John the Ripper (JtR) fait partie des outils de piratage que l'équipe de réponse aux incidents de Varonis a utilisé pour sa première démonstration de cyberattaque en direct, et l'un des programmes de craquage de mots de passe les plus populaires. Dans ce billet, nous allons vous présenter John the Ripper, son fonctionnement et son importance.

Remarques à propos du hacking : le hacking est la recherche de connaissances sur les systèmes, les architectures et les humains. Dans le cas présent, nous parlons de logiciels et de systèmes d'exploitation.

Le hacking n'est pas nécessairement une activité criminelle, même si cette technique peut être utilisée à mauvais escient. Nous défendons un hacking éthique. Restons du côté lumineux de la Force.

Comment John the Ripper fonctionne-t-il ?

JtR prend en charge plusieurs technologies de chiffrement couramment utilisées pour les systèmes UNIX ou Windows (l'édition Mac dispose d'une base UNIX). JtR détecte automatiquement le mode de chiffrement des données hachées et les compare au contenu d'un gros fichier texte de mots de passe courants. Il effectue le hachage de chacun de ces mots de passe et s'arrête lorsqu'il trouve une correspondance. Facile.

Dans sa remarquable démonstration de cyberattaque en direct, l'équipe de réponse aux incidents de Varonis montre comment voler un mot de passe haché, utiliser JtR pour trouver le vrai mot de passe et se connecter ensuite au compte administrateur correspondant. Cet outil est très souvent utilisé dans ce but !

JtR s'accompagne de sa propre liste de mots de passe courants, et ce dans plus de 20 langues. Ces listes fournissent à JtR des milliers de mots de passe possibles, à partir desquels il pourra générer les valeurs hachées correspondantes et tenter de façon efficace de deviner le mot de passe cible. Comme la plupart des gens choisissent des mots de passe faciles à mémoriser, JtR est souvent très efficace, même si l'on n'utilise que ses listes prêtes à l'emploi.

JtR est inclus dans les versions de tests d'intrusion de Kali Linux.

À quelles fins John the Ripper est-il utilisé ?

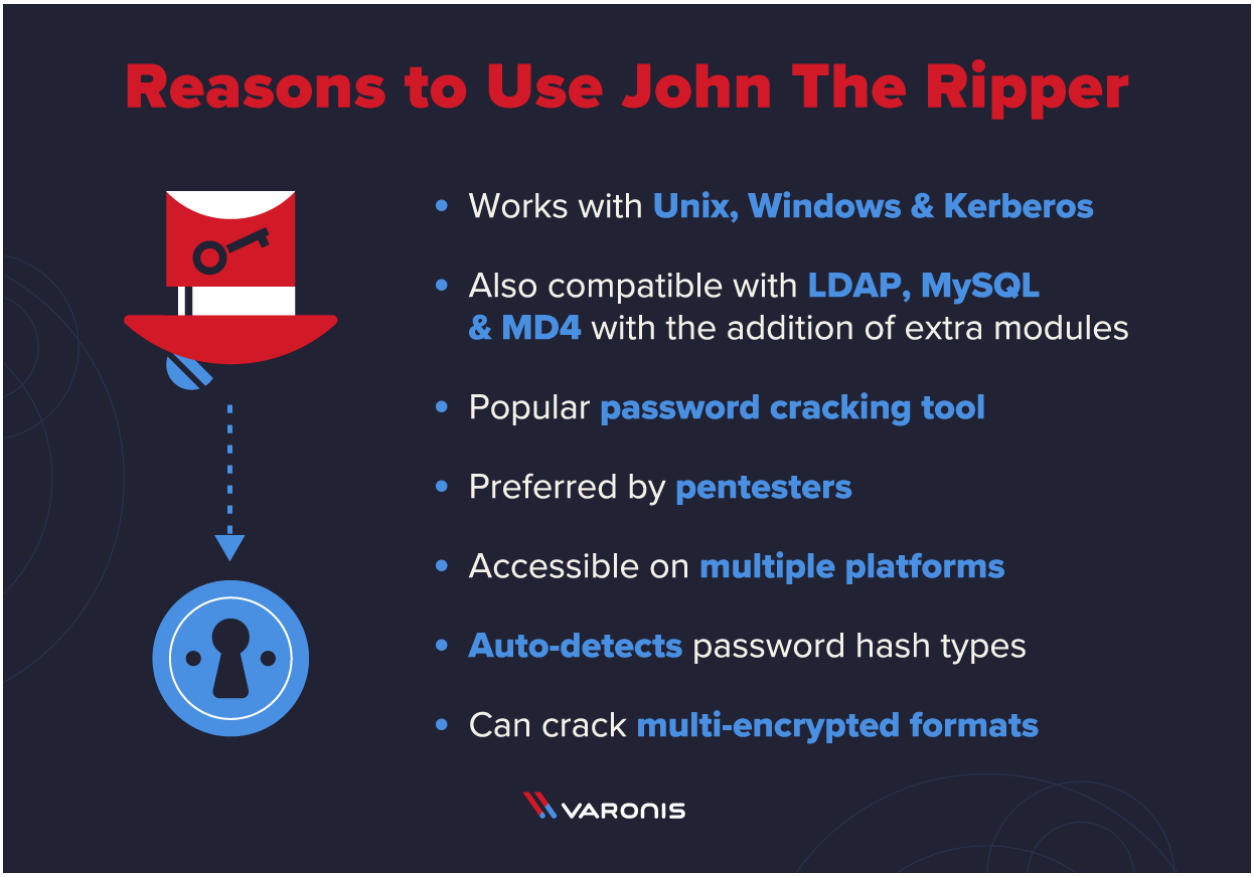
Il est principalement utilisé dans le cadre d'exercices d'intrusion ; il peut aider l'équipe informatique à repérer les mots de passe faibles et les stratégies de mot de passe déficientes.

