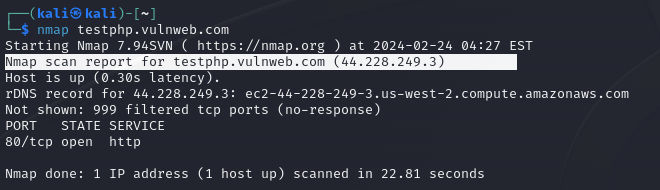
**Nmap: Scan Ports to Detect Services and Vulnerabilities**

* This tutorial explains how to use Nmap to find servers and vulnerabilities behind ports.
* Nmap is one of the most helpful networking tools allowing you to map networks, discover hosts, scan ports, diagnose network problems, detect and exploit vulnerabilities, and more.
* This tutorial focuses on the services version and vulnerabilities detection techniques. Readers unfamiliar with Nmap may prefer to start by reading our  [Nmap basics tutorial](https://linuxhint.com/nmap_basics_tutorial/).

**Scan Ports to Detect Services With Nmap**

Firstly, we will find the IP address of the website .

**Command: nmap testphp.vulnweb.com**



The first section of this tutorial explains how to detect services and their software version listening on open ports.

**Command: nmap -F 44.228.249.3**

A screenshot of a computer program

Description automatically generated

The user knows port 80 is open.

To detect software and versions, the -sV (Version) flag can be passed, as shown in the screenshot below. Wherein you can see, nginx 1.19.0 is detected

**Command : nmap -sV 44.228.249.3**

A screenshot of a computer program

Description automatically generated

The next section of this tutorial describes NSE (Nmap Scripting Engine) techniques. This practical example shows which the –script flag is implemented to incorporate the banner grab script into the scan.

**Command: nmap -p 21 –script=banner 44.228.249.3**

A screenshot of a computer

Description automatically generated

To end this section and continue with vulnerability scan types, the practical example below shows the -O (Operating System) flag implementation to guess the target operating system.

**Command: sudo nmap -O 44.228.249.3**

A screenshot of a computer

Description automatically generated

**Detecting vulnerabilities with NSE (Nmap Scripting Engine)**

The Nmap Scripting Engine is a set of scripts users can include in their scans, designed mainly to detect and exploit vulnerabilities. Users can also write their scripts for custom purposes.

The first step for the NSE scripts is to update the database, making sure Nmap is up to date with the latest vulnerabilities and techniques.

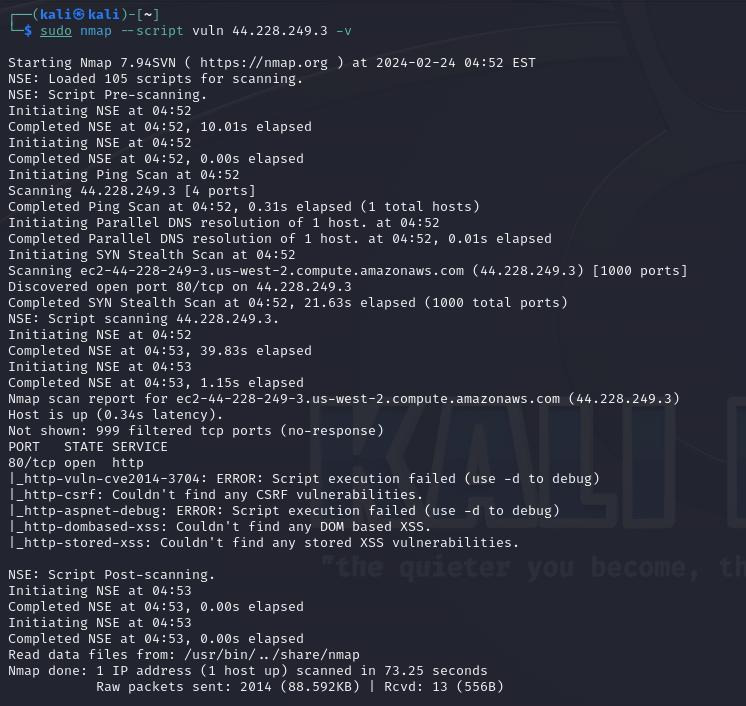
**To update NSE, run the following command: sudo nmap –script-updatedb**

**A screen shot of a computer

Description automatically generated**

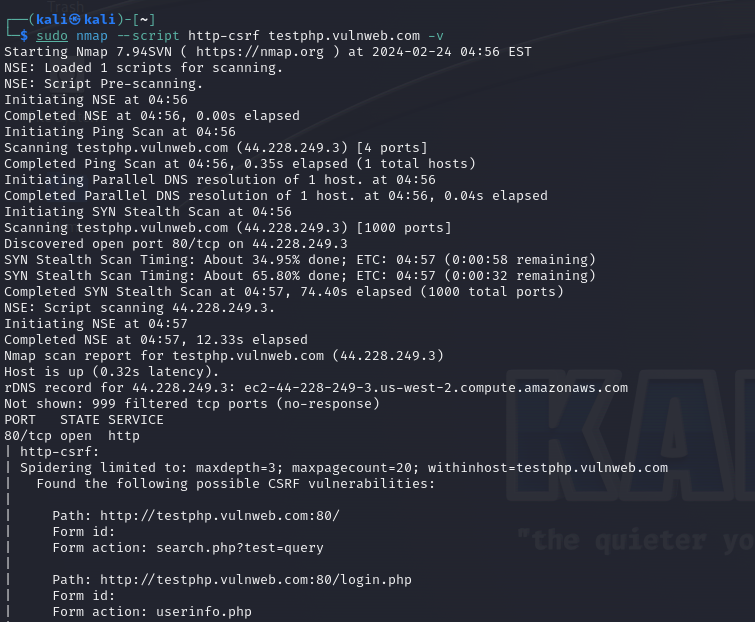
In the following example, the –script flag calls the scripts from the vuln category, scanning for around 150 popular vulnerabilities.

**Command: sudo nmap –script vuln 44.228.249.3 -v**

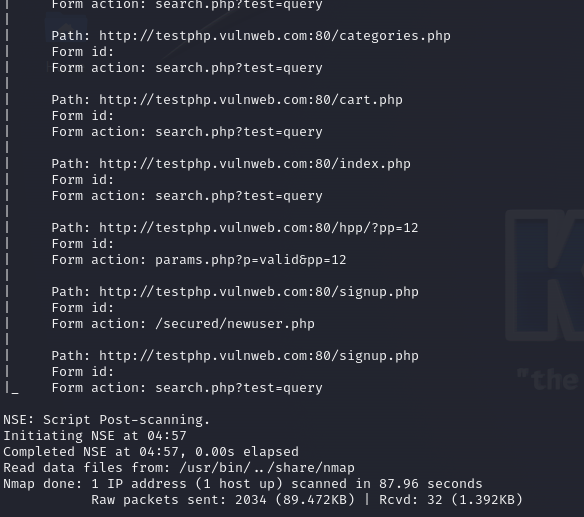


The http-csrf script allows users to scan websites to find csrf (Cross Scripting Request Forgery) vulnerabilities.

**Command: sudo namp –script http-csrf testphp.vulnweb.com -v**



As you can see below, if verbosity (-v) is instructed, Nmap prints the result of all checks it does against the website.



Users can implement wildcards to complete script names. In the following example, the user adds all http-related scripts or all scripts whose name begins with “http”, independently of how it continues.

**Command: sudo nmap –script “http\*” testphp.vulnweb.com -v**

A screenshot of a computer screen

Description automatically generated