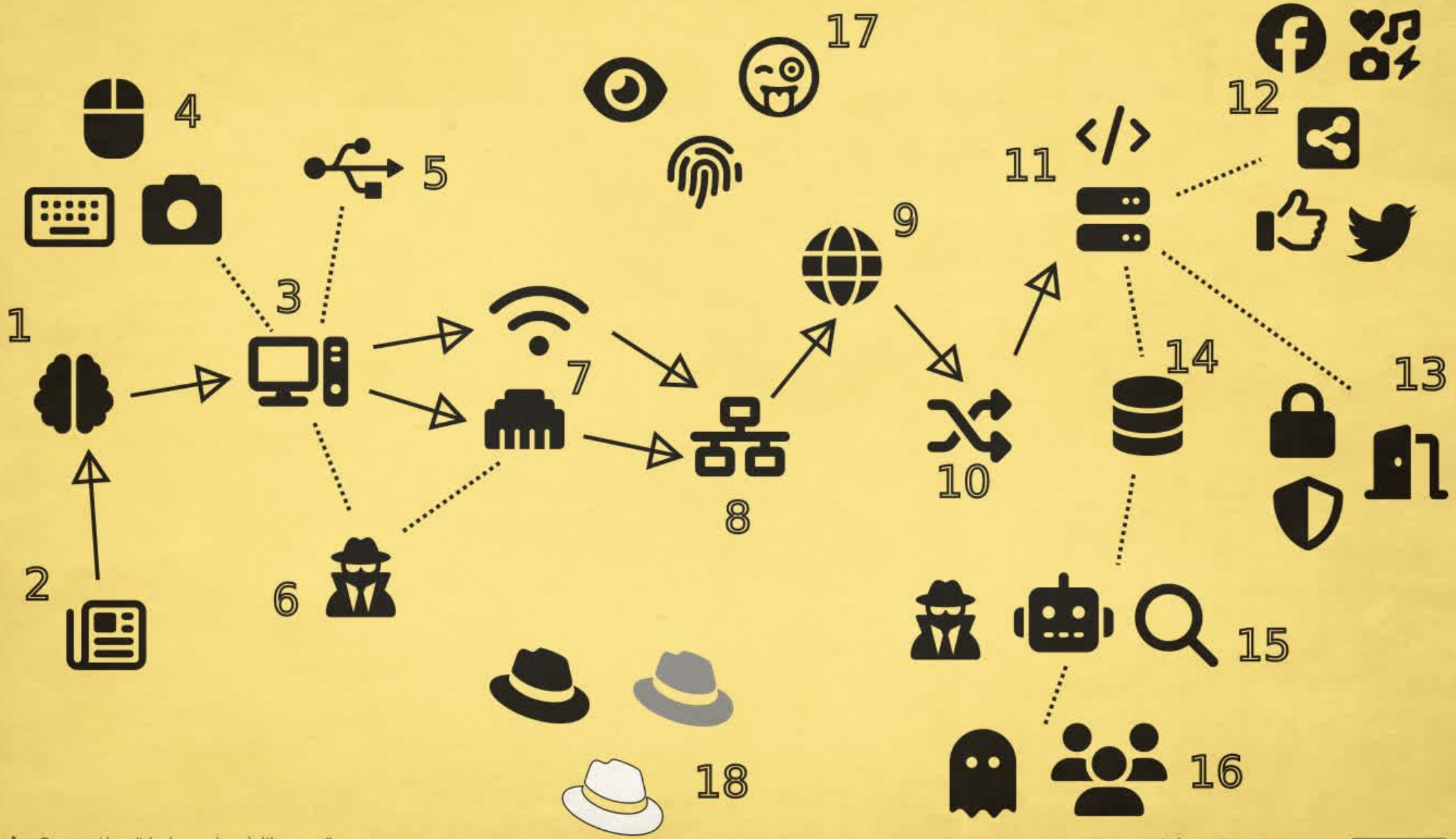
Hack : les bases

Le hack peut se faire à de multiples niveaux. Voici un schéma général de connexion sur un site. D'autres éléments existent par ailleurs.



Conception "de la graine à l'humus"
www.graineahumus.org

Récapitulatif

1-Tout part de l'utilisateur.