Voici la liste des technologies de chiffrement que l'on trouve dans JtR :

- UNIX crypt(3)

- Traditional DES-based
- “bigcrypt”
- BSDI extended DES-based
- FreeBSD MD5-based (linux and Cisco IOS)
- OpenBSD Blowfish-based
- Kerberos/AFS
- Windows LM (DES-based)
- DES-based tripcodes
- SHA-crypt hashes (newer versions of Fedora and Ubuntu)
- SHA-crypt and SUNMD5 hashes (Solaris)

Il s’agit de la liste « officielle ». JtR étant open source, faites quelques recherches si votre chiffrement favori ne figure pas dans cette liste. Il se peut que quelqu’un ait déjà écrit une extension pour ce chiffrement.



Comment télécharger John the Ripper :

JtR est un projet open source. Vous pouvez donc télécharger et compiler vous-même le code source, télécharger les binaires exécutables ou trouver l'outil dans un package de test de pénétration.

La page Web officielle de John the Ripper se trouve sur Openwall et inclut son code source et ses binaires. Vous pouvez également rejoindre le dépôt GitHub pour contribuer au projet.

JtR est disponible dans Kali Linux et fait partie de ses métapaquets de craquage de mots de passe.

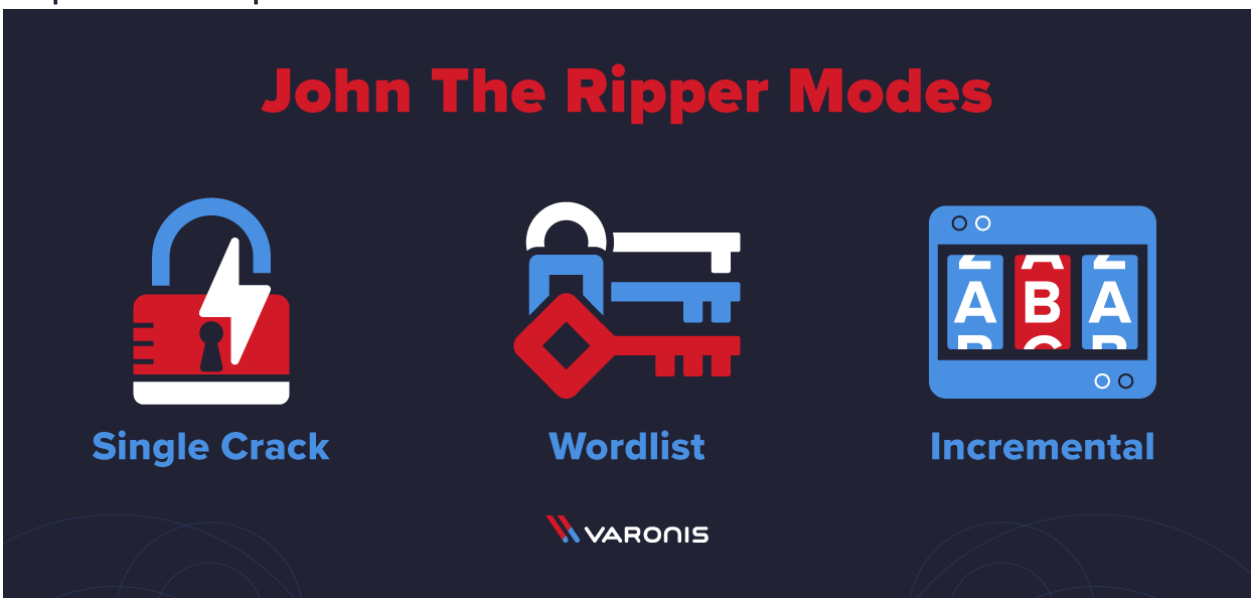
Tutoriels d'utilisation de John the Ripper :

Nous allons passer en revue plusieurs commandes de base nécessaires pour commencer à utiliser John the Ripper. Tout ce qu'il vous faut pour démarrer est un fichier contenant une valeur hachée à déchiffrer.

Si vous avez besoin de la liste des commandes de JtR, exécutez cette commande :

- .\john.exe

Craquer les mots de passe



Pour craquer les mots de passe, les principaux modes d'action de John the Ripper sont le mode simple, l'attaque par dictionnaire et le mode incrémental. Le mode de craquage simple est le mode le plus rapide et le mieux apté si vous avez un fichier de mots de passe à craquer. Le mode dictionnaire compare le hachage à une liste connue de mots de passe possibles. Le mode incrémental est le plus puissant et peut ne jamais aboutir. Il s'agit d'un mode par force brute classique qui teste chaque combinaison possible de caractères jusqu'à aboutir à un résultat.

