Bonjour,

La sécurité dans le monde de l'informatique est un point essentiel et critique.

On parle souvent de sécurité informatique au niveau de l'entreprise.

Au vu de la situation actuelle, on pense beaucoup à sécuriser les entreprises mais beaucoup moins à sécuriser **son propose réseau domestique** ce qui est, à mon avis, tout **aussi important** surtout actuellement**.**

Puisque nous sommes de plus en plus nombreux à faire du télétravail.

Ce qui donne des portes d'accès supplémentaires surtout lorsque nous sommes connecté en VPN à notre entreprise et/ou à nos clients.

Tout comme dans l'entreprise, notre réseau privé **peut être la cible d'attaques** voir d'intrusions de la part de personnes malveillantes.

Il est donc important de sécuriser notre propre réseau afin d'éviter toute fuite de données personnelles ou de nos clients.

Votre réseau privé est le plus souvent constitué de votre box qui est directement reliée à internet et qui joue le rôle d'interface avec l'extérieur.

Donc face à la multiplication des terminaux que nous avons dans nos maisons, il n'est pas toujours facile de trouver le maillon faible dans notre réseau.

Voici deux logiciels qui vous permettent d'y voir plus clair (mais j'ai nettement une préférence pour Bitdefender car plus simple à utiliser mais aussi évite d'avoir vos données qui remontent vers l'éditeur)

Donc, si vous avez beaucoup de terminaux et d'objets connectés à la maison, il serait intéressant de savoir si l'un de vos équipements ne représente pas un risque pour votre sécurité informatique.

Pour le savoir, il vous faut faire un audit de vulnérabilités de votre réseau.

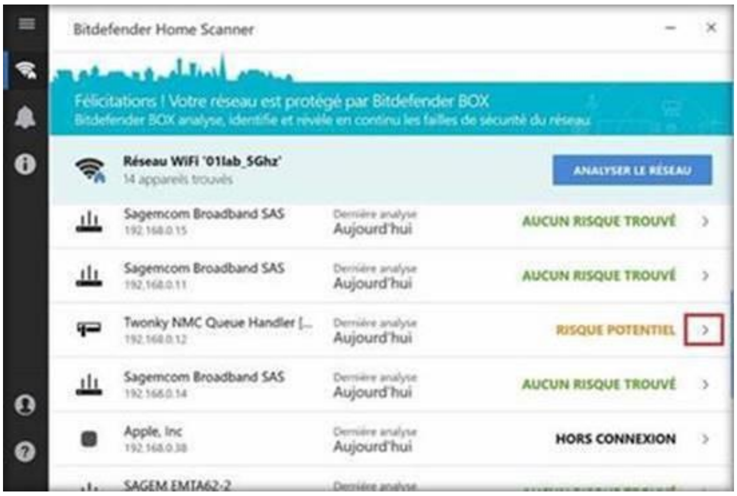
Pour cela je vous conseille d'effectuer cet audit avec l'un des deux logiciels suivants :

- Bitdefender Home Scanner (qui est simple et rapide)
- Nessus Home (qui est un peu plus complexe, mais aussi plus complet mais qui me pose problème du fait que les données remontent chez l'éditeur).

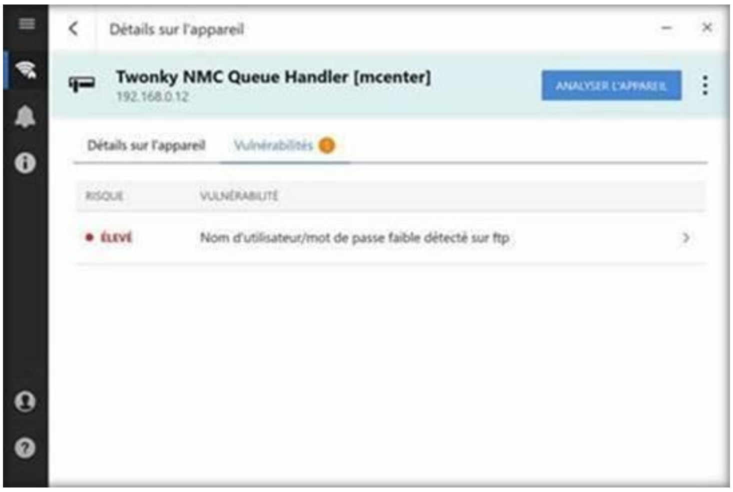
Le faire depuis votre ordinateur personnel et pas depuis le poste de la société bien évidemment, cela vous permettra aussi de conserver ce logiciel chez vous et de vous faire un audit régulièrement après des mises à jour ou des ajouts d'équipement dans votre infrastructure.

