », « Mot2pa$$banquepop ».

Eviter le lien avec la fonction.

« Mot2passeAdmin », « Mot2pa$$Serveur », « Mot2p@sseBox ».

Comment retenir un mot de passe fort

Un mot de passe fort c'est très bien pour la sécurité mais beaucoup moins efficace pour la mémorisation. Comment faire pour retenir « !gM#4aq3w€ » pas simple !!
En fait, c'est dès la conception qu'il faut penser à la mémorisation du mot de passe. Un des moyens les plus simples est de créer une phrase dont on va conserver les premières lettres.
« Magister va vous permettre de mieux organiser votre sécurité » devient
Ma V v p 2 m 0 v $ ➔ **MaVvp2m0v$**
Les caractères surlignés en vert sont des chiffres. Ce mot de passe est simple à retenir

Exercice : Proposez un mot de passe fort à partir de la phrase suivante : « exercice cyber de création de mot de passe fort »

A minima, **l'ANSSI** (Agence Nationale de la Sécurité des Systèmes d'Information) estime que les 8 recommandations suivantes doivent s'appliquer indépendamment de tout contexte. Lorsque les systèmes d'information utilisés le permettent, certaines doivent être imposées techniquement.

R1	Utilisez des mots de passe différents pour vous authentifier auprès de systèmes distincts. En particulier, l'utilisation d'un même mot de passe pour sa messagerie professionnelle et pour sa messagerie personnelle est à proscrire impérativement.
R2	Choisissez un mot de passe qui n'est pas lié à votre identité (mot de passe composé d'un nom de société, d'une date de naissance, etc.).
R3	Ne demandez jamais à un tiers de créer pour vous un mot de passe.
R4	Modifiez systématiquement et au plus tôt les mots de passe par défaut lorsque les systèmes en contiennent.
R5	Renouvelez vos mots de passe avec une fréquence raisonnable. Tous les 90 jours est un bon compromis pour les systèmes contenant des données sensibles.
R6	Ne stockez pas les mots de passe dans un fichier sur un poste informatique particulièrement exposé au risque (exemple : en ligne sur internet), encore moins sur un papier facilement accessible.
R7	Ne vous envoyez pas vos propres mots de passe sur votre messagerie personnelle.
R8	Configurez les logiciels, y compris votre navigateur web, pour qu'ils ne se "souviennent" pas des mots de passe choisis.

- ✔ Allez sur le site http://www.passwordmeter.com et testez la force de quelques mots de passe.

Mail pour le DSI

Pour conclure, écrivez le mail pour le DSI :