NMAP

Nmap, or network mapper, is a toolkit for functionality and penetration testing throughout a network, including port scanning and vulnerability detection and assessment.

Nmap scripting engine (NSE) Script is one of Nmap's most popular and powerful capabilities. These Nmap vulnerability scan scripts are used by hackers to examine commonly known vulnerabilities.

Common Vulnerabilities and Exposures (CVE); is a database of publicly disclosed data security issues. It serves as a reference model for detecting vulnerabilities and threats related to the security of information systems.

In this article, we'll look at how to use Nmap for Vulnerability Scan.

Let's get started!

map Installation

Nmap is pre-installed in almost every Linux distribution. In case it's missing, you need to install it manually. It can be easily installed with the following command.

apt-get install nmap

And you can also install it by cloning the official git Repository.

git clone https://github.com/nmap/nmap.git

Next, navigate to that directory and install the requirements using the below commands.

. /configure

make

make install.

This software's most recent version and binary installers for Windows, macOS, and Linux (RPM) are:

Vulnerability scan with Nmap

Nmap-vulners, vulscan, and vuln are the common and most popular CVE detection scripts in the Nmap search engine. These scripts allow you to discover important information about system security flaws.

Nmap-vulners

One of the most well-known vulnerability scanners is Nmap-Vulner. Let's look at how to set up this tool as well as how to run a basic CVE scan. The Nmap script engine searches HTTP responses to identify CPEs for the given script.

Installation

To install the Nmap-vulners script, navigate to the Nmap scripts directory using the following command.

cd /usr/share/nmap/scripts/

The Next step is to clone the git repository.

git clone https://github.com/vulnersCom/nmap-vulners.git

After cloning the git repository, you won't need to do anything else for the configuration. The tool will be automatically installed.

And if you want to see the NSE scripts present in Nmap-vulners database, use ls command. It will display all the. nse extension scripts on the terminal.

Usage

It's easy to use NSE scripts. Simply pass the -script argument to our Nmap command to instruct what NSE script to use.

nmap -sV --script vulners [--script-args mincvss=<arg_val>] <target>

Don't forget to pass "-sV" argument while using NSE scripts. Nmap-vulners will be unable to access the Vulners exploit database if it does not receive any version information from Nmap. So, the -sV parameter is required all the time.

Example command

The syntax is quite straightforward. Just call the script with the "–script" option and specify the vulners engine and target to begin scanning.

nmap -sV --script nmap-vulners/ <target>

nmap -sV --script nmap-vulners/ <target>

If you wish to scan any specific ports, just add "-p" option to the end of the command and pass the port number you want to scan.

nmap -sV --script nmap-vulners/ <target> -p80,223

Nmap – vuln

NSE scripts are classified according to a set of predetermined categories to which each script belongs. Authentication, broadcast, brute force, intrusive, malware, safe, version, and vuln are some of the categories

The scripts which come under the "vuln" category look for specific known vulnerabilities and only report back if any are identified in the target system.

nmap -sV --script vuln <target>

Nmap-vulscan

Vulscan is an NSE script that assists Nmap in detecting vulnerabilities on targets based on services and version detections. vulscan is like a module for Nmap that transforms it into a vulnerability scanner. The Nmap option -sV allows for per-service version detection, which is used to identify potential exploits for the detected vulnerabilities in the system.

Currently, the following pre-installed databases are available:

- exploitdb.csv
- osvdb.csv
- securitytracker.csv
- openvas.csv
- scipvuldb.csv
- xforce.csv
- securityfocus.csv
- cve.csv

Installation

To install the Vulscan, First, go to the Nmap scripts directory by using the following command.

cd /usr/share/nmap/scripts/

The Next step is to clone the git repository and install all the requirements.

git clone https://github.com/scipag/vulscan.git

ln -s `pwd`/scipag_vulscan /usr/share/nmap/scripts/vulscan
Vulscan makes use of pre-configured databases saved locally on our machine. To update the database, go to the updater directory. Type the following command into a terminal to navigate to the updater directory.
cd vulscan/utilities/updater/

Next, change the permissions of the file to be run in the system.
chmod +x updateFiles.sh

And finally, update the exploit databases with the below command.
./updateFiles.sh

Usage
Let's use vulscan to do a Nmap vulnerability scan. The vulscan NSE script can be used in the same way as nmap-vulners.
nmap -sV --script vulscan <target>

By default, Vulscan will search all of the databases simultaneously. It takes a lot of time to query information using all the databases. Using the vulscandb parameter, you can pass only one CVE database at a time.
--script-args vulscandb=database_name

Example Command
nmap -sV --script vulscan --script-args vulscandb=exploit.csv <target> -p 80,233

