Sensibilisation à la Sécurité Informatique

Éric BERTHOMIER
eric.berthomier@free.fr

16 mars 2022

Version 1.2 - Version Stagiaire

La cybersécurité n'est pas une chimère !

Qu'est ce qu'un système d'informations ?

Quelques éléments de vocabulaire

- Ver

Quelques éléments de vocabulaire

- Ver
- Ransomware

Quelques éléments de vocabulaire

- Ver
- Ransomware
- Adware

Quelques éléments de vocabulaire

- Ver
- Ransomware
- Adware
- Rootkit

Quelques éléments de vocabulaire

- Ver
- Ransomware
- Adware
- Rootkit
- Cheval de Troie

Quelques éléments de vocabulaire

- Ver
- Ransomware
- Adware
- Rootkit
- Cheval de Troie
- Numéroteur

Quelques éléments de vocabulaire

- Ver
- Ransomware
- Adware
- Rootkit
- Cheval de Troie
- Numéroteur
- Hoax

Quelques éléments de vocabulaire

- Ver
- Ransomware
- Adware
- Rootkit
- Cheval de Troie
- Numéroteur
- Hoax
- Keylogger

Quelques éléments de vocabulaire

- Ver
- Ransomware
- Adware
- Rootkit
- Cheval de Troie
- Numéroteur
- Hoax
- Keylogger
- Scareware / Rogue

Quelques éléments de vocabulaire

- Ver
- Ransomware
- Adware
- Rootkit
- Cheval de Troie
- Numéroteur
- Hoax
- Keylogger
- Scareware / Rogue
- SPAM Courriel et SMS

Quelques éléments de vocabulaire

- Ver
- Ransomware
- Adware
- Rootkit
- Cheval de Troie
- Numéroteur
- Hoax
- Keylogger
- Scareware / Rogue
- SPAM Courriel et SMS
- Phishing Courriel et SMS

Quelques éléments de vocabulaire

- Ver
- Ransomware
- Adware
- Rootkit
- Cheval de Troie
- Numéroteur
- Hoax
- Keylogger
- Scareware / Rogue
- SPAM Courriel et SMS
- Phishing Courriel et SMS
- Ingénierie Sociale

Quelques éléments de vocabulaire

- Ver
- Ransomware
- Adware
- Rootkit
- Cheval de Troie
- Numéroteur
- Hoax
- Keylogger
- Scareware / Rogue
- SPAM Courriel et SMS
- Phishing Courriel et SMS
- Ingénierie Sociale
- Multi-composants

Quelques éléments de vocabulaire

- Ver
- Ransomware
- Adware
- Rootkit
- Cheval de Troie
- Numéroteur
- Hoax
- Keylogger
- Scareware / Rogue
- SPAM Courriel et SMS
- Phishing Courriel et SMS
- Ingénierie Sociale
- Multi-composants
- Attaque ciblée / BotNet

Qui sont les méchants ?

- Script Kiddies : pour le plaisir de nuire

Qui sont les méchants ?

- Script Kiddies : pour le plaisir de nuire
- Hacker : pour se faire la main

Qui sont les méchants ?

- Script Kiddies : pour le plaisir de nuire
- Hacker : pour se faire la main
- Idéologies : Les données appartiennent à tous

Qui sont les méchants ?

- Script Kiddies : pour le plaisir de nuire
- Hacker : pour se faire la main
- Idéologies : Les données appartiennent à tous
- Recruteurs / Journalistes peu scrupuleux

Qui sont les méchants ?

- Script Kiddies : pour le plaisir de nuire
- Hacker : pour se faire la main
- Idéologies : Les données appartiennent à tous
- Recruteurs / Journalistes peu scrupuleux
- Terrorisme : pour déstabiliser l'État

Qui sont les méchants ?

- Script Kiddies : pour le plaisir de nuire
- Hacker : pour se faire la main
- Idéologies : Les données appartiennent à tous
- Recruteurs / Journalistes peu scrupuleux
- Terrorisme : pour déstabiliser l'État
- Espionnage : pour voler des informations

Qui sont les méchants ?

- Script Kiddies : pour le plaisir de nuire
- Hacker : pour se faire la main
- Idéologies : Les données appartiennent à tous
- Recruteurs / Journalistes peu scrupuleux
- Terrorisme : pour déstabiliser l'État
- Espionnage : pour voler des informations
- ...

Qui sont les méchants ?

- Script Kiddies : pour le plaisir de nuire
- Hacker : pour se faire la main
- Idéologies : Les données appartiennent à tous
- Recruteurs / Journalistes peu scrupuleux
- Terrorisme : pour déstabiliser l'État
- Espionnage : pour voler des informations
- ...

Qui sont les méchants ?

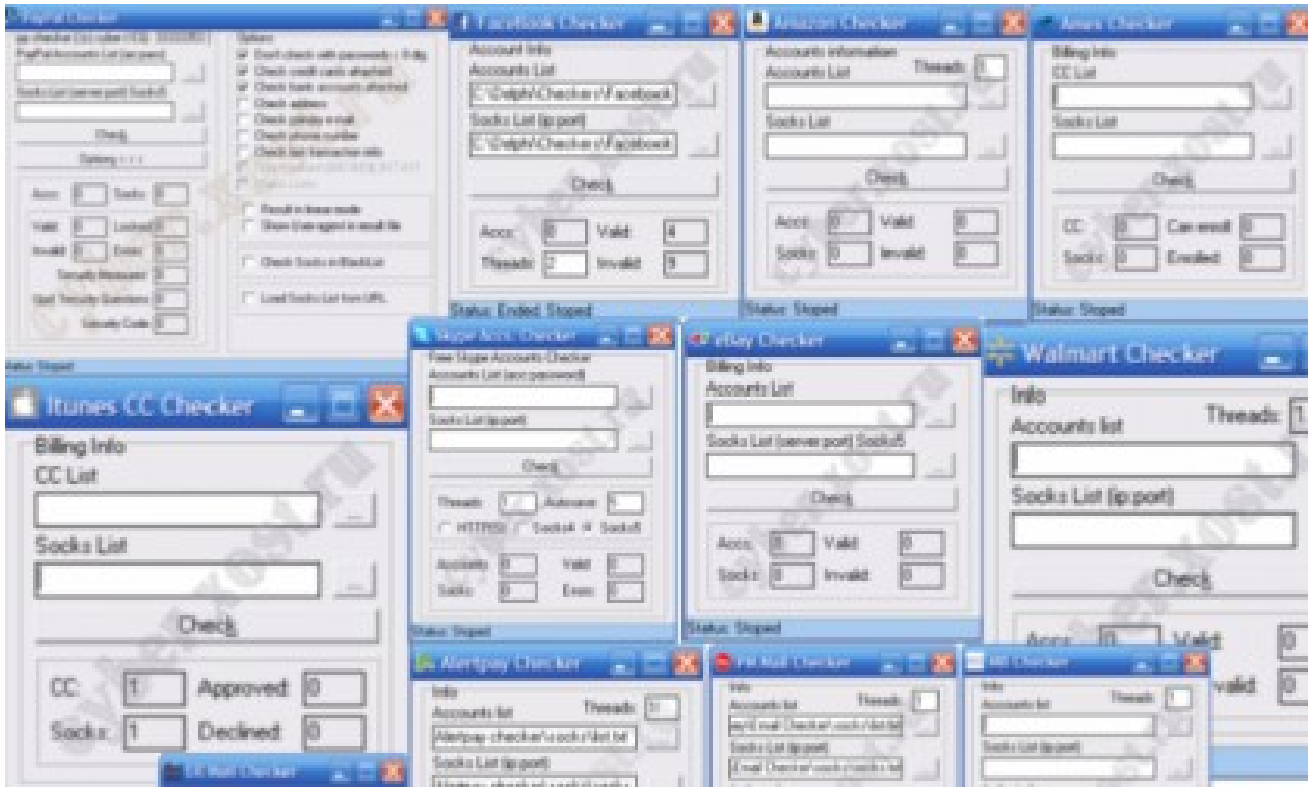
- Script Kiddies : pour le plaisir de nuire
- Hacker : pour se faire la main
- Idéologies : Les données appartiennent à tous
- Recruteurs / Journalistes peu scrupuleux
- Terrorisme : pour déstabiliser l'État
- Espionnage : pour voler des informations
- ...