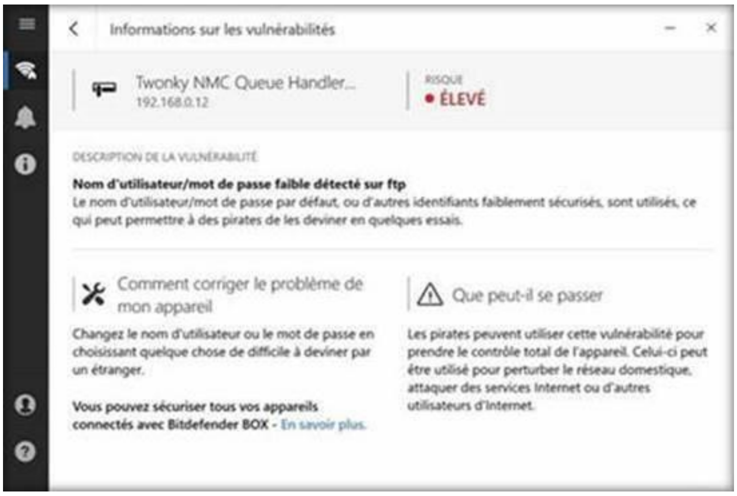
Méthode 1 : Bitdefender Home Scanner

Pour commencer téléchargez l'exécutable d'installation de Bitdefender Home Scanner [sur le site de l'éditeur]().
Une fois l'installation terminée, lancez le logiciel.
Celui-ci vous demandera alors si le réseau sur lequel votre ordinateur est connecté est bien votre réseau domestique.
Confirmez et lancez l'analyse de vulnérabilités, qui prendra quelques minutes.
Une fois l'analyse terminée, le logiciel vous listera tous les équipements connectés à votre réseau, classés par adresse IP.
Il indiquera pour chacun d'eux s'il a trouvé un risque potentiel ou non.



Dans le cas d'un risque potentiel, vous pouvez ensuite cliquer sur la flèche à droite et obtenir des informations plus détaillés sur l'équipement en question et la faille potentielle détectée.
Le cas échéant, Bitdefender Home Scanner vous donnera des conseils pour combler cette brèche.
Généralement, il s'agira de changer un mot de passe ou de mettre à jour le système de l'équipement.

