

Sensibilisation à la Sécurité Informatique

Éric BERTHOMIER
eric.berthomier@free.fr

16 mars 2022



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
- ...

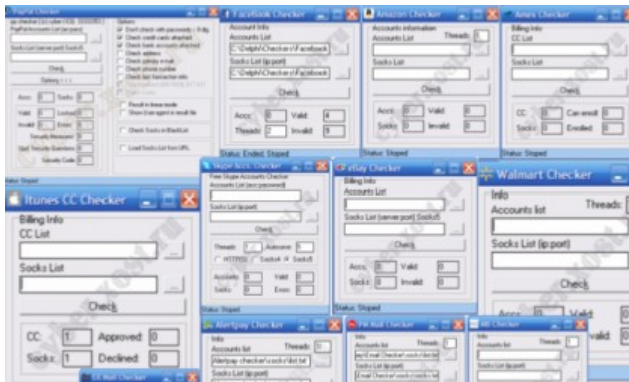
Quel est le prix d'une donnée ?

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

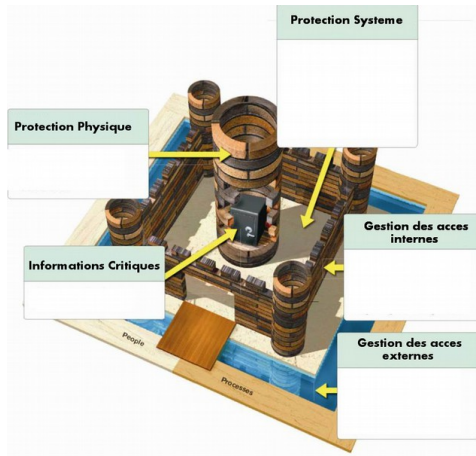
Mon ordinateur n'intéresse personne ... (1/2)



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



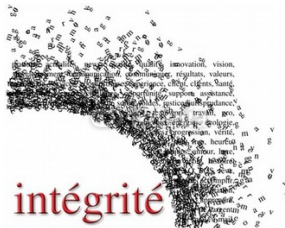
Fondamentaux de la SSI



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



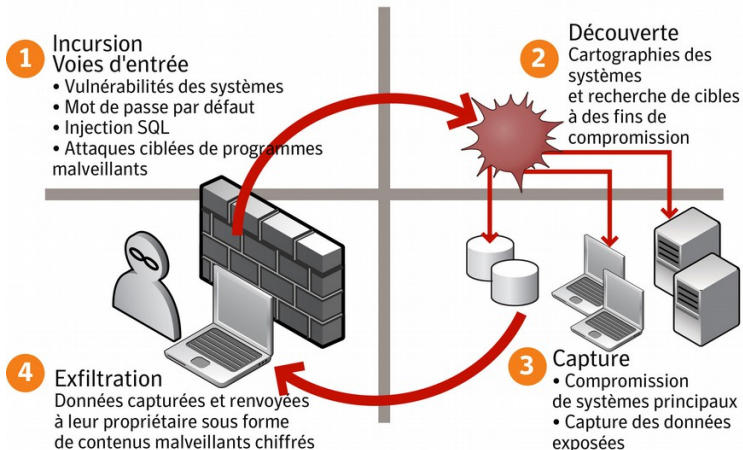
Principe



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

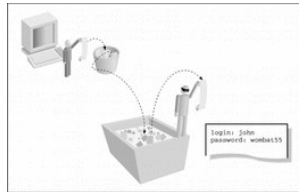
Autopsie d'une attaque



Dumpster diving

Le Hacker :

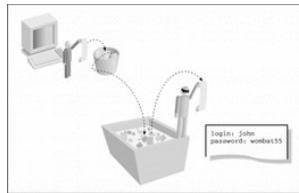
- Recherche des indices dans les poubelles pour pouvoir deviner les mots de passe de protection des ordinateurs.



Dumpster diving

Le Hacker :

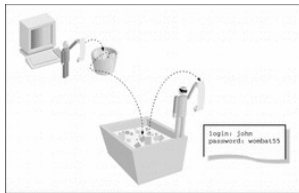
- Recherche des indices dans les poubelles pour pouvoir deviner les mots de passe de protection des ordinateurs.
- Recherche des documents qui n'auraient pas été convenablement détruits.