Quel est le prix d'une donnée ?

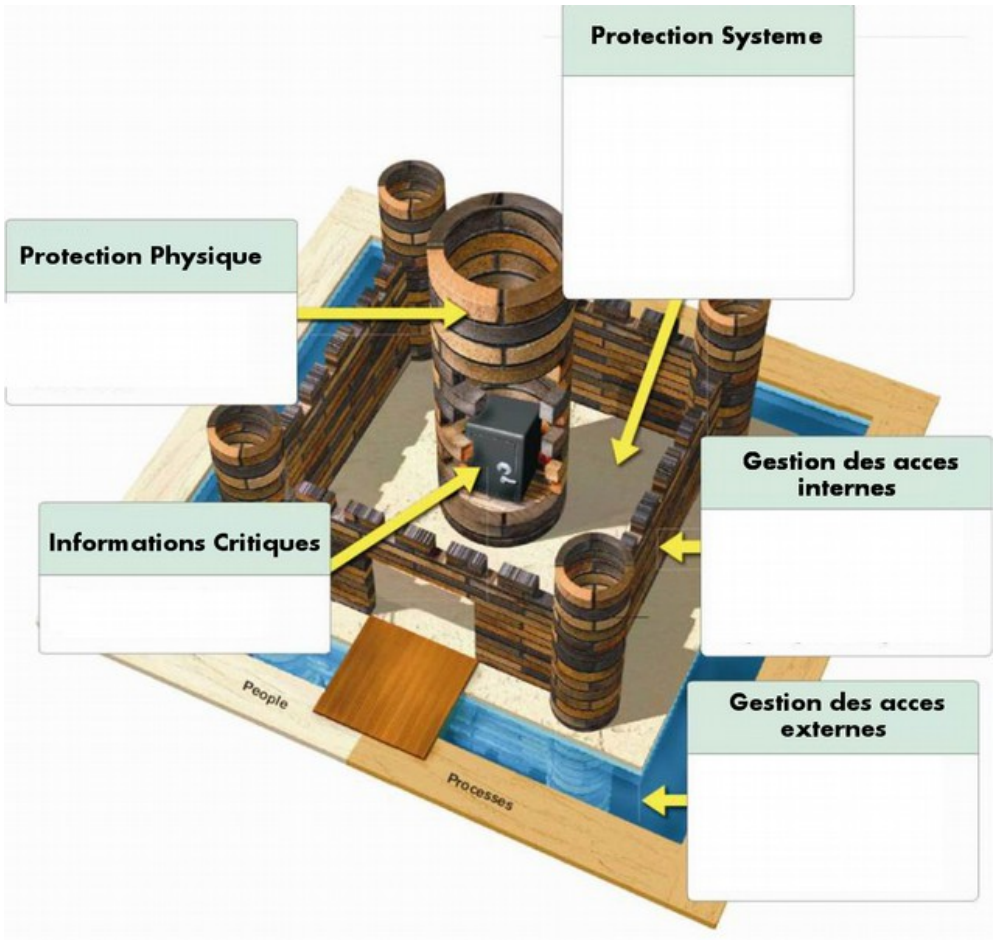
Une information qui n'a pas de valeur ce jour peut en avoir dans un avenir plus ou moins proche.

Mon ordinateur n'intéresse personne ... (1/2)

Mon ordinateur n'intéresse personne ... (2/2)



Fondamentaux de la SSI



Intégrité

Les données doivent :

- Être celles que l'on s'attend à ce qu'elles soient
- Ne doivent pas être altérées de façon fortuite ou volontaire.

Confidentialité

Les données doivent :

- Seules les personnes autorisées ont accès aux informations qui leur sont destinées.
- Tout accès indésirable doit être empêché.

Disponibilité

Les données doivent :

- Fonctionner sans faille durant les plages d'utilisation prévues,
- Garantir l'accès aux services et ressources installées avec le temps de réponse attendu.

