Perform Vulnerability Research with Vulnerability Scoring Systems and Databases

Environnement de travail :

- Machine virtuelle Windows 10.
- Navigateurs internet avec connexion internet
- Privilèges administrateurs pour lancer les outils

Durée du travail

20 minutes

Aperçu sur les vulnérabilités dans les systèmes de notation des vulnérabilités et les bases de données.

Les bases de données de vulnérabilité collectent et maintiennent des informations sur les différentes vulnérabilités présentes dans les systèmes d'information.
Voici quelques-uns des systèmes de notation de vulnérabilité et des bases de données :

- Common weakness Enumeration (CWE).
- Common Vulnerabilities and Exposures.
- National Vulnerability Database (NVD).
- Common Vulnerability Scoring System (CVSS).

Tache 01: Perform Vulnerability Research in Common Weakness Enumeration (CWE).

Ici, nous utiliserons CWE pour afficher les dernières vulnérabilités du système sous-jacent.

1. Allumez la machine virtuelle **Windows 10** et utilisez **Admin** et **P@$$w0rd**.
2. Ouvrez n'importe quel navigateur web (ici, **Mozilla Firefox**) et naviguez vers **https://cwe.mitre.org/**.

Remarque :

- Si une fenêtre pop-up **Default Browser** apparait, décochez **Always perform this check when starting FireFox**, et cliquez sur le bouton **Not now**.
- Si une fenêtre pop-up **New in Firefox** : **Content Blocking** apparait, suivez les étapes puis cliquez sur **Got it** pour finir.

3. Le site web **CWE** apparait, dans **Google Custom Search** sous la section **Search CWE**, tapez **SMB** et cliquez sur l'icône de recherche.

Remarque : ici, nous recherchons les vulnérabilités des services en cours d'exécution qui ont été trouvées dans les systèmes cibles dans les laboratoires du module précédent (**Module 4 Enumération**).

4. Les résultats de la recherche apparaissent, affichant les vulnerabilités sous-jacentes dans le service cible (ici, SMB). Vous pouvez cliquer sur n'importe quel lien pour voir plus de détails sur les informations des vulnérabilités.
5. Maintenant, cliquez sur n'importe quel lien (ici, **CWE-427**) pour voir les informations détaillées de cette vulnérabilité.
6. Une nouvelle page web apparait dans un nouvel onglet, affichant les informations détaillées concernant la vulnérabilité, vous pouvez défiler vers le bas pour plus d'informations.
7. Vous pouvez faire la même chose avec d'autres vulnérabilités.
8. Maintenant, revenez vers le site **CWE**, défilez vers le bas, et cliquez sur le lien **CWE List** présent sous les résultats de la recherche.

9. Une nouvelle page web apparait, affichant **CWE List Version**. Défilez vers le bas, et sous la section **External Mappings**, cliquez **CWE Top 24 (2019)**.
10. Une page web, apparait **CWE VIEW: Weaknesses in the 2019 CWE Top 25 Most Dangerous Software Errors**. Défilez vers le bas et voyez la liste **Weaknesses in the 2019 CWE Top 25 Most Dangerous Software Errors**, sous la section Reltionships. Vous pouvez cliquer sur les faiblesses une à une pour plus de détails.

Remarque : ces informations peuvent être utilisées pour exploiter les vulnérabilités du logiciel et lancer d'autres attaques.

11. Vous pouvez retourner au site web **CWE** et explorer d'autres options.
12. Fin de la démonstration.

Tache 02: Perform Vulnerability Research in Common Vulnerabilities and Exposures (CVE)

1. Dans la machine **Windows 10**, ouvrez **Mozilla Firefox** et naviguez vers **https://cve.mitre.org/**.
2. Le site web **CVE** apparait. Les vulnérabilités récentes s'affichent sous la section **Newest CVE Entries**, qui se trouve dans le volet droit de la fenêtre.
3. Vous pouvez copier le nom de n'importe quelle vulnérabilité sous la section **Newest CVE Entries**, et effectuer une recherche sur **CVE** pour plus de détails (ici, nous choisirons la vulnérabilité **CVE-2019-16404**).
4. Maintenant, cliquez sur l'onglet **Search CVE List**. Sous la section **Search CVE List**, tapez le nom de la vulnérabilité (ici, **CVE-2019-16404**) dans la barre de recherche, puis cliquez sur **Submit**.
5. La page **Search Results** apparait, affichant les informations à propos des vulnérabilités recherchées. Vous pouvez cliquer sur a vulnérabilité pour plus de détails.
6. Dans la section **Search CVE List**, vous pouvez chercher des vulnérabilités en fonction des services ici, par exemple cherchez une vulnérabilité en relation avec le service **SMB**, tapez donc **SMB** puis cliquez sur **Submit**.