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 -

DARPA¹ Shredder Challenge 2011

- Challenge informatique

1. Defense Advanced Research Projects Agency

Un nouveau jeu : le destructeur de documents -

DARPA¹ 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 -

DARPA¹ Shredder Challenge 2011

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

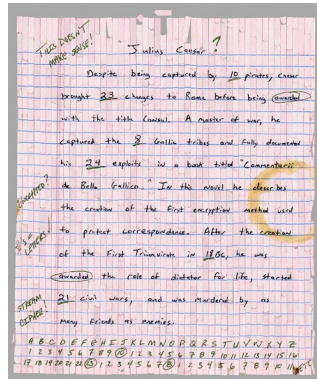
1. Defense Advanced Research Projects Agency

Un nouveau jeu : le destructeur de documents -

DARPA¹ 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

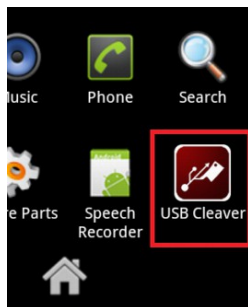
Do it yourself !



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



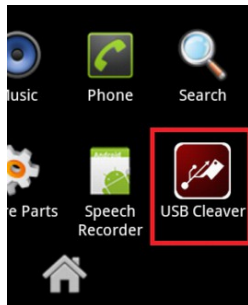
Simple comme un téléchargement



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

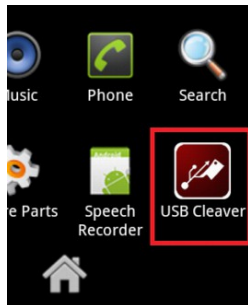


Simple comme un téléchargement

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

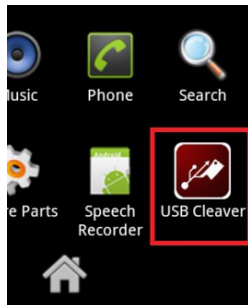


Simple comme un téléchargement

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...

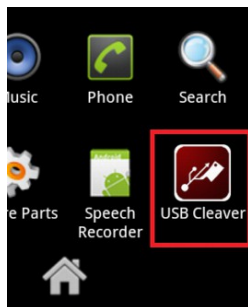


Mon cher téléphone

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



KeyGrabber Keylogger Matériel

Keylogger matériel Wi-Fi USB déjà en vente ! Ce keylogger KeyGrabber Wi-Fi a deux fonctions : **enregistreur de frappe** et **clé USB** pour une lecture de données immédiate. **Compatible avec tout clavier USB**, ne nécessite aucun pilote. Jusqu'à 2 Go de mémoire !

Page d'accueil	Produits	Documents	Télécharger	Contact	Commander
----------------	----------	-----------	-------------	---------	-----------

liens rapides
Page d'accueil
Keylogger matériel USB et PS/2 : comparaison
Enregistreur de frappe - avantages
Comment commander ?
VISA MasterCard American Express
VISA Electron Mastercard UnionPay
Find us on Facebook
YouTube Twitter
YouTube Twitter

Livraison gratuite aux Etats-Unis !
Pour de détails visitez [KeyGrabber](#)

Transport international
\$5.49 ou €3.99 (détails)

Achetez nos produits sur: [Buy.com](#)
[Google Products](#) [Sears](#) [Amazon](#)

English Deutsch Español Français Italiano Português Polski Русский



KeyGrabber Wi-Fi Premium

Le premier keylogger matériel avec **WLAN** incorporé ! Ce keylogger est capable de se connecter à Internet par un Point d'Accès et envoyer les données de frappe enregistrées sous forme d'un **message E-mail**. Grâce à ce **keylogger matériel Wi-Fi**, vous pouvez surveiller votre ordinateur depuis le **monde entier** en consultant juste votre **boîte E-mail**! Absolument indétectable pour le logiciel ! [\[en savoir plus...\]](#)

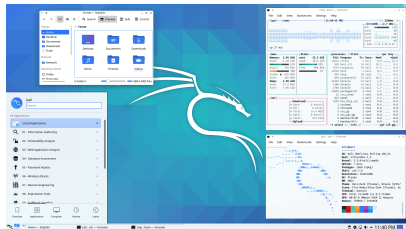
ver USB 2 Go - \$149.99 | €109.99
ver PS/2 2 Go - \$139.99 | €102.99