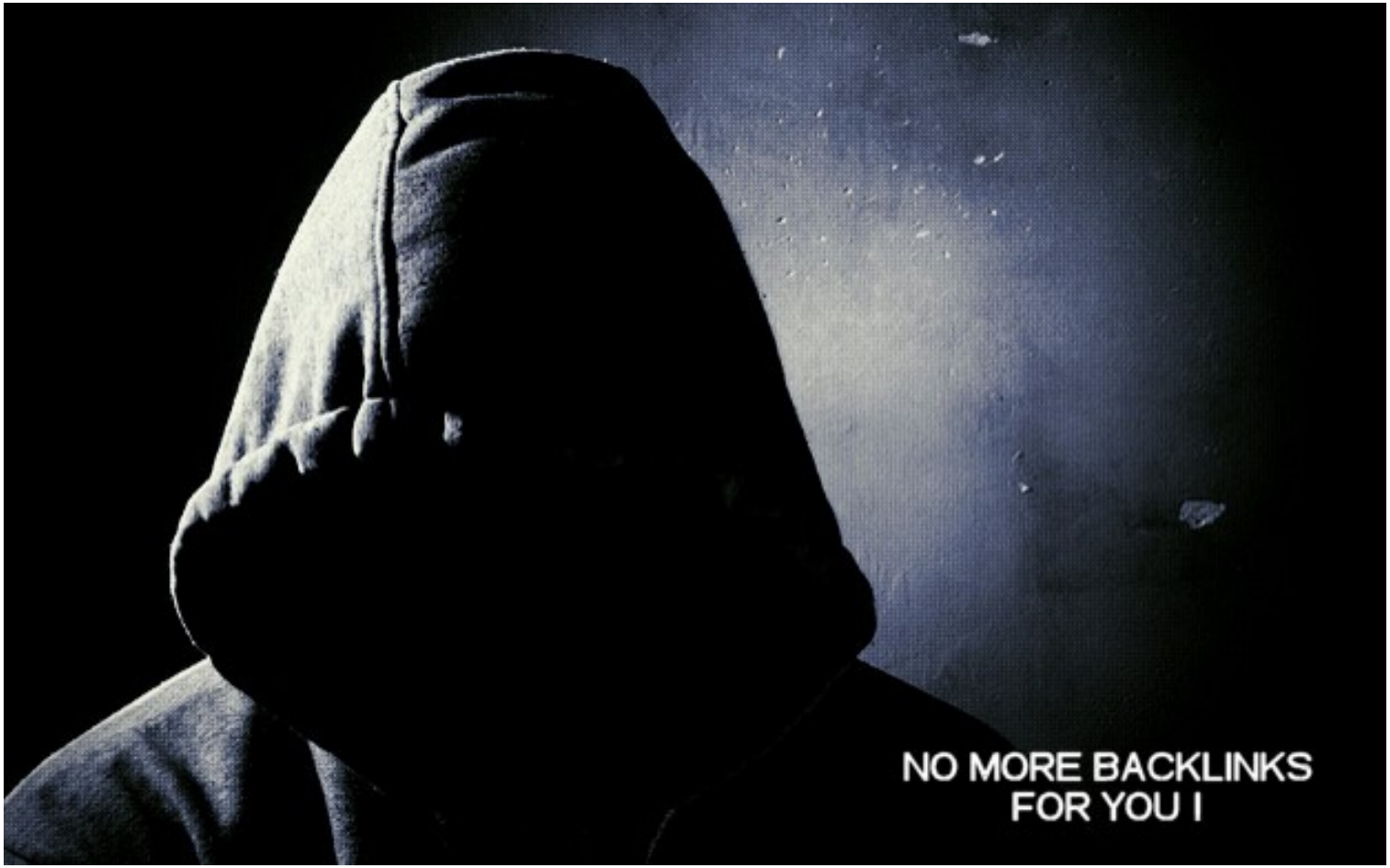
Identification

L'identification des utilisateurs est fondamentale pour gérer les accès aux espaces de travail pertinents et **maintenir la confiance dans les relations d'échange**.

Non répudiation et imputabilité

- Aucun utilisateur ne doit pouvoir contester les opérations qu'il a réalisé dans le cadre de ses actions autorisées,
- Aucun tiers ne doit pouvoir s'attribuer les actions d'un autre utilisateur.

Black Hat

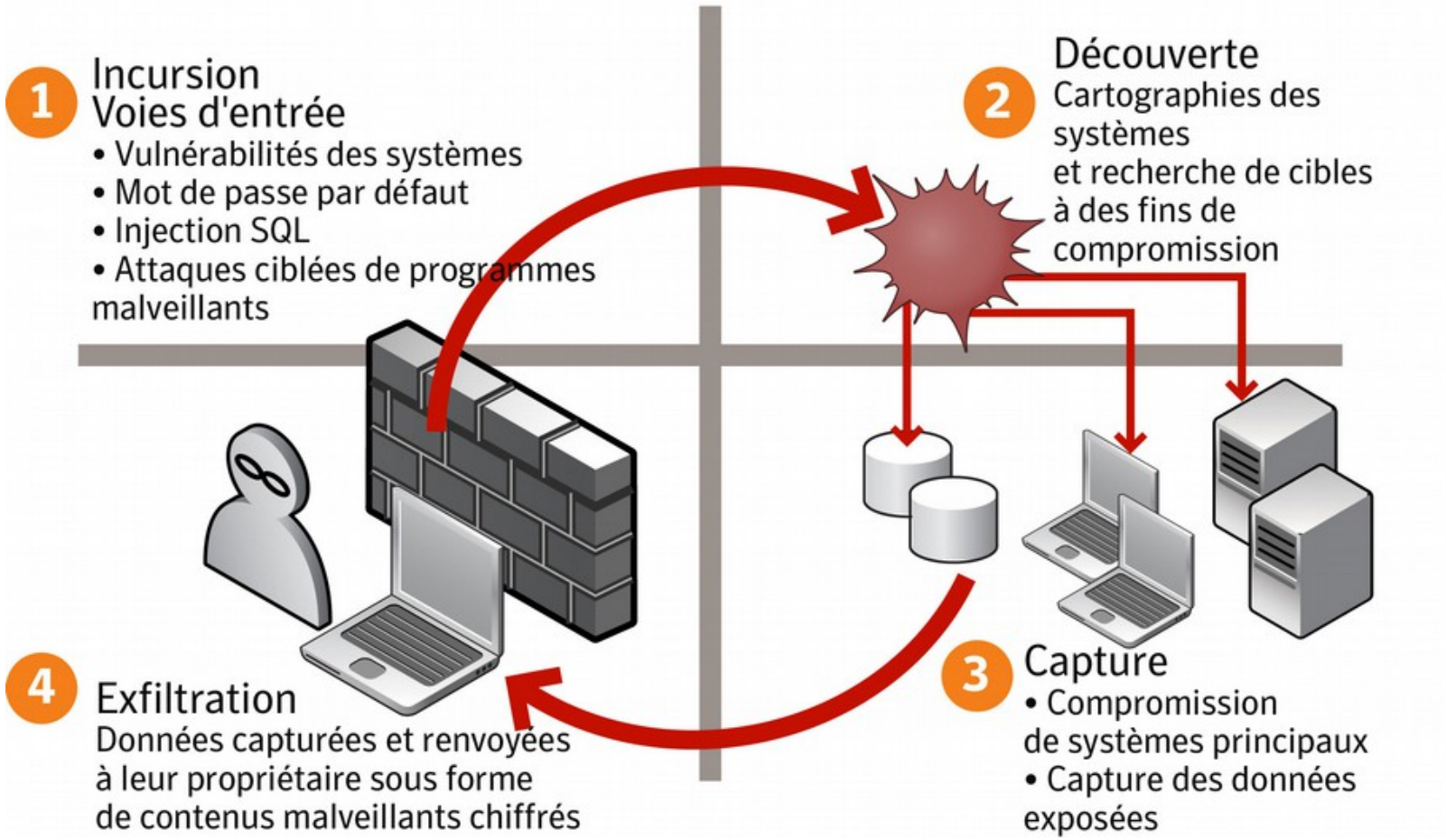


Principe

Connais ton ennemi et connais-toi toi-même ;
eussiez-vous cent guerres à soutenir, cent fois vous serez victorieux.

Sun Tzu L'Art de la Guerre - Article 3

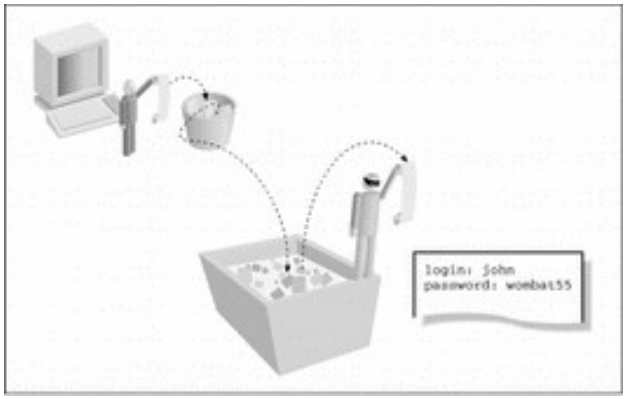
Autopsie d'une attaque



Dumpster diving

Le Hacker :

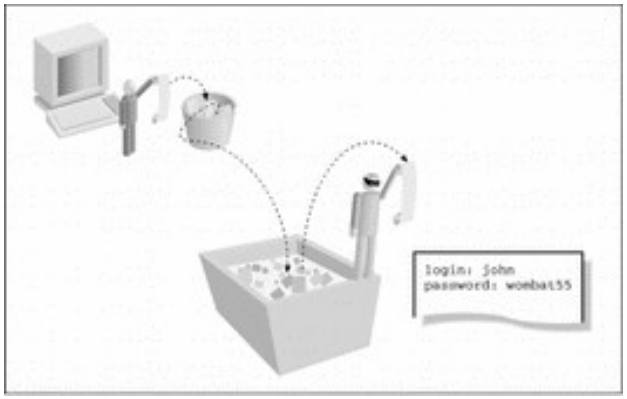
- Recherche des indices dans les poubelles pour pouvoir deviner les mots de passe de protection des ordinateurs.



