## Lab 19: Perform a network vulnerability scan with OpenVAS

### Scenario

PrimeNova, a regional financial services company, has suffered a severe computer and system breach. A hacker exploited a vulnerability in its customer management software, compromising all sensitive customer data, including account details and transaction history. The company heavily depends on its compliance reporting and customer relationship management software, which makes it a critical asset. In response to the incident, the company initiated a thorough investigation to discover and fix vulnerabilities in its computers and systems to prevent this type of attack in the future.

### Solution

The company hires you as a certified cybersecurity practitioner to perform a vulnerability analysis using advanced assessment tools. As an ethical hacker, your task is to simulate a real-world attack scenario to identify weaknesses in the computer systems. You use OpenVAS, a highly regarded open-source vulnerability scanner, to achieve this.

In this lab, you will systematically scan the company’s systems to identify vulnerabilities such as unpatched software, open ports, insecure configurations, and outdated services.

OpenVAS is a robust framework comprising multiple services and tools designed to deliver comprehensive vulnerability scanning and management solutions. It supports both unauthenticated and authenticated testing, as well as a variety of high-level and low-level internet and industrial protocols, and it optimizes performance for large-scale scanning. Additionally, it incorporates a versatile internal programming language for implementing custom vulnerability tests. The security scanner is supplemented by an updated feed of over 50,000 Network Vulnerability Tests (NVTs), ensuring thorough and up-to-date assessments.

The findings from the assessment will help the company prioritize and remediate critical vulnerabilities, strengthening its overall security posture.

**Note:** In this lab, the target IP address we use is **192.168.56.106** of Windows Server 2025. Do not use this lab IP address. Use your virtual machine IP address at the time when you are performing this lab.

|  |
| --- |
| 1. Start your **PattotOS** and **Windows Server 2025** virtual machines. Switch to ParrotOS and open the **Terminal**. Then, execute the **sudo su** command to run programs with root user privileges.    2. Execute the following command: **apt-get update && apt-get upgrade -y** to automatically update the package index and upgrade all installed packages to their latest versions.    3. Execute the following command: **apt-get install docker.io -y** to install Docker in the ParrotOS.    4. Execute the following command: **docker run -d -p 443:443 –-name openvas mikesplain/openvas** to launch OpenVAS.    5. Open any browser in the ParrotOS. Type the following **https://127.0.0.1/** to go to the OpenVAS login page. Log in with username and password **admin**/**admin**. Click on the **Login** button. If a **Warning page** appears. Then Click on the **Advanced.** Click on the **Accept the Risk.** Then Click on the **Continue**.    6. The **OpenVAS** page appears. Click on the **Scans**. Then Click on the **Tasks**. If you see a **Welcome to scan task management!** pop-up window, close it.    7. Hover over the **wand** icon. Then Click on the **Task Wizard**.    8. The **Task Wizard** window opens; enter the target machine **IP address** in the **IP address or hostname** field. Then Click on the **Start Scan** button.    9. The task will appear under the **Tasks** section, and OpenVAS will begin scanning the target IP address. Wait until the status changes from **Requested** to **Done**.  Once the scan is complete, Click the **Done** button under the **Status** column to view the vulnerabilities detected in the target system. The scanning process may take some time.    10. Click on the **Scans.** Then Click on the **Results**.    11. The Results section lists the detected vulnerabilities, their severity, and the port numbers on which they operate. The results may vary when performing this task. Click on any vulnerability in the **Vulnerability** column to obtain more information.    12. Detailed information about the selected vulnerability will be displayed.    12. Now compare the results of the vulnerability assessment report of Windows Server 2025 by enabling Windows Firewall. Switch back to the **Windows Server 2025**. Go to the **Control Panel** **→** **System and Security** **→** **Windows Defender Firewall** **→** **Turn Windows Defender Firewall on or off**, and enable **Windows Defender Firewall**. Then Click on the **OK** button, and after that, close the **Control Panel** window.    13. Repeat the Steps 6 to 9 again. Click on the **Scans.** Then Click on the **Reports**. The target machine’s scan results remain unchanged before and after enabling the Windows Firewall, indicating that the target system is still vulnerable to attack even with the firewall enabled. |