Clé USB : Périphérique offensif

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

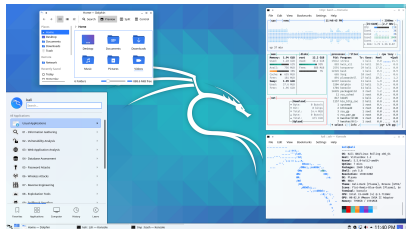
- Outrepasser les protections de l'ordinateur



Clé USB : Périphérique offensif

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

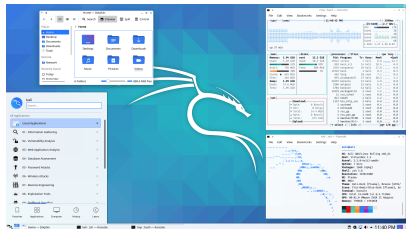
- Outrepasser les protections de l'ordinateur
- Exécuter des logiciels de sécurité informatique



Clé USB : Périphérique offensif

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

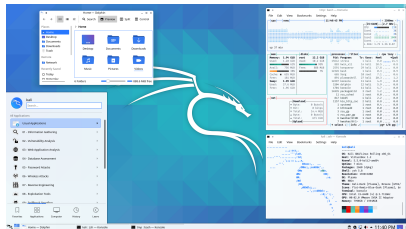
- Outrepasser les protections de l'ordinateur
- Exécuter des logiciels de sécurité informatique
- Voler les informations



Clé USB : Périphérique offensif

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

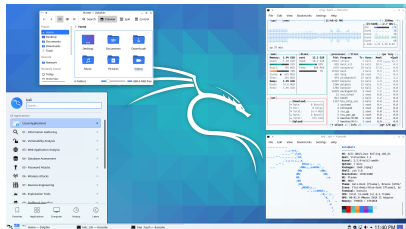
- Outrepasser les protections de l'ordinateur
- Exécuter des logiciels de sécurité informatique
- Voler les informations
- Masquer l'identité du poste



Clé USB : Périphérique offensif

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

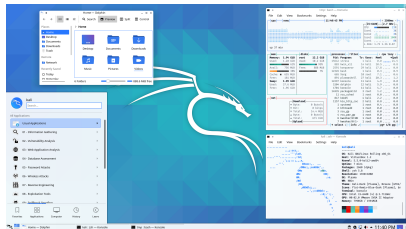
- Outrepasser les protections de l'ordinateur
- Exécuter des logiciels de sécurité informatique
- Voler les informations
- Masquer l'identité du poste
- Implanter des espions



Clé USB : Périphérique offensif

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

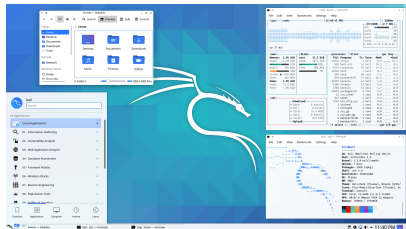
- Outrepasser les protections de l'ordinateur
- Exécuter des logiciels de sécurité informatique
- Voler les informations
- Masquer l'identité du poste
- Implanter des espions
- Observer



Clé USB : Périphérique offensif

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

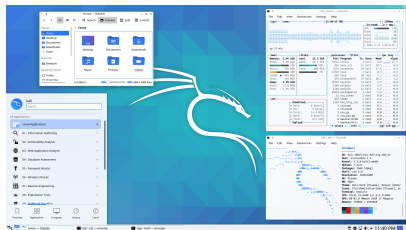
- Outrepasser les protections de l'ordinateur
- Exécuter des logiciels de sécurité informatique
- Voler les informations
- Masquer l'identité du poste
- Implanter des espions
- Observer
- Détruire



Clé USB : Périphérique offensif

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

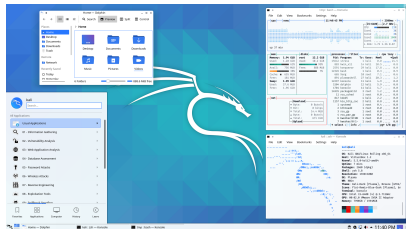
- Outrepasser les protections de l'ordinateur
- Exécuter des logiciels de sécurité informatique
- Voler les informations
- Masquer l'identité du poste
- Implanter des espions
- Observer
- Détruire