Dumpster diving

Le Hacker :

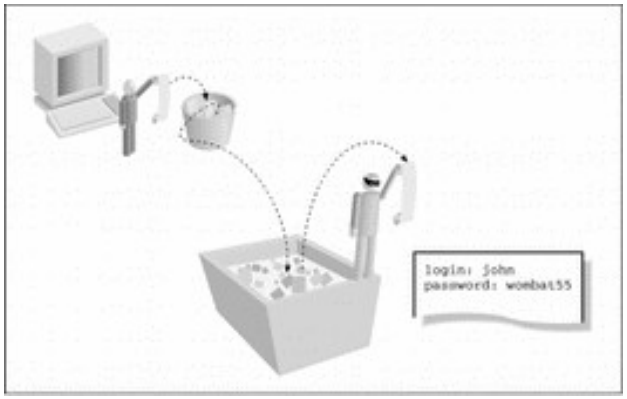
- Recherche des indices dans les poubelles pour pouvoir deviner les mots de passe de protection des ordinateurs.
- Recherche des documents qui n'auraient pas été convenablement détruits.



Dumpster diving

Le Hacker :

- Recherche des indices dans les poubelles pour pouvoir deviner les mots de passe de protection des ordinateurs.
- Recherche des documents qui n'auraient pas été convenablement détruits.
- Recherche à cartographier la structure du service et les relations existantes entre les utilisateurs (notamment de confiance).



Un nouveau jeu : le destructeur de documents -

DARPA [1] Shredder Challenge 2011

- Challenge informatique

1. Defense Advanced Research Projects Agency

Un nouveau jeu : le destructeur de documents -

DARPA [1] Shredder Challenge 2011

- Challenge informatique
- 5 documents découpés en 10.000 morceaux

1. Defense Advanced Research Projects Agency

Un nouveau jeu : le destructeur de documents -

DARPA [1] Shredder Challenge 2011

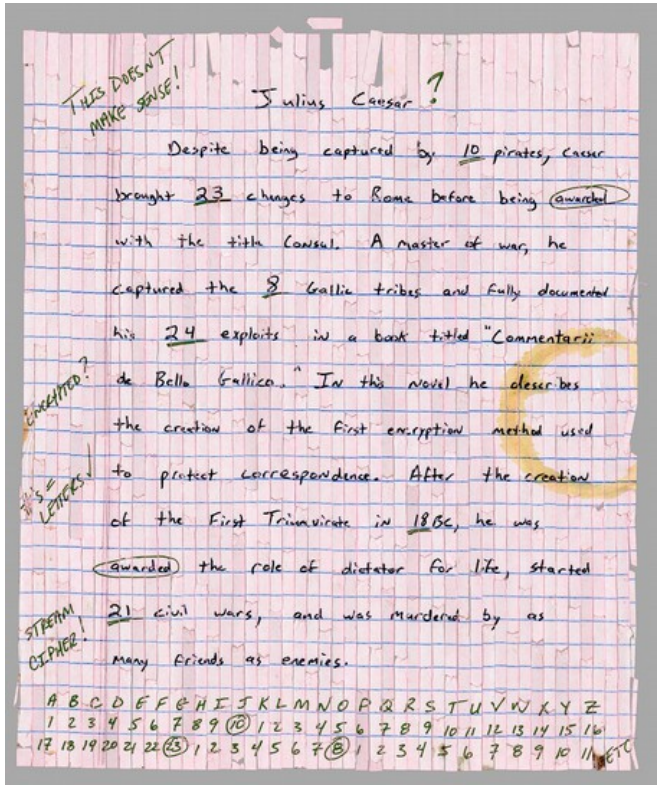
- Challenge informatique
- 5 documents découpés en 10.000 morceaux
- 600 heures de développement

1. Defense Advanced Research Projects Agency

Un nouveau jeu : le destructeur de documents -

DARPA [1] Shredder Challenge 2011

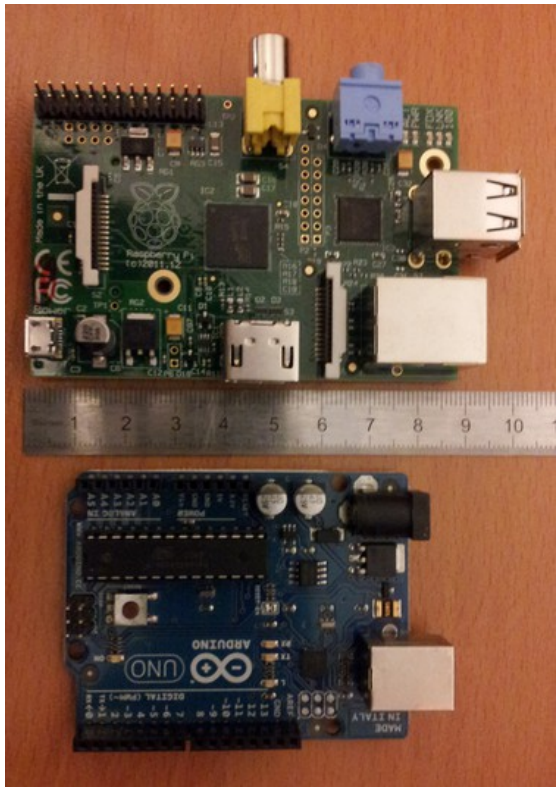
- Challenge informatique
- 5 documents découpés en 10.000 morceaux
- 600 heures de développement



Un résultat sans équivoque

1. Defense Advanced Research Projects Agency

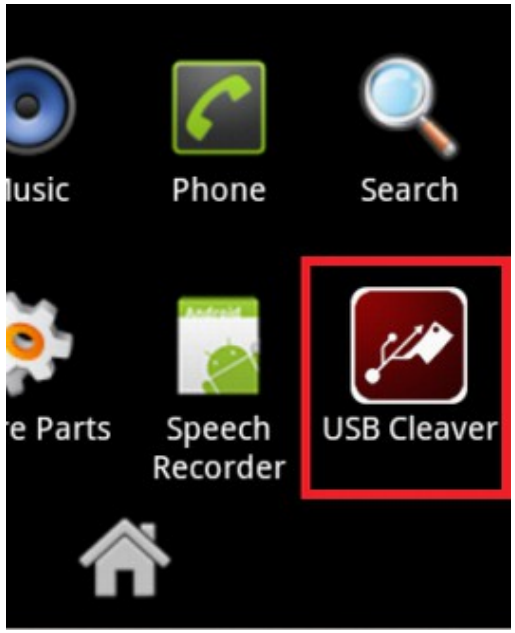
Do it yourself !



Mon cher téléphone

USB Cleaver est un logiciel permettant de voler l'ensemble des informations contenues sur votre ordinateur lorsque vous y connectez votre portable.