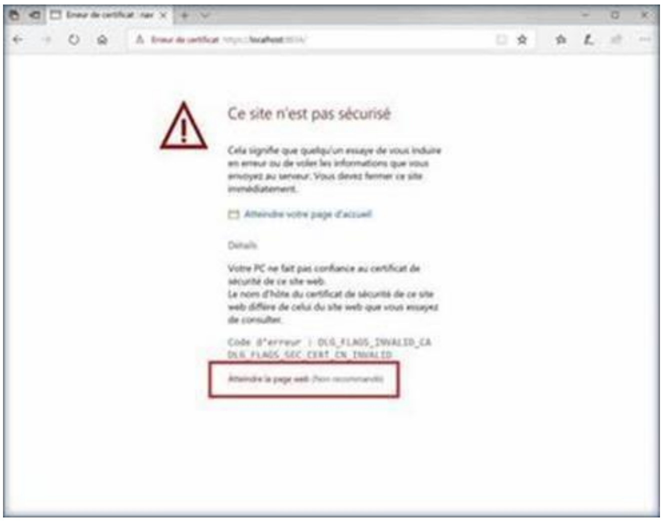




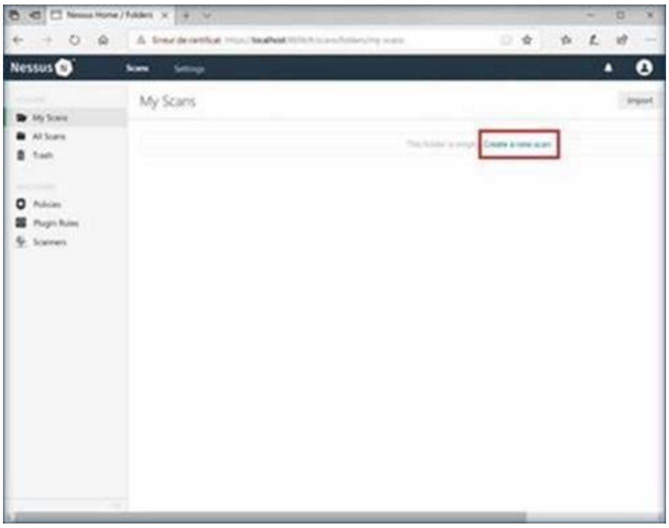
<u>Méthode 2 : Nessus Home</u>

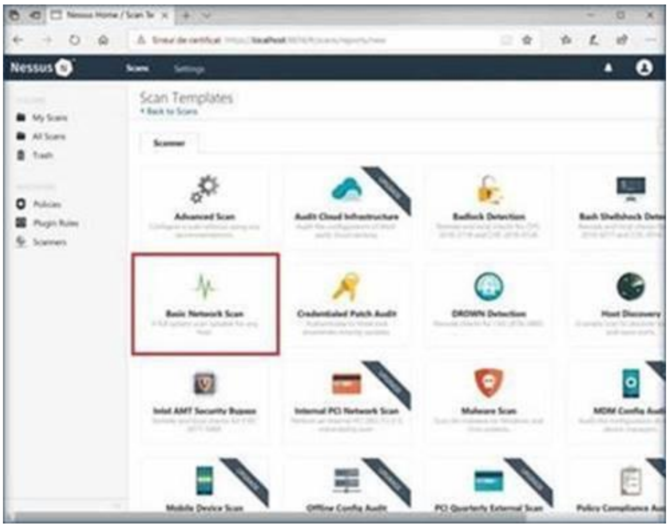
Nessus est un scanner de vulnérabilités professionnel que l'on peut activer avec une licence gratuite « Home », limitée à 16 équipements connectés.
Pour le télécharger, il faut d'abord obtenir une clé de licence [sur le site web de Nessus](), en donnant un nom et une adresse email.
Le téléchargement du logiciel se fait [sur une autre page]().
Choisissez la version correspondant à votre système d'exploitation, téléchargez-la et lancez l'installation.
En fonction de la configuration de la machine, Nessus installera un ou plusieurs logiciels supplémentaires qui l'aideront à faire ses analyses.
Ainsi, sur Windows, il installera le logiciel de capture de paquets WinPCap.
Un fois l'installation terminée, vous êtes invités à vous connecter à l'interface d'administration de Nessus, qui s'exécute sur un serveur web local.
Pour cela, il faut accepter une exception de sécurité liée au certificat SSL auto signé de Nessus.

C'est là ou moi cela me pose problème mais bon vu que l'on donne déjà accès à plein d'informations à google, à Amazone, à Microsoft, etc … peut être que cela ne vous dérangera pas d'en donner à Nessus 😉.