Le moyen le plus simple de tenter de craquer un mot de passe est de laisser JtR suivre une série de modes de craquage courants. La commande ci-dessous indique à JtR de tenter le mode « simple », puis les dictionnaires par défaut contenant des mots de passe possibles, puis le mode « incrémental ».

- .\john.exe passwordfile

Vous pouvez également télécharger d'autres dictionnaires sur Internet ou créer les vôtres, que vous utiliserez avec JtR grâce au paramètre -wordlist.

- .\john.exe passwordfile –wordlist="wordlist.txt"

Si vous voulez spécifier un mode de craquage, utilisez le paramètre précis correspondant à ce mode.

- .\john.exe --single passwordfile .\john.exe --incremental passwordfile

Règles de manipulation des mots (mangling)
La mangling est un préprocesseur utilisé par JtR pour optimiser le dictionnaire et rendre le craquage plus rapide. Utilisez le paramètre -rules pour définir les règles de mangling.

- .\john.exe --wordlist="wordlist.txt" --rules --passwordfile

Affichage des résultats
Pour voir la liste des mots de passe que vous avez craqués, utilisez le paramètre -show.

- .\john.exe –show passwordfile

Si la liste des mots de passe que vous avez craqués est longue, vous pouvez la filtrer en utilisant des paramètres supplémentaires. Vous pouvez également rediriger les résultats en utilisant la fonction de redirection de base de votre shell. Si, par exemple, vous voulez voir si vous avez craqué des utilisateurs root (UID=0), utilisez le paramètre -users.

- .\john.exe --show --users=0 passwordfile

Ou si vous voulez afficher les utilisateurs de groupes privilégiés, utilisez -groups.

- .\john.exe –-show –-groups=0,1 passwordfile