- Copie des informations Système

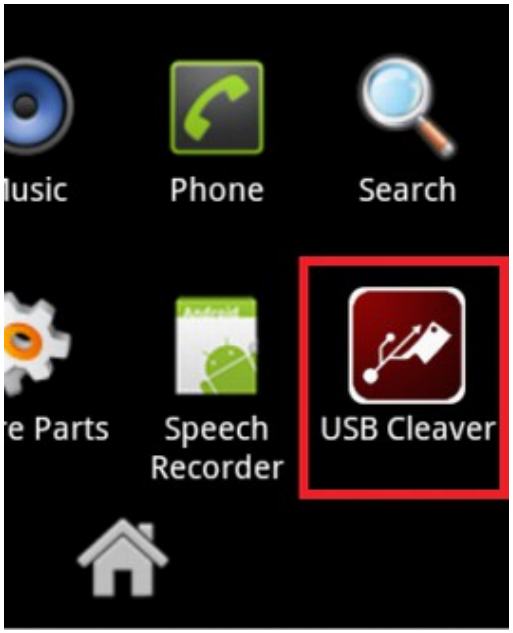


Simple comme un téléchargement . . .

Mon cher téléphone

USB Cleaver est un logiciel permettant de voler l'ensemble des informations contenues sur votre ordinateur lorsque vous y connectez votre portable.

- Copie des informations Système
- Copie des mots de passe IE

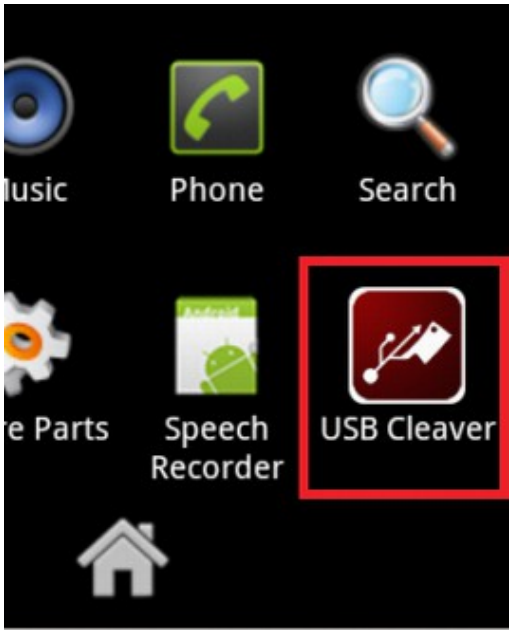


Simple comme un téléchargement . . .

Mon cher téléphone

USB Cleaver est un logiciel permettant de voler l'ensemble des informations contenues sur votre ordinateur lorsque vous y connectez votre portable.

- Copie des informations Système
- Copie des mots de passe IE
- Copie des mots de passe Google Chrome

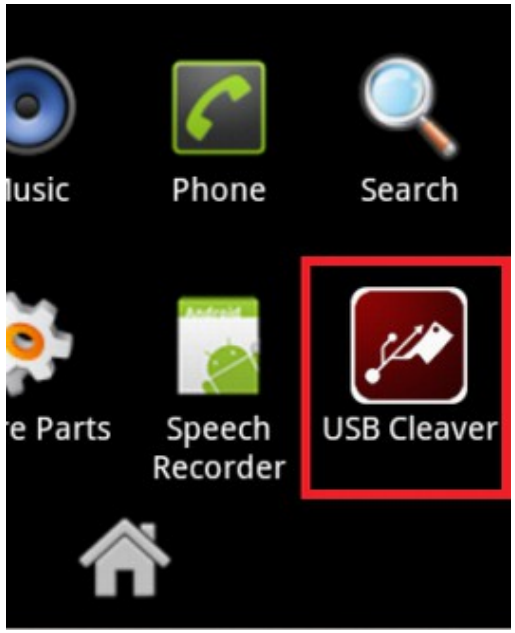


Simple comme un téléchargement . . .

Mon cher téléphone

USB Cleaver est un logiciel permettant de voler l'ensemble des informations contenues sur votre ordinateur lorsque vous y connectez votre portable.

- Copie des informations Système
- Copie des mots de passe IE
- Copie des mots de passe Google Chrome
- Copie des mots de passe Firefox

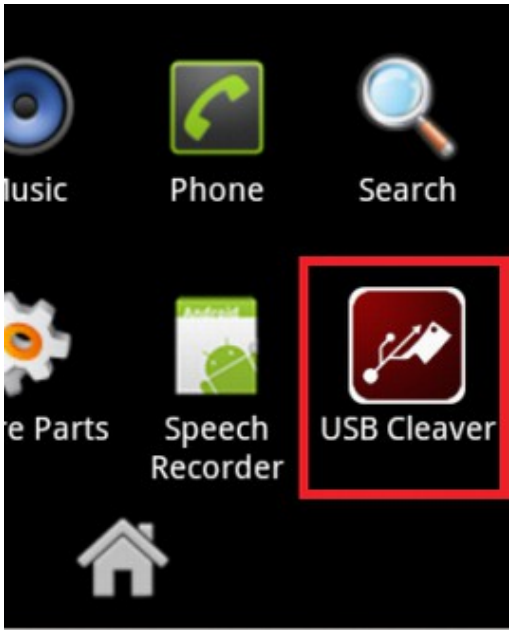


Simple comme un téléchargement . . .

Mon cher téléphone

USB Cleaver est un logiciel permettant de voler l'ensemble des informations contenues sur votre ordinateur lorsque vous y connectez votre portable.

- Copie des informations Système
- Copie des mots de passe IE
- Copie des mots de passe Google Chrome
- Copie des mots de passe Firefox
- Copie des mots de passe Wifi



Simple comme un téléchargement . . .

Clé USB - Périphérique de stockage

- Capacité de stockage : 2 To

Clé USB - Périphérique de stockage

- Capacité de stockage : 2 To
- Perte

Clé USB - Périphérique de stockage

- Capacité de stockage : 2 To
- Perte
- Vol

Clé USB - Périphérique de stockage

- Capacité de stockage : 2 To
- Perte
- Vol
- Informations non protégées

Clé USB - Périphérique de stockage

- Capacité de stockage : 2 To
- Perte
- Vol
- Informations non protégées
- Transport de virus

Clé USB - Périphérique de stockage

- Capacité de stockage : 2 To
- Perte
- Vol
- Informations non protégées
- Transport de virus
- Transport de malwares

Clé USB - Périphérique de stockage

- Capacité de stockage : 2 To
- Perte
- Vol
- Informations non protégées
- Transport de virus
- Transport de malwares

Clé USB - Périphérique de stockage

- Capacité de stockage : 2 To
- Perte
- Vol
- Informations non protégées
- Transport de virus
- Transport de malwares

Si tu ne peux attaquer l'entreprise, attaque l'employé.

Clé USB - Périphérique de destruction

HOME USB KILLER TEST SHIELD USB KILL COMMUNITY CONTACT BLOG FAQ

HOME / USB KILLER / USB KILLER

USB KILLER

49,95 €

Finally available! The USB Killer is a device designed to testing the surge protection of electronics to their limits - and beyond.

LIMITED TIME: Buy with the **Test Shield** and receive **50% discount** on the USB Shield and **free shipping for both products!** *(applied at checkout)*

In Stock!