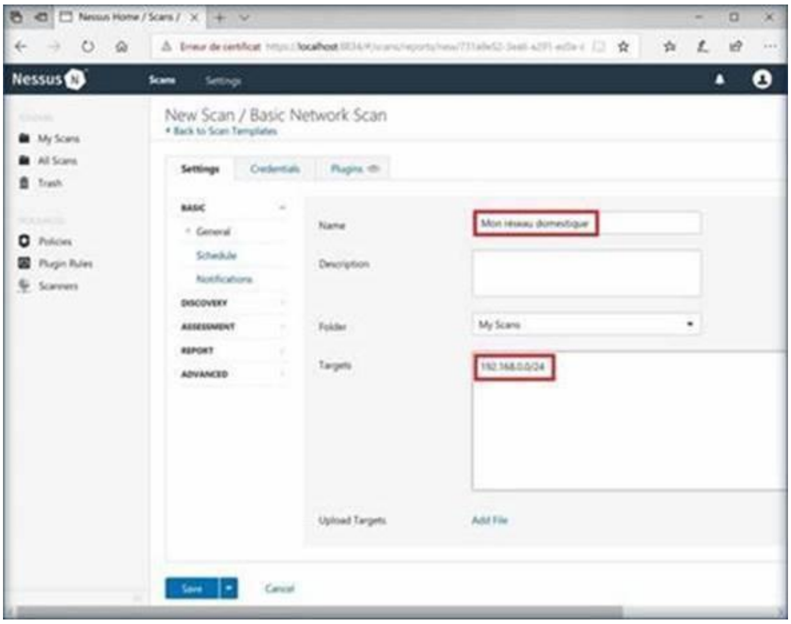


Ensuite, il ne reste plus qu'à créer un compte local pour accéder enfin à l'interface d'administration. Cliquez alors sur « *Create a new scan* », puis sur « *Basic Network Scan* ».

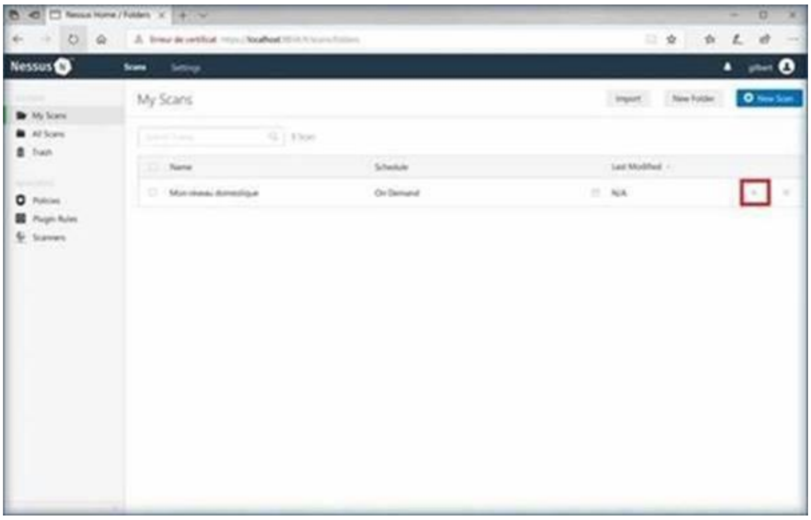




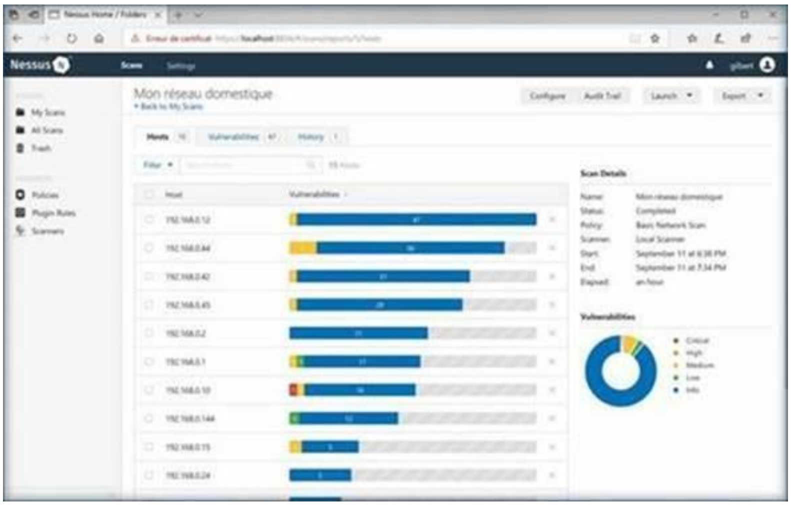
Vous arrivez ensuite sur un formulaire dans lequel il suffit de remplir le champ « Name » et « Targets ».
Pour le premier, vous pouvez mettre ce que vous voulez.
Pour le second, il faut indiquer le champ d'adresses IP de votre réseau local, par exemple 192.168.0.0/24.
Pour trouver ce champ d'adresses, ce n'est pas très compliqué.
Cliquez sur le menu Windows, tapez « **cmd** » dans le champ recherche, exécutez le logiciel cmd.exe et tapez la commande « ipconfig ».
Vous connaitrez alors l'adresse IPv4 locale de la machine, et découvrirez également les trois premiers nombres d'IP.
Sur Nessus, afin de scanner sur l'ensemble du champ d'adresses, il suffit de remplacer le dernier chiffre par 0 et d'ajouter « /24 ».

