Network Vulnerability Discovery Lab

Contents

Lab Objectives and Setting

Overview

Vulnerability discovery (or vulnerability scanning) is one of the most important parts of proactive defense. With regular and periodical vulnerability scan, system and network weaknesses can be identified in advance and many security incidents can thus be avoided. In this lab, you will learn to use vulnerability scanning tools to collect and identify the operating system (OS) information and the system vulnerabilities of a Linux server. You will learn the basic usage of Nmap on port scanning, service and OS detection, as well as advanced usages such as using Nmap scripts to detect the vulnerability. You will also learn how to use OpenVAS Web GUI to conduct a comprehensive vulnerability scan.

Objectives

Upon completion of this lab, students will be able to:

- Practice the basic use of Nmap on host reconnaissance
- Apply Nmap and OpenVAS to detect host vulnerability
- Develop in-depth understanding in vulnerability scanning
- Recognize the difference between Nmap and OpenVAS scan

Prerequisites

- Practical experience with SSH and basic Linux commands;
- Basic knowledge of network protocols.

EZSetup

EZSetup is a Web application capable of creating various user-defined cybersecurity practice environments (e.g., labs and competition scenarios) in one or more computing clouds (e.g., OpenStack or Amazon AWS). EZSetup provides a Web user interface for practice designers to visually create a practice scenario and easily deploy it in a computing cloud, which allows for customization and reduces overhead in creating and using practice environments. End users are shielded from the complexity of creating and maintaining practice environments and therefore can concentrate on cybersecurity practices. More information about EZSetup can be found at https://promise.nexus-lab.org/platform/.

Environment Setting

In this lab, students can access two virtual machines (VM) in the cloud from EZSetup. One acts as the scanner, equipped with OpenVAS and Nmap vulnerability scanners, and the other one is a vulnerable machine with a lot of vulnerabilities. The network topology for this lab is provided in **Error! Reference source not found.**.

The access information about these two virtual machines is provided in Table 1. Please refer to the EZSetup dashboard for the actual public IP addresses and passwords.

Table 1 VM properties and access information

Name	Image	RAM	VCPU	Disk	Login account
Scanner	vulscan-scanner	1GB	1	30GB	See EZSetup
Vulnerable	vulscan-vulnerable	1GB	1	30GB	name: msfadmin password: msfadmin

Note: Instructors who deploy this lab first need to go to the main interface of the chosen cloud, e.g., OpenStack horizon page, and access the console link of the Vulnerable VM (The link might be ready minutes after the lab is successfully deployed). In the console, instructors need to type **Control-D** key combination in order to resume the system boot, after which students can access the Vulnerable VM and perform all the tasks.

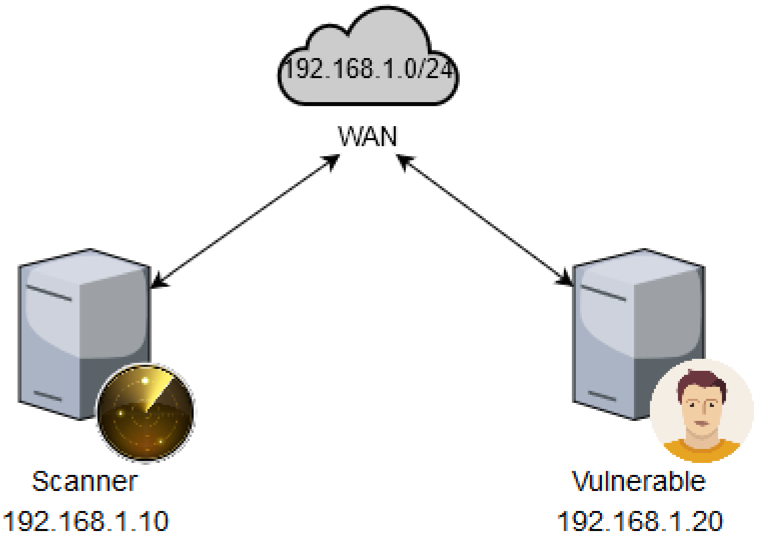

Figure 1 Lab network topology

License

1. Network and Host Scan Using Nmap

Nmap (Network Mapper) is a free and open source utility for network discovery and security auditing. It is widely used during the initial stages of penetration testing. Nmap can be used for displaying exposed ports or services on a target machine along with other useful information such as the MAC address and OS detection.