Remarque : vous pouvez rechercher les vulnérabilités des services en cours d'exécution qui ont été trouvées dans les systèmes cibles dans les laboratoires du module précédent (Module 04 Enumération).

7. La page **Search Results** apparait, affichant une liste de vulnérabilités se trouvant dans le service cible (**SMB**) avec leur description.
8. Vous pouvez aussi cliquez sur **CVE-ID** de n'importe quelle vulnérbilité pour voir ses informations détaillées, ici nous allons cliquez sur le premier lien **CVE-ID**.
9. Les informations détaillées s'affichent avec **Description**, **References**, et **Data Entry Created**. Vous pouvez cliquer sur les liens se trouvant sous la section **References** pour plus de détails.
10. Dans la section **Search CVE List**, vous pouvez rechercher d'autre services cibles.
11. Fin de la démonstration.

Tache 03: Perform Vulnerability Research in National Vulnerability Database (NVD)

1. Dans la machine virtuelle **Windows 10**, ouvrez n'importe quel navigateur web (ici, **Mozilla Firefox**) et naviguez vers **https://nvd.nist.gov/**.
2. Le site web **NATIONAL VULNERABILITY DATABASE** apparait : vous pouvez voir là les vulnérabilités récemment trouvées.
3. Vous pouvez cliquer sur le lien **CVE-ID** (ici, **CVE-2019-2981**) pour voir plus de d'informations détaillées concernant la vulnérabilité.

4. Une nouvelle page web apparait, affichant **CVE-2019-2981 Detail**. Vous pouvez voir des informations détaillées comme **Current Description**, **Severity, References**, et **Weakness Enumeration**.
5. Sous la section **Severity**, cliquez sur le lien **Base Score** pour voir les détails **CVSS** concernant la vulnérabilité.
6. Une nouvelle page web apparait,affichant les informations comme **Base Scores**, **Temporal Score**, et **Environmental Score Overall Score** liées à une vulnérabilité sous forme graphique, sous **Common Vulnerability Scoring System Calculator CVE-2019-2981**.

Remaque :

- **Base Score** : la métrique la plus utilisée par les entreprises et traite des qualités inhérentes à une vulnérabilité. Le tableau ci-dessous décrit la gravité d'une vulnérabilité en fonction de la plage du score de base :

CVSS v3.0 Ratings

Severity	**Base Score Range**
None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 – 8.9
Critical	9.0 – 10.0

CVSS v2.0 Ratings

Severity	Base Score Range
Low	0.0 – 3.9
Medium	4.0 – 6.9
High	7.0 – 10

- **Temporal Score** : représente les qualités de la vulnérabilité qui changent au fil du temps, et le score environnemental représente les qualités de la vulnérabilité qui sont spécifiques à l'environnement de l'utilisateur affecté.
- **Overall Score** : c'est la somme totale des deux scores (**CVSS Base Score, CVSS Temporal Score**).

7. Défilez vers le bas pour voir plus d'informations détaillées à propos des différentes métriques de score comme **Base Score Metrics**, **Temporal Score Metrics** et **Environmental Score Metrics**.
8. Maintenant, naviguez vers la page principale du site web **NATIONAL VULNERABILITY DATABASE**. Agrandissez **Vulnerabilities** et cliquez sur l'option **Search & Statistics**.
9. La page **Search Vulnerability Database** apparait. Dans le champ **Keyword Search**, tapez un service cible (ici, **SMB**) pour trouver des vulnérabilités associées à ce service puis cliquez sur **Search**.
10. La page **Search Results** apparait, affichant les informations détaillées sur les vulnérabilités sous-jacentes dans un service cible.
11. Pour plus d'informations cliquez sur **VULN ID** de chaque vulnérabilité.

12. Dans la section **Search Vulnerability Database**, vous pouvez rechercher les vulnérabilités d'autres services cibles.
13. Fin de la démonstration.