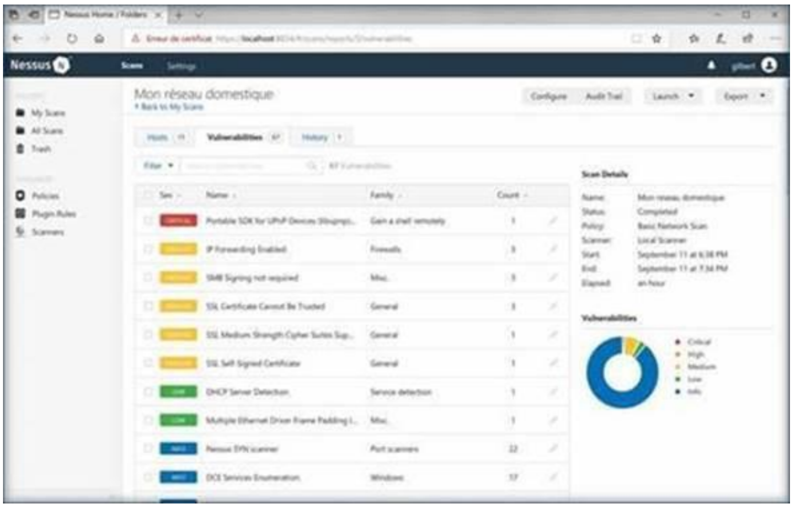


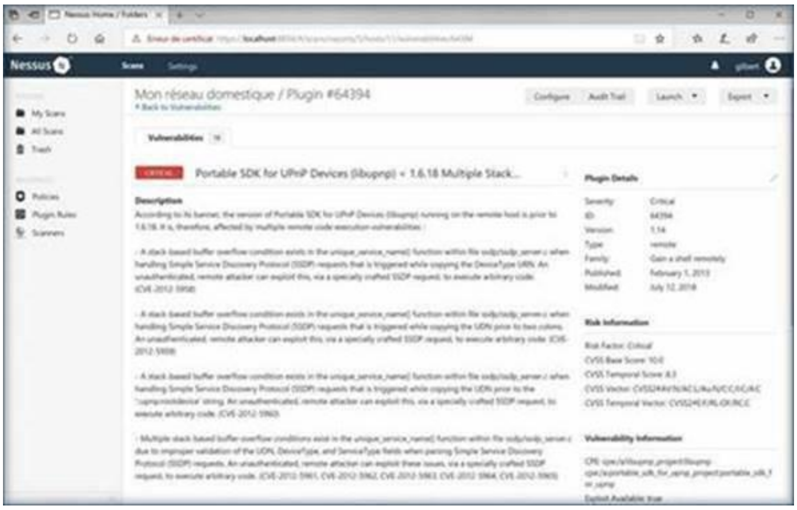
Sauvegardez votre configuration de scan, puis cliquez sur la petite flèche pour lancer l'analyse.
Celle-ci sera sensiblement plus longue que pour Bitdefender Home Scanner.
Allez-vous prendre un petit café ou jouer avec vos enfants ou faire les devoirs ☺ et revenez plus tard.



Une fois l’analyse terminée, le logiciel listera toutes les failles potentielles, classées par adresses IP ou par niveau de criticité.
Là encore, il sera possible d’avoir des informations détaillées sur les équipements, les failles trouvées et les solutions à mettre en œuvre.
Vous remarquerez que celles-ci sont beaucoup plus précises, mais aussi beaucoup plus techniques.
Cliquez sur « *Vulnerabilities* » pour découvrir les failles les plus graves en premier.
Vous pourrez ensuite cliquer sur chaque élément qui pose problème : Nessus vous donnera alors un descriptif complet de la faille et vous proposera le cas échéant une solution pour y remédier.







Pour finir :
Les deux méthodes ne donnent pas forcément les mêmes résultats.
C'est normal, cela permet de faire des compléments ou une double vérification.
Par ailleurs, leurs listes de failles peuvent comporter des faux positifs, c'est-à-dire des failles qui n'existent pas en réalité.
C'est pourquoi il faut toujours vérifier sur l'équipement en question si la faille existe vraiment.