$ sudo nmap teamnebulatest.us-east-1.elasticbeanstalk.com -script vuln -sS -P0 -D 62.232.12.8,ME,65.213.217.241

Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.

Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-14 16:14 EDT

Warning: 34.197.148.58 giving up on port because retransmission cap hit (10).

Nmap scan report for teamnebulatest.us-east-1.elasticbeanstalk.com (34.197.148.58)

Host is up (0.11s latency).

rDNS record for 34.197.148.58: ec2-34-197-148-58.compute-1.amazonaws.com

Not shown: 971 closed ports, 26 filtered ports

PORT STATE SERVICE

22/tcp open ssh

80/tcp open http

| http-aspnet-debug:

|\_ status: DEBUG is enabled

|\_http-csrf: Couldn't find any CSRF vulnerabilities.

|\_http-dombased-xss: Couldn't find any DOM based XSS.

| http-slowloris-check:

| VULNERABLE:

| Slowloris DOS attack

| State: LIKELY VULNERABLE

| IDs: CVE:CVE-2007-6750

| Slowloris tries to keep many connections to the target web server open and hold

| them open as long as possible. It accomplishes this by opening connections to

| the target web server and sending a partial request. By doing so, it starves

| the http server's resources causing Denial Of Service.

|

| Disclosure date: 2009-09-17

| References:

| http://ha.ckers.org/slowloris/

|\_ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750

|\_http-stored-xss: Couldn't find any stored XSS vulnerabilities.

111/tcp open rpcbind

Nmap done: 1 IP address (1 host up) scanned in 5553.00 seconds