Forum:Hack Forums

Thread: Vulnerability assessments for newbs

Perfect - *May 18, 2024, 7:20 pm*

Conducting a Vulnerability Assessment with Nmap and OpenVAS

Introduction

In this tutorial, we'll cover how to perform a basic vulnerability assessment using Nmap and OpenVAS. This is an essential skill for any ethical hacker or cybersecurity enthusiast. Vulnerability assessments help identify security weaknesses in a network, allowing you to take proactive measures to secure your systems.

Tools You'll Need

- Nmap: A powerful network scanning tool.
- OpenVAS: An open-source vulnerability scanner.

Step-by-Step Guide

1. Install Nmap:
First, you'll need to install Nmap. On Linux, you can do this using your package manager. For example:

```
sudo apt-get install nmap
```

On Windows, download the installer from the Nmap website.

2. Install OpenVAS:
OpenVAS can be installed from the Greenbone Community Edition. Follow the installation instructions for your operating system.

3. Run an Initial Nmap Scan:
Use Nmap to perform a network scan and identify open ports on your target system. Open a terminal and run:

```
nmap -sV -p- <target_ip>
```

This command scans all ports (-p-) and attempts to identify services running on those ports (-sV).

4. Analyze Nmap Results:
Review the output from Nmap to identify potential entry points. Look for services that may have known vulnerabilities.

5. Configure OpenVAS:
OpenVAS requires some initial setup. Run the following commands to set it up on Linux:

sudo gvm-setup
sudo gvm-start

Access the OpenVAS web interface by navigating to https://<your_ip>:9392 in your browser.

6. Create a New Scan Task in OpenVAS:
Log in to the OpenVAS web interface. Go to “Scans” > “Tasks” and create a new task. Enter the target IP address and choose a scan configuration.

7. Run the OpenVAS Scan:
Start the scan and wait for it to complete. This may take some time, depending on the complexity of the target system.

8. Review the Scan Report:
Once the scan is complete, OpenVAS will generate a detailed report highlighting any vulnerabilities found. Review this report to understand the risks and plan your remediation steps.

Conclusion

By combining the power of Nmap and OpenVAS, you can perform thorough vulnerability assessments to help secure your network. Regularly scanning your systems and addressing any vulnerabilities found is a crucial part of maintaining a strong security posture.

Remember to always have permission before scanning any network or system. Use these tools ethically and responsibly to contribute positively to the cybersecurity community.

Helpful Resources:

Nmap Documentation - Comprehensive guide and manual for using Nmap.

OpenVAS Documentation - Official documentation for setting up and using OpenVAS.

Syndicate - *May 18, 2024, 7:24 pm*
Very nice thread Perfect! You should have submitted this towards your blog posts. If you get 5 approved blogs, then you will receive an award :)

Perfect - *May 18, 2024, 7:47 pm*
(May 18, 2024 07:24 PM)Syndicate Wrote: *[CITE]* Very nice thread Perfect! You should have submitted this towards your blog posts. If you get 5 approved blogs, then you will receive an award :)
I’ve never posted a blog on here hmm

Syndicate - *May 18, 2024, 8:48 pm*
(May 18, 2024 07:47 PM)Perfect Wrote: *[CITE]* I’ve never posted a blog on here hmm
I think it's a great idea to earn a free award and help out members in the process. ?

elrode - *May 18, 2024, 10:37 pm*

ggooonnnnnnnnnkkkkkkkkkkkkk chese buger ham buger whopper big mack [warn]

Perfect - *May 19, 2024, 6:56 am*

(May 18, 2024 10:37 PM)elrode Wrote: [CITE] ggooonnnnnnnnnkkkkkkkkkkkkk chese buger ham buger whopper big mack [warn]

Why my post lmao ?

You good bro !