Individual vulnerability Scanning
Individual vulnerability scans can also be performed utilizing scripts within each category. Here is a list of all 600+ Nse Scripts and 139 NSE Libraries
Examples

- http-csrf: Cross-Site Request Forgery (CSRF) vulnerabilities are detected by this script.

nmap -sV --script http-csrf <target>
Copy

- http-sherlock: Intends to exploit the "shellshock" vulnerability in web applications.

nmap -sV --script http-sherlock <target>
Copy

- http-slowloris-attack: Without launching a DoS attack, this script checks a web server or a target system for vulnerability to perform the Slowloris DoS attack.

nmap -sV --script http-slowloris-check <target>

- http-vmware-path-vuln: VMWare ESX, ESXi, and Server are all tested for a path-traversal vulnerability.

nmap -sV --script http-vmware-path-vuln <target>

- http-passwd: Attempts to retrieve /etc/passwd or boot.ini to see if a web server is vulnerable to directory traversal.

nmap -sV --script http-passwd <target>

- http-internal-ip-disclosure: When sending an HTTP/1.0 request without a Host header, this check determines if the web server leaks its internal Ip Address

nmap -sV --script http-internal-ip-disclosure <target>

- http-vuln-cve2013-0156: Detects Ruby on Rails servers that are vulnerable to Dos attacks and command injection.

nmap -sV --script http-vuln-cve2013-0156 <target-address>

Burp Suite

How to use Burp Suite:

1. Start Burp Suite: Double-click the Burp Suite icon to launch the application. It may take a few moments to load.
2. Configure your browser to use Burp Suite: By default, Burp Suite runs on port 8080. To configure your browser to use Burp Suite, go to your browser's network settings and set the HTTP and HTTPS proxy to "localhost" with port "8080".
3. Access your target application: Navigate to the one you want to test.
4. Capture traffic: Once you access the target application, Burp Suite will start capturing the traffic. You can view the captured traffic in the "Proxy" tab of Burp Suite.
5. Inspect requests and responses: In the "Proxy" tab, you can view and inspect the requests and responses. You can use this information to identify potential vulnerabilities.
6. Send submissions to the Intruder: To send a request to the Intruder, right-click on demand in the "Proxy" tab and select "Send to Intruder." This will open the Intruder tab.
7. Configure the Intruder: In the Intruder tab, you can configure the attack type, payload, and other settings. For example, you can use the "Sniper" attack type to test a single parameter or the "Battering Ram" attack type to test multiple parameters.
8. Start the attack: Once you have configured the Intruder, click on the "Start Attack" button to begin the attack.
9. Analyze the results: After the attack, you can analyze the results in the "Intruder" tab. You can use this information to identify potential vulnerabilities.
10. Generate a report: Once you have completed your testing, you can use the "Report" tab to generate a detailed description of your findings.
11. That's it! This is just a basic overview of how to use Burp Suite, and there are many more advanced features and techniques that you can explore as you become more familiar with it.

Metasploit

Metasploit is an open-source penetration framework that is used by security engineers to find vulnerabilities on servers and networks. Once vulnerabilities are found the user can take that information to address the weaknesses within a system and find a solution. Metasploit is easily
customizable and can be used with most operating systems because it is open-source.

Metasploit has over 1677 exploits organized over 25 platforms. THis framework consists of 5 parts which are:

- Interfaces- different platforms used to access the metasploit framework
- Libraries- contains different functions that allow users to run exploits without the need of having to write additional code themselves
- Modules- software used to perform task like target exploitation and scanning
- Tools & Plugins - an addon to the framework that is used to extend its functionality

According to “Simplilearn.com” Metasploit provides you with varied use cases, and its benefits include:

Open Source and Actively Developed – Metasploit is preferred to other highly paid penetration testing tools because it allows accessing its source code and adding specific custom modules.

Ease of Use – it is easy to use Metasploit while conducting a large network penetration test. Metasploit conducts automated tests on all systems in order to exploit the vulnerability.

Easy Switching Between Payloads – the set payload command allows easy, quick access to switch payloads. It becomes easy to change the meterpreter or shell-based access into a specific operation.

Cleaner Exits – Metasploit allows a clean exit from the target system it has compromised.

Friendly GUI Environment – friendly GUI and third-party interfaces facilitate the penetrate testing project.

If you are using kali Linux metasploit is preinstalled in your system so there is no need to download it. Github helps to download and install metasploit on both windows and Linux systems.

Basic Commands for the Msfconsole

- Help- will show you every command that is available within the msfconsole
- Show exploits- shows you various exploits that you are able to execute

- Set TARGET- let’s you choose a specific target application and OS when permitted by exploits
- Exit- allows u to exit the metasploit console