le cnam

SEC 102 - TP09
Veille

Date	Version	Description	Auteurs
11/06/2023	1	Retranscription collective des informations présentées en cours	Bartel Cantin Bialas Alexis Dufourt Marvin Faussurier Marc N'Guessan Jérémy

Sommaire

1. Introduction

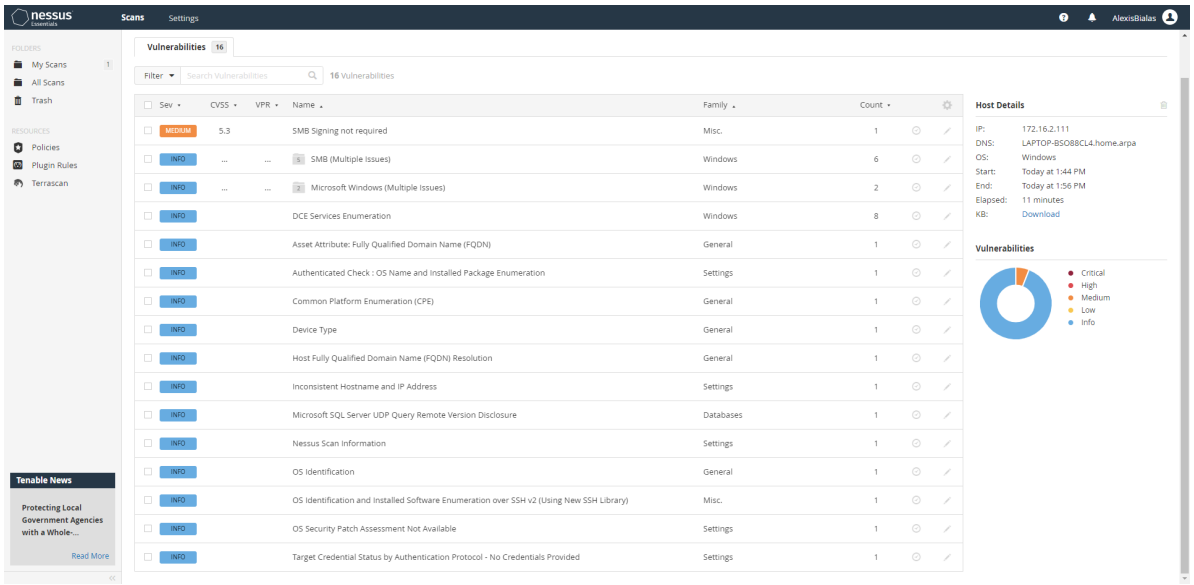
Nessus est un logiciel de sécurité informatique très populaire utilisé pour identifier les vulnérabilités dans les réseaux et les systèmes.

Il aide les entreprises et les particuliers à protéger leurs données en détectant les faiblesses de sécurité avant que les pirates ne les exploitent.

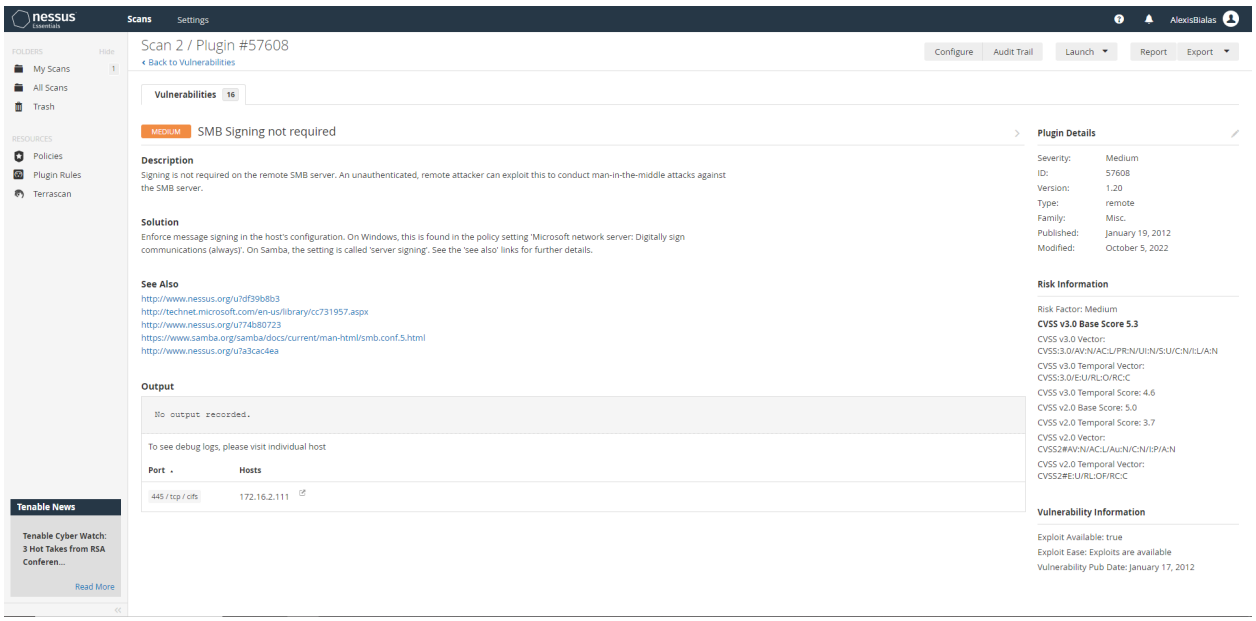
Nessus fonctionne en scannant les systèmes cibles et en comparant leurs configurations avec une base de données de vulnérabilités connues.

