Nama: WIRASWANTI RISMANDA PUTRI

No: 20

Kelas: SIB-4C

Lab - Evaluate Vulnerabilities

Objectives

In this lab, we will review the features of an example of a penetrating testing vulnerability report.

Part 1: Learn About the Creators of a Vulnerability Assessment Report

Part 2: Review Sections of the Report

Background / Scenario

Vulnerability assessments can be conducted in-house or by external contractors. Vulnerability assessments are usually automated. Reachable network hosts are identified, and then scanned with vulnerability assessment tools. The scan creates a lot of data which maps the host IP addresses to the detected vulnerabilities. From this data, summary data and visualizations can be created to simplify interpretation of the report.

When identified, the vulnerabilities are often rated by severity, frequently using a standard means of doing so, such as CVSS. In addition, reference information is often provided to enable deeper research if required. Typically a CVE number will be provided that is easy to investigate further.

The report may suggest common mitigation techniques that provide guidance to cybersecurity personnel about how to eliminate the vulnerabilities that have been identified.

Required Resources

- Computer with internet access
- Sample vulnerability assessment report

Instructions

Part 1: Learn About the Creators of a Vulnerability Assessment Report

Step 1: Research the report source.

The report that we will use for this lab was created by the NCATS Cyber Hygiene service.

Research NCATS on the internet and answer the following questions.
What does NCATS stand for?

Answer: **National Cybersecurity Assessments and Technical Services**

What is the Cyber Hygiene Vulnerability Scanning Service? Search the web for details.

Answer: **Layanan ini merupakan penilaian kerentanan gratis yang disediakan oleh Badan Keamanan Siber dan Infrastruktur (CISA) di bawah Departemen Keamanan Dalam Negeri AS.**

What other cybersecurity services are available from NCATS?

Answer: **Selain pemindaian kerentanan Cyber Hygiene, NCATS juga menyediakan Penilaian Kampanye Phishing, Penilaian Risiko dan Kerentanan, serta Tinjauan Desain Arsitektur yang Divalidasi.**

Who are these services available to?

Answer: **Pemerintah federal, negara bagian, lokal, suku, dan teritorial, serta organisasi infrastruktur penting dari sektor publik dan swasta di Amerika Serikat.**

Step 2: Locate and open the report.

a. The link to the report that we will review is directly under the Cyber Hygiene: Vulnerability Scanning section of the NCATS page. To access the link from the Google search engine, enter the following: **site:us-cert.cisa.gov/ CyHy** .

b. Open the report and review the table of contents to get an idea of what is included.

Part 2: Review Sections of the Report

The first two sections of the report explain its intended use and provide a high-level dashboard-like overview of the report results.

Step 1: Review the How to Use the Report section.

It is important to understand the intended use of any security assessment report. A good report will provide useful and focused guidelines for use of the assessment.

Note: Because this report is an example, the organization that the report was prepared for is referred to as Sample Organization (Sample).

Review section one of the report and answer the following questions.
What is the goal of the report?

Answer: **Untuk membantu organisasi memperkuat sistem keamanan mereka.**

In what section of the report can you find a high-level overview of the assessment results including some comparisons of weekly performance?

Answer: **Cyber Hygiene Report Card**

Where can you find a detailed list of findings and recommend mitigations for each vulnerability?

Answer: **Appendix C**

What allows you to easily open the results of the scan into a spreadsheet or other tabular document?

Answer: **Di Appendix G, Comma-Separated Values (CSV).**

Step 2: Review the Cyber Hygiene Report Card.

Look at the Cyber Hygiene Report Card. This provides a high-level summary of the results of the assessment. This organization is scanned weekly, so there is some trend information that is supplied with the results of the current scan.
What percent of the scanned hosts were found to be vulnerable? How does this compare to the previous scan?

Answer: **Sebanyak 10% atau 393 host terdeteksi rentan, dengan penurunan jumlah sebesar 44 host dibandingkan dengan pemindaian sebelumnya.**

Vulnerabilities are classified by severity. Which level of severity represents the highest number of newly vulnerable hosts?

Answer: **Sebanyak 108 host tambahan baru diidentifikasi memiliki kerentanan tingkat keparahan sedang.**

Which class of vulnerability requires the most time for the organization to mitigate?