2-La désinformation, le hacking social, l'influence, p-hacking, usurpation d'identité (mail, téléphone…) sont les premières causes de hack. Cela peut être ciblé ou massif. Cela peut être légal (médias , religion, politique…) ou non. Intentionnel ou non. On peut aussi être observé à distance. (Exemple de social hacking).

Moyens de défenses :

- Site spécialisé (Conspiracy Watch, Checknews, France TV, Les décodeurs, Les observateurs, Hoaxbuster…)
- Réseau sociaux spécialisés (FAKE Investigation…)
- Outils d'analyse
  - Images : Sauvegardez l'image sur votre disque dur !
  - Images, données contenues dans une image : http://www.imageforensic.org/
  - Images, analyse de l'image : https://29a.ch/photo-forensics/#forensic-magnifier
  - Recherche d'origine d'une image (Tineye, google image, Yandex, autres…)
  - Texte : trouver la source (Recherche, google dorks…)
  - Vidéo (Manuel de vérification, Amnesty international…)
  - Analyse scientifique (Comment vérifier une info scientifique)
- Livre (Petit cours d'autodéfense intellectuelle…)
- Sensibilisation (La méthode scientifique, Horizon-gull, Defakator, Hygiène Mentale, Le chat sceptique, La Tronche en Biais, Ami story, Sabine…)
- Connaissance de l'existence de biais cognitifs
- Compréhension des enjeux d'une information, toujours connaître la source…

Principe de zététique

I. Le droit au rêve a pour pendant le devoir de vigilance.

II. Inexpliqué n'est pas inexplicable.

III. La charge de la preuve revient à celui qui l'affirme.

IV. Une allégation extraordinaire nécessite une preuve plus qu'ordinaire.

V. L'origine de l'information est fondamentale.

VI. Quantité de preuves n'est pas qualité de la preuve.

VII. La cohérence n'est pas une preuve.

VIII. Les croyances créent des illusions.

3-En dehors des virus, chevaux de troie, ransomwares qui s'attaquent à la partie software, il peut être possible d'avoir une faille hardware (du matériel). On peut aussi

attaquer le hardware (Stuxnet, centrales nucléaires, Macron, Hôpitaux, réseaux électriques, rom hack...).

Moyens de défenses :

- Connaissance des hacks hardware (Magazine ou site spécialisé)
- Utilisation de logiciels de confiance
- Protection de son système d'exploitation
- Mise à jour de sécurité
- Ne pas utiliser de système propriétaire (téléphone, box internet, ordinateur,...)
- Éviter les appareils connectés (souvent mal protégé cela fait des portes d'entrées.)
- Bonne utilisation de Linux
- Disque sécurisé par un mot de passe / ordinateur sécurisé par un mot de passe efficace

4-On se méfie peu des périphériques non amovibles.

Pourtant, ils sont des portes d'entrées potentielles. On peut déterminer un mot de passe au son de la frappe. Cacher un appareillage dans le matériel... On peut être observé à distance (jumelle, caméra espion,...) ou sur place (webcam, logiciel de connectivité à distance...)

Moyens de défenses :

- Connaissance des hacks hardware (Magazine ou site spécialisé)
- Sécuriser l'accès à son matériel physique
- USBKill ou autres outils de défense
- Cryptographie des données / dossiers sécurisés par un mot de passe

5-On se méfie un peu plus des périphériques amovibles.

Les moyens d'attaques sont multiples, surtout à partir de dongle (clé USB, un adaptateur WIFI, un émetteur de synchronisation pour lunettes 3D...)

Il existe des tueurs d'ordinateurs.

Moyens de défenses :

- Connaissance des hacks hardware (Magazine ou site spécialisé)
- Sécuriser l'accès à son matériel physique
- USBKill ou autres outils de défense

6-La captation des données par une tierce personne est une méthode assez connue qui connaît de nombreuses déclinaisons.

Moyens de défenses :

- Connaissance des hacks hardware (Magazine ou site spécialisé)
- Sécuriser l'accès à son matériel physique
- Ne pas utiliser de sans fil

- Ne pas se connecter sur des réseaux inconnus ou publics

7-Le sans fil est le moins sécurisé. Cependant, les prises ethernet peuvent être détournées et même écoutées.

