Lab – Investigate Vulnerability Information Sources

Objectives

Use multiple helpful sources to further investigate vulnerabilities.

- Part 1: Investigate Common Vulnerabilities and Exposures (CVEs)
- Part 2: Explore Common Weakness Enumerations (CWEs)
- Part 3: Investigate National Institute of Standards and Technology (NIST) Vulnerability Resources
- Part 4: Research Vulnerabilities in the Common Vulnerability Scoring System (CVSS)

Background / Scenario

In a previous lab, you found several vulnerabilities after scanning a target system. You will now use several widely available sources to dig deeper into the details of the vulnerabilities. You will map and investigate the vulnerabilities to the Common Vulnerabilities and Exposures (CVE) list, the Common Weakness Enumeration (CWE), the NIST National Vulnerability Database, and the Common Vulnerability Scoring System (CVSS).

Required Resources

- Computer with internet connection

Instructions

Part 1: Investigate Common Vulnerabilities and Exposures (CVEs)

Step 1: Explore CVE.

a. Launch the CVE website and navigate to www.cve.org.
b. Read the overview of the CVE program.
    1. Select **About > Overview** in the menu.
    2. View the CVE Program Overview video.
    3. Review the available Podcasts for more detailed information about the CVE program.

What is the mission of the CVE program?

Answer Area

<!----><!---->

Who assigns CVE IDs?

Answer Area

<!----><!---->

What are the two main goals of the CVE Program?

Answer Area

<!----><!---->

Who operates the CVE?

Answer Area

<!----><!---->

Step 2: Use the CVE program to gather information about vulnerabilities.

In an earlier lab, you scanned a target system for vulnerabilities. The list of vulnerabilities found returned the following six CVEs:

- CVE-2021-41617
- CVE-2020-14145
- CVE-2019-16905
- CVE-2019-6111
- CVE-2019-6110
- CVE-2019-6109

a. Enter **CVE-2021-41617** info the search window and click **Find**.
What versions of OpenSSH are subject to this vulnerability?

Answer Area

<!----><!---->

When was this CVE last updated?

Answer Area

<!----><!---->

b. At the bottom of the page click **CVE-2021-41617** to view additional information about the CVE from the NIST National Vulnerability Database (NVD).
What is the CVSS 3.x Severity score for this CVE?

Answer Area

<!----><!---->

c. Repeat steps a and b. to review information for the other five CVEs.
Which of these CVEs involves Man-in-the-Middle attacks from a malicious SCP server?

Answer Area
<!----><!---->

d. On the CVE site (www.cve.org), enter **CVE-2019-6111** into the search box and click **Find**.
e. Scroll down to the bottom of the CVE page and click **CVE-2019-6111** to view additional information on the NVD.
f. On the NVD page for **CVE-2019-6111**, scroll down to the **Weakness Enumeration** section.
What CWE-ID is associated with this CVE?

Answer Area
<!----><!---->

Record this CWE ID for use in Part 2.

g. Repeat steps a through d. to obtain the CWE-IDs associated with the other returned CVEs.
What CWEs are associated with each of the other five CVEs?

Answer Area
<!----><!---->

Record these CWE IDs for use in Part 2.

Part 2: Explore Common Weakness Enumeration (CWE)

Step 1: Explore CWE.

a. Launch the CWE website and navigate to https://cwe.mitre.org.
b. Explore the CVE program.by selecting **About** > **Overview** in the menu.
What is the goal of CWE?

Answer Area
<!----><!---->

What is the difference between a CVE and a CWE?

Answer Area
<!----><!---->

c. IDs you recorded from Part 1 step 2.
1. Enter **22** in the **ID Lookup** box on the top right of the CWE page. (This is the CWE ID for CVE-2019-6111)

What is title of this CWE?

Answer Area

<!----><!---->

2. Scroll through the available information about this CWE.

d. Repeat step c. Look up the remaining CWE IDs that you recorded in Part 1 Step 2g.

Part 3: Investigate National Institute of Standards and Technology (NIST) Vulnerability Resources

Step 1: Explore NIST.

a. Launch the NIST website by navigating to https://www.nist.gov.
b. Select **About NIST** > **About Us** in the menu and review the overview of NIST.
What is the mission of NIST?

Answer Area

<!----><!---->

c. Explore the National Vulnerability Database (NVD).
1. Return to the NIST home page and select **Topics** > **Information Technology** in the menu.
2. Select **National Vulnerability Database** in the **Featured Content** list.
3. Click **General** to view and review General Information about the NVD.

What is the relationship between the NVD and CVEs?

Answer Area

<!----><!---->

4. Expand the menu under **General** and click **NVD Dashboard**.

How many CVE Vulnerabilities are contained in the NVD?

Answer Area

<!----><!---->

What is the most recent scored Vulnerability and what is the CVSS rating?

Answer Area

<!----><!---->

5. Navigate back to the National Vulnerability Database page https://nvd.nist.gov/.
6. Click **Vulnerability Metrics** in the menu on the left of the page.

What method is used to qualitatively measure the severity of vulnerabilities?

Answer Area

<!----><!---->

How many severity ratings does CVSS v3.0 have and what are they?

Answer Area

<!----><!---->

Part 4: Research Vulnerabilities in the Common Vulnerability Scoring System (CVSS)

Step 1: Explore CVSS.

a. Launch the CVSS website and navigate to https://first.org/cvss
b. Review the information on the CVSS.
c. Investigate CVSS ratings by clicking **Specification Document** in the left menu.
What are the three metrics that compose a CVSS rating?

Answer Area

<!----><!---->

How many metrics compose the Base Metric group of a CVSS? What are they?

Answer Area

<!----><!---->

1. Click **Examples** in the left menu.
2. Click the link for **CVSS version 3.1** examples.
3. Scroll down the page and review the example CVEs and how their CVSS v3.1 Base Scores were calculated.
4. Observe the Values given for each metric that makes up the CVSS score.

d. Research the CVSS ratings of the CWEs recorded in Part 1, Step 2.
1. Navigate to www.cve.org.
2. In the search box enter **CVE-2021-41617** and click **Find**.
3. Scroll to bottom of the page and click **CVE-2021-41617** to view additional information on the NVD. This opens the National Vulnerability Database to view details about the CVE.
4. Scroll to the **Severity** section and ensure that **CVSS Version 3.x** is selected.

   Observe the values for the eight CVSS Base metrics in the **Vector**. The corresponding numerical score of these values combine to give a base score of 7.0 HIGH.

5. In a separate browser window, navigate to the CVSS 3.1 Calculator at https://www.first.org/cvss/calculator/3.1.

6. In the Base Score calculator, click the metric names that correspond to the Vector on the NVD page. (**Vector:** CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H)

What Base Score is calculated by the CVSS Calculator?

Answer Area

<!----><!---->

7. Repeat steps 1 – 6 for the other five recorded CVEs from Part 1, Step 2.

Reflection

What is the relationship between CVE, CWE, NVD, and CVSS?

Answer Area

<!----><!---->