To scan the entire network, the following command can be used.

```
nmap -sP 192.168.1.0/24
```

Here -sP refers to Nmap ping scan and this command will return all live hosts in the network. To conduct an Nmap TCP scan against the Vulnerable VM, the following command can be used.

```
nmap -sT 192.168.1.20
```

Here -sT refers to Nmap TCP connect port scan and all the open TCP ports will be displayed by issuing the above command. For remote OS detection, -O option can be used, for instance,

```
nmap -O 192.168.1.20
```

One thing needs to note for the above command is that **root privilege** is usually required in order to get the remote OS information, thus sudo is needed before typing nmap. To detect the services running on the target machine, -sV option can be utilized, for example,

```
nmap -sV 192.168.1.20
```

The above command will return the information about the services running on the Vulnerable VM as well as their version information. These will help administrators to identify possible vulnerabilities in it.

Tasks:

Scan the network and get the detailed information of the Vulnerable VM using Nmap tool on the Scanner VM.

A. Use Nmap quick ping scan to identify any live hosts in the network 192.168.1.0/24 and then list them here.

B. Use Nmap TCP scan against the Vulnerable VM to get its open TCP ports. List the command and results here.

C. Identify the version of Linux that the Vulnerable VM is running on using Nmap operating system scan command.

D. Detect the services along with their version numbers running on the Vulnerable VM and list the r esult here. Identify any vulnerable services by checking the detected service (software) version on national vulnerability database https://nvd.nist.gov.

2. Script Scan with Nmap

Nmap Scripting Engine (NSE) is one of Nmap's most powerful and flexible features. It allows users to write (and share) simple scripts to automate a wide variety of complex networking tasks, e.g., with NSE, we can launch more sophisticated service version detection, handle more demanding vulnerability checks, detect more complex worms and backdoors, and even exploit vulnerabilities, which are valuable for penetration testers.

By using --script option in nmap command, we can easily load any particular script in nmap scan, for instance,

```
nmap --script=default 192.168.1.20
```

Here --script=default is equivalent to -sC option, which enables the most common scripts to do the host-based scan. Different script categories are created to meet different scan purposes, e.g., with --script=vuln, we can load all scripts in the vulnerability scanning category to identify more vulnerabilities. With --script=brute, and --script=exploit, we are able to guess authentication credentials and exploit the detected vulnerabilities against a particular machine.

Tasks:

Advanced vulnerability scanning using Nmap script engine (NSE).

A. Use Nmap -sC option to enable the most common scripts to scan against the Vulnerable VM and list the scan result here.
B. Use Nmap --script=vuln option to load all scripts in vuln category to scan against the Vulnerable VM to get all of its vulnerabilities.
C. Use Nmap brute force script category to perform brute force attacks to guess authentication credentials of the Vulnerable VM.
D. Use Nmap exploit script category to have Nmap actively exploit the detected vulnerabilities and post result here.

3. Vulnerability Scan with OpenVAS

OpenVAS scanner is a comprehensive vulnerability assessment system that can detect security issues in all manner of servers and network devices. OpenVAS is preinstalled on the scanner machine and offers a nice web GUI for easy vulnerability scan. We can access the OpenVAS web GUI through the Scanner VM’s public IP address. Note that OpenVAS runs on port 4000, assuming that the Scanner VM has a public IP address of 172.20.15.134, then the address for accessing the web GUI will be

https://172.20.15.134:4000

The default username and password for the OpenVAS web GUI is admin and admin. After you have successfully logged in, you will be able to see the main interface of OpenVAS. Go to Scans -> Tasks tab to start your vulnerability scan.

Tasks:

Scan system vulnerabilities of the Vulnerable VM using OpenVAS

A. What vulnerabilities can you find on the Vulnerable VM through OpenVAS quick scan option?

B. What is the difference between full and fast scan config and full and very deep scan config? Verify your assumption by showing the scan results against the Vulnerable VM using these two scan configs.

C. How OpenVAS classify the severity of the detected vulnerabilities?

D. Compare the vulnerability scanning results generated by Nmap and OpenVAS and describe the difference. Then give your insights about why they have such difference.

Assignment

Complete all the tasks and save your answer (with screenshots) to each of the tasks into a PDF file. Submit the PDF file.