Answer: **Diperlukan waktu rata-rata 158 hari bagi organisasi untuk mengurangi kerentanan tingkat menengah.**

The scan included 293,005 IP addresses, but assessed only 3,986 hosts. Why do you think this is?

Answer: **Organisasi Sampel memiliki akses ke total 293.005 alamat, namun saat dilakukan pemindaian, hanya 3.986 alamat yang aktif dan dapat diakses untuk pemindaian.**

Step 3: Review the Executive Summary.

Go to the Executive Summary. Read this section and answer the following questions.
What two major functions did the assessment include, and which hosts did it assess?

Answer: **Penilaian dilakukan dengan memetakan jaringan untuk mengidentifikasi host dan informasi terkait lainnya, serta menilai kerentanan host yang dapat diakses melalui internet yang ditemukan selama proses pemetaan.**

How many distinct types of vulnerabilities were identified?

Answer: **63**

Of the top five vulnerabilities by occurrence, what was common system or protocol was most often found to be vulnerable?

Answer: **Sertifikat SSL dan rangkaian sandi.**

Of the top five categories by degree of risk, which vulnerabilities appear to be related to a specific piece of network hardware? What is the device?

Answer: **MikroTik Router OS 6.41.3 SMB dan MikroTik RouterOS HTTP Server Arbitrary. Ini adalah router MikroTik**.

Search the web on “MikroTik Router OS 6.41.3 SMB.” Locate the CVE entry for this vulnerability on the National Vulnerability Database (NVD) website. What is the CVSS base score and severity rating?

Answer: **CVSS base score 9.8, rating critical (CVE-2018-7445).**

Locate the full disclosure report for this CVE by searching on the web or clicking a reference link. In the full disclosure report, what are two ways of mitigating the vulnerability?

Answer: **Router OS harus diperbarui ke versi 6.41.3 atau yang lebih tinggi, atau layanan Server Message Block (SMB) harus dinonaktifkan.**

What type of vulnerability is this, and what can an attacker do when it is exploited?

Answer: **Ini adalah buffer overflow. Penyerang dapat dengan mudah menjalankan kode sistem karena tidak diperlukan autentikasi pengguna untuk memanfaatkannya.**

What should the Sample Organization have done to prevent this critical vulnerability from appearing on their network?

Answer: **Mereka sebaiknya mengikuti rekomendasi produk untuk perangkat keras jaringan yang mereka gunakan. Setelah diberi tahu tentang kerentanan tersebut, mereka seharusnya segera memperbarui versi RouterOS.**

Step 4: Review assessment methodology and process.

It is important to evaluate the methodology that was used to create a vulnerability assessment to determine the quality of the work that was done. Review the material in that section of the report.
In the Process section, the report mentions an IP network from which the scan was performed. What is the IP network, and to whom is it registered? Why is important to tell this to Sample Organization?

Answer

64.69.57.0 /24 . Berbagai situs pencarian alamat IP melaporkan bahwa jaringan IP ini terdaftar di Departemen Keamanan Dalam Negeri AS. Karena proses penilaian kerentanan melakukan pemindaian mendalam pada jaringan organisasi, hal ini dapat diartikan sebagai serangan pengintaian dari pelaku ancaman. Organisasi dapat secara tidak sengaja mencoba mengurangi ancaman dengan memblokir alamat IP di jaringan tersebut di tepi jaringan. Selain itu , agar pemindaian berhasil, alamat dari jaringan ini mungkin perlu diizinkan aksesnya melalui firewall untuk koneksi yang berasal dari luar jaringan.

What qualifies a computer to be designated as a host for the purposes of this report?

Answer: **Host didefinisikan sebagai perangkat yang memiliki alamat dan setidaknya satu layanan yang terbuka atau aktif.**

Which tool did the scan use for network mapping? Which tool was used for vulnerability assessment?

Answer: **Nmap digunakan untuk pemetaan jaringan dan Nessus digunakan untuk pemindaian kerentanan.**

Who offers the Nessus product, and what is the limitation of the freely downloadable version of Nessus?

Answer: **Tenable menyediakan produk Nessus. Versi gratisnya terbatas untuk memindai 16 alamat IP saja.**

Vulnerabilities with what range of CVSS scores are labelled as being of “High” severity?