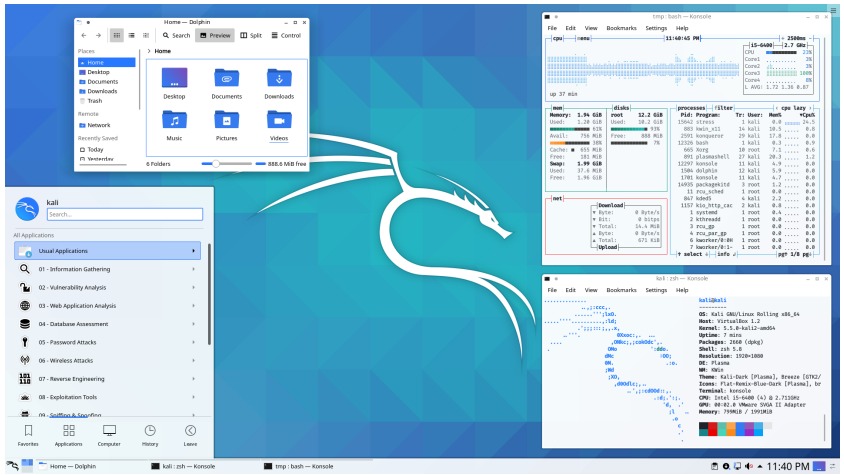
QUANTITY 1 - + ADD TO CART

Clé USB - Périphérique de vol d'informations

Clé USB : Périphérique offensif

Démarrage possible d'un PC sur une clé USB pour :

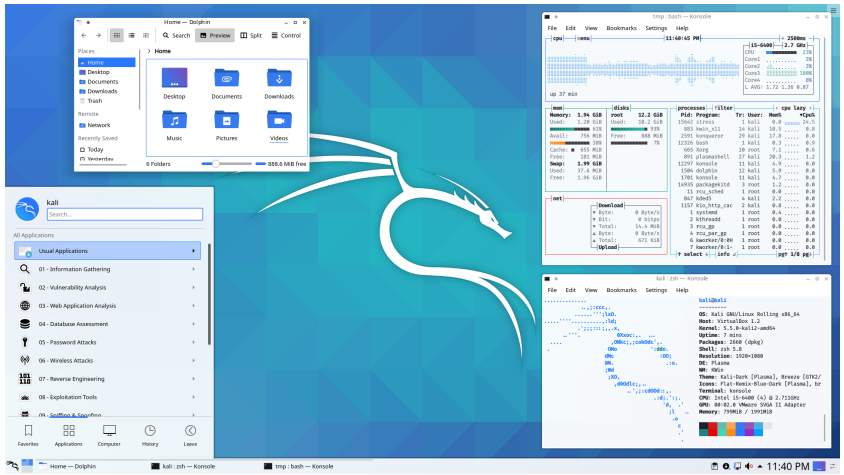
- Outrepasser les protections de l'ordinateur



Clé USB : Périphérique offensif

Démarrage possible d'un PC sur une clé USB pour :

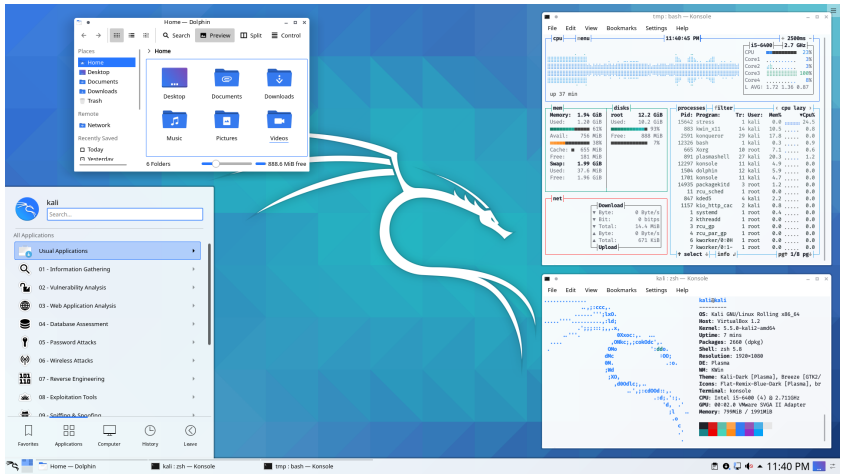
- Outrepasser les protections de l'ordinateur
- Exécuter des logiciels de sécurité informatique



Clé USB : Périphérique offensif

Démarrage possible d'un PC sur une clé USB pour :

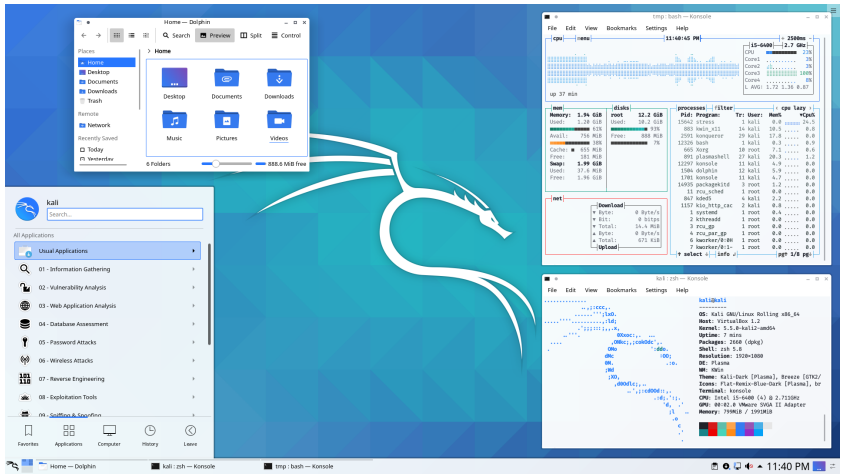
- Outrepasser les protections de l'ordinateur
- Exécuter des logiciels de sécurité informatique
- Voler les informations



Clé USB : Périphérique offensif

Démarrage possible d'un PC sur une clé USB pour :

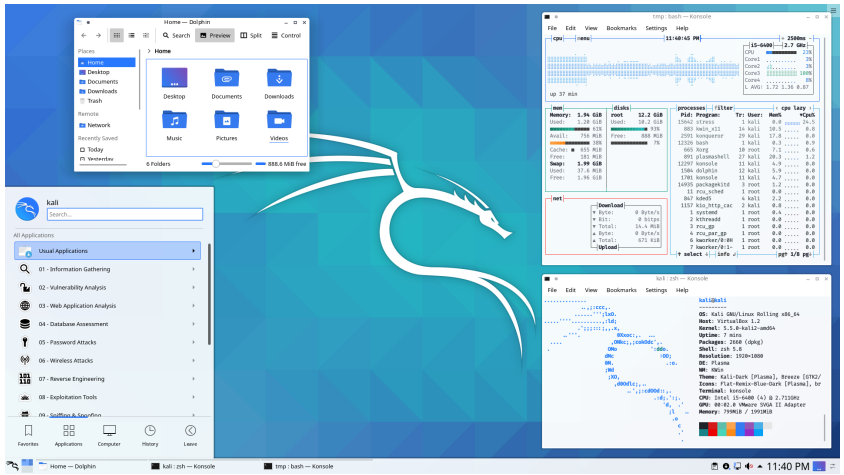
- Outrepasser les protections de l'ordinateur
- Exécuter des logiciels de sécurité informatique
- Voler les informations
- Masquer l'identité du poste