Moyens de défenses :

- Connaissance des hacks hardware (Magazine ou site spécialisé)
- Connaissance du réseau
- Sécuriser l'accès à son matériel physique
- Ne pas utiliser de sans fil
- Utiliser un VPN, utiliser TOR
- Utiliser la cryptographie, clé PGP...

8-Le fournisseur internet peut ne pas agir dans notre intérêt...

Moyens de défenses :

- Utilisation d'un fournisseur d'accès associatif (FDN)

9-Les messages passent par un chemin physique et sont interceptables. (traceroute)

Moyens de défenses :

- Utiliser la cryptographie, clé PGP...

10-Avant d'arriver sur un site, une adresse de type IPV4 (exemple : 212.85.150.133) ou IPV6 (2001:0db8:0000:85a3:0000:0000:ac1f:8001) est redirigée. (DNS, IDN homograph attack : exemple apple).

Moyens de défenses :

- Ne pas cliquer sur un lien, mais le rechercher.
- Ne pas entrer des codes sur un site qui les a déjà enregistré.

11-Les attaques sur les sites sont trop nombreuses et trop changeantes pour les lister. (Injection SQL, code caché dans une image, vulnérabilité zero-day, vulnérabilité d'un outils web pas à jour,...)

Moyens des défenses :

- Mise à jour de sécurité.
- Utilisation de logiciels libres.
- Vérification de codes
- Prévenir les attaques (examens des logs, honeypot...)

12 et 14-Les réseaux sociaux plus spécifiquement récupèrent et revendent nos données (avec notre accord). Cela sert à des fins commerciales, politiques ou idéologiques généralement.

Nos habitudes, recherches, préférences sexuelles, convictions... Tout est passé au peigne fin.

Moyens des défenses :

- Quitter les réseaux sociaux, demander l'effacement de nos données.
- Naviguer en privé.
- Lire les contrats que l'on signe ou ne pas les signer.
- Refuser les cookies ou les trier
- Migrer sur des réseaux sociaux libres et décentralisés (Mastodon, Peertube, MobiliZon, Diaspora…)

13-Chaque site peut avoir des portes dérobées, utiliser plus ou moins de sécurité (CAF, pole emploi, impôts…)

15 et 16-Des failles peuvent être ciblées, automatisées, utiliser l'IA ou encore l'OSINT. Les failles ne sont pas toujours exploitées par des personnes malveillantes.

Lorsqu'elles sont exploitées de manière malveillante, les données peuvent être revendues directement (via des systèmes pas ou peu traçables, voire sur le darknet).

Moyens de défenses :

- Savoir si nos données ont fuité (Have I Been Pwned)
- Pratiquer l'OSINT (Epieos: Holehe, h8mail, shodan, maltego, OSINT Framework permet de voir pas mal d'outils en ligne, débuter en OSINT, autre cours débutant)
- Utiliser un mail poubelle pour certaines utilisations
- Utiliser des mots de passe distincts et sécurisés
- Être en auto-hébergement pour certains usages et utiliser des outils libres
- Utiliser le collectif CHATONS (Collectif des Hébergeurs Alternatifs, Transparents, Ouverts, Neutres et Solidaires) https://www.chatons.org/ pour des outils type GAFAM. Voir aussi https://degooglisons-internet.org/fr/
- Utiliser des outils et ressources libres : https://libre.graineahumus.org (Plus de 200 références ici)

17-À chaque étape, on peut retrouver des espions (humains ou non), mais aussi des plaisantins, des détectives… Ils peuvent utiliser les mêmes méthodes bien que les buts soient différents.

Nos traces numériques nous définissent avec une certaine précision (Suis-je unique ? Stylométrie, Mouvement de souris, comportements de recherche des internautes…)

Moyens de défenses :

- Exodus Privacy pour connaître les pisteurs et les autorisations sur son téléphone.

18-À chaque étape, on trouve des :

- white hat, soit un hacker éthique ou un expert en sécurité informatique.
- black hat, soit un hacker mal intentionné.
- grey hat, soit un hacker qui agit parfois avec éthique, et parfois non.

Un hacker est à l'origine un virtuose pouvant intervenir dans différents domaines de l'informatique ou techniques.

Plus récemment, on tend à en faire un pirate informatique opérant de façon non éthique.

Cette stigmatisation tend à faire oublier « L'éthique et les principes hackers ».

.....