Il fournit ensuite des rapports faciles à comprendre avec des recommandations pour corriger les problèmes détectés.

2. Inventaire de l'écosystème



3. Identification et caractérisation des menaces



4. Pensez-vous que votre inventaire est exact ?

Etant donné que le scan à été fait sur du local, oui celui-ci est correct.

5. Pensez-vous que le fait de disposer d’un parc avec des matériels identiques est un avantage ou un inconvénient ?

Le fait de disposer d'un parc avec des matériels identiques peut être à la fois un avantage et un inconvénient, cela dépend des contextes et des besoins de l'entreprise.

D'un côté, l'avantage principal est la facilité de gestion et de maintenance des matériels. Si tous les matériels sont identiques, l'entreprise peut mieux gérer ses stocks de pièces de rechange, les coûts de maintenance, et former plus facilement les employés à l'utilisation de ceux-ci. De plus, cela permet également de standardiser les procédures, réduire les risques d'erreurs et améliorer l'efficacité globale de l'entreprise.

D'un autre côté, l'inconvénient principal est la perte de flexibilité et de diversité dans l'utilisation des matériels. Si l'entreprise a besoin de fonctionnalités spécifiques à un moment donné, elle risque de se retrouver bloquée. De plus, cela peut limiter la capacité de l'entreprise à s'adapter à des changements dans le marché ou dans les besoins des clients.

6. Conclusion

En conclusion, Nessus est un outil de sécurité informatique essentiel qui offre un service de détection et de correction de vulnérabilités efficace. Malgré quelques défis, son utilisation apporte un niveau de sécurité accru, une meilleure compréhension des risques de cybersécurité et une capacité à anticiper et à répondre aux menaces potentielles. C'est une solution solide et robuste pour toute organisation cherchant à renforcer sa posture de cybersécurité.

7. Glossaire

Veille technologique : Processus systématique de recherche, de traitement et de diffusion d'informations technologiques utiles pour aider à la prise de décision stratégique.

Retranscription collective : Il s'agit d'un processus collaboratif de consignation ou de conversion des informations ou des données d'un format (comme l'audio) à un autre (comme le texte écrit).

Inventaire de l'écosystème : Il s'agit d'une liste détaillée de tous les éléments composant un système ou un réseau, dans le contexte du document, probablement un réseau informatique ou un système.

Menaces : Dans un contexte de cybersécurité, les menaces font référence à tous les facteurs potentiels qui pourraient compromettre la sécurité des systèmes ou des données informatiques.

Parc (de matériels) : Il s'agit de l'ensemble des équipements (hardware) dont dispose une entreprise ou une organisation.

Nessus : C'est un logiciel de sécurité informatique utilisé pour identifier les vulnérabilités dans les réseaux et les systèmes informatiques.

Vulnérabilités : Ce sont des faiblesses dans un système informatique ou un réseau qui peuvent être exploitées pour compromettre la sécurité des données ou du système.

Scan : Dans le contexte de la sécurité informatique, il s'agit d'une analyse systématique d'un système ou d'un réseau pour détecter d'éventuelles vulnérabilités ou problèmes de sécurité.

Local : Il s'agit d'un réseau ou d'un système qui est confiné à un lieu géographique spécifique, comme un bâtiment ou une entreprise.

Posture de cybersécurité : Il s'agit de l'approche et des politiques d'une organisation en matière de prévention, de détection et de réponse aux cybermenaces.