Clé USB : Périphérique offensif

Démarrage possible d'un PC sur une clé USB pour :

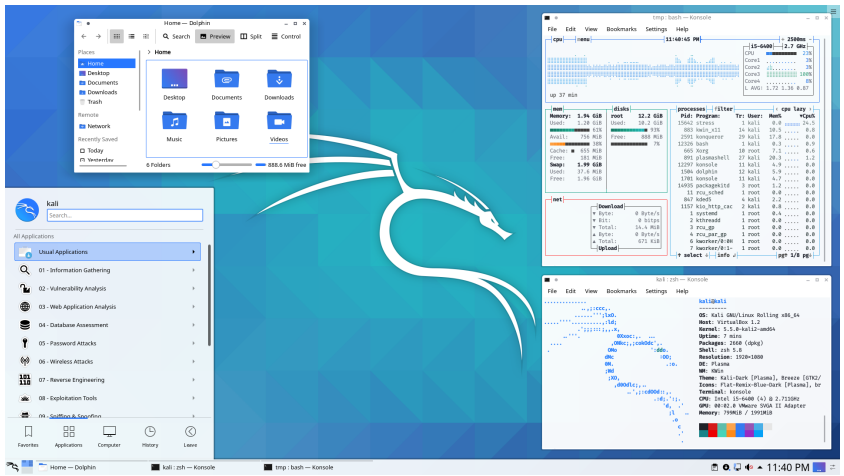
- Outrepasser les protections de l'ordinateur
- Exécuter des logiciels de sécurité informatique
- Voler les informations
- Masquer l'identité du poste
- Implanter des espions



Clé USB : Périphérique offensif

Démarrage possible d'un PC sur une clé USB pour :

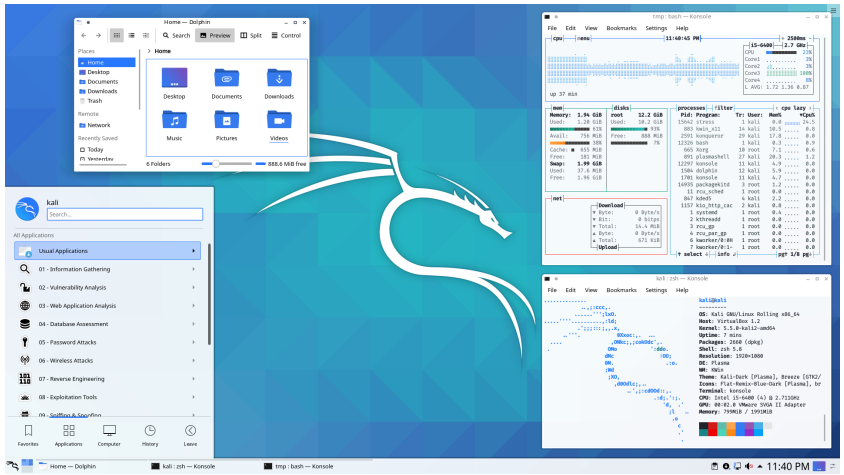
- Outrepasser les protections de l'ordinateur
- Exécuter des logiciels de sécurité informatique
- Voler les informations
- Masquer l'identité du poste
- Implanter des espions
- Observer



Clé USB : Périphérique offensif

Démarrage possible d'un PC sur une clé USB pour :

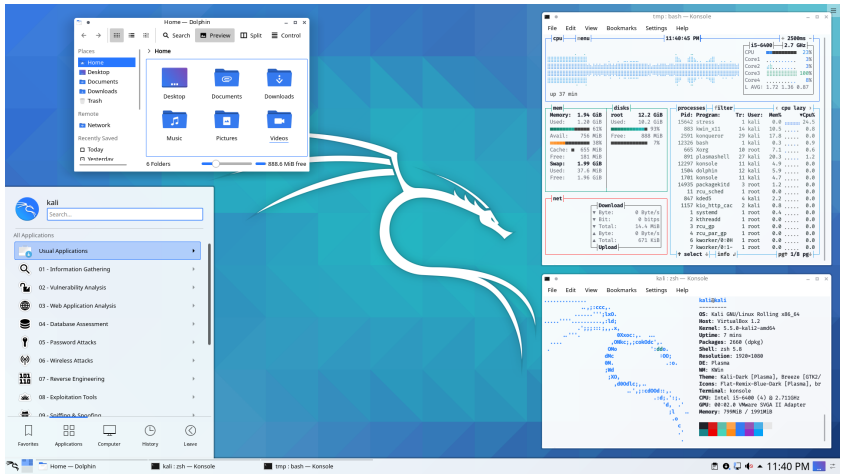
- Outrepasser les protections de l'ordinateur
- Exécuter des logiciels de sécurité informatique
- Voler les informations
- Masquer l'identité du poste
- Implanter des espions
- Observer
- Détruire



Clé USB : Périphérique offensif

Démarrage possible d'un PC sur une clé USB pour :

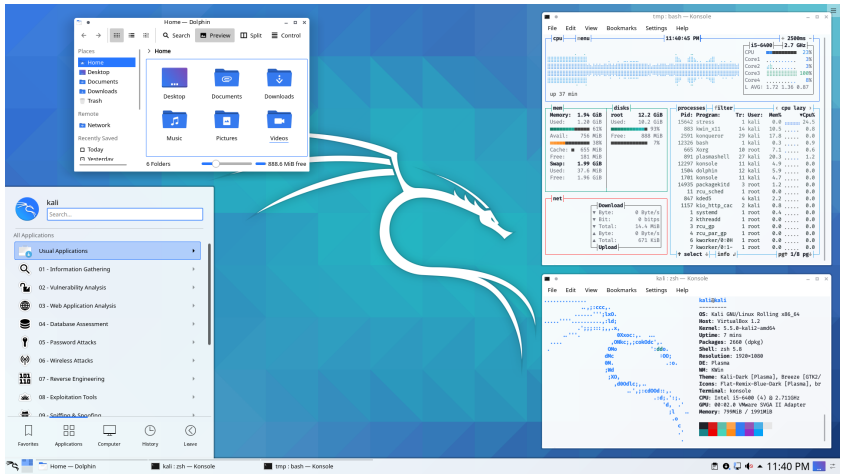
- Outrepasser les protections de l'ordinateur
- Exécuter des logiciels de sécurité informatique
- Voler les informations
- Masquer l'identité du poste
- Implanter des espions
- Observer
- Détruire