Answer: **Kerentanan dengan skor dasar CVSS 7.0-10.0**

Step 5: Investigate detected vulnerabilities.

Go to section 7 of the report and locate Table 6. The Vulnerability Names consist of a standard descriptive phrase. Select a description and search for it on the web. You should see a link to tenable.com for each of them. Tenable maintains reference pages for the vulnerabilities that can be detected by Nessus.

a. Open the reference page for the vulnerability and review the information that is provided to you by Tenable. Read the synopsis and description for the vulnerability. Some reference pages provide suggested mitigation measures.

b. Select three of the vulnerabilities from the top vulnerabilities list and repeat this process. Review the vulnerability, CVE number, description, and mitigation measures, if any. Investigate the vulnerability further if you are interested.

Step 6: Investigate vulnerability mitigation.

Go to Appendix C of the report. Mitigation techniques are listed for many of the detected vulnerabilities. Answer the following questions.
What is the IP address of the host that is running a vulnerable PHP service? Why do you think this vulnerability exists on this host?

Answer: **Host xx124.231 perlu memperbarui perangkat lunaknya. Ternyata, layanan manajemen patch dan pembaruan tidak diterapkan pada host tersebut.**

What should be done to mitigate this vulnerability?

Answer: **Dengan memperbarui perangkat lunak layanan PHP ke versi 5.6.34 atau lebih tinggi.**

There are many problems that are associated with SSL. What are some of the mitigation measures that are recommended in the report?

Answer:

- **Mewajibkan penggunaan SSL untuk beberapa jenis protokol.**
- **Mengakuisisi atau menghasilkan sertifikat yang sesuai untuk layanan.**
- **Mengganti sertifikat yang telah kedaluwarsa.**
- **Mengatur aplikasi agar menggunakan kata sandi dengan tingkat kekuatan yang memadai.**
- **Mengganti SSL versi 2.0 atau 3.0 dengan TLS versi 1.1 atau yang lebih baru.**

Reflection Questions

1. Describe the vulnerability assessment that was conducted by NCCIC, including how it was performed, the tools used and a brief description of the results.

   Answer: **NCCIC menawarkan layanan pemindaian kerentanan secara gratis untuk organisasi pemerintah dan sektor swasta yang memenuhi syarat. Pemindaian dilakukan secara remote dan berkala. Hasil pemindaian dilaporkan kepada penerima manfaat. Laporan tersebut dapat digunakan untuk mengidentifikasi kerentanan, menyiapkan tren dan pembaruan mingguan, serta memberikan panduan untuk mitigasi kerentanan. NCCIC memanfaatkan Nmap untuk membuat peta jaringan yang mengidentifikasi host, dan Nessus untuk memindai host yang teridentifikasi guna mencari kerentanan. Laporan tersebut mencakup berbagai detail, tabel, dan grafik untuk membantu menyampaikan masalah keamanan jaringan yang memerlukan perhatian kepada penerima manfaat. Setiap kerentanan dievaluasi berdasarkan tingkat keparahan yang ditentukan oleh skor CVSS.**

   How are the Vulnerability names useful for further investigation?

   Answer: **Nama kerentanan ini sesuai dengan referensi yang dikelola oleh Tenable, perusahaan yang menyediakan Nessus. Referensi dari Tenable memberikan rincian tambahan tentang kerentanan tersebut dan sering kali menyertakan tautan ke sumber lain untuk informasi lebih lanjut. Selain itu, referensi Tenable juga menyertakan tautan ke spesifikasi CVE terkait kerentanan tersebut dan menyediakan vektor CVSS untuk kerentanan yang sama.**

2. Provide three actions you could take based on the information provided in a Cyber Hygiene report.

   Answer:

   - **Memanfaatkan laporan untuk menemukan kerentanan serius yang perlu ditangani dengan segera.**
   - **Menentukan host yang perlu langkah mitigasi untuk menangani kerentanan, terutama jika host tersebut memiliki beberapa kerentanan.**
   - **Mendeteksi kerentanan yang ada di banyak host dalam jaringan.**
   - **Mengusulkan solusi terpusat, seperti sistem manajemen patch, untuk mengurangi kemungkinan munculnya kerentanan kritis atau yang memiliki tingkat keparahan tinggi dalam jaringan.**