**Using Nmap Scripting Engine**

*Instructions*

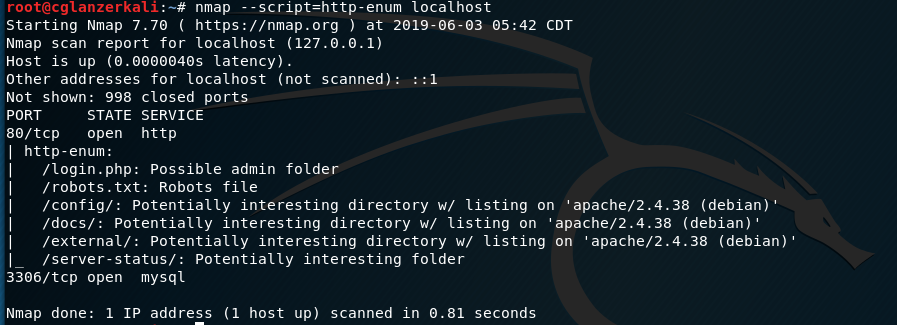
Use the Nmap Scripting Engine to conduct further reconnaissance on DVWA. Use (at a minimum) the following scripts:

* http-enum
* http-frontpage-login
* http-passwd
* http-sql-injection
* http-stored-xss.nse

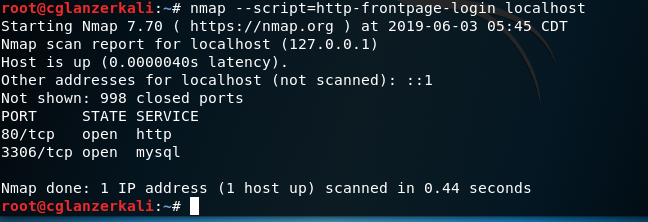
***\*hint\**** Some scripts may require arguments to successfully execute

*Output*

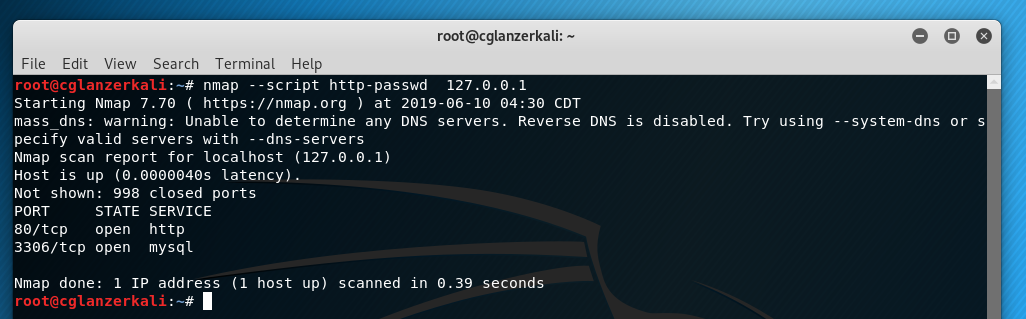
1. Take a screen shot showing each results
2. Describe the purpose of each script listed above?
   1. http-enum
      1. this script attempts to access two different random files in order to detect servers that don't return a proper 404 Not Found status… By default, only pages that return 200 OK or 401 Authentication Required are displayed



* 1. http-frontpage-login
     1. Checks whether target machines are vulnerable to anonymous Frontpage login.

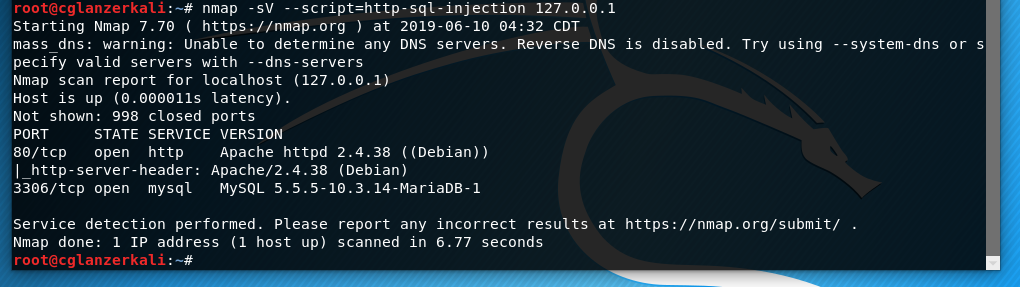


* 1. http-passwd
     1. Checks if a web server is vulnerable to directory traversal by attempting to retrieve /etc/passwd or \boot.ini.



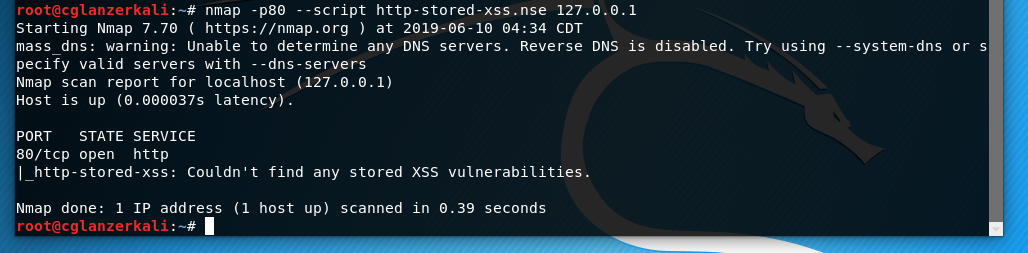
* 1. http-sql-injection

Spiders an HTTP server looking for URLs containing queries vulnerable to an SQL injection attack. It also extracts forms from found websites and tries to identify fields that are vulnerable.



* 1. http-stored-xss.nse

Unfiltered '>' (greater than sign). An indication of potential Cross Site Scripting (XSS) vulnerability.



1. What vulnerabilities did you find by running each script against a web server?

None

**Other than Http-enum none of these scripts provided any information beyond the normal nmap scan, unfortunately (did I do something wrong for frontpage login? I just followed the guide on nmap.org)**