Clé USB : Périphérique offensif

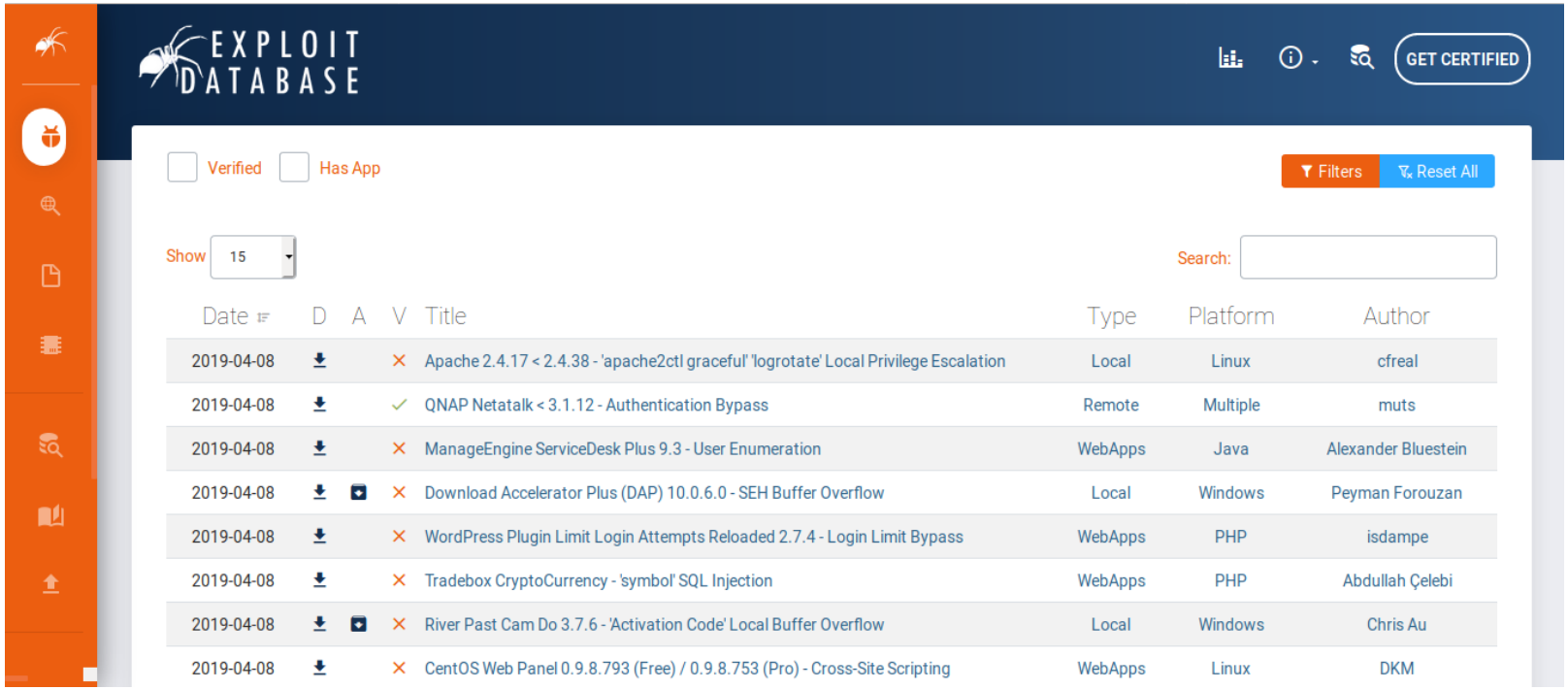
Démarrage possible d'un PC sur une clé USB pour :

- Outrepasser les protections de l'ordinateur
- Exécuter des logiciels de sécurité informatique
- Voler les informations
- Masquer l'identité du poste
- Implanter des espions
- Observer
- Détruire

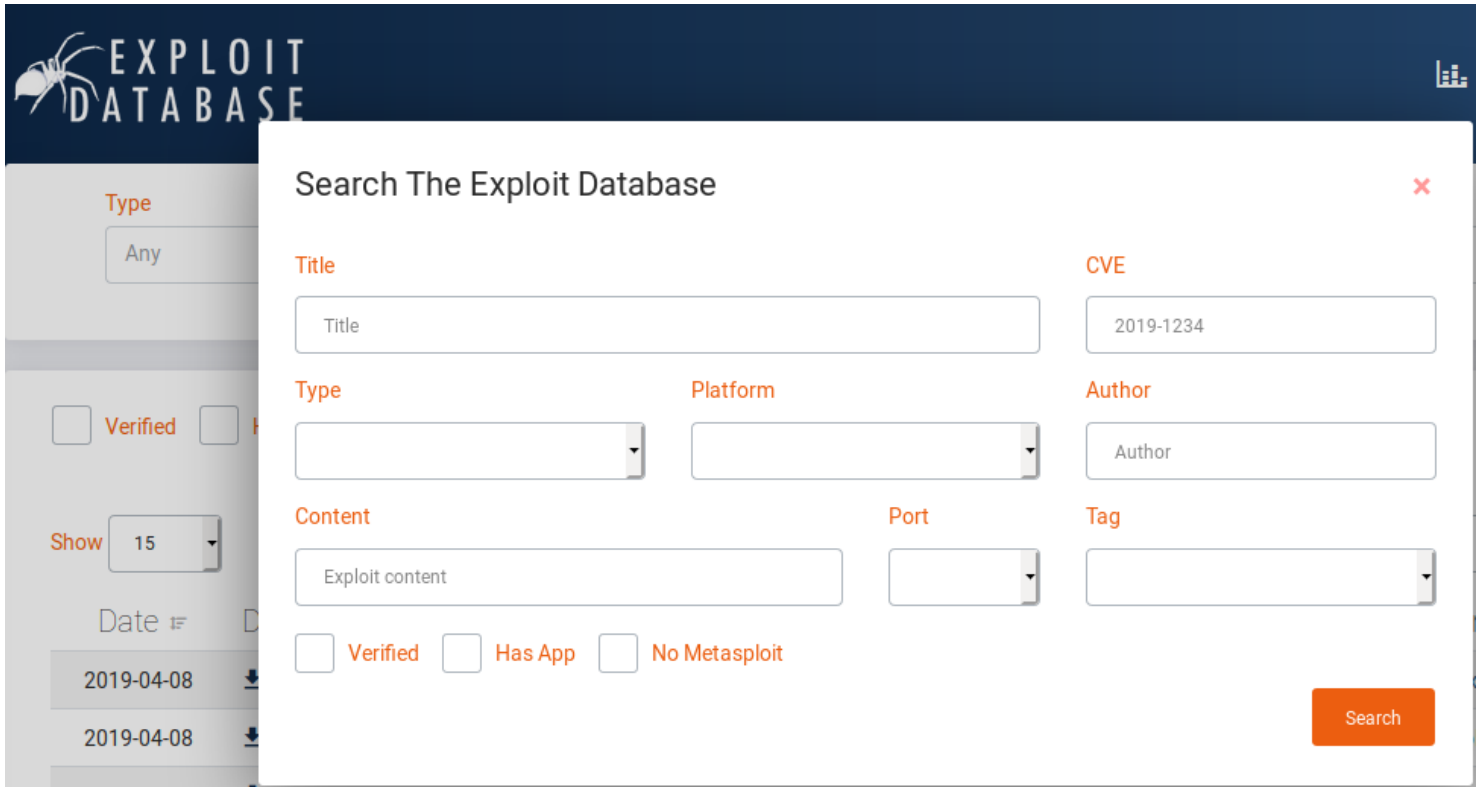


Simple comme un téléchargement. . .

Exploit Database (1/2)



Exploit Database (2/2)



Conclusion - Cyberattaque

On s'est beaucoup plus concentré sur le fait d'augmenter les services qu'on offrait à la population via le numérique qu'au . . .

Conclusion - Cyberattaque

On s'est beaucoup plus concentré sur le fait d'augmenter les services qu'on offrait à la population via le numérique qu'au . . .

fait de **protéger l'architecture des systèmes**.

Christophe BECHU Maire dAngers 21 janvier 2021

Démonstration

Démonstration

Un virus possède, à minima, les mêmes droits que vous !

Des questions ?