Clé USB : Périphérique offensif

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

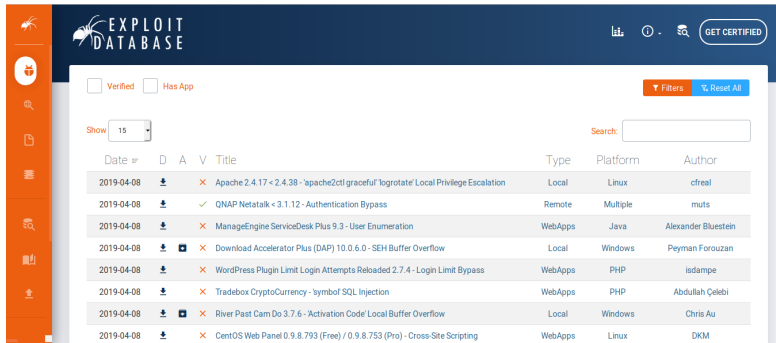
- Outrepasser les protections de l'ordinateur
- Exécuter des logiciels de sécurité informatique
- Voler les informations
- Masquer l'identité du poste
- Implanter des espions
- Observer
- Détruire



Simple comme un téléchargement...



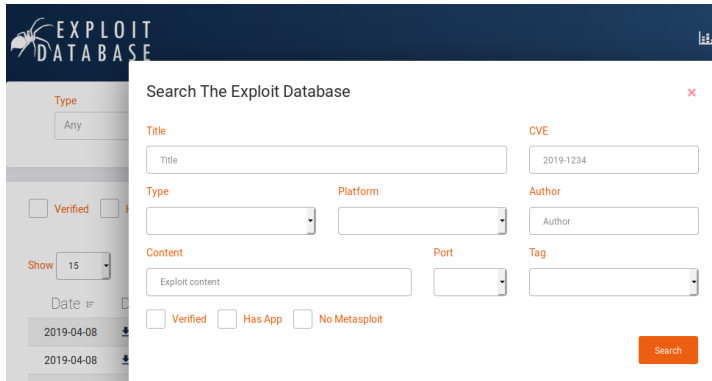
Exploit Database (1/2)



The screenshot shows the Exploit Database website interface. The header includes the logo, navigation icons, and a 'GET CERTIFIED' button. The main content area displays a list of exploits with filters for 'Verified' and 'Has App'. A search bar and a 'Show' dropdown are also present. The table lists exploits with columns for Date, D (Download), A (Add), V (Verify), Title, Type, Platform, and Author.

Date	D	A	V	Title	Type	Platform	Author
2019-04-08	📄	✗		Apache 2.4.17 < 2.4.38 - 'apache2ctl graceful' 'logrotate' Local Privilege Escalation	Local	Linux	cfreal
2019-04-08	📄	✓		QNAP Netatalk < 3.1.12 - Authentication Bypass	Remote	Multiple	muts
2019-04-08	📄	✗		ManageEngine ServiceDesk Plus 9.3 - User Enumeration	WebApps	Java	Alexander Bluestein
2019-04-08	📄	📄	✗	Download Accelerator Plus (DAP) 10.0.6.0 - SEH Buffer Overflow	Local	Windows	Peyman Forouzan
2019-04-08	📄	✗		WordPress Plugin Limit Login Attempts Reloaded 2.7.4 - Login Limit Bypass	WebApps	PHP	isdampe
2019-04-08	📄	✗		Tradebox CryptoCurrency - 'symbol' SQL Injection	WebApps	PHP	Abdullah Çelebi
2019-04-08	📄	📄	✗	River Past Cam Do 3.7.6 - 'Activation Code' Local Buffer Overflow	Local	Windows	Chris Au
2019-04-08	📄	✗		CentOS Web Panel 0.9.8.793 (Free) / 0.9.8.753 (Pro) - Cross-Site Scripting	WebApps	Linux	DKM

Exploit Database (2/2)



EXPLOIT DATABASE

Search The Exploit Database ×

Title
Title

CVE
2019-1234

Type
Type

Platform
Platform

Author
Author

Content
Exploit content

Port
Port

Tag
Tag

☐ Verified ☐ Has App ☐ No Metasploit

Search



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 d'Angers 21 janvier 2021

Démonstration



Démonstration



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



Des questions ?

